z/OS V1R9 Integrated Cryptographic Service Facility (ICSF) Update

Session 05

Prepared by Patrick Kappeler
IBM Consulting IT Specialist
kappeler@fr.ibm.com

Redbooks
International Technical Support Organization

Trademarks

See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.
UNIX is a registered trademark of The Open Group in the United States and other countries.
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the 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.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Acronyms

AES	Advanced Encryption Standard
ARL	Authority Revocation List
CA	Certification Authority
CBC	Cipher Block Chaining
CCA	IBM Common Cryptographic Architecture
CCF	Cryptographic Coprocessor Facility
CDSA	Common Data Security Architecture
CEX2A	Crypto Express 2 Accelerator
CEX2C	Crypto Express 2 Coprocessor
CFB	Cipher FeedBack
CKDS	Cryptographic Key Data Set
CRL	Certificate Revocation List
CRT	Chinese Remainder Theorem
CVC	Card Verification Code
CVV	Card Verification Value
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECB	Electronic Code Book
FIPS	Federal Information Processing Standards
GSS	Generalized Security Services
ICSF	Integrated Cryptographic Service Facility
IETF	Internet Engineering Task Force
IPKI	Internet Public Key Infrastructure
KGUP	Key Generation Utility Program
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MDC	Message Detection Code
MD5	Message Digest 5
OAEP	Optimal Asymmetric Encryption Padding
OCSF	OS/390 Open Cryptographic Services Facility
OCSP	Online Certificate Status Protocol
PCICA	PCI Cryptographic Accelerator
PCICC	PCI Cryptographic Coprocessor
PCIXCC	PCIX Cryptographic Coprocessor
PKA	Public Key Architecture
PKCS	Public Key Cryptographic Standards
PKDS	Public Key Data Set
PKI	Public Key Infrastructure
RA	Registration Authority
RACF	Resource Access Control Facility
RSA	Rivest-Shamir-Adleman
SET	Secure Electronic Transaction
SHA-1	Secure Hash Algorithm 1
SLE	Session Level Encryption
SSL	Secure Sockets Layer
TKE	Trusted Key Entry
TLS	Transport Layer Security
VPN	Virtual Private Network

Agenda

- Cryptography as of Today – A Refresher
  - Why Cryptography ? The Algorithms, the Engines, why Hardware Cryptography
- Hardware Cryptography and the IBM Mainframe
  - System z9 Hardware Cryptography
  - System z Operating Systems hardware Cryptography Infrastructure
- Hardware Cryptography and z/OS
  - ICSF
  - Examples of Hardware Cryptography Exploitation
  - Hardware Cryptography Performance
- Introduction to PKCS#11 support at z/OS V1R9

Cryptography As of Today

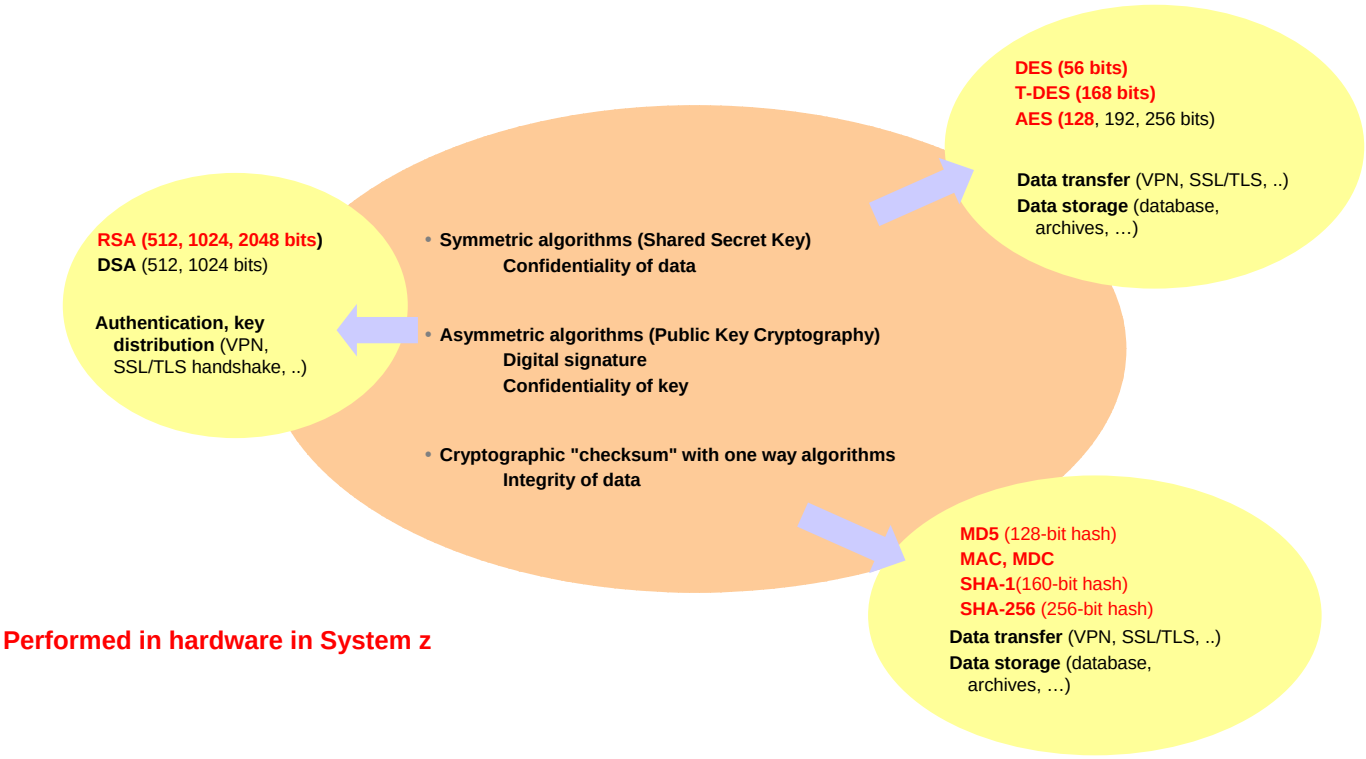
A Refresher

Why Cryptography ?

