IMS/DB2 Database Crypto Support

Ernie Mancill
mancill@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

- **Introduction to Crypto**
  - Crypto Functions
  - IBM Crypto Hardware on System z196
  - ICSF
  - Database Encryption (DB2 and IMS)
  - Other Encryption Exploitation
- **Database Activity Monitoring with Guardium**
- **Conclusion and Reference Resources**

Crypto Functions

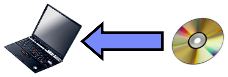
- **Data Confidentiality**
  - Symmetric – DES/TDES, AES
  - Asymmetric – RSA, Diffie-Hellman
- **Data Integrity**
  - Modification Detection
  - Message Authentication
  - Non-repudiation
- **Financial Functions**
- **Key Security & Integrity**

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**

System z Clear Key Crypto Hardware –z196

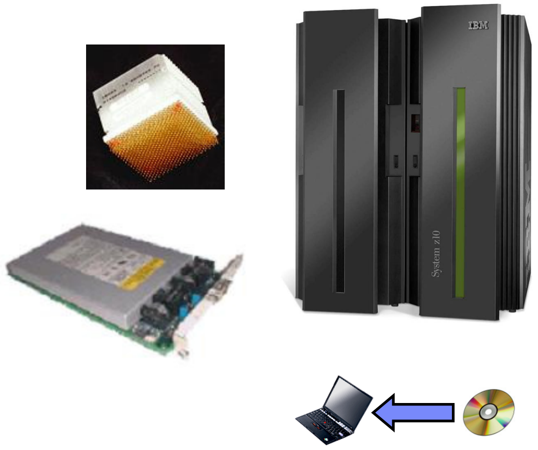
- **CP Assist for Crypto Function (CPACF)**
  - **DES (56-, 112-, 168-bit), new chaining options**
  - **AES-128, AES-192, AES-256, new chaining options**
  - **SHA-1, SHA-256, SHA-384, SHA-512 (SHA-2)**
  - **PRNG**
  - **Protected Key**



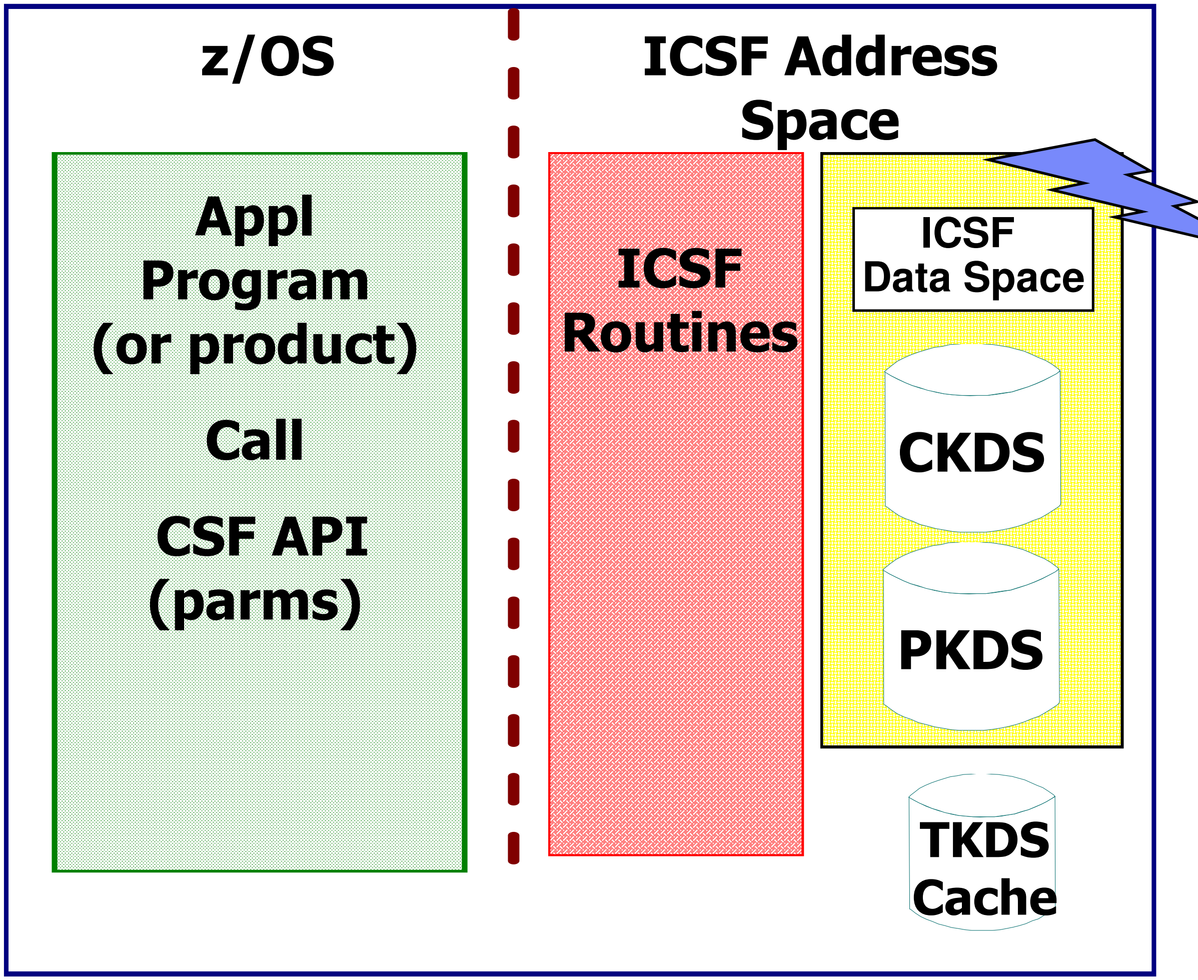
TechDoc WP100810 – A Synopsis of System z Crypto Hardware

