IBM Washington Systems Center
Advanced Technical Support

RDS Training
Hardware Overview

zSeries Security
Advanced Technical Support
Gaithersburg, MD

ON DEMAND BUSINESS™

August 5, 2005

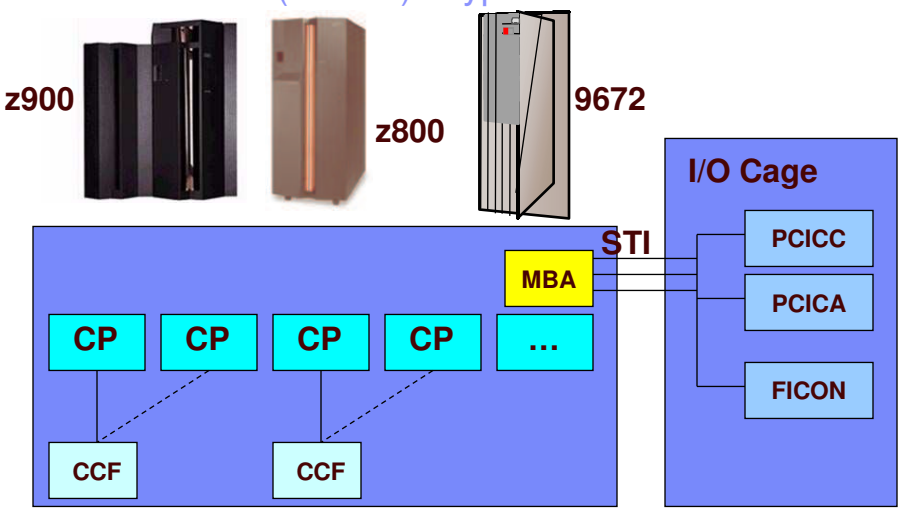
IBM Cryptographic Hardware – z800/z900 and earlier

Crypto Coprocessor Facility (CCF) $e_{mk}(k)$

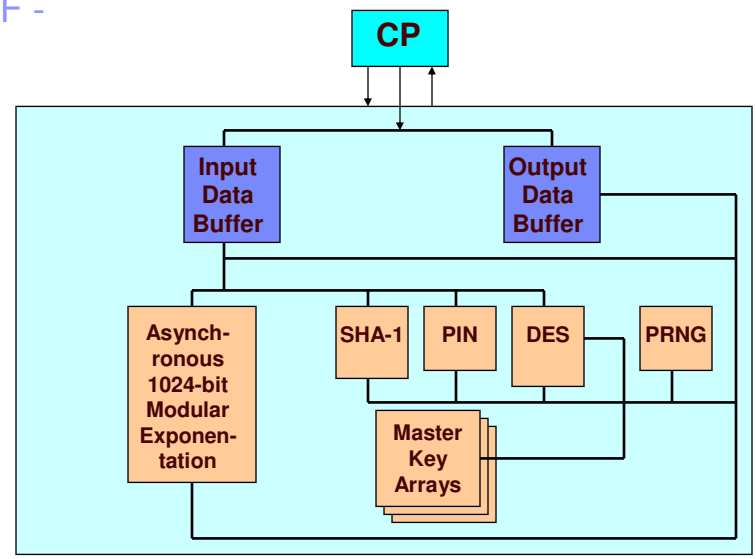
PCI Crypto Coprocessor (PCICC) $e_{mk}(k)$

PCI Crypto Accelerator (PCICA)

Z800/z900/9672 (CMOS) Crypto HW

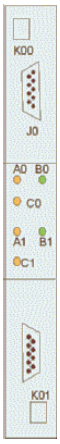


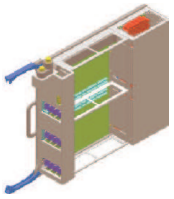
CCF -



PCI Cards (General)