- Traditionally: to hide the meaning of transferred or stored data, but also used to establish:
  - data integrity
  - Authentication
- A required facility today for personal or industrial computing

- Hardware Cryptography
  - Offload cryptographic computation workload
    - Some algorithms consumes huge amounts of MIPS
  - Increased performance
    - Speed of computation by specialized coprocessors
  - Security
    - Always more secure than a software implementation
    - Can implement very sophisticated protection of secrets, depending on device

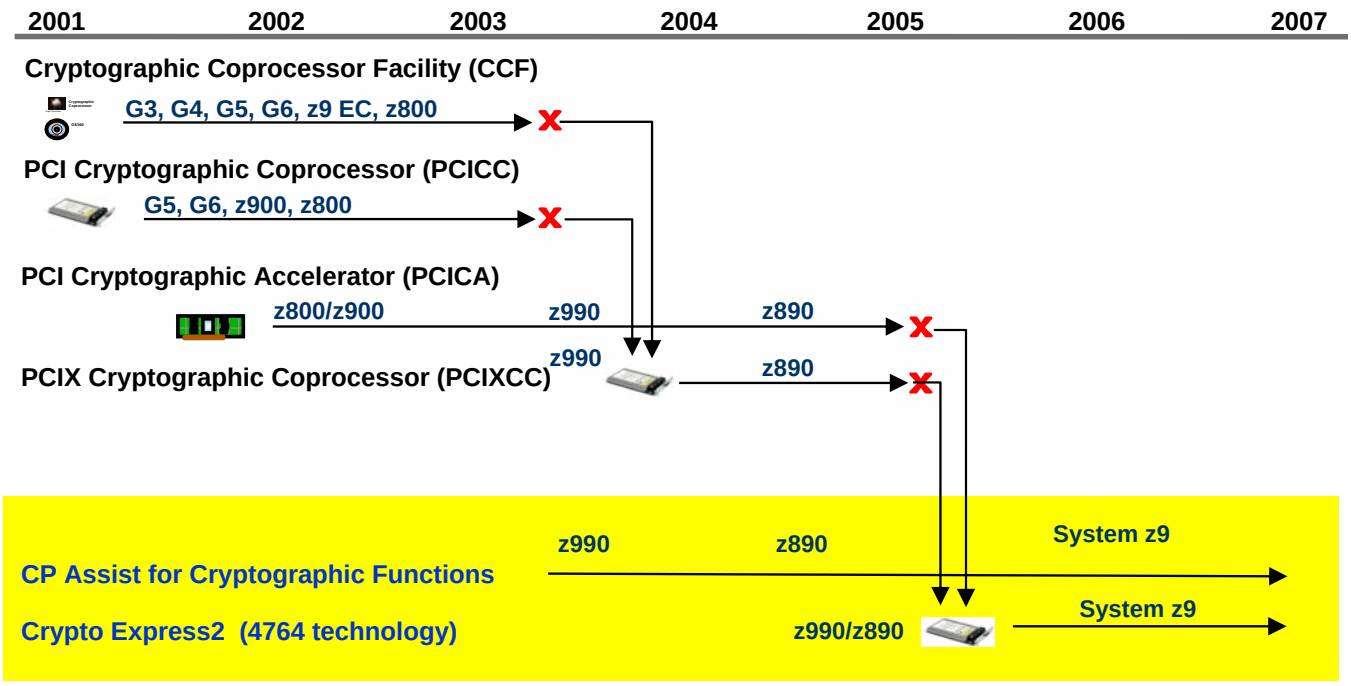
Cryptographic Algorithms And Their Use



Performed in hardware in System z

Mainframe Hardware Cryptography

System z9 And zSeries Crypto Roadmap



The 4764-001 Cryptographic Coprocessor (PCIXCC)

- Hardware device pluggable on PCI-X bus - ("PCIXCC")
- Secure coprocessor - Certified at FIPS 140-2 level 4
- Available across all IBM platforms
  - System p (FC 4764),
  - System i (FC 4806)
  - System x: 4764-001 card
  - System z : Crypto Express 2 Coprocessor (FC 0868/0870)
- Provides the IBM CCA (Common Cryptographic Architecture) services and API
- Can host specific user algorithms as User Defined Extensions (UDX)

IBM Systems Journal paper at
http://domino.research.ibm.com/tchjr/journalindex.nsf/a3807c5b4823c53f85256561006324be/fc9c727abee8d3f985256eb500713360?OpenDocument

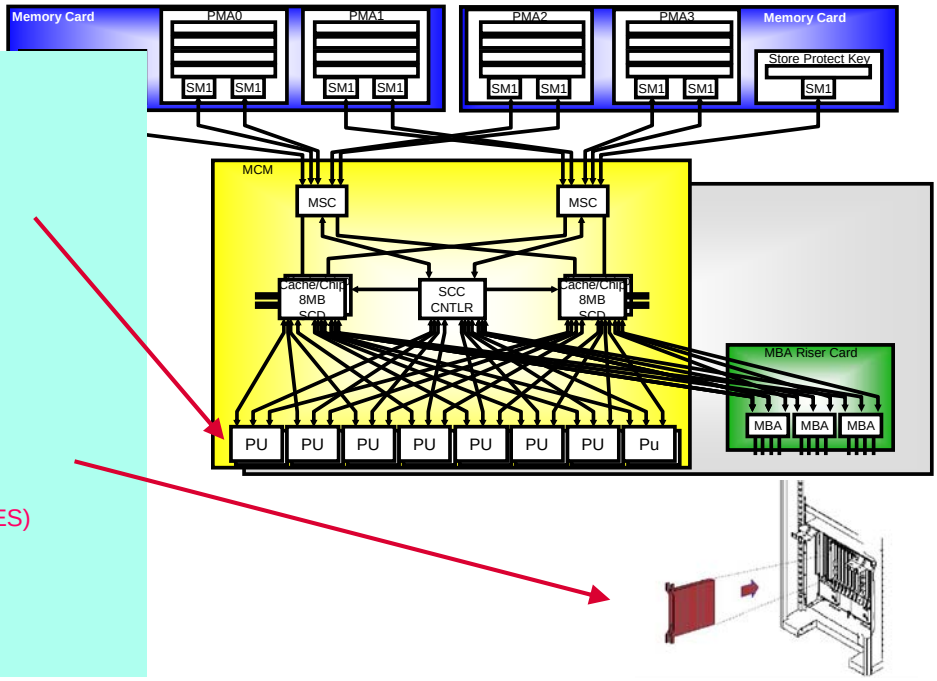
System z9 Hardware Cryptography Implementation

