

**IBM 4758 PCI Cryptographic Coprocessor  
Version 2: 4758-002 and 4758-023  
CCA User Defined Extensions  
Reference and Guide**

12-NOV-01, 14:10

**Note!**

Before using this information and the product it supports, be sure to read the general information under Appendix F, "Notices" on page F-1.

**Third Edition (October, 2001)**

IBM does not stock publications at the address given below. This and other publications related to the IBM 4758 Coprocessor can be obtained in PDF format from the Library page at <http://www.ibm.com/security/cryptocards>.

Reader's comments can be communicated to IBM by using the Comments and Questions Form located on the product Web site at <http://www.ibm.com/security/cryptocards>, or you can respond by mail to:

Department VM9A, MG81/204-3  
IBM Corporation  
8501 IBM Drive  
Charlotte, NC 28262-8563  
U.S.A.

IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 1999, 2001. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

|  |      |
|--|------|
| <b>About This Book</b> . . . . .   | xi   |
| Prerequisite Knowledge . . . . .   | xi   |
| Organization of This Book . . . . .                                      | xi   |
| Typographic Conventions . . . . .  | xiii |
| Related Publications . . . . .   | xiii |
| General Interest . . . . .   | xiii |
| CCA Support Program Publications . . . . .                               | xiii |
| Custom Software Publications . . . . .                                   | xiii |
| Cryptography Publications . . . . .                                      | xiv  |
| Other IBM Cryptographic Product Publications . . . . .                   | xvi  |
| Summary of Changes . . . . .   | xvi  |
| <br>   |      |
| <b>Chapter 1. Understanding the UDX Environment</b> . . . . .            | 1-1  |
| CCA Communication Structures . . . . .                                   | 1-7  |
| <br>   |      |
| <b>Chapter 2. Building a CCA User-Defined Extension</b> . . . . .        | 2-1  |
| Files You Use in Building a UDX . . . . .                                | 2-1  |
| Host Piece of a UDX . . . . .  | 2-3  |
| Coprocessor Piece of a UDX . . . . .                                     | 2-6  |
| <br>   |      |
| <b>Chapter 3. SCC Functions</b> . . . . .                                | 3-1  |
| Host-Side SCC API Functions . . . . .                                    | 3-1  |
| Coprocessor-Side SCC API Functions . . . . .                             | 3-1  |
| <br>   |      |
| <b>Chapter 4. Communications Functions</b> . . . . .                     | 4-1  |
| Header Files for Communications Functions . . . . .                      | 4-1  |
| Summary of Functions . . . . .   | 4-1  |
| BuildParmBlock - Build a Parameter Block . . . . .                       | 4-2  |
| Cas_proc_retc - Prioritize Return Code . . . . .                         | 4-6  |
| CSNC_SP_SCSRFBSS - Send a Request to the Coprocessor . . . . .           | 4-7  |
| CSUC_BULDCPRB - Build CPRB . . . . .                                     | 4-9  |
| CSUC_PROCRET - Prioritize Return Code . . . . .                          | 4-11 |
| FindFirstDataBlock - Search for Address of First Data Block . . . . .    | 4-12 |
| FindNextDataBlock - Search for Address of Next Data Block . . . . .      | 4-13 |
| find_first_key_block - Search for First Key Data Block . . . . .         | 4-14 |
| find_next_key_block - Find Address of Next Key Data Block . . . . .      | 4-15 |
| InitCprbParmPointers - Initialize CPRB Parameter Pointers . . . . .      | 4-16 |
| keyword_in_rule_array - Search for Rule Array Keyword . . . . .          | 4-17 |
| parm_block_valid - Examine and Verify a Parameter Block . . . . .        | 4-18 |
| rule_check - Verify Rule Array . . . . .                                 | 4-19 |
| saf_process_key_label - Process Key Label . . . . .                      | 4-23 |
| <br>   |      |
| <b>Chapter 5. Function Control Vector Management Functions</b> . . . . . | 5-1  |
| Header Files for Function Control Vector Management Functions . . . . .  | 5-1  |
| Summary of Functions . . . . .   | 5-1  |
| getSymmetricMaxModulusLength - Get RSA Key Length . . . . .              | 5-2  |
| isFunctionEnabled - Check Whether a Function is Enabled . . . . .        | 5-3  |
| <br>   |      |
| <b>Chapter 6. CCA Master Key Manager Functions</b> . . . . .             | 6-1  |
| Header Files for Master Key Manager Functions . . . . .                  | 6-1  |

|  |            |
|--|------------|
| Overview of the Coprocessor CCA Master Keys . . . . .                  | 6-1        |
| Location of the Master Keys . . . . .                                  | 6-2        |
| Initialization of the Master Key SRDI . . . . .                        | 6-2        |
| CCA Master Key Manager Interface Functions . . . . .                   | 6-3        |
| Common Entry Processing . . . . .                                      | 6-3        |
| Required Variables . . . . .   | 6-3        |
| Functions to Set and Manage the Master Key Values . . . . .            | 6-5        |
| Summary of Functions . . . . .   | 6-5        |
| clear_master_keys - Clear Master Key . . . . .                         | 6-6        |
| mkmCombineMKParts - Combine Master Key Parts . . . . .                 | 6-7        |
| mkmGenerateMKShares - Generate Master Key Shares . . . . .             | 6-9        |
| mkmGenerateRandomMK - Generate Random Master Key . . . . .             | 6-11       |
| init_master_keys - Create and Initialize Master Keys . . . . .         | 6-12       |
| mkmLoadFirstMKPart - Load First Master Key Part . . . . .              | 6-13       |
| mkmLoadMKFromShares - Load Master Key Shares . . . . .                 | 6-14       |
| reinit_master_keys - Reinitialize Master Keys . . . . .                | 6-16       |
| mkmSetMasterKey - Set Master Key . . . . .                             | 6-17       |
| Functions to Check Master Key Values and Status . . . . .              | 6-18       |
| Summary of Functions . . . . .   | 6-18       |
| compute_mk_verification_pattern . . . . .                              | 6-19       |
| mkmGetMasterKeyStatus - Get Master Key Status . . . . .                | 6-21       |
| get_mk_verification_pattern . . . . .                                  | 6-23       |
| mkmGetAsymVerificationPattern . . . . .                                | 6-24       |
| Functions to Encrypt and Decrypt Using the Master Key . . . . .        | 6-25       |
| Summary of Functions . . . . .   | 6-25       |
| ede3_triple_decrypt_under_master_key . . . . .                         | 6-26       |
| ede3_triple_encrypt_under_master_key . . . . .                         | 6-27       |
| TDESDecryptUnderMasterKey . . . . .                                    | 6-28       |
| TDESEncryptUnderMasterKey . . . . .                                    | 6-29       |
| triple_decrypt_under_master_key . . . . .                              | 6-30       |
| triple_decrypt_under_master_key_with_CV . . . . .                      | 6-31       |
| triple_encrypt_under_master_key . . . . .                              | 6-32       |
| triple_encrypt_under_master_key_with_CV . . . . .                      | 6-33       |
| <b>Chapter 7. SHA-1 Functions . . . . .</b>                            | <b>7-1</b> |
| Header Files for SHA-1 Functions . . . . .                             | 7-1        |
| Summary of Functions . . . . .   | 7-1        |
| computeHMAC_SHA1 - Compute HMAC using SHA-1 Algorithm . . . . .        | 7-2        |
| do_sha_hash_message - Calculate SHA-1 Hash Hardware/Software . . . . . | 7-3        |
| do_sha_hash_msg_to_bfr - SHA-1 Hash . . . . .                          | 7-6        |
| hw_sha_hash_message - Compute SHA-1 Hash in Hardware . . . . .         | 7-7        |
| sha_hash_message - SHA-1 Hash with Chaining . . . . .                  | 7-9        |
| sha_hash_msg_to_bfr - SHA-1 Hash . . . . .                             | 7-12       |
| <b>Chapter 8. DES Utility Functions . . . . .</b>                      | <b>8-1</b> |
| Header Files for DES Utility Functions . . . . .                       | 8-1        |
| Summary of Functions . . . . .   | 8-1        |
| Overview . . . . .   | 8-3        |
| cas_adjust_parity - Adjust Parity . . . . .                            | 8-4        |
| CasBuildCv - Build a Default Control Vector . . . . .                  | 8-5        |
| CasBuildToken - Build a Default Token . . . . .                        | 8-6        |
| CasCurrentMkvp - Current Master Key Verification Pattern . . . . .     | 8-8        |
| CasOldMkvp - Old Master Key Verification Pattern . . . . .             | 8-9        |
| cas_des_key_token_check - Verify the DES Key Token . . . . .           | 8-10       |

|  |      |
|--|------|
| cas_get_key_type - Return Key Type                           | 8-11 |
| cas_key_length - Return Key Length                           | 8-12 |
| cas_key_tokentvv_check - Verify the Token Validation Value   | 8-13 |
| CasMasterKeyCheck - Master Key Version Check                 | 8-14 |
| cas_parity_odd - Verify Parity                               | 8-16 |
| RecoverDesDataKeyWithMK - Recover DES Data Key               | 8-17 |
| RecoverDesKekImporterWithMK - Recover DES Importer KEK       | 8-19 |
| <b>Chapter 9. RSA Functions</b>                              | 9-1  |
| Header Files for RSA Functions                               | 9-1  |
| Summary of Functions   | 9-1  |
| Overview   | 9-4  |
| CalculatenWordLength - Return Word Length of Modulus         | 9-6  |
| CreateInternalKeyTokenWithMK - Create Internal Key Token     | 9-7  |
| CreateRsaInternalSectionWithMK - Create RSA Internal Section | 9-8  |
| delete_KeyToken - Delete a Key From On-Board Storage         | 9-9  |
| GenerateCcaRsaToken - Generate CCA RSA Key Token             | 9-10 |
| GenerateRsaInternalToken - Generate RSA Key Token            | 9-11 |
| generate_dSig - Receives RSA Key Token                       | 9-12 |
| GeteLength - Return RSA Public Exponent Byte Length          | 9-14 |
| getKeyToken - Get a PKA Token From On-Board Storage          | 9-15 |
| GetModulus - Extract and Copy RSA Modulus                    | 9-16 |
| GetnBitLength - Return RSA Modulus Bit Length                | 9-17 |
| GetnByteLength - Return RSA Modulus Byte Length              | 9-18 |
| GetPublicExponent - Extract and Copy Public Exponent         | 9-19 |
| GetRsaPrivateKeySection - Return Private Key                 | 9-20 |
| GetRsaPublicKeySection - Return Public Key                   | 9-21 |
| GetTokenLength - Return Key Token Length                     | 9-22 |
| IsPrivateExponentEven - Verify RSA Private Exponent          | 9-23 |
| IsPrivateKeyEncrypted - Verify Private Key Encryption        | 9-24 |
| IsPublicExponentEven - Verify RSA Public Exponent            | 9-25 |
| IsRsaToken - Verify RSA Key                                  | 9-26 |
| IsTokenInternal - Key Token Format                           | 9-27 |
| PkaHashQueryWithMK - Return Master Key Version               | 9-28 |
| PkaMkvpQueryWithMK - Return Master Key Version               | 9-29 |
| pka96_tvvgen - Calculate Token Validation Value              | 9-30 |
| RecoverPkaClearKeyTokenUnderMkWithMK                         | 9-31 |
| RecoverPkaClearKeyTokenUnderXport                            | 9-33 |
| ReEncipherPkaKeyTokenWithMK - Re-Encipher PKA Key Token      | 9-34 |
| RequestRSACrypto - Perform an RSA Operation                  | 9-35 |
| store_KeyToken - Store Registered or Retained Key            | 9-36 |
| TokenMkvpMatchMasterKey - Test Encryption of RSA Key         | 9-37 |
| ValidatePkaToken - Validate RSA Key Token                    | 9-38 |
| VerifyKeyTokenConsistency - Verify Key Token Consistency     | 9-39 |
| verify_dSig - Verify RSA Key Token Signature                 | 9-40 |
| <b>Chapter 10. CCA SRDI Manager Functions</b>                | 10-1 |
| Header Files for SRDI Manager Functions                      | 10-1 |
| Overview   | 10-1 |
| CCA SRDI Manager Operation                                   | 10-3 |
| Controlling Concurrent Access to an SRDI                     | 10-6 |
| Summary of Functions   | 10-7 |
| close_cca_srdi - Close CCA SRDI                              | 10-8 |
| create_cca_srdi - Create CCA SRDI                            | 10-9 |

|  |       |
|--|-------|
| create4update_cca_srdi - Create CCA SRDI for Update Only             | 10-11 |
| delete_cca_srdi - Delete CCA SRDI                                    | 10-12 |
| get_cca_srdi_length - Get CCA SRDI Length                            | 10-13 |
| open_cca_srdi - Open CCA SRDI  | 10-14 |
| resize_cca_srdi - Resize CCA SRDI                                    | 10-15 |
| save_cca_srdi - Save CCA SRDI  | 10-16 |
| update_cca_srdi - Update an SRDI Item                                | 10-17 |
| Example Code   | 10-18 |
| <b>Chapter 11. Access Control Manager Functions</b>                  | 11-1  |
| Header Files for Access Control Manager Functions                    | 11-1  |
| Summary of Functions   | 11-1  |
| SRDI Files   | 11-2  |
| Data Structures  | 11-2  |
| ac_check_authorization - Check Authorization to Execute Function     | 11-5  |
| ac_chg_prof_auth_data - Change Profile Authentication Data           | 11-6  |
| ac_chg_prof_exp_date - Change Profile Expiration Date                | 11-8  |
| ac_del_profile - Delete User Profile                                 | 11-9  |
| ac_del_role - Delete Role  | 11-10 |
| ac_get_list_sizes - Get Sizes of Role and Profile Lists              | 11-11 |
| ac_get_profile - Get Profile   | 11-12 |
| ac_get_role - Get Role   | 11-13 |
| ac_init - Initialize the Access Control Manager                      | 11-14 |
| ac_list_profiles - List User Profiles                                | 11-15 |
| ac_list_roles - List Roles   | 11-16 |
| ac_load_profiles - Load User Profiles                                | 11-17 |
| ac_load_roles - Load Roles   | 11-19 |
| ac_lu_add_user - Add a User to the List of Logged on Users           | 11-20 |
| ac_lu_drop_user - Remove a User from the Logon List                  | 11-21 |
| ac_lu_get_ks - Get a Copy of a Session Key                           | 11-22 |
| ac_lu_get_num_users - Get the Number of Logged On Users              | 11-23 |
| au_lu_get_role - Get Role from the Logon List                        | 11-24 |
| ac_lu_ks_dec - Decrypt Data with Session Key                         | 11-25 |
| ac_lu_ks_enc - Encrypt Data with Session Key                         | 11-26 |
| ac_lu_ks_hmacgen - Compute an HMAC Using Session Key                 | 11-27 |
| ac_lu_ks_hmacver - Verify an HMAC Using Session Key                  | 11-28 |
| ac_lu_ks_macgen - Compute a MAC using Session Key                    | 11-29 |
| ac_lu_ks_macver - Verify a MAC using Session Key                     | 11-30 |
| ac_lu_list_users - List the IDs of the Logged On Users               | 11-31 |
| au_lu_query_user - Check if a User is Logged On                      | 11-32 |
| ac_query_profile - Return the Length of a User Profile               | 11-33 |
| ac_query_role - Return the Length of a Role                          | 11-34 |
| ac_reinit - Reinitialize the Access Control Manager                  | 11-35 |
| ac_reset_logon_fail_cnt - Reset Logon Failure Count                  | 11-36 |
| acm_xlt_errorcode - Translate an ACM Error Code to a SAPI Error Code | 11-37 |
| <b>Chapter 12. Cache Management Functions</b>                        | 12-1  |
| Header Files for Caching Functions                                   | 12-1  |
| Overview of Cache Management Functions                               | 12-1  |
| Summary of Functions   | 12-2  |
| cache_clear  | 12-3  |
| cache_delete   | 12-4  |
| cache_delete_item  | 12-5  |
| cache_get_item   | 12-6  |

|   |             |
|---|-------------|
| cache_get_item_b . . . . .  | 12-7        |
| cache_init . . . . .  | 12-8        |
| cache_status . . . . .  | 12-9        |
| cache_write_item . . . . .  | 12-10       |
| <b>Chapter 13. Miscellaneous Functions . . . . .</b>                                | <b>13-1</b> |
| Header Files for Miscellaneous Functions . . . . .                                  | 13-1        |
| Summary of Functions . . . . .  | 13-1        |
| check_access_auth_fcn - Verify User Authority . . . . .                             | 13-2        |
| GetKeyLength - Get Length of Key Token . . . . .                                    | 13-4        |
| intel_long_reverse - Convert Long Values . . . . .                                  | 13-5        |
| intel_word_reverse - Convert 2-Byte Values . . . . .                                | 13-6        |
| TOKEN_IS_A_LABEL - Identifies the Token as a Label . . . . .                        | 13-7        |
| TOKEN_LABEL_CHECK - Determine if Key Identifier is a Label . . . . .                | 13-8        |
| <b>Appendix A. UDX Sample Code - Host Piece . . . . .</b>                           | <b>A-1</b>  |
| <b>Appendix B. UDX Sample Code - Coprocessor Piece . . . . .</b>                    | <b>B-1</b>  |
| <b>Appendix C. Moving a UDX from the Model 1 Card to the Model 2 Card . . . . .</b> | <b>C-1</b>  |
| Master Key Manager Changes . . . . .  | C-1         |
| Makefile Changes . . . . .  | C-2         |
| <b>Appendix D. Reserved Values . . . . .</b>  | <b>D-1</b>  |
| <b>Appendix E. Data Structures . . . . .</b>  | <b>E-1</b>  |
| Structures Used in Communications Between NT Host and Coprocessor . . . . .         | E-1         |
| Data Structures for Caching Functions . . . . .                                     | E-7         |
| Other Useful Data Structures . . . . .  | E-8         |
| <b>Appendix F. Notices . . . . .</b>  | <b>F-1</b>  |
| Copying and Distributing Softcopy Files . . . . .                                   | F-2         |
| Trademarks . . . . .  | F-2         |
| <b>List of Abbreviations and Acronyms . . . . .</b>                                 | <b>X-1</b>  |
| <b>Glossary . . . . .</b>   | <b>X-3</b>  |
| <b>Index . . . . .</b>  | <b>X-7</b>  |

|  
|  
|  
|





---

## Figures

|       |   |      |
|-------|---|------|
| 1-1.  | View of CCA with User-Defined Extensions      | 1-2  |
| 1-2.  | Request and Reply Parameter Block Formats     | 1-8  |
| 2-1.  | Example CCA/UDX Function Prototype            | 2-3  |
| 2-2.  | Example UDX Subfunction Codes                 | 2-4  |
| 2-3.  | Example UDX Completion Codes                  | 2-5  |
| 2-4.  | Example UDX Command Processor Prototype       | 2-6  |
| 2-5.  | Example UDX Access Control Points             | 2-7  |
| 2-6.  | Example UDX Command Decoding Array Definition | 2-8  |
| 4-1.  | The RULE_MAP Structure                        | 4-19 |
| 4-2.  | Example Rule Map for Verb CSNBPKI             | 4-21 |
| 4-3.  | Example Rule Map for Verb CSUAACI             | 4-21 |
| 5-1.  | Possible Values                               | 5-4  |
| 6-1.  | Master Key Status Bits                        | 6-21 |
| 10-1. | Master SRDI Manager Overview                  | 10-2 |
| 10-2. | Master SRDI Read Illustration, Part 1         | 10-4 |
| 10-3. | Master SRDI Read Illustration, Part 2         | 10-5 |
| 10-4. | Master SRDI Read Illustration, Part 3         | 10-5 |



---

## About This Book

The *IBM 4758 PCI Cryptographic Coprocessor CCA User Defined Extensions Reference and Guide*, Version 2: 4758-002 and 4758-023 describes the Common Cryptographic Architecture (CCA) application programming interface (API) function calls that are available to user-defined extensions to CCA. A user-defined extension (UDX) allows a developer to add customized operations to IBM's CCA Support Program. UDXs are written and invoked in the same manner as base CCA functions and have access to the same internal functions and services as the CCA Support Program.

This document begins with an overview of the UDX programming environment and the sample files that are provided for use by UDX authors. The remainder of the document is a reference manual that describes a variety of functions that a UDX developer may exploit. The callable functions may be grouped into three classes:

1. Functions that may be called by the portion of a UDX that runs inside the PCI cryptographic coprocessor.
2. Functions that may be called by the portion of a UDX that runs on the host.
3. Functions that are available both inside the coprocessor and on the host.

Most of the functions are in the first class.

The primary audience for this manual is developers who need to write a UDX. This manual should be used in conjunction with the manuals listed under "CCA Support Program Publications" on page xiii and "Custom Software Publications" on page xiii.

---

## Prerequisite Knowledge

The reader of this book should understand how to perform basic tasks (including editing, system configuration, file system navigation, and creating application programs) on the host machine and should understand the use of IBM's CCA Support Program (as described in the *IBM 4758 PCI Cryptographic Coprocessor CCA Support Program Installation Manual* and the *IBM 4758 PCI Cryptographic Coprocessor CCA Basic Services Reference and Guide*). The reader should also understand the OS/390 application environment (as described in the *OS/390 ICSF Application Programmer's Guide* and the *OS/390 ICSF System Programmer's Guide*). Familiarity with the SCC application development process (as described in the *IBM 4758 PCI Cryptographic Coprocessor Custom Software Developer's Toolkit Guide*) is also required.

---

## Organization of This Book

Chapter 1, "Understanding the UDX Environment" discusses the design of the CCA application and the separation of the CCA API into host-side and coprocessor-side components.

Chapter 2, "Building a CCA User-Defined Extension" discusses how to build each portion of a UDX.

Chapter 3, “SCC Functions” summarizes the secure cryptographic coprocessor (SCC) API on top of which IBM’s CCA coprocessor application modules are built. A UDX may use the SCC API if so desired.

Chapter 4, “Communications Functions” describes the functions that allow the piece of a UDX that runs on the host to exchange information with the piece of the UDX that runs in the coprocessor.

Chapter 5, “Function Control Vector Management Functions” describes the functions that allow a UDX to determine which cryptographic operations have been authorized by the CCA function control vector and how long certain cryptographic keys may be.

Chapter 6, “CCA Master Key Manager Functions” describes the functions that allow a UDX to access and manipulate the CCA master key registers, which are used to encrypt and decrypt data and keys using various forms of the Data Encryption Standard (DES) algorithm.

Chapter 7, “SHA-1 Functions” describes the functions that a UDX can use to compute the hash of a block of data using the Secure Hash Algorithm (SHA-1).

Chapter 8, “DES Utility Functions” describes the functions that a UDX can use to manipulate and obtain information about key tokens and other cryptographic structures.

Chapter 9, “RSA Functions” describes the functions that a UDX can use to perform public key cryptographic operations using the RSA (Rivest-Shamir-Adleman) algorithm.

Chapter 10, “CCA SRDI Manager Functions” describes the functions that a UDX can use to store and retrieve data in the coprocessor’s nonvolatile memory areas (flash memory and battery-backed RAM [BBRAM]).

Chapter 11, “Access Control Manager Functions” describes the functions that a UDX can use to manipulate a user’s permissions, change authentication (logon) procedures, or obtain information about permissions and users on the coprocessor.

Chapter 12, “Cache Management Functions” describes the functions that a UDX can use to implement an on-board cache of secure data, and to track the contents of the cache on the host.

Chapter 13, “Miscellaneous Functions” describes several assorted utility functions available to a UDX.

Appendix A, “UDX Sample Code - Host Piece” contains the host-side portion of a sample UDX.

Appendix B, “UDX Sample Code - Coprocessor Piece” contains the coprocessor-side portion of a sample UDX.

Appendix C, “Moving a UDX from the Model 1 Card to the Model 2 Card” contains necessary changes to the UDX codewhen transferring code from a model 1 to a model 2 card.

Appendix D, “Reserved Values” lists the values reserved for UDX developers.

Appendix E, “Data Structures” contains useful data structures from the toolkit header files.

Appendix F, “Notices” includes product and publication notices.

A list of abbreviations, a glossary, and an index complete the manual.

---

## Typographic Conventions

This publication uses the following typographic conventions:

- File names, function names, and return codes are presented in **bold** type.
- Variable information and parameters are presented in *fixed-space* type.
- Web addresses are presented in *italic* type.

---

## Related Publications

Many of the publications listed below under “General Interest,” “CCA Support Program Publications,” and “Custom Software Publications” are available in Adobe Acrobat\*\* portable document format (PDF) at <http://www.ibm.com/security/cryptocards>.

Click **Library** to view or print the books.

### General Interest

The following publications may be of interest to anyone who needs to install, use, or write applications for a PCI Cryptographic Coprocessor:

- *IBM 4758 PCI Cryptographic Coprocessor General Information Manual* (version -01 or later)
- *IBM 4758 PCI Cryptographic Coprocessor Installation Manual*

### CCA Support Program Publications

The following publications may be of interest to readers who intend to use a PCI Cryptographic Coprocessor to run IBM’s Common Cryptographic Architecture (CCA) Support Program:

- *IBM 4758 PCI Cryptographic Coprocessor CCA Support Program Installation Manual*
- *IBM 4758 PCI Cryptographic Coprocessor CCA Basic Services Reference and Guide*

### Custom Software Publications

The following publications may be of interest to persons who intend to write applications that will run on a PCI Cryptographic Coprocessor:

- *IBM 4758 PCI Cryptographic Coprocessor Custom Software Installation Manual*
- *IBM 4758 PCI Cryptographic Coprocessor Custom Software Interface Reference*
- *IBM 4758 PCI Cryptographic Coprocessor Interactive Code Analysis Tool (ICAT) User’s Guide*

- *IBM 4758 PCI Cryptographic Coprocessor Custom Software Developer's Toolkit Guide*
- *IBM 4758 PCI Cryptographic Coprocessor CP/Q Operating System Overview*
- *IBM 4758 PCI Cryptographic Coprocessor CP/Q Operating System Application Programming Reference*
- *IBM 4758 PCI Cryptographic Coprocessor CP/Q Operating System C Runtime Library Reference*
- *AMCC S5933 PCI Controller Data Book*, available from Applied Micro Circuits Corporation, 6290 Sequence Drive, San Diego, CA 92121-4358. Phone 1-800-755-2622 or 1-619-450-9333. The manual is available online as an Adobe Acrobat\*\* PDF file at <http://www.amcc.com/pdfs/5933db.pdf>.

## Cryptography Publications

The following publications describe cryptographic standards, research, and practices applicable to the PCI Cryptographic Coprocessor:

- "Application Support Architecture for a High-Performance, Programmable Secure Coprocessor," J. Dyer, R. Perez, S.W. Smith, and M. Lindemann, 22nd National Information Systems Security Conference, October 1999.
- "Validating a High-Performance, Programmable Secure Coprocessor," S.W. Smith, R. Perez, S.H. Weingart, and V. Austel, 22nd National Information Systems Security Conference, October 1999.
- "Building a High-Performance, Programmable Secure Coprocessor," S.W. Smith and S.H. Weingart, Research Report RC21102, IBM T.J. Watson Research Center, February 1998.
- "Using a High-Performance, Programmable Secure Coprocessor," S.W. Smith, E.R. Palmer, and S.H. Weingart, in *FC98: Proceedings of the Second International Conference on Financial Cryptography*, Anguilla, February 1998. Springer-Verlag LNCS, 1998. ISBN 3-540-64951-4
- "Smart Cards in Hostile Environments," H. Gobiuff, S.W. Smith, J.D. Tygar, and B.S. Yee, *Proceedings of the Second USENIX Workshop on Electronic Commerce*, 1996.
- "Secure Coprocessing Research and Application Issues," S.W. Smith, Los Alamos Unclassified Release LA-UR-96-2805, Los Alamos National Laboratory, August 1996.
- "Secure Coprocessing in Electronic Commerce Applications," B.S. Yee and J.D. Tygar, in *Proceedings of the First USENIX Workshop on Electronic Commerce*, New York, July 1995.
- "Transaction Security Systems," D.G. Abraham, G.M. Dolan, G.P. Double, and J.V. Stevens, in *IBM Systems Journal* Vol. 30 No. 2, 1991, G321-0103.
- "Trusting Trusted Hardware: Towards a Formal Model for Programmable Secure Coprocessors," S.W. Smith and V. Austel, in *Proceedings of the Third USENIX Workshop on Electronic Commerce*, Boston, August 1998.
- "Using Secure Coprocessors," B.S. Yee (Ph.D. thesis), Computer Science Technical Report CMU-CS-94-149, Carnegie-Mellon University, May 1994.

- “Cryptography: It’s Not Just for Electronic Mail Anymore,” J.D. Tygar and B.S. Yee, Computer Science Technical Report, CMU-CS-93-107, Carnegie Mellon University, 1993.
- “Dyad: A System for Using Physically Secure Coprocessors,” J.D. Tygar and B.S. Yee, Harvard-MIT Workshop on Protection of Intellectual Property, April 1993.
- “An Introduction to Citadel—A Secure Crypto Coprocessor for Workstations,” E.R. Palmer, Research Report RC18373, IBM T.J. Watson Research Center, 1992.
- “Introduction to the Citadel Architecture: Security in Physically Exposed Environments,” S.R. White, S.H. Weingart, W.C. Arnold, and E.R. Palmer, Research Report RC16672, IBM T.J. Watson Research Center, 1991.
- “An Evaluation System for the Physical Security of Computing Systems,” S.H. Weingart, S.R. White, W.C. Arnold, and G.P. Double, Sixth Computer Security Applications Conference, 1990.
- “ABYSS: A Trusted Architecture for Software Protection,” S.R. White and L. Comerford, IEEE Security and Privacy, Oakland 1987.
- “Physical Security for the microABYSS System,” S.H. Weingart, IEEE Security and Privacy, Oakland 1987.
- *Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition*, Bruce Schneier, John Wiley & Sons, Inc. ISBN 0-471-12845-7 or ISBN 0-471-11709-9
- *ANSI X9.31 Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry*
- *IBM Systems Journal* Volume 30 Number 2, 1991, G321-0103
- *IBM Systems Journal* Volume 32 Number 3, 1993, G321-5521
- *IBM Journal of Research and Development* Volume 38 Number 2, 1994, G322-0191
- *USA Federal Information Processing Standard (FIPS):*
  - *Data Encryption Standard*, 46-1-1988
  - *Secure Hash Algorithm*, 180-1, May 31, 1994
  - *Cryptographic Module Security*, 140-1
- *Derived Test Requirements for FIPS PUB 140-1*, W. Havener, R. Medlock, L. Mitchell, and R. Walcott. MITRE Corporation, March 1995.
- *ISO 9796 Digital Signal Standard*
- *Internet Engineering Taskforce RFC 1321*, April 1992, MD5
- *Secure Electronic Transaction Protocol Version 1.0*, May 31, 1997

IBM Research Reports can be obtained from:

IBM T.J. Watson Research Center  
Publications Office, 16-220  
P.O. Box 218  
Yorktown Heights, NY 10598

Back issues of the *IBM Systems Journal* and the *IBM Journal of Research and Development* may be ordered by calling (914) 945-3836.

## Other IBM Cryptographic Product Publications

The following publications describe products that utilize the IBM Cryptographic Architecture (CCA) Application Program Interface (API).

- *IBM Transaction Security System General Information Manual*, GA34-2137
- *IBM Transaction Security System Basic CCA Cryptographic Services*, SA34-2362
- *IBM Transaction Security System I/O Programming Guide*, SA34-2363
- *IBM Transaction Security System Finance Industry CCA Cryptographic Programming*, SA34-2364
- *IBM Transaction Security System Workstation Cryptographic Support Installation and I/O Guide*, GC31-4509
- *IBM 4755 Cryptographic Adapter Installation Instructions*, GC31-4503
- *IBM Transaction Security System Physical Planning Manual*, GC31-4505
- *IBM Common Cryptographic Architecture Services/400 Installation and Operators Guide, Version 2*, SC41-0102
- *IBM Common Cryptographic Architecture Services/400 Installation and Operators Guide, Version 3*, SC41-0102
- *IBM ICSF/MVS General Information*, GC23-0093
- *IBM ICSF/MVS Application Programmer's Guide*, SC23-0098
- *OS/390 Integrated Cryptographic Service Facility Overview*, GC23-3972
- *OS/390 Integrated Cryptographic Service Facility Application Programmer's Guide*, SC23-3976
- *OS/390 Integrated Cryptographic Service Facility System Programmer's Guide*, SC23-3974
- *OS/390 ICSF Trusted Key Entry Workstation User's Guide*, SC23-3978

---

## Summary of Changes

This edition of the *CCA User Defined Extensions Reference and Guide* contains product information that is current with IBM 4758 PCI Cryptographic Coprocessor Version 2: 4758-002 and 4758-023. Revision bars ( | ) throughout this manual indicate updates.

Changes made to this first edition in April, 2000 include:

- Chapter 1—Added multithreading capability for the CCA and RSA Managers.
- Chapter 6—Major revision to the chapter.
- Chapter 7—The SHA-1 hashing function can now be performed in either hardware or software. Also added a new function that chooses the most efficient method for calculating the SHA-1 hash.
- Chapter 8—Added the MKSelector parameter to several functions.
- Chapter 9—The Master Key Manager now maintains an on-board cache of unencrypted keys. When an operational (Master Key encrypted) key is decrypted with the function RecoverPkaClearKeyUnderMKWithMK or



RecoverDesClearKeyUnderMkWithMK, it is stored in the on-board cache. Subsequent requests to decipher the same key result in the return of the clear key from the cache, instead of a decryption operation.

- Chapter 10—Added two new functions to create and update an SRDI.
- Chapter 11—The CCA Access Control Manager now uses HMAC instead of TDES MAC for session data integrity protection.

Changes made to this first edition in July, 2000 include:

- Chapter 1—**8** CCA Dispatcher: Updated the discussion on multithreaded design.

Changes made to this first edition in August, 2000 include:

- Chapter 1—Passing Large Data Blocks: Added sample code for both host and card.
- Chapter 4—BuildParmBlock: Updated step 3.  
Rule\_Check: Function is now available for both host and coprocessor.
- Chapter 9—Added generate\_dSig and verify\_dSig functions.

Changes made to this second edition in January, 2001 include:

- Chapter 12—New chapter, Cache Management functions.
- Files included with this toolkit—For this release of the toolkit, we have eliminated the toolkit versions of libraries csuncall.dll, csunsecy.dll, and csundir.dll. The CCA-supplied versions of these files should be in your path when running your UDX.
- Updates to the makefiles—The following changes were made to the included sample makefiles:
  - Hostside makefiles, hst\_msvc.mak and hst\_vac.mak: The libs variable has been changed to reflect the new position of csunsapi.lib, which is *... \udxtk\002\lib\common*.

Changes made to this second edition in February, 2001 include:

- Chapter 9—Added information to RecoverPkaClearKeyTokenUnderMkWithMk that explains what happens if the PKA key is in the on-board cache of the decrypted key.

Changes made to this third edition in October, 2001 include:

- Added new appendix that includes useful data structures from the toolkit header files.



---

## Chapter 1. Understanding the UDX Environment

The *UDX Development Toolkit for the IBM 4758* provides scaffold code, object modules, and header files that you can use to extend the IBM-developed Common Cryptographic Architecture (CCA) application program which employs the IBM 4758 PCI Cryptographic Coprocessor. You can use as much or as little of the CCA application function as required to meet your processing requirements.

This chapter explains the design of the CCA “middleware” application. If you are not familiar with the CCA implementation for the coprocessor, you should first read portions of the *IBM 4758 PCI Cryptographic Coprocessor CCA Basic Services Reference and Guide*. In particular, read chapter 1, the introductory information of chapters 2 through 8, and become aware of the material in appendixes B, C, and D.

This manual also assumes that you are familiar with the techniques for creating and testing coprocessor application programs as described in the *IBM 4758 PCI Cryptographic Coprocessor Custom Software Developer’s Toolkit Guide*. You may benefit from understanding the services that you can obtain from the CP/Q++ application program interface (API). Refer to the *IBM 4758 PCI Cryptographic Coprocessor Custom Software Interface Reference*.

The CCA architecture requires that security-sensitive functions are carried out in an environment where secret or private quantities can safely appear in the clear and where the design of the processing functions can not be altered by an adversary. A coprocessor application program operates in such an environment. However, the confidentiality of secret or private quantities (for example, cryptographic keys or computational values) is also the responsibility of the application program design.

The CCA application operates as a request/response mechanism. Once initialized by CP/Q++ as a result of a coprocessor reset sequence, the CCA application within the coprocessor waits for an external request. The application then performs the requested function and returns a response. The application retains persistent data as a set of security relevant data items (SRDI). The application stores SRDIs in RAM memory, with a backup copy retained in either battery-backed RAM (BBRAM) or (optionally) encrypted in flash memory.

The CCA verbs (callable services) that a host application can request are generally serviced, on a one-for-one basis, by a *command processor* portion of coprocessor application code<sup>1</sup>. A common infrastructure is employed to format a verb request, transport the request to the coprocessor, dispatch the command processor, and return the reply to the host. Command processors and the top layer of CCA host code, security application program interface (SAPI), make extensive use of a set of common subroutines described in this manual.

The code that implements a user-defined extension (UDX) to CCA can be separated into two distinct pieces. One (the “host piece”) runs as a DLL on the host. The other (the “coprocessor piece”) is linked with a library containing IBM’s CCA coprocessor application modules and downloaded to the coprocessor. The

---

<sup>1</sup> A few CCA verbs are implemented as subroutines in the top layer of CCA host code and do not send a request to the coprocessor.

host piece converts requests for service from the user's application into messages to be sent to the coprocessor. These messages are received by the CCA application and routed to the appropriate (CCA or UDX) command processor.

Figure 1-1 depicts the major elements of code that form the CCA implementation for the coprocessor. The boxes with dotted lines designate the UDX components. Each block represents a section of the runtime code. Blocks one through six are host system DLLs (shared libraries) with block six actually split between a DLL and the physical device driver. An overview of these code blocks follows.

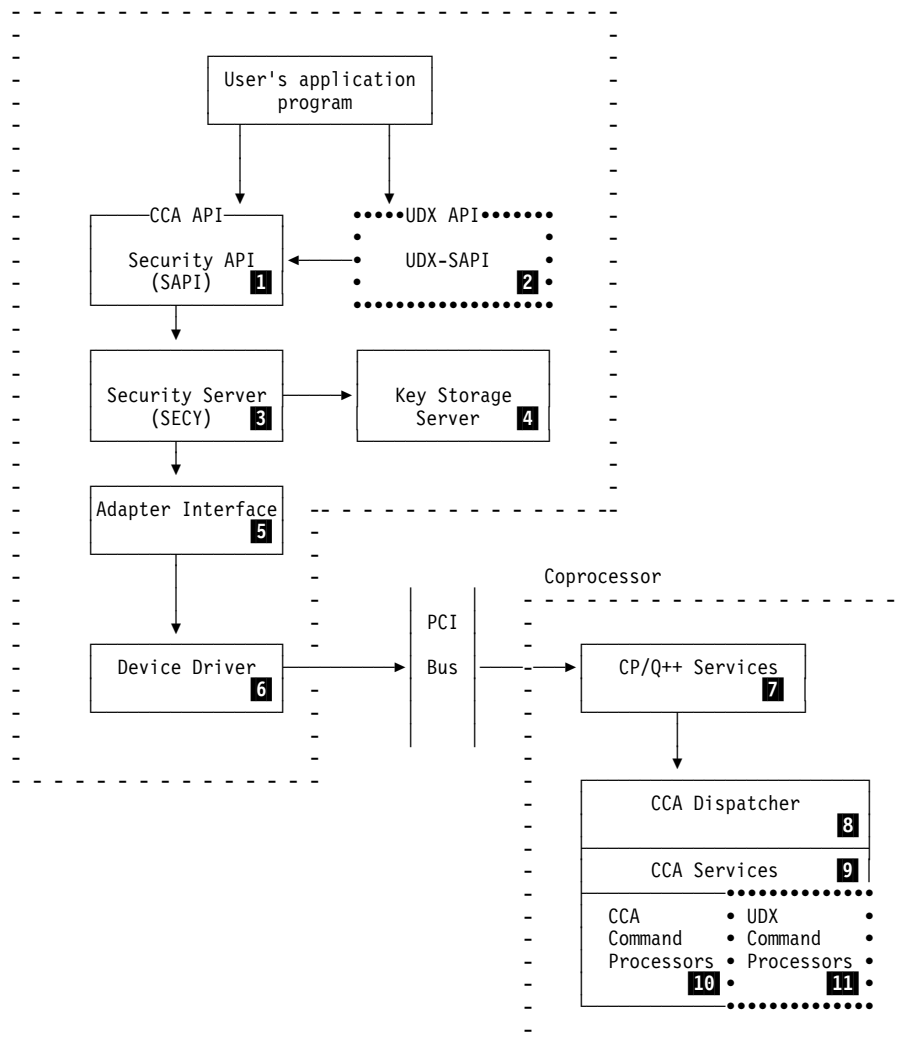


Figure 1-1. View of CCA with User-Defined Extensions

## 1 Security API (SAPI)

The Security API (SAPI) code, CSUxSAPI.DLL<sup>2</sup>, contains the CCA verb entry points. On input SAPI gathers the request information from the variables identified by the verb parameters and constructs a standardized set of control blocks for communication to the coprocessor CCA application. The formatted request is then passed to the security server (SECY) layer **3**. On output, the formatted reply is parsed and the caller's variables are updated with the verb results.

The request is communicated using a Cooperative Processing Request/Reply Block (CPRB) data structure and an appended, variable-length *request parameter block*. The formatted reply is likewise communicated with a CPRB and an appended *reply parameter block* of the same general structure as the request block.

The fixed-length CPRB structure carries a primary function code, return and reason code values, and pointers to, and lengths of, the request and reply parameter blocks and data to be DMAed to/from the coprocessor. The variable-length request and reply parameter blocks (see Figure 1-2 on page 1-8) carry:

- A sub-function code, the identifier of the command processor
- The rule-array elements, encoded in ASCII
- Verb-unique data (VUD)
- Cryptographic key information, key labels or tokens, in "key blocks."

The subroutines used to construct and to parse these control blocks are used by all of the verb routines in SAPI. These same subroutines are entry points that can be called by the UDX-SAPI code **2**. See Chapter 4, "Communications Functions" on page 4-1.

The CCA SAPI routines perform minimal checking on the input variables. The design concept is to perform almost all variable checking within the coprocessor. SAPI is responsible for ensuring that character-based control and data information is encoded in the manner expected by the coprocessor application, regardless of the encoding of this data on the host system. Likewise, SAPI must ensure that integers and other numbers are communicated in the form expected by the coprocessor application; in general, integers must be in little-endian format (Intel byte-reversed format).

Because the CCA SAPI code is compiled for both personal computer and IBM RS/6000 systems, C macros are used to ensure that the integers exchanged with the coprocessor are in little endian format. Note, however, that most CCA data structures, such as key tokens, define integer values as big endian (S/390 integer format) quantities. In these cases, the coprocessor and application program are responsible for ensuring and interpreting the appropriate integer byte-order.

## 2 UDX-SAPI

The UDX callable services are assumed to be analogous to CCA services. Your UDX host-piece code constructs and parses CPRB and request and reply parameter blocks using the same subroutines as employed by the SAPI code. Once the CPRB and request parameter block are constructed, you use the

---

<sup>2</sup> Typical CCA host code file names begin with CSUx where the "x" is "N" for Windows NT, "E" for OS/2, "F" for AIX and "L" for Linux.

CSNC\_SP\_SCSRFBSS() subroutine to pass control to the security server (SECY) layer. Upon regaining control, your code should update the caller's variables with the information that is parsed from the CPRB and reply parameter block. See Appendix A, "UDX Sample Code - Host Piece."

### **3 Security Server (SECY)**

The Security Server (SECY), CSUxSECY.DLL, receives control from SAPI with a pointer to the CPRB. The security server examines the key-block fields of the request and reply parameter blocks to determine if the key storage server should be called to allocate, delete, or list labels in key storage, or to fetch or store key records under key labels already existing in key storage. The security server also passes the name of the key storage files to the directory server. On input, except for a few key-storage services which do not require use of the coprocessor, the security server calls the adapter interface after completing any required key storage actions. Likewise, on output the adapter interface returns control to the security server which completes any required key storage requests and then returns control to SAPI. Information in a key block header (see "Key Blocks" on page 1-11) triggers the security server to process a key block.

### **4 Key Storage Server**

The key storage server, CSUxDIR.DLL, receives control from the security server with pointers to the key storage file names and to the key block on which it should take action. The server is responsible for opening and closing the directory files, allocating records in the indexed sequential files, listing the file names, and fetching and storing key tokens. Separate files are maintained for the DES fixed-length records and the variable-length PKA (public key architecture, RSA) records.

### **5 Adapter Interface**

The adapter interface, CSUxCALL.DLL, receives control from the security server and examines the CPRB to determine the nature of the call it will create to the device driver.

All CCA requests to the adapter interface require that the CPRB and request parameter block be DMAed to the coprocessor. A few requests (for example, data ciphering and MACing requests) also require that data be scheduled for DMA interchange with the coprocessor. The adapter interface layer examines the CPRB request and reply *data* block pointer and length fields and calls the device driver so that the coprocessor application program can cause DMA transfers from/to the identified fields. The adapter interface layer creates the control blocks and issues the I/O request to the device driver DLL.

### **6 Device Driver and Access Layer**

The device driver code is split between a DLL and a physical device driver. The API and function of the device driver is explained in the *IBM 4758 PCI Cryptographic Coprocessor Custom Software Interface Reference*.

The device driver and CP/Q++ work together to ensure that the reply to a request is routed back to the source process and thread that initiated the associated request.

## **7 CP/Q++ Services**

CP/Q++ becomes aware of an application in coprocessor segment three following a reset sequence. The application's entry point is called and CCA registers itself with CP/Q++.

When CP/Q++ receives a request from the host it checks for a registered application identifier; the identifier is a constant prearranged between the adapter interface layer and the CCA application. CCA host requests include the CPRB and request parameter block. The application interface layer presents sufficient information, which is passed on by CP/Q++, so that the CCA Dispatcher can request CP/Q++ to obtain the CPRB and request parameter block.

Other CP/Q++ services for DES, RSA, DSA, random number, date and time, storage of data in BBRAM and flash memory, and communication with external functions as described in the *IBM 4758 PCI Cryptographic Coprocessor CP/Q Operating System Application Programming Reference* and *IBM 4758 PCI Cryptographic Coprocessor CP/Q Operating System C Runtime Library Reference* are available to the UDX code. Note that CCA service subroutines are already available to perform many common functions and therefore command processor code generally does not call CP/Q++ directly.

## **8 CCA Dispatcher**

When CP/Q++ responds to the CCA dispatcher's request for input because of the receipt of a host request, the dispatcher obtains the CPRB and request parameter block. The dispatcher also locates the role that governs the processing of the CCA request, either the default role or the role associated with a logged-on profile.

Each thread of each host process can logon to a role through an associated profile. However, a single profile can be associated with only one host thread at a time; a correct logon to a profile from another thread will be honored and a new session key generated without any indication of this action reported to the "older" logged-on thread (until and if the older thread makes a new request).

The dispatcher uses the sub-function code in the first two bytes of the request parameter block in a table lookup operation to locate a CCA command processor entry point. If a match is not found, the dispatcher checks the UDX entry point table for a match. (Of course, if again no match is found, the dispatcher constructs a reply CRPB and fills it with a return and reason code indicating that no such function exists.) The dispatcher then calls the command processor and passes pointers to the CPRB and request parameter block, and to the role that governs processing for this request.

Later the command processor returns control to the dispatcher which uses CP/Q++ to DMA the reply CPRB, and (optionally) the reply parameter block, back to the host.

The Version 2 CCA implementation is multithreaded (differently than the Version 1 implementation). The multithreading design permits overlapped operation by the CPU, the modular-exponentiation hardware, the DES/TDES/SHA-1 hardware, the random number (bit) generator, and the external communication hardware.

The Main function in the CAMMGR.C module receives control when CP/Q++ loads the CCA application. Main calls various initialization functions in the other

managers (for example, obtain the master keys and role security relevant data items (SRDI), and so on), and then initializes six threads that each wait for CP/Q++ to deliver requests to the CCA message queue. Finally, Main waits on any catastrophic event. Each of the six threads are available to process incoming requests and runs the same code. When a request is received, one of the threads removes the request from the queue, determines which profile and role applies, examines the subfunction code, and calls an appropriate CCA or UDX command processor. When the command processor completes, the code passes the reply to the CP/Q++ Communication Manager and again enqueues on the inbound message queue.

The command decoder calls the UDX entry points. Following these rules ensures that your UDXs are thread-safe.

- Do not use static variables.
- Define semaphores globally, for example, define all semaphores in one particular UDX source code module which can be reached by an extern statement in other UDX source code modules.
- Create no more than 50 semaphores, as the table for storing semaphores is limited.

## **9 CCA Services**

The CCA application supplies many subroutines that command processors use to perform functions in a consistent manner. These routines are described later in this manual. The command processors also make use of three “managers” that localize certain classes of function to the managers:

**SRDI Manager** The CCA coprocessor application code generally uses the SRDI Manager to access information that is held in persistent BBRAM and flash memory. The manager is responsible for serializing the use of the SRDIs to accommodate the multi-tasking environment. See Chapter 10, “CCA SRDI Manager Functions” on page 10-1.

**Access Control Manager** All operations on roles and profiles are carried out by the Access Control Manager. Command processors call the manager to determine if individual control points are authorized. When a command processor is designed, one or more control points are assigned, as required for security purposes, to authorize function within the command processor. See Chapter 11, “Access Control Manager Functions” on page 11-1. The sample SAPI code (Appendix A, “UDX Sample Code - Host Piece” on page A-1) documents a range of control points (and also reason codes and subfunction codes) reserved for UDX developers.

**Master Key Manager** All operations pertaining to the master keys are performed by this manager. Code in other parts of CCA does not access the master key values directly, but rather calls the manager for operations that affect or use the master keys and their registers. See Chapter 6, “CCA Master Key Manager Functions” on page 6-1.

Note that all of the CCA coprocessor code and much of CP/Q++ operates at “protection ring 3” in the Intel 80x86 architecture. Therefore, all of this code has access to memory areas belonging to any portion of CCA. As additional code is created, it should be inspected to ensure that it performs only the intended function and accesses only information appropriate to the intended function.



## 10 CCA Command Processors

In general, each CCA verb results in a call to one command processor, the code in the coprocessor CCA application that performs the function unique to a verb.

Command processor code can call any of the other CCA subroutines and manager functions as well as functions available on the CP/Q++ API. In general, a command processor will perform the following steps. See Appendix B, “UDX Sample Code - Coprocessor Piece.”

- Copy the request CPRB to form the reply CPRB in the memory provided by the dispatcher.
- Set the return code and reason code to 0, 0 using `Cas_proc_retc()` and copy the sub-function code into the reply block.
- Call the Access Control Manager to determine if the appropriate control point is authorized using `CHECK_ACCESS_AUTH()`.
- Because most command processors will need to decrypt or encrypt a key, determine that there is a valid master key(s) using `mkmGetMasterKeyStatus()`.
- Check that the request parameter block is formed in a valid manner by calling `parm_block_valid()`.
- Check the length of the rule array data area by examining the rule array area length bytes. For CCA, this value is  $8x+2$  where  $x=0, 1, \dots, n$ . However, you could make this portion of the request parameter block contain data of almost any length. You can check the rule array elements using `rule_check()`.
- Check the length of any VUD, data formatted to the needs of the command processor. You should establish addressability to the VUD using a structure definition.
- Check the length and content of the zero or more key blocks. You can use the `TOKEN_LABEL_CHECK()` routine to determine if a key identifier is a key label.
- Perform the desired command function.
- Determine that the reply will not exceed the permissible reply size.
- Fill in the reply block with the rule array length and any elements, fill in the VUD length and any data, and fill in the key-block area length and any key blocks.
- Return to the dispatcher.

## 11 UDX Command Processors

UDX command processors are coded in the same way as the existing CCA command processors and have all of the same rights and responsibilities. In addition, you must establish the `ccax_cp_list[]` and the `ccax_cp_list_size` variable to inform the dispatcher of the length and content of the sub-function lookup table with the UDX command processor entry points.

## CCA Communication Structures

Two of the commonly used data structures internal to the CCA implementation are described in this section:

- Request and reply parameter blocks
- Key blocks and their header

CCA key tokens and access control structures are described in Appendix B of the *IBM 4758 PCI Cryptographic Coprocessor CCA Basic Services Reference and Guide*.

## Request and Reply Parameter Block Format

The request and reply parameter blocks immediately follow a data structure of type CPRB\_structure. Figure 1-2 shows the request and reply parameter block format.

