IBM® ATS, Washington Systems Center

IMS/DB2 Database Crypto Support on z/OS

Greg Boyd
boydg@us.ibm.com

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml: AIX, AIX 5L, BladeCenter,Blue Gene, DB2, e-business logo, eServer, IBM, IBM Logo, Infoprint,IntelliStation, iSeries, pSeries, OpenPower, POWER5, POWER5+, Power Architecture, TotalStorage, Websphere, xSeries, z/OS, zSeries

The following are trademarks or registered trademarks of other companies:
Java and all Java based trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries or both
Microsoft, Windows,Windows NT and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries or both.
Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
Other company, product, or service names may be trademarks or service marks of others.

NOTES:
Any performance data contained in this document was determined in a controlled environment. Actual results may vary significantly and are dependent on many factors including system hardware configuration and software design and configuration. Some measurements quoted in this document may have been made on development-level systems. There is no guarantee these measurements will be the same on generally-available systems. Users of this document should verify the applicable data for their specific environment.

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

Information is provided "AS IS" without warranty of any kind.

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 are suggested US list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Any proposed use of claims in this presentation outside of the United States must be reviewed by local IBM country counsel prior to such use.

The 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 makes no representation or warranty regarding third-party products or services including those designated as ServerProven, ClusterProven or BladeCenter Interoperability Program products. Support for these third-party (non-IBM) products is provided by non-IBM Manufacturers.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. Send license inquires, in writing, to IBM Director of Licensing, IBM Corporation, New Castle Drive, Armonk, NY 10504-1785 USA.

Agenda

- Crypto Functions
- IBM Crypto Hardware on System z196
- ICSF
- Tape/DASD
- Exploiting Crypto on the Host
  - Data Encryption Tool for IMS and DB2
  - DB2 UDB Built-In Functions
- Exploiting Crypto in the Network
- Summary and References

Crypto Functions

- Data Confidentiality
  - Symmetric – DES/TDES, AES
  - Asymmetric – RSA, Diffie-Hellman
- Data Integrity
  - Modification Detection
  - Message Authentication
  - Non-repudiation
- Financial Functions
- Key Security & Integrity

System z Clear Key Crypto Hardware –z196

- CP Assist for Crypto Function (CPACF)
  - DES (56-, 112-, 168-bit)
  - AES-128, AES-192, AES-256
  - SHA-1, SHA-256, SHA-384, SHA-512 (SHA-2)
  - PRNG (Pseudo Random Number Generation)
  - Protected Key

TechDoc WP100810 – A Synopsis of System z Crypto Hardware

System z Secure Key Crypto Hardware - CEX3 (z196)

- Secure Key DES/TDES
- Secure Key AES
- Financial (PIN) Functions
- Key Generate/Key Management
- Random Number Generate and Generate Long
- Protected Key Support
- Elliptic Curve Digital Signature Algorithm (ECDSA)
- SSL Handshakes

