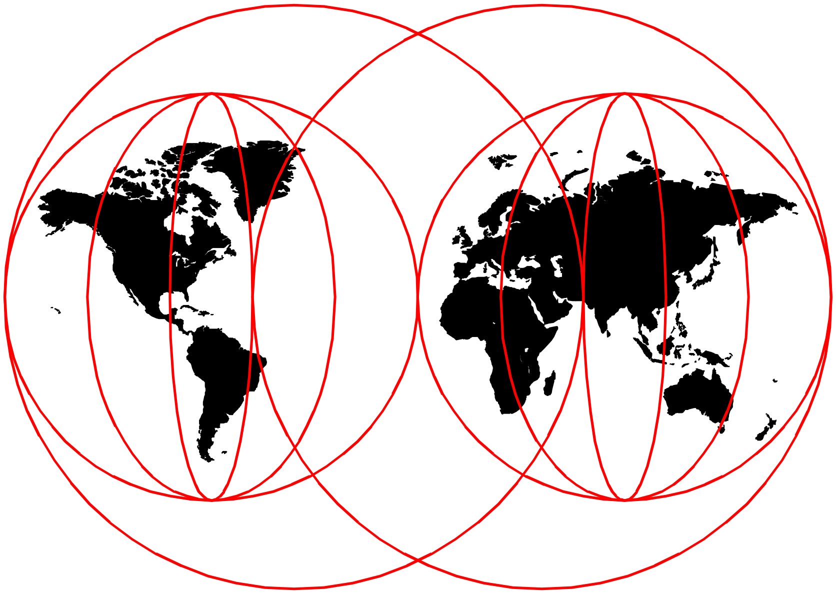
S/390 Crypto PCI Implementation Guide

Moon Kim, Pekka Hanninen, Patrick Kappeler, Robert Malaval, Peter Quizau, Zacharie Zanni



International Technical Support Organization

www.redbooks.ibm.com

SG24-5942-00

SG24-5942-00

International Technical Support Organization

S/390 Crypto PCI Implementation Guide

June 2000

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix D, “Special notices” on page 151.

First Edition (June 2000)

This edition applies to the IBM S/390 Cryptographic Coprocessor (Feature Code 0860) and OS/390 Version 2 Release 9 (Program Number 5647-A01).

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HYJ Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

Contents

Figures vii

Tables xi

Preface xiii
The team that wrote this redbook xiii
Comments welcome xiv

Chapter 1. Introduction 1
1.1 IBM Cryptographic Common Architecture (CCA) 1
1.2 CCA key management functions 1
1.3 Implementation of the CCA key management concepts in S/390 3
1.3.1 S/390 Cryptographic Coprocessor Facility (CCF) 3
1.3.2 S/390 PCI Cryptographic Coprocessor (PCICC) 3
1.4 S/390 integrated cryptography implementation 3
1.4.1 S/390 integrated cryptography implementation 4
1.4.2 Enablement of the cryptographic coprocessors 6
1.4.3 LPAR domains and TKE 6
1.5 Industry standards for cryptographic modules 8

Chapter 2. PCICC product overview 9
2.1 Description of hardware 9
2.1.1 Introduction to the S/390 PCI Cryptographic Coprocessor 9
2.1.2 PCICC data flow 12
2.1.3 PCICC card: physical security, handling, and shipping 15
2.2 Adjunct Processor (AP) management 18
2.2.1 Introduction to Adjunct Processor architecture 18
2.2.2 AP management and PCICC initialization 19
2.3 PCICC microcode load 21
2.3.1 The IBM 4758 CCA application 21
2.3.2 The software hierarchy in the coprocessor 22
2.3.3 PCICC microcode patches 23
2.3.4 Function Control Vector (FCV) enablement 24
2.4 OS/390 2.9 and the Integrated Cryptographic Services Facility (ICSF)25
2.4.1 OS/390 2.9 support for PCICC 25
2.4.2 ICSF overview 25
2.4.3 New SMF Record Type 82 subtypes 29
2.4.4 The new TKE workstation (TKE V3.0) 30

Chapter 3. Planning 31
3.1 Hardware requirements 31

3.2 Feature codes 31
3.3 The PCICC installation task 33
3.3.1 Our installation 33
3.3.2 Concurrent installation of the PCICC 35
3.3.3 Adding a second PCICC. 36
3.3.4 Removing one PCICC 38
3.4 The 9672 channel. 41
3.4.1 The 9672 G6 internal structure 41
3.4.2 The 9672 channel plugging rules 44
3.4.3 I/O cage and channel number topology 45
3.5 Planning list items 49
3.5.1 System microcode 49
3.5.2 Capacity planning considerations 50
3.5.3 Installation of the ordered PCICCs 50
3.6 Software requirements 51
3.6.1 OS/390 V2R9 51
3.6.2 CKDS and PKDS sharing considerations 52
3.7 PR/SM setup 53
3.8 Migrating from TKE V2.x to TKE V3.0. 53
3.8.1 Host definitions. 53
3.8.2 CCF crypto modules, domains, and authority definitions. 53
3.8.3 Authority signature keys on IBM Personal Security Card (PSC) . 53
3.8.4 Authority signature key in the TKE workstation key storage 54
3.8.5 IMP-PKA keys in the workstation key storage. 54
3.8.6 Migration of master or operational key parts on PSC 54
3.9 Site security policy 54

Chapter 4. Installation, configuration and startup of ICSF 55
4.1 PCI Cryptographic Coprocessor Card plugging 55
4.2 PCICC enablement 56
4.2.1 Function Control Vector (FCV) overview. 56
4.2.2 Import FCV. 56
4.2.3 Hardware status of the PCICC 59
4.3 LPAR setup 61
4.3.1 The image profile processor page. 61
4.3.2 Dedicated central processors 64
4.3.3 The Crypto page. 64
4.3.4 The PCI Crypto page 67
4.3.5 PCICC and cryptographic domains 68
4.4 Integrated Cryptographic Services Facility (ICSF) setup 68
4.4.1 Changes from previous release 68
4.4.2 TSO procedure. 69
4.4.3 Started task and the first time start 70

4.4.4 Master Keys 70
4.4.5 Initial Master Key entry with the pass phrase initialization utility . 71
4.4.6 Changing the Master Keys for CCF and PCICC via ICSF panels 78
4.4.7 Management of the PCI Cryptographic Coprocessors. 85

Chapter 5. Customizing PCICC and CCF using a TKE V3.0 89
5.1 Introduction to the new TKE workstation. 89
5.1.1 Major changes 89
5.1.2 Before using the new TKE 91
5.1.3 The TKE V3.0 software. 91
5.1.4 TKE workstation installation generalities. 92
5.1.5 TKE definitions 92
5.2 TKE workstation TCP/IP setup 94
5.2.1 OS/390 TCP/IP Host Transaction Program 97
5.2.2 TKE workstation 4758 setup 97
5.2.3 Starting the TKE application 104
5.3 TKE application: managing host Crypto coprocessors 104
5.3.1 Managing modules 104
5.3.2 PCICC and CCF setup on the TKE workstation 106
5.3.3 Manage and update the Crypto module notebook on TKE 111
5.3.4 PCICC modules notebook 115
5.3.5 Creating roles and authorities in the PCICC 117
5.3.6 Backing up the TKE files. 134
5.4 4753 Key Token Migration facility 135

Chapter 6. Support functions 137
6.1 RACF access control to ICSF services 137
6.1.1 New profiles 137
6.1.2 CSFSERV profiles - cryptographic coprocessor administration. 137
6.2 Crypto usage measurement 138

Appendix A. Exploiting the PCICC 139
A.1 The IBM exploiters 139

Appendix B. Support functions: ICSF services 141
B.1 Enhanced callable services 141
B.1.1 PKA Key Generation (CSNDPKG) 141
B.1.2 PKA Key Token Build (CSNDPKB). 141
B.1.3 PKA Key Import (CSNDPKI). 141
B.1.4 PKA Public Key Extract (CSNDPKX) 142
B.1.5 Digital Signature Generate (CSNDDSG) 142
B.1.6 Symmetric Key Generate (CSNDSYG) 142
B.1.7 Symmetric Key Export (CSNDSYX) 142
B.1.8 Symmetric Key Import (CSNDSYI) 142

B.1.9 SET Block Compose (CSNDSBC) 142
B.1.10 SET Block Decompose (CSNDSBD) 143
B.1.11 PKA Encrypt (CSNDPKE). 143
B.1.12 PKA Decrypt (CSNDPKD) 143
B.1.13 PKDS callable services. 143
B.2 New callable services 143
B.2.1 Retained Key Delete (CSNDRKD) 143
B.2.2 Retained Key List (CSNDRKL) 143

Appendix C. TKE host TCP/IP server setup. 145
C.1 The main TCP/IP files to check and modify 145
C.1.1 TCPIP.HOSTS.LOCAL. 145
C.1.2 TCPIP.DATA 145
C.1.3 TCPIP.PROFILE. 145
C.2 TKE Host Transaction Program installation 147
C.2.1 CSFTTCP started procedure installation 147
C.2.2 The CSFTTKE module 148
C.2.3 The CSFTHTP3 REXX exec 148
C.3 Starting the TKE Host Transaction Program 149

Appendix D. Special notices 151

Appendix E. Related publications. 155
E.1 IBM Redbooks publications 155
E.2 IBM Redbooks collections. 155
E.3 Other resources 155
E.4 Referenced Web site 156

How to get IBM Redbooks 157
IBM Redbooks fax order form 158

Index 159

IBM Redbooks review 163

Figures

1. Example of IBM CCA Master Key and key separation concepts 2
2. S/390 Cryptographic Coprocessors 5
3. Physical coprocessor domains and logical coprocessors 7
4. CCF and PCICC hardware data flow on S/390 G5/G6 12
5. 4758-based Crypto coprocessor hardware data flow 13
6. PCICC card 13
7. PCICC card: end view 14
8. 4758-based card on S/390: longitudinal section 15
9. AP architecture: high-level view 19
10. Crypto software architecture in the IBM 4758 Technology 22
11. Crypto feature codes 33
12. CHPID Report 35
13. PCICC status before FCV loaded in PCI CC Number 1 37
14. PCI CC status after FCV selected and CHPID configured online 38
15. Nondisruptive Hardware Change panel at the Support Element 39
16. Msg. after PCICC Card removed by Nondisruptive Hardware Change . . . 40
17. AP Management - AP1 release 41
18. 9672 G6 internal system structure 43
19. 9672 G5 and G6 channel capacity support 46
20. 9672 I/O Domains and STI assignment 48
21. PCICC configuration main panel view 57
22. PCI Cryptographic Coprocessor detail view 58
23. The result from the Random Number Generator test 59
24. Right-clicked object on CPC Work Area view 60
25. PCI Crypto selected from the CPC Work Area view 61
26. The Activation Profiles List. 62
27. Customize Image Profile page of a selected image. 63
28. Customizing Image Profile: the processor page 63
29. Crypto page of the image profile 65
30. PCI Crypto page of the image profile. 67
31. A new PCICC added to Candidate List 68
32. The first-time ICSF startup messages 70
33. Selecting Pass Phrase Option on the ICSF primary menu panel 72
34. Entering options on the Pass Phrase MK/CKDS Initialization panel 72
35. Pass phrase initialization complete messages 73
36. Coprocessor Status Display selection panel 73
37. Cryptographic Coprocessor Feature hardware status, panel 1 74
38. Cryptographic Coprocessor Feature hardware status, panel 2 75
39. Cryptographic Coprocessor Feature hardware status, panel 3 75
40. The PCICC selection panel 76

41. The PCICC hardware status, panel 1 77
42. The PCICC hardware status, panel 2 77
43. Message on the ICSF startup before the first write to PKDS. 78
44. PCICC does not accept weak keys 79
45. Master Key change failed 80
46. The clear Master Key entry for only one PCICC 81
47. Select the correct PCICC for the clear Master Key entry. 81
48. Entering the first key part values 82
49. After the final key part was entered 82
50. The Master Key change was successful 83
51. Change the CKDSN value in the Options Data Set. 83
52. The final ASYM-MK key part is loaded 84
53. PCICC hardware status after the PKA Master Key changed. 85
54. Selecting the PCICC management from the ICSF main panel 86
55. Select to see the hardware status of the PCICC card 86
56. Deactivate the PCICC card 86
57. Deactivated PCICC card 87
58. TKE workstation configuration according to CMOS models 90
59. TKE workstation and host system 91
60. TCP/IP configuration notebook 94
61. TCP/IP routing tab 95
62. Autostart tab. 96
63. Host Names tab 96
64. TKE workstation predefined roles and profiles 98
65. TKE workstation CNM utility panel. 99
66. CNM utility logon as default TKEADM user with default passphrase . . . 100
67. TKE workstation profile example: TKEUSER default profile 101
68. TKE workstation role example: TKEUSER default role 102
69. TKE workstation MK - first part generate and load 103
70. TKE MK - first part successfully loaded 103
71. Set TKE workstation Master Key successful panel 104
72. Host Crypto module access logon sequence from TKE 106
73. Trusted Key Entry workstation logon panel 107
74. TKE V3.0 application main panel. 107
75. Load signature key; Source: default signature key 108
76. Create a new host panel on TKE workstation example: NTPREP. 109
77. Host logon panel on TKE workstation 109
78. New Crypto module authentication panel 110
79. Create New Group panel 111
80. CCF and PCICC command families 115
81. PCICC notebook general page on TKE. 116
82. PCICC initial role & profile after new card install or card zeroize from SE117
83. PCICC Roles commands. 118

84. PCICC module administration notebook roles definition entry. 119
85. Create Role: SYMMKP1 will load 1st part of SYM MK (DES), domain 5. 120
86. PCICC Create Roles and Authorities example 121
87. PCICC Roles page after new roles have been created 122
88. PCICC module notebook authority management main panel 123
89. Create Authority: JOHN, Authority 03 mapped to SYMMKP2 role 124
90. PCICC Authorities panel after some authorities have been created 125
91. PCICC Domain 5 general page 126
92. PCICC Domain 5 keys page 127
93. PCICC Domain 5 control panel 128
94. Pending command message panel 129
95. Co-sign panel: co-sign pending for create authority issued by TOM 129
96. TKE CCF Crypto Module Details view 130
97. TKE CCF Crypto Module Authorities view 131
98. TKE CCF Crypto Module Access Control view 132
99. TKE CCF Crypto Module Co-Sign view 133
100.KE CCF Crypto Module Domain: new Master Keys first part done 134

Tables

1. PCICC card: Not operational and Test complete indicators 14
2. Indicator status. 14
3. The PCICC status values. 87

Preface

This redbook is designed to help you understand and implement the S/390 Cryptographic PCICC card.

Although this book is focused on the enablement of the S/390 PCICC product, cryptography and the available services on S/390 are also discussed and explained, with special attention given to the new Trusted Key Entry (TKE) workstation. Reader familiarity with the previous S/390 cryptography-related redbook: *Exploiting S/390 Hardware Cryptography with TKE*, SG24-5455, is assumed.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization Poughkeepsie Center.

Moon J Kim is a Senior Technical Staff Member at the International Technical Support Organization, Poughkeepsie Center.

Pekka J Hanninen is a Service Specialist in Finland. He has 25 years of experience in IBM Large Systems software. He has worked at IBM for four years. His areas of expertise include RACF, cryptography and securityadministration. He holds certificates for CISSP and CISA.

Patrick Kappeler is a former computer speciallist in the French Air Force and joined IBM in 1970 as a diagnostic programs designer. He has held several specialist and management positions as well as international assignments, all dealing with S/390 technical support. He joined the EMEA S/390 New Technology Center in Montpellier in 1996, where he now provides consulting and presale technical supports in the area of e-business security.

Robert Malaval is a Product Engineer at the Montpellier System Laboratory in France. He has 12 years of experience as a Product Engineer in the power area of the large systems, and seven years in the CEC area of CMOS. He holds a degree in Electronics from Montpellier University.

Peter Quitzau is an IT specialist in S/390 Hardware support Nordic, working in Copenhagen, Denmark for IBM IGS/ITS. He has 20 years of experience in the ES9000 - S/390 field. From 1988 to 1992 he worked as an IDT specialist in the EMEA Product Support Group - S/390 (EPSG), Montpellier.

Zacharie Zanni is a Product Engineer at the Montpellier Systems Laboratory in France. He has 18 years of experience in Product Engineering, specializing in the CEC area of large systems. He holds a degree in Physics/Chemistry from Strasbourg, France. His areas of expertise include hardware and microcode related to CP, memory, system controller, and crypto chips. He has written extensively on numerous new hardware products. He is currently expanding his area of expertise to system capacity planning and performance.

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Please send us your comments about this or other Redbooks in one of the following ways:

- Fax the evaluation form found in “IBM Redbooks review” on page 163 to the fax number shown on the form.
- Use the online evaluation form found at `http://www.redbooks.ibm.com/`
- Send your comments in an Internet note to `redbook@us.ibm.com`

Chapter 1. Introduction

In this chapter we provide an overview of IBM cryptography, starting with a discussion of the IBM Common Cryptographic Architecture (CCA).

1.1 IBM Cryptographic Common Architecture (CCA)

The IBM Common Cryptographic Architecture defines a set of cryptographic functions, external interfaces, and a set of key management rules which pertain both to the Data Encryption Standard (DES)-based symmetric algorithms and the Public Key Algorithm (PKA) asymmetric algorithms. These provide a consistent, end-to-end, cryptographic architecture across different IBM platforms, such as OS/390, AIX, OS/400, OS/2, and Windows NT, which conforms to American and International Standards.

Functions of the Common Cryptographic Architecture define services for the following:

- **Key Management**, which includes generation and exchange of keys securely across networks and between application programs. The exchanged key is securely encrypted using either DES or a Public Key Algorithm used in the context of symmetric key management.
- **Data Integrity** with the use of a Message Authentication Code (MAC), Modification Detection Code (MDC), or digital signature.
- **Data Confidentiality** with the use of encryption and decryption capabilities accessible at all levels of a network protocol stack.
- **Personal Authentication** with PIN generation, verification, and translation.

CCA was introduced in October 1989 with the IBM Transaction Security System and the IBM Integrated Cryptographic Facility (IBM ICRF) with its supporting Integrated Cryptographic Services Facility/MVS (ICSF/MVS). These products and their follow-ons (for ES/9000 ICRF, the CMOS Enterprise Server/Multiprise Crypto Coprocessor Facility or CCF, and the new 9672 PCI Crypto Coprocessor or PCICC), conform to the IBM CCA Application Programming Interface.

1.2 CCA key management functions

Key management is essential to successful cryptography. Since the algorithm is usually public knowledge, the security of the data depends on the security of the key used to encipher the data. Enciphered data may be obtained by an adversary, but without access to the cryptographic key, the data remains secure. Key management in the IBM CCA includes the following:

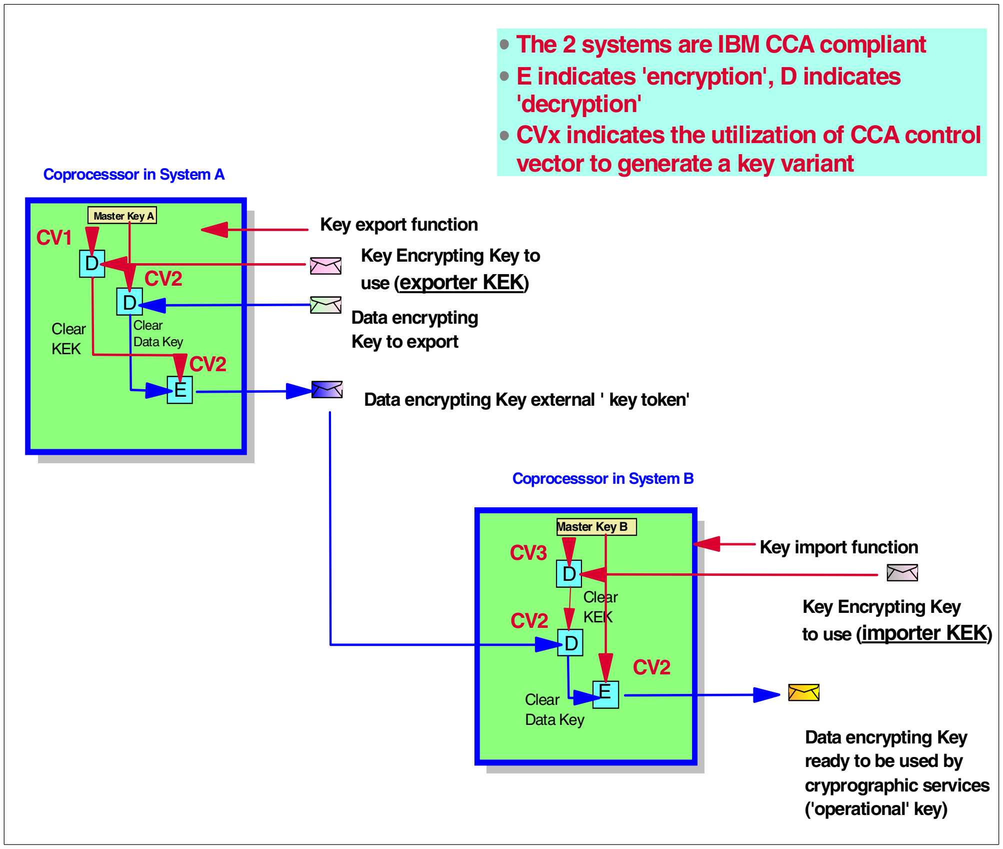
- **Master Key Concept** - Each cryptographic system has a Master Key that is kept in the clear inside the *cryptographic facility*, which is a highly secured physical repository. Each operational DES key is encrypted under the appropriate Master Key variant (see next item). This allows an installation to protect many keys while providing physical protection for only one key.

  The concept of Master Key is also applied to PKA keys that are encrypted under the PKA Master Key.

- **Key Separation** - Cryptographic keys should be used only for their intended function. For DES keys, the IBM CCA enforces key separation through the use of control vectors (CV). A *control vector* is a fixed pattern defined for each key type that the cryptographic facility exclusively ORs with the Master Key to produce a Master Key variant that is used to encrypt the key. Effectively, this produces a unique Master Key for each key type. The Master Key variants protect keys operating on the system; these are called *operational keys*. Note that the control vector concept also applies to the secure transportation of symmetric keys, where the transported key is encrypted under a variant of the key-encrypting-key.

  Note also that the control vector concept is not relevant to the PKA keys; instead, “key usage flag bits” are associated to the PKA key to restrict its usage to signature and/or symmetric key management.

  For example, when a key is stored with a file or sent to another system, the key is encrypted under a key-encrypting key. Figure 1 illustrates these concepts, where the data-encryption key and the key-encrypting key are shown as sealed envelopes to indicate that they are encrypted under the corresponding crypto facility Master Key variant, whereas the external key token is encrypted under a key-encrypting-key variant.



The 2 systems are IBM CCA compliant
E indicates 'encryption', D indicates 'decryption'
CVx indicates the utilization of CCA control vector to generate a key variant
Coprocesssor in System A
Master Key A
CV1
D
CV2
D
Clear KEK
Clear Data Key
CV2
E
Key export function
Key Encrypting Key to use (exporter KEK)
Data encrypting Key to export
Data encrypting Key external ' key token'
Coprocesssor in System B
Master Key B
CV3
D
Clear KEK
CV2
D
CV2
E
Clear Data Key
Key import function
Key Encrypting Key to use (importer KEK)
Data encrypting Key ready to be used by cryprographic services ('operational' key)

Figure 1. Example of IBM CCA Master Key and key separation concepts

Notice the two types of key-encrypting keys: the exporter-KEK on the sending side, and the importer-KEK on the receiving side. These two keys have the same clear value but they have an associated control vector which restricts their function to exportation or importation of other keys.

For more information on the Common Cryptographic Architecture, refer to the following publications:

- *Common Cryptographic Architecture: Cryptographic Application Programming Interface Reference,* SC40-1675

1.3 Implementation of the CCA key management concepts in S/390

This section describes the concepts underlining CCA key management in S/390.

1.3.1 S/390 Cryptographic Coprocessor Facility (CCF)

The S/390 CCF implements three Master Keys:

- The DES Master Key
- The PKA Signature Master Key (SMK)
- The PKA Key Management Master Key (KMMK)

PKA private keys are protected under two layers of DES encryption. They are encrypted under an Object Protection Key (OPK) that in turn is encrypted under the SMK or KMMK. The OPK is generated for each private key at import time.

1.3.2 S/390 PCI Cryptographic Coprocessor (PCICC)

The S/390 PCICC implements two Master Keys:

- The DES Master Key, called the Symmetric Master Key
- The PKA Master Key, called the Asymmetric Master Key

The SMK and KMMK scheme has not been implemented in the PCICC, which has a single PKA Master Key. It is required that the PCICC Asymmetric Master Key has the same value as the CCF SMK, and it is strongly recommended that you set the CCF SMK and KMMK to the same value when at least one PCICC card is also installed in the system.

1.4 S/390 integrated cryptography implementation

IBM led the industry by offering the first CMOS cryptographic coprocessor as a standard feature on the S/390 G4, G5, and G6 servers, and as a priced feature on the G3 server models, in order to meet the increasing needs for data security and integrity.

The S/390 Cryptographic Coprocessor Facility is implemented in CMOS technology on a single chip providing more capability than any previous cryptographic offering. Included in the design is battery-backed non-volatile memory storage, laser delete chip personalization, integrated tamper detection and response, and high speed DES, Triple DES, DSS, RSA, Pseudo Random Number Generation, and hashing algorithms. Depending on the system model, there may be one or two coprocessor chips in operation.

This hardware runs all current Integrated Cryptographic Feature (ICRF) functions previously offered on ES/9000 ® 9021 processors and includes in addition the Public Key Algorithms (RSA) with digital signature generation and verification.

The software that enables this solution and provides the Application Programming Interface (API) is a follow-up release of the ICSF/MVS product. This release is integrated into the base of OS/390 Version 2 Release 5. This enhanced software release supports new functions built into the chip and continues to support all previous ICSF/MVS functions found on prior 9021 machines.

OS/390 Version 2 Release 5 also provides support for applications using SET protocol and Visa/Mastercard CVV/CVC card-verification values including TDES and Double Key MAC. The software supports all the current standards and requirements, as did the previous versions.

Starting June 2000, the PCI Cryptographic Coprocessor (PCICC) is an orderable feature that adds additional cryptographic function and cryptographic performance to G5/G6 servers. Up to 8 PCICC features may be ordered for a G5 or G6 server. Each PCICC feature comprises a 4758 Technology-based cryptographic coprocessor card embedded in an adapter package for installing within a G5 or G6 server. Support for PCICC is provided in OS/390 V2R9 by new ICSF functions.

The PCI Cryptographic Coprocessor feature coexists and augments CMOS CCF functions. ICSF transparently routes application requests for cryptographic services to one of the integrated cryptographic engines, either a CCCF or a PCICC, depending on performance or requested cryptographic function. For example, RSA signature generation and verification operations (with 1024-bit or shorter keys), such as those typically used by SSL, are routed to both CCF and PCICC engines. On the other hand, RSA Key Generation is performed only on PCICC engines.

1.4.1 S/390 integrated cryptography implementation

Figure 2 on page 5 provides a very high-level representation of how the cryptographic coprocessors work in S/390 G5 and G6.

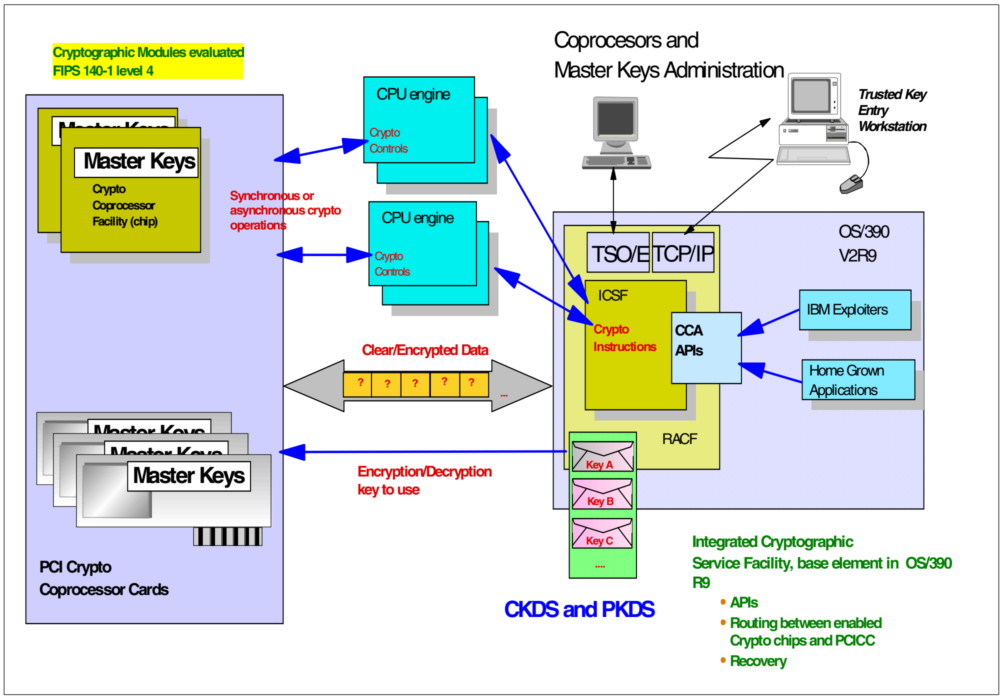


Figure 2. S/390 Cryptographic Coprocessors

- The exploiters of the cryptographic services call the ICSF API. Some functions will be performed by the ICSF software without invoking the cryptographic coprocessor; other functions will result in ICSF going into routines containing the proprietary S/390 crypto instructions.
- These instructions are executed by a CPU engine and result in a work request being generated for a cryptographic coprocessor.
- The crypto coprocessor is provided with the following:
  - Data to encrypt or decrypt from the system memory.
  - The key used to encrypt or decrypt provided by ICSF as per the exploiter's request. Note that these keys are represented as sealed envelopes here, the intent being to stress the fact that these encryption/decryption keys are themselves encrypted and, therefore, unusable when residing outside of the crypto coprocessor.

    Physically, these keys can be stored in ICSF-managed VSAM data sets and pointed to by the application using the label they are stored under. The Cryptographic Key Data Set (CKDS) is used to store the symmetric keys in their encrypted form, and the Private Key Data Set (PKDS) is used to store the asymmetric keys. The application also has the capability of providing an encrypted encryption key or a clear encryption key directly in memory (that is, to use *as is*) to the coprocessor.
  - For high-speed access to symmetric cryptographic keys, the keys in the CKDS are duplicated into an ICSF-owned data space.

Note that applications using ICSF services can still elect to store keys in non-ICSF key data sets and are, therefore, to manage the keys' security by their own means.

The Trusted Key Entry (TKE) Workstation is an optionally-priced feature. This workstation provides a secure, remote, and flexible method of providing Master Key Part Entry and to remotely manage the cryptographic coprocessors. The algorithm utilizes Digital Signature, Diffie-Hellman, and DES functions to provide a highly secure, auditable, and remote method of key entry, and it can be used by those customers requiring very high security for key entry.

Note that a new model of TKE is required to support the PCICC. Differences between this new model and the previous one are described in detail in Chapter 5, “Customizing PCICC and CCF using a TKE V3.0”, on page 89.

1.4.2 Enablement of the cryptographic coprocessors

The S/390 CCF and PCICC are generic cryptographic coprocessors in that they can run various algorithms with different key lengths. However, to conform to export regulations, they are shipped *non-enabled*, meaning that the final user, in the country of use, needs to enable the coprocessors using diskettes provided by IBM. These diskettes allow activation of the algorithms that the customer requested and of which use is granted by US and local regulations.

The diskettes need to be loaded only once and are customized so that they load only on the user’s machine. The diskettes consist of the following:

- One enablement diskette for the CCFs installed in the system. The Licensed Internal Code (LIC) in this diskette allows the setting of the CCF Crypto Configuration Controls (CCC) register. This diskette is customized to the CCF chip’s serial number.
- One enablement diskette for the PCICCs installed in the system, for setting the PCICC Functions Control Vector (FCV). This diskette is customized to the machine’s serial number.

Further details on the cryptographic coprocessors’ enablement are given in Chapter 4, “Installation, configuration and startup of ICSF”, on page 55.

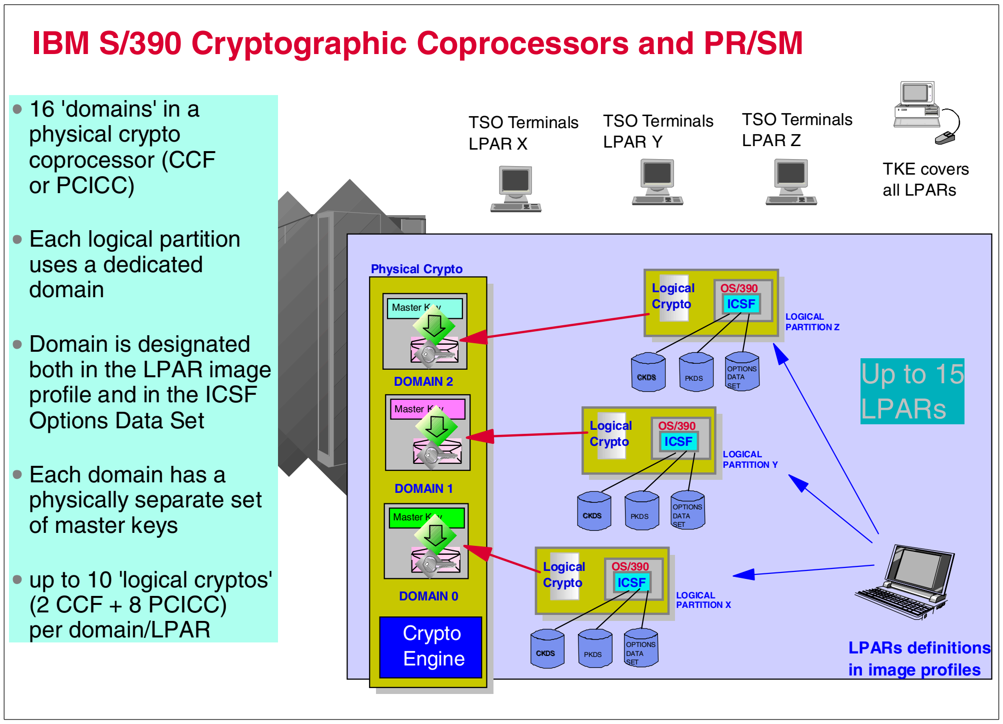
1.4.3 LPAR domains and TKE

This section provides an overview of the relationships between logical partitions, physical crypto coprocessors, and domains. It also gives information on defining, controlling and managing these elements.

1.4.3.1 Overview

A cryptographic coprocessor actually has 16 physical sets of Master Key registers, each set belonging to a *domain*. A domain is allocated to a logical partition via the definition of the partition in its image profile; the same domain must also be allocated to the ICSF instance running in the logical partition via the Options Data Set.

Figure 3 illustrates how logical partitions, physical crypto coprocessors and domains interact:



IBM S/390 Cryptographic Coprocessors and PR/SM

- 16 'domains' in a physical crypto coprocessor (CCF or PCICC)
- Each logical partition uses a dedicated domain
- Domain is designated both in the LPAR image profile and in the ICSF Options Data Set
- Each domain has a physically separate set of master keys
- up to 10 'logical cryptos' (2 CCF + 8 PCICC) per domain/LPAR

Figure 3. Physical coprocessor domains and logical coprocessors

- Each ICSF instance accesses only the Master Keys corresponding to the domain number specified in its image profile, at the system Service Element, and in its Option Data Set. Each ICSF is seeing a *logical crypto coprocessor* made of the physical cryptographic engines shared among the logical partitions and the unique set of registers (the domain) dedicated to this partition.
- Each logical partition, or each ICSF instance, therefore has its own unique Master Key values and can encrypt its own set of users' keys with these unique Master Key values, thereby insuring perfect insulation between users of the shared crypto coprocessors from the standpoint of security.

1.4.3.2 Defining logical cryptographic coprocessors

The logical cryptographic coprocessors are defined to PR/SM by clicking the crypto co-processors shown in the processor view of the image profile. Further details on the PR/SM definitions required for the cryptographic coprocessors are given in Chapter 4, “Installation, configuration and startup of ICSF”, on page 55.

1.4.3.3 Cryptographic controls of the logical partition

There are controls set up at the logical partition level that influence the scope of the cryptographic functions available from the logical cryptographic coprocessor, as seen from the instance of ICSF running in the partition or from the attached TKE. The set of control parameters available through the logical partition image profile is described in Chapter 4, “Installation, configuration and startup of ICSF”, on page 55.

1.4.3.4 Cryptographic services management through the TKE

The Trusted Key Entry (TKE) Workstation provides a centralized control point for administering the multiple physical or logical crypto coprocessors in a single or multi-system configuration. The TKE communicates with one OS/390 instance called the *TKE Host System*. If the TKE Host System is a logical partition, several domains, corresponding to other partitions in this physical system, can be controlled from the Master Keys' administration standpoint by a single TKE. This is achieved securely by having the TKE supporting software in the TKE host issue proprietary calls to the PR/SM microcode for cross-domain Master Keys administration.

This cross-domain capability is available only when using the TKE Workstation, as opposed to the ICSF ISPF panels. However, ICSF ISPF panels can still be used to administer the local Master Keys, whether a TKE is present in the configuration or not.

1.5 Industry standards for cryptographic modules

As the need for computer security grew, the industry needed evaluation criteria for assessing the logical and physical robustness of cryptographic devices. To address this need, the National Institute of Standards and Technology issued the Federal Information Processing Standard (FIPS) 140-1 standard in June 1994. FIPS 140-1 addresses the security requirements of c*ryptographic modules,* that is, cryptographic engines, whether in software, firmware or hardware implementation.

This standard covers 11 areas related to the design and implementation of a cryptographic module. Within most areas, a cryptographic module receives a security level rating (1 to 4, from lowest to highest), depending on what requirements are met. For other areas that do not provide for different levels of security, a cryptographic module receives a rating that reflects fulfillment of all of the requirements for that area.

Cryptographic modules that comply with this standard employ cryptographic algorithms, cryptographic key generation algorithms, key distribution techniques, and authentication techniques that have been FIPS-approved for protecting Federal Government unclassified information.

The S/390 CCF hardware single chip cryptographic module has received the the highest level of FIPS 140-1 (Level 4) certified by both the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) of Canada. The FIPS 140-1 certification is under way for the S/390 PCICC, as of the time of writing.

A formal list of all FIPS 140-1 products and their associated certification levels can be found at:

```
http://csrc.ncsl.nist.gov/cryptval/140-1/1401val.htm
```

The S/390 cryptographic coprocessors are physically secure. They provide a tamper-sensing and tamper-responding environment fitting the needs of sensitive applications. Upon detection of physical attack, including penetration, radiation, voltage, excessive cold or heat, the device is “zeroized” and the sensitive information erased.

Chapter 2. PCICC product overview

This chapter provides an overview of the PCI Cryptographic Coprocessor (PCICC) product provided in the S/390 platform. It briefly describes the IBM 4758 Technology as used in the S/390 PCICC implementation, as well as the cryptographic coprocessor enablement concept, the new functions of the ICSF component of OS/390, and the new workstation feature.

2.1 Description of hardware

This section explains IBM 4758 technology and gives an overview of the hardware data flow implemented in the S/390 PCICC facility.

2.1.1 Introduction to the S/390 PCI Cryptographic Coprocessor

The following definitions will introduce you to S/390 PCICC concepts.

Cryptographic Coprocessor Facility (CCF) refers to the CMOS cryptographic coprocessor feature logic attached to a central processor on S/390 G3, G4, G5, and G6 systems. There are one or two CCFs per system, and each CCF has 16 domains which each hold the following set of Master Keys:

- DES Master Key
- PKA KMMK key management MK
- PKA SMK signature MK

Peripheral Component Interconnect Cryptographic Coprocessor (PCICC) - each PCICC feature is built around the IBM 4758 card technology embedded in a Self-Timed Interface (STI)-attached controller card for installing within a G5 or G6 server. The STI-attached controller package allows STI-to-PCI interface bus conversion and also provides for PCI controller functions.

From a system implementation perspective, the PCICC unit is an *Adjunct Processor* (AP). Note that *AP* designates the processor, while *AP ID* specifies the number associated with it. The number of APs is limited to 8 on G5/G6, and a PCICC is therefore given an AP number between 0 and 7.

The PCICC has 16 cryptographic domains, each holding a set of the following Master Keys:

- One symmetric Master Key (SYM-MK)
- One PKA Master Key (ASYM-MK)

Another concept introduced to S/390 cryptography by the PCICC is the *retained key*, which is an RSA private key generated by the PCICC upon request of the user. The retained key is kept inside the secure area of the coprocessor and is never to leave the secure area of the coprocessor. It is therefore physically tied to the PCICC it has been generated in and is *never backed up*.

Support for PCICC is provided by OS/390 V2R9 with the new ICSF functions. The IBM PCI Cryptographic Coprocessor feature coexists with the CCF, but it also provides additional cryptographic processing power as well as additional capabilities (such as RSA Key Generation) above and beyond the CCF.

2.1.1.1 PCICC general characteristics

When ordered on a G5/G6 system, PCICC is always considered as *a complement to the CCF* that is shipped today--in fact, the ICSF software requires as a prerequisite at least one CCF installed in the CEC in order for the PCICC to be functional.

The PCICC provides two major advantages over today's Crypto Coprocessor Facility:

1. You can improve cryptographic performance by simply adding more PCICC cards.
2. As a statement of direction, IBM will allow the programmable implementation of different cryptographic algorithms on PCICC (the CCF currently doesn't offer that capability). This answers the need to quickly implement new cryptographic algorithms generated from the industry.

The S/390 PCICC was announced on 2/29/2000 and will be available for G5 and G6 CMOS models starting 6/30/2000. It uses IBM 4758 technology packaged in an STI-attached controller card (the PCICC card assembly), with a longer battery life and delivers signals at a different voltage level (3.3 volt) than the IBM 4758-2 card. From a functional standpoint, the PCICC assembly also implements the concept of cryptographic “domains”, which is not relevant to the workstation version of the 4758 cryptographic coprocessor.

With the introduction of the PCICC into the S/390 G5/G6 systems, the TKE workstation is enhanced to allow remote administration of the PCICC cards, while continuing to support the CCF. The new TKE workstation includes a 4758-2 cryptographic adapter card for its own cryptographic needs, as a replacement to the former 4755 cryptographic adapter. See Chapter 5, “Customizing PCICC and CCF using a TKE V3.0” on page 89 for details on the utilization of the TKE workstation.

“Nature” of the PCICC

The PCICC, when plugged in the system, is referred to in three ways:

1. It has an eight-character serial number, for reference in a variety of panels and to keep track of the retained keys.
2. It has a two-digit Adjunct Processor (AP) number or ID. This number is an index used by the system LIC and ICSF.
3. Because of the way it is connected in the system, it has a CHPID number. The CHPID number is not known nor relevant to ICSF, but is used for hardware management of the card.

2.1.1.2 STI and CHPID plugging rules overview on G5/G6

Two types of STI channel attachments are used to connect the CEC and the system’s channels:

- **STI non-direct attached adapters** for parallel and ESCON channels, Coupling Facility links, and OSA-2 adapters. These adapters require a Fast Interface Buffer (FIB) card between the STI and the adapter.
- **STI direct attached adapters** for FICON, OSA Express, and PCI Cryptographic Coprocessor feature cards.

  The STI attached controller cards plug into existing I/O cage card slots and are directly connected to a high-speed STI link. This direct STI attachment eliminates the need for an FIB card and increases processing speed. Up to four STI attached adapters cards can be “chained” together on a single STI link.

  Each PCICC feature card is assigned a CHPID number based on which STI is used and where it appears in the STI chain. Because the CHPID number is attributed to the card, it will no longer be available for normal CHPID use and cannot be used in an IOCDS definition.

Refer to Chapter 3, “Planning” on page 31 for a more detailed explanation of the plugging rules. Also refer to the IBM Configurator output and to the system documentation for accurate STI and CHPID assignments in the system.

2.1.1.3 CCF and PCICC hardware data flow on S/390 G5/G6

Figure 4 on page 12 shows a 9672 G5/G6 CPC cage with two CCFs that are twin tail-attached to CPs. All the logic elements shown, except for the memory, are inside the multichip module (MCM).

It also shows a 9672 I/O cage with the following components:

- An FIB card used to interface CEC with standard channels through STI non-direct attachment
- Two STI attached controller cards (STI direct attachment) with:
  - One PCICC card
  - One FICON Adapter card holding a FICON card

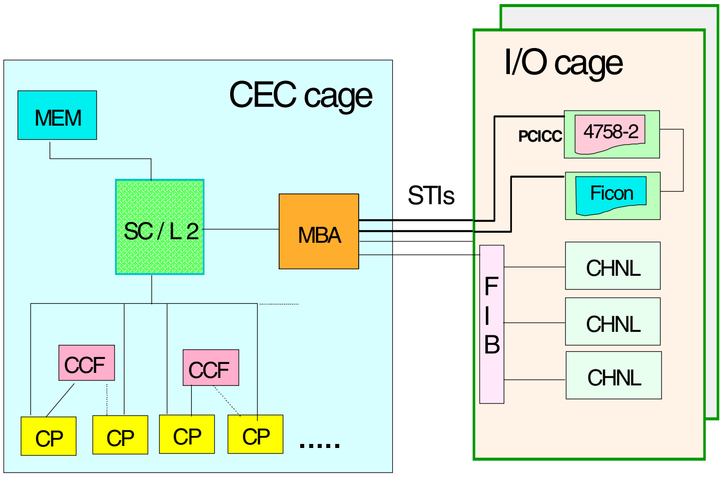


Figure 4. CCF and PCICC hardware data flow on S/390 G5/G6

2.1.2 PCICC data flow

The following section explains how the PCICC data flow occurs.

2.1.2.1 The IBM 4758 technology and the PCICC hardware data flow

An IBM crypto coprocessor chip is attached to a 486-class microprocessor, and is mainly used as an accelerator in order to execute the specialized cryptographic functions in dedicated hardware engines (for example, DES and RSA). All the logic shown in Figure 5 on page 13 is enclosed in the 4758 physically secure area.

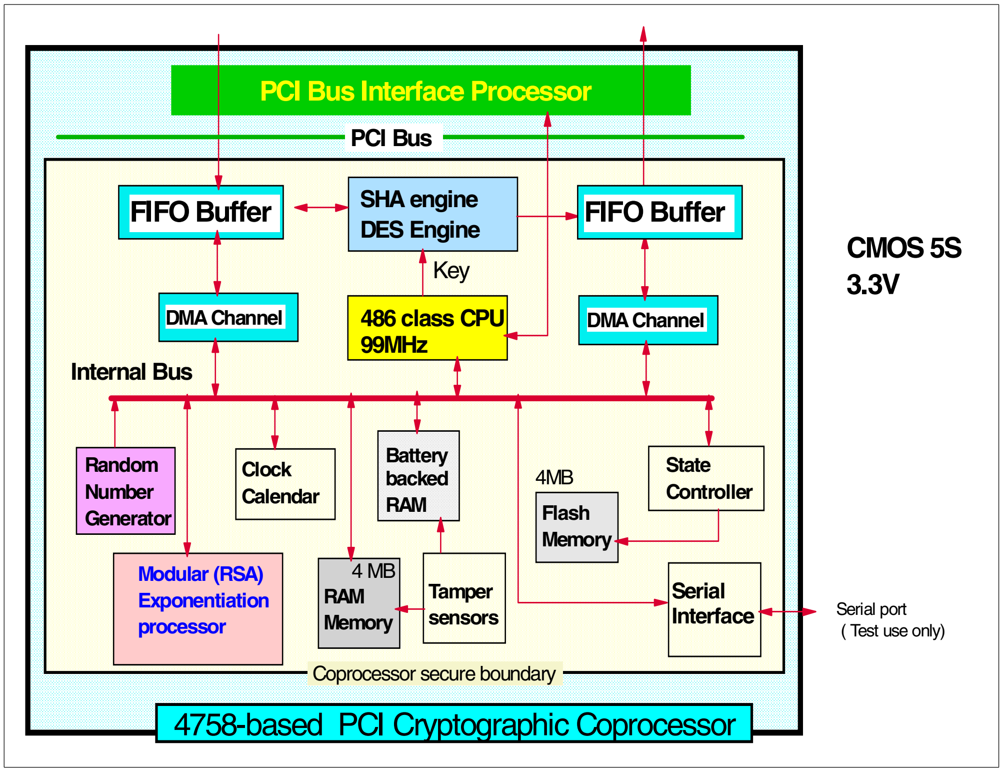


Figure 5. 4758-based Crypto coprocessor hardware data flow

2.1.2.2 The PCICC card

Figure 6 shows a PCICC card consisting of the assembly of an STI controller card and a 4758-based cryptographic coprocessor card. The PCICC card must not be disassembled.

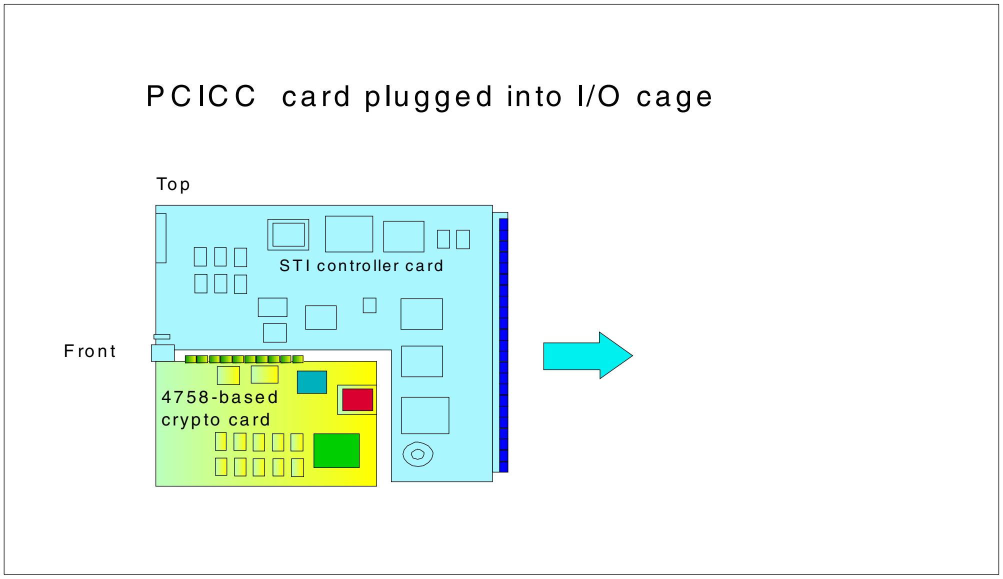


Figure 6. PCICC card

2.1.2.3 PCICC viewing status

Figure 7 illustrates the PCICC end view, showing connectors and indicators.

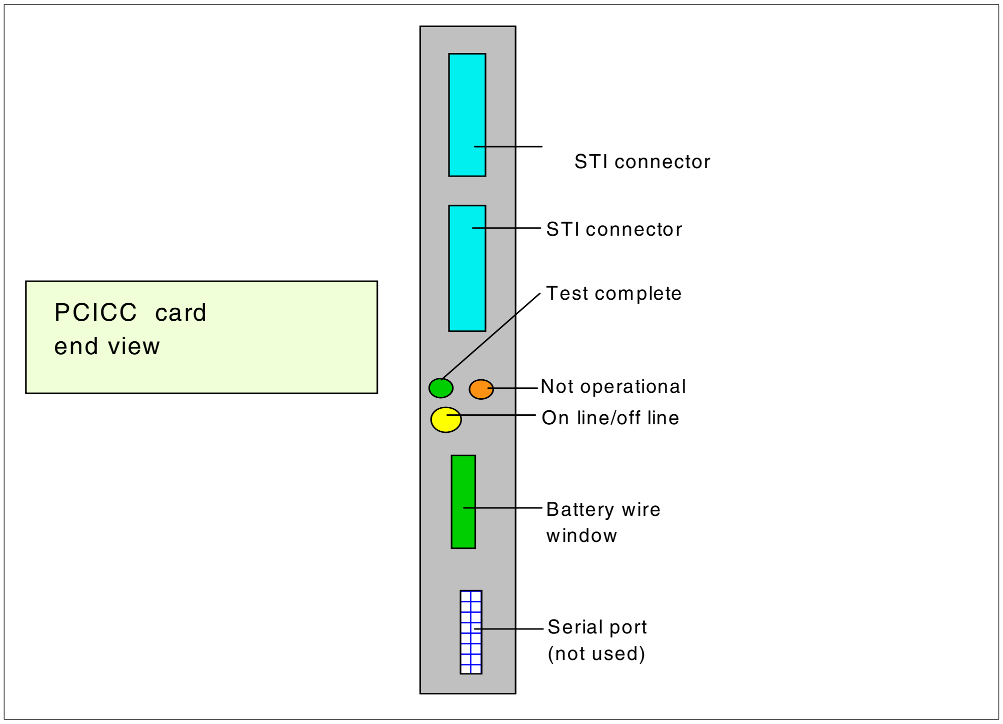


Figure 7. PCICC card: end view

Table 1 lists the meanings of the PCICC card indicators.

Table 1. PCICC card: Not operational and Test complete indicators

Test complete indicator	Not operational indicator	Status
Off	Off	No power to the card or card processor in a loop
Off	Flashing	Diagnostics are running
On	Off	Tests complete, CHPID online
On	On	Hardware error detected
On	Flashing	Invalid combination

Any combination where neither indicator is flashing (both on, both off, or one on and the other off), indicates that the card is powered off or the processor on the card is in a loop; see Table 2.

Table 2. Indicator status

On Line/Off Line Indicator (C)	Status
Off	CHPID for crypto adapter on line and card is communicating with PU
On	CHPID offline for maintenance *or* external test running
Blinking rapidly	Power-on tests running

2.1.3 PCICC card: physical security, handling, and shipping

Any attempt to physically penetrate the secure enclosure, or any abnormal modification of the card's physical environment, is reported to the card hardware as a "tamper detection." Because the tamper detection sensors are always active in the card as soon as it is manufactured, in the following section we describe here the special shipping conditions for the PCICC card.

Figure 8 contains a longitudinal section which shows the PCICC card internal packaging and the secure enclosure of the 4758-based card.

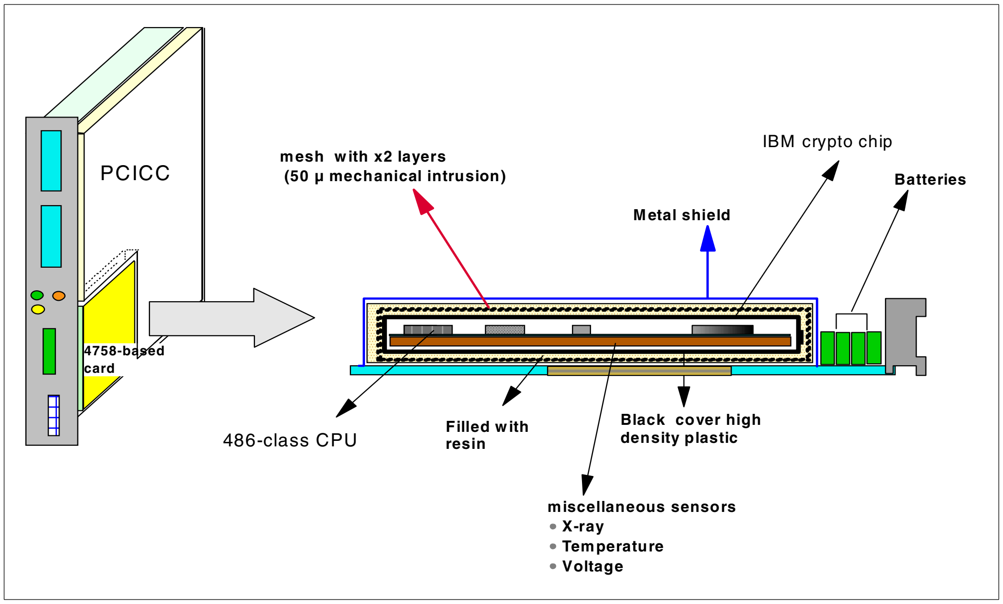


Figure 8. 4758-based card on S/390: longitudinal section

2.1.3.1 Tamper detection conditions

Tamper detection devices are installed to detect physical attempts to obtain the secret values that are stored inside the card. Depending on the abnormal conditions that are sensed, the tamper condition is classified either as *hard* or *soft tamper detection*, with the following results.

Hard tamper detection

When a hard tamper is detected, the Master Keys and other critical security values for the operation of the PCICC card are zeroized by inhibiting power supply to the card both from the system main power supply and from the on-card batteries. As a result, the card is left in an unrecoverable disable state and has to be replaced. Any of the following events will cause a hard tamper detection:

- Mesh sensor opens/shorts
- X-ray exposure
- High voltage on +3.3 V (3.9 ± 0.2 V) or on +12 V (14 V ± 0.2 V)
- A battery dead condition (VBAT less than 2.54 V)
- Temperature below -20C ± 5C or above +95C ± 5C limits

Special care should be taken to avoid these environmental conditions during card shipment. Refer to shipping conditions in 2.1.3.5, “PCICC card shipping conditions” on page 18 for more information.

