IBM @server

IBM

IBM @server zSeries 990 (z990) Cryptography Implementation

- PCIXCC and PCICA installation and customization
- Overview of CPACF
- Review of TKE V4

Chris Rayns
Marilyn F. Allmond
Laurent Boudon
Pekka Hanninen
Patrick Kappeler
Robert Malaval
Vicente Ranieri Jr.
Paul Sheils

Archived

Redbooks

ibm.com/redbooks

Archived

International Technical Support Organization

IBM @server zSeries 990 (z990) Cryptography Implementation

August 2004

Archived

SG24-7070-00

Note: Before using this information and the product it supports, read the information in “Notices” on page vii.

Archived

First Edition (August 2004)

This edition applies to z/OS Version 1, Release 4.

© Copyright International Business Machines Corporation 2004. All rights reserved.
Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices vii
Trademarks viii

Preface ix
The team that wrote this redbook ix
Become a published author xi
Comments welcome xi

Chapter 1. Introduction 1
1.1 Cryptographic function support 2
1.1.1 Cryptographic Synchronous functions 2
1.1.2 Cryptographic Asynchronous functions 2
1.2 z990 Cryptographic processors 4
1.2.1 CP Assist for Cryptographic Function (CPACF) 4
1.2.2 PCI Extended Cryptographic Coprocessor (PCIXCC) 5
1.2.3 PCI Cryptographic Accelerator (PCICA) feature 6
1.3 Cryptographic hardware features 8
1.3.1 PCIX Cryptographic Coprocessor feature 8
1.3.2 The PCICA feature 9
1.3.3 Configuration rules 9
1.3.4 z990 cryptographic feature codes 10
1.4 Integrated Cryptographic Services Facility 10
1.4.1 CKDS and PKDS 12
1.4.2 TKE workstation feature 12
1.5 Cryptographic features comparison 13
1.6 Software requirements 15

Chapter 2. CPACF, PCICA, and PCIXCC product overview 17
2.1 Description of hardware 18
2.1.1 Definitions 18
2.1.2 Hardware implementation 18
2.1.3 Introduction to the z990 PCIXCC, PCICA and CPACF 22
2.1.4 PCXICC card: physical security, handling, and shipping 32
2.2 Adjunct Processor (AP) management 37
2.2.1 Introduction to Adjunct Processor architecture 37
2.2.2 AP management and PCIXCC initialization 38
2.3 PCIXCC microcode load 40
2.3.1 The IBM 4758 CCA application 40
2.3.2 The software hierarchy in the coprocessor 41

© Copyright IBM Corp. 2004. All rights reserved.

2.3.3 Software requirements: cryptographic functions and hardware 42
2.3.4 The TKE V4 workstation 42

Chapter 3. Planning and hardware installation 45
3.1 Hardware requirements 46
3.1.1 Hardware required for z990 46
3.2 Feature codes 48
3.3 Concurrent PCIXCC/PCICA installation tasks 50
3.3.1 Concurrent Install on z990 50
3.3.2 Removing one PCIXCC 56
3.4 Planning list items 57

Chapter 4. PCIXCC using TKE V4 59
4.1 Introduction to the TKE V4 Workstation 60
4.1.1 Major changes 60
4.1.2 Before using the new TKE 64
4.1.3 The TKE V4 software 65
4.1.4 TKE workstation installation - general information 65
4.1.5 TKE definitions 66
4.2 TKE workstation TCP/IP setup 68
4.2.1 TKE workstation 4758 setup 72
4.2.2 TKE access control administration 74
4.2.3 Starting the TKE application 81
4.3 TKE application: managing host Crypto coprocessors 82
4.3.1 Managing modules 82
4.3.2 PCIXCC setup on the TKE workstation 86
4.3.3 Manage and update the Crypto module notebook on TKE 95
4.3.4 PCIXCC module notebook 103
4.3.5 Backing up the TKE files 141
4.4 4753 Key Token Migration facility 143

Chapter 5. ICSF support for CPACF, PCIXCC, and PCICA 145
5.1 CP Assist for Cryptographic Functions (CPACF) feature 146
5.2 LPAR setup 148
5.2.1 Planning considerations 148
5.2.2 The image profile processor page 148
5.2.3 The PCI Crypto page 151
5.2.4 Viewing LPAR Cryptographic Controls 156
5.3 PCIXCC and PCICA feature installation 157
5.3.1 PCIXCC and PCICA enablement 157
5.3.2 Configuring and monitoring the status of PCIXCC and PCICA 162
5.3.3 Security issues with the PCI Cryptographic cards 167
5.4 Integrated Cryptographic Services Facility (ICSF) setup 170
5.4.1 Changes from previous release 170

5.4.2 Started task and the first time start 171
5.4.3 Master Keys 171
5.4.4 Initial Master Key entry with the pass phrase initialization utility . . . 172
5.4.5 Installation of a new PCIXCC or PCICA card 177
5.4.6 PKDS initialization 178

Chapter 6. Performance and monitoring 183
6.1 z990 Crypto hardware performance considerations 184
6.2 Monitoring and reporting 185
6.2.1 RMF reporting 185
6.2.2 ICSF SMF records 193
6.2.3 Example using RMF and SMF data 197

Appendix A. Exploiters 201
A.1 The APIs 202
A.2 Overview of the IBM exploiters 206
A.2.1 z/OS Open Cryptographic Services Facility (OCSF) 209
A.2.2 IBM HTTP Server for z/OS 209
A.2.3 z/OS LDAP server and client 210
A.2.4 CICS Transaction Server and CICS Transaction Gateway 210
A.2.5 z/OS TN3270 server 210
A.2.6 z/OS Firewall Technologies 210
A.2.7 GSKKYMAN 211
A.2.8 z/OS DCE 211
A.2.9 z/OS Network Authentication Service (Kerberos) 211
A.2.10 Payment processing products 211
A.2.11 VTAM Session Level Encryption 212
A.2.12 RACF 212
A.2.13 z/OS Public Key Infrastructure (PKI) services 212
A.2.14 Crypto Based Transactions (CBT) banking solution 212
A.2.15 Java cryptography 213

Related publications 215
IBM Redbooks 215
Other publications 215
Online resources 215
How to get IBM Redbooks 216
Help from IBM 216

Index 217

Archived

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described 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:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

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

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include 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.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

© Copyright IBM Corp. 2004. All rights reserved.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

CICS®
FICON®
IBM Payment Gateway™
IBM®
MVS™
OS/2®
OS/390®
Parallel Sysplex®
PowerPC®
PR/SM™
Redbooks™
Redbooks (logo) ™
RACF®
RETAIN®
RMF™
S/390®
VSE/ESA™
VTAM®
WebSphere®
z/OS®
z/VM®
zSeries®

The following terms are trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Intel, Intel Inside (logos), and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Archived

Preface

The IBM z990 includes both standard cryptographic hardware and optional cryptographic features, to give flexibility and growth capability. IBM® has a long history of providing hardware cryptographic solutions, from the development of Data Encryption Standard (DES) in the 1970s to delivering the only integrated cryptographic hardware in a server to achieve the US Government's highest FIPS 140-2 Level 4 rating for secure cryptographic hardware.

This IBM Redbook is designed to help you understand and implement the z/OS® cryptographic PCIXCC and PCICA cards. Although this book focuses on the enablement of the z/OS PCIXCC and PCICA products, cryptography and the available services on z/OS are also discussed and explained, with special attention given to the new Trusted Key Entry (TKE V4) workstation.

This book also reviews the tools that are available on z/OS for monitoring of z990 cryptographic hardware utilization, plus the analysis of performance.

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, Montpellier Benchmarking Center.

Chris Rayns is a Security Project Leader at the International Technical Support Organization, Poughkeepsie Center. He writes extensively and teaches IBM classes worldwide on all areas of Security.

Marilyn Frazier Allmond is a Certified IT Specialist with IBM Americas Advanced Technical Support with the Washington Systems Center. With close to 30 years in IBM, Marilyn has a broad background in IT from development, marketing support, and system security analysis, to technical support for the mainframe cryptographic hardware and ICSF. She has many years of security experience on IBM mainframes covering design, code, implementation, and operational issues. She has supported the mainframe crypto since 1989, working with clients across many industries. She developed the training course ES801. Marilyn has mentored, taught, and provided services in the crypto area worldwide.

Laurent Boudon is a Product Engineer in the Montpellier support structure for zSeries®. He has six years of experience in IBM zSeries systems test and field

© Copyright IBM Corp. 2004. All rights reserved.

support in the processor, memory, and code area. His main focus today is to work in cooperation with the labs to investigate customers' problems, but also to participate in product development in the crypto code and CEC domain. He is also involved in new product field education and implementation of customer configurations.

Pekka 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 security administration. 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 support 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.

Vicente Ranieri Jr. is an IBM Senior Certified Professional and Consultant I/T Specialist in Brazil supporting customers across Latin America. He has 25 years of experience working with IBM customers, 18 of which were devoted to providing technical consulting in S/390 and zSeries platforms. He writes extensively and teaches IBM classes worldwide in all areas of zSeries security. He holds a postgraduate degree in Marketing Administration from Fundacao Getulio Vargas (EAESP-FGV), Brazil.

Paul Sheils is a zSeries Specialist in the UK. He has worked for IBM for four years. He has 20 years of experience working in IT, mainly on IBM Large Systems. His areas of expertise include z/OS and Parallel Sysplex®.

Thanks also to the following people for their support.

Robert Haimowitz
International Technical Support Organization, Poughkeepsie Center

Richard Conway
International Technical Support Organization, Poughkeepsie Center

Donyelle Mahler, Crypto Test
IBM Poughkeespie

Lucina Green, ICSF Development
IBM Poughkeepsie

Alfred Schwab, editor
International Technical Support Organization, Poughkeepsie Center

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

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

- Use the online **Contact us** review redbook form found at:

  ibm.com/redbooks

- Send your comments in an Internet note to:

  redbook@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYJ Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Archive

Archived

1

Introduction

This chapter provides an overview of the Cryptography functions of the z990. On the z990, a new cryptographic architecture is introduced. The new Cryptographic Assist Architecture (CAA), along with the CP Assist for Cryptographic Function, offers a balanced use of resources and unmatched scalability.

Included in this chapter are:

- "Cryptographic function support" on page 2
- "CP Assist for Cryptographic Function (CPACF)" on page 4
- "PCI Extended Cryptographic Coprocessor (PCIXCC)" on page 5
- "PCI Cryptographic Accelerator (PCICA) feature" on page 6
- "Cryptographic hardware features" on page 8
- "Cryptographic features comparison" on page 13
- "Software requirements" on page 15

© Copyright IBM Corp. 2004. All rights reserved.

1.1 Cryptographic function support

The z990 includes both standard cryptographic hardware and optional cryptographic features, to give flexibility and growth capability. IBM has a long history of providing hardware cryptographic solutions, from the development of Data Encryption Standard (DES) in the 1970s to delivering the only integrated cryptographic hardware in a server to achieve the US Government's highest FIPS 140-2 Level 4 rating for secure cryptographic hardware.

The z990 cryptographic functions include the full range of cryptographic operations needed for e-business, e-commerce, and financial institution applications. In addition, custom cryptographic functions can be added to the set of functions that the z990 offers.

Today, e-business applications are increasingly relying on cryptographic techniques to provide the confidentiality and authentication required in this environment. Secure Sockets Layer (SSL) technology is a key technology for conducting secure e-commerce using Web servers, and it is in use by a rapidly increasing number of e-business applications that demand new levels of security and performance.

1.1.1 Cryptographic Synchronous functions

For clear key functions only, the hardware includes implementation of the following:

- Data encryption/decryption algorithms
  - Data Encryption Standard (DES)
  - Double length-key DES
  - Triple length- key DES
  - AES
- Hashing algorithms SHA-1

1.1.2 Cryptographic Asynchronous functions

For secured key functions, Cryptographic Asynchronous functions process messages that are passed to it.

- Data encryption/decryption algorithms
  - Data Encryption Standard (DES)
  - Double length-key DES
  - Triple length- key DES

Archive

- DES key generation and distribution
- PIN generation, verification and translation functions
- Pseudo Random Number (PRN) Generator
- Message authentication code (MAC): single-key MAC and double-key MAC
- Public Key Algorithm (PKA) Facility

  These commands are intended for application programs using public key algorithms, including:

  - Importing RSA public-private key pairs in clear and encrypted forms
  - Rivest-Shamir-Adelman (RSA)
    - Key generation, up to 2048-bit
    - Signature Verification, up to 2048-bit
    - Import and export of DES keys under an RSA key, up to 2048-bit

Other key functionality of a cryptographic processor serves to enhance the security of public/private key encryption processing:

- Retained key support (RSA private keys generated and kept stored within the secure hardware boundary)
- User Defined Extensions (UDX) support enhancements, including:

  For the Activate UDX request

  - Import UDX File function
  - Reset UDX to IBM default function
  - Query UDX Level function

  UDX allows the user to add customized operations to a cryptographic processor. User Defined Extensions to the Common Cryptographic Architecture (CCA) support program, which executes within the PCIX Cryptographic Coprocessor, will be supported via an IBM Service Offering.

  For unique customer applications, the PCIX Cryptographic Coprocessor will support the loading of customized cryptographic functions on z990. Support is available via ICSF and the z990 Cryptographic Support.

  The cryptocards Web site at:

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

  directs the customer's request to an IBM Global Services (IGS) location appropriate for the customer's geographic location. A special contract will be negotiated between IGS and the customer, covering development of the UDX by IGS per the customer's specifications, as well as an agreed-upon level of the UDX.

Archived

Under a special contract with IBM, PCIX Cryptographic Coprocessor customers will gain the flexibility to define and load custom cryptographic functions themselves. This service offering can be requested via the IBM Cryptocards Web site by selecting the **Custom Programming** option.

- Additional support for 4753 Network Security Processor migration

1.2 z990 Cryptographic processors

Three types of cryptographic hardware features are available on z990. The cryptographic features are usable only when explicitly enabled through IBM.

1.2.1 CP Assist for Cryptographic Function (CPACF)

Each CP has an assist processor on the chip in support of cryptography. The CP Assist for Cryptographic Function (CPACF) provides high performance hardware encryption and decryption support. To that end, the following five new instructions are introduced with the cryptographic assist function:

- KMAC - Compute Message Authentic Code
- KM - Cipher Message
- KMC - Cipher message with chaining
- KIMD - Compute Intermediate Message Digest
- KLMD - Compute Last Message Digest

The CP Assist for Cryptographic Function provides high performance hardware encryption and decryption support.

The CP Assist for Cryptographic Function offers a set of symmetric cryptographic functions that enhance the encryption and decryption performance of clear key operations for SSL, VPN and data storing applications that do not require FIPS 140-2 level 4 security. The cryptographic architecture includes DES, T-DES data encryption and decryption, MAC message authorization and SHA-1 hashing. These functions are directly available to application programs, diminishing programming overhead.

The CP Assist for Cryptographic Function complements, but does not execute, public key (PKA) functions, and it is a prerequisite for the secure cryptographic operations provided by the PCIX Cryptographic Coprocessor (PCIXCC) feature, and the PCI Cryptographic Accelerator (PCICA) feature. The CP Assist for Cryptographic Function runs at z990 processor speed, and since the facility is available on every CP in the system, there are no affinity issues as in earlier CMOS processors.

Archived

The functions of the CP Assist for Cryptographic Function must be enabled or disabled by the manufacturing process to conform to United States export requirements.

1.2.2 PCI Extended Cryptographic Coprocessor (PCIXCC)

The optional Peripheral Component Interconnect Extended Cryptographic Coprocessor provides a high performance cryptographic environment with added function. In fact, the PCIX Cryptographic Coprocessor consolidates the functions previously offered on the z900 by the Cryptographic Coprocessor feature (CCF) and the PCI Cryptographic Coprocessor (PCICC) feature. CCF and PCICC features are not available on the z990. The PCIXCC feature provides asynchronous functions only.

The PCIXCC feature is designed for FIPS 140-2 Level 4 compliance rating for secure cryptographic hardware. Unauthorized removal/reinsertion of the card or feature will zeroize its content.

The PCIX Cryptographic Coprocessor features on the z990 enable the user to do the following:

- Encrypt and decrypt data utilizing secret key algorithms. Triple-length key DES and double-length key DES algorithms are supported.
- Generate, install, and distribute cryptographic keys securely using both public and secret key cryptographic methods.
- Generate, verify, and translate personal identification numbers (PINs).
- Ensure the integrity of data by using message authentication codes (MACs), hashing algorithms, and Rivest-Shamir-Adelman (RSA) public key algorithm (PKA) digital signatures.

Three methods of master key entry are provided by ICSF for the PCIX Cryptographic Coprocessor features:

1. A pass phrase initialization method that generates and enters all master keys that are necessary to fully enable the cryptographic system in a minimal number of steps.
2. A simplified master key entry procedure provided through a series of Clear Master Key Entry panels from a TSO terminal.
3. In enterprises that require enhanced key-entry security, a Trusted Key Entry (TKE) workstation is available as an optional feature.

The security-relevant portion of the cryptographic functions is performed inside the secure physical boundary of a tamper-resistant card. Master keys and other security-relevant information are also maintained inside this secure boundary.

Archive

The PCIXCC features operate with the Integrated Cryptographic Service Facility (ICSF) and IBM Resource Access Control Facility (RACF), or equivalent software products, in a z/OS or OS/390® operating environment to provide data privacy, data integrity, cryptographic key installation and generation, electronic cryptographic key distribution, and personal identification number (PIN) processing.

IBM Processor Resource/System Manager (PR/SM™) fully supports the PCIX Cryptographic Coprocessor features to establish a logically partitioned environment in which multiple logical partitions can use the cryptographic functions. A 128-bit data-protection master key, and one 192-bit Public Key Algorithm (PKA) master key are provided for each of 16 cryptographic domains.

1.2.3 PCI Cryptographic Accelerator (PCICA) feature

The Peripheral Component Interconnect Cryptographic Accelerator (PCICA) is an orderable feature on z990. This optional feature is a reduced-function, performance-enhanced addition to the CPACF and the PCIX Cryptographic Coprocessor with reduced functional characteristics. It does not have FIPS 140-2 level 4 certification and is non-programmable.

The PCICA feature is used for the acceleration of modular arithmetic operations, in particular the complex RSA cryptographic operations used with the SSL protocol.

This is a unique cryptographic feature for SSL encryption. It has a very fast cryptographic processor designed to provide leading-edge performance of the complex Rivest-Shamir-Adelman (RSA) cryptographic operations used in the SSL protocol. In essence it is for SSL acceleration rather than for specialized financial applications for secure, long-term storage of keys or secrets. SSL is an essential and widely used protocol in secure e-business applications.

Since the PCI Cryptographic Accelerator is only involved in clear key operations, it does not need the tamperproof design of the PCIXCC feature.

The PCICA feature provides functions designed for maximum acceleration of the complex RSA cryptographic operations used with the SSL protocol, including:

- High-speed RSA cryptographic accelerator
- 1024- and 2048-bit RSA operations for the Modulus Exponent (ME) and Chinese Remainder Theorem (CRT) formats.

The maximum number of SSL transactions per second that can be supported on a z990 by any combination of CPACF and PCICA features is limited by the amount of cycles available to perform the software portion of the SSL transactions. An IBM 2084 model B16 with 16 CPs active and six PCICA features is designed to provide increased secure Web transaction performance.

In the z, there can be a maximum of six PCI Cryptographic Accelerator (PCICA) features (two per I/O cage), along with a maximum of four PCIX Cryptographic Coprocessor features. The combined number of PCIXCC and PCICA features on a z990 cannot exceed eight. Within these parameters, the PCXICC and PCICA features can coexist in any combination. This scalability provides increasing cryptographic processing capacity as customers expand their use of e-business applications requiring cryptographic processing.

See Figure 1-1 on page 7 for an overview of the z990 using CPACF and PCIXCC.

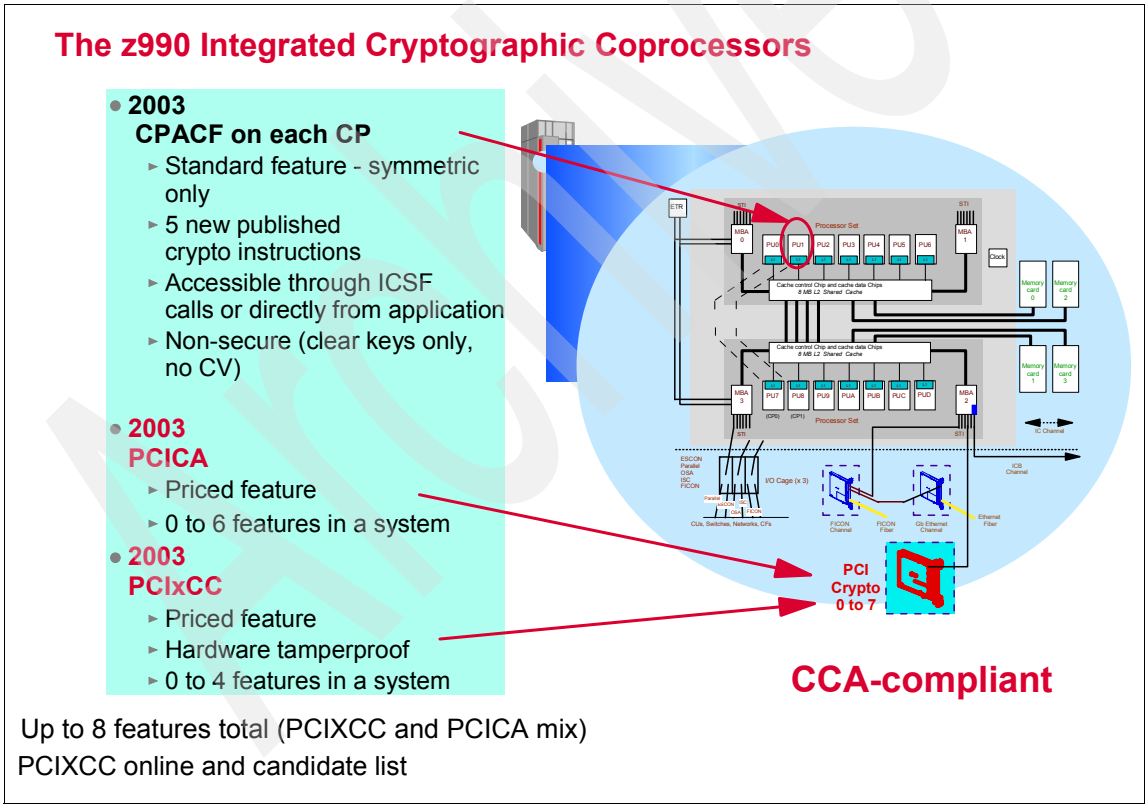

Figure 1-1 Overview of z990 with CPACF and PCIXCC

1.3 Cryptographic hardware features

This section describes the three cryptographic hardware features and the feature codes associated with the cryptographic functions of the z990.

Important: Products which include any of the cryptographic feature codes contain cryptographic functions that are subject to special export licensing requirements by the United States Department of Commerce. It is the customer's responsibility to understand and adhere to these regulations whenever moving, selling, or transferring these products.

1.3.1 PCIX Cryptographic Coprocessor feature

Each PCIX Cryptographic Coprocessor feature contains one cryptographic coprocessor card. The z990 allows for up to four PCIXCC features (or cards) to be installed.

Note: The PCIX Cryptographic Coprocessor feature became available on September 19, 2003.

The card is attached to an STI and has no other external interfaces. Removal of the card or feature zeroizes the content. A physical layout of the PCIXCC card is shown in Figure 1-2.

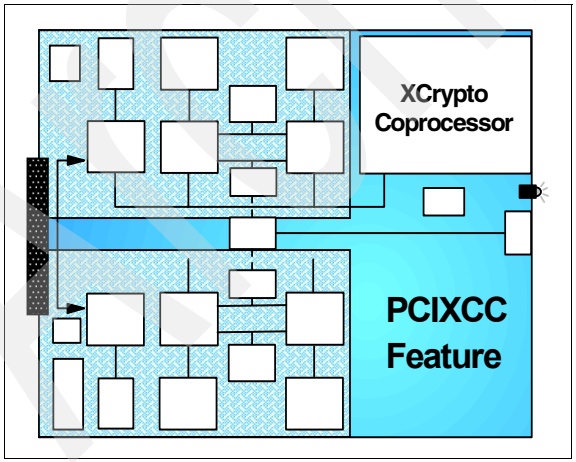

Figure 1-2 PCIX Cryptographic Coprocessor card

The PCIX Cryptographic Coprocessor feature does not use a CHPID, but is assigned a PCHID.

1.3.2 The PCICA feature

Each PCI Cryptographic Accelerator feature contains two cryptographic accelerator cards. The physical layout of the PCICA feature is illustrated in Figure 1-3 on page 9.

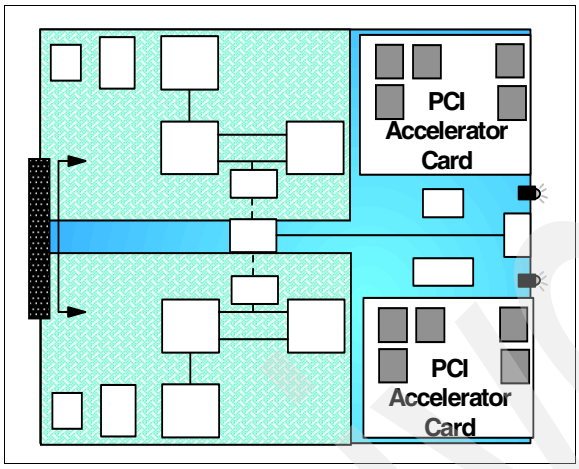

Figure 1-3 PCI Cryptographic Accelerator feature

Each PCICA feature has two cryptographic accelerator cards embedded in an adapter package for installing in I/O slots of the z990 cage. The PCICA feature does not have ports and does not use fiber optic or other cables. The PCICA cards can be shared by any logical partition defined in the system up to 15 logical partitions per card, or 30 logical partitions per feature.

The PCICA feature does not use CHPIDs, but is assigned two PCHIDs (one per accelerator card).

1.3.3 Configuration rules

The following configuration rules apply:

- The z990 allows for up to two PCICA features per I/O cage. This allows for a maximum of six PCICA features or twelve PCICA coprocessors per z990 server.
- The maximum number of PCIXCC features (or cryptographic coprocessors) per I/O cage is four; the maximum number of PCIXCC features per z990 server is also four.
- The total number of cryptographic features may not exceed eight per z990 for any combination of PCIXCC and PCICA features.

Archived

- In addition, any combination of PCIXCC, PCICA, OSA-Express and FICON®-Express features may not exceed 20 features per I/O cage, or 60 features per z990 server.

1.3.4 z990 cryptographic feature codes

Following is a list of the cryptographic features available with the z990:

Feature code	Description
3863	Crypto enablement Crypto enablement feature. Prerequisite to use the CPACF, PCIXCC, and PCICA hardware features.
0868	PCIX Cryptographic Coprocessor (PCIXCC) feature
0862	PCI Cryptographic Accelerator (PCICA) feature
0886	TKE 4.0 hardware for Token Ring TKE workstation hardware with Token Ring connection, DVD drive, and 17-inch monitor.
0889	TKE 4.0 hardware for Ethernet TKE workstation hardware with Token Ring connection, DVD drive, and 17-inch monitor.

Note: The z990 requires a TKE Version V4 workstation. If a z900 with TKE Version 3.x workstations is upgraded to a z990, the TKE Version 3.x workstations can be retained to control other servers—but cannot be used on the z990.

The TKE Version V4 workstation itself supports all models back to CCF support on a G3 CMOS processor.

1.4 Integrated Cryptographic Services Facility

ICSF is a software element of z/OS that works with the hardware cryptographic feature and the Security Server (RACF) to provide secure, high-speed cryptographic services in the z/OS environment. ICSF provides the application programming interfaces by which applications request the cryptographic services.

ICSF supports the IBM Common Cryptographic Architecture (CCA). The CCA is based on the ANSI Data Encryption Algorithm (DEA). DEA is also known as the U.S.National Institute of Science and Technology Data Encryption Standard (DES) algorithm.

Archived

ICSF also supports triple DES encryption for data privacy. Triple DES uses three single-length keys to encipher and decipher the data. This results in a stronger form of cryptography than that available with single DES encipherment.

Figure 1-4 illustrates how ICSF works with other IBM software.

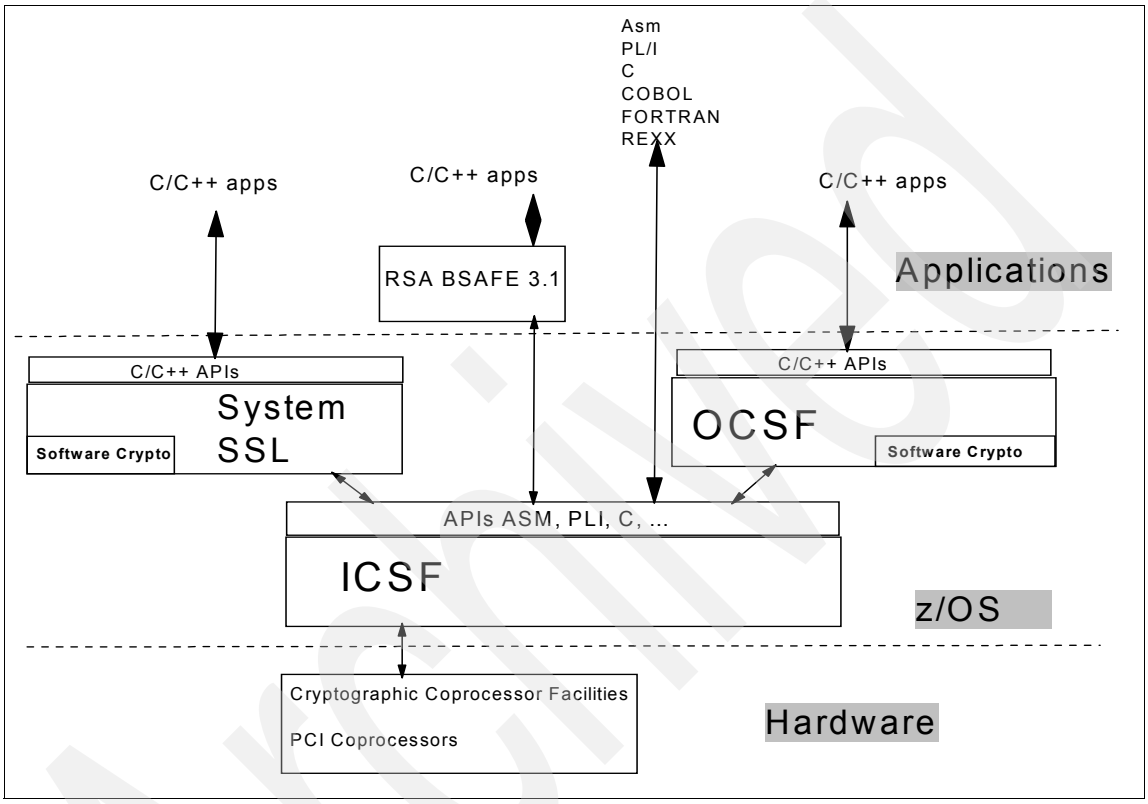

Figure 1-4 ICSF overview

Advanced Encryption Standard (AES) is also supported by ICSF. Data can be encrypted and decrypted using 128-bit, 192-bit, and 256-bit clear keys. CBC and ECB encryption is also supported.

For public key cryptography, ICSF supports both the Rivest-Shamir-Adelman (RSA) algorithm, and the NIST Digital Signature Standard algorithm. RSA and DSS are the most widely used public key encryption algorithms. In this system, each party establishes a pair of cryptographic keys, which includes a public key and a private key.

Archived

1.4.1 CKDS and PKDS

ICSF manages two VSAM datasets where cryptographic keys encrypted by master keys reside: the Cryptographic Key Data Set (CKDS), and the Public Key Data Set (PKDS).

Cryptographic Key Data Set (CKDS)

ICSF stores DES keys in a specialized external VSAM data set called a cryptographic key data set (CKDS). ICSF maintains both a disk copy and an in-storage copy of the CKDS. This makes it possible to refresh the cryptographic keys without interrupting the application programs.

Public Key Data Set (PKDS)

You can store RSA public and private keys in a specialized external VSAM data set that is called a public key data set (PKDS). ICSF optionally maintains a cache of frequently used PKDS records. The size of the PKDS cache is set in the installation options data set (PKDSCACHE). It is an optional feature, with a default of 64 records. If a cache is being maintained, care must be taken when deleting or changing an existing PKDS record.

1.4.2 TKE workstation feature

A TKE workstation is part of a customized solution for using the Integrated Cryptographic Service Facility for z/OS program product to manage cryptographic keys of a z990 that has PCIX Cryptographic Coprocessor features installed and configured for using Data Encryption Standard (DES) and Public Key Algorithm (PKA) cryptographic keys.

The TKE workstation provides secure control of the PCIX Cryptographic Coprocessor features, including loading of master keys.

If one or more logical partitions are customized for using PCIX Cryptographic Coprocessors, the TKE workstation can be used to manage DES master keys and PKA master keys for all cryptographic domains of each PCIX Cryptographic Coprocessor feature assigned to logical partitions defined to the TKE workstation.

Each logical partition using a domain managed through a TKE workstation connection is either a TKE host or a TKE target. A logical partition with TCP/IP connection to the TKE is referred to as the TKE host; all other partitions are TKE targets.

The cryptographic controls set for a logical partition, through the z990 Support Element, determine whether it can be a TKE host or TKE target.

Archive

Figure 1-5 illustrates how logical partitions, physical crypto coprocessors, and domains interact.

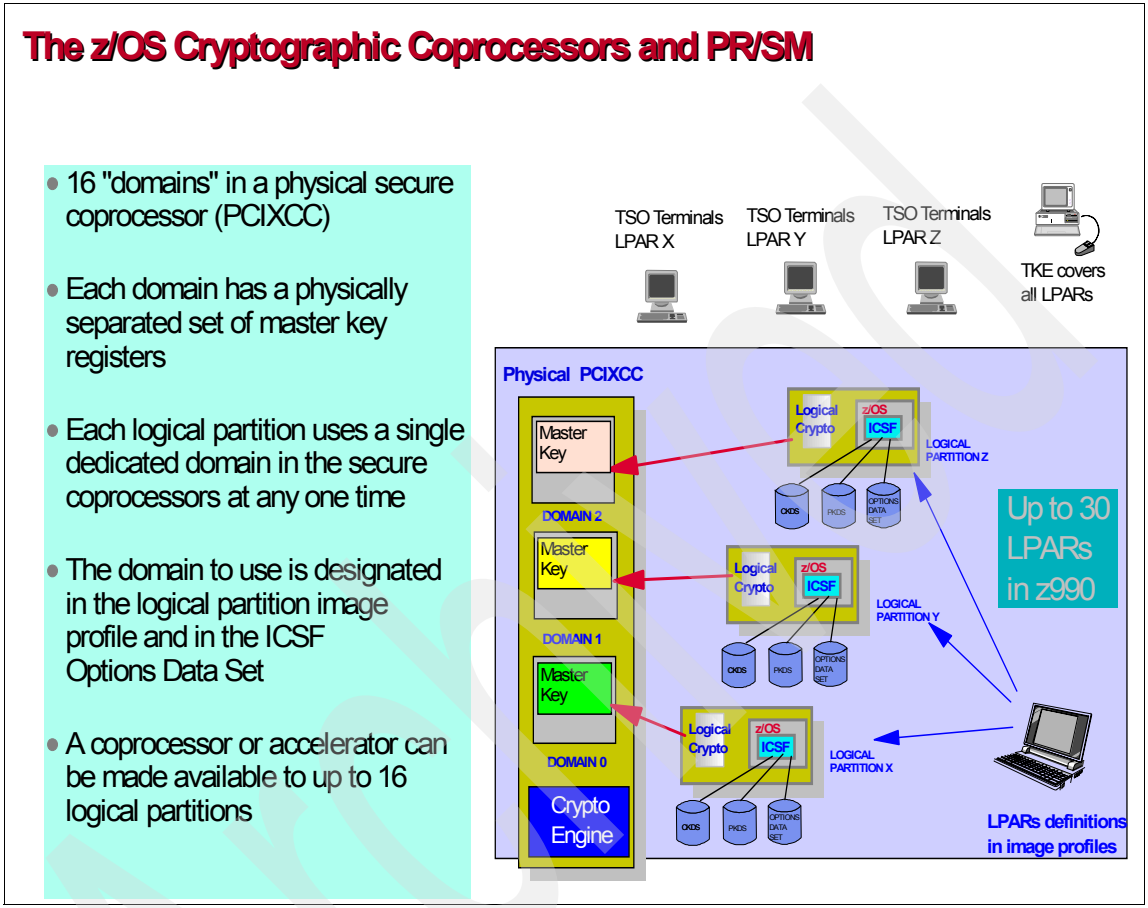

Figure 1-5 Physical coprocessor domains and logical coprocessors

1.5 Cryptographic features comparison

Table 1-1 summarizes the functions and attributes of the cryptographic hardware features.

Table 1-1 Cryptographic features comparison

Functions or attributes	CPACF	PCIXCC	PCICA
Supports z/OS applications using ICSF	X	X	X

Functions or attributes	CPACF	PCIXCC	PCICA
Supports OS/390 applications using ICSF	X	X	X
Encryption and decryption using secret key algorithm		X	
Provides highest SSL handshake performance			X (1)
Provides highest symmetric (clear key) encryption performance	X		
Provides highest asymmetric (clear key) encryption performance			X
Provides highest asymmetric (encrypted key) encryption performance		X	
Disruptive process to enable		(2)	(2)
Requires IOCDS definition			
Uses CHPID numbers			
Is assigned PCHIDs		X (4)	X (4)
Physically imbedded on each Central Processor (CP)	X		
Requires CP Assist for Cryptographic Function enablement	X	X	X (3)
Requires ICSF to be active		X	X
Offers user programming function support (UDX)		X	
Usable for data privacy - encryption and decryption processing	X	X	
Usable for data integrity - hashing and message authentication	X	X	
Usable for financial processes and key management operations		X	
Crypto performance RMF™ monitoring		X	X
Requires system master keys to be loaded		X	
System (master) key storage		X	
Retained key storage		X	
Tamper-resistant hardware packaging		X	
Designed for FIPS 140-2 Level 4 certification		X	
Supports SSL functions	X	X	X
Supports Linux® applications doing SSL handshakes			X
RSA functions		X	X

Archive

Functions or attributes	CPACF	PCIXCC	PCICA
High performance SHA-1, Hash function	X		
Clear key DES/T-DES	X		
Clear key RSA		X	X

(1) Requires CPACF enablement.
(2) In order to make the addition of PCIXCC and PCICA features nondisruptive, the logical partition must be predefined with the appropriate PCI cryptographic processor number selected in its candidate list, on the partition image profile.
(3) Not required for Linux.
(4) PCIXCC is assigned one PCHID per feature. PCICA is assigned two PCHIDs per feature (one per accelerator processor).

1.6 Software requirements

The CP Assist for Cryptographic Function, PCXICC, and PCICA features have specific software requirements.

The Integrated Cryptographic Service Facility (ICSF) is the support program for the cryptographic features: CP Assist for Cryptographic Function, PCIXCC, and PCICA. ICSF is integrated into z/OS.

Support for z/OS releases is made available as Web deliverables.

- Clear key support, when the z990 is initially shipped:
  - z990 Cryptographic CP Assist Support for z/OS V1R3
  - z/OS V1.4 z990 Compatibility Support
- Secure key support, in conjunction with the PCIX Cryptographic Coprocessor:
  - z990 Cryptographic Support for z/OS V1R4, available September 2003.
  - z990 Cryptographic Support, for z/OS V1.2 and z/OS V1.3 available October 2003.
  - z990 Cryptographic Support, for OS/390 V2.10 available December 2003.
- The minimum Linux kernel level needed to gain access to PCICA is 2.4.7.

Table 1-2 summarizes the software support requirements by operating system.

Table 1-2 Software requirements to support cryptographic features

Operating system	CPACF	PCIXCC	PCICA
z/OS V1.4 and later	Y (1)	Y (3)	Y (1)

Archived

Operating system	CPACF	PCIXCC	PCICA
z/OS V1.3	Y (2,4)	Y (4)	Y (2,4)
z/OS V1.2	Y(4)	Y (4)	Y (4)
OS/390 V2.10	Y (5)	Y (5)	Y (5)
z/VM® V4.2 and later (for Linux Guests only)			Y
z//VM V4.2 and later	Y		
z/VM V3.1	Y		
z/VM Guests		SOD (6)	
Linux 2.4.7 for zSeries			Y
VSE/ESA™ V2.7 and IBM TCP/IP for VSE/ESA V1.5			Y

(1) z/OS V1.4 z990 Compatibility support, available June 2003.
(2) z990 Cryptographic CP Assist Support for z/OS V1.3, available June 2003.
(3) z990 Cryptographic support, available September 2003.
(4) z990 Cryptographic support, available October 2003.
(5) z990 Cryptographic support, available December 2003.
(6) Statement of direction: IBM intends to enable Linux for zSeries to support PCIXCC.

Archived

2

CPACF, PCICA, and PCIXCC product overview

In this chapter, we provide an overview of the CP assist for cryptographic functions architecture (CPACF). We also describe the new PCI Cryptographic Coprocessor (PCIXCC) and the PCI Cryptographic Accelerator adapter (PCICA) for z990 servers. We briefly describe the IBM 4758 Technology as used in the S/390 PCICC implementation starting with 9672 G5/G6 systems, as well as the cryptographic coprocessor enablement concept and the enhanced TKE workstation feature.

© Copyright IBM Corp. 2004. All rights reserved.

2.1 Description of hardware

In this section, we explain how the cryptographic coprocessors are implemented in zSeries systems.

2.1.1 Definitions

The following definitions introduce you to zSeries cryptography concepts.

- **CP Assist for Cryptographic Function (CPACF) feature**

  With the new z990 mainframe, each CP now has an assist processor on the chip in support of cryptography. This feature provides high-performance hardware encryption and decryption support.

- **Peripheral Component Interconnect Extended Cryptographic Coprocessor (PCIXCC)**

  The optional Pheripheral Component Interconnect Extended Cryptoraphic Coprocessor (PCIXCC) provides a high-performance cryptographic environment with added function. In fact, the PCIX Cryptographic Coprocessor consolidates the functions previously offered on the z900 by the Cryptographic Coprocessor feature (CCF) and the PCI Cryptographic Coprocessor (PCICC) feature.

  Note: The former z900 PCI Cryptographic Coprocessor feature is not supported on z990.

- **Peripheral Component Interconnect Cryptographic Accelerator (PCICA)**

  The Peripheral Component Interconnect Cryptographic Accelerator (PCICA) is an orderable feature on z990. This optional feature is a reduced-function, performance-enhanced addition to the CPACF and the PCIXCC with reduced functional characteristics.

2.1.2 Hardware implementation

Here we describe the crypto hardware implementation on z990.

On z990, the CPACF facility is available on each CP, but the enablement of this feature has to be done during manufacturing if this option has been ordered by the customer on a new mainframe. This is done by an LIC enablement diskette if the system is already in the field. Both PCIXCC and PCICA are additional optional features. They will be operational only if the CPACF feature is previously enabled on the system.

Archived

Note the following:

- The z990 allows for up to two PCICA features per I/O cage. This allows for a maximum of six PCICA features or twelve PCICA coprocessors per z990 server.
- The maximum number of PCIXCC features per I/O cage is four. The maximum number of PCIXCC features per z990 is also four.
- On z990, the PCIXCC and PCICA features do not use CHPIDs from the logical channel subsystem pool, but each cryptographic coprocessor is assigned to a PCHID as follows:
  - One PCHID is assigned per PCIXCC feature.
  - Two PCHIDs are assigned per PCICA feature.
- The total number of cryptographic features may not exceed eight per z990 for any combination of PCIXCC and PCICA features.

Archived

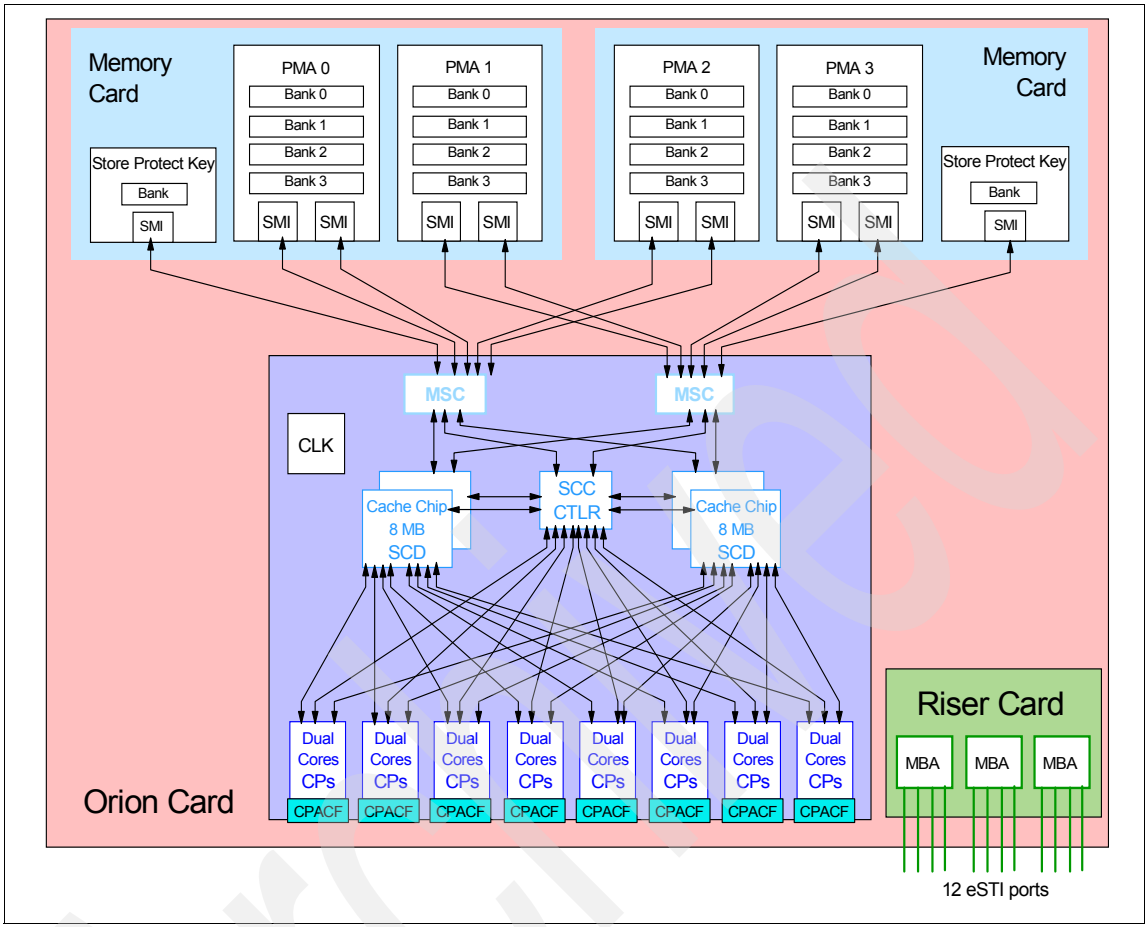

Figure 2-1 Book Orion data flow for an 8-way book

CPACF

There is only one security level for the enablement of CPACF. The installation of the CPACF DES/TDES enablement, feature code 3863, is required to enable the use of the PCIXCC and PCICA features. Feature code 3863 enables the DES and TDES algorithms on the CPACF; the SHA-1 algorithm is always enabled.

PCIXCC/PCICA

As mentioned before, the CPACF enablement is mandatory to use the PCIXCC and PCICA card functions.

The FCV feature is no longer in use on the z990.

Note: Any combination of the PCIXCC, PCICA, OSA-express, and FICON-express features may not exceed 20 features per I/O cage, or 60 features per z990.

STI and PCHID plugging rules overview on zSeries

The z990 I/O cage can house up to seven I/O domains, the same as the z900. Each I/O domain may have up to 4 I/O slots, making a total of 28 I/O slots per cage for the z990.

Each I/O domain is connected to the CPC via a Self-Timed Interface - Multiplexer (STI-M) card and a 2.5 GB/s STI cable. Seven STI-M cards (z990) and STI cables are needed to support a full I/O cage.

Each PCIXCC or PCICA book occupies an I/O slot in a z990 I/O cage.

Figure 2-2 shows a PCIXCC and a PCICA book plugged as part of the channel packaging on a z990 I/O cage. Refer to 3.2, “Feature codes” on page 48 for a description of feature codes.

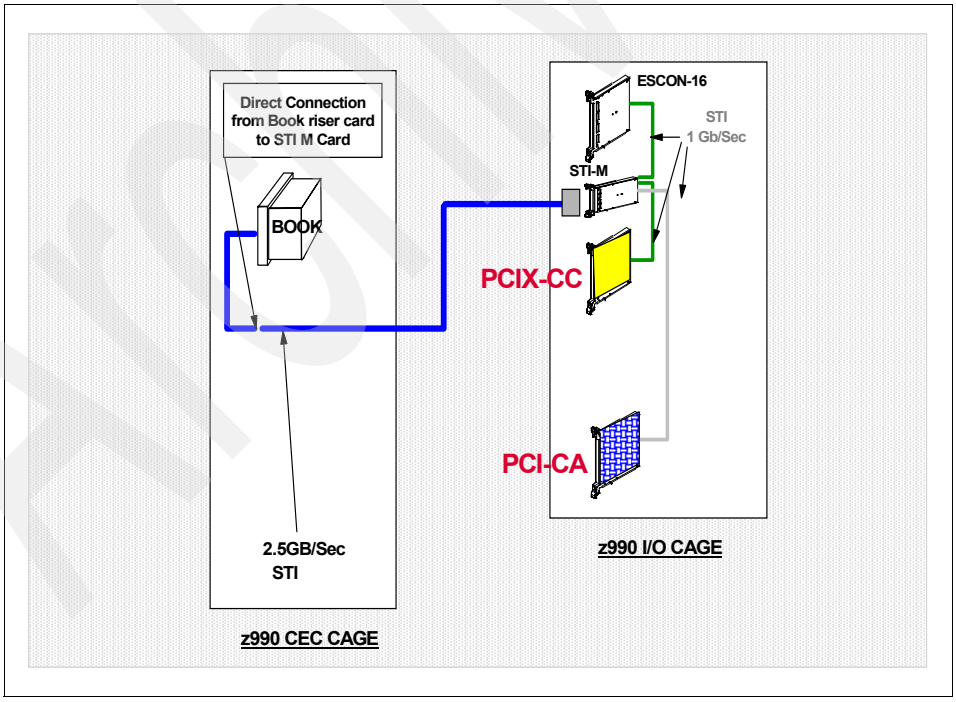

Figure 2-2 Z990 PCIXCC and PCICA packaging overview

2.1.3 Introduction to the z990 PCIXCC, PCICA and CPACF

When ordered on a 9672 G5/G6 or on a zSeries system running OS/390 or z/OS, the PCI crypto coprocessors are always considered a *complement* to the CCF—in fact, the ICSF software requires, as a prerequisite, at least one CCF installed in the CEC in order for the PCI cryptographic coprocessors to be functional.

On zSeries servers, the number of PCICC features cannot exceed eight, while the number of PCICA features is limited to six. PCI crypto coprocessors and PCI crypto engines cannot exceed 16.

From a system implementation perspective, a PCICC or PCICA crypto coprocessor 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 16 on zSeries, and a PCICC or a PCICA is therefore given an AP number between 0 and 15.

CPACF feature for symmetric en/decryption and clear key operations

The zSeries cryptography is further advanced with the introduction of the CPACF architecture implemented on every z990 processor (CPU).

With unprecedented scalability and data rates, the z990 processor provides a set of symmetric cryptographic functions, synchronously executed, which enormously enhance the performance of the encrypt/decrypt function of SSL.

Virtual-private-Network (VPN) and data storing applications do not require FIPS 140-2 level 4 security.

The on-processor crypto functions run at T-Rex processor speed, an order of magnitude faster than the CMOS crypto coprocessor in the z900. As these crypto functions are implemented in each and every CPU, the affinity problem of the pre-z990 systems (which had only two CMOS crypto coprocessors) is eliminated. The crypto assist architecture includes DES and TDES data encryption/decryption, MAC message authentication, and SHA-1 secure hashing. All of these functions are directly available to application programs and so reduce programming overhead. To conform with US export and import regulations of other countries, an SE panel will be provided for proper enabling/disabling of “strong” cryptographic functions.

PCIXCC type for secure operation

A new crypto adapter (PCIXCC) will be introduced as a functional replacement for the CMOS cryptographic coprocessor and for the previous PCICC adapter.

The PCIXCC adapter design introduces a breakthrough concept that supports high security-demanding applications requiring an FIPS 140-2 level4 certified crypto module. It also supports an execution environment for customer-written programs and a high performance path for public key/SSL operations.

The latter PCIXCC adapter option is planned to be supported at GA2 of the T-Rex when Hydra 3.0 as adaptation processor is available.

The “Adjunct Processor” architecture (internal transport architecture for crypto commands and data) is the architectural foundation for attaching both types of adapters with smaller architecture extensions required to support the new PCIXCC adapter.

The X Cryptographic Coprocessor adapter card will contain a new crypto chip (Otello) in the CMOS-8SF technology and an FPGA (Rigoletto) chip to interface a PowerPC® microprocessor and the Otello chip to the host through a PCI-to-PCI-X bridge chip. The Otello chip will contain the following symmetric key engines:

- DES
- TDES
- AES
- Support for SHA-1
- MD5 Ashing
- High performance RSA engine

In addition, the design will also include a “fast path” access to the crypto engines, and two separate interfaces, PowerPC type and add-on, to the Rigoletto FPGA chip. The Rigoletto FPGA chip interfaces the key card components (Host PowerPC microprocessor, and the Otello chip) on the card and implements the associated data paths, data movement controls, and control logic.

The Rigoletto FPGA chip interfaces to the PowerPC microprocessor via a PCI interface and to a PCI-to-PCIX bridge chip via a second PCI interface. The card is designed to provide full checking to meet the high-end server RAS requirements. The on-card PowerPC microprocessor provides for fully programmable functions and User Defined eXtensions (UDX) support.

PCICA type for SSL acceleration and clear key operations

To support the increased number of LPARs available on z990, the configuration options for the crypto PCICA adapter (introduced with z900) will be extended to allow sharing of the PCICA over the whole range (up to 60) of LPARs with a maximum of 16 LPARs sharing one PCICA adapter.

Up to 12 PCICA adapters packaged in six PCICA crypto books can be configured.

The PCICA unit is designed specifically for maximum-speed SSL acceleration, rather than for specialized financial applications or for secure long-term storage of keys and secrets. As a result, it does not need the tamper design of the zSeries CMOS CCF and zSeries PCICC feature.