TechDoc WP100810 – A Synopsis of System z Crypto Hardware

Clear Key / Secure Key / Protected Key

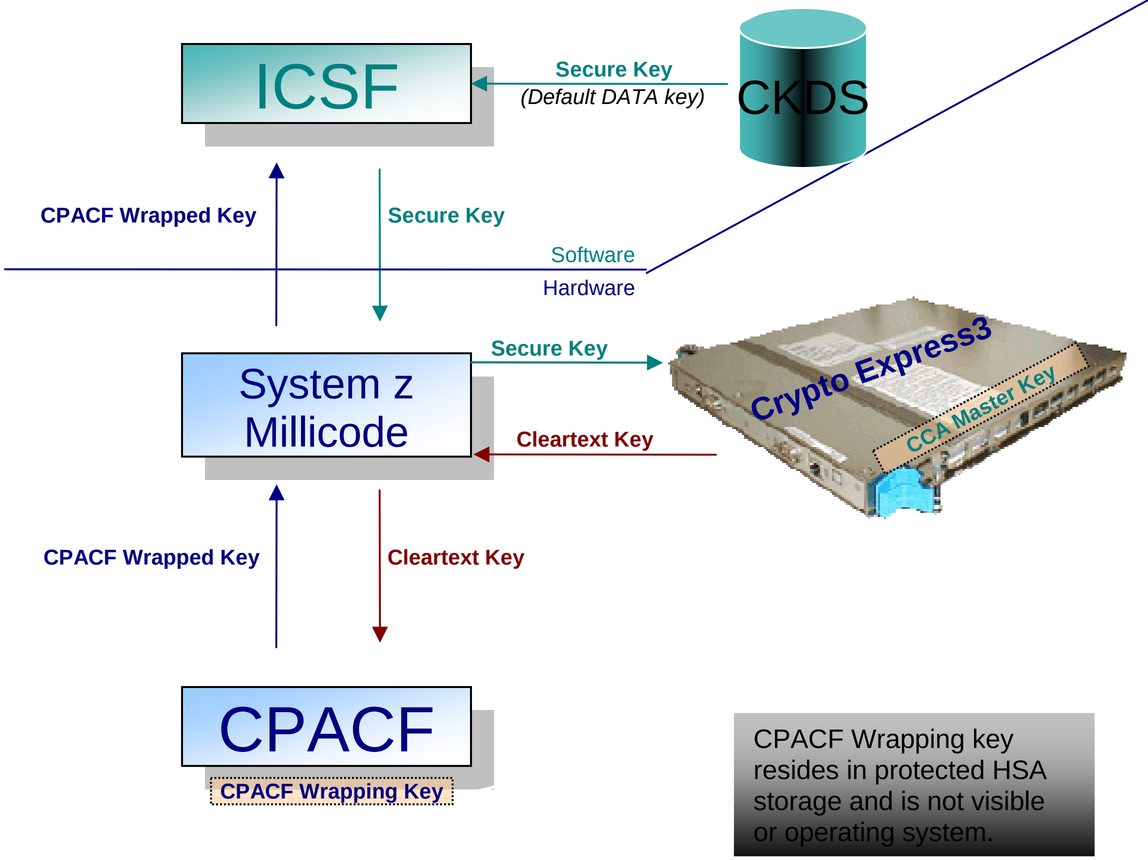
- Clear Key – key may be in the clear, at least briefly, somewhere in the environment
- Secure Key – key value does not exist in the clear outside of the HSM (secure, tamper-resistant boundary of the card)
- Protected Key – key value does not exist outside of physical hardware, although the hardware may not be tamper-resistant

TechDoc WP100647 – A Clear Key / Secure Key / Protected Key Primer

CPACF Protected Key - Key Wrapping

CPACF Wrapped key cached in ICSF address space in.

Source key is stored in CKDS as a CCA MK wrapped key.



CPACF Wrapping key resides in protected HSA storage and is not visible or operating system.

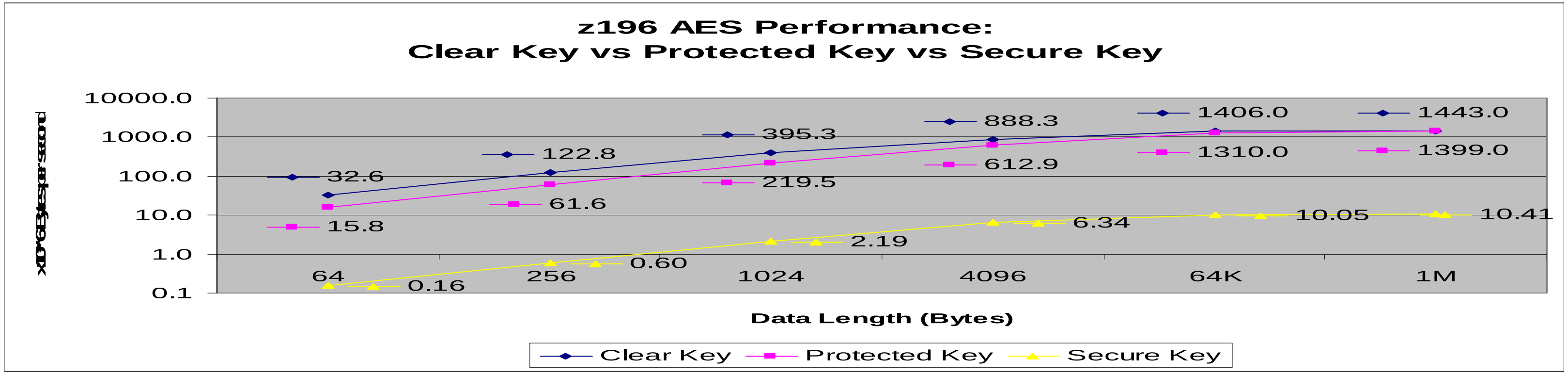
- Create a key ‘ABCD’, store as secure key (i.e. encrypted under Master Key, MK)
  - E_{MK}(x’ABCD’) => x’4A!2’
- Execute CSNBSYE (clear key API) with that key and text to be encrypted of ‘MY MSG ’
- ICSF will pass key value x’4A!2’ to CEX3, recover original key value, then wrap it using wrapping key
  - D_{MK}(x’ 4A!2’) => x’ ABCD’
  - E_{WK}(x’ABCD’) => x’*94E’
- ICSF will pass wrapped key value to CPACF, along with message to be encrypted
- In CPACF, unwrap key and perform encryption
  - D_{wk}(x’ *94E’) => x’ ABCD’
  - $E_{x’ABCD’}$(‘MY MSG ’) => ciphertext of x’ 81FF18019717D183’