**Note:** Be careful that the SAPI code processes the lengths in little-endian format (“Intel byte-reversed order”).

| <i>Figure 1-2. Request and Reply Parameter Block Formats</i> |                   |                   |                 |                         |                  |                         |                  |
|--|-------------------|-------------------|-----------------|-------------------------|------------------|-------------------------|------------------|
| Field:   | Sub-function Code | Rule Array Length | Rule Array Data | Verb Unique Data Length | Verb Unique Data | Key Block Fields Length | Key Block Fields |
| <b>Size:</b>   | 2                 | 2                 | X               | 2                       | Y                | 2                       | Z                |
| <b>Offset:</b>   | 0                 | 2                 | 4               | 4+X                     | 6+X              | 6+X+Y                   | 8+X+Y            |

| Field Name              | Description  |
|-------------------------|--|
| Subfunction code        | A code that identifies the command processor through a CCA dispatcher table lookup operation.  |
| Rule Array Length       | Length in bytes of the rule array portion of the block. Incorporation of rule-array information is optional, but this field must be present. If no rule-array information is specified, this field must be set to 2 (that is, the size of the length field). |
| Rule Array Data         | Zero or more 8-byte character arrays (not NULL-terminated). If no rule-array elements are specified, this field is empty (0-length).   |
| Verb Unique Data Length | Length in bytes of the (optional) data that is unique to this verb call and the length field. This field must always be present. If no data is specified, this field must be set to 2.   |
| Verb Unique Data        | Optional data block to be passed to the verb. For instance, if the verb is to encrypt 8 bytes as a key, the verb unique data might be the clear value of the key. If no data is specified, this field is empty (0-length).                                   |
| Key Block Fields Length | Length in bytes of the optional key block(s) portion of the request or reply parameter block. This field must always be present. If no keys are specified, this field must be set to 2.  |
| Key Block Fields        | Optional key block(s) exchanged between the host and coprocessor code. If no key tokens or key labels are specified, this field should be empty (0-length).  |

While it is possible to construct a request/reply parameter block “by hand” using pointer arithmetic, it is recommended that the UDX developer instead use the CCA-provided utility routine `BuildParmBlock`. The developer calls `BuildParmBlock` three times to build a request/reply parameter block: once for rule information, once for the verb unique data, and once for the key data. The order is important: rules first, then verb unique data, followed by key data. This routine simplifies request/reply parameter block creation by accepting an arbitrary number of

argument pairs (length + data pointer pairs) and constructs the sub-blocks in the previous table.

Similarly, while it is possible to extract data from the request/reply parameter blocks “by hand” using pointer arithmetic, it is recommended that the UDX developer instead use the CCA-provided utility routines FindFirstDataBlock, FindNextDataBlock, find\_first\_key\_block, and find\_next\_key\_block.

**Note:** An example of the use of these functions (BuildParmBlock and CSUC\_BULDCPRB) is in Appendix A, “UDX Sample Code - Host Piece” on page A-1.

### Passing Large Data Blocks

If more data must be passed, it is possible to pass the host address to the coprocessor for reading or writing with the CSUC\_BULDCPRB command. The buffer so addressed for sending to the coprocessor is referred to as a request data block. The length and pointer for the reply data block can be used for reading data from the coprocessor. The data buffers must not overlap and must be a multiple of four bytes long. In order for the device driver to manipulate the buffers efficiently, they should be aligned on 4-byte boundaries. Access to these buffers is managed by the coprocessor application using the sccGetBufferData and sccPutBufferData functions, respectively, using the defined constants CPRB\_REQUEST\_DATA or CPRB\_REPLY\_DATA as buffer indices.

On the host:

```
// First, set the CPRB structures properly, with the Rule Array, Verb Unique Data, and Key Blocks.

// To set the Request Data Block:
LocalRequestTextLength = *pTextLength;
LocalReplyTextLength   = *pTextLength;

CSUC_BULDCPRB( pCprb,
               (UCHAR *) ESSS_FUNCTION_ID_S,

               RequestBlockLength,           // Req.Parm
               pRequestParmBlock,           // block
                                               // len + adr

               LocalRequestTextLength,       // Req.Data
               (UCHAR *) pInpText,          // block
                                               // len + adr

               sizeof( pRequestReplyBuffer->reply_buf ),
               pRequestReplyBuffer->reply_buf,

               LocalReplyTextLength,         // Rep.Data
               (UCHAR *) pOutText);         // block
```

## On the card:

```

// -----
// Get the length of the bulk text first, from
// the CPRB structure.
// -----

BulkBlockLength = pRequestCprb->req_data_block_length;

// -----
// Check that the length of the reply data block
// in the CPRB is long enough (depends on your function)
// -----

if (BulkBlockLength > pRequestCprb->reply_data_block_length )
{
    Cas_proc_retc( pReplyCprb, RT_CONSISTENCY_ERROR );
    return;
}
// -----
// Get the InpTxt
// -----

// It is best to allocate these large blocks of data dynamically.
// But don't forget to free them later!
InpTxt = malloc(BulkBlockLength);
if (InpTxt == NULL)
{
    Cas_proc_retc(pReplyCprb, E_ALLOCATE_MEM);
    return;
}
memset(InpTxt,255,sizeof(InpTxt));

// Get the data from the buffer.
ReturnMsg = sccGetBufferData( RequestId,
                             CPRB_REQUEST_DATA,
                             InpTxt,
                             BulkBlockLength);

if (ReturnMsg != 0)
{
    free(InpTxt);
    Cas_proc_retc( pReplyCprb,
                  RT_CONSISTENCY_ERROR );
    return;
} // End if
//-----
//
// Build the OutTxt
// after completing the function
// and filling the Reply CPRB with the correct information
//-----

OutTxt = malloc(BulkBlockLength);
if (OutTxt == NULL)
{
    free(InpTxt);
    Cas_proc_retc(pReplyCprb, E_ALLOCATE_MEM);
    return;
}

```

```

for (iCnt=0 ; iCnt < BulkBlockLength ; iCnt++)
{
    OutTxt[iCnt] = InpTxt[BulkBlockLength-iCnt-1];
} // End for

free(InpTxt);

// The data we return is the same length as the data which
// was sent, for this function.
ReturnMsg = sccPutBufferData( RequestId,
                              CPRB_REPLY_DATA,
                              OutTxt,
                              BulkBlockLength);

free(OutTxt);
if (ReturnMsg != 0)
{
    Cas_proc_retc( pReplyCprb,
                  RT_CONSISTENCY_ERROR );

    return;
} // End if
//-----
// Write the Length of OutTxt in the CPRB
//-----

pReplyCprb->reply_data_block_length = BulkBlockLength;
//-----
// Then return to the host function
//-----
return;

```

Refer to the *IBM 4758 PCI Cryptographic Coprocessor Custom Software Interface Reference* for more details on using the `sccGetBufferData` and `sccPutBufferData` functions.

## Key Blocks

The key blocks portion of the request and reply parameter blocks is used to transport zero or more key identifiers: key labels and/or key tokens. A key block is a data structure consisting of a header and appended key label and/or key token data.

The key block header is a data structure containing a USHORT *Length* field in little-endian format followed by a USHORT *Flags* field in little-endian format. The *Length* field indicates the length of the header plus the length of the key token or label which follows it, while the *Flags* field informs SECY what functions are required of it. The *Flags* field options are detailed in the following table:

| <b>Flags indicating the type of key (one required)</b>        |   |
|---|---|
| PKA96_TYPE  | Indicates that the key token or label is an PKA token.  |
| DES96_TYPE  | Indicates that the key token or label is a DES key token.   |
| <b>Flags indicating the action to be taken (one required)</b> |   |
| ACTION_READ   | Request SECY to retrieve the key token from the storage file. This header must be followed by a key label.                                      |
| ACTION_WRITE  | Requests SECY to add or overwrite the key token in the storage file. This header must be followed by a key label concatenated with a key token. |
| ACTION_NOOP   | Requests no action from SECY.   |

If a DES key label were being passed with the intent that SECY obtain a key token for forwarding to the coprocessor, the Length and Flags fields would be set as follows:

```
KeyHeader.Flags    = htons(DES96_TYPE | ACTION_READ);
KeyHeader.Length  = htons(KEY_HDR_LEN + sizeof(KeyLabel));
```

This would cause SECY to locate the label which follows this header in the key block within the DES Key Storage File and replace the key label in the key block with the correct key token, for use by the coprocessor.

If an RSA key token were being passed, the Length and Flags fields would be set in this way:

```
KeyHeader.Flags    = htons (PKA96_TYPE | ACTION_NOOP);
KeyHeader.Length  = htons (KEY_HDR_LEN + ntohs(KeyToken.KeyLength));
```

Notice that the KeyLength field of a PKA key token is stored in big-endian format.

### Structuring the Key Block

If a key in the key storage file is to be read from key storage and changed in the command processor (for example, re-enciphering under the current master key) two copies of the key label must be passed from the host to the coprocessor, one with the ACTION\_READ flag set, the other with the ACTION\_NOOP flag set. This ensures that the coprocessor will receive both a key token to work with, and a key label with which to write the token to the key storage file when done. Upon return, the key block is built with one header, the Flags field set to ACTION\_WRITE, followed by the Key Label and the Key Token. See the sample function in Appendix A and Appendix B for an example.

If the key is to be read from the SECY server, but not changed (for example, for an ENCIPHER service) the key label may be passed alone, with the Flags field set to ACTION\_READ. On return, the key block is empty and the length is set to two.

Key Labels and key tokens are further described in the *IBM 4758 PCI Cryptographic Coprocessor CCA Basic Services Reference and Guide*.

---

## Chapter 2. Building a CCA User-Defined Extension

This chapter describes the process you can follow in creating a User-Defined Extension (UDX) for the CCA application that performs within and accesses the coprocessor. The chapter begins with an explanation of the files that you will use and then continues with the steps that you can follow in developing the host and the coprocessor pieces of code. It is assumed that you are familiar with developing and testing applications for the coprocessor, and that you have knowledge of the CP/Q++ API as explained in the other Toolkit publications (see “Related Publications” on page xiii).

---

### Files You Use in Building a UDX

A developer must create the following files (or modify the samples that are provided with the UDX Developer’s Toolkit) to produce a UDX:

- A header file (for example, ***csueextn.h***) that defines the interface the UDX exports to a user’s application. This header file is `#included` by the user’s application and by the host piece of the UDX and should contain a function prototype for each service the UDX provides. Such services are implemented in the same manner as CCA verbs; an example appears in Figure 2-1 on page 2-3.
- A header file (for example, ***cxt\_cmds.h***) that defines the interface between the host piece of the UDX and the coprocessor piece of the UDX. This header file is `#included` by both pieces and should define UDX subfunction codes, a UDX command processor for each subfunction, and the access control points and completion codes used by the UDX. The sample provided with the UDX Developer’s Toolkit includes comments that indicate the range of acceptable values for each of these elements.
- One or more C source files (for example, ***sxt\_samp.c***) that implement the host piece of the UDX. The sample provided with the UDX Developer’s Toolkit is a skeleton that exports a single function to the user’s application. The function checks its input parameters, constructs a request block, sends the request to the coprocessor and receives the reply, extracts the result, and returns it to the user’s application.
- One or more C source files (for example, ***cxt\_cmds.c***) that implement the coprocessor piece of the UDX. The sample provided with the UDX Developer’s Toolkit is a skeleton that receives a request from the host, validates the request and extracts the arguments it contains, performs a simple operation, constructs a reply block, and returns the reply to the host piece of the UDX.

A developer may need to modify the following files that are provided with the UDX Developer’s Toolkit to produce a UDX:

- A makefile that builds the DLL that implements the host piece of the UDX and the import library that describes the entry points the DLL exports. The UDX Developer’s Toolkit provides two such files: ***csueextn.mak*** (which creates ***csueextn.dll*** and ***csueextn.lib***) for use on OS/2 and ***csunextn.mak*** (which creates ***csunextn.dll*** and ***csunextn.lib***) for use on Windows NT. These makefiles are customizable for use with either Microsoft Visual C++ or IBM Visual Age C++.

- A makefile (for example, **camextn.mak**) that builds the executable that implements the coprocessor piece of the UDX. This executable includes the object for the UDX itself as well as a library that implements the coprocessor CCA object modules. This makefile may be customized for use with either Microsoft Visual C++ or IBM Visual Age C++.
- A linker definition file for the DLL that implements the host piece of the UDX. This file specifies the names of the entry points exported by the UDX and lists the CCA functions the host piece of the UDX invokes. The UDX Developer's Toolkit provides two such files: **csueextn.def** for use on OS/2 and **csunextn.def** for use on Windows NT.
- A resource definition file (for example, **csunextn.rc**) that supplies the version information that appears in the properties of the DLL that implements the host piece of the UDX on Windows NT. No resource definition file is needed to build the host piece of a UDX on OS/2.

The following binary files are used to produce a UDX:

- A library that contains definitions of the interface the UDX exports to a user's application. This library is linked with the user's application. The UDX Developer's Toolkit makefiles generate the appropriate library: **csueextn.mak** creates **csueextn.lib** on OS/2 and **csunextn.mak** creates **csunextn.lib** on Windows NT.
- A library that contains the coprocessor CCA object modules. This library is linked with the object files that constitute the coprocessor piece of the UDX. The result is a coprocessor application executable that contains all of the standard CCA functions and those functions provided by the UDX. The UDX Developer's Toolkit provides two libraries: **csuelib.lib** for use when building a UDX on OS/2 and **csunlib.lib** for use when building a UDX on Windows NT.

A UDX developer defines certain constants (for example, subfunction codes, access control points, and completion codes) during development. There is no guarantee that the values the developer chooses for these constants do not collide with the values the developer of another UDX has chosen. This is generally not a problem since all UDXs used by a particular customer are developed by a single organization and procedures to avoid collisions are adopted.

In order to avoid collisions between UDX constants and constants used by future versions of CCA, the following have been reserved for use by developers writing UDXs:

|                            |  |
|----------------------------|--|
| for subfunction codes,     | "WA" - "WZ", "W0" - "W9", "XA" - "XZ", "X0" - "X9", "YA" - "YZ", and "Y0" - "Y9" |
| for completion codes,      | 0x5000 - 0x5FFF  |
| for access control points, | 0x8000 - 0xFFFF  |



## Host Piece of a UDX

The host piece of a UDX is a dynamic link library (DLL) that converts requests for service from the user's application into one or more calls to the standard CCA host API module (*csuesapi.dll* on OS/2, *csunsapi.dll* on Windows NT). The host piece of a UDX typically checks its input parameters, constructs a request block, sends the request to the coprocessor and receives the reply, extracts the result, and returns the result to the user's application.

This section lists the steps a developer must complete in order to create the host piece of a UDX.

### 1. Define the UDX API.

A prototype for each function the UDX exports to the user's application must be placed in a header file (for example, *csueextrn.h*) that is `#included` by the user's application and by the host piece of the UDX. The header file should also contain any ancillary declarations (for example, constant values) the exported interface requires.

Prototypes for the standard CCA API functions may serve as examples and are located in *csueincl.h* (OS/2 versions) and *csunincl.h* (Windows NT versions). Both header files are part of the UDX Developer's Toolkit. Figure 2-1 illustrates a representative prototype.

```
extern void SECURITYAPI
  CCAXFCN1(long      * return_code,
           long      * reason_code,
           long      * exit_data_length,
           unsigned char * exit_data,
           long      * rule_array_count,
           unsigned char * rule_array,
           unsigned long * key_id_length,
           unsigned char * key_identifier
           );
```

Figure 2-1. Example CCA/UDX Function Prototype

UDX prototypes may have any number of parameters, although for consistency reasons it is recommended that all UDX functions include the first six parameters that appear in Figure 2-1 (`return_code`, `reason_code`, `exit_data_length`, `exit_data`, `rule_array_count`, and `rule_array`). Every parameter must either be a pointer to a 32-bit integer, a pointer to an array of bytes, or a pointer to an array of integers. In the case of arrays, the number of elements in the array is by convention passed in a separate parameter.

The prototype in Figure 2-1 defines a function named `CCAXFCN1`. The function takes these parameters: the array of bytes pointed to by `key_identifier` and the integer pointed to by `key_id_length` which contains the number of bytes in the array.

Refer to the *IBM 4758 PCI Cryptographic Coprocessor CCA Basic Services Reference and Guide* for more information about parameter types.

### 2. Define the subfunction codes for the UDX.

The coprocessor piece of a UDX consists of zero or more command processors. The host piece of the UDX uses a "subfunction code" to identify the command processor to which it wants to send a particular request. The

values of subfunction codes must be defined in a header file (for example, *cxt\_cmds.h*) that is `#included` by both pieces of the UDX. Figure 2-2 on page 2-4 contains an example of such a definition.

A list of the subfunction codes for the standard CCA API functions appears in *cmncrypt2.h*, which is part of the UDX Developer's Toolkit.

```

/*****
** ENTER
** your CCA command extension sub-function codes after this comment.
** =====
**
** The xxxx_ID entry is for unsigned short operations on the 2 byte
** sub-function code. Because of the INTEL architecture the hex
** values are reversed.
**
** The xxxx_ID_S entry is for character string operations on the 2
** byte sub-function code. This is the actual order the character
** code appears in the field.
**
** The following 2 character code points have been reserved for CCA
** extensions. If you use other code points they may conflict with
** existing CCA commands.
**
**      WA - WZ, W0 - W9
**      XA - XZ, X0 - X9
**      YA - YZ, Y0 - Y9
*****/
#define CCAXFNC1_ID      0x4158  /* 'XA' - Sample CCA extension 1 */
#define CCAXFNC1_ID_S   "XA"

```

Figure 2-2. Example UDX Subfunction Codes

### 3. Define new completion codes for the UDX.

A UDX function returns a completion code indicating whether the function succeeded or not (and giving some idea of what caused the failure if one occurred). The standard CCA completion codes are defined in *cmnerrcd.h* and their meanings and use are further clarified in an appendix to the *IBM 4758 PCI Cryptographic Coprocessor CCA Basic Services Reference and Guide*. If no standard code is applicable to a particular situation, new completion codes must be defined in a header file (for example, *cxt\_cmds.h*) that is `#included` in both pieces of the UDX. Figure 2-3 on page 2-5 contains an example of such a definition.

```

/*****
** Enter your CCA extension completion codes after this comment.
** =====
**
** The definition of a completion code (0x00yyzzzz) consists of
** 2 parts. Where:
**         yy is the return code ( 00, 04, 08, 0C, 10 ).
**         zzzz is the reason code.
**
** The following range of 2 byte hex reason codes
** have been reserved for CCA extensions.
**
**         0x5000 - 0x5FFF
*****/
#define CXT_INFO_XXXXXX      0x00005000L /* 00/20480 sample */
#define CXT_WARN_XXXXXX     0x00045001L /* 04/20481 sample */
#define CXT_ERR8_XXXXXX     0x00085002L /* 08/20482 sample */
#define CXT_ERR12_XXXXXX    0x000C5003L /* 12/20483 sample */
#define CXT_ERR16_XXXXXX    0x00105004L /* 16/20484 sample */

```

Figure 2-3. Example UDX Completion Codes

#### 4. Design and code the logic of the host piece of the UDX.

The host piece of a UDX is typically straightforward - it essentially constructs a request block, sends the block to the coprocessor, and parses the result. See Appendix A, "UDX Sample Code - Host Piece" on page A-1 for a sample (*sxt\_samp.c*). This sample can be used as a skeleton and customized to meet the requirements of most UDXs.

In general, the host piece of a UDX should be as small as possible. Most of the work should be performed by the coprocessor piece. This approach makes it much easier to port the host piece to different platforms if the need arises.

#### 5. Export the UDX API entry points.

The entry points in the DLL that implements the host piece of the UDX must be exported so that the user's application can invoke them. Sample link definition files for OS/2 (*csueextn.def*) and for Windows NT (*csunextn.def*) are included in the UDX Developer's Toolkit. An EXPORT statement should be added for each function the UDX exports to the user's application.

#### 6. Build the UDX DLL and LIB files.

The UDX Developer's Toolkit includes sample makefiles for OS/2 (*csueextn.mak*) and for Windows NT (*csunextn.mak*). Statements should be added to compile the source files that contain the host piece of the UDX and create the UDX DLL and library file. The user's application links with the library file to resolve references to the functions the UDX exports.

For further information about the build environment, including required compiler options, refer to "Chapter 3, Developing and Debugging an SCC Application" of the *IBM 4758 PCI Cryptographic Coprocessor Custom Software Developer's Toolkit Guide*.

## Coprocessor Piece of a UDX

The coprocessor piece of a UDX is a collection of one or more command processors that is linked with IBM's CCA coprocessor application modules (*csuelib.lib* on OS/2, *csunlib.lib* on Windows NT) to create an executable that can be loaded into the coprocessor. The coprocessor piece of a UDX may invoke any of the CCA services and can also invoke CP/Q++ functions.

This section lists the steps a developer must complete in order to create the coprocessor piece of a UDX.

### 1. Define the UDX command processor API.

A prototype for each command processor the coprocessor piece of the UDX makes available to the host piece of the UDX must be placed in a header file (for example, *cxt\_cmds.h*) that is `#included` by both pieces of the UDX. The prototype must have the same parameters and return type as the example shown in Figure 2-4.

```

/*****
** Enter
** your CCA command extension function prototypes after this comment.
** =====
**
** The entry points must have the following parameter definitions.
**
** *pCprbIn   - (input) Pointer to the input CPRB. The request
**              parameter block exists immediately after the
**              CPRB area.
** *pCprbOut  - (output) Pointer to an area for returning of the
**              CPRB followed by the reply parameter block.
** RequestId  - (input) Adapter request identifier. It is required
**              as input for some scc.... library calls.
** roleID     - (input) The user's role identifier. It is required
**              as input when checking the requestor's access
**              authority to this function.
*****/
void ccax_fcn_1(
    CPRB_structure *pCprbIn,
    CPRB_structure *pCprbOut,
    unsigned long  RequestId,
    role_id_t      roleID);

```

Figure 2-4. Example UDX Command Processor Prototype

On entry to a command processor:

`pCprbIn` contains the address of a cooperative processing request block (CPRB). The CPRB's contents match the contents of the CPRB pointed to by the `pCprb` argument the host piece of the UDX passed to the call to **CSNC\_SP\_SCSRFBSS** that caused the command processor to gain control.

`pCprbOut` contains the address of a buffer large enough to hold a CPRB header and the result of the operation.

`RequestId` contains a handle generated by the coprocessor operating system that uniquely identifies the message that the host sent to the coprocessor

whose receipt caused the command processor to gain control.<sup>1</sup> A command processor that invokes basic coprocessor operating system functions may need to pass this handle as an argument to those functions.

roleID contains the identifier of the role associated with the host process that caused the command processor to gain control. It can be used to verify that the host process has the proper authority to perform the requested function.

## 2. Define access control points for the UDX.

Associated with each profile on the host is a role, or set of coprocessor operations the profile is allowed to invoke. If access to the functions exported by the coprocessor piece of the UDX needs to be restricted in any way, new “access control point” values must be defined in a header file (for example, *cxt\_cmds.h*) that is #included by both pieces of the UDX. Figure 2-5 contains an example of such a definition.

A command processor can use access control points in conjunction with the role identifier supplied as an argument to the command processor to determine whether or not a particular operation is authorized. See “check\_access\_auth\_fcn - Verify User Authority” on page 13-2 for details.

These values must also be added to the *csuap.def* file in the *cnm* subdirectory of the CCA (for example, Program Files\IBM\4758\cnm). The *cnm* utility uses this file to enable editing of roles. Refer to the *IBM 4758 PCI Cryptographic Coprocessor CCA Support Program Installation Manual* manual for more information.

```

/*****
** Enter
** your CCA command extension access control points after this
** comment.
** =====
**
** The following range of 2 byte hex code points have been reserved
** for CCA extension access control points.
**
**      0x8000 - 0xFFFF
*****/
#define CXT_COMMAND_XXXXXX      0x8000 /* Sample definition. */

```

Figure 2-5. Example UDX Access Control Points

## 3. Add the UDX command processors to the command decoding array.

IBM's CCA coprocessor application modules uses an array to determine which UDX command processor to invoke when a request with a particular subfunction code is received. An entry for each command processor must be added to the *ccax\_cp\_list* array, which must be defined in a program file (for example, *cxt\_cmds.c*) that is compiled with both pieces of the UDX. Each entry contains a subfunction code and the name of the corresponding command processor.

The *ccax\_cp\_list\_size* variable must be initialized to the number of entries in the array.

<sup>1</sup> RequestId is the value returned in the *pRequestHeader->RequestID* output from the call to *sccGetNextHeader* that received the message. Refer to the *IBM 4758 PCI Cryptographic Coprocessor Custom Software Interface Reference* for details.

Figure 2-6 on page 2-8 contains an example of the requisite definitions.

```

/*****
** Enter
** your CCA command extension array entry after this comment.
** =====
**
** Each element of the table is a CCAX_CP_DEF type. That is,
** it contains one 2 character sub-function code, and a
** pointer to the corresponding command processor function.
**
*****/

CCAX_CP_DEF ccax_cp_list[] = { { CCAXFNC1_ID, ccax_fcn_1 },
                              { CCAXFNC2_ID, ccax_fcn_2 } };

/*****
** Declare a variable which holds the number of CCA extension
** command processors defined in the ccax_cp_list table above.
*****/

ULONG ccax_cp_list_size = (sizeof(ccax_cp_list)/sizeof(CCAX_CP_DEF));

```

Figure 2-6. Example UDX Command Decoding Array Definition

#### 4. Design and code the logic of the coprocessor piece of the UDX.

The coprocessor piece of a UDX has access to the same internal functions and services as the CCA coprocessor application modules and may be quite complex. A sample (*cxt\_samp.c*) appears in Appendix B, “UDX Sample Code - Coprocessor Piece” on page B-1. It can be used as a skeleton and customized to meet the requirements of most UDXs.

#### 5. Build the UDX coprocessor executable.

The UDX Developer’s Toolkit includes a sample makefile (*camextrn.mak*) that works on OS/2 and on Windows NT. Statements should be added to compile the source files that contain the coprocessor piece of the UDX. The makefile generates two versions of the UDX binary, one that contains debug information and one that does not. The version without debug information should be incorporated into a read-only disk image using the SCCRODSK utility and downloaded to the coprocessor using the DRUID utility. The version with debug information remains on the host and is used by the ICAT debugger to support source-level debug of the UDX. See the *IBM 4758 PCI Cryptographic Coprocessor Custom Software Developer’s Toolkit Guide* for more information.

**Note:** To securely load your application into a coprocessor requires that the application be signed with keys certified by Development in IBM Charlotte. See the *IBM 4758 PCI Cryptographic Coprocessor Custom Software Developer’s Toolkit Guide* for an explanation of the process to obtain certified keys and to sign your application.

---

## Chapter 3. SCC Functions

The CCA API is built on top of the secure cryptographic coprocessor (SCC) API, a lower level API that allows the host piece of IBM's CCA Support Program to interact with the coprocessor piece of the CCA Support Program and allows the coprocessor piece of the CCA Support Program to perform various cryptographic operations and to manipulate persistent storage on the coprocessor. SCC API functions can also be invoked by a UDX. The SCC API includes a set of functions an application running on the host may invoke (the host-side API) and a set of functions an application running on the coprocessor may invoke (the coprocessor-side API).

This section briefly describes SCC API. A more detailed description may be found in the *IBM 4758 PCI Cryptographic Coprocessor Custom Software Interface Reference*.

---

### Host-Side SCC API Functions

The host-side portion of the SCC API (host API) allows an application running on the host to exchange information with an application running on a coprocessor. The host API provides a uniform interface for applications running on AIX, OS/2, and Windows NT.

Host API calls can be used to determine the number of cryptographic coprocessors installed in the host, establish a communications channel to a specific coprocessor, exchange information via the channel with a specific application running on the coprocessor, and close the channel.

---

### Coprocessor-Side SCC API Functions

The coprocessor API includes functions in the following categories:

| Functions Category                | Description  |
|-----------------------------------|--|
| <b>Communications</b>             | Allows a coprocessor application to interact with a host application and obtain permission to request services from the coprocessor device managers.   |
| <b>Hash</b>                       | Allows a coprocessor application to compute a condensed representation of a block of data using various standard hash algorithms.  |
| <b>DES</b>                        | Allows a coprocessor application to request services from the Data Encryption Standard (DES) Manager, which uses the coprocessor's DES chip to support DES operations with key lengths of 40, 56, 112, or 168 bits and the Commercial Data Masking Facility (CDMF) algorithm. <sup>1</sup> |
| <b>Public Key Algorithm</b>       | Allows a coprocessor application to request services from the Public Key Algorithm (PKA) Manager, which uses the coprocessor's large-integer modular math hardware to support public key cryptographic algorithms.   |
| <b>Large Integer Modular Math</b> | Allows a coprocessor application to direct the PKA Manager to perform specific operations on large integers.   |

| <b>Functions Category</b>  | <b>Description</b>  |
|--|---|
| <b>Random Number Generator</b>   | Allows a coprocessor application to request services from the Random Number Generator (RNG) Manager, which uses a hardware noise source to deliver random bits that meet the standards described in FIPS Publication 140-1, section 4.11. |
| <b>Nonvolatile Memory</b>  | Allows a coprocessor application to request services from the Program Proprietary Data (PPD) Manager, which controls the coprocessor's nonvolatile memory areas (flash memory and battery-backed RAM [BBRAM]).                            |
| <b>Coprocessor Configuration</b>   | Configures certain processor features or return information about the coprocessor.  |
| <sup>1</sup> CDMF is a DES-based data confidentiality algorithm with a key strength equivalent to 40 bits. In general, it is used when import or export regulations prohibit the use of longer keys. |   |



---

## Chapter 4. Communications Functions

In CCA, the host and coprocessor communicate by exchanging well-formed request and reply data blocks. For consistency, UDX routines also follow this paradigm.

This section describes functions needed to allow the host and coprocessor to exchange requests and replies.

### Header Files for Communications Functions

When using these functions, your program must include the following header files.

```
#include "cmncrypt2.h"           /* Cryptographic definitions      */
#include "cmnfunct.h"           /* Common library routines.      */
#include "cassub.h"             /* for Cas_proc_retc             */
```

### Summary of Functions

Request and reply processing includes the following functions.

|                              |  |
|------------------------------|--|
| <b>BuildParmBlock</b>        | Build a parameter block.                     |
| <b>Cas_proc_retc</b>         | Prioritizes a return code in the reply CPRB. |
| <b>CSNC_SP_SCSRFBSS</b>      | Send a request to the coprocessor.           |
| <b>CSUC_BULDCPRB</b>         | Construct a well-formed CPRB block.          |
| <b>CSUC_PROCRETC</b>         | Prioritize a return code.                    |
| <b>FindFirstDataBlock</b>    | Search for the first data block.             |
| <b>FindNextDataBlock</b>     | Search for the next data block.              |
| <b>find_first_key_block</b>  | Search for the first key block.              |
| <b>find_next_key_block</b>   | Search for the next key block.               |
| <b>InitCprbParmPointers</b>  | Initialize CPRB parameter pointers.          |
| <b>keyword_in_rule_array</b> | Search for a keyword in the rule array.      |
| <b>parm_block_valid</b>      | Examine and verify a parameter block.        |
| <b>rule_check</b>            | Verify a rule array.                         |
| <b>saf_process_key_label</b> | Process a key label.                         |

## BuildParmBlock - Build a Parameter Block

**Note:** This function is available on both the host and the coprocessor.

BuildParmBlock constructs a parameter block, containing a two-byte length field, followed by a variable number of data fields. The function accepts pairs of data descriptors, each consisting of a pointer to the data item, and a value containing the item's length. For each pair, the first value is an unsigned short containing the length, and the second value is an unsigned char pointer giving the location of the data.

*BuildParmBlock* is used in building the Reply Parameter Block for the response to a host request as well as the Request Parameter Block.

The function result contains the total length of the block built by the function.

### Function Prototype

```
USHORT BuildParmBlock  
(  
    UCHAR *pBuffer,  
    USHORT pairs,  
    USHORT Data1_length,  
    UCHAR *pData1  
    ... )
```

### Input

On entry to this routine:

*pBuffer* is the starting address of the parameter block section to be built.

*pairs* is the number of argument pairs which are to be added to the parameter block section.

*Data<sub>i</sub>\_length* is the length of the *i*th. item, in bytes.

*Data<sub>i</sub>* is a pointer to the *i*th data item to be added.

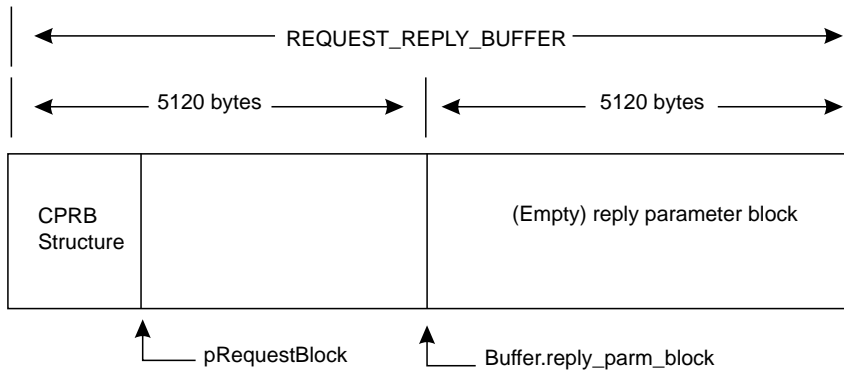
**Note:** If no items are to be added, *Data1\_length* = 0 and *Data1* = NULL.

If 2 or more items of verb unique data are to be added, each item should be preceded by a short field containing the length of the individual item +2. This will allow the function FindNextDataBlock to parse the result.

```

BlockLength = 0;
pCprb = (CPRB *)&(Buffer.request_parm_buffer[0]);
pRequestBlock = &(Buffer.request_parm_buffer[0]) +sizeof(CPRB_structur

```

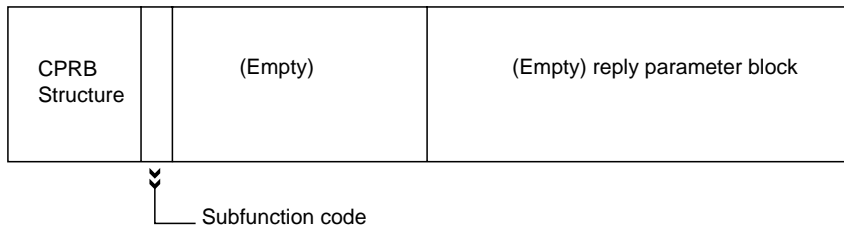


**Step one: add the subfunction code**

```

BlockLength +=2;
*((USHORT *) pReqBlk) = htoas ( CCAXFNC1_ID ) ;

```

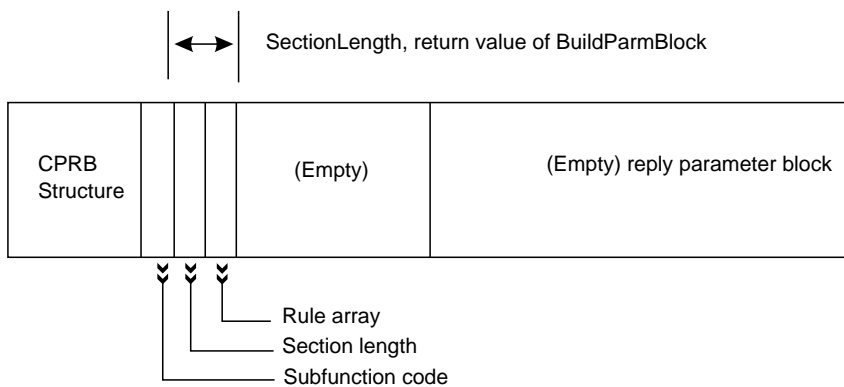


**Step two: add the rule array**

```

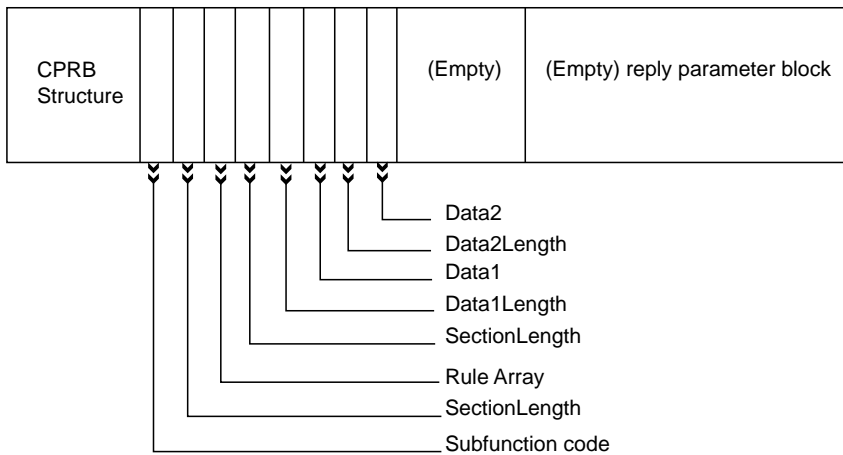
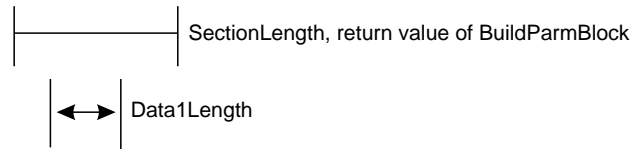
BlockLength += BuildParmBlock(pRequestBlock+BlockLength,
    1, /* adding 1 rule array */
    (*pRuleArrayCount) *8, /* length of rule array */
    pRuleArray);

```



**Step three: add the verb unique data**

```
Data1Length = Data1Size + sizeof(short);
Data2Length = Data2Size + sizeof(short);
BlockLength += BuildParmBlock(pRequestBlock + BlockLength,
                             4, /* adding 2 data items, plus their lengths */
                             sizeof(short), &Data1Length, /* length of 1st item, including this field */
                             Data1Size, pData1,
                             sizeof(short), &Data2Length, /* length of 2nd item, including this field */
                             Data2Size, pData2);
```



**Step four: add the key blocks**

```
KeyHeaderI.Length = KeyTokenLength + sizeof(KEY_FIELD_HEADER);
KeyHeaderI.Flags = storageOptions;

BlockLength = BuildParmBlock(pRequestBlock + BlockLength,
                             2, /*adding a key block header and a key token*/
                             sizeof(KEY_FIELD_HEADER), &KeyHeaderI,
                             KeyTokenLength, &KeyToken);
```

**Output**

On successful exit from this function:

BuildParmBlock returns the total length of the block built by the function. The buffer at pBuffer contains the parameter block.

**Return and Reason Codes**

This function has no return codes.

## **Notes**

### **Building the Parameter Blocks**

There are three types of parameter blocks: the rule array block, the verb unique data block, and the key block. They must all be present in the CPRB message, in this order. If any of the blocks is unnecessary, a length field of 2 must be present to indicate an empty parameter block. This may be achieved by calling `BuildParmBlock(pBuffer, 0,0,NULL);`

The rule array is a byte array, with 8 bytes for each rule present. Each rule is 8 bytes long, padded on the right with spaces. It is important to note that the entire 8 bytes are compared - these are not strings as C and C++ define them. No allowance is made for a null terminator, so be careful when copying rule data into the array. No more than one rule array is used per call, although up to 5 separate rules can be included in the array.

For more information about key block structures, see "Key Blocks" on page 1-11.

See Appendix A, UDX Sample Code - Host Piece for sample code which includes key label to token translation and parameter block building.

### **Byte Alignment of Structures**

It is important that all structures which are passed from the host to the coprocessor or the coprocessor to the host be aligned on 1-byte boundaries. If you are passing a user-defined structure to the coprocessor, either as verb unique data or as key data, you must ensure that your compiler aligns the structure on one-byte boundaries. This can be done by adding a `"#pragma pack(1)"` directive in the include file before the structure is defined, or by compiling with the `"/Zp1"` (for MSVC++) or `"Sp1"` (for VACPP) directives in the makefile.

## Cas\_proc\_retc - Prioritize Return Code

**Note:** This function is available on the coprocessor.

Cas\_proc\_retc is used when you encounter an error, and need to set a return code in the reply CPRB. The function compares your new return code, passed in *msg*, with the return code already present in the CPRB. It uses a priority evaluation scheme to decide whether your new return code, or the one already in the CPRB indicates a more critical error, and it leaves whichever is higher priority in the CPRB.

### Function Prototype

```
long Cas_proc_retc
(
    CPRB_structure *pCprb,
    long           msg
)
```

### Input

On entry to this routine:

*pCprb* is a pointer to the reply CPRB structure.

*msg* is the CCA (SAPI) return code for the error just encountered.

### Output

On successful exit from this routine:

*pCprb->return\_code* and *pCprb->reason\_code* contain the reason codes of *msg*, if the return code of *msg* was greater than the return code formerly in *pCprb->return\_code*.

### Return and Reason Codes

Common return codes generated by this routine are:

- |              |   |
|--------------|---|
| <b>OK</b>    | The operation was successful.   |
| <b>ERROR</b> | The return code in <i>msg</i> was greater than Warning level (level 4). |

## CSNC\_SP\_SCSRFBSS - Send a Request to the Coprocessor

**Note:** This function is available on the host.

CSNC\_SP\_SCSRFBSS passes a request to the coprocessor, and receives the response.<sup>1</sup> The input and output are passed using a pointer to the CPRB structure. The SAPI error code is returned in the variable pointed to by *pMsg*.

If the user is currently logged on to the CCA application in the coprocessor, requests and replies are protected using a MAC computed with the user's session key. This processing is handled automatically when you use CSNC\_SP\_SCSRFBSS.

### Function Prototype

```
long CSNC_SP_SCSRFBSS
(
    CPRB_ptr  pCprb,
    long      *pMsg
)
```

### Input

On entry to this routine:

*pCprb* is a pointer to the CPRB structure. It contains the request CPRB, with the concatenated Request Parameter Block.

*pMsg* is a pointer to a variable for the return code of the function.

### Output

On successful exit from this routine:

*pCprb* contains the reply CPRB, with the concatenated Reply Parameter Block.

*pMsg* is a pointer to a location where the SAPI return code and reason code is stored, on return from the requested function.

CSNC\_SP\_SCSRFBSS returns OK if there were no errors or ERROR if the *pMsg* buffer contains an error.

---

<sup>1</sup> The name of this function is rather obscure. It is inherited from the FBSS interfaces, which later became LAN/DP, the LAN Distributed Platform. This function was a remote procedure call under FBSS, to pass a request to a server where it would be processed. This is also the origin of the CPRB.

### Return and Reason Codes

Common return codes generated by this routine are:

|                          |  |
|--------------------------|--|
| <b>E_ALLOCATE_MEM</b>    | Unable to allocate memory for checking data.                   |
| <b>RT_SWERR</b>          | An error was encountered in the CPRB.                          |
| <b>E_INVALID_MAC_VAL</b> | The data returned from the coprocessor could not be validated. |

Other error codes may be returned, depending on the functions called in the coprocessor section of the code.



## CSUC\_BULDCPRB - Build CPRB

**Note:** This function is available on the host.

CSUC\_BULDCPRB builds a new CPRB from a request or reply block built with BuildParmBlock and an optional data field.

### Function Prototype

```
void CSUC_BULDCPRB
( CPRB_ptr          pCprb,
  unsigned char    *fid_ptr,
  unsigned short   rqpb_l,
  unsigned char    *rqpb_ptr,
  unsigned long    rqdb_l,
  unsigned char    *rqdb_ptr,
  unsigned short   rppb_l,
  unsigned char    *rppb_ptr,
  unsigned long    rpdb_l,
  unsigned char    *rpdb_ptr
)
```

### Input

On entry to this routine:

pCprb is a pointer to the buffer where the new CPRB is returned.

fid\_ptr is a pointer to the two-byte main function ID.

rqpb\_l is the length of the Request Parameter Block, in bytes.

rqpb\_ptr is the address of the Request Parameter Block.

rqdb\_l is the length of the Request Data Block, in bytes.

rqdb\_ptr is a pointer to the Request Data Block. This block must be aligned on a 4-byte boundary, and must be a multiple of 4 bytes long.

rppb\_l is the length of the Reply Parameter Block, in bytes.

rppb\_ptr is the address of the Reply Parameter Block.

rpdb\_l is the length of the Reply Data Block, in bytes.

rpdb\_ptr is a pointer to the Reply Data Block. This block must be aligned on a 4-byte boundary, and must be a multiple of 4 bytes long.

## Output

On successful exit from this routine:

The buffer pointed to by pCprb contains a CPRB structure with the following values:

- `function_id` contains the function ID specified in the call.
- `req_parm_block_length` is the length of the request parameter block.
- `req_parm_block` is the address of the request parameter block (it immediately follows the CPRB).
- `req_data_block_length` is the length of the data block provided in the call.
- `req_data_block` is a pointer to the data in the host memory. It must begin on a 4-byte boundary.
- `reply_parm_block_length` is the length of the reply parameter block.
- `reply_parm_block` is the address of the reply parameter block (it immediately follows the request parameter block).
- `reply_data_block_length` is the length of the reply data block.
- `reply_data_block` is a pointer to the reply data block in the host memory. It must begin on a 4-byte boundary.

**Note:** The request data block and reply data block are not copied into the message which is sent to the coprocessor. The coprocessor will read them directly from the host machine. The communications method requires that they begin on 4-byte boundaries.

## Return and Reason Codes

This function has no return codes.

## CSUC\_PROCRET - Prioritize Return Code

**Note:** This function is available on the host.

CSUC\_PROCRET examines an error code, compares it to the return code already in effect, and sets that return code to whichever of the two is higher priority. If the new return code, passed in *msg*, is more serious than the return code already in the variables pointed to by *return\_code\_ptr* and *reason\_code\_ptr*, then the values pointed to by those parameters are replaced by the new code.

### Function Prototype

```
long CSUC_PROCRET
(
    ADDRESS4_PTR  return_code_ptr,
    ADDRESS4_PTR  reason_code_ptr,
    long          msg
)
```

### Input

On entry to this routine:

*return\_code\_ptr* is a pointer to the current SAPI return code for this verb.

*reason\_code\_ptr* is a pointer to the current SAPI reason code for this verb.

*msg* is an error code corresponding to a new problem, just detected. This code contains both the return code and the reason code for that error, concatenated in a single four-byte integer. The return code occupies the two high-order bytes, while the reason code occupies the two low-order bytes.

### Output

On successful exit from this routine:

*return\_code\_ptr* contains the higher of the original value or the value of the two high bytes of *msg*.

*reason\_code\_ptr* contains the reason code matching the priority of *return\_code\_ptr*.

CSUC\_PROCRET returns OK if the message return code was a warning level (4) or lower, or ERROR if the return code was an error code.

### Return and Reason Codes

This function has no return codes.

## FindFirstDataBlock - Search for Address of First Data Block

**Note:** This function is available on both the host and the coprocessor.

FindFirstDataBlock locates the address of the first data block in the Verb Unique Data (VUD) section of the parameter block attached to the specified CPRB. If the parameter block contains Verb Unique Data, the address of the first data block is returned and the function result is set to TRUE. If there is no Verb Unique Data, the function result is set to FALSE.

### Function Prototype

```
boolean FindFirstDataBlock( CPRB_structure   *pCprb,  
                           unsigned int     ParmBlockChoice,  
                           VUD_DATA_RECORD **ppFirstDataBlock )
```

### Input

On entry to this routine:

pCprb is a pointer to the CPRB, which has the parameter block attached.

ParmBlockChoice is a value of either SEL\_REQ\_BLK or SEL\_REPLY\_BLK, indicating whether the structure you have passed is a Request Parameter Block or a Reply Parameter Block.

### Output

On successful exit from this routine:

ppFirstDataBlock is a location where the function stores the address of the first data block in the Verb Unique Data.

### Return and Reason Codes

This function has no return codes.

## FindNextDataBlock - Search for Address of Next Data Block

**Note:** This function is available on both the host and the coprocessor.

Given the address of a block in the Verb Unique Data (VUD) section of a parameter block, find and return the address of the *next* data block within the same parameter block. If another data block exists, return its address and set the function result to TRUE. If there is no other data block, set the function result to FALSE.

### Function Prototype

```
boolean FindNextDataBlock( CPRB_structure   *pCprb,
                          unsigned int     ParmBlockChoice,
                          VUD_DATA_RECORD *pThisDataBlock,
                          VUD_DATA_RECORD **ppNextDataBlock )
```

### Input

On entry to this routine:

pCprb is a pointer to the CPRB, which has the parameter block attached.

ParmBlockChoice is a value of either SEL\_REQ\_BLK or SEL\_REPLY\_BLK, indicating whether the structure you have passed is a Request Parameter Block or a Reply Parameter Block.

pThisDataBlock is a pointer to the current data block. The function attempts to find the data block *following* the one that this parameter points to.

### Output

On successful exit from this routine:

ppNextDataBlock is a location where the function stores the address of the data block after *pThisDataBlock* or Null if none was found.

FindNextDataBlock returns a boolean value indicating whether a block was found.

### Return and Reason Codes

This function has no return codes.

## find\_first\_key\_block - Search for First Key Data Block

**Note:** This function is available on both the host and the coprocessor.

find\_first\_key\_block finds the address of the first key data block attached to the specified Parameter Block. If there is key data in the parameter block, it returns the address of the first key block, and sets the function result to TRUE. If there is no key data, it sets the function result to FALSE.

This function is used in conjunction with *find\_next\_key\_block*, which is used to locate key blocks after the first one in the parameter block.

### Function Prototype

```
boolean find_first_key_block(CPRB_structure *pCprb,  
                             key_data_structure **first_keyblock,  
                             unsigned int parm_block_choice)
```

### Input

On entry to this routine:

pCprb is a pointer to the CPRB. The parameter block is expected to be concatenated to the CPRB.

parm\_block\_choice is a value of either SEL\_REQ\_BLK or SEL\_REPLY\_BLK, indicating whether the structure you have passed is a Request Parameter Block or a Reply Parameter Block.

### Output

On successful exit from this routine:

first\_keyblock is a location which receives the address of the first key block contained in the parameter block attached to *pCprb*.

find\_first\_key\_block returns a boolean value of true if key data was found, false otherwise.

### Return and Reason Codes

This function has no return codes.

## find\_next\_key\_block - Find Address of Next Key Data Block

**Note:** This function is available on both the host and the coprocessor.

Given the address of a key data block, find and return the address of the next key data block within the specified Parameter Block. If the requested block exist, return its address and set the function result to TRUE. If the block does not exist, set the function result to FALSE.

This function is used in conjunction with *find\_first\_key\_block*, which is used to locate the first key block in the parameter block.

Argument *parm\_block\_choice* indicates whether the parameter block being examined is a Request Parameter Block or a Reply Parameter Block.

### Function Prototype

```
boolean find_next_key_block(CPRB_structure    *pCprb,
                           key_data_structure *this_keyblock,
                           key_data_structure **next_keyblock,
                           unsigned int      parm_block_choice)
```

### Input

On entry to this routine:

*pCprb* is a pointer to the CPRB. The parameter block is expected to be concatenated to the CPRB.

*this\_keyblock* is a pointer to a key block within the parameter block. The function attempts to locate the key block following this one.

*parm\_block\_choice* is a value of either `SEL_REQ_BLK` or `SEL_REPLY_BLK`, indicating whether the structure you have passed is a Request Parameter Block or a Reply Parameter Block.

### Output

On successful exit from this routine:

*next\_keyblock* is a pointer to a location where the function puts the address of the key block following the one specified by *this\_keyblock* or NULL if none was found.

*find\_next\_key\_block* returns a boolean value indicating whether new key data was found.

### Return and Reason Codes

This function has no return codes.

## InitCprbParmPointers - Initialize CPRB Parameter Pointers

**Note:** This function is available on the coprocessor.

InitCprbParmPointers initializes the pointers to the request and reply data buffers for both the input and the output CPRBs. It assumes that these buffers immediately follow the CPRB blocks.

### Function Prototype

```
void InitCprbParmPointers
(
    CPRB_structure    *pInputCprb,
    CPRB_structure    *pOutputCprb
)
```

### Input

On entry to this routine:

pInputCprb is a pointer to the input CPRB block, which has been passed to the coprocessor.

pOutputCprb is a pointer to the output CPRB block, which is returned to the host.

### Output

This function has no output. On successful exit from this routine:

The req\_parm\_block and reply\_parm\_block fields of InputCprb and OutputCprb are correctly initialized.

### Return and Reason Codes

This function has no return codes.



## keyword\_in\_rule\_array - Search for Rule Array Keyword

**Note:** This function is available on both the host and the coprocessor.

keyword\_in\_rule\_array determines whether a specified rule array keyword is present in the rule array passed with the given CPRB. The CPRB contains a pointer to the request parameter block, which in turn contains the rule array and related data.

Input parameters are a pointer to the CPRB, and a string containing the desired keyword. Note that comparisons are case-sensitive (although this should not matter, since all keywords should be in uppercase).

The function returns TRUE if the keyword is in the rule array, and FALSE if it is not.

**Note:** Before using this function, the caller should have verified the integrity of the CPRB using function *parm\_block\_valid*. See page 4-18 for information about *parm\_block\_valid*.

### Function Prototype

```
boolean keyword_in_rule_array
(
    CPRB_structure      *pCprb,
    rule_array_element keyword
)
```

### Input

On entry to this routine:

pCprb is a pointer to the CPRB structure. The parameter block is expected to be concatenated to the end of the CPRB.

keyword is the keyword you are looking for in the rule array.