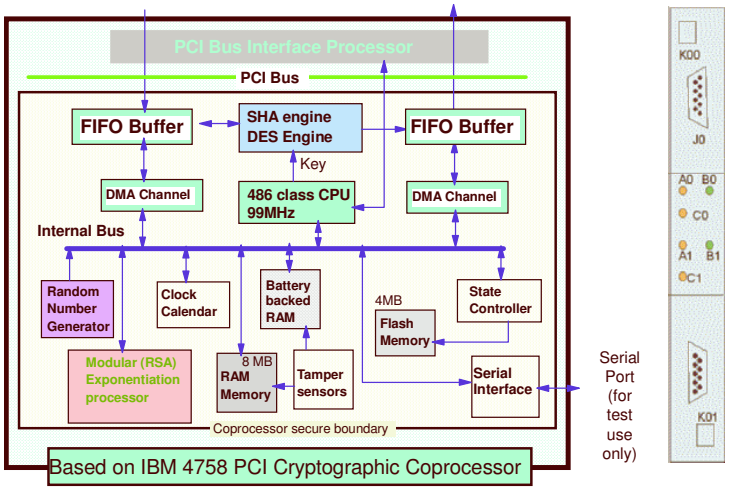
- **Feature – Packaged as a book**
- **May consist of a single- or dual-card**





- **Card may also be referred to as a port**
- **On 9672, z900/z800 a book is associated with a CHPID**
- **On a z890/z990 a book is associated with a PCHPID**

PCICC

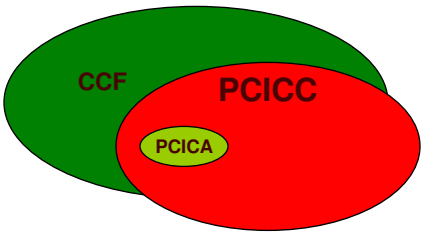


Original Chart provided courtesy of ITSO.

PCICA

- **It does one thing, and one thing only, but it does it very fast**
  - CSNDPKD – Public Key Decrypt API
    - Decrypt of the Pre-Master Secret

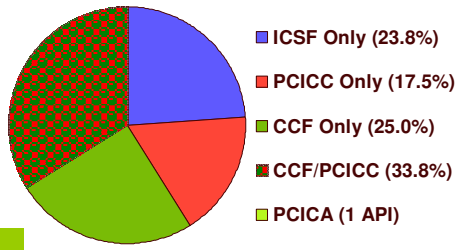
APIs on CCF/PCICC/PCICA



On a CCF Only system, 66 APIs are available

With a CCF & PCICC, 80 APIs are available

PCICA supports only 1 API



zSeries Cryptographic Hardware – z890/z990

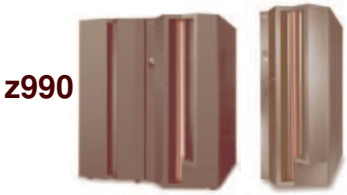
CP Assist for Crypto Functions (CPACF)

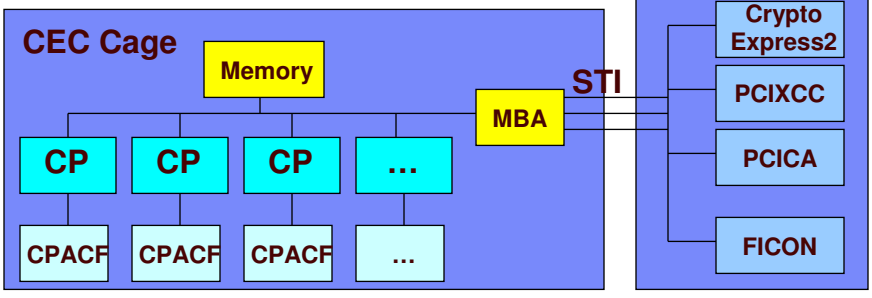
Crypto Express2 $e_{mk}(k)$

PCI Crypto Accelerator (PCICA)

PCI X Crypto Coprocessor (PCIXCC) $e_{mk}(k)$

Z890/z990 Crypto HW



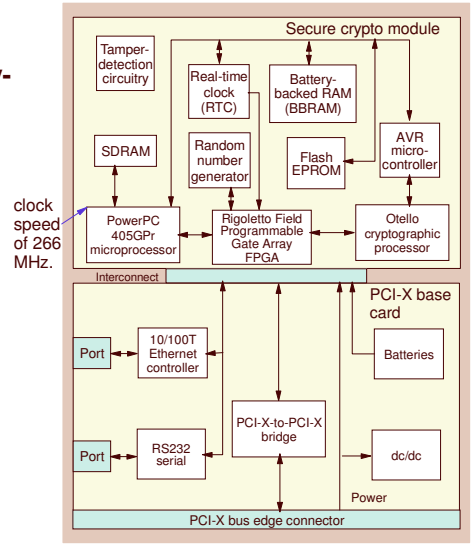


PCICA

- **It does three things, and only three things, but it does them very fast**
  - CSNDPKD – Public Key Decrypt API
    - Decrypt of the Pre-Master Secret
  - CSNDPKE – Public Key Encrypt API
    - Encrypt of the Pre-Master Secret
  - CSNDDSV – Digital Signature Verify API
    - Verifies a Digital Signature