Soft tamper detection

When a soft tamper is detected, the card enters an internal reset state. The card appears temporarily unavailable to all external requests when in this state. Once the soft tamper condition is removed, the internal reset condition is dropped and the card becomes usable again. The keys and secret values are not zeroized on a soft tamper condition.

Any of the following events will cause an internal card reset:

- Low voltage on +3.3 V (2.9 V ± 0.1 V)
- Low voltage on +12V (10.5 V ± 0.15 V)
- Crypto module internal operating temperature out of window limits (0C±2C/75C± 3C)
- An attempt to load unauthorized code in the PCICC

2.1.3.2 System-detected conditions

Either of these events will cause a warning at the system console issued by the system’s licensed internal code. These events are explained in detail in following sections:

- An intrusion latch trip
- A battery low condition (VBAT less than 2.70 V)

Intrusion latch

The intrusion latch is part of the 4758-based card logic and is used to detect when the card is unplugged from the system board. On a subsequent replug, the secret values in the card will be zeroized. Note the following points:

- When the PCICC card is removed from the system board, the intrusion latch is set.
- The CCA code which runs on the crypto microprocessor checks and resets the intrusion latch at each card power on. The code will zeroize the secret values if it finds that the intrusion latch has been set since the last card power on. If the intrusion latch has not been set, the code proceeds with the card initialization without zeroizing the secret values.
- The intrusion latch will not be set if the cage is moved and the PCICC remains plugged into the cage.

Notes

1. The PCICC card should be pulled out of the system I/O cage only if necessary**.** If the PCICC card is unplugged for any reason (maintenance or CHPID MES upgrades), the customer will have to be present to reinstall the keys back into the PCICC card.
2. The intrusion latch mechanism will also trigger the card zeroizing if the 4758-based card is pulled out of the PCICC assembly and is, for instance, re-installed in a workstation.
3. All retained RSA private keys are permanently lost when the PCICC is zeroized. There is, by definition, no backup capability for a retained key.

A battery low condition

Because the PCICC card contains enough batteries to last for the expected card life (which is 8 to 10 years, under normal usage), a battery low condition should normally not occur. The S/390 licensed internal code monitors the low battery bit, so if this unexpected condition is detected, a timely warning is issued to the operator.

A service action should then be taken relatively soon to replace the PCICC card assembly FRU, as the card will likely fail and become permanently disabled in two to four weeks if the FRU is not replaced.

Note that in this case, the PCICC card must be replaced with a new card containing fresh batteries; the customer will have to be present to reinstall the cryptographic keys in the new card.

2.1.3.3 Zeroizing

Zeroizing the card results in the following values being rendered permanently useless:

- The SYM-MK and ASYM-MK Master Keys in all domains.
- The users' retained keys in all domains.
- All the roles and profiles defined. The DEFAULT role is reset to the initial state. Roles and profiles are further explained in 5.3, "TKE application: managing host Crypto coprocessors" on page 104.

Note that, as for the CCF, you must differentiate *coprocessor zeroizing* from *domain zeroizing*. Coprocessor zeroize is either invoked from the system Support Element cryptographic controls, or is automatically triggered when the card detects during power on that the intrusion latch has been set. In contrast, domain zeroize can be invoked from the TKE workstation only, and has its effects limited to the selected domain, as explained in 5.3.5.5, "PCICC notebook DOMAINS page" on page 125.

Important

There are two buttons in the Support Element panel for zeroizing the PCICC: one button is for zeroizing one individual PCICC card, and the other button is for zeroizing *all* installed PCICC cards. Choosing to zeroize all PCICC cards also deletes the FCV in HSA. A subsequent attempt to initialize a PCICC card will put the card in check stop state, as there is no FCV to be loaded from HSA.

2.1.3.4 Cutting the card disable wire loop

Normally when a PCICC card is to be returned to IBM due to a hardware problem, an upgrade, or for some other reason, the customer's keys are zeroized via a Support Element panel before the card is removed.

To assure customers that keys have actually been destroyed and that the card has been disabled before IBM removes it from their premises, the card disable wire loop can be cut by service personnel to ensure destruction of the secret values by removing all power to the card. Be aware, though, that cutting this wire loop not only destroys the keys, but also *permanently disables the card*.

The wire loop can be accessed by removing a sticker on the tailstock of the PCICC card and reaching through a small hole in the tailstock with a pair of wire cutters. This wire loop is white, about a half-inch long, and is erected perpendicular to the PCICC card printed circuit.

Note

IBM support should not perform this procedure unless the customer requests it because Engineering will not be able to perform failure analysis after the wire is cut.

2.1.3.5 PCICC card shipping conditions

The PCICC card is shipped in such a way that the temperature-sensitive resisters inside the card are not exposed to less than 5 degrees F (-15C). Also the card should not be exposed to above 80% humidity, as condensation may cause tamper detection circuits to falsely trip. Each PCICC card is shipped in one large thermal container with five pounds of thermal gel inside the container.

2.2 Adjunct Processor (AP) management

In this section, we develop the concept of the Adjunct Processor as implemented in the 9672 G5/G6 and the related system management tasks.

2.2.1 Introduction to Adjunct Processor architecture

The system sees the PCICC as an "Adjunct Processor", that is, a coprocessor reachable through the STI cable. Therefore, each PCICC card installed in the system is assigned an AP number between 0 and 7. The system also establishes the correspondence between the AP number assigned to a card and this PCICC card serial number.

An AP is message-driven and operates asynchronously with respect to the CPUs that invoke it. It is conceptually a queue server handling requests from any client CPU. Figure 9 on page 19 is an high-level representation of the AP implementation model.

Cryptographic work to be done is enqueued to a selected AP queue, and then, from a queue, a command request message is sent to an AP. In return, a command reply message is received from an AP.

An AP queue provides accessibility to a given AP from all CPs in the configuration, as opposed to the CCF implementation, where the CCF is physically attached to a central processor. There is a separate AP queue for each domain in domain within an AP, the AP queues reside in Hardware System Area (HSA) storage.

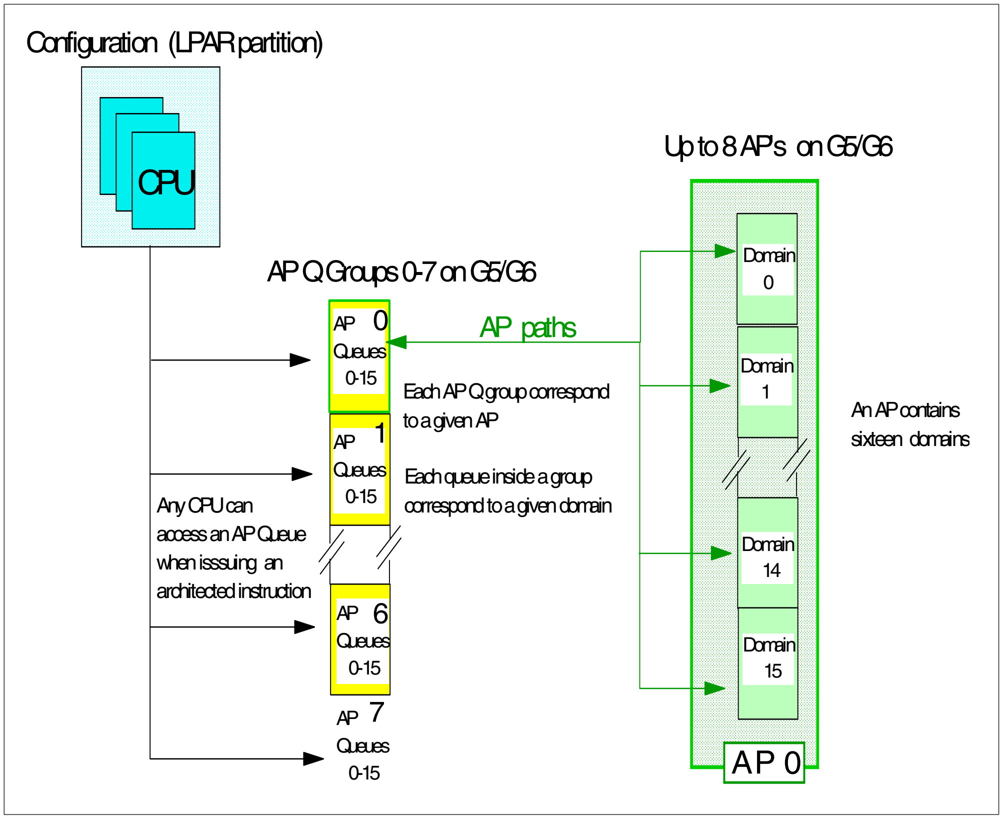

Configuration (LPAR partition)
CPU
AP Q Groups 0-7 on G5/G6
AP 0 Queues 0-15
AP 1 Queues 0-15
AP 6 Queues 0-15
AP 7 Queues 0-15
AP paths
Each AP Q group correspond to a given AP
Each queue inside a group correspond to a given domain
Any CPU can access an AP Queue when isssuing an architected instruction
Up to 8 APs on G5/G6
Domain 0
Domain 1
Domain 14
Domain 15
AP 0
An AP contains sixteen domains

Figure 9. AP architecture: high-level view

2.2.2 AP management and PCICC initialization

2.2.2.1 AP and CHPID number

For internal system management purposes, an AP is also tied to a CHPID number which is automatically attributed to the PCICC card at installation. Therefore, from a system management standpoint, a PCICC is also a new CHPID type, and this requires the typical changes (LPAR, Advanced Facilities, etc.) scattered throughout the Support Element. As a consequence, a PCICC card will appear tagged with a CHPID number in the Support Element panels, and can be varied online or offline by using the same facilities as for a normal CHPID.

Note, however, that OS/390 will never see the PCICC as an S/390 CHPID, but only as an AP.

Note

Crypto PCIs will not be defined in an IOCDS. However, if there are CHPID definition conflicts in the IOCDS (that is, if a CHPID is defined in the IOCDS with a number that matches the CHPID number attributed to the PCICC as per the plugging rules), a system power-on reset will cause both the already IOCDS-defined CHPID and the PCICC to not come online, and an error message will be displayed.

2.2.2.2 AP number assignment

The AP number assignment for a newly installed PCICC card is done at system power-on time or during the PCICC concurrent installation procedure (note that we did not practice the concurrent installation process, as it was not available at the time of this residency). The AP numbers are assigned to the PCICC cards in sequence, starting with AP 00. From this point on the AP number is bound to the PCICC card serial number.

At system power-on reset, the following occurs:

- The SE (support element) passes the cryptographic configuration information to the system Licensed Internal Code (LIC), including the AP IDs-to-CHPID assignment information.
- The system LIC allocates the Hardware System Area space needed for the maximum possible number of PCICC APs (which is eight), whether they are actually installed or not. This will allow the hotplugging of additional cards in the future.

Releasing an AP ID--that is, severing the relationship between an AP number and the PCICC card serial number--can only be done by a manual intervention at the system Support Element. This has to be done when replacing the PCICC card, as an AP/PCICC card affinity should not be changed even if card is moved around in a system. 3.3.4, “Removing one PCICC” on page 38 contains an example of AP ID release.

2.2.2.3 Moving PCICC cards

The following sections describe how and why PCICC cards can be moved within a system.

Adding a PCI card (hotplugging or powering off)

This card addition can take place either while the system is running (hotplugging), or while it is powered off. Note, however, that if the system is powered off, the AP assignment will not occur until the system is powered on. The AP assignment looks for any unassigned AP IDs and assigns one of them to the newly installed card.

Moving a PCICC card within a system

A PCICC feature card can be moved in the system (and this may possibly be an MES installation requirement) without changing the AP ID-to-PCICC card serial number relationship.

To uninstall a PCICC card, IBM service personnel first use the Nondestructive Hardware Change icon (in the CPC Configuration task) at the system Support Element, then the Remove function. Note that *this does not free up the AP ID.*

Repairing or replacing a PCICC card

If you repair or replace a PCICC card, the new PCICC card gets assigned the same AP number as the old card.

Moving a PCICC card between systems

When a PCICC card is removed from the system, either by an MES or as the result of a repair action, service personnel use the AP Manager window on the system Support Element and use the Release function to release the AP ID of the card being removed.

2.3 PCICC microcode load

In the following sections we describe the organization of the firmware in the 4758-based PCICC and the related installation and system management tasks.

2.3.1 The IBM 4758 CCA application

The IBM 4758 CCA application is a set of firmware which resides in the 4758-based card memory. This firmware implements the CCA functions that can be performed by the card. The CCA application firmware uses the 4758 hardware engines to perform DES, RSA, and other cryptographic functions. The related functions are architected according to a requestor/server model where:

- The server is in a secure processing environment coprocessor.
- The major components of the server are a command distributor, command processors, an access control manager, and a Master Key manager.
- The requests, as served by the card, are atomic units of work.
- The coprocessor maintains the state of:
  - The Function Control Vector (FCV)
  - The roles and profiles
  - The Master Keys and associated registers
  - The retained keys

The 4758-based card contains firmware to manage its specialized hardware and to control the loading of additional software. The supporting firmware includes the IBM CP/Q++ control program, that is the operating system for the 486 processor, which provides the base for cryptographic application support within the card. The integrity of the card firmware is controlled by digital signature when it is loaded.

The PCICC hardware on G5/G6 supports the secure loading into the PCICC firmware of user-customized extensions to the cryptographic functions provided. Software support to enable this capability will be provided in a future release of OS/390: the User Defined Extension (UDX) facility can be used to add custom functions to the standard CCA command set. Custom functions are executed inside the secure module of the 4758-based card with the same security as the other CCA functions.

2.3.2 The software hierarchy in the coprocessor

As shown in Figure 10, three segments of microcode need to be loaded into the card

- Seg 1 Miniboot, which is the “factory” default level when shipped
- Seg 2 CP/Q++, which is empty when shipped from the factory
- Seg 3 CCA, which is empty when shipped from the factory

Segments must be loaded or reloaded in sequence 1, 2, 3. During Load/Reload, each segment signature is verified. As one segment is reloaded, the higher segment is erased and also has to be reloaded.

In the PCICC, the card’s firmware is reloaded only when there is a mismatch detected between the code and FCV image kept in the system HSA, and the code and FCV currently loaded into the card. The reload can take place only during a system power-on reset or during a CHPID reset of the PCICC. Note that the card is not automatically zeroized when such a reload occurs.

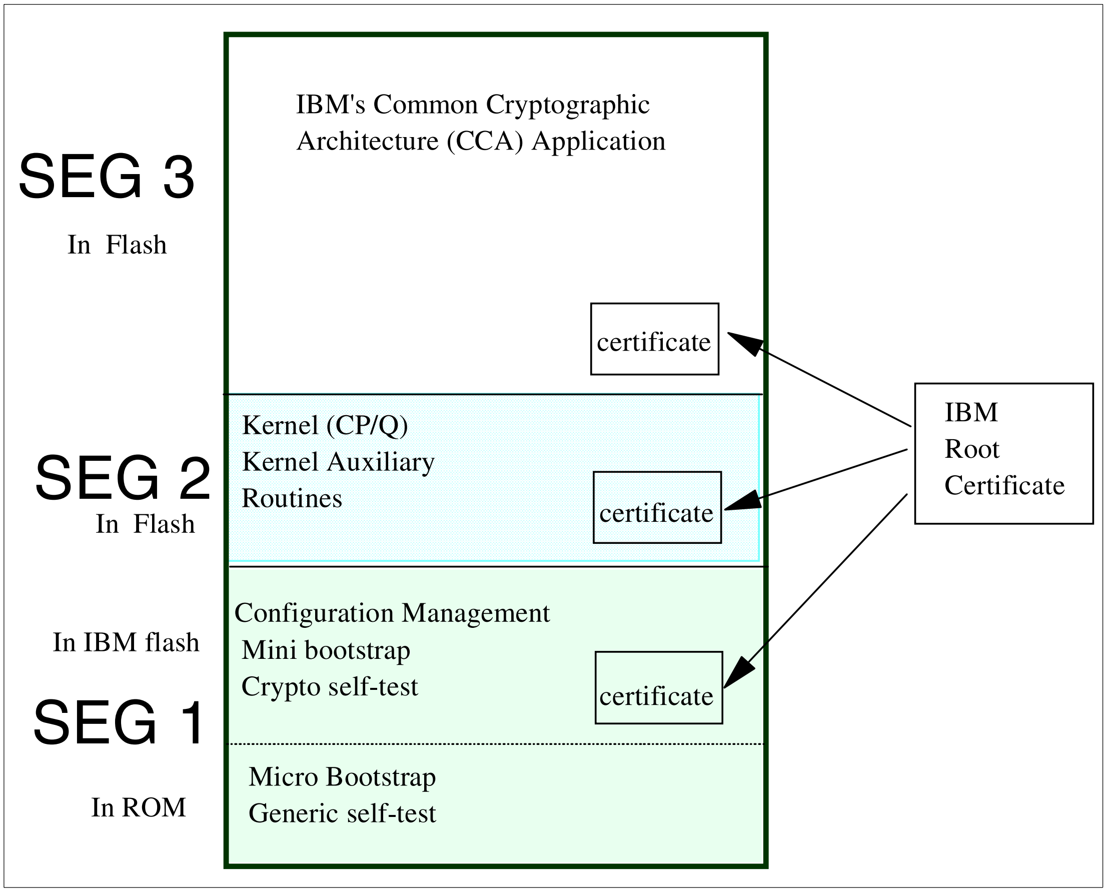


Figure 10. Crypto software architecture in the IBM 4758 Technology

2.3.2.1 Segments definition

The design for the IBM 4758 Technology was motivated by the need to simultaneously satisfy the following requirements:

1. Code must not be loaded into the coprocessor unless IBM has authorized the operation.

2. Once loaded into the coprocessor, the code must not run or accumulate state unless the environment in which it runs is trustworthy.
3. Agents outside the coprocessor that interact with code running on the coprocessor must be able to verify that the code is legitimate and that the coprocessor is authentic and has not been tampered with.
4. The shipment and configuration of coprocessors, their maintenance, and upgrades to the code inside a coprocessor must not require trusted couriers or security officers.

To satisfy these requirements, the card design defines four “segments”:

- **Segment 0** is in ROM and contains one portion of “Miniboot”. Miniboot0 is the most privileged software in the coprocessor and, among other things, runs a basic health test of the card and securely loads segment 1, if needed.
- **Segment 1** is in flash memory and contains the other portion of “Miniboot”. The division of Miniboot into a ROM portion and a Flash portion preserves flexibility (the Flash portion can be changed if necessary), while guaranteeing a basic level of security implemented in the unmodified ROM portion.

  Miniboot 1 runs a more extensive health test (POST) on the card and securely loads segment 1 (itself), segment 2, and segment 3, if required.
- **Segment 2** is in flash memory and contains the 486 operating system with the device drivers that are used to control the cryptographic engines and the PCI bus interface.
- **Segment 3** is in flash memory and contains the CCA applications.

Detailed information on the 4758 Technology code segments concepts and mechanisms can be found at the IBM 4758 PCI Cryptographic Coprocessor site:

```
http://www.ibm.com/security/cryptocards
```

You then click the **Library** link.

2.3.2.2 Code-Signing Key Hierarchy

The code-signing key hierarchy consists of a pair of asymmetric keys assigned to each segment, the principle being that segment level n verifies the signature of segment level n+1 contents and associated information. This mechanism is used to guarantee both the integrity of the code executed inside the coprocessor, and that the code is executed on an identified and known coprocessor.

2.3.3 PCICC microcode patches

You can patch PCICC code, when necessary, by using the standard microcode change process (MCL). The microcode changes can affect the 4758-based card microcode itself and/or the STI adapter and controller unit in the PCICC. Such changes are not expected to be disruptive to the system, because activating a patch requires you to reset the PCICC, which makes it only temporarily unavailable to the applications.

As usual, patch apply is concurrent whenever possible. In some special cases, when both the 4758-based card and the STI controller need a microcode update, then the patch is flagged as disruptive and can only be applied with a POR.

Segments 1 to 3 of the PCICC can be Licenced Internal Code (LIC)-updated through the MCL process.

2.3.4 Function Control Vector (FCV) enablement

This section briefly describes the PCICC enablement concept using the FCV diskette. The diskette must be ordered from IBM and installed either by the customer or by IBM service.

As for the CCF enablement diskette, it is intended to enable the cryptographic capabilities of the device while still meeting export and country of use regulations. 3.2, “Feature codes” on page 31 provides information about the feature codes pertaining to the PCICC FCV diskette.

2.3.4.1 Enablement of the CCF

Since its original implementation on G3 systems, the CCF Crypto Configuration Control (CCC) bits are set according to a Crypto configuration file installed on the system Support Element hard disk. The CCC bits dictate to the CCF hardware which algorithms and key lengths are enabled. The system is shipped out of manufacturing with the CCF CCC bits reset.

The Crypto configuration files are installed by “importing” to the Support Element hard disk the contents of the Crypto Enablement Diskette obtained from IBM. The CCF CCC bits will be set during the system Power-on reset which follows, if the imported file has been selected by the “Select for Next Activation” option on the Support Element.

If the CCF was already enabled and if the just-imported diskette corresponds to a new CCC bits configuration, then the system power-on reset will set the new value in the CCC bits but will also zeroize the CCF (that is, Master Keys and authorities will have to be entered again).

Each Crypto configuration file is unique and intended for a specific CCF Crypto Module ID (CMID), which is the number that uniquely identifies a CCF chip. In practice, there is a CCF enablement diskette per system that contains the configuration files applying to the two CCF chips installed on that system.

2.3.4.2 Enablement of the PCICC

The equivalent PCICC configuration value is known as the Function Control Vector (FCV). Note that an FCV is *not unique* to each PCICC, but *it is unique* to the S/390 machine serial number.

The FCV is delivered on a diskette. Because it is specific to the machine serial number, it is common to *all* PCICC cards installed in this system. As a consequence, there is no need to import a new FCV during a PCICC repair or when installing an additional PCICC. As a matter of fact, in contrast to the CCF, a spare PCICC card from the stock will not come with an FCV diskette.

The FCV enablement process

The FCV enablement process consists of the following steps:

1. The Import FCV function at the Support Element copies the PCICC Crypto configuration files to the Support Element hard disk.

2. The FCV is then uploaded into the system Hardware System Area (HSA), either as a result of a system power-on reset, or by an option named Load FCV to HSA Immediately at the Support Element.
3. The FCV is downloaded from the HSA into the PCICC cards as a result of either a system power-on reset or of a CHPID reset (that is, by varying a CHPID offline, then online, at the Support Element).

Important

1. Installed PCICC cards go into a check stop state if there is no FCV in HSA when performing a system power-on reset or a CHPID reset.
2. Replacing an existing FCV with a new one can only be done by a system power-on reset. The PCICC card is not zeroized as a consequence of replacing the FCV.

4.2.2, “Import FCV” on page 56 provides more details on PCICC enablement operations.

2.4 OS/390 2.9 and the Integrated Cryptographic Services Facility (ICSF)

This section contains a brief description of the changes implemented in OS/390 2.9 and its Integrated Cryptographic Service Facility (ICSF) component to support the PCICC and the new version of the TKE workstation.

2.4.1 OS/390 2.9 support for PCICC

OS/390 2.9 provides for the support of the PCI Crypto coprocessor in two ways:

1. The IO Supervisor functions have been enhanced to detect and report the change in card condition when the card is being varied online from the Support Element menu.
2. ICSF 2.3 is part of the OS/390 2.9 base. ICSF 2.3 provides the functions required to support the PCI Crypto Coprocessor (PCICC) along with the Crypto Coprocessor Facility (CCF) chip. It also provides the software piece required to establish connectivity between the TKE and the Crypto coprocessors via TCP/IP protocol.

   Note that, starting with OS/390 2.4, ICSF is an OS/390 “exclusive” product, meaning that it cannot be delivered outside of the base OS/390; therefore ICSF 2.3 should be referred to externally as *OS/390 2.9 ICSF* in order to avoid any confusion.

2.4.2 ICSF overview

ICSF provides support for the following:

- The Commercial Data Masking Facility (CDMF), an exportable version of DES cryptography
- DES and Triple DES encryption for privacy
- The transport of data keys through the use of the Rivest-Shamir-Adelman (RSA) public key algorithm

- The generation and verification of digital signatures through the use of both the RSA and the Digital Signature Standard (DSS) algorithm
- The generation of RSA and DSS key.
- The SET Secure Electronic Transaction standard, which was created by Visa International and MasterCard
- The PKA Encrypt and PKA Decrypt callable services that can be used to enhance the security and performance of Secure Sockets Layer (SSL) security protocol applications

2.4.2.1 ICSF 2.3

ICSF 2.3 contains FMID HCRP230 (product 5647-A01) and supports both the CCF and the PCI CC in terms of providing cryptographic services to the requesting applications; providing device specific management facilities; providing routing to the best fit device (that is, either the Crypto chip or the PCI card, based on the requested service and/or an attempt to balance the cryptographic workload between the installed coprocessors).

As with previous releases, ICSF provides an interface to manage the cryptographic coprocessors via TSO/E ISPF panels and/or the TKE application menus. The TKE application menus are discussed in 5.3, “TKE application: managing host Crypto coprocessors” on page 104.

Among the new ICSF ISPF panels, the PCICC management panel allows you to do the following:

- Display the state of PCICCs
  - Online/Offline
  - Active
  - Temporarily Unavailable
  - Deactivated
  - Hardware Error detected
  - Unknown
- Deactivate a PCICC
- Activate a PCICC

2.4.2.2 Managing Master Keys

There are new hardware status panels to display detailed status and verification patterns of the PCI Crypto coprocessor Master Key registers. The display is provided for all PCICCs or for each PCICC individually, and the panels allow you to enter Master Keys again for all PCICCs or for each PCICC individually.
The format and structure of the panels are the same as for the CCFs, with two coprocessors per panel.

2.4.2.3 Enhanced Pass Phrase Initialization

Using Pass Phrase Initialization is an easy way to initialize Master Keys (both for DES and PKA Master Keys) and the Cryptographic Key Data Set (CKDS) for the first time: by having the user enter a pass phrase, the system will automatically generate related Master Key values (both for the DES and the PKA Master Keys). It will also install them in the CCFs and initialize the target empty CKDS with the just-generated DES Master Key.

Pass phrase initialization at OS/390 2.9 is extended to install Master Keys for all online PCICCs. Furthermore, as new PCICCs are installed, the Pass Phrase can also be used to initialize the new PCICCs (the same Pass Phrase yields the same key value).

Pass Phrase Initialization offers the option of setting the CCF SMK equal to KMMK, which is the recommended option when PCICCs are in operation in the system.

2.4.2.4 RSA key token change

A new private key section, with identifier X'08', is now available for internal and external key tokens. This is the optimized Chinese Remainder Theorem form of the private key, which yields better performance than the Modulus-Exponent (ME) tokens for modulus of the same length. The supported modulus bit length is 512 to 2048.

Note: CRT tokens are only usable by the PCICC.

A new ME form of the private key internal token, X'06', can be used on CCF or PCICC. This new form is intended for compatibility purpose with the existing 4758 applications. The supported modulus bit length is 512 to 1024.

The current external form of the private key token, X'02', is left unchanged, and can be converted to the X’06’ form through re-import of the token on a system with PCICC.

The Symmetric Key Generate/Export/Import and the PKA Encrypt/Decrypt services allow you to specify a new RSA key usage indicator in the rules array: KM-ONLY. This keyword indicates that the key may only be used for key distribution functions and not for digital signatures.

2.4.2.5 Retained keys support

Retained keys are generated in a PCICC and the private key never appears outside the secure hardware in any form. The public key token of the retained key is written to the Public Key Data Set (PKDS) with the serial number of the PCICC that contains the private key. A retained key may only be used from the same domain it was created in, and applications that use the retained key will fail if the specific PCICC is not online.

A request for retained key generation is routed by ICSF to any ACTIVE PCICC. Two new services are made available for retained key management: Retained Key Delete (CSNDRKD) and Retained Key List (CSNDRKL).

2.4.2.6 Routing work between CCF and PCICC

The routing of work between CCF and PCICC is based on the following criteria:

- The functional capability required for the requested service.
- The best performance in accomplishing the requested service.
- The best security environment provided when performing the service.

Functional capabilities

The following functions use the PCICC:

- Utilization of CRT tokens
- Utilization of retained keys
- RSA key generation

The following functions use the CCF:

- Utilization of the Digital Signature Standard (DSS)
- Utilization of the existing ME X'02' tokens

Considerations for performance

The following existing synchronous CCF functions perform considerably faster on CCF:

- DES, MAC, and the hashing function
- PIN functions
- DES key management functions

Public key operations which perform considerably better on CCF are Digital Signature Verify and PKA Encrypt.

Considerations for security

The functions Set Block Compose/Decompose and Symmetric Key Generate/Export/Import, as implemented with the CCF, allow the symmetric DES key to be briefly exposed in storage.

In contrast, the PCICC implementation of these functions keeps the symmetric DES keys in the coprocessor secure area at all times.

Where function, performance, or security are not issues (such as with Digital Signature Generate and PKA Decrypt), calls will be routed to CCFs or PCICCs using the ICSF internal work balancing algorithm.

Note

For maximum flexibility, the CCF Signature Master Key (SMK) should be the same as the Key Management Master Key (KMMK).

2.4.2.7 Enhanced callable services

The following PKA services have been enhanced to take into account the new CRT form tokens and the preferred coprocessor type to execute these services..

- PKA Key Generate (CSNDPKG)
- PKA Key Token Build (CSNDPKB)
- PKA Key Import (CSNDPKI)
- PKA Public Key Extract (CSNDPKX)
- Digital Signature Generate (CSNDDSG)
- Symmetric Key Generate (CSNDSYG)
- Symmetric Key Export (CSNDSYX)
- Symmetric Key Import (CSNDSYI)
- Set Block Compose (CSNDSBC)
- Set Block Decompose (CSNDSBD)
- PKA Encrypt (CSNDPKE)
- PKA Decrypt (CSNDPKD)
- PKDS Record Create (CSNDKRC)
- PKDS Record Delete (CSNDKRD)
- PKDS Record Write (CSNDKRW)

These services are documented in *OS/390 ICSF Application Programmer's Guide,* SC23-3976. A high-level overview of these enhancements is provided in Appendix B, “Support functions: ICSF services” on page 141.

2.4.2.8 New callable services

The following new PKA services have been implemented to take into account the specific capabilities of the PCICC.

- Retained Key Delete (CSNDRKD)
- Retained Key List (CSNDRKL)
- PCI Interface Service (CSFPCI) - this service is the equivalent, for the PCICC, of the Public Key Secure Cable (PKSC) service that is used for secure communication between the CCF and the TKE. As for the PKSC service, PCICC is not intended to be documented to ICSF users.

These services are documented in *OS/390 ICSF Application Programmer's Guide*, SC23-3976. A high-level overview of these new services is provided in Appendix B, "Support functions: ICSF services" on page 141.

2.4.2.9 ICSF/TSS Reason code conversion option

ICSF and TSS have consistent API for callable services. Their return codes are consistent, but the reason codes are mostly specific to either one of them. There is a reason code conversion option available via new variables in the Options Data Set:

- REASONCODE(ICSF) is the default option. It indicates that all reason codes returned by the callable services abide with the reason code values designated for ICSF.

- REASONCODE(TSS) indicates that the reason codes returned by the callable services match the TSS reason codes. This option is intended to facilitate the migration of TSS applications onto S/390.

Note: There is no one-to-one correspondence between ICSF and TSS reason codes; in fact, there is often a one-to-many or many-to-one relationship, or there may be no correspondence at all.

Keep this in mind when using REASONCODE(TSS); you may have to modify the migrated applications so they will properly handle ambiguous results.

2.4.2.10 System symbol recognition

ICSF 2.3 supports system symbol recognition in the Installation Options Data Set parameters. This allows customers to manage multiple LPARs or systems using the same options data set and one startup procedure.

The logical records of the options data set are echoed into the diagnostic data set CSFLIST in the startup procedure. Each record is listed before and after symbol substitution. Therefore, the CSFLIST must *not* be shared between ICSF instances.

2.4.3 New SMF Record Type 82 subtypes

This release also includes support for the following new subtypes for SMF Record Type 82:

- Subtype 14 – PCI Cryptographic Coprocessor Clear Master Key Entry

- Subtype 15 – PCI Cryptographic Coprocessor Retained Key Create/Delete
  Subtype 16 – PCI Cryptographic Coprocessor TKE

- Subtype 17 – PCI Cryptographic Coprocessor Timing

- Subtype 18 – PCI Cryptographic Coprocessor Configuration

2.4.4 The new TKE workstation (TKE V3.0)

A new TKE workstation version (TKE V3.0) is required to support the PCICC. Details are provided in Chapter 5, “Customizing PCICC and CCF using a TKE V3.0” on page 89.

You can check your current TKE level; it is briefly displayed at the bottom of the screen when the TKE application starts.

Notes

1. TKE V3.0 communicates with the OS/390 host using TCP/IP.
2. It uses a 4758-2 cryptographic adapter card.
3. The Key Transfer function, which enabled the secure extraction of a Master Key from one system and its transfer to another system, is no longer available.
4. The TKE V3.0 does not support a smart card reader, as of the writing of this book.
5. The previous TKE versions are not upgradable to the new TKE V3.0.

Chapter 3. Planning

In this chapter we describe the hardware requirements when installing the PCICC, as well as the feature codes you should order and the 9672 plugging rules.

3.1 Hardware requirements

The hardware requirements for PCICC installation are as follows:

- The PCICC is only supported by 9672 G5, G6, and follow-on systems.
- The maximum number of PCI Cards that can be installed in a 9672 G5 or G6 is eight.
- The 9672 minimum LIC level required is Driver 26.
- The PCICC cannot operate if the CCF itself is not enabled and in operation.
- The HSA space consumed by the PCICC is 14.5 MB. This value is independent of the number of installed cards.

IBM Customer Engineers are responsible for installing the hardware by following the Installation Instructions that are generated for a specific system serial number. These instructions describe the card movements which may be required on the specific system to perform the PCICC card installation, and they are therefore dependent on the accuracy of the system configuration as recorded in the IBM Vital Product Data (VPD) database.

3.2 Feature codes

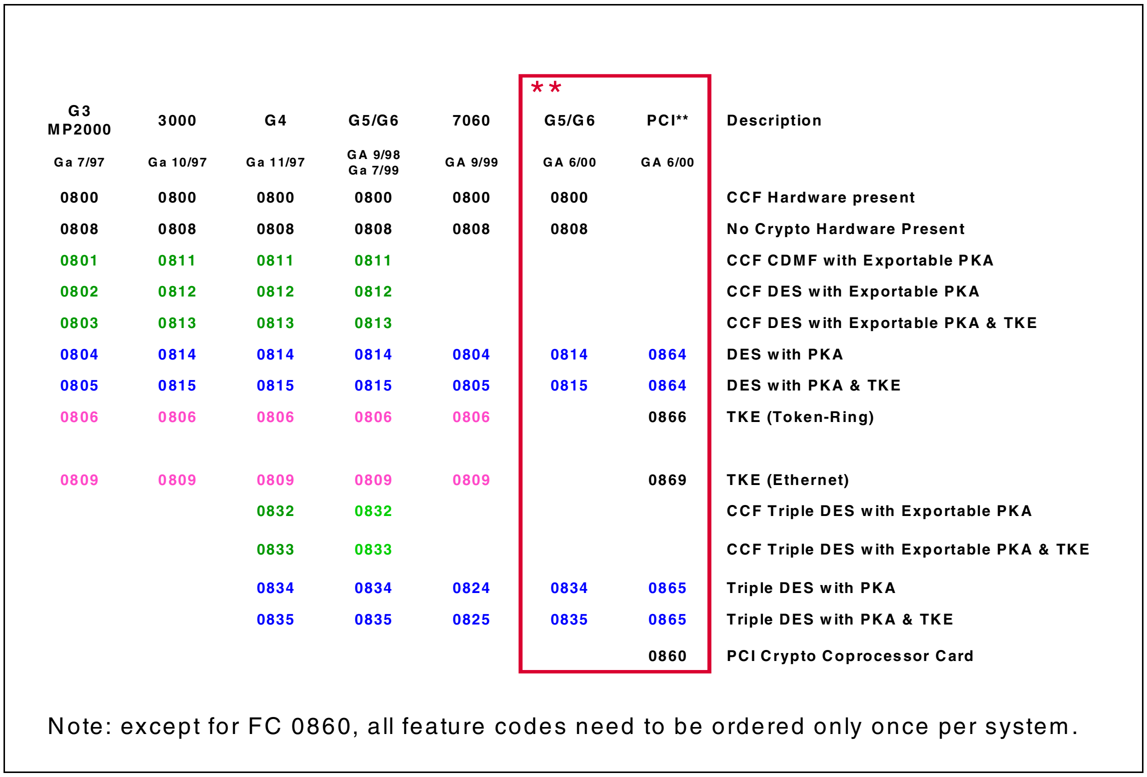
Figure 11 on page 33 summarizes the CCF and PCICC feature codes. Note the following points:

- Because CCF enablement is a prerequisite to the installation of a PCICC, the feature codes 0814, 0815, 0834, or 0835 must have been ordered and installed. These are the features corresponding to the CCF enablement diskette, as the CCF hardware feature (0800) is standard on G4 systems and above.
- The TKE enablement feature pertains only to the CCF feature codes. TKE enablement is specified by ordering CCF feature code 0815 or 0835.
- The TKE hardware itself (TKE V3.0) is orderable by selecting the feature code 0866 (TKE workstation with a token ring adapter), or the feature code 0869 (TKE workstation with an ethernet adapter).

- As of the time of writing, a Security Interface Unit (SIU) is not proposed for attachment to the TKE V3.0.
- Each PCICC card to be installed in the system has feature code 0860.
- The PCICC enablement diskette (FCV) is orderable by using the feature code 0864 (DES with PKA) or 0865 (T-DES with PKA). This feature code must also match the encryption strength ordered for the CCF. As already mentioned, there is no PCICC feature code pertaining to the TKE enablement. Also, you only order the feature code once, since a single FCV diskette covers all possible PCICC cards in a given system serial number.

In Figure 11 on page 33, the valid feature codes for a 9672 G5 or G6 are inside the box marked with a double asterisk (**). For example, for a PCICC card enabled for T-DES and managed by a TKE, the following feature codes have to be ordered:

- 0865
- 0866 or 0869
- 0860



G3 MP2000	3000	G4	G5/G6	7060	** G5/G6	PCI**	Description
Ga 7/97	Ga 10/97	Ga 11/97	GA 9/98 Ga 7/99	GA 9/99	GA 6/00	GA 6/00	
0800	0800	0800	0800	0800	0800		CCF Hardware present
0808	0808	0808	0808	0808	0808		No Crypto Hardware Present
0801	0811	0811	0811				CCF CDMF with Exportable PKA
0802	0812	0812	0812				CCF DES with Exportable PKA
0803	0813	0813	0813				CCF DES with Exportable PKA & TKE
0804	0814	0814	0814	0804	0814	0864	DES with PKA
0805	0815	0815	0815	0805	0815	0864	DES with PKA & TKE
0806	0806	0806	0806	0806		0866	TKE (Token-Ring)
0809	0809	0809	0809	0809		0869	TKE (Ethernet)
		0832	0832				CCF Triple DES with Exportable PKA
		0833	0833				CCF Triple DES with Exportable PKA & TKE
		0834	0834	0824	0834	0865	Triple DES with PKA
		0835	0835	0825	0835	0865	Triple DES with PKA & TKE
						0860	PCI Crypto Coprocessor Card

Note: except for FC 0860, all feature codes need to be ordered only once per system.

Figure 11. Crypto feature codes

3.3 The PCICC installation task

In this section we discuss the steps involved in performing a PCICC installation, using an actual scenario as an example.

3.3.1 Our installation

We performed a PCICC installation on the Montpellier Products and Solutions Support Center (PSSC) 9672 RX6 system by executing the following steps:

1. We first upgraded the Support Element code from Driver 22 to Driver 26. (This is expected to be the most common case for G5 and G6 at general availability of the PCICC.)

   As a preliminary step for the EC upgrade, the HMC needs to be at Driver 26. The HMC can be upgraded concurrently with the system operations.

   We used an SE code CD-ROM at Driver 26 and loaded the code from the HMC to the SE, using the EC upgrade from the HMC option.

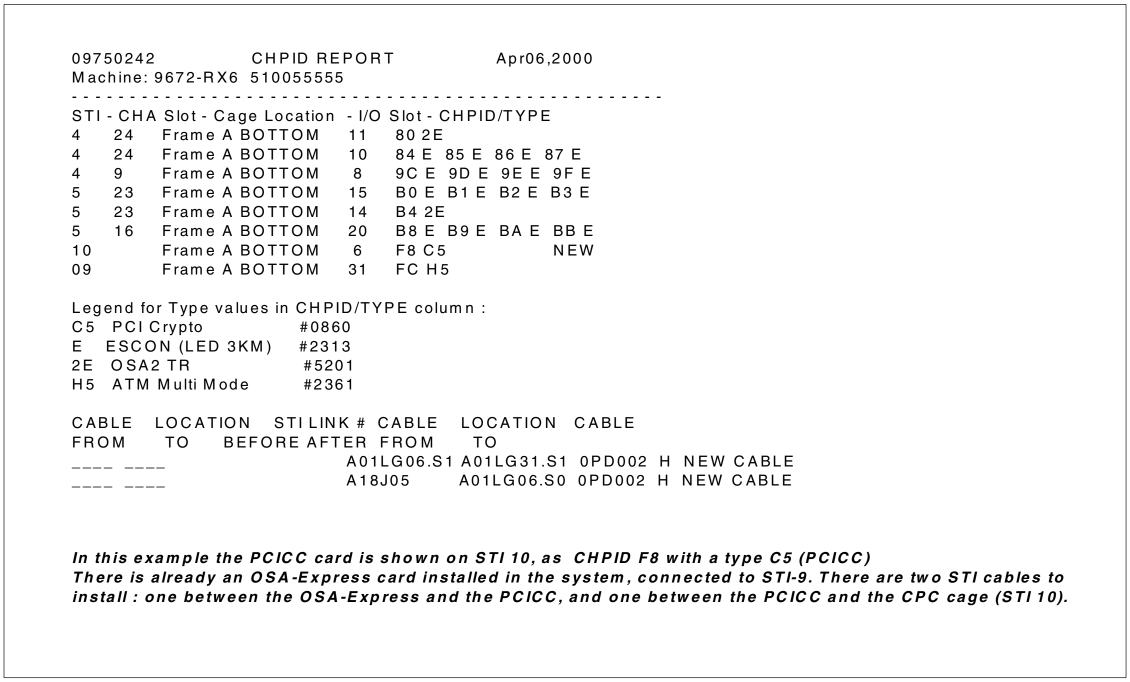
Note: Driver 26 installation on the SE is disruptive for the system.

2. We obtained the latest MCLs, then installed and activated them. In most cases these MCLs are pre-pulled into a Service Update Level - Read Only Cartridge (SUL-ROC).
3. We then verified that the correct CCF cryptographic configuration had been enabled by using the Cryptographic Coprocessor Configuration icon on the SE.

   In our case we wanted to install PCICC feature code 0865, which required CCF feature code 0835 (as we also intended to use the TKE). The CCF feature code was actually 0812, so we had to get and import a CCF enablement diskette with feature code 0835. The enablement was completed by a system power-on reset.

   All the SE-related tasks are described in *Support Element Operations Guide*, GC38-0608.
4. At the time of our residency, there was no concurrent plug capability for the PCICC card; therefore, we installed our PCICC MES with the system being powered off. We installed the PCICC card at a pre-defined location as indicated in the MES Installation Instructions, where the configurator CFREPORT/CHPID REPORT outputs are given. The STI cable was also plugged in according to the locations given by the MES Installation Instructions.

   Refer to Figure 12 on page 35 for the CFREPORT/CHPID REPORT that was produced for our system.
5. We imported the FCV diskette and selected the FCV at the SE. This enabled the PCICC cryptographic functions at the following power-on reset.
6. We then updated the image profiles of the logical partitions that needed access to the cryptographic coprocessors. 4.3, “LPAR setup” on page 61 provides further details on how to set up the logical partition image profiles.
7. The system was activated.



```
09750242            CHPID REPORT            Apr06,2000
Machine: 9672-RX6  510055555
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
STI - CHA Slot - Cage Location  - I/O Slot - CHPID/TYPE
4    24    Frame A BOTTOM    11    80 2E
4    24    Frame A BOTTOM    10    84 E  85 E  86 E  87 E
4    9     Frame A BOTTOM     8    9C E  9D E  9E E  9F E
5    23    Frame A BOTTOM    15    B0 E  B1 E  B2 E  B3 E
5    23    Frame A BOTTOM    14    B4 2E
5    16    Frame A BOTTOM    20    B8 E  B9 E  BA E  BB E
10         Frame A BOTTOM     6    F8 C5              NEW
09         Frame A BOTTOM    31    FC H5

Legend for Type values in CHPID/TYPE column :
C5   PCI Crypto            #0860
E   ESCON (LED 3KM)     #2313
2E   OSA2 TR               #5201
H5   ATM Multi Mode        #2361

CABLE   LOCATION   STI LINK #  CABLE   LOCATION   CABLE
FROM     TO     BEFORE AFTER  FROM      TO
____  ____                    A01LG06.S1 A01LG31.S1  0PD002  H  NEW CABLE
____  ____                    A18J05      A01LG06.S0  0PD002  H  NEW CABLE
```

In this example the PCICC card is shown on STI 10, as CHPID F8 with a type C5 (PCICC)
There is already an OSA-Express card installed in the system, connected to STI-9. There are two STI cables to install : one between the OSA-Express and the PCICC, and one between the PCICC and the CPC cage (STI 10).

Figure 12. CHPID Report

3.3.2 Concurrent installation of the PCICC

At the time of writing, the ability to install the PCICC without disrupting system operations was not available. Therefore, this section describes our exercising of the technical ability, not an actual experience.

Assumptions

- The system Support Element has already been upgraded to Driver 26, and the MCLs required for the concurrent installation of the PCICC have been installed and activated.
- The CCF cryptographic configuration in effect matches the PCICC intended configuration. As an example, the CCF has been enabled with feature code 0815 and the PCICC to install will have feature code 0864.
- The logical partitions' image profiles have already been set up with the new PCICC page, where the PCICC APs intended to be installed have been entered into the candidate list.

  Note: This setup is *not dynamic*. While it does not require the cards to be physically installed in the system, it must be done with the logical partition de-activated. Refer to 4.3, “LPAR setup” on page 61 for details about this setup.

- The IBM CE has the PCICC cards, the new STI cables, the PCICC FCV diskette, and the MES Installation Instructions available.
- Installing a PCICC, a FICON, or an OSA-Express requires that you follow the plugging rules described in 3.4, “The 9672 channel” on page 41. (A complete description of these rules can be found in the *FICON Planning Guide,* SG24-5445.)

  As a consequence of these rules, the movement of already-installed channel cards (ESCON, OSA2, or parallel) may be necessary. These channel cards can be moved concurrently, but will get new CHPID numbers and therefore will require a dynamic I/O configuration change.

  Note: If Coupling Facility channels need to be moved, it is a disruptive action since the CFC mother card cannot be unplugged or plugged concurrently.

  The PCICC card location and CHPID number is known from the Sales Ordering System the day the order is entered. The report from the configurator contains the relevant data in the CFREPORT/CHPID REPORT, and is normally supplied to the customer for planning purposes. Using this data it is possible to check for possible HCD configuration changes and to determine whether the CHPID number required for PCICC installation is free.
- The CE installs the PCICC cards and the STI cables using the Non-Disruptive Hardware Change option at the Support Element, and then imports the FCV diskette and selects the Load FCV to HSA Immediately option to upload the FCV to HSA without doing a system power-on reset.
- Finally, the PCICC CHPID must be configured online at the Support Element. This will trigger the loading of the microcode and FCV into the PCICC and make it available for crypto-enabled LPARs.

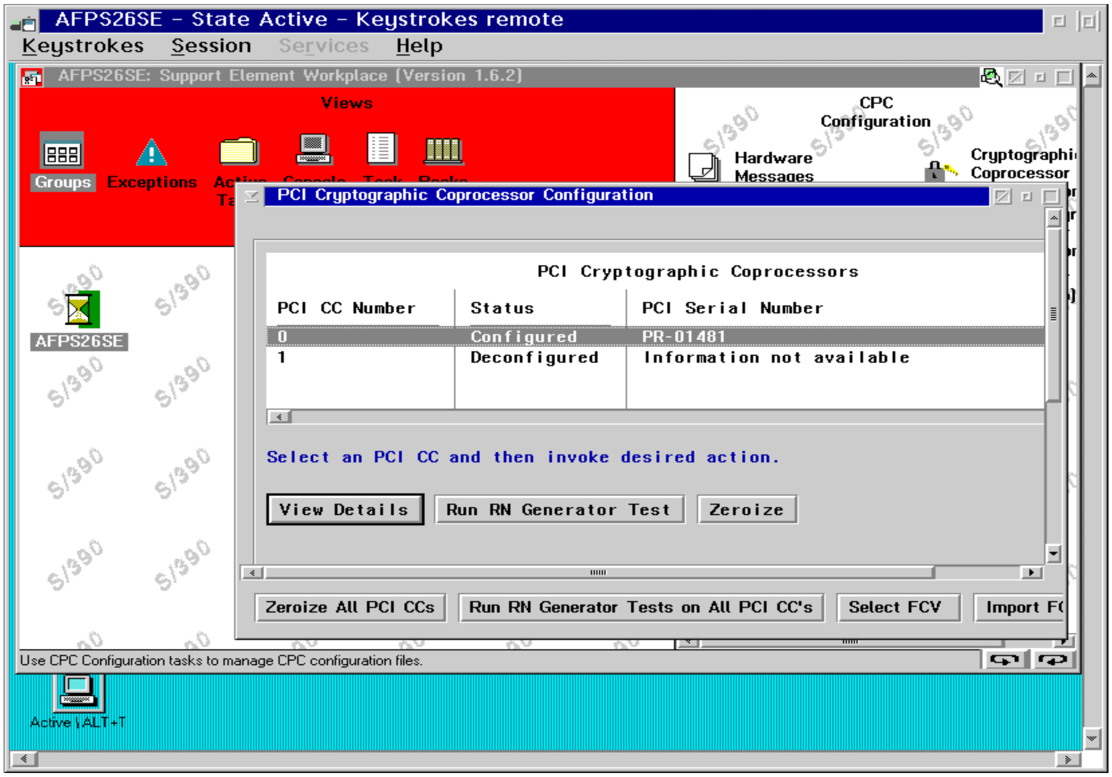
3.3.3 Adding a second PCICC

We performed the installation of a second PCICC card and captured some Support Element screens that are representative of the installation main steps.

The system has an OSA-Express on STI-9, CHPID FC, and the first PCICC on STI-10, CHPID F8. According to the plugging rules, the second PCICC will be installed in slot 32 of the I/O cage, as CHPID FD, and will also be connected on STI-9. That is, the new PCICC card will be “STI-chained” by connecting a short STI cable on the OSA-Express adapter and then connecting the new PCICC card to this cable.

Figure 13 shows the status of the two PCICC cards in the system.The first PCICC, AP0 (serial number PR-01481) is already configured. The second PCICC, AP1, has just been plugged in.

Looking at the CHPID status (which is not shown here), the first PCICC is CHPID F8 and is Online, Shared and Operating, whereas the second PCICC, CHPID FD, is in Standby.


AFPS26SE - State Active - Keystrokes remote
Keystrokes
Session
Services
Help
AFPS26SE: Support Element Workplace (Version 1.6.2)
Views
Groups
Exceptions
Hardware Messages
CPC Configuration
Cryptographic Coprocessor
AFPS26SE
PCI Cryptographic Coprocessor Configuration
View Details
Run RN Generator Test
Zeroize
Zeroize All PCI CCs
Run RN Generator Tests on All PCI CC's
Select FCV
Import F
Active \ ALT+T

PCI Cryptographic Coprocessors

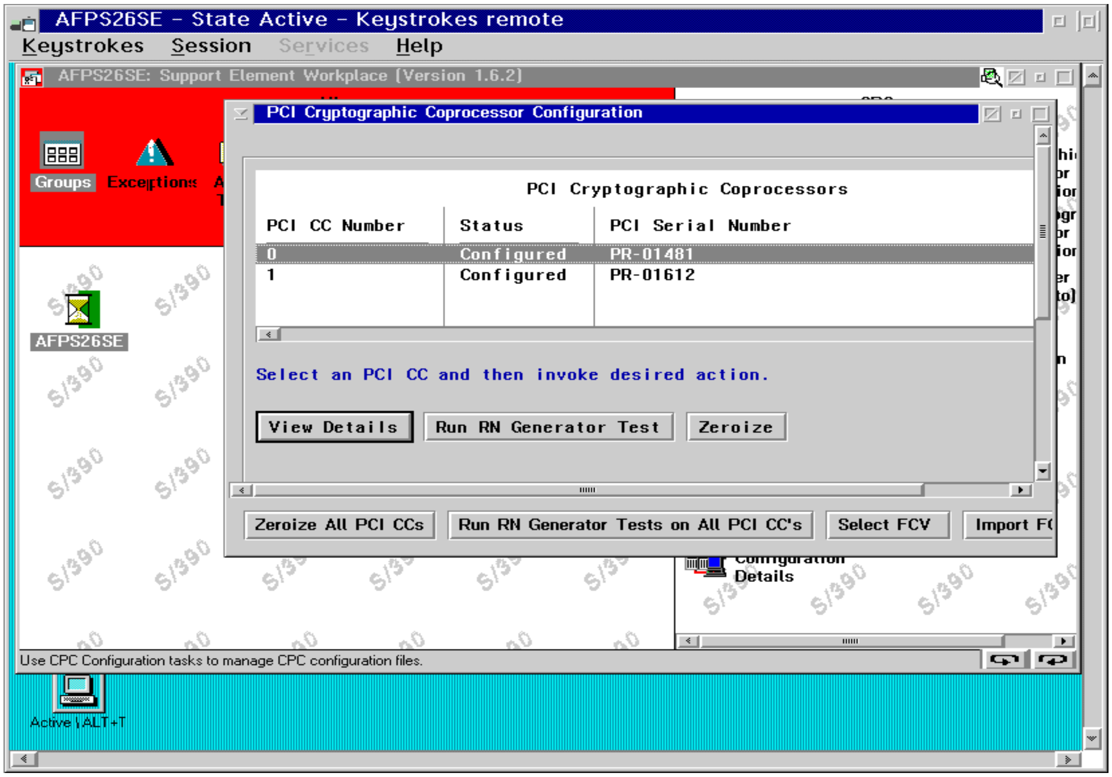
PCI CC Number	Status	PCI Serial Number
0	Configured	PR-01481
1	Deconfigured	Information not available

Select an PCI CC and then invoke desired action.

Use CPC Configuration tasks to manage CPC configuration files.

Figure 13. PCICC status before FCV loaded in PCI CC Number 1

After configuring the CHPID FD online, the AP1 becomes configured, as shown in Figure 14 on page 38, and the PCICC card serial number PR-01612 is displayed. Note that in this case there is already one FCV active in the system and we do not need to select the FCV for the second card.



PCI Cryptographic Coprocessor Configuration

PCI Cryptographic Coprocessors

PCI CC Number	Status	PCI Serial Number
0	Configured	PR-01481
1	Configured	PR-01612

Select an PCI CC and then invoke desired action.

Use CPC Configuration tasks to manage CPC configuration files.

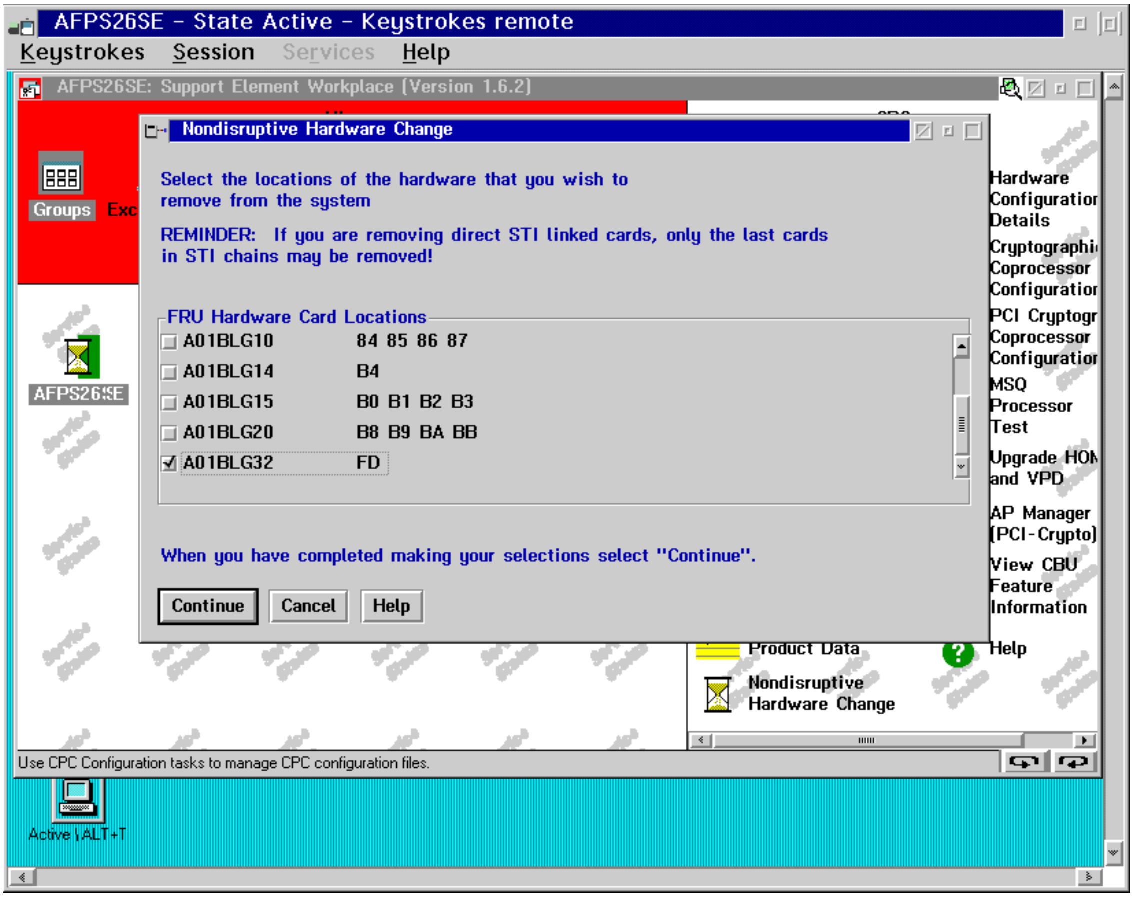
Figure 14. PCI CC status after FCV selected and CHPID configured online

3.3.4 Removing one PCICC

As an experiment, we removed a PCICC card from the system by executing the following steps:

1. We deactivated AP1 in the ICSF PCICC Management panel. The deactivate action is explained in more detail in 4.4.7, “Management of the PCI Cryptographic Coprocessors” on page 85.
2. We configured CHPID FD offline at the Support Element.
3. We invoked the Nondisruptive Hardware Change option at the Support Element, and removed the PCICC Card at position LG32 (that is, CHPID FD).