### Output

On successful exit from this routine:

keyword\_in\_rule\_array returns a boolean value indicating TRUE if the keyword is in the rule array, and FALSE if it is not.

### Return and Reason Codes

This function has no return codes.

## parm\_block\_valid - Examine and Verify a Parameter Block

**Note:** This function is available on both the host and the coprocessor.

parm\_block\_valid examines the parameter block associated with a specified cooperative processing request block (CPRB), and verifies that the parameter block is valid. In particular, it verifies that all the sub-fields and their data are present, so that other functions can use that data with confidence that it is valid. It also verifies that the function ID in the CPRB is that which is expected.

The function returns a value of TRUE if the parameter block is OK, and returns FALSE if it is not.

### Function Prototype

```
boolean parm_block_valid
(
    CPRB_structure *pCprb,
    unsigned int   parm_block_choice
)
```

### Input

On entry to this routine:

pCprb is a pointer to the CPRB structure. The parameter block is expected to be concatenated to the end of the CPRB.

parm\_block\_choice is a value of either SEL\_REQ\_BLK or SEL\_REPLY\_BLK, indicating whether the CPRB contains a Request Parameter Block or a Reply Parameter Block.

### Output

On successful exit from this routine:

parm\_block\_valid returns a boolean value of TRUE if the parameter block is OK, and returns FALSE if it is not.

### Return and Reason Codes

This function has no return codes.

## rule\_check - Verify Rule Array

**Note:** This function is available on both the coprocessor and the host.

`rule_check` can be used to verify the contents of the rule array in a received Request Parameter Block. In the simplest use, it gives a quick indication whether your rule array contains a valid combination of keywords. The function returns a value of TRUE if the rule array appears to be valid, or FALSE if it does not. If it returns FALSE, parameter `pReturn_Message` indicates the cause of the error.

The more complex way to use `rule_check` enables you to determine exactly what rule array elements appear in the request parameter block, without having to search through them yourself. It provides an ordered index, returned in parameter `pRule_value`, where each element of the index corresponds to one keyword, or one group of keywords where *only one* should be in the rule array. In each index element, the function returns a value indicating exactly what rule array keyword appeared, which is useful for the case where one keyword should be used out of a group. Examples later in this section may help clarify the process.

The function operates on the basis of a *rule map*, which describes the rule array elements you expect, and how they should be reported. The map is an array of `RULE_MAP` structures, where `RULE_MAP` is defined as follows.

```
typedef struct
{
    UCHAR    keyword[9];    /* 8 characters plus null terminator */
    BYTE    order_no;      /* Rule array grouping number. */
    int     map_value;     /* Element value within rule array grp */
} RULE_MAP;
```

Figure 4-1. The `RULE_MAP` Structure

The rule map contains one of these structures for each keyword that you expect for your verb. The three elements of the structure have the following meanings.

- |                  |   |
|------------------|---|
| <b>keyword</b>   | This is the eight-character rule array keyword.   |
| <b>order_no</b>  | This integer indicates which element of the returned <code>pRule_value</code> array should be set if the keyword in <code>keyword</code> is present in your rule array.<br><br>A value of 1 refers to the first element of the array, corresponding to a C-language array index of 0. |
| <b>map_value</b> | This is the value that is stored in the output array <code>pRule_value</code> if the rule array keyword in <code>keyword</code> is in your rule array. The value is stored in the element indicated by <code>order_no</code> .  |

### Function Prototype

```
boolean rule_check(
    RULE_BLOCK *pParm_block,
    unsigned int rule_map_count,
    RULE_MAP *pRule_map,
    int *pRule_value,
    long *pReturn_message)
```

## Input

On entry to this routine:

*pParm\_block* is a pointer to the start of the rule array block in your Request Parameter Block. This should point to the start of the *length* field, not to the start of the first rule array element.

*rule\_map\_count* is the number of elements in the array specified by the *pRule\_map* parameter.

*pRule\_map* is a pointer to the rule map for this verb.

*pRule\_value* is a pointer to the array that receives the output rule array index.

**Note:** On input, all elements of *pRule\_value* must be set to the value `INVALID_RULE`.

## Output

On successful exit from this routine:

*pReturn\_message* is a pointer to the location where the function stores the error code, if the rule array is not correct.

*pRule\_value* contains an array of integers, the *ith* integer is the map value of the keyword from the *ith* set which is present in the rule array, or `INVALID_RULE` if there is no keyword from that set.

## Return and Reason Codes

Common return codes generated by this routine are:

|                             |  |
|-----------------------------|--|
| <b>E_RULE_ARRAY_KWD</b>     | Indicates that a required rule array keyword was missing. This also applies if only one keyword must be present out of a group of keywords, but none from the group are in your rule array.                            |
| <b>E_RULE_ARRAY_COMBINE</b> | Indicates that a rule array keyword appears more than one time in the input rule array. It can also indicate that more than one keyword appears from a group, where only one from the group is supposed to be present. |

## Examples

The following examples may help clarify the use of this function.

### Checking the Rule Array for Verb CSNBPKI

CSNBPKI (Key Part Import) requires a rule array that contains exactly one of the following keywords.

- FIRST
- MIDDLE
- LAST

To check the incoming rule array for validity, *rule\_check* can be used with the following three-element rule map.

```
static RULE_MAP RuleMap[3] = { { "FIRST  ", 1, 1 } ,
                               { "MIDDLE ", 1, 2 } ,
                               { "LAST   ", 1, 3 } };
```

Figure 4-2. Example Rule Map for Verb CSNBPKI

This is a *group* of keywords that are mutually exclusive. Only one can appear in the rule array, and for this verb, there are no other keywords that can appear. In the rule map, the values for *order\_no* are the same for each keyword; they all specify a value of 1. This means that when any of these keywords appear in the rule array, the first element of the output array *pRule\_value* is set. The value that goes into the first element of the output array is 1 for FIRST, 2 for MIDDLE, and 3 for LAST, as defined by the *map\_value* elements of the rule map.

Since all three keywords have the same value for *order\_no*, error code *pReturn\_message* is set to E\_RULE\_ARRAY\_COMBINE if more than one of the three keywords is present in your rule array.

### Checking the Rule Array for Verb CSUAACI

CSUAACI (Access Control Initialization) has a slightly more complicated rule array than CSNBPKI described previously. It has the following characteristics.

- The rule array *must* contain exactly one of the following keywords.
  - INIT-AC
  - CHGEXPDT
  - CHG-AD
  - RESET-FC
- The rule array can *optionally* contain the keyword PROTECTD.
- The rule array can *optionally* contain the keyword REPLACE.

To check this rule array, we can use the following six-element rule map.

```
static RULE_MAP RuleMap[6] = { { "INIT-AC ", 1, 1 } ,
                               { "CHGEXPDT", 1, 2 } ,
                               { "CHG-AD  ", 1, 3 } ,
                               { "RESET-FC", 1, 4 } ,
                               { "PROTECTD", 2, 5 } ,
                               { "REPLACE ", 3, 6 } };
```

Figure 4-3. Example Rule Map for Verb CSUAACI

The first four elements describe the keywords for which *only one* must be present. The *order\_no* for each of these is the same; a value of 1. Thus, the first element of output array *pRule\_value* is set when any of these keywords are found in the rule array. The value for *map\_value* is the value that goes into that element of the output array. Thus, if the rule array contains CHGEXPDT, the first element of the output array is set to 2. If more than one of these four keywords is in the rule array, the return code variable *pReturn\_message* is set to E\_RULE\_ARRAY\_COMBINE.

The last two elements, for PROTECTD and REPLACE, describe optional keywords. Any combination of these two is valid - neither, one, or both can be in the rule array. Thus, we treat these independently from any other keywords. They are assigned, respectively, to elements 2 and 3 of the output array, and the values to be stored there are 5 if PROTECTD is present, and 6 if REPLACE is present.

For the following set of rules, where either COPY or REVERSE is required, and OFFSET is optional:

```

int RuleValue[2];          /* to hold the rule values only 2 */
USHORT RuleMapCount = 3;
static RULE_MAP RuleMap[] = { {"COPY   ", 1 , COPY },
                              {"REVERSE ", 1 , REVERSE },
                              {"OFFSET  ", 2 , OFFSET }},};

/*****
error checking, etc.
*****/
/*****
** Compare for valid rule array values.
*****/

RuleValue[0] = INVALID_RULE;          /* initialize */
RuleValue[1] = INVALID_RULE;

if ( rule_check ((RULE_BLOCK *) &pReqBlk->rule_array_length,
                RuleMapCount,
                &RuleMap[0], &RuleValue[0], &ReturnMsg)
    == false)
{
    Cas_proc_retc(pCprbOut, ReturnMsg);
    return;
}
/*****
verb unique data and keys, if needed
*****/

if (RuleValue[1] == OFFSET)
{
    /* Do what OFFSET requires */
} else
{
    /* Do default things */
}

if (RuleValue[0] == COPY)
{
    /* copy the data */
} else if (RuleValue[0] == REVERSE)
{
    /* reverse the data */
}
/*Return needed data */

```

## saf\_process\_key\_label - Process Key Label

**Note:** This function is available on the host.

saf\_process\_key\_label accepts a key label, verifies that it has no errors, and returns an updated label processed according to the following steps.

1. Initializes the output field to all blanks.
2. Makes the label all uppercase.
3. Verifies that the first character is either a letter or a national character.
4. Allows only letters and national characters for the first character.
5. Validates each name token and checks for wildcards.
6. Removes the name token delimiter ('.').
7. Left justifies and copies each name token into an 8-byte output area.

The function result is set to TRUE if the input key label is valid, and to FALSE if it is not.

### Function Prototype

```
boolean saf_process_key_label(  
    unsigned char *pKeyLabel,  
    boolean      wildcard_flag,  
    unsigned char *pLabelOut)
```

### Input

On entry to this routine:

pKeyLabel is a pointer to the input key label.

wildcard\_flag is a boolean value of TRUE if the input key label can have wildcard characters, and FALSE if they are not allowed.

### Output

On successful exit from this routine:

pLabelOut is the process key label produced by the function, if pKeyLabel was a valid label.

saf\_process\_key\_label returns a boolean value indicating TRUE if the input key label is valid, and FALSE otherwise.

### Return and Reason Codes

This function has no return codes.





---

## Chapter 5. Function Control Vector Management Functions

This section describes functions used to interact with the function control vector (FCV) in the coprocessor. The FCV contains information describing what operations are permitted on this coprocessor, based on the export regulations governing the coprocessor's location and the business of its owner.

The FCV is loaded into the coprocessor using the *csuncnm* utility on Windows NT, *csuecnm* utility on OS/2, and the *csufcnm* utility on AIX. Refer to *IBM 4758 PCI Cryptographic Coprocessor CCA Support Program Installation Manual* for more detailed information.

**Note:** All functions within this chapter are available only on the coprocessor.

### Header Files for Function Control Vector Management Functions

When using these functions, your program must include the following header files.

```
#include "cmncrypt2.h"           /* Crypto ESSS definitions    */
#include "cam_fcv.h"            /* Function control vector def. */
```

### Summary of Functions

Functions that interact with FCV include the following:

|                                     |  |
|-------------------------------------|--|
| <b>getSymmetricMaxModulusLength</b> | Gets the maximum RSA key length.                         |
| <b>isFunctionEnabled</b>            | Determines whether the FCV allows a particular function. |

## getSymmetricMaxModulusLength - Get RSA Key Length

getSymmetricMaxModulusLength returns the maximum RSA key modulus length (in bits) that can be used for encrypting symmetric algorithm encryption keys.

### Function Prototype

```
long getSymmetricMaxModulusLength(  
    unsigned short * pModLength)
```

### Input

pModLength is a pointer to an unsigned short variable.

### Output

On successful exit from this routine:

pModLength contains the modulus maximum length.

### Return Codes

Common return codes generated by this routine are:

|                           |                                |
|---------------------------|--------------------------------|
| <b>OK</b>                 | The operation was successful.  |
| <b>srdi_ALLOC_ERROR</b>   | Out of memory to open the FCV. |
| <b>srdi_READ_ERROR</b>    | Error reading the FCV.         |
| <b>srdi_GENERAL_ERROR</b> | Could not read the FCV.        |
| <b>srdi_NOT_FOUND</b>     | The FCV was not found.         |

## **isFunctionEnabled - Check Whether a Function is Enabled**

isFunctionEnabled returns a boolean value indicating whether the specified function is enabled or disabled in the Function Control Vector. This is used to determine whether a function is permitted under the export rules governing this particular coprocessor.

The function result is TRUE if the specified function is enabled, and FALSE if it is disabled.

### **Function Prototype**

```
boolean isFunctionEnabled(  
    long          FunctionByteIndex,  
    unsigned char FunctionBitSelect)
```

### **Input**

On entry to this routine:

FunctionByteIndex is an index into the Function Control Vector, giving the location of the byte to be checked. See Figure 5-1 on page 5-4 for a list of possible values.

FunctionBitSelect is the bit to be checked in the specified Function Control Vector byte. See Figure 5-1 on page 5-4 for a list of possible values.

### **Output**

On successful exit from this routine:

isFunctionEnabled returns a boolean value indicating whether the specified function is enabled or disabled in the Function Control Vector.

## Notes

The following figure shows how the byte or bit corresponds to a particular function.

*Figure 5-1. Possible Values*

| Function Byte Name     | Function Bit Name | Description                                  |
|------------------------|-------------------|--|
| CCA_BASE_FUNCTION_BYTE |                   | Byte index of the CCA base services bits.    |
|                        | FCV_CCA_BASE      | Base CCA services-enabled bit.               |
| DES_FUNCTION_BYTE      |                   | Byte index of the DES-enabled bits.          |
|                        | FCV_CDMF_DES      | CDMF function-enabled bit                    |
|                        | FCV_56_BIT_DES    | 56-bit DES enabled bit                       |
|                        | FCV_TRIPLE_DES    | Triple DES enabled bit                       |
| SET_FUNCTION_BYTE      |                   | Byte index of the bits that are SET™ enabled |
|                        | FCV_SET_SERVICES  | SET services enabled bits                    |

## Return Codes

This function has no return codes.

## Examples

To determine whether SET functions for encoding and decoding are enabled in the coprocessor:

```
if (! IsFunctionEnabled(SET_FUNCTION_BYTE, FCV_SET_SERVICES) )
{
    /* cancel this section, SET functions are not allowed. */
}
```

To see if 56-bit DES encryption is allowed:

```
if ( IsFunctionEnabled(DES_FUNCTION_BYTE, FCV_56_BIT_DES) )
{
    /* use 56-bit DES encryption */
}
```

---

## Chapter 6. CCA Master Key Manager Functions

### Header Files for Master Key Manager Functions

When using these functions, your program must include the following header files.

```
#include "cmncrypt.h"           /* Cryptographic definitions */
#include "cam_xtrn.h"           /* SRDI manager definitions */
```

The CCA Master Key Manager provides access to the CCA master key registers on the PCI cryptographic coprocessor, as required by the CCA application. The CCA command processors never access the master keys directly, and in fact they have no need to know how or where the master keys and related information are stored. The Master Key Manager provides a set of functions to load the key values, and to use the keys to encipher and decipher data. It can be viewed as an object, with internal data, and with methods that can be used to operate on and with that data.

Since the master key storage mechanism is hidden from master key users, that mechanism can be changed without affecting any command processors that make use of the master keys. In the coprocessor, the master key data is stored in flash EPROM.

**Note:** All functions within this chapter are available only on the coprocessor.

---

### Overview of the Coprocessor CCA Master Keys

The coprocessor uses triple-length master keys, each consisting of three independent eight-byte DES keys. The master keys are used to protect other data in the following two ways.

- Single-length (eight-byte) keys are protected using EDE encryption, with three independent keys. To encrypt an eight-byte key K with master key M, the process is as follows:
  1. Encrypt K using part 1 of key M.
  2. Decrypt the result of step 1 using part 2 of key M.
  3. Encrypt the result of step 2 using part 3 of key M.
- Data longer than eight bytes, such as PKA key components, is encrypted using the EDE3 triple encryption algorithm.

CCA supports two sets of master keys, one set for PKA keys (ASYM\_MK) and a second set for DES keys (SYM\_MK). Each set consists of three master key values.

- Old Master Key (OMK)—The version of the master key that was in use prior to the current value. It is maintained to permit recovery of keys that were enciphered under the old master key.
- Current Master Key (CMK)—The current, operational master key. All keys in use in the system are enciphered under this key.
- New Master Key (NMK)—A new master key, which is being entered into the system to replace the current master key. It is entered in the form of one or more *key parts*, which are combined to form the final key.

Each of the three master keys is stored in a logical *register* within the Master Key Manager. In addition, the Master Key Manager holds data associated with each of these key values.

- A **Verification Pattern** is stored for each of the three keys. The verification pattern is a 20-byte value which is calculated using a strong one-way function on the key value. This value can be used to verify that the key value matches another key, or the key originally used in some process. The verification pattern can be public, without endangering the value of the key itself.

This value is calculated using SHA-1.

- The **status** of the key. For the CMK and the OMK, two status values are possible.
  - The register contains a valid key value.
  - The register does not contain a valid key value.

For the NMK register, three status values are possible.

- The register is empty. It does not contain any portion of a new master key value.
- The register is partially full. The last key part has not yet been combined into the value in the register.
- The NMK register is full. All key parts have been combined to form the final key value.

The verification pattern and the status can be read from the Master Key Manager using its interface functions. The values of the keys themselves can never be read.

## Location of the Master Keys

The master keys and their associated data are Security Relevant Data Items (SRDIs). Their secure storage and retrieval are handled through use of the SRDI Manager, and its API functions.

Each SRDI has an eight character name. The master key data SRDI for DES keys is named MSTRKEYS. The master key data SRDI for asymmetric keys is ASYMKMKS.

## Initialization of the Master Key SRDI

When the CCA application is first loaded into a new coprocessor, no master key SRDI exists in the flash EPROM. The Master Key Manager includes an initialization function *init\_master\_keys()*, which creates and initializes this SRDI the first time it is called. The SRDI is initialized with the following values.

- The three master key registers, NMK, CMK, and OMK, are all set to binary zeroes.
- The state of CMK and OMK is set to *invalid*. The state of NMK is set to *Empty*.
- The master key verification patterns are set to binary zeroes.

## CCA Master Key Manager Interface Functions

The following sections describe the functions that comprise the Master Key Manager interface. CCA command processors use these functions to manage master key values, and to encipher or decipher data using the master keys.

Each of these functions returns an error code as the function result.

### Common Entry Processing

A portion of the processing is common to all of the Master Key Manager interface functions. This code is in a common function, which is called by each of the API functions listed as follows.

The common entry processing performs the following functions.

1. If the Master Key Manager has already opened the Master Key SRDI, then error code *mk\_NO\_ERROR* is returned to the caller. Otherwise, continue with step 2.
2. Open the Master Key SRDI, *MSTRKEYS*. If no error occurs opening the SRDI, then error code *mk\_NO\_ERROR* is returned to the caller. Otherwise, error code *mk\_SRDI\_OPEN\_ERROR* is returned.

### Required Variables

In order to specify which master key register is to be used, many of the master key functions require a variable of type *mk\_selectors*. This variable has three parameters:

- The master key set (*mk\_set*) that specifies which set of master keys is to be accessed, for environments where more than one set of master keys may exist. Where there is only one set of master keys, *mk\_set* must be set to *MK\_SET\_DEFAULT*.
- The master key register (*mk\_register*) within the specified master key set. This can be any of the defined values *old\_mk*, *current\_mk*, or *new\_mk*, representing the old master key, the current master key, and the new master key.
- The master key type (*type\_mks*) which defines the type of key to be encrypted with this set of master keys. This variable can be any of *ASYM\_MK*, *SYM\_MK*, or *BOTH\_MK*.

The following functions are summarized in this chapter.

| Function                                    | Page |
|---|------|
| <i>clear_master_keys</i>                    | 6-6  |
| <i>combine_mk_parts</i>                     | 6-7  |
| <i>compute_mk_verification_pattern</i>      | 6-19 |
| <i>ede3_triple_decrypt_under_master_key</i> | 6-26 |
| <i>ede3_triple_encrypt_under_master_key</i> | 6-27 |
| <i>generate_mk_shares</i>                   | 6-9  |
| <i>generate_random_mk</i>                   | 6-11 |
| <i>get_master_key_status</i>                | 6-21 |

| <b>Function</b>                         | <b>Page</b> |
|---|-------------|
| get_mk_verification_pattern             | 6-23        |
| init_master_keys                        | 6-12        |
| mkmCombineMKParts                       | 6-7         |
| mkmGenerateMKShares                     | 6-9         |
| mkmGenerateRandomMK                     | 6-11        |
| mkmGetAsymVerificationPattern           | 6-24        |
| mkmLoadFirstMKPart                      | 6-13        |
| mkmLoadMKFromShares                     | 6-14        |
| mkmSetMasterKey                         | 6-17        |
| reinit_master_keys                      | 6-16        |
| TDESDecryptUnderMasterKey               | 6-28        |
| TDESEncryptUnderMasterKey               | 6-29        |
| triple_decrypt_under_master_key         | 6-30        |
| triple_decrypt_under_master_key_with_CV | 6-31        |
| triple_encrypt_under_master_key         | 6-32        |
| triple_encrypt_under_master_key_with_CV | 6-33        |



---

## Functions to Set and Manage the Master Key Values

The following functions are used to load, clear, or initialize master key registers. Other functions in this category are used in other ways related to generation and distribution of master keys.

### Summary of Functions

|                            |  |
|----------------------------|--|
| <b>clear_master_keys</b>   | Clears a specified master key register.  |
| <b>combine_mk_parts</b>    | Combines an additional master key part into the value already in the New Master Key register.                                  |
| <b>generate_mk_shares</b>  | Splits a 24-byte master key into shares.   |
| <b>generate_random_mk</b>  | Generates a random 24-byte master key.   |
| <b>init_master_keys</b>    | Creates and initializes the master key SRDI.   |
| <b>load_first_mk_part</b>  | Loads the first part of a multi-part master key into the new master key register.  |
| <b>load_mk_from_shares</b> | Reconstructs the shares that were produced using generate_mk_shares and loads the master key into the new master key register. |
| <b>mkmCombineMKParts</b>   | Combines an additional master key part into the value already in the New Master Key register.                                  |
| <b>mkmGenerateMKShares</b> | Splits a 24-byte master key into shares.   |
| <b>mkmGenerateRandomMK</b> | Generates a random 24-byte master key.   |
| <b>mkmLoadFirstMKPart</b>  | Loads the first part of a multi-part master key into the new master key register.  |
| <b>mkmLoadMKFromShares</b> | Reconstructs the shares that were produced using generate_mk_shares and loads the master key into the new master key register. |
| <b>reinit_master_keys</b>  | Deletes all master key data and then creates and initializes the master key SRDI.  |
| <b>set_master_key</b>      | Activates the master key.  |

## clear\_master\_keys - Clear Master Key

clear\_master\_keys clears a specified master key register. All bytes of the specified register are set to a value of X'00', and the state of the register is set to *Empty* for NMK, or *invalid* for CMK or OMK.

Three separate calls are required in order to clear *all* of the master key registers.

### Function Prototype

```
long clear_master_keys(mk_selectors MKSelector);
```

### Input

On entry to this routine:

mk\_selector is a pointer to a variable which must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register is set to either old\_mk, current\_mk, or new\_mk, representing the key which should be cleared.
- type\_mks should be set to ASYM\_MK if this set of master keys is intended for PKA key encryption or SYM\_MK if this set of master keys is used for DES key encryption. If type\_mks is BOTH\_MK and the state of the specified master key register of both the master key sets is the same, the specified master key register will be cleared and the state set to empty for both master key registers; otherwise an error message will be returned.

### Output

This function returns no output. On successful exit from this routine:

clear\_master\_keys clears a specified master key register.

### Return Codes

Common return codes generated by this routine are:

|                                |                                       |
|--------------------------------|---------------------------------------|
| <b>mk_NO_ERROR</b>             | The operation was successful.         |
| <b>mk_SRDI_OPEN_ERROR</b>      | Could not open the master key SRDI.   |
| <b>mk_INVALID_KEY_SELECTOR</b> | The input parameters are not valid.   |
| <b>mk_SEM_CLAIM_FAILED</b>     | Could not access the master key SRDI. |

## mkmCombineMKParts - Combine Master Key Parts

mkmCombineMKParts combines an additional master key part into the value already in the NMK register for the `mk_set` being processed. The NMK register must be in the Partially Full state when this function is called; otherwise, an error is returned. The key part is designated as the *final* part, if the key is complete after this part has been combined into the register.

Return codes are used to notify the caller if the combined key value has bad parity, or if it has equal left and right halves. These are informative return codes, and are not considered errors by the Master Key Manager.

**Note:** The purpose behind requiring a `load_first_mk_part` separately from `combine_mk_parts` is to enforce security. Different roles may be required for each of these functions, ensuring that no one person has input all of the parts of the master key.

### Function Prototype

```
long mkmCombineMKParts(TRIPLE_LENGTH_KEY *key_part,
                      mk_selectors      MKSelector,
                      boolean           final_part);
long combine_mk_parts (TRIPLE_LENGTH_KEY *key_part,
                     boolean           final_part);
```

The `combine_mk_parts` function is the equivalent of calling the `mkmCombineMKParts` with the `MKSelector` variable set to `{MK_SET_DEFAULT, current_mk, SYM_MK}`

### Input

On entry to this routine:

`key_part` is a 24-byte cleartext key part, which is combined into the value in the NMK register.

`MKSelector` is a parameter of type `mk_selectors`, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- `mk_set` is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to `MK_SET_DEFAULT`.
- `mk_register` must be set to `new_mk` or `current_mk`
- `type_mks` should be set to `ASYM_MK` if this set of master keys is intended for PKA key encryption or `SYM_MK` if this set of master keys is used for DES key encryption. If `type_mks` is `BOTH_MK` and the state and the value of the new master key register of both the master key sets is the same, the key part will be combined into both new master key registers; otherwise an error message will be returned.

`final_part` is a boolean value, which the caller sets to `TRUE` when the key part is the final part of a new master key.

The NMK register must have been initialized with a call to `load_first_mk_part` and zero or more calls to `combine_mk_parts`.

## Output

This function returns no output. On successful exit from this routine:

mkmCombineMKParts combines an additional master key part into the value already in the NMK register. If `final_part` was TRUE, the NMK register is left in a Full state. Otherwise, the state of NMK is Partially Full.

## Return Codes

Common return codes generated by this routine are:

|                            |   |
|----------------------------|---|
| <b>mk_NO_ERROR</b>         | The operation was successful.   |
| <b>mk_SRDI_OPEN_ERROR</b>  | Could not open the master key SRDI.   |
| <b>mk_SEM_CLAIM_FAILED</b> | Could not access the SRDI Manager, the operation cannot be completed.                                     |
| <b>mk_INCORRECT_STATE</b>  | The New Master Key register was not Partially Full.   |
| <b>mk_WEAK_KEY</b>         | <code>final_part</code> was TRUE and the resulting key was a weak key. The prior state has been restored. |

## mkmGenerateMKShares - Generate Master Key Shares

mkmGenerateMKShares splits a 24-byte master key into shares for the `mk_set` being processed. The key is split into  $n$  separate shares, where any  $m$  of the shares can be used to recreate the master key value at a later time.

The shares are distributed to separate individuals for safekeeping. When the coprocessor has to be initialized with the master key, any  $m$  of these individuals must present their master key shares in order to create the complete key in the coprocessor.

The source of the master key is specified with the *KeySource* parameter.

### Function Prototype

```

long mkmGenerateMKShares(mk_selectors  MKSelector,
                        mk_src_t       KeySource,
                        UCHAR          mShareKey,
                        UCHAR          nShareGen,
                        UCHAR          *pShares[]);
long generate_mk_shares (mk_src_t       KeySource,
                        UCHAR          mShareKey,
                        UCHAR          nShareGen,
                        UCHAR          *pShares[]);

```

The `generate_mk_shares` function is the equivalent of calling the `mkmGenerateMKShares` with the `MKSelector` parameter set to `{MK_SET_DEFAULT, current_mk, SYM_MK}`.

### Input

On entry to this routine:

`MKSelector` is a parameter of type `mk_selectors`, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- `mk_set` is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to `MK_SET_DEFAULT`.
- `mk_register` must be set to `new_mk` or `current_mk`
- `type_mks` should be set to `ASYM_MK` if this set of master keys is intended for PKA key encryption or `SYM_MK` if this set of master keys is used for DES key encryption. If `type_mks` is `BOTH_MK` and the key source is the new, current, or old master key register, and the state and value of the specified master key register is the same for both the master key sets, the shares will be generated from the specified register; otherwise an error message will be returned.

`KeySource` is a value which specifies the source for the master key value that is split. The possible values are:

#### Source

Randomly generated value  
(`src_random`)

#### Description

The function generates a new, random key value, and splits it into the specified number of shares. The value is discarded after the shares have been returned.

| Source   | Description   |
|--|---|
| New Master Key (NMK) Register<br>(src_nmk)     | The value in the NMK register is split into shares.<br>An error is returned if the NMK state is not <i>Full</i> .           |
| Current Master Key (CMK) Register<br>(src_cmk) | The value in the CMK register is split into shares.<br>An error is returned if the register does not contain a valid value. |
| Old Master Key (OMK) Register<br>(src_omk)     | The value in the OMK register is split into shares.<br>An error is returned if the register does not contain a valid value. |

mShareKey is the number of shares that are required in order to reconstruct the master key value. This is the number of shares that must be given to the function *load\_mk\_from\_shares* in order to load the key.

nShareGen is the total number of shares to generate and return. Any *m* of these shares can be used to reconstruct the key.

pShares is a pointer to an area which is large enough to store *n* key shares, each of which is 25 bytes in length.

## Output

On successful exit from this routine:

\*pShares[] is a pointer to an array where the function stores the generated key shares. This area must be large enough to hold *n* key shares, each of which is 25 bytes in length.

## Return Codes

Common return codes generated by this routine are:

|                                |   |
|--------------------------------|---|
| <b>mk_NO_ERROR</b>             | The operation was successful.   |
| <b>mk_SRDI_OPEN_ERROR</b>      | Could not open the master key SRDI.                                   |
| <b>mk_SEM_CLAIM_FAILED</b>     | Could not access the SRDI Manager, the operation cannot be completed. |
| <b>mk_INCORRECT_STATE</b>      | The master key is not valid.  |
| <b>mk_UNSUPPORTED_SCHEME</b>   | The values of mShareKey and nShareGen were inconsistent.              |
| <b>mk_KEY_SHARE_SPLIT_FAIL</b> | An error occurred in the splitting process.                           |

## mkmGenerateRandomMK - Generate Random Master Key

mkmGenerateRandomMK generates a random 24-byte master key, and stores the value in the NMK register for the `mk_set` being processed.

The NMK register must be in the *Empty* state when this function is called; otherwise, an error is returned. If the function completes successfully, the NMK register is left in the *Full* state.

### Function Prototype

```
long mkmGenerateRandomMK(mk_selectors MKSelector);
long generate_random_mk (void);
```

The `generate_random_mk` function is the equivalent of calling the `mkmGenerateRandomMK` with the `MKSelector` parameter set to `{MK_SET_DEFAULT, current_mk, SYM_MK}`.

### Input

On entry to this routine:

`MKSelector` is a parameter of type `mk_selectors`, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- `mk_set` is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to `MK_SET_DEFAULT`.
- `mk_register` must be set to `new_mk` or `current_mk`
- `type_mks` should be set to `ASYM_MK` if this set of master keys is intended for PKA key encryption or `SYM_MK` if this set of master keys is used for DES key encryption. If `type_mks` is `BOTH_MK` and the new master key register of both the master key sets is empty, a random master key will be generated and loaded into both new master key registers; otherwise an error message will be returned.

### Output

This function returns no output. On successful exit from this routine:

The new master key is generated and stored in the NMK register. In order to use this master key, `set_master_key()` must be called.

### Return Codes

Common return codes generated by this routine are:

|                            |   |
|----------------------------|---|
| <b>mk_NO_ERROR</b>         | The operation was successful.   |
| <b>mk_SRDI_OPEN_ERROR</b>  | Could not open the master key SRDI.   |
| <b>mk_SEM_CLAIM_FAILED</b> | Could not access the SRDI Manager, the operation cannot be completed.   |
| <b>mk_INCORRECT_STATE</b>  | The master key is in the incorrect state. If the verification patterns match with the previous, current, or old master keys, another random key is generated. |
| <b>mk_SAVE_ERROR</b>       | Unable to save the master key to flash memory.  |

## init\_master\_keys - Create and Initialize Master Keys

init\_master\_keys creates and initializes the master key SRDI, if it doesn't already exist.

### Function Prototype

```
long init_master_keys(void);
```

### Input

This function has no input.

### Output

This function returns no output. On successful exit from this routine:

The master key SRDI is generated and initialized.

### Return Codes

Common return codes generated by this routine are:

|                           |   |
|---------------------------|---|
| <b>mk_NO_ERROR</b>        | The operation was successful.                             |
| <b>srdi_EXISTS</b>        | The master keys already exist, and cannot be initialized. |
| <b>srdi_GENERAL_ERROR</b> | Failed to access the SRDI manager.                        |
| <b>srdi_ALLOC_ERROR</b>   | Could not allocate memory for the master keys.            |



## mkmLoadFirstMKPart - Load First Master Key Part

mkmLoadFirstMKPart loads the first part of a multi-part cleartext master key into the new master key (NMK) register for the mk\_set being processed.

**Note:** The purpose behind requiring a load\_first\_mk\_part separately from combine\_mk\_parts is to enforce security. Different roles may be required for each of these functions, ensuring that no one person has input all of the parts of the master key.

### Function Prototype

```
long mkmLoadFirstMKPart(TRIPLE_LENGTH_KEY *key_part,
                        mk_selectors      MKSelector);
long load_first_mk_part(TRIPLE_LENGTH_KEY *key_part);
```

The load\_first\_mk\_part function is the equivalent of calling the mkmLoadFirstMKPart function with the MKSelector parameter set to {MK\_SET\_DEFAULT, current\_mk, SYM\_MK}.

### Input

On entry to this routine:

key\_part is a 24-byte cleartext key part, which is stored in the NMK register.

The check\_and\_adjust parity routines make sure that the input key part has odd parity. If it does not, the parity is adjusted.

MKSelector is a parameter of type mk\_selectors, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register must be set to new\_mk or current\_mk
- type\_mks should be set to ASYM\_MK if this set of master keys is intended for PKA key encryption or SYM\_MK if this set of master keys is used for DES key encryption. If type\_mks is BOTH\_MK and the new master key register of both the master key sets is empty, the key part will be loaded into both new master key registers; otherwise an error message will be returned.

### Output

This function returns no output. On successful exit from this routine:

load\_first\_mk\_part loads the first part of a multi-part cleartext master key into the new master key register.

### Return Codes

Common return codes generated by this routine are:

**mk\_NO\_ERROR** The operation was successful.

**mk\_bad\_key\_parity** The input parity has been adjusted to odd parity.

## mkmLoadMKFromShares - Load Master Key Shares

mkmLoadMKFromShares loads a master key into the New Master Key register, reconstructing the key from *m* supplied shares, which were originally produced by the *generate\_mk\_shares* function for the *mk\_set* being processed.

The shares are distributed to separate individuals for safekeeping. When the coprocessor has to be initialized with the master key, any *m* of these individuals must present their master key shares to create the complete key in the coprocessor.

The New Master Key (NMK) register must be in the *Empty* state when this function is called. It is in the *Full* state if the function completes successfully. The key value is left in the NMK register; you must use the *set\_master\_key* function to make it the current master key.

### Function Prototype

```
long mkmLoadMKFromShares(mk_selectors MKSelector,
                        UCHAR          mShareKey,
                        UCHAR          nShareGen,
                        UCHAR          *pShares[]);
long load_mk_from_shares(UCHAR          mShareKey,
                        UCHAR          nShareGen,
                        UCHAR          *pShares[]);
```

The *load\_mk\_from\_shares* function is the equivalent of calling the *mkmLoadMKFromShares* function with the *MKSelector* parameter set to {*MK\_SET\_DEFAULT*, *current\_mk*, *SYM\_MK*}.

### Input

On entry to this routine:

*MKSelector* is a parameter of type *mk\_selectors*, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- *mk\_set* is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to *MK\_SET\_DEFAULT*.
- *mk\_register* must be set to *new\_mk* or *current\_mk*
- *type\_mks* should be set to *ASYM\_MK* if this set of master keys is intended for PKA key encryption or *SYM\_MK* if this set of master keys is used for DES key encryption. If *type\_mks* is *BOTH\_MK* and the new master key register of both the master key sets is empty, both new master key registers will be loaded with the master key value; otherwise an error message will be returned.

*mShareKey* is the number of shares required to reconstruct the master key. This is the number of shares that are provided in the *shares[]* array.

*nShareGen* is the total number of shares that were generated for this key, by the *generate\_mk\_shares* function.

*\*pShares[]* is a pointer to an array which contains the *m* shares that are used to reconstruct the master key. Each share is 25 bytes in length.

**Output**

This function has no output. On successful exit from this routine:

The new master key is generated in the NMK register.

**Return Codes**

Common return codes generated by this routine are:

|                                   |  |
|-----------------------------------|--|
| <b>mk_NO_ERROR</b>                | The operation was successful.  |
| <b>mk_SRDI_OPEN_ERROR</b>         | Unable to open the SRDI item.  |
| <b>mk_SEM_CLAIM_FAILED</b>        | Unable to access the SRDI Manager.   |
| <b>mk_INCORRECT_STATE</b>         | The NMK is not in the Empty state.   |
| <b>mk_UNSUPPORTED_SCHEME</b>      | mShareKey or nShareGen have invalid values.  |
| <b>mk_KEY_SHARE_RECOVER_FAIL</b>  | Unable to recover the master key.  |
| <b>mk_VP_CALCULATE_FAIL</b>       | SHA calculation error.   |
| <b>mk_SAVE_ERROR</b>              | An SRDI error occurred while attempting to save the new master key in flash memory.        |
| <b>mk_VP_MATCHES_EXISTING_KEY</b> | Verification patterns match one of the existing master keys.                               |
| <b>mk_EQUAL_KEY_HALFS</b>         | Two of the three parts of the new key are equal. This is a warning, no action is required. |
| <b>mk_WEAK_KEY</b>                | One of the key parts is a weak key. The key should be regenerated before use.              |

## reinit\_master\_keys - Reinitialize Master Keys

reinit\_master\_keys deletes all master key data, then recreates and initializes the master key SRDI to the default state.

The function returns TRUE if the operation completed successfully, and FALSE if it did not.

**Note:** This function erases master key data. Once this function is complete, all operational keys which have been encrypted under any master key are unusable.

### Function Prototype

```
long reinit_master_keys(void);
```

### Input

This function has no input.

### Output

This function returns no output. On successful exit from this routine:

All master keys are created and initialized.

### Return Codes

Common return codes generated by this routine are:

|                           |                                       |
|---------------------------|---------------------------------------|
| <b>srdi_NO_ERROR</b>      | The operation was successful.         |
| <b>srdi_GENERAL_ERROR</b> | Unable to access the master key SRDI. |

## mkmSetMasterKey - Set Master Key

mkmSetMasterKey activates the master key which has been accumulated in the NMK register for the mk\_set being processed. The key value is transferred to the Current Master Key (CMK) register. If a valid key is present in the CMK register, it is transferred to the Old Master Key (OMK) register. The key verification patterns are transferred from CMK to OMK, and from NMK to CMK.

### Function Prototype

```
Long mkmSetMasterKey(mk_selectors *pMKSelector);
Long set_master_key (void);
```

The set\_master\_key function is the equivalent of calling the mkmSetMasterKey function with the MKSelector parameter set to {MK\_SET\_DEFAULT, current\_mk, SYM\_MK}.

### Input

On entry to this routine:

MKSelector is a parameter of type mk\_selectors, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register must be set to new\_mk or current\_mk
- type\_mks should be set to ASYM\_MK if this set of master keys is intended for PKA key encryption or SYM\_MK if this set of master keys is used for DES key encryption. If type\_mks is BOTH\_MK and the new master key register of both the master key sets is full and the value in the new master key register of both the new master key sets is the same, then the current\_mk registers will be set to the new\_mk value; otherwise an error message will be returned.

### Output

This function returns no output. On successful exit from this routine:

The master keys have been changed.

### Return Codes

Common return codes generated by this routine are:

|                            |  |
|----------------------------|--|
| <b>mk_NO_ERROR</b>         | The operation was successful.                    |
| <b>mk_SRDI_OPEN_ERROR</b>  | Unable to open the SRDI item.                    |
| <b>mk_SEM_CLAIM_FAILED</b> | Unable to access the SRDI Manager.               |
| <b>mk_INCORRECT_STATE</b>  | The NMK register is not in the Full state.       |
| <b>mk_SAVE_ERROR</b>       | Unable to save the master key into flash memory. |

---

## Functions to Check Master Key Values and Status

### Summary of Functions

|  |   |
|--|---|
| <code>compute_mk_verification_pattern</code> | Computes a key verification pattern.  |
| <code>get_mk_verification_pattern</code>     | Returns the 20-byte master key verification pattern for a specified master key. |
| <code>mkmGetAsymVerificationPattern</code>   | Returns the verification pattern for asymmetric master keys.                    |

## compute\_mk\_verification\_pattern

compute\_mk\_verification\_pattern computes a key verification pattern for the contents of the specified master key register. The verification pattern can be used to determine which master key (old or current) was used to encrypt a given operational key. The returned verification pattern is 20 bytes in length. For the symmetric-keys master key (SYM\_MK), if the first and third key parts of the register specified are the same, the OS/390 ICSF algorithm for the generation of the master key verification pattern will be used. If the key parts are not the same, the verification pattern is a SHA-1 hash of the key, combined with a header. The header is a one-byte value which is used to differentiate this hash from any other hash on the master key, which might be computed for a different purpose. The value of the header byte is X'01'. For the asymmetric-keys master key (ASYM\_MK), the MDC-4 algorithm will be used to compute the verification pattern.

### Function Prototype

```
long compute_mk_verification_pattern(UCHAR      *ver_pattern,
                                   mk_selectors *mk_selector,
                                   VP_ALG_TYPE  vp_algorithm);
```

### Input

On entry to this routine:

ver\_pattern is a pointer to a 20-byte location where the computed key verification pattern is returned.

mk\_selector is a pointer to a variable which must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register is set to either old\_mk, current\_mk, or new\_mk, representing the key which should be cleared.
- type\_mks should be set to ASYM\_MK if this set of master keys is intended for PKA key encryption or SYM\_MK if this set of master keys is used for DES key encryption.

The type\_mks variable should be set to SYM\_MK, as this function calculates the verification pattern for a master key for symmetric keys. If type\_mks is BOTH\_MK and the state and value of the specified master key register of both the master key sets is the same, the verification pattern of the specified register will be calculated on the Symmetric Keys master key set; otherwise an error message will be returned.

- vp\_algorithm must be one of VP\_ALG\_DEFAULT, VP\_ALG\_MDC4, VP\_ALG\_SHA1.

Note that the default for PKA tokens is VP\_ALG\_MDC4 (for a 16-byte MDC-4 hash), the default for DES tokens is VP\_ALG\_SHA1. PKA tokens for the model 1 card use VP\_ALG\_SHA1.

**Output**

On successful exit from this routine:

ver\_pattern contains the verification pattern.

**Return Codes**

Common return codes generated by this routine are:

|                             |                                    |
|-----------------------------|------------------------------------|
| <b>mk_NO_ERROR</b>          | The operation was successful.      |
| <b>mk_SRDI_OPEN_ERROR</b>   | Unable to open the SRDI item.      |
| <b>mk_SEM_CLAIM_FAILED</b>  | Unable to access the SRDI Manager. |
| <b>mk_VP_CALCULATE_FAIL</b> | SHA calculation error.             |



## mkmGetMasterKeyStatus - Get Master Key Status

mkmGetMasterKeyStatus returns the status of the three master key registers for the mk\_set being processed. The results indicate whether the register holds a valid value, and whether a value in the NMK register is complete.

### Function Prototype

```
long mkmGetMasterKeyStatus(mk_selectors  MKSelector,
                           mk_status_var *mk_status);
long get_master_key_status(mk_status_var *mk_status);
```

The get\_master\_key\_status function is the equivalent of calling the mkmGetMasterKeyStatus with the MKSelector parameter set to {MK\_SET\_DEFAULT, current\_mk, SYM\_MK}.

### Input

On entry to this routine:

MKSelector is a parameter of type mk\_selectors, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register must be set to new\_mk or current\_mk.
- type\_mks should be set to ASYM\_MK if the request is to get the status of the asymmetric-keys master key or to SYM\_MK if the request is to get the status of the symmetric-keys master key.

mk\_status is a pointer to a one-byte variable.

### Output

On successful exit from this routine:

mk\_status contains the status of the 3 master key registers as a bitmapped value. Individual bits have the meanings defined in Figure 6-1.

|             |                                   |
|-------------|-----------------------------------|
| Bit 0 (LSB) | NMK register is empty.            |
| Bit 1       | NMK register is partially full.   |
| Bit 2       | NMK register is full.             |
| Bit 3       | CMK register holds a valid value. |
| Bit 4       | OMK register holds a valid value. |
| Bits 5-7    | Reserved, set to 0.               |

mk\_status returns a code indicating the success or failure of the operation.

**Return Codes**

Common return codes generated by this routine are:

- mk\_NO\_ERROR**                    The operation was successful.
- mk\_SRDI\_OPEN\_ERROR**        Unable to open the SRDI item.
- mk\_SEM\_CLAIM\_FAILED**        Unable to access the SRDI Manager.

## get\_mk\_verification\_pattern

get\_mk\_verification\_pattern returns the pre-computed 20-byte master key verification pattern (MKVP) for a specified master key. This value is computed and saved when the master key is first loaded, and may be used to determine which of the master keys was used to encrypt a given operational key.

### Function Prototype

```
long get_mk_verification_pattern(UCHAR      *ver_pattern,
                               mk_selectors *mk_selector);
```

### Input

On entry to this routine:

ver\_pattern is a pointer to a 20-byte location where the master key verification pattern is returned.

mk\_selector is a pointer to a variable which must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register is set to either old\_mk, current\_mk, or new\_mk, representing the key which should be cleared.
- type\_mks should be set to ASYM\_MK if the request is to get the verification pattern of the asymmetric-keys master key or to SYM\_MK if the request is to get the verification pattern of the symmetric-keys master key.

The type\_mks variable should be set to SYM\_MK, as this function calculates the verification pattern for a master key for symmetric keys.

### Output

On successful exit from this routine:

ver\_pattern contains the verification pattern.

### Return Codes

Common return codes generated by this routine are:

|                                |  |
|--------------------------------|--|
| <b>mk_NO_ERROR</b>             | The operation was successful.              |
| <b>mk_INVALID_KEY_SELECTOR</b> | The input parameters are not valid.        |
| <b>mk_SEM_CLAIM_FAILED</b>     | Unable to access the SRDI Manager.         |
| <b>mk_KEY_NOT_VALID</b>        | The selected key was not in a valid state. |

## mkmGetAsymVerificationPattern

mkmGetAsymVerificationPattern returns the pre-computed verification pattern for a set of keys used to encrypt and decrypt PKA keys. This value is computed and saved when the master keys are first loaded, and may be used to determine which of the master keys was used to encrypt a given operational key.

### Function Prototype

```
long mkmGetAsymVerificationPattern(mk_selectors MKSelector,
                                   UCHAR * sha_1[],
                                   UCHAR * mdc_4[]);
```

### Input

On entry to this routine:

MKSelector is a variable which must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register is set to either old\_mk, current\_mk, or new\_mk, representing the key which should be cleared.
- type\_mks is set to ASYM\_MK.

sha\_1 is a pointer to a 20-byte buffer where the SHA-1 hash verification pattern of the master key can be stored.

mdc\_4 is a pointer to a 16-byte buffer where the MDC-4 hash verification pattern of the master key can be stored.

### Output

On successful exit from this routine:

sha\_1 contains the 20-byte verification pattern of the asymmetric master key requested.

mdc\_4 contains the 16-byte MDC-4 verification pattern of the asymmetric master key requested.

### Return Codes

Common return codes generated by this routine are:

|                                |   |
|--------------------------------|---|
| <b>mk_NO_ERROR</b>             | The operation was successful.               |
| <b>mk_INVALID_KEY_SELECTOR</b> | The input parameters are not valid.         |
| <b>mk_KEY_NOT_VALID</b>        | The requested key was not in a valid state. |
| <b>mk_SEM_CLAIM_FAILED</b>     | Unable to access the SRDI Manager.          |

---

## Functions to Encrypt and Decrypt Using the Master Key

### Summary of Functions

|  |   |
|--|---|
| <code>ede3_triple_decrypt_under_master_key</code>    | Triple decrypts multiple 8-byte data strings using EDE3 triple DES. |
| <code>ede3_triple_encrypt_under_master_key</code>    | Triple encrypts multiple 8-byte data strings using EDE3 triple DES. |
| <code>TDESDecryptUnderMasterKey</code>               | Triple-DES decrypts data using the master key.                      |
| <code>TDESEncryptUnderMasterKey</code>               | Triple-DES encrypts data under the master key.                      |
| <code>triple_decrypt_under_master_key</code>         | Triple-DES decrypts an 8-byte block of data.                        |
| <code>triple_decrypt_under_master_key_with_CV</code> | Triple-DES decrypts an 8-byte block of data using a control vector. |
| <code>triple_encrypt_under_master_key</code>         | Triple-DES encrypts an 8-byte block of data.                        |
| <code>triple_encrypt_under_master_key_with_CV</code> | Triple-DES encrypts an 8-byte block of data using a control vector. |

## ede3\_triple\_decrypt\_under\_master\_key

ede3\_triple\_decrypt\_under\_master\_key triple decrypts a string of data using EDE3 triple DES. The data length must be a multiple of eight bytes.

### Function Prototype

```
long ede3_triple_decrypt_under_master_key(mk_selectors *mk_selector,
                                         UCHAR          *cleartext,
                                         UCHAR          *ciphertext,
                                         ULONG         data_length);
```

### Input

On entry to this routine:

mk\_selector is a pointer to a variable which must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register is set to either old\_mk, current\_mk, or new\_mk, representing the key which should be cleared.
- type\_mks should be set to ASYM\_MK if the data is to be decrypted with the asymmetric-keys master key or to SYM\_MK if the data is to be decrypted with the symmetric-keys master key.

cleartext is a pointer to a buffer large enough to store the ciphertext. This may be the same as the ciphertext buffer.

ciphertext is a pointer to a buffer containing the data to be deciphered.

data\_length is the number of bytes of data to be deciphered. This value must be a multiple of eight.

### Output

On successful exit from this routine:

cleartext contains where the deciphered data is placed. This buffer may be the same as the ciphertext buffer, if desired.

### Return Codes

Common return codes generated by this routine are:

|                                |   |
|--------------------------------|---|
| <b>mk_NO_ERROR</b>             | The operation was successful.               |
| <b>mk_INVALID_DATA_LENGTH</b>  | The data length is not a multiple of eight. |
| <b>mk_SRDI_OPEN_ERROR</b>      | Could not open the master key SRDI.         |
| <b>mk_SEM_CLAIM_FAILED</b>     | Unable to access the SRDI Manager.          |
| <b>mk_KEY_NOT_VALID</b>        | The designated master key is not valid.     |
| <b>mk_INVALID_KEY_SELECTOR</b> | The input parameters are not valid.         |

## ede3\_triple\_encrypt\_under\_master\_key

ede3\_triple\_encrypt\_under\_master\_key triple encrypts a string of data using EDE3 triple DES. The data length must be a multiple of eight bytes.

### Function Prototype

```
long ede3_triple_encrypt_under_master_key(mk_selectors *mk_selector,
                                         UCHAR          *cleartext,
                                         UCHAR          *ciphertext,
                                         ULONG          data_length);
```

### Input

On entry to this routine:

mk\_selector is a pointer to a variable which must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register is set to either old\_mk, current\_mk, or new\_mk, representing the key which should be cleared.
- type\_mks should be set to ASYM\_MK if the data is to be encrypted with the asymmetric-keys master key or to SYM\_MK if the data is to be encrypted with the symmetric-keys master key.

cleartext is a pointer to a buffer containing the data to be enciphered.

ciphertext is a pointer to a buffer large enough to store the cleartext. This buffer may be the same as the cleartext buffer.

data\_length is the number of bytes of data to be enciphered. This value must be a multiple of eight.

### Output

On successful exit from this routine:

ciphertext contains where the enciphered data is placed. This buffer may be the same as the cleartext buffer, if desired.

### Return Codes

Common return codes generated by this routine are:

|                                |   |
|--------------------------------|---|
| <b>mk_NO_ERROR</b>             | The operation was successful.               |
| <b>mk_INVALID_DATA_LENGTH</b>  | The data length is not a multiple of eight. |
| <b>mk_SRDI_OPEN_ERROR</b>      | Could not open the master key SRDI.         |
| <b>mk_SEM_CLAIM_FAILED</b>     | Unable to access the SRDI Manager.          |
| <b>mk_KEY_NOT_VALID</b>        | The designated master key is not valid.     |
| <b>mk_INVALID_KEY_SELECTOR</b> | The input parameters are not valid.         |

## TDESDecryptUnderMasterKey

TDESDecryptUnderMasterKey decrypts data which has been encrypted with a master key using the Triple DES algorithm. The master key which was used for encryption must be specified, and the cipher text provided must be a multiple of 8 bytes long.