CP Assist for Cryptographic Functions (CPACF)

- A facility integrated in each PU
- standard orderable feature
- non-secure (clear keys only) symmetric, hash, …

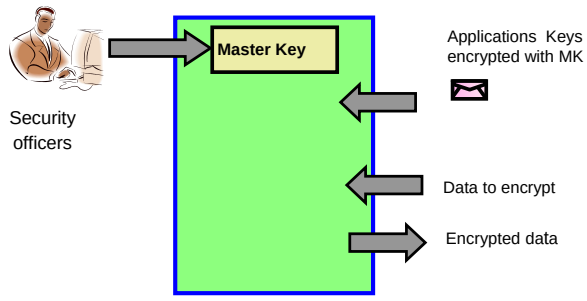
Crypto Express 2 (CEX2C)

- Priced feature
- 0 to 8 features in a system
- 2 secure 4764 coprocessors per feature
- Secure keys symmetric (DES, T-DES) and asymmetric (RSA)
- PR/SM sharable
- Manually configurable into an RSA accelerator (CEX2A)



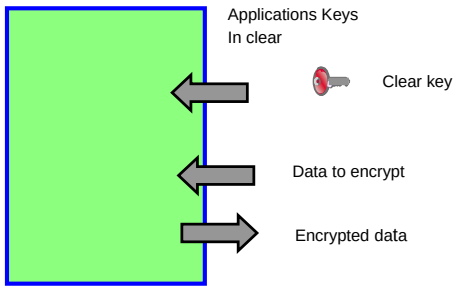
Secure And Non-Secure Coprocessors

secure coprocessor (e.g. CEX2C)



+ Master Key zeroization in case of tampering attempt

non-secure coprocessor or 'accelerator (e.g. CPACF, CEX2A)



Risks vs simplicity and performance

FIPS 140-2 Certification (4 levels)

http://csrc.nist.gov/cryptval/140-1/1401val2006.htm look for certificate #661

The CP Assist For Cryptographic Functions (CPACF)

Implementation of the IBM Message Security Architecture (MSA) Instructions

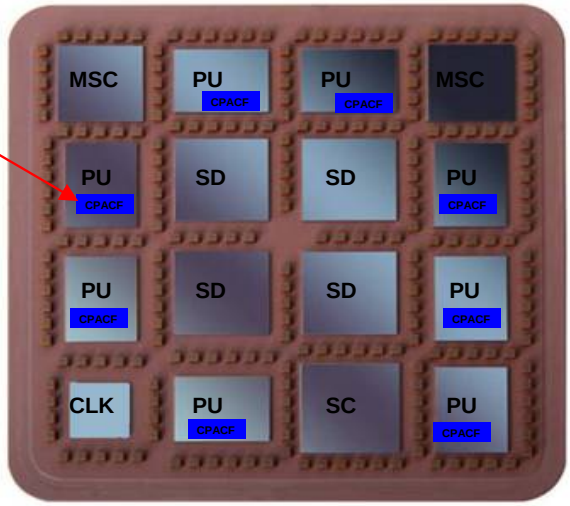
(refer to z/Architecture Principles Of Operation SA22-7832)