System z Secure Key Crypto Hardware - CEX3 (z196)

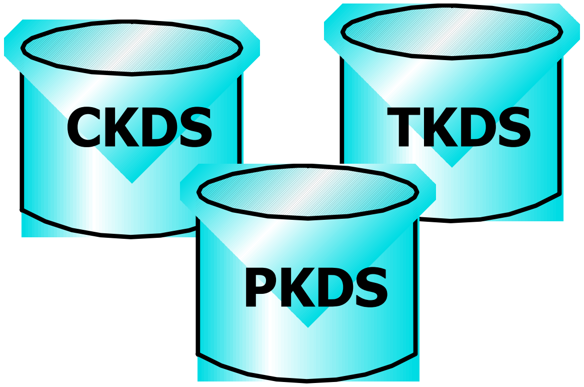
- **Secure Key DES/TDES**
- **Secure Key AES**
- **Financial (PIN) Functions**
- **Key Generate/Key Management**
- **Random Number Generate and Generate Long**
- **Protected Key Support**
- **SSL Handshakes, ECDSA support**



ICSF – Interface to the Crypto Hardware



- APIs
- Key Storage
- Load Balancing
- Security



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

Enabling Protected Key

- **Install HCR7770 or later**
  - CSFINIT replaces CSFMMAIN
- **Install Crypto Express3 on z10 with Driver 79 or on z196**
- **Install RACF (OA29193) and SAF (OA29194) APARs**
- **Create secure keys which will be used as protected keys**
- **Create/update RACF profiles for the keys, with SYMCPACFWRAP(YES)**

Encryption and “Data at Rest” Protection

- **Key requirement for most of the “popular” data protection initiatives**
- **Main requirement is to protect “data at rest” to ensure that only access if 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 controlled via RACF from direct access outside of DB2 via 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