z196 Crypto Performance

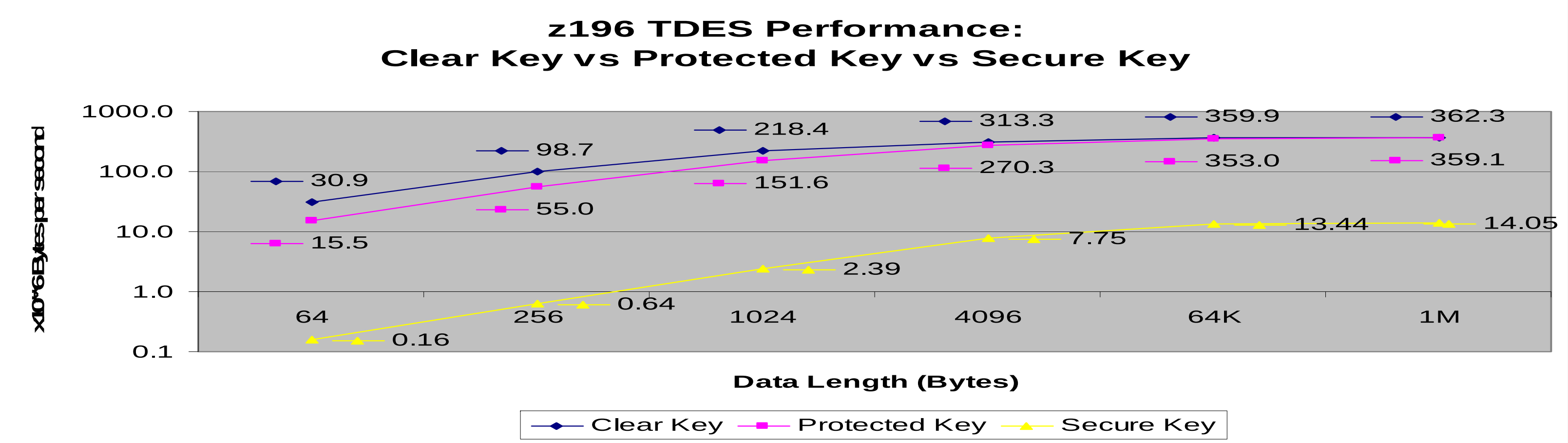
- From the Crypto Performance Whitepapers