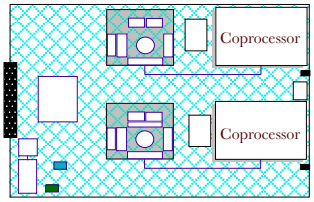
PCIXCC

Adapter card with all security-related components encased in a tamper responding security module

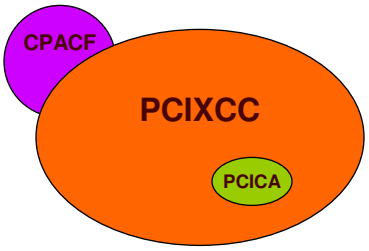


Crypto Express2

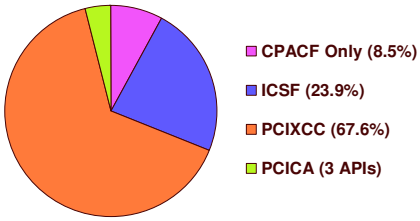
- **Combines functionality of PCIXCC and PCICA into a single feature**



APIs on CPACF, PCIXCC, PCICA



In a CPACF only system, there are 14 APIs available (6 are routed to the CPACF, and 8 to ICSF)



With a PCIXCC, 71 APIs are available

PCICA supports 3 APIs

zSeries Cryptographic Hardware – z9 109

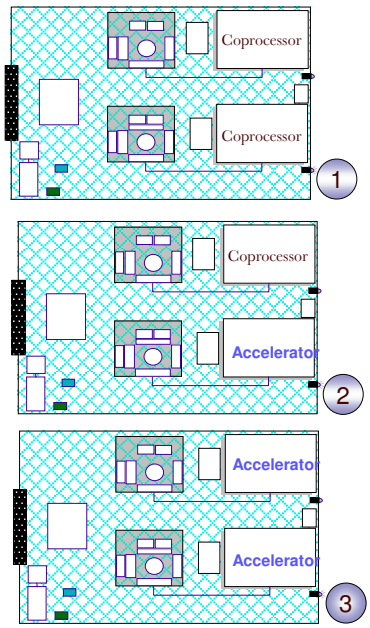
CP Assist for Crypto Functions (CPACF)

Crypto Express2 $e_{mk}(k)$

Z9 109 Crypto Express2 Configuration

- **Secure Coprocessor** (default)
  - Provides both Secure key" and "Public key" functionality and performance equivalent to Crypto Express2 features on z990
  - "Secure key" improved performance compared to PCIXCC on z990 (requires multitasking)
  - "Public key" equivalent performance to PCICA on z990
  - No action required
- **Accelerator**
  - Provides only "Public key" functionality with enhanced performance
  - Must be configured using the HMC

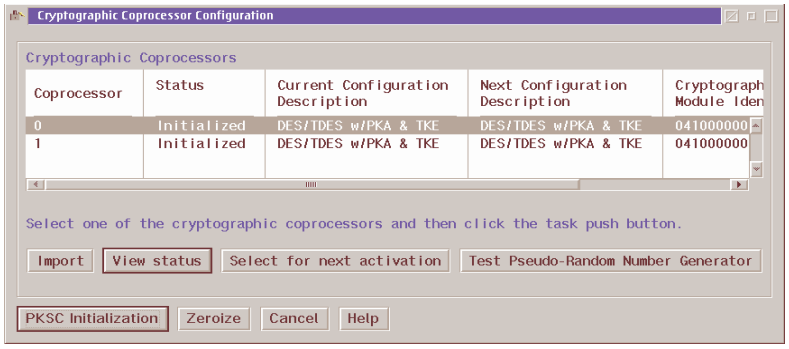
NEW!