Clear key
- DES, T-DES
- AES128

- SHA-1
- SHA-256
- PRNG

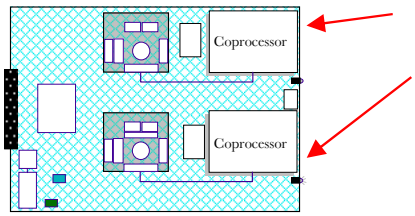
Available on

- CP
- IFL
- zAAP
- zIIP



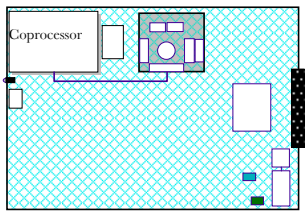
Enablement with FC 3863

The Crypto Express 2



System z9 EC, z9 BC

PCIXCC (4764-001) Card in coprocessor or accelerator mode

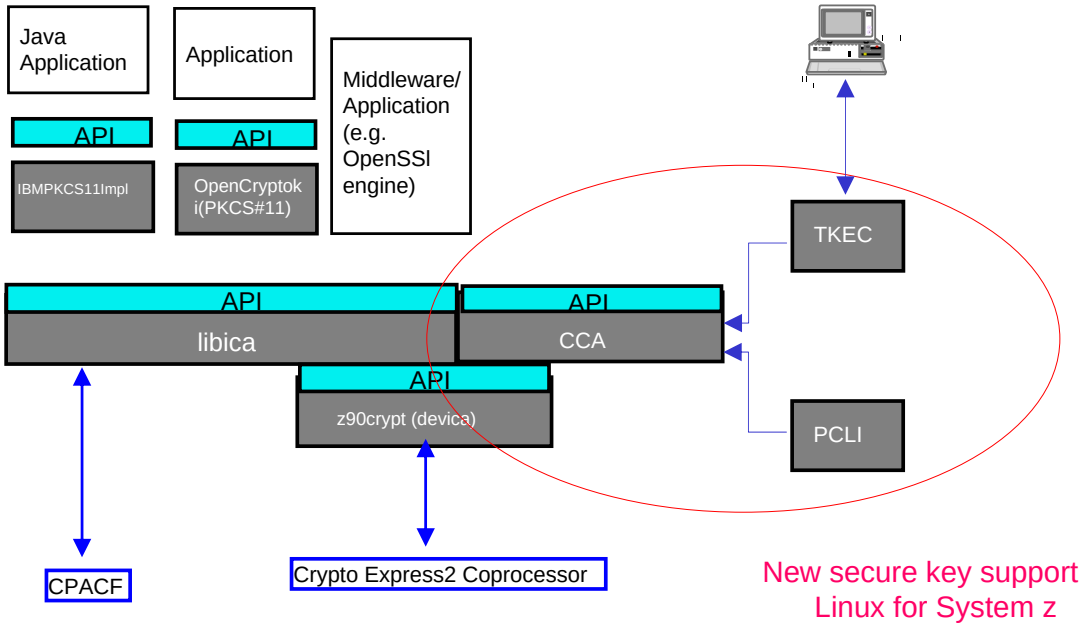


System z9 BC only (2007)

- "4764" (PCIXCC) based technology
- Provides **secure key** functions (FIPS 140-2 Level 4 certified)
  - **Symmetric** DES, T-DES encryption/decryption
  - Message authentication, hashing
  - PIN processing
  - **RSA asymmetric** encryption/decryption and digital signature generation/verification
  - Key generation and management, random number generation
  - EMV support
  - 4753 support
  - **User Defined Extension** (UDX) – Built under contract by IBM or 3rd party approved vendor
- Provides clear key RSA functions for **SSL/TLS acceleration**