  http://www.ibm.com/systems/z/advantages/security/z10cryptography.html

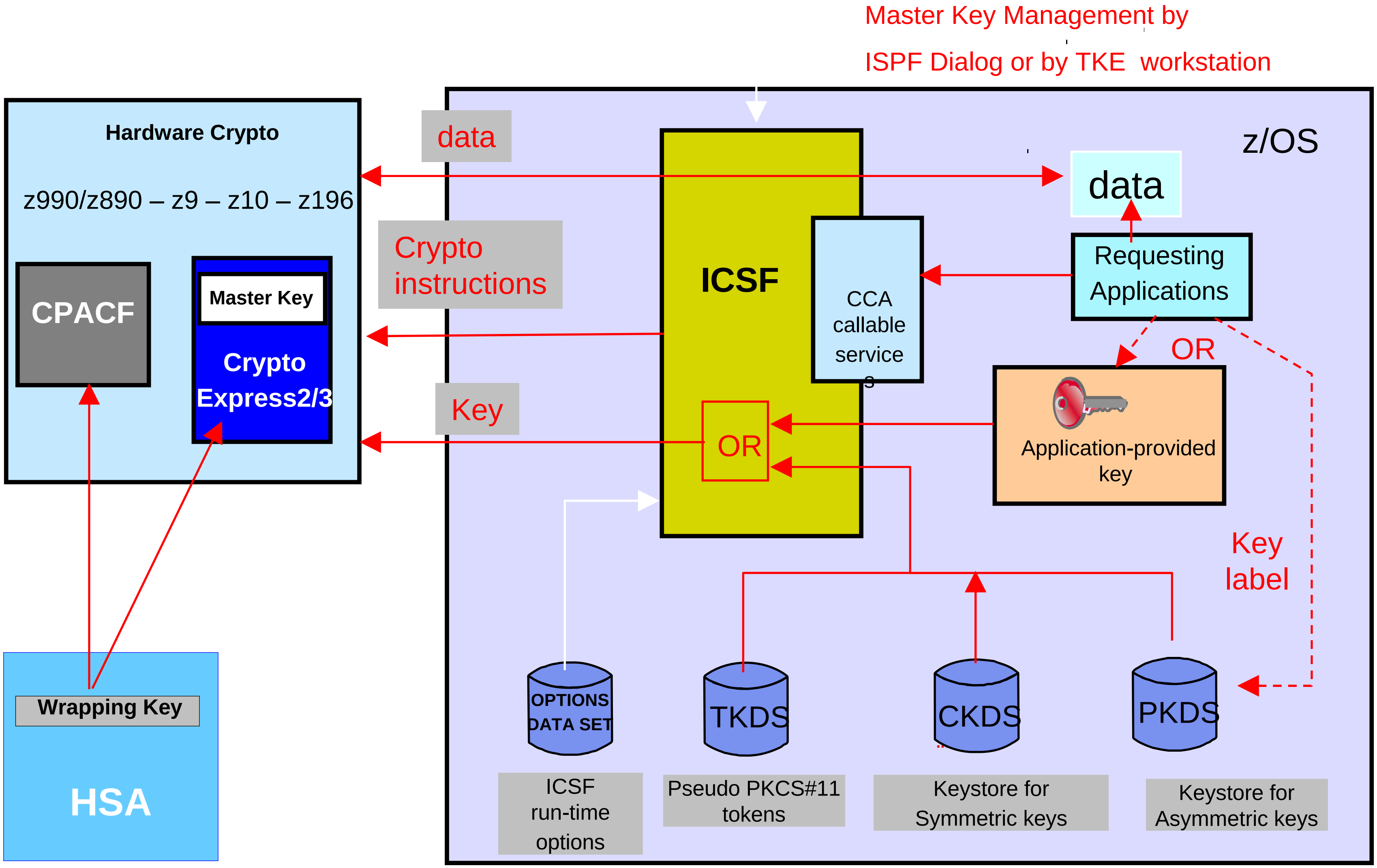
- AES Encryption



- TDES Encryption



z/OS Integrated Cryptographic Services Facility



Wrapping Key only supported on z10 or z196 with CEX3

SAF Protection

- ICSF uses SAF to protect resources
  - CSFKEYS Class
    - Protects the key by its label
  - CSFSERV Class
    - Profiles to protect the APIs
    - Profiles to protect ISPF panels
  - CSFKGUP profile to protect the Key Generation Utility Program
- Key Store Policies
  - Key Token Authorization Checking
  - Default Key Label Checking
  - Duplicate Key Token Checking
  - Granular Key Label Access Control
  - Symmetric Key Label Export Control

Refer to the z/OS ICSF Administration Guide for a list of *service_names* that can be protected