### Function Prototype

```
long mkmTDESDecryptUnderMasterKey(mk_selectors MKSelector,
                                   UCHAR          *cipher_text,
                                   UCHAR          *clear_text,
                                   ULONG         text_length);
```

### Input

On entry to this routine:

MKSelector is a pointer to a variable which must be initialized as follows:

- `mk_set` is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to `MK_SET_DEFAULT`.
- `mk_register` is set to either `old_mk`, `current_mk`, or `new_mk`, representing the key which should be cleared.
- `type_mks` should be set to `ASYM_MK` if the data is to be decrypted with the asymmetric-keys master key or to `SYM_MK` if the data is to be decrypted with the symmetric-keys master key.

`cipher_text` is a pointer to a buffer which contains the encrypted text. This text must be a multiple of 8 bytes long.

`clear_text` is a pointer to a buffer to hold the decrypted text. This buffer must be as long as `text_length`.

`text_length` is the number of bytes of data in the `cipher_text` buffer. This is also the number of bytes of encrypted text returned in the `clear_text` buffer.

### Output

On successful exit from this routine:

`clear_text` contains `text_length` bytes of data decrypted from the `cipher_data` using the Triple DES algorithm.

### Return Codes

Common return codes generated by this routine are:

|                                |   |
|--------------------------------|---|
| <b>mk_NO_ERROR</b>             | The operation was successful.               |
| <b>mk_INVALID_DATA_LENGTH</b>  | The data length is not a multiple of eight. |
| <b>mk_SRDI_OPEN_ERROR</b>      | Could not open the master key SRDI.         |
| <b>mk_SEM_CLAIM_FAILED</b>     | Unable to access the SRDI Manager.          |
| <b>mk_KEY_NOT_VALID</b>        | The designated master key is not valid.     |
| <b>mk_INVALID_KEY_SELECTOR</b> | The input parameters are not valid.         |



## TDESEncryptUnderMasterKey

TDESEncryptUnderMasterKey takes a variable amount of data in a multiple of 8 bytes and encrypts it using the Triple DES algorithm.

### Function Prototype

```
long mkmTDESEncryptUnderMasterKey(mk_selectors MKSelector,
                                   UCHAR        *clear_text,
                                   UCHAR        *cipher_text,
                                   ULONG        text_length);
```

### Input

On entry to this routine:

MKSelector is a pointer to a variable which must be initialized as follows:

- `mk_set` is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to `MK_SET_DEFAULT`.
- `mk_register` is set to either `old_mk`, `current_mk`, or `new_mk`, representing the key which should be cleared.
- `type_mks` should be set to `ASYM_MK` if the data is to be encrypted with the asymmetric-keys master key or to `SYM_MK` if the data is to be encrypted with the symmetric-keys master key.

`clear_text` is a pointer to the text which you wish to encipher. This text must be a multiple of 8 bytes long.

`cipher_text` is a pointer to a buffer in which to store the encrypted text. This buffer must be at least as long as the `clear_text`.

`text_length` is the number of bytes of data in the `clear_text` buffer. This is also the number of bytes of encrypted text returned in the `cipher_text` buffer.

### Output

On successful exit from this routine:

`cipher_text` contains `text_length` bytes of data encrypted from the `clear_data` using the Triple DES algorithm.

### Return Codes

Common return codes generated by this routine are:

|                                |   |
|--------------------------------|---|
| <b>mk_NO_ERROR</b>             | The operation was successful.               |
| <b>mk_INVALID_DATA_LENGTH</b>  | The data length is not a multiple of eight. |
| <b>mk_SRDI_OPEN_ERROR</b>      | Could not open the master key SRDI.         |
| <b>mk_SEM_CLAIM_FAILED</b>     | Unable to access the SRDI Manager.          |
| <b>mk_KEY_NOT_VALID</b>        | The designated master key is not valid.     |
| <b>mk_INVALID_KEY_SELECTOR</b> | The input parameters are not valid.         |

## triple\_decrypt\_under\_master\_key

triple\_decrypt\_under\_master\_key triple decrypts eight bytes of data with the EDE algorithm, using the specified master key register.

### Function Prototype

```
long triple_decrypt_under_master_key(mk_selectors *mk_selector,
                                     UCHAR          *ciphertext,
                                     UCHAR          *cleartext);
```

### Input

On entry to this routine:

mk\_selector is a pointer to a variable which must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register is set to either old\_mk, current\_mk, or new\_mk, representing the key which should be cleared.
- type\_mks should be set to ASYM\_MK if the data is to be decrypted with the asymmetric-keys master key or to SYM\_MK if the data is to be decrypted with the symmetric-keys master key.

ciphertext is a pointer to a buffer containing the data to be deciphered.

cleartext is a pointer to a buffer 8 bytes in length. This may be the same as the ciphertext buffer.

### Output

On successful exit from this routine:

cleartext contains where the deciphered data is placed. This buffer may be the same as the ciphertext buffer, if desired.

### Return Codes

Common return codes generated by this routine are:

|                                |  |
|--------------------------------|--|
| <b>mk_NO_ERROR</b>             | The operation was successful.  |
| <b>mk_SRDI_OPEN_ERROR</b>      | Could not open the master key SRDI.                                      |
| <b>mk_KEY_NOT_VALID</b>        | The master key could not be validated, therefore cleartext is unchanged. |
| <b>mk_INVALID_KEY_SELECTOR</b> | The input parameters are not valid.                                      |

## triple\_decrypt\_under\_master\_key\_with\_CV

triple\_decrypt\_under\_master\_key\_with\_CV triple decrypts eight bytes of data with the EDE algorithm, using a control vector with the specified master key.

**Note:** This function does not check the validity of the control vector.

### Function Prototype

```
long triple_decrypt_under_master_key_with_CV(mk_selectors *mk_selector,
                                             eightbyte   *cv,
                                             UCHAR        *ciphertext,
                                             UCHAR        *cleartext)
```

### Input

On entry to this routine:

mk\_selector is a pointer to a variable which must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register is set to either old\_mk, current\_mk, or new\_mk, representing the key which should be cleared.
- type\_mks should be set to ASYM\_MK if the data is to be decrypted with the asymmetric-keys master key or to SYM\_MK if the data is to be decrypted with the symmetric-keys master key.

cv is a pointer to a double-length CCA control vector, which is exclusive-ORed with the specified key value before the key is used.

ciphertext is a pointer to a buffer containing the data to be deciphered.

cleartext is a pointer to a buffer 8 bytes in length. This may be the same as the ciphertext buffer.

### Output

On successful exit from this routine:

cleartext is a pointer to the buffer where the deciphered data is placed. This buffer may be the same as the ciphertext buffer, if desired.

### Return Codes

Common return codes generated by this routine are:

|                                |                                     |
|--------------------------------|-------------------------------------|
| <b>mk_NO_ERROR</b>             | The operation was successful.       |
| <b>mk_SRDI_OPEN_ERROR</b>      | Could not open the master key SRDI. |
| <b>mk_SEM_CLAIM_FAILED</b>     | Unable to access the SRDI Manager.  |
| <b>mk_INVALID_KEY_SELECTOR</b> | The input parameters are not valid. |

## triple\_encrypt\_under\_master\_key

triple\_encrypt\_under\_master\_key triple encrypts eight bytes of data with the EDE algorithm, using the specified master key register.

### Function Prototype

```
long triple_encrypt_under_master_key(mk_selectors *mk_selector,
                                     UCHAR          *cleartext,
                                     UCHAR          *ciphertext);
```

### Input

On entry to this routine:

mk\_selector is a pointer to a variable which must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register is set to either old\_mk, current\_mk, or new\_mk, representing the key which should be cleared.
- type\_mks should be set to ASYM\_MK if the data is to be encrypted with the asymmetric-keys master key or to SYM\_MK if the data is to be encrypted with the symmetric-keys master key.

cleartext is a pointer to a buffer containing the data to be enciphered.

ciphertext is a pointer to a buffer which is 8 bytes in length. This may be the same as the cleartext buffer.

### Output

On successful exit from this routine:

ciphertext is a pointer to the buffer where the enciphered data is placed. This buffer may be the same as the cleartext buffer, if desired.

### Return Codes

Common return codes generated by this routine are:

|                                |   |
|--------------------------------|---|
| <b>mk_NO_ERROR</b>             | The operation was successful.                         |
| <b>mk_SRDI_OPEN_ERROR</b>      | Could not open the master key SRDI.                   |
| <b>mk_SEM_CLAIM_FAILED</b>     | Unable to access the SRDI Manager.                    |
| <b>mk_KEY_NOT_VALID</b>        | The master key (OMK, CMK, or NMK) is not a valid key. |
| <b>mk_INVALID_KEY_SELECTOR</b> | The input parameters are not valid.                   |

## triple\_encrypt\_under\_master\_key\_with\_CV

triple\_encrypt\_under\_master\_key\_with\_CV triple encrypts eight bytes of data with the EDE algorithm, using a control vector with the specified master key.

**Note:** This function does not check the validity of the control vector.

### Function Prototype

```
long triple_encrypt_under_master_key_with_CV(mk_selectors *mk_selector,
                                             eightbyte   *cv,
                                             UCHAR        *cleartext,
                                             UCHAR        *ciphertext)
```

### Input

On entry to this routine:

mk\_selector is a pointer to a variable which must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register is set to either old\_mk, current\_mk, or new\_mk, representing the key which should be cleared.
- type\_mks should be set to ASYM\_MK if the data is to be encrypted with the asymmetric-keys master key or to SYM\_MK if the data is to be encrypted with the symmetric-keys master key.

cv is a pointer to a double-length CCA control vector, which is exclusive-ORed with the specified key value before the key is used.

cleartext is a pointer to a buffer containing the data that is enciphered.

ciphertext is a pointer to a buffer which can hold 8 bytes of data. This may be the same as the cleartext buffer.

### Output

On successful exit from this routine:

ciphertext is a pointer to the buffer where the enciphered data is placed. This buffer may be the same as the cleartext buffer, if desired.

### Return Codes

Common return codes generated by this routine are:

- |                            |                                     |
|----------------------------|-------------------------------------|
| <b>mk_NO_ERROR</b>         | The operation was successful.       |
| <b>mk_SRDI_OPEN_ERROR</b>  | Could not open the master key SRDI. |
| <b>mk_SEM_CLAIM_FAILED</b> | Unable to access the SRDI Manager.  |



---

## Chapter 7. SHA-1 Functions

The functions described in this chapter allow a UDX to compute the hash of a block of data using the Secure Hash Algorithm (SHA-1) as defined in FIPS Publication 180-1.

**Note:** All functions within this chapter are available only on the coprocessor.

### Header Files for SHA-1 Functions

When using these functions, your program must include the following header files:

```
#include "cmncrypt2.h"           /* Cryptographic types      */
#include "cmn_sha.h"             /* SHA external definitions. */
```

### Summary of Functions

The following functions are described in this chapter:

|                               |  |
|-------------------------------|--|
| <b>computeHMAC_SHA1</b>       | Compute a keyed-hash for message authentication code (HMAC) for a given set of data using the Secure Hash Algorithm (SHA-1). |
| <b>do_sha_hash_message</b>    | Compute the hash of a block of data using the SHA-1 algorithm.   |
| <b>do_sha_hash_msg_to_bfr</b> | “wrapper” for sha_hash_message.  |
| <b>hw_sha_hash_message</b>    | Compute a SHA-1 hash of the requested data on the hashing hardware.  |
| <b>sha_hash_message</b>       | Compute the hash of a block of data using the SHA-1 algorithm.   |
| <b>sha_hash_msg_to_bfr</b>    | “wrapper” for sha_hash_message.  |

## computeHMAC\_SHA1 - Compute HMAC using SHA-1 Algorithm

computeHMAC\_SHA1 computes a keyed-hash for message authentication code (HMAC) for a given set of data, using the SHA-1 algorithm and a provided key.

### Function Prototype

```
void computeHMAC_SHA1 (char      *pBuffer, int buffer_length,  
                      char      *pKey,   int key_length,  
                      char      *pHmac);
```

### Input

On entry to this routine:

pBuffer is a pointer to an array which holds the data to be hashed for message authentication codes.

buffer\_length is the number of bytes of data in pBuffer.

pKey is a pointer to a key (a random string of bits, preferably 64 bytes long).

key\_length is the number of bytes of data in pKey.

pHmac is a pointer to a buffer 20 bytes long, which will hold the returned data.

### Output

On successful exit from this routine:

pHmac contains the HMAC-SHA1 of the data in pBuffer.

### Return Codes

This function has no return codes.



## do\_sha\_hash\_message - Calculate SHA-1 Hash Hardware/Software

do\_sha\_hash\_message calculates the SHA-1 hash of the data using the coprocessor hardware if the data is longer than 8192 bits, or the software if the data is shorter.

### Function Prototype

```
ULONG do_sha_hash_message (UCHAR      *pBlock,
                          UCHAR      *pHash,
                          dbl_ulong  *pBitCount,
                          sha_context *pContext,
                          owh_sequence MsgPart);
```

### Input

On entry to this routine:

MsgPart controls the operation of the function and must be one of the following constants:

- only        The input data constitutes the entire block of data to be hashed. The hash value is computed and returned.
- first      The input data constitutes the first portion of a block of data to be hashed. See "Chained Operations" on page 7-4 for details.
- middle     The input data constitutes an additional portion of a block of data to be hashed. See "Chained Operations" on page 7-4 for details.
- final      The input data constitutes the final portion of a block of data to be hashed. See "Chained Operations" on page 7-4 for details.

pBlock must contain the address of the block of data that is to be incorporated into the hash.

pHash must contain the address of a buffer to which the hash value may be written. The buffer must be at least 20 bytes long. pHash is used only if MsgPart specifies only or final.

pBitCount must contain the address of a buffer that contains the length in *bits* of the block of data referenced by pBlock. \*pBitCount is interpreted as a 64-bit integer. pBitCount->upper contains the most-significant 32 bits of \*pBitCount and pBitCount->lower contains the least-significant 32 bits of \*pBitCount.

**Note:** Both fields are regular 32-bit integers (that is, C unsigned longs) that are stored in the native byte order of the processor on which the code is running.

For example, pBitCount->lower and pBitCount->upper are stored in little-endian order on the coprocessor.

If MsgPart specifies first or middle, \*pBitCount must be a multiple of 512, or data will be lost.

pContext must contain the address of a context buffer from which the function may initialize its internal state and to which the function may write its final internal state. See "Chained Operations" on page 7-4 for details.

If MsgPart specifies only or first, the initial value of \*pContext is ignored.

## Output

On successful exit from this routine:

The buffer referenced by pHash contains the hash value of the input data if MsgPart specifies *only* or *final*. In the latter case, the hash value incorporates the initial hash value provided in \*pContext.

\*pContext has been updated to incorporate changes to the function's internal state caused by incorporating \*pBlock into the hash.

## Notes

### Chained Operations

A block of data to be hashed may be processed in a single operation. It may be necessary, however, to break the operation into several steps, each of which processes only a portion of the block. (For example, an application may want to compute a hash that covers several discontinuous fields in a structure.)

A chained operation is initiated by calling do\_sha\_hash\_message with MsgPart set to *first* and the first piece of the block of data to hash identified by pBlock and \*pBitCount. On return, \*pContext contains context information that must be preserved and passed to sha\_hash\_message when the next piece of the block of data to hash is processed.

Subsequent pieces of the block are processed by calling sha\_hash\_message with MsgPart set to *middle* (or to *final* if the piece in question is the last) and the location and length of the piece identified by pBlock and \*pBitCount. \*pContext must contain the value returned in that structure by the call to sha\_hash\_message that processed the previous piece of the block. The function hashes the piece and updates \*pContext and pHash appropriately.

### Return Codes

Common return codes generated by this routine are:

- sh\_NO\_ERROR (i.e., 0)** The operation was successful.
- sh\_MSG\_PART\_INVALID** The MsgPart argument was not *only*, *first*, *middle*, or *last*.

### Examples

To compute the SHA-1 hash of a contiguous block of 150 bytes of text at pBlock:

```
BitCount = ((dbl_ulong) 150)*8;
memset ((UCHAR *)pContext, 0x00, sizeof(sha_context) );

do_sha_hash_message(pBlock, &Hash, &BitCount, pContext, only);
```

To compute the SHA-1 hash of only the name fields of the following structure:

```
struct emp_data{
    char ID[10];
    double salary;
    char name[64];
}employee[MAX_EMP];

BitCount = (dbl_ulong)512;
memset ((UCHAR *)&Context, 0x00, sizeof(sha_context));
/* Start the hash with "first" */
sha_hash_message(employee[i].name, &Hash, &Bitcount, &Context, first);
/* hash the middle portions */
for (i = 1; i < MAX_EMP-1; i++)
{
    /* it is important that the value in BitCount is divisible by 512 */
    do_sha_hash_message(employee[i].name, &Hash, &BitCount, &Context, middle);
}
/* hash the final portion */
sha_hash_message(employee[MAX_EMP-1].name, &Hash, &BitCount, &Context, final);
/* at this point, the value in Hash is the SHA-1 hash of the names */
```

## do\_sha\_hash\_msg\_to\_bfr - SHA-1 Hash

do\_sha\_hash\_msg\_to\_bfr is a wrapper for sha\_hash\_message that simplifies the interface when chained operations (see page 7-4) are not necessary.

### Function Prototype

```
void do_sha_hash_msg_to_bfr(UCHAR      *pBlock,  
                           UCHAR      *pHash,  
                           dbl_ulong  *pBitCount);
```

### Input

On entry to this routine:

pBlock must contain the address of the block of data that is to be hashed.

pHash must contain the address of a buffer to which the hash value may be written. The buffer must be at least 20 bytes long.

pBitCount must contain the address of a buffer that contains the length in *bits* of the block of data referenced by pBlock. \*pBitCount is interpreted as a 64-bit integer. pBitCount->upper contains the most-significant 32 bits of \*pBitCount and pBitCount->lower contains the least-significant 32 bits of \*pBitCount.

**Note:** Both fields are regular 32-bit integers (that is, C unsigned longs) that are stored in the native byte order of the processor on which the code is running.

For example, pBitCount->lower and pBitCount->upper are stored in little-endian order on the coprocessor.

### Output

On successful exit from this routine:

The buffer referenced by pHash contains the hash value of the input data.

### Notes

#### Function Wraps sha\_hash\_message

sha\_hash\_msg\_to\_bfr(pBlock,pHash,pBitCount) performs the same function as

```
{  
    sha_context Context;  
    memset(&Context,0,sizeof(Context));  
    do_sha_hash_message(pBlock,pHash,pBitCount,&Context,only);  
}
```

### Return Codes

This function has no return codes.

## hw\_sha\_hash\_message - Compute SHA-1 Hash in Hardware

hw\_sha\_hash\_message computes a SHA-1 hash of the requested data on the hashing hardware in the coprocessor.

### Function Prototype

```
void hw_sha_hash_message(UCHAR    *pText,
                        long      text_length,
                        sha_context *chain_vector,
                        long      RequestId,
                        ULONG     options,
                        UCHAR     *final_data,
                        long      *pMsg);
```

### Input

On entry to this routine:

pText is a pointer to the data which is to be hashed.

text\_length is the number of bytes of data at pText.

chain\_vector is the context of this request. If this is the first block of data, or the only block, this variable should be initialized to zeros. On subsequent calls, this variable should be returned to the next call without change.

RequestId is the ID of the caller.

options may include SHA\_MSGPART\_FIRST, SHA\_MSGPART\_MIDDLE, SHA\_MSGPART\_FINAL, or SHA\_MSGPART\_ONLY, as well as SHA\_INTERNAL\_INPUT or SHA\_EXTERNAL\_INPUT. These constants are defined in the **scc\_int.h** header file.

final\_data is a pointer to a buffer at least 20 bytes long, to hold the result of the hash.

pMsg is a pointer to a 4-byte block.

### Output

On successful exit from this routine:

chain\_vector contains the chaining information for the next call to the function, unless this call was with the final or only block of data. This variable should be passed unchanged to the next call.

final\_data contains the final hash value, if this call was with the final or only data block.

pMsg contains the return code for the function.

**Return Codes**

Common return codes generated by this routine are:

|                            |  |
|----------------------------|--|
| <b>OK</b>                  | The operation was successful.  |
| <b>SHA1_DATA64_ERROR</b>   | The options argument specified SHA_MSGPART_FIRST or SHA_MSGPART_MIDDLE but the length of the data to process is not a multiple of 64.  |
| <b>SHA1_DATA32MB_ERROR</b> | The length of the data to process is 32M or greater.   |
| <b>SHA1_FINAL_ERROR</b>    | An error occurred while attempting to pad the input data as directed by the SHA-1 algorithm or while attempting to hash the pad bytes. |

## sha\_hash\_message - SHA-1 Hash with Chaining

sha\_hash\_message computes the hash of a block of data using the Secure Hash Algorithm (SHA-1) and optionally incorporates the result into an initial hash value. This function calculates the hash in software.

### Function Prototype

```
ULONG sha_hash_message (UCHAR      *pBlock,
                        UCHAR      *pHash,
                        dbl_ulong  *pBitCount,
                        sha_context *pContext,
                        owh_sequence MsgPart);
```

### Input

On entry to this routine:

MsgPart controls the operation of the function and must be one of the following constants:

- only        The input data constitutes the entire block of data to be hashed. The hash value is computed and returned.
- first      The input data constitutes the first portion of a block of data to be hashed. See “Chained Operations” on page 7-10 for details.
- middle     The input data constitutes an additional portion of a block of data to be hashed. See “Chained Operations” on page 7-10 for details.
- final      The input data constitutes the final portion of a block of data to be hashed. See “Chained Operations” on page 7-10 for details.

pBlock must contain the address of the block of data that is to be incorporated into the hash.

pHash must contain the address of a buffer to which the hash value may be written. The buffer must be at least 20 bytes long. pHash is used only if MsgPart specifies only or final.

pBitCount must contain the address of a buffer that contains the length in *bits* of the block of data referenced by pBlock. \*pBitCount is interpreted as a 64-bit integer. pBitCount->upper contains the most-significant 32 bits of \*pBitCount and pBitCount->lower contains the least-significant 32 bits of \*pBitCount.

**Note:** Both fields are regular 32-bit integers (that is, C unsigned longs) that are stored in the native byte order of the processor on which the code is running.

For example, pBitCount->lower and pBitCount->upper are stored in little-endian order on the coprocessor.

If MsgPart specifies first or middle, \*pBitCount must be a multiple of 512, or data will be lost.

pContext must contain the address of a context buffer from which the function may initialize its internal state and to which the function may write its final internal state. See “Chained Operations” on page 7-10 for details.

If MsgPart specifies only or first, the initial value of \*pContext is ignored.

## Output

On successful exit from this routine:

The buffer referenced by pHash contains the hash value of the input data if MsgPart specifies *only* or *final*. In the latter case, the hash value incorporates the initial hash value provided in \*pContext.

\*pContext has been updated to incorporate changes to the function's internal state caused by incorporating \*pBlock into the hash.

## Notes

### Chained Operations

A block of data to be hashed may be processed in a single operation. It may be necessary, however, to break the operation into several steps, each of which processes only a portion of the block. (For example, an application may want to compute a hash that covers several discontinuous fields in a structure.)

A chained operation is initiated by calling sha\_hash\_message with MsgPart set to *first* and the first piece of the block of data to hash identified by pBlock and \*pBitCount. On return, \*pContext contains context information that must be preserved and passed to sha\_hash\_message when the next piece of the block of data to hash is processed.

Subsequent pieces of the block are processed by calling sha\_hash\_message with MsgPart set to *middle* (or to *final* if the piece in question is the last) and the location and length of the piece identified by pBlock and \*pBitCount. \*pContext must contain the value returned in that structure by the call to sha\_hash\_message that processed the previous piece of the block. The function hashes the piece and updates \*pContext and pHash appropriately.

### Return Codes

Common return codes generated by this routine are:

- sh\_NO\_ERROR (i.e., 0)** The operation was successful.
- sh\_MSG\_PART\_INVALID** The MsgPart argument was not *only*, *first*, *middle*, or *last*.

### Examples

To compute the SHA-1 hash of a contiguous block of 150 bytes of text at pBlock:

```
BitCount = ((dbl_ulong) 150)*8;
memset ((UCHAR *)pContext, 0x00, sizeof(sha_context) );

sha_hash_message(pBlock, &Hash, &BitCount, pContext, only);
```



To compute the SHA-1 hash of only the name fields of the following structure:

```
struct emp_data{
    char ID[10];
    double salary;
    char name[64];
}employee[MAX_EMP];

BitCount = (dbl_ulong)512;
memset ((UCHAR *)&Context, 0x00, sizeof(sha_context));
/* Start the hash with "first" */
sha_hash_message(employee[i].name, &Hash, &Bitcount, &Context, first);
/* hash the middle portions */
for (i = 1; i < MAX_EMP-1; i++)
{
    /* it is important that the value in BitCount is divisible by 512 */
    sha_hash_message(employee[i].name, &Hash, &BitCount, &Context, middle);
}
/* hash the final portion */
sha_hash_message(employee[MAX_EMP-1].name, &Hash, &BitCount, &Context, final);
/* at this point, the value in Hash is the SHA-1 hash of the names */
```

## sha\_hash\_msg\_to\_bfr - SHA-1 Hash

sha\_hash\_msg\_to\_bfr is a wrapper for sha\_hash\_message that simplifies the interface when chained operations (see page 7-10) are not necessary.

### Function Prototype

```
void sha_hash_msg_to_bfr(UCHAR      *pBlock,  
                        UCHAR      *pHash,  
                        dbl_ulong  *pBitCount);
```

### Input

On entry to this routine:

pBlock must contain the address of the block of data that is to be hashed.

pHash must contain the address of a buffer to which the hash value may be written. The buffer must be at least 20 bytes long.

pBitCount must contain the address of a buffer that contains the length in *bits* of the block of data referenced by pBlock. \*pBitCount is interpreted as a 64-bit integer. pBitCount->upper contains the most-significant 32 bits of \*pBitCount and pBitCount->lower contains the least-significant 32 bits of \*pBitCount.

**Note:** Both fields are regular 32-bit integers (that is, C unsigned longs) that are stored in the native byte order of the processor on which the code is running.

For example, pBitCount->lower and pBitCount->upper are stored in little-endian order on the coprocessor.

### Output

On successful exit from this routine:

The buffer referenced by pHash contains the hash value of the input data.

### Notes

#### Function Wraps sha\_hash\_message

sha\_hash\_msg\_to\_bfr(pBlock,pHash,pBitCount) performs the same function as

```
{  
    sha_context Context;  
    memset(&Context,0,sizeof(Context));  
    sha_hash_message(pBlock,pHash,pBitCount,&Context,only);  
}
```

### Return Codes

This function has no return codes.

## Chapter 8. DES Utility Functions

This chapter describes functions to assist in the use of key tokens and other cryptographic structures.

You should understand the use of the CCA control-vector before using the functions in this chapter. Control vectors are explained and described in Appendix C of the *CCA Basic Services Reference and Guide*. Three bits in the basic control vector have been reserved for UDX developers. Setting Bit 61 will prevent a key token from being used in any CCA standard verb except the import and export verbs. Bits 4 and 5 of the control vector will be checked by any standard CCA code. This allows developers to use these three bits to indicate their own, UDX specific keys, which can be used only by UDX verbs. (These verbs must be written to test the required bits.)

**Note:** All functions within this chapter are available only on the coprocessor.

### Header Files for DES Utility Functions

When using these functions, your program must include the following header files.

```
#include "cmncrypt2.h"           /* T2 structures, constants, functions */
#include "castyped.h"           /* Adapter typedefs and structures */
#include "cassub.h"             /* DES 96 function prototypes */
#include "casfunct.h"
```

### Summary of Functions

DES utility routines includes the following functions.

|                                |  |
|--------------------------------|--|
| <b>CasBuildCv</b>              | Builds a default control vector. See page 8-5.                     |
| <b>CasBuildToken</b>           | Builds a default DES key token. See page 8-6.                      |
| <b>CasCurrentMkvp</b>          | Returns the current master key verification pattern. See page 8-8. |
| <b>CasOldMkvp</b>              | Returns the old master key verification pattern. See page 8-9.     |
| <b>CasMasterKeyCheck</b>       | Performs a master key version check. See page 8-14.                |
| <b>cas_adjust_parity</b>       | Adjusts the parity of a DES key token. See page 8-4.               |
| <b>cas_des_key_token_check</b> | Verifies the integrity of a DES key token. See page 8-10.          |
| <b>cas_get_key_type</b>        | Returns the type of DES key token. See page 8-11.                  |
| <b>cas_key_length</b>          | Returns the length of a DES key. See page 8-12.                    |

|                                    |   |
|------------------------------------|---|
| <b>cas_key_tokentvv_check</b>      | Verifies a DES key token validation value. See page 8-13.                     |
| <b>cas_parity_odd</b>              | Determines whether a DES key has odd parity. See page 8-16.                   |
| <b>RecoverDesDataKeyWithMK</b>     | Recovers the cleartext form of a DES importer data key. See page 8-17.        |
| <b>RecoverDesKekImporterWithMK</b> | Recovers the cleartext form of a DES key encrypting key (KEK). See page 8-19. |

## Overview

The routines described in this chapter are used to analyze, modify, and validate CCA DES key tokens.

Refer to the *IBM 4758 PCI Cryptographic Coprocessor CCA Basic Services Reference and Guide* for more information. Chapter 5, "Basic CCA DES Key Management" includes an in-depth discussion of DES key token management within CCA. You can also refer to Appendix B, "Data Structures" for a description of the DES key tokens structures and Appendix C, "CCA Control Vector Definitions and Key Encryption" for a discussion of control vectors.

Keys used in these functions are one of the following KEY\_TYPES:

|                       |  |
|-----------------------|--|
| <b>DATA_KEY</b>       | For the encryption and decryption of data.   |
| <b>DATAXLATE_KEY</b>  | To re-encipher data from one key to another.   |
| <b>CIPHER_KEY</b>     | A symmetric key to encipher and decipher data.   |
| <b>ENCIPHER_KEY</b>   | A non-symmetric key, which only enciphers data.  |
| <b>DECIPHER_KEY</b>   | A non-symmetric key, which only deciphers data.  |
| <b>MAC_KEY</b>        | For generating and verify Message Authentication Codes.  |
| <b>MACVER_KEY</b>     | For verifying Message Authentication Codes.  |
| <b>IMPORTER_KEY</b>   | For decoding keys imported from other engines, or translating keys from one encoding to another.   |
| <b>EXPORTER_KEY</b>   | For encoding keys for export (to other engines), or translating keys from one encoding to another. |
| <b>IKEYXLATE_KEY</b>  | For inputting a key translation.   |
| <b>OKEYXLATE_KEY</b>  | For outputting a key translation.  |
| <b>PINGEN_KEY</b>     | For generating PINs.   |
| <b>PINVER_KEY</b>     | For verifying PINs.  |
| <b>IPINENC_KEY</b>    | For importing PINs.  |
| <b>OPINENC_KEY</b>    | For exporting PINs.  |
| <b>KEYGEN_KEY</b>     | Used for key generation.   |
| <b>KEY_TYPE_TOKEN</b> | A key token, rather than a key.  |

## cas\_adjust\_parity - Adjust Parity

cas\_adjust\_parity adjusts each byte of the passed string, as necessary, so that every byte has odd parity. This is useful when adjusting DES keys for correct parity.

### Function Prototype

```
void cas_adjust_parity( UCHAR      *DataBytes,  
                      unsigned int Length)
```

### Input

On entry to this routine:

DataBytes is a pointer to the string that is to be parity-adjusted.

Length is the number of bytes in the string at location *DataBytes*.

### Output

On successful exit from this routine:

DataBytes is a pointer to the string that has been parity-adjusted.

### Return Codes

This function has no return codes.

## CasBuildCv - Build a Default Control Vector

CasBuildCv builds a default control vector for the specified key type.

### Function Prototype

```
boolean CasBuildCv      ( KEY_TYPES  KeyType,  
                        CV_LENGTHS  CV_Length,  
                        UCHAR       *pCV )  
void   cas_build_default_cv( KEY_TYPES  KeyType,  
                           UCHAR       *pCV )
```

cas\_build\_default\_cv has the same effect as calling CasBuildCv after setting the CV\_Length parameter to CV\_DEFAULT.

### Input

On entry to this routine:

KeyType is the type of key your control vector is used with.

pCv is a pointer to a 20-byte location which will hold the new control vector.

CV\_Length is one of CV\_DOUBLE, CV\_SINGLE, or CV\_DEFAULT, depending on what length of key you are building a control vector for.

### Output

On successful exit from this routine:

CasBuildCv returns true if the build was successful, and false otherwise. (For example, if the length requested was not legal for the key type.)

pCv contains the new control vector.

### Return Codes

This function has no return codes.

## CasBuildToken - Build a Default Token

CasBuildToken builds a default key token, of the type specified by parameter *KeyType* for the *mk\_set* being processed.

### Function Prototype

```
boolean CasBuildToken ( UCHAR          TokenFlag,
                       KEY_TYPES      KeyType,
                       CV_LENGTHS     CV_Length,
                       mk_selectors    *pMKSelector,
                       des_key_token_structure *pKeyToken )
void cas_build_default_token( UCHAR          TokenFlag,
                             KEY_TYPES      KeyType,
                             des_key_token_structure *pKeyToken )
```

*cas\_build\_default\_token* has the same effect as calling *CasBuildToken* with *CV\_Length* set to *CV\_DEFAULT* and *MKSelector* set to {*MK\_SET\_DEFAULT*, *current\_mk*, *SYM\_MK*}.

### Input

On entry to this routine:

*TokenFlag* is the token flag used in constructing the new key token. Legal values for this field are *INTERNAL\_TOKEN\_FLAG* and *EXTERNAL\_TOKEN\_FLAG*.

*KeyType* is the type of key token to be generated. Examples include data key, exporter key, and MAC key.

*CV\_Length* is one of *CV\_DOUBLE*, *CV\_SINGLE*, or *CV\_DEFAULT*, depending on what length of key you are building a control vector for.

*MKSelector* is a parameter of type *mk\_selectors*, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- *mk\_set* is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to *MK\_SET\_DEFAULT*.
- *mk\_register* must be set to *new\_mk* or *current\_mk*.
- *type\_mks* should be set to *ASYM\_MK* if this set of master keys is intended for PKA key encryption or *SYM\_MK* if this set of master keys is used for DES key encryption.

*pKeyToken* is a pointer to a 64-byte buffer which can store a key token.



**Output**

On successful exit from this routine:

pKeyToken contains the token constructed by the function.

**Return Codes**

This function has no return codes.

## CasCurrentMkvp - Current Master Key Verification Pattern

CasCurrentMkvp returns the 20-byte master key verification pattern (MKVP) for the current master key for the `mk_set` being processed. The MKVP is a cryptographically calculated checksum on the master key value. It is used in all internal (master-key encrypted) DES key tokens, to indicate which master key was used to encrypt the key.

### Function Prototype

```
boolean CasCurrentMkvp ( mk_selectors *pMKSelector,
                        UCHAR         *pMKVP )
boolean cas_current_mkvp( UCHAR         *pMKVP )
```

`cas_current_mkvp` has the same effect as calling `CasCurrentMkvp` with the `pMKSelector` parameter set to `{MK_SET_DEFAULT, current_mk, SYM_MK}`.

### Input

On entry to this routine:

`MKSelector` is a parameter of type `mk_selectors`, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- `mk_set` is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to `MK_SET_DEFAULT`.
- `mk_register` must be set to `new_mk` or `current_mk`.
- `type_mks` should be set to `ASYM_MK` if this set of master keys is intended for PKA key encryption or `SYM_MK` if this set of master keys is used for DES key encryption.

`pMKVP` must contain the address of a variable in which a 20-byte master key verification pattern can be stored.

### Output

On successful exit from this routine:

`pMKVP` contains the current master key verification pattern.

`cas_current_mkvp` returns `TRUE` if the verification pattern was found, and `FALSE` otherwise.

### Return Codes

This function has no return codes.

## CasOldMkvp - Old Master Key Verification Pattern

CasOldMkvp returns the 20-byte master key verification pattern (MKVP) for the old master key for the `mk_set` being processed. The MKVP is a cryptographically calculated checksum on the master key value. It is used in all internal (master-key encrypted) DES key tokens, to indicate which master key was used to encrypt the key.

### Function Prototype

```
boolean CasOldMkvp ( mk_selectors *pMKSelector,
                    UCHAR          *pMKVP )
boolean cas_old_mkvp( UCHAR          *pMKVP )
```

`cas_old_mkvp` has the same effect as calling `CasOldMkvp` with the `pMKSelector` parameter set to `{MK_SET_DEFAULT, current_mk, SYM_MK}`.

### Input

On entry to this routine:

`MKSelector` is a parameter of type `mk_selectors`, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- `mk_set` is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to `MK_SET_DEFAULT`.
- `mk_register` must be set to `new_mk` or `current_mk`.
- `type_mks` should be set to `ASYM_MK` if this set of master keys is intended for PKA key encryption or `SYM_MK` if this set of master keys is used for DES key encryption.

`pMKVP` must contain the address of a variable in which a 20-byte master key verification pattern can be stored.

### Output

On successful exit from this routine:

`pMKVP` contains the current master key verification pattern.

`cas_current_mkvp` returns `TRUE` if the verification pattern was found, and `FALSE` otherwise.

### Return Codes

This function has no return codes.

## cas\_des\_key\_token\_check - Verify the DES Key Token

cas\_des\_key\_token\_check performs the following checks to verify the integrity of an internal DES key token.

- Check that all reserved fields are zero.
- Check the token flag.
- Check the version number.
- Check the flags.

If no errors are found, the function returns TRUE. If there is an error, the function returns FALSE and parameter *pMessageFlag* indicates the cause of the error.

Either version 0 or version 1 DES key tokens may be validated.

### Function Prototype

```
boolean cas_des_key_token_check( des_key_token_structure *pKeyToken,
                                DES_TOKEN_CHECK          *pMessageFlag )
```

### Input

On entry to this routine:

pKeyToken is a pointer to the internal DES key token that is to be checked.

### Output

On successful exit from this routine:

pMessageFlag is a pointer to a location where the function stores an error code, if the key token is found to have an error.

cas\_des\_key\_token\_check returns a boolean value of TRUE, if the token has no errors, or FALSE otherwise.

### Return Codes

Common return codes generated by this routine are:

|   |   |
|---|---|
| <b>DES_TOKEN_CHECK_VALID</b>            | The token is valid.                         |
| <b>DES_TOKEN_CHECK_TOKENFLAG</b>        | The token is not an internal DES key token. |
| <b>DES_TOKEN_CHECK_RESERVED<i>i</i></b> | Reserved field <i>i</i> is incorrectly set. |
| <b>DES_TOKEN_CHECK_VERSION</b>          | The version number is incorrect.            |
| <b>DES_TOKEN_CHECK_FLAGBYTES</b>        | The token flag is incorrect.                |
| <b>DES_TOKEN_CHECK_FLAG_NOCV</b>        | The token has no control vector set.        |
| <b>DES_TOKEN_CHECK_NOKEY</b>            | The token does not contain a key.           |

**cas\_get\_key\_type - Return Key Type**

cas\_get\_key\_type returns the key type corresponding to the specified key token.

**Function Prototype**

```
KEY_TYPES cas_get_key_type( des_key_token_structure *pKeyToken )
```

**Input**

On entry to this routine:

pKeyToken is a pointer to the key token which is to be examined.

**Output**

This function returns no output. On successful exit from this routine:

cas\_get\_key\_type returns the key type corresponding to the specified key token.

**Return Codes**

This function has no return codes.

## cas\_key\_length - Return Key Length

cas\_key\_length determines the length of a key, based on the Control Vector. The key length is returned as the function result.

### Function Prototype

```
LENGTH_KEYWORD cas_key_length( eightbyte CvBase,  
                                eightbyte CvExtension )
```

### Input

On entry to this routine:

CvBase is the control vector base.

CvExtension is the control vector extension.

### Output

On successful exit from this routine:

cas\_key\_length returns SINGLE or DOUBLE, depending on whether the specified key is single or double length.

### Examples

To determine the length of the key stored in DataKey:

```
switch(cas_key_length(DataKey,cvBase, DataKey.cvExten) )  
{  
  case SINGLE:  
    /* deal with a single length key */  
    break;  
  case DOUBLE:  
    /* deal with a double length key */  
    break;  
  default :  
    /*return with an error */  
}
```

### Return Codes

This function has no return codes.

## cas\_key\_tokentvv\_check - Verify the Token Validation Value

cas\_key\_tokentvv\_check verifies the Token Validation Value (TVV) in the specified internal DES key token. The TVV is an integrity check value used to detect corruption of the token.

The function returns TRUE if the TVV verifies, and FALSE if not.

### Function Prototype

```
boolean cas_key_tokentvv_check( des_key_token_structure *pKeyToken )
```

### Input

On entry to this routine:

pKeyToken is a pointer to the internal DES key token that you want to check.

### Output

On successful exit from this routine:

cas\_key\_token\_tvv\_check returns a boolean value of TRUE if the TVV verifies, and FALSE if not.

### Return Codes

This function has no return codes.

## CasMasterKeyCheck - Master Key Version Check

CasMasterKeyCheck determines which version of the master key was used to encrypt the specified key token for the `mk_set` being processed. The response indicates whether the key token is encrypted using the current master key, the old master key, or a master key that is no longer available.

### Function Prototype

```
UNDER_MASTER_KEY CasMasterKeyCheck ( mk_selectors          *pMKSelector,
                                     des_key_token_structure *pKeyToken )
UNDER_MASTER_KEY cas_master_key_check( des_key_token_structure *pKeyToken )
```

`cas_master_key_check` has the same effect as calling `CasMasterKeyCheck` with the `pMKSelector` parameter set to `{MK_SET_DEFAULT, current_mk, SYM_MK}`.

### Input

On entry to this routine:

`MKSelector` is a parameter of type `mk_selectors`, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- `mk_set` is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to `MK_SET_DEFAULT`.
- `mk_register` must be set to `new_mk` or `current_mk`.
- `type_mks` should be set to `ASYM_MK` if this set of master keys is intended for PKA key encryption or `SYM_MK` if this set of master keys is used for DES key encryption.

`pKeyToken` is a pointer to the key token which is to be examined.

### Output

On successful exit from this routine:

`cas_master_key_check` returns either `OLD`, `CURRENT`, or `OUT_OF_DATE` which identifies which master key (old, current, or no longer available) the key token is encrypted under.

### Notes

In CCA, an “operational key” is a key that has been multiply-enciphered with the master key. In order to use an operational key, it must first be deciphered using the master key.

When the user (security officers, and so on) updates the master key, CCA maintains a copy of the old master key. This routine determines which version of the master key was used to encipher the specified key token (CCA does this by maintaining a hash value of the master key called the master key verification pattern which is stored in the DES key token). Refer to Appendix B of the *IBM 4758 PCI Cryptographic Coprocessor CCA Basic Services Reference and Guide* for more information.



Since CCA only stores 2 versions of the master key (current and old), upon encountering a key token enciphered with the old master key, the UDX developer may opt to re-encipher the key token using the current master key.

**Return Codes**

This function has no return codes.

## cas\_parity\_odd - Verify Parity

cas\_parity\_odd determines whether the specified byte has odd or even parity.

### Function Prototype

```
boolean cas_parity_odd( UCHAR DataByte )
```

### Input

On entry to this routine:

DataByte is the byte that is to be checked.

### Output

On successful exit from this routine:

cas\_parity\_odd returns TRUE if the specified byte has odd parity, or FALSE if it has even parity.

### Return Codes

This function has no return codes.

## RecoverDesDataKeyWithMK - Recover DES Data Key

RecoverDesDataKeyWithMK recovers the cleartext form of a DES data key that has been enciphered with the master key for the mk\_set being processed. The input token is checked to ensure it is valid.

### Function Prototype

```

long RecoverDesDataKeyWithMK (des_key_token_structure *pDesToken,
                             mk_selectors             *pMKSelector,
                             UCHAR                    *pClearKey,
                             long                     *pMsg)
long RecoverDesDataKey      (des_key_token_structure *pDesToken,
                             UCHAR                    *pClearKey,
                             long                     *pMsg)

```

RecoverDesDataKey is the equivalent of calling RecoverDesDataKeyWithMK after setting the MKSelector parameter to {MK\_SET\_DEFAULT, current\_mk, SYM\_MK}.

### Input

On entry to this routine:

pDesToken is a pointer to the input key token.

MKSelector is a parameter of type mk\_selectors, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register must be set to new\_mk or current\_mk.
- type\_mks should be set to ASYM\_MK if this set of master keys is intended for PKA key encryption or SYM\_MK if this set of master keys is used for DES key encryption.

### Output

On successful exit from this routine:

pClearKey is a pointer to the location where the function stores the recovered, cleartext key.

pMsg is the error code.

### Return Codes

Common return codes generated by this routine are:

|                           |  |
|---------------------------|--|
| <b>OK</b>                 | The operation was successful.                            |
| <b>ERROR</b>              | pMsg contains the error code.                            |
| <b>RT_OMK_TOKEN_USED</b>  | The key was encrypted with the Old master key (warning). |
| <b>E_INTRN_TOKEN_TV</b>   | The token is not valid.                                  |
| <b>mk_SRDI_OPEN_ERROR</b> | Could not open the master key SRDI.                      |

|                            |  |
|----------------------------|--|
| <b>mk_SEM_CLAIM_FAILED</b> | Unable to access the master key SRDI.                  |
| <b>RT_KEY_INV_MKVN</b>     | The key was encrypted using an out-of-date master key. |
| <b>RT_KDATA_NOTODD</b>     | The cleartext key failed a parity check.               |

## RecoverDesKekImporterWithMK - Recover DES Importer KEK

RecoverDesKekImporterWithMK recovers the cleartext form of a DES importer key encrypting key (KEK) that has been enciphered with the master key for the `mk_set` being processed. The token validation value is then confirmed, and the key is checked for parity.

### Function Prototype

```
long RecoverDesKekImporterWithMK ( des_key_token_structure *pDesToken,
                                   mk_selectors                *pMKSelector,
                                   UCHAR                      *pClearKey,
                                   long                        *pMsg )
long RecoverDesKekImporter      ( des_key_token_structure *pDesToken,
                                   UCHAR                      *pClearKey,
                                   long                        *pMsg )
```

RecoverDesKekImporter is the equivalent of calling RecoverDesKekImporterWithMK with the MKSelector parameter set to {MK\_SET\_DEFAULT, current\_mk, SYM\_MK}.

### Input

On entry to this routine:

`pDesToken` is a pointer to the input key token.

`MKSelector` is a parameter of type `mk_selectors`, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- `mk_set` is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to `MK_SET_DEFAULT`.
- `mk_register` must be set to `new_mk` or `current_mk`.
- `type_mks` should be set to `ASYM_MK` if this set of master keys is intended for PKA key encryption or `SYM_MK` if this set of master keys is used for DES key encryption.

### Output

On successful exit from this routine:

`pClearKey` is a pointer to the location where the function stored the recovered, cleartext key.

`pMsg` is the error code.

### Return Codes

Common return codes generated by this routine are:

|                           |  |
|---------------------------|--|
| <b>OK</b>                 | The operation was successful.                            |
| <b>ERROR</b>              | <code>pMsg</code> contains the error code.               |
| <b>RT_OMK_TOKEN_USED</b>  | The key was encrypted with the Old master key (warning). |
| <b>E_INTRN_TOKEN_TVV</b>  | The token is not valid.                                  |
| <b>mk_SRDI_OPEN_ERROR</b> | Could not open the master key SRDI.                      |

|                            |  |
|----------------------------|--|
| <b>mk_SEM_CLAIM_FAILED</b> | Unable to access the master key SRDI.                  |
| <b>RT_KEY_INV_MKVN</b>     | The key was encrypted using an out-of-date master key. |
| <b>RT_KDATA_NOTODD</b>     | The cleartext key failed a parity check.               |

## Chapter 9. RSA Functions

This chapter contains functions for dealing with RSA keys and key tokens.

Refer to Appendix B of the *IBM 4758 PCI Cryptographic Coprocessor CCA Basic Services Reference and Guide* for an overview of public and private key token structures.

**Note:** All functions within this chapter are available only on the coprocessor.

### Header Files for RSA Functions

When using these functions, your program must include the following header files.

```
#include "cmncrypt2.h"           /* T2 CPRB definitions      */
#include "scc_int.h"             /* CP/Q++ API               */
#include "cam_xtrn.h"           /* CCA managers             */
#include "cacdtkn.h"            /* public header file       */
#include "casfunct.h"           /* functions for generating RSA
#include "cacmkld.h"            /* signatures and registered keys */
```

### Summary of Functions

RSA keys and key tokens include the following functions.

|                                       |  |
|---------------------------------------|--|
| <b>CalculatenWordLength</b>           | Returns the word length. See page 9-6.   |
| <b>CreateInternalKeytokenWithMK</b>   | Receives a clear key token and creates the internal form. See page 9-7.  |
| <b>CreateRsaInternalSectionWithMK</b> | Creates the RSA internal section. See page 9-8.  |
| <b>delete_KeyToken</b>                | Remove a registered public or private key from storage. See page 9-9.  |
| <b>GenerateCcaRsaToken</b>            | Generates a CCA RSA key token from an internal format key token and a CCA PKA skeleton token. See page 9-10.                       |
| <b>GenerateRsaInternalToken</b>       | Creates an internal RSA token from a CCA RSA key token. See page 9-11.   |
| <b>generate_dSig</b>                  | Receives an RSA key token (in operational format) and a buffer of data (with the length and the digital signature). See page 9-12. |
| <b>GeteLength</b>                     | Returns the RSA public exponent byte length. See page 9-14.  |

|                                |   |
|--------------------------------|---|
| <b>getKeyToken</b>             | Retrieves a PKA token from the SRDI where it is stored. See page 9-15.                                  |
| <b>GetModulus</b>              | Extracts and copies the RSA modulus. See page 9-16.   |
| <b>GetnBitLength</b>           | Returns the bit length of the RSA modulus. See page 9-17.   |
| <b>GetnByteLength</b>          | Returns the byte length of the RSA modulus. See page 9-18.  |
| <b>GetPublicExponent</b>       | Extracts and copies the RSA key public exponent. See page 9-19.   |
| <b>GetRsaPrivateKeySection</b> | Returns a pointer to the private key section of an RSA key token. See page 9-20.                        |
| <b>GetRsaPublicKeySection</b>  | Returns a pointer to the public key section of an RSA key token. See page 9-21.                         |
| <b>GetTokenLength</b>          | Returns the length of the specified token. See page 9-22.   |
| <b>IsPrivateExponentEven</b>   | Verifies whether the RSA private exponent is an even valued integer. See page 9-23.                     |
| <b>IsPrivateKeyEncrypted</b>   | Verifies whether the private key section of the specified key token is encrypted. See page 9-24.        |
| <b>IsPublicExponentEven</b>    | Verifies whether the RSA public exponent is an even valued integer. See page 9-25.                      |
| <b>IsRsaToken</b>              | Verifies whether the key token contains an RSA key. See page 9-26.                                      |
| <b>IsTokenInternal</b>         | Identifies whether the key token is in internal format. See page 9-27.                                  |
| <b>PkaHashQueryWithMK</b>      | Returns the master key version used to encrypt the specified token. See page 9-28.                      |
| <b>PkaMkvpQueryWithMK</b>      | Returns a value indicating which master key was used to encrypt the specified key token. See page 9-29. |
| <b>pka96_tvngen</b>            | Calculates the token validation value (TVV) for the specified key token. See page 9-30.                 |



|   |  |
|---|--|
| <b>RecoverPkaClearKeyTokenUnderMkWithMK</b> | Recovers the PKA clear key token under the master key. See page 9-31.                                    |
| <b>RecoverPkaClearKeyTokenUnderXport</b>    | Recovers the PKA clear key token under the DES export key. See page 9-33.                                |
| <b>ReEncipherPkaKeyTokenWithMK</b>          | Re-enciphers an internal PKA key token from the old master key to the current master key. See page 9-34. |
| <b>RequestRSACrypto</b>                     | Performs an RSA operation. See page 9-35.  |
| <b>store_KeyToken</b>                       | Saves a public or private key to the SRDI. See page 9-36.  |
| <b>TokenMkvpMatchMasterKey</b>              | Tests whether the key token was encrypted using a specified version of the master key. See page 9-37.    |
| <b>ValidatePkaToken</b>                     | Verifies that the RSA key token is valid for use in the system. See page 9-38.                           |
| <b>VerifyKeyTokenConsistency</b>            | Verifies the consistency of a key token. See page 9-39.  |
| <b>verify_dSig</b>                          | Verifies the RSA key token signature. See page 9-40.   |

## Overview

An RSA key consists of a public modulus which is the product of two large prime numbers, a public exponent which is relatively prime to the modulus, and a private exponent  $d$ . In the coprocessor, keys may be stored in CCA RSA tokens in the key storage file and used in the SCC complete tokens. Either form of key has a public and a private version.