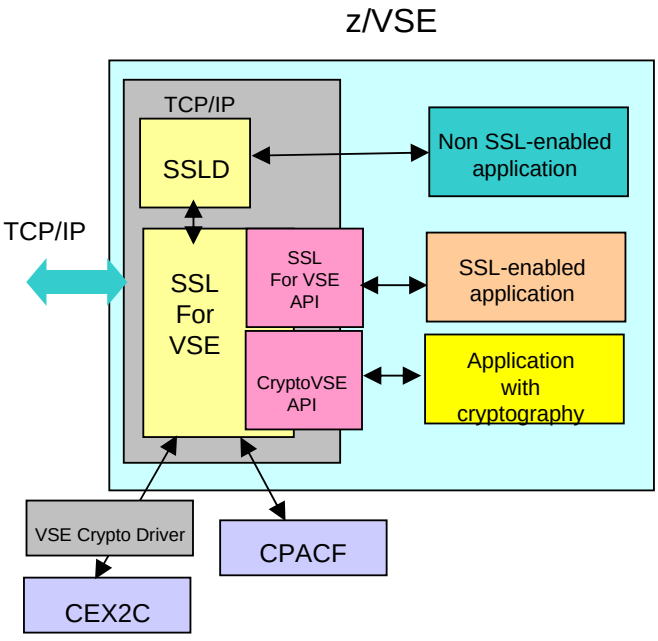
Enablement with FC 3863

Linux For System z Crypto Infrastructure



New secure key support in Linux for System z

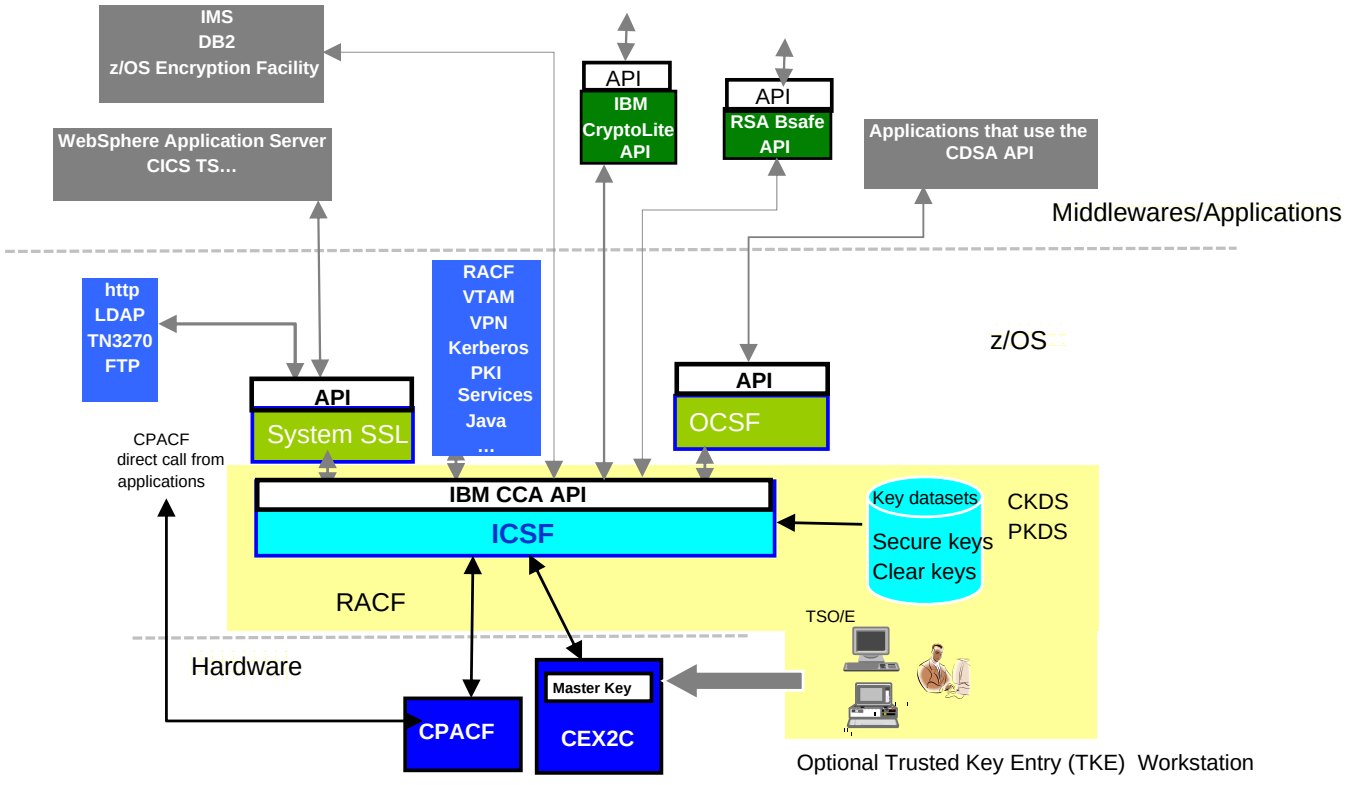
z/VSE Crypto Infrastructure



Clear RSA key only

Focusing on Hardware Cryptography And z/OS

An Example Of Crypto Infrastructure – z/OS V1R8



ICSF Releases

SMP/E installable
downloadable FMID
(z/OS V1R6 and above)

HCR7730 – support for z9 New CPACF functions
support for clear AES key token
support for z9 CEX2A
CKDS Sysplex support

SMP/E installable
downloadable FMID
(z/OS V1R6 and above)
In z/OS V1R8
Cryptographic Services

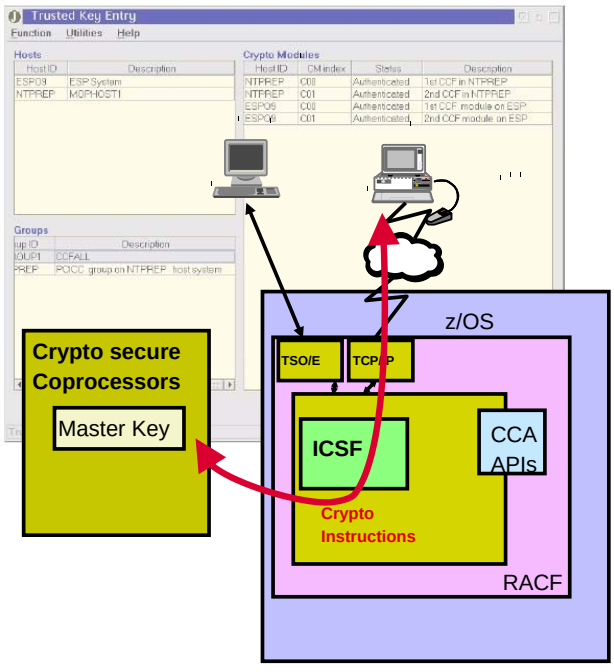
HCR7731 – HCR7730 +
PKDS Key management
new Remote Key Loading service API
updated API for ISO 16609 CBC Mode TDES

In z/OS V1R9
Cryptographic Services

HCR7740 – HCR7731
+ PKCS#11 Support new callable services
+ CFB, PKCS#7 padding

http://www-1.ibm.com/servers/eserver/zseries/zos/downloads

The Trusted Key Entry Workstation



Priced optional feature - A highly secure alternative to TSO/E for the management of secure coprocessors Master Keys and operational keys

Encrypted and signed communications over TCP/IP
- •Listener in ICSF
- •End point is the coprocessor

Increased security for
- •Access to secure cryptographic coprocessors
- •Authorities (security officers) identified by their password and digital signature
- •Option to require multiple signatures before performing a crypto function
- •smart card support

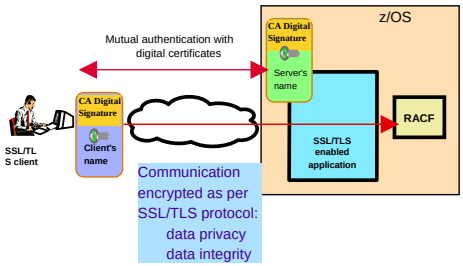
Coprocessors can be administered as groups

Can be used on Linux with secure keys

z/OS Exploitation Of Hardware Crypto - Examples

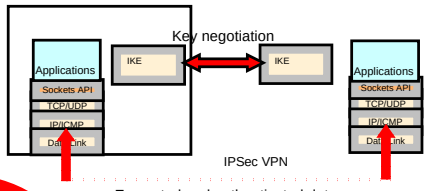
SSL/TLS

- z/OS System SSL provides the API to applications
- z/OS System SSL calls
  - CEX2C for handshake (RSA) – via ICSF
  - CPACF for data transfer (DES or T-DES) - direct call via instructions

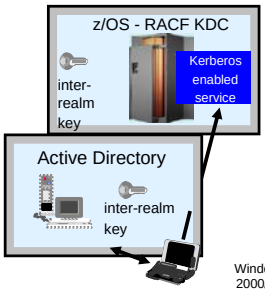


z/OS Communications Server – IPSec VPNs

- CEX2C for Key Server authentication via ICSF
- CPACF for DES or T-DES data encryption via ICSF