IBM Tape Based Encryption

- LTO4 and LTO5 - Open Systems
- TS1120, TS1130, TS1140 - Open Systems and Mainframe
- AES-256 bit encryption
- All files on the tape are protected using a single key
  - Which is in turn encrypted using RSA (public/private key algorithms)
- TKLM, Tivoli Key Lifecycle Manager or just announced, ISKLM IBM Security Key Lifecycle Manager is required for DS8000 and recommended for Tapes

IBM DS8000 Disk Encryption - Characteristics

- Customer data at rest is encrypted
  - Data at rest = data on any disk or in any persistent memory
- Customer data in flight is not encrypted
  - Data in flight = on I/O interfaces or in dynamic memories (Cache, NVS)
    - If you can read/write to disk, you get access to clear-text data.
- Uses Encrypting Disk
  - Encryption hardware in disk (AES 128)
  - Runs at full data rate (146/300/450 GBs 15K RPM)- No measurable performance impact
- Integrated with Tivoli Key Lifecycle Manager (TKLM) or IBM Security Key Lifecycle Manager (ISKLM)
  - DS8000 automatically communicates with TKLM when configuring encryption group or at power on to obtain necessary encryption keys to access customer data
  - Each disk has an encryption key
    - Data is always encrypted on write and decrypted on read
    - Encryption key is wrapped with access credential and maintained within the disk
    - Access credential maintained by TKLM/ISKLM
    - Establishing a new encryption key causes cryptographic erasure
- Key attack vectors prevented:
  - Disk removed (repair, or stolen)
  - Box removed (retire, or stolen)

Encryption of Data within the Database

- Critical requirement for most of the “popular” data protection initiatives: To protect “data at rest” to ensure that the only access is for business need-to-know, and through mechanisms which can be controlled by the native security mechanisms (such as RACF)
- Consider the following scenario - DB2 Linear VSAM datasets are protected via RACF from direct access outside of DB2 using dataset access rules
    - DBA or Storage Administrator has RACF authority to read VSAM datasets in order to perform legitimate storage administration activities
    - Administration privileges can be abused to read the linear VSAM datasets directly and access clear-text data outside of DB2/RACF protections
- Now consider the above scenario, but with the underlying Linear VSAM datasets encrypted
    - When DBA or Storage Administrator uses their RACF dataset authorities in a manner which is outside of business need-to-know, the data retrieved is cybertext and thus remains encrypted and protected
    - Only way to access and obtain clear-text data will be via SQL which can be protected via DB2/RACF interface