Each zSeries PCI Cryptographic Accelerator Feature contains two cryptographic accelerator cards and can support up to 2100 SSL handshakes/sec. However, the maximum number of SSL handshakes/sec that can be supported on a zSeries server by any combination of CMOS crypto, PCIXCC crypto, and PCICA crypto is limited by the amount of CPU cycles available to perform the software portion of the SSL handshake.

Unlike the IBM 4758-2 cryptographic coprocessor, there is no microprocessor subsystem (CPU, DRAM, Flash, and so on). The overall operation control, including command decoding, is implemented in the hardware.

Similar to the PCIXCC feature, two PCICA units are embedded in a Self-Timed Interface (STI)-attached controller card for installing within a zSeries server. The STI-attached controller package allows STI-to-PCIX interface bus conversion, and also provides for PCI controller functions.

The accelerator will use the same PCHID type of PCI-Crypto as is used by the PCIXCC cards. The customer will see it as an Adjunct Processor (AP).

The crypto accelerator also has the following differences from the PCICC feature:

- It does not support zeroize.
- It does not support the Random Number Generator function.
- It does not have tampering detection.
- It does not have an intrusion latch or battery.
- It does not support the new UDX functions.

From a system implementation perspective, the PCICA unit is a PCIXCC unit, an Adjunct Processor (AP).

Starting with z/OS V1R2, ICSF and system SSL functions will automatically use PCICA processors, if available. Usage includes: z/OS HTTP server, WebSphere®, TN3270 server, LDAP server, and the CICS® Transaction Gateway server, which are all applications that call ICSF directly for clear key RSA operations.

Linux for zSeries will also support the PCICA card for SSL usage. This applies whether the Linux-only model is used, or the Integrated Facility for Linux (IFL) on a general-purpose model is used, or when Linux is running under a normal CP, or when Linux is under VM.

Archive

Nature of the PCIXCC/PCICA features:

These PCI features are referred to in three ways:

- PCIXCC has an eight-character serial number, for reference in a variety of panels and to keep track of the retained keys. This serial number is visible when the PCIXCC status is online/operating (PCIXCC configured).

  The zSeries PCIXCC feature contains one IBM 4758-based cryptographic coprocessor.

  The zSeries PCICA feature contains two IBM cryptographic accelerators.
- Both types of PCI features have a two-digit Adjunct Processor (AP) number or ID. This number is an index used by the system LIC and ICSF.
- Because of the way the crypto feature is connected in the system, both the crypto coprocessor and accelerator have a PCHID number. This number is not known nor relevant to ICSF, but is used for hardware management of the feature.

PCIXCC data flow

Now we explain the PCIXCC data flow.

Archive

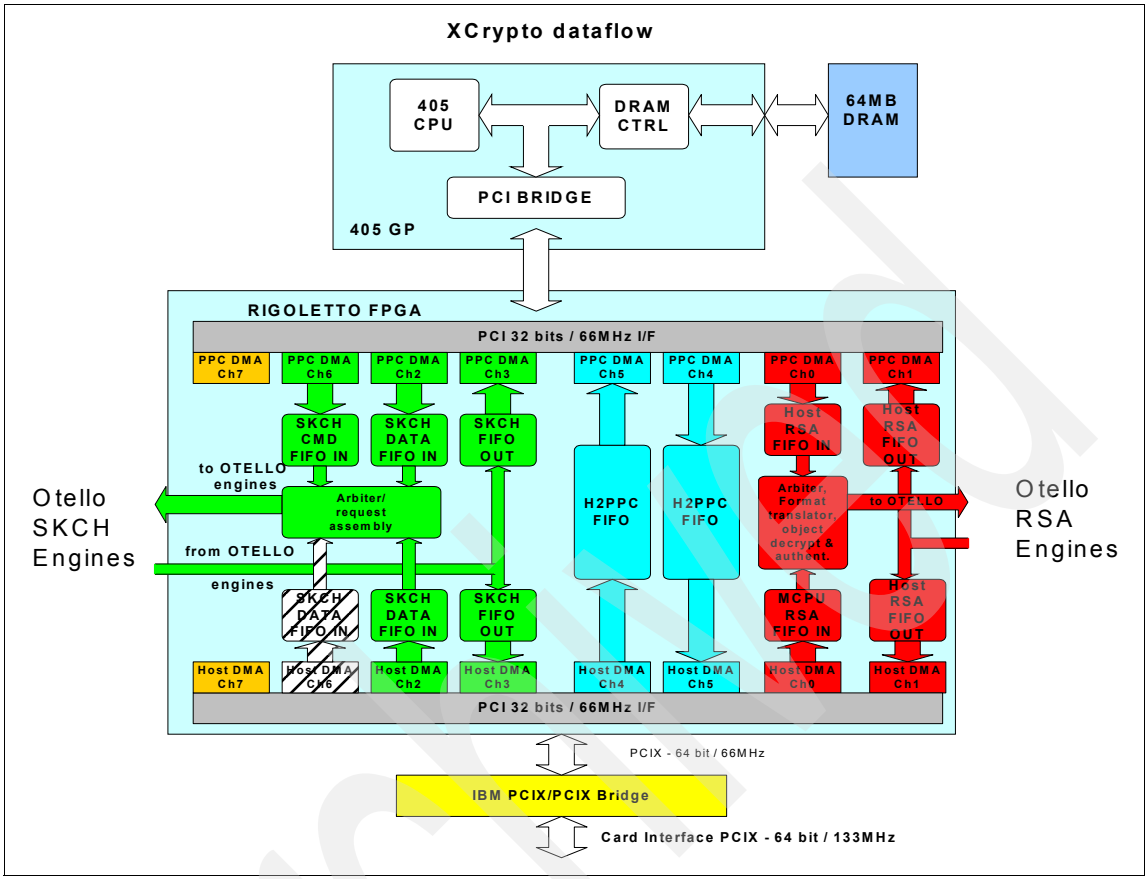

Figure 2-3 PCIXCC data flow chart

The IBM 4758 technology and the PCIXCC 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 2-3 is enclosed in the 4758 physically secure area.

The PCIXCC card

Figure 2-4 on page 27 shows a PCIXCC card consisting of the assembly of an STI controller. Each feature contains one 4758-based cryptographic coprocessor card. The PCIXCC card must *not* be disassembled.

Archived

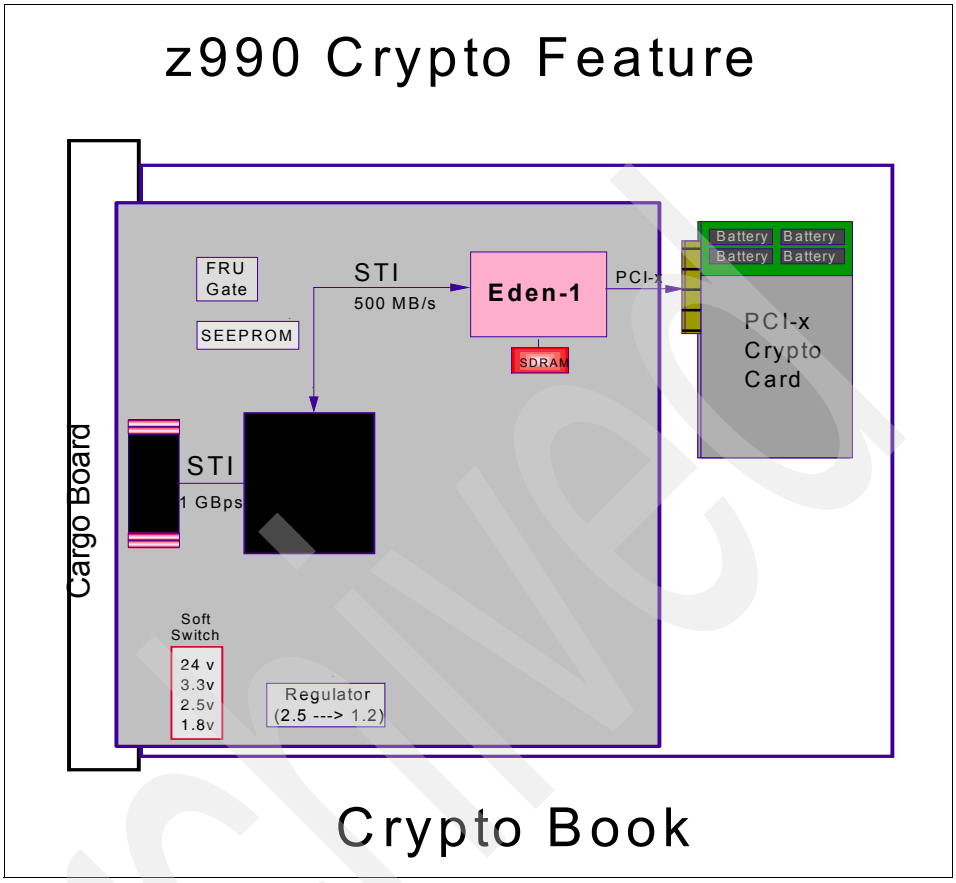

Figure 2-4 PCIXCC card plugged into a z990 system

Figure 2-5 on page 28 shows a PCICA book consisting of the assembly of an STI controller card and two PCI Crypto Accelerator cards. The PCICA card must *not* be disassembled.

Archive

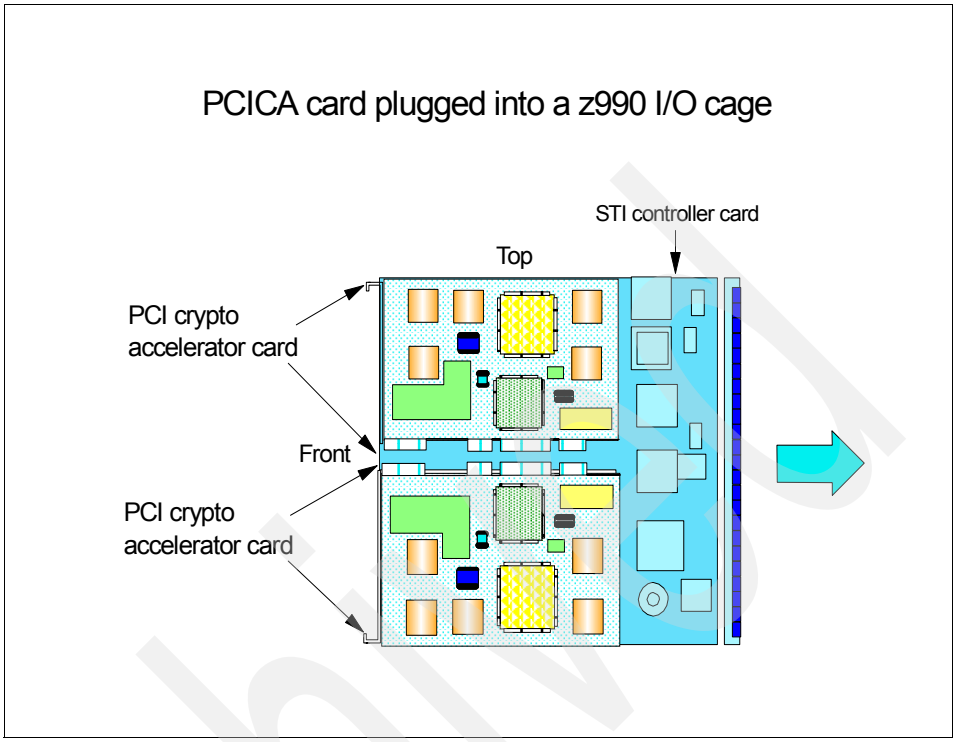

Figure 2-5 PCICA card plugged into a z990 system

PCIXCC and PCICA viewing status

Figure 2-6 on page 29 illustrates the PCIXCC and PCICA end view.

Archive

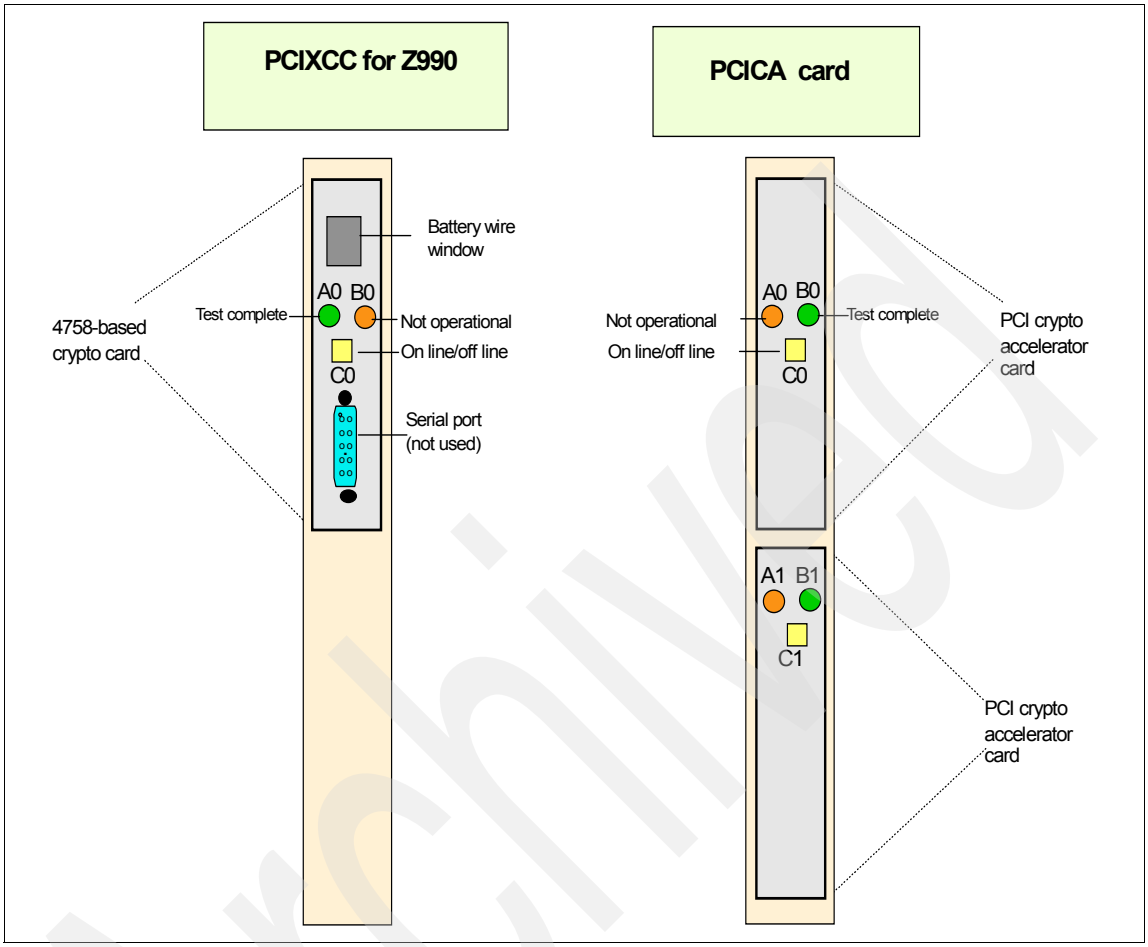

Figure 2-6 zSeries PCIXCC and PCICA cards end view

Table 1 lists the meanings of the PCIXCC card indicators (A) and (B).

Table 1 PCIXCC and PCICA LEDs (A0/A1 and B0/B1 indicators)

Test complete indicator LED (A) green	**Not operational LED (B) amber**	**Card status**
Off	Off	There is no power to the card, or the card processor is in a loop.
Off	Flashing	Diagnostics are running.

Test complete indicator LED (A) green	Not operational LED (B) amber	Card status
Off	On	Status after a card is replaced, from power-on until tests start.
On	Off	The PCI crypto is online (this is the normal status).
Flashing	On	A hardware error is detected.
Flashing	Off	Diagnostics are complete.

Table 2 lists the meanings of the PCIXCC/PCICA card indicator (C).

Table 2 PCIXCC and PCICA LED (C) indicator

Online/Offline indicator (C0/C1)	Status
Off	CHPID for crypto adapter is online, and card is communicating with PU.
On	CHPID is offline for maintenance, or an external test is running.
Blinking rapidly	Power-on tests are running.

Archived

PCICA data flow

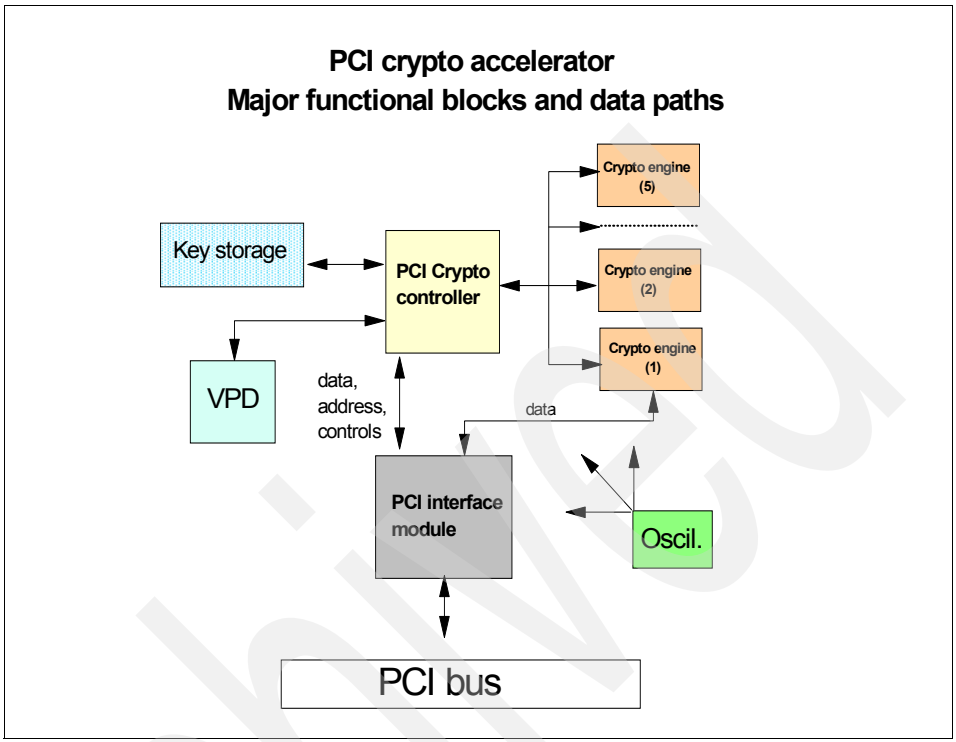

Figure 2-7 PCICA data flow chart

PCICA data flow is illustrated in Figure 2-7. The main components of the PCI Crypto Accelerator card are:

- Five IBM Ultra Cypher cryptographic engines that perform the following functions:
  - RSA (modular exponentiation) with data key lengths up to 2048 bits
  - Math and special RSA functions up to 2048-bit results
  - DES, T-DES, SHA, and MAC functions
- Random number generator
- Crypto controller module
- PCI interface module
- SRAM used as key storage
- Serial EEPROM used as VPD storage device

Major components and their emplacements are shown in Figure 2-8 on page 32.

Archive

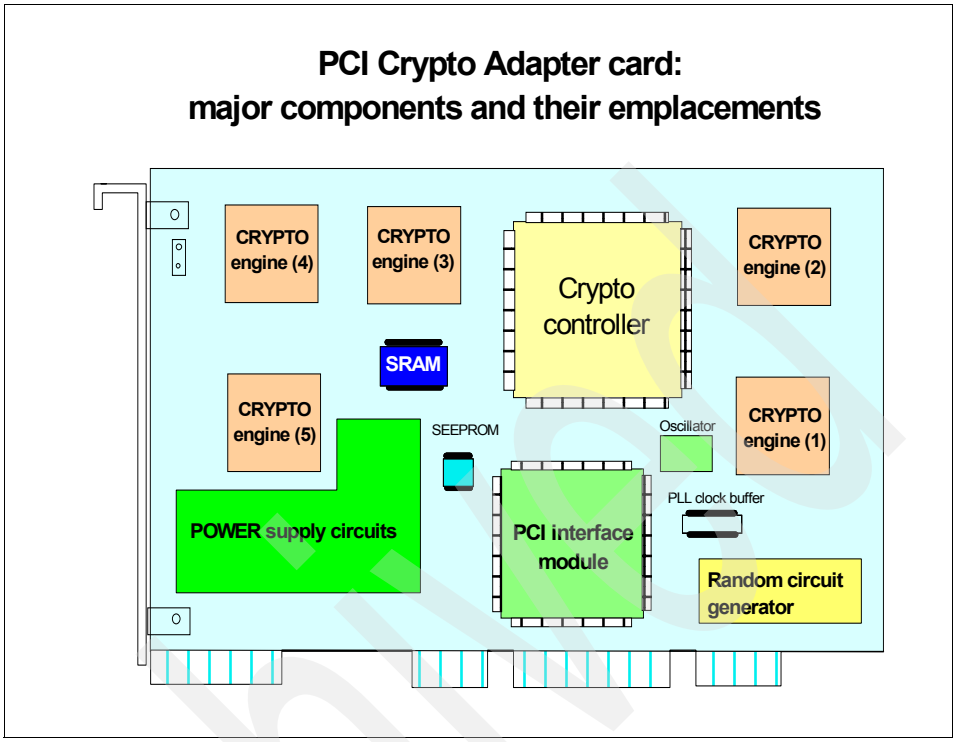

Figure 2-8 Inside the PCI Crypto Adapter (PCICA) card

2.1.4 PCXICC card: physical security, handling, and shipping

Figure 2-9 on page 33 contains a longitudinal section that shows the PCIXCC card internal packaging and the secure enclosure of the 4758-based card.

A dedicated electronic circuit on the Crypto card is aimed to detect the intrusion and tampering attempts to a protected area, in order to meet the “Security Requirements for Cryptographic Modules” FIPS PUB 140-2 Security Level 4 and applications requiring lower security levels. The circuit described here protects the area where sensitive data is stored, by performing the following:

- Tamper detection, being able to distinguish between false alarms and true alarms
- Continuous monitoring of critical electrical parameters (gauges)
- Responding to a validated alarm by erasing the sensitive data that is protected

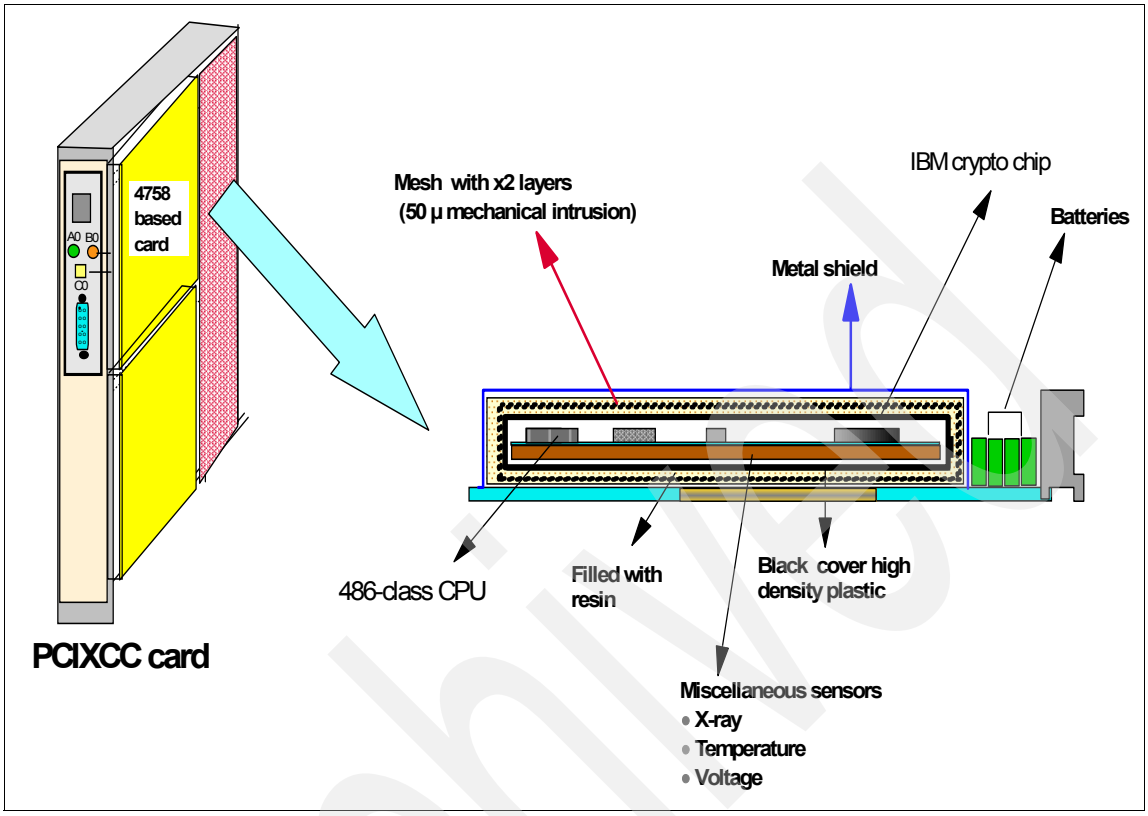

Figure 2-9 4758-based card on z990: longitudinal section

Compared with the state of the art protection systems, this digital one introduces the following innovations in the application of the low power detection systems:

- Two analog comparators are used to monitor several gauges
- The comparators raise an alarm that wakes a microprocessor
- The microprocessor validates the alarm and initiates the response
- Redundancy in case the microprocessor fails
- Redundancy in case of sophisticated physical intrusion

The advantages are:

- Few components and very low power consumption
- Increased security
- Reliability
- Programmability

Cryptographic products have to meet security standards that are very restrictive if the required security level is high. In order to meet these standards, special

circuits are designed to detect any attempt to violate security. In the case of cryptographic cards, it is current practice to use a special tamper respondent sensor (named membrane or mesh) to detect volumetric physical penetration.

The membrane, powered by a voltage source, is designed with control points that maintain a known voltage level proportional to the voltage source. In case of intrusion, these levels change and the variations are detected. The circuit issues a command to destroy the sensitive data inside the protected area. Generally, two comparators with open collector outputs are used for each measurement point. All the outputs are connected and the common output signal is sent to an electronic switch that is able to power off the voltage source and erase the sensitive data.

In this new circuit, the decision to erase the internal sensitive data due to a tamper attack depends on two different results: One is a measurement point out of the acceptance limits, and the other is an intelligent evaluation of the measured voltage.

This methodology avoids the possibility of having false triggers due to spikes or external noises and performs a reliable detection of the attack.

A microcontroller collects and stores data even if batteries are removed after the tamper event.

Only “Ultra Low Power” ICs (amplifiers, comparators and microcontrollers) are used in this design.

Mesh pretamper detector

The pretamper detector is a new concept introduced on this circuit.

All the mesh test points are connected to the noninverting input of the corresponding high-Z buffer Op Amp. The Op Amp is used as impedance adapter; the Op Amp output voltage reproduces the input voltage (the mesh measurement point voltage) and converts the high impedance of the membrane into a low one. The low impedance PCB tracks are now less sensitive to noise and external disturbances. Using an appropriate layout, it's possible to minimize the high impedance path and in this way solve the problem connected with high impedance management (typically noise sensibility). Membranes having control points set at 50% or more of the supplied voltage require full rail-to-rail Op Amp modules.

The output of any single Op Amp is connected to a pair of diodes, one with the cathode and the other with the anode. All the required diodes are connected at the other side; the two common points are collecting the diode's cathodes and anodes.

Archive

Temperature and battery voltage sensors

The temperature sensor circuit is based on an NTC resistor that changes its value as a function of the temperature. Two comparators are set to control the acceptable temperature limits. These limits reflect the functional temperature range of the protected package. If one of these values goes over range, a pretamper signal is issued to the microcontroller

Pretamper memory and delay

All the pretamper signals coming out from different circuits are ORed together to start a Set Reset Flip Flop. At the same time the pretamper signals wake up the microcontroller, which is able to measure and evaluate analog signals.

An appropriate code is used to control whether the tamper is true. In this case the microcontroller issues the tamper signal to destroy the sensitive data.

The flip/flop has two functions:

- Start a short duration timer.
- Store the pretamper alarm.

When a pretamper signal has been issued to the flip/flop and to the microcontroller, the flip/flop toggles and starts the timer. At the same time the controller wakes up and starts testing the controlled points. If a true tamper failure is detected, the “Tamper I/O” signal is sent to the OR circuit. The OR circuit immediately responds by sending the “Tamper” signal to erase the internal sensitive data. If the controller does not confirm a real failure, because the pretamper signal was due to noise or temporary disturbances, the “Single shot reset” is issued. In this case the timer circuit is immediately cleared and the security data is maintained.

The timer circuit is very important in order to guarantee that the tamper circuit will work even if, for any reason, the controller hangs (redundant security concept). In this case, when time expires, the “Tamper” is forced anyway.

Enhanced data security circuit

This circuit is a new concept block capable of improving the secure-data protection in case an intruder is able to force “someway” the sensitive module supply voltage and tries to bypass the tamper effect. The fuse intervention time is fast enough to prevent the probing of sensitive data.

Protection mechanism

The tamper reaction to security attacks is performed in different ways:

- Hard tamper protection

Archived

A “hard tamper” occurs when a critical parameter has been modified too much, so the card security is compromised. The secret data stored inside the crypto environment (CSP) are fully zeroized and the card is made permanently inoperative.

- Soft tamper protection

  A soft tamper occurs when an environmental condition may cause an unreliable operating mode of the card itself, or unpredictable results can be generated. In this case a general card RESET is immediately forced to stop the electronics. This condition is automatically removed when the environmental parameters go back to their functional values.

- Warnings

  These conditions do not affect the card functionality and the user can reset these flags after restoring the standard parameters.

Sensed parameters

Many different sensors are located inside the secure package to trigger the alarms:

- Resistive sensors (mesh), detecting the physical penetration
- Temperature detectors
- Voltage detectors
- Radiation detectors

Operating modes

The tamper is fully operative under any circumstances:

- Under battery: during card storage and when card is powered off
- When the card is powered by the host

When the card is powered, the user is automatically warned if batteries have to be replaced. You can also get the tamper status to inspect warnings anytime. If the machine covers were removed for any reason, an “External Intrusion” flag would be set.

Card Physical Security

The X-Crypto card shall comply with FIPS PUB 140-2 Security Level 4 requirements.

Hard tamper detection

The following events will cause a power shutdown and SECURE DATA ZEROIZATION:

- Mesh sensor opens/shorts

Archived

- X-ray exposure
- High voltage on +3.3V (3.9 ± 0.2V)
- Battery dead (VBAT less then 2.54 V)
- Shipping/storage temperature below -20C ± 5C, or above +95C ± 5C limits

Soft Tamper detection

The following events will cause a card GLOBAL RESET:

- Low voltage on +3.3V (2,9V ± 0.1V)
- Crypto operating temperature out of window limits (0C± 2C/75C± 3C)
- Triggered reset from AVR microcontroller

Software-detected warnings

The following events will cause a WARNING:

- Battery low (VBAT less than 2.7V)
- External Intrusion Latch trip

2.2 Adjunct Processor (AP) management

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

2.2.1 Introduction to Adjunct Processor architecture

The system sees the PCI unit as an Adjunct Processor, that is, a coprocessor reachable through the STI cable. Therefore, each PCI unit 4758-based card installed in the system is assigned an AP number between 0 and 15. The system also establishes the correspondence between the AP number assigned to a card and its PC-CC 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 2-10 on page 38 is a 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

Archived

each domain within an AP, and the AP queues reside in Hardware System Area (HSA) storage.

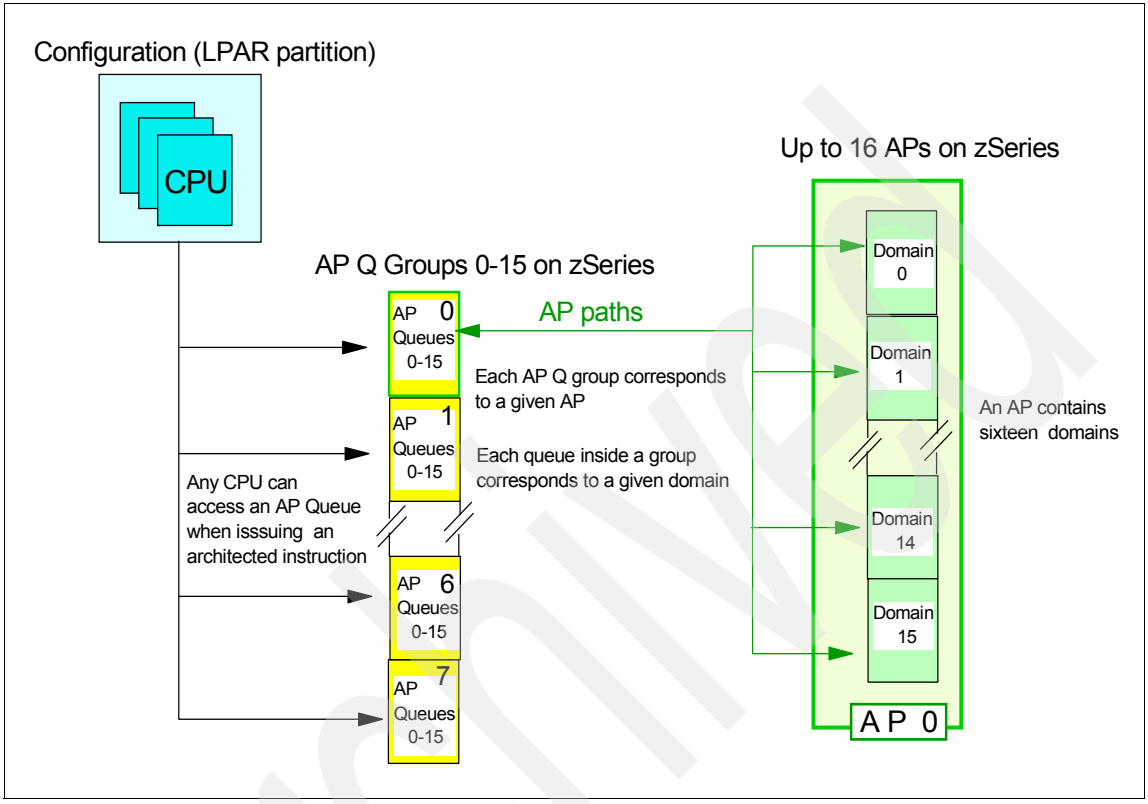

Figure 2-10 AP architecture: high-level view

2.2.2 AP management and PCIXCC initialization

In the following sections, we explain the relationship between an AP and a PCHID number, AP number assignment, and how and why to move PCIXCC cards.

AP and PCHID number

For internal system management purposes, an AP is also tied to a PCHID number that is automatically attributed to the PCIXCC card at installation. Therefore, from a system management standpoint, a PCIXCC is also a new PCHID type, and this requires the typical changes (LPAR, Advanced Facilities, and so on) scattered throughout the Support Element.

Archived

As a consequence, a PCIXCC card will appear tagged with a PCHID number in the Support Element panels, and can be varied online or offline by using the same facilities as for a normal PCHID.

Note: z/OS will never see the PCIXCC as an S/390 PCHID, but only as an AP.

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

AP number assignment

AP number assignment for a newly installed PCIXCC feature card is done at system power-on time or during the PCIXCC concurrent installation procedure. The AP numbers are assigned to the PCIXCC cards in sequence, starting with AP 00. From this point on, the AP number is bound to the crypto PCI card serial number (4758-based card).

At system Power-on Reset, the following occurs:

- The Support Element (SE) passes the cryptographic configuration information to the system Licensed Internal Code (LIC), including the AP IDs-to-PCHID assignment information.
- The system LIC allocates the Hardware System Area space needed for the maximum possible number of PCIXCC APs (which is 16), whether they are actually installed or not. This allows the hotplugging of additional cards in the future.

Releasing an AP ID—that is, severing the relationship between an AP number and the PCIXCC card serial number—can only be done by a manual intervention at the system Support Element. This has to be done when replacing the PCIXCC card, as an AP/PCIXCC card affinity should not be changed even if the card is moved around in a system.

Moving PCIXCC cards

The following sections describe how and why PCIXCC 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 PCIXCC card within a system

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

To uninstall a PCIXCC card, IBM service personnel first use the Nondisruptive 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 PCIXCC card

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

Moving a PCIXCC card between systems

When a PCIXCC 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 PCIXCC microcode load

In the following sections, we describe the organization of the firmware in the 4758-based PCIXCC, as well as 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 that 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 roles and profiles

Archived

- 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, which is the operating system for the 486 processor that 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 zSeries. The User Defined Extensions (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

Code loading for xCrypto Hydra differs from previous systems, as follows:

- Due to RETAIN® data size limitations (4 MB tested, 10 MB absolute)
- Due to legal concerns (Linux only on systems with xCrypto)

Normally the HUL file for Hydra is assembled and built as a single object.

For xCrypto, the HUL is broken up into seven components and assembled by SE code.

The components are:

- Base HUL file (“proto-HUL”)

  This is the only one that can be concurrent (that is, no vary off/on, no IPL, not disruptive to customer operation).

  The total HUL size is still estimated to be 16 MB maximum (HSA-allocated size).

- Segment components
  - 2x Segment3 (about 4 MB each)
  - 2x Segment2 (about 3 MB each)
  - 2x Segment1 (about 150 KB each)
  - 1x FPGA segment (about 850 KB to 1.3 MB)

  UDX-allocated size is a minimum of 4 MB.

  Note: FCV space is still allocated but not used (see Initialization).

- PCIXCC microcode patches

  You can patch PCIXCC 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 PCIXCC. Such changes are not expected to be disruptive to the system, because activating a patch requires you to reset the PCIXCC, which makes it only temporarily unavailable to the applications.

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

  All the segments of the PCIXCC can be Licensed Internal Code (LIC) updated through the MCL process.

2.3.3 Software requirements: cryptographic functions and hardware

This section contains a brief description of the software requirements to support CPACF, PCIXCC, PCICA, and the new TKE V4 workstation.

- z990 Cryptographic CP assist Support for z/OS V1.3

  This will be a Web deliverable, including integrated cryptographic service facility (ICSF) support for the CP assist for cryptographic functions and the PCI cryptographic accelerator (FC0862).

- z/OS V1.4 z990 compatibility support

  This orderable (and optional) feature will include integrated cryptographic service facility (ICSF) support and system secure sockets layer (SSL) support on z/OS V1.4 for the CP Assist for cryptographic function and the PCI cryptographic Accelerator.

2.3.4 The TKE V4 workstation

TKE version V4 is the workstation version currently required to support the PCIXCC. Details about this workstation are provided in Chapter 4, “PCIXCC using TKE V4” on page 59.

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

Archived

Notes:

- TKE V4 communicates with the z/OS host using TCP/IP.
- It uses a 4758-2 cryptographic adapter card.
- 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.

Archived

Archived

3

Planning and hardware installation

In this chapter we describe the hardware requirements when installing the CPACF, PCIXCC and PCICA, as well as the feature codes you should order for zSeries.

Archived

© Copyright IBM Corp. 2004. All rights reserved.

3.1 Hardware requirements

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 PCIXCC/PCICA card installation, and they are therefore dependent on the accuracy of the system configuration as recorded in the IBM Vital Product Data (VPD) database.

3.1.1 Hardware required for z990

The following hardware is required.

CPACF

The CPACF function, as described in Chapter 2, “CPACF, PCICA, and PCIXCC product overview” on page 17 is imbedded in each CPU.

The CPACF is enabled using the appropriate “CPACF enablement” diskette. One diskette will enable the CPACF on all the CPUs on each of the nodes in the system.

On z990, we have only one diskette covering the CPACF/Memory/CPU encryption process. This encryption is applied to book 0 (BIC) and the information is then transmitted to all other nodes for cryptographic function enablement.

You can either have this feature installed on your system, if you have ordered it on a brand new box or if you are performing an MES. After processing your order, you will receive only a diskette to enable the CPACF feature.

PCIXCC and PCICA

Chapter 2, “CPACF, PCICA, and PCIXCC product overview” on page 17 contains a product overview. The plugging rules for PCI Crypto cards are addressed in I/O Support and STI and Channel Plugging Rules.

The new spare card comes from stock with no diskette.

The hardware requirements for the installation of PCI crypto cards on z990 are as follows:

- The PCIXCC feature (Hydra 1.75 fc0868) is only supported on zSeries z990 systems at a GA 2 code level. Feature code 3863 (crypto assist) must be installed as a prerequisite for PCIXCC installation. This feature code is included in the LICCC record of book 0.

Archived

- The PCICA feature (0862) is supported on zSeries systems. Feature code FC3863 is a prerequisite.
- The maximum number of PCIXCC features is four per system and four per I/O cage.
- The maximum number of PCICA features is six per system and two per I/O cage.
- The PCIXCC feature (FC 0868) consists of one card to plug into the system. Note that for zSeries z990 the PCIXCC feature contains one IBM 4758-based cryptographic coprocessor. CIXCC cards can be plugged only on the front side of an I/O Cargo cage.

  No FCV diskette is needed for PCIXCC on z990.
- The PCICA feature (FC 0862) consists of a hardware PCICA card only (no FCV is required). The zSeries PCICA card contains two IBM cryptographic accelerators.
- From an ICSF software point of view, the PCIXCC or the PCICA cannot operate if FC3863 (CP assist) is not installed.
- The HSA space consumed by the PCIXCC is 18 MB. This value is independent of the number of installed cards.

PCIXCC and PCICA cards can be exchanged in the field as part of a repair action. The new spare card comes from stock with no diskette.

Archived

Repair action on BOOK/ PCICA / PCIXCC:

Important: When a service action requires the removal of the battery backup from the cryptographic unit, the Master Keys and configuration data are lost.

This will happen on z990 when unplugging a PCIXCC card in the z990 I/O cage (intrusion latch is the cause). A special procedure exists if keys in the cards need to be saved.

As a consequence:

- Master Keys stored in the PCIXCC card will be lost. It is the customer's responsibility, upon completion of the maintenance task, to restore the Master Keys and any existing retain keys in all domains.
- If a customer is using a TKE workstation, then the corresponding configuration data (PCIXCC) is lost and needs to be restored. It is the customer's responsibility, upon completion of the maintenance task, to restore this data from the TKE for all domains.

  For more information, refer to Chapter 5, "ICSF support for CPACF, PCIXCC, and PCICA" on page 145 and Chapter 4, "PCIXCC using TKE V4" on page 59.

Repair action on PCIXCC or PCICA is concurrent.

If a repair action has to be done on a book, we have two possible scenarios:

- The defective book is number 1/2/3.

  The book will be replaced but there is no need to reactivate the CPACF function. This will be automatic.
- The defective book is number 0.

  Since this is the book supporting the LIC CC code for CPACF enablement, the new seeprom will have to contain the crypto enablement function.

3.2 Feature codes

See Table 3-1 on page 49 for a summary of PCIXCC and PCICA feature codes.

PCIXCC and PCICA plugging rules for zSeries 2084-z990:

- Number of PCIXCC cards plugged: 0 to 4 cards with a maximum of 4 per I/O cage.
- Number of PCICA cards plugged: 0 to 6 cards with a maximum of 2 per I//O cage.

Table 3-1 Feature Codes

Description	2084-Z990
Crypo Assist function	3863
TKE Ethernet Workstation	0889
TKE Token Ring Workstation	0886
PCIXCC Crypto cards (hardware only)	0868
Upgrade TKE to 4.0 code Level	0851
PCICA Crypto cards (hardware only)	862

Note the following points:

- The Trusted Key Entry unit (TKE) will continue to be offered as an optional feature on z990 and is available in two communication formats: Token Ring and Ethernet. The TKE provides a means by which the customer can further restrict access via coded key entries, thus limiting who may use or operate the system.

  The TKE hardware itself (TKE V4) is orderable by selecting feature code 0886 (TKE workstation with a token ring adapter), or feature code 0889 (TKE workstation with an Ethernet adapter).
- Each PCIXCC card to be installed in the system has feature code 0868.
- There is no FCV diskette for PCIXCC (z990).
- Each PCICA card to be installed in the system has feature code 0862. There is no enablement diskette for PCICA.

  The PCIXCC or PCICA card should be plugged using the normal plugging rules. The order increment is 2 engines/1 card.

Archived

3.3 Concurrent PCIXCC/PCICA installation tasks

In this section we discuss the steps involved in performing PCIXCC and PCICA installation and activation.

3.3.1 Concurrent Install on z990

System references

We performed the cryptographic products installation on a z990 system (machine type 2084, model B16) located in the Montpellier Products and Solutions Support Center (PSSC). CPACF was enabled on the system and the PCIXCC/PCICA cards were not installed.

The system was shipped from manufacturing with a Support Element code at Driver 52G, plus the latest MCLs.

The system was shipped with the following crypto feature codes (refer to Table 3-1 on page 49):

- CPACF FC 3863 already enabled
- 2 FC 0868 (PCIXCC card)
- 2 FC 0862 (PCICA card)

Assumptions

- The system support element is already at driver 52 with EJ12560 MCL050 minimum level installed.
- The logical partition image profiles have already been set up with the new PCIXCC page, then activated with these profiles. Control domain and usage domains must have been defined, and the same index must be selected in both control and usage domain. On the partition where a TKE is connected, all the domains you want to control from this TKE must be selected. PCIXCC cards must be defined at least in the candidate list. If not done, partitions will need to be deactivated, profiles changed and partitions activated again, so the installation will not be really concurrent.

  Figure 3-1 on page 51 shows a crypto page for one partition. Control and usage domain 1 is selected. TKE is connected to this partition and can control partitions 0, 1, 2, 3. This is why control domain 0, 2, 3 are also selected. All entries in the candidate list have been selected, so any PCIXCC (up to 4) or PCICA (up to 6) installation will be concurrent for this partition.

Archived

Installation of CPACF

Crypto assist enablement

If feature code 3863 (the crypto assist feature) is not installed on the system, a model conversion diskette will be shipped with the MES. The crypto assist feature is defined in the LICCC record of book 0.

This diskette is an LICCC4 diskette and has to be imported on the support element from the Model conversion panel using the book diskette upgrade option. This upgrade is concurrent.

Installation of PCICA/PCIXCC

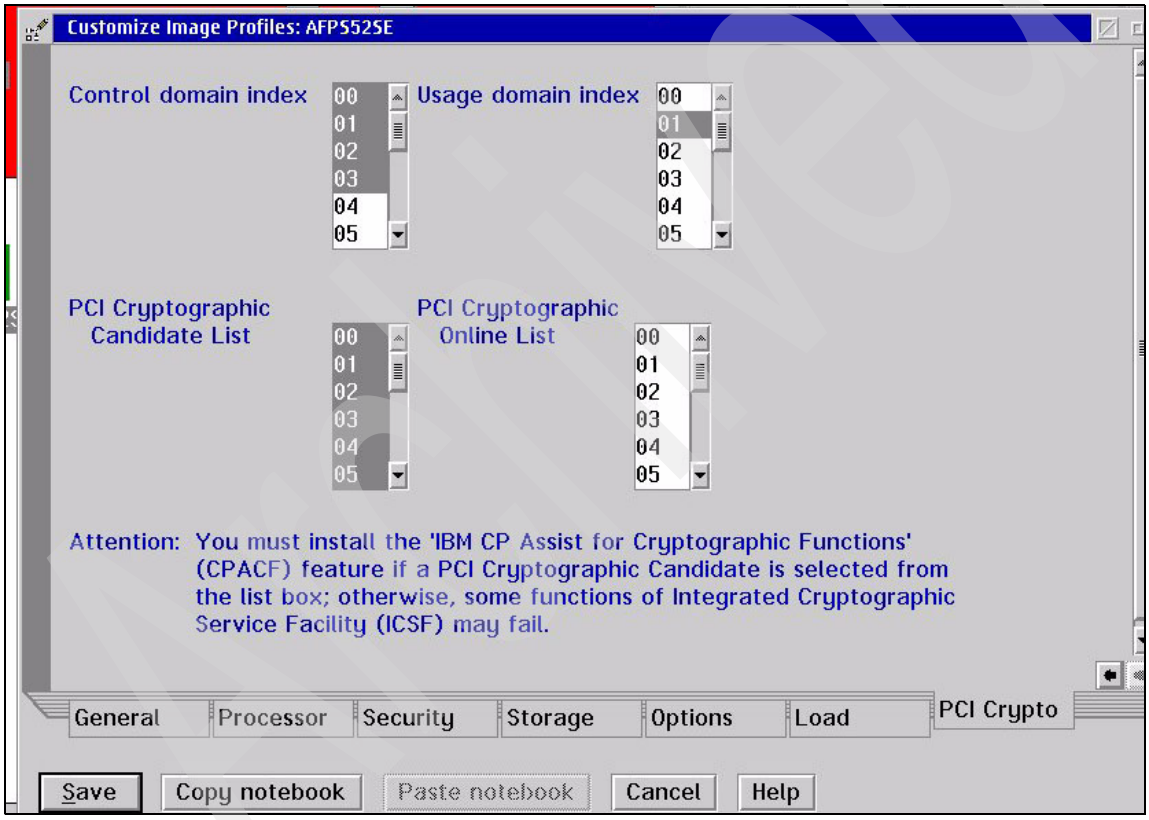

Figure 3-1 Z990 partition profiles to be set up before install: PCI crypto page

An empty slot must be available on the front side of the I/O cargo cage. If not, some other channel cards have to be moved to the back side (may be concurrent) or if no slot is available, a new cage may be needed (adding a cage

is not concurrent). In our example, slot 3 in cage A01 is the position for the PCIXCC installation.

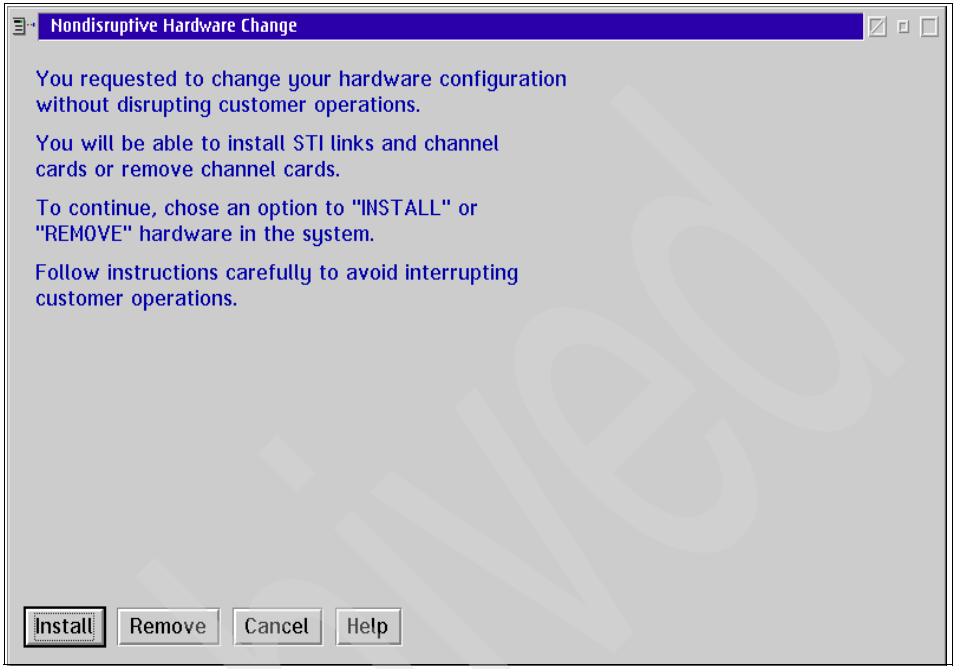

Figure 3-2 Nondisruptive hardware change menu at startup for install

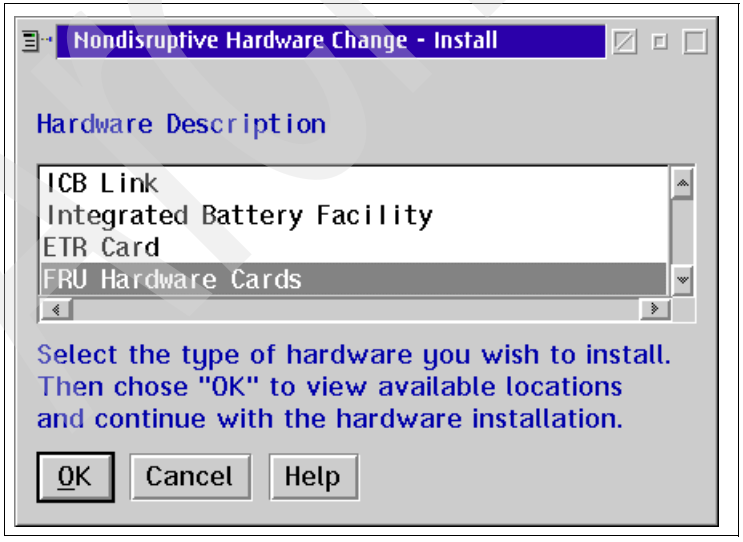

Figure 3-3 FRU hardware to select when installing PCIXCC/PCICA

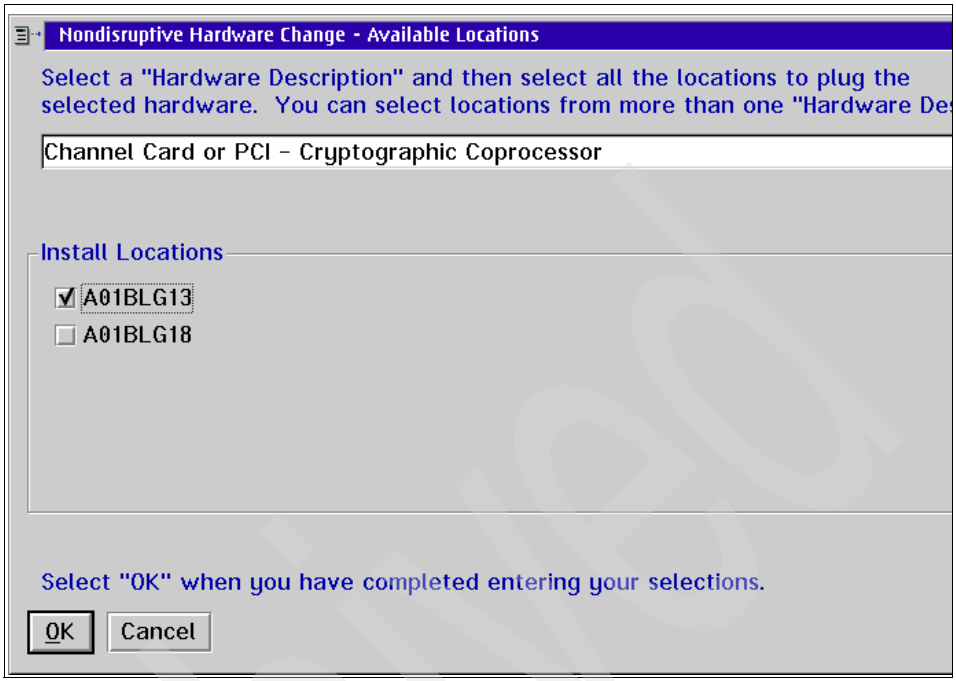

Figure 3-4 In this case A01BLG03 will be plugged into the system

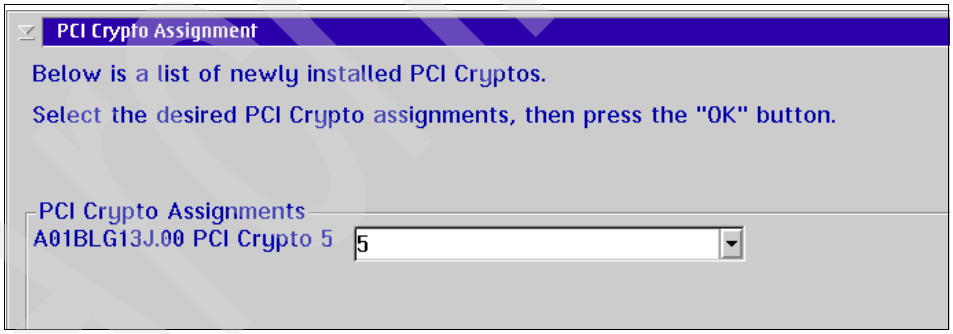

Figure 3-5 Step where you have to select the AP number

By default, the system gives us the next available AP number in the list. For example, here AP1 to AP4 are occupied, so the next available number is AP5.