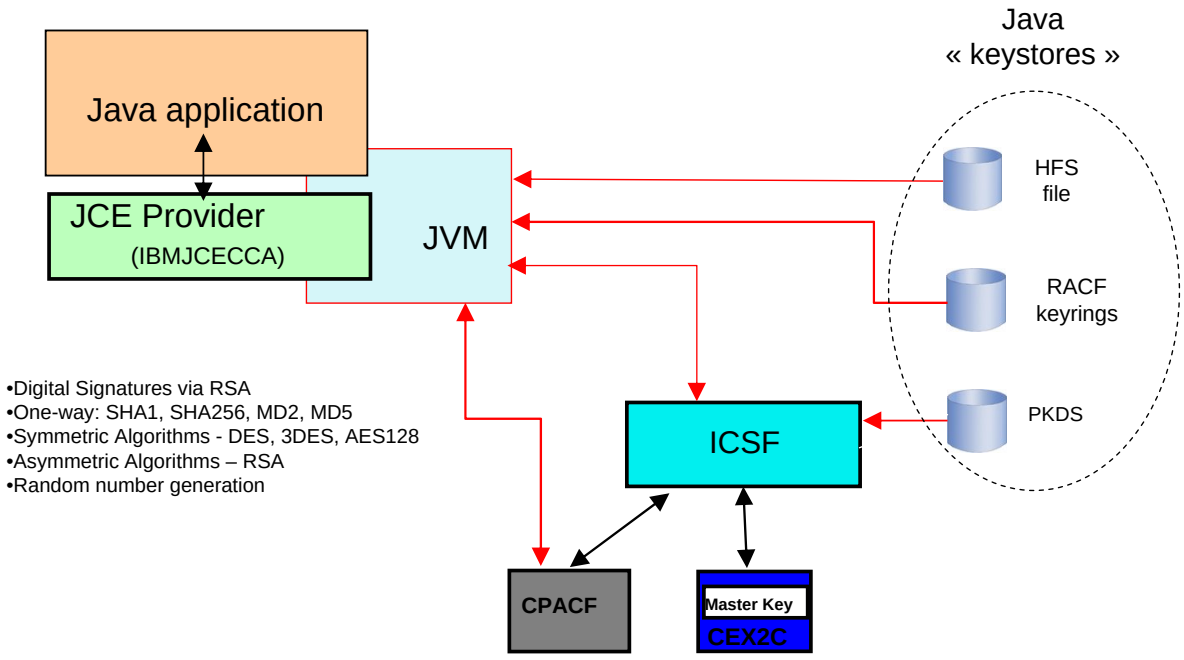
See Session 10



Kerberos (z/OS Network Authentication Service)

- CEX2C for DES or T-DES authentication and data encryption via ICSF

z/OS Exploitation Of Hardware Crypto - Java



- Digital Signatures via RSA
- One-way: SHA1, SHA256, MD2, MD5
- Symmetric Algorithms - DES, 3DES, AES128
- Asymmetric Algorithms – RSA
- Random number generation

z/OS And Linux Crypto Measured Performance

www.ibm.com/servers/eserver/zseries/security/cryptography.html

One CPACF called with assembler instructions: 400+MB/sec DES, 160+MB/secT-DES, 350+MB/sec SHA-1

Crypto Express 2 (Coprocessor Mode – CEX2C) with ICSF

DES – 4KB blocks = 5.2 MB/sec for one CEX2C feature
T-DES – 4KB blocks = 4.8 MB/sec
MAC – 4KB blocks = 4.8 MB/sec
DSG (CRT – 1024-bit) = 2200/sec

SSL handshakes
PKD-CRT 1024-bit = 2100/sec

Crypto Express 2 (Accelerator Mode – CEX2A) with ICSF

SSL handshakes
PKD-CRT 1024-bit = 6000/sec for one feature with two CEX2A

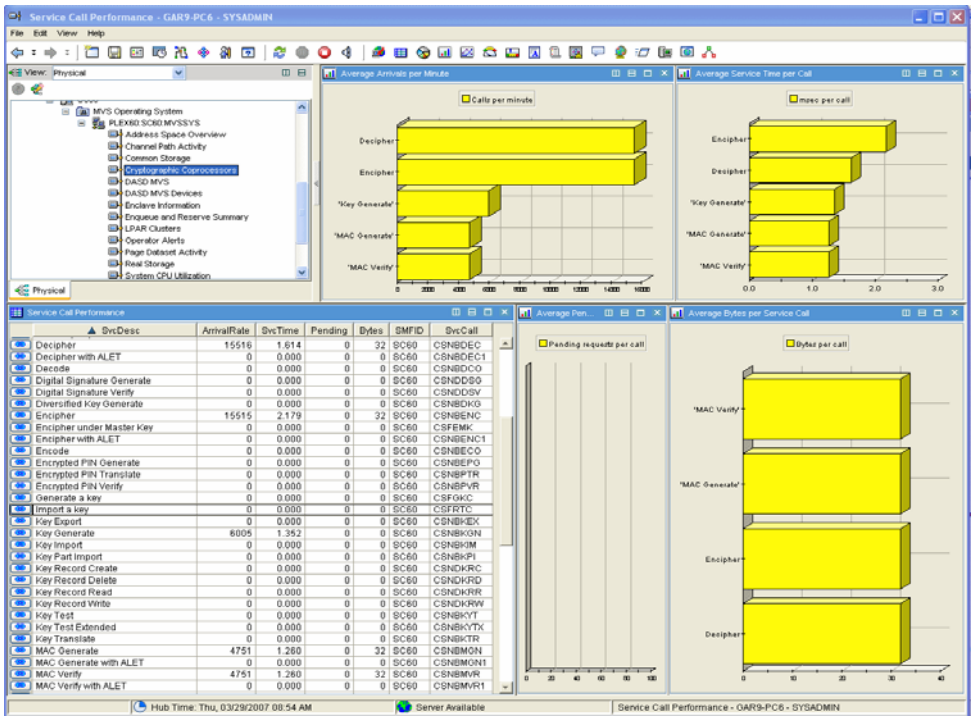
z/OS RMF Crypto Activity

```
                                C R Y P T O   H A R D W A R E   A C T I V I T Y                                  PAGE    6

           z/OS V1R8              SYSTEM ID   SYS1          DATE 11/28/2006          INTERVAL 14.59.946
                                  RPT VERSION V1R8 RMF      TIME 16.30.00            CYCLE 1.000 SECONDS

-------- CRYPTOGRAPHIC COPROCESSOR --------
          ------ TOTAL --------    KEY-GEN
TYPE   ID   RATE  EXEC TIME UTIL%    RATE
PCIXCC  0   0.00        0.0   0.0    0.00
        1   0.01       3205  32.1    0.01
        2  83.04        1.1   8.8       0
        3   0.00        0.0   0.0    0.00
CEX2C   4 210.8         4.4  93.3    1.91
        5 186.4         4.8  89.6    1.85


------------------------------------------------------ CRYPTOGRAPHIC ACCELERATOR ------------------------------------------------------
          -------- TOTAL --------   ------ ME(1024) -------   ------ ME(2048) ------   ------ CRT(1024) ------   ------ CRT(2048) ------
TYPE   ID   RATE  EXEC TIME  UTIL%    RATE  EXEC TIME  UTIL%   RATE  EXEC TIME  UTIL%   RATE  EXEC TIME  UTIL%   RATE  EXEC TIME  UTIL%
PCICA   6 165.2         1.3   21.5   107.1        1.1   11.8      0         0      0   58.1        1.7    9.7      0         0      0
        7 892.3         3.6   64.3   350.1        4.1   28.6   0.00       0.0    0.0  512.6        2.4   24.7  29.65      18.5   11.0
        8 684.8         3.5   47.8   260.4        4.0   21.0   0.00       0.0    0.0  402.4        2.3   18.6  22.02      18.5    8.1


------- ICSF SERVICES --------------------------------------------------------------------------

        DES ENCRYPTION    DES DECRYPTION    ----- MAC ------    ----- HASH ----    ------ PIN -------
        SINGLE  TRIPLE    SINGLE  TRIPLE    GENERATE  VERIFY    SHA-1   SHA-256   TRANSLATE   VERIFY
RATE      4975K  497.5     12438    1244K      12438    4975K   497.5       0.0        1244K    1244
SIZE      0.75     100K     10.00    0.01       10.00    0.01    10000         0
```