Enablement Diskettes

- **CCF**
  - Shipped Inactive, must be enabled
  - Config file unique to each CCF
  - Config files are loaded into the CCF
- **PCICC**
  - Single config file loaded into HSA and shared among PCICCs
- **CPACF**
  - Secure Hash Algorithms available without Microcode load
  - DES/TDES/AES requires Microcode load

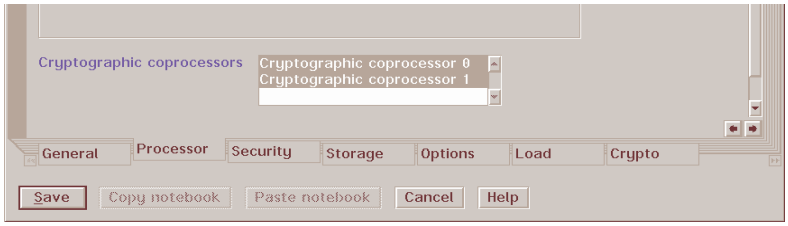
Z900 SE CCF Config



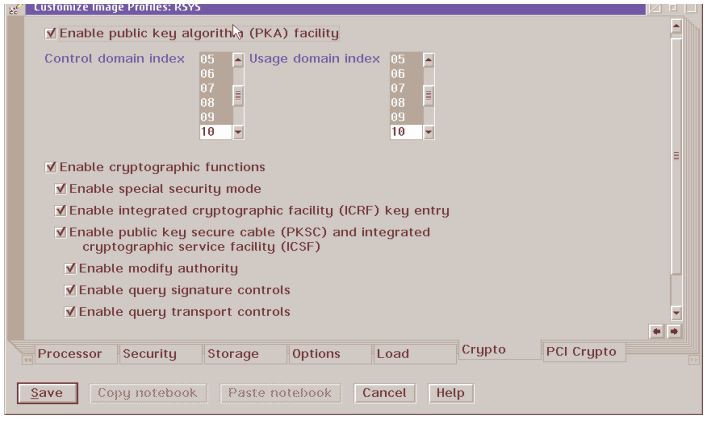
SE z/900 PCI Cards

Processor Tab for ROSP6 (Top)

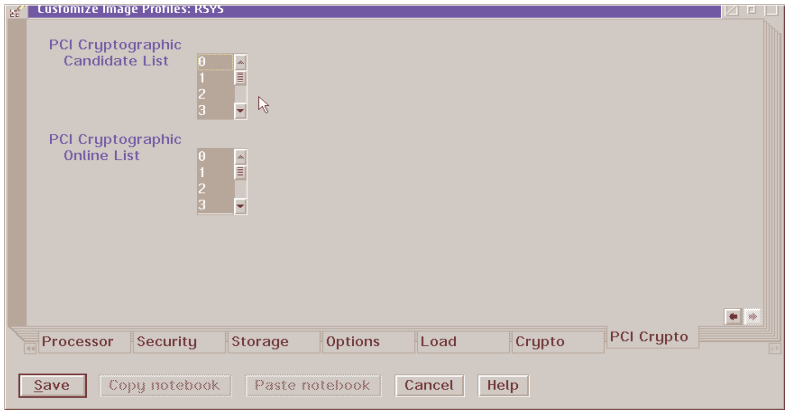
Processor Tab for ROSP6 (Bottom)