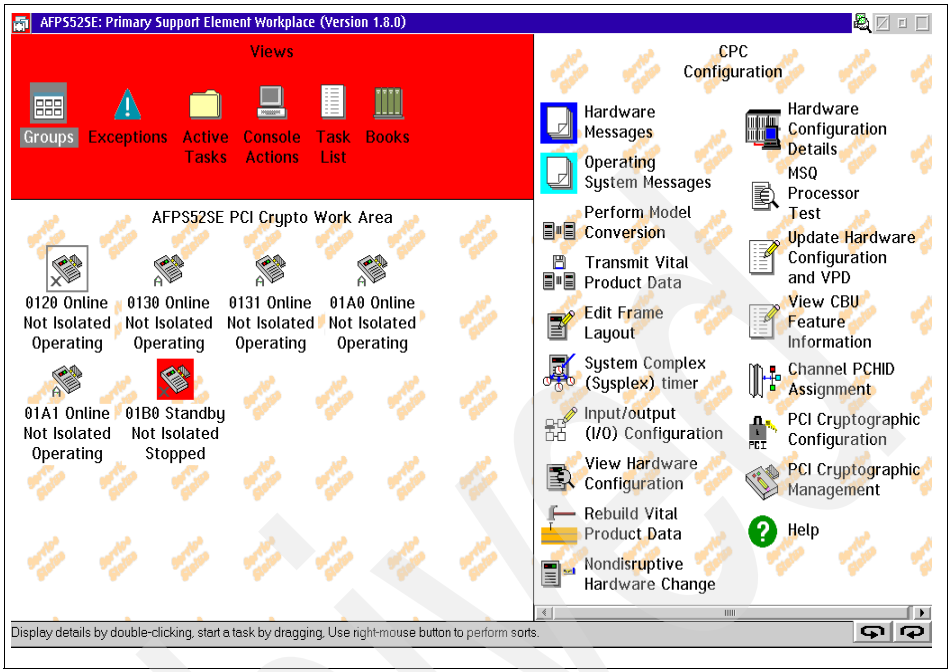

Figure 3-6 PCI crypto work area

Archive

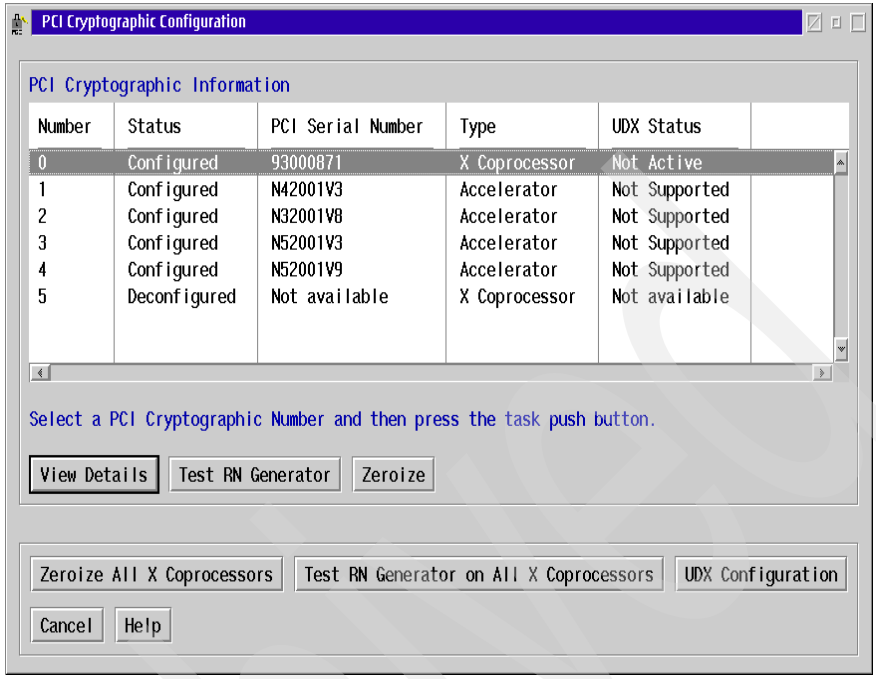

Figure 3-7 Status of the X coprocessor after finishing a nondisruptive hardware change

After the card installation has been completed, the CPHIP has to be varied online to be configured and available.

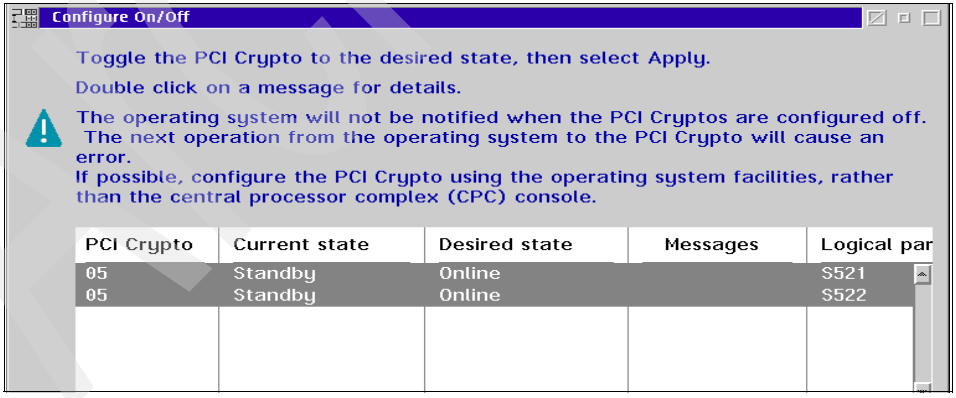

Figure 3-8 Chpid configured online

The card is now installed and activated from a hardware point of view.

3.3.2 Removing one PCIXCC

Remove a PCIXCC card from the system by executing the following steps (in our case we removed the card in position LG03, having AP 5 assigned to it):

1. Deactivate AP5 in the ICSF PCIXCC Management panel.
2. Configure crypto CHPIDs offline at the Support Element.
3. Put crypto CHPIDs in Service-Reserved On (CHPID task).
4. Invoke the Nondisruptive Hardware Change option at the Support Element, and remove the PCIXCC Card at position LG03.
5. If needed, release the AP, using the PCI Cryptographic Management icon. In this case, AP5 is released.

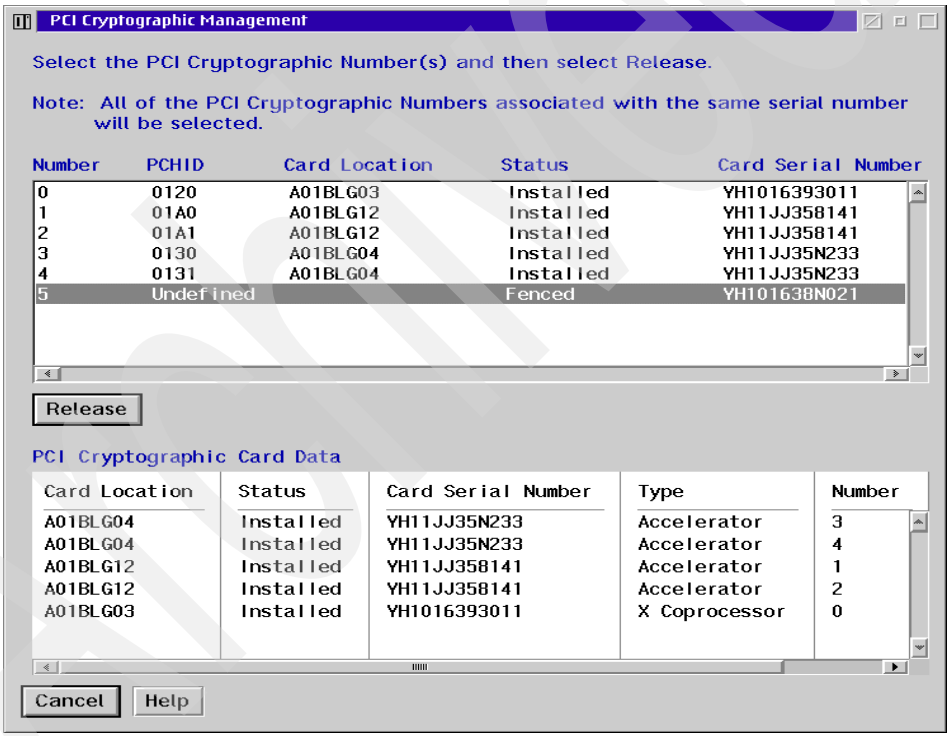

Figure 3-9 Panel to release the AP for the removed card

3.4 Planning list items

Here we discuss the planning and installation considerations and their requirements.

Installation of the ordered PCIXCCs

Note the following installation considerations.

On new build machines

- All PCI crypto cards (FC 0868 PCIXCC) are shipped in thermal containers to avoid the risk of thermal tamper detection during shipment.
- The PCIXCC cards are removed from the machine after testing at the system manufacturing plant, and the Customer Engineer has to replug the PCIXCC cards at the customer's site according to the instructions given in the installation manual.
- If the TKE has been ordered with feature code 0869/0879 or 0866/0876, then the IBM-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.

MES upgrades

For MES upgrades, installation of the PCIXCC cards can be done concurrently with system operations if *both* of the following conditions are met:

- CPACF is enabled and in operation.
- 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 is accurate.

Miscellaneous recommendations

- 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 PCIXCC cards, those cards will be zeroized. Refer to Chapter 2, "CPACF, PCICA, and PCIXCC product overview" on page 17 for more information about this subject.
- The PCIXCC and PCICA CHPIDs are 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 PCIXCC. This will prevent I/O dynamic reconfiguration, and if a system Power-On Reset is performed, neither the

Archived

defined CHPID nor the PCIXCC will come online and a POR error message will be received.

Archived

4

PCIXCC using TKE V4

This chapter provides an overview of the management and operations of the Trusted Key Entry (TKE) Workstation V4.

Archived

© Copyright IBM Corp. 2004. All rights reserved.

4.1 Introduction to the TKE V4 Workstation

Note: This chapter is relevant to z990/z890 PCIXCC card management only. If you are also managing cryptographic coprocessors on G5/G6/z800/z900 (CCF and PCICC modules), refer to zSeries Crypto Guide Update, SG24-6870.

With the introduction of the PCICC card for 9672 G5/G6, z800 and z900 processors, the TKE workstation has been enhanced to allow remote administration of the PCICC cards. It also continues to support the standard Cryptographic Coprocessor Feature. This was TKE V3.X.

With the introduction of the PCIXCC card for z990 at GA2 and z890, a new TKE code level V4 has been released to support remote administration of PCIXCC. TKE 3.X code can be upgraded to 4.0 or 4.1.

Security and secrecy are provided by encrypted and signed transactions between the TKE workstation and the remote Crypto coprocessors. Diffie-Hellman generated keys are used to protect the key parts transported between the TKE and the z990/z890 host cryptographic coprocessors. Requests and responses flowing over the network are authenticated using public key cryptography.

The graphical interface has also been revised, so users should find the module management panels and menus of the TKE V4 application friendlier to use. More details can be found in the *ICSF TKE Workstation User's Guide,* SA22-7524-05.

4.1.1 Major changes

The following are brief descriptions of the major changes to this workstation.

- The cryptographic functions in the TKE V4 are performed by an IBM 4758 model 002 cryptographic coprocessor installed in the workstation (same as TKE V3.X). Upgrading version 3.X to version 4 is done by updating code in the workstation. Note that old TKE V2.x (based on 4755 cryptographic adapter) hardware cannot be upgraded to TKE 4. A new workstation must be shipped (see key migration procedure from TKE V2.x to 4 in *ICSF TKE Workstation User's Guide,* SA22-7524-05).
- TKE V4 can manage PCICCs, PCIXCCs and CCFs (TKE V2.x supports only the CCF modules, and there is no upgrade path between TKE V2 and TKE V4).
- The CCF feature is not available on z990/z890. The Crypto assist feature (FC3863) is a prerequisite for PCIXCC installation.

Archived

- Figure 4-1 illustrates the compatibility between the TKE versions and models of 9672 and zSeries servers.

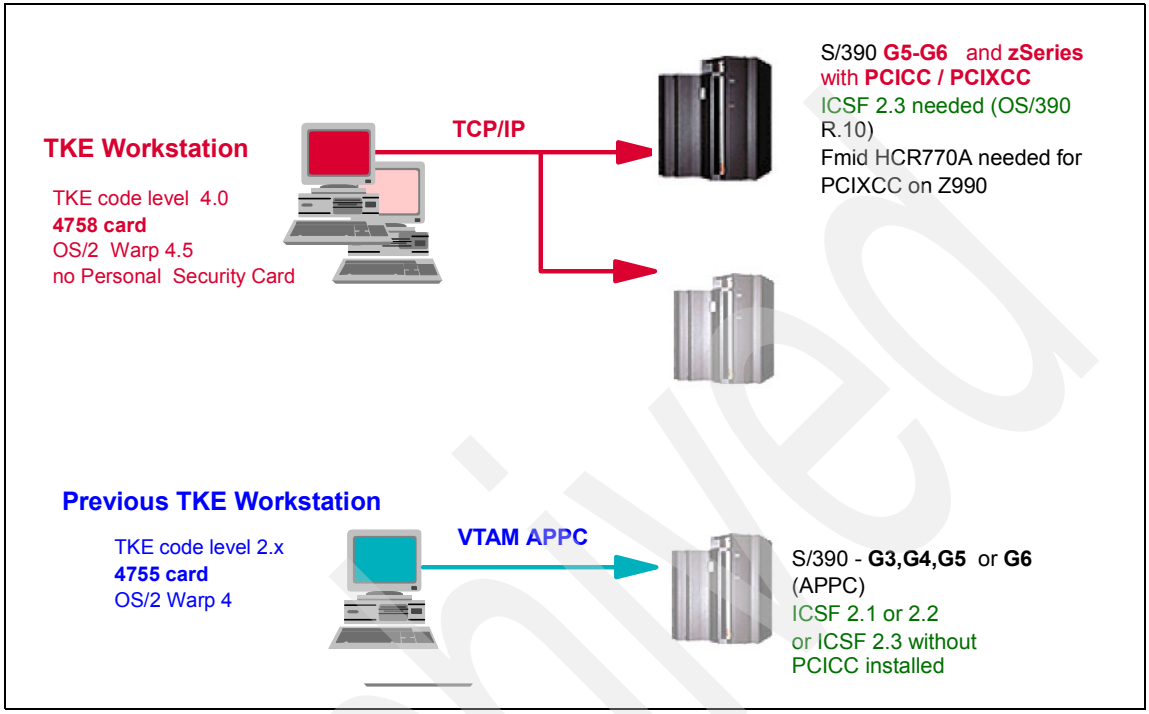

Figure 4-1 TKE workstation configuration according to CMOS models

- The TKE workstation V4 communicates with the host system using the TCP/IP network via a Token Ring or Ethernet adapter card, as shown in Figure 4-2 on page 62.

  The TKE z/OS host must run—on top of TCP/IP and ICSF—a TKE Host Transaction Program that listens over a dedicated TCP/IP port and serves the requests issued by the connected TKEs.

Note: For G4/G5/G6/Z800/Z900 the TKE option feature must be ordered with the CCF enablement feature code, because there is no PCICC FCV enablement feature code that includes TKE support.

Archive

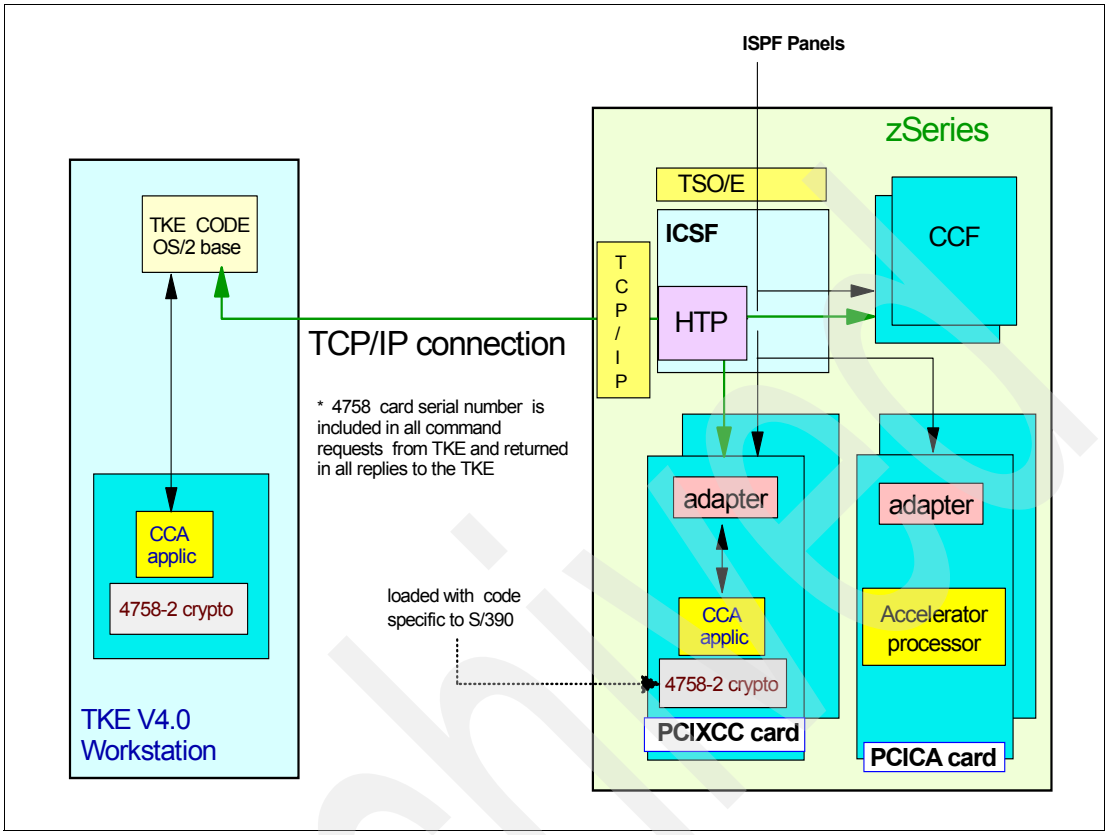

Figure 4-2 TKE workstation in a PCIXCC environment

- TKE customization

  The TKE workstation is shipped from manufacturing with code already loaded and parameters set to default values.

  - Step one will define TKE authorities (administrator, keymen), set the TKE Master Key, and define TKEUSER profiles (people who will manage host cryptographic processors). TCP/IP connection parameters to the host partition must also be entered; see Figure 4-3 on page 63.
  - Step two will define and customize host names, host PCIXCC authorities, and access control parameters; see Figure 4-4 on page 64. If several TKEs access the same cryptographic coprocessors, authorities and access control must be defined only from the first installed TKE.
  - If G5/G6/Z800/Z900 cryptographic coprocessors must also be controlled from the TKE, see *zSeries Crypto Guide Update,* SG24-6870.

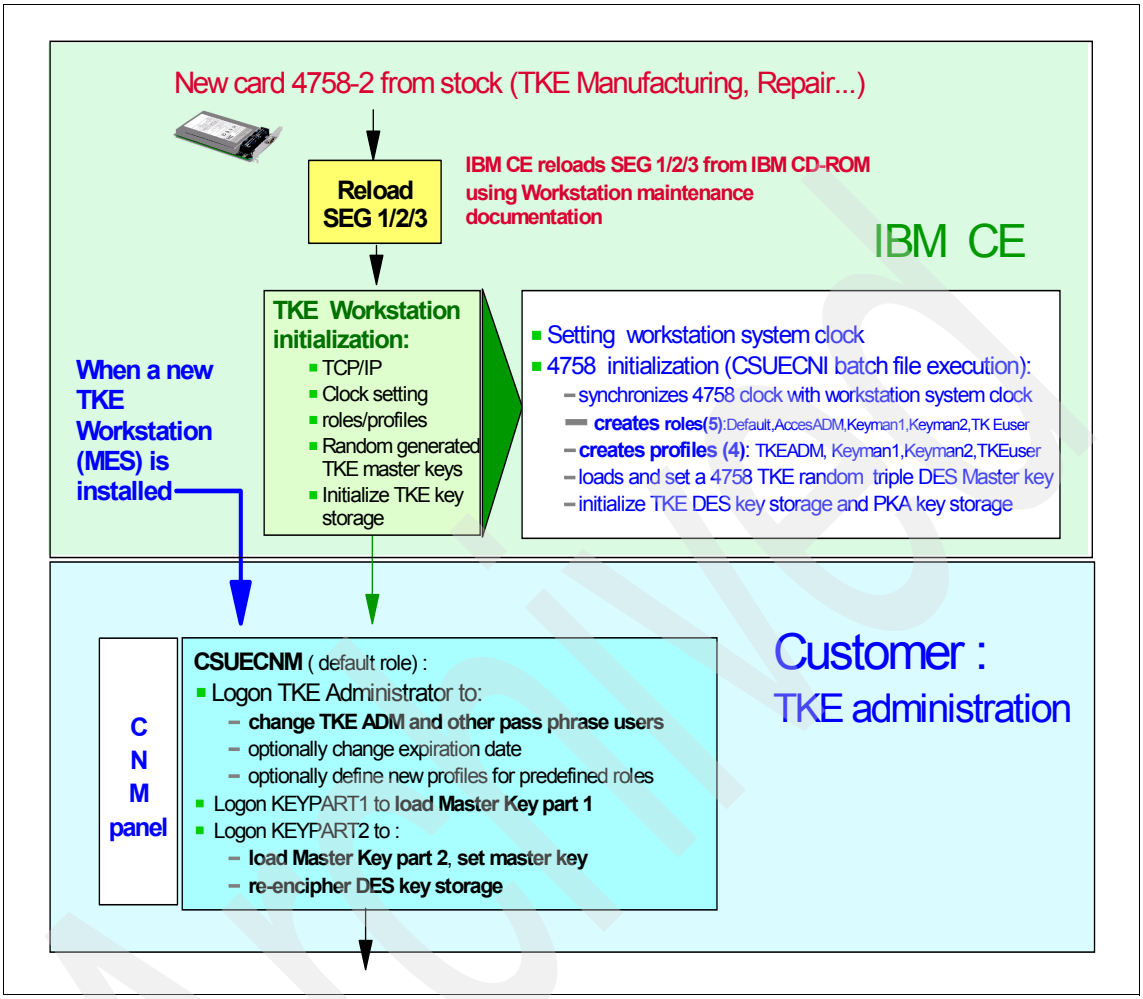

Figure 4-3 TKE V4 internal card 4758 setup process data flow - part 1

Archive

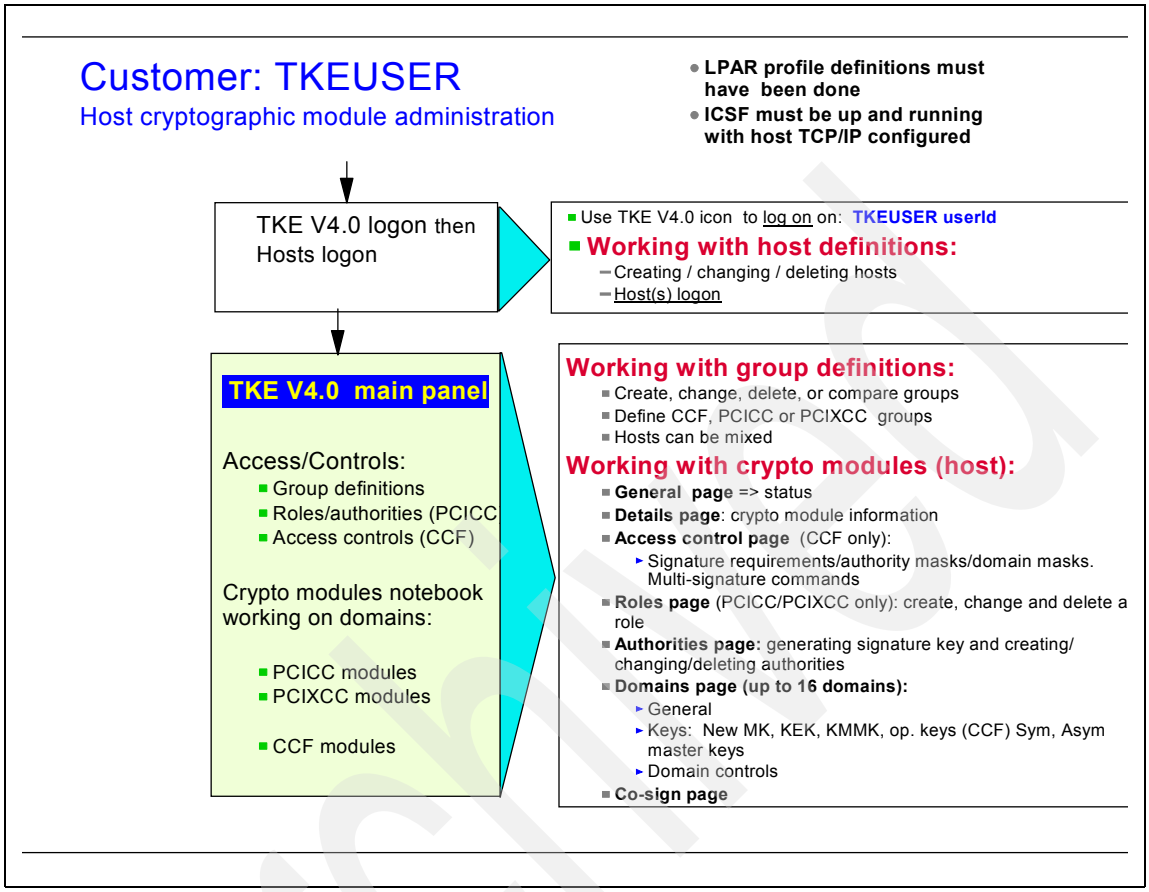

Figure 4-4 TKE process data flow part 2: host definitions, host CCFs, and PCIXCC/PCICC customization

4.1.2 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 *ICSF TKE Workstation User's Guide,* SA22-7524-05, 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 officers; the TKE users; the Host Crypto modules security officers; the Host Master Keys officers, and so on.
2. The logical partitions' cryptographic coprocessor definitions should be done, and the proper LPARs should be activated. See PR/SM guide and *ICSF TKE*

Workstation User's Guide, SA22-7524-05 Appendix D, "LPAR considerations."

3. The TKE z/OS host should have TCP/IP, ICSF, and the TKE Host Transaction Program properly configured and started. Refer to 4.3, "TKE application: managing host Crypto coprocessors" on page 82.

4.1.3 The TKE V4 software

The software installed on the TKE V4 includes the following:

- OS/2® Warp 4.5
- 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. It 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 4
- Java™ runtime environment 1.3.1

4.1.4 TKE workstation installation - general information

During the manufacturing process, the TKE workstation application is installed on the PC (currently, an IBM 8503, but also IBM 6862 and 6578) hard disk. TKE IBM 4758 mod 002 card internal CCA code segments 1, 2, 3, and FCV are also loaded into 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, because 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
- See *ICSF TKE Workstation User's Guide,* SA22-7524-05.

The TKE workstation application can be reloaded from the TKE CD-ROM and the previously saved backup diskette. When upgrading from TKE V3.x to V4, customized data are saved on a TKE backup diskette and a binary backup diskette before installing the new code from CD-ROM.

Note: 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. This is 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 *Maintenance Information for Desktop Consoles,* GC38-3115.

4.1.5 TKE definitions

In this section we explain the TKE terminology.

TKE workstation access control

TKE 4758 cryptographic card access control mechanisms use the *roles and profiles* concept (refer to Figure 4-5 on page 67). 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 the customer security policy. This facility, included in TKE code, is started from an OS/2 window session as shown in Figure 4-11 on page 75.

Role

A role defines a class of TKE users. When creating or changing a role, the TKE administrator defines the TKE 4758 Crypto card commands that will be authorized for users mapped to this role. Each command the card can perform can be individually enabled or disabled according to the setting of an “Access Control Point” assigned to that command. See the IBM 4758 CCA code support documentation for details on the control access points.

TKE has a DEFAULT role. Use of the DEFAULT role does not require a user profile. Any user can use the services permitted by the DEFAULT role without logging onto or being authenticated by the coprocessor. However, the role is limited in the operations it is allowed to perform.

Note: 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 4-10 on page 74.

Archive

Profile

A profile defines a specific user. It contains a user name and pass phrase information and is mapped to one, 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 can 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 pass phrase. We recommend that you change this pass phrase after TKE setup to insure full access security.

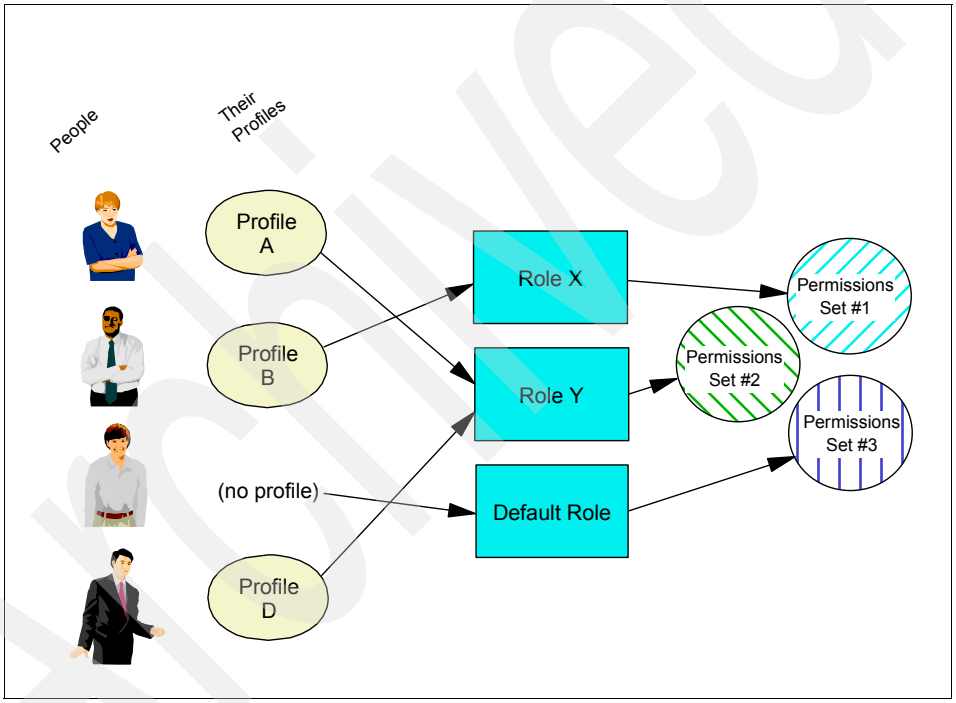

Figure 4-5 Role-based access control

The TKE administrator has to create all user profiles required by the security policy in effect; see Figure 4-13 on page 77.

Archived

Important: The PCIXCC card chips in the host systems use a very similar access control concept, because they also use roles and authorities. However, these roles and authorities apply to the S/390 coprocessors and must not be confused with TKE 4758 roles and profiles.

To summarize:

- The TKE workstation has its own *roles* and *user profiles*.
- The PCIXCC modules have their own *roles* and *authorities*.

TKE Master Key

The TKE IBM 4758 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 to be stored on the TKE hard disk in files DESSTORE.DAT and PKASTORE.DAT (also named TKE keystores). 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, 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 storage

The TKE workstation key storage consists of files on hard disks 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 the clear outside of the TKE 4758 secure hardware.

There are two key storage files 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)

4.2 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 4-6.

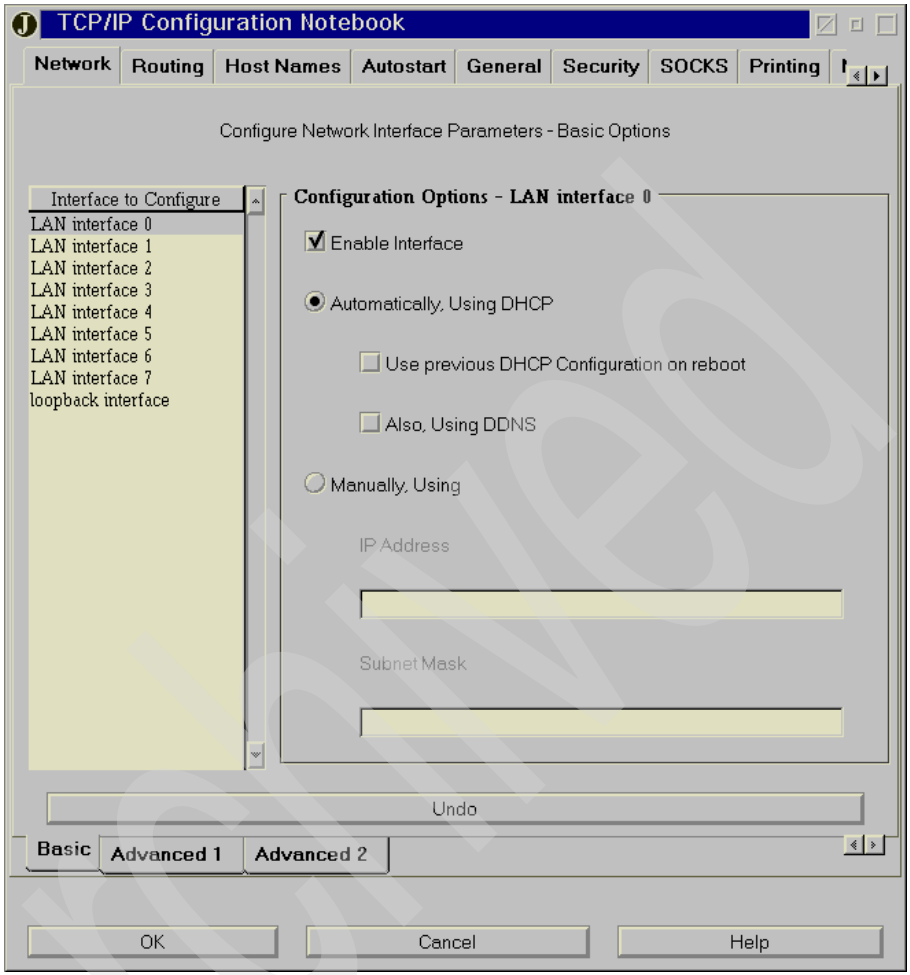

Figure 4-6 TCP/IP Configuration Notebook

1. Fill in 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.

2. Read the Configure Routing Information online help at the Routing tab to determine if any special situations apply to the computer you are configuring.

   If so, you may need to complete the field on the Configure Routing Information page (however, this was not needed in the case of our DHCP network); refer to Figure 4-7 on page 70.

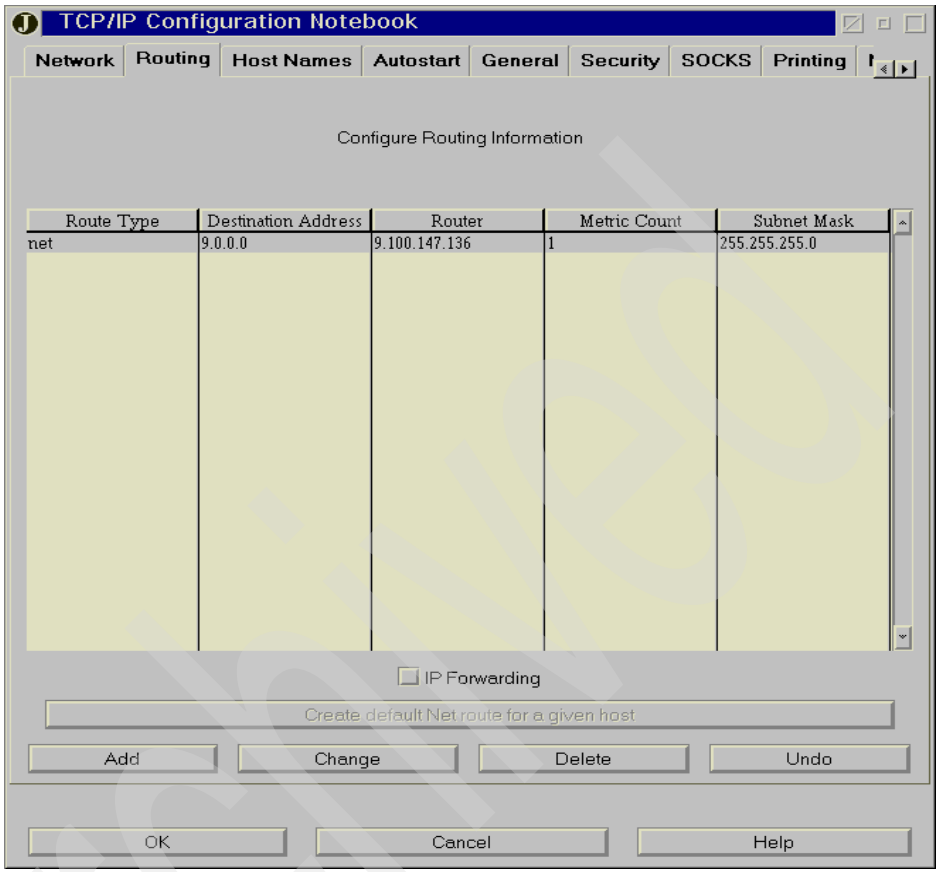

Figure 4-7 TCP/IP routing tab

3. 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 4-8 on page 71.

Archive

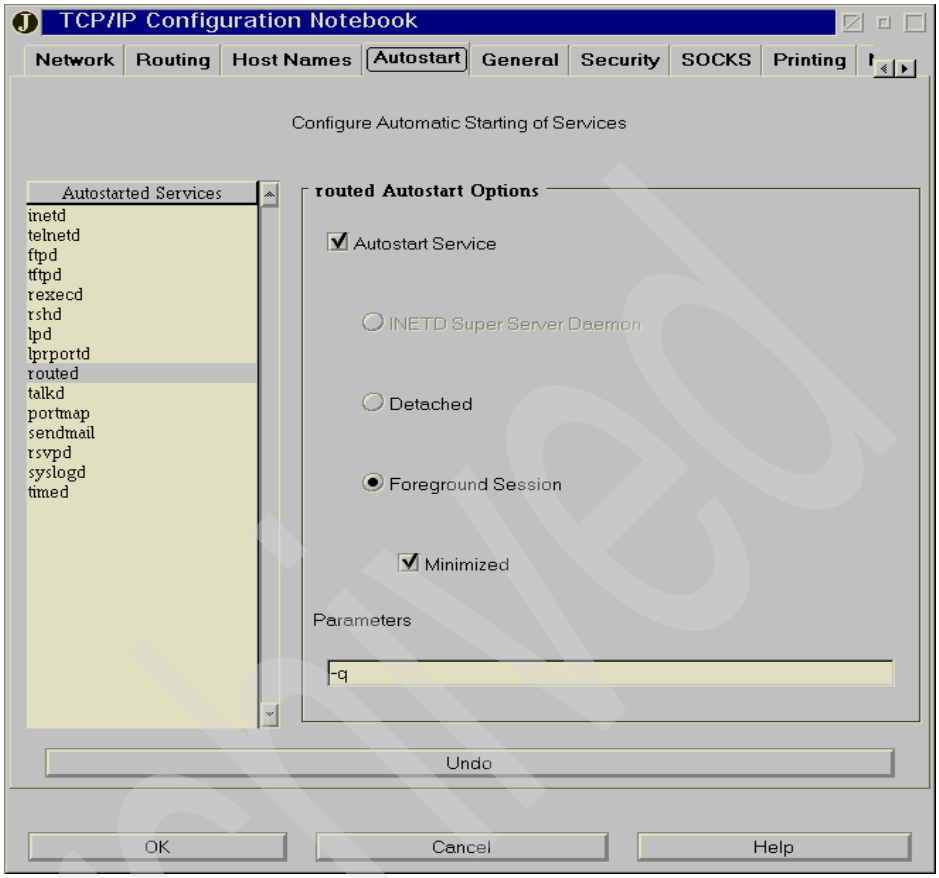

Figure 4-8 Autostart tab

4. Select the **Host Names** tab and on the Configure Name Resolution Services page, provide the host name, local domain, and name service addresses, as shown in Figure 4-9 on page 72. (This is not needed with a DHCP network.)

Archived

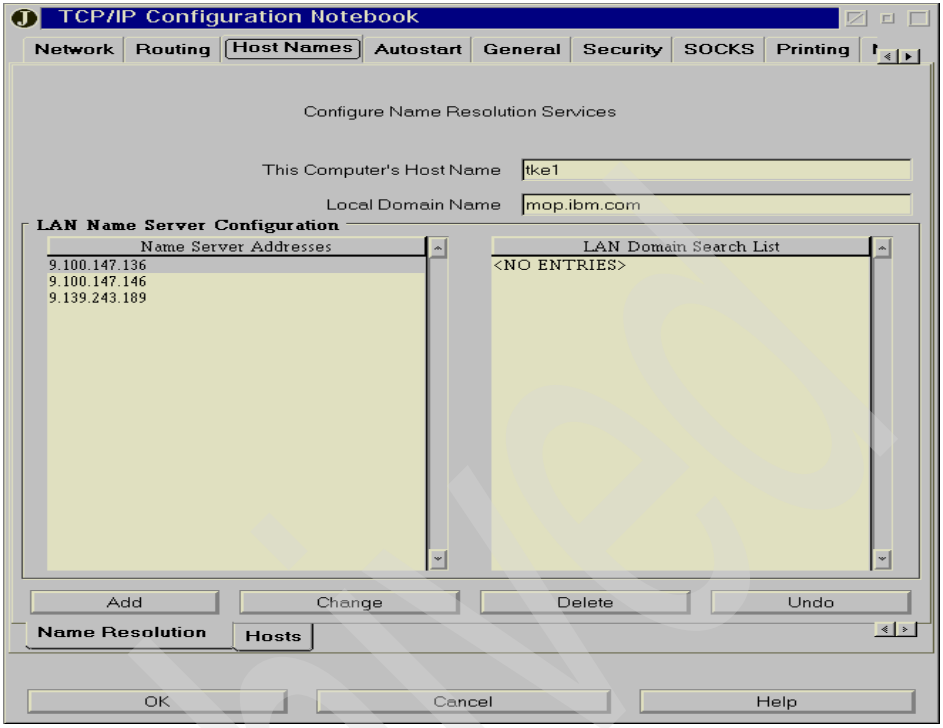

Figure 4-9 Host Names tab

4.2.1 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 are available.

Normal restoration of a failing TKE must be done using the CD-ROM and the backup diskettes.

Important: 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 storage; refer to 4.3.5, “Backing up the TKE files” on page 141 for more information.

TKE workstation initialization

This is done 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.

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:

1. It sets the 4758 clock.
2. It creates five TKE default roles (shown in Figure 4-10 on page 74).
   - The DEFAULT role allows you to view roles and profiles, and to re-initialize the 4758. This is publicly accessible, and no pass phrase is needed (simply press Cancel when prompted for profile name and pass phrase). Note that the **initialize** command from the CNM panel (selecting **Crypto node** then **initialize** in the pull-down menu) will erase all setup done by batch file 4758initialize.cni. If this option is used, you will have to run the TKE initialization batch file again.
   - 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 code releases.

   - The KEYMAN1 role allows you to clear the TKE 4758 new Master Key register 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 4.4, “4753 Key Token Migration facility” on page 143 for more information about this facility). This is the TKE general user role.
3. It creates four TKE default profiles, as shown in Figure 4-10 on page 74.
   - The TKEADM profile is mapped to the TKEADM role, with the pass phrase TKEADM.

- The KEYMAN1 profile is mapped to the KEYMAN1 role, with the pass phrase KEYMAN1.
- The KEYMAN2 profile is mapped to the KEYMAN2 role, with the pass phrase KEYMAN2.
- The TKEUSER profile is mapped to the TKEUSER role, with the pass phrase 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.

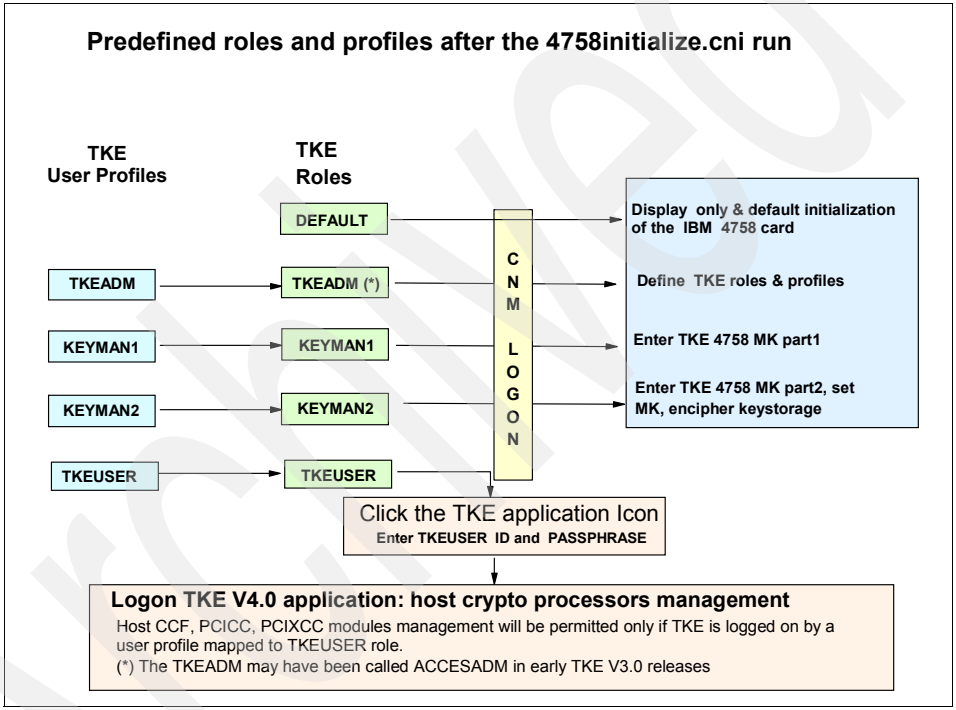

Figure 4-10 TKE workstation predefined roles and profiles

4.2.2 TKE access control administration

This step is used to change the TKE user profiles default pass phrases and replace the IBM 4758 Master Key which was randomly generated during the TKE initialization process, because no backup is available to recover this key. These tasks are executed using the Cryptographic Node Management (CNM) utility.