Encryption and DB2 for z/OS

- **IBM Data Server Drivers starting in V9.5 support SSL protocol and AES encryption.**
- **Starting with Fix Pack 2, non-Java clients supports the Secure Sockets Layer (SSL) protocol. All DB2 Version 9.5 clients now support SSL. In addition, Java and CLI clients now support 256-bit AES encryption.**
- **SSL connectivity and AES user ID and password encryption requires Communication's AT-TLS configured and ICSF started.**
- **Starting with DB2 for z/OS V8, column level encryption implemented via SQL primitives is supported. TDES 128 bit support only.**
- **Row level encryption implemented for all supported releases of DB2 for z/OS using the IBM Infosphere Guardium Encryption Tool for IMS and DB2 databases**
- **DS8000 family DASD Based Encryption**
- **TS1120/TS1130 Tape Based Encryption**
  - TKLM (Tivoli Key Lifecycle Manager) Required for DS8000 and recommended for TS1120/TS1130

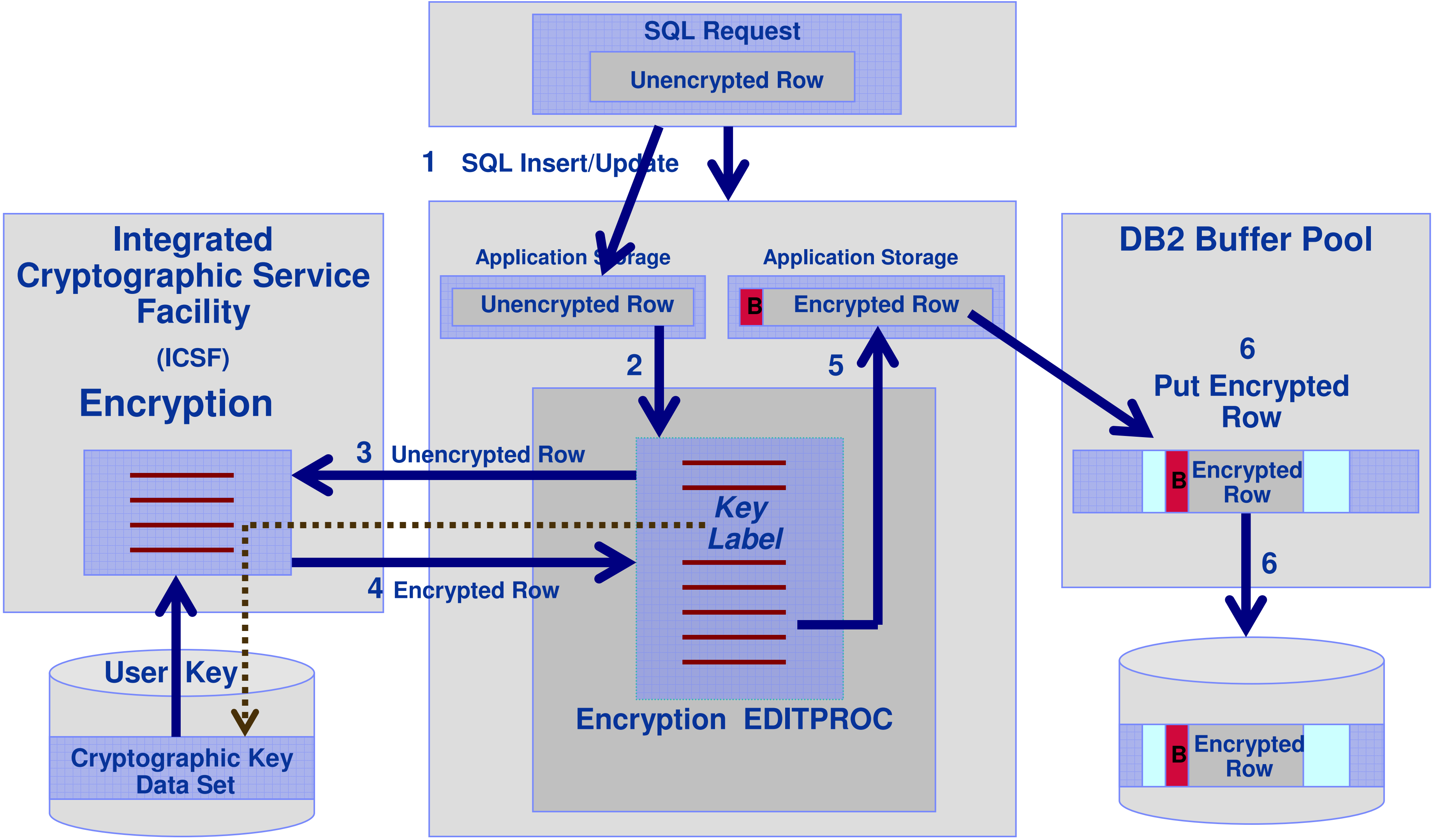
Database Encryption

- **DB2 UDB Version 8/9 Built-In Functions**
- **IMS Data Encryption Tool for IMS & DB2 Databases (5799-P03)**

How is crypto invoked with the Data Encryption Tool?

- **Via an EDITPROC, for every row processed by any SQL Utility for DB2 or IMS**
  - Encrypted row same length as clear row
  - 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

DB2 Data Encryption Flow – Insert / Update



How is crypto invoked with DB2 Built-In Functions?

- **Within the application, for every field that contains encrypted data 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)

Crypto Keys and Indexes

- **Data Encryption Tool**
  - EDITPROC encrypts the entire row, so the data is in the encrypted, but the index is not
    - Bad for security, good for performance