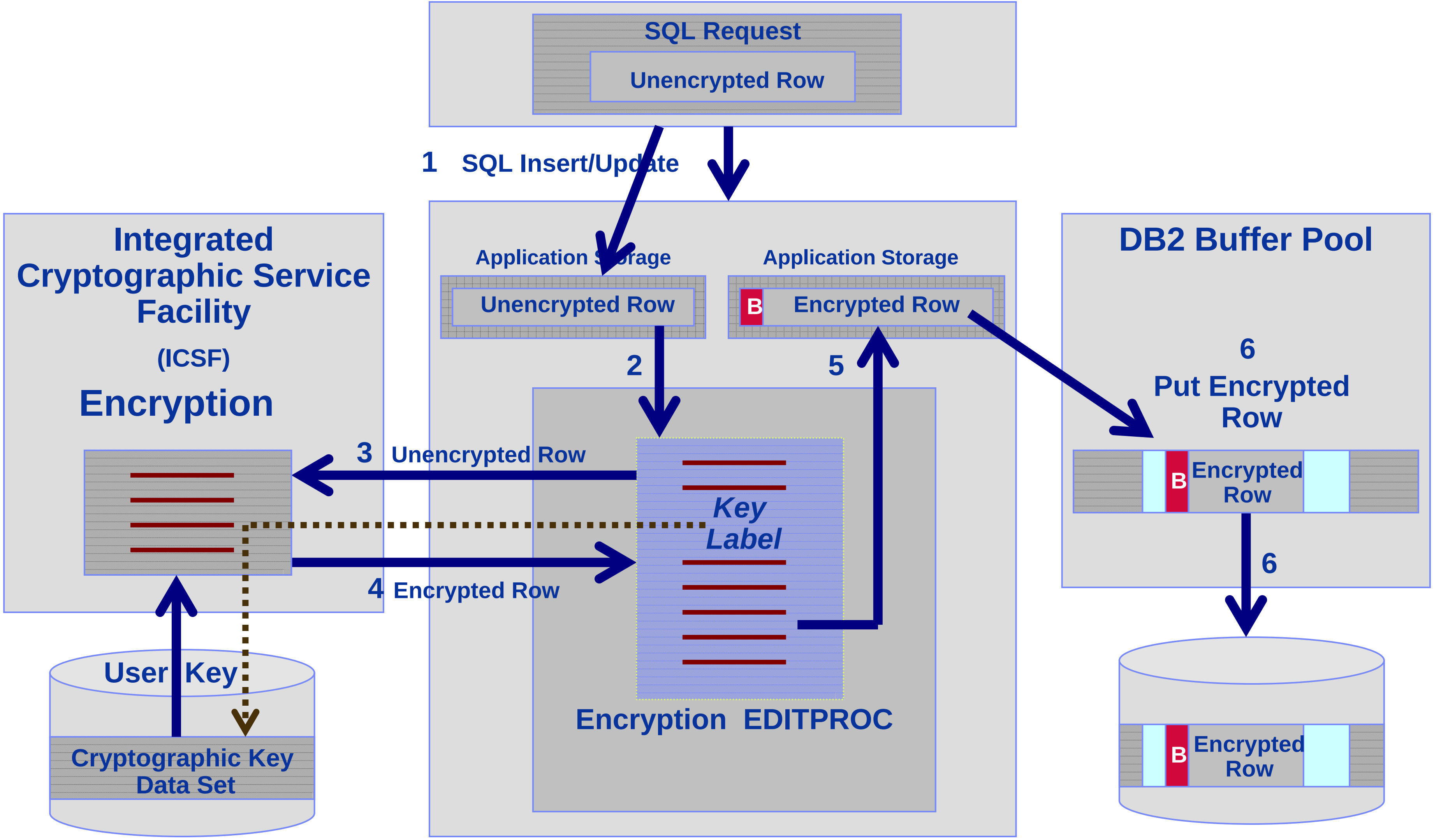
Database Encryption

- Data Encryption Tool for IMS & DB2 Databases (5799-P03)
- DB2 UDB Built-In Functions

The Data Encryption Tool – How It Works

- Via an EDITPROC, for every row processed by any SQL Utility for DB2 or IMS
  - No application changes required
  - One key per table or segment specified in the EDITPROC
  - Can use Clear Key, Secure Key or Protected Key
    - Protected key requires HCR7770 or later and CEX3
  - Encrypted row same length as clear row

DB2 Data Encryption Flow – Insert / Update



DB2 Built-In Functions – How It Works

- Under application control - for every field that must be encrypted ex. encrypt(data,'password for encryption',hint)
  - 'Password for Encryption' is hashed to generate a unique key
  - Hint can be used as a prompt for remembering the key
  - Encrypted field must be defined as VARCHAR (since it will contain binary data once its encrypted) and the encrypted field will be longer (next multiple of 8 bytes + 24 bytes of MetaData + 32 bytes for optional hint field)
    - Password is hashed via MD5 to create 128 bit key
    - Password + data is then encrypted using TDES with 128 bit key

Cryptographic Keys

- Data Encryption Tool
  - Clear Key or Secure Key or Protected Key
  - Key must be stored in the CKDS
  - When the table with an EDITPROC is in use, the key is available in the DB2 address space
- DB2 BIF
  - Clear key only (it’s calculated from the password for encryption in software)
  - Keys are not stored in a dataset, but the password for encryption is stored in the table

Cryptographic Key Changes

- Data Encryption Tool
  - Unload, change EDITPROC to reference new key, reload
  - Unload, change current key, DB2 restart, reload
- DB2 BIF
  - Under application control

Database Indexes

- Data Encryption Tool
  - EDITPROC encrypts the entire row, so the data is encrypted, but the index is not
    - Bad for security, good for performance
- DB2 BIF
  - Application encrypts the field, if that field is an index, then the index is encrypted
    - Good for security, bad for performance

Crypto Hardware for Data Encryption Tool

- Clear Key

z196/z10/z9/z890/z990	CPACF (& PCIXCC or CEXnC for CKDS*)