Archived

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, because 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
```

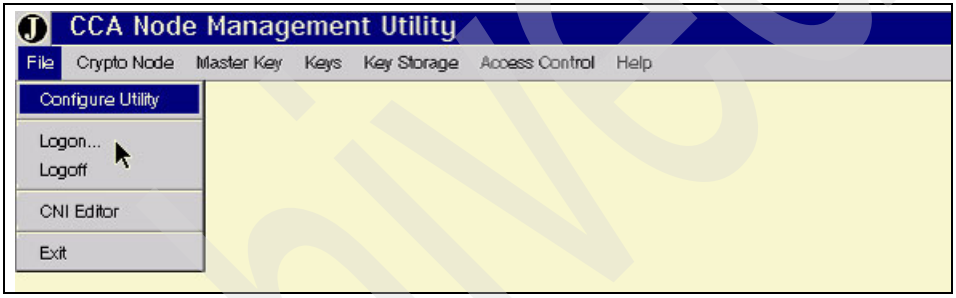

Figure 4-11 TKE workstation CNM utility panel

The panel shown in Figure 4-11 will be displayed. When the CNM utility is started, only the DEFAULT role commands are permitted. As previously mentioned, the DEFAULT role allows you only to display roles and profiles and to initialize the 4758.

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 4-12 on page 76. Note that the user ID and pass phrase are case sensitive.

Figure 4-12 CNM utility logon as default TKEADM user with default pass phrase

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 pass phrases 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 **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 4-13 on page 77.

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 security policy at your site.

Archived

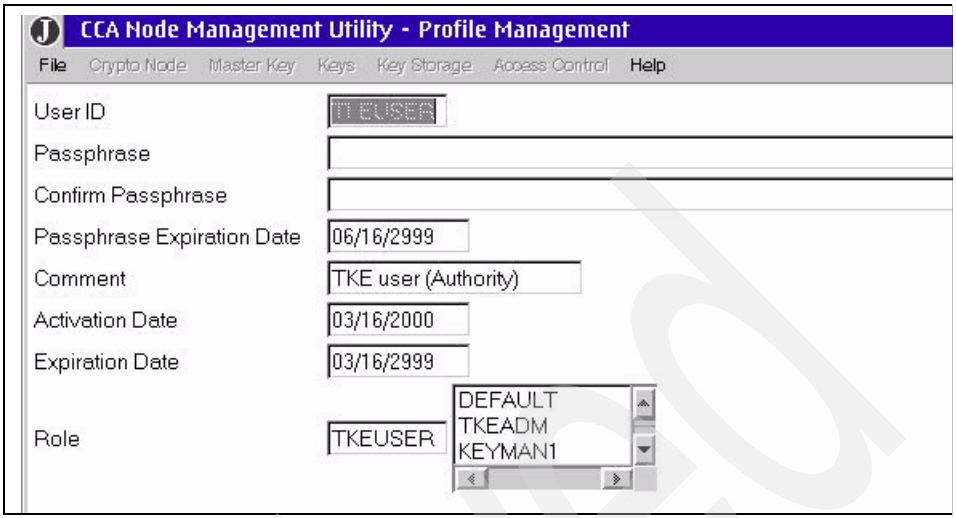

Figure 4-13 TKE workstation profile example: TKEUSER default profile

To create or change roles, select **Roles** in the access control pull-down menu and then press **New** (to create a role) or **Edit** (to change a selected existing role). An example is shown in Figure 4-14 on page 78.

As explained in 4.1.5, “TKE definitions” on page 66, 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 predefined roles. However, you can use this as an opportunity to change the validity days specification.

Archived

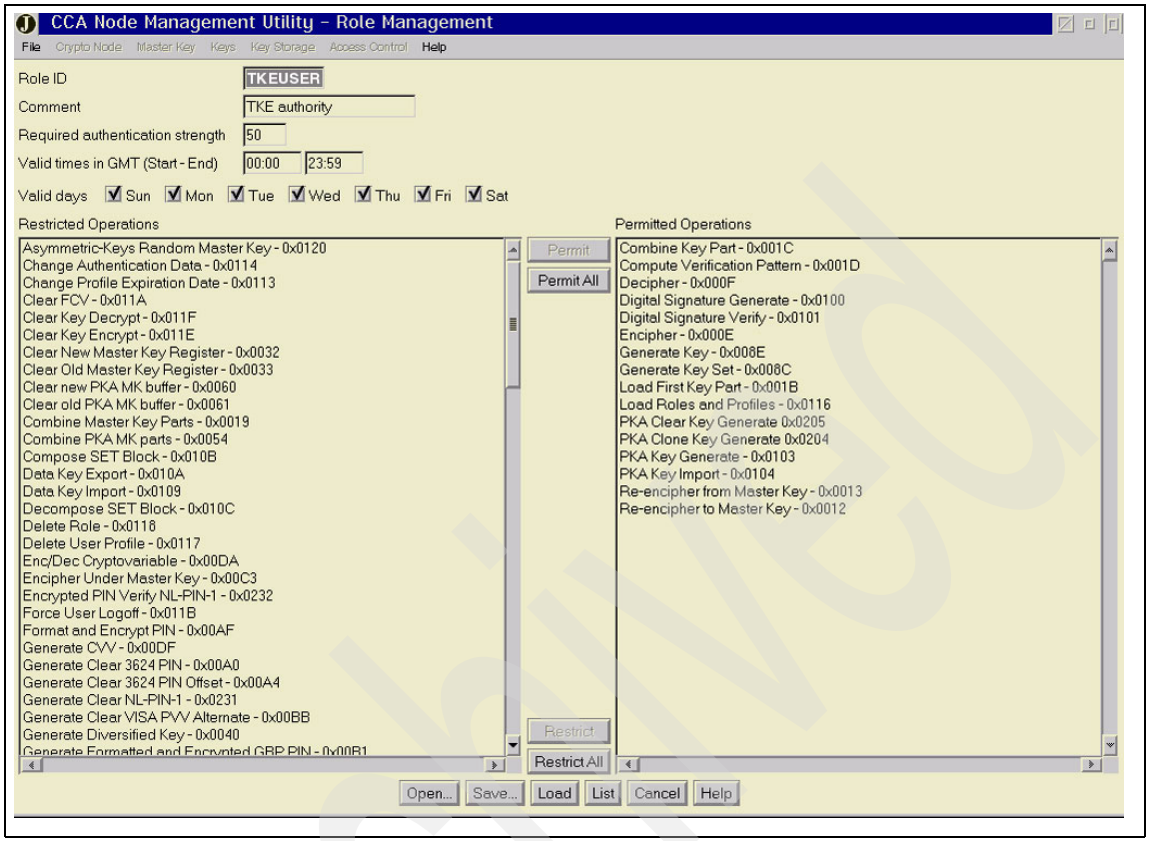

Figure 4-14 TKE workstation role example: TKEUSER default role

As shown in Figure 4-14, the left column of the role panel shows the unauthorized operations and the right column shows the operations permitted for the role. You can move operations from one column to the other, according to the specific requirements of your site—but keep in mind that any change in the roles default commands setup may cause unexpected results when using TKE to manage host Crypto modules. Valid days of the week can also be selected.

When the creation or modification of roles, profiles, and pass phrases is complete, the TKEADM user ID has to log off from the Crypto node using the File drop-down 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

Archived

using KEYMAN1 for the first key part and KEYMAN2 for the middle and last key parts, as follows:

- Log on to the CNM utility as KEYMAN1.
- 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**.

Notes:

- 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 drop-down menu.
- Ensure that you *save* the key part for backup purposes.The key part can be saved on paper or saved on diskette by using **Save...**; refer to Figure 4-15 and Figure 4-16 on page 79 for illustrations.

- KEYMAN1 must then log off from CNM.

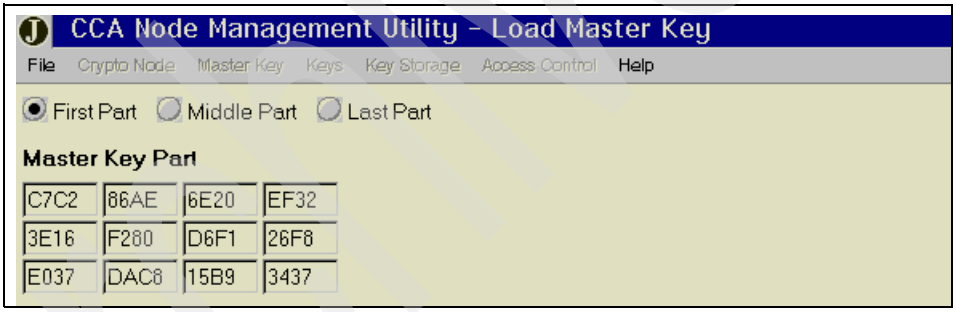

Figure 4-15 TKE workstation MK - first part generate and load

Figure 4-16 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:

- Log on to the CNM utility as KEYMAN2.

- 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.

Setting the Master Key and REENCIPHER DES and PKA key storage

To set this key and storages, do the following:

- Stay logged on as KEYMAN2.
- 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 4-17.

Figure 4-17 Set TKE workstation Master Key successful panel

KEYMAN2 now has to re-encipher the DES and PKA key storage. To proceed, do the following:

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

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

Customize tke.ini parameters

You can customize a number of parameters by editing the tke.ini file; first issue this command:

```
cd tke\tke
```

Then, using TEDIT or `E`, edit the tke.ini file, as follows.

- Blind key entry option

  This option masks 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 add the following statement, if it does not already exist:

  BLIND_KEY_ENTRY=TRUE

Archived

- TRANSPORT_KEY_POLICY (keys used to protect TKE-to-Host transactions)

  This option selects the default key transport policy. The allowed values are 1, 2, or 3. This value is more conveniently changed from the TKE main application panel function; refer to Figure 4-18.

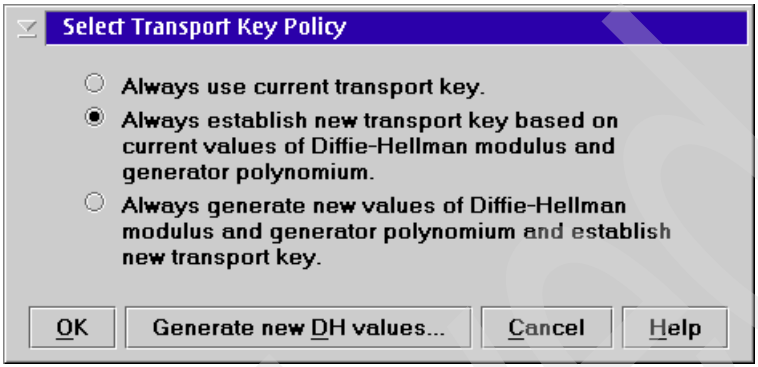

Figure 4-18 Define key policy on the main TKE panel

- DEFAULT DIRECTORY

  This option specifies the directory selected when opening a window to specify where to save an authority signature or a key part.

  Initially this is set to default; it will be changed the first time you save a key to a binary file.

- SERIALIZE_PATH

  This option specifies where the TKE saves internal information about hosts and groups. The files HOST.DAT and GROUPS.DAT are saved there.

- MESSAGE_PATH

  This option specifies the directory where TKE (on user request) saves the error information in a file named TKE.MSG.

- If your security policy requires that generated keys be saved to diskette and not to the hard drive, you must enable the FLOPPY_DRIVE_ONLY feature.

  This function forces generated key parts to be saved on floppy diskettes. Make sure FLOPPY_DRIVE_ONLY=TRUE.

Save the file and close the OS/2 window.

4.2.3 Starting the TKE application

TKE initialization and setup is now complete. You can start the application by opening the TKE folder and double-clicking the TKE V4.x icon.

Archived

4.3 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 z/OS host system.

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

4.3.1 Managing modules

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

All coprocessors in the group will be updated at the same time, except when loading operational key parts to key part registers, when only the master PCIXCC will be loaded.

The TKE administrator has to be very careful when defining groups for the PCIXCC.

- On z990/z890, at system activation profile definition, the same domain control index and the same domain usage index can be defined for more than one logical partition. However, the cryptographic coprocessor number coupled with the usage domain index must be unique across all active partitions.
- Since the TKE Host LPAR needs access to all the cards, no other LPAR can have the same usage domain index as the TKE LPAR. For the TKE target LPARs, the number of group domains defined really depends on how the LPARs are set up—domain and card availability and whether the same keys will be loaded. Remember, cards can only be shared as long as the same usage domain index is not being selected. For example, if you have four PCIXCC cards and the following LPAR definitions:

Archived

TKE host LP 0	TKE target LP 1	TKE target LP 2	TKE target LP3
Control Domain 0 1 3	Control domain 1	Control domain 1	Control domain 3
Usage domain 0	usage domain 1	usage domain 1	usage domain 3
Candidate list 00 01 02 03	candidate list 00 01	candidate list 02 03	candidate list 00 01 02 03

One group profile could be defined with all the cards to control LPAR 0 and LPAR 3. Assuming that LPAR 1 and 2 do not share the same master keys, then two more groups would need to be defined. One group would contain cards 00 and 01 and the other group cards 02 and 03. If, however, LPAR 1 and LPAR2 share the same master keys, then only one group would need to be defined that contained all the cards.

As you can see, the TKE Administrator really needs to understand how the LPARs have been defined for usage domain and card allocation and, if possible, what keys will be loaded.

Note: Because it is important that *all* Crypto modules in the group are in the same state (that is, they have the same definition of roles and authorities for PCIXCC 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 that 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 compare function in the notebook main panel will compare the module and list the differences, if any.

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

Required levels of authorization

Working with the z990/z890 Crypto coprocessors requires the following three levels of authorization (this is illustrated in Figure 4-19 on page 85):

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 requires a TSO user ID and password known by 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 PCIXCC card has a preset default authority mapped to a default role (INITADM). This authority will be used until new roles and authorities have been defined for PCIXCC administration.

     An *authority* is identified by its index and has its own signature key pair. Authority 00 is the preset default authority for the PCIXCC. 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) PCIXCC. UP to 100 authorities can be created for PCIXCC cards.

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

     Note: If G5/G6/Z800/Z900 CCF Crypto coprocessors have to be managed by the same authorities, keep in mind that a CCF module has 16 preset authorities and that there is no way to create or delete authorities. To keep consistency in coprocessors management it may be recommended to use the same authorities for all these coprocessors and so to use a maximum of 16 authorities. See *zSeries Crypto Guide Update,* SG24-6870 for details.

     The default signature must be loaded (from the TKE main panel functions pull-down menu) so that commands can be accepted by a newly installed (or zeroized) CCF customized according to the installation's security policy.

– In a system with multiple Crypto modules, there is no requirement that an authority have the same authority index for each module; however, it is recommended to do so.

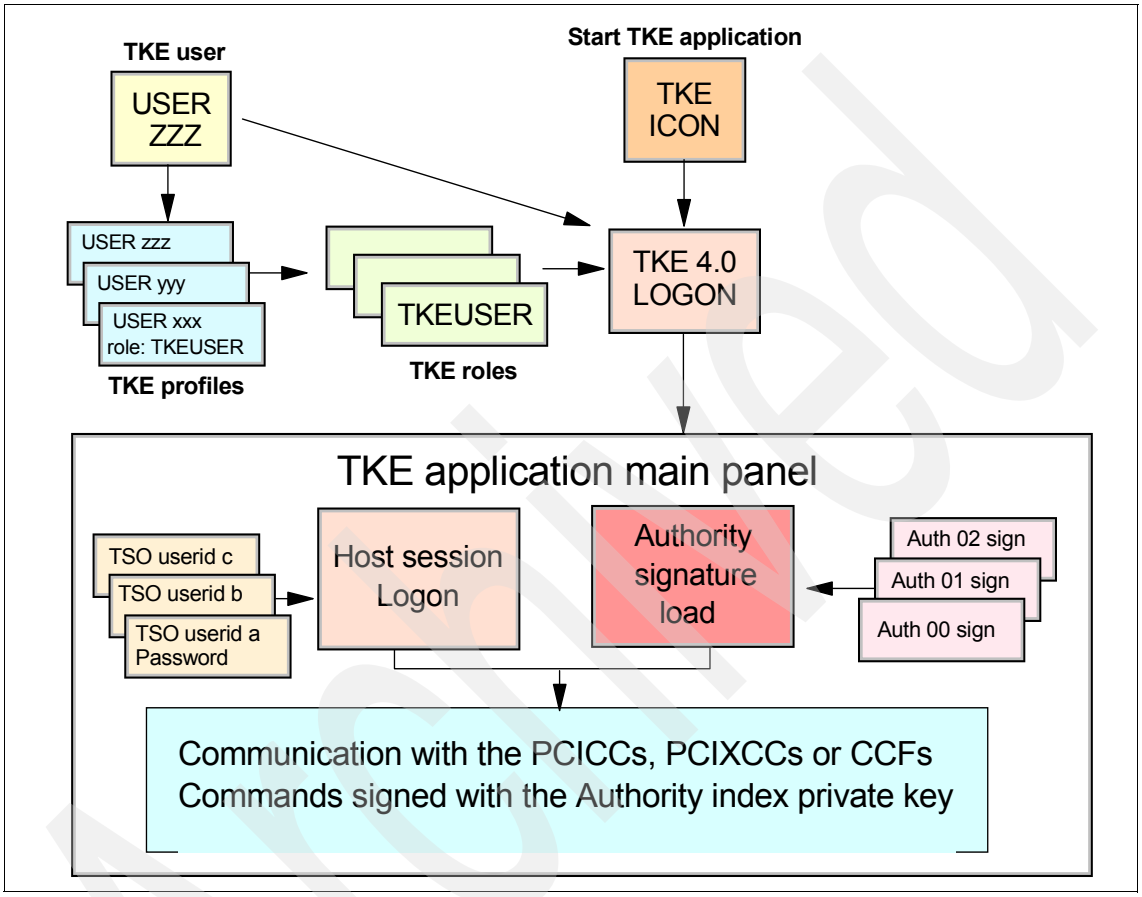

Figure 4-19 Host Crypto modules access logon sequence from TKE

Authority signature key indicator

An informational message indicating `Authority signature key loaded` or `not loaded` is displayed at the lower right-hand corner of the TKE main 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 message will appear, requiring a signature key source to be entered.

Note: If a signature key is already loaded, there is no information about its owner. This signature key will be used to sign any further commands. 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 the TKE entry main panel and then load your signature key again.

4.3.2 PCIXCC setup on the TKE workstation

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

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 V4.x** icon. Enter the user ID and pass phrase (remember, the characters are case sensitive) as shown in Figure 4-20. As already mentioned, we kept the default TKEUSER profile.

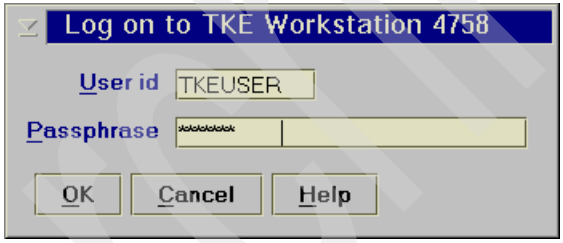

Figure 4-20 TKE workstation logon panel

The main TKE panel is displayed. Initially this panel is empty, as shown in Figure 4-21 on page 87.

Archived

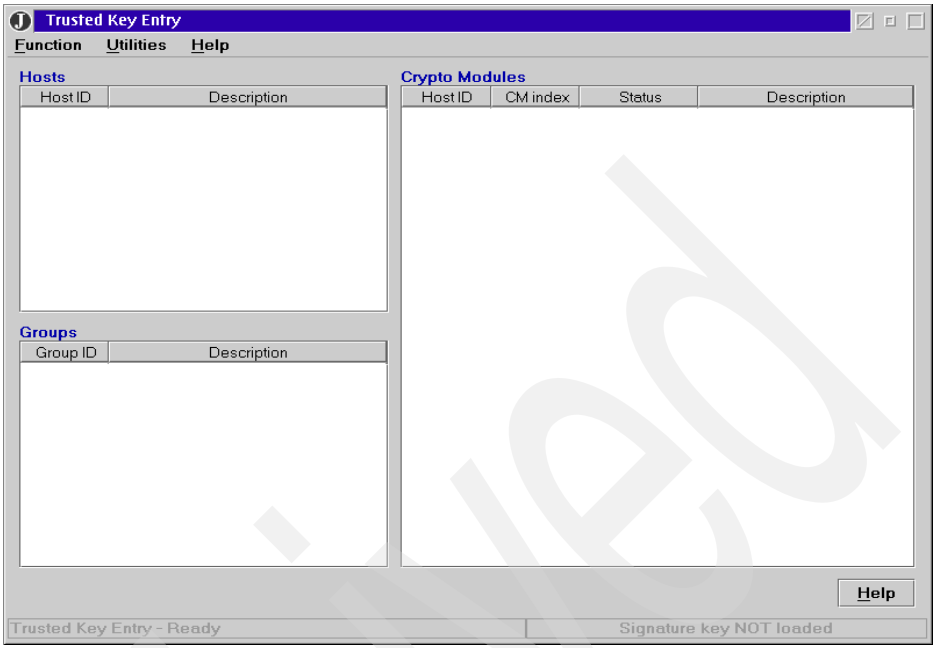

Figure 4-21 TKE V4 application main panel at first logon

Use this main panel to log on to the host system, then select a Crypto module or a group of the same type (existing types are: PCICC, PCIXCC or CCF) of Crypto modules. As a prerequisite, you must enter host and group definitions in the empty panels. (Figure 4-21 displays the informational message: `Signature key NOT loaded` in the lower right-hand corner.)

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

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

Function pull-down menu

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 4-22 on page 88.
- When dealing with a *new* PCIXCC coprocessor, you must select **Default key** for authority index 00, as these are the values preset in the coprocessor.

Archived

(If working with modules already customized, you will have to select Binary file to import the signature of the desired authority index.)

Only one authority index signature can be loaded, so loading the signature must be done each time authority dealing with the host crypto is changed.

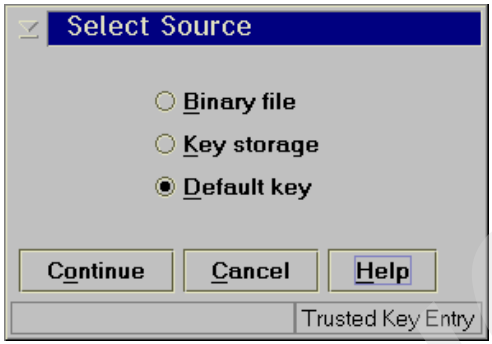

Figure 4-22 Loading signature key; Source: default signature key

- 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 *ICSF TKE Workstation User's Guide,* SA22-7524-05, for further details about these options.

- Exit.

Utilities pull-down menu

The Utilities pull-down menu allows you to manage TKE DES key storage and PKA key storage. From this panel, you can delete existing keys saved in DES or PKA keystore; see Figure 4-23 on page 89. Refer to *ICSF TKE Workstation User's Guide,* SA22-7524-05 for details.

Archived

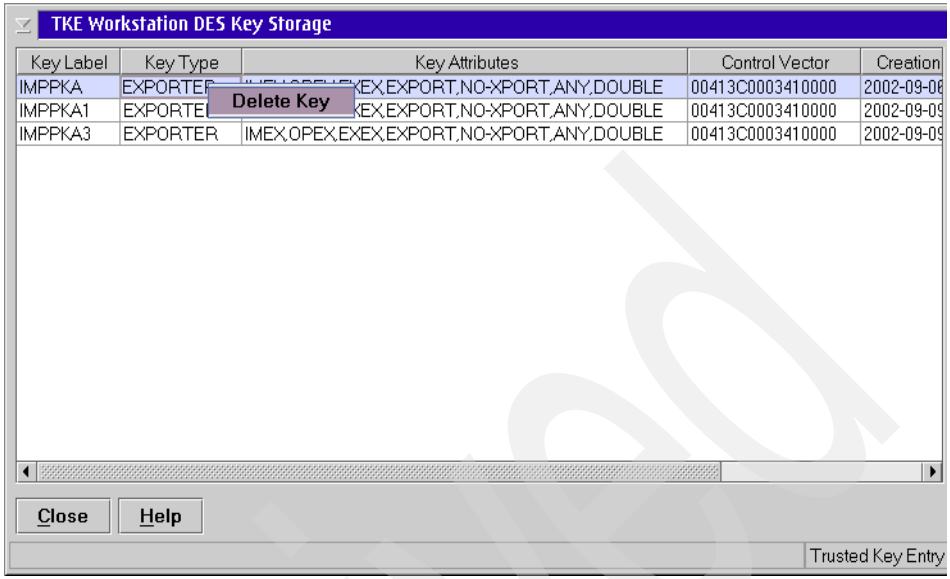

Figure 4-23 Keystore management: Delete Key option

Host system definition and logon from TKE

In this section we describe how to create a host. Initially, the host container is empty.

1. Create a host ID by right-clicking in the TKE main panel host panel 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 z/OS host, as shown in Figure 4-25 on page 90.
3. Pressing **OK** creates a line for this host in the host panel.

Archived

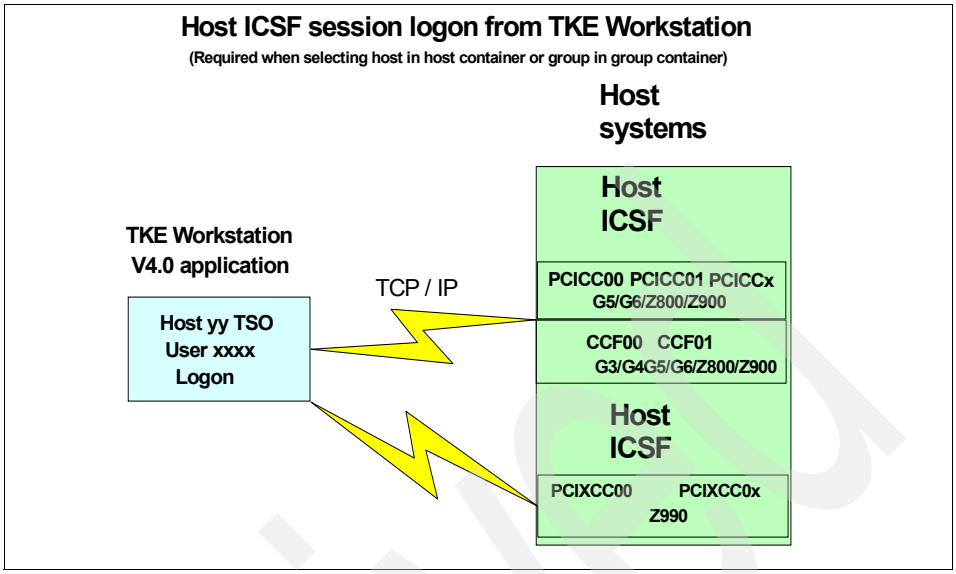

Figure 4-24 TSO host user ID logon from the TKE workstation

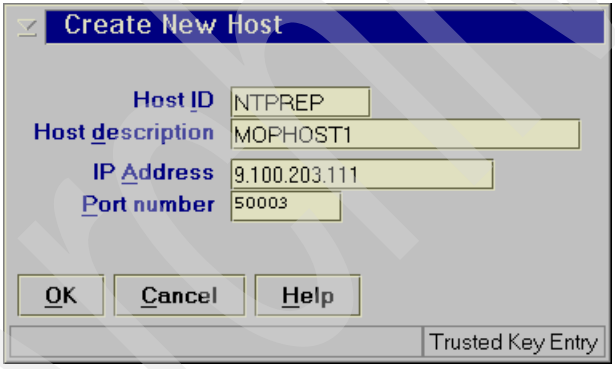

Figure 4-25 Create a new host panel on the TKE workstation - example: NTPREP

To log on to the host, do the following:

1. Click the target host ID line in the host panel. The dialog box shown in Figure 4-26 on page 91 appears.
2. Fill in the fields Host user ID and Password with a TSO user ID and password defined in the target host.

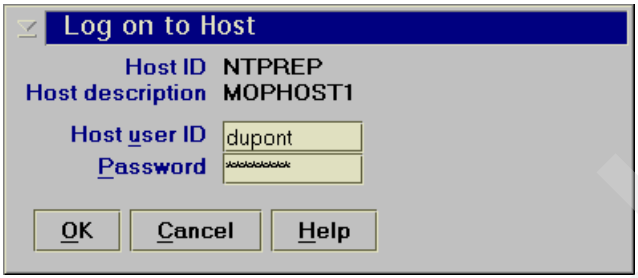

Figure 4-26 Host logon panel on the TKE workstation

Because further processing at the z/OS will be performed under this user ID, we recommend that you consider setting up the appropriate RACF profiles.

Several hosts can be logged on at the same time.

Automated Crypto module recognition

The host PCIXCCs are automatically recognized by the TKE at the time it establishes the first connection with the host. If you added new PCIXCCs and the host is already connected, then exit the TKE application, log on using a user profile mapped to a TKEUSER role, and then perform a logon to the target host by clicking **Select host** on the main TKE panel host panel 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 PCIXCC CMID. The Crypto Module Identifier (CMID) is a serial number burned into secure hardware during the manufacturing process, and 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 the PCIXCC 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 4-27 on page 92.

Note: Contrary to the CCF, the PCICC or PCIXCC module identification does not include verification of the CMPM, because these values are provided signed with the IBM private key and verified by the TKE code.

A Crypto module is recognized when its status on the host system is “Configured”. See Figure 4-28 on page 93.

Note that there are two PCICC processors per card installed in the system, while there is only one PCIXCC processor per card.

Restriction: There is no Crypto module recognition for the PCICA (in fact, PCICA will not be referenced in the TKE workstation).

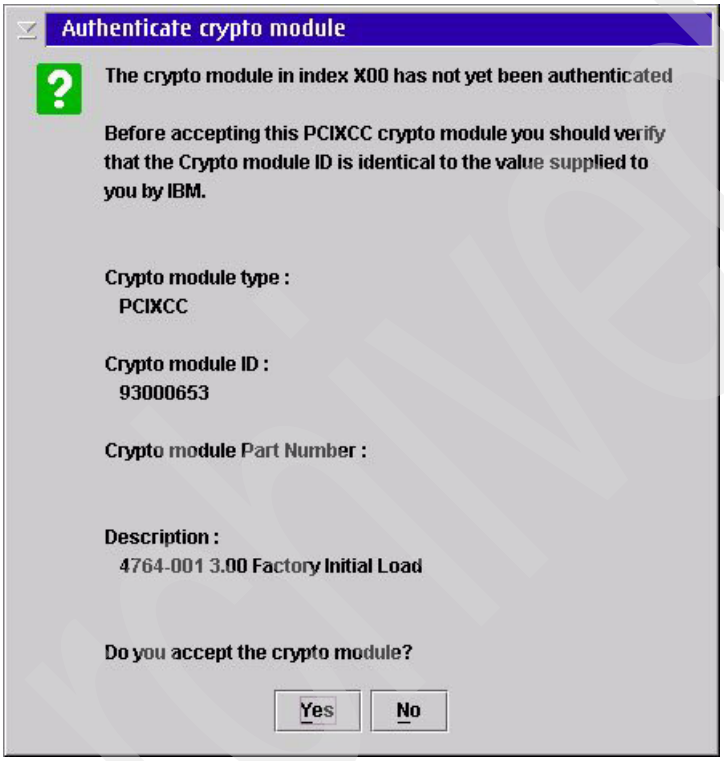

Figure 4-27 PCIXCC module identification panel

Archive

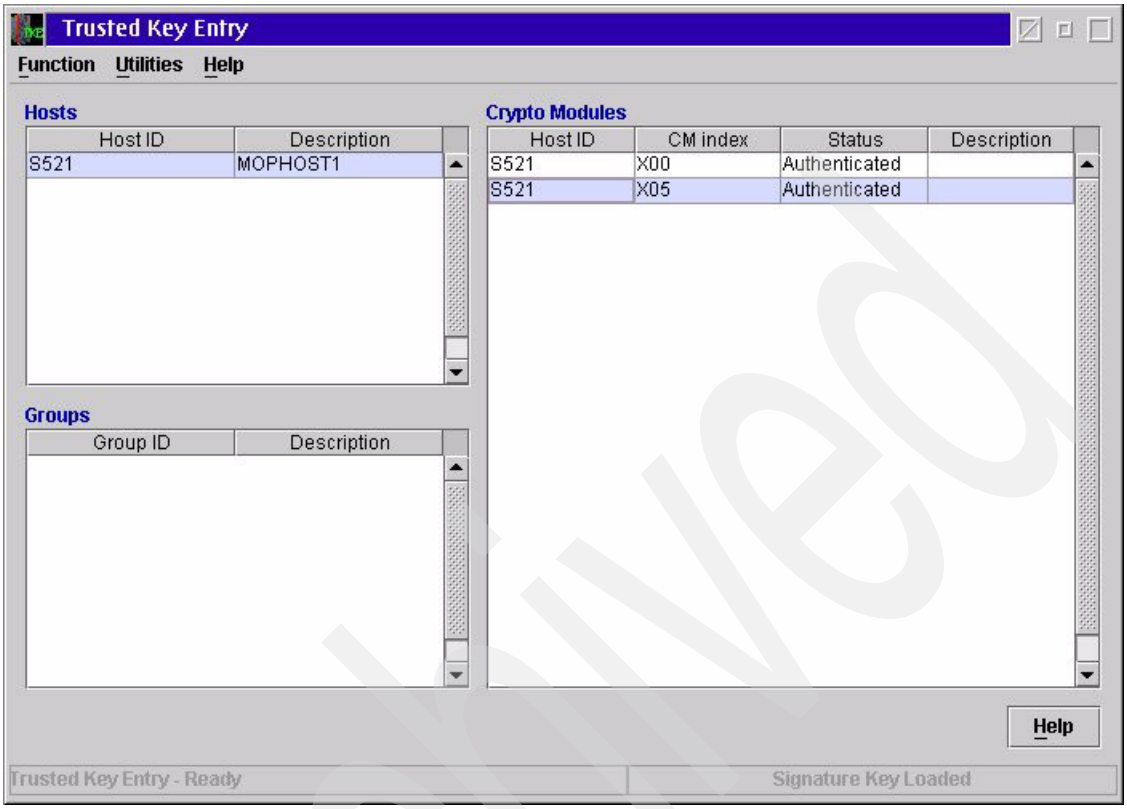

Figure 4-28 TKE main panel after PCIXCC module authentication

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 CCF, PCICC, or PCIXCC group. Right-click the Groups panel and select **New** or **Change.**

Enter (or modify) the group name and group information to specify the module type, select **Host**, highlight Crypto module in Crypto module available on host list and then **Add** (or **Remove**) coprocessors in the group. This is illustrated in Figure 4-29 on page 94.

Archived

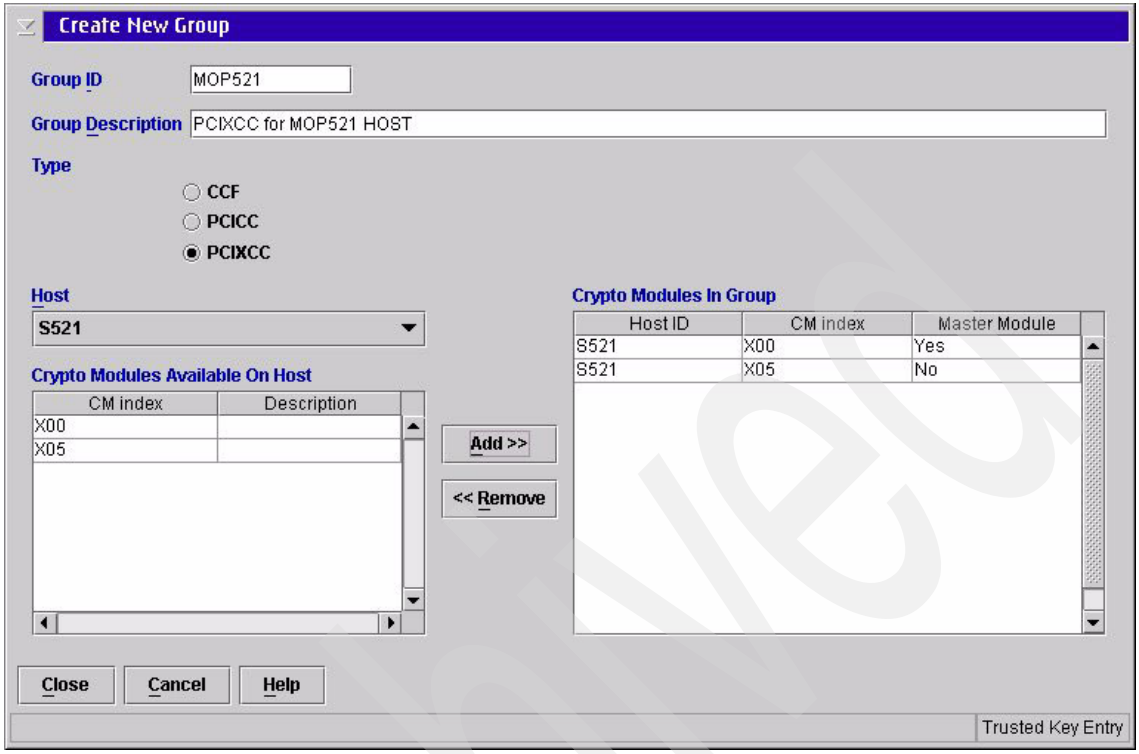

Figure 4-29 Create New Group panel: PCIXCC group consisting of X00 and X05

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 available 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 any module in the group container, and then selecting **Master** in the pull-down menu. The states of the Crypto coprocessors 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 clicking a specific group in the group container on the TKE main panel, and then clicking any module in the module container.

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.

A main TKE panel after definition of host system MOP521 (a Z990) and definition of one PCIXCC group in the z990 is shown in Figure 4-30.

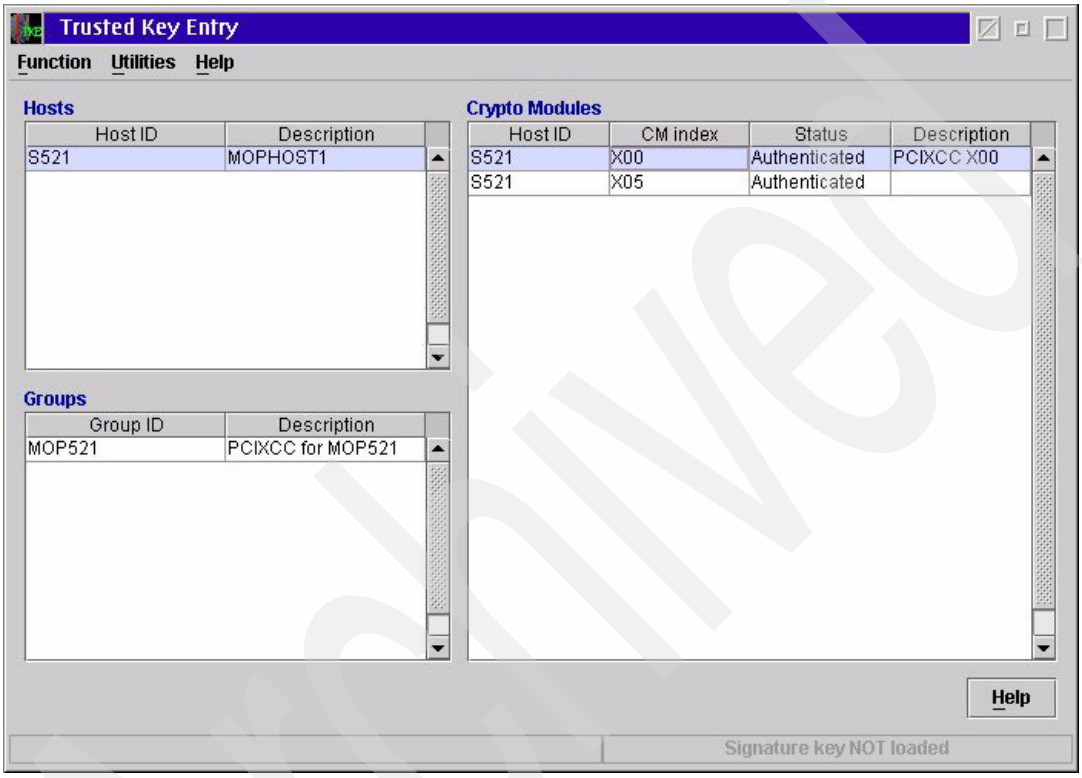

Figure 4-30 PCIXCC group (Z990) created

4.3.3 Manage and update the Crypto module notebook on TKE

The Crypto module notebook is opened by clicking a module in the Crypto module panel. Figure 4-33 on page 98 shows the first page of a PCIXCC notebook. Further information and controls are accessed by selecting the tabs of the notebook. Panels and functions are the same for legacy PCICC and new PCIXCC modules. The only difference is in the domain key page where new functions have been implemented for PCIXCC cards to generate and load Operational keys and RSA keys.

Starting with a new host cryptographic module, you will have to customize authorities and roles for PCXICC, as shown in Figure 4-31 on page 96.

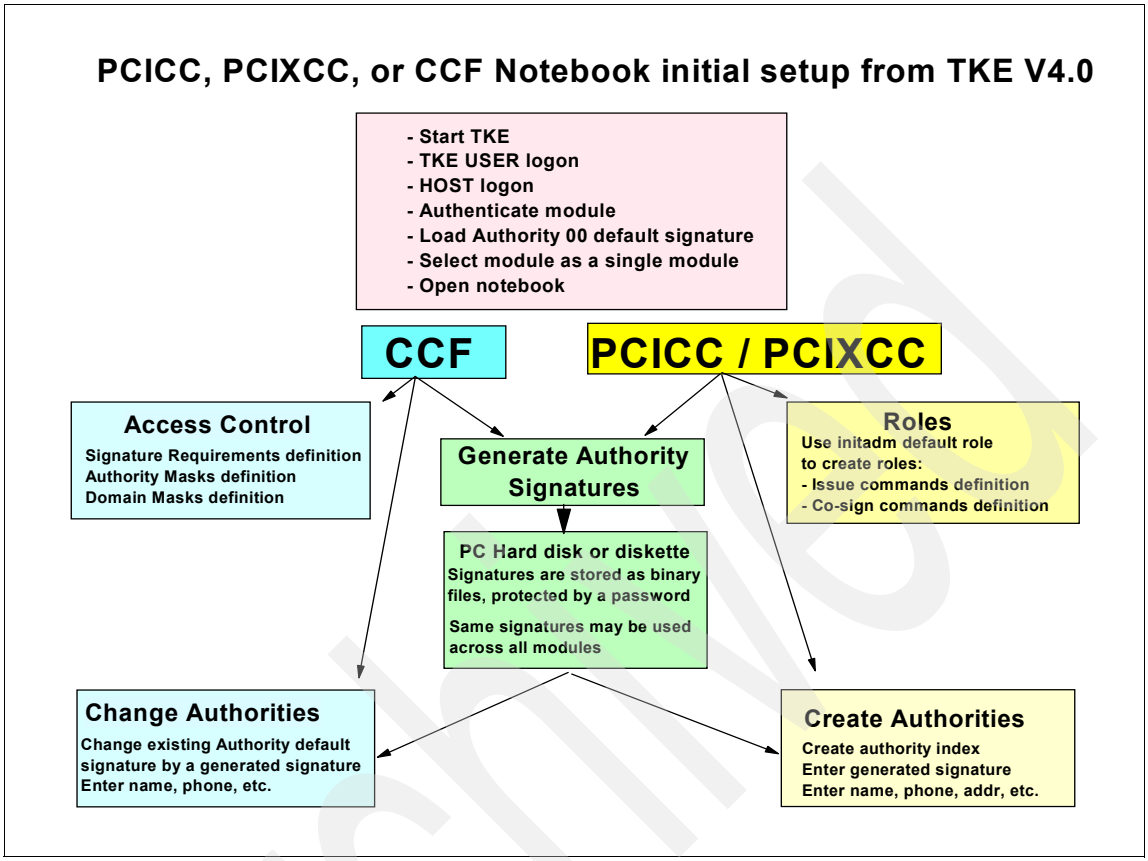

Figure 4-31 PCICC, PCIXCC, and CCF modules initial setup

At this point, you must define the different authorities that will be authorized to manage the Crypto modules according to your own security policy. Signatures will be created for each authority and sent to host cryptographic processors. Control access (CCF) and roles (PCICC and PCIXCC) will be customized for each authority.

Here we have kept the four TKE workstation default roles and profiles, and created five TKE user profiles mapped to the TKEUSER default role (Paul, Mike, John, Tom, and Bill). In our example, a customer wants to manage different types of cryptographic processors on different systems (z990 but also G5/G6/z800/z900).

These five TKE users have been defined as authorities 01, 02, 03, 04, and 05 for PCICC, PCIXCC, and CCF modules. The default TKEUSER has been defined as authority 00, using the default signature assigned to the INITADM role

Archived

(PCIXCC) and LAP/LCB command (CCF) to prevent any locked situations during training. (Note that this authority will have to be changed or removed during real use of TKE.) Authority 12 has the allpower role (all commands can be issued by this authority) that was also created for residency leader usage only.

Figure 4-32 shows an example of authority organization.

Figure 4-34 on page 102 contains tables that establish a parallel between the multi-signature commands in the CCF and the PCICC/PCIXCC functions. Using these tables, if needed, you can determine how to maintain consistency between the authorities defined in the CCF and the ones defined in the PCICC/PCIXCC.

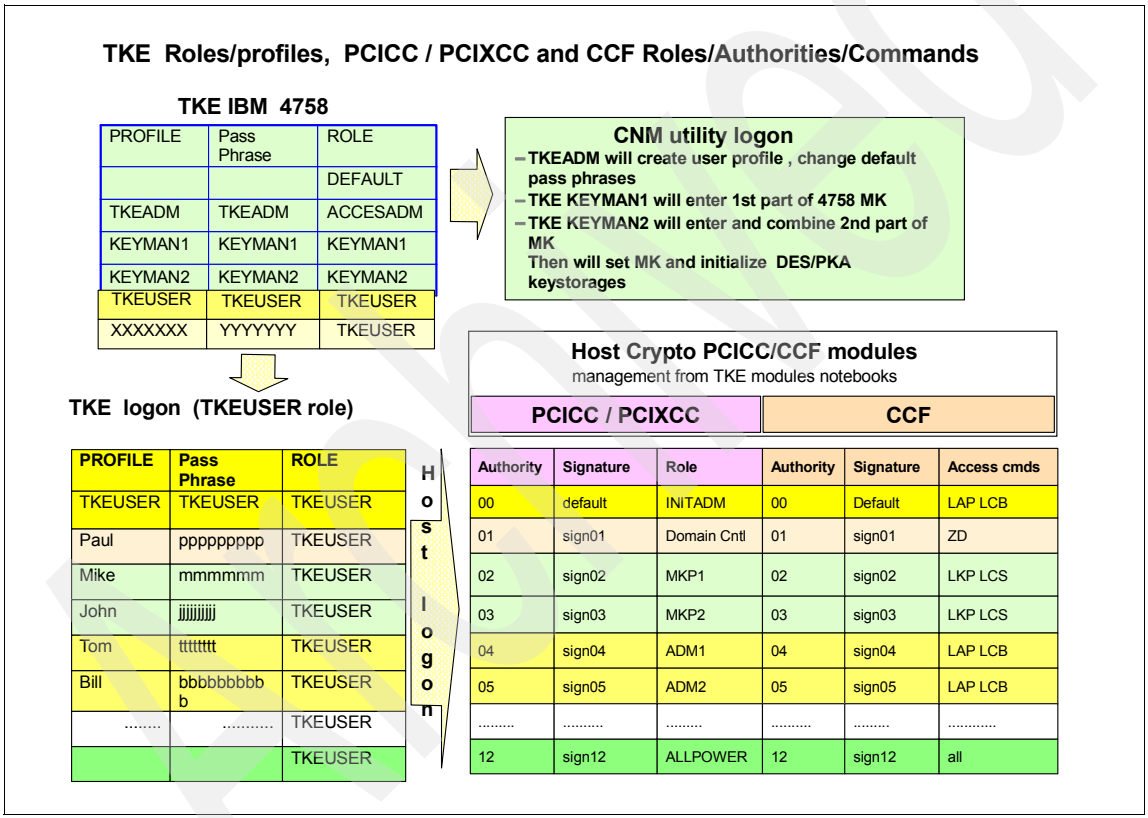

Figure 4-32 TKE roles/profiles, PCICC/PCIXCC/CCF roles, authorities and commands

PCIXCC Crypto module notebook considerations

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

The PCIXCC Crypto module notebook allows access to information related to a Crypto module (single or group): the CMID, all the authorized commands, the authorities public modulus, the LPAR domain controls, and so on.

Updating a group of modules

If working with a newly created group made up of empty or zeroized modules, first select the group from the group container and then click any Crypto module in the module container to open the Crypto module notebook (only Crypto modules that belong to the group are listed in the module container).

The notebook will 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. The Notebook main panel top line will indicate whether the notebook is working with a group or with an individual module.

Updating a single module

To access a single module (as opposed to a group), first select the host in the host panel and then select the desired Crypto module in the Crypto modules panel. The difference with the group access is that you went through the host selection instead of a group selection. The title line on the panel indicates whether you are working with a group (module group administration) or with a single module (module administration).

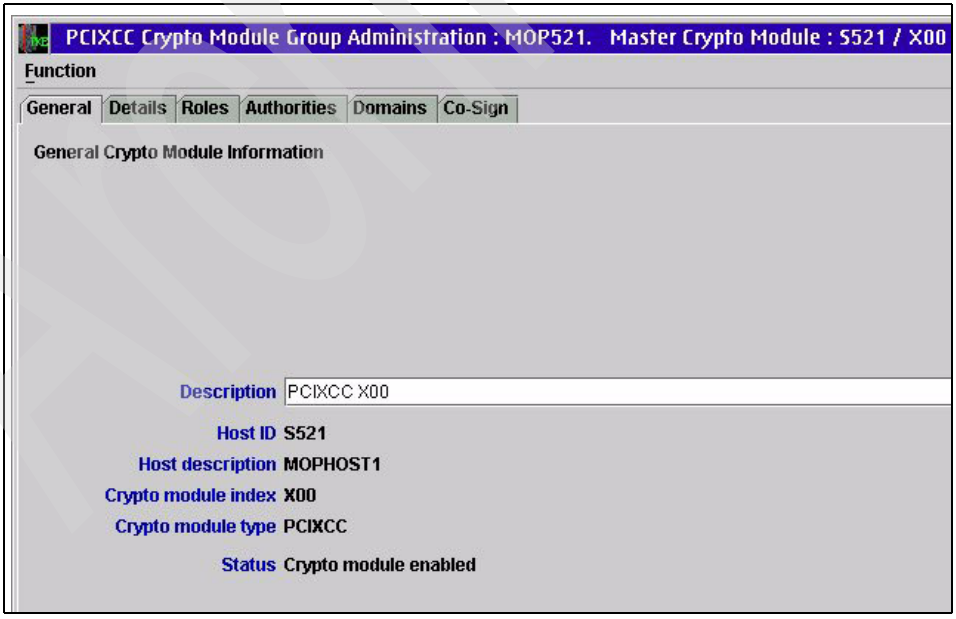

Figure 4-33 Notebook: working with a PCIXCC group; X00 is master

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 whether you are dealing with a group or an individual coprocessor.

Notebook modes

Notebook opens in one of the following modes: update, read-only, pending command, or locked read-only.

- Update mode

  In this 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.

- Read-only mode

  In this 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.

- Pending command mode

  In this mode, the module or group this notebook pertains to has recorded that there is a pending command waiting to be co-signed.

- Locked read-only mode

  The notebook for a group opens in this mode if one or more modules in the group cannot be accessed from the TKE.

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

Notebook functions pull-down menu

- Refresh notebook - Refresh will read the information from the host again.
- Change signature index - This option allows you to change the authority index associated with the currently loaded signature. This can be used only if an authority uses the same signature on different hosts, but has a different authority index on each host.

  If the signature of the new index is different, you must return to the TKE application main panel function to load the right signature for this index.

Archived

- Release Crypto module - If the module is locked by another user, this allows you to release the module. Be careful, though, because releasing a module can damage an ongoing operation initiated by another authority.
- Compare - When working with a group, this compares the parameters of all modules in the group.

PCIXCC Crypto module notebook pages

- General

  This displays only the coprocessor type and index and the host name, as shown in Figure 4-35 on page 105. For PCIXCC there is the possibility to enable or disable the Crypto module; see more details in 4.3.4, "PCIXCC module notebook" on page 103.

- Details

  This shows two pages of information for the PCIXCC. No changes are allowed in any of these pages.

- Roles

  The PCIXCC uses *role-based* access control. From the TKE workstation, an administrator defines a set of roles in the PCIXCC 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 PCIXCC, 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 workstation. PCIXCC roles and profiles are further explained in "Roles and profiles structure example" on page 112.

  Figure 4-39 on page 109 shows the commands accessible to the roles in the PCIXCC.

  Important: The manipulation of roles in the PCIXCC 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 preset DEFAULT role in the PCIXCC. This DEFAULT role is not accessible for setup.

- Authorities

  This 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)

Archive

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 its signature key in the TKE. This page also allows you to send 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 PCIXCC 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.

Note: If CCF modules have also to be managed by the same security organization, keep in mind that the CCF has a fixed number of sixteen authority indices (00 to 15) in effect. We recommend that you use the same indices consistently across all coprocessor types in the installation.

- Domains

  This entry defines the LPAR domains that can have DES and PKA Master Keys and operational keys loaded (loading of operational keys is a new function for PCIXCC) and changed from the TKEs. It also provides domain controls.

  Note: 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 two signatures for the PCIXCC) is issued by one authority, it 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.

  – A PCIXCC authority is mapped to a PCIXCC 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 PCIXCC 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 4-34 establishes a parallel between the multi-signature commands in the CCF and the PCIXCC 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 or PCIXCC, if needed.

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

CCF	PCICC/PCIXCC
LAP Load Authority public modulus: Issued when sending an authority signature key from 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 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 parts 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 4-34 Command families: equivalent CCF and PCICC/PCIXCC commands

4.3.4 PCIXCC module notebook

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

Intrusion Latch on the PCIXCC

Under normal operation, the intrusion latch is tripped when the card is removed. This causes all installation data, master keys, retained keys, roles, and profile definitions to be lost when it is reinstalled.

A new feature has been implemented (for PCIXCC only) to retain all the data. If the card needs to be removed and reinstalled, use the following procedure to disable PCIXCC (this process will require you to switch between the TKE application, the ICSF coprocessor management panel, and the support element):

1. Open a 3270 session on TKE, log on to your TSO userid, and from the ICSF primary option menu select option 1 for coprocessor management. Leave this panel displayed during the rest of the procedure. You will be required to press Enter on this panel at different times. *Do not exit* this panel until the process is complete.
2. Open the TKE host where the PCIXCC to be removed is installed. Load the right authority key, open the PCIXCC notebook, and click **Disable Crypto Module**.
3. After the PCIXCC has been disabled from TKE, click **Enter** on the ICSF coprocessor management panel. The status should change to DISABLED.
4. Configure *off* the PCIXCC from the support element. After the card has been taken offline, click **Enter** on the ICSF coprocessor management panel. The status should change to OFFLINE.
5. Remove the card, perform what needs to be done, and replace the card.
6. Configure *on* the PCIXCC from the support element. When the initialization process is complete, click **Enter** on the ICSF coprocessor management panel. The status should change to DISABLED.
7. From the TKE workstation Crypto module general page, click **Enable Crypto Module**.
8. After the PCIXCC has been enabled from TKE, click **Enter** on the ICSF coprocessor management panel. The status should return to its original state. If it was ACTIVE in step 1, it should return to ACTIVE.

All installation data, master keys, roles, and authorities should still be available. The PCIXCC data was not cleared because it was disabled first via the TKE.

Archive

PCIXCC notebook GENERAL page

The panel top line indicates whether you are working with a group of Crypto modules or with an individual Crypto module.

The panel shown in Figure 4-35 contains a short description of the module (which can be changed), the module type, the module index, and the host or group name. The PCIXCC 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 and enable functions is to permit easy control of the usage of cryptographic modules (for example, during service maintenance or non-working hours, and so forth).

Important: A single (or group) PCIXCC is disabled for *all* LPARs, not just for the LPAR that the disable command was issued from.

Archived

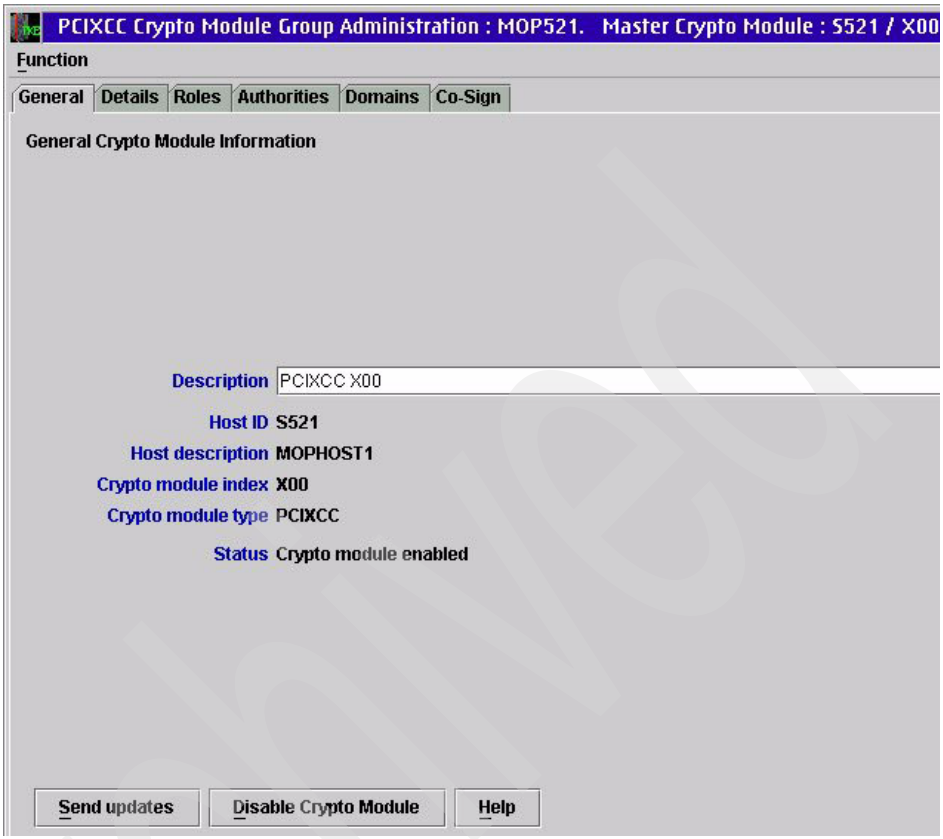

Figure 4-35 PCIXCC notebook General page on TKE

PCIXCC notebook DETAILS page

The PCIXCC DETAILS page is subdivided 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 key lengths, 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.

PCIXCC notebook ROLES page

Newly installed PCIXCCs (or previously zeroized PCIXCCs) have a predefined AUTHORITY 00 index assigned to the predefined INITADM role in the PCIXCC. This role can both issue and co-sign access control commands; that is, only one, single authority can perform these commands. See Figure 4-36.

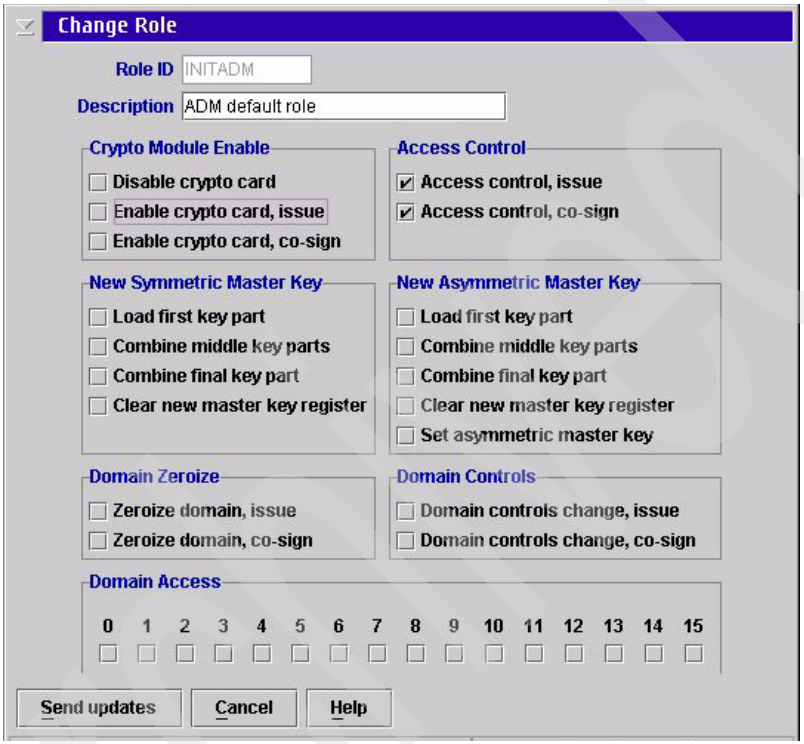

Figure 4-36 PCIXCC default INITADM ROLE: Access control

Create New Role page was modified for TKE V4.1 (Figure 4-37) to introduce the Operational Key functions available for PCIXCC cards only. This modification offers the four new fields shown under Operational Key in Figure 4-37. These are: Load first key part, Load additional key part, Complete Key, and Clear operational key register.

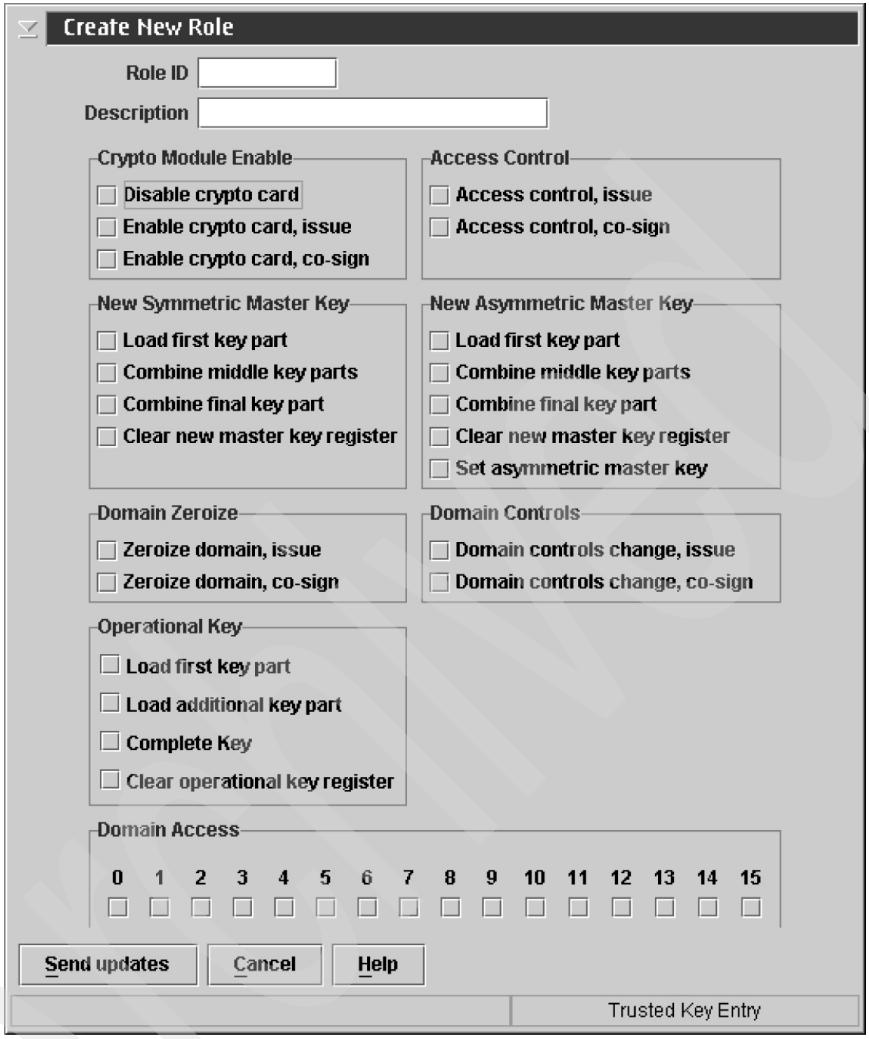

Figure 4-37 Create New Role page at TKE V4.1

Create new role page commands allow you to create all the necessary roles and authorities that can be required by the customer security policy for the PCIXCC. 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 4-38 illustrates the flow of role and authorities creation in the PCIXCC.

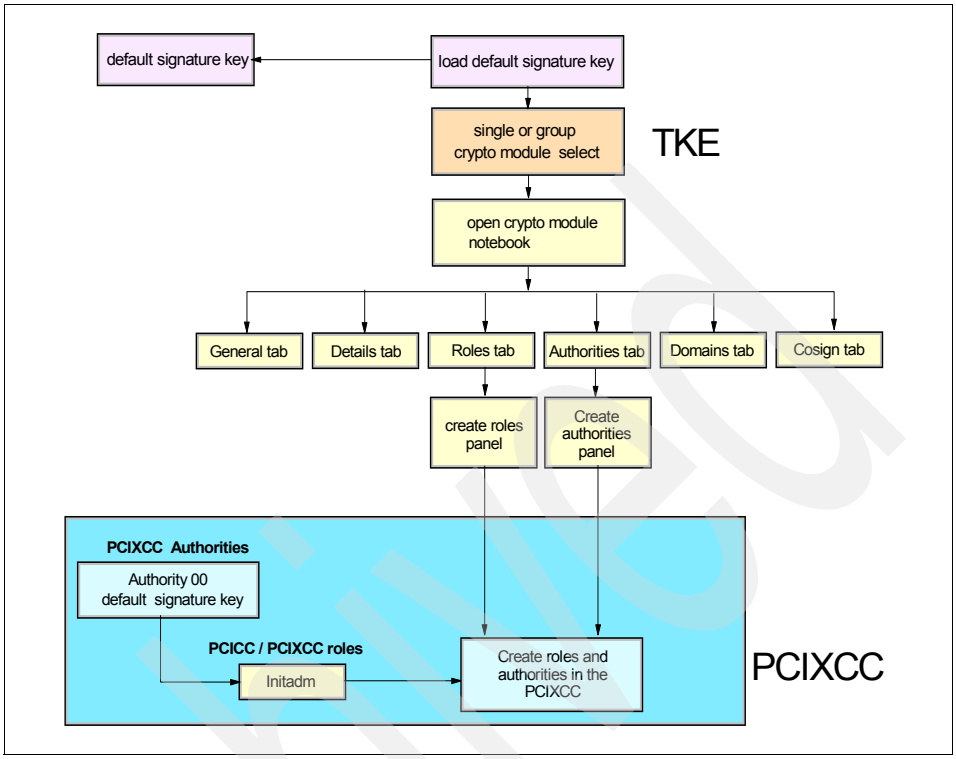

Figure 4-38 PCIXCC initial role and profile after new card install or card zeroize from SE

Creating roles in the PCIXCC

Figure 4-39 on page 109 shows the commands that can be assigned to a PCIXCC role for a specific domain. There are basically two types of commands: dual-signature commands, and single-signature commands.

Note: Roles and authorities can be defined or modified by initial default authority INITADM using a default signature (to be loaded in keystore), or later on by any authority mapped to a role with Access Control command privilege (issue and/or co-sign) using its own authority key (to be loaded in keystore)

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 PCIXCC from the disable state to the enable state.

- Access control

  This command is issued with all creation, change, or deletion of roles or authorities. Here there is no domain to be specified—it affects the entire card.

- 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.

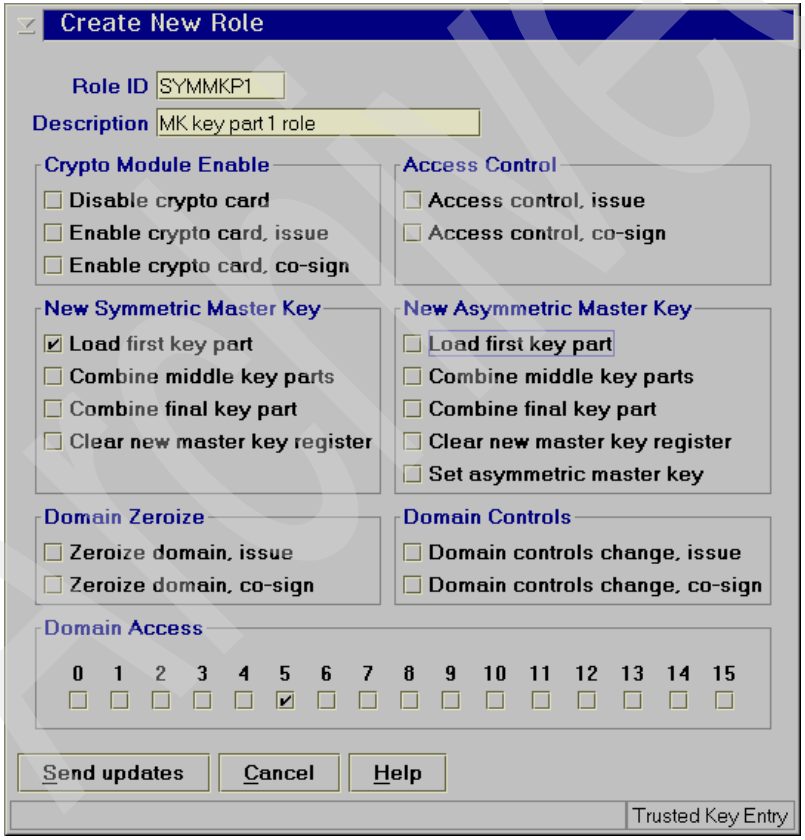

Figure 4-39 PCIXCC roles commands definition panel

Single-signature commands

- Disable crypto card - Issued from the notebook general page when changing from enable to disable module.
- Load first key part - Issued from the Domain key page.
- 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 Administrator. The default INITADM role provides this control.

Before sending any command, the authority index 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 PCIXCC is new or zeroized. The signature index and authority index must be the same, so if the authority index is changed, the signature key index must also be changed, with the new index even using the same default signature (use the change signature index option in the notebook function menu to make this change).

To create or change a role, the Crypto module administrator, after loading the signature key, right-clicks the role page panel, and then selects **Create** or **Change.**

In the new role panel, the administrator defines a Role ID (if creating the role) and writes a short text description; refer to Figure 4-40.

Archived

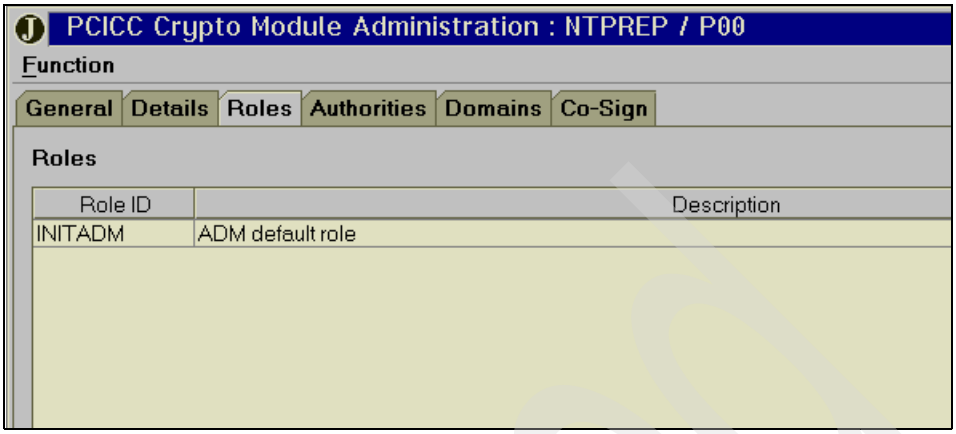

Figure 4-40 PCIXCC module administration notebook roles definition entry panel

The administrator then checks the command boxes required for the role, enters the role name with a short definition, checks target domains, and then selects **Send updates** to send the new role to the PCIXCC host module, as shown in Figure 4-41 on page 112.

Archive

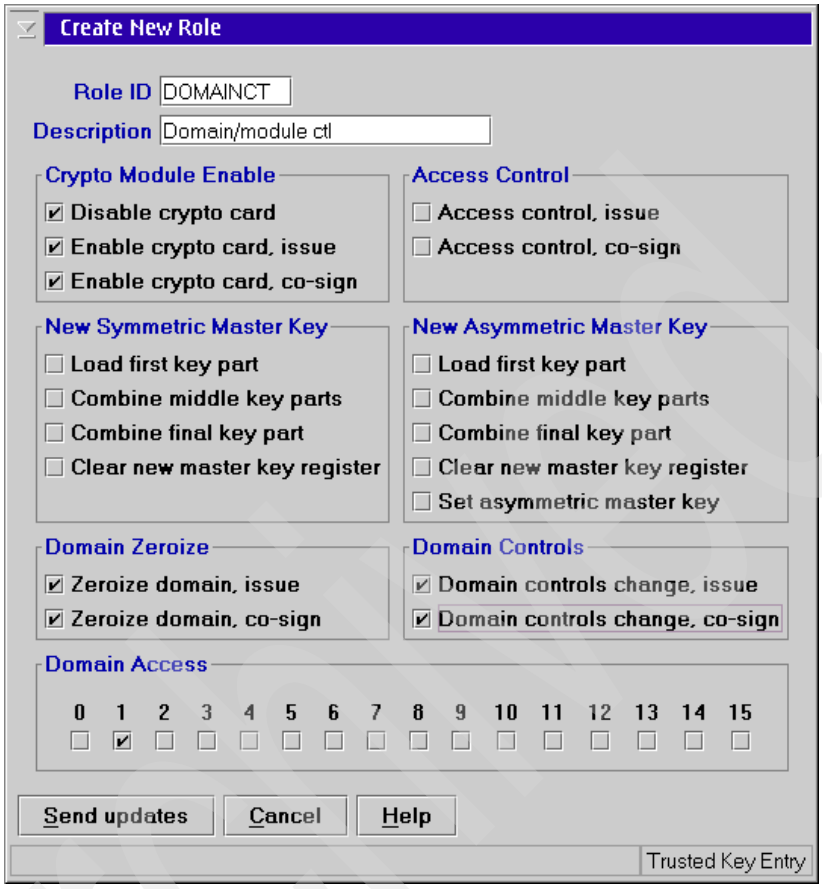

Figure 4-41 Create Role example: Domain controller role, domain 5, module cntl

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 (that is, the initial default INITADM role has both sign and co-sign commands).

Roles and profiles structure example

In our example, we created five roles and five authorities, using the default INITADM role. Figure 4-42 on page 113 is a graphical representation of our roles and authorities structure.

- Authority 01 is mapped to the DOMAINCTL role. This role has the Domain Controls and module control privileges.

- Authority 02 is mapped to the MKP1 role. This role permits you to clear new Master Key reg and to load a symmetric and asymmetric Master Key part 1 in a Domain (here domain 1).
- Authority 03 is mapped to the MKP2 role. This role permits you to load and combine a symmetric and asymmetric Master Key last part in Domain. This role can also set a new asymmetric key.
- Authority 04 is mapped to SYSADM1. This role has the access control privileges that permit you to create or change Roles and Authorities, It can also disable & enable crypto modules.
- Authority 05 is mapped to SYSADM2. This role allows you to co-sign commands previously issued by a user logged on with a profile mapped on SYSADM1. It can also disable the Crypto module.

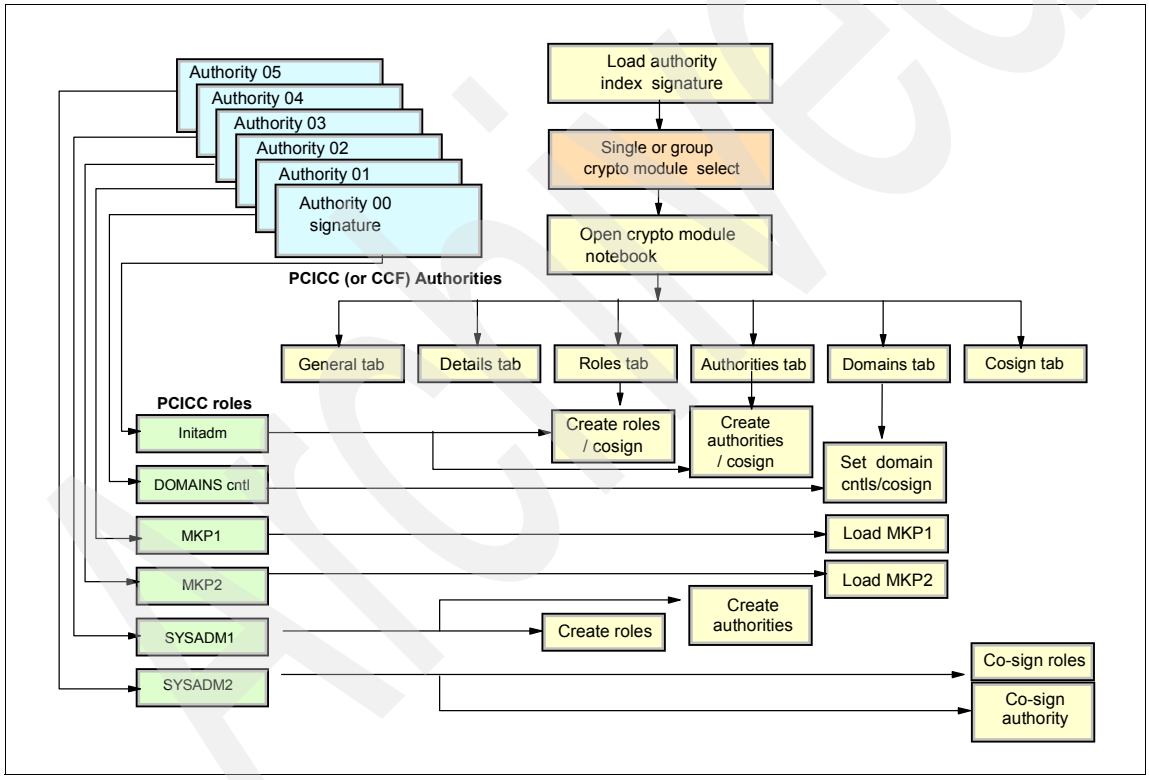

Figure 4-42 PCIXCC roles and authorities mapping example

MKP1 and MKP2 roles are shown Figure 4-43 and in Figure 4-44 on page 115.

Figure 4-43 PCIXCC role MKP1: Clear new Master Key reg and enter MK part 1

Archive

Figure 4-44 MKP2 role: combine key parts; set Asymmetric Master Key

SYSADMIN1 is shown in Figure 4-45 on page 116; SYSADMIN2 is shown in Figure 4-46 on page 117.

Figure 4-45 Sysadmin 1 role: access control command issue

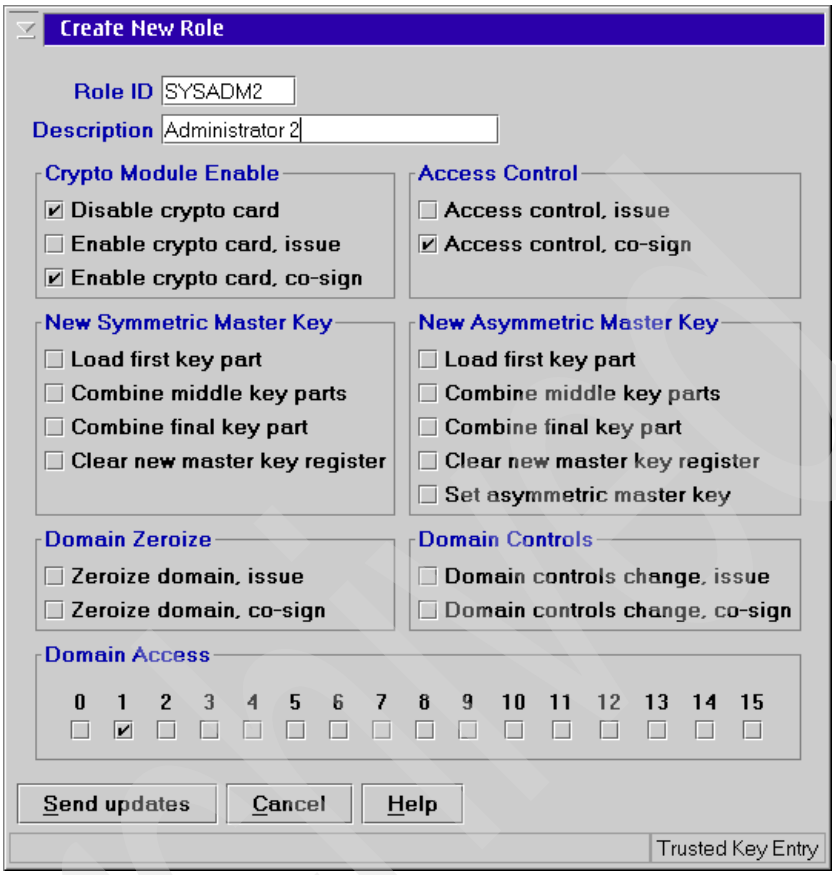

Figure 4-46 Sysadmin 2 role: access control command co-sign

Figure 4-47 on page 118 shows the Roles page after the five new roles have been created.

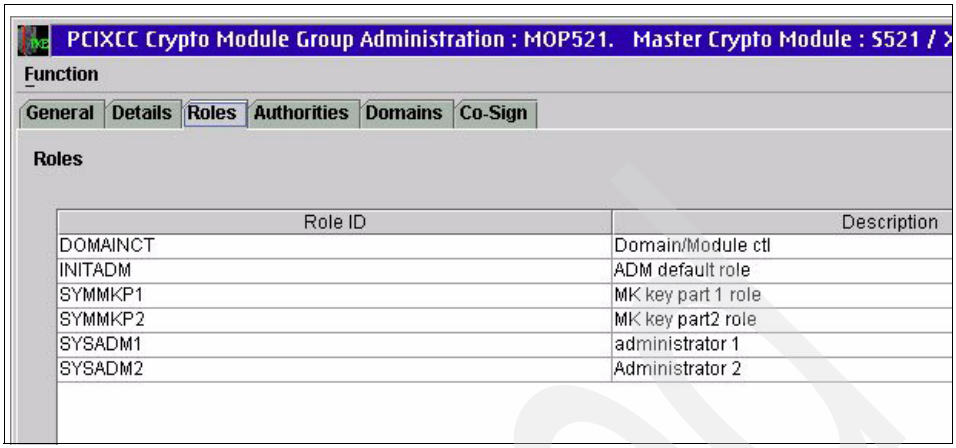

Figure 4-47 PCIXCC Roles page after new roles have been created

PCIXCC notebook AUTHORITIES pages

PCIXCC authorities are individual profiles mapped to one role.

The PCIXCC notebook AUTHORITIES pages contain the following selections:

Generate PCIXCC signature keys

Before creating a PCIXCC new authority index, you need to generate a signature key for the index. To generate this key, select the **Authorities** tab and then right-click the Authorities panel, as shown in Figure 4-48 on page 119. Then select **Generate Signature Key**.

Archive

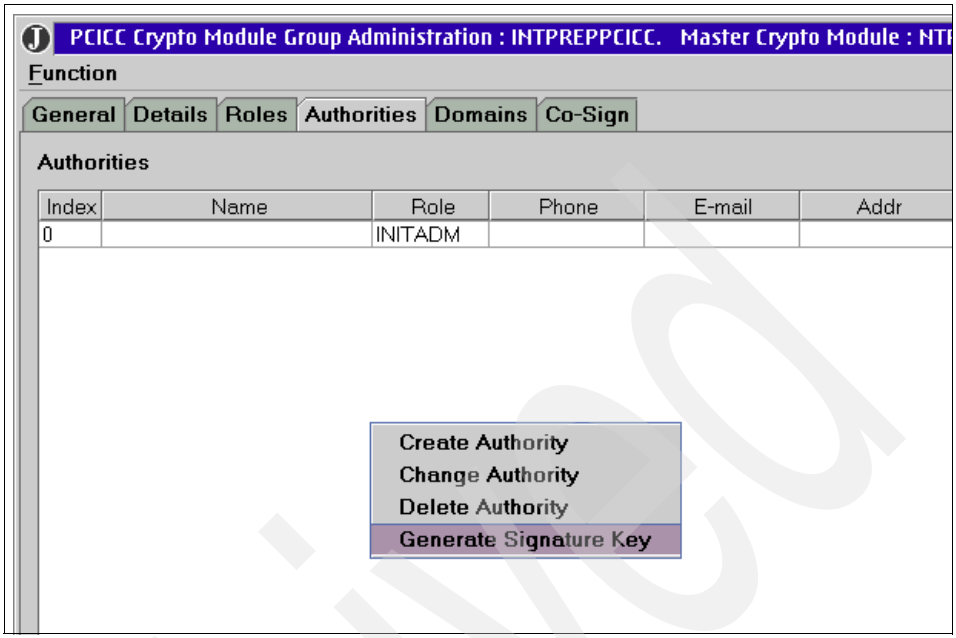

Figure 4-48 PCIXCC module notebook authority management main panel

On the next panel, Figure 4-49, enter the Authority index and relevant information such as name, phone number, e-mail, address, and so on, and then press **Continue**.

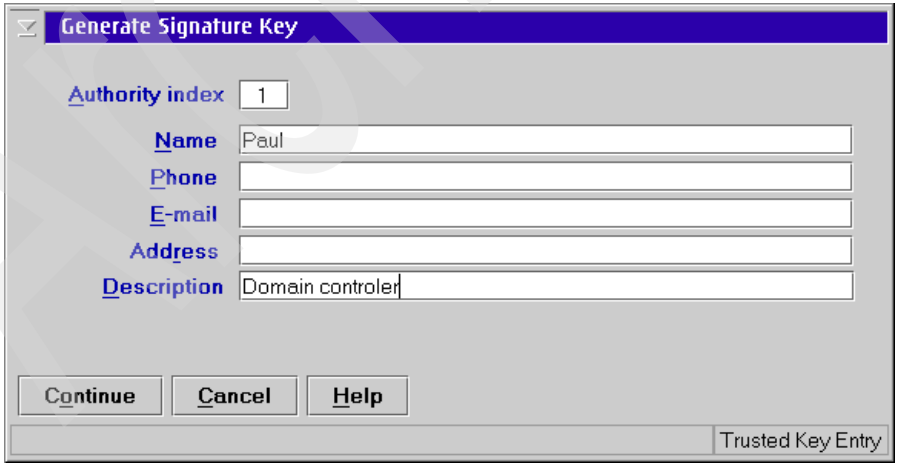

Figure 4-49 Create a signature panel

Then you will be asked to save the newly generated signature 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, so keep this password in a safe place. We also recommend that you save the key again, in a different place.

Notes:

- Only *one* authority signature key can be saved in TKE PKA keystore.
- 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 PCIXCC and in the CCF (if needed).

Create a PCIXCC new authority

To create a PCIXCC new authority, right-click the window on the authority page, then select **Create**. A new authority signature key source is requested.

If you select:

- Keystore - The information associated with the key that you previously generated appears immediately in the window.
- 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 4-50 on page 121.
- Default key - No associated information is 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 the authority public key will be sent to the host Crypto module by pressing **Send**. 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 requires an authority with the proper role to co-sign.

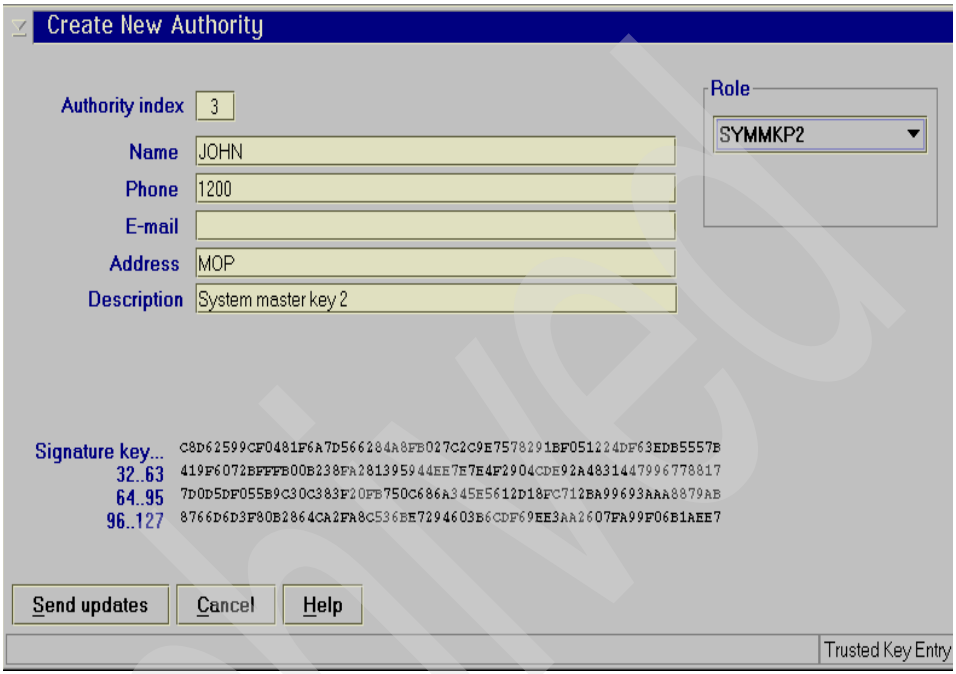

Figure 4-50 Create Authority: JOHN, Authority 03 mapped to SYMMKP2 role

Note: Authorities mapped to the role with access control privileges, such as the INITADM default PCIXCC role, can create, change, or delete any other role and authorities. A security measure we strongly suggest is to *replace* the INITADM role with *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 PCIXCC authority

Activating this selection will allow you to make changes to the authority information and to replace the authority public modulus in the Crypto module.

The authority index remains fixed. Before changing an authority signature you need to generate a new one with the same index.

Select **Get signature key** to open a select key source window and load the signature key window. The contents of the selected key file replace the public modulus in the change authority window.

The role can also be changed.

Pressing **Send updates** uploads the new information to the Crypto module.

Delete Authority

PCIXCC authorities 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 4-51 shows the Authorities main panel after the five new authorities have been created.

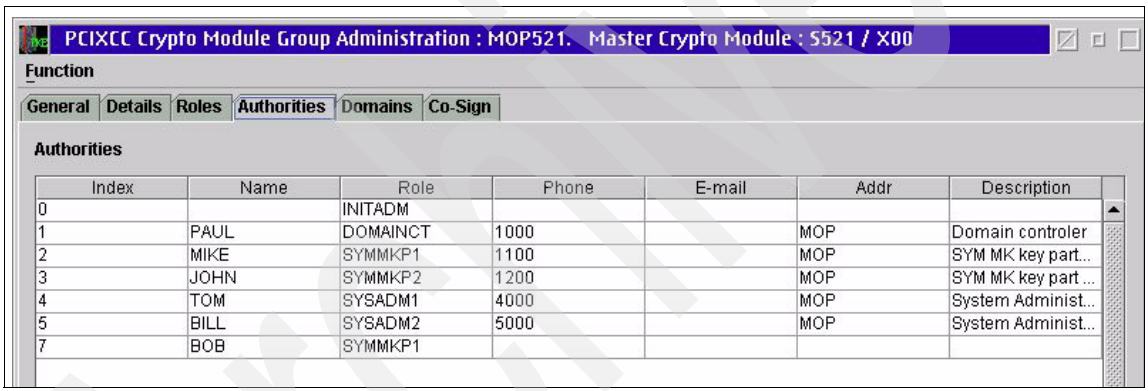

Figure 4-51 PCIXCCAuthorities panel after several authorities have been created

PCIXCC notebook DOMAINS page

The PCIXCC 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 left-hand 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.

Archived

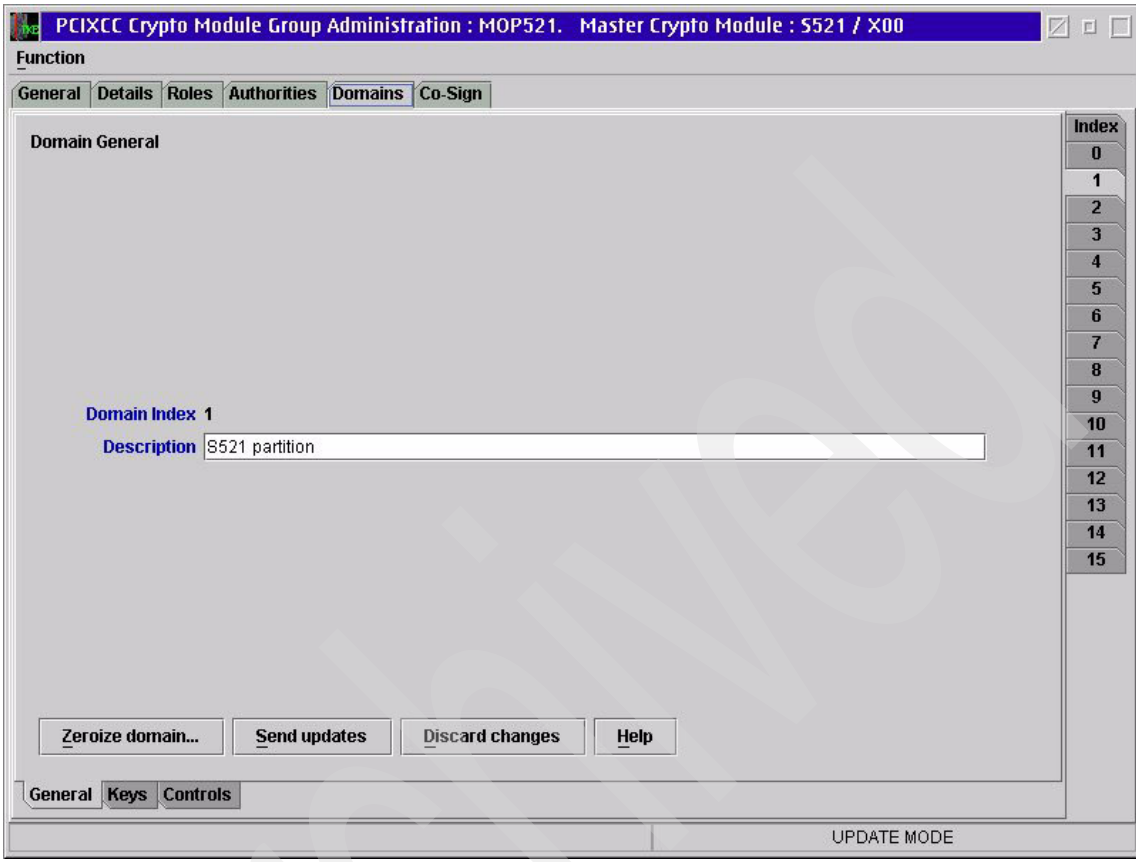

Figure 4-52 PCIXCC Domain 1 general page

PCIXCC Domain general page

This page is shown in Figure 4-52. From here you can select the Description and zeroize the domain.

- To change the description, edit the description entry and press **Send updates**.
- If you choose **Zeroize domain**, a warning message will inform you that the initiated process will clear all the keys in the domain. If you continue, you will 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. If you are reassigning a domain to another use, zeroize is a good practice for security.

Important: After domain zeroization, be aware that the ICSF panel services shown in Figure 4-73 on page 138 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.

PCIXCC 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 4-53 on page 125.

New Symmetric and Asymmetric Master Keys can be generated and loaded for PCIXCC cards.

Running TKE V4 code, operational keys (IMP-PKA and IMPORTER) and RSA keys can be generated, enciphered and loaded for PCIXCC cards (new vs. PCICC).

TKE V4.1 code supports additional operational key types.

When right-clicking a key type from the key panel, the following actions become available:

- Generate

  This generates a key part and write it to a file. Media and file naming is a user responsibility. The number of key parts needed to create a new Master Key depends on your security policy, so as many parts as needed have to be created and saved.

- Clear

  This clears the key register or key part register. Before loading the first Master Key part, the key register must be cleared.

- Load

  This loads 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 4.2.1, “TKE workstation 4758 setup” on page 72.

Archive

- Set

  Setting the ASYM-MK key transfers the current Master Key to the old Master Key register, and the new Master Key to the current Master Key register.

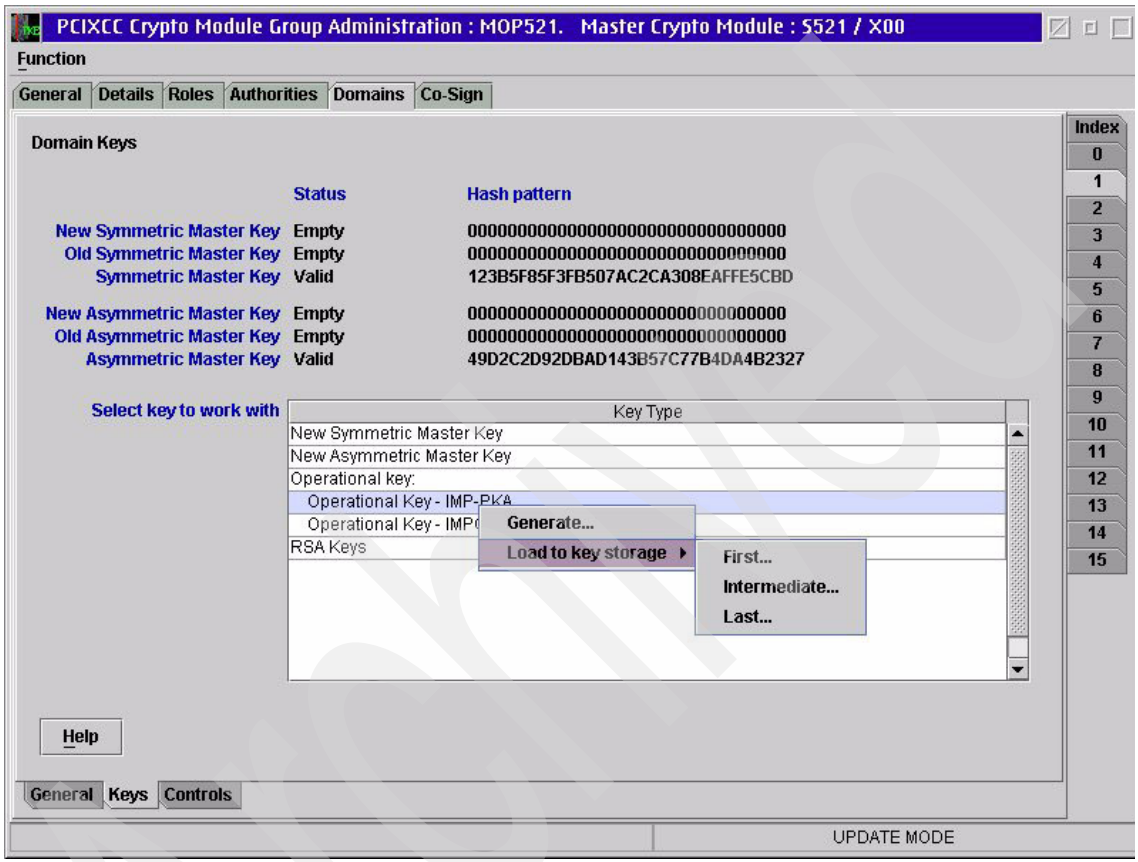

Figure 4-53 PCIXCC Domain key page at TKE V4

New functions are available for PCIXCC cards:

- TKE V4 Operational keys IMP-PKA and IMPORTER can be generated and loaded in key store. Operational keys have also to be saved to file to import and store these keys in the CKDS. Operational IMP-PKA keys will be used to protect RSA keys during transport from the workstation to the ICSF. IMPORTER keys will be used to protect DES keys.

  Two or more IMP-PKA key parts have to be generated first to create an IMP-PKA key type saved in TKE keystore.

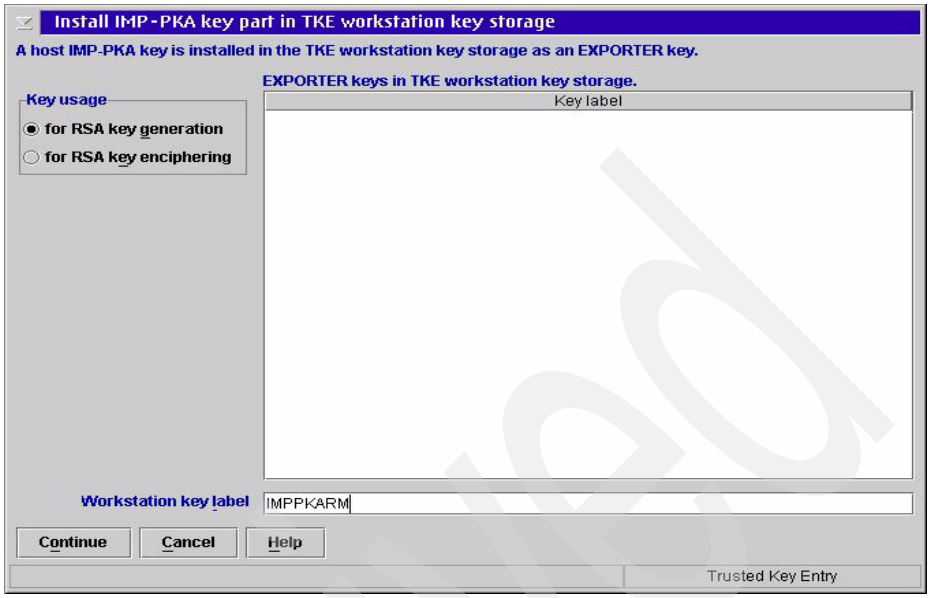

Figure 4-54 Load IMPPKA key part 1 in keystore: key name IMPPKARM

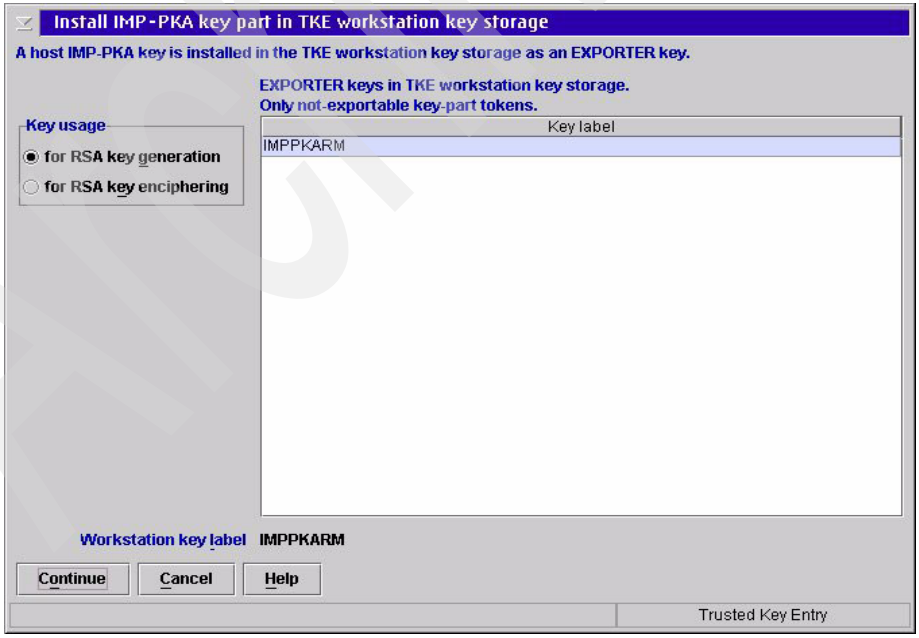

Figure 4-55 Load IMPPKA key part 2 in keystore: key name IMPPKARM

Archived

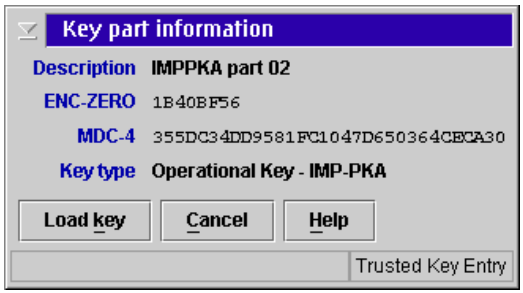

Figure 4-56 Load keypart 2 for IMP-PKA key name: IMPPKARM

The same sequence must be used to create IMPORTER key types and load them in Keystore.

- TKE V4.1 Operational keys can be loaded on a PCIXCC. All ICSF operational key types are supported on TKE V4.1, including a USER DEFINED key type, where the user provides his own control vector for the key you are generating. With the USER DEFINED key type you can enter all key types available in CCA. Figure 4-57 on page 128 presents the PCIXCC domain keys page, with Operational keys support available on TKE V4.1.

Archive

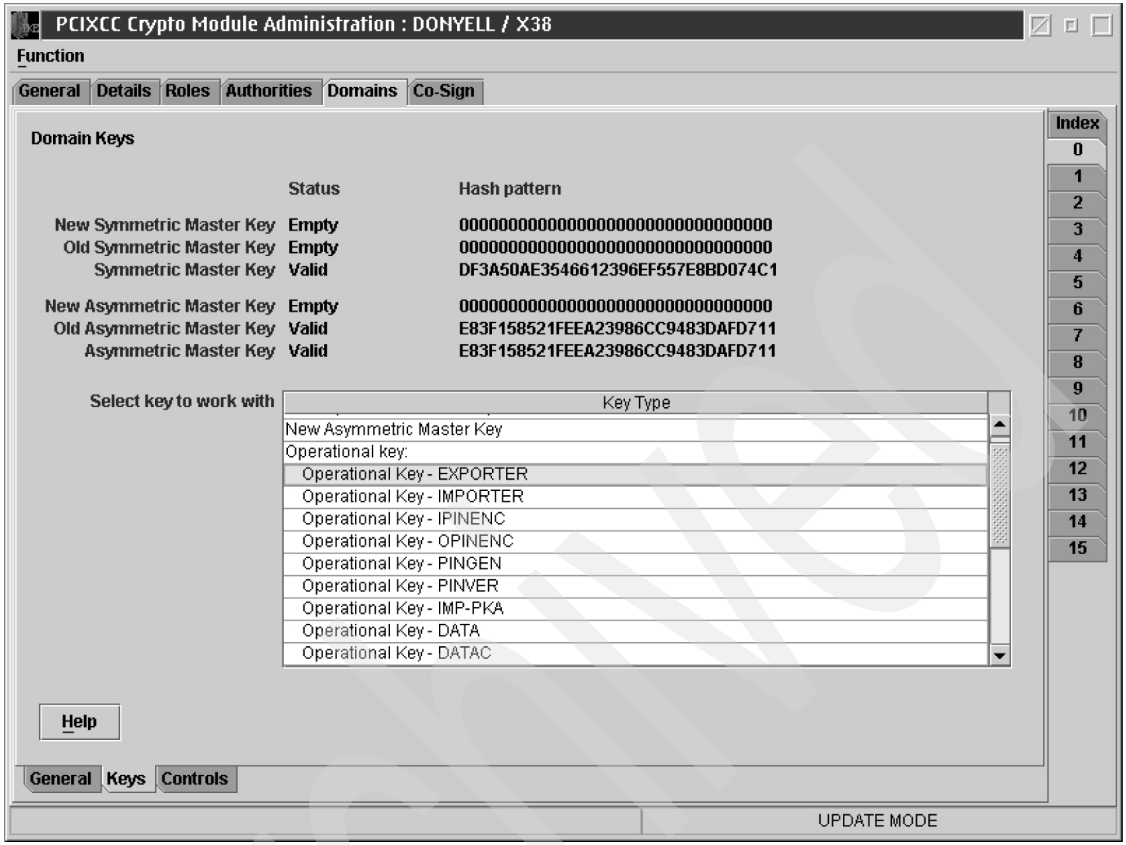

Figure 4-57 PCIXCC Domain Keys page running TKE V4.1

- Operational key part registers permit Operational keys to be loaded and accumulated on a PCIXCC. Each card supports up to 100 key part registers distributed across all domains. After entering all key parts, and the key is Complete, it is necessary to remove the key from the key part register and load it into the CKDS. There are two methods to perform this loading: ICSF panels, or using a new option on KGUP JCL.
- At least two key parts must be entered, and there is no maximum number of key parts. A key part register is freed after loading a Complete key into CKDS, after zeroizing the domain through TKE or when the key part register is cleared from TKE.
- New access control points in the role definition controls the use of Operational key part registers on the PCIXCC cards, as shown on Figure 4-37 on page 107. Load First Key Part, Load Additional Key Part, Complete Key, and Clear Operational Key Part Register are the new access control points.

- Generate Operational Key Parts

  When Generate is selected for a Default Operational Key, the Generate Operational Key window is displayed showing the key type, key length, description, and control vector, but only the description field is allowed for updating. Key length can be updated only if the key type supports different lengths. Figure 4-58 shows the Generate Operational Key window for the default ICSF key type.

Figure 4-58 Generate Operational Key Type EXPORTER

- Generate supports the USER DEFINED key

  For USER DEFINED key type the Generate Operational Key window is displayed showing key type, key length, description, and blank control vector fields, where the control vector entered must conform to the rules for a valid control vector. All but the key type can be updated.

- Selecting **Continue** on the Generate Operational Key panel prompts the user with a choice of saving the key, either on a binary file or on a print file, as shown by Figure 4-59.

Archive

Figure 4-59 Select where the key is to be saved

- Selecting Binary or Print file, the user has to specify where the key is to be saved. The “Save key part” panel lets you point to where the file is going to be saved, as shown in Figure 4-60.

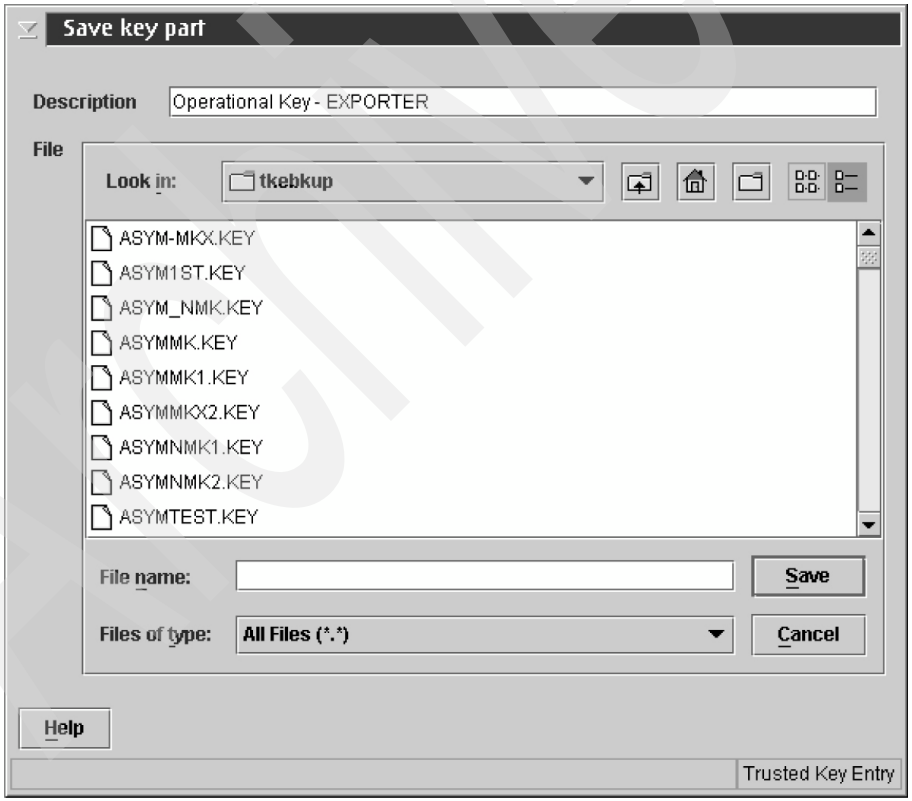

Figure 4-60 Save key part panel

Archived

- Load to Key Part Register - First

  When Load to Key Part Register First is selected, the user must choose the source of the key, which can be a binary file or keyboard, as shown in Figure 4-61.

Figure 4-61 Select the source of the key

- If Keyboard was selected, the Enter key value panel is displayed, as shown in Figure 4-62.

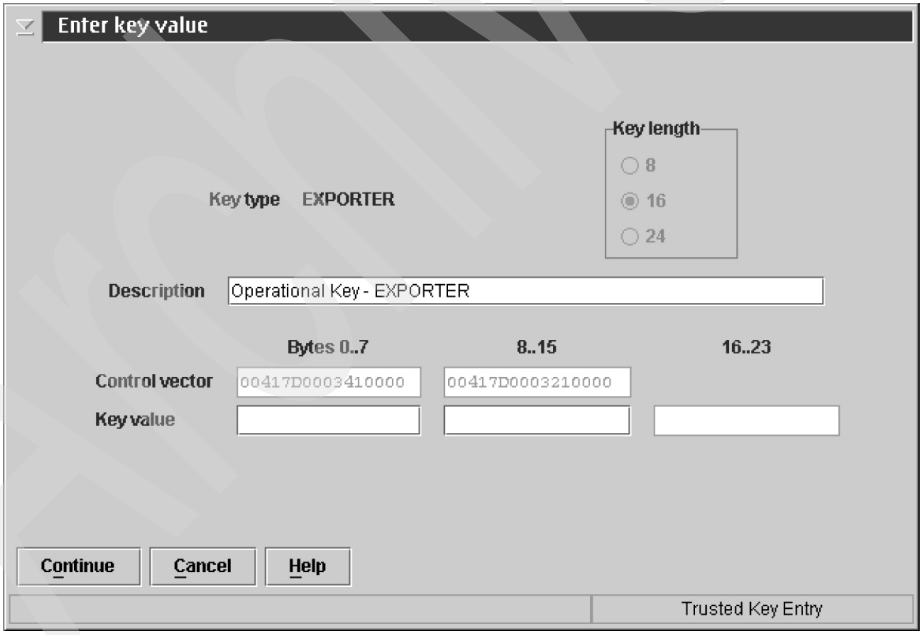

Figure 4-62 Enter key value - Keyboard source

- When the key type is USER DEFINED, all the fields on the “Enter key value” panel can be updated, including the control vector. After the binary file is read

Archived

or the key part is entered, the ENC-ZERO and MDC-4 values for the key part are calculated and displayed, as shown on Figure 4-63.

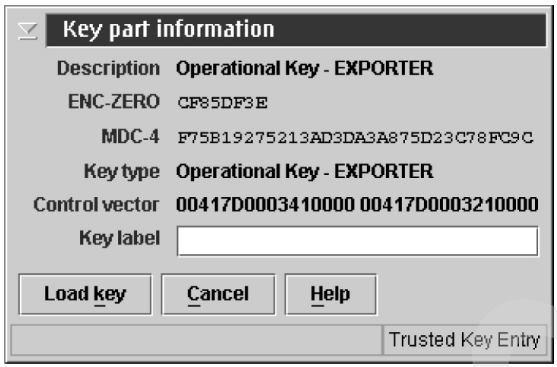

Figure 4-63 Key part information - first key part

- When loading additional key parts, the key part register will be selected by the key label entered. This label must not already exist. The key label must conform to valid key label names in CKDS.
- If the information provided on the “Key part information” panel is correct, the key part is loaded to the key register by selecting **Load Key**. After loading the key part, the key part register information window is displayed, presenting the information shown on Figure 4-64.

Figure 4-64 Key part register information

- The same procedure is performed to load as many key parts as your policy requires. At least two parts are required by ICSF.
- If **Binary file** is selected, the correct file name is chosen by you. If **Keyboard** is selected and the key type is a default Operational key, the Enter Key Value window is displayed.

Archived

- If the key type is USER DEFINED then the Load Operational Key Part Register window is displayed with a drop down menu of available control vectors, as show on Figure 4-65

Figure 4-65 Load Operational Key Part Register with USER DEFINED key type

- You select the control vector for the key to be loaded. After the control vector has been selected, the Enter Key Value window is displayed. Once the binary file is read or the key part is entered, the “Key part information” window is displayed. Click **Load key** to complete the key part load.

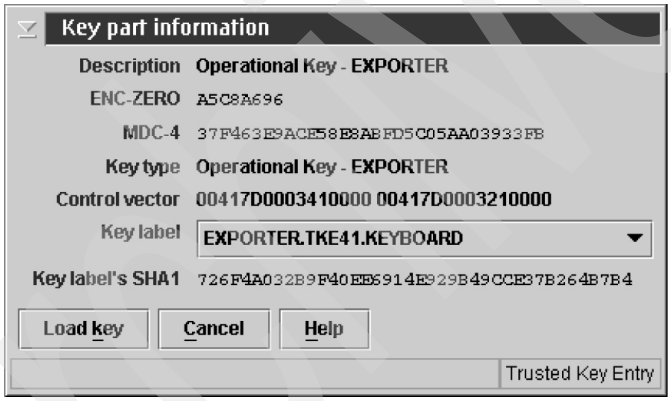

Figure 4-66 Key part information

- When Key Part Register has been loaded and selected for a user-defined key type, the Complete Operational Key Part Register window is displayed with all the domain’s key part registers that are in the intermediate state, as shown in Figure 4-67.

Figure 4-67 Complete Operational Key Part Register

- After the key labels have been selected, the “Key part register information” window is displayed for each label that was selected. The ENC-ZERO value is shown for the complete key and the state is complete.

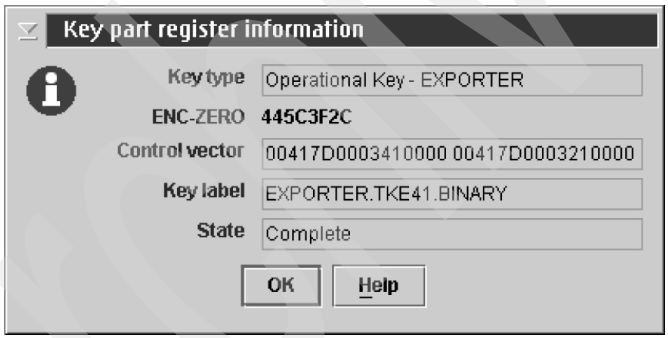

Figure 4-68 View key part register information - complete key

- After all the key labels that were selected are processed, the view key register window is displayed indicating that the command was executed successfully.
- RSA keys can be generated, enciphered, loaded to PKDS, or loaded to a data set
  - Generate the RSA key and encrypt it under an IMP-PKA key previously created. The encrypted RSA key is then saved on the TKE hard disk or media.

    RSA key usage control specifies whether the key can be used for key management purposes. Key length, public exponent, host, PKDS, and workstation key label must also be entered; see Figure 4-69 on page 135.

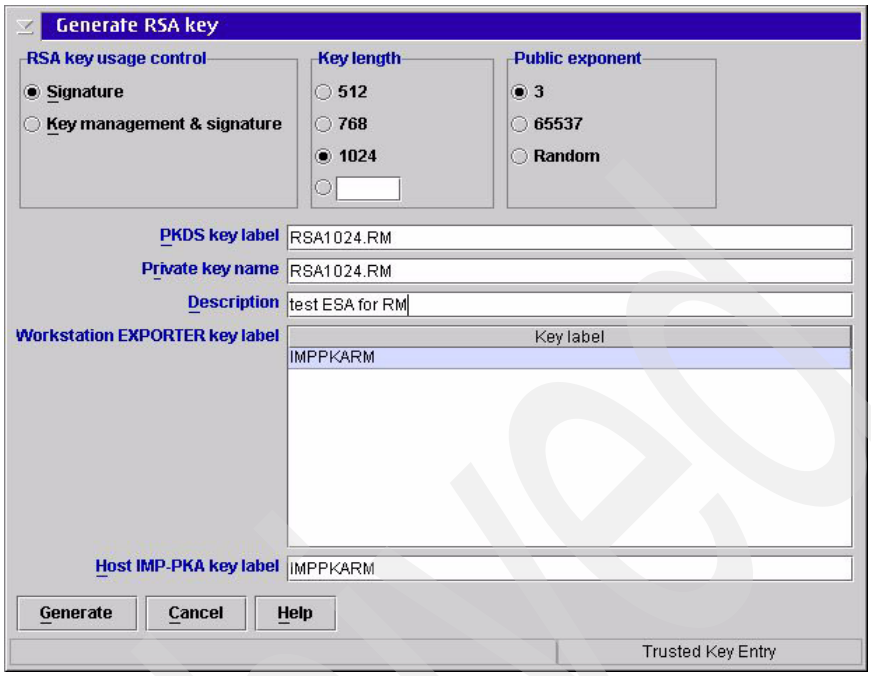

Figure 4-69 RSA key generation, encrypted under IMPPKARM

Archive

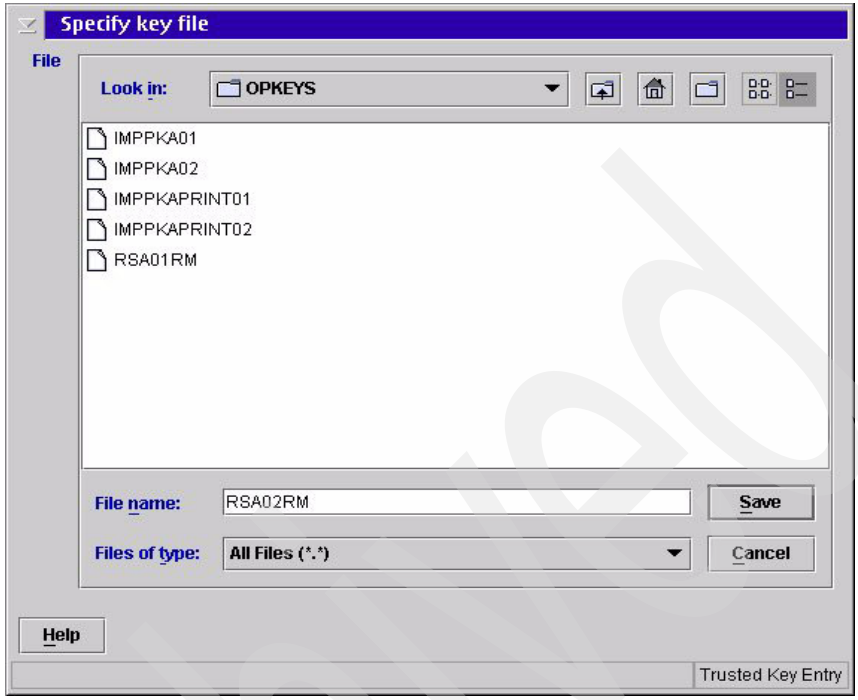

Figure 4-70 Newly created RSA key saved as RSA02RM

– Encipher an RSA key - Encipher an unencrypted RSA key under an IMP-PKA key.

– Load an RSA key to PKDS - Load an RSA key to the PKDS active in the logical partition where the host transaction program is started.

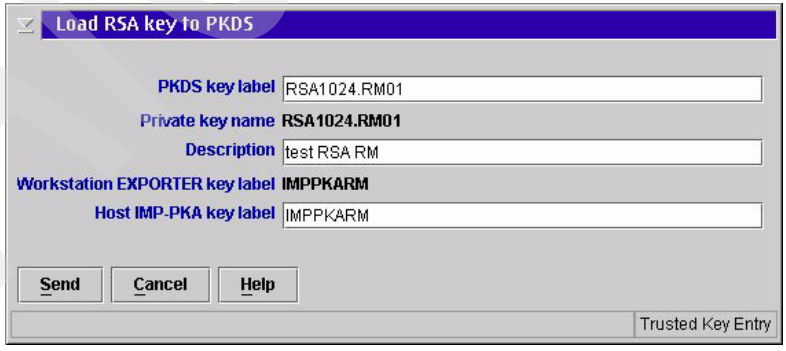

Figure 4-71 Load an RSA key to the PKDS panel

– Load an RSA key to a host data set.

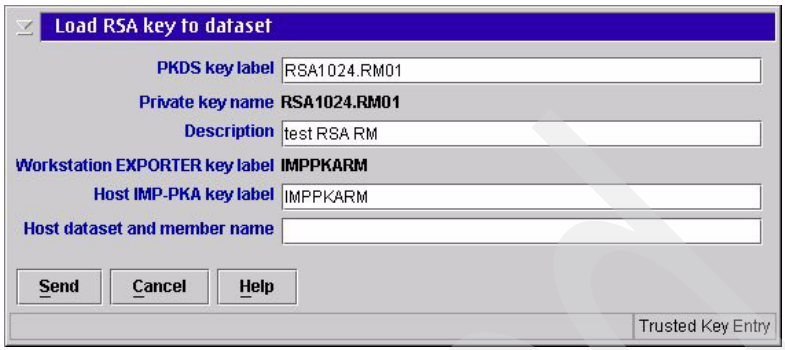

Figure 4-72 LOAD RSA key to data set panel

See Chapter 4 in *ICSF TKE Workstation User's Guide,* SA22-7524-05 for details.

PCIXCC Domain control page

This page, also named the "control access point," displays the cryptographic service functions that are enabled for the domain in the ICSF ISPF panels, as follows:

- Clear New ASYM Master Key Register
- Clear New SYM Master Key Register
- Combine ASYM Master Key Parts
- Combine SYM Master Key Parts
- Load First ASYM Master Key Part
- Load First SYM Master Key Part
- Set ASYM Master Key
- Set SYM Master Key

These functions are shown in Figure 4-73 on page 138.

Archive

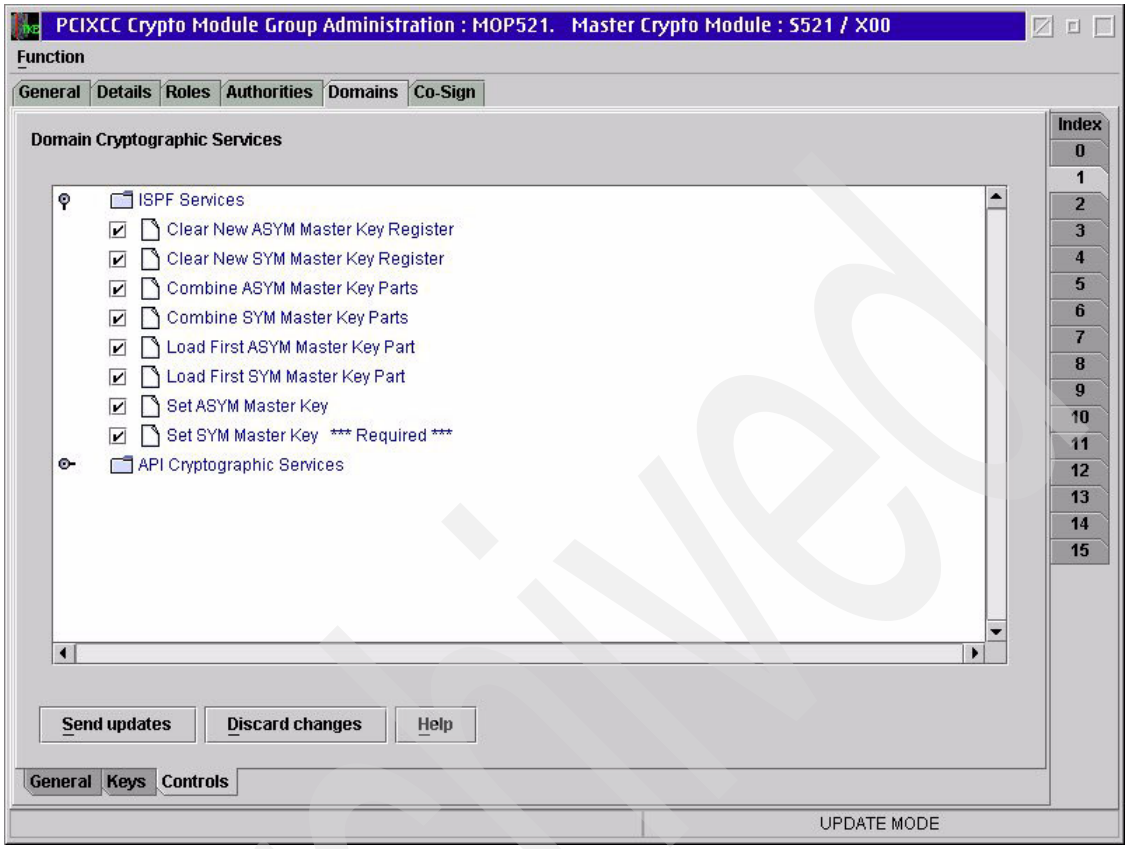

Figure 4-73 PCIXCC Domain 1 control panel: ISPF services

Note: These functions will be permitted from the ICSF panel only if the boxes are checked (but they can be performed, in any case, from the TKE). However, there is an exposure if these functions are not permitted on this panel—if the TKE fails and no other TKE is available.

Archived

Introduced with TKE 3.1, the Domain control page also displays a list of all API services available. Users must check the API boxes they want to be permitted and uncheck the API boxes they do not want to be permitted; see Figure 4-74.

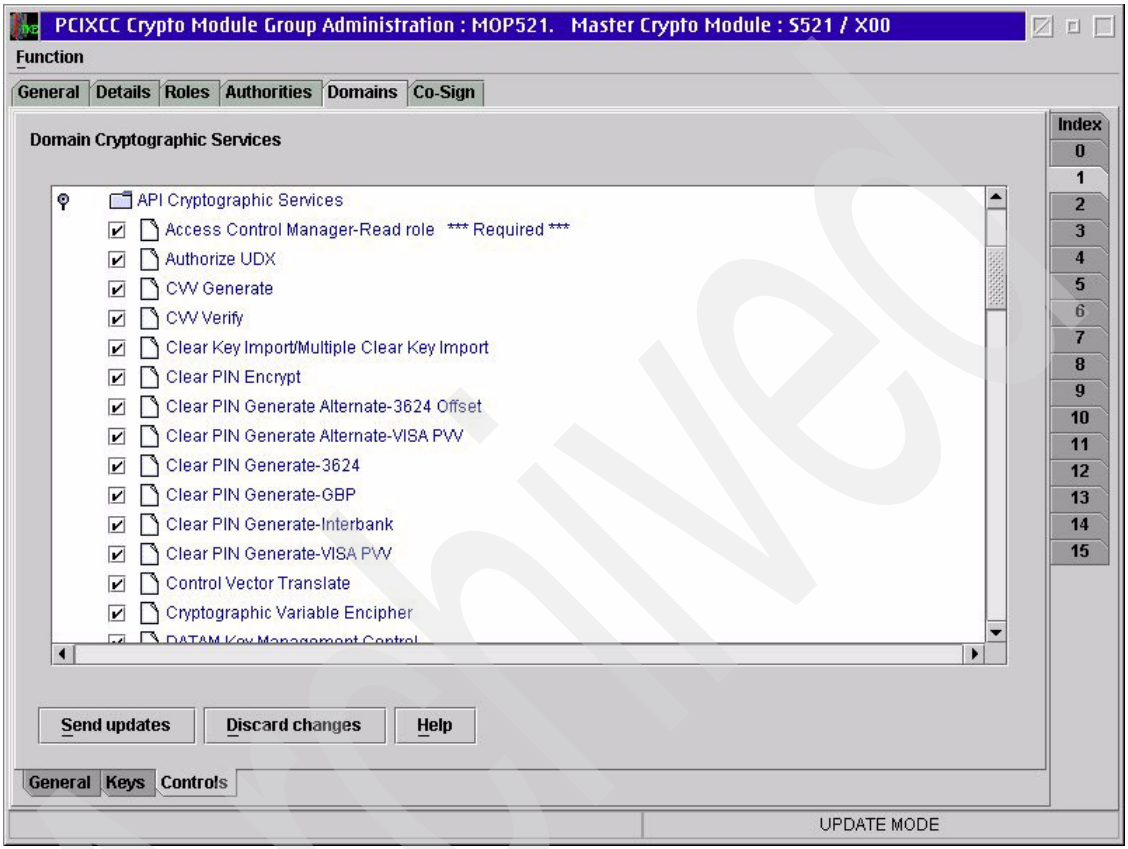

Figure 4-74 PCIXCC domain 1 control panel: API services

A list of available UDXs is shown in the Domain control page. This list appears only if UDX functions are installed in your host system. See Figure 4-75 on page 140.

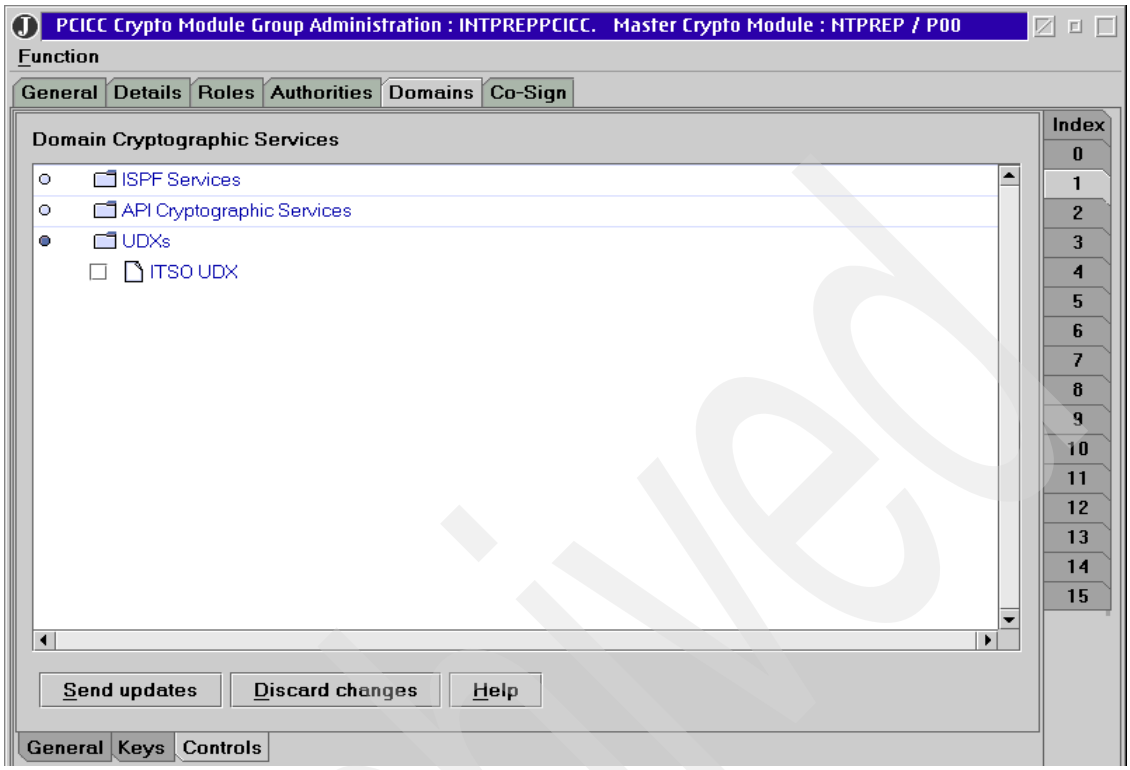

Figure 4-75 PCIXCC Domain control: UDX list

PCIXCC co-sign page

For PCIXCC 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, notifying the user that the command is pending and awaiting co-sign, as shown in Figure 4-76.

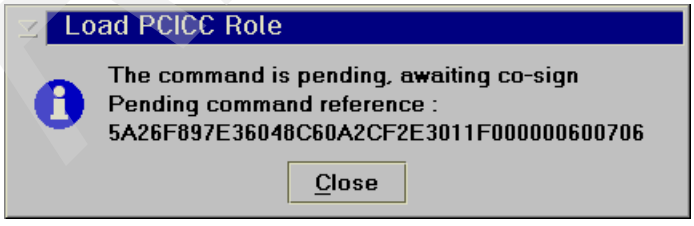

Figure 4-76 Pending command message panel

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 that has already signed and the authorities that are permitted to sign this type of command; see Figure 4-77.

- 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.

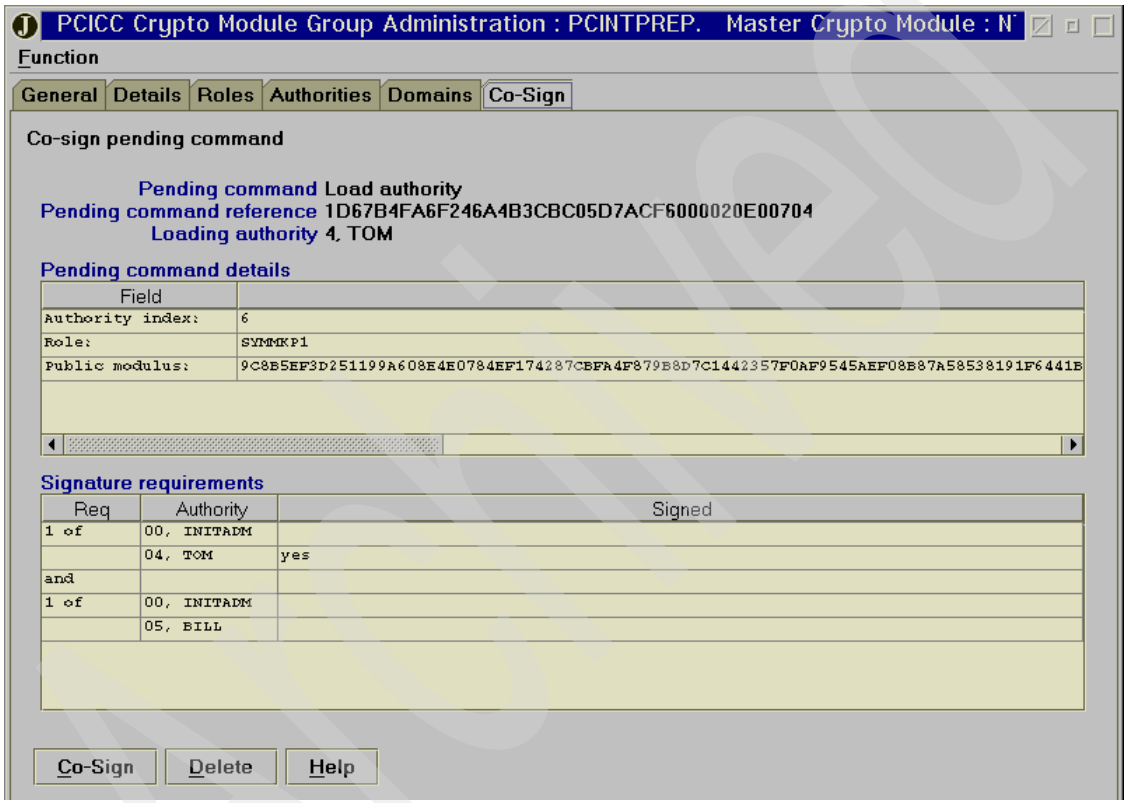

Figure 4-77 Co-sign pending for create authority command issued by TOM

4.3.5 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 TKE 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.

Workstation files

You should systematically back up files on your workstation. Double-click the **Backup** icon and follow the instructions given there. The TKE backup diskette is labelled ACTKEBKP.

- 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 module 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 be 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.

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.

This data set contains definitions for the Crypto modules, domains, and authorities. It is updated any time you make changes in the TKE application windows and Crypto module notebooks.

Archived

4.4 4753 Key Token Migration facility

A facility is provided in TKE V4 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.

If running TKE V4.1, ICSF FMID HCR770B is required for processing the migrated keys data set. If you are running ICSF HCR770A or earlier, then APAR OA07394 is required.

We did not practice with this utility during our project; therefore, this information is provided for reference only. For further information, refer to Appendix G of the *ICSF TKE Workstation User's Guide,* SA22-7524-05, which provides the detailed procedure.

Archived

Archived

5

ICSF support for CPACF, PCIXCC, and PCICA

In this chapter we describe an overview of the installation of the PCIXCC and PCICA cards and the initialization and setup steps to be performed by the customer to use the installed PCIXCC/PCICA cards. We also describe the new CP Assist for Cryptographic Functions (CPACF) feature, which requires Operating System updates and functional changes in ICSF.

The goal is to make the installation of the PCIXCC and PCICA cards concurrent (that is, without any interruptions). The first steps of this installation are performed at the Support Element or Hardware Management Console (HMC). This includes the verification that the CPACF feature is installed, and the cryptographic coprocessor assignment and authorization setup in the image profiles of the logical partitions, 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 CP Assist for Cryptographic Functions (CPACF) must be installed before use of the PCIXCC or PCICA cards, and the cryptographic cards must be configured “online.” (See 5.3.1, “PCIXCC and PCICA enablement” on page 157.)

© Copyright IBM Corp. 2004. All rights reserved.

Notes:

- *Operator command*

  Several manuals that we used while writing this book refer to use of an "operator command" to vary the PCIXCC/PCICA online or offline.

  No such command exists that enables z/OS operators to display the status or configure a PCIXCC/PCICA online or offline from the system console. This can only be accomplished at the system Support Element or HMC.

- *Online*

  When it is applied to the PCIXCC/PCICA, the term "online" requires precision regarding the context in which it is used, as follows:

  - If referring to the PCICC/PCICA PCHID, the meaning of "online" is the same as for a PCHID being in an online or stopped state: A device in the online state is accessible to the software that is running in the partition or in the system, whereas a device in the stopped state is no longer accessible.
  - If referring to the PCIXCC facility as seen by ICSF, "online" means that the device is accessible but must have its Master Keys properly set. A PCIXCC is fully operational when in the "active" state, as described in 5.4.5, "Installation of a new PCIXCC or PCICA card" on page 177.
  - PCICA is seen by ICSF as "active" as soon as the PCICA state is set by PCHID to "online" because there are no Master Keys in PCICA.

- As we wrote this redbook, the operating system needed an update for selected releases. The update provides ICSF support for both secure keys and clear keys using the CP Assist for Cryptographic Functions (CPACF), PCICA, and the PCIXCC adapters.

  This update and its installation instructions can be found at:

  http://www.ibm.com/eserver/zseries/zos/downloads

5.1 CP Assist for Cryptographic Functions (CPACF) feature

The installation of the CP Assist for Cryptographic Functions (CPACF) DES/TDES enablement, feature code 3863, is required to enable the use of PCIXCC and PCICA features. Feature code 3863 enables DES and TDES algorithm on the CPACF. (The SHA-1 algorithm is always enabled.)

The verification that CPACF is installed in the system can be done using the Support Element or HMC Single Object Operations session using the logon ID SERVICE or SYSPROG.

1. From the Views area, open **Groups and CPC**.
2. Select the CPC icon in the CPC Work Area view and double-click to open the CPC details window shown in Figure 5-1.

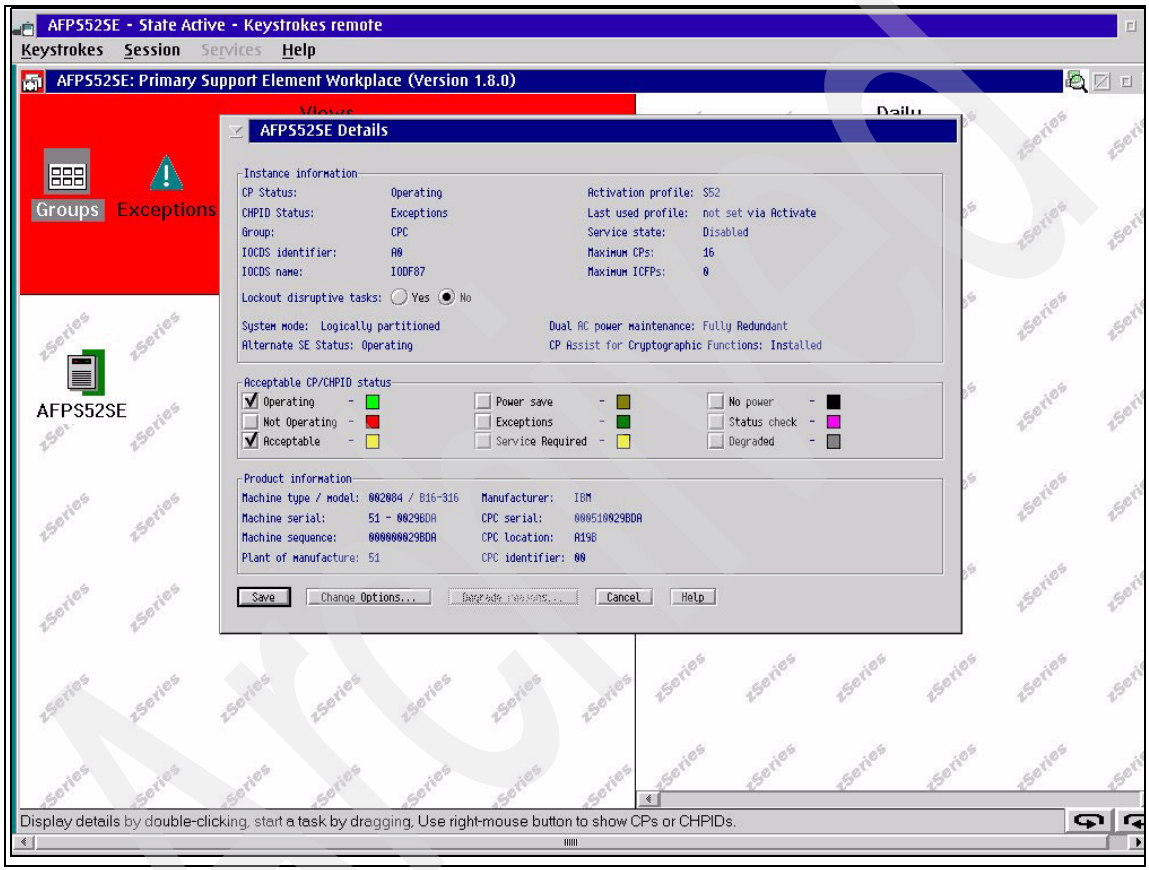

Figure 5-1 CPACF feature installed

3. In the window, verify the CPACF enablement feature.
   - If the window displays `CP Assist for Cryptographic Functions: Installed`, it means that the cryptographic enablement feature code 3863 is installed.
   - If the window displays `CP Assist for Cryptographic Functions: Not Installed`, then feature code 3863 is not installed. You may still be able to

customize the partition image profiles, but cryptographic functions will not operate.

If you are planning to use PCIXCC or PCICA cards, you should contact IBM to get the feature code 3863 installed. The installation of the feature code is concurrent and is done by an IBM CE.

5.2 LPAR setup

This section contains the specific system setups that must be done prior to the installation of the PCIXCC and PCICA cards. This way, the cryptographic coprocessor installation can be done concurrently.

5.2.1 Planning considerations

The z990 always operates in LPAR mode. The concept of a dedicated coprocessor does not apply to PCIXCC or PCICA. PCI X Cryptographic Coprocessors are made available to logical partitions as directed by the domain assignment and the candidate list, regardless of the shared or dedicated status given to the CPs in the partition.

The z990 allows for up to 30 logical partitions to be active concurrently. Each PCIXCC or PCICA coprocessor supports 16 domains. If more than 16 active logical partitions on the z990 require concurrent access to a PCICA or PCI X Cryptographic Coprocessor, the configuration must include at least the following:

- Two PCI Cryptographic Accelerators in one PCICA feature
- Two PCI X Cryptographic Coprocessors in two PCIXCC features

Note: More features may be needed to satisfy application performance or availability requirements.

5.2.2 The image profile processor page

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 about the contents of the image profile pages, refer to *PR/SM Planning Guide,* SB10-7036.

The Image profile processor page enables the selection of:

- The number of logical processors that will be made available to the logical partition

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

Start the customizing of the image profile for the logical partition by performing 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 window shown in Figure 5-2 appears.

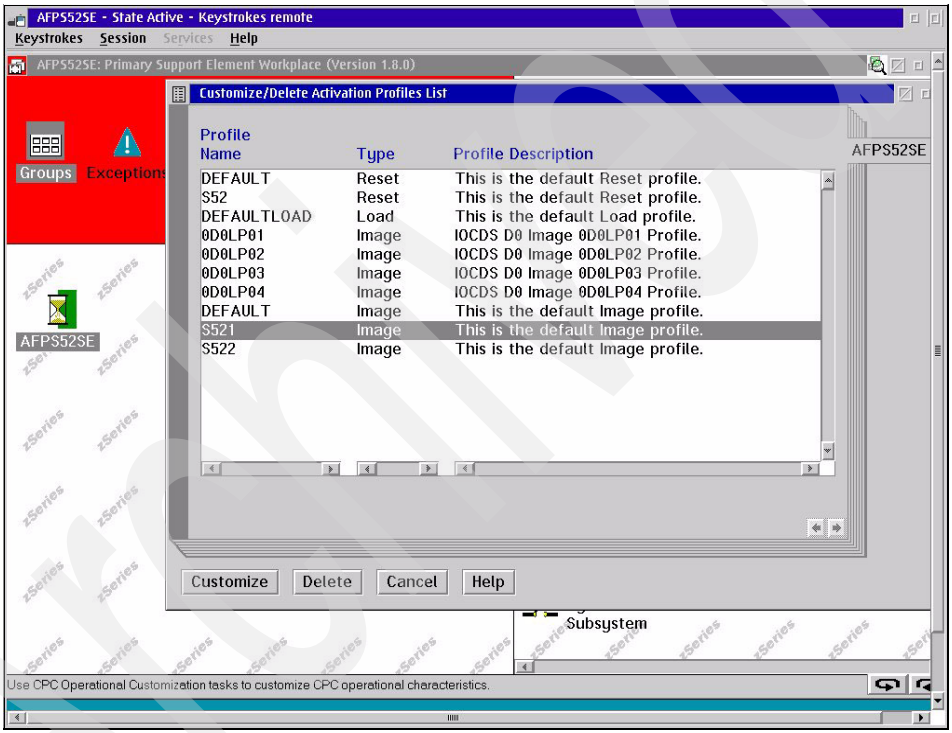

Figure 5-2 The Activation Profiles list

3. Select the image profile you want to work with and click **Customize**. In our case, we are working with the S521 image profile. The first page of the image profile is displayed as shown in Figure 5-3 on page 150.

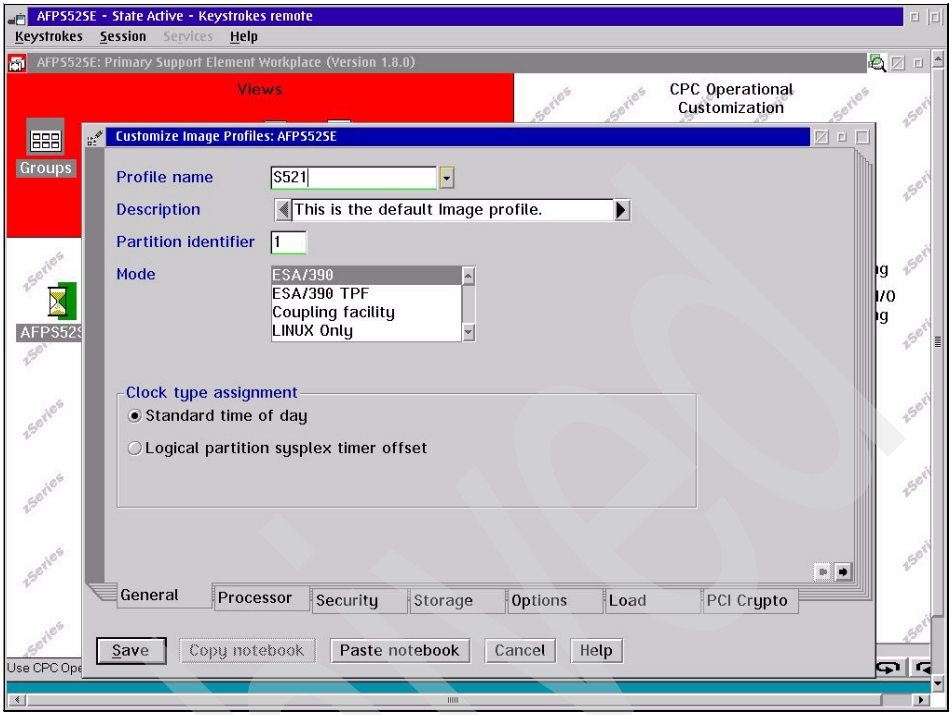

Figure 5-3 Customize Image Profile page of the selected image

4. Select the **Processor** tab to open the processor page (Figure 5-4 on page 151).

Archive

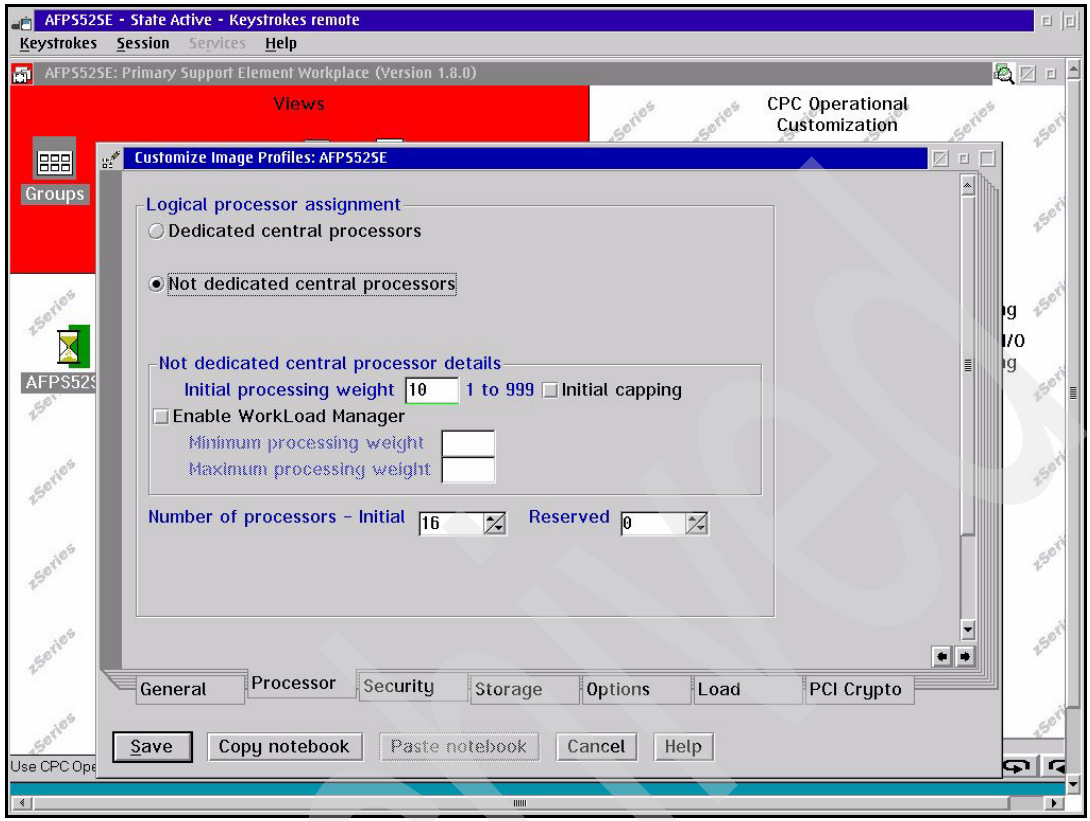

Figure 5-4 Customizing Image Profile: the processor page

The Image Profile processor page shown in Figure 5-4 no longer contains a selection for any cryptographic coprocessors.

Dedicated central processors

Electing to run a logical partition with dedicated central processors does not apply to PCIXCC or PCICA on z990.

5.2.3 The PCI Crypto page

The Crypto page allows the selection of parameters for the cryptographic setup of the logical partition. The definitions can be changed in the image profile, whether or not the logical partition is active. However, the new definitions will not take effect until the next time the partition is deactivated and activated again.

The definition of domain indexes and cryptographic coprocessor numbers in the Candidate list for each logical partition should be planned ahead to prepare your cryptographic configuration for non-disruptive changes.

Table 5-1 illustrates a simplified configuration map. Each row identifies a logical partition and each column identifies a cryptographic coprocessor, which is either installed or in plan. Each cell indicates the planned Usage Domain Index number or numbers to be assigned to the partition in its image profile. (We recommend that you work with a spreadsheet.)

Table 5-1 Planning LPAR domain and cryptographic coprocessor

Coprocessor ID	**00**	**01**	**02**	**03**	**04**	**05**	../..
Type	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC	
LPAR LP0	0	0			0	0	
LPAR LP1			0	0			
LPAR LP2	0	0	0	0			
LPAR LP3	4 14	4 14	4 14	4 14	4 14	4 14	
LPAR LP4			1	1	1	1	
.../...							

Up to 30 partitions can be defined and active, and each coprocessor has 16 domains. Within a row, the specified domain index number or numbers are identical, because the domain index applies to all selected cryptographic coprocessors in the partition Candidate list.

There is a potential conflict when, for a given column, different cells contain the same domain number.

In the example shown in Table 5-1:

- Both logical partitions LP0 and LP1 use domain 0, but are assigned different cryptographic coprocessors. The combination domain number and cryptographic coprocessor number is unique across partitions. Both partitions LP0 and LP1 can be active at the same time.
- Logical partition LP3 uses domain 4 and 14. Because no other partition uses the same domain numbers, there is no conflict.

Archived

- Logical partition LP4 uses domain 1 and no other partition uses the same domain number. Again, there is no conflict.
- Logical partition LP2 uses domain 0 on the set of cryptographic coprocessors that is already used by LP0 and LP1. Partition LP2 cannot be active concurrently with LP0 or LP1. However, this may be a valid configuration to cover for backup situations.

Figure 5-5 shows the selections that we made on the PCI Crypto page of the image profile of our S521 partition. See Chapter 3, “Planning and hardware installation” on page 45.

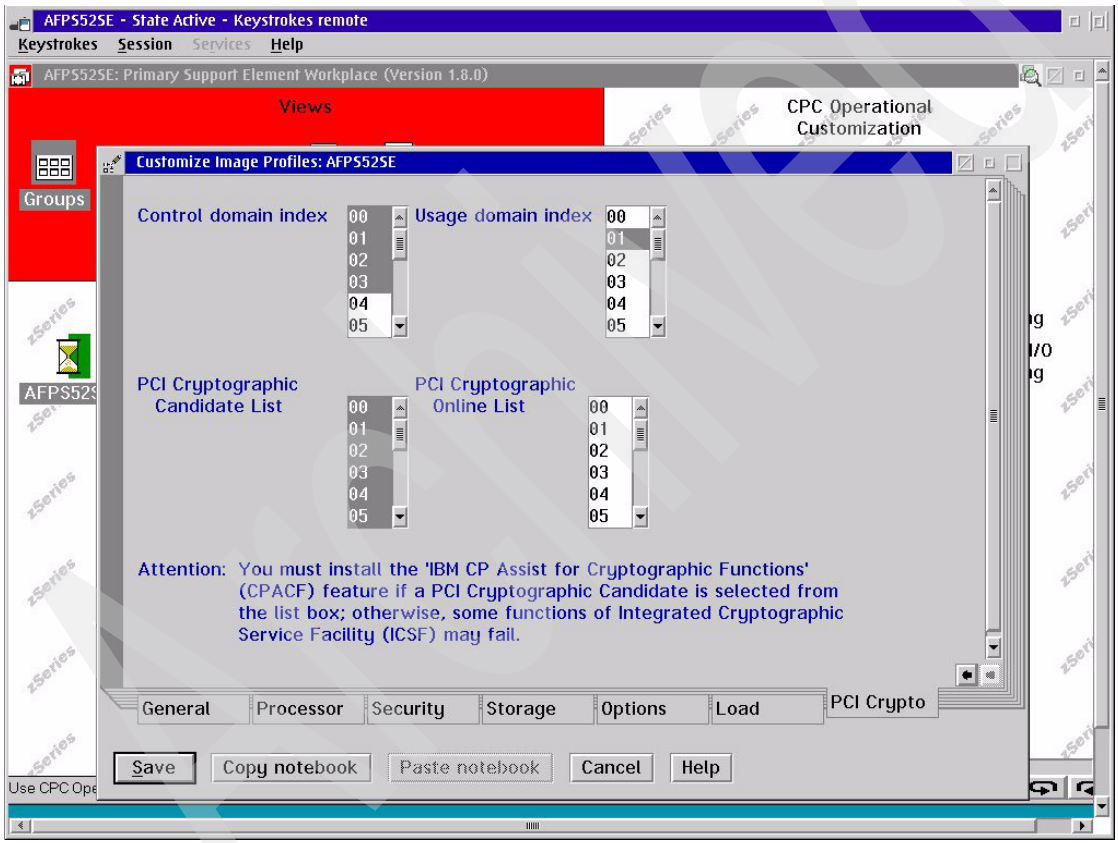

Figure 5-5 PCI Crypto page of the image profile

- Usage domain index

  This must point to the domain number or numbers for this logical partition, and it should match the domain number or numbers that were entered in the Options dataset when starting this partition’s instance of ICSF.

The same usage domain index can be used by multiple partitions regardless of which LCSS they are defined to, but the combination of cryptographic coprocessor number and usage domain index number must be *unique* across all partitions that are planned to be active at the same time.

Although it is possible to define duplicate combinations of cryptographic coprocessor numbers and usage domain indexes, such logical partitions cannot be concurrently active. This is a valid option, for example, for backup configurations.

Note: Beginning with z/OS1.2, the Usage Domain information is optional in the Options dataset if only one Usage Domain is defined for the logical partition. If more than one domain is specified as the Usage Domain on this panel, or if you are running ICSF in native mode, then domain information is required in the Options dataset.

When multiple domains are specified in the Usage Domain and no information is in the Options dataset, you will see the following message in the system log after ICSF is started:

```
$HASP373 CSF     STARTED
CSFM409E MULTIPLE DOMAINS AVAILABLE. SELECT ONE IN OPTIONS DATA
SET.
$HASP395 CSF      ENDED
```

- Control domain index

  This identifies the logical crypto coprocessor domain number as defined in other logical partitions that can be administered from this logical partition having been set up as the TCP/IP host for the TKE.

  If you are setting up the host TCP/IP in this logical partition for communicating with the TKE, this is the partition that will be used as a path to other domains' Master Keys. Indicate all of the domains that you want to access (including this partition's own domains) from this partition as control domains. In the example shown in Figure 5-5 on page 153, you can access Master Keys for domains 0, 1, 2, and 3 from the TKE.

- PCI Cryptographic Candidate List

  This identifies the cryptographic coprocessor numbers that are eligible to be accessed by this logical partition. From the scrollable list, select the coprocessor number or numbers, from 0 to 15, that identify the PCIXCC or PCICA Cryptographic Coprocessor to be accessed by this partition.

  When a selected cryptographic coprocessor number in the partition Candidate list is not available to the partition when the partition is activated, either because it is configured off or not installed, no error condition is

reported. The cryptographic coprocessor number is ignored and the activation process continues.

When a new cryptographic coprocessor is installed and its number has been previously selected in the partition Candidate list, it can be dynamically configured on to the partition from the Support Element using the Configure On/Off option in the Crypto Service Operations task list.

A cryptographic coprocessor number that is not in the partition Candidate list cannot be configured on to the partition.

- PCI Cryptographic Online List

  This identifies the cryptographic coprocessor numbers that are automatically brought online during logical partition activation. The coprocessor numbers that are selected in the Online list must also be part of the Candidate list.

  When the partition is activated, no error condition is reported if a cryptographic coprocessor number that is selected in the partition Online list is not installed. In this case, the Cryptographic Coprocessor is ignored and the activation process continues.

  When a cryptographic coprocessor number that is selected in the partition Online list has been previously configured off to the partition, it is automatically configured back on when the partition is next activated.

  If the cryptographic coprocessor number and usage domain index combination for the coprocessor selected in the partition Online list is already in use by another active logical partition, activation of the logical partition will fail and an error window is displayed.

When you have completed the PCI Crypto definitions for the partition, click **Save**. This brings you back to the Customize/Delete Activation Profiles List shown in Figure 5-2 on page 149.

Important: A Power-On Reset is not necessary, but the new definitions that have been entered in the partition image profile will not take effect until the next time the partition is deactivated and activated again.

After the next partition activation, installed PCI Cryptographic Coprocessors that are on the partition PCI Cryptographic Candidate list but not on the PCI Cryptographic Online list are in a *configured off* state (Standby or Not Isolated). They can be configured on to the partition later from the Support Element or HMC by using the Configure On/Off option in Crypto Service Operations task list. (See 5.3.1, “PCIXCC and PCICA enablement” on page 157.)

5.2.4 Viewing LPAR Cryptographic Controls

The LPAR Cryptographic Control definitions can be viewed without changing them accidentally. To see the LPAR Cryptographic Controls view, follow these steps to get access to the page:

1. Select the **CPC** icon in the CPC Work Area view (from the SE or SE Workplace).
2. Double-click **View LPAR Cryptographic Controls** in CPC Operational Customization. The panel shown in Figure 5-6 on page 156 appears.

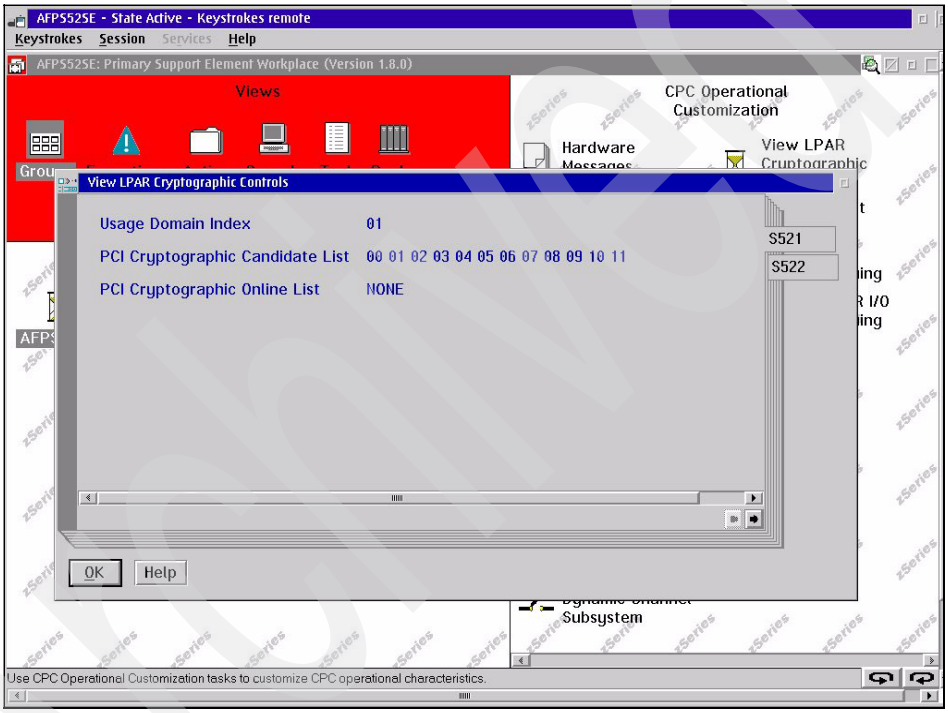

Figure 5-6 LPAR Cryptographic Controls view

On this window you can see what Usage Domain values are assigned and what PCI Cryptographic Candidate and Online selections have been chosen for the LPAR. This window cannot be used to change any of these values.

5.3 PCIXCC and PCICA feature installation

Keep in mind the following points:

- The PCIXCC or PCICA feature installation is done concurrently by the authorized personnel (IBM CE) using the Nondisruptive Hardware Change task on the Support Element.
- The STI-attached PCIXCC/PCICA cards are installed in channel card slots, so the corresponding PCHID number must be free (that is, not used in the IOCDS definition); otherwise, a configuration conflict will occur.
- A PCIXCC card serial number is automatically associated to a free adjunct processor (AP) number starting from 00.

  A PCICA card does have a serial number and it is also associated to a free adjunct processor (AP) number.
- When relocating a PCIXCC card to another system, the Master 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.

5.3.1 PCIXCC and PCICA enablement

The following section describes how to enable the PCIXCC and PCICA cards after installation. This is done by configuring the cards online using the Configure On/Off task. To do this:

1. Select from the **Crypto Service Operations** from Task List work area in the SE Workplace.
2. Select the **CPC** icon in the CPC Work Area view.
3. Right-click the CPC icon. The context menu enables you to select CPs, Channels, or PCI Crypto, as shown in Figure 5-7

Archive

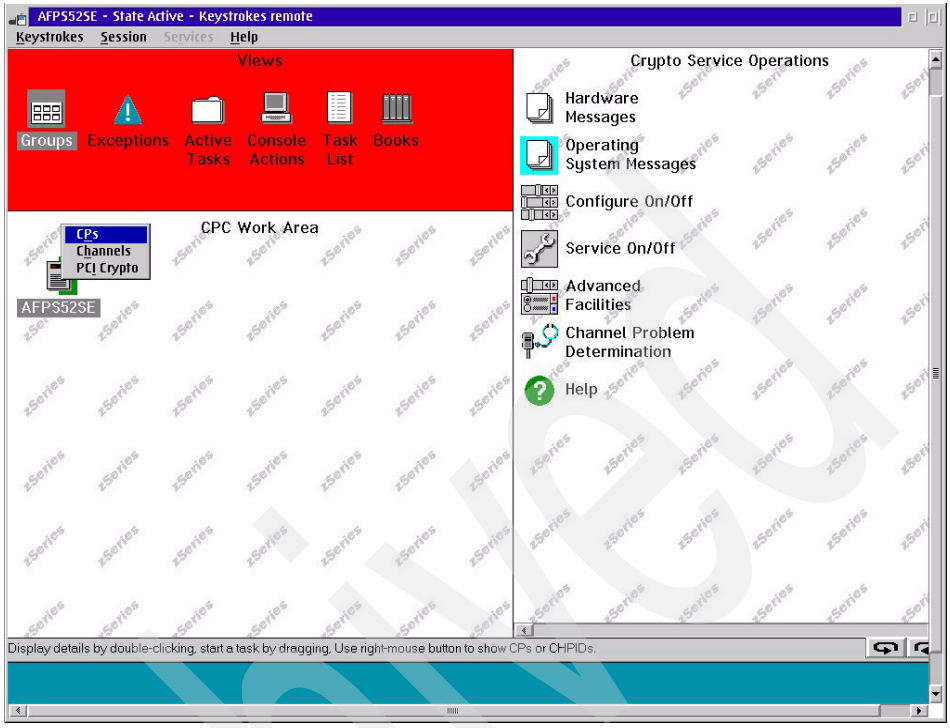

Figure 5-7 Right-clicked object on CPC Work Area view

4. Select **PCI Crypto** to open the window shown in Figure 5-8. This displays all of the PCI Crypto cards that are installed and their status. A letter X or A indicates the type of card (X means PCIXCC and A means PCICA).

Archived

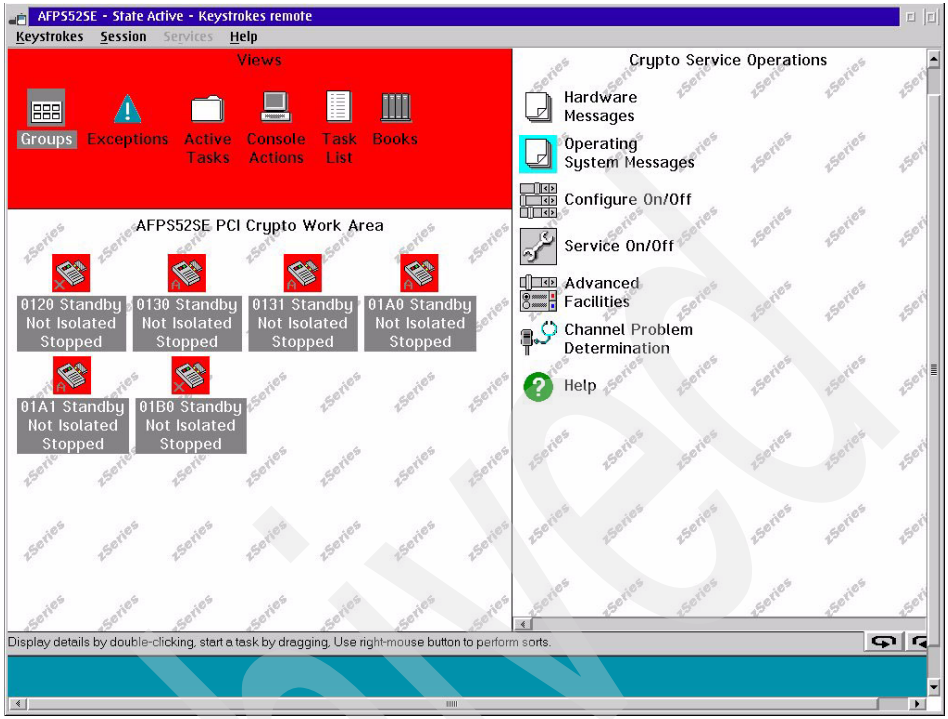

Figure 5-8 PCI Crypto Work Area view

5. Mark all of the PCI Crypto cards that you want to configure on by clicking the PCI Crypto icon (this has been done in Figure 5-8), and double-click **Configure On/Off task**. The Configure On/Off window is displayed, as shown in Figure 5-9 on page 160.

Archived

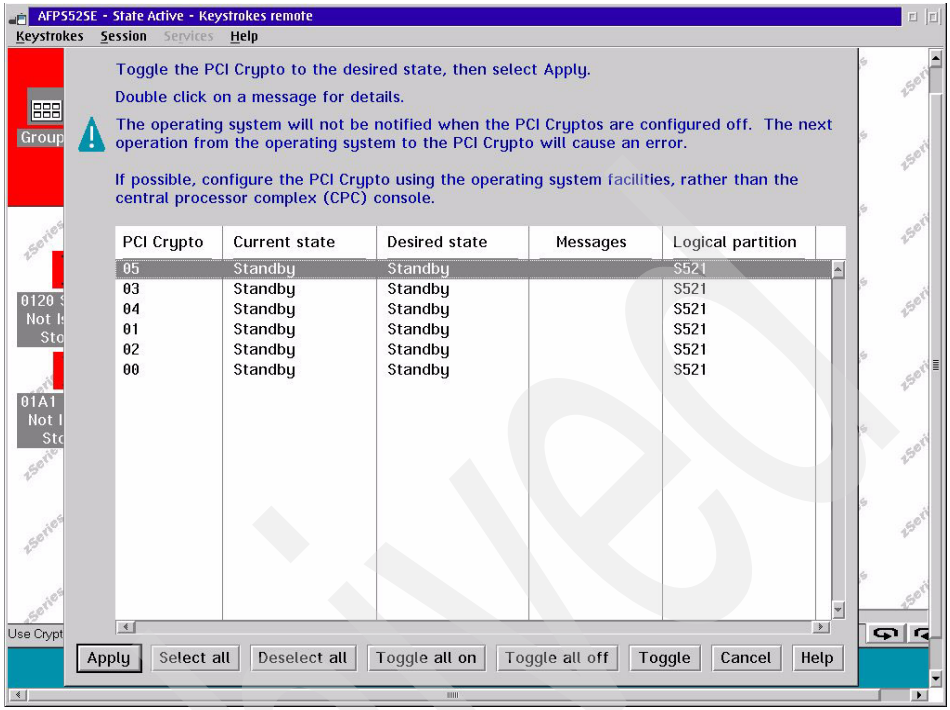

Figure 5-9 Configure On/Off window

6. Select the coprocessors that you want to configure on and click **Toggle** to change the status of the Cryptographic. Then click **Apply** to see the progress window displayed in Figure 5-10 on page 161.

Archive

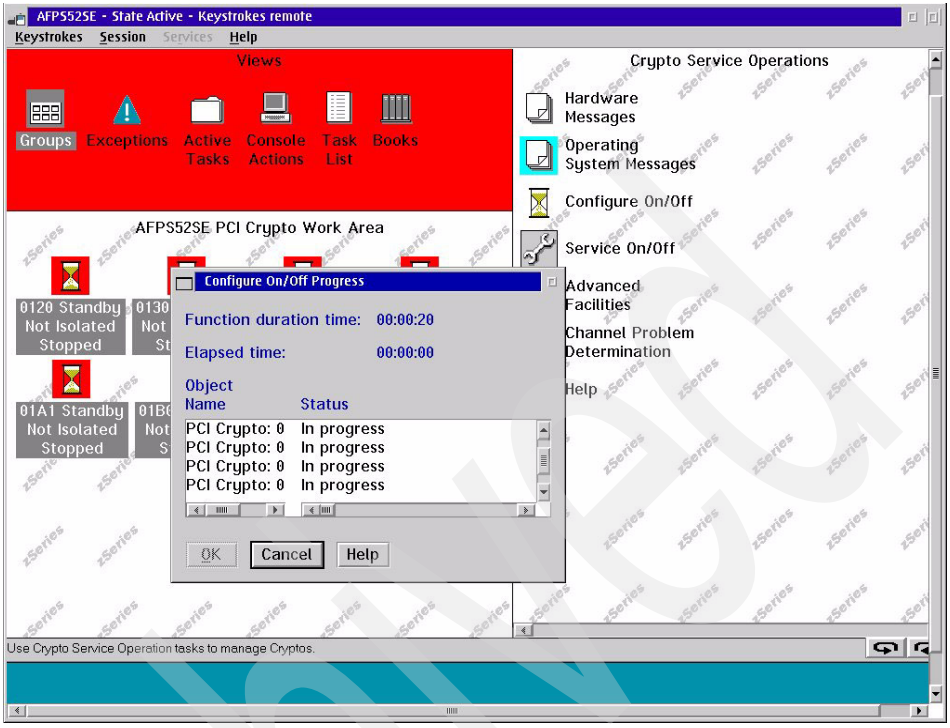

Figure 5-10 The PCI cards are configured "on"

Note: In the configuration process, the selected cryptographic coprocessors are brought online and the microcode is loaded into the PCIXCC. This process takes several minutes before loading is finished.

After the PCI cryptographic cards are configured on, you see the result as shown in Figure 5-11 on page 162, where the status has changed to Online, Not Isolated, and Operating. This status is given when the PCI cryptographic cards are viewed using the CPC Work Area. The same status on an Image from the Image Work Area will show Online, Shared, and Operating.

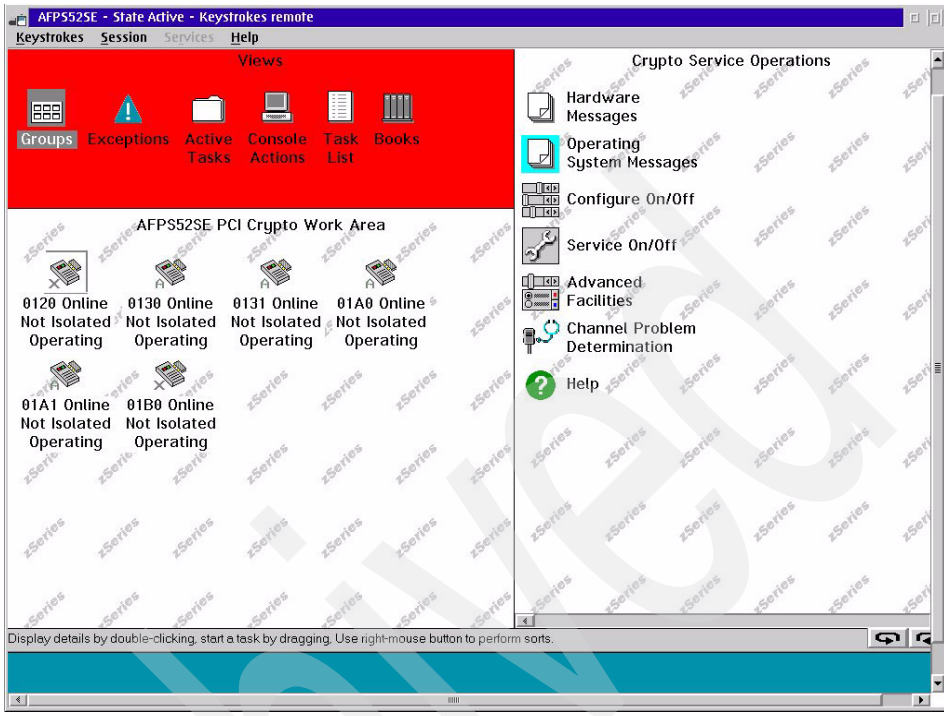

Figure 5-11 PCI Cryptographic cards after configuration online

After this the PCIX cryptographic coprocessors become visible to ICSF because the coprocessor numbers are part of the partition PCI Cryptographic Candidate list.

5.3.2 Configuring and monitoring the status of PCIXCC and PCICA

This section describes the configuration and monitoring tasks for PCIXCC and PCICA cards. For this the Support Element or HMC must be logged on in SERVICE or SYSPROG mode to enable access to the panel.

1. Select the **CPC** icon in the CPC Work Area in the SE Workplace.
2. In the CPC Configuration task list, select the task **PCI Cryptographic Configuration**, shown in Figure 5-12 on page 163.

Archived

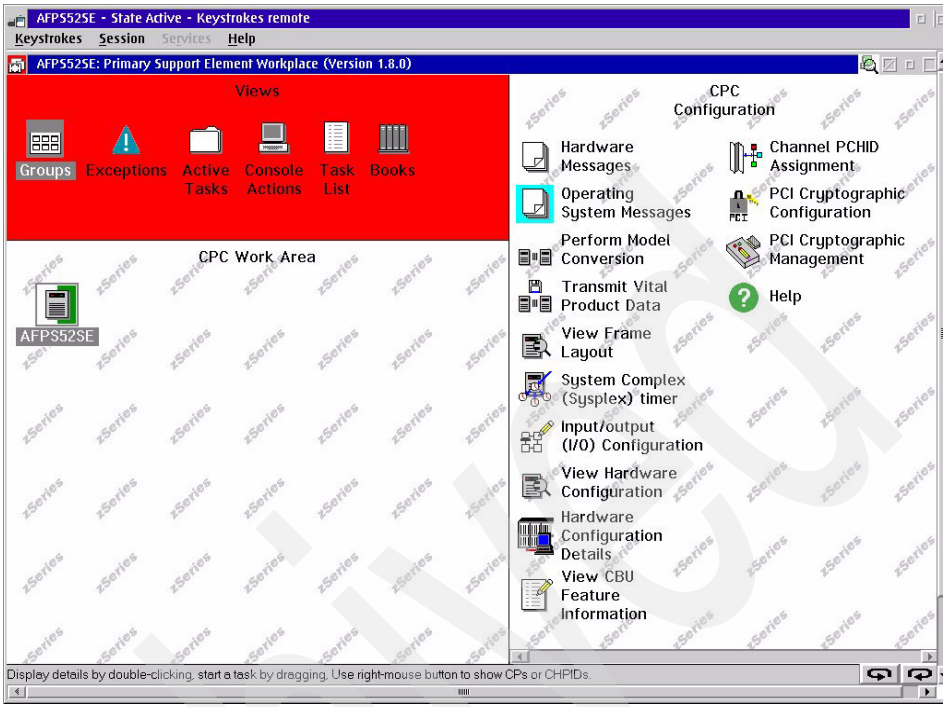

Figure 5-12 CPC Configuration task list selection

3. Double-clicking the **PCI Cryptographic Configuration** icon shows the main panel (Figure 5-13 on page 164) with the following information about the installed cards:
   - Number (that is, the AP number)
   - Status
   - PCI serial number
   - Type (which is either X Coprocessor for PCXICC or Accelerator for PCICA)
   - UDX status (User Defined eXtensions are only loadable into a PCIXCC)

Archive

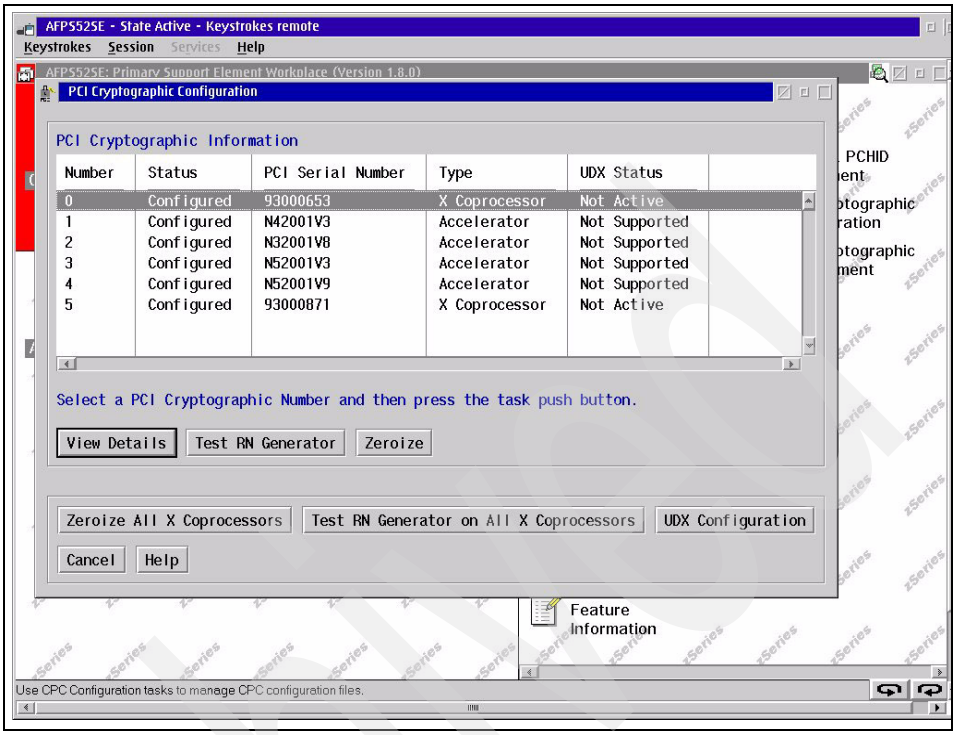

Figure 5-13 PCI Cryptographic Configuration main panel view

4. Selecting a PCIXCC processor and pressing **View Details** in the main panel displays the panel shown in Figure 5-14 on page 165.

Archive

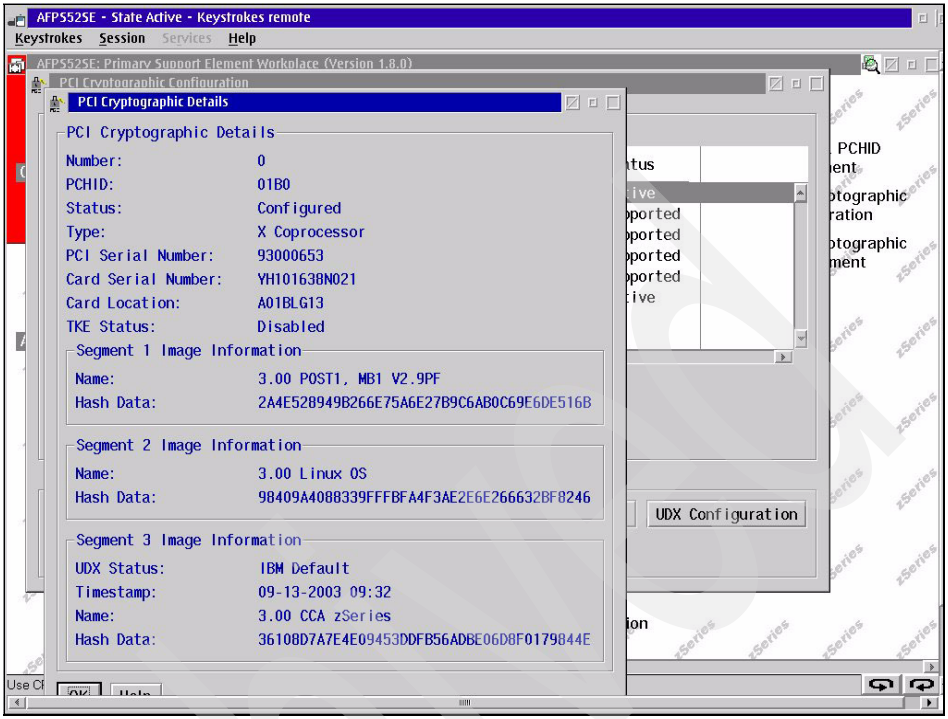

Figure 5-14 PCIXCC detail view

This view shows information about the AP number, PCHID, status, and serial numbers. The PCIXCC card PCI serial number is also shown in the ICSF Coprocessor Management panel. The detailed view also shows information about all three segments in the card and the hash values for each segment.

5. Selecting a PCICA processor and pressing **View Details** in the PCI Cryptographic Configuration main panel displays the window shown in Figure 5-15 on page 166.

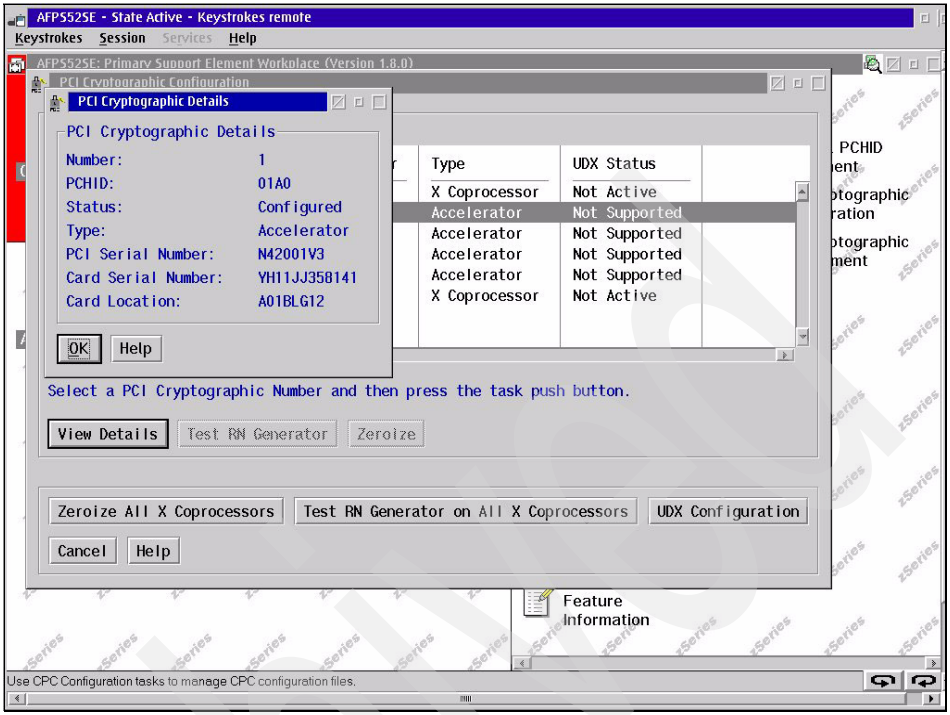

Figure 5-15 PCICA detail view

Figure 5-15 shows information about the AP number, PCHID, status, and the STI-attached Controller Card Serial Number.

In the PCI Cryptographic Configuration main panel, you can at any time (if the CPC is powered on) click **Test RN Generator** to test only the selected PCIXCC, or **Test RN Generator on All X Coprocessors,** which runs the same Random Number test on all PCIXCCs that are configured in the system.

If the test works correctly, you see the display shown in Figure 5-16 on page 167.

Archive

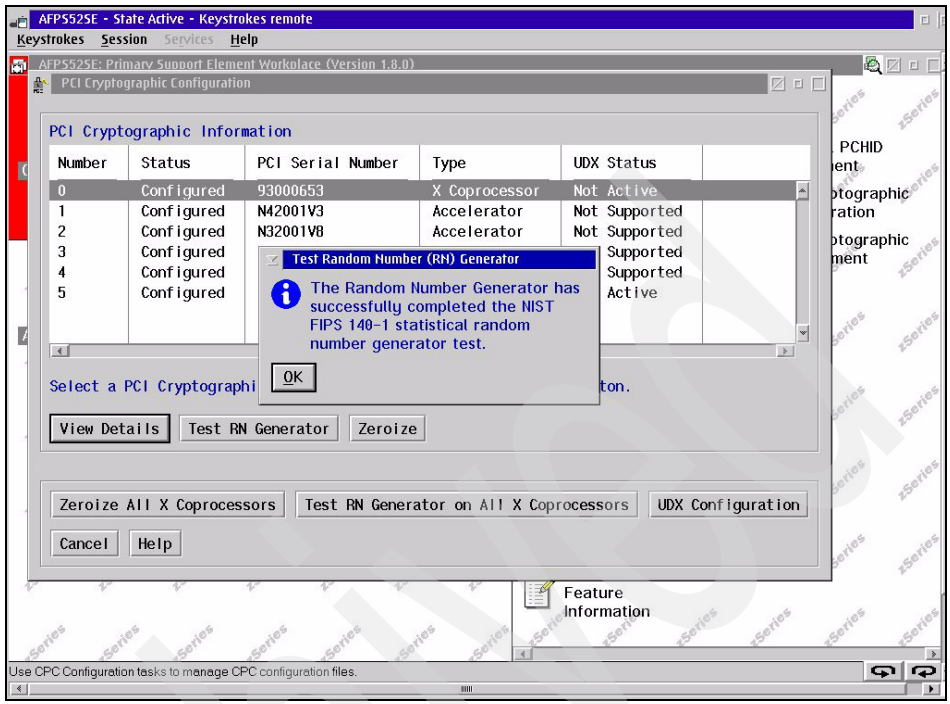

Figure 5-16 The result from the Random Number Generator test

5.3.3 Security issues with the PCI Cryptographic cards

This section describes what can be done if a PCI Cryptographic card has to be removed from the system. Some actions are applicable only to PCIXCC.

Attention: Using the retained private keys on PCIXCC creates a single point of failure because RSA retained private keys cannot be copied or backed up.

Zeroizing the PCIXCC before removal

If a PCIXCC has to be removed permanently from the system to be shipped back to IBM or for any other reason, you can zeroize the card. To do this, use the option on the PCI Cryptographic Configuration main panel. (See Figure 5-13 on page 164.)

Clicking **Zeroize** on the panel zeroizes all of the cryptographic keys and configuration data and resets the authorities and profiles in the selected card. The **`zeroize`** command can also be sent to all installed PCIXCCs by clicking **Zeroize All X Coprocessors**.

After clicking **Zeroize**, you see a confirmation window (Figure 5-17), where you must again click **Zeroize** to confirm the action.

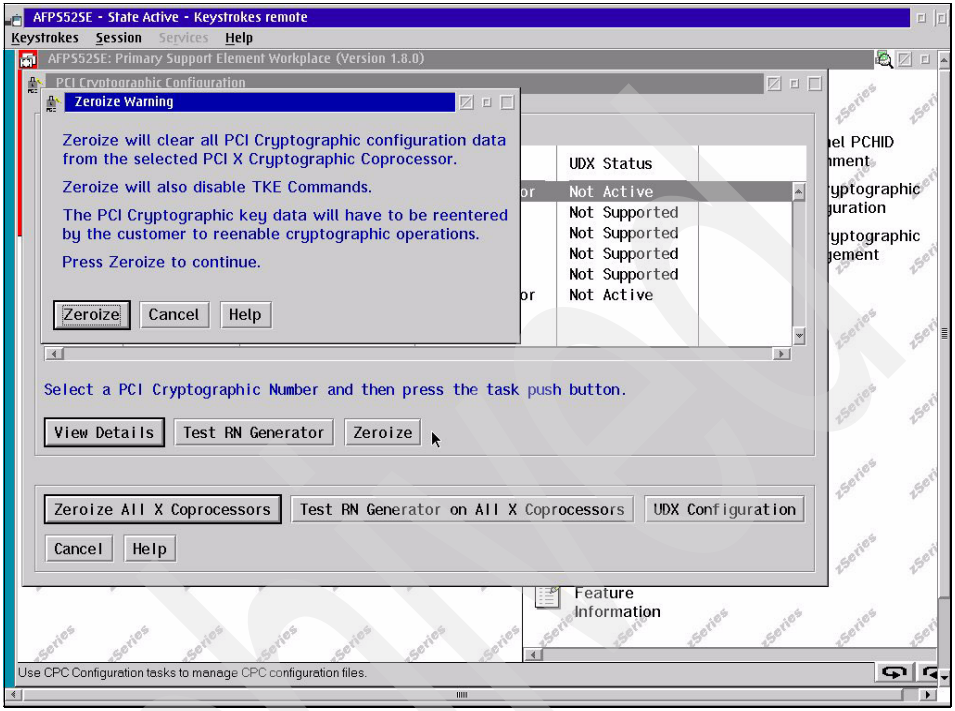

Figure 5-17 Zeroizing the PCIXCC must be confirmed

Important: There is an intrusion latch in the PCI X Cryptographic Coprocessor logic that is set any time the feature is removed from the system. If the feature is re-installed and power is applied, the coprocessor keys and secrets are zeroized and the intrusion latch is reset.

PCIXCC temporary removal

If the PCIXCC card is temporarily removed from the system (for example, for service) to be installed again in the same position with a TKE workstation available, the coprocessor may first be disabled from the TKE workstation before removing the feature from the system. In this case, when the feature is re-installed, the coprocessor keys and secrets are not zeroized, but the intrusion latch is reset and the coprocessor remains in the disabled state. The coprocessor then may be enabled from the TKE and normal operations may resume. See more detailed instructions from *ICSF TKE Workstation User's Guide,* SA22-7524-05.

Releasing the PCIXCC or PCICA for removal from the system

If a PCIXCC or PCICA has to be removed permanently from the CPC, you should remove the relationship between a PCI cryptographic feature serial number and the assigned coprocessor number (or numbers). To do this:

- Select the **CPC** icon in the CPC Work Area in the SE Workplace.
- In the CPC Configuration task list, select the task **PCI Cryptographic Management** (see Figure 5-12 on page 163).
- Select the cryptographic card to be released and click **Release** (Figure 5-18). If selecting the PCICA, it has two numbers for the same card serial number, so both will be released

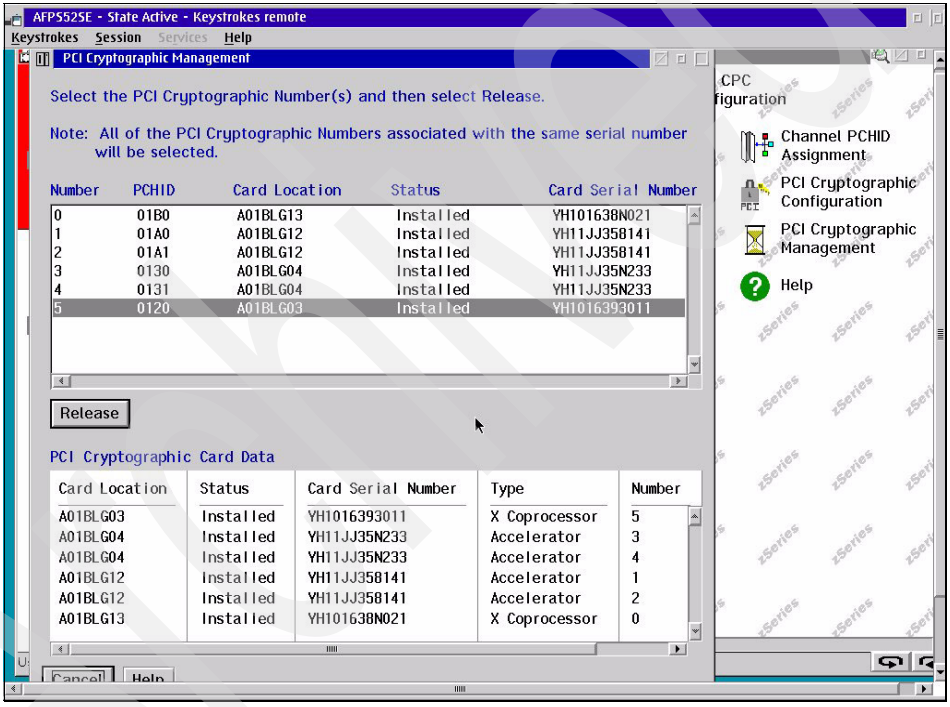

Figure 5-18 Releasing the PCI Cryptographic card

Removing the relationship enables coprocessor numbers to be freed, making them available to be assigned to a new feature serial number.

Important: The coprocessor number is assigned to the feature serial number, *not* to the installed location. If a feature is removed from one location to be reinstalled in another, the coprocessor number assignment remains.

5.4 Integrated Cryptographic Services Facility (ICSF) setup

In the following sections we describe the major changes from the previous release, as well as how to perform ICSF setup.

5.4.1 Changes from previous release

zzz PCI X Cryptographic Coprocessor (PCIXCC) support

Support for the new PCIXCC to be used on the z990 includes:

- Changes for many callable services
- Additional services added to the default CICS wait list
- New access control points

Note: The Commercial Data Masking Facility (CDMF) and DSS keys are no longer supported on the PCIXCC.

Options Data Set changes

With this release, the new CKTAUTH parameter has been added to the Options Data Set. This parameter decides whether authentication will be performed for every CKDS record that is read from DASD. If you specify this parameter with a value of NO, ICSF gains a small enhancement of performance. If CKTAUTH is not specified, the default value is NO.

ICSF TSO panels

The ICSF TSO panels have been added and updated.

- Pass Phrase initialization has been enhanced to intitialize a PKDS and the PCIXCC.
- The CKDS initialization panel has been changed (no need for many system keys).
- A new panel has been added to initialize PKDS.

CKDS and PKDS

The PCIXCC eliminates the need for many of the system keys in CKDS. If a CKDS is shared with the previous-level systems and initialization is needed, the CKDS must be initialized on the lower-level system.

The PKDS must be initialized first before it can be used by the callable services.

Archived

5.4.2 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, for OS/390 V2.8 or later.

Access to the ICSF administrative tasks or services can be restricted using RACF Facility class profiles.

When you start ICSF for the first time, you see the messages shown in Figure 5-19. You receive the CSFM411E message for each Cryptographic Accelelator Feature you have online, because they do not have to be initialized.