Resource : z/OS Resource Measurement Facility Report Analysis - SC33-7991

ITSO Redpaper REDP-4358 in preparation

Omegamon XE For z/OS – Crypto Activity



ITSO Redpaper REDP-4358 in preparation

Other Exploiters Of z/OS Cryptography

IBM Data Encryption For IMS And DB2 Database

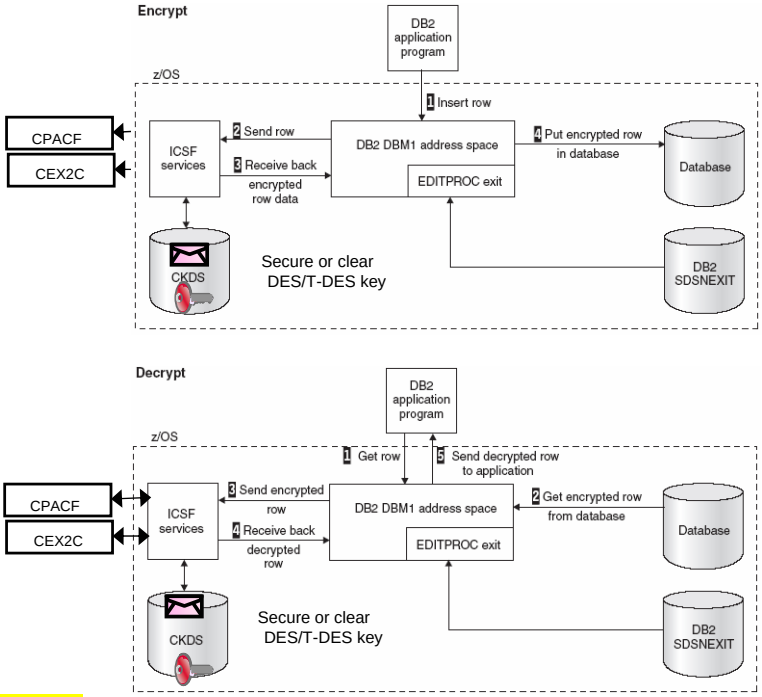
(product number 5655-P03)

EDITPROC exits
IMS Segment Edit/Compression exit
- DECENC00 – Secure key
- DECENA00 – clear key

Specified in the
EDITPROC clause of the SQL
CREATE TABLE statement

Keys installed with the KGUP (Key Generation Utility Program) in the CKDS with a label

One different key per table if desired

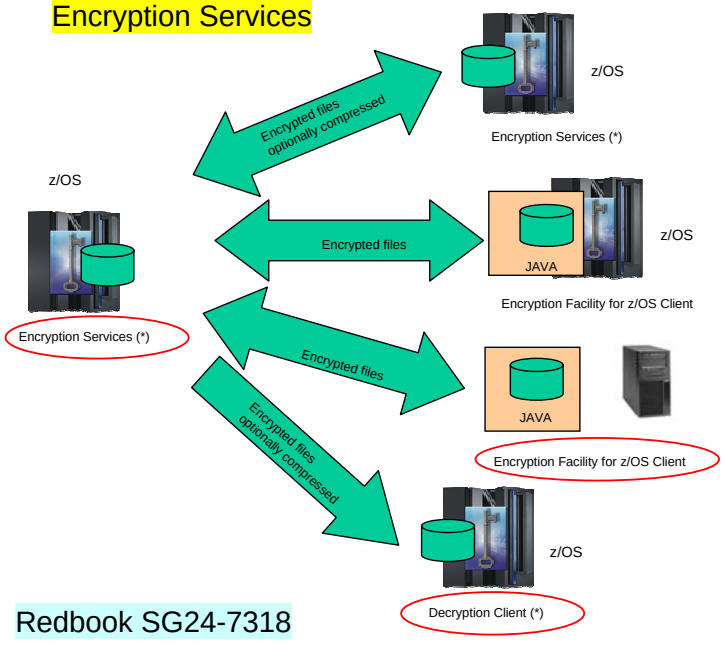


Similar implementation for IMS DB encryption

Encryption Facility For z/OS V1.2

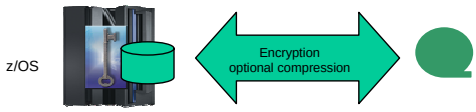
(Program Product 5655-P97)