The public version SCC complete token of a key contains the modulus and the public exponent of the key, and the length of each. The private version may be in either modulus exponent or Chinese remainder format, and contains the modulus and public and private exponents for each. This version of a key is used in the cryptographic engine for `sccRSA()` requests and is the type returned by `sccRSAKeyGenerate()`.

CCA RSA tokens consist of a token header, followed by

1. an optional private key section which holds the decrypting information (the private key and the public modulus), verification data, and key-encryption data
2. and a required public key section which holds encryption information (the public exponent and the modulus.)

Parts of the private key section may be encrypted under the master key (*internal keys*) or under a transport key (*external keys*). This is the version of a key which is stored in the key-storage file.

The functions in this chapter can be separated into the following categories:

**Informational:** (All of these functions operate on CCA RSA key tokens)

|                                   |  |
|-----------------------------------|--|
| <code>CalculatenWordLength</code> | Returns the length of the modulus in 16-bit words. |
| <code>GeteLength</code>           | Returns the length of the public exponent.         |
| <code>GetnBitLength</code>        | Returns the length of the modulus in bits.         |
| <code>GetnByteLength</code>       | Returns the length of the modulus in bytes.        |
| <code>GetTokenLength</code>       | Returns the length of the CCA RSA key token.       |

### Key checking

|                                      |   |
|--------------------------------------|---|
| <code>IsPrivateExponentEven</code>   | Verifies whether the private exponent of the CCA RSA key token is even.   |
| <code>IsPrivateKeyEncrypted</code>   | Verifies whether the private key section of the CCA RSA key token is encrypted.                                     |
| <code>IsPublicExponentEven</code>    | Verifies whether the public exponent of the CCA RSA key token is even.  |
| <code>IsRsaToken</code>              | Verifies whether the supplied token is an RSA token.  |
| <code>IsTokenInternal</code>         | Verifies whether the CCA RSA key token has been encrypted with the master key (that is, an <i>internal token</i> ). |
| <code>PkaMkvpQuery</code>            | Identifies which master key was used to encrypt the specified internal CCA RSA key token.                           |
| <code>TokenMkvpMatchMasterKey</code> | Tests whether the internal CCA RSA key token was encrypted with the specified master key.                           |
| <code>ValidatePkaToken</code>        | Verifies that a CCA RSA key token is valid for use in the system.   |

VerifyKeyTokenConsistency Tests the length fields of the CCA RSA key token, ensuring that they are consistent.

### Key manipulation

|                                      |   |
|--------------------------------------|---|
| CreateInternalKeyToken               | Receives a clear CCA RSA key token and encrypts the private key data, creating an internal CCA RSA key token.       |
| CreateRsaInternalSection             | Receives an SCC complete token and creates an internal CCA RSA key token, including encrypting with the master key. |
| GenerateRsaInternalToken             | Receives a CCA RSA key token and creates an SCC complete token.   |
| GetModulus                           | Returns the public modulus of the CCA RSA key token.  |
| GetPublicExponent                    | Returns the public exponent of the CCA RSA key token.   |
| GetRsaPrivateKeySection              | Returns a pointer to the private key section of the CCA RSA key token.  |
| GetRsaPublicKeySection               | Returns a pointer to the private key section of the CCA RSA key token.  |
| pka96_tvngen                         | Calculates the token validation value for the CCA RSA key token.  |
| RecoverPkaClearKeyTokenUnderMkWithMK | Decrypts an internal CCA RSA key token.   |
| RecoverPkaClearKeyTokenUnderXport    | Decrypts an external CCA RSA key token.   |
| ReEncipherPkaKeyToken                | Decrypts a CCA RSA key token with the old master key and encrypts it with the current master key.                   |
| RequestRSACrypto                     | Performs an encryption or decryption operation with the CCA RSA key token.  |

## CalculatenWordLength - Return Word Length of Modulus

CalculatenWordLength returns the length of the modulus in terms of the number of 16-bit *words* it occupies.

### Function Prototype

```
USHORT CalculatenWordLength ( RsaKeyTokenHeader *pToken )
```

### Input

On entry to this routine:

pToken is a pointer to the key token.

### Output

On successful exit from this routine:

CalculatenWordLength returns the length of the modulus in 16-bit words.

### Return Codes

This function has no return codes.

## CreateInternalKeyTokenWithMK - Create Internal Key Token

CreateInternalKeyTokenWithMK receives a clear CCA RSA key token and creates the internal form by encrypting the private key areas under the master key for the mk\_set being processed.

### Function Prototype

```
long CreateInternalKeyTokenWithMK ( RsaKeyTokenHeader *pTokenIn,
                                   mk_selectors      *pMKSelector,
                                   RsaKeyTokenHeader *pTokenOut )
long CreateInternalKeyToken      ( RsaKeyTokenHeader *pTokenIn,
                                   RsaKeyTokenHeader *pTokenOut )
```

CreateInternalKeyToken has the same effect as calling CreateInternalKeyTokenWithMK after setting the MKSelector parameter to {MK\_SET\_DEFAULT, current\_mk, ASYM\_MK}.

### Input

On entry to this routine:

pTokenIn is a pointer to the cleartext key token.

MKSelector is a parameter of type mk\_selectors, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register must be set to new\_mk or current\_mk
- type\_mks should be set to ASYM\_MK.

### Output

On successful exit from this routine:

pTokenOut is a pointer to a location which contains the encrypted internal key token.

### Return Codes

Common return codes generated by this routine are:

|                            |  |
|----------------------------|--|
| <b>ERROR</b>               | The token is not an RSA token, or already has an internal section. |
| <b>mk_KEY_NOT_VALID</b>    | The current master key is not valid.                               |
| <b>mk_SEM_CLAIM_FAILED</b> | Could not access the master keys.                                  |

## CreateRsaInternalSectionWithMK - Create RSA Internal Section

CreateRsaInternalSectionWithMK receives an SCC complete token and creates an internal CCA RSA key token by calculating the validation values and encrypting under the master key for the mk\_set being processed.

### Function Prototype

```
long CreateRsaInternalSectionWithMK ( RsaKeyTokenHeader *pTokenOut,
                                     mk_selectors      *pMKSelector,
                                     sccRSAKeyToken_t  *pRsaTokenIn )
long CreateRsaInternalSection      ( RsaKeyTokenHeader *pTokenOut,
                                     sccRSAKeyToken_t  *pRsaTokenIn )
```

CreateRsaInternalSection has the same effect as calling CreateRsaInternalSectionWithMK after setting the MKSelector parameter to {MK\_SET\_DEFAULT, current\_mk, ASYM\_MK}.

**Note:** This function only works with version 0 tokens.

### Input

On entry to this routine:

pTokenOut is a pointer to a variable which will hold the new CCA RSA key token.

MKSelector is a parameter of type mk\_selectors, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register must be set to new\_mk or current\_mk.
- type\_mks should be set to ASYM\_MK if this set of master keys is intended for PKA key encryption or SYM\_MK if this set of master keys is used for DES key encryption.

pRsaTokenIn is a pointer to the internal SCC key structure.

### Output

This function returns no output. On successful exit from this routine:

The internal section of the CCA RSA key token is created.

pTokenOut contains the new CCA RSA token.

### Return Codes

Common return codes generated by this routine are:

|                            |                                      |
|----------------------------|--------------------------------------|
| <b>OK</b>                  | The operation was successful.        |
| <b>mk_KEY_NOT_VALID</b>    | The current master key is not valid. |
| <b>mk_SEM_CLAIM_FAILED</b> | Could not access the master keys.    |

## delete\_KeyToken - Delete a Key From On-Board Storage

delete\_KeyToken permanently removes a registered public key or retained private key from storage in the coprocessor.

### Function Prototype

```
delete_KeyToken ( char *pKeyName )
```

### Input

On entry to this routine:

pKeyName is a pointer to a 64 byte array containing the name of the key to be deleted.

### Output

This function returns no output. On successful exit from this routine:

The key referenced by pKeyName is no longer in storage, and the key storage SRDI has been resized.

### Return Codes

Common return codes generated by this routine are:

|                           |  |
|---------------------------|--|
| <b>OK</b>                 | The operation was successful.          |
| <b>Key_NAME_NOT_FOUND</b> | The key was not found in the list.     |
| <b>CP_MEMORY_NAVAIL</b>   | Out of memory error.                   |
| <b>PKEY_SRDI_ERROR</b>    | Unable to access the key storage SRDI. |

## GenerateCcaRsaToken - Generate CCA RSA Key Token

GenerateCcaRsaToken generates a CCA RSA key token from an internal (CP/Q++) format key token and a CCA PKA skeleton token. The skeleton token must be initialized to indicate the required format of the final token.

### Function Prototype

```
long GenerateCcaRsaToken ( RsaKeyTokenHeader *pPkaToken,  
                          sccRSAKeyToken_t *pRsaKeyToken)
```

### Input

On entry to this routine:

pPkaToken must be a pointer to a CCA RSA key token header whose nextSection field contains the desired CCA Key token type (RSA\_PRIVATE\_SECTION\_NOPT, RSA\_PRIVATE\_SECTION\_CR, RSA\_PRIVATE\_SECTION\_NOPT\_VAR, (for version 0 keys)).

pRsaKeyToken must be a pointer to a valid internal (CP/Q++) RSA key token.

### Output

On successful exit from this routine:

pPkaToken contains a valid CCA RSA token of the type desired.

### Return Codes

Common return codes generated by this routine are:

- |              |   |
|--------------|---|
| <b>OK</b>    | The operation was successful.           |
| <b>ERROR</b> | The skeleton token was not initialized. |



## GenerateRsaInternalToken - Generate RSA Key Token

GenerateRsaInternalToken receives a CCA RSA key token and creates an SCC complete token with all data aligned on 4-byte boundaries, for use in RSA computations.

### Function Prototype

```
long GenerateRsaInternalToken  
(  
    RsaKeyTokenHeader *pPkaTokenIn,  
    sccRSAKeyToken_t  *pRsaKeyTokenOut  
)
```

### Input

On entry to this routine:

pPkaTokenIn is a pointer to the CCA RSA key token.

### Output

On successful exit from this routine:

pRsaKeyTokenOut is a pointer to the location where the function stores the internal SCC complete key token it creates from the specified CCA RSA token.

### Return Codes

Common return codes generated by this routine are:

- |              |  |
|--------------|--|
| <b>OK</b>    | The operation was successful.                |
| <b>ERROR</b> | The input key token is not an RSA key token. |

## generate\_dSig - Receives RSA Key Token

generate\_dSig receives an RSA key token in operational format and a buffer of data, with the length of the data and the expected length of the digital signature. The key token is deciphered and the input data is hashed with SHA-1, then the data is formatted according to the requested Type before signing with the clear key. The format may be one of ISO-9796, PKCS #1 block type 0 or 1, or zero-padded.

### Function Prototype

```
long generate_dSig ( RsaKeyTokenHeader *pTokenIn,
                   UCHAR              *pDataIn,
                   long                DataLength,
                   UCHAR              *pSignatureOut,
                   USHORT              *pSignatureBitLength,
                   UCHAR              Type )
```

### Input

On entry to this routine:

pTokenIn is a pointer to the operational key token.

pDataIn is a pointer to the data which is to be signed.

DataLenth is the length of the data to be signed, in bytes.

pSignatureOut is a pointer to a buffer which is to hold the returned signature.

pSignatureBitLength is a pointer to the length of the buffer pSignatureOut, in bits.

Type is one of the following:

- M\_IS09796 if the data is to be formatted according to the ISO-9796 standard before signing.
- M\_PKCS10 if the data is to be formatted as specified in the RSADataSecurity, Inc., *Public Key Cryptography Standards #1* block type 00 before signing.
- M\_PKCS11 if the data is to be formatted as specified in the RSADataSecurity, Inc., *Public Key Cryptography Standards #1* block type 01 before signing.
- M\_ZEROPAD if the Data is to be placed in the low-order bits of a bit-string of the same length as the modulus with all other bit-positions set to zero before signing.

### Output

On successful exit from this routine:

pSignatureBitLength contains the length (in bits) of the calculated digital signature.

pSignatureOut contains the digital signature.

**Return Codes**

Common return Codes generated by this routine are:

- |                   |  |
|-------------------|--|
| <b>OK</b>         | The operation was successful.                                      |
| <b>E_SIZE</b>     | The provided buffer was not large enough to contain the signature. |
| <b>PKABadAddr</b> | The key token is not valid.  |

## GetLength - Return RSA Public Exponent Byte Length

GetLength returns the byte length of the RSA public exponent field, as contained in the member field of the key token.

**Note:** The member field is a 16-bit field and is in zSeries (big-endian) format. This routine returns the 16-bit integer in Intel\*\* (little-endian) format.

### Function Prototype

```
USHORT GetLength ( RsaKeyTokenHeader *pToken )
```

### Input

On entry to this routine:

pToken is a pointer to the key token.

### Output

On successful exit from this routine:

GetLength returns the byte length of the RSA public exponent field.

### Return Codes

This function has no return codes.

## getKeyToken - Get a PKA Token From On-Board Storage

getKeyToken retrieves a PKA retained private key or registered public key from the SRDI where it is stored.

### Function Prototype

```
long getKeyToken ( char *pLabel,  
                  char *pKey,  
                  USHORT *pFlags )
```

### Input

On entry to this routine:

pLabel is a pointer to a string containing the label associated with the requested key.

pKey is a pointer to a buffer in which the key token can be written. The maximum length required is 2500 bytes.

pFlags is a pointer to a 2-byte buffer which can hold returned flags from the key token.

### Output

On successful exit from this routine:

pKey contains the clear key token associated with the label at pLabel.

pFlags contains the flags associated with the key.

### Return Codes

Common return codes generated for this function are:

|                          |   |
|--------------------------|---|
| <b>srdi_NO_ERROR</b>     | The command completed successfully.               |
| <b>PKEY_NOT_REGISTER</b> | The key was not found.                            |
| <b>PKEY_SRDI_ERROR</b>   | The registered key manager could not be accessed. |

## GetModulus - Extract and Copy RSA Modulus

GetModulus extracts the RSA key modulus from the specified key token, and copies it to the buffer provided.

### Function Prototype

```
void GetModulus ( RsaKeyTokenHeader *pToken,  
                 UCHAR              *pModulus )
```

### Input

On entry to this routine:

pToken is a pointer to the key token.

pModulus is a pointer to a buffer for the modulus.

### Output

On successful exit from this routine:

pModulus is a pointer to the provided buffer where the RSA key modulus is stored.

### Return Codes

This function has no return codes.

## GetnBitLength - Return RSA Modulus Bit Length

GetnBitLength returns the bit length of the RSA modulus as contained in the member field of the key token.

**Note:** The member field is a 16-bit field and is in zSeries (big-endian) format. This routine returns the 16-bit integer in Intel\*\* (little-endian) format.

### Function Prototype

```
USHORT GetnBitLength ( RsaKeyTokenHeader *pToken )
```

### Input

On entry to this routine:

pToken is a pointer to the key token.

### Output

On successful exit from this routine:

GetnBitLength returns the bit length of the RSA modulus.

### Return Codes

This function has no return codes.

## GetnByteLength - Return RSA Modulus Byte Length

GetnByteLength returns the length of the RSA modulus, in bytes.

**Note:** The key token contains a member field which indicates the modulus byte length. This field may not be the actual byte length, but is an indication of the length of the field containing the modulus. This function returns the *actual* byte length of the modulus by calculating it from the bit length. It does not use the byte length member field from the key token.

### Function Prototype

```
USHORT GetnByteLength ( RsaKeyTokenHeader *pToken )
```

### Input

On entry to this routine:

pToken is a pointer to the key token.

### Output

On successful exit from this routine:

GetnByteLength returns the length of the RSA modulus, in bytes.

### Return Codes

This function has no return codes.



## GetPublicExponent - Extract and Copy Public Exponent

GetPublicExponent extracts the RSA key public exponent from the specified key token, and copies it to the provided buffer *pDest*.

### Function Prototype

```
USHORT GetPublicExponent ( RsaKeyTokenHeader *pToken,  
                           UCHAR *pDest )
```

### Input

On entry to this routine:

*pToken* is a pointer to the key token.

*pDest* is a pointer to the 64-byte buffer provided for the exponent.

### Output

On successful exit from this routine:

*pDest* is a pointer to the caller's buffer where the RSA key public exponent is stored.

GetPublicExponent returns the length of the exponent.

### Return Codes

This function has no return codes.

## GetRsaPrivateKeySection - Return Private Key

GetRsaPrivateKeySection returns a pointer to the private key section of an RSA key token, if it is present. Otherwise, the function returns a null pointer.

### Function Prototype

```
void * GetRsaPrivateKeySection ( RsaKeyTokenHeader *pToken )
```

### Input

On entry to this routine:

pToken is a pointer to the RSA key token.

### Output

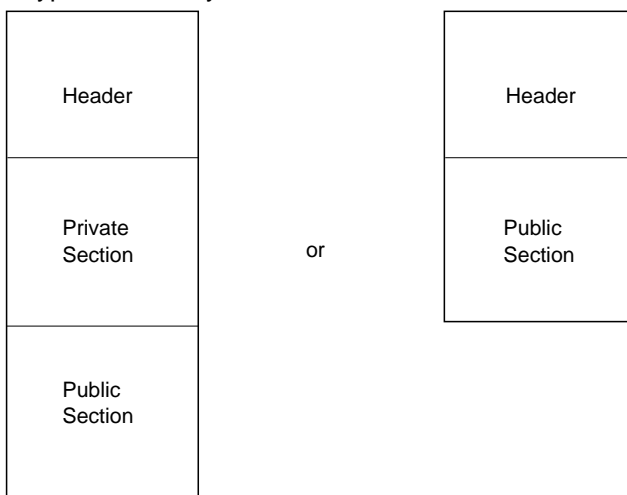
This function returns no output. On successful exit from this routine:

GetRsaPrivateKeySection returns a pointer to the private key section of an RSA key token.

### Notes

Refer to Appendix B of the *IBM 4758 PCI Cryptographic Coprocessor CCA Basic Services Reference and Guide* for a diagram of the key token structure.

A typical RSA key token looks similar to the following:



### Return Codes

This function has no return codes.

## GetRsaPublicKeySection - Return Public Key

GetRsaPublicKeySection returns a pointer to the public key section of an RSA key token, if it is present. If not, the function returns a null pointer.

**Note:** If no public key section is present an internal error has occurred, since all RSA tokens should contain a public key section.

### Function Prototype

```
void * GetRsaPublicKeySection ( RsaKeyTokenHeader *pToken )
```

### Input

On entry to this routine:

pToken is a pointer to the RSA key token.

### Output

On successful exit from this routine:

GetRsaPublicKeySection returns a pointer to the public key section of an RSA key token.

### Return Codes

This function has no return codes.

## GetTokenLength - Return Key Token Length

GetTokenLength returns the length of the specified token, as contained in the member field of the header.

**Note:** The member field is a 16-bit field and is in zSeries (big-endian) format. This routine returns the 16-bit integer in Intel\*\* (little-endian) format.

### Function Prototype

```
USHORT GetTokenLength ( RsaKeyTokenHeader *pToken )
```

### Input

On entry to this routine:

pToken is a pointer to the key token.

### Output

On successful exit from this routine:

GetTokenLength returns the length of the specified token.

### Return Codes

This function has no return codes.

## IsPrivateExponentEven - Verify RSA Private Exponent

IsPrivateExponentEven returns TRUE if the private exponent in the specified key token is an even valued integer; otherwise, it returns FALSE.

### Function Prototype

```
boolean IsPrivateExponentEven ( RsaKeyTokenHeader *pToken )
```

### Input

On entry to this routine:

pToken is a pointer to the key token.

### Output

On successful exit from this routine:

IsPrivateExponentEven returns TRUE if the private exponent in the specified key token is an even valued integer, and FALSE if it is not.

### Return Codes

This function has no return codes.

## IsPrivateKeyEncrypted - Verify Private Key Encryption

IsPrivateKeyEncrypted returns TRUE if the private key section of the specified PKA key token is in encrypted form, or FALSE if not.

### Function Prototype

```
boolean IsPrivateKeyEncrypted ( RsaKeyTokenHeader *pToken )
```

### Input

On entry to this routine:

pToken is a pointer to the key token.

### Output

On successful exit from this routine:

IsPrivateKeyEncrypted returns TRUE if the private key section of the specified PKA key token is in encrypted form, and FALSE if it is not.

### Return Codes

This function has no return codes.

## IsPublicExponentEven - Verify RSA Public Exponent

IsPublicExponentEven returns TRUE if the public exponent in the specified key token is an even valued integer; otherwise, it returns FALSE.

### Function Prototype

```
boolean IsPublicExponentEven ( RsaKeyTokenHeader *pToken )
```

### Input

On entry to this routine:

pToken is a pointer to the key token.

### Output

On successful exit from this routine:

IsPublicExponentEven returns TRUE if the public exponent in the specified key token is an even valued integer, and FALSE if it is not.

### Return Codes

This function has no return codes.

## IsRsaToken - Verify RSA Key

IsRsaToken returns TRUE if the specified key token contains an RSA key, or FALSE if it does not.

### Function Prototype

```
boolean IsRsaToken ( RsaKeyTokenHeader *pToken )
```

### Input

On entry to this routine:

pToken is a pointer to the key token.

### Output

On successful exit from this routine:

IsRsaToken returns TRUE if the specified key token contains an RSA key, and FALSE if it is not an RSA key token.

### Return Codes

This function has no return codes.



## IsTokenInternal - Key Token Format

IsTokenInternal returns TRUE if the specified key token is in *internal* format, or FALSE if it is in *external* format.

### Function Prototype

```
boolean IsTokenInternal ( RsaKeyTokenHeader *pToken )
```

### Input

On entry to this routine:

pToken is a pointer to the key token.

### Output

On successful exit from this routine:

IsTokenInternal returns TRUE if the specified key token is in *internal* format, or FALSE if it is in *external* format.

### Notes

Internal key tokens contain private key information that has been multiply-enciphered with the master key. RecoverPkaClearKeyTokenUnderMk() is used to decipher an internal key token so that it may be used.

### Return Codes

This function has no return codes.

## PkaHashQueryWithMK - Return Master Key Version

PkaHashQueryWithMK returns a value indicating which master key was used to encrypt the specified key token for the mk\_set being processed.

### Function Prototype

```
MK_VERSION PkaHashQueryWithMK ( RsaKeyTokenHeader *pToken,  
                                mk_selectors      *pMKSelector )
```

### Input

On entry to this routine:

pToken is a pointer to a variable which will hold the new CCA RSA key token.

MKSelector is a parameter of type mk\_selectors, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register must be set to new\_mk, current\_mk, or old\_mk.
- type\_mks should be set to ASYM\_MK.

### Output

This function returns no output. On successful exit from this routine: pToken returns the version of the master key (MK\_CURRENT, MK\_OLD, or MK\_OUT\_OF\_DATE) that was used to encrypt the specified key token.

### Return Codes

Common return codes generated by this routine are:

|                            |                                      |
|----------------------------|--------------------------------------|
| <b>OK</b>                  | The operation was successful.        |
| <b>mk_KEY_NOT_VALID</b>    | The current master key is not valid. |
| <b>mk_SEM_CLAIM_FAILED</b> | Could not access the master keys.    |

## PkaMkvpQueryWithMK - Return Master Key Version

PkaMkvpQueryWithMK returns a value indicating which master key was used to encrypt the specified key token for the `mk_set` being processed.

### Function Prototype

```

MK_VERSION PkaMkvpQueryWithMK ( RsaKeyTokenHeader *pToken,
                                mk_selectors      *pMKSelector
MK_VERSION PkaMkvpQuery      ( RsaKeyTokenHeader *pToken )

```

PkaMkvpQuery has the same effect as calling PkaMkvpQueryWithMK after setting the MKSelector parameter to {MK\_SET\_DEFAULT, current\_mk, ASYM\_MK}.

This function only works with version 0 tokens.

### Input

On entry to this routine:

`pToken` is a pointer to the key token that is checked.

`MKSelector` is a parameter of type `mk_selectors`, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- `mk_set` is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to `MK_SET_DEFAULT`.
- `mk_register` must be set to `new_mk` or `current_mk`
- `type_mks` should be set to `ASYM_MK`.

### Output

On successful exit from this routine:

PkaMkvpQuery returns the version of the master key (`MK_CURRENT`, `MK_OLD`, or `MK_OUT_OF_DATE`) that was used to encrypt the specified key token.

### Return Codes

This function has no return codes.

## pka96\_tvvgen - Calculate Token Validation Value

pka96\_tvvgen calculates the token validation value (TVV) for the specified key token.

### Function Prototype

```
void pka96_tvvgen ( USHORT token_len, UCHAR *key_token_ptr, ULONG *tvv )
```

### Input

On entry to this routine:

token\_len is the length of the token specified with parameter *key\_token\_ptr*.

key\_token\_ptr is a pointer to the key token whose TVV is calculated.

### Output

On successful exit from this routine:

tvv is a pointer to the location where the calculated TVV is stored.

### Return Codes

This function has no return codes.

## RecoverPkaClearKeyTokenUnderMkWithMK

RecoverPkaClearKeyTokenUnderMkWithMK receives a PKA key token which is encrypted under the master key for the `mk_set` which is currently in use. If the key is in the on-board cache of decrypted keys, this key is returned to the calling function. Otherwise, the clear form of the key is recovered by decrypting the private areas of the key and verifying the SHA-1 hashes of those sections. The clear key is then added to the on-board cache before being returned to the calling function.

### Function Prototype

```

long RecoverPkaClearTokenUnderMkWithMK( RsaKeyTokenHeader *pTokenIn,
                                         RsaKeyTokenHeader *pTokenOut,
                                         mk_selectors      *pMKSelector,
                                         long                *pMsg )
long RecoverPkaClearKeyTokenUnderMk    ( RsaKeyTokenHeader *pTokenIn,
                                         RsaKeyTokenHeader *pTokenOut,
                                         long                *pMsg )

```

RecoverPkaClearKeyTokenUnderMk has the same effect as calling RecoverPkaClearTokenUnderMkWithMK after setting the MKSelector parameter to {MK\_SET\_DEFAULT, current\_mk, ASYM\_MK}.

### Input

On entry to this routine:

`pTokenIn` is a pointer to the encrypted key token.

`MKSelector` is a parameter of type `mk_selectors`, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- `mk_set` is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to `MK_SET_DEFAULT`.
- `mk_register` must be set to `new_mk` or `current_mk`
- `type_mks` should be set to `ASYM_MK`.

### Output

On successful exit from this routine:

`pTokenOut` is a pointer to the location which contains the decrypted key token.

`pMsg` is the error code.

### Notes

RecoverPkaClearKeyTokenUnderMk determines which master key was used to encipher.

This function does not change the value of byte 28 of the private key, the Key format and Security byte. If you are planning to store this key in clear form, you should change this byte to the appropriate value before storing. Refer to Appendix B of the *CCA Basic Services Reference and Guide* for the appropriate values for different RSA key token formats.

**Return Codes**

Common return codes generated by this routine are:

|                            |   |
|----------------------------|---|
| <b>OK</b>                  | The operation was successful.                               |
| <b>ERROR</b>               | pRC returns a CP/Q error indicating the cause of the error. |
| <b>RT_TKN_UNUSEABLE</b>    | The token was not an RSA token.                             |
| <b>RT_KEY_INV_MKVN</b>     | The key was encrypted with an invalid master key.           |
| <b>mk_SRDI_OPEN_ERROR</b>  | Could not open the master key.                              |
| <b>mk_SEM_CLAIM_FAILED</b> | Unable to access the SRDI Manager.                          |

## RecoverPkaClearKeyTokenUnderXport

RecoverPkaClearKeyTokenUnderXport receives a PKA key token which is encrypted under a DES export key, and recovers the clear form by decrypting the private key areas and then verifying the SHA-1 hashes contained in those areas.

### Function Prototype

```
long RecoverPkaClearKeyTokenUnderXport( RsaKeyTokenHeader *pTokenIn,  
                                         double_length_key *desKey,  
                                         RsaKeyTokenHeader *pTokenOut )
```

### Input

On entry to this routine:

pTokenIn is a pointer to the encrypted key token.

desKey is a pointer to the DES exporter key token.

pTokenOut is a pointer to a location which can store a key token.

### Output

On successful exit from this routine:

pTokenOut contains the cleartext key token that it recovers.

### Return Codes

Common return codes generated by this routine are:

|              |                               |
|--------------|-------------------------------|
| <b>OK</b>    | The operation was successful. |
| <b>ERROR</b> | The operation failed.         |

## ReEncipherPkaKeyTokenWithMK - Re-Encipher PKA Key Token

ReEncipherPkaKeyTokenWithMK re-enciphers an internal PKA key token from the old master key to the current master key for the `mk_set` being processed.

### Function Prototype

```

long ReEncipherPkaKeyTokenWithMK( RsaKeyTokenHeader *pToken,
                                   mk_selectors      *pMKSelector,
                                   UCHAR              *pWorkArea )
long ReEncipherPkaKeyToken      ( RsaKeyTokenHeader *pToken,
                                   UCHAR              *pWorkArea )

```

ReEncipherPkaKeyToken has the same effect as calling ReEncipherPkaKeyTokenWithMK after setting the `PMKSelector` parameter to `{MK_SET_DEFAULT, current_mk, ASYM_MK}`.

### Input

On entry to this routine:

`pToken` is a pointer to the input key token, enciphered under the old master key.

`MKSelector` is a parameter of type `mk_selectors`, indicating which set of master keys to use in this function. This variable must be initialized as follows:

- `mk_set` is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to `MK_SET_DEFAULT`.
- `mk_register` must be set to `new_mk` or `current_mk`
- `type_mks` should be set to `ASYM_MK`.

`pWorkArea` is a pointer to a variable which can hold a private key. This is used as a work area when decrypting.

### Output

On successful exit from this routine:

`pToken` contains the key token, which has been enciphered under the current master key.

### Return Codes

Common return codes generated by this routine are:

|              |  |
|--------------|--|
| <b>OK</b>    | The operation was successful.            |
| <b>ERROR</b> | The input token is not an RSA token.     |
| <b>FALSE</b> | Unable to verify the current master key. |



## RequestRSACrypto - Perform an RSA Operation

RequestRSACrypto converts the specified CCA RSA key token to the RSA internal key token format that the RSA engine requires, and then requests that the RSA engine perform the specified RSA function.

**Note:** Prior to using this routine, ensure that you've deciphered the private key (if you're using it) using the routine RecoverPkaClearKeyTokenUnderMkWithMk().

### Function Prototype

```
long RequestRSACrypto
(
    void                *pInput,
    RsaKeyTokenHeader *pKeyToken,
    void                *pOutput,
    ULONG               DataBitLength,
    ULONG               RsaOperation
)
```

### Input

On entry to this routine:

pInput is a pointer to the input data for the RSA operation.

pKeyToken is a pointer to the key token for the RSA key. This is a CCA format RSA key token.

DataBitLength is the length of the input data, in bits. This number is presumed to be equal to the length of the output data buffer, in bits. If this number is *larger* than the modulus length in bits, the data which will be operated on is in the rightmost modulusLength bits of the input data buffer, and the result will be placed in the rightmost modulusLength bits of the output data buffer.

RsaOperation is the requested RSA operation, such as RSA\_ENCRYPT (public key operation) or RSA\_DECRYPT (private key operation).

### Output

On successful exit from this routine:

pOutput is a pointer to a buffer that receives the results of the requested RSA operation.

### Return Codes

Common return codes generated by this routine are:

|                   |   |
|-------------------|---|
| <b>OK</b>         | The operation was successful.                           |
| <b>ERROR</b>      | Could not create a buffer to receive the RSA key token. |
| <b>E_SIZE</b>     | The data is smaller than the modulus.                   |
| <b>PKABadAddr</b> | The key token is not valid.                             |
| <b>PKANoSpace</b> | Unable to allocate sufficient memory.                   |

## store\_KeyToken - Store Registered or Retained Key

store\_KeyToken saves a registered public key or retained private key to the key retain SRDI on the coprocessor. Once stored in this area, a key may not be changed except by deleting with delete\_KeyToken.

### Function Prototype

```
long store_KeyToken ( KEY_register_data_t *pKey )
```

### Input

On entry to this routine:

pKey is a pointer to a KEY\_register\_data\_t, whose fields must be initialized as follows:

- version - The version of the key token stored in this record. Legal values are 0 and 1.
- reserved - This short variable must be initialized to 0.
- length - The length of this record, in little-endian format.
- label - Contains a 64-byte key name.
- flags - Valued to CCA\_CLONE if this key is allowed to participate in master key cloning operations, or 0 otherwise.
- keydata - The beginning of the actual key token.

### Output

This function returns no output. On successful exit from this routine:

The KeyRetain SRDI has been expanded to include the data a pKey.

### Return Codes

Common return codes generated by this routine are:

|                         |   |
|-------------------------|---|
| <b>srdi_NO_ERROR</b>    | The operation was successful.                   |
| <b>CP_MEMORY_NAVAIL</b> | Out of memory error.                            |
| <b>PK_SRDI_ERROR</b>    | Unable to access the key storage SRDI.          |
| <b>DUPLICATE_NAME</b>   | A key with the same name is already registered. |

## TokenMkvpMatchMasterKey - Test Encryption of RSA Key

TokenMkvpMatchMasterKey tests whether the specified key token was encrypted using a specified version of the master key. The Master Key Verification Pattern (MKVP) of the specified key token is compared to the MKVP for the specified master key. If the two are equal, the function returns TRUE; if not, it returns FALSE.

### Function Prototype

```
boolean TokenMkvpMatchMasterKey( mk_selectors      *mk_selector,  
                                RsaKeyTokenHeader *pToken )
```

### Input

On entry to this routine:

mk\_selector is a pointer to a variable which must be initialized as follows:

- mk\_set is a pointer to the set of master keys which is to be accessed, if more than one set is allowed on this operating system. Where there is only one set of master keys, this must be set to MK\_SET\_DEFAULT.
- mk\_register is set to either old\_mk, current\_mk, or new\_mk, representing the key which should be cleared.
- type\_mks should be set to ASYM\_MK.

pToken is a pointer to the key token that you want to test.

### Output

On successful exit from this routine:

TokenMkvpMatchMasterKey returns TRUE if the MKVP of the specified key token is equal to the MKVP for the specified master key, and FALSE if it is not.

### Return Codes

This function has no return codes.

## ValidatePkaToken - Validate RSA Key Token

ValidatePkaToken accepts a cleartext RSA key token, and verifies that the token is valid for use in the system.

### Function Prototype

```
long ValidatePkaToken( RsaKeyTokenHeader *pToken,  
                      long *pErrorCode )
```

### Input

On entry to this routine:

pToken is a pointer to the RSA key token.

pErrorCode is a pointer to the location where the function stores an error code, if a critical error occurs.

### Output

This function returns no output.

### Return Codes

Common return codes generated by this routine are:

|                         |   |
|-------------------------|---|
| <b>OK</b>               | The operation was successful.                                 |
| <b>ERROR</b>            | The input token is not an RSA key token.                      |
| <b>RSA_KEY_INVALID</b>  | The input token is not an internal or external RSA key token. |
| <b>RT_TKN_UNUSEABLE</b> | The input token is not an RSA key token.                      |
| <b>E_KEY_TKNVER</b>     | Incorrect version data in input token.                        |
| <b>E_PKA_KEYINVALID</b> | An error was found in the token.                              |

## VerifyKeyTokenConsistency - Verify Key Token Consistency

VerifyKeyTokenConsistency verifies that the length specified in the input matches the length of the RSA key token, and that the length contained in the token is consistent with the lengths of all of the parts of the token.

### Function Prototype

```
long VerifyKeyTokenConsistency( RsaKeyTokenHeader *pToken,  
                                USHORT tokenLengthIn )
```

### Input

On entry to this routine:

*pToken* is a pointer to the key token.

*tokenLengthIn* is the length of the token specified by *pToken*.

### Output

On successful exit from this routine:

VerifyKeyTokenConsistency returns OK if the key token was consistent, and FALSE otherwise.

### Return Codes

This function has no return codes.

## verify\_dSig - Verify RSA Key Token Signature

verify\_dSig receives an RSA key token in operational form, a buffer of data (with the length of the data), a digital signature and the length of the digital signature (in bytes), as well as the format of the digital signature. The data is hashed with SHA-1 and formatted according to the Type variable before being compared with the encrypted signature. The return code indicates whether the signature was verified.

### Function Prototype

```
long verify_dSig ( RsaKeyTokenHeader *pTokenIn,
                  UCHAR              *pDataIn,
                  long               DataLength,
                  UCHAR              *pDigitalSignature,
                  USHORT             SignatureLength,
                  UCHAR              Type)
```

### Input

On entry to this routine:

pTokenIn is a pointer to the operational key token.

pDataIn is a pointer to the data which is to be hashed and compared with the encrypted signature.

DataLenth is the length of the data to be signed, in bytes.

pSignatureOut is a pointer to a buffer which contains the signature to be verified.

SignatureLength is the length of the buffer pSignatureOut, in bytes.

Type is one of the following:

- M\_IS09796 if the data is to be formatted according to the ISO-9796 standard before signing.
- M\_PKCS10 if the data is to be formatted as specified in the RSADDataSecurity, Inc., *Public Key Cryptography Standards #1* block type 00 before signing.
- M\_PKCS11 if the data is to be formatted as specified in the RSADDataSecurity, Inc., *Public Key Cryptography Standards #1* block type 01 before signing.
- M\_ZEROPAD if the Data is to be placed in the low-order bits of a bit-string of the same length as the modulus with all other bit-positions set to zero before signing.

### Return Codes

Common return Codes generated by this routine are:

|                          |  |
|--------------------------|--|
| <b>OK</b>                | The operation was successful.                                      |
| <b>DSIG_NOT_VERIFIED</b> | The digital signature was not verified.                            |
| <b>E_SIZE</b>            | The provided buffer was not large enough to contain the signature. |
| <b>PKABadAddr</b>        | The key token is not valid.  |

---

## Chapter 10. CCA SRDI Manager Functions

This section describes the CCA SRDI Manager, which manages the storage and retrieval of persistent data in the coprocessor.

**Note:** All functions within this chapter are available only on the coprocessor.

### Header Files for SRDI Manager Functions

When using these functions, your program must include the following header files.

```
#include "cmncrypt.h"           /* Cryptographic definitions */
#include "cam_xtrn.h"           /* SRDI manager definitions  */
```

### Overview

The security relevant data item (SRDI)<sup>1</sup> Manager is the single interface through which all CCA-related functions access security related data. Only the SRDI Manager interacts with the physical medium on which the SRDI data is stored. The CCA verbs and any other CCA code read and write SRDI information only through the SRDI Manager interface. In turn, the SRDI Manager accesses the physical SRDI storage through the CP/Q++ PPD Manager, which controls the flash EPROM and BBRAM memories. This relationship is shown in Figure 10-1 on page 10-2.

---

<sup>1</sup> SRDI's are the sensitive data elements owned by the cryptographic application, and requiring protection. Examples include cryptographic keys and access control profiles.

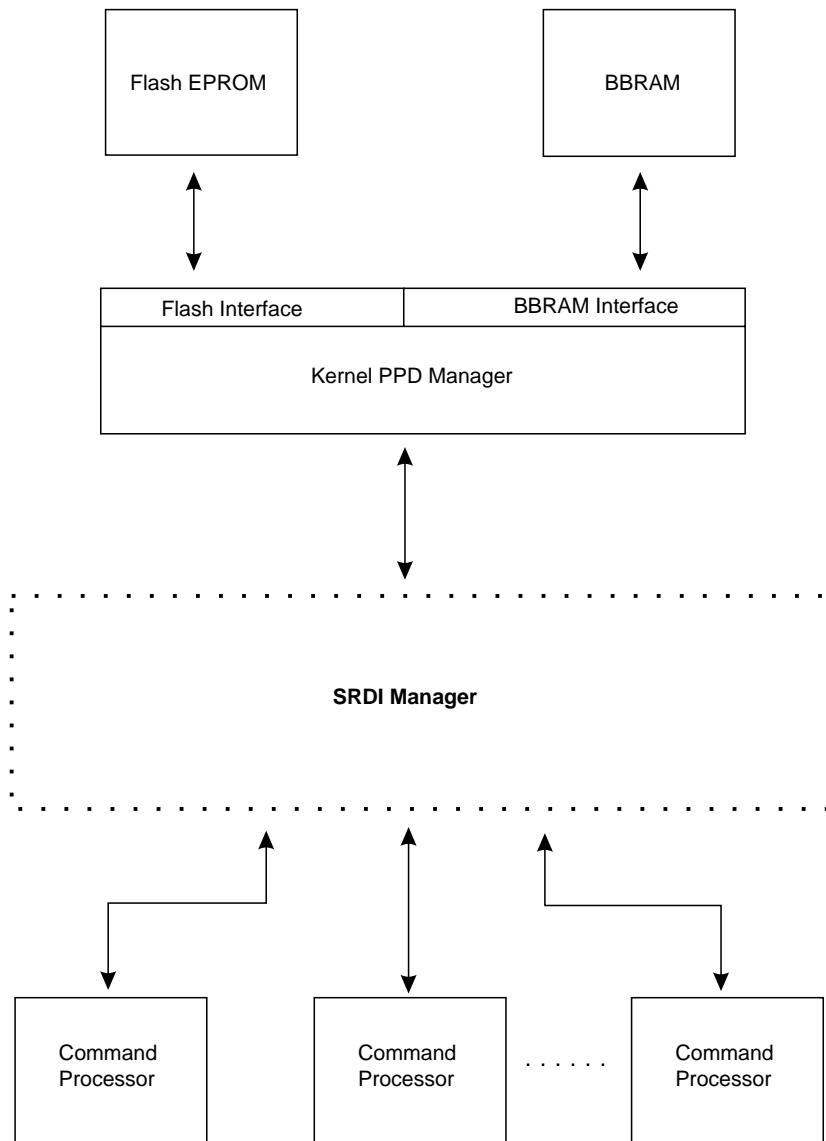


Figure 10-1. Master SRDI Manager Overview

Encapsulation of the SRDI physical storage mechanism makes it possible to change that mechanism without any effect on the CCA application code.

Each SRDI is identified by a name, much like a file name. The SRDI name is an eight character ASCII string, with no null terminator. Names that are less than eight characters should be left-justified, and padded on the right with ASCII spaces.



## CCA SRDI Manager Operation

The CP/Q++ PPD Manager can store SRDI data in either of two physical memory types.

**Flash EPROM** The flash memory is very large, but very slow to write. In addition, it has a limited lifetime in terms of write cycles; after 100,000 writes to any single memory cell, that cell may fail.

The flash memory can only be written in segments of 64K bytes. Thus, when any SRDI is written to flash, the CP/Q++ PPD Manager will usually have to rewrite a large amount of data that is not associated with that particular SRDI, but happens to lie in the same 64K byte page. This means that the 100,000 cycle lifetime may be reached much more quickly than expected, if a calculation is made based only on the number of times a specific SRDI is stored.

These characteristics make flash the appropriate location for SRDI data that is large, and infrequently changed. Examples include access control profiles, and stable cryptographic keys.

**BBRAM** BBRAM is small, but fast, and it has no limitations on the number of times it can be written. This makes it the appropriate choice for SRDI data that is small, and frequently updated. Examples include session keys, sequence counters, and state information.

The interface functions provide a parameter to select whether an SRDI is created in flash or BBRAM.

CCA applications do not have direct access to the SRDI information in the persistent memories.<sup>2</sup> When an SRDI is opened, the SRDI Manager creates a cleartext copy in RAM, in the CCA application address space. The caller receives a pointer to this location in RAM, and uses that space for all read and write references to the SRDI.

Only one working copy of an SRDI exists in RAM at any time, regardless of how many different callers open that same SRDI. The SRDI Manager maintains an open count for each open SRDI, indicating how many callers are using it. This count is initialized to one when the first caller opens the SRDI, and incremented for each additional open request on the same SRDI. When a caller closes the SRDI, the count is decremented. If the count reaches zero, indicating that no callers are using the SRDI, the working copy is deleted from memory.

When the caller asks to store the SRDI data, the SRDI Manager copies it to the persistent memory. Since there is only one physical working copy of the data at any one time, each caller's changes are made to the same SRDI data area, and all are saved when any of the callers requests that the SRDI be stored.

---

<sup>2</sup> Persistent memories are those that preserve their contents even when power is turned off. In the coprocessor, the flash EPROM and the BBRAM are persistent. The main system RAM used for executing programs and their data is *not* persistent.

## An Example: Opening an SRDI

Figures 10-2, 10-3, and 10-4 describe the steps when an SRDI is opened. The following text explains the sequence of events, using reference numbers that match those on the figures.

| Step | Description  |
|------|--|
| 1.   | A CCA command processor sends a request to the CCA SRDI Manager, asking for access to an SRDI named <i>ABC</i> , which resides in flash EPROM.<br><br>At this time, SRDI <i>ABC</i> is not open. No copy of the SRDI data exists in the CCA application RAM address space. |
| 2.   | The CCA Manager sends a request to the Kernel PPD Manager, asking for the length of SRDI <i>ABC</i> . It needs to know the length, so it can allocate the required buffer in RAM.  |
| 3.   | The Kernel PPD Manager returns the length of SRDI <i>ABC</i> .   |
| 4.   | The CCA SRDI Manager allocates a buffer to hold <i>ABC</i> . This buffer is in RAM addressable by the CCA application.   |

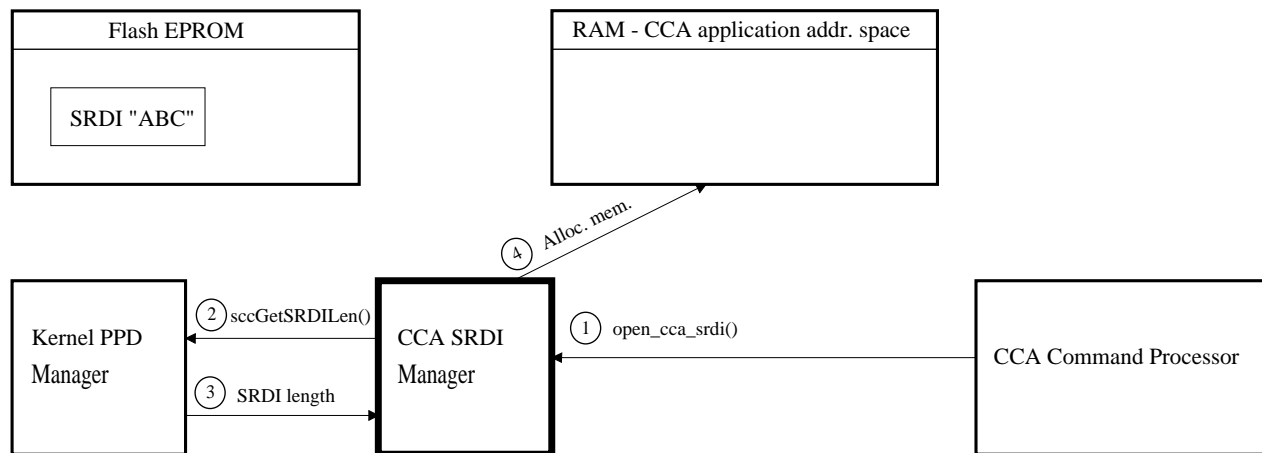


Figure 10-2. Master SRDI Read Illustration, Part 1

| Step | Description   |
|------|---|
| 5.   | The CCA SRDI Manager sends a request to the Kernel PPD Manager, asking it to read <i>ABC</i> into the buffer allocated in step 4 above. |
| 6.   | The SRDI is read from flash EPROM, decrypted, and deposited in the specified buffer.  |

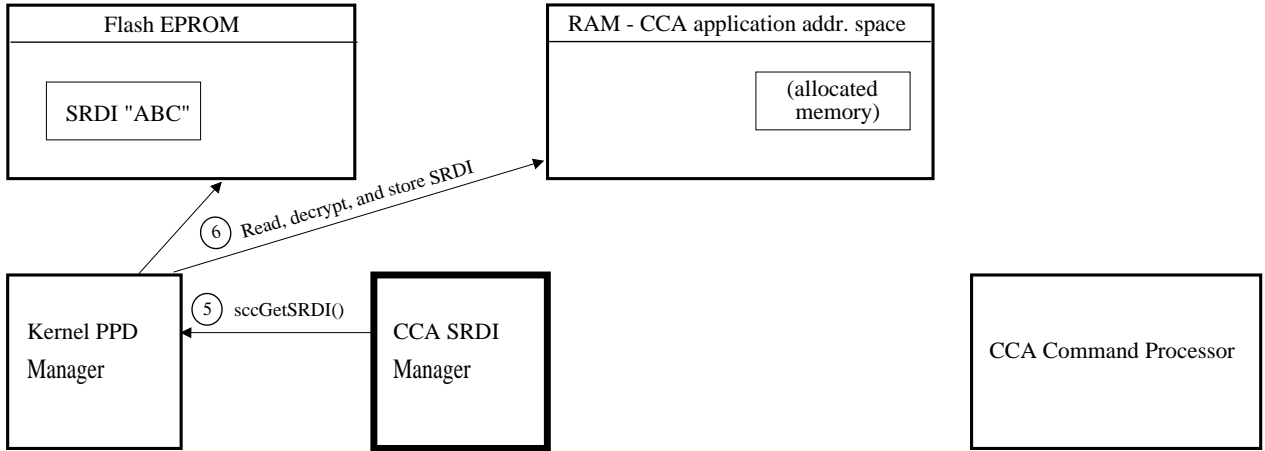


Figure 10-3. Master SRDI Read Illustration, Part 2

| Step | Description  |
|------|--|
| 7.   | The CCA SRDI Manager returns the buffer address to the CCA command processor. The command processor then uses the RAM copy of the SRDI whenever it needs to read or alter <i>ABC</i> . |

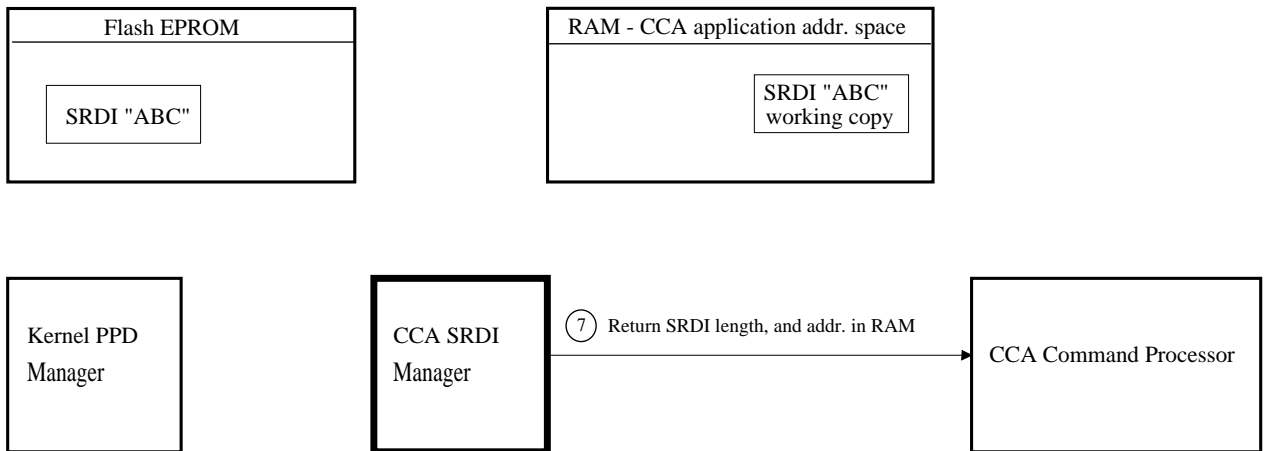


Figure 10-4. Master SRDI Read Illustration, Part 3

## Controlling Concurrent Access to an SRDI

Since the CCA application is multi-threaded, different callers may access an SRDI at the same time. If one caller is altering data in the SRDI while a different caller is either reading or writing that same data, corruption results.

Serialization semaphores are used to prevent this from occurring. Each time the SRDI Manager retrieves an SRDI from flash EPROM or BBRAM, it allocates a semaphore for that SRDI. The SVid which identifies this semaphore is passed back to the caller whenever an SRDI is opened.

Every SRDI user in the CCA application is *required* to gain ownership of the semaphore before either reading or writing to the SRDI. This guarantees that no other caller is simultaneously accessing that same SRDI. As soon as the SRDI is no longer needed, the semaphore is released so that others can use the SRDI.

The semaphore is controlled by use of the CP/Q system calls *CPSemClaim* and *CPSemRelease*. The CCA application should never, under any circumstances, destroy the semaphore; this is done by the SRDI Manager when the last user closes the SRDI.