   Figure 15 on page 39 shows the Nondisruptive Hardware Change panel at the SE.



Nondisruptive Hardware Change

Select the locations of the hardware that you wish to remove from the system

REMINDER: If you are removing direct STI linked cards, only the last cards in STI chains may be removed!

FRU Hardware Card Locations

- □ A01BLG10 84 85 86 87
- □ A01BLG14 B4
- □ A01BLG15 B0 B1 B2 B3
- □ A01BLG20 B8 B9 BA BB
- ☑ A01BLG32 FD

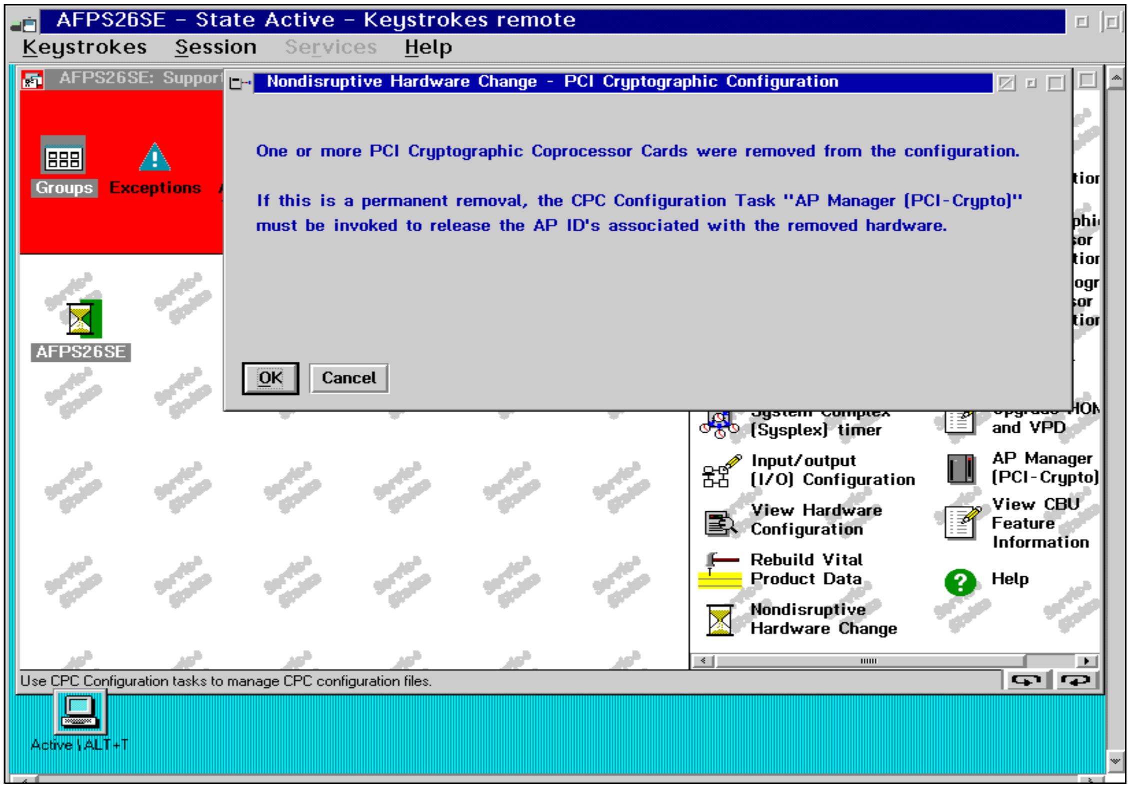
When you have completed making your selections select "Continue".

Use CPC Configuration tasks to manage CPC configuration files.

AFPS26SE - State Active - Keystrokes remote
Keystrokes
Session
Services
Help
AFPS26SE: Support Element Workplace (Version 1.6.2)
Groups
Exc
AFPS26SE
Continue
Cancel
Help
Hardware Configuration Details
Cryptographi Coprocessor Configuratior
PCI Cryptogr Coprocessor Configuratior
MSQ Processor Test
Upgrade HON and VPD
AP Manager (PCI-Crypto)
View CBU Feature Information
Product Data
Help
Nondisruptive Hardware Change
Active \ ALT+T

Figure 15. Nondisruptive Hardware Change panel at the Support Element

Figure 16 on page 40 shows the message received after physically removing the PCICC card from the I/O cage.



AFPS26SE - State Active - Keystrokes remote
Keystrokes
Session
Services
Help
AFPS26SE: Support
Nondisruptive Hardware Change - PCI Cryptographic Configuration
Groups
Exceptions
AFPS26SE
OK
Cancel
System Complex (Sysplex) timer
Upgrade HON and VPD
Input/output (I/O) Configuration
AP Manager (PCI-Crypto)
View Hardware Configuration
View CBU Feature Information
Rebuild Vital Product Data
Help
Nondisruptive Hardware Change
Active \ALT+T

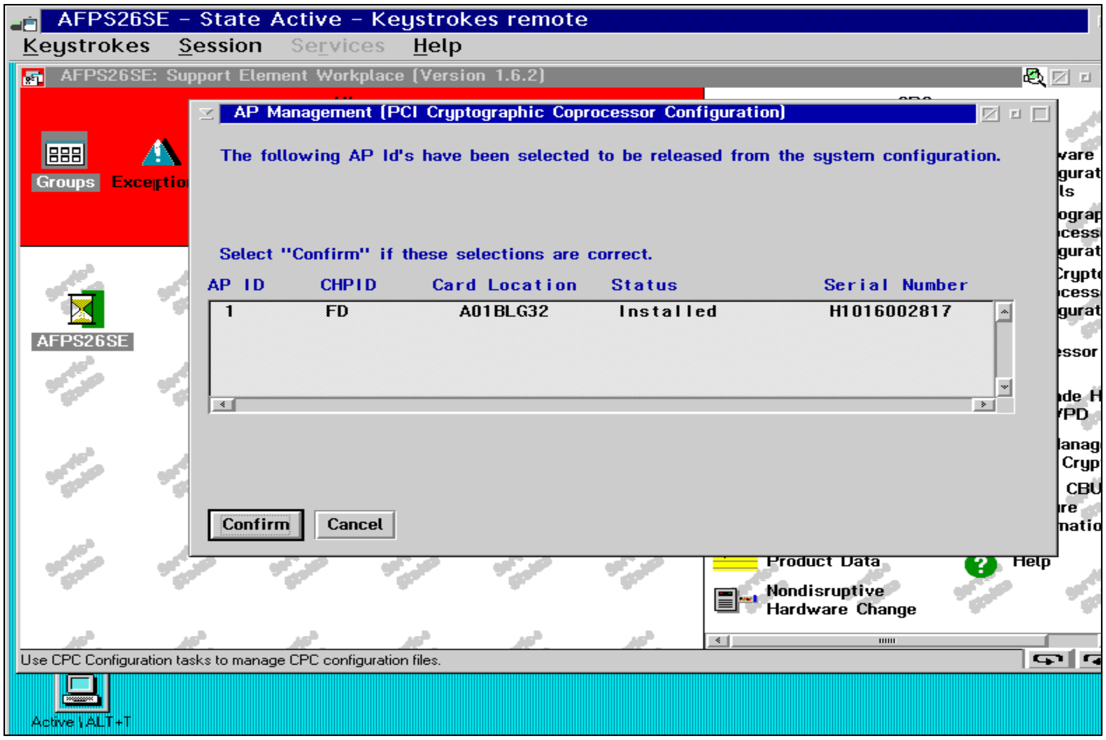
One or more PCI Cryptographic Coprocessor Cards were removed from the configuration.

If this is a permanent removal, the CPC Configuration Task "AP Manager (PCI-Crypto)" must be invoked to release the AP ID's associated with the removed hardware.

Use CPC Configuration tasks to manage CPC configuration files.

Figure 16. Msg. after PCICC Card removed by Nondisruptive Hardware Change

4. The last step is to release AP1, using the SE panel shown in Figure 17 on page 41.


AFPS26SE - State Active - Keystrokes remote
Keystrokes
Session
Services
Help
AFPS26SE: Support Element Workplace (Version 1.6.2)
AP Management (PCI Cryptographic Coprocessor Configuration)
Groups
Exceptio
AFPS26SE
Confirm
Cancel
Product Data
Help
Nondisruptive Hardware Change
Active \ ALT+T

The following AP Id's have been selected to be released from the system configuration.

Select "Confirm" if these selections are correct.

AP ID	CHPID	Card Location	Status	Serial Number
1	FD	A01BLG32	Installed	H1016002817

Use CPC Configuration tasks to manage CPC configuration files.

Figure 17. AP Management - AP1 release

Note

The intent of this experiment was to go through the steps leading to the release of an AP.

The removal of a PCICC as such is not supported, as is also the case for OSA-Express and FICON cards. For those cards, only card replacement is supported.

3.4 The 9672 channel

In the following sections we briefly describe the 9672 internal structure and the channel plugging rules.

3.4.1 The 9672 G6 internal structure

Figure 18 on page 43 shows the 9672 G6 system structure, with a logical representation of the data flow including the processing units (PUs), the level

2 cache (L2), the memory cards, and the memory bus adapters (MBAs) which connect to the channels through Self-Timed Interconnect (STI) cables.

All 9672 G6 models have two processor sets, with each set having seven PUs, two MBAs and an 8 MB L2 shared cache. Therefore, a complete system has 14 PUs, 4 MBAs and 16 MB L2 cache. Each PU has its own 256 KB cache level 1 (L1), designed as a store-through cache, meaning that the altered data must also be stored into the next upper-level cache.

IBM S/390 9672 G6 Servers - Processor Design

9672 G6 System Structure

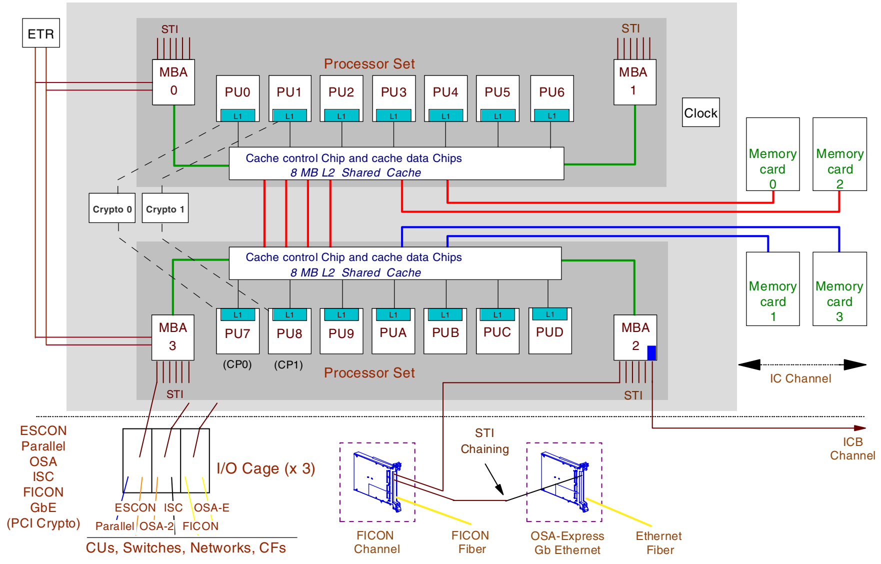


Figure 18. 9672 G6 internal system structure

A PU can be assigned as a central processor (CP), a system assist processor (SAP), or an Internal Coupling Facility (ICF). If not assigned, it becomes a spare PU. A spare PU can be used for CP sparing, SAP sparing, or ICF sparing.

There are 24 STI buses that are used for the connections to I/O domains, or direct connect chaining to FICON, OSA-Express or PCICC channels, or direct connect without chaining for ICBs. Each STI has a bidirectional bandwidth of 333 MB/sec.

An STI is an interconnection path to the Memory Bus Adapter (MBA) and can be used to connect:

- ESCON channels, parallel channels, or OSA-2 cards (via a FIBB card and a channel adapter (CHA) card)
- FICON channels
- OSA-Express channels

- PCICCs
- ISCs (coupling links) via an Intersystem Channel Adapter (ISC-M) card and a FIBB card
- Integrated Cluster Buses (ICBs) channels

Up to four FICON, OSA-Express or PCICC channels (which are high bandwidth channels) can be chained in the same STI; this is called *four-deep chaining*.

All 9672 G6 models have internal dual Cryptographic Coprocessors (CCFs) with dual paths to each processor set on a twin-tailed configuration. This allows continuity of cryptographic operations should the attached CP in control fail by sparing this CP at the next power-on reset.

Note: Only one of the attached CPs is in control of the CCF at a given time. The system structure shown in Figure 18 on page 43 is similar for the 9672 G5, with the exception that the 9672 G5 only has twelve PUs and a smaller cache size.

3.4.2 The 9672 channel plugging rules

The 9672 internal connections between FICON channels, OSA-Express or PCICC, and the CPC cage are via direct connect chaining STI connections. The following rules apply to making these connections:

- A direct connect chaining STI can support up to four FICON or OSA-Express or PCICC channels, or any mix of these channels (up to a total of four), in an STI chain.
- Each STI chain requires one STI connector at the CPC cage.
- Each direct connect STI chain is assigned four channel numbers (CHPIDs), one for each channel that can be potentially installed in the STI chain
- The FICON, OSA-Express or PCICC channels are installed across an assigned pair of STIs:
  - FICON, OSA-Express or PCICC channels 1, 3, and 5 are installed on the first STI of the pair.
  - FICON, OSA-Express or PCICC channels 2, 4, and 6 are installed on the second STI of the pair.
  - Later two more FICON, OSA-Express or PCICC channels can be installed, where the seventh channel is installed on the first STI and the eighth channel is installed on the second STI of the pair.

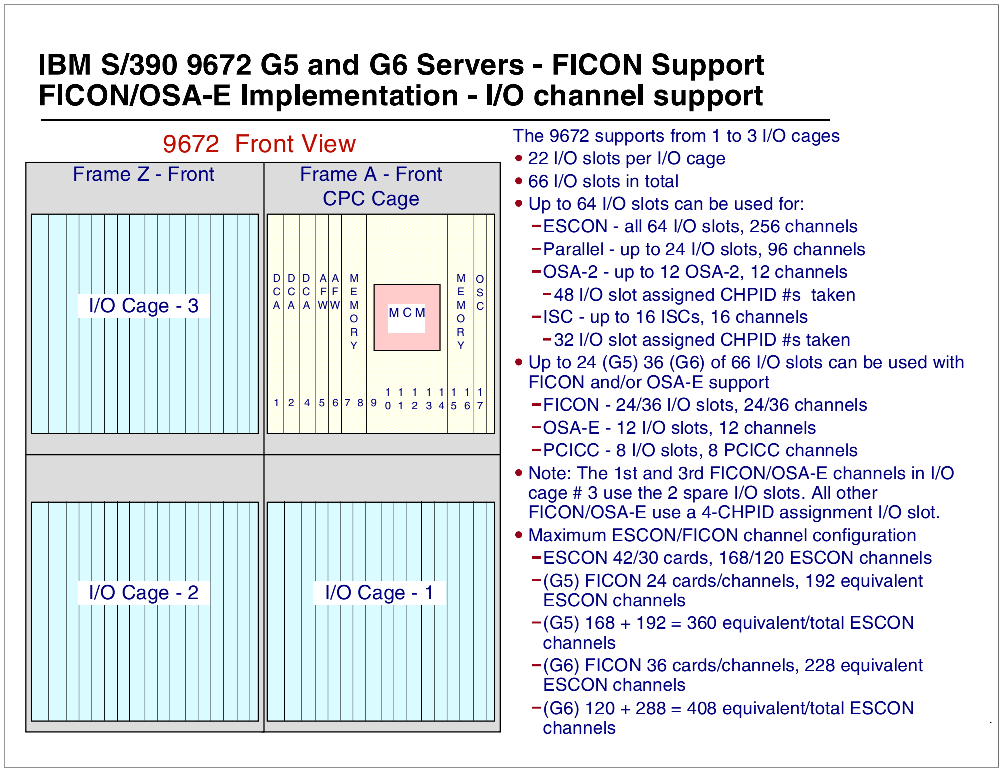
- In all cases, the last channel installed on the first STI is “chained” to the last channel installed on the second STI of the pair. This cross-chaining between STI is for recovery or repair purposes. For example, if the first FICON channel fails, then the second STI of the pair automatically takes over control of the FICON, OSA-Express and PCICC channels 2, 4, 6, 8, 7, 5, and 3.

The 9672 internal connection paths to ESCON channels are via “I/O domain”, with STI connections to the I/O cages on the basis of the I/O domain structure. Note the following points:

- There can be from one to three I/O cages in the total system configuration, each with three I/O domains.
- Each I/O domain requires one STI connection.
- Each I/O domain STI supports 16, 24, or 32 I/O domain channels.

3.4.3 I/O cage and channel number topology

Figure 19 on page 46 is a graphic representation of the I/O cage layout, with a summary of the cage configuration characteristics.



IBM S/390 9672 G5 and G6 Servers - FICON Support
FICON/OSA-E Implementation - I/O channel support

The 9672 supports from 1 to 3 I/O cages

- 22 I/O slots per I/O cage
- 66 I/O slots in total
- Up to 64 I/O slots can be used for:
  - ESCON - all 64 I/O slots, 256 channels
  - Parallel - up to 24 I/O slots, 96 channels
  - OSA-2 - up to 12 OSA-2, 12 channels
    - 48 I/O slot assigned CHPID #s taken
  - ISC - up to 16 ISCs, 16 channels
    - 32 I/O slot assigned CHPID #s taken
- Up to 24 (G5) 36 (G6) of 66 I/O slots can be used with FICON and/or OSA-E support
  - FICON - 24/36 I/O slots, 24/36 channels
  - OSA-E - 12 I/O slots, 12 channels
  - PCICC - 8 I/O slots, 8 PCICC channels
- Note: The 1st and 3rd FICON/OSA-E channels in I/O cage # 3 use the 2 spare I/O slots. All other FICON/OSA-E use a 4-CHPID assignment I/O slot.
- Maximum ESCON/FICON channel configuration
  - ESCON 42/30 cards, 168/120 ESCON channels
  - (G5) FICON 24 cards/channels, 192 equivalent ESCON channels
  - (G5) 168 + 192 = 360 equivalent/total ESCON channels
  - (G6) FICON 36 cards/channels, 228 equivalent ESCON channels
  - (G6) 120 + 288 = 408 equivalent/total ESCON channels

Figure 19. 9672 G5 and G6 channel capacity support

The IBM 9672 G5 and G6 support from 1 to 3 I/O cages having the following configurations:

- There are 22 I/O slots per I/O cage. When used by an I/O domain channel, each I/O slot is assigned four CHPID numbers.
- In total, there are 66 I/O slots.
- Up to 64 of the I/O slots can be used as follows:
  - ESCON: up to 64 channel cards (this provides for 256 ESCON channels in total).
  - Parallel: up to 24 channel cards (this provides for 96 parallel channels in total).
  - OSA-2: up to 12 OSA-2 channel cards. This provides for 12 OSA-2 CHPIDs, that is there is only one CHPID number per I/O cage slot in this case.

  - ISC: up to 32 ISCs channel adapter cards in total. Each ISC adapter card receives one or two ISC channels; that is, there are one or two CHPID numbers per slot in this case.

- On 9672 G5, up to 24 of 66 I/O slots can be used to plug FICON, OSA-Express or PCICC cards.
  - FICON: up to 24 channel cards (for a total of 24 CHPIDs, each of them consuming an I/O slot).
  - OSA-Express: up to 12 channel cards (for a total of 12 CHPIDs, each of them consuming one I/O slot).
  - PCICC: up to 8 channel cards (for a total of 8 CHPIDs, each of them consuming one I/O slot).
- On 9672 G6, up to 36 of 66 I/O slots can be used to plug FICON, OSA-Express or PCICC cards.
  - FICON: up to 36 channel cards (for a total of 36 CHPIDs, each of them consuming one I/O slot).
  - OSA-Express: up to 12 channel cards (for a total of 12 CHPIDs, each of them consuming one I/O slot).
  - PCICC: up to 8 channel cards (for a total of 8 CHPIDs, each of them consuming one I/O slot).

Note: The first and third FICON, OSA-Express or PCICC channels in I/O cage # 3 use the two spare I/O slots (I/O slot number 31 and 32). All other FICON, OSA-Express and PCICC channels use a 4-CHPID number assigned I/O slot.

The 24 STI connections in the 9672 G5 and G6 processors are assigned as follows:

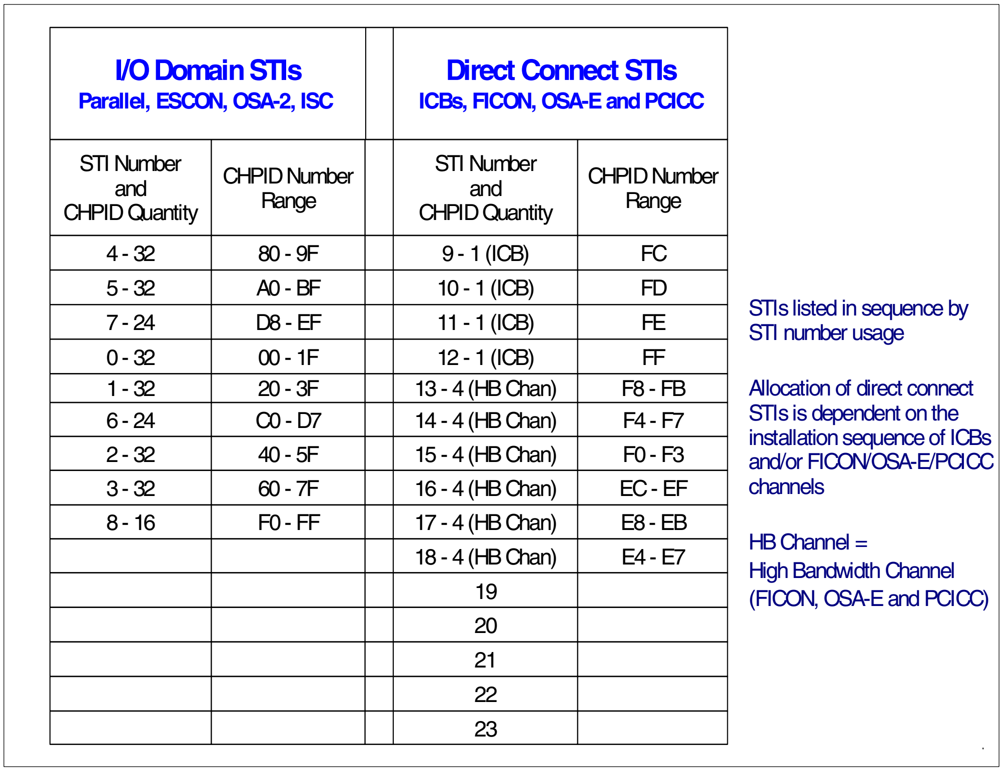
  - STI numbers 0 to 8 are usually assigned to I/O domains. STIs 9 to 23 are available as “direct connect” STIs for FICON, OSA-Express and PCICC channels, which means that the cards will be “chained” over the STI connection.

  - STIs 9 to 23 can also be used as direct connect STIs for the connection of ICB channels; however, in the case of ICBs, there is no STI chaining capability.

Figure 20 on page 48 summarizes the relationships between STI cables and CHPID numbers.

- It shows STIs 0 to 8 assigned to I/O domains, as well as the CHPID numbers that would be assigned to each of these STIs.

- STIs 9 to 12 (in this example) have been assigned to ICB channel, and each of these STIs is assigned one CHPID number.
- STIs 13 to 18 (in this example) have been assigned to high bandwidth (HB) channels (FICON, OSA-Express or PCICC channels), and each of these STIs is assigned four CHPID numbers, as shown.



I/O Domain STIs Parallel, ESCON, OSA-2, ISC		Direct Connect STIs ICBs, FICON, OSA-E and PCICC	
STI Number and CHPID Quantity	CHPID Number Range	STI Number and CHPID Quantity	CHPID Number Range
4 - 32	80 - 9F	9 - 1 (ICB)	FC
5 - 32	A0 - BF	10 - 1 (ICB)	FD
7 - 24	D8 - EF	11 - 1 (ICB)	FE
0 - 32	00 - 1F	12 - 1 (ICB)	FF
1 - 32	20 - 3F	13 - 4 (HB Chan)	F8 - FB
6 - 24	C0 - D7	14 - 4 (HB Chan)	F4 - F7
2 - 32	40 - 5F	15 - 4 (HB Chan)	F0 - F3
3 - 32	60 - 7F	16 - 4 (HB Chan)	EC - EF
8 - 16	F0 - FF	17 - 4 (HB Chan)	E8 - EB
		18 - 4 (HB Chan)	E4 - E7
		19	
		20	
		21	
		22	
		23	

STIs listed in sequence by STI number usage

Allocation of direct connect STIs is dependent on the installation sequence of ICBs and/or FICON/OSA-E/PCICC channels

HB Channel =
High Bandwidth Channel
(FICON, OSA-E and PCICC)

Figure 20. 9672 I/O Domains and STI assignment

The CHPID number assignment is as follows:

- I/O domain channel CHPID numbers (Parallel, ESCON, OSA-2 and ISC) are assigned in groups of 16, 24, and 32 per STI.
- ICB channel CHPID numbers are assigned in two groups of 4 for the first 8 ICBs, and then 1 for each additional ICB. This applies to all 9672 G5 and G6 models with the exception of the 9672 G5 RA6 to RD6 models; for these models, the ICB channel CHPID numbers are assigned one at a time.

- FICON, OSA-Express and PCICC channel CHPID numbers are assigned in groups of 4, and they are used one at a time when one of these channel types are installed.
- IC Channel CHPID numbers are assigned by the customer.

The FICON, OSA-Express and PCICC CHPID numbers are assigned from the highest group of 4 CHPID numbers not already assigned or reserved by any other direct connect STI (direct connect STIs are used by FICON, OSA-Express, PCICC and ICB).

3.5 Planning list items

In the following sections we describe microcode level requirements and capacity planning and installation considerations.

3.5.1 System microcode

The minimum LIC requirement for PCICC support on the G5 and G6 9672 Enterprise server is Driver 26, that is:

- CPC System Code EC F99939A (Common Group B/M for SE Code)
- CPC level: EC F99918 + MCLs
- PCI Crypto level: EC F99905 + MCLs. The base PCI crypto level is 1.18.
- HMC System Code EC F99938 (Common Group B/M for HMC)
- HMC level: EC F99933 + MCLs

3.5.2 Capacity planning considerations

As of the time of writing, there is no capacity planning data available.

3.5.3 Installation of the ordered PCICCs

Note the following installation considerations.

3.5.3.1 On new build machines

- All PCI crypto cards (FC 0860 PCICC) are shipped in thermal containers to avoid the risk of thermal tamper detection during shipment.
- The PCICC cards are removed from the machine after testing at the system manufacturing plant, and the Customer Engineer has to replug the PCICC cards and the STI cables at the customer's site according to the instructions given in theinstallation manual.
- The FCV crypto enablement diskette is also imported during the installation, once per system only, even if more than one feature code 0860 is installed.
- If the TKE has been ordered with feature code 0869 or 0866, the 4758 adapter is removed from the workstation at the plant of manufacture and shipped in a thermal container. The Customer Engineer has to replug the 4758 crypto adapter at the customer's site.

3.5.3.2 MES upgrade

Installation of the PCICC cards can be done concurrent with system operations if *all* of the following conditions are met:

- At a minimum, LIC Driver 26 is already installed, with the concurrent installation MCL activated.
- At least one CCF is enabled and in operation, with an enablement feature matching the PCICC-intended cryptographic configuration.
- The machine configuration does not require that an ISC adapter be moved.
- Because MES Installation Instructions are always generated for a specific machine serial number, it is very important that the last Vital Product Data (VPD) transmitted to IBM for this machine be accurate.

3.5.3.3 Miscellaneous recommendations

- If you have to move channel cards, refer to the redbook *Fiber Channel (FICON) Implementation Planning*, SG24-5445, for card sequencing or movement and cabling requirements.

- Make sure that any unique customer requirements have been conveyed through the ordering process and taken into consideration prior to starting installation.
- If you move PCICC cards, those cards will be zeroized. Refer to 2.1.3.3, “Zeroizing” on page 17.
- The PCICC CHPID is not defined in the IOCDS, but a CHPID definition conflict may occur if a CHPID is already defined in the IOCDS with the same number as the PCICC. This will prevent I/O dynamic reconfiguration, and if a system power-on reset is performed, neither the defined CHPID nor the PCICC will come online and a POR error message will be received.
- In addition to FCV load at POR, FCV can also be loaded during a reset to the PCICC (CHPID reset), provided that the FCV already resides in HSA. That is the case for a hotplugged PCICC card which gets its FCV loaded when the CHPID is being configured on at the Support Element.

Changing the FCV value

The only way to change the FCV data is to import the new FCV into the Support Element and run a system Power-on reset. *The PCICC is not zeroized when it loads a new FCV*.

3.6 Software requirements

In the following sections we give an overview of the software requirements for the support of the PCICC.

3.6.1 OS/390 V2R9

OS/390 2.9 is the minimum OS/390 level needed to support the PCICC. OS/390 2.9 includes ICSF 2.3 as an exclusive feature: that is, ICSF 2.3 cannot be ordered separately and cannot be installed on prior OS/390 releases.

3.6.1.1 TCP/IP enablement in OS/390

If using the TKE workstation, there are two implications:

1. Only TKE V3.0 supports the PCICC.
2. TKE V3.0 supports only TCP/IP as the communication network with the TKE OS/390 host.

3.6.1.2 Migrating from prior OS/390 levels

- When migrating from ICSF 2.2 (which is the level of ICSF delivered with OS/390 releases 6, 7 and 8), the PKDS has to be installed (if not already done), as ICSF 2.3 will not initialize if there is no PKDS defined in the Options Data Set.
  - In order to provide maximum flexibility in the dynamic selection of the crypto coprocessor by ICSF, we strongly recommend that the value for the Signature Master Key and the Key Management Master Key in the CCF (s) be the same.
- The following considerations pertain to applications:
  - Existing X'02' RSA internal key tokens must be re-imported to be usable on PCICC, where they become X’06’ internal key tokens usable both on CCF and PCICC. Both tokens are in the modulus-exponent format.
  - You should consider converting from the modulus-exponent tokens to the Chinese Remainder Theorem (CRT) format X’08’ internal tokens for better performance. ICSF routes all services using the CRT format tokens to the PCICC only.

3.6.2 CKDS and PKDS sharing considerations

Note the following considerations:

- The OS/390 2.9 ICSF CKDS may be shared with pre-OS/390 2.9 systems. There have been no new key types added since OS/390 2.6 (that is, since ICSF 2.2).
- However, sharing the OS/390 2.9 PKDS with pre-2.9 systems requires a toleration PTF which has the following functions:
  - It does not allow use of any token > 1024 bytes.
  - It does not allow updates to PKDS records of retained keys.
  - It converts the new 2.9 X'06' token to the existing X'02' token to use on CCF. Be aware that this token may still not be usable on CCF if the PKA Signature Master Key (SMK) does not have the same value as the PKA Key Management Master Key (KMMK).

The *ICSF System Programmer’s Guide*, SC23-3974, provides the APAR numbers to be installed on the sharing systems.

3.7 PR/SM setup

This item is discussed in detail in 4.3, “LPAR setup” on page 61. Note, however, that the PCICC candidate list in the partition image profile cannot be updated dynamically.

3.8 Migrating from TKE V2.x to TKE V3.0

There are no migration tools provided for migrating to TKE V3.0. You must consider the impact on the following and perform the appropriate actions.

3.8.1 Host definitions

The V2 host definitions are for VTAM APPC-connected hosts. You must redefine these hosts for the TKE V3.0 support of TCP/IP only.

3.8.2 CCF crypto modules, domains, and authority definitions

The TKE V2.x TKECM dataset is not compatible with the TKE V3.0 data set. You must redefine the CCF crypto modules, domains, and authority in the new TKECM data set. If you plan to use the same dataset name for V3.0 as you used for V2.0, *you must delete or rename the existing data set*.

3.8.3 Authority signature keys on IBM Personal Security Card (PSC)

Authority signature keys on PSC cannot be used on the TKE V3.0. The following alternatives are suggested:

1. While still working with the TKE 2.x workstation: change the signature requirements so that signature keys stored in PSCs are not needed any more. From the Crypto Module window, update the appropriate commands with the new signature requirements. Remove any authority whose signature key was stored on PSCs.

   Note: Be careful however not to create security exposures by removing these signature requirements.

2. As an alternative, still on the TKE 2.x workstation, you can generate and load new signature keys to the host as follows:

   - From the Authority Administration window, generate a new signature key and save it to a binary file. Read the public modulus. Send the updated authority definition the host, copy the binary file to a diskette, and restore the diskette files to the new TKE workstation.

3.8.4 Authority signature key in the TKE workstation key storage

There is no direct migration for PKA tokens from the 4755 crypto adapter card to the 4758. You must perform the same operations as in 3.8.3, “Authority signature keys on IBM Personal Security Card (PSC)” on page 53.

3.8.5 IMP-PKA keys in the workstation key storage

You must generate and load new IMP-PKA tokens in the TKE V3.0 key storage.

3.8.6 Migration of master or operational key parts on PSC

Because TKE V3.0 does not support the 4754 SIU or the PSC, you need to migrate the PSC data blocks to files. You can accomplish this while still working with TKE V2 by using the TSS HIKM utility. The *TKE Workstation User’s Guide 2000*, GA22-7430, describes this operation in detail in the chapter “Migrating from TKE V2 to TKE V3”.

3.9 Site security policy

The site security policy must take into account the following:

- The impact of new concepts in the cryptographic services (such as “retained keys”), in terms of the availability of services.
- The new RACF profiles pertaining to the PCICC-specific panels and functions. Refer to 6.1, “RACF access control to ICSF services” on page 137 for details on the RACF profiles.
- The changes brought by the new TKE workstation, as follows:
    - The communication network is a TCP/IP network. A “listener” host transaction program runs in the host OS/390 and can be secured using new RACF profiles (see Appendix C, “TKE host TCP/IP server setup” on page 145, for further details).
    - Both the TKE cryptographic adapter and the PCICC management introduce the notion of roles and profiles. These notions are further explained in Chapter 5, “Customizing PCICC and CCF using a TKE V3.0” on page 89.

Chapter 4. Installation, configuration and startup of ICSF

In this chapter we describe the physical installation of the PCICC card and all the initialization and setup steps to be performed to enable the customer to use the newly installed PCICC card. We do not describe the TKE workstation setup, which is done in Chapter 5, "Customizing PCICC and CCF using a TKE V3.0" on page 89.

The first steps of the initialization are performed at the Support Element or Hardware Management Console (HMC). This includes the cryptographic coprocessor assignment and authorization setup in the logical partitions image profiles, which must be done before activating the partitions.

- ICSF is used to enter the Master Keys in the hardware and to initialize and manage the cryptographic keys data sets.
- The Cryptographic Coprocessor Facility (CCF) must be in operation before using the PCICC cards, and the CCF cryptographic configuration must match the PCICC FCV feature codes.

Warning 1

Several manuals that we used during the writing of this book refer to "operator command" to vary the PCICC online or offline. There is no such command for the OS/390 operator that would allow configuring a PCICC online or offline from the system console. Configuring a PCICC online or offline can only be accomplished at the system Support Element or HMC.

Warning 2

The term "online" when applied to the PCICC requires precision regarding the context in which it is used:

- If referring to the PCICC CHPID, the meaning is the same as for a CHPID being in an online or standby state. A device in the online state is accessible to the software running in the partition or in the system, whereas a device in the standby state is no longer accessible.
- If referring to the PCICC facility as seen by ICSF, "online" means that the device is accessible but needs to have its master keys properly set. A PCICC is fully operational when in the "active" state, as described in 4.4.7, "Management of the PCI Cryptographic Coprocessors", on page 85.

4.1 PCI Cryptographic Coprocessor Card plugging

We briefly stress the following points again:

- It is mandatory to follow the Installation Instructions provided with the MES, as part movements specific to the machine serial number are involved.
- The STI-attached PCICC cards are installed in channel card slots, so the corresponding CHPID number must be free, that is: not used in the IOCDS definition, otherwise a configuration conflict will occur.

- A PCICC card serial number is automatically associated to a free adjunct processor (AP) number, starting with number 0.
- Relocating a PCI card to another system: the Master KeyMaster Keys are zeroized when the card is replugged. The customer has to reinstall the Master Keys.
- A card can be moved inside the system without changing its AP number.
- There is no explicit declaration of the PCICC card to ICSF; OS/390 2.9 notifies ICSF of the physical presence of a PCICC card via an ENF signal.

4.2 PCICC enablement

The following sections describe how to enable the PCICC.

4.2.1 Function Control Vector (FCV) overview

- The Function Control Vector (FCV) enables the specific cryptographic functions with the authorized key lengths in the PCICC hardware.
- The FCV is shipped from manufacturing on a diskette, according to the requested feature code, when the first PCICC card is ordered or when the current cryptographic configuration needs to be changed.
- The PCICC FCV is specific to the system serial number and as such appears common to all PCI cards installed in the system.
- The installation of the FCV is a two-step process:
  1. The FCV files are imported from the diskette onto the Support Element hard disk. This has to be done only when installing the first PCICC in the system or when changing the current cryptographic configuration. It can be done concurrently with system operations.
  2. During the next system Power-on reset the FCV is first uploaded to the system HSA, then downloaded into each PCICC card. Or, if it is the first FCV imported to the system, it can be immediately loaded into HSA as an option in the Support Element panel.
- If the FCV already resides in the HSA, it can be loaded or reloaded into the card without a system Power On Reset. This is achieved by configuring the PCICC CHPID offline, then online at the Support Element (CHPID reset). To select a PCICC at the support element:
  - Right-click the CPC icon in the CPC Work Area. A drop-down menu appears with these options: CPs, CHPIDs and PCI Crypto.
  - Select **PCI Crypto**; this displays the PCICCs installed in the system.

  From this point on you can refer to the *Support Element Operations Guide*, GC38-0608, for a description of how to configure a CHPID on or off.

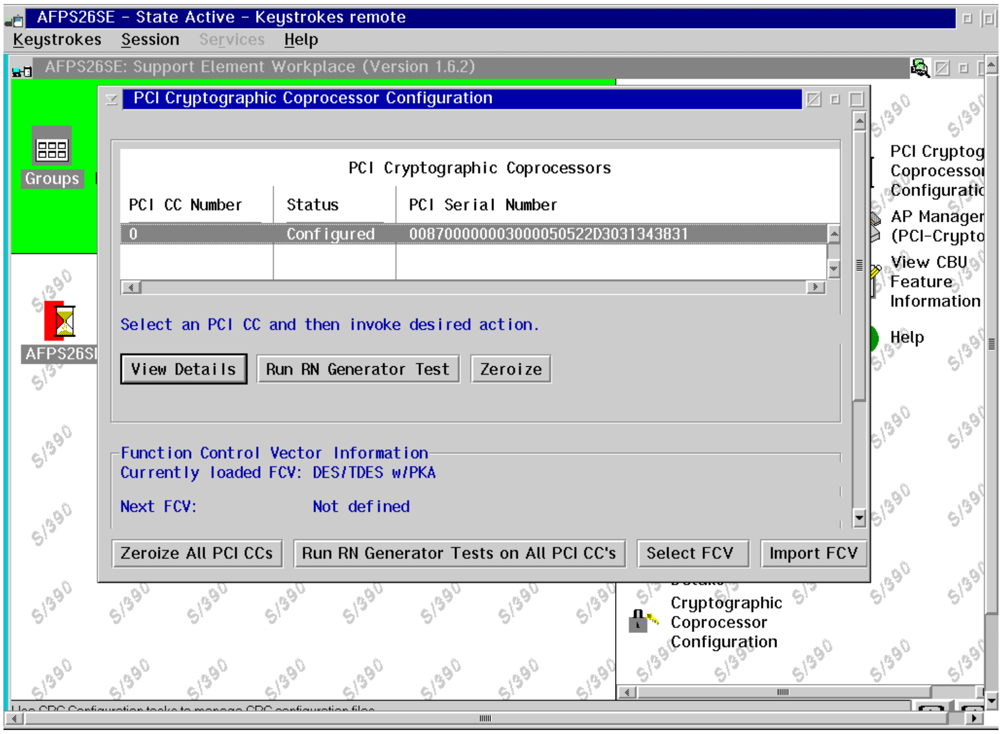
4.2.2 Import FCV

The Support Element must be logged on in SERVICE or SYSPROG, and the CPC logic must be powered on to get access to this panel.

- Select the CPC icon in the CPC Work Area.
- In the CPC configuration task list, select the **PCI Cryptographic Coprocess or Configuration** task.

The PCICC configuration main panel (see Figure 21), shows the following information:

- PCICC number, that is, the AP number
- PCICC status
- PCICC serial number



PCI Cryptographic Coprocessors

PCI CC Number	Status	PCI Serial Number
0	Configured	00870000000300005052 2D3031343831

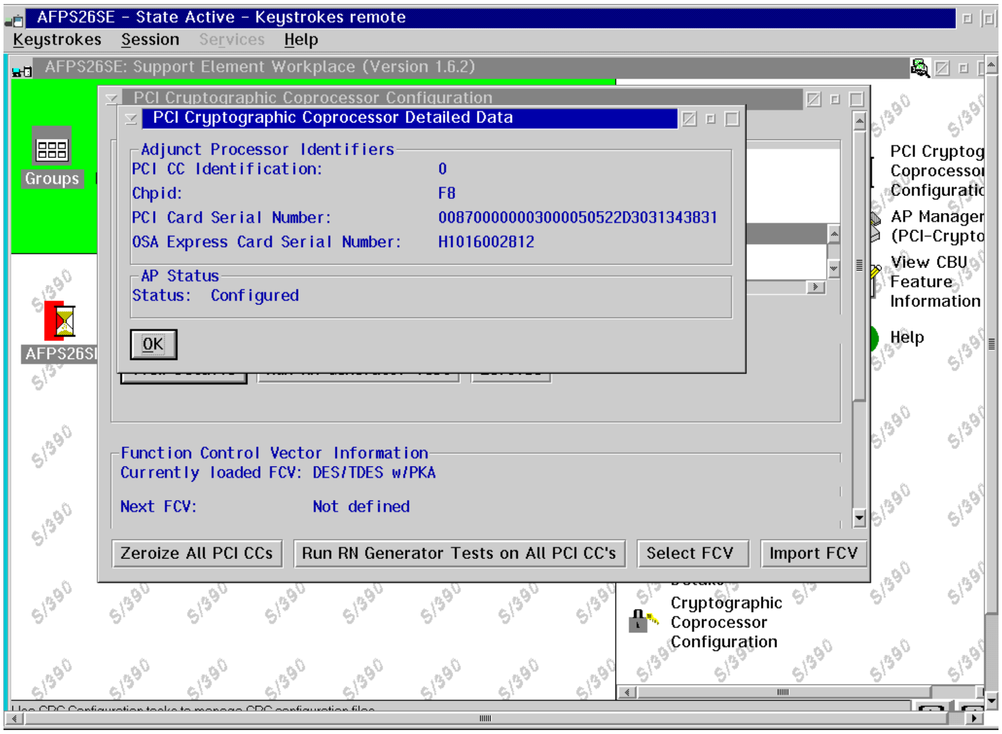
Select an PCI CC and then invoke desired action.

Function Control Vector Information
Currently loaded FCV: DES/TDES w/PKA

Next FCV: Not defined

Figure 21. PCICC configuration main panel view

Pressing **View details** yields the panel shown in Figure 22 on page 58.


AFPS26SE - State Active - Keystrokes remote
Keystrokes
Session
Services
Help
AFPS26SE: Support Element Workplace (Version 1.6.2)
Groups
AFPS26SE
PCI Cryptographic Coprocessor Configuration
PCI Cryptographic Coprocessor Detailed Data
OK
Zeroize All PCI CCs
Run RN Generator Tests on All PCI CC's
Select FCV
Import FCV
PCI Cryptographic Coprocessor Configuration
AP Manager (PCI-Crypto
View CBU Feature Information
Help
Cryptographic Coprocessor Configuration

Adjunct Processor Identifiers

```
PCI CC Identification:          0
Chpid:                          F8
PCI Card Serial Number:         0087000000030000505220303134383 1
OSA Express Card Serial Number: H1016002812
```

AP Status

```
Status:  Configured
```

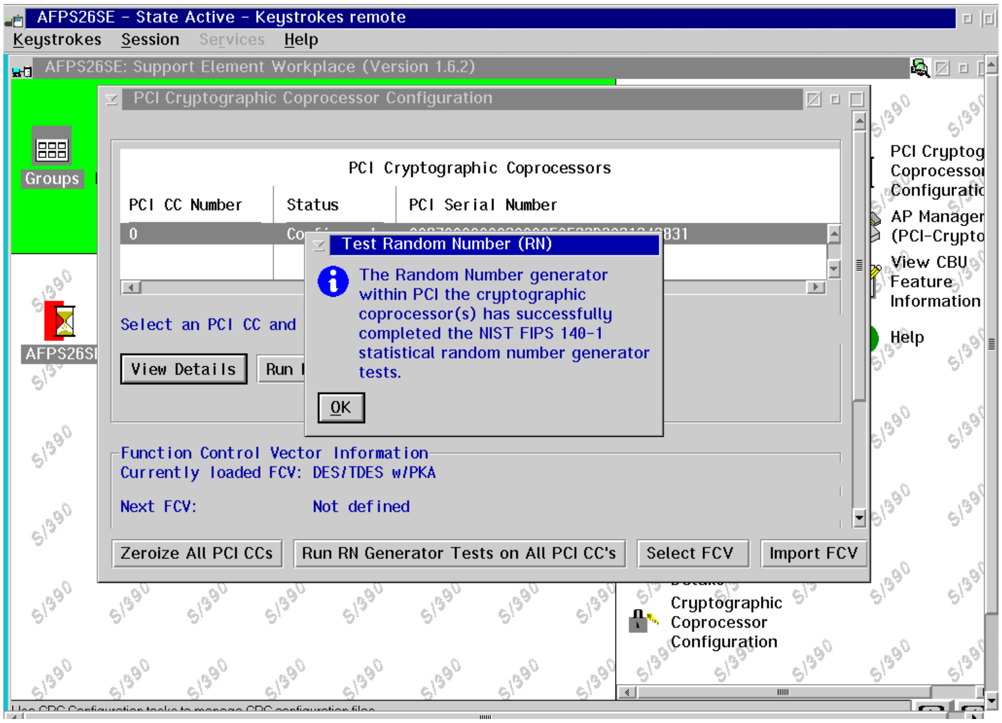
Function Control Vector Information

```
Currently loaded FCV: DES/TDES w/PKA

Next FCV:             Not defined
```

Figure 22. PCI Cryptographic Coprocessor detail view

This view shows information about the CHPID and the STI-attached Controller Card Serial Number, which can be used to identify the correct card in case the PCICC is later removed from the system.

In the PCICC configuration main panel you can, at any time (provided the CPC is powered on), press **Run RN Generator Test** to test only the selected PCICC, or **Run RN Generator Tests on All PCICC's,** which will run the same Random Number test on all PCICCs that are configured in the system. If the test works correctly, you will get the view shown in Figure 23 on page 59. (Note that this differs from the CCF, where it is required that ICSF started at least once before being able to run the pseudo random number generator test.)



AFPS26SE - State Active - Keystrokes remote

AFPS26SE: Support Element Workplace (Version 1.6.2)

PCI Cryptographic Coprocessor Configuration

PCI Cryptographic Coprocessors

PCI CC Number	Status	PCI Serial Number
0	Co	831

Select an PCI CC and

Function Control Vector Information
Currently loaded FCV: DES/TDES w/PKA

Next FCV: Not defined

Test Random Number (RN)

The Random Number generator within PCI the cryptographic coprocessor(s) has successfully completed the NIST FIPS 140-1 statistical random number generator tests.

Keystrokes
Session
Services
Help
Groups
AFPS26SI
View Details
Run I
OK
Zeroize All PCI CCs
Run RN Generator Tests on All PCI CC's
Select FCV
Import FCV
PCI Cryptog Coprocessor Configuratic
AP Manager (PCI-Crypto
View CBU Feature Information
Help
Cryptographic Coprocessor Configuration

Figure 23. The result from the Random Number Generator test

Pressing **Zeroize** on the PCICC configuration main panel (see Figure 21) will zeroize all the cryptographic keys and configuration data and reset the authorities and profiles in the selected card. The zeroize command can also be sent to all the installed PCICCs.

Zeroize All PCICCs

When this option is selected, it also erases the FCV loaded in HSA. The FCV must be imported again, or the next attempt to initialize a PCICC card will result in the card entering a check stop state.

When installing the first PCICC in the machine, or when changing the current FCV, the IMPORT FCV option is selected to copy the FCV files from the diskette to the Support Element hard disk.

Then, after selecting the line of the target PCICC, the option SELECT FCV will allow you to force the loading of the imported FCV into the PCICC hardware during the next initialization, that is, the next system Power On Reset when changing the FCV, or PCICC CHPID configure off, then on, when this is the first FCV imported into the system.

4.2.3 Hardware status of the PCICC

To see the hardware status of the PCICC you can double-click **PCI Cryptographic Coprocessor Configuration** on the CPC configuration task, when the CPC icon has been selected. Another possibility is to right-click the **CPC** icon in the CPC Work Area, which allows you to select **CPs**, or **CHPIDs,** or **PCI Crypto,** as shown in Figure 24 on page 60**.**

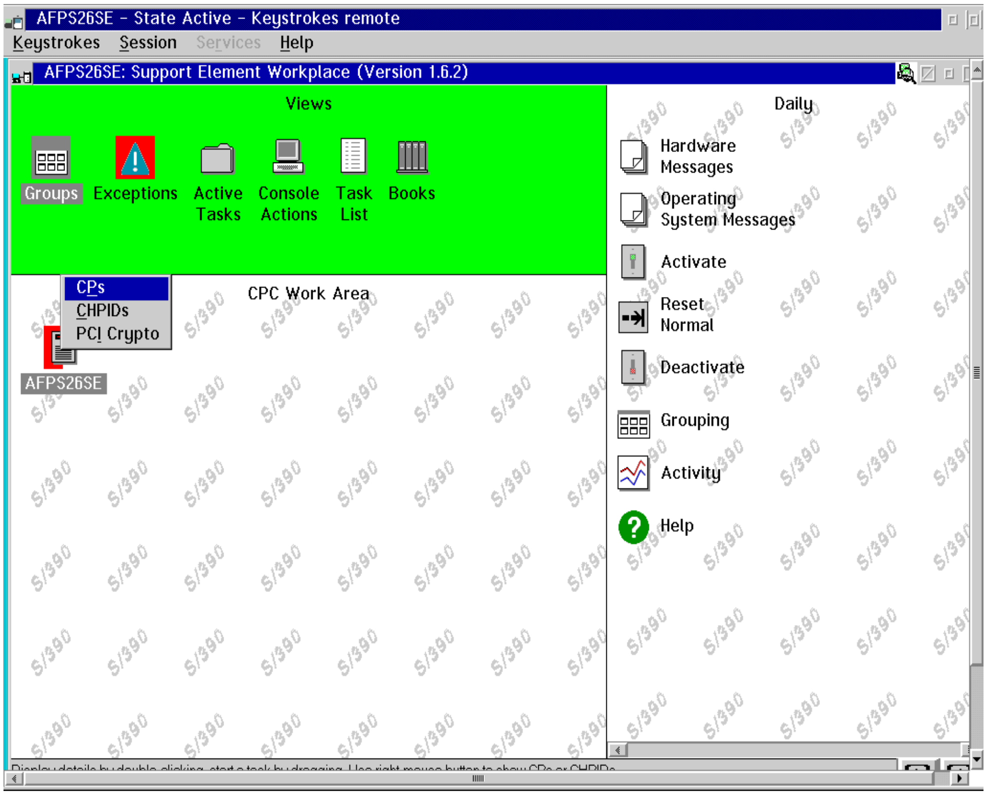


Figure 24. Right-clicked object on CPC Work Area view

When you select **PCI Crypto**, the panel shown in Figure 25 on page 61 displays all the PCICC cards that are installed, and their status.

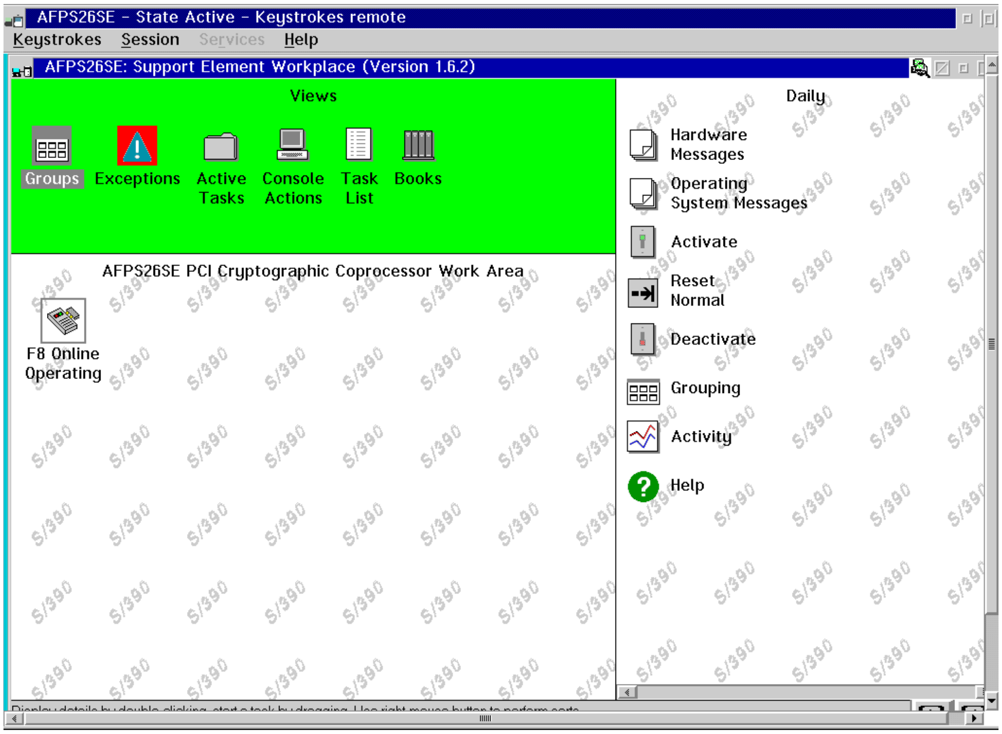


Figure 25. PCI Crypto selected from the CPC Work Area view

4.3 LPAR setup

This section highlights the specific system setups when using the cryptographic coprocessors in a PR/SM environment. Many of the involved tasks have already been described in *Exploiting S/390 Hardware Cryptography with Trusted Key Entry*, SG24-5455. This chapter concentrates on the changes that come with the PCICC.

The logical partition image profile is used by the system to set up the proper environment characteristics when activating the logical partition. The profile is made up of several pages and is kept recorded on the system Support Element hard disk. For further details on the contents of the image profile pages, refer to *PR/SM Planning Guide*, GA22-7236.