```
S CSFSTART
$HASP100 CSFSTART ON STCINRDR
IEF695I START CSFSTART WITH JOBNAME CSFSTART IS ASSIGNED TO USER
SYSTASK
 , GROUP SYS1
$HASP373 CSFSTART STARTED
CSFM101E PKA KEY DATA SET, CSF.SCSFPKDS IS NOT INITIALIZED.
CSFM419E INCORRECT MASTER KEY (BOTH) ON PCI X CRYPTOGRAPHIC
COPROCESSOR
X00, SERIAL NUMBER 93000653.
CSFM419E INCORRECT MASTER KEY (BOTH) ON PCI X CRYPTOGRAPHIC
COPROCESSOR
X05, SERIAL NUMBER 93000871.
CSFM411I PCI CRYPTOGRAPHIC ACCELERATOR A01 IS ACTIVE
CSFM411I PCI CRYPTOGRAPHIC ACCELERATOR A02 IS ACTIVE
CSFM411I PCI CRYPTOGRAPHIC ACCELERATOR A03 IS ACTIVE
CSFM411I PCI CRYPTOGRAPHIC ACCELERATOR A04 IS ACTIVE
CSFM100E CRYPTOGRAPHIC KEY DATA SET, CSF.SCSFCKDS IS NOT
INITIALIZED.
CSFM009I NO ACCESS CONTROL AVAILABLE FOR ICSF SERVICES OR KEYS
CSFM001I ICSF INITIALIZATION COMPLETE
CSFM400I CRYPTOGRAPHY - SERVICES ARE NOW AVAILABLE.
```

Figure 5-19 The first-time ICSF startup messages

5.4.3 Master Keys

ICSF uses two Master Keys to protect the keys that are used with the PCXICC.

- Symmetric-keys Master Key

This key (SYM-MK) is a double-length (128-bit) key that is used to protect DES keys that are used on the PCI X Cryptographic Coprocessor. The SYM-MK is actually a triple-length (192-bit) Master Key that ICSF enforces to be equivalent to a double-length (128-bit) Master Key.

This key must have the same value as the PCICC Symmetric-keys Master Key and the DES Master Key in the CCF if you want to share the Cryptographic Key Data Set (CKDS) with the lower-level systems.

- 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 X Cryptographic Coprocessor.

  This key must have the same value as the PCICC Asymmetric-keys Master Key and the SMK in the CCF if you want to share the Public Key Data Set (PKDS) with the lower-level systems.

5.4.4 Initial Master Key entry with the pass phrase initialization utility

The pass phrase initialization utility can be used to initialize the CKDS and the PKDS and install both the SYM-MK and the ASYM-MK on all PCI X Cryptographic Coprocessors on the z990.

To use this utility, all of the Master Key registers in the targeted coprocessors must be empty. Also, the designated CKDS and PKDS must not already be initialized (that is, they are both empty VSAM data sets).

Note: The PKDS initialization is mandatory on z990. Until this is done, PKA callable services cannot be enabled. This initialization can be done in Pass Phrase initialization or using a PKDS initialization panel.

When you access the ICSF panels, the Primary menu panel appears, as shown in Figure 5-20 on page 173.

Archived

```
HCR770A  -------------- Integrated Cryptographic Service
Facility-----------
Enter the number of the desired option.

 1 COPROCESSOR MGMT -  Management of Cryptographic Coprocessors
  2  MASTER KEY       -  Master key set or change, CKDS/PKDS
Processing
  3  OPSTAT          -  Installation options
  4  ADMINCNTL       -  Administrative Control Functions
  5  UTILITY          -  ICSF Utilities
  6  PPINIT          -  Pass Phrase Master Key/CKDS Initialization
  7  TKE             -  TKE Master and Operational Key processing
  8  KGUP             -  Key Generator Utility processes
  9  UDX MGMT         -  Management of User Defined Extensions

    Licensed Materials - Property of IBM
     5694-A01 (C) Copyright IBM Corp. 1989, 2003.  All rights
reserved.
   US Government Users Restricted Rights - Use, duplication or
     disclosure restricted by GSA ADP Schedule Contract with IBM
Corp.


Press ENTER to go to the selected option.
Press END   to exit to the previous menu.
OPTION ===> 6
```

Figure 5-20 Selecting the Pass Phrase option on the ICSF Primary menu panel

1. To begin the pass phrase initialization utility, select option **6 PPINIT**, and press Enter. Then type the pass phrase and the data set names in the provided spaces as shown in Figure 5-21 on page 174.
2. Answer `Y` to the question `Initialize the CKDS and PKDS?` For this first time, both CKDS and PKDS must be initialized.
3. Press Enter to run the utility. Its progress is indicated by messages, as shown in Figure 5-22 on page 174.

Archived

```
----------------- ICSF - Pass Phrase MK/KDS Initial  INITIALIZATION
COMPLETE

 Enter your pass phrase and the names of the CKDS and PKDS:

   Pass Phrase (16 to 64 characters)
   ===> Z990 CRYPTO UPDATE
   CKDS
   ===> 'CSF.SCSFCKDS'
   PKDS
   ===> 'CSF.SCSFPKDS'

   Initialize the CKDS and PKDS? (Y/N) ===> Y
   Initialize new PCIXCCs only ? (Y/N) ===> N

   The master key registers have been loaded.
   Initializing the key data sets...




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

Figure 5-21 Pass Phrase initialization complete messages

4. After pass phrase initialization, messages in the system log show that both PCIXCC cards are active and ICSF is ready for work (Figure 5-22).

```
 CSFM416I BOTH MASTER KEYS CORRECT ON PCI X CRYPTOGRAPHIC
COPROCESSOR X00, SERIAL NUMBER 93000653.
 CSFM416I BOTH MASTER KEYS CORRECT ON PCI X CRYPTOGRAPHIC
COPROCESSOR X05, SERIAL NUMBER 93000871.
```

Figure 5-22 Both PCIXCC cards becomes active after Pass Phrase initialization

Hardware status display after Pass Phrase initialization

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

1. Select **1 COPROCESSOR MGMT** on the ICSF Primary menu panel. This displays the panel shown in Figure 5-23 on page 175.

Archived

```
----------------------- ICSF Coprocessor Management -------- Row 1
to 6 of 6

 Select the coprocessors to be processed and press ENTER.
 Action characters are: A, D, E, R and S. See the help panel for
details.

   COPROCESSOR     SERIAL NUMBER   STATUS
   -----------     -------------   ------
.  A01                            ACTIVE
.  A02                            ACTIVE
.  A03                            ACTIVE
.  A04                            ACTIVE
s  X00             93000653        ACTIVE
s  X05             93000871        ACTIVE
***************************** Bottom of data
********************************
```

Figure 5-23 ICSF Coprocessor Management panel view

2. From this panel, select the processor (or processors) with the content that you want to see by entering S in front of the processor line, then press Enter.
3. The scrollable Coprocessor Hardware Status panel appears (Figure 5-24 on page 176). On this panel, you can view the status of the PCI X Cryptographic Coprocessors. You can check whether a card 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 hash pattern values.

Archived

```
---------------------- ICSF - Coprocessor Hardware Status
-------------------
                                                                CRYPTO
DOMAIN: 1

REGISTER STATUS                   COPROCESSOR X00         COPROCESSOR
X05

More:   +
 Crypto Serial Number         : 93000653             93000871
 Status                      : ACTIVE               ACTIVE
 Symmetric-Keys Master Key
   New Master Key register    : EMPTY                EMPTY
     Verification pattern     :
     Hash pattern             :
                              :
   Old Master Key register    : EMPTY                EMPTY
     Verification pattern     :
     Hash pattern             :
                              :
   Current Master Key register : VALID                VALID
      Verification pattern      : 1CB1F8FAB88F3CAE
1CB1F8FAB88F3CAE
     Hash pattern              : 123B5F85F3FB507A
123B5F85F3FB507A
                               : C2CA308EAFFE5CBD
C2CA308EAFFE5CBD
 Asymmetric-Keys Master Key
   New Master Key register    : EMPTY                EMPTY
     Hash pattern             :
                              :
   Old Master Key register    : EMPTY                EMPTY
     Hash pattern             :
                              :
   Current Master Key register : VALID                VALID
      Hash pattern             : 49D2C2D92DBAD143
49D2C2D92DBAD143
                               : B57C77B4DA4B2327
B57C77B4DA4B2327

Press ENTER to refresh the hardware status display.
```

Figure 5-24 Coprocessor Hardware Status view

Archived

4. The dynamic access to CKDS and PKA services is enabled after the pass phrase initialization. This can be seen by selecting option **4 ADMINCNTL** from the main panel. See Figure 5-25 on page 177 for details.

```
----------------- ICSF - Administrative Control Functions -- Row 1
to 4 of 4

       Active CKDS: CSF.SCSFCKDS
       Active PKDS: CSF.SCSFPKDS


 To change the status of a control, enter the appropriate character
 (E - ENABLE, D - DISABLE) and press ENTER.


    FUNCTION                                        STATUS
    --------                                        ------
.   Dynamic CKDS Access                             ENABLED
.   PKA Callable Services                           ENABLED
.   PKDS Read Access                                ENABLED
.   PKDS Write, Create, and Delete Access            ENABLED
***************************** Bottom of data
*******************************
```

Figure 5-25 Dynamic access to CKDS and PKA services enabled

5.4.5 Installation of a new PCIXCC or PCICA card

When concurrently installing a PCI X Cryptographic Coprocessor (PCIXCC) zzz or PCI Cryptographic Accelerator (PCICA) cards, PCICA cards become active because they work with clear key cryptography and do not use ICSF Master Keys.

To get a PCIXCC card active, it must have the same Symmetric Master Keys and the same Asymmetric Master Keys as on the previously installed PCIXCC.

1. To enter the same Master Key values to the newly installed PCIXCC card, the Pass Phrase initialization panel has an option for initializing only new PCIXCC. From the ICSF main panel, select option **6 PPINIT**.
2. On the Pass Phrase initialization panel, enter the same pass phrase as before. There is no need to fill in the names of the CKDS and PKDS. Respond `Y` to the question of initializing only new PCIXCCs. After you press Enter, PCIXCC initialization will be complete. An example of this is shown in Figure 5-26 on page 178.

Archived

```
----------------- ICSF - Pass Phrase MK/KDS Initial  INITIALIZATION
COMPLETE

 Enter your pass phrase and the names of the CKDS and PKDS:

   Pass Phrase (16 to 64 characters)
   ===> z990 crypto update
   CKDS
   ===>
   PKDS
   ===>

   Initialize the CKDS and PKDS? (Y/N) ===> N
   Initialize new PCIXCCs only ? (Y/N) ===> Y

   The master key registers have been loaded.
   Processing the key data sets...



Press ENTER to process.
Press END   to exit to the previous menu.
```

Figure 5-26 Pass Phrase Initialization for the new PCIXCC

The system log message that is displayed in Figure 5-27 shows that the entered Master Keys match and the new PCIXCC card is active.

```
 CSFM416I BOTH MASTER KEYS CORRECT ON PCI X CRYPTOGRAPHIC
COPROCESSOR XO5, SERIAL NUMBER 93000871.
```

Figure 5-27 The PCIXCC becomes active after initialization

5.4.6 PKDS initialization

The PKDS initialization is mandatory on z990. If the Pass Phrase initialization option cannot be used and the PKDS will be shared with lower-level systems, there might be a need to initialize the PKDS.

1. This can done by selecting **2 MASTER KEY** on the ICSF main panel (see this in Figure 5-20 on page 173) and pressing Enter.

Archived

```
---------------------- ICSF - Master Key Management
------------------------

Enter the number of the desired option.

 1  INIT/REFRESH CKDS -  Initialize a Cryptographic Key Data Set or
                            activate an updated Cryptographic Key Data
Set
  2  SET MK          -  Set a DES/symmetric-keys master key
   3  REENCIPHER CKDS    -  Reencipher the CKDS prior to changing the
DES
                         master key
   4  CHANGE MK          -  Change the DES/symmetric-keys master key
and
                        activate the reenciphered CKDS

 5  INITIALIZE PKDS   -  Initialize or update a PKDS Cryptographic
                         Key Data Set header record
   6  REENCIPHER PKDS    -  Reencipher the PKA Cryptographic Key Data
Set
   7  ACTIVATE PKDS      -  Activate the PKDS after it has been
reenciphered
  8  REFRESH CACHE     -  Refresh the PKDS Cache if enabled

Press ENTER to go to the selected option.
Press END   to exit to the previous menu.

OPTION ===> 5
```

Figure 5-28 Master Key management panel view

2. On the Master Key Management panel, shown in Figure 5-28, select **5 INITIALIZE PKDS** and press Enter.
3. The PKDS initialization panel is displayed. Type the name of the PKDS into the provided space and press Enter to initialize the PKDS, as shown in Figure 5-29 on page 180.

Archived

```
------------- ICSF - Initialize PKA Cryptographic K         PKDS
INITIALIZED

Enter the name of the PKDS below.

  PKDS ===> 'CSF.SCSFPKDS'









Press ENTER to initialize the PKDS.
Press END   to exit to the previous menu.
```

Figure 5-29 PKDS Initialization processed

After pressing Enter on the PKDS Initialization panel, messages shown in Figure 5-30 indicate that verification of the Hash pattern between the PCIXCC cards and PKDS Header record is done and the result is correct.

```
CSFM416I BOTH MASTER KEYS CORRECT ON PCI X CRYPTOGRAPHIC COPROCESSOR
X00
, SERIAL NUMBER 93000871.
CSFM416I BOTH MASTER KEYS CORRECT ON PCI X CRYPTOGRAPHIC COPROCESSOR
X05
, SERIAL NUMBER 93000653.
```

Figure 5-30 Message after PKDS initialization

This process does not enable PKA services. This is done with option **4 ADMINCNTL** from the ICSF main panel. Press Enter, and the Administrative Control Functions panel is shown. To enable PKA services, enter e in front of the PKA service rows, as shown in Figure 5-31 on page 181.

Archived

```
----------------- ICSF - Administrative Control Functions -- Row 1
to 4 of 4

       Active CKDS: CSF.SCSFCKDS
       Active PKDS: CSF.SCSFPKDS


 To change the status of a control, enter the appropriate character
 (E - ENABLE, D - DISABLE) and press ENTER.


   FUNCTION                                          STATUS
   --------                                          ------
.  Dynamic CKDS Access                               ENABLED
e  PKA Callable Services                             DISABLED
e  PKDS Read Access                                  DISABLED
e  PKDS Write, Create, and Delete Access              DISABLED
***************************** Bottom of data
********************************
```

Figure 5-31 Enabling the PKA services

Again, a confirmation message appears, as shown in Figure 5-30 on page 180, to indicate that both PCIXCC cards have valid Master Keys.

Archived

Archived

6

Performance and monitoring

In this chapter, we describe the tools that are available on z/OS for monitoring of the z990 cryptographic hardware utilization plus the analysis of performance.

Archived

© Copyright IBM Corp. 2004. All rights reserved.

6.1 z990 Crypto hardware performance considerations

Most cryptographic hardware in zSeries processors can only be used through ICSF (which is a standard component of OS/390 and z/OS). ICSF is invoked by the application requesting a cryptographic service via an API. Thus, ICSF shields the complexity of the hardware communication from the user.

The ICSF API call has a system path length that has to be added (from an application's view) to the execution time of the cryptographic hardware. For example, for symmetric key operations, it is advisable to have the application initiate a single API call for the *total* block of data, in order to limit the number of ICSF API calls.

It should be noted that since CCFs and PCICC cards are not supported on z990, the path length for some functions will change. Functions that were previously handled by CCF, but which must now be handled by PCIXCC, have a longer path length due to the nature of the interface to the cards, leading to an apparent lessening of throughput. On the other hand, functions that were handled by PCICC will not show much change under PCIXCC.

With the z990, some operations have been architected into the processor core itself. Several new machine instructions have been made available which do not require ICSF service calls to be made (though ICSF itself must be active). When CPACF is enabled, every CP has a cryptographic engine associated with it. Thus, when a crypto-related instruction is executed, the cryptographic processing takes place in the CP's own CPACF engine. Therefore there are none of the potential scheduling delays associated with the CCF affinity to just one or two CPs as in previous processors.

These instructions only support clear key operations for symmetric encryption/decryption and secure hashing. In this way some of the most frequently used operations have very low latency; there is no additional instruction path length.

Applications in the Internet environment will not use the cryptographic operations themselves; instead, they will follow protocol standards as, for example, Secure Socket Layer (SSL). Executing the SSL protocol for a server (or client) on a zSeries system will result in a series of cryptographic operations which, under z/OS and ICSF, will either exploit available cryptographic hardware or be executed in software.

The SSL protocol will result in CPU path length (due to the protocol itself and due to ICSF), the symmetric key operations execution time (synchronous to the CPU), and the execution time of the public key operations (which may be parallel to the CPU operation). With z990, using z/OS or OS/390 with the appropriate

Web update, SSL will use the CPACF and PCICA hardware assists if available for handshake and data transfer, thus potentially reducing the instruction path length.

For more information see the articles available on the IBM Techdocs - Technical Sales Library Web site:

`http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/Techdocs`

Some useful documents can be found at:

`http://www.ibm.com/support/techdocs/astmastr.nsf/Webindex/WP100345`

6.2 Monitoring and reporting

In this section we describe how to use SMF data to investigate crypto hardware usage.

There are several SMF record types that record z990 crypto hardware usage:

- Type 30 (Common Address Space Work)

  Field SMF30CSC in the Processor Accounting Section records the number of cryptographic instructions executed on behalf of the caller (within the caller's address space).

- Type 70 (RMF Processor Activity)

  Beginning with z/OS 1.2 and APAR OW49808, record type 70 has a new subtype 2 for measurements of cryptographic processors. The data in the original type 70 is now recorded in type 70 subtype 1.

- Type 72 (RMF Workload Activity and Storage Data)

  In WLM goal mode, subtype 3 reports on each service or report class in the active WLM policy. In the Service/Report Class Period Data Section there are fields reporting cryptographic coprocessor usage and delays.

- Type 82 (ICSF record)

  The subtypes of this record report information about events and operations against ICSF. Subtypes 17 (for PCICC) and 19 (for PCIXCC) are written periodically and are the only records that report any coprocessor statistics; all others report operational or administrative activity.

6.2.1 RMF reporting

Starting with z/OS V1R2, RMF adds more transparency in the area of cryptographic processing by reporting Crypto Using and Delay values in the

Archived

Goals vs. Actuals section of the Postprocessor WLMGL report. Tasks that are found to be using or waiting for a crypto processor (synchronous or asynchronous) are reported on a service or report class period level.

In addition, RMF provides the Postprocessor Crypto Hardware Activity report, which is based on a new SMF record - type 70 subtype 2. Besides detailed utilization information about each configured PCIXCC and PCICA card (in the case of the z990), the report provides performance measurements on selected ICSF activities on the crypto hardware. The data shown for PCIXCC and PCICA always reflects the total activity in a CPC.

This functionality is available for z/OS 1.2 and beyond and is installed as RMF APAR OW49808 and ICSF APAR OW51003. In addition RMF APAR OW56656 should be installed for proper support of the z990.

RMF has a third overview reporting function to select specific fields for reporting. We show JCL examples here, but all the reports can also be generated using the ISPF panels of RMF. See *z/OS RMF User's Guide,* SC33-7990 for details.

Crypto Hardware Activity report

The Crypto Hardware Activity report shows the usage of the different crypto coprocessors. This information is gathered by Monitor I by default; specify

```
NOCRYPTO
```

in the RMF Monitor I options if you want to suppress data gathering.

The report is generated by the RMF post-processor using the option:

```
REPORTS(CRYPTO)
```

Other RMF options can be used to limit the reporting intervals etc. Figure 6-1 on page 186 shows JCL which can be used to produce the report. The DD name MFPINPUT points to the SMF dataset containing the RMF records.

```
//PK3RMF JOB (),PS,CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
//*
//RMFP EXEC PGM=ERBRMFPP
//MFPINPUT DD DISP=SHR,DSN=MVS.SMF.SAVE
//MFPMSGDS DD SYSOUT=*
//SYSIN   DD *
 SYSOUT(X)
 REPORTS(CRYPTO)
//
```

Figure 6-1 JCL to produce the RMF report

The report, which is generated under the DD name PPORPnnn (where nnn is 001, 002 etc. for each system in the SMF data), will look something like Figure 6-2 (note this is truncated on the right in this image).

```
 C R Y P T O  H A R D W A R E  A C T I V I T Y

           z/OS V1R4                SYSTEM ID VSPK            DATE 10/27/2003           INT
                                    RPT VERSION V1R2 RMF      TIME 19.00.00             CYC
-------- CRYPTOGRAPHIC COPROCESSOR --------
          -------- TOTAL --------  KEY-GEN
TYPE   ID   RATE  EXEC TIME  UTIL%   RATE
PCIXCC  0  375.9      1.4    54.4    0.27
        5  180.5      2.2    39.3    0.29

-------- CRYPTOGRAPHIC ACCELERATOR ----------------------------------------------------------
          -------- TOTAL -------  ------- ME(1024) -----  ----- ME(2048) ------  ------ CRT(1
TYPE   ID   RATE  EXEC TIME UTIL%   RATE  EXEC TIME UTIL%   RATE EXEC TIME UTIL%   RATE  EXEC
PCICA   1   0.00      0.0     0.0   0.00      0.0     0.0   0.00      0.0     0.0   0.00      0
        2   0.00      0.0     0.0   0.00      0.0     0.0   0.00      0.0     0.0   0.00      0
        3   0.00      0.0     0.0   0.00      0.0     0.0   0.00      0.0     0.0   0.00      0
        4   0.00      0.0     0.0   0.00      0.0     0.0   0.00      0.0     0.0   0.00      0

-------- ICSF SERVICES EXECUTED ON PCIXCC ---------------------------------------------------
       DES ENCRYPTION    DES DECRYPTION    ----- MAC ------    - HASH -    ------ PIN -------
       SINGLE  TRIPLE    SINGLE  TRIPLE    GENERATE  VERIFY              TRANSLATE  VERIFIY
RATE     0.00    0.00     166.8    0.00       111.2    0.00       0.00       55.59    55.59
SIZE     0.00    0.00      2936    0.00        4400    0.00       0.00
```

Figure 6-2 RMF Crypto hardware activity report

See *z/OS RMF Report Analysis,* SC33-7991 for full descriptions of the fields.

Note: With APAR OW56656 (z990 RMF support), the report has been updated to clarify the utilization of different coprocessor types on z990.

Important: Ensure you have APAR OA05379 installed to get the correct values in the DES encryption/decryption fields.

Workload Activity report

The Service/Report Class Period option of the Workload Activity report shows the usage and delay values attributable to crypto coprocessors. The report can be generated using the option:

```
SYSRPTS(WLMGL(SCPER))
```

Sample JCL is given in Figure 6-3. By default, all service class names are reported. A list of class names can be specified on the SCPER keyword for reports of selected classes.

```
//PK3RMF JOB (),PS,CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
//*
//RMFP EXEC PGM=ERBRMFPP
//MFPINPUT DD DISP=SHR,DSN=MVS.SMF.TEMP
//MFPMSGDS DD SYSOUT=*
//SYSIN   DD *
 SYSOUT(X)
 SYSRPTS(WLMGL(SCPER))
```

Figure 6-3 JCL showing the SCPEr keyword

Figure 6-4 shows the relevant lines of the report with fields for crypto usage and delays.

```
--USING%--  ------------ EXECUTION DELAYS % ------------  ---DLY%-- -CRYPTO%-    %
 CPU   I/O  TOTAL                                        UNKN IDLE  USG  DLY QUIE


 3.2   0.0    0.0                                       98.4  0.0 51.2  0.0  0.0
```

Figure 6-4 Delays report

Restriction: WLM only records usage and delay data for PCIXCC cards, PCICA cards are not included.

RMF Overview reports

The Overview report option provides a way to produce a report of selected fields from the various RMF records, to your own specification. For example, in Figure 6-5 we show how to produce a report showing the values for the transaction rate and card utilization for the two PCIXCC cards.

The OVW statements define the conditions to be reported on. For example, the first statement selects the condition CRYCTR for PCIXCC card 0. This is the card transaction rate in operations per second, and will appear on the report under the heading CCTR0. The second statement selects the condition CRYCTU for card 0, which is the card utilization percentage. This will appear under the CCTU0 heading, and so on.

Archived

```
//PK3RMF JOB (),PS,CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
//*
//RMFP EXEC PGM=ERBRMFPP
//MFPINPUT DD DISP=SHR,DSN=MVS.SMF.TEMP
//MFPMSGDS DD SYSOUT=*
//SYSIN   DD *
 SYSOUT(X)
 OVERVIEW(REPORT)
 OVW(CCTRO(CRYCTR(0)))
 OVW(CCTUO(CRYCTU(0)))
 OVW(CCTR5(CRYCTR(5)))
 OVW(CCTU5(CRYCTU(5)))
//
```

Figure 6-5 JCJ for Transaction rate and card Utilization report

The report looks like Figure 6-6.

```
 R M F   O V E R V I E W   R E P O R T

           z/OS  V1R4              SYSTEM ID VSPK
                                   RPT VERSION V1R2 RMF

NUMBER OF INTERVALS 172      TOTAL LENGTH OF INTERVALS 14.20.00
DATE   TIME   INT    CCTRO    CCTUO    CCTR5    CCTU5
MM/DD HH.MM.SS MM.SS
11/01 12.11.18 05.00     157.65      40.6      0.00       0.0
11/01 12.16.18 04.59     176.29      45.5      0.01       0.0
11/01 12.21.18 05.00       0.00       0.0      0.00       0.0
11/01 12.26.18 04.59      33.45       8.7      0.00       0.0
11/01 12.31.18 05.00      33.34       8.6      0.00       0.0
.
.
.
```

Figure 6-6 Transaction rate and card Utilization report

Archived

If desired, an overview record dataset can also be produced. This will contain the selected fields in a format more suitable for further batch processing or analysis, for example.