## Summary of Functions

These functions are used by the CCA command processor to read and write SRDI data.

|                               |   |
|-------------------------------|---|
| <b>close_cca_srди</b>         | Closes the open copy of an SRDI.                        |
| <b>create_cca_srди</b>        | Creates an SRDI.  |
| <b>create4update_cca_srди</b> | Creates an SRDI in BBRAM.                               |
| <b>delete_cca_srди</b>        | Deletes an SRDI from memory.                            |
| <b>get_cca_srди_length</b>    | Obtains the length of an SRDI, in bytes.                |
| <b>open_cca_srди</b>          | Opens and gains access to an SRDI.                      |
| <b>resize_cca_srди</b>        | Increases or decreases the length of an SRDI, in bytes. |
| <b>save_cca_srди</b>          | Stores SRDI data.                                       |
| <b>update_cca_srди</b>        | Updates an SRDI with the provided data.                 |

## close\_cca\_srди - Close CCA SRDI

close\_cca\_srди deactivates the open copy of the SRDI, which is managed by the SRDI Manager. If no other applications are using the SRDI, the RAM which held the working copy of the SRDI is released.

**Note:** If the working copy of the SRDI has been changed, the application must issue the *save\_cca\_srди()* function in order to have the SRDI saved. SRDI data is not automatically saved when the SRDI is closed.

### Function Prototype

```
long close_cca_srди(char *srди_name);
```

### Input

On entry to this routine

srди\_name is a pointer to an eight character ASCII string containing the name of the desired SRDI. This string does not contain a null terminator.

### Output

This function returns no output. On successful exit from this routine:

close\_cca\_srди deactivates the open copy of the SRDI.

### Return Codes

Common return codes generated by this routine are:

|                           |   |
|---------------------------|---|
| <b>srди_NO_ERROR</b>      | The operation was successful.                                       |
| <b>srди_GENERAL_ERROR</b> | Can not access the SRDI Manager, the operation cannot be completed. |
| <b>srди_NOT_OPEN</b>      | The SRDI item is not in the open state.                             |

## create\_cca\_srdi - Create CCA SRDI

create\_cca\_srdi creates an SRDI in flash EPROM or BBRAM using the specified name.

### Function Prototype

```
long create_cca_srdi(char *srdi_name, ULONG srdi_options,
                    char *srdi_addr, ULONG srdi_length);
```

### Input

On entry to this routine:

srdi\_name is a pointer to an eight character ASCII string containing the name of the desired SRDI. This string does not contain a null terminator, and should be padded on the right with blanks.

srdi\_options holds bit-significant options which are passed on to the CP/Q++ PPD Manager's *sccSaveSRDI()* function. There are two fields in the options value:

1. A value that indicates whether the SRDI data should be stored in flash EPROM, or in BBRAM. Flash is large, but slow to access, and each cell has a limited number of possible write cycles before it fails. BBRAM is fast and has unlimited write cycles, but it is much smaller than the flash.
2. A value which indicates how the SRDI data should be encrypted, if it is to be stored in flash EPROM.<sup>3</sup> There are three options.
  - a. Do not encrypt the data at all.
  - b. Single-encrypt with DES.
  - c. Triple-encrypt with DES.

The options are defined with constants in header file *scc\_int.h*. The values defined there are as follows.

| Symbol     | Value | Description  |
|------------|-------|--|
| PPD_BBRAM  | X'01' | Store in BBRAM   |
| PPD_SINGLE | X'10' | Store in flash, encrypted using a single-length DES key. |
| PPD_TRIPLE | X'30' | Store in flash, encrypted using DES triple encryption.   |
| PPD_NONE   | X'00' | Store in flash, unencrypted.                             |

srdi\_addr is a pointer to the address of the SRDI data. This data is written to the newly created SRDI.

srdi\_length is the length of the SRDI data, in bytes.

<sup>3</sup> Data is only encrypted when stored in the flash EPROM; it is never encrypted in BBRAM. The BBRAM contents are destroyed on intrusion, so there is no need to protect the data there by way of encryption.

**Output**

This function returns no output. On successful exit from this routine:

create\_cca\_srди creates an SRDI in flash EPROM or BBRAM using the specified name.

**Return Codes**

Common return codes generated by this routine are:

|                           |   |
|---------------------------|---|
| <b>srdi_NO_ERROR</b>      | The operation was successful.                                       |
| <b>srdi_GENERAL_ERROR</b> | Can not access the SRDI Manager, the operation cannot be completed. |
| <b>srdi_EXISTS</b>        | The SRDI item already exists.                                       |



## create4update\_cca\_srdi - Create CCA SRDI for Update Only

create4update\_cca\_srdi creates an SRDI in BBRAM. The SRDI may not be resized after creation. The SRDI is stored in unencrypted form.

### Function Prototype

```
long create4update_cca_srdi(char *pSrdiName,  
                           char *pSrdiAddr,  
                           ULONG SrdiLength);
```

### Input

On entry to this routine:

pSrdiName is a pointer to an eight character ASCII string containing the name of the desired SRDI. This string does not contain a null terminator, and should be padded on the right with blanks.

pSrdiAddr is a pointer to the data which should be written to the SRDI.

SrdiLength contains the length of the data pointed to by pSrdiAddr, and the permanent length of this SRDI.

### Output

This function returns no output. On successful exit from this routine, the data has been stored in BBRAM under the requested name.

### Return Codes

Common return codes generated by this routine are:

|                           |   |
|---------------------------|---|
| <b>srdi_NO_ERROR</b>      | The operation was successful.                   |
| <b>srdi_EXISTS</b>        | The SRDI item already exists.                   |
| <b>srdi_GENERAL_ERROR</b> | The SRDI Manager was unable to create the SRDI. |

## delete\_cca\_srди - Delete CCA SRDI

delete\_cca\_srди deletes an SRDI from the persistent memory area where it is stored (either flash EPROM or BBRAM). This is equivalent to erasing a file from a hard disk.

### Function Prototype

```
long delete_cca_srди(char *srди_name);
```

### Input

On entry to this routine:

srди\_name is a pointer to an eight character ASCII string containing the name of the desired SRDI. This string does not contain a null terminator, and should be padded on the right with blanks.

### Output

This function returns no output. On successful exit from this routine:

delete\_cca\_srди deletes an SRDI from the persistent memory area where it is stored.

### Return Codes

Common return codes generated by this routine are:

|                           |   |
|---------------------------|---|
| <b>srди_NO_ERROR</b>      | The operation was successful.                                       |
| <b>srди_GENERAL_ERROR</b> | Can not access the SRDI Manager, the operation cannot be completed. |
| <b>srди_NOT_FOUND</b>     | SRDI item does not exist.   |
| <b>srди_OPEN</b>          | The SRDI item is not in the closed state.                           |

**Note:** An SRDI cannot be deleted if it is in the “open” state, since another application may be using it.

## get\_cca\_srdi\_length - Get CCA SRDI Length

get\_cca\_srdi\_length obtains the length of the specified SRDI, in bytes.

### Function Prototype

```
long get_cca_srdi_length(char *srdi_name, ULONG *srdi_length);
```

### Input

On entry to this routine:

srdi\_name is a pointer to an eight character ASCII string containing the name of the desired SRDI. This string does not contain a null terminator.

srdi\_length is a pointer to the ULONG variable.

### Output

On successful exit from this routine:

srdi\_length contains the length of the SRDI data, in bytes.

### Return Codes

Common return codes generated by this routine are:

|                           |   |
|---------------------------|---|
| <b>srdi_NO_ERROR</b>      | The operation was successful.                                       |
| <b>srdi_GENERAL_ERROR</b> | Can not access the SRDI Manager, the operation cannot be completed. |
| <b>srdi_READ_ERROR</b>    | Unable to read the SRDI item from BBRAM or flash.                   |

## open\_cca\_srdi - Open CCA SRDI

open\_cca\_srdi opens an SRDI, gaining access to its contents. The function returns the address and length of the SRDI data, where the address points to a cleartext working copy of the actual SRDI, which is stored in flash EPROM or BBRAM.

If multiple callers open the same SRDI, they all have access to the same shared copy in RAM. Any modifications to the SRDI are visible immediately to all functions that open that SRDI.

In addition to the SRDI address and length, the function returns a semaphore ID for the selected SRDI. This semaphore is used to gain exclusive access to the SRDI, to prevent errors when one thread is writing data, while another is simultaneously either reading or writing that same data. See "Controlling Concurrent Access to an SRDI" on page 10-6 for further details.

### Function Prototype

```
long open_cca_srdi(char *srdi_name, char **srdi_addr, ULONG *srdi_length
                  ULONG *semSVid);
```

### Input

On entry to this routine:

srdi\_name is a pointer to an eight character ASCII string containing the name of the desired SRDI. This string does not contain a null terminator.

### Output

On successful exit from this routine:

srdi\_addr is a pointer to a pointer variable, in which the SRDI Manager returns the address of the SRDI. This is an address in RAM, where the SRDI Manager places a copy of the SRDI data.

srdi\_length is a pointer to a location where the SRDI Manager stores the length of the SRDI data, in bytes.

semSVid is the SVid for the semaphore assigned to the specified SRDI.

### Return Codes

Common return codes generated by this routine are:

|                           |   |
|---------------------------|---|
| <b>srdi_NO_ERROR</b>      | The operation was successful.                                       |
| <b>srdi_NOT_FOUND</b>     | The SRDI item could not be found.                                   |
| <b>srdi_READ_ERROR</b>    | Unable to read the SRDI item from BBRAM or flash.                   |
| <b>srdi_ALLOC_ERROR</b>   | Unable to allocate memory for the SRDI item.                        |
| <b>srdi_GENERAL_ERROR</b> | Could not access the SRDI Manager, the operation was not completed. |

## resize\_cca\_srdi - Resize CCA SRDI

resize\_cca\_srdi increases or decreases the length of the specified CCA SRDI, in bytes.

An SRDI can only be resized if you are the only requestor who has it open. If the SRDI is opened by more than one user concurrently, it cannot be resized; the address of the RAM copy changes when it is resized, and there is no way to notify other callers of this.

### Function Prototype

```
long resize_cca_srdi(char *srdi_name, ULONG srdi_length,  
                    char **new_srdi_addr);
```

### Input

On entry to this routine:

srdi\_name is a pointer to an eight character ASCII string containing the name of the desired SRDI. This string does not contain a null terminator.

srdi\_length is the new length for the SRDI, in bytes.

### Output

On successful exit from this routine:

new\_srdi\_addr is a pointer to a location where the function returns the address of the resized SRDI. After resizing, the SRDI buffer is relocated from its previous address.

### Return Codes

Common return codes generated by this routine are:

|                           |   |
|---------------------------|---|
| <b>srdi_NO_ERROR</b>      | The operation was successful.                                       |
| <b>srdi_NOT_FOUND</b>     | The SRDI item could not be found.                                   |
| <b>srdi_READ_ERROR</b>    | Unable to read the SRDI item from BBRAM or flash.                   |
| <b>srdi_ALLOC_ERROR</b>   | Unable to allocate memory for the SRDI item.                        |
| <b>srdi_GENERAL_ERROR</b> | Could not access the SRDI Manager, the operation was not completed. |

## save\_cca\_srди - Save CCA SRDI

save\_cca\_srди stores the SRDI data on a persistent storage medium (flash or BBRAM) using the encryption method specified when the SRDI was created.

This function ensures that no thread is updating the SRDI while it is being stored by gaining exclusive access rights using the SRDI semaphore. See “Controlling Concurrent Access to an SRDI” on page 10-6 for details on this semaphore.

### Function Prototype

```
long save_cca_srди(char *srди_name);
```

### Input

On entry to this routine:

srди\_name is a pointer to an eight character ASCII string containing the name of the desired SRDI. This string does not contain a null terminator.

**Note:** No two SRDI's can have the same name, even if one resides in flash EPROM and the other resides in BBRAM. The CP/Q++ PPD Manager enforces this restriction.

### Output

This function returns no output. On successful exit from this routine:

save\_cca\_srди stores the SRDI data on a persistent storage medium.

### Return Codes

Common return codes generated by this routine are:

|                           |   |
|---------------------------|---|
| <b>srди_NO_ERROR</b>      | The operation was successful.                                       |
| <b>srди_NOT_OPEN</b>      | The SRDI item is not in the open state.                             |
| <b>srди_WRITE_ERROR</b>   | Unable to write to flash or BBRAM.                                  |
| <b>srди_GENERAL_ERROR</b> | Could not access the SRDI Manager, the operation was not completed. |

## update\_cca\_srди - Update an SRDI Item

update\_cca\_srди updates an SRDI with provided data.

### Function Prototype

```
long update_cca_srди(char *pSrдиName,  
                    char *pDatabuffer,  
                    unsigned long Datalength,  
                    unsigned long Dataoffset);
```

### Input

On entry to this routine:

pSrдиName is a pointer to an eight character string containing the name of the SRDI to be changed. This string does not contain a null terminator and should be padded on the right with blanks. This SRDI must have been opened using the open\_cca\_srди call.

pDatabuffer is a pointer to a buffer containing the data with which to update the SRDI.

Datalength contains the length of the data to be changed, in bytes.

Dataoffset contains the offset of the first byte of data to change from pDatabuffer.

### Output

This function returns no output. On successful exit from this routine, the SRDI item has been changed.

### Return Codes

Common return codes generated by this routine are:

|                         |                                       |
|-------------------------|---------------------------------------|
| <b>srdi_NO_ERROR</b>    | The operation was successful.         |
| <b>srdi_WRITE_ERROR</b> | The operation could not be completed. |

## Example Code

The following C-language code shows a general structure for the way a CCA application would open, use, and close an SRDI.

```

1  #define QSVCGOOD 0          /* CP/Q semaphore fcn. error code */
2  #define TIMEOUT_FOREVER 0xFFFFFFFF /* Parameter for CPSemClaim */
3  #define MY_SRDI_NAME "MY_SRDI " /* Name of SRDI we're using */
4
5  USHORT srdi_rc;           /* SRDI fcn. return code */
6  char * my_srdi_addr;     /* Pointer to clear SRDI data in RAM*/
7  ULONG my_srdi_length;    /* Length of SRDI data, in bytes */
8  ULONG semaphore_id;      /* SVID of SRDI access semaphore */
9
10 void srdi_stuff(void)
11 {
12     /* Open the SRDI */
13
14     srdi_rc = open_cca_srdi(MY_SRDI_NAME, &my_srdi_addr, &my_srdi_length,
15                             &semaphore_id);
16
17     if (srdi_NO_ERROR == srdi_rc) /* If no errors opening SRDI...*/
18     {
19         /* do other stuff as needed... */
20
21         /* Gain exclusive access rights to the SRDI */
22
23         if (QSVCGOOD == CPSemClaim(semaphore_id, TIMEOUT_FOREVER))
24         {
25             /* This is where the code will read and/or write to the SRDI data,
26              in the area pointed to by my_srdi_addr. */
27
28             /* Release semaphore, allowing others to access the SRDI */
29
30
31             if (QSVCGOOD == CPSemRelease(semaphore_id))
32             {
33                 /* do other stuff as needed... */
34             }
35             else
36             {
37                 /* handle semaphore release error... */
38             }
39         }
40     }
41
42     else
43     {
44         /* handle semaphore claim error... */
45     }
46
47     /* Close the SRDI */
48
49     srdi_rc = close_cca_srdi(MY_SRDI_NAME);
50
51     if (srdi_NO_ERROR != srdi_rc)
52     {
53         /* handle SRDI close error... */
54     }
55 }
56
57
58
59
60 else
61 {
62     /* handle SRDI open error... */
63 }
64

```



---

## Chapter 11. Access Control Manager Functions

The functions described in this chapter enable a UDX to initialize or update access control tables, log users on or off of the coprocessor, or check a user's authority to perform a specified function.

**Note:** All functions within this chapter are available only on the coprocessor.

### Header Files for Access Control Manager Functions

When using these functions, your program must include the following header files.

```
#include "camxtrn.h"           /* CCA managers          */
#include "camacm.h"           /* Access Control Manager routines */
#include "camacm_p.h"         /* Access Control Manager routines */
```

### Summary of Functions

Access Control Manager includes the following functions.

|                               |   |
|-------------------------------|---|
| <b>ac_check_authorization</b> | Check whether a user is authorized to execute a specified function.                   |
| <b>ac_chg_prof_auth_data</b>  | Change the authentication data for a user profile.                                    |
| <b>ac_chg_prof_exp_date</b>   | Change the expiration date of a user profile.   |
| <b>ac_del_profile</b>         | Delete a user profile.  |
| <b>ac_del_role</b>            | Delete a role definition.   |
| <b>ac_get_list_sizes</b>      | Find out how many roles and how many profiles exist on the coprocessor.               |
| <b>ac_get_profile</b>         | Read the contents of a specified user profile.  |
| <b>ac_get_role</b>            | Read the contents of a specified role.  |
| <b>ac_init</b>                | Initialize the access control system, including setup of role and profile tables.     |
| <b>ac_list_profiles</b>       | Get a list of all the user IDs for which there are profiles.                          |
| <b>ac_list_roles</b>          | Get a list of all the role IDs.   |
| <b>ac_load_profiles</b>       | Load one or more user profiles.   |
| <b>ac_load_roles</b>          | Load one or more role definitions.  |
| <b>ac_lu_add_user</b>         | Add a user to the table of logged-on users, and generate a session key for that user. |
| <b>ac_lu_drop_user</b>        | Drop a user from the table of logged-on users.  |
| <b>ac_lu_get_ks</b>           | Get a copy of a specified user's session key.   |
| <b>ac_lu_get_num_users</b>    | Find out how many users are currently logged on.                                      |
| <b>ac_lu_get_role</b>         | Get the role ID for a specified logged-on user.                                       |
| <b>ac_lu_ks_dec</b>           | Decrypt data with a specified user's session key.                                     |

|                                |   |
|--------------------------------|---|
| <b>ac_lu_ks_enc</b>            | Encrypt data with a specified user's session key.                                 |
| <b>ac_lu_ks_hmacgen</b>        | Computes a HMAC on a message using the session key.                               |
| <b>ac_lu_ks_hmacver</b>        | Verifies an HMAC using the session key.   |
| <b>ac_lu_ks_macgen</b>         | Compute a MAC (message authentication code) using a specified user's session key. |
| <b>ac_lu_ks_macver</b>         | Verify a MAC (message authentication code) using a specified user's session key.  |
| <b>ac_lu_list_users</b>        | Get a list of all the logged-on users.  |
| <b>ac_lu_query_user</b>        | Check whether a specified user is currently logged on (authenticated).            |
| <b>ac_query_profile</b>        | Verify that a specified profile exists on the coprocessor, and return its length. |
| <b>ac_query_role</b>           | Verify that a specified role exists on the coprocessor.                           |
| <b>ac_reinit</b>               | Reinitialize the access control system, to the default state.                     |
| <b>ac_reset_logon_fail_cnt</b> | Reset the logon failure count in a user profile.                                  |
| <b>acm_xlt_errorcode</b>       | Translates an ACM error code to an SAPI error code.                               |

## SRDI Files

The Access Control Manager uses two SRDI files, stored in flash EPROM.

- *Profiles* - holds all the user profiles that are enrolled on the coprocessor.
- *Roles* - holds all the roles that have been defined on the coprocessor.

Each of these SRDIs has a similar format. The file begins with a 4-byte header, in which the first two bytes contain an integer specifying how many items are in the file, and the second two bytes are reserved and set to X'0000'. The number of items reflects either the number of profiles or the number of roles, depending on the SRDI in question.

The profiles or roles follow the header. The first one is concatenated to the end of the header, and each successive role or profile is concatenated to its predecessor. Neither roles nor profiles are ordered in any meaningful way.

For quicker access, the Access Control Manager builds indexes in RAM for the roles and the profiles. For each role or profile in the SRDIs, the respective index table holds the name of the role or profile and its offset from the start of the SRDI.

## Data Structures

This section contains definitions for common data structures used in the Access Control Manager.

## Generic Data Types

The following types are used in various other definitions.

```
typedef unsigned char two_byte[2];    // "Big-endian" 2-byte integer
```

It is assumed that all of the “standard” types are available, such as UCHAR, UINT, USHORT, and boolean.

## Profile Structures

The Profile ID is an eight character unterminated string, as follows.

```
typedef UCHAR profile_id_t[8];       // Profile ID
```

The activation and expiration dates use the following format.

```
typedef struct {
    two_byte year;
    UCHAR month;
    UCHAR day;
} prof_date_t;
```

The profile consists of a fixed structure, with the authentication data concatenated to the end. The fixed portion is defined with the structure below.

```
typedef struct {
    two_byte profile_vers;           // Profile structure version
    two_byte profile_lth;           // Length of entire profile
    char comment[20];               // Descriptive comment
    two_byte cksum;                 // Checksum for integrity
    UCHAR failure_cnt;              // Logon failure count
    UCHAR reserved_1;               // Reserved field
    profile_id_t user_id;            // User ID
    role_id_t role_id;              // Role ID
    prof_date_t act_date;            // Activation date
    prof_date_t exp_date;           // Expiration date
    // The variable-length authentication data appears here
} user_profile_t;
```

## Role Structures

The Role ID is an eight character unterminated string, as follows.

```
typedef UCHAR role_id_t[8];         // Role ID
```

The role definition consists of a fixed structure, with the list of permitted access control points appended at the end. The fixed part of the structure is defined by the following type declaration.

```

typedef struct {
    two_byte role_vers;           // Role structure version
    two_byte role_lth;           // Length of role structure
    char comment[20];            // Descriptive comment
    two_byte cksum;              // Checksum for integrity
    two_byte reserved_1;         // Reserved field
    role_id_t role_id;           // Role ID
    two_byte reqd_auth_str;      // Required authentication strength
    role_time_t upper_time_limit; // Upper time limit for access
    dow_t valid_dow;             // Valid days of the week for access
    UCHAR reserved_2;           // Reserved field
    // Permitted operations definition (access control points) attached here
    role_time_t lower_time_limit; // Lower time limit for access
} role_t

```

### User Information Structures

The Access Control Manager holds the following data for each user logged on to the coprocessor.

- The profile ID (user ID)
- The role ID for that user
- The session key  $K_S$  for the user

The structures defining this data are as follows.

```

typedef UCHAR des_key[8];           // DES key

typedef user_session_key_t des_key[3]; // Triple-length DES session key

typedef struct {
    profile_id_t userid;           // User ID
    role_id_t role_id;            // User's role
    dl_des_key ks;                // User's session key
} user_info_t;

#define INITIAL_USER_TBL_SIZE 20    // Initial number of spaces
in table

// There will be a static pointer to an array of user_info_t elements. If the
// array fills, a new and larger array will be allocated and assigned to the
// pointer, and the contents of the old array copied over.

```

## ac\_check\_authorization - Check Authorization to Execute Function

ac\_check\_authorization determines if a user is permitted to execute a specified function, based on the user's role, access control state information, and other access control parameters.

### Function Prototype

```
long ac_check_authorization(role_id_t role, USHORT requested_fcn,  
                           boolean *granted);
```

### Input

role\_id\_t is a pointer to the role SRDI.

role is the role under which the user is operating.

requested\_fcn is an index into the *Access Control Points* table, indicating which function the user wants to execute.

granted is a pointer to a variable that will receive the response, indicating whether the user is allowed to execute the desired function.

### Output

On successful exit from this routine:

ac\_check\_authorization returns a boolean value of TRUE indicating the user is allowed to use the specified function in the CCA application, and FALSE if not.

### Return Codes

Common return codes generated by this routine are:

|                           |                                   |
|---------------------------|-----------------------------------|
| <b>acm_NO_ERROR</b>       | The operation was successful.     |
| <b>acm_ROLE_NOT_FOUND</b> | The specified role was not found. |

## ac\_chg\_prof\_auth\_data - Change Profile Authentication Data

ac\_chg\_prof\_auth\_data replaces the authentication data in a user profile, for a specific authentication mechanism. The old data is replaced with the new data, but only if the *Replacable* flag is set in the attributes of the old authentication data.

Alternatively, if no data exists in the profile for the specified mechanism, the data is appended to the authentication data already present in that profile.

### Function Prototype

```
long ac_chg_prof_auth_data(profile_id_t profile_id, void *auth_data);
```

### Input

profile\_id is the 8-byte, non-NULL terminated ID of the profile whose authentication data is to be changed.

auth\_data is a pointer to a buffer containing the new authentication data, in the following format:

- a variable of type profs\_authen\_mech\_t which contains:
  - numbytes - the number of bytes of data in the buffer.
  - mech\_Id - an identifier which describes the authentication mechanism - for passphrase authentication, the mechanism ID is X'01'
  - mech\_strength - an integer which defines the strength of this authentication method. X'00' is reserved for users who have not been authenticated.
  - exp\_date - a prof\_date\_t variable containing the expiration date for this authentication data. The format is:
    - year is a 2-byte integer in big-endian order
    - month is a one-byte integer (1-12)
    - date is a one-byte integer (1-31)
  - mech\_attr - a bit-flag to represent any attributes needed to describe the operation and use of this authentication mechanism. The only currently defined value is RENEWABLE, in the most significant bit. The presence of this flag indicates that an authentication method may be updated by the user (for example, a passphrase change).
- concatenated to the profs\_authen\_mech\_t variable, a variable length field containing the authentication data for this user and method. For passphrases, this field contains the 20-byte SHA-1 hash of the user's passphrase. This hash is computed in the host.

### Output

This function returns no output. On successful exit from this routine:

The profile specified in profile\_id has been updated in one of the following two ways:

1. If the profile previously had an authentication with the same mechanism ID, its authentication method has been changed.
2. If the profile previously had NO authentication with an identical mechanism ID, the authentication data has been ADDED to the profile.

The PROFILES SRDI has been saved to flash EPROM.

**Return Codes**

Common return codes generated by this routine are:

|                                 |  |
|---------------------------------|--|
| <b>acm_NO_ERROR</b>             | The operation was successful.                          |
| <b>acm_INVALID_AUTHENT_DATA</b> | The authentication data was invalid.                   |
| <b>acm_PROFILE_NOT_FOUND</b>    | The specified profile was not in the profile list.     |
| <b>acm_NON_REPLACABLE_DATA</b>  | The REPLACABLE flag was not set in the user's profile. |
| <b>acm_MEM_ALLOC_ERROR</b>      | There was insufficient memory to store the new data.   |

## ac\_chg\_prof\_exp\_date - Change Profile Expiration Date

ac\_chg\_prof\_exp\_date changes the expiration date in a specified user profile. This function is used to re-enable a user whose profile has expired, or to extend the lifetime of a profile that is about to expire.

### Function Prototype

```
long ac_chg_prof_exp_date(profile_id_t profile_id, prof_exp_date_t exp_date);
```

### Input

profile\_id is the ID of the profile whose expiration date should be changed.

exp\_date is the new expiration date, in the following format:

- year is a 2-byte integer in big-endian order
- month is a one-byte number representing the month (1-12)
- date is a one-byte number representing the date (1-31)

### Output

This function returns no output. On successful exit from this routine:

The expiration date of profile\_id has been changed to exp\_date, and the PROFILES SRDI has been saved to flash EPROM.

### Return Codes

Common return codes generated by this routine are:

- |                              |  |
|------------------------------|--|
| <b>acm_NO_ERROR</b>          | The operation was successful.                      |
| <b>acm_PROFILE_NOT_FOUND</b> | The specified profile was not in the profile list. |



## ac\_del\_profile - Delete User Profile

ac\_del\_profile deletes a user profile from the coprocessor. The specified profile is deleted from the table of enrolled profiles. In addition, if the specified user is logged on, they are logged off.

### Function Prototype

```
long ac_del_profile(profile_id_t profile_id);
```

### Input

profile\_id is the 8-byte, non-NULL terminated ID of the profile to be deleted.

### Output

This function returns no output. On successful exit from this routine:

The user specified by profile\_id has been logged off the system (if needed) and the profile has been removed from the profiles list. In addition, the PROFILES SRDI has been saved to flash memory.

### Return Codes

Common return codes generated by this routine are:

- |                              |  |
|------------------------------|--|
| <b>acm_NO_ERROR</b>          | The operation was successful.                      |
| <b>acm_PROFILE_NOT_FOUND</b> | The specified profile was not in the profile list. |

## ac\_del\_role - Delete Role

ac\_del\_role deletes a specified role definition from the coprocessor. In addition, if any logged on users have their authority defined by this role, those users are logged off.

If the request is to delete the DEFAULT role, the role is not actually deleted; the default role must always be present on the coprocessor. Instead, it is reset to the default values for that role.

### Function Prototype

```
long ac_del_role(role_id_t role_id);
```

### Input

role\_id is the 8-byte, non-NULL terminated ID of the role to be deleted.

### Output

This function returns no output. On successful exit from this routine:

The specified role has been deleted, unless the role specified was DEFAULT. If the specified role was DEFAULT, the Default role has been reset to its original contents. The list of roles has been saved to flash memory.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR**            The operation was successful.

**acm\_ROLE\_NOT\_FOUND**    The specified role was not found.

## ac\_get\_list\_sizes - Get Sizes of Role and Profile Lists

ac\_get\_list\_sizes is used to find out how much data will be returned by the ac\_list\_profiles and ac\_list\_roles functions. By calling this function first, the application can ensure it has a large enough buffer for the data it will receive.

### Function Prototype

```
long ac_get_list_sizes(ULONG *num_profiles, ULONG *num_roles);
```

### Input

num\_profiles is a pointer to a variable that will receive the number of profiles on the coprocessor.

num\_roles is a pointer to a variable that will receive the number of roles on the coprocessor.

### Output

On successful exit from this routine:

num\_profiles contains the number of profiles returned.

num\_roles contains the number of roles returned.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.

## ac\_get\_profile - Get Profile

ac\_get\_profile returns the information from a specified user profile. The data begins with the fixed profile contents, defined by data type user\_profile\_t. The user's authentication data is concatenated to the end of this structure.

### Function Prototype

```
long ac_get_profile(profile_id_t profile_id,  
                   ULONG *profile_size, void *profile_data);
```

### Input

profile\_id is an 8-byte character string non-NULL terminated containing the name of the profile to be returned.

profile\_size is a pointer to a variable which contains the size of the profile\_data buffer, in bytes.

profile\_data is a pointer to a buffer where the profile will be stored.

### Output

On successful exit from this routine:

profile\_size contains the actual size of the returned profile data.

profile\_data contains the profile data.

### Return Codes

Common return codes generated by this routine are:

|                              |   |
|------------------------------|---|
| <b>acm_NO_ERROR</b>          | The operation was successful.   |
| <b>acm_PROFILE_NOT_FOUND</b> | The specified profile was not in the profile list.  |
| <b>acm_BFR_TOO_SMALL</b>     | The buffer was not large enough to hold the profile data. The buffer size required is in the profile_size variable. |

## ac\_get\_role - Get Role

ac\_get\_role returns the information from a specified role.

### Function Prototype

```
long ac_get_role(role_id_t role_id, ULONG *role_size, void *role_data);
```

### Input

role\_id is an 8-byte character string non-NULL terminated containing the name of the role to be returned.

role\_size is a pointer to a variable which contains the size of the role\_data buffer, in bytes.

role\_data is a pointer to a buffer where the role data will be stored.

### Output

On successful exit from this routine:

role\_size contains the actual size of the returned role data.

role\_data contains the role data.

### Return Codes

Common return codes generated by this routine are:

- |                           |  |
|---------------------------|--|
| <b>acm_NO_ERROR</b>       | The operation was successful.  |
| <b>acm_ROLE_NOT_FOUND</b> | The specified role was not found.  |
| <b>acm_BFR_TOO_SMALL</b>  | The buffer was not large enough to hold the role data.<br>The buffer size required is in the role_size variable. |

## ac\_init - Initialize the Access Control Manager

ac\_init initializes the Access Control Manager including all data areas and state information. In addition, creates and initializes the role and profile SRDIs if they do not already exist, including creation of a DEFAULT role.

### Function Prototype

```
long ac_init(void);
```

### Input

This function has no input.

### Output

This function has no output. On successful exit from this routine:

ac\_init creates and initializes the Access Control Manager.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.

## ac\_list\_profiles - List User Profiles

ac\_list\_profiles returns a list of all the user IDs for the profiles enrolled on the coprocessor. This is a series of unordered 8-byte user IDs.

### Function Prototype

```
long ac_list_profiles(profile_id_t[] profile_list  
                     ULONG *num_profiles);
```

### Input

profile\_list is a pointer to an array of 8-byte elements to hold the user IDs.

num\_profiles is a pointer to the maximum number of 8-byte values which the array can hold.

### Output

On successful exit from this routine:

profile\_list contains the list of IDs (non-NULL terminated 8-byte strings).

num\_profiles contains the number of profile IDs which were returned.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR**           The operation was successful.

**acm\_BFR\_TOO\_SMALL**   The array is not large enough to hold all the profile IDs.

## ac\_list\_roles - List Roles

ac\_list\_roles returns a list of the role IDs for each role defined on the coprocessor. This is a series of unordered 8-byte role IDs.

### Function Prototype

```
long ac_list_roles(role_id_t[] role_list, ULONG *num_roles);
```

### Input

role\_list is a pointer to an array to hold the list of role IDs.

num\_roles is a pointer to a variable containing the maximum number of 8-byte IDs which the array can hold.

### Output

On successful exit from this routine:

role\_list contains the list of role IDs.

num\_roles contains the number of role IDs returned.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.

**acm\_BFR\_TOO\_SMALL** The array was not large enough to hold all of the role IDs.



## ac\_load\_profiles - Load User Profiles

ac\_load\_profiles loads one or more user profiles into the coprocessor. Existing profiles can be replaced, if new ones have the same name.

The user profiles are an aggregate structure, where any number of profiles can be concatenated into a single message.

### Function Prototype

```
long ac_load_profiles(void *profile_list, boolean replace_profiles);
```

### Input

On entry to this routine:

profile\_list is a pointer to a variable length buffer of the following form:

- a 4-byte variable containing the number of profiles in this list followed by
- a 4-byte variable containing X'0000' followed by
- the first profile followed by
- any profiles in between followed by
- the last profile

Each of the profiles in the profile list is a user\_profile\_t variable initialized to the following values:

- profile\_vers - the profile structure version, currently X'01'.
- profile\_lth - the length of this profile, in bytes.
- comment - a descriptive comment, of 19 bytes or less in length, NULL terminated.
- cksum - a checksum value to ensure the integrity of the data.
- failure\_cnt - the number of logon failures, initialized to 0.
- user\_id - the user ID associated with this profile. An 8-byte, non-NULL terminated string.
- role\_id - an existing Role from the ROLES SRDI. An 8-byte, non-NULL terminated string.
- act\_date - the activation date of this user, a prof\_date\_t variable with the following values:
  - year - a 2-byte variable with the year (4 digits) in big-endian format
  - month - a one-byte character representing the month (1-12)
  - day - a one-byte character representing the date (1-31)
- exp\_date - the expiration date of this user, a prof\_date\_t variable with the values as the act\_date structure
- authentication data is included at this point. The variable length nature of authentication data is the reason for the profile\_lth field.

replace\_profiles is a boolean variable with TRUE indicating that existing profiles should be changed, FALSE indicating that they should not.

### Output

This function returns no output. On successful exit from this routine:

The PROFILES SRDI has been updated and saved to flash memory.

**Return Codes**

Common return codes generated by this routine are:

|                             |   |
|-----------------------------|---|
| <b>acm_NO_ERROR</b>         | The operation was successful.   |
| <b>acm_FLASH_SPACE_FULL</b> | There is insufficient memory in the flash EPROM to store the new profile list.                            |
| <b>acm_MEM_ALLOC_ERROR</b>  | The function was unable to allocate sufficient memory to install the new profiles.                        |
| <b>acm_PROFILE_EXISTS</b>   | The user_id is already in the PROFILES SRDI, and replace_profiles was FALSE. No profiles have been added. |

## ac\_load\_roles - Load Roles

ac\_load\_roles loads one or more roles into the coprocessor. The roles are passed in an aggregate structure, which can contain any number of concatenated role definitions.

### Function Prototype

```
long ac_load_roles(void *role_list);
```

### Input

On entry to this routine:

role\_list is a pointer to a variable length buffer of the following form:

- a 4-byte variable containing the number of roles in this list followed by
- a 4-byte variable containing 0 followed by
- the first role followed by
- any roles in between followed by
- the last role

Each role is a variable length role initialized to the following:

- A role\_t variable containing:
  - role\_vers - the role structure version, X'01'
  - role\_lth - the number of bytes in this role
  - comment - a 20-byte comment, NULL-terminated, describing this role
  - cksum - checksum, for determining role integrity
  - role\_id - an 8-byte, non-NULL terminated string, the ID for this role.
  - reqd\_auth\_str - the required authentication strength for this role. Each method of authentication is assigned a strength value, with 0 being no authentication. A role may be restricted to users who have logged on with a more stringent method (that is, passphrase rather than PIN) if more than one method has been supplied.
  - lower\_time\_limit
  - upper\_time\_limit
  - valid\_dow
- Followed by an access control point list for the role.

### Output

This function has no output. On successful exit from this routine:

The new role is added to the existing set of roles. If the role exists, it is replaced with the new role.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.

## ac\_lu\_add\_user - Add a User to the List of Logged on Users

ac\_lu\_add\_user informs the Access Control Manager that a specified user has successfully authenticated, and should be added to the list of logged-on users.

The Access Control Manager adds a new entry to the table of logged on users, inserting the specified profile ID as the search key used to identify the entry. It finds the profile and looks up the role, and also puts that in the table entry. This saves the cost of finding the profile each time the user's role is required for future access control operations. Finally, the Access Control Manager generates a session key for the user, and inserts that in the table with the ID and the role.

If the specified profile ID is already in the table of logged on users, the request is rejected.

### Function Prototype

```
long ac_lu_add_user(profile_id_t profile_id);
```

### Input

profile\_id is an 8-byte, non-NULL terminated string representing the user to be logged on.

### Output

This function has no output. On successful exit from this routine:

The user has been added to the list of logged-on users.

### Return Codes

Common return codes generated by this routine are:

|                              |  |
|------------------------------|--|
| <b>acm_NO_ERROR</b>          | The operation was successful.  |
| <b>acm_ALREADY_LOGGED_ON</b> | The user was already logged on.  |
| <b>acm_MEM_ALLOC_ERROR</b>   | The function was unable to allocate sufficient memory to add the role. |
| <b>acm_ROLE_NOT_FOUND</b>    | The specified role was not found.                                      |
| <b>acm_PROFILE_NOT_FOUND</b> | The specified profile was not in the profile list.                     |

## ac\_lu\_drop\_user - Remove a User from the Logon List

ac\_lu\_drop\_user informs the Access Control Manager that a user should be logged off, dropping that user from the logged-on users table.

### Function Prototype

```
long ac_lu_drop_user(profile_id_t profile_id);
```

### Input

profile\_id is an 8-byte, non-NULL terminated string containing the name of the profile to be removed.

### Output

This function returns no output. On successful exit from this routine:

ac\_lu\_drop\_user removes the user from the logged-on users table.

### Return Codes

Common return codes generated by this routine are:

|                          |                               |
|--------------------------|-------------------------------|
| <b>acm_NO_ERROR</b>      | The operation was successful. |
| <b>acm_NOT_LOGGED_ON</b> | The user was not logged on.   |

## ac\_lu\_get\_ks - Get a Copy of a Session Key

ac\_lu\_get\_ks gets a copy of the session key for a specified logged-on user.

### Function Prototype

```
long ac_lu_get_ks(profile_id_t profile_id,  
                 user_session_key_t *session_key);
```

### Input

profile\_id is an 8-byte, non-NULL terminated string containing the name of the profile whose session key you want to retrieve.

session\_key is a pointer to the caller's variable which will receive the cleartext session key  $K_s$  for the specified user.

### Output

On successful exit from this routine:

session\_key contains the cleartext session key  $K_s$  for the specified user.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.

## ac\_lu\_get\_num\_users - Get the Number of Logged On Users

ac\_lu\_get\_num\_users returns the number of users who are currently logged on to the coprocessor. This can be used to determine how much data will be returned by the ac\_lu\_list\_users function.

### Function Prototype

```
long ac_lu_get_num_users(ULONG *num_users);
```

### Input

num\_users is a pointer to a variable which receives the number of logged-on users.

### Output

On successful exit from this routine:

num\_users contains the number of users who are currently logged on to the coprocessor.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.

## au\_lu\_get\_role - Get Role from the Logon List

au\_lu\_get\_role returns the role ID for a specified logged-on user.

### Function Prototype

```
long ac_lu_get_role(profile_id_t profile_id, role_id_t role);
```

### Input

profile\_id is an 8-byte, non-NULL terminated ID of the profile that you want to retrieve.

role is a variable which receives the role ID for the specified user.

### Output

On successful exit from this routine:

role contains the role ID for the specified user.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.



## ac\_lu\_ks\_dec - Decrypt Data with Session Key

ac\_lu\_ks\_dec decrypts a string of data with a specified user's session key. The data length must be a multiple of eight bytes. Decryption is performed using triple-DES CBC mode, with an IV of X'0000000000000000'.

### Function Prototype

```
long ac_lu_ks_dec(profile_id_t profile_id,  
                 UCHAR *ciphertext, UCHAR *cleartext,  
                 ULONG text_length);
```

### Input

profile\_id is an 8-byte, non-NULL terminated string representing the name of the profile whose session key should be used to decrypt the data.

ciphertext is a pointer to the buffer containing the data to be deciphered.

cleartext is a pointer to a buffer where the deciphered data will be stored. This buffer must be at least as large as the *ciphertext* buffer.

text\_length is the length of the data to be deciphered, in bytes. This value must be a multiple of eight.

### Output

On successful exit from this routine:

cleartext contains the deciphered data.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.

## ac\_lu\_ks\_enc - Encrypt Data with Session Key

Encrypt a string of data with a specified user's session key. The data length must be a multiple of eight bytes. Encryption is performed using triple-DES CBC mode, with an IV of X'0000000000000000'.

### Function Prototype

```
long ac_lu_ks_enc(profile_id_t profile_id,  
                 UCHAR *cleartext, UCHAR *ciphertext,  
                 ULONG text_length);
```

### Input

`profile_id` is an 8-byte, non-NULL terminated string representing the name of the profile whose session key should be used to encrypt the data.

`cleartext` is a pointer to the buffer containing the data to be enciphered.

`ciphertext` is a pointer to a buffer where the enciphered data will be stored. This buffer must be at least as large as the `cleartext` buffer.

`text_length` is the length of the data to be enciphered, in bytes. This value must be a multiple of eight.

### Output

On successful exit from this routine:

`ciphertext` contains the enciphered data.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.

## ac\_lu\_ks\_hmacgen - Compute an HMAC Using Session Key

Computes the HMAC on a message, using the supplied session key.

### Function Prototype

```
long ac_lu_ks_hmacgen(profile_id_t profile_id,  
                      UCHAR        *messagetext,  
                      ULONG        msg_length,  
                      mac_t        mac )
```

### Input

On entry to this routine:

profile\_id must contain the ID of the profile of the logged-on user.

messagetext is a pointer to a buffer containing the message.

msg\_length is the number of bytes of data in messagetext.

mac is an 8-byte buffer.

### Output

On successful exit from this routine:

mac contains the 8-byte HMAC of the messagetext, computed with the session key associated with profile\_id.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.

## ac\_lu\_ks\_hmacver - Verify an HMAC Using Session Key

Verifies a supplied MAC on a supplied message, using the user's session key.

### Function Prototype

```
long ac_lu_ks_hmacver(profile_id_t profile_id,  
                     UCHAR      *messagetext,  
                     ULONG      msg_length,  
                     mac_t      mac  
                     USHORT      mac_length,  
                     boolean     *verified );
```

### Input

On entry to this routine:

profile\_id should contain the user's profile ID.

messagetext is a pointer to the message that is to be verified.

msg\_length is the number of bytes in the message.

mac is the 8-byte HMAC which is to be verified.

verified is a pointer to a boolean variable, in which the answer will be supplied.

### Output

On successful exit from this routine:

verified contains true if the MAC was verified, and false if it was not.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.

## ac\_lu\_ks\_macgen - Compute a MAC using Session Key

ac\_lu\_ks\_macgen computes a triple-DES MAC (message authentication code) using the specified user's session key. The full 8-byte MAC result is returned.

The data length must be a multiple of eight bytes. The MAC is computed using an IV of X'0000000000000000'.

### Function Prototype

```
long ac_lu_ks_macgen(profile_id_t profile_id,  
                    UCHAR *messagetext,  
                    ULONG msg_length,  
                    mac_t *mac);
```

### Input

profile\_id is an 8-byte, non-NULL terminated string representing the name of the profile whose session key should be used to compute the MAC.

messagetext is a pointer to a buffer containing the data for which you want to calculate the MAC.

msg\_length is the number of bytes of data in buffer messagetext. This must be a multiple of eight.

mac is a pointer to a buffer which will receive the 8-byte MAC.

### Output

On successful exit from this routine:

mac contains the 8-byte MAC.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.

## ac\_lu\_ks\_macver - Verify a MAC using Session Key

ac\_lu\_ks\_macver verifies a triple-DES MAC (message authentication code) using the specified user's session key. The MAC can be any length up to the full eight bytes. The result is a boolean value indicating whether the supplied MAC matched the computed value.

The MAC is computed using an IV of X'0000000000000000'.

### Function Prototype

```
long ac_lu_ks_macver(profile_id_t profile_id, UCHAR *messagetext,  
                    ULONG msg_length,  
                    mac_t mac, USHORT mac_length, boolean *verified);
```

### Input

profile\_id is an 8-byte, non-NULL terminated string representing the name of the profile whose session key should be used to compute the MAC.

messagetext is a pointer to a buffer containing the data on which you want to verify the MAC.

msg\_length is the number of bytes of data in buffer *messagetext*. This must be a multiple of eight.

mac is the input MAC, which is to be compared with the calculated MAC.

mac\_length is the length of the *mac* parameter, in bytes. It can range from 1 to 8.

### Output

On successful exit from this routine:

verified is a pointer to a boolean variable which receives the verification result. The value is TRUE if the MAC verifies, and FALSE if it does not.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.

## ac\_lu\_list\_users - List the IDs of the Logged On Users

ac\_lu\_list\_users returns a list of the user IDs for each logged-on user.

### Function Prototype

```
long ac_lu_list_users(profile_id_t[] user_list, ULONG *num_users);
```

### Input

user\_list is an array which receives the list of logged-on users.

num\_users is a pointer to a variable containing the number of elements in user\_list.

### Output

On successful exit from this routine:

user\_list contains the (unordered) list of users.

num\_users receives the number of elements returned in the user\_list array.

### Return Codes

Common return codes generated by this routine are:

|                          |  |
|--------------------------|--|
| <b>acm_NO_ERROR</b>      | The operation was successful.                              |
| <b>acm_BFR_TOO_SMALL</b> | The array is not large enough to hold the number of users. |

## au\_lu\_query\_user - Check if a User is Logged On

au\_lu\_query\_user determines whether a specified user is currently logged on to the coprocessor. This is an indication that the user has successfully authenticated to the coprocessor according to one of the enrolled user profiles.

### Function Prototype

```
long ac_lu_query_user(profile_id_t profile_id, boolean *logged_on);
```

### Input

profile\_id is an 8-byte, non-NULL terminated string representing the name of the user being checked.

logged\_on is a pointer to a boolean variable which receives the response to your query.

### Output

On successful exit from this routine:

au\_lu\_query\_user returns a boolean value of TRUE if the user is logged on, and FALSE if not.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.



## ac\_query\_profile - Return the Length of a User Profile

ac\_query\_profile returns the length of a specified user profile, or zero if the profile does not exist on the coprocessor.

### Function Prototype

```
long ac_query_profile(profile_id_t profile_id, ULONG *profile_length);
```

### Input

profile\_id is an 8-byte, non-NULL terminated string representing the name of the profile being checked.

profile\_length is a pointer to variable that will receive the profile structure length, in bytes. The length will be zero if the profile does not exist.

### Output

On successful exit from this routine:

profile\_length contains the length, in bytes. If the profile does not exist, a length of zero is returned.

### Return Codes

Common return codes generated by this routine are:

- |                              |  |
|------------------------------|--|
| <b>acm_NO_ERROR</b>          | The operation was successful.                      |
| <b>acm_PROFILE_NOT_FOUND</b> | The specified profile was not in the profile list. |

## ac\_query\_role - Return the Length of a Role

ac\_query\_role returns the length of a specified role, or zero if the role does not exist on the coprocessor.

### Function Prototype

```
long ac_query_role(role_id_t role_id, ULONG *role_length);
```

### Input

role\_id is an 8-byte, non-NULL terminated ID of the role to be queried.

role\_length is a pointer to a variable which receives the length of the specified role, in bytes.

### Output

On successful exit from this routine:

role\_length contains the length, in bytes. If the role does not exist, a length of zero is returned.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR**            The operation was successful.

**acm\_ROLE\_NOT\_FOUND**    The role does not exist in the SRDI.

## ac\_reinit - Reinitialize the Access Control Manager

ac\_reinit reinitializes the Access Control Manager, deletes all existing roles, profiles, and other data, and reinitializes to the access control state of a new coprocessor.

### Function Prototype

```
long ac_reinit(void);
```

### Input

This function has no input.

### Output

This function has no output. On successful exit from this routine:

ac\_reinit reinitializes the Access Control Manager.

### Return Codes

Common return codes generated by this routine are:

**acm\_NO\_ERROR** The operation was successful.

## ac\_reset\_logon\_fail\_cnt - Reset Logon Failure Count

ac\_reset\_logon\_fail\_cnt resets the logon failure count in the specified user profile. This is the count of the number of consecutive times the user has tried unsuccessfully to authenticate themselves to the coprocessor. The count is reset to zero.

### Function Prototype

```
long ac_reset_logon_fail_cnt(profile_id_t profile_id);
```

### Input

profile\_id is an 8-byte, non-NULL terminated character string ID for the profile to be reset.

### Output

This function returns no output. On successful exit from this routine:

The logon failure count of the specified profile has been set to zero.

### Return Codes

Common return codes generated by this routine are:

- |                              |  |
|------------------------------|--|
| <b>acm_NO_ERROR</b>          | The operation was successful.                      |
| <b>acm_PROFILE_NOT_FOUND</b> | The specified profile was not in the profile list. |

## **acm\_xlt\_errorcode - Translate an ACM Error Code to a SAPI Error Code**

Translates an ACM error code (defined in **camacm.h**) to an SAPI error code (defined in **cmnerrcd.h**).

### **Function Prototype**

```
int acm_xlt_errorcode( long acm_code,  
                      long *sapi_code )
```

### **Input**

On entry to this routine:

`acm_code` contains the error code returned by the Access Control Manager.

`sapi_code` is a pointer to a 4-byte buffer, which will hold the translated code.

### **Output**

On successful exit from this routine:

`acm_xlt_errorcode` returns true if the provided ACM code was found, and false otherwise.

If `acm_xlt_errorcode` returned true, `sapi_code` contains the corresponding SAPI error code.

### **Return Codes**

This function has no return codes.



---

## Chapter 12. Cache Management Functions

This section describes functions used to maintain an on-board cache of security relevant data. For example, the CCA API currently uses these functions to maintain a cache of decrypted private keys.

**Note:** All functions within this chapter are available on both the host and the coprocessor.

### Header Files for Caching Functions

When using these functions, your program must include the following header file.

```
#include "cache.h" /* Cache management functions*/
```

### Overview of Cache Management Functions

The cache management functions allow the operation of a cache of data in the DRAM of the coprocessor. Each entry in the cache consists of a data item and its unique identifier. The cache is indexed on two bytes of data supplied by the user, for example a predefined label or two chosen bytes of a hash of the item or two bytes of the unique identifier. The cache uses a Least Recently Used (LRU) replacement system, eliminating the item which has been unused the longest when more space is needed in the cache.

Data in the cache is stored and accessed using a two-level lookup process. An item is referenced using a "tag", which is any arbitrary-length byte string that uniquely identifies an item. In addition, every access to an item passes a 2-byte "short" tag, which should also be as unique as possible to the item being accessed. It is up to the user to decide how to create the short tags - examples might include a hash of the full tag, the first two bytes of the full tag, or two fixed-position bytes of ciphertext for items that contain encrypted data.

The short tag is broken into two separate one-byte tags, referred to as tag1 and tag2. Tag1 is used as an index into a 256-entry array, where each element either contains a pointer to a list of items that are further addressed using tag2, or NULL if the cache does not contain any items with the indexed tag1 value.

The tag2 lists are linked-lists, where each element contains the data of a cached item. The linked-list, once addressed through the tag1 array, is searched linearly for items with tag2 entries matching the passed tag2 value. For each tag2 match, the entire full tag is compared with that stored in the item, to find the one that is the desired object. (Note that it is possible for multiple items to share identical tag1 and tag2 values, although it is unlikely for good choices of tag1/tag2 computation methods, unless the cache holds a very large number of items.)

## Summary of Functions

These functions are used by the cache manager to manage the cache.

|                          |  |
|--------------------------|--|
| <b>cache_clear</b>       | Remove all entries from a cache.   |
| <b>cache_delete</b>      | Remove an existing cache.  |
| <b>cache_delete_item</b> | Remove a specific item from the cache.                                   |
| <b>cache_get_item</b>    | Retrieve an item from the cache, copying it into a user-supplied buffer. |
| <b>cache_get_item_b</b>  | Retrieve an item from the cache after allocating memory to hold it.      |
| <b>cache_init</b>        | Open a new cache.  |
| <b>cache_status</b>      | Check the status of an existing cache.                                   |
| <b>cache_write_item</b>  | Store an item in the cache.  |



## cache\_clear

cache\_clear clears all data from the specified cache.