4.3.1 The image profile processor page

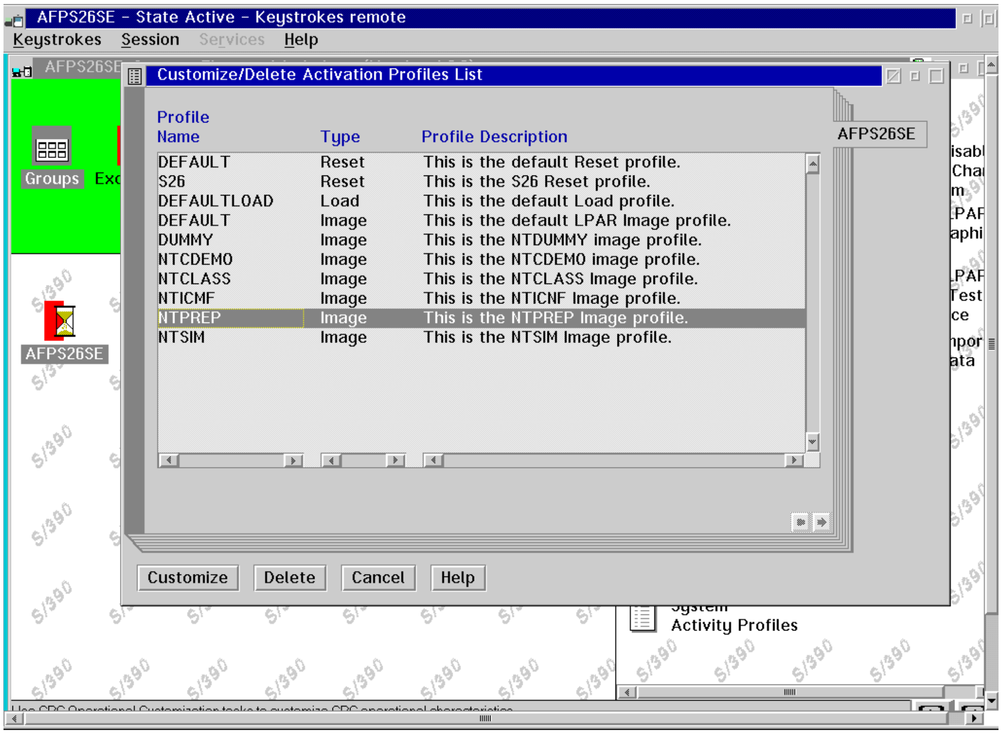
The processor page allows the selection of:

- The number of logical processors that will be made available to the logical partition
- Whether the partition will be dedicated or shared
- The number of logical crypto coprocessors that will be made available to the logical partition

When invoking the customizing of the image profile for the logical partition, perform the following steps to get access to the processor page:

1. Select the **CPC** icon in the CPC Work Area view.

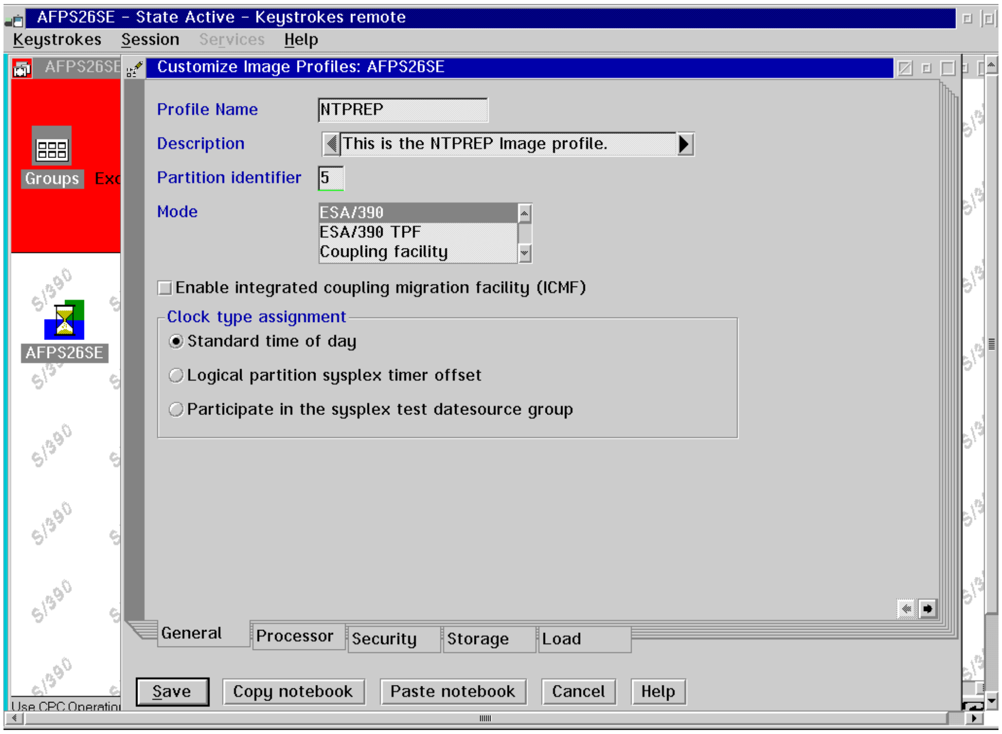
2. Double-click **Customize / Delete Activation Profile** in CPC Operational Customization. The panel shown in Figure 26 appears.



Profile Name	Type	Profile Description
DEFAULT	Reset	This is the default Reset profile.
S26	Reset	This is the S26 Reset profile.
DEFAULTLOAD	Load	This is the default Load profile.
DEFAULT	Image	This is the default LPAR Image profile.
DUMMY	Image	This is the NTDUMMY image profile.
NTCDEMO	Image	This is the NTCDEMO image profile.
NTCLASS	Image	This is the NTCLASS Image profile.
NTICMF	Image	This is the NTICNF Image profile.
NTPREP	Image	This is the NTPREP Image profile.
NTSIM	Image	This is the NTSIM Image profile.

Figure 26. The Activation Profiles List

3. Select the image profile you want to work with and click **Customize**. In our case, we are working with the NTPREP image profile. The first page of the image profile is displayed, as shown in Figure 27 on page 63.



Profile Name: NTPREP

Description: This is the NTPREP Image profile.

Partition identifier: 5

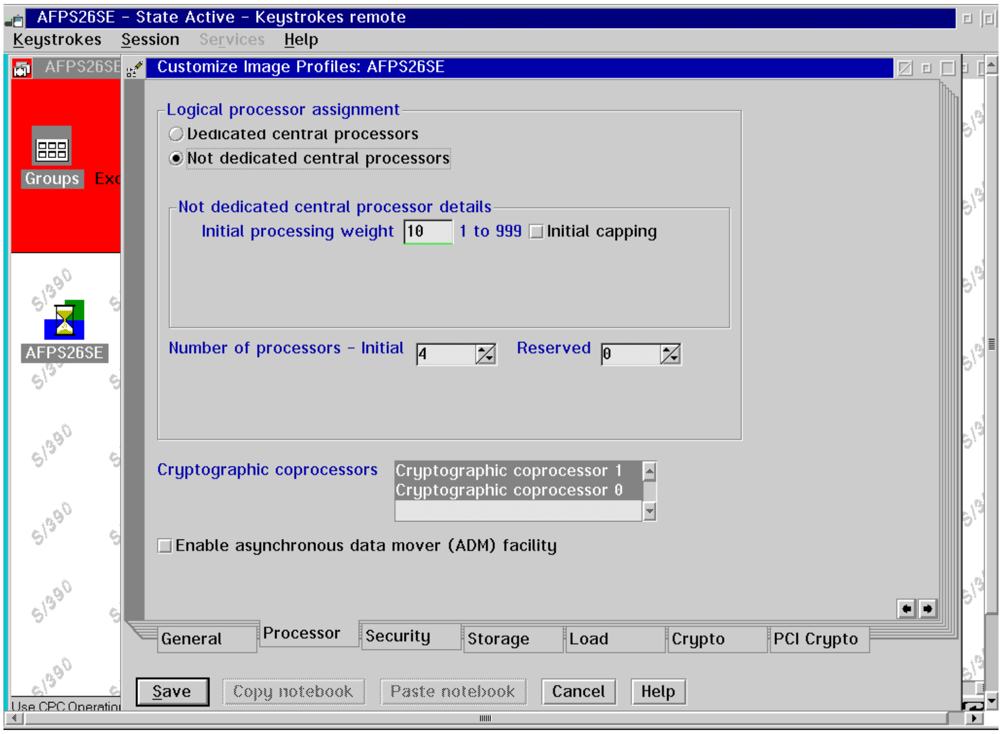
Mode:
ESA/390
ESA/390 TPF
Coupling facility

□ Enable integrated coupling migration facility (ICMF)

Clock type assignment
- ● Standard time of day
- ○ Logical partition sysplex timer offset
- ○ Participate in the sysplex test datesource group

Figure 27. Customize Image Profile page of a selected image

4. Select the **Processor** tab to see the processor page; see Figure 28.



Logical processor assignment
- ○ Dedicated central processors
- ● Not dedicated central processors

Not dedicated central processor details

Initial processing weight: 10 1 to 999 □ Initial capping

Number of processors - Initial: 4 Reserved: 0

Cryptographic coprocessors:
Cryptographic coprocessor 1
Cryptographic coprocessor 0

□ Enable asynchronous data mover (ADM) facility

Figure 28. Customizing Image Profile: the processor page

The Image Profile processor page in Figure 28 contains the *Cryptographic coprocessors* window, indicating how many CCFs are physically available in the system. Selecting one or two of these chips allocates one or two logical crypto coprocessors for the logical partition. These logical crypto coprocessors will actually be backed up by physical resources only when the logical partition is activated. Note that there are initially no *Crypto* and *PCI Crypto* tabs offered for selection at the bottom of the pages. As soon as a logical processor has been allocated to the partition, the *Crypto* and *PCI Crypto* tabs appear as shown in Figure 28.

4.3.2 Dedicated central processors

Electing to run a logical partition with dedicated central processors *and* cryptographic coprocessors has a very dramatic effect on the rest of the system when this logical partition is activated, because there is a physical affinity between the crypto chips and two physical processors in the system. The PR/SM microcode will allocate one or two of these physical processors, depending on the number of logical cryptographic coprocessors selected, to the dedicated logical partition, thus making these physical processors unavailable to other logical partitions. This can also result in not being able to activate the dedicated partition because of other shared partitions already sharing the physical crypto chips.

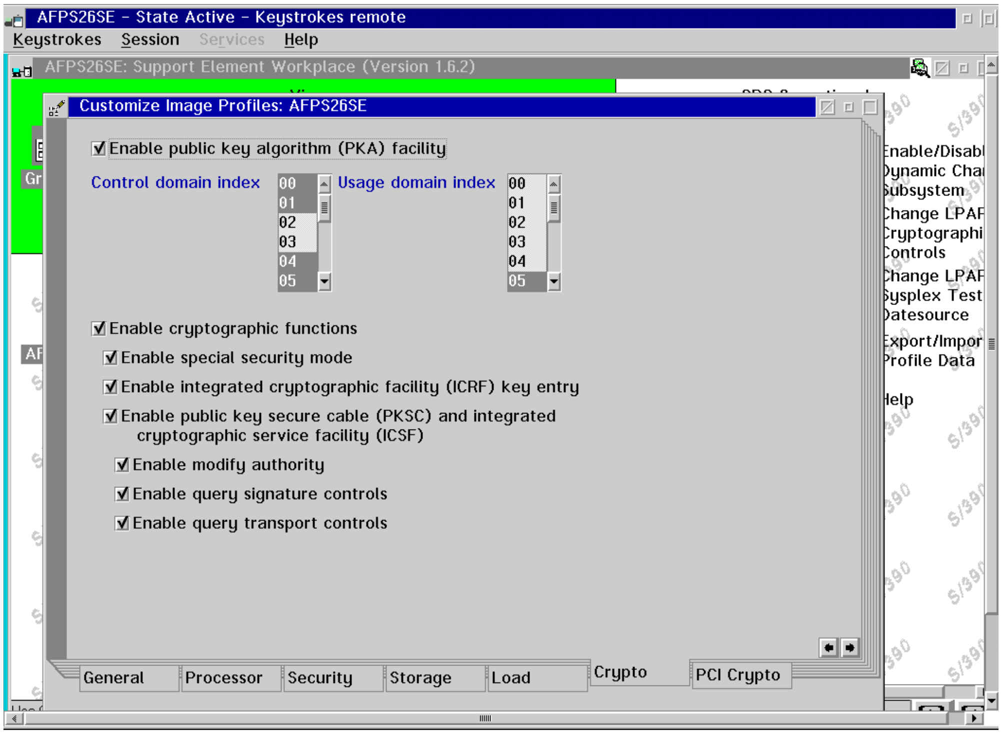
Important

The concept of coprocessor dedication does not apply to PCICC. A PCICC is by nature accessible from several partitions as directed by the online and candidate lists, regardless of the shared or dedicated status given to the CCF.

4.3.3 The Crypto page

The Crypto page allows the selection of parameters for the cryptographic setup of the logical partition. These setup parameters are taken into account at logical partition activation. Note that these selections, except for the contents of the control and usage domain lists, can be dynamically changed without needing to deactivate and then reactivate the logical partition, using the “Change LPAR Cryptographic Controls” in the CPC Operational Customization task list.

The selections shown in Figure 29 on page 65 were made on the Crypto page of the image profile of our NTPREP partition.



Customize Image Profiles: AFPS26SE

☑ Enable public key algorithm (PKA) facility

Control domain index: 00, 01, 02, 03, 04, 05

Usage domain index: 00, 01, 02, 03, 04, 05

☑ Enable cryptographic functions

☑ Enable special security mode

☑ Enable integrated cryptographic facility (ICRF) key entry

☑ Enable public key secure cable (PKSC) and integrated cryptographic service facility (ICSF)

☑ Enable modify authority

☑ Enable query signature controls

☑ Enable query transport controls

Figure 29. Crypto page of the image profile

- **Enable public key algorithm (PKA) facility** - The original intent of this selection was to select PKA-only functions, as opposed to the DES-based functions. Although this option seems to imply that you may also have the choice of not enabling your logical crypto coprocessors for PKA types of functions, this selection is *mandatory* in order to have ICSF start correctly.
- **Usage domain index** - This must point to the domain numbers allowed to this logical partition, which should also match the domain numbers entered in the Options data set when starting this partition's instance of ICSF.

  This is the domain number that you are giving to this partition. We recommend that you choose a number equal to the partition ID for a clear relationship between logical partition and domain.
- **Control domain index** - This pertains to the logical crypto coprocessors defined in other logical partitions that can be administered from this logical partition being set up as the TCP/IP (or APPC) host for the TKE.

  If you are setting up the host TCP/IP (or APPC) in this logical partition for communicating with the TKE, this is the partition that will be used as path to other domains' Master Keys. Indicate all the domains you want to access (including this partition's own domain) from this partition as control domains. In the example shown in Figure 29, you are able to access Master Keys for domains 0, 1, 4 and 5 from the TKE.

Current problem

As of a recently identified problem, domain 0 *must* always be specified in the TKE host Control Domains list when working with the TKE V3.0 and PCICC cards. Failure to do so results in the TKE not being able to open the Roles and Authorities pages for any domain.

This problem is expected to be resolved in the second half of year 2000.

- **Enable cryptographic functions** - This actually pertains to the DES-based *ICRF functions* as they were known in the ES/9000-9021, but also includes the DES Master Key management functions.

  It must be selected for normal operation of the logical cryptographic coprocessors.
- **Enable special security mode** - This is the mode of operation required for KGUP to permit generation or entry of clear keys, and to enable the secure key import or clear pin generate callable services. ICSF will work with the clear keys (as opposed to keys encrypted under a Master Key or a Transport Key) only if Special Security Mode (SSM) is selected on this page of the image profile and also specified as SSM YES in the Options data set. Only deselecting this option in the image profile is enough to prevent ICSF from accepting clear keys. Note that the status of the SSM can also be modified for the domain at the TKE. This is accomplished by the setting of the SSM bit in the ECM.

  The setting of this selection is actually a matter of security policies and procedures at the installation. Refer to these customer procedures to decide what to do.
- **Enable integrated cryptographic facility (ICRF) key entry** - This option must be selected to permit the loading of Master Keys in the usage domain from the TKE. No selection implies that the Master Keys can only be entered from the ICSF ISPF panels. Select whether you want to use the TKE to enter Master Keys into the usage domain of this partition.
- **Enable public key secure cable (PKSC) and integrated cryptographic service facility (ICSF)** - Do not be misled, there is no choice here: This *has* to be selected. Furthermore, it gives access to the last three options.
- **Enable modify authority** - There can be only one active logical partition at one time with this option selected. The definitions of authority and authority signatures will be transmitted into the physical cryptographic coprocessor from the TKE through this logical partition, if this is selected. Refer to the security policies and procedures for the installation before selecting.
- **Enable query signature controls** - This enables the TKE to get, through this logical partition, the status of the multi-signature command in progress; in other words, what are the multi-signature commands defined by the installation? What is the one in progress? Has the crypto coprocessor received all the necessary signatures? Refer to the security policies and procedures for the installation.
- **Enable query transport controls** - This allows the logical partition to participate in a key transfer operation with the TKE workstation. Refer to the security policies and procedures for the installation.

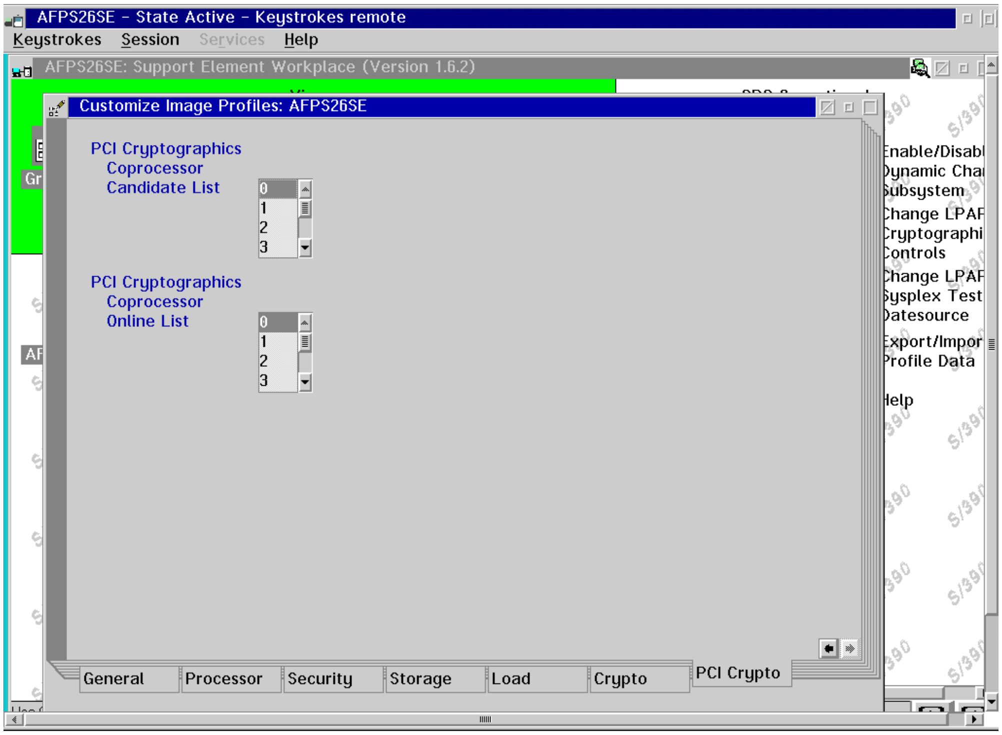
4.3.4 The PCI Crypto page

The PCI Crypto page (see Figure 30) allows for the selection of the AP numbers to be put in the online and candidate lists.

- **PCI Cryptographics Coprocessor Candidate List** - This pertains to the AP numbers that are accessible for this logical partition but require to be manually brought online to the partition.
- **PCI Cryptographics Coprocessor Online List** - This pertains to the APs that are automatically brought online during logical partition activation. If not all the selected APs are online, an activation error condition is reported. The APs selected in the Online List must also be part of the Candidate List.

> **Note**
>
> The PCI Cryptographics Coprocessor Online and Candidate List selection cannot be changed dynamically; that is, any change to these lists requires deactivating and then reactivating the logical partition to be taken into account. In other words, additions of a PCICC in the system must be planned ahead of LPAR activation to be truly concurrent.

After installing the first PCICC, we initially made the following selections on the PCI Crypto page of the image profile; see Figure 30.



PCI Cryptographics Coprocessor Candidate List: 0 (selected), 1, 2, 3

PCI Cryptographics Coprocessor Online List: 0 (selected), 1, 2, 3

Figure 30. PCI Crypto page of the image profile

In Figure 31 we added a new AP to the PCI Cryptographic Coprocessor Candidate List. This was in preparation for the concurrent installation of an additional PCICC, so that we could activate the logical partition now without needing to deactivate and then reactivate it again when the other PCICC is installed.

.

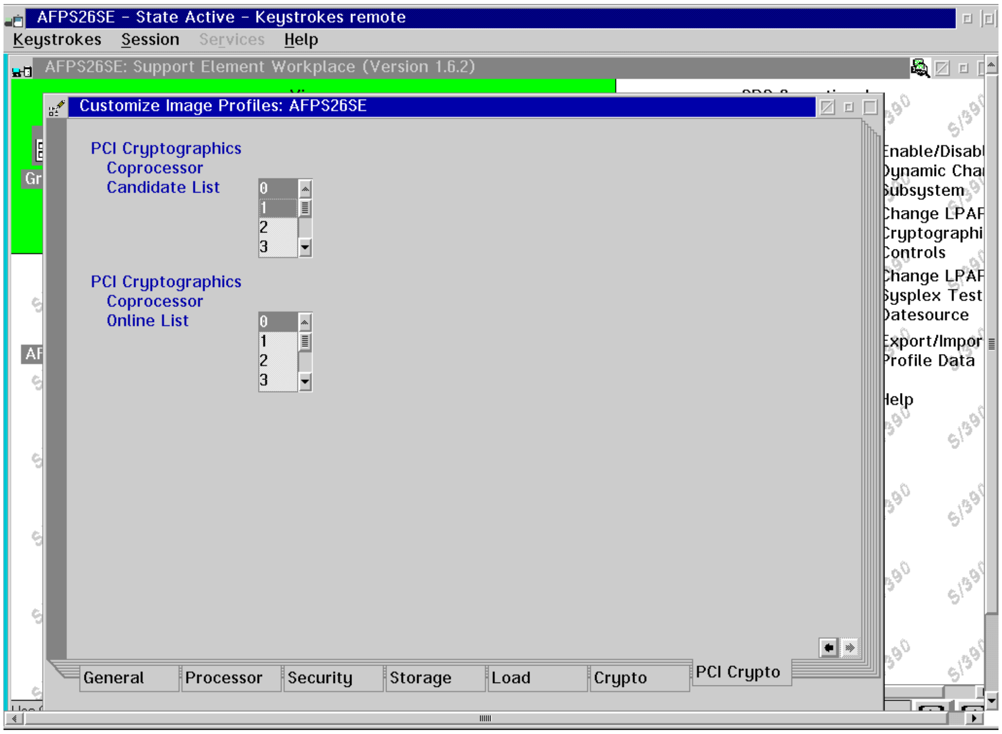

AFPS26SE - State Active - Keystrokes remote
Keystrokes Session Services Help
AFPS26SE: Support Element Workplace (Version 1.6.2)
Customize Image Profiles: AFPS26SE
PCI Cryptographics Coprocessor Candidate List
0
1
2
3
PCI Cryptographics Coprocessor Online List
0
1
2
3
General
Processor
Security
Storage
Load
Crypto
PCI Crypto
Enable/Disabl
Dynamic Char
Subsystem
Change LPAR
Cryptographi
Controls
Change LPAR
Sysplex Test
Datesource
Export/Impor
Profile Data
Help

Figure 31. A new PCICC added to Candidate List

4.3.5 PCICC and cryptographic domains

The AP identification number, from 0 to 7, is used when defining the PCICC on the PCI Crypto page. Every PCICC installed into the system is a separate Cryptographic processor that has its own Domains, from 0 to 15. It is not possible to assign PCICC Domain indices to a logical partition. The CCF domain indices in the Crypto page (control and usage domains) are propagated to the PCICC. ICSF accesses the CCF and PCICC Domain whose index value is given in the Options Data Set, provided that this domain index value is in the domain usage list for the partition.

4.4 Integrated Cryptographic Services Facility (ICSF) setup

The following sections describe how to perform ICSF setup, and discuss what is changed -- and unchanged -- from the previous release.

4.4.1 Changes from previous release

4.4.1.1 Mandatory PKDS

The PKDS must now, as of OS/390 2.9, be allocated and specified with the PKDSN parameter in the Options Data Set when you start ICSF. The PKDS is a VSAM key-sequenced data set with variable length records. Allocate the PKDS on a permanently resident volume.

4.4.1.2 Options Data Set

Starting with OS/390 2.9, support is provided for the use of system symbols in the installation Options Data Set. System symbols can be used as values for any of the parameters. They are specified in the IEASYMxx member of SYS1.PARMLIB; the IEASYM statement of the LOADxx member specifies the IEASYMxx members to be used for their resolution. We defined the symbol PARDOM in our IEASYMxx:

```
SYSDEF  SYMDEF(&PARDOM='5')
```

And we used the following symbol in our Options Data Set:

```
DOMAIN(&PARDOM.)
```

Note that viewing the system options via the ISPF panel shows the substitution for the symbolic values.

A new installation option is available that specifies the set of reason codes to be returned from callable services: ICSF or TSS reason codes. We set:

```
REASONCODES(ICSF)
```

Still the same

At OS/390 2.9, the following is still in effect:

- The CKDS content is loaded into an in-storage CKDS, which gives the capability to dynamically reencipher the CKDS. The PKDS content resides only in the PKDS data set and there is no dynamic reenciphering capability for the PKDS.
- It takes a manual procedure to synchronize or resynchronize the in-storage CKDSs in a parallel sysplex configuration.

4.4.1.3 ICSF ISPF panels

The panels and options referring to the PCICC will be visible only if at least one PCICC card has been detected in the system. Otherwise, these panels look very much the same as the panels in the previous ICSF release.

4.4.1.4 Initialize CKDS option

This option now combines, at ICSF 2.3, the following functions:

- Write of the header record
- Set of Master Keys
- Write system keys

In previous ICSF releases, the “Initialize an empty CKDS” option was only writing the header record.

4.4.2 TSO procedure

For convenience we set up a TSO procedure, CRYPTO, for the residents. We specified the ICSF libraries in the files allocations executed by CRYPTO:

- SCSFTLIB goes to ISPTLIB.
- SCSFCLI0 goes to SYSPROC.
- SCSFPNL0 goes to ISPPLIB.

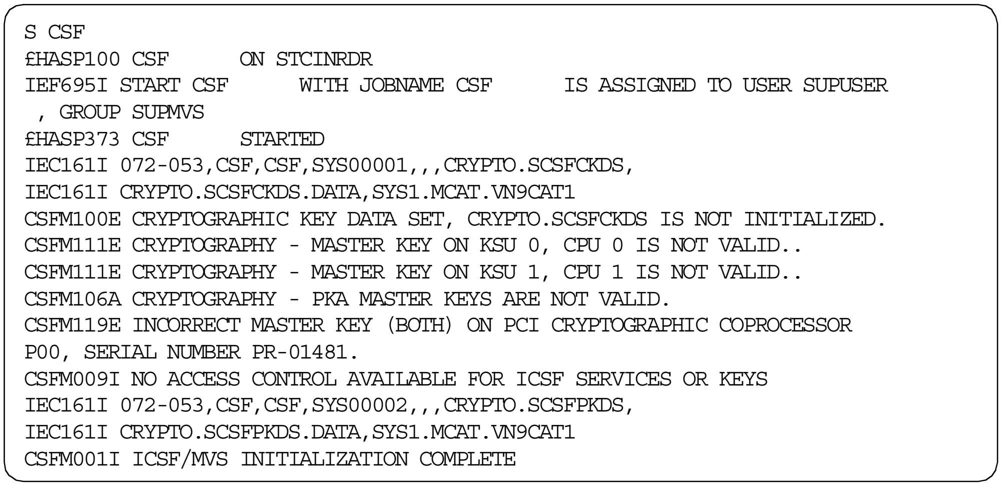
- SCSFSKL0 goes to ISPSLIB.
- SCSFMSG0 goes to ISPMLIB.
- SCSFMOD0 goes to ISPLLIB.

4.4.3 Started task and the first time start

To protect the ICSF started task user ID from being revoked through malicious or inadvertent incorrect password attempts, we recommend that you use a protected user ID, that is, one with the NOPASSWORD attribute. For more information, see *Security Server (RACF) Security Administrator's Guide,* SC28-1915, OS/390 2.8 or later.

Access to the ICSF administrative tasks or services can be restricted using RACF Facility class profiles. Refer to 6.1, "RACF access control to ICSF services", on page 137.

When you start ICSF for the first time, you will see the messages shown in Figure 32. You receive the message CSFM111E for each Cryptographic Coprocessor Feature you have online. If you are running with PCICCs, you receive the message CSFM119E for each PCICC that is online ("online" meaning here that the PCICC is accessible by ICSF but does not have the Master Keys set or does not have the correct Master Key values; refer to 4.4.7, "Management of the PCI Cryptographic Coprocessors", on page 85 for futher details).



```
S CSF
£HASP100 CSF      ON STCINRDR
IEF695I START CSF      WITH JOBNAME CSF      IS ASSIGNED TO USER SUPUSER
 , GROUP SUPMVS
£HASP373 CSF      STARTED
IEC161I 072-053,CSF,CSF,SYS00001,,,CRYPTO.SCSFCKDS,
IEC161I CRYPTO.SCSFCKDS.DATA,SYS1.MCAT.VN9CAT1
CSFM100E CRYPTOGRAPHIC KEY DATA SET, CRYPTO.SCSFCKDS IS NOT INITIALIZED.
CSFM111E CRYPTOGRAPHY - MASTER KEY ON KSU 0, CPU 0 IS NOT VALID..
CSFM111E CRYPTOGRAPHY - MASTER KEY ON KSU 1, CPU 1 IS NOT VALID..
CSFM106A CRYPTOGRAPHY - PKA MASTER KEYS ARE NOT VALID.
CSFM119E INCORRECT MASTER KEY (BOTH) ON PCI CRYPTOGRAPHIC COPROCESSOR
P00, SERIAL NUMBER PR-01481.
CSFM009I NO ACCESS CONTROL AVAILABLE FOR ICSF SERVICES OR KEYS
IEC161I 072-053,CSF,CSF,SYS00002,,,CRYPTO.SCSFPKDS,
IEC161I CRYPTO.SCSFPKDS.DATA,SYS1.MCAT.VN9CAT1
CSFM001I ICSF/MVS INITIALIZATION COMPLETE
```

Figure 32. The first-time ICSF startup messages

4.4.4 Master Keys

ICSF uses three Master Keys to protect the keys that are used with the S/390 CCF, and two Master Keys to protect the keys that are used with the PCICC. The Master Keys in the CCF are:

The DES Master Key

This key is a double-length (128-bit) key that is used to protect DES and CDMF keys by encrypting these keys with the triple DES algorithm.

The PKA Key Management Master Key

This key (KMMK) is a triple-length (192-bit) key. The KMMK protects PKA private keys that are used in both the digital signature services and in the CDMF and DES data key distribution functions.

The PKA Signature Master Key

This key (SMK) is a triple-length (192-bit) key. The SMK protects PKA private keys that are used only in digital signature services.

The Master Keys in the PCICC are:

Symmetric-keys Master Key

This key (SYM-MK) is a double-length (128-bit) key that is used to protect DES keys used on the PCI Cryptographic Coprocessor. The SYM-MK is actually a triple-length (192-bit) Master Key inside the PCICC that ICSF enforces to be equivalent to a double-length (128-bit) Master Key. This key must have the same value as the DES Master Key in the CCF.

Asymmetric-keys Master Key

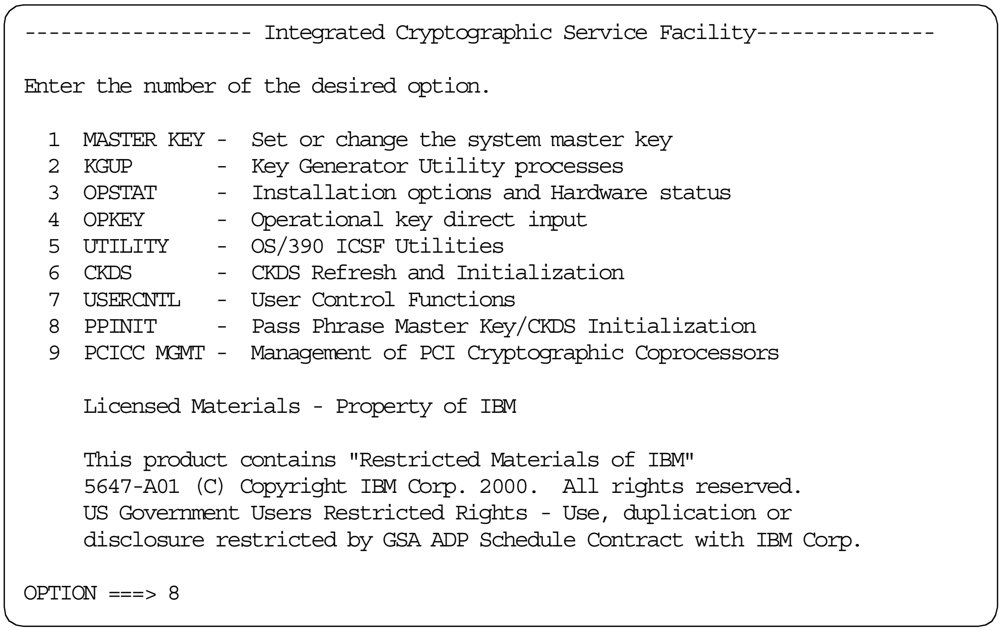
This key (ASYM-MK) is a triple-length (192-bit) key. The ASYM-MK protects PKA private keys that are used on the PCI Cryptographic Coprocessor. This key must have the same value as the SMK in the CCF.

4.4.5 Initial Master Key entry with the pass phrase initialization utility

The pass phrase initialization utility can be used to initialize the CKDS and the coprocessor. You can also use this utility to install both the SYM-MK and the ASYM-MK on all PCI Cryptographic Coprocessors on S/390 G5 Enterprise Servers, or later.

To use this utility, the special secure mode must be enabled, and all the Master Key registers in the targeted coprocessors must be empty. Also, the designated CKDS must not be already initialized, that is, it is just an empty VSAM data set. Therefore, you cannot use this utility to change the Master Keys.

When you access the ICSF panels, the primary menu panel appears, as shown in Figure 33 on page 72.

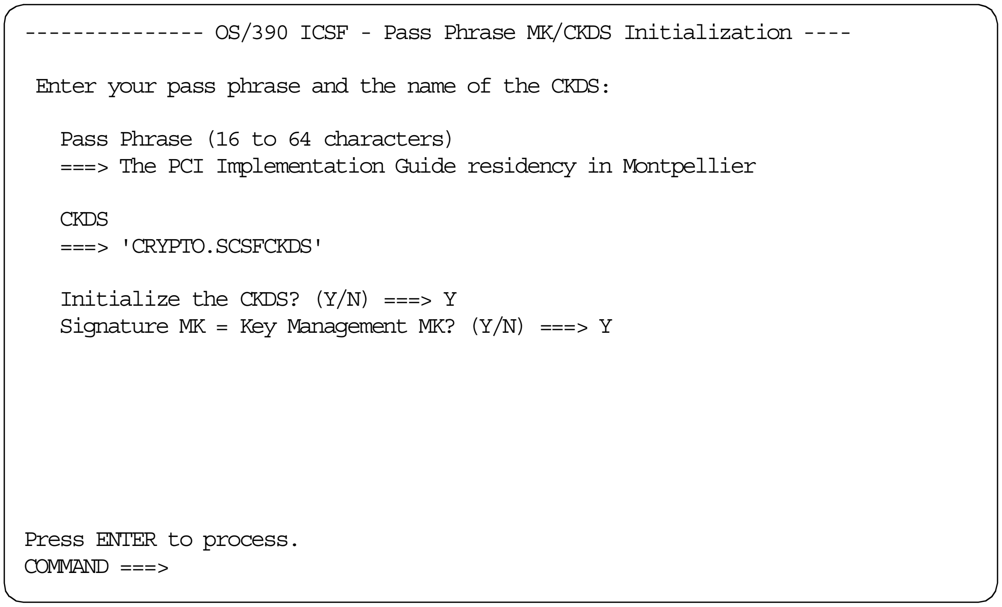


```
------------------ Integrated Cryptographic Service Facility---------------

Enter the number of the desired option.

  1  MASTER KEY -  Set or change the system master key
  2  KGUP       -  Key Generator Utility processes
  3  OPSTAT     -  Installation options and Hardware status
  4  OPKEY      -  Operational key direct input
  5  UTILITY    -  OS/390 ICSF Utilities
  6  CKDS       -  CKDS Refresh and Initialization
  7  USERCNTL   -  User Control Functions
  8  PPINIT     -  Pass Phrase Master Key/CKDS Initialization
  9  PCICC MGMT -  Management of PCI Cryptographic Coprocessors

     Licensed Materials - Property of IBM

     This product contains "Restricted Materials of IBM"
     5647-A01 (C) Copyright IBM Corp. 2000.  All rights reserved.
     US Government Users Restricted Rights - Use, duplication or
     disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

OPTION ===> 8
```

Figure 33. Selecting Pass Phrase Option on the ICSF primary menu panel

Select option 8, **PPINIT**, and press Enter to begin the pass phrase initialization utility. Then type the pass phrase and the data set name in the provided spaces.

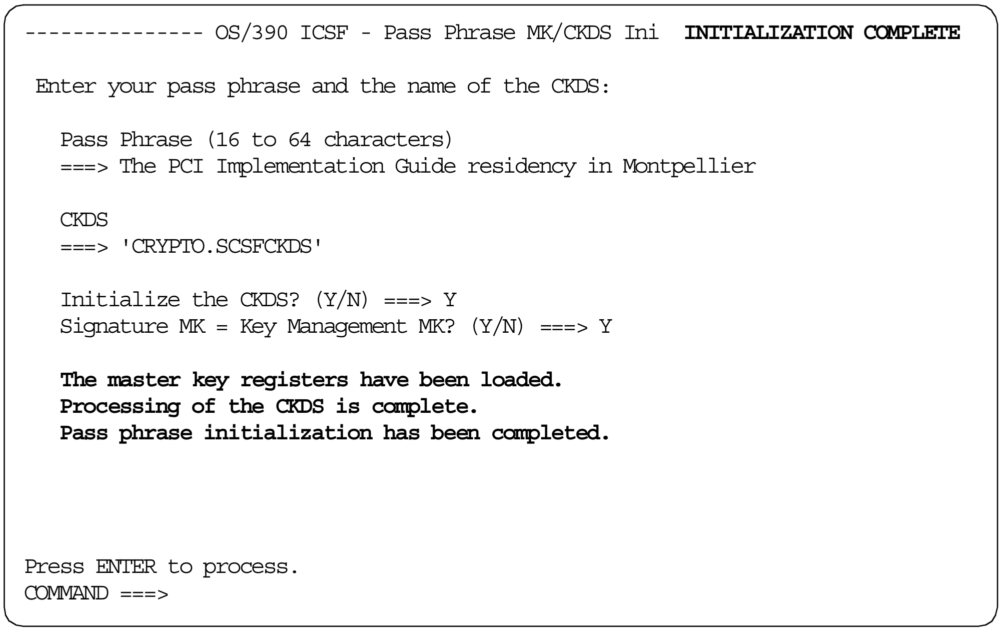
Answer `Y` to the Signature MK = Key Management MK? question: the signature Master Key and the Key Management Master Key in the CCFs will have the same value as the ASYM-MK on the PCI Cryptographic Coprocessors.



```
-------------- OS/390 ICSF - Pass Phrase MK/CKDS Initialization ----

 Enter your pass phrase and the name of the CKDS:

   Pass Phrase (16 to 64 characters)
   ===> The PCI Implementation Guide residency in Montpellier

   CKDS
   ===> 'CRYPTO.SCSFCKDS'

   Initialize the CKDS? (Y/N) ===> Y
   Signature MK = Key Management MK? (Y/N) ===> Y







Press ENTER to process.
COMMAND ===>
```

Figure 34. Entering options on the Pass Phrase MK/CKDS Initialization panel

Press Enter to run the utility. Its progress is indicated by messages, as shown in Figure 35 on page 73.



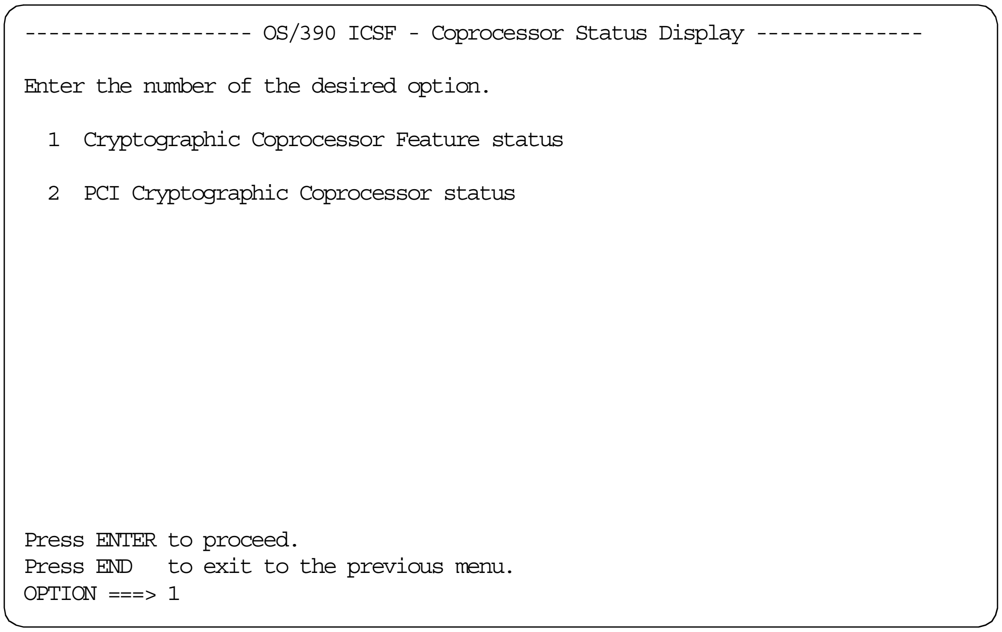
```
--------------- OS/390 ICSF - Pass Phrase MK/CKDS Ini  INITIALIZATION COMPLETE

 Enter your pass phrase and the name of the CKDS:

   Pass Phrase (16 to 64 characters)
   ===> The PCI Implementation Guide residency in Montpellier

   CKDS
   ===> 'CRYPTO.SCSFCKDS'

   Initialize the CKDS? (Y/N) ===> Y
   Signature MK = Key Management MK? (Y/N) ===> Y

   The master key registers have been loaded.
   Processing of the CKDS is complete.
   Pass phrase initialization has been completed.




Press ENTER to process.
COMMAND ===>
```

Figure 35. Pass phrase initialization complete messages

4.4.5.1 Hardware status display after the pass phrase initialization

To display the hardware status using the ICSF/ISPF panels:

1. Select option 3, **OPSTAT**, on the ICSF primary menu panel.
2. Select option 2, **STATUS**, from the Installation Options and Status panel. You will get the Coprocessor Status Display shown in Figure 36.



```
------------------- OS/390 ICSF - Coprocessor Status Display --------------

Enter the number of the desired option.

  1  Cryptographic Coprocessor Feature status

  2  PCI Cryptographic Coprocessor status











Press ENTER to proceed.
Press END   to exit to the previous menu.
OPTION ===> 1
```

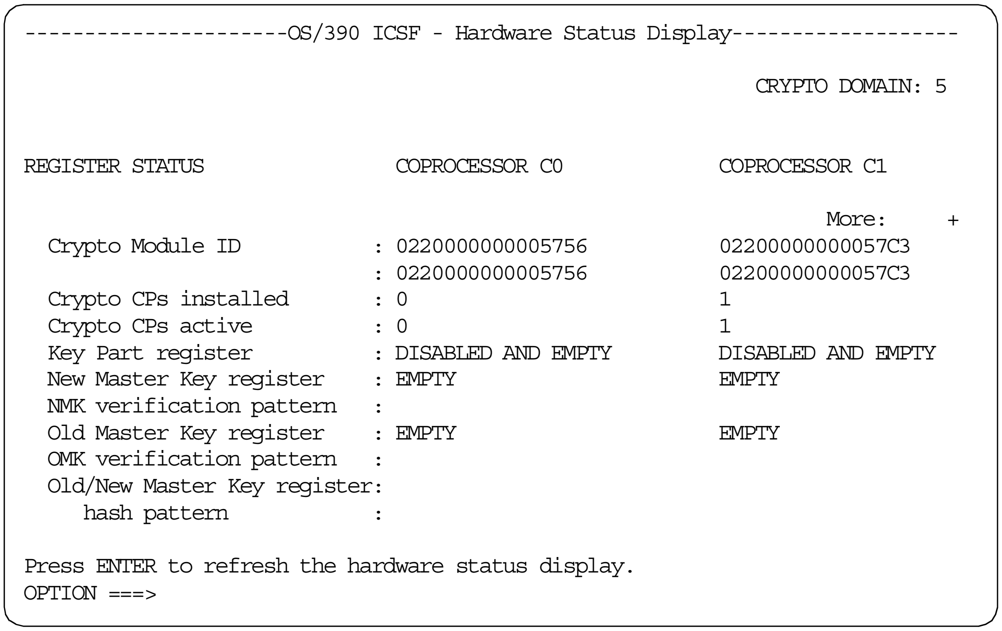
Figure 36. Coprocessor Status Display selection panel

3. To display the status of the Cryptographic Coprocessor Feature, select option **1**.

The scrollable Hardware Status Display panel appears as shown in Figure 37, in Figure 38 on page 75, and in Figure 39 on page 75. On these panels, you can view the status of the Cryptographic Coprocessor Feature. You can check whether a unit is active and whether its registers are in the correct state.

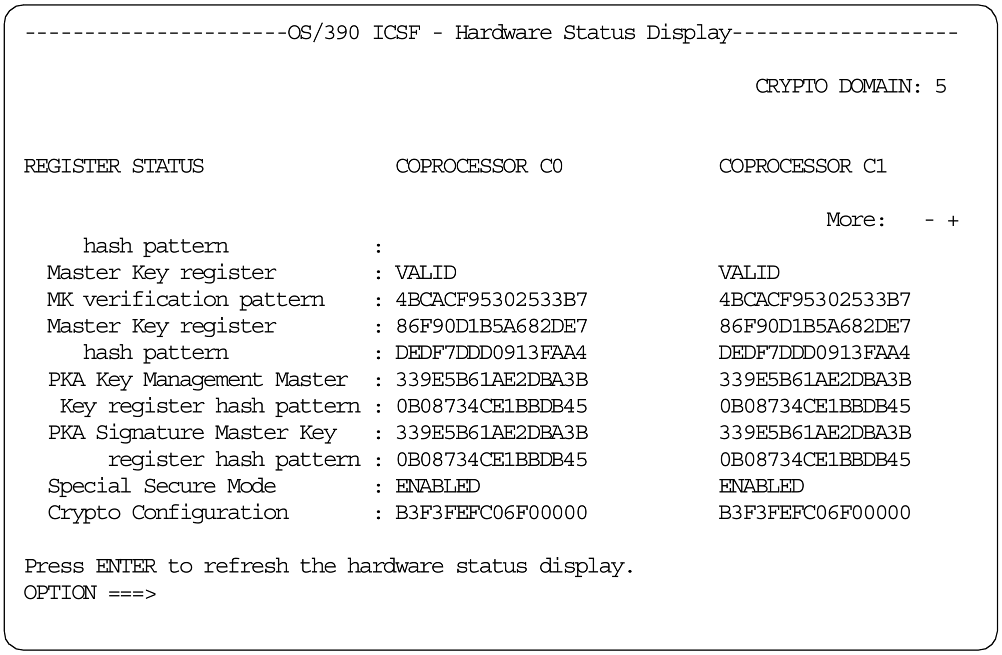
The key register fields show the state of the registers and their verification pattern and/or hash pattern values. In Figure 38 on page 75 you can see most clearly that both Cryptographic Coprocessors have the same DES Master Key installed, since the Master Key Verification Pattern values are the same.

The PKA Key Management Master Key register hash pattern and the PKA Signature Master Key register hash pattern are also equal, which was the requirement when we started the pass phrase initialization utility.



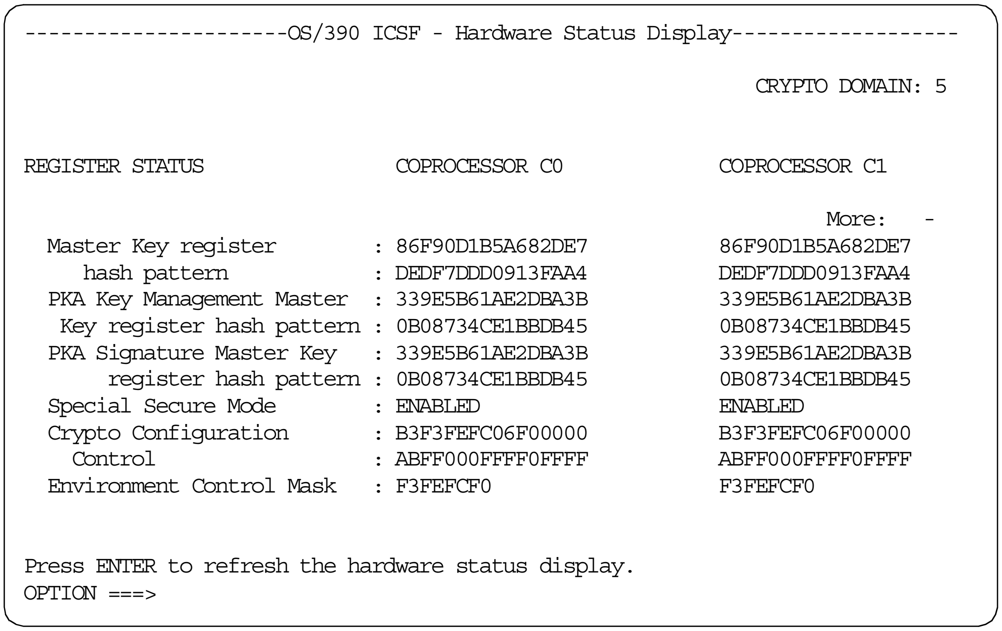
```
----------------------OS/390 ICSF - Hardware Status Display-------------------

                                                              CRYPTO DOMAIN: 5


REGISTER STATUS                COPROCESSOR C0             COPROCESSOR C1

                                                                   More:     +
  Crypto Module ID           : 0220000000005756           02200000000057C3
                             : 0220000000005756           02200000000057C3
  Crypto CPs installed       : 0                          1
  Crypto CPs active          : 0                          1
  Key Part register          : DISABLED AND EMPTY         DISABLED AND EMPTY
  New Master Key register    : EMPTY                      EMPTY
  NMK verification pattern   :
  Old Master Key register    : EMPTY                      EMPTY
  OMK verification pattern   :
  Old/New Master Key register:
     hash pattern            :

Press ENTER to refresh the hardware status display.
OPTION ===>
```

Figure 37. Cryptographic Coprocessor Feature hardware status, panel 1



```
---------------------OS/390 ICSF - Hardware Status Display-------------------
                                                              CRYPTO DOMAIN: 5


REGISTER STATUS                COPROCESSOR C0             COPROCESSOR C1

                                                                More:   - +
     hash pattern           :
  Master Key register       : VALID                       VALID
  MK verification pattern   : 4BCACF95302533B7            4BCACF95302533B7
  Master Key register       : 86F90D1B5A682DE7            86F90D1B5A682DE7
     hash pattern           : DEDF7DDD0913FAA4            DEDF7DDD0913FAA4
  PKA Key Management Master : 339E5B61AE2DBA3B            339E5B61AE2DBA3B
   Key register hash pattern : 0B08734CE1BBDB45           0B08734CE1BBDB45
  PKA Signature Master Key  : 339E5B61AE2DBA3B            339E5B61AE2DBA3B
       register hash pattern : 0B08734CE1BBDB45           0B08734CE1BBDB45
  Special Secure Mode       : ENABLED                     ENABLED
  Crypto Configuration      : B3F3FEFC06F00000            B3F3FEFC06F00000

Press ENTER to refresh the hardware status display.
OPTION ===>
```

Figure 38. Cryptographic Coprocessor Feature hardware status, panel 2

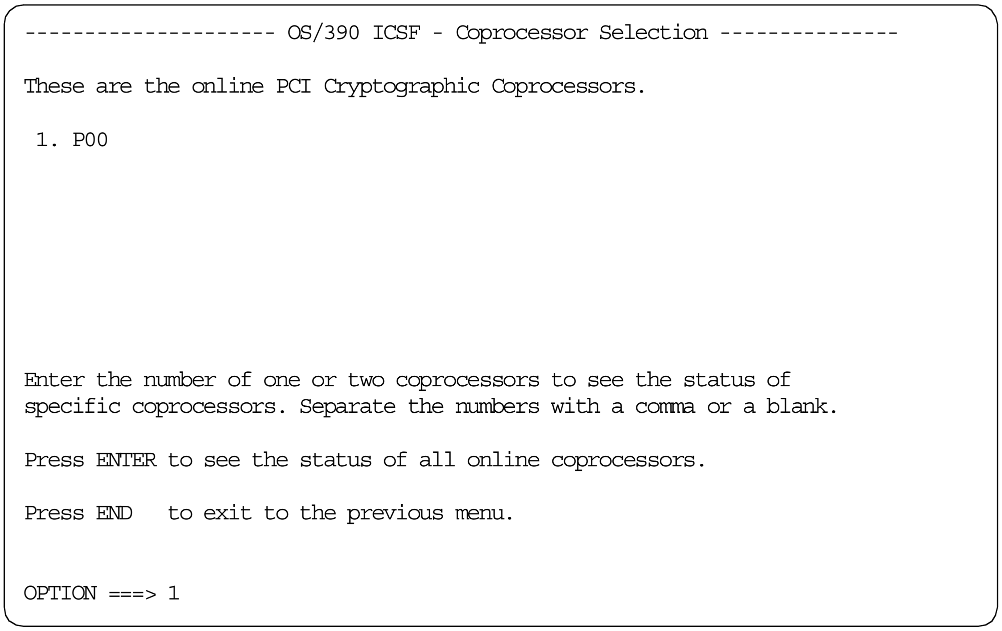


```
---------------------OS/390 ICSF - Hardware Status Display-------------------
                                                              CRYPTO DOMAIN: 5


REGISTER STATUS                COPROCESSOR C0             COPROCESSOR C1

                                                                More:   -
  Master Key register       : 86F90D1B5A682DE7            86F90D1B5A682DE7
     hash pattern           : DEDF7DDD0913FAA4            DEDF7DDD0913FAA4
  PKA Key Management Master : 339E5B61AE2DBA3B            339E5B61AE2DBA3B
   Key register hash pattern : 0B08734CE1BBDB45           0B08734CE1BBDB45
  PKA Signature Master Key  : 339E5B61AE2DBA3B            339E5B61AE2DBA3B
       register hash pattern : 0B08734CE1BBDB45           0B08734CE1BBDB45
  Special Secure Mode       : ENABLED                     ENABLED
  Crypto Configuration      : B3F3FEFC06F00000            B3F3FEFC06F00000
    Control                 : ABFF000FFFF0FFFF            ABFF000FFFF0FFFF
  Environment Control Mask  : F3FEFCF0                    F3FEFCF0


Press ENTER to refresh the hardware status display.
OPTION ===>
```

Figure 39. Cryptographic Coprocessor Feature hardware status, panel 3

To display the status of the PCICCs, select option **2** in Figure 36 on page 73 and a selection panel appears as shown in Figure 40 on page 76.

To see the status of one or two PCICCs, enter their AP number separated by a blank or comma, or press Enter without entering any specific number to see all of them. In our case we only installed one PCICC.