Encryption Services

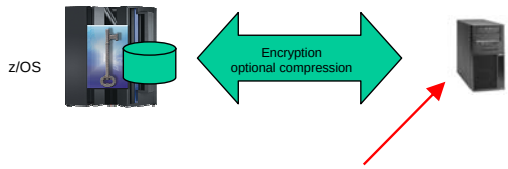


Redbook SG24-7318

DFSMSdss Encryption



OpenPGP Support

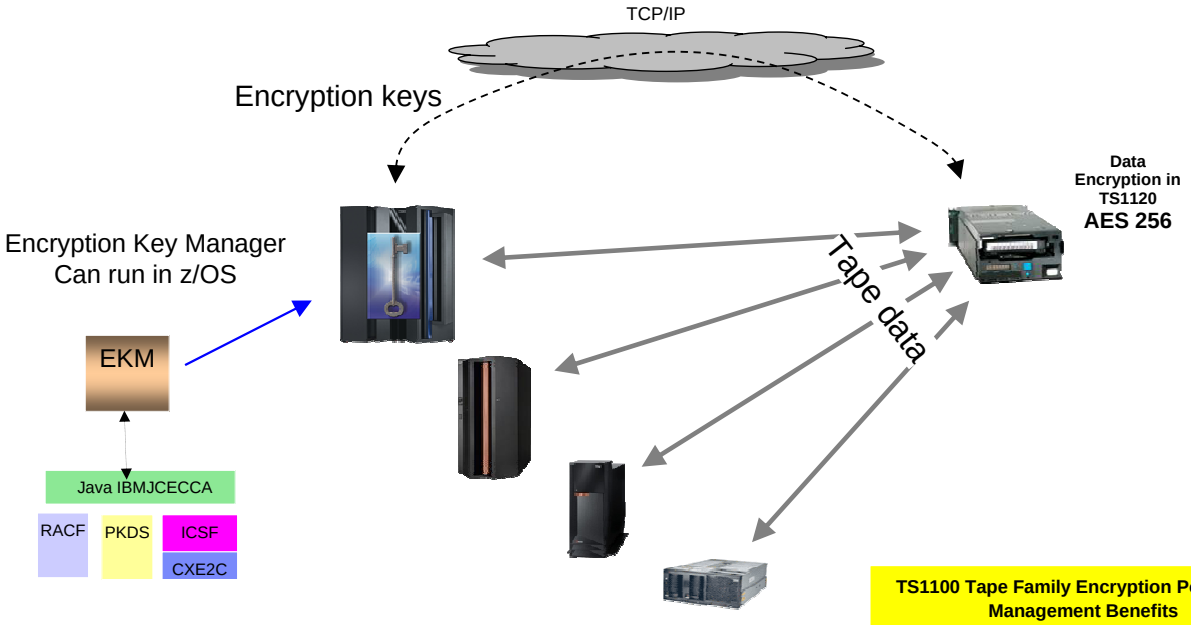


Any platform that supports OpenPGP (RFC 2440)

Redbook SG24-7434

Sizing services at
http://w3-03.ibm.com/support/techdocs/atsmastr.nsf/84279f6ed9ffde6f86256ccf00653ad3/5dd1cd0d735d3e23862570af0048710f?OpenDocument

Tape Encryption Infrastructure



- Symmetric key generation
- Symmetric key RSA wrapping/unwrapping
- RSA keys repository

TS1100 Tape Family Encryption Potential Management Benefits

- Variety of implementation methods
- Heterogeneous server support
- Avoid host MIPS encryption overhead
- Minimize impact to existing processes and applications

New Support At z/OS V1R9 (ICSF HCR7740)

PKCS#11 Support

New callable service
- CSFPTRC - Token Record Create
- CSFPTRD - Token Record Delete
- CSFPTRL - Token Record List
- CSFPSAV - Set Attribute Value
- CSFPGAV - Get Attribute ValueChanged information

Cipher Feedback Mode (CFB) and PKCS #7 padding for encryption

Changed callable services
- CSNBSYD - Symmetric Key Decipher (new CFB and PKCS-PAD keywords)
- CSNBSYE - Symmetric Key Encipher (new CFB and PKCS-PAD keywords)

Thank You

Any Questions ?

Appendix

- z/OS ICSF Overview — SA22-7519
- z/OS ICSF System Programmer's Guide — SA22-7520
- z/OS ICSF Application Programmer's Guide — SA22-7522
- z/OS ICSF Administrator's Guide — SA22-7521
- z/OS ICSF Messages — SA22-7523
- z/OS Trusted Key Entry PCIX Workstation User's Guide — SA23-2211
- Writing PKCS #11 Applications — SA23-2231

Redbook SG24-5455 Exploiting S/390 Hardware Cryptography with Trusted Key Entry
Redbook SG24-5942 S/390 PCI Crypto Coprocessor Implementation Guide
Redbook SG24-6870 zSeries Crypto Update
Redbook SG24-7070 z990 Cryptography Implementation
Redbook SG24-6499 TKE V4.2 Update
Redbook SG24-7123 System z9 and TKE V5.0 Crypto Update
Redpaper REDP-4358 Monitoring Hardware Cryptography Activity on System z

z/990-z/890 redpaper at
http://publib-b.boulder.ibm.com/Redbooks.nsf/3c7330a3359c75a68525698b007bbec9/06f28a0ffb4292fd85256d8c00666813?OpenDocument

IBM Systems Journal paper at
http://domino.research.ibm.com/tchjr/journalindex.nsf/a3807c5b4823c53f85256561006324be/fc9c727abee8d3f985256eb500713360?OpenDocument