- Secure Key

z890/z990	Requires a PCIXCC or CEX2
Z9	Requires a CEX2C
z10	Requires a CEX2C or CEX3C
z196	Requires a CEX3C

- Protected Key

z10/z196	Requires a CEX3C**

*Prior to HCR7750, a CEXnC is required to create and use a CKDS, beginning with HCR7751 ICSF supports a clear key only CKDS

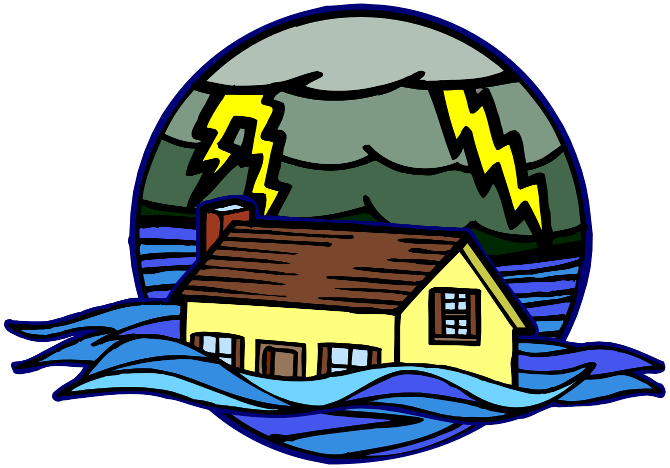
**Protected Key support requires HCR7770 or higher

Crypto Hardware for DB2 BIFs

- z196/z10/z9/z990/z890
  - CPACF (uses MSA instructions, not the ICSF APIs), but ICSF must be started to provide hashing support
  - TDES only

Disaster Recovery Considerations

- The major requirement is that the appropriate crypto hardware be available at the DR site
  - Clear Key / Secure Key / Protected Key
  - Key lengths
- Master keys must be available at the DR site



Side-by-side Comparison

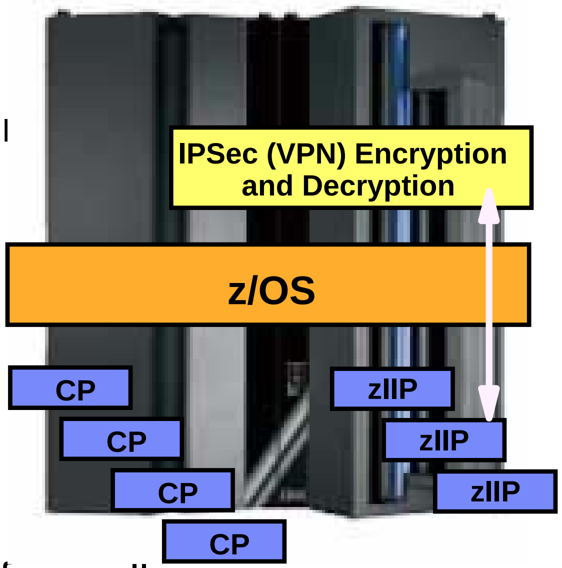
	Column (DB2 Built-In Functions)	Row/Table (IBM Encryption Tool for IMS and DB2)
DB2 Support	▪V8, V9, V10 ▪Data in indexes is encrypted ▪Does not work w/DB2 Load Utility ▪Data type of encrypted columns must be FOR BIT DATA	▪V7.x, V8.x, V9.x, v10.x ▪DB2 index data is not encrypted. ▪Works with all DB2 utilities
Application Change Required	▪Application must change to invoke the BIFs for the columns that will be encrypted	▪No application change, but each table will need to be recreated with an EDITPROC
Transaction Processing Overhead	▪The cost overhead depends on hardware, DB2 and application access	▪Each row individually encrypted
Key Management	▪Application has responsibility for the encryption key	▪Keys are managed by and accessed through ICSF
Pre-Reqs	▪ICSF must be active ▪CPACF hardware	▪ICSF must be active ▪Secure PCI card, unless running HCR7751 or later and clear key only CKDS