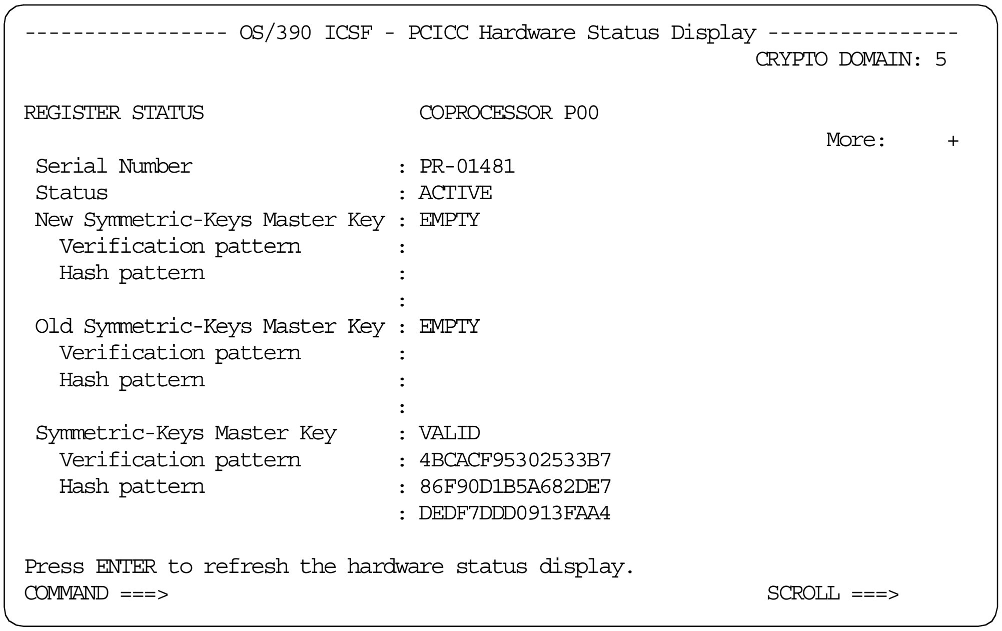


```
-------------------- OS/390 ICSF - Coprocessor Selection ---------------

These are the online PCI Cryptographic Coprocessors.

 1. P00









Enter the number of one or two coprocessors to see the status of
specific coprocessors. Separate the numbers with a comma or a blank.

Press ENTER to see the status of all online coprocessors.

Press END   to exit to the previous menu.


OPTION ===> 1
```

Figure 40. The PCICC selection panel

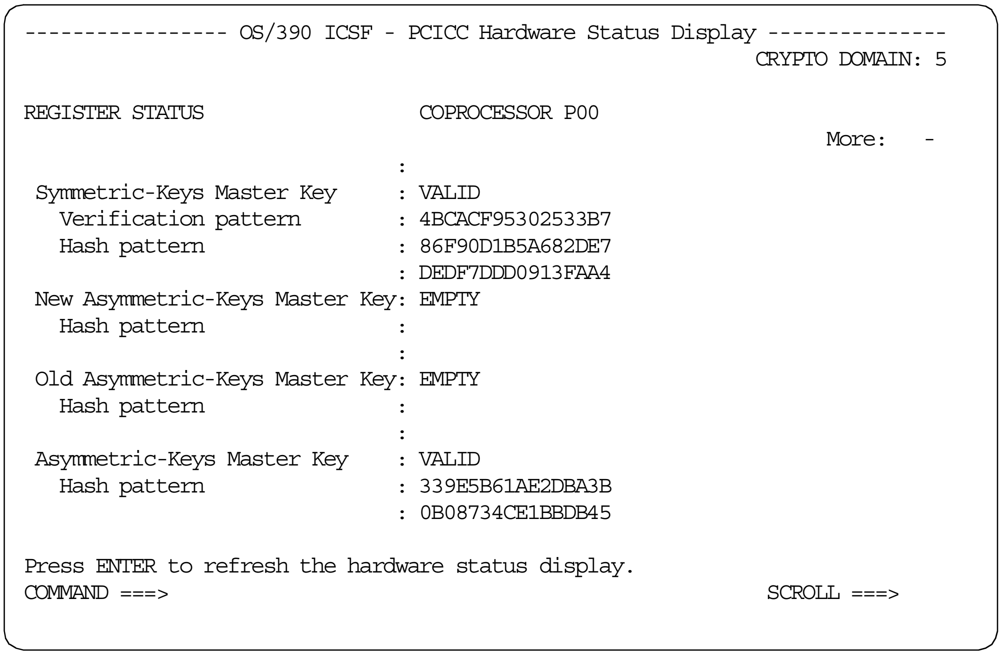
The scrollable PCI Hardware Status Display panel appears as shown in Figure 41 on page 77 and in Figure 42 on page 77. On these panels, you can view the status of the PCI Cryptographic Coprocessors. If you selected to view all PCICCs, you can also scroll right and left with the PFkeys, to see information pertaining to the other PCICCs.

Note that the Symmetric-Keys Master Key Verification pattern in Figure 41 on page 77 matches the DES MK verification pattern shown in Figure 38 on page 75. Also, the Asymmetric-Keys Master Key Hash pattern in Figure 42 on page 77 matches the PKA KMMK and SMK register hash patterns in Figure 39 on page 75.



```
----------------- OS/390 ICSF - PCICC Hardware Status Display ----------------
                                                            CRYPTO DOMAIN: 5

REGISTER STATUS                  COPROCESSOR P00
                                                                  More:     +
 Serial Number                 : PR-01481
 Status                        : ACTIVE
 New Symmetric-Keys Master Key : EMPTY
   Verification pattern        :
   Hash pattern                :
                               :
 Old Symmetric-Keys Master Key : EMPTY
   Verification pattern        :
   Hash pattern                :
                               :
 Symmetric-Keys Master Key     : VALID
   Verification pattern        : 4BCACF95302533B7
   Hash pattern                : 86F90D1B5A682DE7
                               : DEDF7DDD0913FAA4

Press ENTER to refresh the hardware status display.
COMMAND ===>                                                 SCROLL ===>
```

Figure 41. The PCICC hardware status, panel 1



```
----------------- OS/390 ICSF - PCICC Hardware Status Display ---------------
                                                            CRYPTO DOMAIN: 5

REGISTER STATUS                  COPROCESSOR P00
                                                                  More:   -
                               :
 Symmetric-Keys Master Key     : VALID
   Verification pattern        : 4BCACF95302533B7
   Hash pattern                : 86F90D1B5A682DE7
                               : DEDF7DDD0913FAA4
 New Asymmetric-Keys Master Key: EMPTY
   Hash pattern                :
                               :
 Old Asymmetric-Keys Master Key: EMPTY
   Hash pattern                :
                               :
 Asymmetric-Keys Master Key    : VALID
   Hash pattern                : 339E5B61AE2DBA3B
                               : 0B08734CE1BBDB45

Press ENTER to refresh the hardware status display.
COMMAND ===>                                                 SCROLL ===>
```

Figure 42. The PCICC hardware status, panel 2

4.4.5.2 PKDS status after the pass phrase initialization

Pass phrase Initialization does not write the PKDS.

The PKDS designated in the Options Data Set is written with one record, the “header record,” when ICSF starts for the first time. The fields in the header record comprise the hash patterns for the current KMMK and SMK PKA, which are set to 0s at the time of this first writing. They will be updated when the first key is stored in the PKDS. If you stop and restart ICSF before this first storing of a key in the PKDS, you will see the message shown in Figure 43. The other implication of this situation is that ICSF automatically disallows read and write access to the PKDS by the application. It takes a manual intervention via the ICSF USERCNTL panel to enable these accesses.

```
CSFM405A AUTHENTICATION CODE IN PKDS HEADER RECORD DOES NOT MATCH
COMPUTED VALUE.
```

Figure 43. Message on the ICSF startup before the first write to PKDS

You can avoid this problem, if deemed necessary, by either writing a record into the PKDS via your own coded routine or by importing an RSA key. Before writing the record to the PKDS, insure that the write to PKDS is enabled, as indicated before. The CKDS is completely initialized, with system keys written in the data set, during the pass phrase initialization process.

4.4.6 Changing the Master Keys for CCF and PCICC via ICSF panels

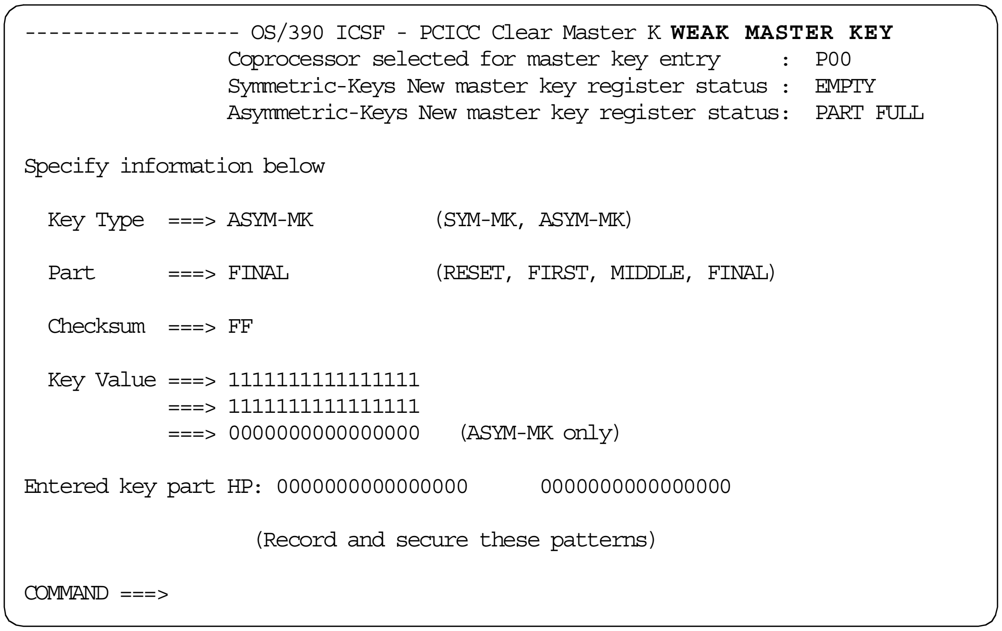
The pass phrase initialization utility is intended to get you started easily and quickly with ICSF and coprocessor initialization. However, this is not a secure way of administering Master Keys since the pass phrase character string is the “synonym” of the clear key values. It is therefore recommended that you proceed with a Master Key change, using new Master Keys generated and entered according to your site security policy. Also, for security reasons, you may want to periodically change your Master Keys.

If the Master Keys have been cleared from the crypto coprocessors due to a tamper detection, or if you zeroized the domain from the TKE workstation, the keys in the CKDS that are still enciphered under that Master Key must be recovered. In order to do this, you must reenter the same Master Keys as before and activate them, and then you may change the Master Keys if desired.

4.4.6.1 Weak Master Keys

The PCICC tests whether the entered new Master Key is a DES “weak key”. A DES weak key is a bit string with such a configuration that the so-called “subkeys”, generated in the DES algorithm internal process, do not have the variance level required to insure maximum security. This test is done after the final part of the new Master Key has been entered and combined with the previous parts. If the new Master Key, be it the SYM-MK or the ASYM-MK, is a DES weak key, then the Master Key has to be entered with new values.

To illustrate this, here is an example (see Figure 44 on page 79), where the new Master Key is rejected because it is a DES weak key.



```
------------------ OS/390 ICSF - PCICC Clear Master K WEAK MASTER KEY
                 Coprocessor selected for master key entry     :  P00
                 Symmetric-Keys New master key register status :  EMPTY
                 Asymmetric-Keys New master key register status:  PART FULL

Specify information below

  Key Type  ===> ASYM-MK          (SYM-MK, ASYM-MK)

  Part      ===> FINAL            (RESET, FIRST, MIDDLE, FINAL)

  Checksum  ===> FF

  Key Value ===> 1111111111111111
            ===> 1111111111111111
            ===> 0000000000000000   (ASYM-MK only)

Entered key part HP: 0000000000000000      0000000000000000

                   (Record and secure these patterns)

COMMAND ===>
```

Figure 44. PCICC does not accept weak keys

Recommendation

Start entering the DES Master Keys and the PKA Master Keys first from the PCI Cryptographic Coprocessor, and then generate at least one key part using a random number generator to get an acceptable Master Key.

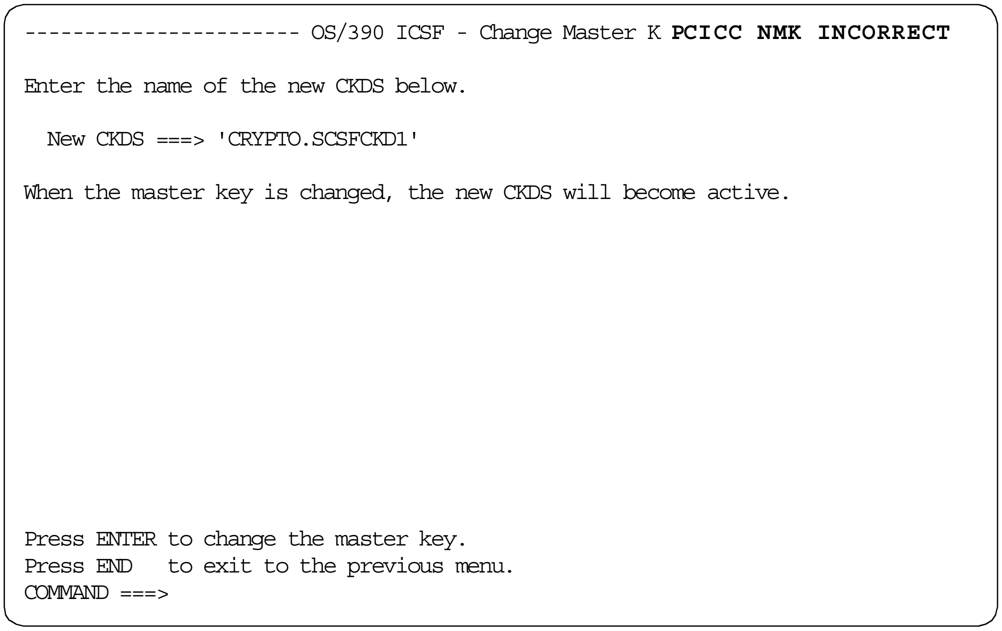
4.4.6.2 Changing the DES Master Key

Changing a DES Master Key implies first to load a new DES Master Key in the new Master Key register and then, usually, to reencipher the current CKDS with the new Master Key, unless you want to start from scratch with a new CKDS.

To load the DES new Master Key register, we enter the new key at least in two key parts using the ICSF clear Master Key entry panels. Each of the key parts is 16 bytes long. When the key parts are entered manually, ICSF asks for a checksum that must be entered to verify that integrity of the key part. The checksum has to be computed in advance by using, for example, the ICSF utilities panel. After a key part and its checksum are entered, an eight-byte verification pattern is computed and displayed by ICSF.

Then the reencipherment of the CKDS into a new CKDS is triggered from the Change/Reencipher panel. Note that if ICSF is using two CCFs, they must both have the same new Master Key value in the new Master Key register, otherwise ICSF refuses to proceed with the reencipher. When the CKDS is enciphered under the new Master Key, ICSF stores the new Master Key verification pattern in the new CKDS header record. In our example, we reencyphered from CRYPTO.SCSFCKDS to CRYPTO.SCSFCKD1’.

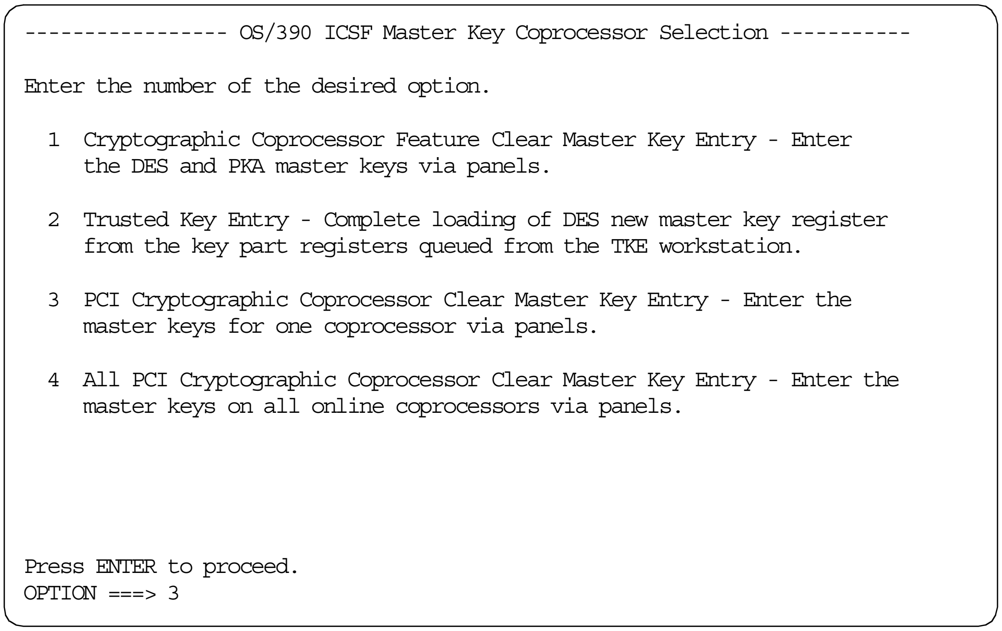
At this point the new Master Key is still in the new Master Key register. It must be loaded in the current DES Master Key register using the CHANGE option in the Change/Reencipher panel. It is required that all the new Master Key registers, new DES Master Key registers, and SYM-MK registers have the same value, otherwise ICSF refuses to change the Master Key with the error message shown in Figure 45.



```
---------------------- OS/390 ICSF - Change Master K PCICC NMK INCORRECT

Enter the name of the new CKDS below.

  New CKDS ===> 'CRYPTO.SCSFCKD1'

When the master key is changed, the new CKDS will become active.











Press ENTER to change the master key.
Press END   to exit to the previous menu.
COMMAND ===>
```

Figure 45. Master Key change failed

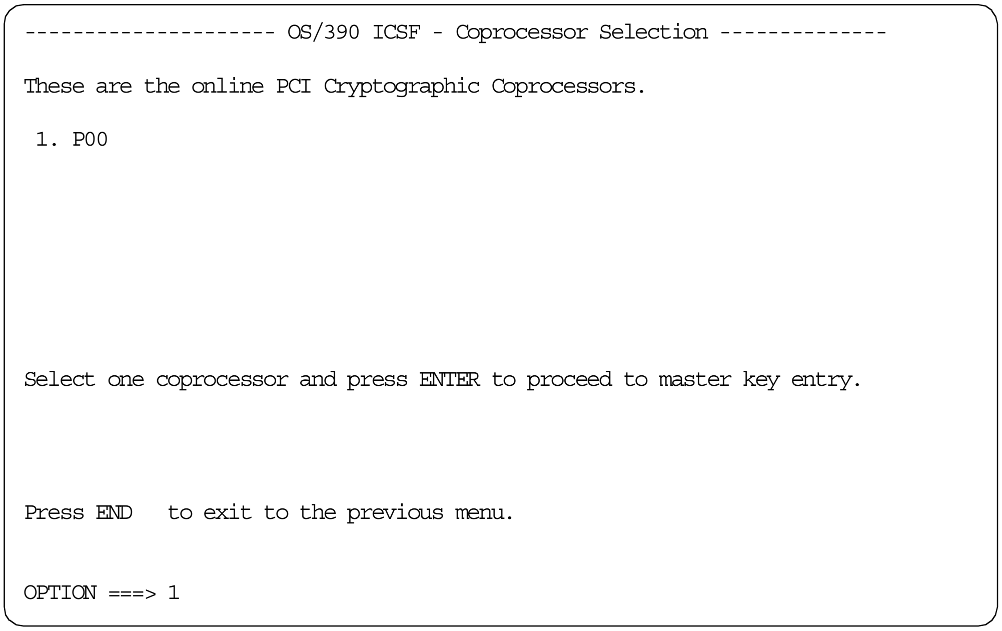
The process to load the new Master Key in the PCICC is similar to that of the CCF. The entry process starts from the ICSF main panel selecting option 1, and you will get the panel shown in Figure 46 on page 81. There you can select whether the Master Key entry will affect all PCICCs that are online, or whether the Master Key entry affects only a specific PCICC. We recommend that you select option 4 to easily enter the new Master Key in all PCICCs. We selected in our case option 3, because we had only one PCICC.



```
----------------- OS/390 ICSF Master Key Coprocessor Selection -----------

Enter the number of the desired option.

  1  Cryptographic Coprocessor Feature Clear Master Key Entry - Enter
     the DES and PKA master keys via panels.

  2  Trusted Key Entry - Complete loading of DES new master key register
     from the key part registers queued from the TKE workstation.

  3  PCI Cryptographic Coprocessor Clear Master Key Entry - Enter the
     master keys for one coprocessor via panels.

  4  All PCI Cryptographic Coprocessor Clear Master Key Entry - Enter the
     master keys on all online coprocessors via panels.




Press ENTER to proceed.
OPTION ===> 3
```

Figure 46. The clear Master Key entry for only one PCICC

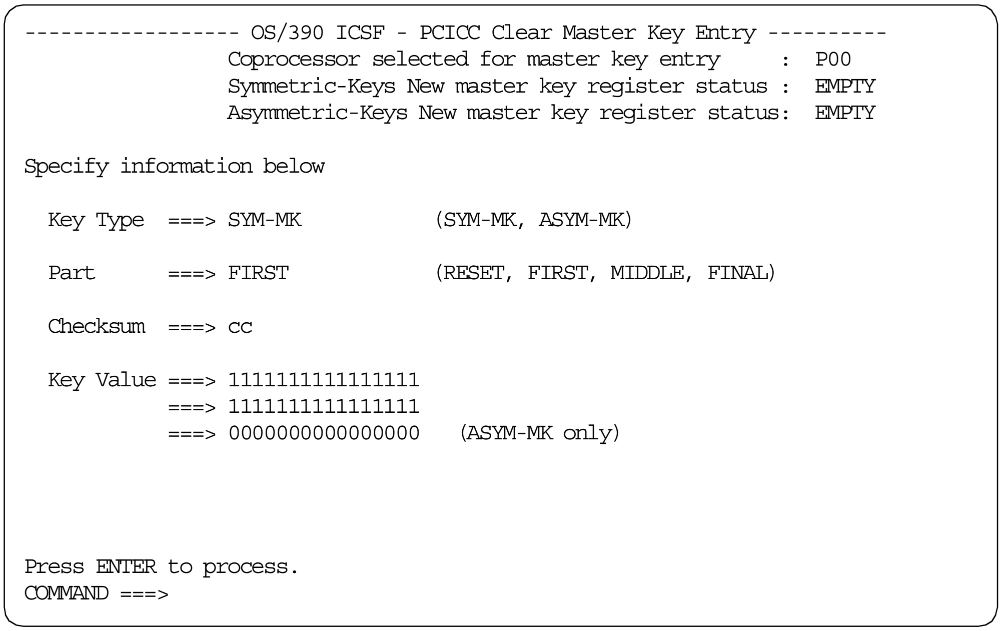
After selecting option 3 and pressing Enter, the panel shown in Figure 47 appears. Here we select option **1**.



```
--------------------- OS/390 ICSF - Coprocessor Selection --------------

These are the online PCI Cryptographic Coprocessors.

 1. P00







Select one coprocessor and press ENTER to proceed to master key entry.




Press END   to exit to the previous menu.


OPTION ===> 1
```

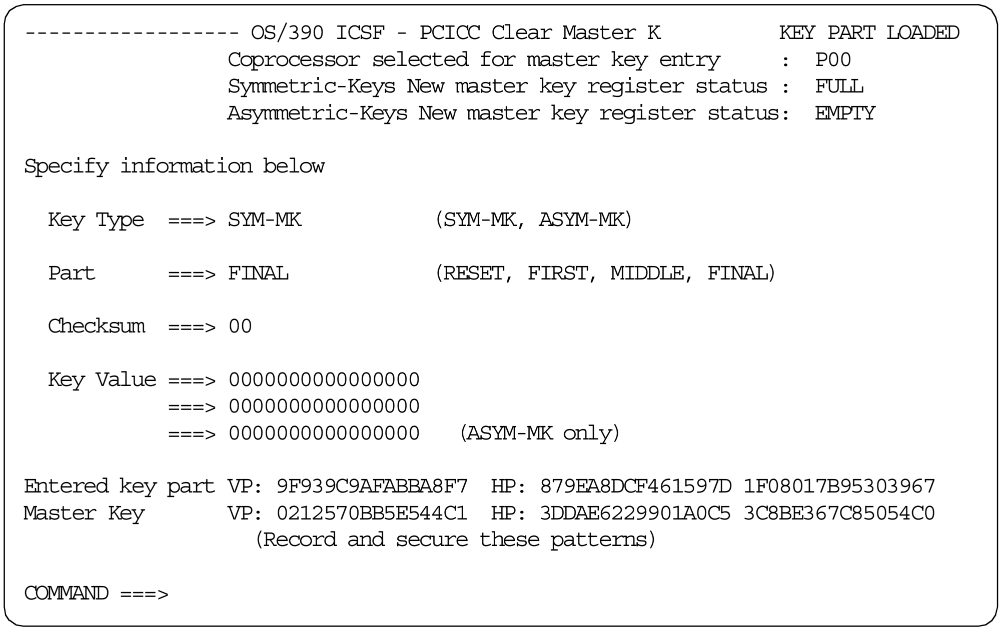
Figure 47. Select the correct PCICC for the clear Master Key entry

In the next panel, shown in Figure 48 on page 82, the new key type is entered, along with the usual information on the key part position and the clear key part value. The final key part is loaded in Figure 49 on page 82.



```
------------------ OS/390 ICSF - PCICC Clear Master Key Entry ----------
                 Coprocessor selected for master key entry     :  P00
                 Symmetric-Keys New master key register status :  EMPTY
                 Asymmetric-Keys New master key register status:  EMPTY

Specify information below

  Key Type  ===> SYM-MK           (SYM-MK, ASYM-MK)

  Part      ===> FIRST            (RESET, FIRST, MIDDLE, FINAL)

  Checksum  ===> cc

  Key Value ===> 1111111111111111
            ===> 1111111111111111
            ===> 0000000000000000   (ASYM-MK only)




Press ENTER to process.
COMMAND ===>
```

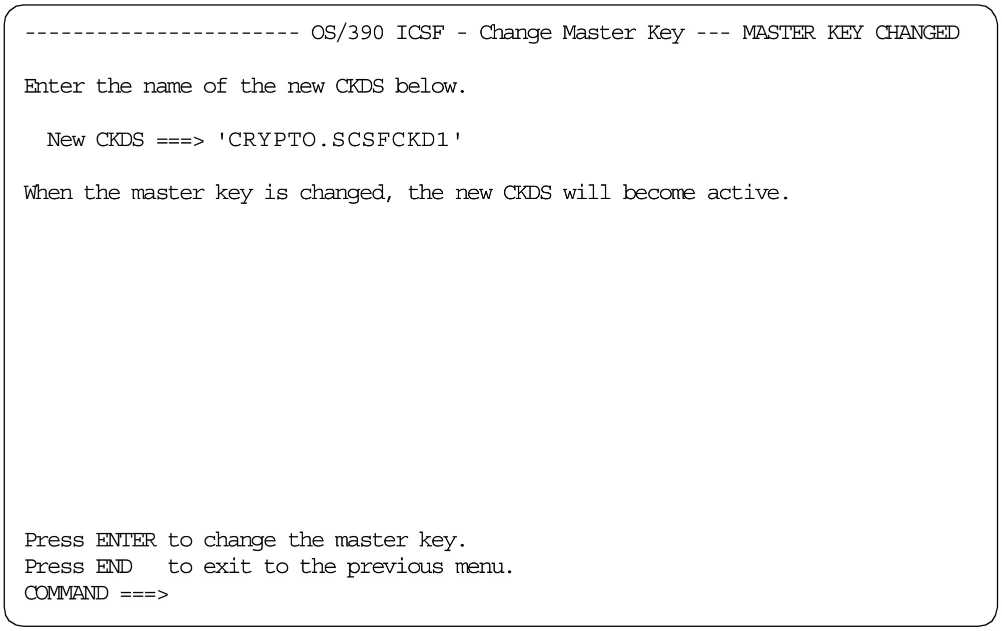
Figure 48. Entering the first key part values



```
------------------ OS/390 ICSF - PCICC Clear Master K          KEY PART LOADED
                 Coprocessor selected for master key entry     :  P00
                 Symmetric-Keys New master key register status :  FULL
                 Asymmetric-Keys New master key register status:  EMPTY

Specify information below

  Key Type  ===> SYM-MK           (SYM-MK, ASYM-MK)

  Part      ===> FINAL            (RESET, FIRST, MIDDLE, FINAL)

  Checksum  ===> 00

  Key Value ===> 0000000000000000
            ===> 0000000000000000
            ===> 0000000000000000   (ASYM-MK only)

Entered key part VP: 9F939C9AFABBA8F7  HP: 879EA8DCF461597D 1F08017B95303967
Master Key       VP: 0212570BB5E544C1  HP: 3DDAE6229901A0C5 3C8BE367C85054C0
                   (Record and secure these patterns)

COMMAND ===>
```

Figure 49. After the final key part was entered

When both cryptographic processors (CCF and PCICC) have the same DES new Master Key, the actual Master Key change can be done as shown in Figure 50 on page 83.

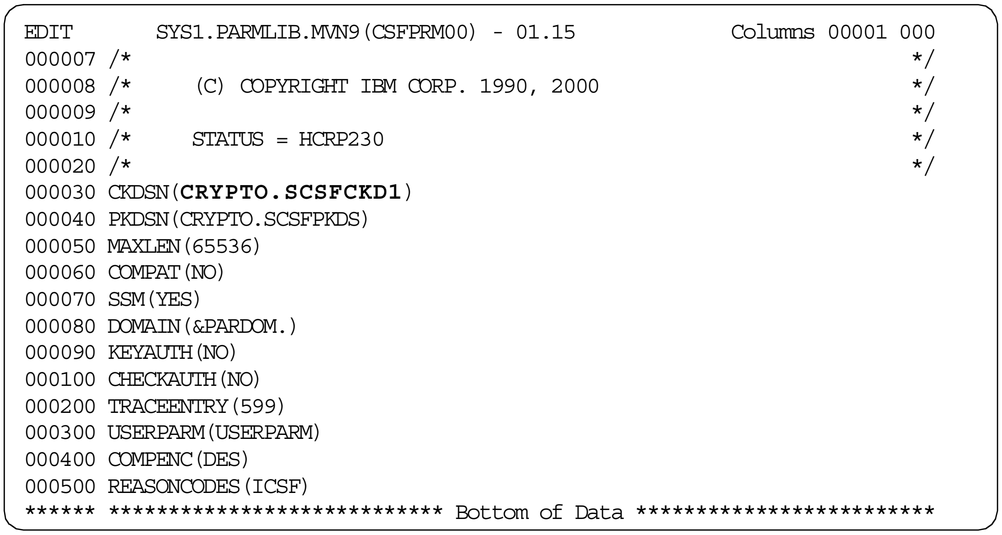


```
---------------------- OS/390 ICSF - Change Master Key --- MASTER KEY CHANGED

Enter the name of the new CKDS below.

  New CKDS ===> 'CRYPTO.SCSFCKD1'

When the master key is changed, the new CKDS will become active.











Press ENTER to change the master key.
Press END   to exit to the previous menu.
COMMAND ===>
```

Figure 50. The Master Key change was successful

As part of the Master Key change, ICSF loads the reenciphered disk copy of the CKDS data set into storage where it becomes the in-storage CKDS in operation, and loads the current Master Key register with the contents of the new Master Key register in all the coprocessors.

Remember to change the CKDSN value in the Options Data Set to reflect the new CKDS name (see Figure 51). The change in the Options Data Set is necessary for the next start of ICSF.



```
EDIT       SYS1.PARMLIB.MVN9(CSFPRM00) - 01.15           Columns 00001 000
000007 /*                                                               */
000008 /*     (C) COPYRIGHT IBM CORP. 1990, 2000                        */
000009 /*                                                               */
000010 /*     STATUS = HCRP230                                          */
000020 /*                                                               */
000030 CKDSN(CRYPTO.SCSFCKD1)
000040 PKDSN(CRYPTO.SCSFPKDS)
000050 MAXLEN(65536)
000060 COMPAT(NO)
000070 SSM(YES)
000080 DOMAIN(&PARDOM.)
000090 KEYAUTH(NO)
000100 CHECKAUTH(NO)
000200 TRACEENTRY(599)
000300 USERPARM(USERPARM)
000400 COMPENC(DES)
000500 REASONCODES(ICSF)
****** **************************** Bottom of Data *************************
```

Figure 51. Change the CKDSN value in the Options Data Set

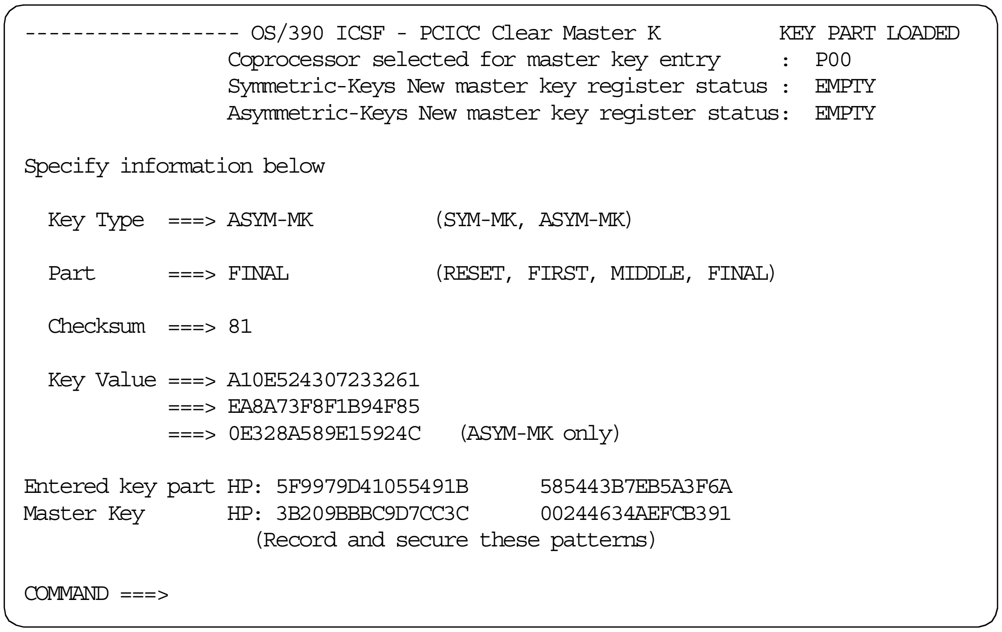
4.4.6.3 Changing the PKA Master Keys

Changing the PKA Master Keys will make all internal tokens in the current PKDS unusable. There is no dynamic reencipherment of the PKDS. You will need to re-create the PKA application key tokens manually under the new PKA Master Keys in order to use them with the changed Master Key.

To change the PKA Master Keys, go to the user control functions by selecting option 7, USERCNTL on the primary menu panel, and disable the PKA callable services by selecting option 4 and pressing Enter.

We entered all PKA Master Key parts starting with the PCICC, then we entered the same two values into the CCFs. This was motivated by PCICC needing at least two key parts, first and final, whereas CCF, although not recommended, can have only one PKA Master Key part. The differences in the loading process of the PKA Master Key between the CCF and the PCICC are:

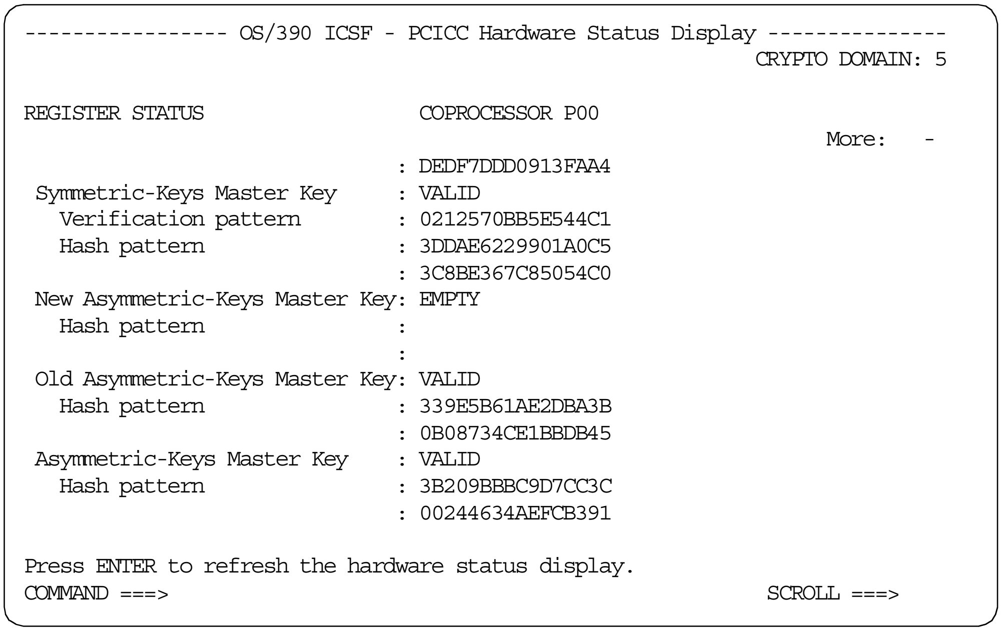
- The CCF requires that you:
  1. RESET the PKA Master Key register to be loaded.
  2. Proceed with entering the key parts, at least one key part. The key parts are combined in the PKA Master Key register.
- The PCICC has three ASYM-MK registers: a new register, the current Master Key and the old Master Key register. These registers are visible in the hardware status panel, which shows the hash patterns of all three registers.
  1. The RESET affects the new ASYM-MK register only.
  2. The new ASYM-MK key parts are loaded and combined into the new Master Key register. The system requires at least two key parts.
  3. When the key part entered is flagged as FINAL, the new Master Key is tested for a DES weak key value. If not a weak key, the current ASYM-MK register is automatically loaded with the contents of the new Master Key register. Figure 52 illustrates this process.



```
------------------ OS/390 ICSF - PCICC Clear Master K          KEY PART LOADED
                 Coprocessor selected for master key entry     :  P00
                 Symmetric-Keys New master key register status :  EMPTY
                 Asymmetric-Keys New master key register status:  EMPTY

Specify information below

  Key Type  ===> ASYM-MK          (SYM-MK, ASYM-MK)

  Part      ===> FINAL            (RESET, FIRST, MIDDLE, FINAL)

  Checksum  ===> 81

  Key Value ===> A10E524307233261
            ===> EA8A73F8F1B94F85
            ===> 0E328A589E15924C   (ASYM-MK only)

Entered key part HP: 5F9979D41055491B      585443B7EB5A3F6A
Master Key       HP: 3B209BBBC9D7CC3C      00244634AEFCB391
                   (Record and secure these patterns)

COMMAND ===>
```

Figure 52. The final ASYM-MK key part is loaded

In the PCICC hardware status pane in Figure 53, we see that the previous Asymmetric-Keys Master Key has been moved to the old Asymmetric-Keys Master Key register.



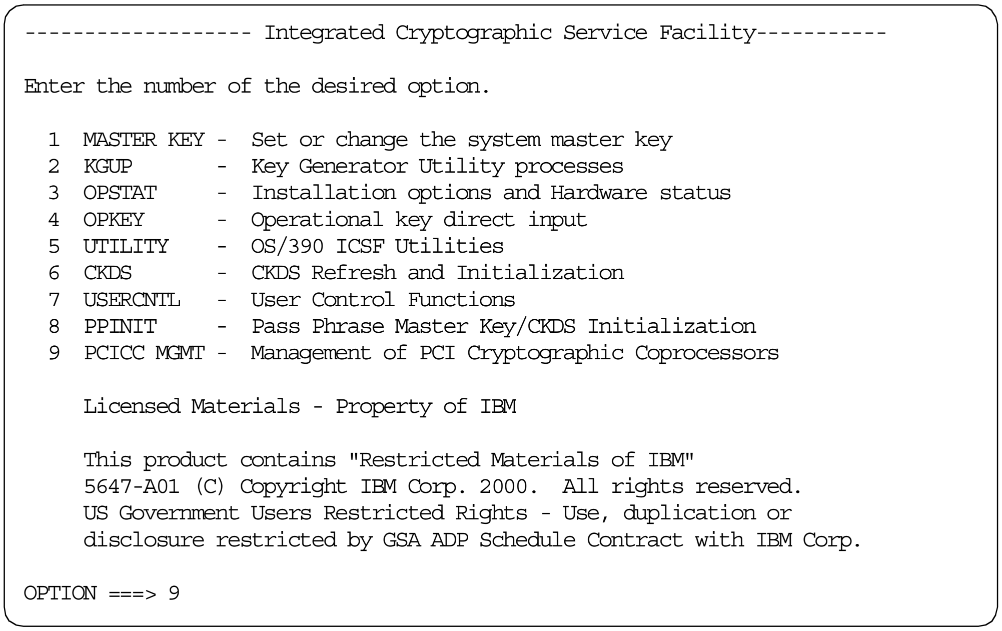
```
----------------- OS/390 ICSF - PCICC Hardware Status Display ---------------
                                                            CRYPTO DOMAIN: 5

REGISTER STATUS                  COPROCESSOR P00
                                                                  More:   -
                               : DEDF7DDD0913FAA4
 Symmetric-Keys Master Key     : VALID
   Verification pattern        : 0212570BB5E544C1
   Hash pattern                : 3DDAE6229901A0C5
                               : 3C8BE367C85054C0
 New Asymmetric-Keys Master Key: EMPTY
   Hash pattern                :
                               :
 Old Asymmetric-Keys Master Key: VALID
   Hash pattern                : 339E5B61AE2DBA3B
                               : 0B08734CE1BBDB45
 Asymmetric-Keys Master Key    : VALID
   Hash pattern                : 3B209BBBC9D7CC3C
                               : 00244634AEFCB391

Press ENTER to refresh the hardware status display.
COMMAND ===>                                                 SCROLL ===>
```

Figure 53. PCICC hardware status after the PKA Master Key changed

When all the Master Keys have been changed, enable the PKA services by selecting option **7**, **USERCNTL**, in the primary menu panel, and then selecting option 3, **ENABLE**, and then pressing Enter.

4.4.7 Management of the PCI Cryptographic Coprocessors

The PCICC Management panel displays the status of all the PCICCs defined to the partition or installed in the system; select option **9** from the main panel, as shown in Figure 54 on page 86.



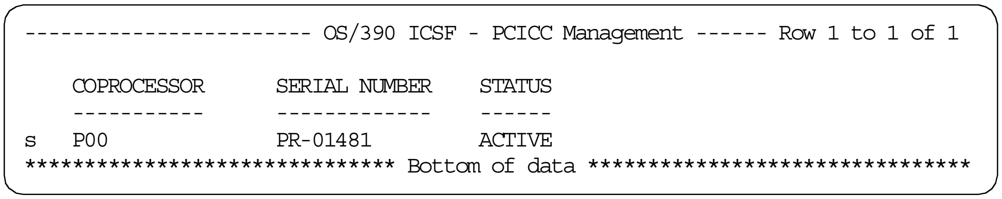
```
------------------ Integrated Cryptographic Service Facility-----------

Enter the number of the desired option.

  1  MASTER KEY -  Set or change the system master key
  2  KGUP       -  Key Generator Utility processes
  3  OPSTAT     -  Installation options and Hardware status
  4  OPKEY      -  Operational key direct input
  5  UTILITY    -  OS/390 ICSF Utilities
  6  CKDS       -  CKDS Refresh and Initialization
  7  USERCNTL   -  User Control Functions
  8  PPINIT     -  Pass Phrase Master Key/CKDS Initialization
  9  PCICC MGMT -  Management of PCI Cryptographic Coprocessors

     Licensed Materials - Property of IBM

     This product contains "Restricted Materials of IBM"
     5647-A01 (C) Copyright IBM Corp. 2000.  All rights reserved.
     US Government Users Restricted Rights - Use, duplication or
     disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

OPTION ===> 9
```

Figure 54. Selecting the PCICC management from the ICSF main panel

When you press Enter you will get the panel shown in Figure 55, where in our case there is only one logical PCICC defined to the partition.

A PCICC must be in the “active” state to perform the cryptographic services requested by the applications.

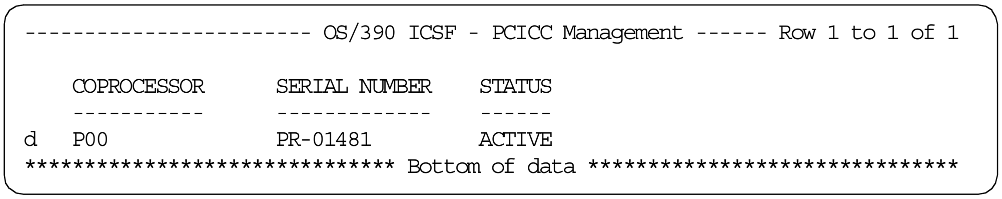
There are four action characters that can be entered on the left of the coprocessor number. When you select action character “s” or “/”, you will get the same PCICC Hardware Status Display as shown in Figure 41 on page 77.



```
----------------------- OS/390 ICSF - PCICC Management ------ Row 1 to 1 of 1

    COPROCESSOR      SERIAL NUMBER    STATUS
    -----------      -------------    ------
s   P00              PR-01481         ACTIVE
******************************* Bottom of data ********************************
```

Figure 55. Select to see the hardware status of the PCICC card

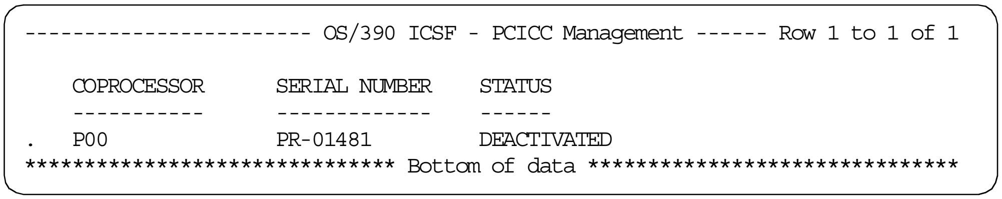
If you select the action character “d”, as shown in Figure 56, it will make the PCICC unavailable to ICSF. This is done when there is a need to remove the PCICC from the system.



```
----------------------- OS/390 ICSF - PCICC Management ------ Row 1 to 1 of 1

    COPROCESSOR      SERIAL NUMBER    STATUS
    -----------      -------------    ------
d   P00              PR-01481         ACTIVE
******************************* Bottom of data *******************************
```

Figure 56. Deactivate the PCICC card

When the request is made, the status of the PCICC becomes DEACTIVATED as shown in Figure 57. To make the deactivated PCICC available, you can use the action character “a”. When the request is made and if the PCICC is online and the Master Keys are correct, the status will be ACTIVE.



```
----------------------- OS/390 ICSF - PCICC Management ------ Row 1 to 1 of 1

    COPROCESSOR      SERIAL NUMBER    STATUS
    -----------      -------------    ------
.   P00              PR-01481         DEACTIVATED
****************************** Bottom of data ******************************
```

Figure 57. Deactivated PCICC card

Table 3 shows the status values and their explanations.

Table 3. The PCICC status values

Status	Explanation
ONLINE	The PCICC is available for certain commands, but either one or both of the Master Keys are incorrect. That is, there is no SYM-MK or ASYM-MK entered, or they respectively do not match the CCF DES MK and SMK.
OFFLINE	A PCICC may be physically present but it is not available to the operating system. Either it has never been configured online or it has been configured offline at the Support Element.
ACTIVE	The PCICC has correct Master Keys, that is, both SYM-MK and ASYM-MK match the CCF DES MK and SMK, and can be used for all eligible commands.
DEACTIVATED	The PCICC is online and may have correct Master Keys, but it has been removed from service with this management panel.
DISABLED	A Trusted Key Entry (TKE) workstation has removed the PCICC from service. Only a TKE workstation can enable the PCICC again.
UNKNOWN: CODE = cccc/ssss	The PCICC has returned an unrecognizable code in response to an attempt to determine its status. The return/reason code appears as the value of CODE.
TEMPORARILY UNAVAILABLE	An unexpected error has been returned from the card. The system goes into recovery to try to reset the card. If the reset is successful, the card is usable again. The user must press Enter to refresh the status.

Status	Explanation
HARDWARE ERROR	The PCICC has been stopped.

Note on “Activate”

The Activate action triggers the key test in the PCICC, that is, the check that the SYM-MK and ASYM-MK are set and identical, respectively, to the CCF DES MK and SMK. In this way you can make a PCICC switch from the ONLINE status to the ACTIVE status.

Chapter 5. Customizing PCICC and CCF using a TKE V3.0

This chapter provides an overview of the management and operations of the new Trusted Key Entry (TKE) workstation (TKE V3.0).

5.1 Introduction to the new TKE workstation

With the introduction of the PCICC card for 9672 G5/G6 processors, the TKE workstation has been enhanced to allow remote administration of the PCI card(s). It also continues to support the standard Cryptographic Coprocessor Feature.

Security and secrecy are provided by encrypted and signed transactions between the TKE and the remote Crypto coprocessors. Diffie-Hellman generated keys are used to protect the key parts transported between the TKE and the S/390 host cryptographic coprocessors, and requests and responses flowing over the network are authenticated using public key cryptography.

The graphical interface has also been revisited, so users should find the module management panels and menus of the TKE V3.0 application friendlier to use. More details can be found in the *TKE Workstation User's Guide 2000*, GA22-7430.

5.1.1 Major changes

Following are brief descriptions of the major changes to this workstation.

- The cryptographic functions in the TKE V3.0 are performed by an IBM 4758 model 002 cryptographic coprocessor installed in the workstation (the TKE V2.x uses a 4755 cryptographic adapter).
- The TKE V3.0 can manage both PCICCS and CCFs. (The TKE V2.x supports only the CCF modules, and there is no upgrade path between TKE V2 and TKE V3.)

  Figure 58 on page 90 illustrates the compatibility between the TKE versions and models of the 9672 Enterprise Server.

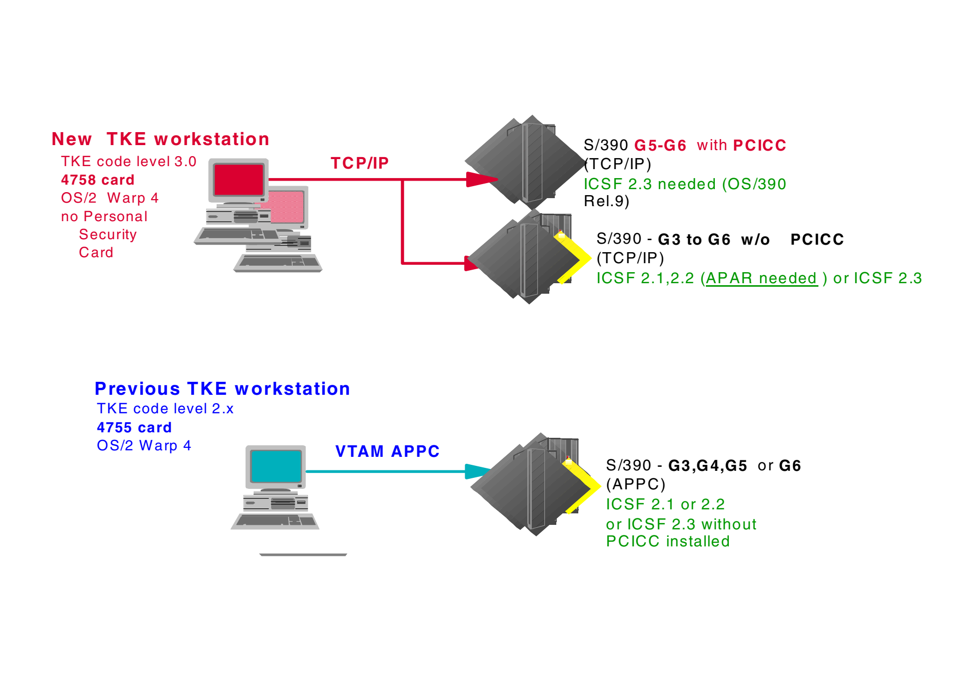


Figure 58. TKE workstation configuration according to CMOS models

4. The TKE workstation V3.0 communicates with the host system using the TCP/IP network, via a token ring or ethernet adapter card, as shown in Figure 59 on page 91. The TKE OS/390 host has started, on top of TCP/IP and ICSF, a TKE Host Transaction Program which listens over a dedicated TCP/IP port and serves the requests issued by the connected TKE(s).

   Refer to Appendix C, “TKE host TCP/IP server setup” on page 145 for further information on how to start the TKE Host Transaction Program.

   Note: The TKE option feature must be ordered with the CCF enablement feature code as there is no PCICC FCV enablement feature code that includes the TKE support.

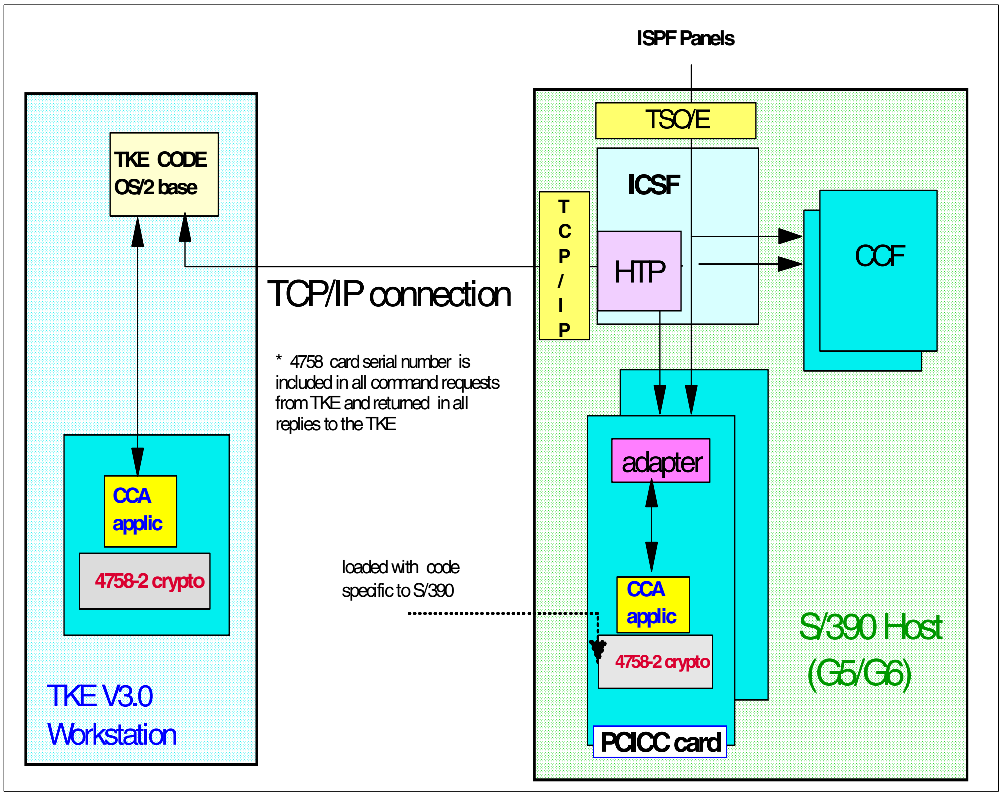


Figure 59. TKE workstation and host system

5.1.2 Before using the new TKE

Some initialization and configuration steps must be performed before using the new TKE workstation. These are described in detail in the *TKE Workstation User's Guide 2000*, GA22-7430, Appendix A.

Some preliminary setups are also required:

1. The customer security policy should be defined and roles assigned: the TKE security officer; the TKE Master Key officer(s); the TKE user(s); the Host Crypto modules security officer(s); the Host Master Keys officer(s) and so on.
2. The logical partitions' cryptographic coprocessor definitions should be done and the proper LPARs should be activated.
3. The TKE OS/390 host should have TCP/IP, ICSF, and the TKE Host Transaction Program properly configured and started. Refer to 5.3, "TKE application: managing host Crypto coprocessors", on page 104 for more information.

5.1.3 The TKE V3.0 software

Software installed on TKE V3.0 includes the following:

- OS/2 Warp 4.0
- IBM4758 PCI cryptographic coprocessor CCA support program 2.20 for OS/2. This code is loaded in the 4758 card at the TKE workstation manufacturing location. This code controls the secure cryptographic functions performed inside the 4758 secure hardware. The code integrity and security is protected

by the IBM private key signature when loaded into the card. Any further reload or update of this code will be integrity-guaranteed by the same mechanism.

- Trusted Key Entry Version 3.0 (versus 2.x)
- Java runtime environment 1.1.8

5.1.4 TKE workstation installation generalities

During the manufacturing process, the TKE workstation application is loaded in the PC (currently, an IBM 6862l) hard disk. TKE IBM4758 mod 002 card internal CCA code segments 1, 2, 3, and FCV are also loaded in the cryptographic card.

The TKE is then tested. Just before shipment, the cryptographic coprocessor card IBM 4758 is removed from the workstation and shipped in a special thermal-protected container. When received at the customer location, it is re-plugged in the TKE workstation by an IBM representative.

Note: When manipulating the 4758 card, *never remove the batteries*; otherwise, the tamper protection mechanism will definitively disable the card.

The following are shipped along with the workstation: a CD-ROM containing the TKE code; a TKE backup diskette; a TKE binary diskette; the *TKE Workstation User's Guide 2000*, GA22-7430.The TKE workstation application can be reloaded from the TKE CD-ROM and the previously saved backup diskette.

If, for any reason, the IBM 4758 Crypto card has to be replaced, then the internal CCA code segments 1, 2, and 3 have to be reloaded because new spare 4758 cards only have the minimum code bootstrap loaded at the card manufacturing plant. It will also be necessary to reload the FCV. You can accomplish this using the procedure described in the document *Workstation Maintenance***,** GC38-3115**,** to load the code files that are kept on the workstation hard disk.

5.1.5 TKE definitions

In this section we explain TKE terminology.

5.1.5.1 TKE workstation access control

The TKE 4758 cryptographic card access control mechanisms use the *roles and profiles* concept. When necessary, these roles and profiles are defined using the Crypto Node Management (CNM**)** software facility. This is done under the control of a TKE administrator and according to customer security policy. This facility, included in TKE code, is started from an OS\2 window session as shown in Figure 65 on page 99.

ROLE

A *role* defines a class of TKE users. When creating or changing a role, the TKE administrator will define the TKE 4758 Crypto card commands that will be authorized for users mapped to this role. There are 128 commands available, also called “control access points”, which can be authorized or unauthorized to the role being created. See the IBM4758 CCA code support documentation for details on the control access points.

Predefined roles are set up during TKE initialization, and there is no need to change these roles for normal use of the TKE application, as shown in Figure 64 on page 98.

PROFILE

A *profile* defines a specific user. It contains a user name and a logon passphrase and is mapped to one role, and only one role. However, as many profiles as needed can be created and mapped to the same role. After logging on under his/her profile, the TKE user will be able to perform only the commands authorized by the role mapped to the profile. Validity dates may also be defined on a role basis to enforce specific security policies.