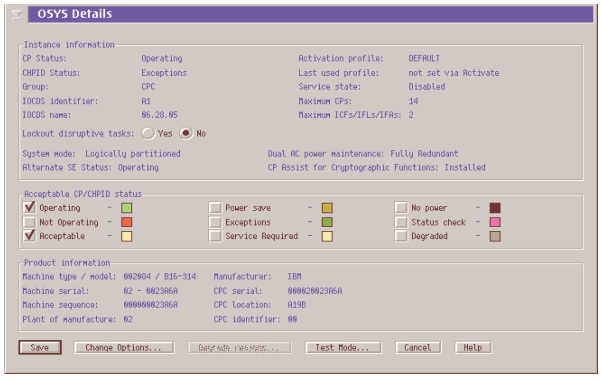
Crypto Tab for ROSP6



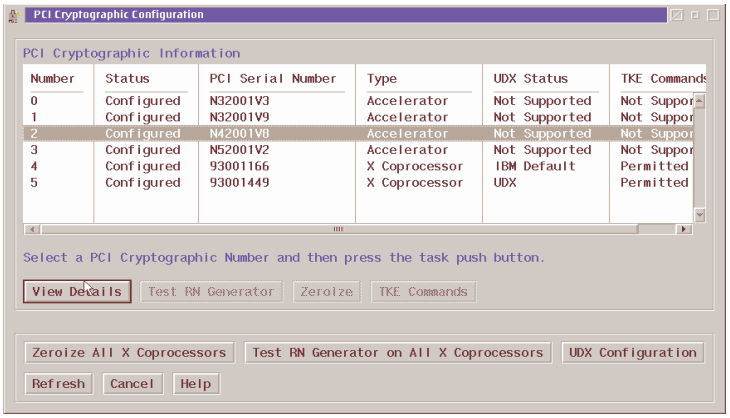
PCI Crypto Tab for ROSP6



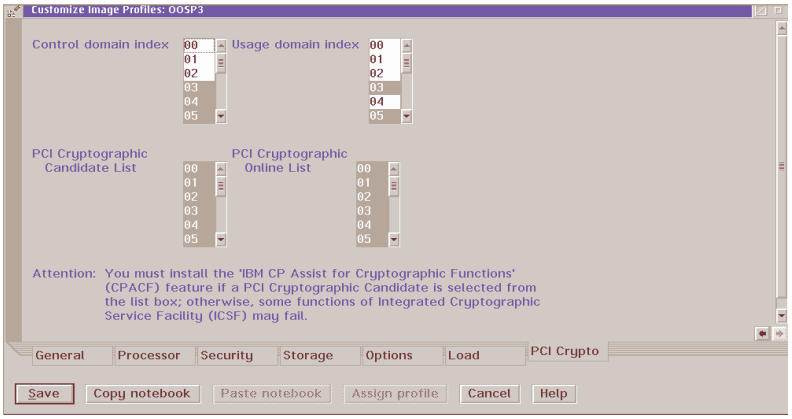
SE z990 OSYS Details



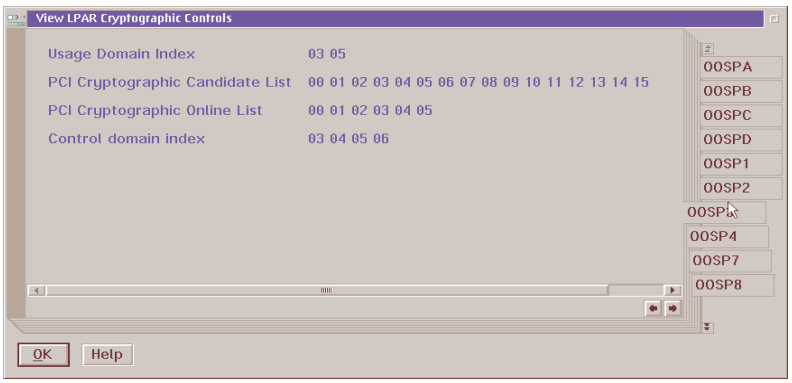
SE z990 PCI Cards



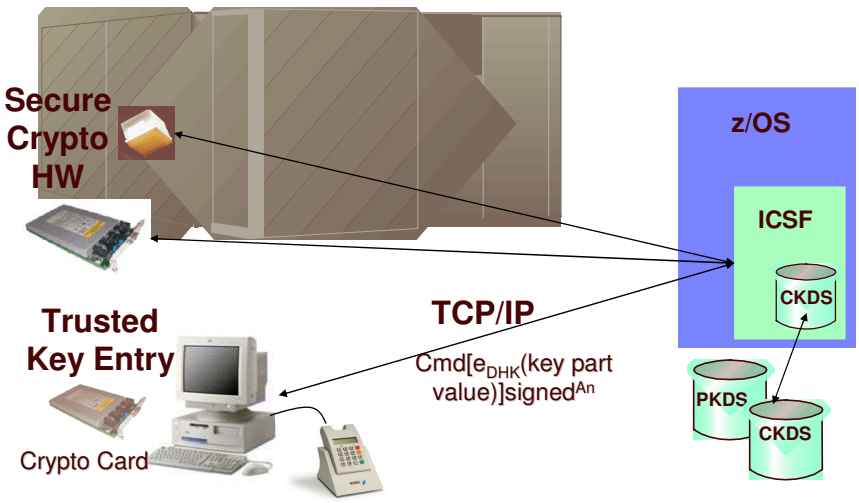
OOSP3 Image – PCICrypto Tab



Crypto Defined to LPAR OOSP3 on z990



TKE – Trusted Key Entry Workstation



Questions?

Trademarks