Note: APAR OW56656 changes the condition names (though the original names are still supported) in Overview and Exception reports. Conditions named PCICCxxx or PCICAxxx are renamed to CRYCxxx or CRYAxxx. For example, PCICCTR is replaced by CRYCTR. All conditions based on ICSF activities are renamed from CCFxxxx to CRYIxxxx. For example, CCFSDER is replaced by CRYISDER.

Generating spreadsheets

The RMF Spreadsheet Reporter does not support Crypto Hardware records, but the Overview report or records dataset can be used to create the spreadsheets of your choice.

For example, using the Overview report produced above, the columns of data can be cut and pasted into a spreadsheet. If the report is large, save the report in a dataset, either by changing the JCL to add an Overview report DD name of the form PPORPnnn (Figure 6-7), or saving the SYSOUT using a tool like SDSF.

```
//RMFP EXEC PGM=ERBRMFPP
//MFPINPUT DD DISP=SHR,DSN=MVS.SMF.TEMP
//MFPMSGDS DD SYSOUT=*
//PPORP001 DD DSN=PK3.RMF.OVERVIEW,DISP=(,CATLG),
//  SPACE=(CYL,(1,1)),UNIT=3390
//SYSIN   DD *
```

Figure 6-7 JCL for saving the report to an Overview data set

The data set can then be transferred to a PC using the transfer mechanism of your choice, for example FTP or IBM PC 3270 File Transfer. Ensure that the data is transferred in ASCII mode. The data can then be imported into the spreadsheet of your choice and manipulated as required.

Figure 6-8 on page 191 shows a simple graph of the transaction rate for one card for a mix of jobs. This was produced from an Overview report with a 5-minute interval.

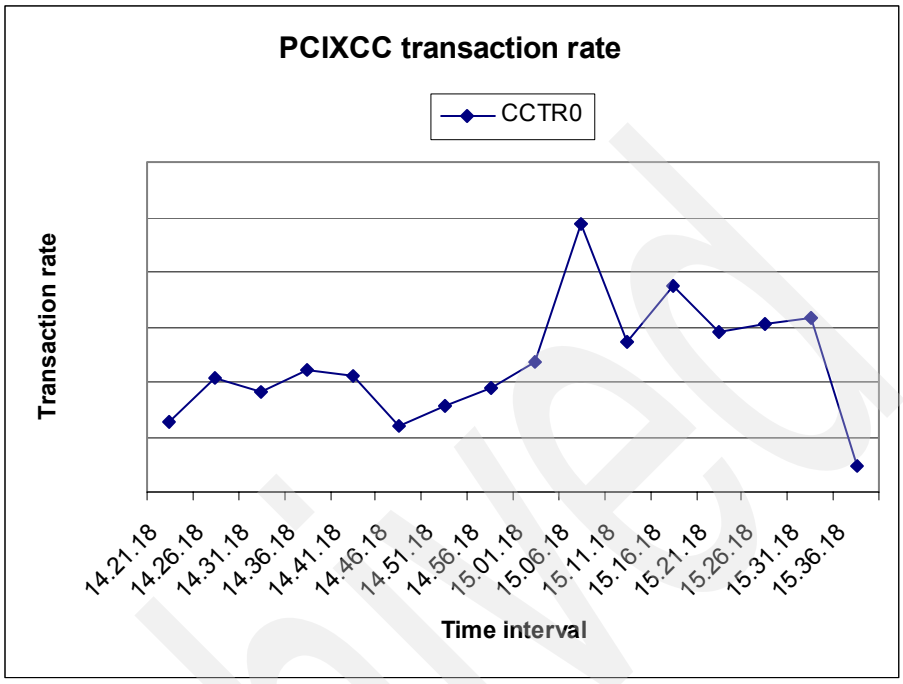

Figure 6-8 Transaction rate graph

RMF examples using test jobs

We ran 10 test jobs simultaneously, each using different crypto calls to capture data that would be reported by RMF.

The jobs each ran a loop executing a different function, either:

- Single or Triple DES encryption or decryption, data size of 8000 bytes
- Single or Triple DES MAC generation or verification, data size of 8000 bytes
- PIN translate or verify

We set up the loops so that the jobs ran over several RMF intervals, which we had set to 5 minutes. The z990 system was otherwise lightly loaded.

The relevant parts of the Crypto Hardware report are shown in Figure 6-9.

Archive

```
-------- CRYPTOGRAPHIC COPROCESSOR --------
            -------- TOTAL --------  KEY-GEN
TYPE    ID   RATE  EXEC TIME  UTIL%    RATE
PCIXCC  0  561.0      1.8    99.4     0.00
        5  485.1      2.0    98.7     0.00
.
.
.
-------- ICSF SERVICES EXECUTED ON PCIXCC -----------------------------------------------------
        DES ENCRYPTION    DES DECRYPTION    ----- MAC ------    - HASH -    ------ PIN -------
        SINGLE  TRIPLE    SINGLE  TRIPLE    GENERATE  VERIFY              TRANSLATE  VERIFIY
RATE      0.00    0.00     183.6   181.9       218.9   217.2       0.00       122.5    121.9
SIZE      0.00    0.00      8000    8000        8000    8000       0.00
```

Figure 6-9 Crypto hardware report

The report shows the display for one 5-minute interval. The top part shows that two PCIXCC cards are installed, numbered 0 and 5. This numbering is because the second card was installed after the first PCIXCC card (which gets number 0), and four PCICA cards (see Figure 6-2 on page 187).

In this example, card 0 averaged over 560 operations per second, with an average execution time of 1.8 milliseconds, and the card was utilized for 99.4% of the interval. Card 5 has similar figures.

The middle section, which reports PCICA figures is not shown here, as the jobs only exercised the PCIXCC cards.

The bottom part shows the execution rate on all PCIXCC cards by ICSF function. There are separate fields for single or triple encryption and decryption. Single or triple key length is not distinguished between for MAC operations. PIN operations do not have data sizes recorded as the PIN blocks sizes are fixed. You can see that the average block size is 8000 for those functions with variable block sizes, corresponding to the requests in our test jobs.

Note: We did not have the fix for APAR OA05379 available to us at this stage, so the DES encryption and decryption values are not reported correctly in the sample reports.

Graphing an Overview report of the each card's utilization shows how both cards were at nearly 100% utilization during the periods containing the test runs (Figure 6-10 on page 193).

Archived

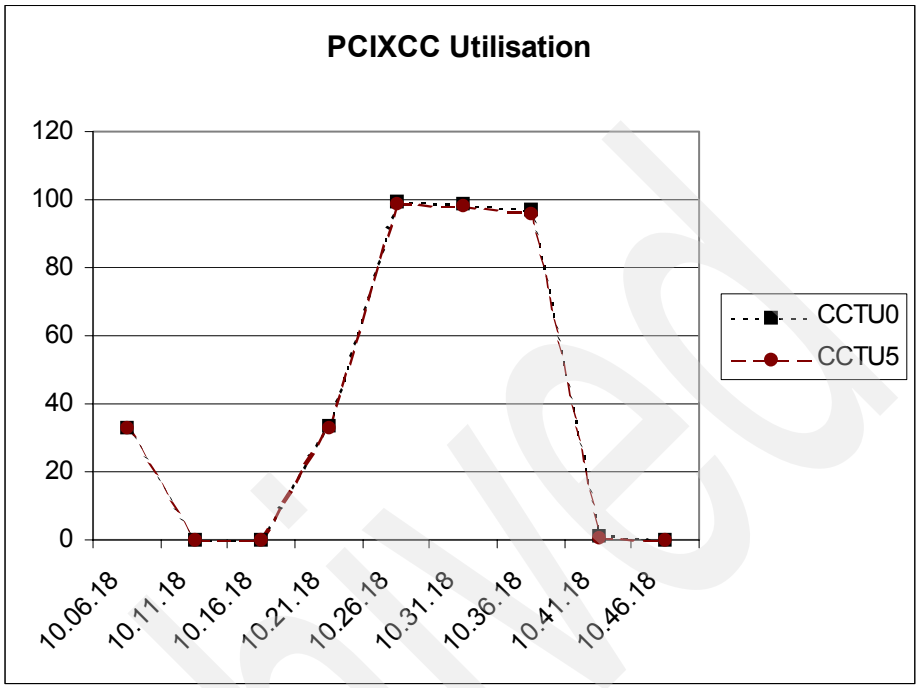

Figure 6-10 Overview Graph

Hashing functions

In the z990, only the SHA-1 hashing algorithm is counted in the HASH rate column, the other supported algorithms (MD5 and RIPEMD-160) are not. It should also be noted that on z990, SHA-1 is handled by CPACF, not PCIXCC.

6.2.2 ICSF SMF records

From z/OS 1.3 onwards, a sample job is supplied to format the ICSF type 82 SMF records, which gives a report of ICSF activity. The job is available in `SYS1.SAMPLIB(CSFSMFJ)`, which runs Rexx exec `SYS1.SAMPLIB(CSFSMFR)`. The JCL will need to be modified to fit your system standards. The modified version we used is shown in Figure 6-11 on page 194.

See *z/OS MVS System Management Facilities (SMF),* SA22-7630 or *z/OS ICSF System Programmer's Guide,* SA22-7520 for a fuller explanation of the data recorded in the SMF type 82 records.

Archived

```
//PK3ICSF JOB (),PS,CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
//*-------------------------------------------------------------------*
//*   UNLOAD SMF 82 RECORDS FROM VSAM TO VBS                          *
//*-------------------------------------------------------------------*
//SMFDMP   EXEC  PGM=IFASMFDP
//DUMPIN   DD    DISP=SHR,DSN=MVS.SMF.SAVE
//DUMPOUT  DD    DISP=(NEW,PASS),DSN=&&VBS,UNIT=3390,
//       SPACE=(CYL,(10,10)),DCB=(LRECL=32760,RECFM=VBS,BLKSIZE=4096)
//SYSPRINT DD    SYSOUT=*
//SYSIN    DD    *
    INDD(DUMPIN,OPTIONS(DUMP))
    OUTDD(DUMPOUT,TYPE(82))
//*
//*-------------------------------------------------------------------*
//*   COPY VBS TO SHORTER VB AND SORT ON DATE/TIME                    *
//*-------------------------------------------------------------------*
//COPYSORT EXEC PGM=SORT,REGION=6000K
//STEPLIB  DD DISP=SHR,DSN=SYS1.SORTLPA
//         DD DISP=SHR,DSN=SYS1.SICELINK
//SYSOUT   DD SYSOUT=*
//SORTWK01 DD UNIT=3390,SPACE=(CYL,10)
//SORTIN   DD DISP=(OLD,DELETE),DSN=&&VBS
//SORTOUT  DD    DISP=(NEW,PASS),DSN=&&VB,UNIT=3390,
//         SPACE=(CYL,(1,1)),DCB=(LRECL=3000,RECFM=VB)
//SYSIN    DD *
 SORT FIELDS=(11,4,A,7,4,A),FORMAT=BI,SIZE=E4000
//*
//*-------------------------------------------------------------------*
//*   FORMAT TYPE 82 RECORDS                                          *
//*-------------------------------------------------------------------*
//FMT     EXEC PGM=IKJEFT01,REGION=5128K,DYNAMNBR=100
//SYSPROC  DD DISP=SHR,DSN=SYS1.SAMPLIB
//SYSTSPRT DD SYSOUT=*
//INDD     DD DISP=(OLD,DELETE),DSN=&&VB
//OUTDD    DD SYSOUT=*
//SYSTSIN DD *
  %CSFSMFR
```

Figure 6-11 CSFSMFJ modified JCL

A portion of a report showing a processor being brought online and a processor timing record is shown in Figure 6-12 on page 195.

Archived

```
************************************************
Subtype=0012 Cryptographic Coprocessor Configuration
Written when a cryptographic coprocessor comes online or offline
24 Oct 2003 13:37:27.63
   TME... 004AD73B DTE... 0103297F SID... VSPK     SSI... 00000000 STY... 0012
   CGB... 80C00000 CGX... 00 CGS... 93000653
     CGB 80 coprocessor brought online
     CGB 00C0 Coprocessor is a PCIXCC
************************************************
Subtype=0013 PCI X Cryptographic Coprocessor Timing
Written periodically to provide some indication of PCIX Cryptographic Coprocessor usage
27 Oct 2003 19:05:22.35
   TME... 0068DCAB DTE... 010330OF SID... VSPK     SSI... 00000000 STY... 0013
   CTN... BA3BE739944EB6C8 CTD... BA3BE73995431D0C CTW... BA3BE73995442B08
   CTQ... 00000000 CTF... 4543 CTX... 05
   CTS... 93000871 CTM... 01 CTR... 01
```

Figure 6-12 Processor timing record report

The subtype 17 and 19 records have time stamps that can be used to give an indication of how a particular coprocessor is performing.

Using the timing records

By extracting the time stamps from the records, and calculating the elapsed time for the card activity and the time for the data to get the data back to the caller's address space, a picture can be drawn of how the cards have processed over time.

We extracted the following fields:

- CTN - the time stamp just before queueing the request to the coprocessor
- CTD - the time stamp just after dequeueing the result from the coprocessor
- CTW - the time stamp just after returning the result to the caller's address space

We then calculated the following values:

- (CTD-CTN) - this approximates to the response time from the card
- (CTW-CTD) - this approximates to the time taken to transfer the data back to the caller

Archived

Note: The time stamps are in 64-bit TOD clock format. A simple conversion of the time stamps from hexadecimal to decimal is allowed for normal arithmetic operations. The subtractions produced a number representing the number of clock “ticks” between the two events. According to *z/Architecture Principles of Operation,* SA22-7832, bit 51 of the TOD clock is changed every microsecond. By dividing the resulting numbers by 2^{13}, we end up with a number of microseconds. These can then be adjusted into fractions of a second.

We loaded the times produced into a spreadsheet, and graphed the results (Figure 6-13).

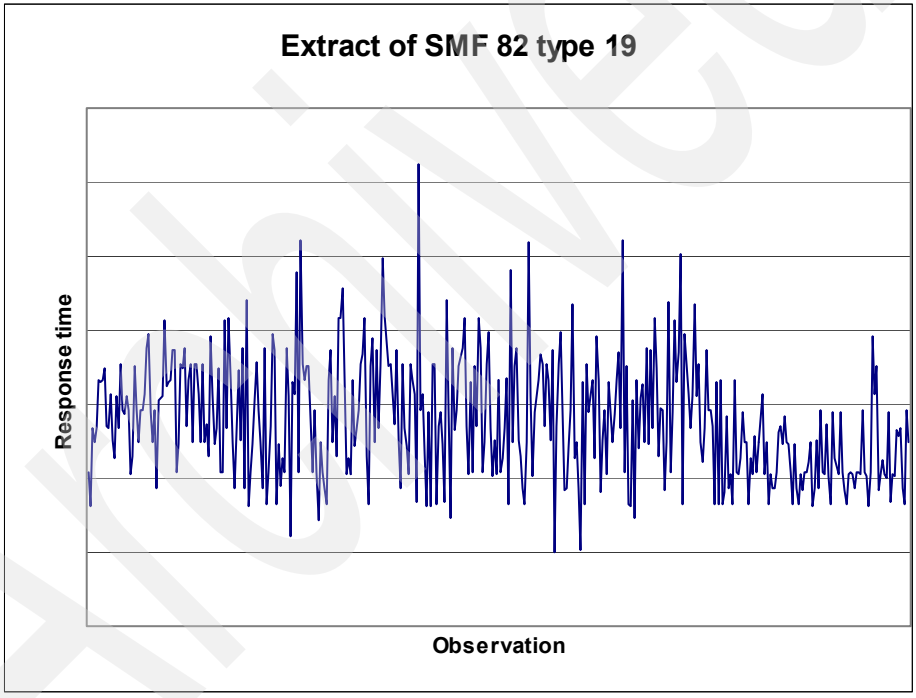

Figure 6-13 SMF 82 Extract graph

In this way, it is easier to spot trends. This graph is an extract of data produced during our test runs, and contains the card response time data from 400 SMF type 82 records produced over a period of 70 seconds. This shows that a lot of records can be produced when the cards are being heavily used, though the records themselves are quite small. The SMF records contain the card serial number, function code, etc., so further filtering is possible.

Archived

However, it is important to remember that these records are only periodic and not necessarily regular, so the records do not provide an accurate time series, and are only representative of the overall activity. They may be useful when trying to track delays, but this is not guaranteed.

Also, note that there are different function codes recorded in these records, each with different characteristics. As can seen from the graph, some of them have much longer elapsed times than others, in normal operation, so you need to ensure you are comparing the response times of the same functions. The amounts of data being processed per operation will also affect the elapsed times, but this is not recorded in the data.

In particular, since the RMF records are regularly spaced in time, unlike the ICSF records, correlating the two types of data will require some effort. One approach to correlate the data involves grouping the ICSF records into the same time intervals as reported in RMF, e.g. every 5 minutes, and averaging the response times by card and function. In this way the variable numbers of records produced can be reduced to fewer observations. Any intervals without records can be assigned zero values. This should then produce consolidated time-sequenced values, which can then be compared against RMF reports.

6.2.3 Example using RMF and SMF data

Here we describe how the different sources of data can be used to interpret the performance of PCIXCC, and to illustrate some of its characteristics, bearing in mind the descriptions of the effect of path length on performance.

We ran two sets of 10 test jobs, each using Triple DES encryption with different block sizes, in a tight loop. For the first run we used 800-byte blocks per encryption call, in the second we used 8000-byte blocks. The groups were run one after the other, with a gap of a few minutes. We graphed the reported transaction rate (Figure 6-14 on page 198) and percentage utilization (Figure 6-15 on page 198) from RMF, with a 5-minute reporting interval.

The first part of the data line in each of the following graphs covers the 800-byte test jobs, the second part covers the 8000-byte test jobs.

Archive

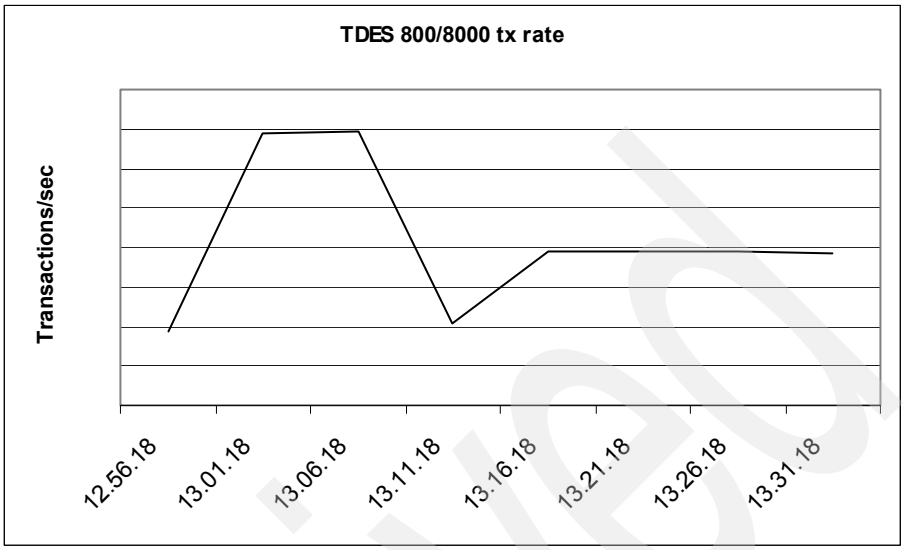

Figure 6-14 Transaction rate graph

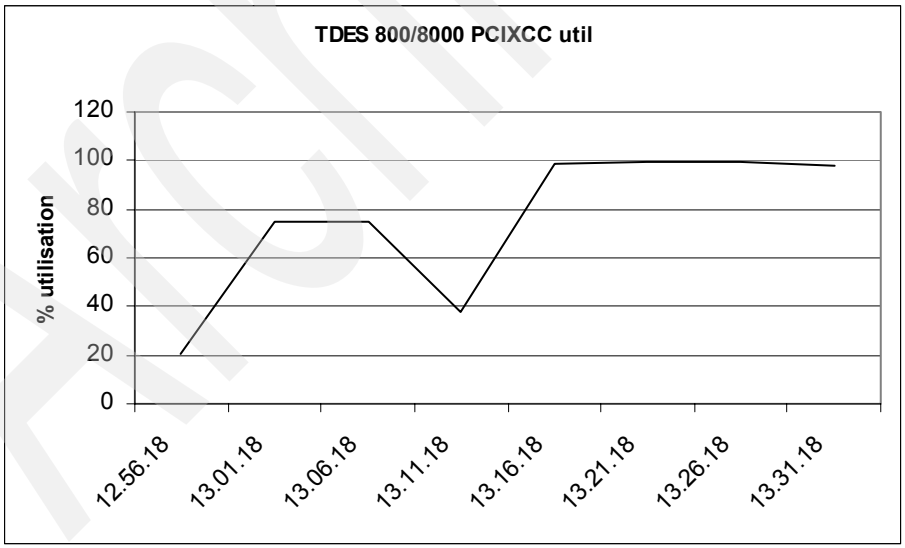

Figure 6-15 Percentage utilization graph

We extracted the ICSF SMF type 82 subtype 19 records, which record the card operation timing, as described above. The records were for both PCIXCC cards,

Archived

and all for the same function code, so that we could compare the times properly. We performed the calculations noted above to provide an elapsed time for each recorded operation. These times were then averaged over 1 second intervals (to provide a regular time sequence). We then plotted the results with further averaging to smooth the graph (Figure 6-16).

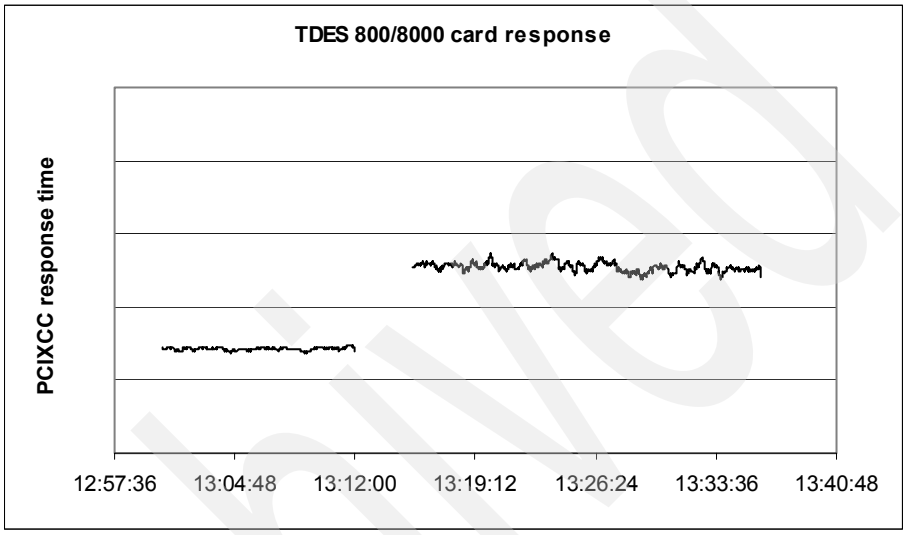

Figure 6-16 TDES graph

The data starts when the first jobs started running at 13:00, and continues until approximately 13:12, when the first tests completed. The second set started at 13:15 and completed around 13:36.

The differences in the time stamps between the RMF and the extracted SMF data are due to the different start times of the data. Further adjustments could be made to synchronize the graphs, if required.

The results show several things:

- A 10-fold increase in block size does not lead to a 10-fold increase in elapsed time, either per card operation or in job elapsed time. The increase is actually just less than double, in this case.
- With 800-byte blocks, we could get over 70% utilization, but with 8000-byte blocks, we could drive it to almost 100%.
- Card operation times are, on average, fairly constant over time, for a particular function and data length.

Archived

- The application design, illustrated in this case by the choice of data length, does affect the card response time, and therefore application performance.
- The ICSF SMF records are produced much more frequently than RMF records, when the PCIXCC cards are being used. They may show variations in the card performance that could be masked by RMF sampling. Note that the default RMF sampling rate of 1 second can be reduced to as little as 50 milliseconds, but this does not necessarily produce statistically more accurate data.
- ICSF SMF data is not produced when there are no ICSF calls being made.
- The ICSF SMF records can be processed to provide data that correlates with the RMF reports.

The ICSF SMF data reports are useful but should be used with care. The data is basically only a sample of the activity against the cards. They should be used in conjunction with:

- An understanding of the RMF reports for the same time intervals.
- The crypto hardware installed and the crypto functions they support.
- The applications using cryptographic functions, the functions and data sizes they use, and the hardware they exploit.

Archived

A

Exploiters

In this appendix we provide brief descriptions of the IBM software products that exploit z990 hardware cryptography.

Archived

© Copyright IBM Corp. 2004. All rights reserved.

A.1 The APIs

The main API to exploit the zSeries hardware cryptographic coprocessors is ICSF. ICSF dynamically routes the requests to either the CPACF, the PCICA, or the PCIXCC, transparently to the application.

Note that the CPACF can also be invoked directly from one application using non-privileged assembler instructions. See the zArchitecture Principle of Operations for the instructions Compute Intermediate Message Digest (KIMD), Compute Last Message Digest (KLMD), Cipher Message (KM), Cipher With Chaining (KMC), and Compute Message Authentication Code (KMAC). CPACF is also called by ICSF for the following services:

- MDC Generate (CSNBMDG,CSNBMDG1)
- One-Way Hash (CSNBOWH,CSNBOWH1) SHA-1
- Symmetric Key Decipher (CSNBSYD, CSNBSYD1) and Symmetric Key Encipher (CSNBSYE, CSNBSYE1)
  - Clear keys only
  - Single-, double- and triple-length keys
  - CBC, X9.23, CUSP, IPS, ECB processing
- Encode (CSNBECO) (DES, clear key)
- Decode (CSNBDCO) (DES, clear key)

Application designers cannot directly specify which coprocessor is to be used. ICSF makes the decision based on the required functions, which coprocessor type supports it, and performance considerations. As an example of the latter: If the function required is the CSNDPKE or CSNDPKD service (the SSL handshake assist) with a clear RSA private key, and if a PCICA is active in the system, then ICSF routes the request to a PCICA even though the PCIXCC can also provide the function.

The z/OS Base Cryptographic Services provide access to the hardware cryptographic coprocessors in the following three ways, as shown in Figure A-1 on page 205.

- ICSF is the most direct path for an application to get access to the coprocessors, by calling the ICSF IBM CCA services. ICSF also provides compatibility API for previous MVS-based cryptographic products:
  - The IBM Program Cryptographic Facility (PCF) API, which was a pure software cryptographic engine. In that case, the PCF functions are executed by the PCIXCC card.
  - The IBM 4753-Hardware Support Program (HSP), which also requires a PCIXCC card to be available to provide the IBM 4753 services.

Archived

The ICSF API is available to assembler programs and to high-level languages as well. Note that the ICSF API is also accessible to REXX programs using a link “stub.”

All z/OS components using hardware cryptography, if not going through System SSL or OCSF, are directly using the ICSF CCA API.

Note: although ICSF will only start if the hardware cryptography is enabled (FC 3863 on), some ICSF services are always provided by software. They are:

- One-Way Hash (CSNBOWH,CSNBOWH1)
- MD5
  - RIPEMD160
  - PKA Key Token Build (CSNDPKB)
- Code Conversion (CSNBXEA, CSNBXAE)
- Character/Nibble Conversion (CSNBXBC, CSNBXCB)
- X9.9 Data Editing (CSNB9ED)
- AES encryption or decryption, using clear key (CSNBSYD, CSNBSYE)

Attention: The following ICSF services that were provided using CCF and PCICC on other zSeries models are not available any more on z990:

- Support for DSA signatures and key generation
- Support for ANSI x9.17 services (offset and notarization), and associated key types
- Support for Ciphertext_translate(CSNBCTT)
- Support for German Bank Pool - Pin Offset
- Support for CSFUDK - use CSNBDKG instead
- Support for CDMF (40-bit encryption)

- Open Cryptographic Service Facilities (OCSF) is a z/OS implementation of the Intel® Common Data Security Architecture (CDSA) API. The intent of the CDSA API is mostly to provide the services required in a Public Key Infrastructure (PKI) environment. These services are actually provided by OCSF service providers’ plug-in modules.

  IBM delivers three OCSF cryptographic service providers in z/OS: the IBM Software Cryptographic Service Provider, the IBM Weak Software Provider (to satisfy requirements for shorter keys only, if any) and the IBM CCA Cryptographic Module. When the latter is invoked (“attached” in CDSA terminology) by the application, the following OCSF-provided functions actually call ICSF:

  – MD5 and SHA-1
  – Random number generation

- DES encryption and decryption
- RSA signature generation and verification
- RSA DES Key exchange using PKCS or ISO9796 format
- RSA Optimal Asymmetric Encryption Padding (OAEP)

OCSF is used today in z/OS by the LDAP server for encryption of the userPassword attribute in LDAP entries, and the IPSec VPN Internet Key Exchange (IKE) daemon.

Note: The use of the IBM Software Cryptographic Service Provider of OCSF may be subject to licensing by RSA Data Security Inc. if explicitly called by a commercial application. Refer to the note in *z/OS Open Cryptographic Services Facility Application Programming,* SC24-5899.

- System SSL is a set of dynamically loaded libraries that implement an API, to be used by a C/C++ application, which allows z/OS applications to initiate SSL/TLS communications over TCP/IP sockets. The application can use System SSL either on the SSL client side, or on the SSL server side. System SSL is exploited by many SSL-enabled servers and clients running on z/OS and is explained in further details below.
- A fourth way of accessing the ICSF services is by using the BSAFE Toolkit 3.1 (or later version/release). The BSAFE Toolkit is available from RSA Security Inc. on a license fee basis. It provides cryptographic services API which calls ICSF to do the following:

  - Compute message digests or hashes
  - Generate random numbers
  - Encipher and decipher data using the DES algorithm
  - Generate and verify RSA digital signatures

  The BSAFE ToolKit is accessed by the C application using the linkage stubs implemented at compilation and link-edit. The BSAFE ToolKit uses the BHAPI, proprietary to BSAFE, to interface with ICSF, as shown in Figure A-1 on page 205.

Archive

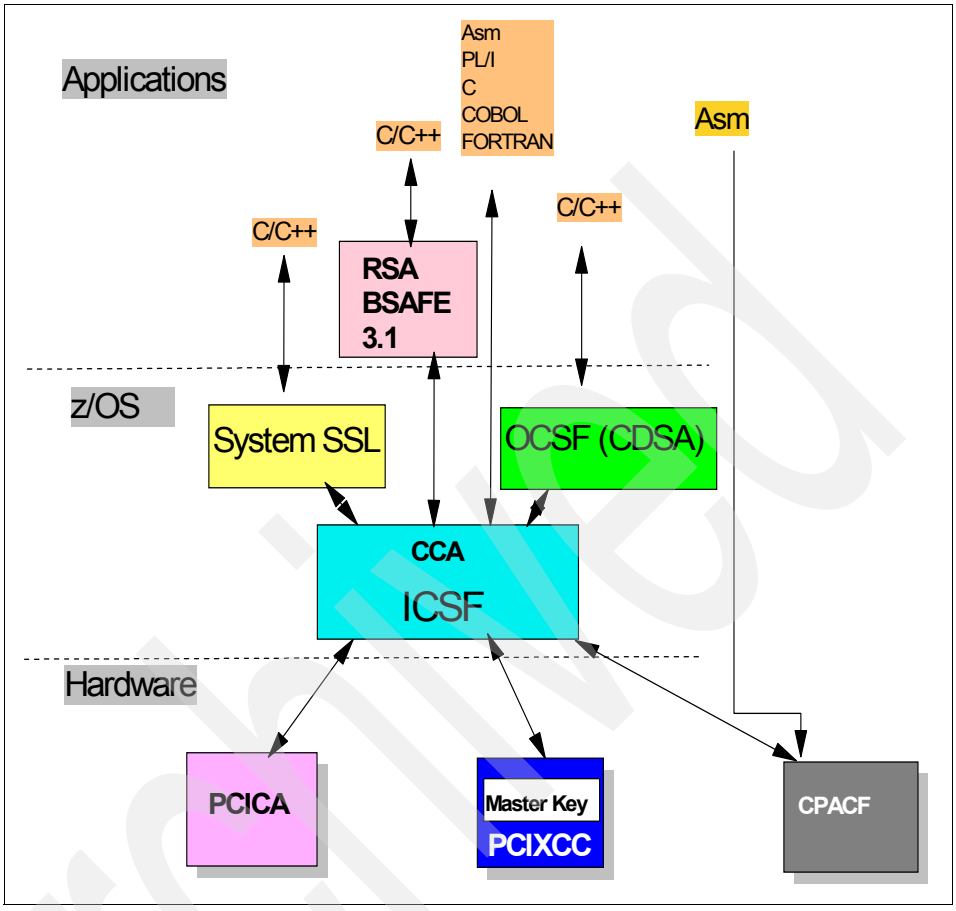

Figure A-1 Exploitation of the hardware coprocessors

Archived

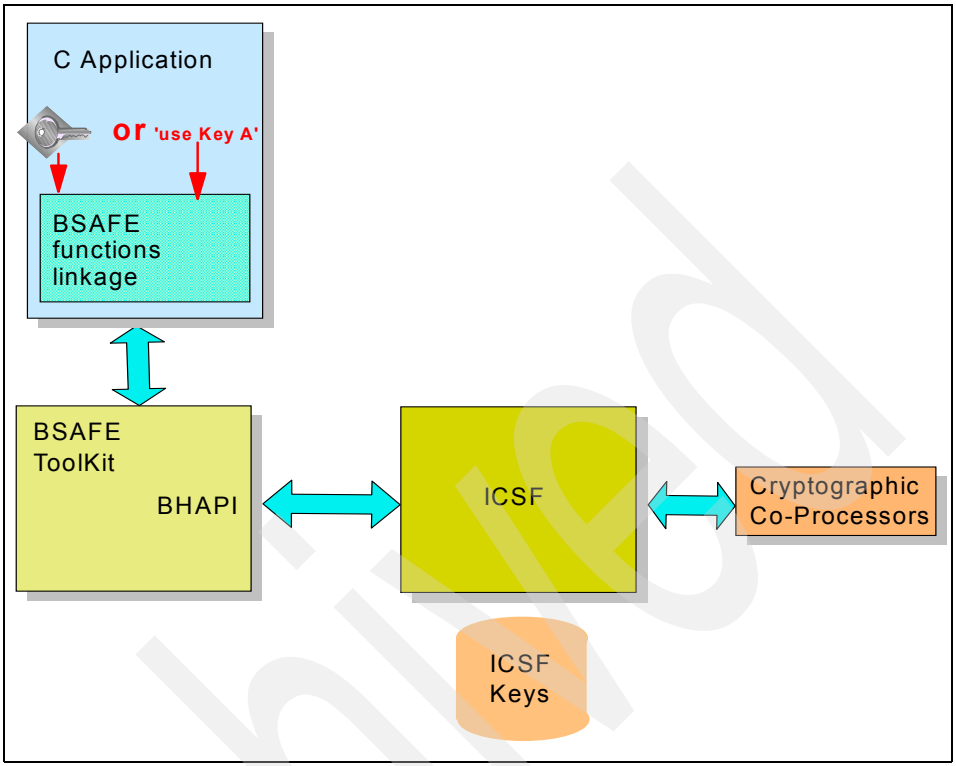

Figure A-2 z/OS BSafe implementation

A.2 Overview of the IBM exploiters

The following applications and programs are calling ICSF services that imply the use of operational keys encrypted under a Master Key or a Key-Encrypting-Key. Therefore, they require at least one PCIXCC to be in operation for the z/OS image.

- Access Method Services Cryptographic option
- CICS attachment facility
- CKDS Conversion program
- CSFEUTIL program for CKDS re-encipher, refresh, change master key, and pass phrase initialization functions
- CSFPUTIL program for PKDS activate, cache refresh, re-encipher, and initialization functions
- Distributed Key Management System (DKMS)
- Key Generation Utility Program (KGUP)
- PCF applications

- UDX (User Defined Extension) support
- VTAM® Session Level Encryption
- 4753-HSP applications

Applications that access ICSF services through the BSAFE interfaces

In this section, we briefly describe the IBM software products that exploit zSeries hardware cryptography. In all cases, these exploiters use their own software cryptographic services if ICSF is not active on the system, or if they need cryptographic functions/algorithms that are not supported by ICSF (except for VTAM, which *does* require a cryptographic facility, either software or hardware, to be available to provide session-level encryption).

Notes:

The use of key lengths longer than 64 bits is still controlled to the extent that a specific FMID must be ordered for the z/OS components intended to use keys above this value.

Which ICSF services are actually called by the exploiters may depend on the software release. If there is a need to precisely identify which services are called, our recommendation is to set up a "catch all" RACF profile in the CSFSERV class of profiles, defined in warning mode. All calls to ICSF services will be allowed, but also indicated by a RACF message on the system console.

Such a profile is defined with:

```
RDEF CSFSERV * UACC(NONE) WARNING
```

z/OS System SSL

Secure Network Layer (SSL) is a de facto standard developed by Netscape. It implements application-to-application security over TCP/IP networks by using both asymmetric and symmetric encryption, for authentication, data confidentiality, and integrity. SSL is being replaced by an IETF standardized protocol: Transaction Layer Security (TLS), which is described in RFC 2246. TLS-enabled servers and clients also support SSL. System SSL supports TLS beginning with z/OS 1.2.

System SSL, since its initial release in OS/390 2.7, went through some rewriting for functions and performance enhancements. Initially it was internally using a BSAFE software engine, which, in turn, was invoking ICSF for crypto-supported algorithms. In z/OS 1.4 System SSL has been rewritten to use its own IBM software cryptographic engine, which also invokes ICSF for hardware-supported

algorithms. This last change also had noticeable consequences on the performance of System SSL, as shown in Chapter 6, “Performance and monitoring” on page 183. If the algorithms to be used are supported by ICSF, System SSL checks the availability of the crypto hardware and drives the requests to ICSF. In the case when ICSF is not started or the proper coprocessor is not available, System SSL performs the cryptographic functions by software only.

Note that if a request to ICSF fails in z/OS 1.4, we observed that System SSL reverts “silently” to software cryptography. This can be seen in the System SSL trace.

Since OS/390 V2R10, all z/OS SSL-enabled servers and clients invoke the common System SSL DLLs provided in the base OS/390. Note that System SSL is usable both by SSL clients and servers running in OS/390.

Today, in z/OS V1R4, the SSL-enabled servers (which therefore use System SSL) are the following:

- IBM HTTP server
- CICS Transaction System and CICS Transaction Gateway
- TN3270 server
- FTP server and client
- LDAP server and client
- WebSphere Application Server
- WebSphere MQ

System SSL senses if CSF has been started in z/OS, and will use the hardware coprocessors for:

- Random number generation
- DES or Triple DES encryption and decryption, if DES or Triple DES are selected by the client and the server during the SSL handshake ciphersuites negotiation

  If RC2 or RC4 are selected, then System SSL performs encryption and decryption by software only.
- Encryption of the premaster secret at the SSL client, with the server’s public key
- Decryption of the premaster secret at the SSL server, with the server’s private key

System SSL comes with the GSKKYMAN utility for managing keys and certificates in HFS key databases. GSKKYMAN also calls for ICSF, if it has been started in the system.

Archived

The use of symmetric key lengths greater than 64 bits requires the installation of the System SSL Security Level 3 FMID.

Note that System SSL, when running on z990, uses the CPACF for symmetric encryption of data, if the negotiated algorithm is DES or T-DES and the key is in clear.

A.2.1 z/OS Open Cryptographic Services Facility (OCSF)

OCSF in z/OS comes with three cryptographic service providers (CSPs). There are two software CSPs, which differ in the maximum key strength allowed for various symmetric and asymmetric encryption algorithms. And there is one hardware CSP: the IBM CCA Cryptographic Module.

An application that invokes the hardware CSP gets the following cryptographic services from ICSF:

- Digest MD5 and SHA-1 generation
- Random number generation
- DES or triple DES encryption and decryption
- RSA digital signature generate and verify
- RSA key pair generation (when a PCICC is available in the system)
- DES key exchange using RSA encryption
- Data encryption/decryption using RSA Optimal Asymmetric Encryption Padding (OAEP) algorithm (part of Secure Electronic Transaction (SET) protocol)

The use of key lengths greater than 64 bits requires the installation of the OCSF Security Level 3 FMID.

A.2.2 IBM HTTP Server for z/OS

The IBM HTTP Server for z/OS requires cryptographic services when requested to engage an SSL communication. It uses the System SSL DLLs, and therefore ICSF (if started in the system), beginning with OS/390 V2R10. Previous to OS/390 V2R10, IHS was delivered with its own SSL code.

If you intend to use symmetric keys longer than 64 bits, the IHS North American Secure FMID must be installed.

Archive

A.2.3 z/OS LDAP server and client

The z/OS LDAP server or client requires cryptographic services when requested to engage an SSL communication. They use the System SSL DLLs, and therefore ICSF (if started in the system), beginning with OS/390 V2R7. Previous to OS/390 V2R7, the LDAP server and client were delivered with their own SSL code.

A.2.4 CICS Transaction Server and CICS Transaction Gateway

The CICS transaction Server and Transaction Gateway require cryptographic services for their optional SSL communications.

- CICS Transaction Server is SSL-enabled at TS 1.3 and above. It uses the System SSL API.
- CICS Transaction Gateway calls the System SSL API, starting with Version 3. Previous to Version 3 it used its own, software-only, cryptographic services.

A.2.5 z/OS TN3270 server

The z/OS TN3270 server requires cryptographic services when requested to engage an SSL communication. It uses the System SSL DLLs, and therefore ICSF (if started in the system), beginning with OS/390 V2R10. Previous to OS/390 V2R10, the TN3270 server was delivered with its own SSL code.

A.2.6 z/OS Firewall Technologies

Three components of the z/OS Firewall Technologies use cryptographic services:

- IPSEC “tunnels,” which call ICSF (if active on the system) for DES or triple-DES encryption and decryption

  These calls are actually issued by the z/OS TCP/IP code. The Communications Server Security Level 3 FMID is required if triple-DES is to be used.

> **Note:** The service names that z/OS Firewall Technologies uses are CSFCKI (Clear key Import), CSFDEC1 (Decypher), CSFENC1 (Encypher), CSFRNG (Random Number generation), CSFCKM (Multiple Key Import), and CSFOWH1 (One Way Hash Generate). Note that if triple-DES hardware crypto support is not available on your S/390 processor, the CSFCKM service is not used.

Archived

- The Firewall Technologies Configuration Server, which communicates with an optional GUI client workstation

  The server and the client communicate using SSL and the server piece, on z/OS, uses System SSL.

- The Internet Security Association Key Management Protocol (ISAKMP) daemon

  This daemon, in OS/390 2.8 and later, is used to dynamically establish IPSEC tunnels secret keys, using the Internet Key Exchange (IKE) protocol. The two parties involved in an IKE negotiation can identify themselves, and initiate secure communications, using a digital certificate and asymmetric and symmetric algorithms. The z/OS ISAKMP daemon calls OCSF for the related cryptographic services.

A.2.7 GSKKYMAN

GSKKYMAN invokes miscellaneous ICSF services, such as CSFDSV (digital signature verify), CSFPKI (PKA Key Import), CSFCKI (Clear key Import).

A.2.8 z/OS DCE

z/OS DCE calls ICSF (if active on the system) for DES encryption or decryption, provided that the message length is greater than 60 bytes.

A.2.9 z/OS Network Authentication Service (Kerberos)

z/OS NAS issues calls to ICSF for DES and triple-DES encryption/decryption beginning with z/OS V1R2. The use of triple-DES requires the installation of the Security Server Network Authentication Service Level 3 FMID.

A.2.10 Payment processing products

The IBM Payment Gateway™ for OS/390 and WebSphere Payment Manager support the use of either the SSL or SET protocol for secure transaction.

- When using SSL, the Payment Gateway calls System SSL for the required cryptographic services, whereas the Payment Manager uses its own (Java) SSL code.
- When using SET, the Payment Gateway detects the presence of an active ICSF instance that it will invoke for the following:
  - RSA digital signature generation and verification
  - Random number generation
  - DES encryption and decryption

Archived

– OAEP block compose and decompose

The WebSphere Payment Manager or Payment Gateway utilization of hardware cryptography for the SET protocol is left to the user to decide, via a parameter in the SET configuration table (Payment Manager) or an environment variable (Payment Gateway).

Note that for the Payment Gateway, hardware cryptography support is required to get the SET gateway certification from the major card associations (Visa and MasterCard).

A.2.11 VTAM Session Level Encryption

VTAM provides Session Level Encryption if a cryptographic product is available on the system; that is, VTAM does *not* provide its own cryptographic software. Historically, the Programmed Cryptographic Facility (PCF) software product provided the cryptographic services to VTAM before the availability of ICSF.

A.2.12 RACF

Two components of RACF indirectly invoke external cryptographic services:

- The Open Cryptography Enhanced Plug-in (OCEP) is an OCSF Trust Policy and Data Library plug-in that allows you to work with the keys and certificates in the RACF Data Base. As such, it can request for OCSF cryptographic services.
- The RACDCERT RACF command permits you to generate RSA key pairs, using PCICC with z/OS V1R4, and to optionally store the private key into the PKDS, which is encrypted under the asymmetric Master Key. It also calls ICSF for certificate signature if the private key is stored in the PKDS.

A.2.13 z/OS Public Key Infrastructure (PKI) services

This z/OS Security Server component provides all the services expected from a PKI-compliant Certification Authority, beginning with z/OS V1R3. It uses ICSF through the RACF RACDCERT command.

A.2.14 Crypto Based Transactions (CBT) banking solution

CBT is an IBM-specific solution to provide end-to-end security for transactions occurring between a client on the Internet and a z/OS transaction running as a batch or CICS program. It provides data confidentiality, integrity and non-repudiation. CBT on the z/OS end uses the Crypto Server Module (CSM) API, which relies on zSeries hardware cryptography.

A.2.15 Java cryptography

The Java 2 platform-independent cryptography API is provided in the Java Cryptographic Extension (JCE) classes. As of IBM SDK 1.3.1, a new set of JCE classes known as IBMJCE4758 classes are an IBM implementation of JCE that invoke ICSF for the following cryptographic services:

- DES and triple-DES encryption and decryption
- MD2, MD5, and SHA1 hashing
- RSA signature generation and verification
- DSA signature generation and verification

Archived

Archived

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information on ordering these publications, see “How to get IBM Redbooks” on page 216. Note that some of the documents referenced here may be available in softcopy only.

- *zSeries Crypto Guide Update,* SG24-6870

Other publications

These publications are also relevant as further information sources:

- *ICSF TKE Workstation User’s Guide,* SA22-7524-05
- *PR/SM Planning Guide,* SB10-7036
- *Security Server (RACF) Security Administrator’s Guide,* SC28-1915
- *z/OS RMF User’s Guide,* SC33-7990
- *z/OS RMF Report Analysis,* SC33-7991
- *z/OS MVS System Management Facilities (SMF),* SA22-7630
- *z/OS ICSF System Programmer’s Guide,* SA22-7520
- *z/Architecture Principles of Operation,* SA22-7832
- *Maintenance Information for Desktop Consoles,* GC38-3115

Online resources

These Web sites and URLs are also relevant as further information sources:

- UDX Web site

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

Archived

© Copyright IBM Corp. 2004. All rights reserved.

- Update of ICSF support for both secure keys and clear keys using the CP Assist for Cryptographic Functions (CPACF), PCICA and the PCIXCC adapters

  `http://www.ibm.com/eserver/zseries/zos/downloads`

- IBM Techdocs - Technical Sales Library Web site

  `http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/Techdocs`

- More useful Techdocs

  `http://www.ibm.com/support/techdocs/astmastr.nsf/Webindex/WP100345`

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Archived

Index

A
Adjunct Processor 22, 24
  AP ID 22
  management 37
Adjunct Processor (AP) 24
Advanced Facilities 57
AES 2
AES support 170
asymmetric-keys 172
Asymmetric-keys Master Key 172
ASYM-MK 172

B
BSAFE
  Toolkit 204

C
C/C++ client 204
CCF 18, 22
  notebook 103
CEC 22
CHPIDs 9
CICS Transaction Server and Gateway 210
CKDS 12
  ICSF 12
CMOS 22
Control domain index 154
CP Assist for Cryptographic Function (CPACF) 4
CPC 21, 149, 156–157
crypto assist enablement 51
Crypto Hardware Activity report 186
Crypto Node Management (CNM) 66
Crypto page 151
Crypto report
  Workload activity report 187
Crypto reports
  Crypto Hardware acivity report 186
Cryptographic Asynchronous Function 2
Cryptographic Coprocessor Feature (CCF) 5
cryptographic function support 2
cryptographic processors 4
Cryptographic Synchronous Function 2
Cryptography hardware implementation on z800 22
CSM (Crypto Server Module) 212

D
Data Encryption Standard (DES) 2
DCE 211
dedicated central processors 151
DES key 172
double length-key DES 2

E
ENCIPHER DES and PKA key storage 80
ESCON 21

F
FCV
  overview 162
feature code 48–49
FICON 21
Function Control Vector 49

G
generating spreadsheets 190
GSKKYMAN 208

H
hardware 49
hardware status display 174
hashing functions 193
HSA 38

I
IBM 4758 26, 57
IBM 4758 CCA application 40
IBM 4758-2 cryptographic coprocessor 24
IBM HTTP Server for z/OS 209
IBM Vital Product Data (VPD) database 46
ICSF
  changes from previous release 170
  CKDS 12

© Copyright IBM Corp. 2004. All rights reserved.

PCICC Management panel 56
PKDS 12
setup 170
SMF records 193
software 22
TSO panels 170
IFL (Integrated Facility for Linux) 24
IKE (Internet Key Exchange) protocol 211
Image Profile 151
IML 39
Initial Master Key entry with the pass phrase initialization utility 172
Integrated Cryptographic Service Facility 6
IOCDS 56
IPSEC 211

J

Java Cryptographic Extension (JCE) classes 213
Java Cryptography 213
JCE classes 213

K

KIMD - Compute Intermediate Message Digest 4
KLMD - Compute Last Message Digest 4
KM - Cipher Message 4
KMAC - Compute Message Authentic Code 4
KMC - Cipher message with chaining 4

L

LDAP server 24
Linux 15
LPAR 145
LPAR Cryptographic Controls 156

M

master key entry 5
master keys 171
MES upgrade 57

N

NOPASSWORD 171

O

OCSF 211
Open Cryptography Enhanced Plug-in (OCEP) 212
OS/390 V2R9 23
OSA-Express 10, 21

P

PCHID type 24
PCHIDs 9
PCI Crypto Accelerator card 31
PCI Cryptographic card
security issues 167
PCI Cryptographic Online List 155
PCICA 9
data flow 31
feature code 47
PCICA feature
PCHID 19
PCICC 23, 145
data flow 25
PCI-CC and PCI-CA viewing status 28
PCIX Cryptographic Coprocessor 5
PCIXCC
card 26
physical security, handling, and shipping 32
Co-Sign page 140
create a PCIXCC new authority 120
data flow 25
data flow chart 26
Delete Authority 122
Domain Keys page 124
enablement 157
feature code 47
feature installation 157
Generate PCIXCC signature keys 118
initialization 38
microcode load 40
microcode patches 42
modules notebook 103
removal 56
roles 100
setup on the TKE workstation 86
zeroize 167
PCIXCC card 24
PCIXCC feature 5, 8, 24
PCHID 19
PCXICC card
physical security 32
Peripheral Component Interconnect extended Cryptographic Coprocessor (PCIXCC) 18
PKDS 12
ICSF 12

Archived

PKDS initialization 178
Power On 39
Power-On Reset (POR) 39
PPINIT 173
PR/SM 148
Public Key Algorithm 3

R

Redbooks Web site 216
  Contact us xi
REENCIPHER. 80
RMF
  overview reports 188
RMF examples using test jobs 191
RMF Processor Activity 185
RMF Workload Activity and Storage Data) 185
RSA 3, 41
  Optimal Asymmetric Encryption Padding (OAEP) 209

S

SE 39
Secure Sockets Layer (SSL) 2
Self-Timed Interface 21
SHA-1 22
single-signature commands 110
SMF data 185
SSL
  SSL clients 208
  SSL DLLs 208
STI and PCHID
  plugging rules 21
STI controller card 26
STI-M cards 21
Support Element 38, 148
symmetric-keys 172
symmetric-keys Master Key 171

T

TCP/IP 42
  host for the TKE 154
TKE 17, 145
  access control administration 74
  application start 81
  Authority signature key indicator 85
  customize TKE.INI parameters 80
  definitions 66
  Host system S/390 definition and logon from TKE 89
  Introduction to the TKE V3.1 workstation 60
  Loading the first part of the TKE Master Key 78
  logon 86
  major changes 60
  Master Key 64, 68
  Master Key load 78
  OS/2 desktop 68
  PROFILE 67
  ROLE 66
  starting the application 81
  V3.1 software 65
  Workstation access control 66
  Workstation initialization 73
  Workstation installation 65
  Workstation key storage 68
  workstation setup for PCIXCC 86
  Workstation TCP/IP setup 68
TKE Host Transaction Program 61
TKE V4.0 Workstation 42, 60
TKEUSER role 76
TKEUSERs profiles 62
T-Rex processor 22
Triple length- key DES 2
Trusted Key Entry 5
Trusted Key Entry Version 65
TSO 42

U

UDX 3, 41
  status 163
usage domain index 153
User Defined Extensions 41

V

VTAM 207

W

WebSphere Payment Manager 212
Workload Activity report 187

Z

z/OS
  Firewall Technologies 210
  ISAKMP 211
  Network Authentication Service (Kerberos) 211

Archived

Open Cryptographic Services Facility 209
TN3270 Server 210
V1.4
z990 compatibility support 42
z800 23
z990 1
crypto hardware performance 184
Cryptographic CP assist support for z/OS V1.3 42
hardware needed 46
I/O cage
PCIXCC 21
server 10
z990 Cryptographic Support 3
zeroizing the PCIXCC 167
zSeries 22
zSeries z990 46

Archived

REDBOOKS

(0.2”spine)
0.17”<->0.473”
90<->249 pages

Archived

Archived

IBM @server zSeries 990 (z990) Cryptography Implementation

PCIXCC and PCICA installation and customization

Overview of CPACF

Review of TKE V4

The IBM z990 includes both standard cryptographic hardware and optional cryptographic features, to give flexibility and growth capability. IBM has a long history of providing hardware cryptographic solutions, from the development of Data Encryption Standard (DES) in the 1970s to delivering the only integrated cryptographic hardware in a server to achieve the US Government's highest FIPS 140-2 Level 4 rating for secure cryptographic hardware.

This IBM Redbook is designed to help you understand and implement the z/OS Cryptographic PCIXCC and PCICA cards. Although this book focuses on the enablement of the z/OS PCIXCC and PCICA products, cryptography and the available services on z/OS are also discussed and explained, with special attention given to the new Trusted Key Entry (TKE V4) workstation.

This book also reviews the tools that are available on z/OS for the monitoring of z990 cryptographic hardware utilization, plus the analysis of performance.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-7070-00 ISBN 0738490369