Default profiles are set up during TKE initialization and have a default known passphrase. We therefore recommend that you change this passphrase after TKE setup to insure full access security.

The TKE administrator will have to create all user profiles required by the security policy in effect; see Figure 67 on page 101.

Caution

The PCICC cards and CCF chips in the host system use a very similar access control concept. They also use roles and authorities. However, these roles and authorities apply to the S/390 coprocessors and must not be confused with the TKE 4758 roles and profiles.

To summarize:

- The TKE workstation has its own ROLES and USERS PROFILES.
- The PCICC modules have their own ROLES and AUTHORITIES.
- The CCF modules have their own AUTHORITIES.

TKE Master Key

The TKE IBM4758 card contains one Master Key (referred to as the “DES Master Key”) to encrypt the TKE operational DES keys, and one Master Key (referred to as the “PKA Master Key”) to encrypt the PKA keys. The CNM utility is used to set these two Master Keys.

You enter the DES Master Key in several key parts loaded by different key officers (generally two officers) through the CNM utility. The entered key parts can be imported from a file, or manually keyed, or randomly generated.

Once the last Master Key part is loaded, the officer sets the Master Key via the CNM utility, which causes both the DES Master Key and the PKA Master Key to be set from these key part values in the TKE 4758. Then the officer uses CNM to encipher or re-encipher the key storages.

TKE workstation key storages

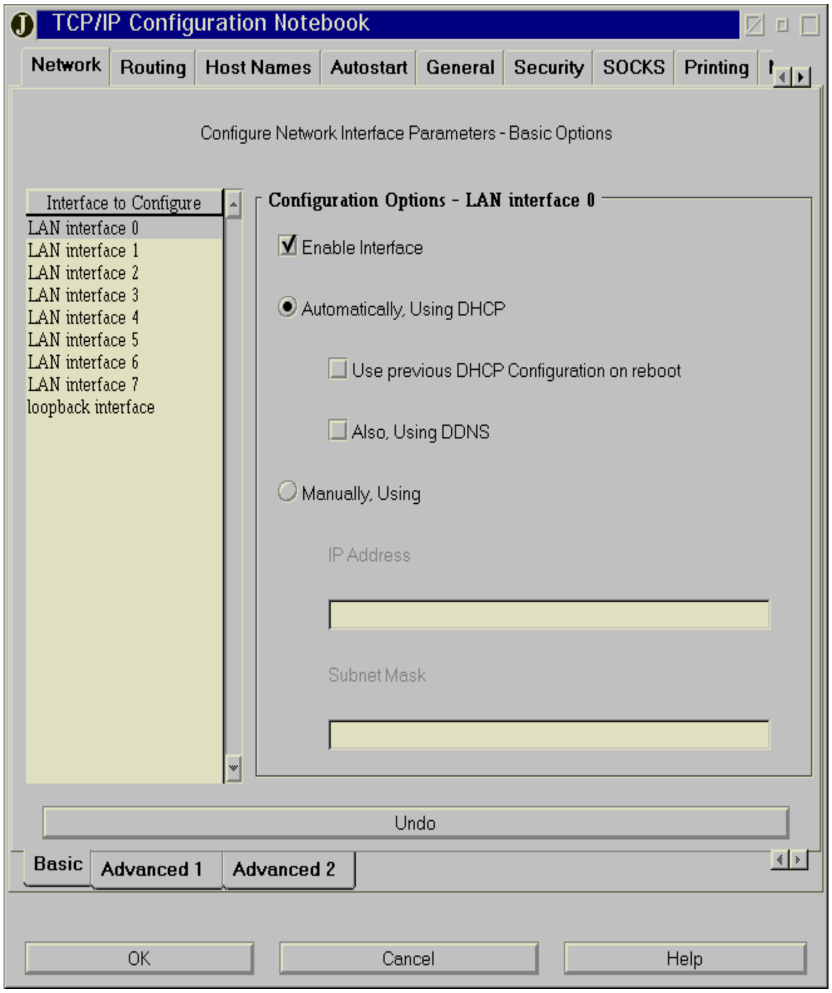
The TKE workstation key storages are files on hard disk where the operational keys encrypted under the TKE IBM 4758 Master Key are stored. When these keys need to be used, they are loaded into the 4758 secure hardware, so that they never appear in clear outside of the TKE 4758 secure hardware.

There are two key storages implemented in the TKE:

- DES key storage to store symmetric keys (C:\ibm4758\DESSTORE.DAT)
- PKA key storage to store asymmetric keys (C:\ibm4758\PKASTORE.DAT)

5.2 TKE workstation TCP/IP setup

The TKE administrator must configure the workstation for access via a TCP/IP network. To start this configuration, from the TKE OS/2 desktop double-click the TCP/IP icon to open the Configuration Notebook, as shown in Figure 60.


TCP/IP Configuration Notebook

Configure Network Interface Parameters - Basic Options

Interface to Configure
LAN interface 0
LAN interface 1
LAN interface 2
LAN interface 3
LAN interface 4
LAN interface 5
LAN interface 6
LAN interface 7
loopback interface

Configuration Options - LAN interface 0

☑ Enable Interface

● Automatically, Using DHCP

□ Use previous DHCP Configuration on reboot

□ Also, Using DDNS

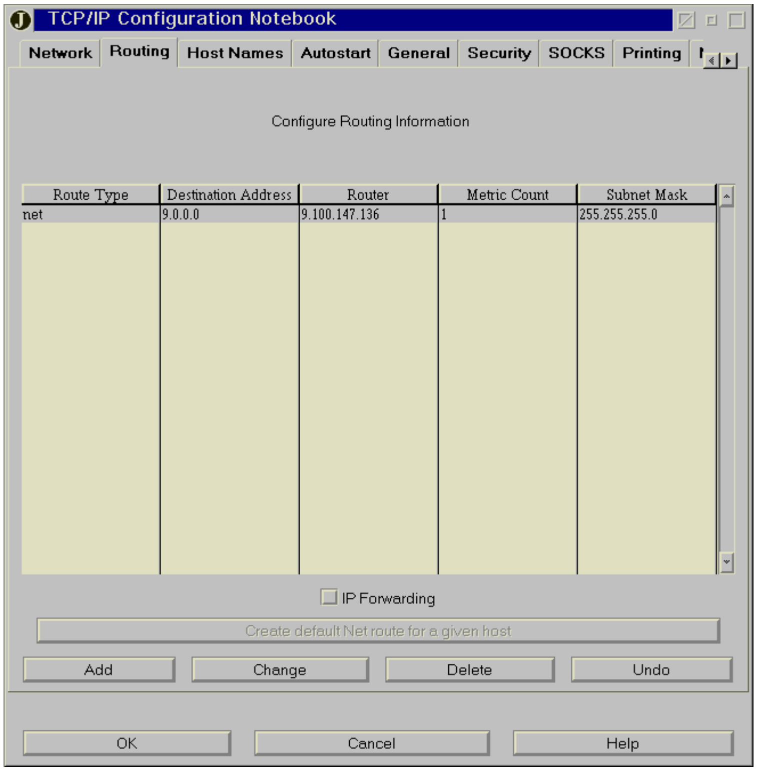
○ Manually, Using

IP Address

Subnet Mask

Figure 60. TCP/IP configuration notebook

- Fill the basic options page of the Network tab for at least one adapter, typically LAN interface 0.
- In our example, the option Automatically using DHCP was used. This setup is dependent on the specific network implementation and has to be performed with the assistance of the customer network support personnel.
- Read the Configure Routing Information online help to determine if any special situations apply to the computer you are configuring. If so, you may need to complete the field on the Routing tab (however, this was not needed in the case of our DHCP network); refer to Figure 61 on page 95.



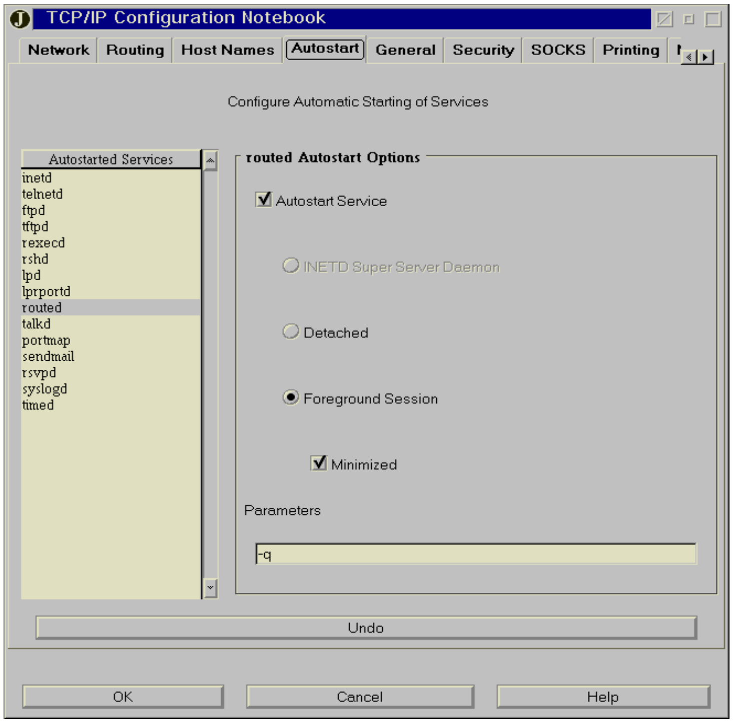
Configure Routing Information

Route Type	Destination Address	Router	Metric Count	Subnet Mask
net	9.0.0.0	9.100.147.136	1	255.255.255.0

□ IP Forwarding

Figure 61. TCP/IP routing tab

- Then go to the Autostart tab in the Configure Automatic Starting of Services page. Select **routed** from the Autostarted Services list, check the **Autostart Service** box, and then press **OK**. We started the routed daemon in our configuration. This is shown in Figure 62 on page 96.



Configure Automatic Starting of Services

Autostarted Services:
inetd
telnetd
ftpd
tftpd
rexecd
rshd
lpd
lprportd
routed
talkd
portmap
sendmail
rsvpd
syslogd
timed

routed Autostart Options

☑ Autostart Service

○ INETD Super Server Daemon

○ Detached

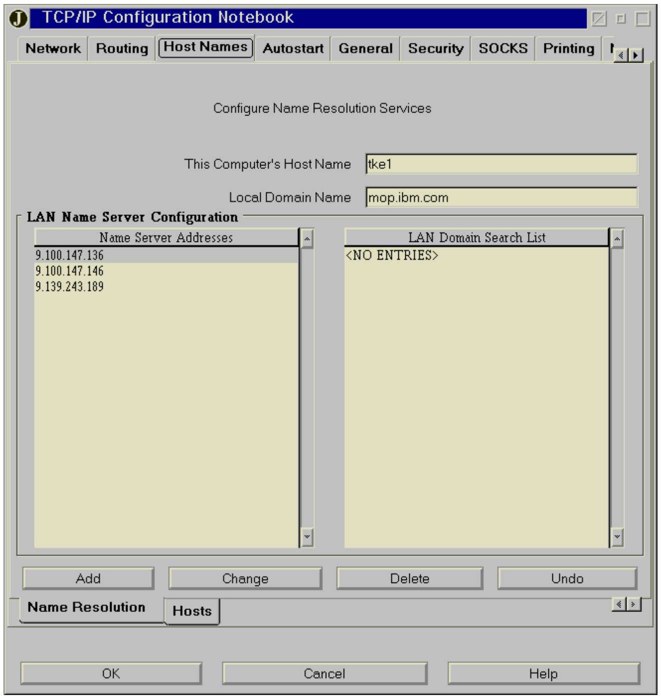
● Foreground Session

☑ Minimized

Parameters: -q

Figure 62. Autostart tab

- On the Configure Name Resolution Services pages, select the **Host Names** tab and provide the host name, local domain, and name service addresses as shown in Figure 63. (This is not needed with a DHCP network.)



Configure Name Resolution Services

This Computer's Host Name: tke1

Local Domain Name: mop.ibm.com

LAN Name Server Configuration

Name Server Addresses:
9.100.147.136
9.100.147.146
9.139.243.189

LAN Domain Search List:
<NO ENTRIES>

Figure 63. Host Names tab

5.2.1 OS/390 TCP/IP Host Transaction Program

The setup of the Host Transaction Program is explained in Appendix C, “TKE host TCP/IP server setup” on page 145.

5.2.2 TKE workstation 4758 setup

TKE workstation initialization has to be done only when installing a new TKE or after a TKE misuse, when there is no TKE role or profile available to manage the TKE and no backup diskettes available. Normal restore of a failing TKE must be done using the CD-ROM and the backup diskettes.

> **Caution**
>
> If the workstation you are working on is already in use, and if some keys are already stored in key storages, then *ensure that you have a backup copy of both key storage files and the TKE 4758 card Master Keys parts*. Otherwise, you will not be able to recover the keys in the key storages; see 5.3.6, “Backing up the TKE files”, on page 134 for more information.

5.2.2.1 TKE workstation initialization

This step is performed at the manufacturing location before the TKE is shipped and does not have to be done again when you receive the TKE. However, it can be re-executed without any problem. The description of the actual TKE customer.setup begins at 5.2.2.2, “TKE access control administration”, on page 98.

To start TKE workstation initialization, enter the following from the OS/2 window:

```
c:\ibm4758\cnm\ csuecni c:\tke\4758access\4758initialize.cni
```

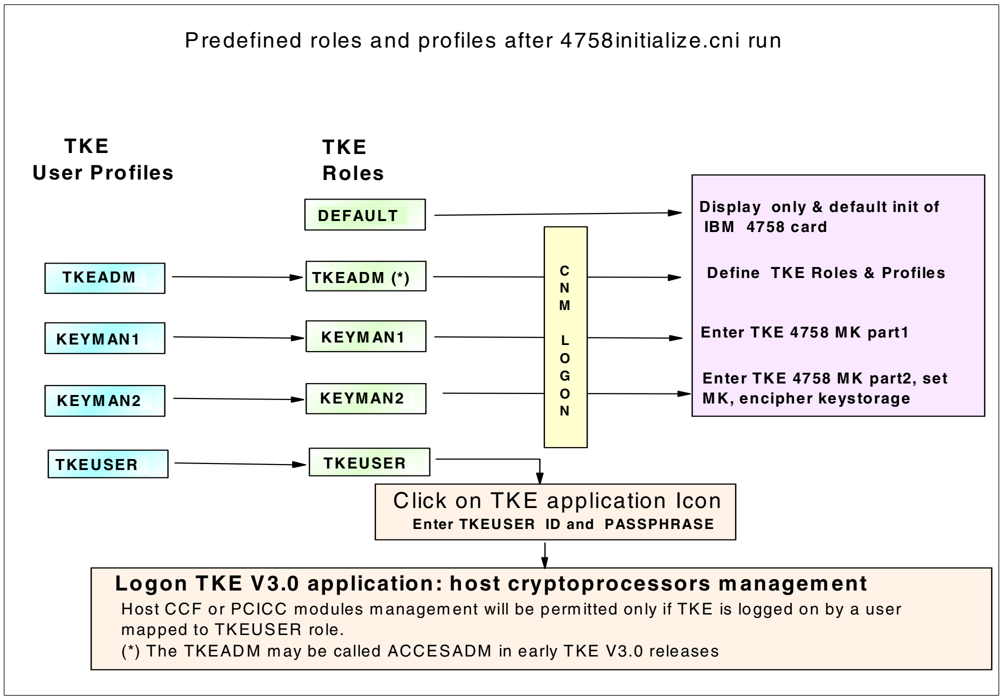
This CSUECNI command runs the batch file 4758initialize.cni, which will perform the following steps:

1. It sets the 4758 clock.
2. It creates five TKE default roles (shown in Figure 64 on page 98).
   - The DEFAULT role allows you to view roles and profiles, and to re-initialize the 4758. This is a public access, and no passphrase is needed (you simply press cancel when prompted for profile name and passphrase).
   - The TKEADM role is the default administrator role, allowing the user to perform security administration for the TKE workstation and to create, change, or delete TKE roles and profiles.

     Note: The TKEADM role may have been called the ACCESADM role in early TKE V3.0 code releases.
   - The KEYMAN1 role allows you to clear the TKE 4758 new Master Key reg and to load the first Master Key part.
   - The KEYMAN2 role allows you to load the middle and last Master Key parts, to set the Master Key, and to re-encipher the TKE key storage.
   - The TKEUSER role allows you to communicate with the host Crypto modules, and to manage them. This role is also used by the 4753 migration facility (see 5.4, “4753 Key Token Migration facility”, on page 135 for more information about this facility). This is the TKE general user role.

3. It creates four TKE default profiles, as shown in Figure 64 on page 98:
   - The TKEADM profile is mapped to the TKEADM role, with the passphrase TKEADM.

     Note: The TKEADM role may have been called the ACCESADM role in early TKE V3.0 code releases.
   - The KEYMAN1 profile is mapped to the KEYMAN1 role, with the passphrase KEYMAN1.
   - The KEYMAN2 profile is mapped to the KEYMAN2 role, with the passphrase KEYMAN2.
   - The TKEUSER profile is mapped to the TKEUSER role, with the passphrase TKEUSER.
4. It loads and sets a TKE IBM 4758 random DES Master Key.
5. It initializes TKE DES key storage and TKE PKA key storage.


Predefined roles and profiles after 4758initialize.cni run
TKE User Profiles
TKE Roles
DEFAULT
TKEADM
TKEADM (*)
KEYMAN1
KEYMAN1
KEYMAN2
KEYMAN2
TKEUSER
TKEUSER
CNM LOGON
Display only & default init of IBM 4758 card
Define TKE Roles & Profiles
Enter TKE 4758 MK part1
Enter TKE 4758 MK part2, set MK, encipher keystorage
Click on TKE application Icon
Enter TKEUSER ID and PASSPHRASE
Logon TKE V3.0 application: host cryptoprocessors management

Host CCF or PCICC modules management will be permitted only if TKE is logged on by a user mapped to TKEUSER role.

(*) The TKEADM may be called ACCESADM in early TKE V3.0 releases

Figure 64. TKE workstation predefined roles and profiles

5.2.2.2 TKE access control administration

This step is used to change the TKE user profiles default passphrases and replace the IBM4758 Master Key which was randomly generated during the TKE initialization process, as no backup is available to recover this key. These tasks are executed using the Cryptographic Node Management (CNM) utility.

The CNM utility is a basic application delivered with the IBM 4758 cryptographic coprocessor. Only a subset of the CNM functions is required to customize the TKE and to manage the workstation application.

Note: We strongly recommend that you *do not use other CNM functions*, as this can lead to unpredictable results. In particular the CNM Initialize function must not be confused with the TKE initialization previously described. Refer to the IBM 4758 PCI Cryptographic Coprocessor CCA Support Program installation manual for additional details on CNM.

To start the CNM utility, enter the following command from an OS/2 window:

```
C:\ibm4758\cnm\CSUECNM
```

The panel shown in Figure 65 will be displayed. When the CNM utility is started, only the DEFAULT role commands are permitted. As previously mentioned, the DEFAULT role allows you to only display roles and profiles and to initialize the 4758.

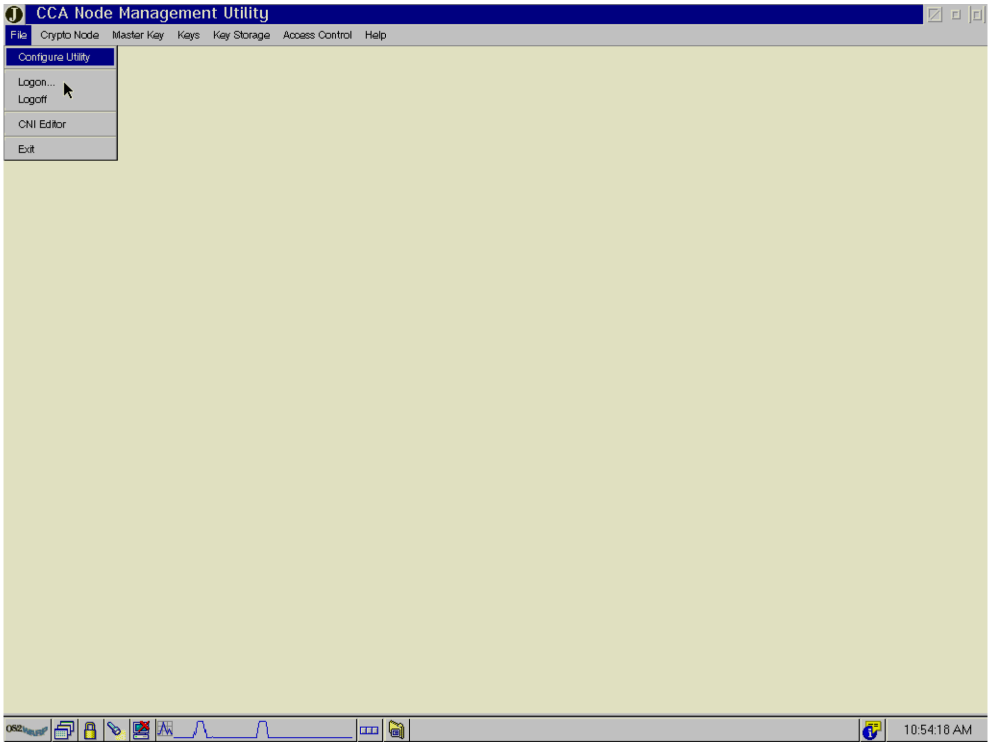
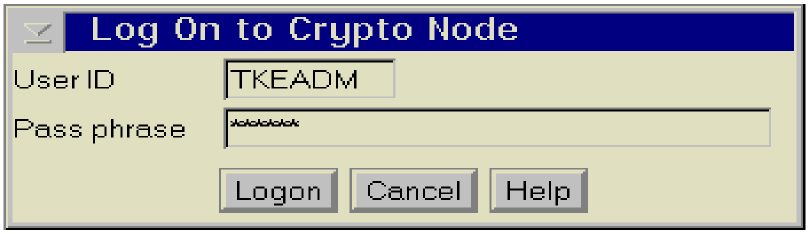


Figure 65. TKE workstation CNM utility panel

CNM TKE administrator logon

From the File pull-down menu on the CNM panel, select **logon**. Enter the user ID `TKEADM` and the pass phrase `TKEADM` (these are the default values set at TKE initialization), as shown in Figure 66. Note that the user ID and pass phrase are case sensitive.



Log On to Crypto Node

User ID: TKEADM

Pass phrase: ******

Figure 66. CNM utility logon as default TKEADM user with default passphrase

Once logged on, the TKE administrator needs to change the pass phrase and may also change the activation and expiration dates for the TKEADM profile. For detailed information on how to edit profiles, refer to the IBM 4758 PCI Crypto Coprocessor CCA Support Program manual.

At this time the administrator should also change the default passphrases in the other predefined profiles and, if needed, create new user profiles mapped to the predefined roles.

To create or change profiles**,** select **profiles** in the access control pull-down menu and then press **New** (to create a new user profile) or press **edit** (to modify a selected existing profile). The administrator must fill in the panel with the information on the new user and the pass phrase (the pass phrase may be typed in by the user). The administrator will also need to define which role is attributed to this user. An example is shown in Figure 67 on page 101.

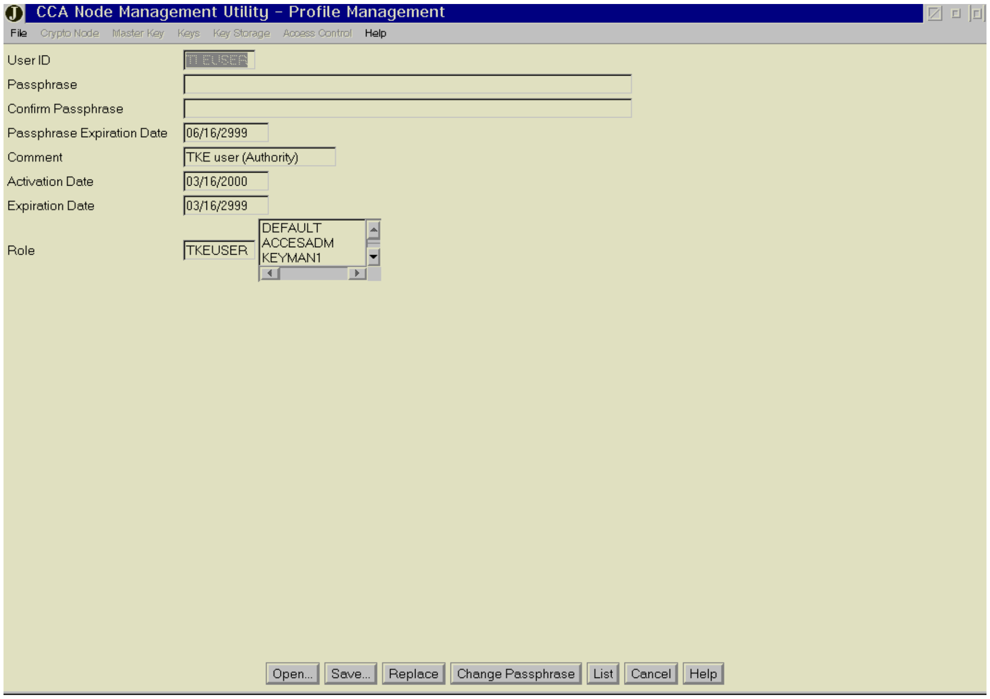
It is expected that most of the new user profiles will be mapped to the predefined TKEUSER role, as this is the only predefined role permitted for communication with the host Crypto modules.

In our example we decided to keep the default TKEUSER user ID and pass phrase. This, of course, may change according to the customer security policy at your site.

Important

The administrator role TKEADM is a critical asset for TKE workstation security, as it allows you to create other roles and profiles, with any permission, to all the functions of the IBM 4758 card in the TKE. Note that the TKEADM role may have been called ACCESADM role in early TKE V3.0 releases.

Therefore the default pass phrase of the TKEADM profile *must be changed and kept secret.* This also applies to the KEYMAN1 and KEYMAN2 roles.

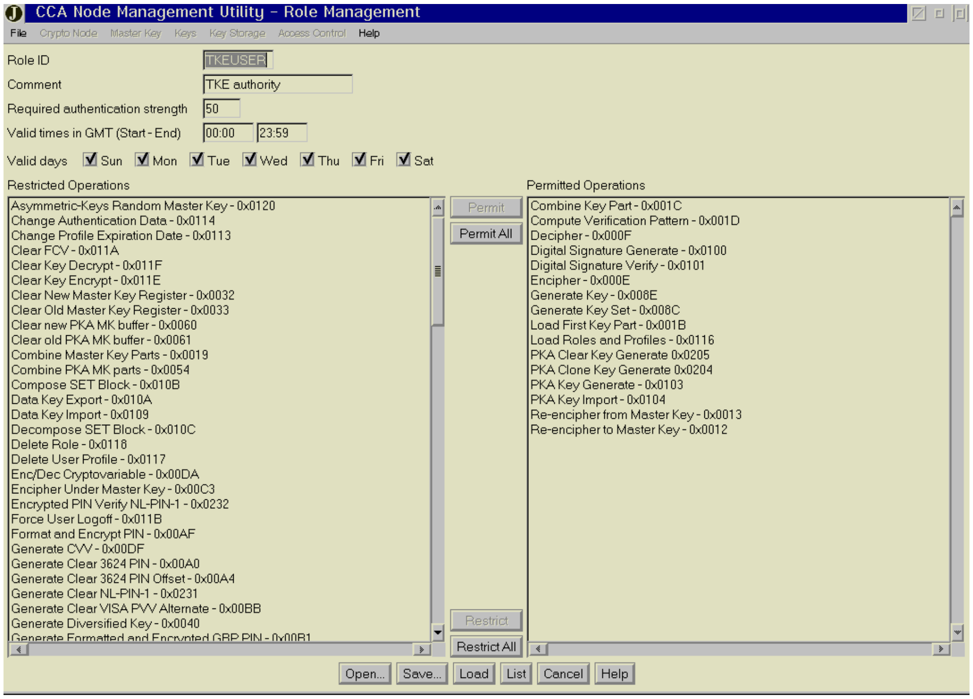


User ID TKEUSER
Passphrase
Confirm Passphrase
Passphrase Expiration Date 06/16/2999
Comment TKE user (Authority)
Activation Date 03/16/2000
Expiration Date 03/16/2999
Role TKEUSER
DEFAULT
ACCESADM
KEYMAN1

Figure 67. TKE workstation profile example: TKEUSER default profile

To create or change roles, select **roles** in the access control pull-down menu and then press **New (**to create a role) or press **edit** (to change a selected existing role). An example is shown in Figure 68 on page 102.

As explained in 5.1.5, “TKE definitions”, on page 92, there is normally no need to change or create roles for the TKE workstation IBM 4758 card since the required functions are already permitted in the pre-defined roles. However, you can use this as an opportunity to change the validity days specification.



Role ID TKEUSER

Comment TKE authority

Required authentication strength 50

Valid times in GMT (Start - End) 00:00 23:59

Valid days ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Restricted Operations

```
Asymmetric-Keys Random Master Key - 0x0120
Change Authentication Data - 0x0114
Change Profile Expiration Date - 0x0113
Clear FCV - 0x011A
Clear Key Decrypt - 0x011F
Clear Key Encrypt - 0x011E
Clear New Master Key Register - 0x0032
Clear Old Master Key Register - 0x0033
Clear new PKA MK buffer - 0x0060
Clear old PKA MK buffer - 0x0061
Combine Master Key Parts - 0x0019
Combine PKA MK parts - 0x0054
Compose SET Block - 0x010B
Data Key Export - 0x010A
Data Key Import - 0x0109
Decompose SET Block - 0x010C
Delete Role - 0x0118
Delete User Profile - 0x0117
Enc/Dec Cryptovariable - 0x00DA
Encipher Under Master Key - 0x00C3
Encrypted PIN Verify NL-PIN-1 - 0x0232
Force User Logoff - 0x011B
Format and Encrypt PIN - 0x00AF
Generate CVV - 0x00DF
Generate Clear 3624 PIN - 0x00A0
Generate Clear 3624 PIN Offset - 0x00A4
Generate Clear NL-PIN-1 - 0x0231
Generate Clear VISA PVV Alternate - 0x00BB
Generate Diversified Key - 0x0040
Generate Formatted and Encrypted GBP PIN - 0x00B1
```

Permitted Operations

```
Combine Key Part - 0x001C
Compute Verification Pattern - 0x001D
Decipher - 0x000F
Digital Signature Generate - 0x0100
Digital Signature Verify - 0x0101
Encipher - 0x000E
Generate Key - 0x008E
Generate Key Set - 0x008C
Load First Key Part - 0x001B
Load Roles and Profiles - 0x0116
PKA Clear Key Generate 0x0205
PKA Clone Key Generate 0x0204
PKA Key Generate - 0x0103
PKA Key Import - 0x0104
Re-encipher from Master Key - 0x0013
Re-encipher to Master Key - 0x0012
```

Figure 68. TKE workstation role example: TKEUSER default role

In Figure 69, the left column of the role panel shows the unauthorized operations and the right column shows the operations permitted to the role. You can move operations from one column to the other, as per the specific requirements of your site. Valid days in the week can be also selected.

When the creation or modification of roles, profiles, and passphrases is complete, the TKEADM user ID logs off from the Crypto node using the file dropdown menu logoff option.

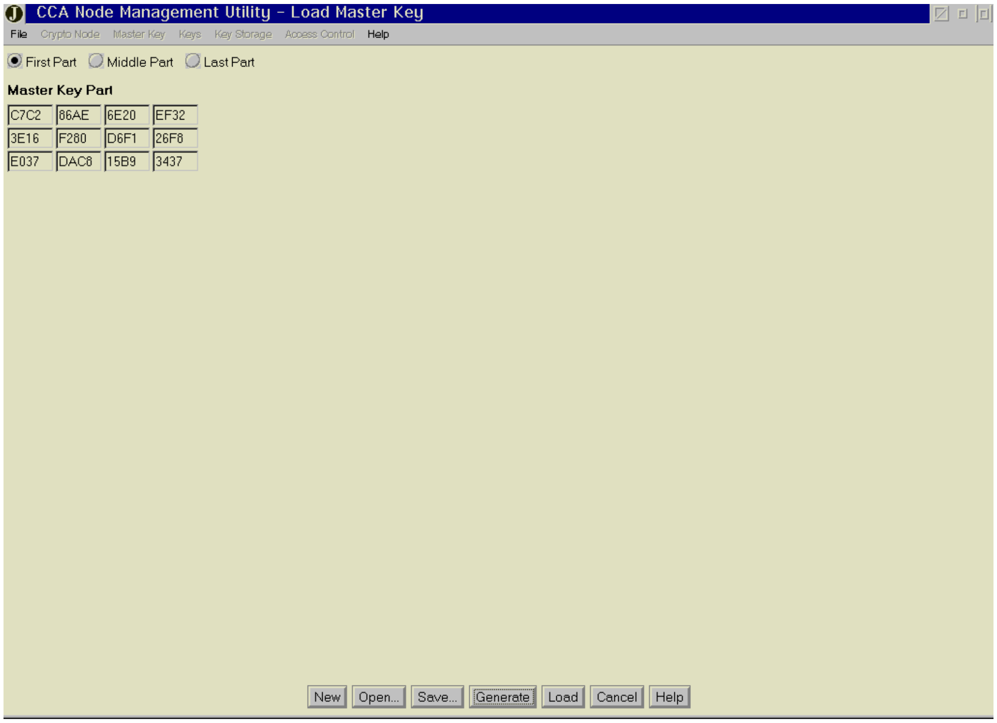
Loading the first part of the TKE Master Key

During TKE initialization, the TKE IBM 4758 DES Master Key is loaded using randomly generated key parts. We strongly recommend, for recovery purposes, that you change this Master Key with your own backed-up key parts. This is done by using KEYMAN1 for the first key part and KEYMAN2 for the middle and last key parts, as follows:

1. Logon to the CNM utility as KEYMAN1.
2. From the Master Key pull-down menu, select **Parts** and then **first key part**. Manually enter the 24 bytes of the first key part, or else select **generate random** key part. Then select **Load**.

   Note: Ensure that you *save* the key part for backup purposes; refer to Figure 69 and Figure 70 on page 103 for illustrations.
3. KEYMAN1 must then logoff from CNM.

The 4758 new Master Key register must be empty before you begin this task. To clear the new Master Key register, select **clear new register** from the Master Key dropdown menu.

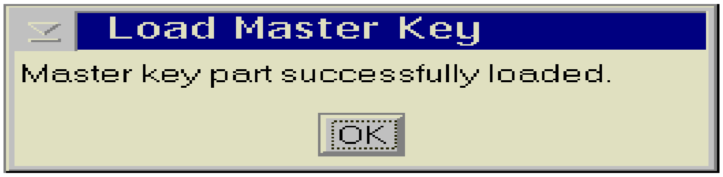


● First Part ○ Middle Part ○ Last Part

Master Key Part

C7C2	86AE	6E20	EF32
3E16	F280	D6F1	26F8
E037	DAC8	15B9	3437

Figure 69. TKE workstation MK - first part generate and load



Master key part successfully loaded.

Figure 70. TKE MK - first part successfully loaded

Loading the last key part of the TKE Master Key

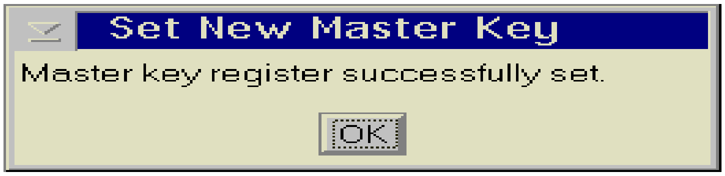
To load the last key part of the TKE Master Key, do the following:

1. Logon to the CNM utility as KEYMAN2.
2. From the Master Key pull-down menu select **parts,** and then **enter and load a middle key part** (optional) and the **last key part.** Perform a save for each one of them.

Setting the Master Key and ENCIPHER DES and PKA key storage

To set this key and storages, do the following:

1. Stay logged on as KEYMAN2.
2. From the Master Key pull-down menu, select **SET** to set the IBM 4758 Master Key. A successful completion message must be displayed, as shown in Figure 71 on page 104.



Master key register successfully set.

Figure 71. Set TKE workstation Master Key successful panel

KEYMAN2 now has to reencipher the DES and PKA key storages. To proceed, do the following:

1. From the key storage pull-down menu, select **DES storage**, **Manage**, then press REENCIPHER.
2. Repeat the operation for PKA storage.

At completion, KEYMAN2 must logoff from the Crypto node and then close the CNM utility.

Blind key entry option

This option will mask the key parts as they are entered at TKE when working with the host system Crypto modules. If it is required by the security policy, you will have to edit C:\tke\tke\TKE.INI from an OS/2 window, and then add the following statement, if not already existing:

```
'BLIND_KEY_ENTRY=TRUE'
```

Then close the OS/2 window.

5.2.3 Starting the TKE application

TKE initialization and setup is now complete. You can start the application by opening the TKE folder and double-clicking on the TKE V3.0 icon.

5.3 TKE application: managing host Crypto coprocessors

At this point it is assumed that the TKE initialization and setup have been performed, and that TCP/IP, ICSF, and the Host Transaction program have been started in the TKE OS/390 host system.

The definition of the S/390 coprocessors and their handling at the TKE will be done according to the customer policy. Therefore it is assumed that as a preamble to this chapter the user has already defined which users are authorized to: change the Crypto modules setup; change the domain Master Keys; zeroize a domain; enable or disable a module; and so on.

5.3.1 Managing modules

When a new PCICC card is added, it must be configured in the TKE application. A PCICC card or CCF module can be managed at the TKE as a single PCICC or CCF coprocessor, or can be included in a PCICC or CCF coprocessor group.

Managing the coprocessors as a group provides easier management when dealing with several coprocessors in the installation. Group management introduces the concept of the “master” Crypto coprocessor in the group, which is a single coprocessor that will be representative of the status of all the other coprocessors in the group.

Because it is important that *all Crypto modules in the group are in the same state* (that is, they have the same definition of signature requirements for CCF, or roles/authorities for PCICC cards), we recommend that you continue to control at the group level once this has been initiated.

If it happens that a command issued to a group is performed only by some modules in the group, then the TKE application adds two new group definitions: one group contains the Crypto coprocessors where the command has been properly executed, and one group contains the coprocessors which have not properly executed the command. These two new groups can be used to manually resolve the differences in the module states and synchronize them again. Once this is done, these groups can be deleted.

Before adding a new module in an already existing group, the administrator and/or different authorities will have to customize the new Crypto module as a single entity; then, when the status of the coprocessor is identical to the group’s master coprocessor, it can be added to the group.

The decision to work either with single coprocessors or with groups of coprocessors should be made at the installation level.

5.3.1.1 Required levels of authorization

Working with the S/390 Crypto coprocessors requires the following three levels of authorization (this is illustrated in Figure 72 on page 106):

1. All commands initiated on the TKE workstation that imply communication with host Crypto coprocessors will have to be performed with the TKE application logged on using a user profile mapped to the TKEUSER role (or to a role with equivalent permissions). This is controlled by ROLES and PROFILES defined at the TKE level by the TKE administrator.
2. Access to the host system cryptographic facilities is requested by using a TSO user ID and password known from the host system.
3. The TKE authority sending the command to a specific host Crypto coprocessor must be authorized to perform and sign this command. This is defined at the host system Crypto coprocessors for each authority index by the authority administrator.

   A just-installed PCICC card has a pre-set default authority mapped to a default role (INITADM). This authority will be used until new roles and authorities have been defined for PCICC administration.

   An *authority* is identified by its index and has its own signature key pair. Authority 00 is the pre-set default authority for the PCICC. At the TKE the authority 00 default signature key must be loaded (from the TKE main panel functions pull-down menu) so that commands can be accepted by a newly installed (or zeroized) PCICC.

   This initial default authority 00 is mapped to a predefined INITADM role in the PCICC, which is authorized to create new roles and authorities in the PCICC card.

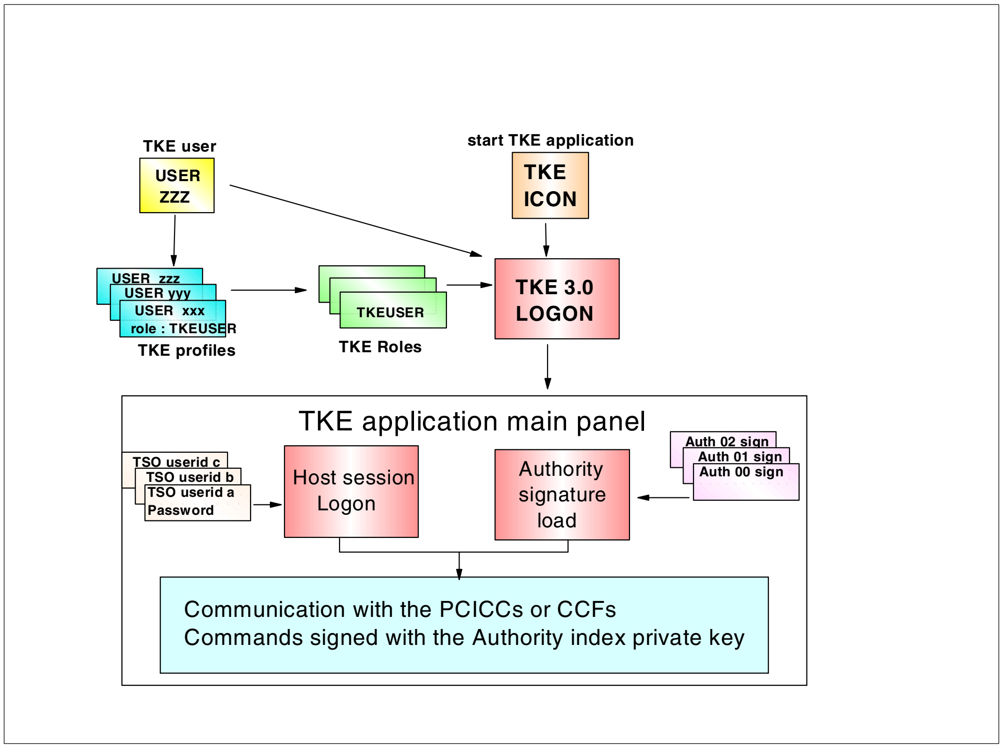


Figure 72. Host Crypto module access logon sequence from TKE

Authority signature key indicator

An informational message indicating `authority signature key loaded` or `not loaded` is displayed at the low right-hand corner of the TKE window. This indicates whether the TKE can sign commands sent to host coprocessors. Only one signature key can be loaded at a time. It can be changed only from the TKE main panel, and the signature key source can be a binary file, the key storage, or the default signature key.

If no signature key is loaded and if an authority attempts to send a command to any host Crypto module, a pop-up msg will appear, requiring a signature key source to be entered.

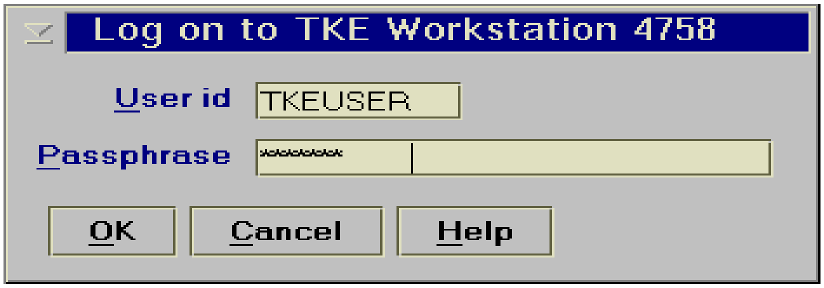
Note, however, that if a signature key is already loaded, there is no information about its owner. This signature key will be used to sign any further command. Hence, before sending commands, be sure that *the loaded signature key is the one you intended*. If in doubt, the safest action is to return to TKE entry main panel and then load your signature key again.

5.3.2 PCICC and CCF setup on the TKE workstation

The following sections provide details on how to perform these setups.

5.3.2.1 TKE logon

The TKE must be logged on using a profile mapped to the TKEUSER role. If the TKE application is already active, close the application and restart it by clicking the **Trusted Key Entry** folder and then the **TKE V3.0** icon. Enter the user ID and passphrase (remember, the characters are case sensitive) as shown in Figure 73. As already mentioned, we kept the default TKEUSER profile.



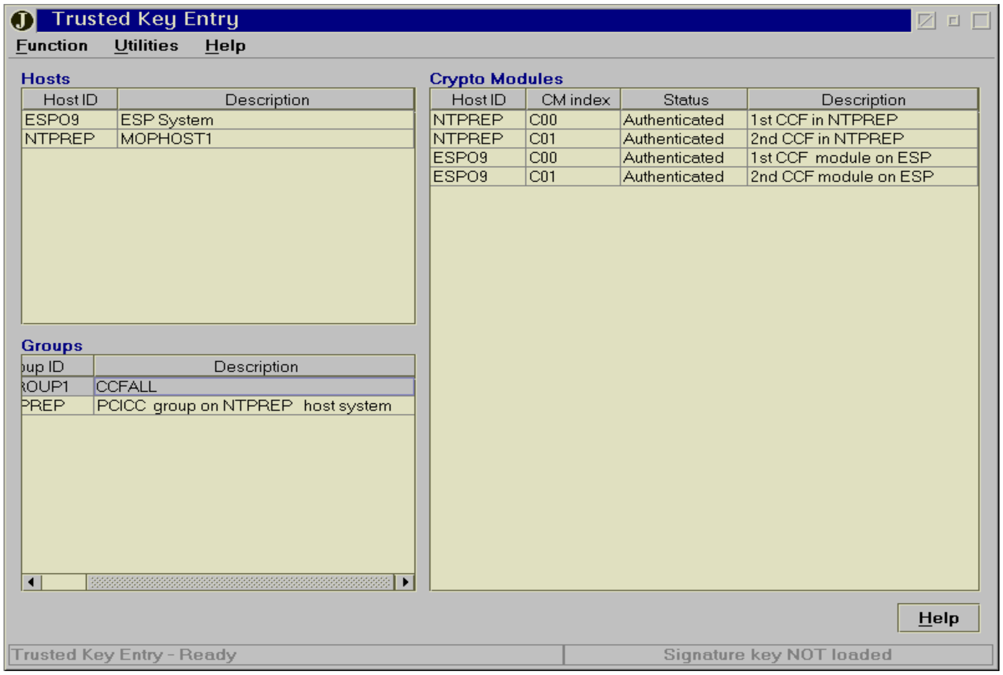
Log on to TKE Workstation 4758

User id: TKEUSER

Passphrase: ********

Figure 73. Trusted Key Entry workstation logon panel

The main TKE panel is displayed. Initially this panel is empty; in Figure 74 we show this panel after we entered our definitions.



Hosts

Host ID	Description
ESPO9	ESP System
NTPREP	MOPHOST1

Groups

up ID	Description
OUP1	CCFALL
PREP	PCICC group on NTPREP host system

Crypto Modules

Host ID	CM index	Status	Description
NTPREP	C00	Authenticated	1st CCF in NTPREP
NTPREP	C01	Authenticated	2nd CCF in NTPREP
ESPO9	C00	Authenticated	1st CCF module on ESP
ESPO9	C01	Authenticated	2nd CCF module on ESP

Trusted Key Entry - Ready

Signature key NOT loaded

Figure 74. TKE V3.0 application main panel

Use this main panel to select a Crypto module or a group of the same type (PCICC or CCF) of Crypto modules. As a prerequisite, you must enter host and group definitions in the empty panes. Notice in Figure 74 that the informational message `Signature key NOT loaded` is displayed in the lower right-hand corner.

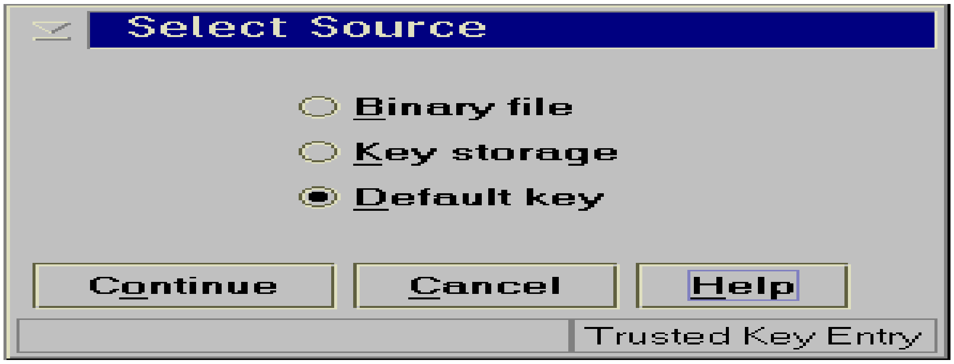
The main panel has three panes labeled: Hosts, Groups, Crypto Modules. These panes are blank until a host is created, modules are authenticated, and groups are defined.

This panel also contains three pull-down menus: Function, Utilities, Help. We explain the Function and Utilities menus in further detail in the next sections.

The Function pull-down menu allows you to:

- Load a signature key by selecting the **Load signature key** in this menu, then selecting the key source, as shown in Figure 75.

  When dealing with a *new* PCICC or CCF coprocessor, you must select the **default signature key** for authority 00, as these are the values pre-set in the coprocessor.



○ Binary file
○ Key storage
● Default key

Figure 75. Load signature key; Source: default signature key

- Define a transport key policy by selecting the **Define transport key policy** option.

  This defines the policy that the user wants to enforce when generating the TKE and host coprocessor transport key by the Diffie Hellman algorithm. A pop-up menu proposes three policy options; refer to the *TKE Workstation User's Guide 2000*, GA22-7430, for further details about these options.

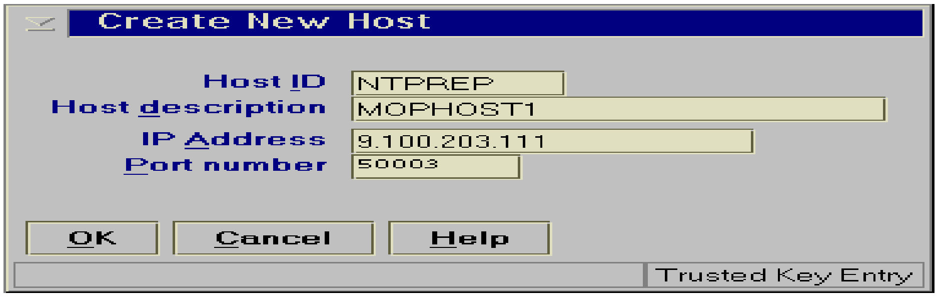
- Exit.

The Utilities pull-down menu allows you to manage TKE key storages; refer to the *TKE Workstation User's Guide 2000* for details.

5.3.2.2 Host system S/390 definition and logon from TKE

In this section we describe how to create a host. Initially, the host container is empty. To create a host, perform the following tasks:

1. Create a host ID by right-clicking in the TKE main panel host pane and selecting **create**.
2. Enter the Host ID, Host description, Host TCP/IP Address, and the Port number used by the Host Transaction Program. Only the TCP/IP address and port must correspond to actual definitions in the OS/390 host, as shown in Figure 76 on page 109.
3. Pressing **OK** creates a line for this host in the host pane.



Create New Host

Host ID NTPREP

Host description MOPHOST1

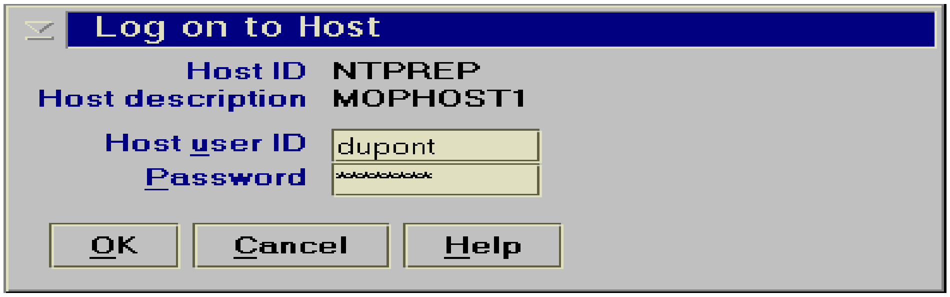
IP Address 9.100.203.111

Port number 50003

Figure 76. Create a new host panel on TKE workstation example: NTPREP

To log on to the host, do the following:

1. Click the target host ID line in the hosts pane. The dialog box shown in Figure 77 appears.
2. Fill in the fields Host user ID and Password with a TSO user ID and password defined in the target host.



Log on to Host

Host ID NTPREP

Host description MOPHOST1

Host user ID dupont

Password ********

Figure 77. Host logon panel on TKE workstation

Because further processing at the OS/390 will be performed under this user ID, we recommend that you consider setting the appropriate RACF profiles as described in 6.1, “RACF access control to ICSF services”, on page 137 and Appendix C, “TKE host TCP/IP server setup” on page 145.

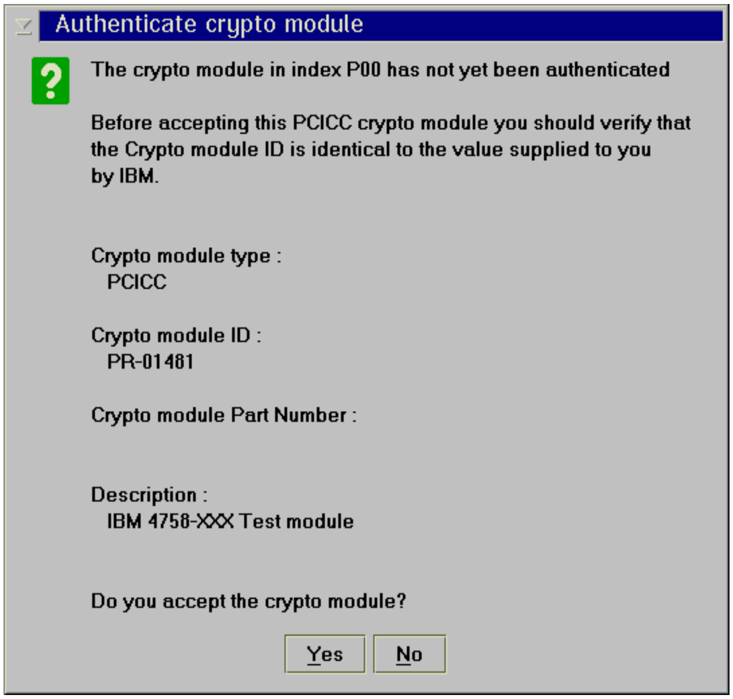
5.3.2.3 Crypto module recognition

The host PCICCs and CCFs are automatically recognized by the TKE at the time it establishes the connection with the host. If you added new PCICCs and the host is already connected, then exit the TKE application, log on using a TKEUSER profile, and then perform a logon to the target host by clicking **select host** on the main TKE panel host pane to take into account any new Crypto coprocessor installed in the machine.

The TKE user is notified of any new Crypto coprocessor discovered in the host and then needs to authenticate this module PCICC CMID. The Crypto Module Identifier (CMID) is a serial number burned into secure hardware during the manufacturing process, and it is used to identify the module or the card as a unique one. The CMID is displayed at the TKE and must be verified with information from PCICC configuration panel on the support element.

After the Crypto module is accepted by the user as the right one, the CMID and Crypto Module Public Modulus (CMPM) are saved in the TKE workstation for the following communications. The module authentication is illustrated in Figure 78.

Note that, contrary to the CCF, the module identification does not include the verification of the CMPM, as these values are provided signed with the IBM private key and verified by the TKE code.



Authenticate crypto module

The crypto module in index P00 has not yet been authenticated

Before accepting this PCICC crypto module you should verify that the Crypto module ID is identical to the value supplied to you by IBM.

Crypto module type :
PCICC

Crypto module ID :
PR-01481

Crypto module Part Number :

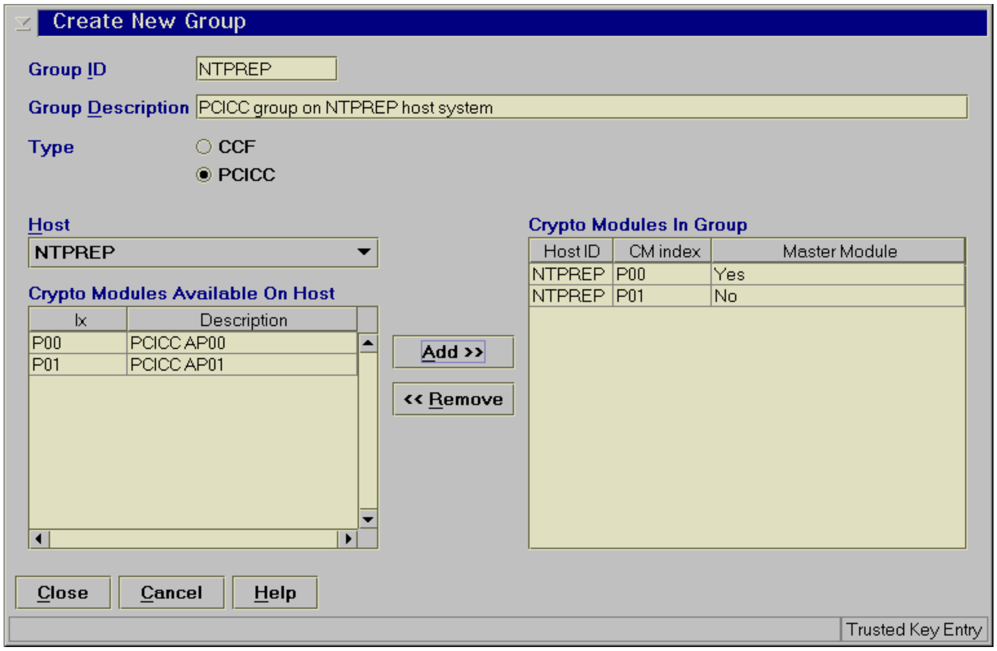
Description :
IBM 4758-XXX Test module

Do you accept the crypto module?