Decisions, Decisions …

- Ownership (i.e. politics)
  - Data Administrator - Data Encryption Tool
    - sets up the EDITPROC and specifies the key to be used for the entire table
    - Key must be defined to/managed by ICSF (stored in the CKDS)
  - Application - DB2
    - Application logic determines which key to use for each field/column
    - Password is managed by the application
- Security requirements
- Performance requirements
- Application/production support
- Space considerations
- Crypto hardware available

zIIP Assisted IPSec (VPN) on z/OS

- **Benefits of having secure channel end-point on z/OS**
  - Security regulations compliance - No clear-text data on any networ segments
  - End-to-end authentication of secure channel end-points
    - Both end-point authentication and message authentication
  - Key management and storage done on System z by z/OS
  - Compliance with end-to-end security regulations
- **System z CPU cost is a concern**
  - Encryption/decryption CPU cost can be a significant percentage of overall CPU cost for a given application
  - Especially the case for streaming workloads (file transfer type of workload)
- **zIIP processors**
  - Specialty processor on System z9 or later hardware
  - zIIPs priced lower than general purpose processors
  - No IBM software charges on zIIPs
- **zIIP Assisted IPSec**
  - Use zIIP processors for most IPSec encryption/decryption
  - Lower the cost of doing IPSec processing on z/OS



System z9 or later
z/OS CS V1R8 + PTFs
z/OS CS V1R9

Closing Thoughts

- Encryption has a cost
  - Crypto hardware more efficient with large blocks of data
- Secure Key on a PCI Card – longer pathlength
- Clear Key exists in the DB2 Address Space; Protected Key and Secure Key as well, but they are encrypted under the Wrapping Key or Master Key

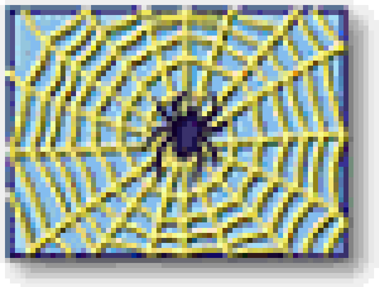
References

- Cryptography Books
  - Bruce Schneier, ‘Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in “C”’, Addison Wesley Longman, Inc., 1997
  - Simon Singh, ‘The Code Book’, Anchor Books, 1999
  - Niels Ferguson, Bruce Schneier, ‘Practical Cryptography’, Wiley Publishing, Inc. 2003
- Standards
  - www.ietf.org – Internet Engineering Task Force
  - www.csrc.nist.gov – Computer Security Resource Center of NIST
  - www.rsasecurity.com/rsalabs - Research site for RSA Security
- Free Stuff
  - www.scmagazine.com - SC Magazine
  - www.counterpane.com – Bruce Schneier web site with monthly newsletter

IBM Pubs

- ICSF Overview, SA22-7519
- ICSF Administrator’s Guide, SA22-7521
- ICSF Application Programmer’s Guide, SA22-7522
- ICSF System Programmer’s Guide, SA22-7520

IBM Resources (on the web)



- Redbooks – www.redbooks.ibm.com ‘Crypto’
  - z9-109 Crypto and TKE V5 Update, SG24-7123
  - IBM zEnterprise System Technical Introduction, SG24-7832
  - IBM zEnterprise System Technical Guide, SG24-7833
  - IBM zEnterprise 196 Configuration Setup, SG24-7834
- ATS TechDocs Web Site www.ibm.com/support/techdocs (Search All Documents for keyword of ‘Crypto’)
  - WP100810 – A Synopsis of System z Crypto Hardware
  - WP100647 – A Clear Key/Secure Key/Protected Key Primer
- Web Download Site
  - http://www.ibm.com/systems/z/os/zos/downloads/

Data Encryption for DB2 - Reference Materials

- SC18-9549 IBM Data Encryption Tool for IMS and DB2 Databases User Guide
  - Includes an appendix on activating crypto on your hardware
- ICSF Manuals
  - SA22-7520 ICSF System Programmer’s Guide
  - SA22-7521 ICSF Administrator’s Guide
- Redbooks
  - DB2 UDB for z/OS Version 8 Performance Topics – SG24-6465
- Articles
  - IMS Newletter article: “Encrypt your IMS and DB2 data on z/OS” - ftp://ftp.software.ibm.com/software/data/ims/shelf/quarterly/fall2005.pdf

Questions ?!?
MICHEL