### Function Prototype

```
cacheError cache_clear(cacheHandle handle);
```

### Input

On entry to this routine:

handle must be set to a valid cacheHandle.

### Output

This function returns no output. On successful exit, all data has been cleared from the specified cache.

### Return Codes

Common return codes generated by this routine are:

|                      |                                      |
|----------------------|--------------------------------------|
| <b>ce_OK</b>         | The function completed successfully. |
| <b>ce_BAD_HANDLE</b> | The specified cache does not exist.  |

## cache\_delete

cache\_delete will remove an existing cache, recovering all memory.

### Function Prototype

```
cacheError cache_delete(cacheHandle handle);
```

### Input

On entry to this routine:

handle must be set to a valid cacheHandle.

### Output

This function returns no output. On successful exit, all data has been cleared from the specified cache, the cache has been removed, and all associated memory objects have been freed.

### Return Codes

Common return codes generated by this routine are:

- |                      |                                      |
|----------------------|--------------------------------------|
| <b>ce_OK</b>         | The function completed successfully. |
| <b>ce_BAD_HANDLE</b> | The specified cache does not exist.  |

## cache\_delete\_item

cache\_delete\_item deletes the specified item from the cache.

### Function Prototype

```
cacheError cache_delete_item(cacheHandle handle,  
                             short_tag_t short_tag,  
                             ULONG full_tag_length,  
                             UCHAR *full_tag);
```

### Input

On entry to this routine:

handle contains the handle of the specified cache.

short\_tag is the two-byte tag used for indexing the cache items.

full\_tag\_length is the length of the unique identifier of the item to be deleted.

full\_tag is a buffer which contains the unique identifier of the item to be deleted.

### Output

This function returns no output. On successful completion, the data item referenced by the short\_tag and the full\_tag has been removed from the cache.

### Return Codes

Common return codes generated by this routine are:

|                          |  |
|--------------------------|--|
| <b>ce_OK</b>             | The function completed successfully.           |
| <b>ce_BAD_HANDLE</b>     | The specified cache does not exist.            |
| <b>ce_ITEM_NOT_FOUND</b> | The specified item was not found in the cache. |

## cache\_get\_item

cache\_get\_item retrieves a specific item from the cache and copies it into a buffer supplied by the user.

### Function Prototype

```
cacheError cache_get_item(cacheHandle handle,
                          ULONG      *bfrSize,
                          UCHAR      *bfr,
                          short_tag_t short_tag,
                          ULONG      full_tag_length,
                          UCHAR      *full_tag);
```

### Input

On entry to this routine:

handle contains the handle for the specified cache.

bfrSize is a pointer to the length of the available space in the supplied buffer.

bfr is a pointer to the buffer in which the retrieved item will be returned.

short\_tag is the two-byte tag which is used to index the item in the cache.

full\_tag\_length is the length of the unique identifier of the item in the cache.

full\_tag is the unique identifier of the item to be retrieved from the cache.

### Output

On successful exit to this routine:

bfrSize is a pointer to the length of the item which was retrieved from the cache.

bfr contains the item which was retrieved.

### Return Codes

Common return codes generated by this routine are:

|                          |  |
|--------------------------|--|
| <b>ce_OK</b>             | The function completed successfully.                       |
| <b>ce_BAD_HANDLE</b>     | The specified cache does not exist.                        |
| <b>ce_ITEM_NOT_FOUND</b> | The specified item was not found in the cache.             |
| <b>ce_BFR_TOO_SMALL</b>  | The provided buffer was not large enough to hold the item. |

## cache\_get\_item\_b

cache\_get\_item retrieves a specific item from the cache and copies it into a buffer which is allocated by the function. This function is useful when the cache holds items with very different sizes.

**Note:** The calling function is responsible for freeing the memory allocated for the item when the item is no longer needed. However, if the function fails to complete successfully, the buffer is not allocated.

### Function Prototype

```
cacheError cache_get_item_b(cacheHandle handle,
                           ULONG      *bfrSize,
                           UCHAR     **bfr,
                           short_tag_t short_tag,
                           ULONG      full_tag_length,
                           UCHAR     *full_tag);
```

### Input

On entry to this routine:

handle is the handle which specifies the required cache.

short\_tag is the two-byte tag used to index the item within the cache.

full\_tag\_length is the length of the unique identifier for the item.

full\_tag is the unique identifier of the item.

### Output

On successful exit from this routine:

bfrSize is a pointer to the size of the buffer returned.

bfr is a pointer to a buffer containing the recovered item. This buffer has been allocated by the function.

### Return Codes

Common return codes generated by this routine are:

|                           |   |
|---------------------------|---|
| <b>ce_OK</b>              | The function completed successfully.  |
| <b>ce_BAD_HANDLE</b>      | The specified cache does not exist.   |
| <b>ce_ITEM_NOT_FOUND</b>  | The specified item was not found in the cache.                                |
| <b>ce_MEM_ALLOC_ERROR</b> | The function was unable to allocate memory for the buffer to return the item. |

## cache\_init

cache\_init opens a new cache, returning a handle with which to access the cache. The caller specifies the maximum size of the cache and the maximum size of the items within the cache.

### Function Prototype

```
cacheError cache_init(ULONG      maxBytes,  
                     ULONG      maxItemBytes,  
                     cacheHandle *handle);
```

### Input

On entry to this routine:

maxBytes contains the maximum number of bytes to be used in the cache. This number must be large enough to hold at least one item of maxItemBytes, along with extra room for control structures. This number determines at which point the LRU algorithm will come into play, replacing old items with new ones.

maxItemBytes contains the maximum number of bytes which an item will occupy. This value should include both the maximum size of the item and the maximum size of the unique identifier.

handle is a pointer to an item of cacheHandle type, in which the function will return the handle for accessing the cache.

### Output

On successful exit from this routine:

handle contains the cacheHandle used to access the new cache.

### Return Codes

Common return codes generated by this routine are:

- |                           |  |
|---------------------------|--|
| <b>ce_OK</b>              | The function completed successfully.                               |
| <b>ce_ITEM_TOO_LARGE</b>  | The maxItemBytes parameter is too large for the maxBytes.          |
| <b>ce_MEM_ALLOC_ERROR</b> | The function was unable to allocate memory for the cache overhead. |

## cache\_status

cache\_status returns the status of the specified cache, that is bytes used by each item (including overhead), bytes used altogether, number of items currently in the cache.

### Function Prototype

```
cacheError cache_status(cacheHandle handle,
                        ULONG          *maxBytes,
                        ULONG          *maxItemBytes,
                        ULONG          *bytesUsed,
                        ULONG          *itemsStored) ;
```

### Input

On entry to this routine:

handle is the handle of the cache to be queried.

maxBytes is a pointer to a long data item.

maxItemBytes is a pointer to a long data item.

bytesUsed is a pointer to a long data item.

itemsStored is a pointer to a long data item.

### Output

On successful exit from this routine:

maxBytes is a pointer to the maximum number of bytes to be used in the cache, including overhead.

maxItemBytes is a pointer to the maximum number of bytes each entry will use, including the data item, the unique identifier, and the overhead.

bytesUsed is a pointer to the number of bytes currently used in the cache, including data and overhead.

itemsStored is a pointer to the number of items which are currently stored in the cache.

### Return Codes

Common return codes generated by this routine are:

|                        |   |
|------------------------|---|
| <b>ce_OK</b>           | The function completed successfully.      |
| <b>ce_NULL_POINTER</b> | One of the parameters was a null pointer. |
| <b>ce_BAD_HANDLE</b>   | The specified cache does not exist.       |

## cache\_write\_item

cache\_write\_item writes an item to the specified cache. If the cache is full, the function will delete the least recently used item from the cache before storing the new item.

### Function Prototype

```
cacheError cache_write_item(cacheHandle handle,
                           ULONG         item_length,
                           UCHAR        *item,
                           short_tag_t  short_tag,
                           ULONG        full_tag_length,
                           UCHAR        *full_tag) ;
```

### Input

On entry to this routine:

handle is the handle which identifies the cache.

item\_length is the length of the item to be stored. This length plus the full\_tag\_length must be smaller than the maxItemBytes specified when the cache was initialized.

item is a pointer to a buffer containing the item to be stored.

short\_tag is the two-byte tag to be used to index this item within the cache.

full\_tag\_length is the length of the unique identifier for the item. This length plus item\_length must be less than the maxItemBytes specified when the cache was initialized.

full\_tag is the unique identifier for this data item.

### Output

This function returns no output. On successful completion, the item has been added to the cache.

### Return Codes

Common return codes generated by this routine are:

|                          |   |
|--------------------------|---|
| <b>ce_OK</b>             | The function completed successfully.  |
| <b>ce_NULL_POINTER</b>   | One of the parameters was a null pointer.   |
| <b>ce_BAD_HANDLE</b>     | The specified cache does not exist.   |
| <b>ce_ITEM_TOO_LARGE</b> | The sum of the full_tag_length and the item_length is greater than the maximum item size for the cache. |



---

## Chapter 13. Miscellaneous Functions

This chapter describes functions that do not fit into any of the previously described categories.

### Header Files for Miscellaneous Functions

When using these functions, your program must include the following header files.

```
#include "cassub.h"                /* DES 96 function prototypes */
#include "camacm.h"
#include "cmnfunct.h"
```

### Summary of Functions

|                              |  |
|------------------------------|--|
| <b>check_access_auth_fcn</b> | Verifies the user's authority.               |
| <b>GetKeyLength</b>          | Returns the length of a specified key token. |
| <b>intel_long_reverse</b>    | Byte-reverses a 4-byte block of data.        |
| <b>intel_word_reverse</b>    | Byte-reverses a 2-byte block of data.        |

## check\_access\_auth\_fcn - Verify User Authority

**Note:** This function is available on the coprocessor.

check\_access\_auth\_fcn performs operations that are necessary before executing a requested CCA command.

1. It checks to see if the user who sent the request is authorized to perform the requested function. This is done by passing a function code, known as an *Access Control Point*. A user's role contains a list of the Access Control Points corresponding to functions that the user is permitted to execute.
2. If the user is authorized to execute the command, the reply CPRB and parameter block are initialized.

The function returns a boolean value in *pGranted* to indicate whether the specified function was authorized.

### Function Prototype

```
#define CHECK_ACCESS_AUTH(Rqc, Rpc,r,c,g) check_access_auth_fcn(Rqc, Rpc, r, c, g)
ULONG check_access_auth_fcn( CPRB_ptr    pRequestCprb,
                             CPRB_ptr    pReplyCprb,
                             role_id_t    roleID,
                             USHORT       requested_fcn_code,
                             boolean      *pGranted)
```

### Input

On entry to this routine:

pRequestCprb is a pointer to the request (input) CPRB structure.

pReplyCprb is a pointer to a buffer which receives the initialized reply (output) CPRB structure.

roleID is the eight-character Role ID defining the access control role for the user who sent this request. The Role ID is an input parameter, passed to every CCA command processor when it is called.

requested\_fcn\_code is the Access Control Point corresponding to the CCA verb you are executing. The Access Control Manager determines if the user is allowed to execute this verb, based on whether the Access Control Point is enabled in the user's role.

### Output

On successful exit from this routine:

pGranted is a pointer to a location where the boolean result is returned. The value stored in *pGranted* is TRUE if the user has authorization, and FALSE if not.

**Notes**

Access is granted to role IDs using the *csuncnm* utility. New access control points are added to the file *csuap.def*.

This function may also be called using the macro `CHECK_ACCESS_AUTH`, with the same parameters as previously described.

**Return Codes**

Common return codes generated by this routine are:

**OK** The operation was successful.

**acm\_ROLE\_NOT\_FOUND** The role is not in the SRDI.

## GetKeyLength - Get Length of Key Token

**Note:** This function is available on the host.

GetKeyLength returns the length of a specified key token.

### Function Prototype

```
USHORT GetKeyLength  
(  
    UCHAR * keyid_ptr,  
    long * key_parm_length_ptr,  
    long * message_ptr  
)
```

### Input

On entry to this routine:

`keyid_ptr` is a pointer to the start of the input key data.

`key_parm_length_ptr` is a pointer to the expected key length, if this is an RSA key token, or NULL if not an RSA token. (RSA tokens are passed to the host with a parameter length, because they are variable sized. This function returns an error if the RSA token is larger than this expected size.)

`message_ptr` is a pointer to an address which stores the return code.

### Output

On successful exit to this routine:

GetKeyLength returns the length of the token, or -1 if an error occurred.

`message_ptr` contains the return code. If there is no error, this is set to S\_OK (0).

### Return Codes

Common return codes generated by this routine are:

- |                    |  |
|--------------------|--|
| <b>ERROR</b>       | If the error code pointed to by <i>message_ptr</i> is S_OK, the function result is set to the length of the key. Otherwise, the function returns a value of ERROR (-1), and the value pointed to by <i>message_ptr</i> is a SAPI error code. |
| <b>E_KEY_LEN</b>   | The key has a length less than 1 byte.   |
| <b>E_SIZE</b>      | The key is longer than the expected length in <i>key_parm_length_ptr</i> .   |
| <b>E_KEY_TOKEN</b> | <i>keyid_ptr</i> was not pointing at a valid key token.  |

## intel\_long\_reverse - Convert Long Values

**Note:** This function is available on both the host and the coprocessor.

intel\_long\_reverse reverses the order of the bytes in a long (4-byte) integer. This is used to convert long values between big-endian and little-endian formats.

### Function Prototype

```
ULONG intel_long_reverse(ULONG long_val)
```

For portability reasons, the following macros have been conditionally defined for integer translation.

```
#ifdef BIG_ENDIAN
#define xtoh1(d) ((ULONG)d)
#define htoh1(d) ((ULONG)d)
#define atoh1(d) intel_long_reverse((ULONG)d)
#define htoah1(d) intel_long_reverse((ULONG)d)
#else
#define xtoh1(d) intel_long_reverse((ULONG)d)
#define htoh1(d) intel_long_reverse((ULONG)d)
#define atoh1(d) ((ULONG)d)
#define htoah1(d) ((ULONG)d)
#endif
```

### Input

On entry to this routine:

long\_val is the input value. It is reversed in byte order, and returned as the function result.

### Output

This function returns no output. On successful exit to this routine:

intel\_long\_reverse returns the bytes from long\_val in reverse order.

### Return Codes

This function has no return codes.

## intel\_word\_reverse - Convert 2-Byte Values

**Note:** This function is available on both the host and the coprocessor.

intel\_word\_reverse reverses the order of the bytes in a word (2-bytes) of data. This is used to convert 2-byte values between big-endian and little-endian formats.

For portability reasons, the following macros have been conditionally defined for integer translation.

```
#ifdef BIG_ENDIAN
#define xtohs(d) ((USHORT)d)
#define htoxs(d) ((USHORT)d)
#define atohs(d) intel_word_reverse((USHORT)d)
#define htogas(d) intel_word_reverse((USHORT)d)
#else
#define xtohs(d) intel_word_reverse((USHORT)d)
#define htoxs(d) intel_word_reverse((USHORT)d)
#define atohs(d) ((USHORT)d)
#define htogas(d) ((USHORT)d)
#endif
```

*where:*

x External  
h Host  
a Adapter

### Function Prototype

```
USHORT intel_word_reverse(USHORT intel_int)
```

### Input

On entry to this routine:

intel\_int is the input word. It is reversed in byte order, and returned as the function result.

### Output

On successful exit from this routine:

intel\_word\_reverse returns the bytes from intel\_int in reverse order.

### Return Codes

This function has no return codes.

**TOKEN\_IS\_A\_LABEL - Identifies the Token as a Label**

This macro has a value of TRUE when the first byte of the key identifier input is valid for a key label. All key labels have a first byte between 0x20 and 0xFE. TOKEN\_IS\_A\_LABEL should be used when a token is available for checking.

```
#define TOKEN_IS_A_LABEL(keyid) \  
    (( keyid[0] >= MIN_FOR_LABEL ) && ( keyid[0] <= MAX_FOR_LABEL ))
```

**TOKEN\_LABEL\_CHECK - Determine if Key Identifier is a Label**

This macro has a value of TRUE when the character input is valid for a key label. All key labels have a first byte between 0x20 and 0xFE. TOKEN\_LABEL\_CHECK should be used when only one byte is available for checking.

```
#define TOKEN_LABEL_CHECK(keyid) \  
    (( keyid >= MIN_FOR_LABEL ) && ( keyid <= MAX_FOR_LABEL ))
```



## Appendix A. UDX Sample Code - Host Piece

This appendix contains a listing of the sample file *sxt\_samp.c*. This file is a skeleton for the design of the host piece of a CCA extension.

```

/*****
** Bring in the include files
*****/
#include <stdlib.h>
#include <string.h>

#include "cmncrypt2.h"          /* Cryptographic types          */
#include "cmnerrcd.h"          /* Common error codes.          */
#include "cmnlibr.h"           /* Common library routines.     */

#include "safhead1.h"          /* External SAPI functions.     */
#include "safcextn.h"          /* External SAPI functions.     */

#include "csueextn.h"          /* CCA extensions for SAPI API  */
#include "cxt_cmds.h"          /* CCA extensions for SAPI, cmdproc*/

/*****
/*          CCAXFCN1
/*-----*/
/* Purpose
/* This is the entry point for a sample CCA API extension verb.
/*
/* This sample's input parameters are similiar to a CCA verb's
/* parameters. Following is an explanation of the parameters.
/*
/* pReturnCode -- Where to return the return code value.
/* pReasonCode -- Where to return the completion reason.
/* pExitDataLength -- Unused parameter placeholder.
/* pExitData -- Unused parameter placeholder.
/* pRuleArrayCount -- Pointer to number of 8 byte rule array
/* entries.
/* pRuleArray -- Pointer to the rule array values.
/* pKeyId -- Pointer to a 64 byte key or a key token.
/*
/*****
void SECURITYAPI CCAXFCN1
(
    long          * pReturnCode,
    long          * pReasonCode,
    long          * pExitDataLength,
    unsigned char * pExitData,
    long          * pRuleArrayCount,
    unsigned char * pRuleArray,
    unsigned char * pKeyId
)
{
/*****
** Local variables.
*****/
long          ErrorMsg;          /* Error message of SAPI routines */
CPRB_ptr     pCprb;             /* CPRB pointer                    */
UCHAR        *pReqBlk;          /* request parm blk pointer        */

USHORT       ReqBlkLen;         /* request parm buffer length      */

USHORT       KeyIdLength;       /* Length of key id/token.         */

KEY_FIELD_HEADER KeyBlkHeader;  /* Key block header area.          */
KEY_FIELD_HEADER KeyBlkReturn;  /* Key block header return area.   */

REQUEST_REPLY_BUF * pReqReplyBuf; /* Buffer area pointer for request*/
/* and reply CPRB/parm areas.    */

UCHAR        KeyLabel[64];      /* A key token with no data.       */
boolean      KeyIdIsLabel;      /* Truth value that the key id was*/

```

```

                                /* passed as a label          */
key_data_structure *pKeyBlock;    /* Ptr. to generated key    */
key_data_structure *pNextKeyBlock; /* Ptr. to generated key    */
generic_key_block_structure *pKeyField; /* Ptr. to start of a key field.*/

/*****
** Assure we can return values without causing an address exception
** by checking for NULL pointers.
*****/
if ( (pReturnCode == NULL) || (pReasonCode == NULL) )
    return;

/*****
** Initialize return code and return code.
*****/

*pReturnCode = 0;                /* reset return code      */
*pReasonCode = 0;                /* reset reason code      */

/*****
** Assure we can use the passed pointers without causing an
** address exception by checking that required pointers are
** not NULL.
*****/
if ( (pRuleArrayCount == NULL) || (pRuleArray == NULL) ||
      (pKeyId == NULL) )
{
    CSUC_PROCRET(pReturnCode, pReasonCode, E_NULL_PTR);
    return;
}

/*****
** OPTIONAL ----- depends on whether your CCA extension has
**                    rule array values.
**
** Assure that the rule count is reasonable.
*****/
if ( (*pRuleArrayCount < RAC_MIN) || (*pRuleArrayCount > RAC_MAX) )
{
    CSUC_PROCRET(pReturnCode, pReasonCode, E_RULE_ARRAY_CNT);
    return;
}

/*****
** OPTIONAL ----- depends on whether your CCA extension uses
**                    key tokens.
**
** Get the length of the key identifier field and check for validity.
*****/
KeyIdLength = GetKeyLength( pKeyId, NULL, &ErrorMsg);

if( (ErrorMsg != S_OK) &&
      (CSUC_PROCRET(pReturnCode, pReasonCode, ErrorMsg) == ERROR) )
{
    return;
}

/*****
**
**
** Add your own checking, etc. logic here.
**
*****/

/*****
** Build the 4 parts of the CPRB "T2" Request Parameter Block
** that is sent to the adapter for processing.
** The block consists of the following fields.
**
** +-----+-----+-----//+-----+-----//+-----+-----//+
** |Sub-   |Rule Array   |Verb Unique   |Key Block   |

```

```

** |Function |           |           |           |           |           |           |
** |Code     | Length | Array  | Length | Data  | Length | Fields |
** |-----+-----+-----+-----+-----+-----+-----+
** | 0       | 2     | 4      | 2+X   | 4+X   | 2+X+Y | 4+X+Y |
** |-----+-----+-----+-----+-----+-----+-----+
** |<-- 2 -->|<-- X  ----->|<-- Y  ----->|<-- Z  ----->|
**
*****/

/*****
** Allocate working space for the sending CPRB, request
** parameter block, returning CPRB and the reply
** parameter block.
*****/
pReqReplyBuf = malloc( sizeof(REQUEST_REPLY_BUF) );

if ( pReqReplyBuf == NULL )
{
    CSUC_PROCRET ( pReturnCode, pReasonCode, E_ALLOCATE_MEM );
    return;
}

/*****
** Establish addressability to the CPRB area and the request
** parameter block.
**
** NOTE: The CPRB and the request parameter block must be built
**       in the allocated structure in the following manner.
**       +-----+-----+
**       |CPRB   | Request parameter |
**       |structure| block           |
**       +-----+-----+
*****/
pCprb = (CPRB_ptr) &(pReqReplyBuf->request_buf[0]);
pReqBlk = &(pReqReplyBuf->request_buf[0]) +
          sizeof(CPRB_structure);

/*****
** Part 1 of 4.
**
** Put the 2-byte subfunction code at the beginning of the
** request parameter area.
**
** NOTE- Replace CCAXFNC1_ID with the subfunction code for your
**       CCA API extension.
*****/
ReqBlkLen = 2;
*((USHORT *) pReqBlk) = htoas ( CCAXFNC1_ID );

/*****
** Part 2 of 4.
**
** Add the rule array block to the request parameter area.
**
** NOTE- If there are no rule array values, a 2 byte length field
**       with a value of 2 must be added.
*****/
ReqBlkLen += BuildParmBlock(pReqBlk + ReqBlkLen, /* Target address*/
                            1, /* # of blocks to add.*/
                            (USHORT) (8 * *pRuleArrayCount),
                            pRuleArray );

/*****
** Part 3 of 4.
**
** Add the verb unique data block to the request parameter area.
**
** NOTE- If there is no verb unique data block, a 2 byte length field
**       with a value of 2 must be added. This is an example of how
**       to just add a 2 byte length field when there is no
**       additional data.

```

```

*****/
ReqBlkLen += BuildParmBlock(pReqBlk + ReqBlkLen, /* Target address */
                           0, /* # of blocks to add. */
                           0, NULL);

/*****
** Part 4 of 4.
**
** Add the key block to the request parameter area. The
** key block can consist of key tokens or key labels.
**
** NOTE- If there is no key block, a 2 byte length field
** with a value of 2 must be added.
*****/
/* Check first byte to determine if pKeyId is a label or a token */
if ( (*pKeyId >= MIN_FOR_LABEL) &&
      (*pKeyId <= MAX_FOR_LABEL) )
{
  /*****
  ** The application specified a key label for the key token.
  ** The key label will be replaced by a key token from the key
  ** storage file prior to sending this request to the adapter.
  **
  ** NOTE- When a key token is going to be updated in the key
  ** storage file by this operation, the second key block
  ** must be specified for returning and updating of
  ** the key token in the key storage file.
  *****/
  if ( saf_process_key_label( pKeyId, true, KeyLabel )
        == false )
  {
    /*****
    ** The format of the key label is invalid.
    *****/
    free( pReqReplyBuf );
    CSUC_PROCRET( pReturnCode, pReasonCode, E_KEY_LABEL_FMT );
    return;
  }

  KeyIdIsLabel = true;
  KeyBlkHeader.Flags = htoas ( DES96_TYPE | ACTION_READ );
  KeyBlkHeader.Length = htoas ( KEY_HDR_LEN + sizeof(KeyLabel) );

  KeyBlkReturn.Flags = htoas ( DES96_TYPE | ACTION_NOOP );
  KeyBlkReturn.Length = htoas ( KEY_HDR_LEN + sizeof(KeyLabel) );

  ReqBlkLen += BuildParmBlock(pReqBlk + ReqBlkLen, /* Target address*/
                              4, /* # of blocks to add.*/
                              sizeof(KeyBlkHeader), &KeyBlkHeader,
                              sizeof(KeyLabel), KeyLabel,
                              sizeof(KeyBlkReturn), &KeyBlkReturn,
                              sizeof(KeyLabel), KeyLabel);
}
else
{
  /*****
  ** A key token was specified for the key identifier.
  ** An actual key token is being passed instead of a key label.
  *****/
  KeyIdIsLabel = false;
  KeyBlkHeader.Flags = htoas ( DES96_TYPE | ACTION_NOOP );
  KeyBlkHeader.Length = htoas ( KEY_HDR_LEN + KeyIdLength );

  ReqBlkLen += BuildParmBlock(pReqBlk + ReqBlkLen, /* Target address*/
                              2, /* # of blocks to add.*/
                              sizeof(KeyBlkHeader), &KeyBlkHeader,
                              KeyIdLength, pKeyId );
}

/*****
** Build the CPRB
**

```

```

** NOTE- If your extension uses the data buffer, you must change
**       the request/reply data buffer parameters in the following
**       statement.
**       *****/
CSUC_BULDCPRB(pCprb,
              (UCHAR *) ESSS_FUNCTION_ID_S,
              ReqBlkLen, pReqBlk,          /* Request parm. buffer */
              0, (UCHAR *) NULL,          /* Request data buffer */
              sizeof( pReqReplyBuf->reply_buf ),
              pReqReplyBuf->reply_buf,     /* Reply parameter buffer */
              0, (UCHAR *) NULL);         /* Reply data buffer */

/*****
**
** SEND REQUEST TO THE COPROCESSOR FOR EXECUTION.
**
** The CPRB request is sent to the Security Server which in turn then
** forwards it to the device driver.
**       *****/
CSNC_SP_SCSRFBSS( pCprb, &ErrorMsg);

/*****
** Check the return/reason codes of the completed operation.
**
** NOTE- CSUC_PROCRET returns ERROR if the error code in msg is higher
**       than the error code already in *pReturnCode and *pReasonCode.
**       msg is the return code and reason code, concatenated in a single
**       long integer - for example, msg=00080012 is equivalent to return
**       code 8, reason code 12.
**       *****/

if ( (ErrorMsg != S_OK) &&
      (CSUC_PROCRET(pReturnCode, pReasonCode, ErrorMsg) == ERROR) )
{
    free( pReqReplyBuf );
    return;
}

/*****
** Process the returned data, which is in the reply parameter block.
** The reply parameter block must have the same format as the
** request parameter block.
**
** Examine the reply parameter block to make sure it is OK. If not,
** something went wrong in the adapter - it should return valid data.
**       *****/
if ( parm_block_valid( pCprb, SEL_REPLY_BLK ) == false)
{
    CSUC_PROCRET( pReturnCode, pReasonCode, CP_DEV_HWERR );
    free( pReqReplyBuf );
    return;
}

/*****
** OPTIONAL ----- depends on your CCA extension.
**
** Find the first key in the key block of the reply parameter block.
** This will be the newly generated key, which we will pass back to the
** caller. If there is no key, abort with an error.
**       *****/
if ( find_first_key_block( pCprb, &pKeyBlock, SEL_REPLY_BLK ) == false)
{
    CSUC_PROCRET( pReturnCode, pReasonCode, FT_INCONSIST_DATA);
    free( pReqReplyBuf );
    return;
}

/*****
** OPTIONAL ----- depends on your CCA extension.
**
** Assure that only one key block is returned.

```

```

*****/
if ( find_next_key_block( pCprb, pKeyBlock,
                        &pNextKeyBlock, SEL_REPLY_BLK) == true)
{
    CSUC_PROCRET( pReturnCode, pReasonCode, FT_INCONSIST_DATA);
    free( pReqReplyBuf );
    return;
}

/*****
** OPTIONAL ----- depends on your CCA extension.
**
** We've successfully located the first key in the key block, and its
** address is in pKeyBlock.  Everything looks OK.
*****/
pKeyField = (generic_key_block_structure *) pKeyBlock;
if ( KeyIdIsLabel == false )
{
    /*****
    ** Since KeyId is not a label, we need to pass the re-enciphered
    ** key token back to the caller. pKeyBlock points to the start of the
    ** entire key field, including the key field header (length and flag
    ** bytes).
    *****/
    memcpy( pKeyId, &(pKeyField->label_or_token), DES_TOKEN_LENGTH);
}

/*****
** Free the space allocated for the CPRB and the request/reply
** data areas and then return to the calling application.
*****/
free( pReqReplyBuf );
return;

} /* end-of CCAXFCN1() */
UDXKEN1.PLX.

```

## Appendix B. UDX Sample Code - Coprocessor Piece

This appendix contains a listing of the sample file *cxt\_samp.c*. This file is a skeleton for the design of the adapter piece of a CCA extension, including the command processor.

```

/*****
** Bring in the include files
**
** If you are using any of the "C" functions provided by CPQ,
** include the following CPQ files instead of the standard
** "C" files ( stdlib.h, string.h, etc. ).
**
** #include <clib.h>
** #include <cpqlib.h>
** #include <sys\stat.h>
** #include <qrm_cnst.h>
**
*****/

#include "cmncrypt2.h"          /* CCA common definitions      */
#include "camacm.h"            /* Access manager definitions  */

#include "cmnerrcd.h"          /* Common error codes.         */
#include "cam_xtrn.h"          /* CCA managers                */

#include "cassub.h"
#include "casfunct.h"          /* Common command processor funct's */
#include "cacdtkn.h"          /* PKA token subroutines.      */
#include "cacscacp.h"          /* Access control codes        */

#include "cxt_cmds.h"          /* CCA command extensions.     */

/*****
** ENTER
**     your CCA command extension array entry after this comment.
**     =====
**
** Each element of the table is a CCAX_CP_DEF type. That is, it
** contains one 2 character sub-function code, and a pointer to
** the corresponding command processor function.
**
*****/

CCAX_CP_DEF ccax_cp_list[] = { { CCAXFNC1_ID, ccax_fcn_1 } };

/*****
**
** Declare a variable which holds the number of CCA extension verbs
** defined in the ccax_cp_list table above.
**
*****/
ULONG ccax_cp_list_size = 0;          // NOTE:
                                       // Once you add your first entry to
                                       // "ccax_cp_list", delete this
                                       // statement and un-comment the
                                       // following statement.

// ULONG ccax_cp_list_size = ( sizeof(ccax_cp_list) / sizeof(CCAX_CP_DEF) );

/*****
** Local rule array value definitions.
*****/
#define KEY_CLR      11
#define KEY_ENC      12
#define KEY_CLRD     13

```

```

#define KEY_ENCD 14
#define KEY_KM 15
#define KEY_NKM 16
#define KEY_OKM 17
#define GENERATE 20
#define VERIFY 21
#define DFLT_CF 31
#define ADAPTER 32

/*****
/*
/*-----
/* Purpose:
/* This sample CCA extension shows the general structure of a
/* command processor.
/*
/* Linkage: see below
/*
/* Input: See below
/*
/* Output:
/* The output CPRB and reply parameter blocks contains the
/* results.
/*
/* Return Code:
/* Passed back in the CPRB.
*****/
void ccax_fcn_1(
    CPRB_structure *pCprbIn, /* (input) request CPRB */
    CPRB_structure *pCprbOut, /* (output) reply CPRB */
    unsigned long RequestId, /* (input) Adapter request
/* identifier.
/*
    role_id_t roleID ) /* (input) role ID ptr
/*
{
    /*****
    ** Define the rule array for converting 8 character rules into
    ** integer values. This example has 11 rules divided into 3 groups.
    ** On every request, there can be 3 choices, 1 from each group.
    *****/
    int RuleValue[ 3 ]; /* Variable to encrypt rule values.*/
    USHORT RuleMapCount = 11;
    static RULE_MAP RuleMap[] = {{"KEY-CLR ", 1 , KEY_CLR },
    {"KEY-ENC ", 1 , KEY_ENC },
    {"KEY-CLRD", 1 , KEY_CLRD},
    {"KEY-ENCD", 1 , KEY_ENCD},
    {"KEY-KM ", 1 , KEY_KM },
    {"KEY-NKM ", 1 , KEY_NKM },
    {"KEY-OKM ", 1 , KEY_OKM },
    {"GENERATE", 2 , GENERATE},
    {"VERIFY ", 2 , VERIFY },
    {"DFLT-CF ", 3 , DFLT_CF },
    {"ADAPTER ", 3 , ADAPTER },};

    /*****
    ** Define local variables.
    *****/
    long ReturnMsg; /* Return code messages. */

    RBFPTR pReqBlk ;
    RBFPTR pReplyBlk ;
    void *pToken;

    UCHAR *pKeyBlock ;
    UCHAR *pLabel;
    USHORT ReplyLength;

    des_key_token_structure *pDesToken;
    verb_unique_data_structure *pVerbData;
    generic_key_block_structure *pKeyBlockStruct;

    mk_status_var MstrKeyStatus;

```



```

boolean      KeyIdIsLabel;    /* Truth value that the key id was */
                               /* passed as a label                */

long   ReplyBlockLength;     /* length of the data added to the */
                               /* reply block                      */
KEY_FIELD_HEADER KeyHeader;  /* header for key in reply block  */
boolean Authorized;

if ( RequestId == 0)         /* Do nothing statement to get rid of */
    ReplyLength = 0;        /* compiler warning messages because */
                               /* RequestId is not used.            */

/*****
** Copy input CPRB to the output area.
***/
memcpy ( pCprbOut, pCprbIn, pCprbIn->CPRB_length );

Cas_proc_ret( pCprbOut, S_OK );

/*****
** Initialize the CPRB request/reply parameter pointers and then
** set my local pointers to the request and reply parameter blocks.
***/
InitCprbParmPointers( pCprbIn, pCprbOut );

pReqBlk = pCprbIn->req_parm_block;
pReplyBlk = pCprbOut->reply_parm_block;

/*****
** Set the reply subfunction code early, because the Cas_proc_ret
** routine needs it set for negative return codes.
***/
pReplyBlk->subfunction_code = pReqBlk->subfunction_code;

/*****
** OPTIONAL ----- depends on your CCA extension.
**
** Make sure this service is authorized before we go any further
**
** NOTE: Replace SCA_COMMAND_BKTC with your own access point for
** this extension. CACSCACP.H defines what range of access
** points are available for extension services.
***/
CHECK_ACCESS_AUTH( pCprbIn,
                  pCprbOut,
                  roleID,
                  SCA_COMMAND_BKTC, // Access control point.
                  &Authorized );

if ( Authorized == false )
{
    Cas_proc_ret( pCprbOut, CP_NOT_AUTH );
    return ;
}

/*****
** OPTIONAL ----- depends on your CCA extension.
**
** Make sure the current master key is valid before we go
** any further.
***/
switch ( get_master_key_status ( &MstrKeyStatus ) )
{
    case MK_NO_ERROR :
        if ( (MstrKeyStatus & mks_CMK_VALID) != mks_CMK_VALID )
        {
            Cas_proc_ret( pCprbOut, MASTER_KEY_ERROR );
            return ;
        }

        break ;
}

```

```

case MK_SRDI_OPEN_ERROR :
    Cas_proc_retc ( pCprbOut, FT_MK_SRDI_OPENERR );
    return ;
    break ;

default :
    Cas_proc_retc ( pCprbOut, MASTER_KEY_MGR_ERROR );
    return ;
}

/*****
** Perform consistency check on the request parameter block
***/
if ( parm_block_valid( pCprbIn, SEL_REQ_BLK ) == false )
{
    Cas_proc_retc ( pCprbOut, RT_CONSISTENCY_ERROR );
    return ;
}

/*****
** OPTIONAL ----- depends on your CCA extension.
**
** Perform consistency check on the rule array - for this verb, the
** rule array always has one value.
***/
if ( pReqBlk->rule_array_length != ( sizeof(pReqBlk->rule_array_length)
                                     + sizeof(rule_array_element) ) )
{
    Cas_proc_retc( pCprbOut, E_RULE_ARRAY_CNT );
    return ;
}

/*****
** OPTIONAL ----- depends on your CCA extension.
**
** Compare for valid rule array values.
***/
RuleValue[0] = INVALID_RULE; /* rule_check requires this initialization.*/
RuleValue[1] = INVALID_RULE; /* rule_check requires this initialization.*/
RuleValue[2] = INVALID_RULE; /* rule_check requires this initialization.*/

if ( rule_check ( (RULE_BLOCK *) &pReqBlk->rule_array_length,
                  RuleMapCount,
                  &RuleMap[0], &RuleValue[0], &ReturnMsg )
    == false )
{
    Cas_proc_retc ( pCprbOut, ReturnMsg );
    return ;
}

/*****
** OPTIONAL ----- depends on your CCA extension.
**
** Perform consistency check on the verb unique data - for this verb,
** the verb unique data is not used.
***/
pVerbData = (verb_unique_data_structure *)
             ((UCHAR *) &(pReqBlk->rule_array_length) +
              pReqBlk->rule_array_length );

if ( pVerbData->verb_unique_data_length != NO_VERBDATA )
{
    Cas_proc_retc ( pCprbOut, E_SIZE );
    return ;
}

/*****
** OPTIONAL ----- depends on your CCA extension.
**
** Perform consistency check on the key block - there should be
** 1 or 2 key block fields for this verb.
***/

```

```

if ( find_first_key_block( pCprbIn,
                          (key_data_structure **) &pToken,
                          SEL_REQ_BLK ) == false )
{
    Cas_proc_retc ( pCprbOut, RT_CONSISTENCY_ERROR );    /* @pic */
    return ;
}

if ( find_next_key_block( pCprbIn,
                          (key_data_structure *) pToken,
                          (key_data_structure **) &pKeyBlockStruct,
                          SEL_REQ_BLK ) == true )
{
    pLabel = &(pKeyBlockStruct->label_or_token);
    KeyIdIsLabel = true;
}
else
    KeyIdIsLabel = false;

/*****
** OPTIONAL ---- depends on your CCA extension.
**
** Check for unexpected key label. When SECY cannot find the requested
** key storage record, the key label is forwarded.
*****/
pKeyBlock = (UCHAR *) &(( generic_key_block_structure *)
                          pToken->label_or_token );
if ( TOKEN_LABEL_CHECK( *pKeyBlock ) == TRUE )
{
    Cas_proc_retc ( pCprbOut, RT_KEYLABEL_NEXIST );
    return;
}

/*****
** OK, the input looks pretty good, but will the reply buffer hold the
** output from this CCA extension.
*****/
ReplyLength = pCprbIn->CPRB_length + sizeof(pReqBlk->subfunction_code) +
              ( 3 * sizeof(1thfield) ) + KEY_HDR_LEN + DES_TOKEN_LENGTH;

if ( pCprbIn->reply_parm_block_length < ReplyLength )
{
    Cas_proc_retc ( pCprbOut, BUFFER_LENGTH_ERROR );
    return ;
}

/*****
**
**
** Add code to perform the requested function.
**
*****/

/*****
** Build 4 parts in the following Reply Parameter Block.
**
** +-----+-----+-----//+-----+-----//+-----+-----//+
** |Sub-   |Rule Array   |Verb Unique   |Key Block
** |Function|   |   |   |   |   |   |   |   |   |   |   |   |   |   |
** |Code   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
** |-----|Length| Elements|Length| Data |Length| Fields |
** +-----+-----+-----//+-----+-----//+-----+-----//+
** 0       2     4       2+X  4+X   2+X+Y  4+X+Y
**
** |<-- 2 -->|<-- X ----->|<-- Y ----->|<-- Z ----->|
**
*****/

/*****
** Build the response for returning the re-enciphered key token.
*****/

```

```

pCprbOut->reply_parm_block = pReplyBlk ;
pReplyBlk->rule_array_length = NO_RULEARRAY ;

pVerbData = (verb_unique_data_structure *)
             ((UCHAR *) &pReplyBlk->rule_array_length +
              pReplyBlk->rule_array_length ) ;
pVerbData->verb_unique_data_length = NO_VERBDATA ;

pKeyBlock = ((UCHAR *) &pVerbData->verb_unique_data_length +
             pVerbData->verb_unique_data_length ) ;

ReplyBlockLength = BLOCK_LENGTH + NO_RULEARRAY + NO_VERBDATA;

if ( KeyIdIsLabel == true )
{
    KeyHeader.Length = KEY_HDR_LEN + KEY_LABEL_LEN + DES_TOKEN_LENGTH;
    KeyHeader.Flags = DES96_TYPE | ACTION_WRITE;

    ReplyBlockLength += BuildParmBlock( pKeyBlock,
                                       3,
                                       KEY_HDR_LEN, &KeyHeader,
                                       KEY_LABEL_LEN, pLabel,
                                       DES_TOKEN_LENGTH, pDesToken);
}
else
{
    KeyHeader.Length = KEY_HDR_LEN + DES_TOKEN_LENGTH;
    KeyHeader.Flags = DES96_TYPE | ACTION_NOOP;

    ReplyBlockLength += BuildParmBlock( pKeyBlock,
                                       2,
                                       KEY_HDR_LEN, &KeyHeader,
                                       DES_TOKEN_LENGTH, pDesToken);
}

/*****
** Set the replied parameter block length and return to caller.
*****/
pCprbOut->replied_parm_block_length = ReplyBlockLength;
return;

```

```

} /* end-of ccax_fcn_1() */

```

*udx\_ken1.c.*

---

## Appendix C. Moving a UDX from the Model 1 Card to the Model 2 Card

Because of the changes in the functionality of CCA, transferring code from a model 1 environment to a model 2 environment may require changes to the UDX code, particularly in the following segments:

---

### Master Key Manager Changes

For the model 2 PKA token structures, the verification pattern stored in the operational key is the 16-byte MDC4 hash of the master key. Thus, there are new master key structures which contain this 16-byte field as well as the 20-byte SHA-1 hash of the older PKA tokens. This has no effect on your UDX code unless you are building your own master keys. (The functions provided (combine\_mk\_parts, load\_mk\_from\_shares, and so on) will take care of this automatically.)

Because of the separate verification pattern, separate master keys are stored for the PKA keys and the DES keys. The mk\_selectors structure has a new field, type\_mks, which may be one of SYM\_MK (for symmetric keys), ASYM\_MK (for PKA keys), BOTH\_MK (if you are using only one master key set). This structure must be updated/set if you are using any of the functions in Chapter 6, CCA Master Key Manager Functions, especially:

```
clear_master_keys
get_mk_verification_pattern
ede3_triple_decrypt_under_master_key_with_CV
ede3_triple_encrypt_under_master_key_with_CV
ede3_triple_decrypt_under_master_key_with_CV
ede3_triple_encrypt_under_master_key_with_CV
triple_decrypt_under_master_key
triple_encrypt_under_master_key
triple_decrypt_under_master_key_with_CV
triple_encrypt_under_master_key_with_CV
```

These functions already used the mk\_selectors parameter, so the structure will be filled improperly unless the code is changed.

All of other master key manager functions except init\_master\_keys() and reinit\_master\_keys() now take the mk\_selectors parameter. The functions used in the old toolkit are still available, however they map to the SYM\_MK keyset automatically. Any calls to these functions should be checked and if necessary, changed to use the appropriate set of keys. For example, if you are using PKA keys, you will want to replace any calls to generate\_random\_master\_key() with:

```
mk_selector.mk_set=MK_SET_DEFAULT;
mk_selector.mk_register = MK_NEW;
mk_selector.mk_type = ASYM_MK;
mkmGenerateRandomMK(mk_selector);
```

The KEY\_STORE\_MKVP\_TOKEN structure, the first structure in the key storage file, has changed (names only, not the actual byte information.) If you have written a function which sets up a key storage file which uses the CCA key storage structures, this will need to be changed.

The CPRB structure has changed (again, only in the names of the fields). Some fields which were included in reserved fields have been added to allow closer linkage with zSeries functions (domain, and so on). There will be no issues here as long as you have initialized the CPRB structure to 0x00 before filling, or use the CSUC\_BULDCPRB() function to fill the CPRB structure.

---

## Makefile Changes

The UDX toolkit for the Model 2 card uses a different set of basic library functions. When building the card-side portion of the UDX, it is important to link clib.lib from the ...\\UDXTK\002\lib\nt\msvc or ...\\UDXTK\002\lib\zSeries\msvc, or ...\\UDXTK\002\lib\nt\vac or ...\\UDXTK\002\lib\zSeries\vac directory, rather than scctk\002\lib\sccl\nt\msvcasm or scctk\002\lib\sccl\nt\vacppasm. Adjust your makefiles accordingly. The other scctk libraries may be included from the scctk library directories, as they were for the Model 1.

---

## Appendix D. Reserved Values

Certain values have been reserved for the use of UDX developers. IBM will not use these values in future upgrades to the CCA, so there will be no overlap between a UDX using these values and an upgrade of the toolkit. The specific values are as follows:

For completion codes: The values between 0x5000 and 0x5FFF have been reserved for UDX writers.

For access control points: For zSeries, the values between 0x8000 and 0xFFFF may be used. (Values between 0xF000 and 0xFFFF will be used on zSeries by IBM UDX writers.)

For subfunction codes: The values between "XA" (0x5841) to "XZ" (0x585A), "YA" (0x5941) to "YZ" (0x595A), "X0" (0x5830) to "X9" (0x5839), and "Y0" (0x5930) to "Y9" (0x5939) are reserved for UDX writers. The values between "WA" (0x5741) to "WZ" (0x575A) and "W0" (0x5730) to "W9" (0x5739) are also reserved for UDX writers. On the zSeries server, these values (beginning with "W") will be used by IBM UDX writers. On other platforms, they are available for all UDX writers.

For DES control vectors: Bits 4, 5, and 61 will not affect or be affected by the import or export of a key. Bits 4 and 5 will be ignored by the CCA at all times. Bit 61 will prevent a key from use in any standard CCA verb, thus reserving a key for use only in a UDX function.





## Appendix E. Data Structures

This appendix identifies useful data structures from the toolkit header files.

### Structures Used in Communications Between NT Host and Coprocessor

These structures may be used on the coprocessor or on the NT host machine. If you are writing code for the zSeries 4758, the host side instructions in this section will be useful only for building the NT test DLL.

A `REQUEST_REPLY_BUF` structure should be declared in the host function to allocate the data storage for the CPRB Structures and the request and reply buffers. This structure has two fields, both of 5120 bytes (`BLK_LEN_MAX`).

#### `REQUEST_REPLY_BUF`

| Field name               | Size of field | Purpose  |
|--------------------------|---------------|--|
| <code>request_buf</code> | 5120 bytes    | Holds the CPRB structure and the request block.        |
| <code>reply_buf</code>   | 5120 bytes    | Holds the (return) CPRB structure and the reply block. |

The `REQUEST_REPLY_BUF` structure is filled with the following structures (hence they are declared as pointers into the `REQUEST_REPLY_BUF` structure).

First, a CPRB structure:

Note that the (request) CPRB structure is filled (as completely as it needs to be) by calling `CSUC_BULDCPRB()` with the appropriate lengths and pointers from within the host function. Fields not filled by this function will be filled by the Security Server when the coprocessor is called. Within the coprocessor code, the output CPRB fields are filled by copying the values from the input CPRB. Changing the values of these fields is not recommended, except for the `replied_parm_block_length` and `replied_data_block_length` fields in the coprocessor code.

Changing the values in a "FILLED AUTOMATICALLY" field will have one of two effects:

1. SECY will overwrite the changed value with the correct value.
2. The call will fail because of an invalid value.

Since the `CPRB_structure` is used exclusively as a pointer into the `REQUEST_REPLY_BUF` structure, the type `CPRB_ptr` has been typedefed as a pointer to the `CPRB_structure`.

#### `CPRB_structure`, or `*CPRB_ptr`

| Field name               | Size/Type | Purpose   |
|--------------------------|-----------|---|
| <code>CPRB_length</code> | USHORT    | This field should contain D'112' (little endian). |

| Field name                | Size/Type         | Purpose   |
|---------------------------|-------------------|---|
| cprb_version_id           | 1 byte            | Flag indicating the version of this structure.  |
| MAC_content_flags         | 1 byte            | Flags for the message authentication function. FILLED AUTOMATICALLY                                 |
| SRPI_return_code          | unsigned long     | Return code from SECY.  |
| SRPI_verb_type            | 1 byte            | This field should have the value X'1' . FILLED AUTOMATICALLY  |
| reserved_1                | 1 byte            | This field should contain X'0'.   |
| function_id               | 2 bytes           | This field should contain 'T2'  |
| S390Checkpoint            | 1 byte            | FILLED AUTOMATICALLY.   |
| reserved_2                | 1 byte            | This field should contain X'0'.   |
| req_parm_block_length     | unsigned short    | Request parameter block length (little-endian).   |
| req_parm_block            | pointer (4 bytes) | Address of the request parameter block.   |
| req_data_block_length     | unsigned long     | Request data block length (little-endian)   |
| req_data_block_addr       | pointer (4 bytes) | Address of request data block.  |
| reply_parm_block_length   | unsigned short    | Reply parameter block length (little-endian)  |
| pad_001                   | unsigned short    | Number of bytes to pad to ensure proper alignment. FILLED AUTOMATICALLY. (little-endian)            |
| reply_parm_block          | pointer (4 bytes) | Address of reply parameter block.   |
| reply_data_block_length   | unsigned long     | Reply data block length (little-endian)   |
| reply_data_block          | pointer (4 bytes) | Address of reply data block   |
| secy_return_code          | unsigned long     | This is the returnCode]]reasonCode combination.   |
| replied_parm_block_length | unsigned short    | The length of the reply data returned from the coprocessor in the reply parameter block.            |
| MAC_data_length           | unsigned short    | The length of the data to be authenticated. FILLED AUTOMATICALLY. (little-endian)                   |
| replied_data_block_length | unsigned long     | The length of the reply data returned from the coprocessor in the reply DATA block. (little-endian) |
| requestor_id              | unsigned short    | ID of requestor FILLED BY ROUTER.   |
| resource_origin           | 8 bytes           | FILLED AUTOMATICALLY.   |

| Field name              | Size/Type      | Purpose  |
|-------------------------|----------------|--|
| MAC_value               | 4 bytes        | FILLED AUTOMATICALLY.  |
| logon_identifier        | 8 bytes        | FILLED AUTOMATICALLY.  |
| Domain                  | unsigned short | Usage/control domain. FILLED AUTOMATICALLY.                        |
| UsageDomainMask         | 4 bytes        | Usage domain mask. FILLED AUTOMATICALLY.                           |
| ControlDomainMask       | 4 bytes        | Control domain mask. FILLED AUTOMATICALLY.                         |
| S390EnforcementMask     | 4 bytes        | S390 Enforcement mask. FILLED AUTOMATICALLY.                       |
| reserved_for_requestors | 6 bytes        | Reserved for requestors. FILLED AUTOMATICALLY.                     |
| secy_name_length        | unsigned short | Length of the security server name (8 bytes) FILLED AUTOMATICALLY. |
| server_name             | 8 bytes        | Security server name ("SECY ") FILLED AUTOMATICALLY.               |

On the host side, you will only need one `CPRB_ptr`, since the request CPRB you build will be replaced by the reply CPRB from the coprocessor during the call to `CSNC_SP_SCSRFBSS( )`. On the coprocessor, two of the parameters for a command function are `pCprbIn`, and `pCprbOut`. Therefore, you do not need to declare either a `REQUEST_REPLY_BUF` or a `CPRB_ptr`.

Following the `CPRB_structure` in the buffer is a request block:

The `ESSS_request_block_structure` defines the structure for the request or reply block. Since request and reply blocks are variable length, this structure is used purely as a pointer into the `request_buf` or `reply_buf` field of the `REQUEST_REPLY_BUF` structure. `RBFPTR` is typedefed as a pointer to an `ESSS_request_block_structure`, and thus is more commonly used.

On the host side, you may want to declare an `RBFPTR` for the request buffer. On the coprocessor code, you may want to declare an `RBFPTR` for both the request buffer and the reply buffer.