Figure 78. New Crypto module authentication panel

5.3.2.4 Create or change a group

If you have chosen to work with coprocessor groups, you will have to create a new group or change an already existing PCICC group. With the mouse right button, click in the Group pane and select **NEW** or **CHANGE.** Enter (or modify) the group name and group information to specify the module type, select **Host**, and then **Add** (or **Remove**) coprocessors in the group. This is illustrated in Figure 79 on page 111.



Create New Group

Group ID: NTPREP

Group Description: PCICC group on NTPREP host system

Type: ○ CCF ● PCICC

Host: NTPREP

Crypto Modules Available On Host

Ix	Description
P00	PCICC AP00
P01	PCICC AP01

Crypto Modules In Group

Host ID	CM index	Master Module
NTPREP	P00	Yes
NTPREP	P01	No

Figure 79. Create New Group panel

To choose the coprocessors to be part of a group, select a host in the host list. If not connected to the host, you will be requested to log on. Once connected to the host, this host's coprocessors are displayed and they can be added to the group.

A master Crypto module in the group is also defined; by default it is the first module added to the group, but it can also be any one of the group's modules. The master module can be changed by right-clicking on any module in the group container, and then selecting **master** in the pull-down menu. The states of the Crypto processors can be compared within a group by the administrator.

You can compare the Crypto modules in a group in order to ensure they are all in an identical state by highlighting and clicking a specific group in the group pane. When the Crypto module notebook is opened, click **Functions** and select **Compare Group.** The TKE reads and compares information from all modules in the group and displays any mismatch it finds. Based on these results, the user can correct mismatches or change group definitions and contents.

5.3.3 Manage and update the Crypto module notebook on TKE

The Crypto module notebook is opened by clicking a module in the Crypto pane. Figure 81 on page 116 shows the first page of a Crypto module notebook. Further information and controls are accessed by selecting the tabs of the notebook.

Crypto module notebook considerations

Working with a Crypto module notebook implies that the TKE workstation has been logged on by a TKE user ID whose profile is mapped to the TKEUSER role, a host session has been established, and a valid PCICC or CCF Authority signature key has been loaded in the TKE.

The Crypto module notebook contains all the information related to a Crypto module (CCF or PCICC): the CMID, OS/390 host, all the authorized commands, the authorities signature keys, the LPAR domain controls, and so on.

Updating a group of modules

If working with a newly created group made of empty or zeroized modules, select the group from the group container and then click any Crypto module in the module container to open the Crypto module notebook**.** The notebook will in fact internally refer to the group's master coprocessor, but all actions initiated via the notebook will be propagated to all the modules in the group.

Updating a single module

To access a single module (as opposed to a group), select the host in the host pane and then select the desired Crypto module in the Crypto modules pane. The difference with the group access is that you went through the host selection instead of a group selection.

Once you have selected a Crypto module or group of Crypto modules, the Crypto module notebook opens on the general page. The Crypto module information displayed is related to the master Crypto module in the group or to a single selected module. The title line of the notebook will state if you are dealing with a group or an individual coprocessor.

The notebook opens in one of the following notebook modes**:**

- In *update mode***,** you have exclusive control of the module or group of modules. Other TKE users subsequently opening the notebook will get access in read-only mode.
- In *read only mode*, the notebook is already opened by another TKE user. The other user's exclusive control can be released by selecting **release** in the Function pull-down menu.

  Note: Be aware, though, that release, because it is designed to exit from an unrecoverable lockup situation, may seriously interfere with the work of another TKE with an open notebook for the module.
- In *pending command mode*, the module or group this notebook pertains to has recorded that there is a pending command waiting to be co-signed.
- In *locked read-only mode*, the notebook for a group opens in this mode if one or more module in the group cannot be accessed from the TKE.

The notebook mode is indicated in the lower right-hand corner of the notebook window.

PCICC and CCF Crypto module notebook pages

- *General* displays only the coprocessor type and index and the host name, as shown in Figure 81 on page 116.
- *Details* shows five pages of information for the CCF, and two pages for the PCICC. No changes are allowed in any of these pages.
- *Access control* (CCF only) are the definitions of the signature requirements for each signed command, with the relevant masks. The contents are unchanged from the previous TKE V2, only the presentation differs. Note however that key extract and transfer is not available with the TKE V3.0.

- *Roles* (PCICC only)**:** The PCICC uses *role-based access control*. From the TKE workstation, an administrator defines in the PCICC a set of roles which correspond to classes of TKE users (also known as *authorities*).

  Each *role* defines a set of commands to be permitted. Each TKE authority has a *profile* in the PCICC, designated by an authority index, mapped to one of the defined roles.

  The authority can perform only the commands permitted by the role, and these commands have to be signed by the authority signature key at the TKE. PCICC Roles and profiles are further explained in 5.3.5.3, “Roles and profiles structure example”, on page 120.

  Figure 83 on page 118 shows the commands accessible to the roles in the PCICC.

Attention

The manipulation of roles in the PCICC can only be executed from the TKE workstation. Any command performed from the ICSF ISPF panel, or any cryptographic service requested by an application, will be executed under the pre-set DEFAULT role in the PCICC. This DEFAULT role is not accessible for setup.

- *Authorities* is a common function used to define authorities and to manage the key pair associated with an authority. Private and public key parts will be stored in TKE key storage and/or stored on media (diskette or TKE hard disk) protected by a password. Note that only one signature key can reside at one time in the key storage.

  Before sending or signing a command to a host Crypto module, the authority has to load his/her signature key. This page also allows you to sent the public modulus of the authorities to the Crypto modules. This is a prerequisite before sending any signed command to the Crypto modules (except for the default authority key, for which the public modulus is initially known by the Crypto modules).

- The *CCF* has a fixed number of sixteen authority indices (00 to 15) in effect. We recommend you use the same indices consistently across all coprocessors in the installation.
- The *PCICC* can record up to 100 authority indices (00 to 99). The number of authority indices in effect is not fixed; it varies with the administrator interventions to add or delete authorities. We recommend, for consistency, that you only use indices 00 to 15.
- *Domains*: This entry defines the LPAR domains that can have DES and PKA Master Keys (CCF and PCICCC notebooks) and operational keys (CCF notebook only) loaded and changed from the TKEs. It also provides domain controls.

  For each of the 16 domains, there are three pages that can be selected with the tabs at the bottom of the window: the domain general page, the domain keys page, and the domain controls page.

- *Co-sign*: Pending commands are processed from this page. When a command requiring multiple signatures (up to 16 signatures for the CCF, or up to two signatures for the PCICC) is issued by one authority, this command stays in pending status until all the signature requirements are completed. The co-sign page displays the pending command details and the signature requirement status. The co-signing authority can either sign the command in this page or delete the pending command.

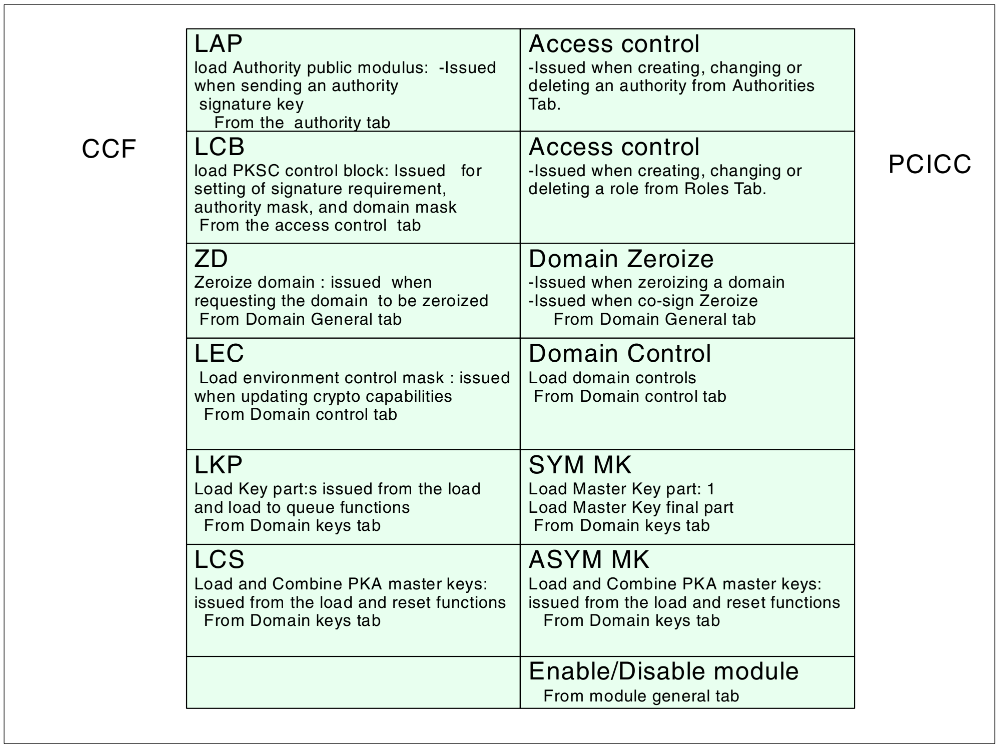
There is a difference in the co-sign mechanism between CCF and PCICC for multiple signature commands:

- All authorities defined in the CCF signature requirements panel can indifferently issue or co-sign a command. There is no restriction on which authorities must be the ones requesting the command first in sequence, and which authorities can subsequently co-sign the issued command.
- Unlike the CCF authority, a PCICC authority is mapped to a PCICC role as being the issuer of a command *or* as the co-signer of a command. Note that there can be only *one* co-signer to an issued command; while several authorities could co-sign the command, only one co-sign of the command is required.

  However, a PCICC role can be given both issuer and co-signer privileges. When an authority mapped to such a role issues a command, the command is executed at once since it is implicitly co-signed.

Figure 80 on page 115 establishes a parallel between the multi-signature commands in the CCF and the PCICC functions. Using this table, you can determine how to maintain consistency between the authorities defined in the CCF and the ones defined in the PCICC.

For example, the LAP and LCB commands on CCF and the Access Control Role on PCICC may have the same authorities index because of the similarities of the functions.The LKP (CCF) and SYM MK (PCICC) may also have the same authorities index.



CCF	PCICC
LAP load Authority public modulus: -Issued when sending an authority signature key From the authority tab	Access control -Issued when creating, changing or deleting an authority from Authorities Tab.
LCB load PKSC control block: Issued for setting of signature requirement, authority mask, and domain mask From the access control tab	Access control -Issued when creating, changing or deleting a role from Roles Tab.
ZD Zeroize domain : issued when requesting the domain to be zeroized From Domain General tab	Domain Zeroize -Issued when zeroizing a domain -Issued when co-sign Zeroize From Domain General tab
LEC Load environment control mask : issued when updating crypto capabilities From Domain control tab	Domain Control Load domain controls From Domain control tab
LKP Load Key part:s issued from the load and load to queue functions From Domain keys tab	SYM MK Load Master Key part: 1 Load Master Key final part From Domain keys tab
LCS Load and Combine PKA master keys: issued from the load and reset functions From Domain keys tab	ASYM MK Load and Combine PKA master keys: issued from the load and reset functions From Domain keys tab
	Enable/Disable module From module general tab

Figure 80. CCF and PCICC command families

5.3.4 PCICC modules notebook

In this section we discuss details of the PCICC Crypto module notebook.

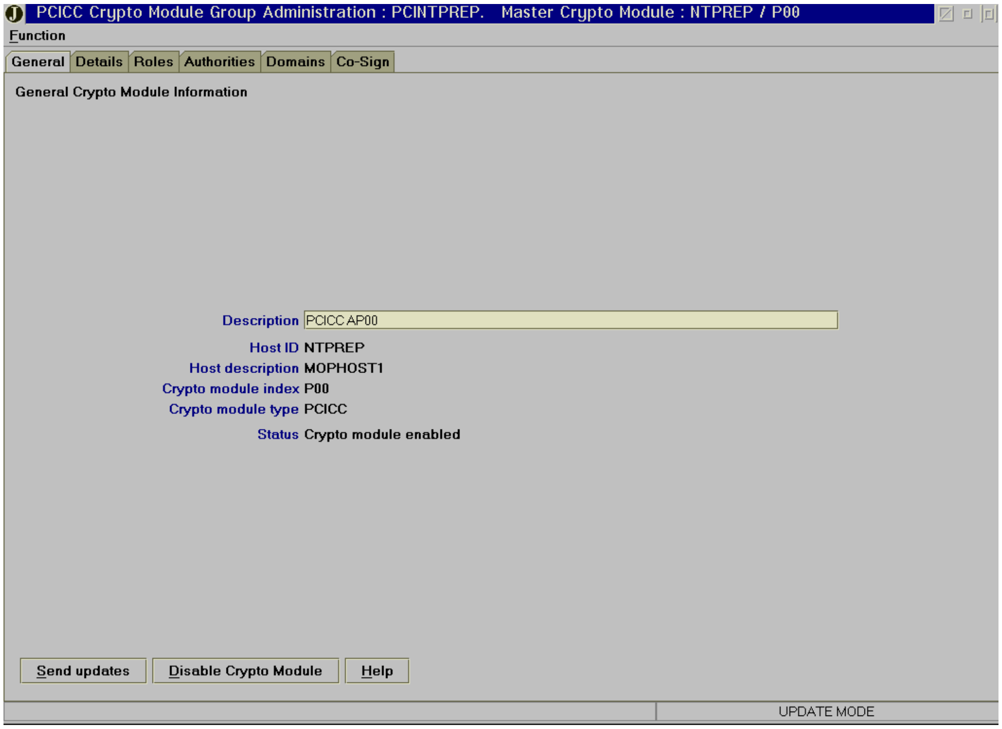
5.3.4.1 PCICC notebook GENERAL page

The panel shown in Figure 81 on page 116 contains a short description of the module (which can be changed), the module type, the module index and the host or group name. The PCICC can be *disabled* from this panel (this command requires a single signature) or *enabled* (dual signatures are required for enabling a module).

Although a disabled module does not provide cryptographic services to the applications, all information in the module is preserved. The intent of the disable or enable function is to permit easy control of the usage of cryptographic modules, for example during service maintenance, non-working hours, and so forth.

PCICC disable

A PCICC is disabled for *all* LPARs, not just for the LPAR that the disable command was issued from.


PCICC Crypto Module Group Administration : PCINTPREP. Master Crypto Module : NTPREP / P00

General Crypto Module Information

Description PCICC AP00

Host ID NTPREP

Host description MOPHOST1

Crypto module index P00

Crypto module type PCICC

Status Crypto module enabled

UPDATE MODE

Figure 81. PCICC notebook general page on TKE

5.3.4.2 PCICC notebook DETAILS page

The PCICC DETAILS page is sub-divided into two sections that are individually selectable: Crypto Module and Crypto services.

The Crypto module page contains details such as the CMID (module identifier), the module public modulus used by TKE to verify the signed replies from the Crypto module, the Transaction Sequence Number, and the hash pattern of the current DH transport key for this Crypto module.

The Crypto services page contains details on the FCV, such as the DES keys length, length of RSA keys, and base CCA availability. This information is loaded into the Crypto module at initialization of the S/390 system and cannot be changed from this panel.

5.3.4.3 PCICC notebook ROLES page

Newly installed PCICCs (or previously zeroized PCICCs) have a predefined AUTHORITY 00 index assigned to the predefined INITADM role in the PCICC. This role can both issue and co-sign access control commands; that is, only one single authority can perform these commands.

These commands allow you to create all the necessary roles and authorities that can be required by the customer security policy for the PCICC. Once the ultimate roles and authorities are established, remove the default values by deleting or changing authority 00 and/or by not having any authority mapped to the INITADM role. Figure 82 on page 117 illustrates the flow of role and authorities creation in the PCICC.

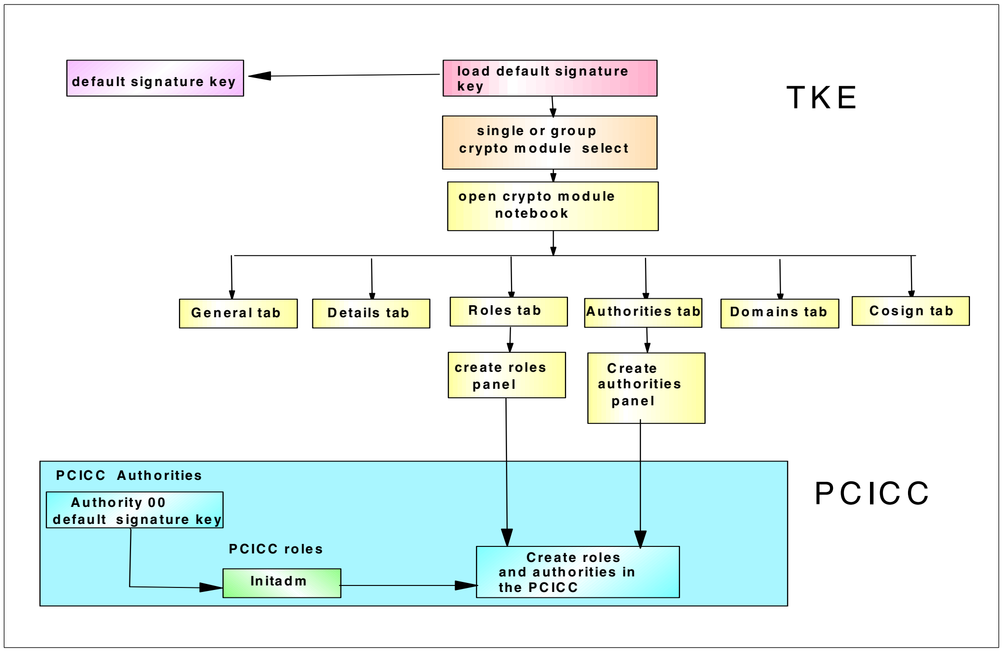


Figure 82. PCICC initial role & profile after new card install or card zeroize from SE

5.3.5 Creating roles and authorities in the PCICC

Figure 83 on page 118 shows the commands that can be assigned to a PCICC role. There are basically two types of commands: dual-signature commands and single-signature commands.

5.3.5.1 Dual-signature commands

Four commands always require *two* signatures (co-sign): one from the authority issuing the command, and one from an authority co-signing the command.

- `Enable crypto card`

  This command is issued from the Crypto notebook general page when switching the PCICC from the disable state to the enable state.

- `Access control`

  This command is issued with all creation, change, or deletion of roles or authorities.

- `Zeroize a domain`

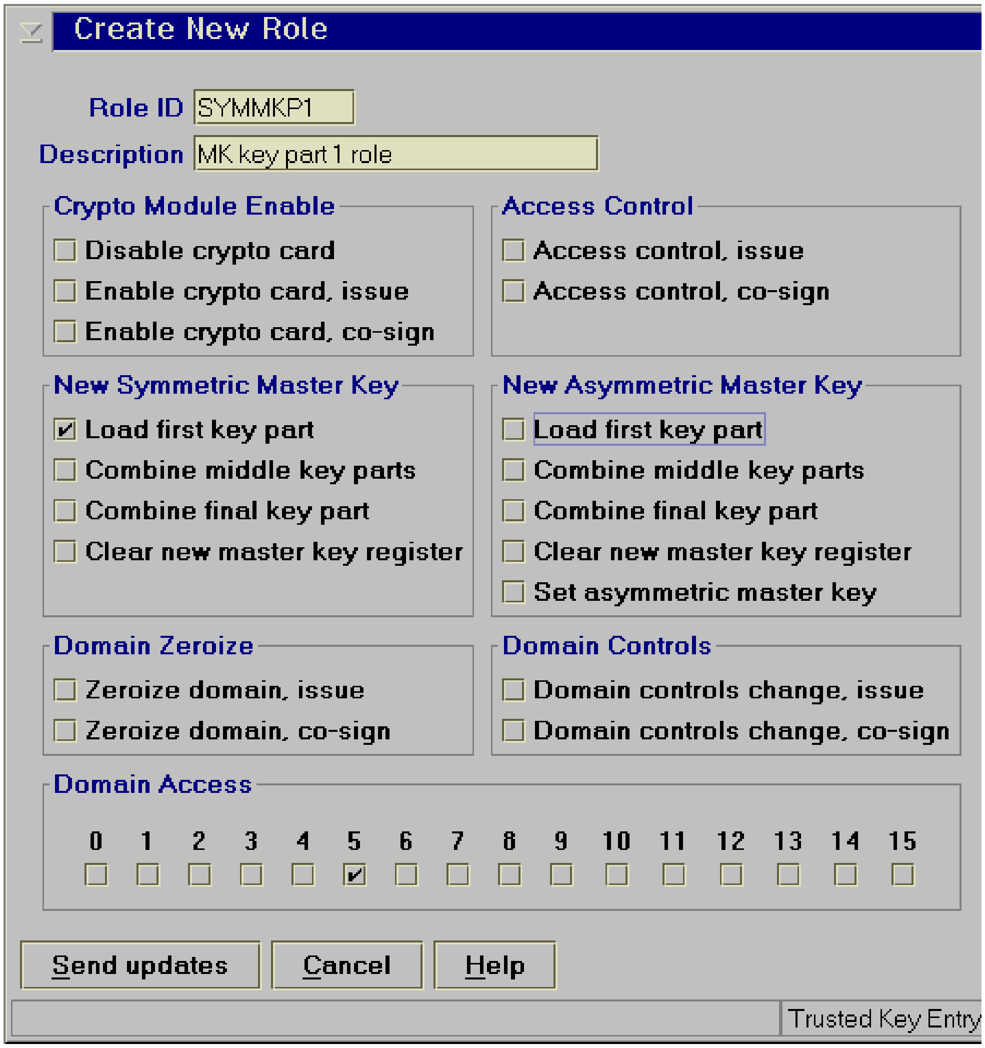
  This command is issued from the domain general page when zeroizing a domain.

- `Domain controls`

  This command is issued from the domain control page with any update to the domain control settings.

The co-sign requirement can be alleviated by creating a role where the sign and co-sign conditions are both enabled.

.



Role ID SYMMKP1

Description MK key part 1 role

Crypto Module Enable

□ Disable crypto card
□ Enable crypto card, issue
□ Enable crypto card, co-sign

Access Control

□ Access control, issue
□ Access control, co-sign

New Symmetric Master Key

☑ Load first key part
□ Combine middle key parts
□ Combine final key part
□ Clear new master key register

New Asymmetric Master Key

□ Load first key part
□ Combine middle key parts
□ Combine final key part
□ Clear new master key register
□ Set asymmetric master key

Domain Zeroize

□ Zeroize domain, issue
□ Zeroize domain, co-sign

Domain Controls

□ Domain controls change, issue
□ Domain controls change, co-sign

Domain Access

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□

Figure 83. PCICC Roles commands

5.3.5.2 Single-signature commands

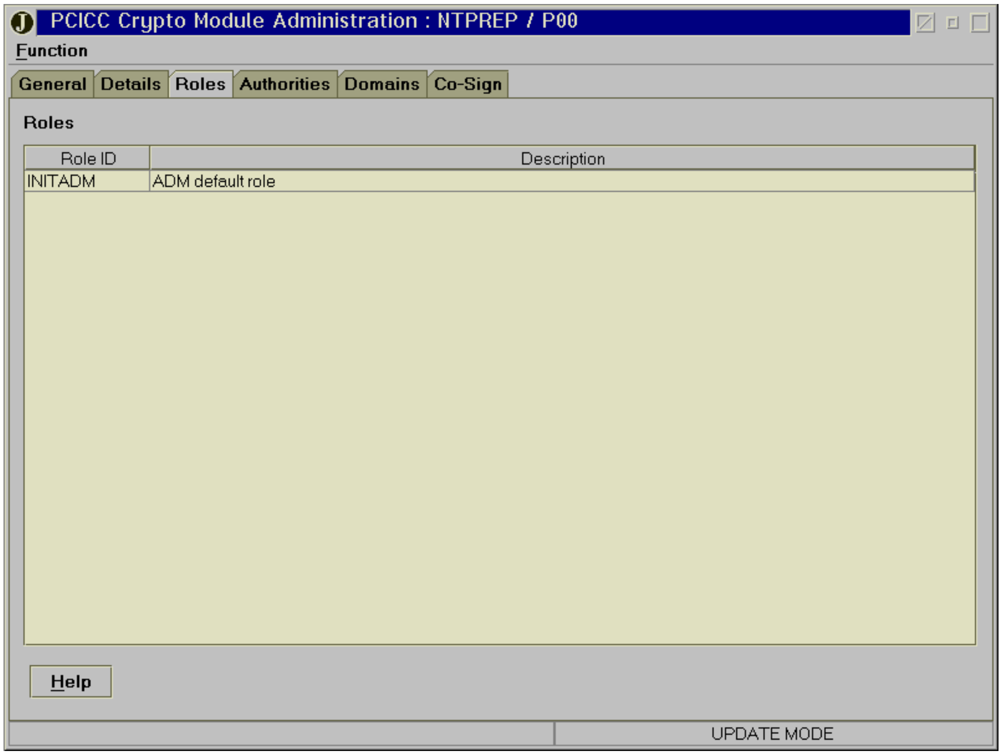
- `Disable crypto card`
- `Load first key part`
- `Combine middle key parts`
- `Combine final key part`
- `Clear new Master Key register`
- `Set asymmetric Master Key`

Creating or changing roles can be performed only by a Crypto module authority having a profile mapped to a role authorized to perform ACCESS CONTROL commands, generally named the Crypto module(s) Administrator. The default INITADM role provides this control.

Before sending any command, the authority signature key *must* have been loaded via the TKE main panel Functions pull-down menu or by the pop-up panel displayed when an action is selected and no signature key is loaded. The **Default** signature key must be selected if the PCICC is new or zeroized.

To create or change a role, the Crypto module administrator, after loading his/her signature key, clicks the right mouse button in the role page pane, and then selects **Create** or **Change.**

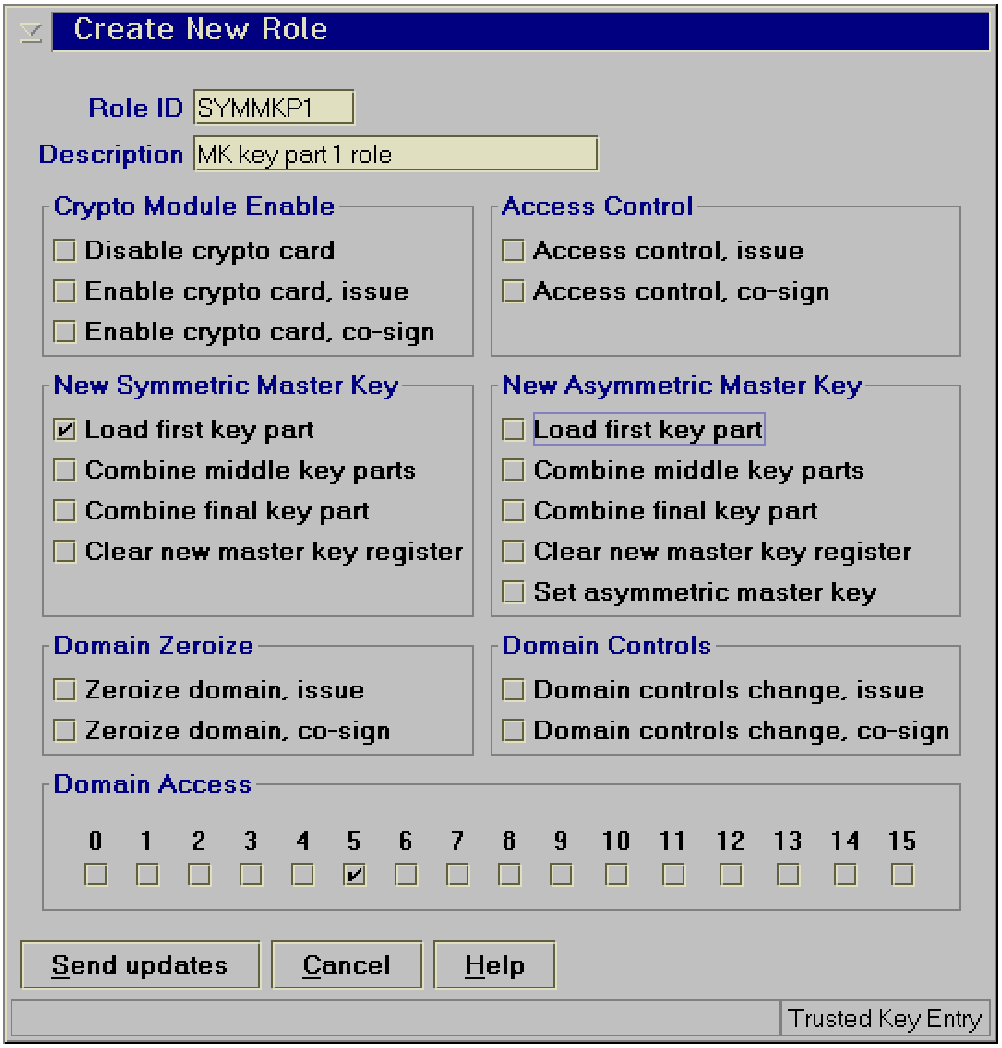
In the new role panel, he defines a Role ID (if creating the role), and writes a short text description; see Figure 84.


PCICC Crypto Module Administration : NTPREP / P00

Role ID	Description
INITADM	ADM default role

Figure 84. PCICC module administration notebook roles definition entry

He then checks the command boxes required for the role, and selects **Send updates** to send the new role to the PCICC host module, as shown in Figure 85 on page 120.



Role ID SYMMKP1

Description MK key part 1 role

Crypto Module Enable
- □ Disable crypto card
- □ Enable crypto card, issue
- □ Enable crypto card, co-sign

Access Control
- □ Access control, issue
- □ Access control, co-sign

New Symmetric Master Key
- ☑ Load first key part
- □ Combine middle key parts
- □ Combine final key part
- □ Clear new master key register

New Asymmetric Master Key
- □ Load first key part
- □ Combine middle key parts
- □ Combine final key part
- □ Clear new master key register
- □ Set asymmetric master key

Domain Zeroize
- □ Zeroize domain, issue
- □ Zeroize domain, co-sign

Domain Controls
- □ Domain controls change, issue
- □ Domain controls change, co-sign

Domain Access

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□

Figure 85. Create Role: SYMMKP1 will load 1st part of SYM MK (DES), domain 5

Note: Creating or changing a role is a dual-signature command, so another authority needs to co-sign, unless the administrator has been given a role where the access control commands are both issued and co-signed.

5.3.5.3 Roles and profiles structure example

In our example we create five roles and five authorities, using the default INITADM role. Figure 86 on page 121 is a graphical representation of our roles and authorities structure.

- Authority 01 is mapped to the DOMAINS role. This role has the Domain Controls privileges.
- Authority 02 is mapped to the SYMMKP1 role. This role permits to load symmetric Master Key part 1 in domain 5.
- Authority 03 is mapped to SYMMKP2 role. This role permits to load and combine symmetric Master Key last part in Domain5.
- Authority 04 is mapped to SYSADM1. This role has the Access Control privileges that permit to create or change Roles and Authorities.

- Authority 05 mapped to SYSADM2. This role allows you to co-sign commands previously issued by a user logged on with a profile mapped on SYSADM1.

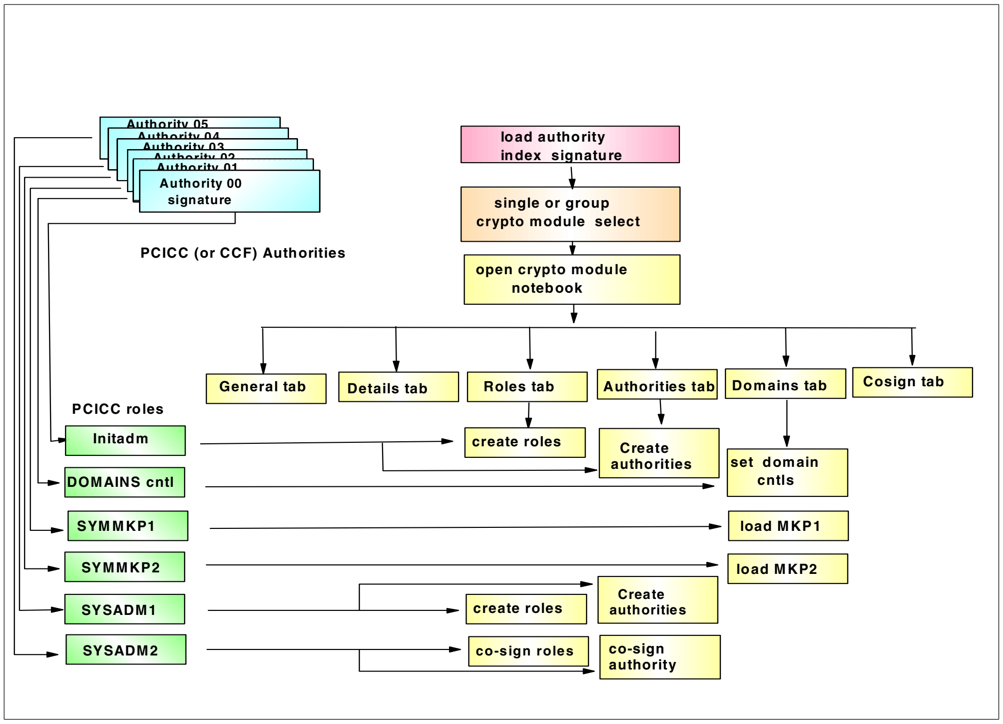
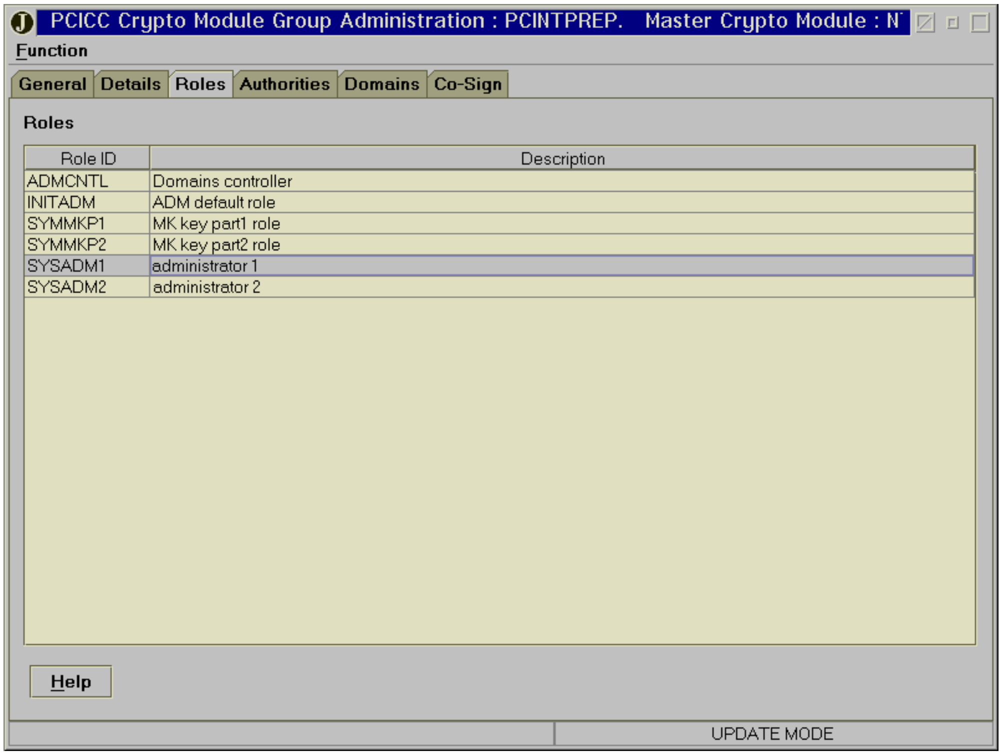


Figure 86. PCICC Create Roles and Authorities example

Figure 87 on page 122 shows the Roles page after the five new roles have been created.



PCICC Crypto Module Group Administration : PCINTPREP.   Master Crypto Module : N
Function
General
Details
Roles
Authorities
Domains
Co-Sign
Roles
Help
UPDATE MODE

Role ID	Description
ADMCNTL	Domains controller
INITADM	ADM default role
SYMMKP1	MK key part1 role
SYMMKP2	MK key part2 role
SYSADM1	administrator 1
SYSADM2	administrator 2

Figure 87. PCICC Roles page after new roles have been created

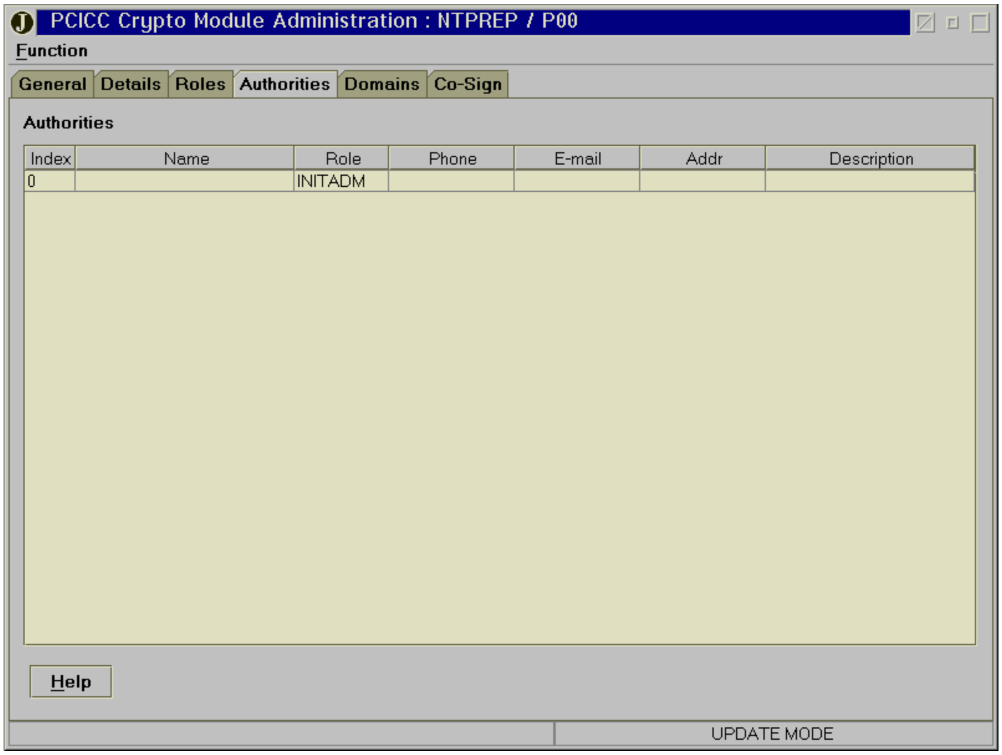
5.3.5.4 PCICC notebook AUTHORITIES pages

The PCICC notebook AUTHORITIES pages contain the following selections:

Generate PCICC signature keys

Before creating a PCICC new authority index, you need to generate a signature key for the index. To generate this key, select the **Authorities** tab and then click the right button of the mouse in the Authorities pane, as shown in Figure 88 on page 123.

Select **Generate signature** and enter the Authority index and relevant information such as name, phone number, e-mail, address and so on, and then press **Continue**.



Authorities

Index	Name	Role	Phone	E-mail	Addr	Description
0		INITADM				

Figure 88. PCICC module notebook authority management main panel

The newly generated key may be saved on a diskette, or on a TKE hard disk, or in TKE PKA keystore. If the keys are to be saved on a diskette or hard disk file, a password is required to encrypt the key file. We also recommend that you save it again in a different place.

Note: *Only one authority signature key* can be saved in TKE PKA keystore, and also be aware that an authority key loaded in the PKA keystore is *loadable without providing a password*.

You can create as many authority signature keys as needed, and you can save them for a later association with authorities. If you have decided (as we recommend) to keep the same and consistent authority indices across all coprocessors in the configuration, the same signature key files can be used when establishing authorities in the PCICC and in the CCF.

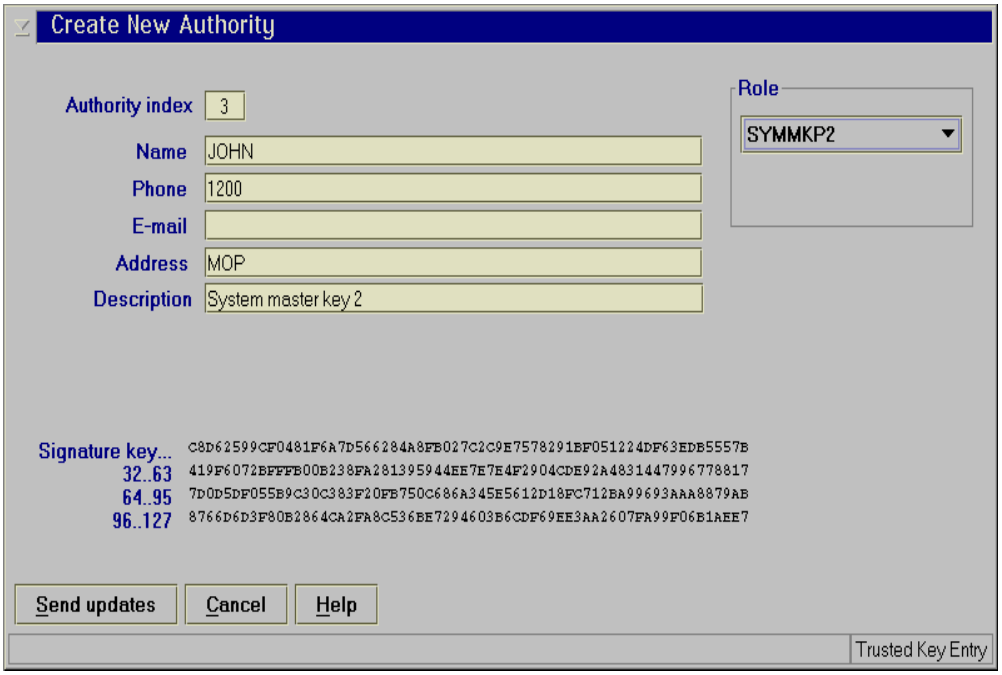
Create a PCICC new authority

To create a PCICC new authority, click the right mouse button in the window on the authority page, then select **Create**. A new authority key source is requested.

If you select keystore, the information associated with the key that you previously generated appear immediately in the window. If you select binary, you will have to specify the signature key file to be loaded from the hard disk or diskette. This authority signature key is protected by the password entered when it was generated. This is illustrated in Figure 89 on page 124. If you select the default key, there is no associated information provided with the default key.

This panel shows the following fields:

- The authority index
- The authority information (name, phone, address, short description)
- Role: this field provides a list of previously defined roles. The authority will be mapped to the role you select.
- Authority Signature key public modulus: this part of authority public key will be sent to the host Crypto module by pressing the Send updates button. It will be used later on by the Crypto module to verify the signed commands sent from TKE by this authority index.
- Send updates: this is a dual signature command and will require an authority with the proper role to co-sign.



Create New Authority

Authority index: 3
Name: JOHN
Phone: 1200
E-mail:
Address: MOP
Description: System master key 2
Role: SYMMKP2

```
Signature key... C8D62599CF0481F6A7D566284A8FB027C2C9E7578291BF051224DF63EDB5557B
          32..63 419F6072BFFFB00B238FA281395944EE7E7E4F2904CDE92A4831447996778817
          64..95 7D0D5DF055B9C30C383F20FB750C686A345E5612D18FC712BA99693AAA8879AB
         96..127 8766D6D3F80B2864CA2FA8C536BE7294603B6CDF69EE3AA2607FA99F06B1AEE7
```

Figure 89. Create Authority: JOHN, Authority 03 mapped to SYMMKP2 role

Note: TKE authorities mapped to the role with Access Control privileges, such as the INITADM default PCICC role, can create, change, or delete any other role and authorities. A security measure we strongly suggest is to *replace the INITADM role by two new administrator roles:* the first one to issue access control commands, and the second to co-sign these commands. Or, at a minimum, change the authority 00 signature key mapped to the INITADM role and keep it in a secure place.

In our example, we created SYSADM1 and SYSADM2 roles, and Authorities 4 and 5 were mapped to these administrator roles.

Change a PCICC authority

Activating this selection will allow you make changes to the authority information and to replace the authority public modulus in the Crypto module. The authority index remains fixed.

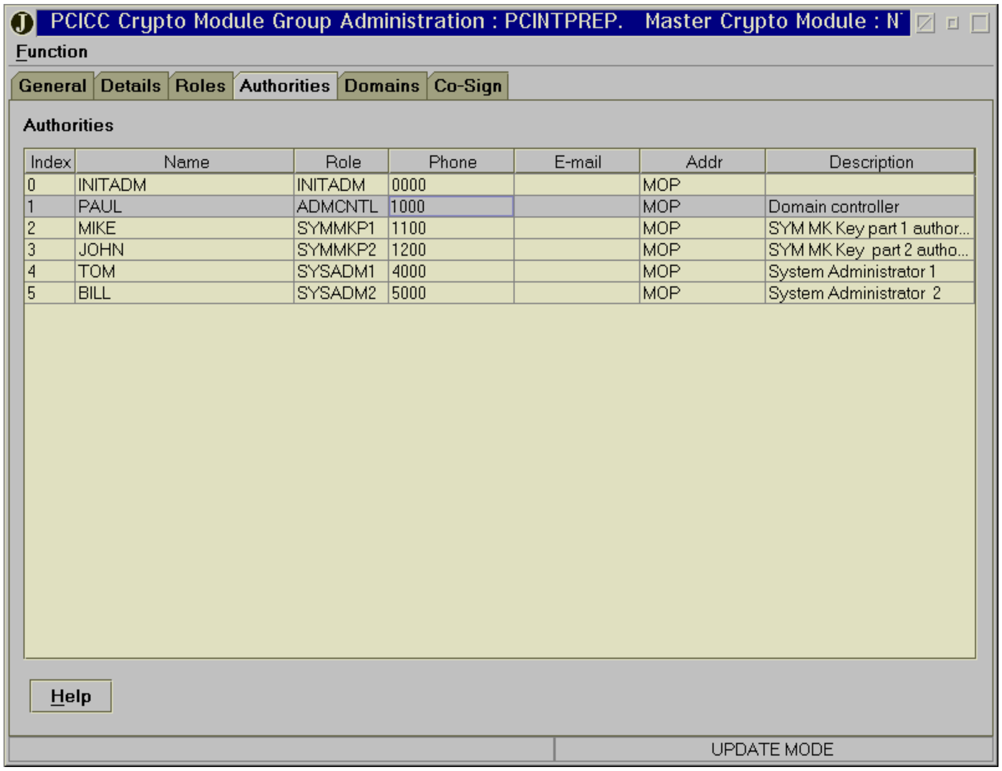
Select **Get signature key** to open a select key source window and load signature key window. The contents of the selected key file replaces the public modulus in the change authority window.

Pressing **Send updates** uploads the new information to the Crypto module.

Delete Authority

PCICC authorities (unlike CCF) can be deleted from the TKE. A consistency check of roles and profiles is performed to ensure that access to the Crypto module is not lost.

Figure 90 shows the Authorities main panel after the five new authorities have been created.


PCICC Crypto Module Group Administration : PCINTPREP.   Master Crypto Module : N
Function
General
Details
Roles
Authorities
Domains
Co-Sign
Authorities
Help
UPDATE MODE

Index	Name	Role	Phone	E-mail	Addr	Description
0	INITADM	INITADM	0000		MOP	
1	PAUL	ADMCNTL	1000		MOP	Domain controller
2	MIKE	SYMMKP1	1100		MOP	SYM MK Key part 1 author...
3	JOHN	SYMMKP2	1200		MOP	SYM MK Key part 2 autho...
4	TOM	SYSADM1	4000		MOP	System Administrator 1
5	BILL	SYSADM2	5000		MOP	System Administrator 2

Figure 90. PCICC Authorities panel after some authorities have been created

5.3.5.5 PCICC notebook DOMAINS page

The PCICC domains entry page displays general information about each of the 16 possible LPAR domains. Selecting tabs on the right will open the specific domain general page.

Three page tabs are located at the lower lefthand side of the domain window: General, Keys, and Control. These refer to the domain general page, the domain keys page, and the domain control page; we discuss these in detail in the following sections.

- Domain general page - this page is shown in Figure 91 on page 126. From here you can select the tasks **change description** and **Zeroize the domain**.
  - To change the description, edit the description entry and press **Send updates**.

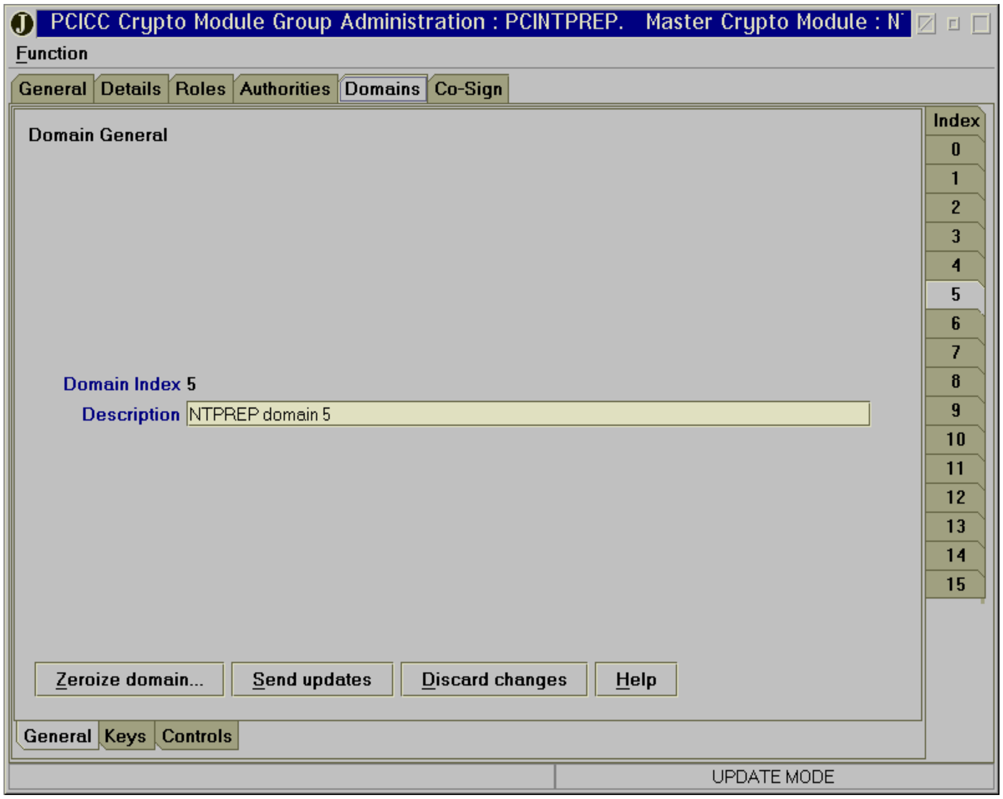
- If you choose Zeroize a domain, you can do the following:
  - Erase the domain’s Master Keys
  - Erase the domain’s retained keys
  - Reset the domain controls.

  Note: User-defined roles and profiles are not changed.

Zeroize can be done by a user logged on with an authority mapped to a role that is authorized to perform zeroize and then co-signed.

Important

After domain zeroization, be aware that the ICSF panel services shown in Figure 93 on page 128 are in a disabled state, except for Key token change. If these services are needed, they must be manually restored to the enabled state in the domain controls page.

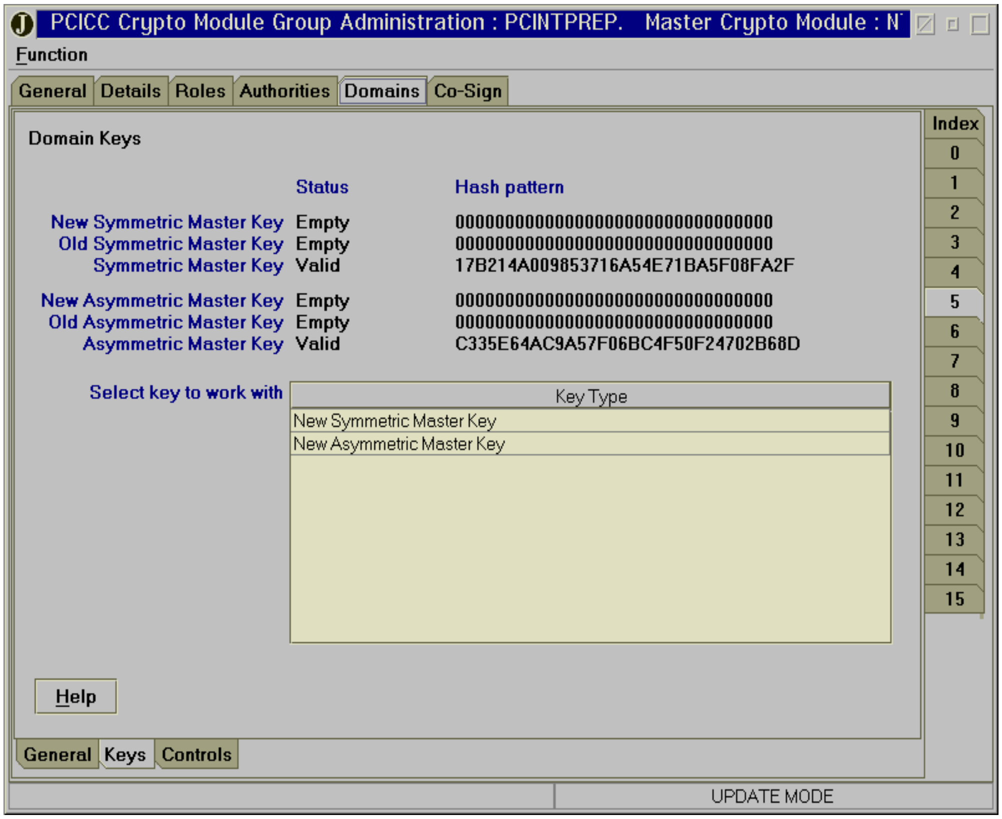


Domain Index 5
Description NTPREP domain 5

Figure 91. PCICC Domain 5 general page

- Domain Keys page - this page shows the Master Key status and allows you to generate, load, and clear domain key registers as shown in Figure 92 on page 127. When right-clicking a key type from the key pane, the following actions become available:
  - **Generate** will generate a key part and write it to a file.
  - **Clear** will clear the key register.

- **Load** will load a key or a key part (first, intermediate, or last) from a binary file or from the keyboard into the new Master Key register. A blind key option exists for keyboard entry as explained in 5.2.2, “TKE workstation 4758 setup”, on page 97.
- **Set -** setting the ASYM-MK key will transfer the current Master Key to the old Master Key register and the new Master Key to the current Master Key register.



Domain Keys

	Status	Hash pattern
New Symmetric Master Key	Empty	00000000000000000000000000000000
Old Symmetric Master Key	Empty	00000000000000000000000000000000
Symmetric Master Key	Valid	17B214A009853716A54E71BA5F08FA2F
New Asymmetric Master Key	Empty	00000000000000000000000000000000
Old Asymmetric Master Key	Empty	00000000000000000000000000000000
Asymmetric Master Key	Valid	C335E64AC9A57F06BC4F50F24702B68D

Select key to work with

Key Type
New Symmetric Master Key
New Asymmetric Master Key

Figure 92. PCICC Domain 5 keys page

- Domain control page - this page, shown in Figure 93 on page 128, displays the cryptographic service functions that are enabled for the domain in the ICSF ISPF panels, as follows:
  - Clear New Master Key Register
  - Load First Master Key Part
  - Combine Master Key Part
  - Key Token Change

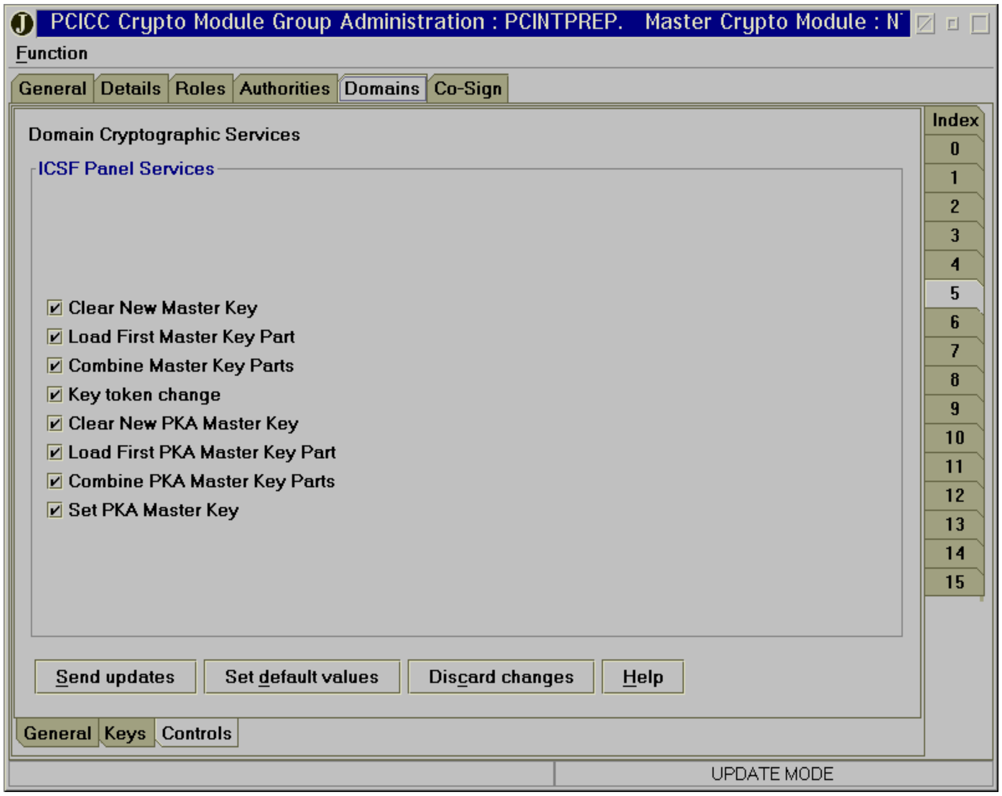
Key Token Change

Key Token Change does not really relate to a service available through an ICSF panel. This option allows the PCICC to proceed with reenciphering a DES key token under the DES old Master Key, subsequently to a CKDS re-encipher. We recommend that you always have the option selected.

- Clear New PKA Master Key
- Load First PKA Master Key Part
- Combine PKA Master Key Part
- Set PKA Master Key

Set default values (to be done after zeroize) will enable key token change.

Note: These functions will be permitted from the ICSF panel only if the boxes are checked, but can be performed in any case from TKE.



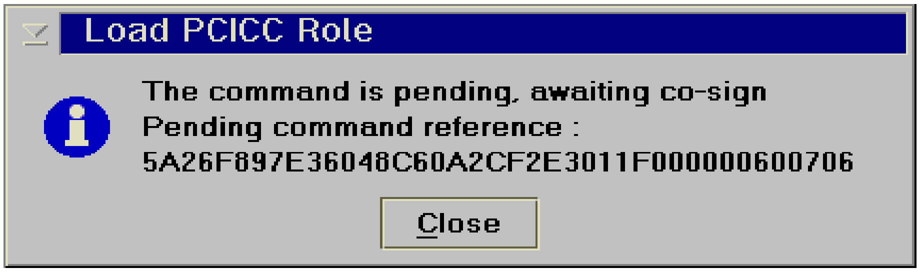
Domain Cryptographic Services

ICSF Panel Services

☑ Clear New Master Key
☑ Load First Master Key Part
☑ Combine Master Key Parts
☑ Key token change
☑ Clear New PKA Master Key
☑ Load First PKA Master Key Part
☑ Combine PKA Master Key Parts
☑ Set PKA Master Key

Figure 93. PCICC Domain 5 control panel

- PCICC Co-Sign page - for PCICC modules, some commands require two signatures before they can be executed by the Crypto module. Once an authority has issued such a command (for example, creating an authority), a pop-up message is displayed to notify the user that the command is pending and awaiting co-sign, as shown in Figure 94.



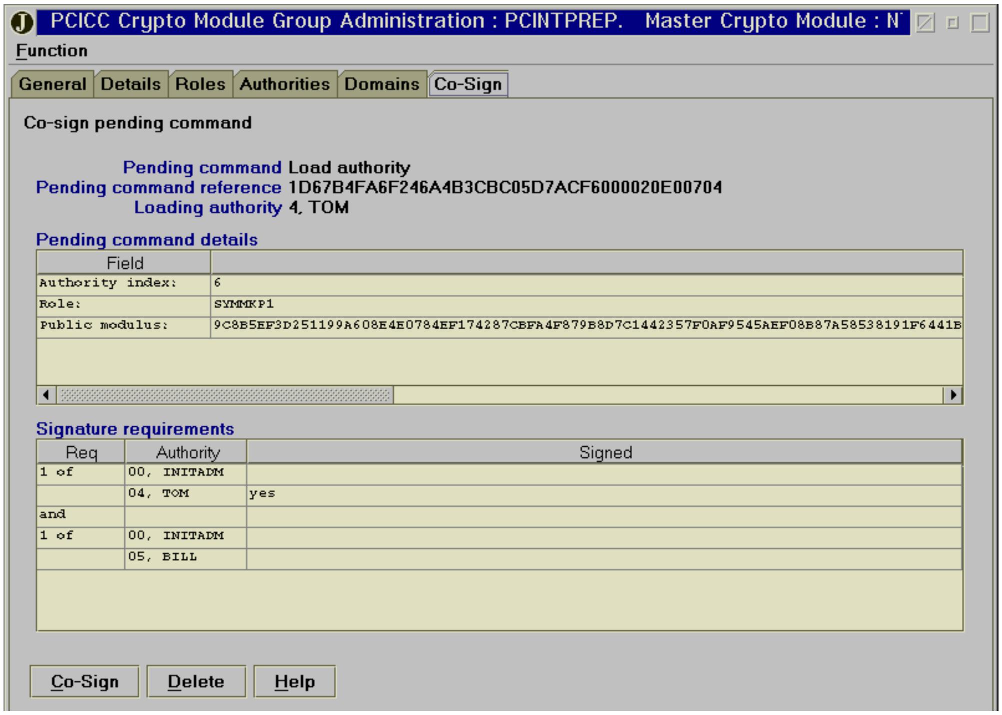
The command is pending, awaiting co-sign
Pending command reference :
5A26F897E36048C60A2CF2E3011F000000600706

Figure 94. Pending command message panel

This pending command can be displayed in the co-sign page. This page shows the details of the pending command and loading authority. The signature requirement field displays the authority who has already signed and the authorities that are permitted to sign this type of command; see Figure 95.

Pressing **Co-sign** initiates the signing and will require the source of the signature key to be loaded with the authority index associated with that key.

Pressing **Delete** will delete the pending command.


PCICC Crypto Module Group Administration : PCINTPREP. Master Crypto Module : N
Function
General
Details
Roles
Authorities
Domains
Co-Sign
Co-Sign
Delete
Help

Co-sign pending command

Pending command Load authority
Pending command reference 1D67B4FA6F246A4B3CBC05D7ACF6000020E00704
Loading authority 4, TOM

Pending command details

Field	
Authority index:	6
Role:	SYMMKP1
Public modulus:	9C8B5EF3D251199A608E4E0784EF174287CBFA4F879B8D7C1442357F0AF9545AEF08B87A58538191F6441B

Signature requirements

Req	Authority	Signed
1 of	00, INITADM	
	04, TOM	yes
and		
1 of	00, INITADM	
	05, BILL	

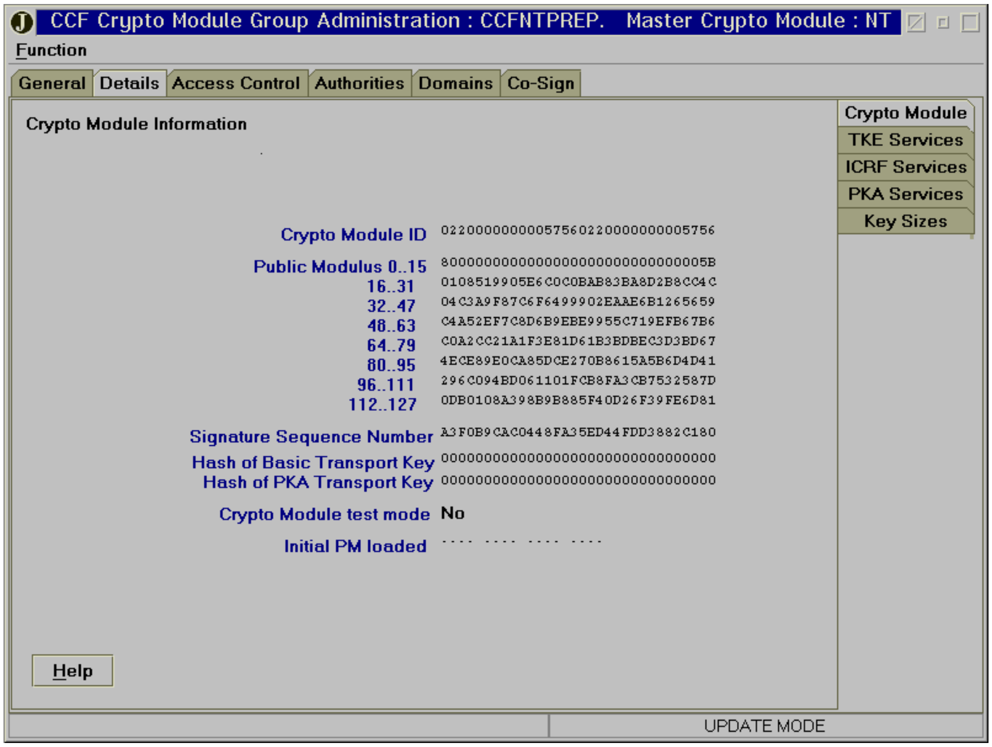
Figure 95. Co-sign panel: co-sign pending for create authority issued by TOM

5.3.5.6 Crypto CCF notebook

On the TKE main panel, you can select Crypto Module C00 or C01 or a group of CCFs to display the *CCF Crypto Module Group Administration notebook*. The notebook is the central point of control for displaying and changing all information related to a specific CCF or a group of CCF modules.

CCF Details Page

The CCF Details Page is sub-divided into 5 sections which are individually selectable: Crypto Module; TKE services; ICRF services; PKA services; Key sizes. All information in these sections are read only and cannot be changed. This page is shown in Figure 96 on page 130.



CCF Crypto Module Group Administration : CCFNTPREP. Master Crypto Module : NT

Crypto Module Information

Crypto Module ID 02200000000057560220000000005756

Public Modulus 0..15 800000000000000000000000000005B
16..31 0108519905E6C0C0BAB83BA8D2B8CC4C
32..47 04C3A9F87C6F6499902EAAE6B1265659
48..63 C4A52EF7C8D6B9EBE9955C719EFB67B6
64..79 C0A2CC21A1F3E81D61B3BDBEC3D3BD67
80..95 4ECE89E0CA85DCE270B8615A5B6D4D41
96..111 296C094BD061101FCB8FA3CB7532587D
112..127 0DB0108A398B9B885F40D26F39FE6D81

Signature Sequence Number A3F0B9CAC0448FA35ED44FDD3882C180
Hash of Basic Transport Key 00000000000000000000000000000000
Hash of PKA Transport Key 00000000000000000000000000000000

Crypto Module test mode No

Initial PM loaded ---- ---- ---- ----

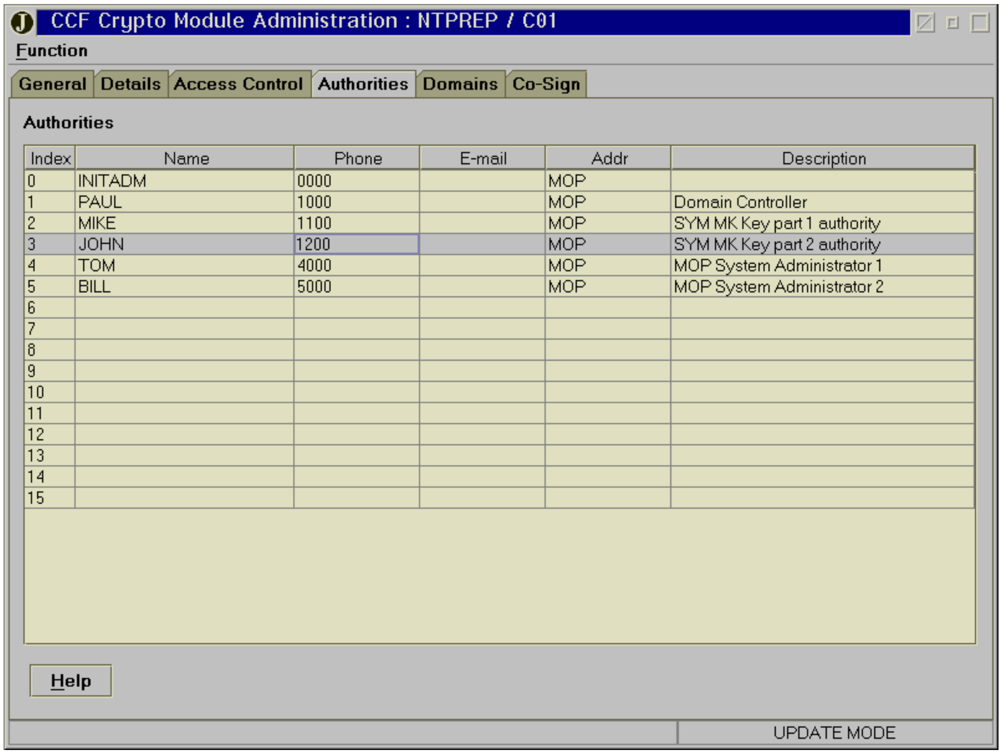
Figure 96. TKE CCF Crypto Module Details view

CCF Authorities page

This page is shown in Figure 97 on page 131. The CCF implements 16 predefined authorities, while the PCICC allows a variable number of authorities (0 to 99). We recommend you use the same indices across the installation and use only the first sixteen indices for PCICC.

Unlike the PCICC, the CCF Crypto module administration doesn’t allow you to create or delete an authority; however, change authority *is* allowed so that an authority signature key can be replaced.

After CCF initialization, the 16 authorities are set up with default signature keys in the CCF. These authority signature keys should be changed to new generated signature keys, accordingly to the site security policy.



Authorities

Index	Name	Phone	E-mail	Addr	Description
0	INITADM	0000		MOP	
1	PAUL	1000		MOP	Domain Controller
2	MIKE	1100		MOP	SYM MK Key part 1 authority
3	JOHN	1200		MOP	SYM MK Key part 2 authority
4	TOM	4000		MOP	MOP System Administrator 1
5	BILL	5000		MOP	MOP System Administrator 2
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

Figure 97. TKE CCF Crypto Module Authorities view

CCF Access Control page

This page displays the signature requirements, the authority masks, and the domain masks. As an example, Figure 98 on page 132 shows four commands with signature requirements among the six authorities:

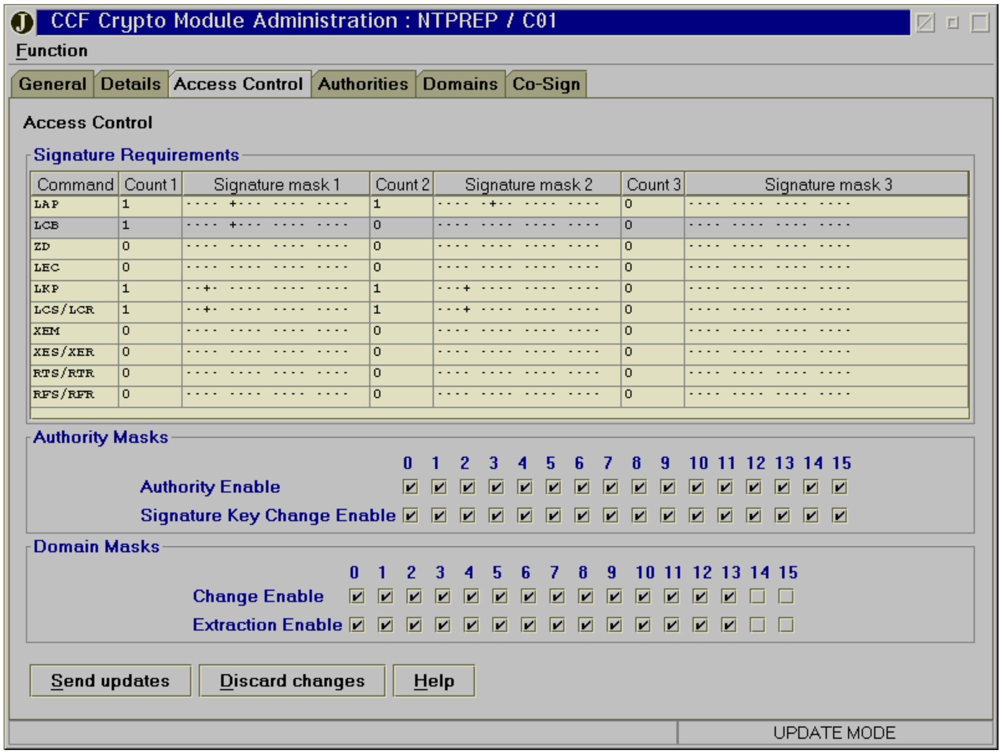
- The LAP command needs signatures from authorities 4 and 5.
- The LCB command needs a signature from authority 4.
- The LKP command needs signatures from authorities 2 and 3.
- The LCS/LCR commands need signatures from authorities 2 and 3.

Double-clicking on one of the signature requirement entries brings up a dialog box allowing changes to the signature requirements for the command.

Important

You could be “locked out” of a CCF or a PCICC when, for example, due to an improper sequence of commands, the keys for the authorities able to sign an LCB or Access Control command do not match between the TKE and the coprocessor.

This situation can be recovered only by *zeroizing the coprocessor at the Support Elemen*t (in the case of CCF, you also have to perform a system power-on reset). The only way to prevent this situation is to carefully track all operations involving the setup of authorities, roles, masks, and signature keys and, above all, to clearly understand their implications.



Access Control

Signature Requirements

Command	Count 1	Signature mask 1	Count 2	Signature mask 2	Count 3	Signature mask 3
LAP	1	---- +--- ---- ----	1	---- -+-- ---- ----	0	---- ---- ---- ----
LCB	1	---- +--- ---- ----	0	---- ---- ---- ----	0	---- ---- ---- ----
ZD	0	---- ---- ---- ----	0	---- ---- ---- ----	0	---- ---- ---- ----
LEC	0	---- ---- ---- ----	0	---- ---- ---- ----	0	---- ---- ---- ----
LKP	1	--+- ---- ---- ----	1	---+ ---- ---- ----	0	---- ---- ---- ----
LCS/LCR	1	--+- ---- ---- ----	1	---+ ---- ---- ----	0	---- ---- ---- ----
XEM	0	---- ---- ---- ----	0	---- ---- ---- ----	0	---- ---- ---- ----
XES/XER	0	---- ---- ---- ----	0	---- ---- ---- ----	0	---- ---- ---- ----
RTS/RTR	0	---- ---- ---- ----	0	---- ---- ---- ----	0	---- ---- ---- ----
RFS/RFR	0	---- ---- ---- ----	0	---- ---- ---- ----	0	---- ---- ---- ----

Authority Masks

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Authority Enable	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Signature Key Change Enable	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

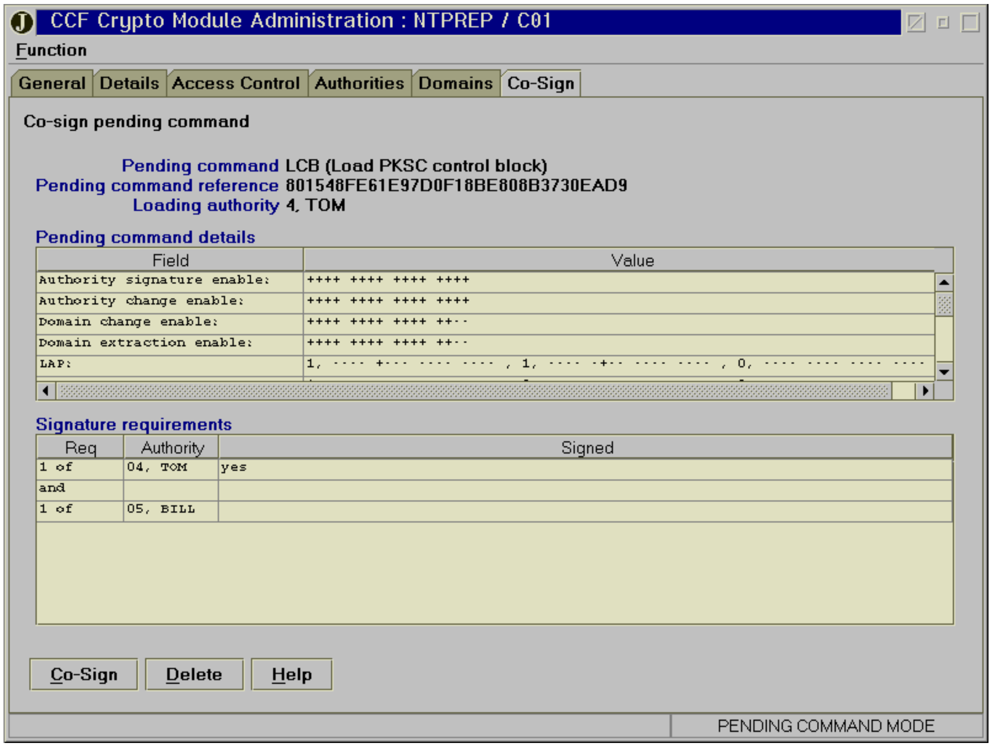
Domain Masks

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Change Enable	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□	□
Extraction Enable	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□	□

Figure 98. TKE CCF Crypto Module Access Control view

CCF Co-sign

In our example, shown in Figure 99 on page 133, the signatures from authorities 04 and 05 are required for an LCB command. Authority 04 has issued the LCB command and the command is pending, waiting for the authority 05 signature.



Co-sign pending command

Pending command LCB (Load PKSC control block)
Pending command reference 801548FE61E97D0F18BE808B3730EAD9
Loading authority 4, TOM

Pending command details

Field	Value
Authority signature enable:	++++ ++++ ++++ ++++
Authority change enable:	++++ ++++ ++++ ++++
Domain change enable:	++++ ++++ ++++ ++--
Domain extraction enable:	++++ ++++ ++++ ++--
LAP:	1, ---- +--- ---- ---- , 1, ---- -+-- ---- ---- , 0, ---- ---- ---- ----

Signature requirements

Req	Authority	Signed
1 of	04, TOM	yes
and		
1 of	05, BILL	

Figure 99. TKE CCF Crypto Module Co-Sign view

CCF Domains page

The CCF Domains page defines the domains that can have DES, PKA Master Keys, and operational keys loaded and changed from the TKE, as well as the domain controls set.

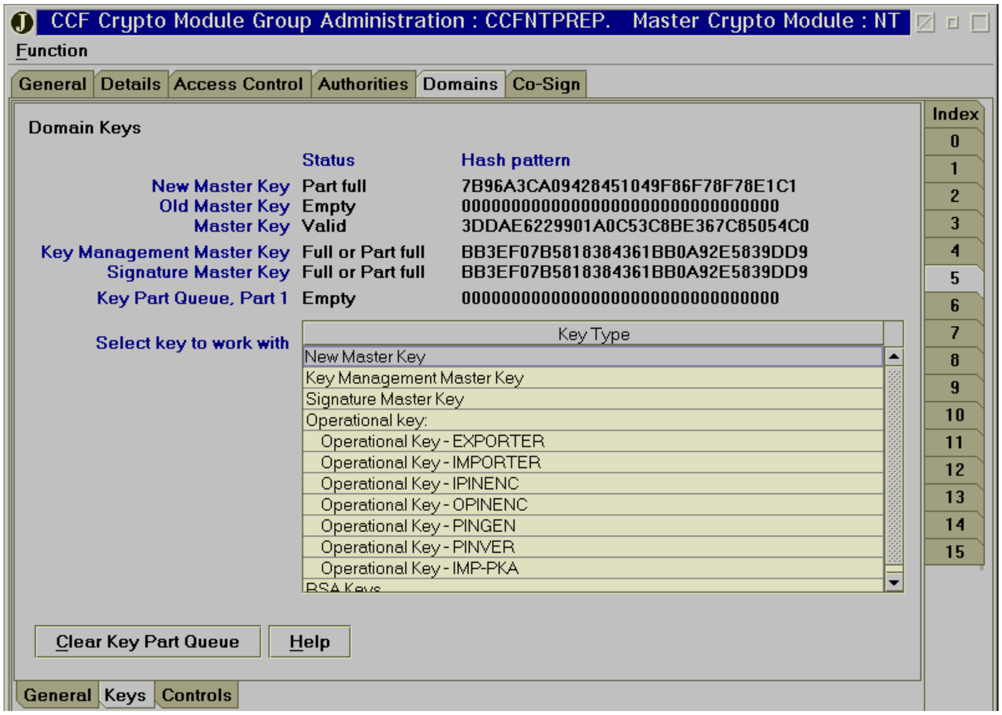
The page is subdivided into three parts: General; Keys; Controls. These parts are discussed in the following sections.

- **General** appears when a domain is selected. From there, the domain can be zeroized. When a domain is zeroized from the TKE, displaying the CCF modules status in the ICSF panels shows the module in STANDBY condition.

  After a domain zeroize, the ICSF cryptographic functions must be enabled in the Domain control panel to allow loading of the Master Keys through the TKE workstation. Providing access to the clear Master Key entry function via the ISPF panels should be based on the site security policy.

- **Keys** displays Master Key status information, and allows you to generate, load, and clear domain key registers. It also allows you to create and load operational keys and RSA keys. Figure 100 on page 134 shows the domain keys page; this screen was captured after the First Master Key part had been loaded for domain 5.

- **Controls** is the Crypto function enablement panel. This permits enabling/disabling cryptographic functions, special secure mode, and access to the clear Master Key entry panels in the Environmental Control Mask (ECM). Cryptographic functions *must* be enabled in order to access the Crypto coprocessors.



Domain Keys

	Status	Hash pattern
New Master Key	Part full	7B96A3CA09428451049F86F78F78E1C1
Old Master Key	Empty	00000000000000000000000000000000
Master Key	Valid	3DDAE6229901A0C53C8BE367C85054C0
Key Management Master Key	Full or Part full	BB3EF07B5818384361BB0A92E5839DD9
Signature Master Key	Full or Part full	BB3EF07B5818384361BB0A92E5839DD9
Key Part Queue, Part 1	Empty	00000000000000000000000000000000

Select key to work with

Key Type
New Master Key
Key Management Master Key
Signature Master Key
Operational key:
Operational Key - EXPORTER
Operational Key - IMPORTER
Operational Key - IPINENC
Operational Key - OPINENC
Operational Key - PINGEN
Operational Key - PINVER
Operational Key - IMP-PKA
RSA Keys

Figure 100. KE CCF Crypto Module Domain: new Master Keys first part done

5.3.6 Backing up the TKE files

There are a number of files that should be backed up when the TKE initialization tasks have been completed. These include any roles and profiles defined using the CCA support program CSUECNM tool and saved to disk. It also includes the authority signature keys saved to binary files.

5.3.6.1 Workstation files

You should systematically back up files on your workstation. Double-click on the **Backup** icon and follow the instructions.

- HOST.DAT contains the definitions for the host sessions and related data. It also contains the CMID and public modulus key for each module.
- GROUP.DAT contains definitions for host modules groups.
- TKE.INI contains customization information for TKE.

These files should be backed up whenever definitions for any of the above are changed.

- DESSTORE.DAT and DESSTORE.NDX. These are the DES key storage areas used to hold IMP-PKA keys for encrypting RSA keys and EXPORTER keys used by the 4753 migration facility.
- PKASTORE.DAT and PKASTORE.NDX. These are the PKA key storage areas used to hold one authority signature key.

Additionally, if you have saved authorities signature keys or Master Key parts to a binary file on the hard drive, they should be backed up as well. If you have previously generated and loaded DES Master Key parts during the TKE IBM 4758 initialization and saved them to the hard drive, they must backed up. Since these files are named by you, there is no automated procedure to back them up. You must manually copy the files to the TKE binary diskette that is shipped with the TKE workstation.

Note: Do *not* use the backup diskette for this purpose.

5.3.6.2 Host files

The Crypto module (CM) data set on the MVS Host system must be backed up. The name of the data set is defined in the parameters of the Host Transaction Program. Refer to Appendix C, “TKE host TCP/IP server setup” on page 145, to find out the name given to this file in your installation.

This data set contains definitions for the Crypto modules, domains, and authorities. It is updated any time the user makes changes in the TKE application windows and Crypto module notebooks.

5.4 4753 Key Token Migration facility

A facility is provided in the TKE V3.0 to migrate 4753 key tokens into the ICSF cryptographic key data set. It runs a migration utility in the TKE workstation and provides the transfer facility, so that the migrated tokens can be transferred into the host CKDS.

We did not practice with this utility during the residency; therefore, this information is provided for reference only and to point you to the *TKE Workstation User’s Guide 2000*, GA22-7430, which provides the detailed procedure in its Appendix F.

Chapter 6. Support functions

In this chapter we describe the additional support functions provided by OS/390 for the PCICC.

6.1 RACF access control to ICSF services

These sections describe changes in RACF profiles.

6.1.1 New profiles

The following new profiles have been added in the CSFSERV general resource class:

CSFDKCS Protects the clear Master Key entry panel for the PCICC

CSFPCI Protects the TKE interface functions for communicating with the PCICC

CSFPCM Protects the PCICC management panel

CSFRKD Protects the Retained Key Delete callable service

CSFRKL Protects the Retained Key List callable service

6.1.2 CSFSERV profiles - cryptographic coprocessor administration

This section describes how RACF profiles can be used to restrict the coprocessors' administration services to a selected set of users. The restrictions are enforced only when the CSFSERV general resource class is active; to activate the class, enter the following commands:

```
SETROPTS CLASSACT(CSFSERV)

SETROPTS RACLIST(CSFSERV)
```

After permitting specific users to the profile, the RACF administrator must refresh the in-storage profiles by issuing this command:

```
SETROPTS RACLIST(CSFSERV) REFRESH
```

6.1.2.1 CSFDKCS and CSFDKEF

When not permitted to these profiles, the user cannot enter the Master Key's parts into the new Master Key registers or the PKA Master Key registers.

6.1.2.2 CSFPMCI

This profile allows you to initialize the coprocessors' Master Keys and the CKDS by using a passphrase.

6.1.2.3 CSFPCI and CSFPKSC

The TKE host TCP/IP server (in our case, user ID TKEUSER) must be permitted to these two profiles. CSFPCI allows interactions between the TKE and the PCICC, while CSFPKSC allows interactions between the TKE and the CCF.

6.1.2.4 CSFSMK and CSFPCM

CSFSMK allows you to get access to the set Master Key panel. CSFPCM gives access to the PCICC Management panel.

6.1.2.5 CSFREFR and CSFRENC

CSFREFR allows you to access the CKDS Refresh function. CSFRENC allows you to access the Re-encipher CKDS function.

6.2 Crypto usage measurement

As of today, there is no specific measurement or instrumentation facility provided with ICSF. Instead, you have to exploit the contents of SMF records type 30 or type 82 to observe OS/390 ICSF activity.

Appendix A. Exploiting the PCICC

In this appendix we list the software products you can use to take advantage of the PCI Cryptographic Coprocessor functions.

A.1 The IBM exploiters

The following software products exploit the S/390 cryptographic solution:

- IBM HTTP Server for OS/390
- OS/390 System SSL
- OS/390 LDAP Server
- CICS Transaction Gateway
- IBM Payment Suite e-commerce solutions on OS/390
- OS/390 TN3270 Server
- OS/390 Firewall Technology IPsec and Internet Key Exchange (IKE)
- DCE Security Server
- VTAM Session Level Encryption
- BSAFE Toolkit for OS/390
- OS/390 Open Cryptographic Services Facility
- CBT (Crypto Based Transactions) banking solution
- RACF
- Financial Institution Applications

Appendix B. Support functions: ICSF services

ICSF provides callable services that perform cryptographic functions. This appendix describes these enhanced callable services.

B.1 Enhanced callable services

The enhanced callable services are detailed in the following sections.

B.1.1 PKA Key Generation (CSNDPKG)

- Adds support for the generation of the RSA key in CRT and ME form for a modulus length of 512 to 2048 bits
  - The public exponent may be 3, 2^{16} +1, or random.
- There are new rule array keywords:
  - CLEAR means the RSA token will be generated in the clear.
  - MASTER means the RSA key is generated in internal form.
  - RETAIN means the RSA key is retained in the PCICC.
  - CLONE means the Retained key may be cloned from one PCICC to another securely (future function).
- Regeneration data may be supplied to always generate the same key (for RSA keys only).
- The generated key may be written directly to the PKDS.
- The routing is as follows: RSA key generation on PCICC, DSS generation on CCF.

B.1.2 PKA Key Token Build (CSNDPKB)

- Adds support to build external PKA clear, encrypted, or skeleton tokens for a new CRT form.
- There are new rule array keywords:
  - RSA-CRT builds an RSA private key in optimized CRT form.
  - KM-ONLY is a new key usage specification that indicates a key may be used only in key distribution services and not in any digital signature services.
- There is a new key value structure for CRT tokens.
- This is not a cryptographic function; it executes in ICSF.

B.1.3 PKA Key Import (CSNDPKI)

- This service imports a PKA token from an external form to an internal form.
- For DSS tokens, this service is routed to a CCF.
- For RSA tokens, this service is routed to an ACTIVE PCICC if available for both CRT and ME tokens.
  - Exception for an ME token if modulus length is <512 bits.
  - If no PCICC is available, this service is routed to CCF. The service will fail for CRT tokens.
- The target key identifier may be a labelname, in which case the imported key is written directly to the PKDS.

B.1.4 PKA Public Key Extract (CSNDPKX)

- This service now executes in the ICSF address space (previously it executed in the caller's address space). RACF checking of service call, pre-processing, and post-processing exits are now enabled.
- The new CRT and ME tokens are supported.
- PKDS labelname is now supported for source key identifier.
- If labelname is used, the caller must be in task mode (not SRB mode).
- A new CSNDPKX stub module is shipped, but the old stub and the new stub will both call the new service module.
- This is not a cryptographic function; it executes in ICSF.

B.1.5 Digital Signature Generate (CSNDDSG)

- This service now supports the new CRT and ME tokens and retained keys.
- Routing of this service depends on the form of the input private key identifier, as follows:
  - If the source is a DSS token - route to CCF.
  - If the source is an RSA token:
    - ME x'02' - route to CCF.
    - CRT - route to PCICC.
    - ME x'06' - use round robin to CCF and PCICC, if possible.
- For a rule array keyword of ZERO-PAD, the maximum hash length supported is 32 bytes.

B.1.6 Symmetric Key Generate (CSNDSYG)

- This service has a preference for PCICC, so that the symmetric key never appears in host storage.
- This service will be routed to an ACTIVE PCICC unless the modulus bit length < 512, or if no PCICC is available.

B.1.7 Symmetric Key Export (CSNDSYX)

- This service has a preference for PCICC in order that the symmetric key never appears in host storage
- Service will be routed to an ACTIVE PCICC unless the modulus bit length < 512, or if no PCICC is available.

B.1.8 Symmetric Key Import (CSNDSYI)

- This service has a preference for PCICC, so that the symmetric key never appears in host storage.
- CRT and retained keys are routed to PCICC.
- For ME x'02' tokens - route to CCF.
- For ME x'06' - route to PCICC if available; otherwise route to CCF if SMK = KMMK.

B.1.9 SET Block Compose (CSNDSBC)

- This service has a preference for PCICC, so that the symmetric key never appears in host storage.
- This service will be routed to an ACTIVE PCICC for OAEP processing unless the modulus bit length < 512, or if no PCICC is available.
- DES encryption and hashing are always executed on CCF.

B.1.10 SET Block Decompose (CSNDSBD)

- This service has a preference for PCICC, so that the symmetric key never appears in host storage.
- It the RSA token is ME x'02' - route to CCF.
- If the RSA token is CRT or retained key - route to PCICC for OAEP processing.
- If the RSA token is ME x'06' - route to PCICC, if available; otherwise route to CCF.
- DES encryption and hashing is always executed on CCF.

B.1.11 PKA Encrypt (CSNDPKE)

- This is an RSA public key function with no security requirements.
- This service is always routed to CCF for better performance for modulus bit length <= 1024 bits.

B.1.12 PKA Decrypt (CSNDPKD)

- This service support CRT and retained keys on PCICC.
  - For ME x'02' tokens or modulus bit length < 512 bits - route to CCF.
  - For ME x'06' - route to PCICC if available; otherwise route to CCF if SMK = KMMK.

B.1.13 PKDS callable services

PKDS callable services cannot be used to create/update/delete the PKDS records of retained keys. This is enforced in the PKDS Record Create/Write/Delete services (CSNDKRC, CSNDKRW, CSNDKRD).

B.2 New callable services

The following callable services have been added.

B.2.1 Retained Key Delete (CSNDRKD)

- This service will delete the PKDS record and retained key in the PCICC of the key label supplied.
- Delete must be done from the same domain as the creation of the retained key.
- This service will delete a record of a retained key in the PKDS even if there is no retained key in the specified PCICC.
- This service will also delete a retained key in the specified PCICC even if there is no PKDS record:
  - Use the FORCE keyword with the Serial Number in the rule array.

B.2.2 Retained Key List (CSNDRKL)

- This service returns a list of retained keys for each ACTIVE PCICC created in this domain.
- Each PCICC is identified with a /*serial number, followed by list of keylabels of retained keys in that PCICC. This structure differs from other CSNDRKL implementations, since other platforms do not support multiple PCICCs.

- You must supply a labelname mask, optionally terminated with a wild card symbol (*), to filter the list of labelnames returned.
- A mask of (*) will return all retained keys in all ACTIVE PCICCs created from that domain.

Appendix C. TKE host TCP/IP server setup

This appendix describes the TCP/IP setup and customization required for proper TKE and TKE host communication.

C.1 The main TCP/IP files to check and modify

At this point, we assume that your TCP/IP stack has already been installed and configured. This section discusses the parameters of interest for TKE communications.

Note: In the following examples, TCPIP has to be replaced by the high-level qualifier that you defined to your installation with the DATASETPREFIX statement in TCPI.DATA.

C.1.1 TCPIP.HOSTS.LOCAL

This file contains TCP/IP hosts IP addresses and their corresponding domain names. This is the Site Table, which is intended to replace or to complement the services provided by the Domain Name Server from which you are requesting IP address resolution. Note that this information is exploited by the TKE TCP/IP server for informational purposes only; messages in the server print file may be issued that mention the local host name and IP address.

As an example, following is the entry from our TCPIP.HOSTS.LOCAL file. Our TKE host is named MVN9 and has IP address 9.100.203.111.

```
HOST : 9.100.203.111 : MVN9 ::::
```

C.1.2 TCPIP.DATA

For standard servers and clients, the anchor configuration data set is the TCPIP.DATA data set. This is the main resolver configuration data set, with information on host name, domain origin, etc.

In addition it holds the TCPIPJOBNAME parameter (which identifies the TCP/IP stack to use), and the DATASETPREFIX parameter (which is used by the resolver code when allocating the other configuration data sets).

In our configuration, TCPIP.DATA contains these entries :

```
HOSTNAME  MVN9
DATASETPREFIX TCPIP.OMVS
TCPIPJOBNAME TCPIPOE
```

C.1.3 TCPIP.PROFILE

The PORT statement in the TCPIP.PROFILE file is used to declare reserved ports, that is, ports which cannot be attributed as a result of port request by any application. Only the application which runs with the jobname specifically indicated in the PORT statement can get access to the designated port.

In our configuration, we had the following entries in our TCPIP.PROFILE:

```
50003 TCP CSFTTCP           ; TKE server
```

This entry indicates that port 50003 is reserved for the exclusive use of job CSFTTCP, which starts the TKE TCP/IP server in the TKE host system. It also indicates that port 50003 will be used for communications via the TCP transport layer.

The modifications made in the TCPIP.PROFILE are taken into account by stopping and restarting the related TCP/IP stack, or are made dynamically by using the VARY TCPIP,OBEYFILE command. In order to bring a new PORT dynamically, we entered the port statement to be dynamically executed in TCPIP.TCPPARMS(OBEYTKE), as shown.

```
BROWSE    TCPIP.TCPPARMS(OBEYTKE) - 01.02           Line 00000000 Col 001 080
******************************** Top of Data *********************************
; ----------------------------------------------------------------------
; Reserve ports for the following servers.
PORT
 50003 TCP CSFTTCP    ; crypto TKE server
******************************* Bottom of Data *******************************
```

Then we issued the VARY TCPIP command followed by a D TCPIP,NETSTAT to check that the CSFTTCP port was actually dynamically reserved. Note that, since we had only one TCP/IP instance running in the system, we did not enter the TCP/IP task name in the commands.

```
V TCPIP,,OBEYFILE,TCPIP.TCPPARMS(OBEYTKE)
EZZ0060I PROCESSING COMMAND: VARY TCPIP,,OBEYFILE,TCPIP.TCPPARMS(OBE
YTKE)
EZZ0300I OPENED OBEYFILE FILE 'TCPIP.TCPPARMS(OBEYTKE)'
EZZ0309I PROFILE PROCESSING BEGINNING FOR 'TCPIP.TCPPARMS(OBEYTKE)'
EZZ0316I PROFILE PROCESSING COMPLETE FOR FILE 'TCPIP.TCPPARMS(OBEYTK
E)'
EZZ0053I COMMAND VARY OBEY COMPLETED SUCCESSFULLY
D TCPIP,,N,PORTL
EZZ2500I NETSTAT CS V2R8 TCPIPOE 637
PORT# PROT USER     FLAGS RANGE
00020 TCP  OMVS     D
00021 TCP  OMVS     DA
00023 TCP  OMVS     DA
00080 TCP  OMVS     DA
00111 TCP  OMVS     DA
50003 TCP  CSFTTCP DA
```

The change resulting from the OBEYFILE command is not carried across stopping and starting of the TCP/IP instance; therefore you must edit the TCPIP.PROFILE in order to permanently install the change.

C.2 TKE Host Transaction Program installation

The Host Transaction Program is the interface between the TKE workstation and the crypto coprocessors. It includes the following software components:

- The CSFTTCP started procedure, which invokes the Terminal Monitor Program which, in turn, executes the CSFTHTP3 REXX exec
- The CSFTHTP3 REXX exec, which is a member of CSF.SCSFCLI0 (where CSF can be another high-level qualifier specific to your installation).
- A parameter file CSFTPRM, used by the CSFTHTP3 exec
- The CSFTTKE module in the CSF.SCSFMOD0 library
- The so-called “Crypto Module (CM) Data Set”, which is used to maintain information about the crypto coprocessors in the configuration

C.2.1 CSFTTCP started procedure installation

CSFTTCP can be copied from SYS1.SAMPLIB into the procedure library of the installation and customized as per your installation requirements. In our installation we decided to implement the parameter file CSFTPRM as a member of our SYS1.PARMLIB.MVN9 data set, as follows.

```
//*******************************************************************
//CSFTTCP  PROC LEVEL=SYS1,MEMBER=CSFTHTP3,
//            CPARM=''
//CLIST    EXEC PGM=IKJEFT01,
//            TIME=1440,
//            PARM='EX ''&LEVEL..SCSFCLI0(&MEMBER)'' ''&CPARM'' EXEC'
//SYSPRINT  DD SYSOUT=*
//SYSEXEC   DD DSN=&LEVEL..SCSFCLI0,DISP=SHR
//SYSPROC   DD DSN=&LEVEL..SCSFCLI0,DISP=SHR
//SYSTSPRT  DD SYSOUT=*
//SYSTSIN   DD DUMMY
//TKEPARMS  DD DSN=&LEVEL..PARMLIB.&SYSNAME.(CSFTPRM),DISP=SHR
//*
//* CUSTOMIZE THE DSN TO BE TCPIP DATASET ON YOUR SYSTEM
//SYSTCPD   DD DISP=SHR,DSN=TCPIP.TCPPARMS(TCPDATOE)
```

Execution of the TKE Host Transaction Program must occur under External Security Manager control (in our case, RACF). A new facility profile, CSFTTKE, must be defined, and the user ID given to the started task must be permitted to the profile.

We created a user ID TKEUSER with a TSO segment but, for security purposes, with the NOPASSWORD attribute; that is, it is a “protected” user. (Note that we do not show the creation of the user catalog or any other specific user-related facilities that may be required by your installation policy.) In our case, we also had to permit TKEUSER to SYS1.PARMLIB so that the task can read the CSFTPRM file; see the following sample.

```
AU TKEUSER NOPASSWORD TSO(ACCTNUM(AX0000) PROC(IKJSYS) UNIT(SYSDA))
ADDSD 'TKEUSER.**' OWNER(SYS1) UACC(NONE)
PE 'SYS1.**' ACC(READ) ID(TKEUSER)
RDEFINE STARTED CSFTTCP.* STDATA(USER(TKEUSER))
SETROPTS RACLIST(STARTED) REFRESH
RDEFINE FACILITY CSFTTKE UACC(NONE) OWNER(SYS1)
PERMIT CSFTTKE CLASS(FACILITY) ID(TKEUSER)
SETROPTS CLASSACT(FACILITY)
SETROPTS RACLIST(FACILITY) REFRESH
```

An additional level of security can be implemented by defining the APPL class profile CSFTTKE in RACF, and by permitting to this profile the approved TKE users only (as individual RACF user IDs or as a RACF group).

```
SETROPTS CLASSACT(APPL)
SETROPTS RACLIST(APPL)
RDEFINE APPL CSFTTKE UACC(NONE)
PERMIT CSFTTKE CLASS(APPL) ID(userid or group) ACCESS(READ)
SETROPTS RACLIST(APPL) REFRESH
```

Note that if the RACF CSFSERV general resource class is active, the CSFTTCP user ID (TKEUSER, in our case) has to be permitted to CSFPCI and CSFPKCS. Information on these profiles can be found in 6.1, “RACF access control to ICSF services” on page 137.

```
PERMIT CSFPKSC CLASS(CSFSERV) ACC(READ) ID(TKEUSER)
PERMIT CSFPCI CLASS(CSFSERV) ACC(READ) ID(TKEUSER)
SETROPTS RACLIST(CSFSERV) REFRESH
```

C.2.2 The CSFTTKE module

The CSFTTKE command must be authorized in member IKJTSOxx of SYS1.PARMLIB (the CSFTTKE module resides in CSF.SCSFMOD0). The change to IKJTSOxx can be made dynamically by using the PARMLIB UPDATE(xx) command, where xx is the suffix of the modified IKJTSO member.

```
AUTHCMD NAMES(              /****** AUTHORIZED COMMANDS ***********/ +

CSFTTKE                    /* AUTHORIZE TKE SERVER              */ +
```

C.2.3 The CSFTHTP3 REXX exec

This exec resides in the CSF.SCSFCLI0 library. It is invoked by the CSFTTCP procedure and goes through an initialization phase before listening to the TKE request over the TCP/IP socket. During its initialization, CSFTHTP3 reads the parameter file designated in the TKEPARMS DD card of CSFTTCP, that is, SYS1.PARMLIB(CSFTPRM).

CSFTPRM has to be edited to indicate what CM data set to use and which TCPIP port to connect to. The default values are, respectively, &SYSNAME..TKECM and 50003. Our edited CSFTPRM is shown:

```
 BROWSE    SYS1.PARMLIB.MVN9(CSFTPRM) - 01.08        Line 00000000 Col 001 080
******************************** Top of Data *********************************
SET THE TKE DATA SETS;'TKEUSER.TKECM'
PORT;50003
SET DISPLAY LEVEL;TRACE ALL
******************************* Bottom of Data *******************************
```

Note that we selected the TRACE ALL options. Other options are TRACE NON-ZERO, which traces non-zero return codes obtained during the transactions, and TRANACTION TRACE, which traces transactions inputs and outputs. TRACE NON-ZERO is the default when no display level option is specified.

Note

We found that CSFTTCP fails if CSFTPRM contains sequence numbers in col 73 to 80. When editing CSFTPRM, ensure you have the sequence numbering on UNNUM.

C.3 Starting the TKE Host Transaction Program

We recommend that you perform a preliminary check of TCPIP connectivity using a simple PING command from any workstation that can reach the TKE host TCP/IP stack.

When you issue the START CSFTTCP command, CSFTTHTP3 is started and then listens for any incoming TCP/IP request.

Miscellaneous information, complemented with trace entries if tracing is active, is found in the SYSTSPRT DD data set, as shown in the following sample.

```
CSFTHTP3 started at 19 Apr 2000, 09:50:54.
  Generic user id.:       TKEUSER
  CM   dataset:           'TKEUSER.TKECM'
  RACF environment:       "Cipher"
  TCP/IP port:            50003
  Display level           "Trace all"
==============================================================================
19 Apr 2000 09:50:55 SocketSetList: ReturnCode=0, SocketSetList: ''
Misc. host info:
  REXX/SOCKETS version  = REXX/SOCKETS CS V2R6 APR 17,1998
  Domain name           =
  Host Id (ipaddress)   = 9.100.203.111
  Host Name             = MVN9
  Fully qual. host name = MVN9
  Job id.               = CSFTTCP syslog start csfttcp
```

Appendix D. Special notices

This publication is intended to help systems programmers and security personnel enable the S/390 PCICC. The information in this publication is not intended as the specification of any programming interfaces that are provided by the OS/390 operating system. See the PUBLICATIONS section of the IBM Programming Announcement for the OS/390 operating system for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

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.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

This document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

IBM ®
PR/SM
RACF
RETAIN
RS/6000
S/390
SecureWay
SP
SP1
System/390
VTAM
400
Lotus
Notes

The following terms are trademarks of other companies:

Tivoli, Manage. Anything. Anywhere.,The Power To Manage., Anything. Anywhere.,TME, NetView, Cross-Site, Tivoli Ready, Tivoli Certified, Planet Tivoli, and Tivoli Enterprise are trademarks or registered trademarks of Tivoli Systems Inc., an IBM company, in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer - Tivoli A/S.

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Appendix E. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

E.1 IBM Redbooks publications

For information on ordering these publications see “How to get IBM Redbooks” on page 157.

- *Fiber Channel (FICON) Implementation Planning*, SG24-5445
- *Exploiting S/390 Hardware Cryptography with Trusted Key Entry*, SG24-5455

E.2 IBM Redbooks collections

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at http://www.redbooks.ibm.com/ for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	**Collection Kit Number**
System/390 Redbooks Collection	SK2T-2177
Networking and Systems Management Redbooks Collection	SK2T-6022
Transaction Processing and Data Management Redbooks Collection	SK2T-8038
Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
AS/400 Redbooks Collection	SK2T-2849
Netfinity Hardware and Software Redbooks Collection	SK2T-8046
RS/6000 Redbooks Collection (BkMgr)	SK2T-8040
RS/6000 Redbooks Collection (PDF Format)	SK2T-8043
Application Development Redbooks Collection	SK2T-8037
IBM Enterprise Storage and Systems Management Solutions	SK3T-3694

E.3 Other resources

These publications are also relevant as further information sources:

- *Common Cryptographic Architecture: Cryptographic Application Programming Interface Reference,* SC40-1675
- *Support Element Operations Guide*, GC38-0608
- *ICSF System Programmer’s Guide*, SC23-3974
- *Workstation Maintenance***,** GC38-3115
- *PR/SM Planning Guide*, GA22-7236
- *Security Server (RACF) Security Administrator’s Guide,* SC28-1915
- *TKE Workstation User’s Guide 2000*, GA22-7430

E.4 Referenced Web site

This Web site is also relevant as a further information source:

- `http://csrc.ncsl.nist.gov/cryptval/140-1/1401val.htm`

How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about IBM Redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** http://www.redbooks.ibm.com/

  Search for, view, download, or order hardcopy/CD-ROM Redbooks from the Redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this Redbooks site.

  Redpieces are Redbooks in progress; not all Redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

  Send orders by e-mail including information from the IBM Redbooks fax order form to:

	e-mail address
In United States	usib6fpl@ibmmail.com
Outside North America	Contact information is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the Redbooks Web site.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and Redbooks by accessing the IBM Intranet Web site at http://w3.itso.ibm.com/ and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access MyNews at http://w3.ibm.com/ for redbook, residency, and workshop announcements.

IBM Redbooks fax order form

Please send me the following:

Title	**Order Number**	**Quantity**

First name	Last name	
Company		
Address		
City	Postal code	Country
Telephone number	Telefax number	VAT number

□ Invoice to customer number

□ Credit card number

Credit card expiration date	Card issued to	Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Index

A

Adjunct Processor 9
Advanced Facilities 51
AIX 1
asymmetric-keys 71
ASYM-MK 71
authority definition 53

B

Battery 16
BSAFE 4

C

callable service 29
CCA 2, 22
CCF 9, 10, 25, 31, 84
CDMF 71
CD-ROM 33
CEC 10
Central Processor 43
CHA 43
CHPID 11
CHPID reset 51
CKDS 5, 26
CKDSN 83
CMOS 3
Code-Signing Key 23
Control domain index 65
Control Vector 2
Coupling Links 44
CP/Q 22
CPC 61
CRT 141
crypto module 53
Cryptographic Key Data Set 5
CSFSERV 137
CSFTPRM 147
CSFTTCP 147
CSFTTKE 148
CSNDPKX 142
CSNDRKL 143
CV 2
CW/CVC 4

D

Data Confidentiality 1
Data integrity 1
dedicated central processor 64
DES 3, 6, 70
DES key 71
DES Master key 79
device status 26
Diffie-Hellman 6
digital signature 4, 6
Digital Signature Standard 29
diskette 24
Domain 6, 68
domain 53
Double Key MAC 4
DSS 3, 29, 141

E

Enable cryptographic functions 66
Enable Integrated Cryptographic Facility (ICRF) key entry 66
Enable modify authority 66
Enable public key algorithm (PKA) facility 65
Enable Public Key Secure Cable (PKSC) and the integrated cryptographic service facility 66
Enable query signature controls 66
Enable query transport controls 66
Enable special security mode 66
Enhanced Pass Phrase 26
ESCON 36

F

FCV 6, 21, 36, 56
Feature Code 32
FIB 11
FIBB 43
FICON 36
FIPS-4 15
FRU 17
Function Control Vector 32

H

Hard Tamper 15
hardware 32
Hardware status display 73
hashing algorithms 3

HCRP230 26
HMC 33
hotplugged PCICC card 51
HSA 19, 25

I
I/O cage 45
I/O domain 47
I/O slot 46
IBM Integrated Cryptographic Facility 1
IBM Transaction Security System 1
ICB 49
ICRF 1, 4
ICSF 5, 6, 142
ICSF/MVS 1
IEASYM 69
Image Profile 64
IML 20
Impor 24
Integrated Cluster Buses 44
Integrated Cryptographic Services Facility/MVS 1
Internal Coupling Facility 43
Intersystem Channel Adapter 44
Intrusion Latch 16
IO Supervisor 25
IOCDS 36

K
Key Management 1
Key Separation 2

L
LIC 6
logical crypto coprocessor 64
logical partition 64
LPAR 55
LPAR image 36

M
MAC 29
Master Key 71
Master Key Concept 1
MasterCard 26
MBA 42
MDC 29
Memory Bus Adapter 42
MES 17, 34, 55
MES upgrade 50
Miniboot 22
MVN9 145

N
NOPASSWORD 70

O
OAEP 142
OBEYTKE 146
Online List 67
OPK 3
Option Data Set 7
OS/390 1
OS/390 R9 56
OS/390 V2R9 10
OS/400 1
OSA-2 11
OSA2 36

P
Pass Phrase 77
PCICC 10, 55, 84
Personal Authentication 1
personal identification number 29
PIN 29
PING 149
PKA 65, 74
PKA Key management 3
PKDS 5, 141, 143
PORT 145
Power On 20, 34
PPINIT 72
PR/SM 7, 8, 61
Private Key Data Set 5
PSC 53
Pseudo Random Number Generation 3
public key algorithm 65
Public Key Algorithms (RSA) 4

R
RACF 137, 142, 147
REASONCODE 29
REENCHIPER 80
RESET 84
Retained key 27
routing 27

RSA 3, 4, 21, 29, 141

S

Sales Ordering System 36
SAP 43
SE 20
SecureWay 3
segment 23
SET 4
signature key 53
SMF 29
Soft Tamper 16
STI 34
STI chain 44
SUL-ROC 34
Support Element 25, 61
symmetric-keys 71

T

TCP/IP 30, 145, 149
TDES 36
Thermal container 18
thermal container 18
thermal gel 18
TKE 8, 9, 55, 71
TKE Workstation 6
Toggle 56
Triple DES 3
TSO 30, 147
TSO/E ISPF 26

U

UDX 21
Usage domain index 65
User Defined Extension 21
USERCNTL 84

V

VBAT 15
Visa 26
Visa/Mastercard CW/CVC card-verification 4

X

X-ray exposure 15

Z

zeroize 17
ZERO-PAD 142

IBM Redbooks review

Your feedback is valued by the Redbook authors. In particular we are interested in situations where a Redbook "made the difference" in a task or problem you encountered. Using one of the following methods, **please review the Redbook, addressing value, subject matter, structure, depth and quality as appropriate.**

- Use the online **Contact us** review redbook form found at `http://www.redbooks.ibm.com/`
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to `redbook@us.ibm.com`

Document Number **Redbook Title**	SG24-5942-00 S/390 Crypto PCI Implementation Guide
Review	
What other subjects would you like to see IBM Redbooks address?	
Please rate your overall satisfaction:	○ Very Good ○ Good ○ Average ○ Poor
Please identify yourself as belonging to one of the following groups:	○ Customer ○ Business Partner ○ Solution Developer ○ IBM, Lotus or Tivoli Employee ○ None of the above
Your email address: The data you provide here may be used to provide you with information from IBM or our business partners about our products, services or activities.	 ○ Please do not use the information collected here for future marketing or promotional contacts or other communications beyond the scope of this transaction.
Questions about IBM's privacy policy?	The following link explains how we protect your personal information. `http://www.ibm.com/privacy/yourprivacy/`

SG24-5942-00
Printed in the U.S.A.

S/390 Crypto PCI Implementation Guide

SG24-5942-00