#### **ESSS\_request\_block\_structure, or \*RBFPTR**

| Field name               | Size of field  | Purpose  |
|--------------------------|----------------|--|
| subfunction_code         | unsigned short | Holds the two-byte subfunction code in little-endian format.   |
| rule_array_length        | unsigned short | Total length of rule array and this field, in little-endian format.  |
| first_rule_array_element | 1 byte         | First character of first rule array element, if <code>rule_array_length</code> is greater than 2. Otherwise, this will be the first byte of the verb unique data length field. |

Filling the rule array is easy using the BuildParmBlock() function:

```
BuildParmBlock (ptr1,
                1,
                SIZE_OF_RULE * (*pRuleCount), pRuleArray);
```

To parse a rule array with the rule\_check( ) function, two more structures are used. A pointer to a RULE\_BLOCK is passed to the function to be parsed. Note that the rule array format within the ESSS\_request\_block structure is, in fact, a RULE\_BLOCK:

### RULE\_BLOCK

| Field name | Size/Type      | Purpose                                     |
|------------|----------------|---|
| length     | unsigned short | Total length of rule block. (little-endian) |
| data       | 80 bytes       | Up to 10 (8-byte) rules.                    |

The other structure required is a RULE\_MAP structure. This maps 8-byte strings into a value array, assigning a unique value to each string, and 1 or more strings to each position in the array, depending on mutual exclusion issues.

### RULE\_MAP

| Field name | Size/Type                              | Purpose   |
|------------|--|---|
| keyword    | 9 bytes (8 chars plus null terminator) | String to be matched in rule array.   |
| order_no   | 1 byte                                 | Group number: all rules which are mutually exclusive to each other will have the same group number. |
| map_value  | int (4 bytes)                          | The numeric value associated with this rule.  |

To check the values in the rule array, use the rule\_check() function:

```
rule_check((RULE_BLOCK *)&pReq->rule_array_length,
           sizeof(aRuleMap)/sizeof(RULE_MAP),
           aRuleMap,
           aRuleValue,
           &returnMessage);
```

Immediately following the rule array in the REQUEST\_REPLY\_BUF is the verb unique data. Two types of structures are supplied for working with verb unique data, the VUD\_DATA\_RECORD, which is a length/tag/data structure ( the data preceded by a DATA\_RECORD\_HEADER structure), and the verb\_unique\_data\_structure, which is a length/data structure.

### DATA\_RECORD\_HEADER

| Field name | Size           | Purpose                             |
|------------|----------------|-------------------------------------|
| Length     | unsigned short | Length of this verb data.           |
| Flag       | unsigned short | User defined: usually type of data. |

```
#define DATA_HEADER_LENGTH  sizeof( DATA_RECORD_HEADER )
```

If you want to use the length/tag/data format for your verb unique data, declare a `DATA_RECORD_HEADER` structure to place before the data, and use the `BuildParmBlock()` function to place it before the data.

```
BuildParmBlock(ptr,
               2,
               DATA_HEADER_LENGTH, &DataHeader,
               dataLength, &Data[0]);
```

The `FindFirstDataBlock()` function returns a pointer to a `VUD_DATA_RECORD`, so that you can access your data in this format easily:

### VUD\_DATA\_RECORD

| Field name | Size/Type      | Purpose                                   |
|------------|----------------|---|
| Length     | unsigned short | Length of this verb data                  |
| Flag       | unsigned short | See above <code>DATA_RECORD_HEADER</code> |
| Data       | 1 byte         | The first byte of the data.               |

```
FindFirstDataBlock(pCPRB, SEL_REPLY_BLK, &pVerbDataRecord);
if(pVerbDataRecord->Flag == EncryptedKey)
{
  memcpy(pKeyParameter, &pVerbDataRecord->Data,
         pVerbDataRecord->Length - DATA_HEADER_LENGTH);
}
```

On the other hand, if you have no need to access the `Flags` field, you can use the `verb_unique_data_structure` type instead:

### verb\_unique\_data\_structure

| Field name                           | Size/Type      | Purpose                    |
|--------------------------------------|----------------|----------------------------|
| <code>verb_unique_data_length</code> | unsigned short | Length of this verb data   |
| <code>verb_unique_data</code>        | 1 byte         | The first byte of the data |

```
BuildParmBlock(ptr,
               2,
               sizeof(short), &vudLength,
               dataLength, &Data);
```

To retrieve the above data, you must first cast the `verb_unique_data_structure` as a `VUD_DATA_RECORD`:

```
FindFirstDataBlock ( pCPRB, SEL_REPLY_BLK, (VUD_DATA_RECORD **)&pVerbUniqueDataStructure);
*pLengthParm = ntohs(pVerbUniqueDataStructure->
  verb_unique_data_length) - LENGTH_FIELD_SIZE;
memcpy(pReturnedData,
       &pVerbUniqueDataStructure->verb_unique_data, *pLengthParm);
```

If the only piece of data which is being passed has a fixed length (for example, if it is a structure), you need not use either of the verb structures shown:

```
BuildParmBlock(ptr,
               1,
               sizeof(Structure), &Structure);
```

Then to access the data:

```
FindFirstDataBlock(pCPRB, SEL_REPLY_BLOCK, (VUD_DATA_RECORD **) &pData);
memcpy(&Structure, pData, sizeof(Structure));
```

If you use this method, you must not pass more than one piece of verb unique data, as the FindNextDataBlock() function uses the length field to determine where to look for the next piece of data.

Following the verb unique data, the key data is organized into key fields and key data structures. Each key is preceded by a KEY\_FIELD\_HEADER structure:

### KEY\_FIELD\_HEADER

| Field name | Size/Type      | Purpose  |
|------------|----------------|--|
| Length     | unsigned short | Total length of this key block. (little-endian)                          |
| Flags      | unsigned short | Flags indication action required by the Security Server and type of key. |

On the host side, you will need to declare a KEY\_FIELD\_HEADER structure for each key you will be passing to the coprocessor. On the coprocessor, you will need to declare a KEY\_FIELD\_HEADER structure for each key you will be passing to the host. If you are passing a token to be written to the key storage file, you must declare *two* KEY\_FIELD\_HEADER structures, and pass first the label of the key to write to, then the key token to write into the key storage file.

```
BuildParmBlock(ptr,
               4, // 2 for each key you will be passing
               sizeof(KEY_FIELD_HEADER), &keyFieldHeader1,
               KEY_LABEL_LENGTH, keyLabel,
               sizeof(KEY_FIELD_HEADER), &keyFieldHeader2,
               keyTokenLength, keyToken);
```

The find\_first\_key\_block() function returns a pointer to a key\_data\_structure:

### key\_data\_structure

| Field name            | Size/Type      | Purpose                            |
|-----------------------|----------------|------------------------------------|
| key_field_data_length | unsigned short | Total length of this key data.     |
| key_data              | 1 byte         | First byte of keyFieldHeader.Flags |

Since there is no reason to access the first byte of the keyFieldHeader.Flags field, you will usually declare a generic\_key\_block\_structure pointer, and cast it as a key\_data\_structure in the function call.

### generic\_key\_block\_structure

| Field name     | Size/Type      | Purpose  |
|----------------|----------------|--|
| length         | unsigned short | Total length of this key data. (little-endian) |
| flags          | unsigned short | Flag bytes (little-endian) (ignore)            |
| label_or_token | 1 byte         | First byte of key token or label.              |

```

find_first_key_block(pCprb, (key_data_structure **)&pGenericKeyBlockStructure,SEL_REQ_BLK);
    keyLength = ntohs(pGenericKeyBlockStructure->length) -
        sizeof(KEY_FIELD_HEADER);
    pKeyToken = &pGenericKeyBlockStructure->label_or_token;

```

Notice that the value of the byte in the `label_or_token` field can be used in the macro `TOKEN_LABEL_CHECK` to determine whether the token is a key token with key data or the label of a key in key storage.

If the key which has been passed is an RSA key, some of the functions which manipulate and check it take parameters of type `RsaKeyTokenHeader`:

#### **RsaKeyTokenHeader**

| Field name  | Size/Type      | Purpose  |
|-------------|----------------|--|
| tokenId     | 1 byte         | Indicates Internal PKA, External PKA, Label, or "not RSA"  |
| version     | 1 byte         | Version of RSA token   |
| tokenLength | unsigned short | Total length of token (big-endian)   |
| reserved    | 4 bytes        | valued to 0  |
| nextSection | 1 byte         | First byte of next token section - indicates public or privateModexponent, private Chinese remainder, and so on. |

In most cases, you should simply cast the pointer to the token as an `RsaKeyTokenHeader` pointer.

---

## **Data Structures for Caching Functions**

Only one new data structure is required for the use of the cache functions, the `short_tag_t`:

#### **short\_tag\_t**

| Field name | Size/Type | Purpose   |
|------------|-----------|---|
| tag_1      | 1 byte    | First byte of 2 byte short tag, index into linked list of second bytes. |
| tag_2      | 1 byte    | Second byte of 2 byte short tag, index into linked list of entries.     |

You may choose to cast a 2-byte value as a `short_tag_t` for the function call.

## Other Useful Data Structures

The `mk_selectors` data structure is used to indicate which of several master keys to use in a given master key function.

### `mk_selectors`

| Field name               | Size/Type      | Purpose   |
|--------------------------|----------------|---|
| <code>mk_set</code>      | unsigned short | Domain of master key set:<br>MK_SET_DEFAULT   |
| <code>mk_register</code> | enumeration    | <code>old_mk</code> , <code>current_mk</code> , <code>new_mk</code> to determine which of the three registers to access.    |
| <code>type_mks</code>    | enumeration    | <code>SYM_MK</code> , <code>ASYM_MK</code> , <code>Both_MK</code> , to determine which type of master key to use or change. |

The `RsaRecoverClearKeyTokenUnderXport()` function requires a type of `double_length_key`.

### `double_length_key`

| Field name         | Size/Type | Purpose                |
|--------------------|-----------|------------------------|
| <code>left</code>  | 8 bytes   | First 8 bytes of key.  |
| <code>right</code> | 8 bytes   | Second 8 bytes of key. |

The functions `load_first_mk_part()` and `combine_mk_parts()` require a `TRIPLE_LENGTH_KEY`:

### `TRIPLE_LENGTH_KEY`

| Field name          | Size/Type | Purpose                |
|---------------------|-----------|------------------------|
| <code>first</code>  | 8 bytes   | First 8 bytes of key.  |
| <code>middle</code> | 8 bytes   | Second 8 bytes of key. |
| <code>last</code>   | 8 bytes   | Third 8 bytes of key.  |

The `dbl_ulong` (double, unsigned, long) data type is used to pass the number of bits of data for SHA1 hashing:

### `dbl_ulong`

| Field name         | Size/Type     | Purpose                              |
|--------------------|---------------|--------------------------------------|
| <code>upper</code> | unsigned long | The high-order 8 bytes of the value. |
| <code>lower</code> | unsigned long | The low-order 8 bytes of the value.  |



---

## Appendix F. Notices

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY, 10504-1785, USA.

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information that you supply in any way it believes appropriate without incurring any obligation to you.

**COPYRIGHT LICENSE:** This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

---

## Copying and Distributing Softcopy Files

For online versions of this book, we authorize you to:

- Copy, modify, and print the documentation contained on the media, for use within your enterprise, provided you reproduce the copyright notice, all warning statements, and other required statements on each copy or partial copy.
- Transfer the original unaltered copy of the documentation when you transfer the related IBM product (which may be either machines you own, or programs, if the program's license terms permit a transfer). You must, at the same time, destroy all other copies of the documentation.

You are responsible for payment of any taxes, including personal property taxes, resulting from this authorization.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Your failure to comply with the terms above terminates this authorization. Upon termination, you must destroy your machine readable documentation.

---

## Trademarks

The following terms are trademarks or registered trademarks of the IBM Corporation in the United States, or other countries, or both:

AIX  
IBM  
OS/2  
S/390

Intel is a registered trademark of Intel Corporation in the United States, or other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States, or other countries, or both.

SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

UNIX is a registered trademark in the United States, or other countries, or both and is licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be the trademarks or service marks of others.

---

## List of Abbreviations and Acronyms

|              |  |             |                                   |
|--------------|--|-------------|-----------------------------------|
| <b>AIX</b>   | Advanced Interactive Executive (operating system)  | <b>MAC</b>  | message authentication code       |
| <b>API</b>   | application program interface                      | <b>MKVP</b> | master key verification pattern   |
| <b>ASCII</b> | American Standard Code for Information Interchange | <b>NMK</b>  | new master key                    |
| <b>BBRAM</b> | battery-backed random access memory                | <b>OMK</b>  | old master key                    |
| <b>CCA</b>   | Common Cryptographic Architecture                  | <b>OS/2</b> | Operating System/2                |
| <b>CDMF</b>  | Commercial Data Masking Facility                   | <b>PCI</b>  | peripheral component interconnect |
| <b>CMK</b>   | current master key                                 | <b>PDF</b>  | portable document format          |
| <b>CP/Q</b>  | Control Program/Q                                  | <b>PIN</b>  | personal identification number    |
| <b>CPRB</b>  | Cooperative Processing Request Block               | <b>PKA</b>  | public key algorithm              |
| <b>DES</b>   | Data Encryption Standard                           | <b>PPD</b>  | program proprietary data          |
| <b>DLL</b>   | dynamic load library                               | <b>RAM</b>  | random access memory              |
| <b>EPROM</b> | erasable programmable read-only memory             | <b>RNG</b>  | random number generator           |
| <b>FIPS</b>  | Federal Information Processing Standard            | <b>RSA</b>  | Rivest-Shamir-Adleman (algorithm) |
| <b>KEK</b>   | key encrypting key                                 | <b>SCC</b>  | secure cryptographic coprocessor  |
| <b>IBM</b>   | International Business Machines                    | <b>SET</b>  | Secure Electronic Transaction     |
|              |  | <b>SHA</b>  | Secure Hash Algorithm             |
|              |  | <b>SRDI</b> | security relevant data item       |
|              |  | <b>TVV</b>  | token validation value            |
|              |  | <b>UDX</b>  | user-defined extensions           |
|              |  | <b>VUD</b>  | verb unique data                  |



## Glossary

This glossary includes terms and definitions from the *IBM Dictionary of Computing*, New York: McGraw Hill, 1994. This glossary also includes terms and definitions taken from:

- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42 Street, New York, New York 10036. Definitions are identified by the symbol (A) following the definition.
- The *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) following the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) following the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.

### A

**access.** In computer security, a specific type of interaction between a subject and an object that results in the flow of information from one to the other.

**access control.** Ensuring that the resources of a computer system can be accessed only by authorized users and in authorized ways.

**Advanced Interactive Executive (AIX) operating system.** The IBM implementation of the UNIX\*\* operating system.

**agent.** (1) An application that runs within the IBM 4758 PCI Cryptographic Coprocessor. (2) Synonym for *secure cryptographic coprocessor application*.

**AIX operating system.** Advanced Interactive Executive operating system.

**American National Standards Institute (ANSI).** An organization consisting of producers, consumers, and general interest groups that establishes the procedures by which accredited organizations create and maintain voluntary industry standards for the United States. (A)

**ANSI.** American National Standards Institute.

**API.** Application program interface.

**application program interface (API).** A functional interface supplied by the operating system, or by a separate program, that allows an application program written in a high-level language to use specific data or functions of the operating system or that separate program.

**authentication.** (1) A process used to verify the integrity of transmitted data, especially a message. (T) (2) In computer security, a process used to verify the user of an information system or protected resource.

**authorization.** (1) In computer security, the right granted to a user to communicate with or make use of a computer system. (T) (2) The process of granting a user either complete or restricted access to an object, resource, or function.

**authorize.** To permit or give authority to a user to communicate with or make use of an object, resource, or function.

### B

**battery-backed random access memory (BBRAM).** Random access memory that uses battery power to retain data while the system is powered off. The IBM 4758 PCI Cryptographic Coprocessor uses BBRAM to store persistent data for SCC applications, as well as the coprocessor device key.

**BBRAM.** Battery-backed random access memory.

### C

**call.** The action of bringing a computer program, a routine, or a subroutine into effect, usually by specifying the entry conditions and jumping to an entry point. (I) (A)

**card.** (1) An electronic circuit board that is plugged into an expansion slot of a system unit. (2) A plug-in circuit assembly.

**CBC.** Cipher Block Chain.

**CCA.** Common Cryptographic Architecture.

**CDMF algorithm.** Commercial Data Masking Facility algorithm.

**ciphertext.** (1) Data that has been altered by any cryptographic process. (2) See *clear data*.

**cipher block chain (CBC).** A mode of operation that cryptographically connects one block of ciphertext to the next clear data block.

**cleartext.** (1) Data that has not been altered by any cryptographic process. (2) See *clear data*. (3) See also *ciphertext*.

**clear data.** Data that is not enciphered.

**Commercial Data Masking Facility (CDMF) algorithm.** An algorithm for data confidentiality applications; it is based on the DES algorithm and has an effective key strength of 40 bits.

**Common Cryptographic Architecture (CCA).** A comprehensive set of cryptographic services that furnishes a consistent approach to cryptography on major IBM computing platforms. Application programs can access these services through the CCA application program interface.

**Common Cryptographic Architecture (CCA) API.** The application program interface used to call Common Cryptographic Architecture functions; it is described in the *IBM 4758 PCI Cryptographic Coprocessor CCA Basic Services Reference and Guide*.

**Control Program/Q (CP/Q).** The operating system embedded within the IBM 4758 PCI Cryptographic Coprocessor. The version of CP/Q used by the coprocessor—including extensions to support cryptographic and security-related functions—is known as CP/Q++.

**coprocessor.** (1) A supplementary processor that performs operations in conjunction with another processor. (2) A microprocessor on an expansion card that extends the address range of the processor in the host system, or adds specialized instructions to handle a particular category of operations; for example, an I/O coprocessor, math coprocessor, or a network coprocessor.

**CP/Q.** Control Program/Q.

**Cryptographic Coprocessor (IBM 4758).** An expansion card that provides a comprehensive set of cryptographic functions to a workstation.

**cryptography.** (1) The transformation of data to conceal its meaning. (2) In computer security, the principles, means, and methods used to transform data.

## D

**data encrypting key.** (1) A key used to encipher, decipher, or authenticate data. (2) Contrast with *key-encrypting key*.

**Data Encryption Standard (DES).** The National Institute of Standards and Technology (NIST) Data Encryption Standard, adopted by the U.S. government as Federal Information Processing Standard (FIPS) Publication 46, which allows only hardware implementation of the data encryption algorithm.

**decipher.** (1) To convert enciphered data into clear data. (2) Contrast with *encipher*.

**DES.** Data Encryption Standard.

## E

**encipher.** (1) To scramble data or convert it to a secret code that masks its meaning. (2) Contrast with *decipher*.

**enciphered data.** (1) Data whose meaning is concealed from unauthorized users or observers. (2) See also *ciphertext*.

**EPROM.** Erasable programmable read-only memory.

**erasable programmable read-only memory (EPROM).** Programmable read-only memory that can be erased by a special process and reused.

## F

**feature.** A part of an IBM product that can be ordered separately from the essential components of the product.

**Federal Information Processing Standard (FIPS).** A standard that is published by the US National Institute of Science and Technology.

**FIPS.** Federal Information Processing Standard

**flash memory.** A specialized version of erasable programmable read-only memory (EPROM) commonly used to store code in small computers.

## H

**host.** As regards to the IBM 4758 PCI Cryptographic Coprocessor, the workstation into which the coprocessor is installed.

**I**

**interface.** (1) A boundary shared by two functional units, as defined by functional characteristics, signal characteristics, or other characteristics as appropriate. The concept includes specification of the connection between two devices having different functions. (T) (2) Hardware, software, or both that links systems, programs, and devices.

**K**

**key.** In computer security, a sequence of symbols used with an algorithm to encipher or decipher data.

**L****M**

**MAC.** Message authentication code.

**master key.** In computer security, the top-level key in a hierarchy of KEKs.

**message authentication code (MAC).** In computer security, (1) a number or value derived by processing data with an authentication algorithm, (2) the cryptographic result of block cipher operations, on text or data, using the cipher block chain (CBC) mode of operation.

**N**

**NT.** See *Windows NT*.

**O**

**Operating System/2 (OS/2).** An IBM operating system for personal computers.

**OS/2.** Operating System/2.

**P**

**PKA.** Public key algorithm.

**PPD.** Program proprietary data.

**private key.** (1) In computer security, a key that is known only to the owner and used with a public key algorithm to decipher data. Data is enciphered using the related public key. (2) Contrast with *public key*. (3) See also *public key algorithm*.

**procedure call.** In programming languages, a language construct for invoking execution of a procedure. (I) A procedure call usually includes an entry name and the applicable parameters.

**program proprietary data (PPD).** Persistent data stored within the IBM 4758 PCI Cryptographic Coprocessor flash memory or battery-backed RAM that is associated with a particular agent.

**public key.** (1) In computer security, a key that is widely known and used with a public key algorithm to encipher data. The enciphered data can be deciphered only with the related private key. (2) Contrast with *private key*. (3) See also *public key algorithm*.

**public key algorithm (PKA).** (1) In computer security, an asymmetric cryptographic process that uses a public key to encipher data and a related private key to decipher data. (2) See also *RSA algorithm*.

**R**

**RAM.** Random access memory.

**random access memory (RAM).** A storage device into which data is entered and from which data is retrieved in a non-sequential manner.

**random number generator (RNG).** A system designed to output values that cannot be predicted. Since software-based systems generate predictable, pseudo-random values, the IBM 4758 PCI Cryptographic Coprocessor uses a hardware-based system to generate true random values for cryptographic use.

**return code.** (1) A code used to influence the execution of succeeding instructions. (A) (2) A value returned to a program to indicate the results of an operation requested by that program.

**RNG.** Random number generator.

**RSA algorithm.** A public key encryption algorithm developed by R. Rivest, A. Shamir, and L. Adleman.

**S**

**SCC.** Secure cryptographic coprocessor.

**secure cryptographic coprocessor (SCC).** An alternate name for the IBM 4758 PCI Cryptographic Coprocessor. The abbreviation "SCC" is used within the product software code.

**secure cryptographic coprocessor (SCC) application.** (1) An application that runs within the

IBM 4758 PCI Cryptographic Coprocessor.  
(2) Synonym for *agent*.

**security.** The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

## T

## U

**utility program.** A computer program in general support of computer processes.(T)

## V

**verb.** A function possessing an *entry\_point\_name* and a fixed-length parameter list. The procedure call for a verb uses the syntax standard to programming languages.

## W

**Windows NT.** A Microsoft operating system for personal computers.

## Numerics

**IBM 4758.** IBM 4758 PCI Cryptographic Coprocessor.



# Index

## Numerics

2-byte values, convert 13-6

## A

ac\_check\_authorization 11-5  
 ac\_chg\_prof\_auth\_data 11-6  
 ac\_chg\_prof\_exp\_date 11-8  
 ac\_del\_profile 11-9  
 ac\_del\_role 11-10  
 ac\_get\_list\_sizes 11-11  
 ac\_get\_profile 11-12  
 ac\_get\_role 11-13  
 ac\_init 11-14  
 ac\_list\_profiles 11-15  
 ac\_list\_roles 11-16  
 ac\_load\_profiles 11-17  
 ac\_load\_roles 11-19  
 ac\_lu\_add\_user 11-20  
 ac\_lu\_drop\_user 11-21  
 ac\_lu\_get\_ks 11-22  
 ac\_lu\_get\_num\_users 11-23  
 ac\_lu\_get\_role 11-24  
 ac\_lu\_ks\_dec 11-25  
 ac\_lu\_ks\_enc 11-26  
 ac\_lu\_ks\_hmacgen 11-27  
 ac\_lu\_ks\_hmacver 11-28  
 ac\_lu\_ks\_macgen 11-29  
 ac\_lu\_ks\_macver 11-30  
 ac\_lu\_list\_users 11-31  
 ac\_lu\_query\_user 11-32  
 ac\_query\_profile 11-33  
 ac\_query\_role 11-34  
 ac\_reinit 11-35  
 ac\_reset\_logon\_fail\_cnt 11-36  
 Access Control Manager functions  
   ac\_check\_authorization 11-5  
   ac\_chg\_prof\_auth\_data 11-6  
   ac\_chg\_prof\_exp\_date 11-8  
   ac\_del\_profile 11-9  
   ac\_del\_role 11-10  
   ac\_get\_list\_sizes 11-11  
   ac\_get\_profile 11-12  
   ac\_get\_role 11-13  
   ac\_init 11-14  
   ac\_list\_profiles 11-15  
   ac\_list\_roles 11-16  
   ac\_load\_profiles 11-17  
   ac\_load\_roles 11-19  
   ac\_lu\_add\_user 11-20  
   ac\_lu\_drop\_user 11-21

## Access Control Manager functions (*continued*)

ac\_lu\_get\_ks 11-22  
 ac\_lu\_get\_num\_users 11-23  
 ac\_lu\_get\_role 11-24  
 ac\_lu\_ks\_dec 11-25  
 ac\_lu\_ks\_enc 11-26  
 ac\_lu\_ks\_hmacgen 11-27  
 ac\_lu\_ks\_hmacver 11-28  
 ac\_lu\_ks\_macgen 11-29  
 ac\_lu\_ks\_macver 11-30  
 ac\_lu\_list\_users 11-31  
 ac\_lu\_query\_user 11-32  
 ac\_query\_profile 11-33  
 ac\_query\_role 11-34  
 ac\_reinit 11-35  
 ac\_reset\_logon\_fail\_cnt 11-36  
 acm\_xlt\_errorcode 11-37  
 access control points, defining 2-7  
 acm\_xlt\_errorcode 11-37  
 adapter interface 1-4  
 adjust parity 8-4  
 architecture of the UDX environment 1-1  
 authority, user 13-2

## B

building a CCA user-defined extension 2-1  
 building a CPRB in the host 4-9  
 building a parameter block 4-2  
 building a UDX 2-1  
 BuildParmBlock 4-2

## C

cache management functions  
   cache\_clear 12-3  
   cache\_delete 12-4  
   cache\_delete\_item 12-5  
   cache\_get\_item 12-6  
   cache\_get\_item\_b 12-7  
   cache\_init 12-8  
   cache\_status 12-9  
   cache\_write\_item 12-10  
   overview 12-1  
 cache\_clear 12-3  
 cache\_delete 12-4  
 cache\_delete\_item 12-5  
 cache\_get\_item 12-6  
 cache\_get\_item\_b 12-7  
 cache\_init 12-8  
 cache\_status 12-9

cache\_write\_item 12-10  
 caching functions, data structures E-7  
 calculate token validation value 9-30  
 CalculatenWordLength 9-6  
 callable functions  
   ac\_check\_authorization 11-5  
   ac\_chg\_prof\_auth\_data 11-6  
   ac\_chg\_prof\_exp\_date 11-8  
   ac\_del\_profile 11-9  
   ac\_del\_role 11-10  
   ac\_get\_list\_sizes 11-11  
   ac\_get\_profile 11-12  
   ac\_get\_role 11-13  
   ac\_init 11-14  
   ac\_list\_profiles 11-15  
   ac\_list\_roles 11-16  
   ac\_load\_profiles 11-17  
   ac\_load\_roles 11-19  
   ac\_lu\_add\_user 11-20  
   ac\_lu\_drop\_user 11-21  
   ac\_lu\_get\_ks 11-22  
   ac\_lu\_get\_num\_users 11-23  
   ac\_lu\_get\_role 11-24  
   ac\_lu\_ks\_dec 11-25  
   ac\_lu\_ks\_enc 11-26  
   ac\_lu\_ks\_hmacgen 11-27  
   ac\_lu\_ks\_hmacver 11-28  
   ac\_lu\_ks\_macgen 11-29  
   ac\_lu\_ks\_macver 11-30  
   ac\_lu\_list\_users 11-31  
   ac\_lu\_query\_user 11-32  
   ac\_query\_profile 11-33  
   ac\_query\_role 11-34  
   ac\_reinit 11-35  
   ac\_reset\_logon\_fail\_cnt 11-36  
   acm\_xlt\_errorcode 11-37  
   BuildParmBlock 4-2  
   cache\_clear 12-3  
   cache\_delete 12-4  
   cache\_delete\_item 12-5  
   cache\_get\_item 12-6  
   cache\_get\_item\_b 12-7  
   cache\_init 12-8  
   cache\_status 12-9  
   cache\_write\_item 12-10  
   CalculatenWordLength 9-6  
   cas\_adjust\_parity 8-4  
   cas\_build\_default\_cv 8-5  
   cas\_build\_default\_token 8-6  
   cas\_current\_mkvp 8-8  
   cas\_des\_key\_token\_check 8-10  
   cas\_get\_key\_type 8-11  
   cas\_key\_length 8-12  
   cas\_key\_tokentvv\_check 8-13  
   cas\_master\_key\_check 8-14  
   cas\_old\_mkvp 8-9  
   callable functions (*continued*)  
   cas\_parity\_odd 8-16  
   Cas\_proc\_retc 4-6  
   CasBuildCv 8-5  
   CasBuildToken 8-6  
   CasCurrentMkvp 8-8  
   CasMasterKeyCheck 8-14  
   CasOldMkvp 8-9  
   check\_access\_auth\_fcn 13-2  
   clear\_master\_keys 6-6  
   close\_cca\_srds 10-8  
   combine\_mk\_parts 6-7  
   compute\_mk\_verification\_pattern 6-19  
   computeHMAC\_SHA1 7-2  
   create\_cca\_srds 10-9  
   create4update\_cca\_srds 10-11  
   CreateInternalKeyToken 9-7  
   CreateInternalKeyTokenWithMK 9-7  
   CreateRsaInternalSection 9-8  
   CreateRsaInternalSectionWithMK 9-8  
   CSNC\_SP\_SCSRFBSS 4-7  
   CSUC\_BULDCPRB 4-9  
   CSUC\_PROCRET 4-11  
   delete\_cca\_srds 10-12  
   delete\_KeyToken 9-9  
   do\_sha\_hash\_message 7-3  
   do\_sha\_hash\_msg\_to\_bfr 7-6  
   ede3\_triple\_decrypt\_under\_master\_key 6-26  
   ede3\_triple\_encrypt\_under\_master\_key 6-27  
   find\_first\_key\_block 4-14  
   find\_next\_key\_block 4-15  
   FindFirstDataBlock 4-12  
   FindNextDataBlock 4-13  
   generate\_dSig 9-12  
   generate\_mk\_shares 6-9  
   generate\_random\_mk 6-11  
   GenerateCcaRsaToken 9-10  
   GenerateRsaInternalToken 9-11  
   get\_cca\_srds\_length 10-13  
   get\_mk\_verification\_pattern 6-23  
   GetLength 9-14  
   GetKeyLength 13-4  
   getKeyToken 9-15  
   GetModulus 9-16  
   GetnBitLength 9-17  
   GetnByteLength 9-18  
   GetPublicExponent 9-19  
   GetRsaPrivateKeySection 9-20  
   GetRsaPublicKeySection 9-21  
   getSymmetricMaxModulusLength 5-2  
   GetTokenLength 9-22  
   hw\_sha\_hash\_message 7-7  
   init\_master\_keys 6-12  
   InitCprbParmPointers 4-16  
   intel\_long\_reverse 13-5  
   intel\_word\_reverse 13-6

callable functions (*continued*)

- isFunctionEnabled 5-3
- IsPrivateExponentEven 9-23
- IsPrivateKeyEncrypted 9-24
- IsPublicExponentEven 9-25
- IsRsaToken 9-26
- IsTokenInternal 9-27
- key register status 6-21
- keyword\_in\_rule\_array 4-17
- load\_first\_mk\_part 6-13
- load\_mk\_from\_shares 6-14
- mkmCombineMKParts 6-7
- mkmGenerateMKShares 6-9
- mkmGenerateRandomMK 6-11
- mkmGetAsymVerificationPattern 6-24
- mkmGetMasterKeyStatus 6-21
- mkmLoadFirstMKPart 6-13
- mkmLoadMKFromShares 6-14
- mkmSetMasterKey 6-17
- open\_cca\_srdi 10-14
- parm\_block\_valid 4-18
- pka96\_tvngen 9-30
- PkaHashQueryWithMK 9-28
- PkaMkvpQuery 9-29
- PkaMkvpQueryWithMK 9-29
- RecoverDesDataKey 8-17
- RecoverDesDataKeyWithMK 8-17
- RecoverDesKekImporter 8-19
- RecoverDesKekImporterWithMK 8-19
- RecoverPkaClearKeyTokenUnderMk 9-31
- RecoverPkaClearKeyTokenUnderMkWithMK 9-31
- RecoverPkaClearKeyTokenUnderXport 9-33
- ReEncipherPkaKeyToken 9-34
- ReEncipherPkaKeyTokenWithMK 9-34
- reinit\_master\_keys 6-16
- RequestRSACrypto 9-35
- resize\_cca\_srdi 10-15
- rule\_check 4-19
- saf\_process\_key\_label 4-23
- save\_cca\_srdi 10-16
- set\_master\_key 6-17
- sha\_hash\_message 7-9
- sha\_hash\_msg\_to\_bfr 7-12
- store\_KeyToken 9-36
- TDESDecryptUnderMasterKey 6-28
- TDESEncryptUnderMasterKey 6-29
- TokenMkvpMatchMasterKey 9-37
- triple\_decrypt\_under\_master\_key 6-30
- triple\_decrypt\_under\_master\_key\_with\_CV 6-31
- triple\_encrypt\_under\_master\_key 6-32
- triple\_encrypt\_under\_master\_key\_with\_CV 6-33
- update\_cca\_srdi 10-17
- ValidatePkaToken 9-38
- verify\_dSig 9-40
- VerifyKeyTokenConsistency 9-39
- cas\_adjust\_parity 8-4
- cas\_build\_default\_cv 8-5
- cas\_build\_default\_token 8-6
- cas\_current\_mkvp 8-8
- cas\_des\_key\_token\_check 8-10
- cas\_get\_key\_type 8-11
- cas\_key\_length 8-12
- cas\_key\_tokentvv\_check 8-13
- cas\_master\_key\_check 8-14
- cas\_old\_mkvp 8-9
- cas\_parity\_odd 8-16
- Cas\_proc\_retc 4-6
- CasBuildCv 8-5
- CasBuildToken 8-6
- CasCurrentMkvp 8-8
- CasMasterKeyCheck 8-14
- CasOldMkvp 8-9
- CCA communication structures 1-7
- chaining, SHA-1 hash 7-9
- check authorization, Access Control Manager function 11-5
- check key label 4-23
- CHECK\_ACCESS\_AUTH
  - See check\_access\_auth\_fcn
- check\_access\_auth\_fcn 13-2
- clear cache 12-3
- clear master key 6-6
- clear\_master\_keys 6-6
- close\_cca\_srdi 10-8
- code sample
  - coprocessor piece B-1
  - host piece A-1
- combine master key 6-7
- combine\_mk\_parts 6-7
- command processor 1-1, 1-7
- command processor API, defining 2-6
- command processor, identifier 1-3
- command processors to array, adding 2-7
- communication functions
  - BuildParmBlock 4-2
  - Cas\_proc\_retc 4-6
  - find\_first\_key\_block 4-14
  - find\_next\_key\_block 4-15
  - FindFirstDataBlock 4-12
  - FindNextDataBlock 4-13
  - InitCprbParmPointers 4-16
  - keyword\_in\_rule\_array 4-17
  - parm\_block\_valid 4-18
  - rule\_check 4-19
- communication structures, CCA 1-7
- communications, structures used between host and coprocessor E-1
- completion codes, defining new 2-4
- compute verification pattern, master key 6-19
- compute\_mk\_verification\_pattern 6-19

computeHMAC\_SHA1 7-2  
 control points 1-6  
 cooperative processing request/reply block (CPRB) 1-3  
 coprocessor piece of a UDX 2-6  
   adding command processors to the array 2-7  
   building the executable 2-8  
   defining access control points 2-7  
   defining the command processor API 2-6  
   designing and coding the logic 2-8  
 CPRB 1-3  
 CPRB parameter pointers, initialize 4-16  
 CPRB, building in the host 4-9  
 create\_cca\_srdi 10-9  
 create, master key 6-12  
 create4update\_cca\_srdi 10-11  
 CreateInternalKeyToken 9-7  
 CreateInternalKeyTokenWithMK 9-7  
 CreateRsaInternalSection 9-8  
 CreateRsaInternalSectionWithMK 9-8  
 CSNC\_SP\_SCSRFBSS 4-7  
 CSUC\_BULDCPRB 4-9  
 CSUC\_PROCRET 4-11  
 current master key verification pattern 8-8  
 CXT\_SAMP.C listing B-1

## D

data structures E-1  
   caching functions E-7  
   communications between host and computer E-1  
   other useful E-8  
 data structures, Access Control Manager 11-2  
   generic 11-3  
   profile 11-3  
   role 11-3  
   user information 11-4  
 data, clear from cache 12-3  
 decrypted private keys, cache 12-1  
 default control vector, build 8-5  
 default token, build 8-6  
 delete\_cca\_srdi 10-12  
 delete\_KeyToken 9-9  
 DES data key, recover 8-17  
 DES importer KEK, recover 8-19  
 DES key token, verify 8-10  
 DES utility functions  
   cas\_adjust\_parity 8-4  
   cas\_build\_default\_cv 8-5  
   cas\_build\_default\_token 8-6  
   cas\_current\_mkvp 8-8  
   cas\_des\_key\_token\_check 8-10  
   cas\_get\_key\_type 8-11  
   cas\_key\_length 8-12  
   cas\_key\_tokentvv\_check 8-13  
   cas\_master\_key\_check 8-14

DES utility functions (*continued*)  
   cas\_old\_mkvp 8-9  
   cas\_parity\_odd 8-16  
   CasBuildCv 8-5  
   CasBuildToken 8-6  
   CasCurrentMkvp 8-8  
   CasMasterKeyCheck 8-14  
   CasOldMkvp 8-9  
   RecoverDesDataKey 8-17  
   RecoverDesDataKeyWithMK 8-17  
   RecoverDesKekImporter 8-19  
   RecoverDesKekImporterWithMK 8-19  
 development overview 2-1  
 do\_sha\_hash\_message 7-3  
 do\_sha\_hash\_msg\_to\_bfr 7-6

## E

EDE3 triple decrypt master key 6-26  
 EDE3 triple encrypt master key 6-27  
 ede3\_triple\_decrypt\_under\_master\_key 6-26  
 ede3\_triple\_encrypt\_under\_master\_key 6-27  
 enabled function, check 5-3  
 entry points, exporting 2-5  
 examine parameter block 4-18  
 executable, building 2-8

## F

files  
   binary, used to produce a UDX 2-2  
   created by the developer 2-1  
   host 2-1  
   provided with UDX 2-1  
 files you use in building a UDX 2-1  
 find address of next key data block 4-15  
 find\_first\_key\_block 4-14  
 find\_next\_key\_block 4-15  
 FindFirstDataBlock 4-12  
 FindNextDataBlock 4-13  
 first data block, search for address 4-12  
 first key data block, search 4-14  
 format, key token 9-27  
 function control vector management functions  
   getSymmetricMaxModulusLength 5-2  
   isFunctionEnabled 5-3  
 functions  
   See callable functions

## G

generate random, master key 6-11  
 generate shares, master key 6-9  
 generate\_dSig 9-12  
 generate\_mk\_shares 6-9

generate\_random\_mk 6-11  
 GenerateCcaRsaToken 9-10  
 GenerateRsaInternalToken 9-11  
 get\_cca\_srDI\_length 10-13  
 get\_master\_key\_status 6-21  
 get\_mk\_verification\_pattern 6-23  
 GetLength 9-14  
 GetKeyLength 13-4  
 getKeyToken 9-15  
 GetModulus 9-16  
 GetnBitLength 9-17  
 GetnByteLength 9-18  
 GetPublicExponent 9-19  
 GetRsaPrivateKeySection 9-20  
 getSymmetricMaxModulusLength 5-2  
 GetTokenLength 9-22

## H

hardware, calculate SHA-1 hash 7-3  
 hash in hardware, compute SHA-1 7-7  
 hash of requested data, SHA-1 7-7  
 hash, calculate SHA-1 7-3  
 hash, SHA-1 wrapper 7-6  
 hashing functions, SHA-1 7-1  
 header files
 

- Access Control Manager functions 11-1
- Caching functions 12-1
- Communications functions 4-1
- DES utility functions 8-1
- Function Control Vector functions 5-1
- Master Key Manager functions 6-1
- Miscellaneous functions 13-1
- RSA functions 9-1
- SHA-1 functions 7-1
- SRDI Manager functions 10-1

 HMAC-SHA1, computing 7-2  
 host piece of the UDX 2-3
 

- building the DLL and LIB files 2-5
- defining new completion codes 2-4
- defining the API 2-3
- defining the subfunction code 2-3
- designing and coding the logic 2-5
- exporting the API entry points 2-5

 hw\_sha\_hash\_message 7-7

## I

init\_master\_keys 6-12  
 InitCprbParmPointers 4-16  
 initialize CPRB parameter pointers 4-16  
 initialize master key 6-12  
 initialize the Access Control Manager 11-14  
 intel\_long\_reverse 13-5  
 intel\_word\_reverse 13-6

internal key token, create 9-7  
 isFunctionEnabled 5-3  
 IsPrivateExponentEven 9-23  
 IsPrivateKeyEncrypted 9-24  
 IsPublicExponentEven 9-25  
 IsRsaToken 9-26  
 IsTokenInternal 9-27

## K

key block 1-4  
 key blocks 1-3  
 key label 1-4  
 key label, checking and processing 4-23  
 key length, return 8-12  
 key record 1-4  
 key storage server 1-4  
 key token 1-4
 

- consistency, verify 9-39
- format 9-27
- length 9-22, 13-4
- signature 9-40

 key type, return 8-11  
 keyword\_in\_rule\_array 4-17

## L

load first part, master key 6-13  
 load shares, master key 6-14  
 load\_first\_mk\_part 6-13  
 load\_mk\_from\_shares 6-14  
 logged on users, Access Control Manager
 

- add to list 11-20
- copy session key 11-22
- list 11-31
- number of 11-23
- query 11-32
- remove 11-21
- role 11-24

 logic, designing and coding 2-5, 2-8  
 logon failure count, reset (Access Control Manager) 11-36  
 long values, convert 13-5

## M

Master Key Manager (CCA) functions
 

- clear\_master\_keys 6-6
- combine\_mk\_parts 6-7
- common processing 6-3
- compute\_mk\_verification\_pattern 6-19
- ede3\_triple\_decrypt\_under\_master\_key 6-26
- ede3\_triple\_encrypt\_under\_master\_key 6-27
- generate\_mk\_shares 6-9
- generate\_random\_mk 6-11
- get\_master\_key\_status 6-21

Master Key Manager (CCA) functions (*continued*)

- get\_mk\_verification\_pattern 6-23
- initialization of the SRDI 6-2
- initializing the SRDI 6-12
- key register status 6-2, 6-21
- load\_first\_mk\_part 6-13
- load\_mk\_from\_shares 6-14
- location 6-2
- master key registers 6-1
- mkmCombineMKParts 6-7
- mkmGenerateMKShares 6-9
- mkmGenerateRandomMK 6-11
- mkmGetAsymVerificationPattern 6-24
- mkmGetMasterKeyStatus 6-21
- mkmLoadFirstMKPart 6-13
- mkmLoadMKFromShares 6-14
- mkmSetMasterKey 6-17
- overview 6-1
- reinitializing 6-16
- required variables 6-3
- set\_master\_key 6-17
- TDESDecryptUnderMasterKey 6-28
- TDESEncryptUnderMasterKey 6-29
- test encryption 9-37
- triple\_decrypt\_under\_master\_key 6-30
- triple\_decrypt\_under\_master\_key\_with\_CV 6-31
- triple\_encrypt\_under\_master\_key 6-32
- triple\_encrypt\_under\_master\_key\_with\_CV 6-33
- variables, required 6-3
- verification pattern 6-2
- version 9-29
- version check 8-14
- master key status 6-21
- master key, return version 9-28
- master key, set 6-17
- miscellaneous functions
  - Cas\_proc\_retch 4-6
  - check\_access\_auth\_fcn 13-2
  - GetKeyLength 13-4
  - intel\_long\_reverse 13-5
  - intel\_word\_reverse 13-6
  - TOKEN\_IS\_A\_LABEL 13-7
  - TOKEN\_LABEL\_CHECK 13-8
- mkmCombineMKParts 6-7
- mkmGenerateMKShares 6-9
- mkmGenerateRandomMK 6-11
- mkmGetAsymVerificationPattern 6-24
- mkmGetMasterKeyStatus 6-21
- mkmLoadFirstMKPart 6-13
- mkmLoadMKFromShares 6-14
- mkmSetMasterKey 6-17
- model 1 card to model 2 card, transferring code C-1
- moving UDX from model 1 card to model 2 card C-1
  - makefile changes C-2
  - Master Key Manager changes C-1

**N**

- next data block, search for address 4-13
- next key data block, find address 4-15

**O**

- old master key verification pattern 8-9
- open\_cca\_srDI 10-14
- overview of cache functions 12-1
- overview, development 2-1

**P**

- parameter block
  - building 4-2
  - examine 4-18
  - verify 4-18
- parity, adjust 8-4
- parity, verify 8-16
- parm\_block\_valid 4-18
- parts, master key 6-7
- PKA clear key
  - clear under DES export key, recover 9-33
  - re-encipher 9-34
  - recover under master key 9-31
- pka96\_tvvgen 9-30
- PkaHashQueryWithMK 9-28
- PkaMkvpQuery 9-29
- PkaMkvpQueryWithMK 9-29
- private key encryption, verify 9-24
- private key, return 9-20
- process key label 4-23
- public exponent, extract and copy 9-19
- public key, return 9-21
- publications, related xiii

**R**

- recover DES data key 8-17
- recover DES importer KEK 8-19
- RecoverDesDataKey 8-17
- RecoverDesDataKeyWithMK 8-17
- RecoverDesKekImporter 8-19
- RecoverDesKekImporterWithMK 8-19
- RecoverPkaClearKeyTokenUnderMk 9-31
- RecoverPkaClearKeyTokenUnderMkWithMK 9-31
- RecoverPkaClearKeyTokenUnderXport 9-33
- ReEncipherPkaKeyToken 9-34
- ReEncipherPkaKeyTokenWithMK 9-34
- reinit\_master\_keys 6-16
- reinitialize master key 6-16
- reinitialize the Access Control Manager 11-35
- related publications xiii
- reply parameter block 1-3
- request and reply blocks, format 1-8

- request parameter block 1-3
  - request, sending to the coprocessor 4-7
  - requested data SHA-1 hash 7-7
  - RequestRSACrypto 9-35
  - reserved values D-1
  - reset logon failure count, Access Control Manager 11-36
  - resize\_cca\_srди 10-15
  - return code, prioritize 4-6, 4-11
  - return key length 8-12
  - return key type 8-11
  - return master key version 9-28
  - role, Access Control Manager
    - delete 11-10
    - get information 11-13
    - length 11-34
    - list 11-16
    - load 11-19
    - size of profile list 11-11
  - RSA functions
    - CalculatenWordLength 9-6
    - CreateInternalKeyToken 9-7
    - CreateInternalKeyTokenWithMK 9-7
    - CreateRsaInternalSection 9-8
    - CreateRsaInternalSectionWithMK 9-8
    - delete\_KeyToken 9-9
    - generate\_dSig 9-12
    - GenerateCcaRsaToken 9-10
    - GenerateRsaInternalToken 9-11
    - GetLength 9-14
    - getKeyToken 9-15
    - GetModulus 9-16
    - GetnBitLength 9-17
    - GetnByteLength 9-18
    - GetPublicExponent 9-19
    - GetRsaPrivateKeySection 9-20
    - GetRsaPublicKeySection 9-21
    - GetTokenLength 9-22
    - IsPrivateExponentEven 9-23
    - IsPrivateKeyEncrypted 9-24
    - IsPublicExponentEven 9-25
    - IsRsaToken 9-26
    - IsTokenInternal 9-27
    - overview 9-4
    - pka96\_tvngen 9-30
    - PkaHashQueryWithMK 9-28
    - PkaMkvpQuery 9-29
    - PkaMkvpQueryWithMK 9-29
    - RecoverPkaClearKeyTokenUnderMk 9-31
    - RecoverPkaClearKeyTokenUnderMkWithMK 9-31
    - RecoverPkaClearKeyTokenUnderXport 9-33
    - ReEncipherPkaKeyToken 9-34
    - ReEncipherPkaKeyTokenWithMK 9-34
    - RequestRSACrypto 9-35
    - store\_KeyToken 9-36
    - TokenMkvpMatchMasterKey 9-37
  - RSA functions (*continued*)
    - ValidatePkaToken 9-38
    - verify\_dSig 9-40
    - VerifyKeyTokenConsistency 9-39
  - RSA internal section, create 9-8
  - RSA key
    - format 9-27
    - generate 9-11
    - generate CCA RSA key token 9-10
    - length 5-2, 9-22, 13-4
    - validate 9-38
    - verify 9-26, 9-39
    - verify signature 9-40
  - RSA modulus
    - bit length 9-17
    - byte length 9-18
    - extract and copy 9-16
  - RSA operation, perform 9-35
  - RSA private exponent, verify 9-23
  - RSA public exponent
    - byte length 9-14
    - generate\_dSig 9-12
    - get PKA token 9-15
    - verify 9-25
  - rule array
    - CSNBPKI 4-20
      - rule map example 4-21
    - CSUAACI 4-21
      - rule map example 4-21
    - verify 4-19
  - rule array keyword, search 4-17
  - rule\_check 4-19
- S**
- saf\_process\_key\_label 4-23
  - save\_cca\_srди 10-16
  - SCC API functions
    - coprocessor-side API functions 3-1
    - host-side API functions 3-1
  - search for first key data block 4-14
  - security relevant data items 1-1
  - security server, SECY 1-4
  - SECY 1-4
  - sending a request to the coprocessor 4-7
  - session key, Access Control Manager
    - compute a MAC 11-29
    - compute HMAC using Session key 11-27
    - decrypt data 11-25
    - encrypt data 11-26
    - translate ACM error code 11-37
    - verify a MAC 11-30
    - verify HMAC using Session key 11-28
  - set master key 6-17
  - set\_master\_key 6-17

## SHA-1 functions

- computeHMAC\_SHA1 7-2
- do\_sha\_hash\_message 7-3
- do\_sha\_hash\_msg\_to\_bfr 7-6
- hw\_sha\_hash\_message 7-7
- sha\_hash\_message 7-9
- sha\_hash\_msg\_to\_bfr 7-12

SHA-1 hash 7-3, 7-6, 7-7, 7-9, 7-12

SHA-1, compute an HMAC 7-2

sha\_hash\_message 7-9

sha\_hash\_msg\_to\_bfr 7-12

shares, master key 6-9

software, calculate SHA-1 hash 7-3

## SRDI 1-1

- close 10-8
- create 10-9, 10-11
- delete 10-12
- files 11-2
- length 10-13
- open 10-14
- resize 10-15
- save 10-16
- update 10-17

## SRDI Manager (CCA) functions

- close\_cca\_srди 10-8
- concurrent access protection 10-6
- create\_cca\_srди 10-9
- create4update\_cca\_srди 10-11
- delete\_cca\_srди 10-12
- example code 10-18
- get\_cca\_srди\_length 10-13
- open\_cca\_srди 10-14
- opening an SRDI, example 10-4
- operation 10-3
- overview 10-1
- resize\_cca\_srди 10-15
- save\_cca\_srди 10-16
- semaphore to control concurrent access 10-6
- update\_cca\_srди 10-17

status, master key 6-21

store\_KeyToken 9-36

structures, data E-1

structures, data (Access Control Manager) 11-2

- generic 11-3
- profile 11-3
- role 11-3

- user information 11-4

sub-function code 1-3

subfunction code, defining 2-3

SXT\_SAMP.C listing A-1

**T**

TDESDecryptUnderMasterKey 6-28

TDESEncryptUnderMasterKey 6-29

test encryption of master key 9-37

token validation value, calculate 9-30

token validation value, verify 8-13

TOKEN\_IS\_A\_LABEL 13-7

TOKEN\_LABEL\_CHECK 13-8

TokenMkvpMatchMasterKey 9-37

transferring code from model 1 to model 2 C-1

triple decrypt

- master key 6-30

- master key with CV 6-31

triple DES decrypt data using a master key 6-28

triple DES encrypt data under master key 6-29

triple encrypt

- master key 6-32

- master key with CV 6-33

triple\_decrypt\_under\_master\_key 6-30

triple\_decrypt\_under\_master\_key\_with\_CV 6-31

triple\_encrypt\_under\_master\_key 6-32

triple\_encrypt\_under\_master\_key\_with\_CV 6-33

**U**

UDX environment 1-1

update\_cca\_srди 10-17

user authority, verify 13-2

**V**

ValidatePkaToken 9-38

values, reserved D-1

verb unique data 1-3

verification pattern

- current master key 8-8

- old master key 8-9

- specified master key 6-23, 6-24

verify parameter block 4-18

verify rule array 4-19

verify\_dSig 9-40

VerifyKeyTokenConsistency 9-39

version check, master key 8-14

version, master key 9-28, 9-29

VUD 1-3

**W**

word length of modulus, return 9-6

wrapper, SHA-1 hash 7-6, 7-12