    - Encryption key is stored in the CKDS, when not in use
    - When in use, the key is brought into the DB2 Address Space
- **DB2 V8/V9/V10**
  - Application encrypts the field, if that field is an index, then the index is encrypted
    - Good for security, bad for performance
    - Key value is in the DB2 Address Space

Crypto Hardware for Data Encryption Tool

- **Clear Key**

– z800/z900/G6	Requires a CCF
– z10/z9/z890/z990	CPACF (& PCIXCC, CEX2C for CKDS)*

- **Secure Key**

– z800/z900/G6	Requires a CCF
– 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

Crypto Hardware for DB2 V8/V9/V10 BIFs

- **z900/z800/G6**
  - – These machines only supported Secure Key via the CCF hardware, so all work is done using secure key APIs
- **z196/z10/z9/z990/z890**
  - – CPACF (uses MSA instructions, not the ICSF APIs), but ICSF must be started to provide hashing support
  - – TDES only

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	▪High overhead due to the amount of data encryptions
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

Who owns the data and who is responsible for it’s security?

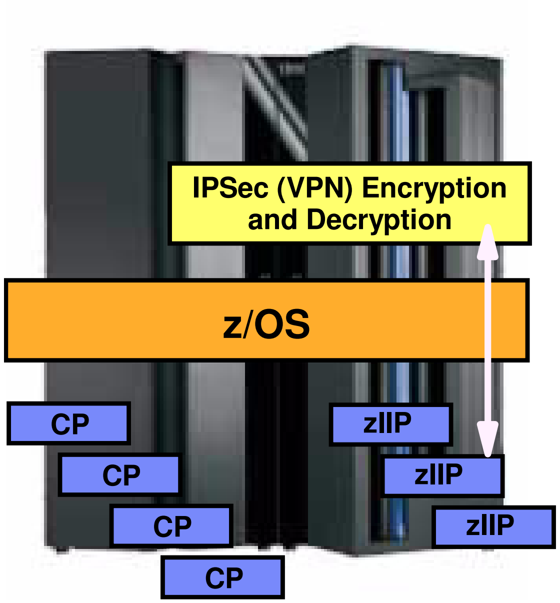
- **Data Administrator - Data Encryption Tool**
  - sets up the EDITPROC and specifies the key to be used for the entire table
  - Key must be defined to/managed by ICSF (stored in the CKDS)
- **Application - DB2 V8/V9/V10**
  - Application logic determines which key to use for each field/column
  - Password is managed by the application

Decisions, Decisions

- **Which should you implement**
  - Depends on
    - 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
  - No clear-text data on any network segments
    - Security regulations compliance
  - 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



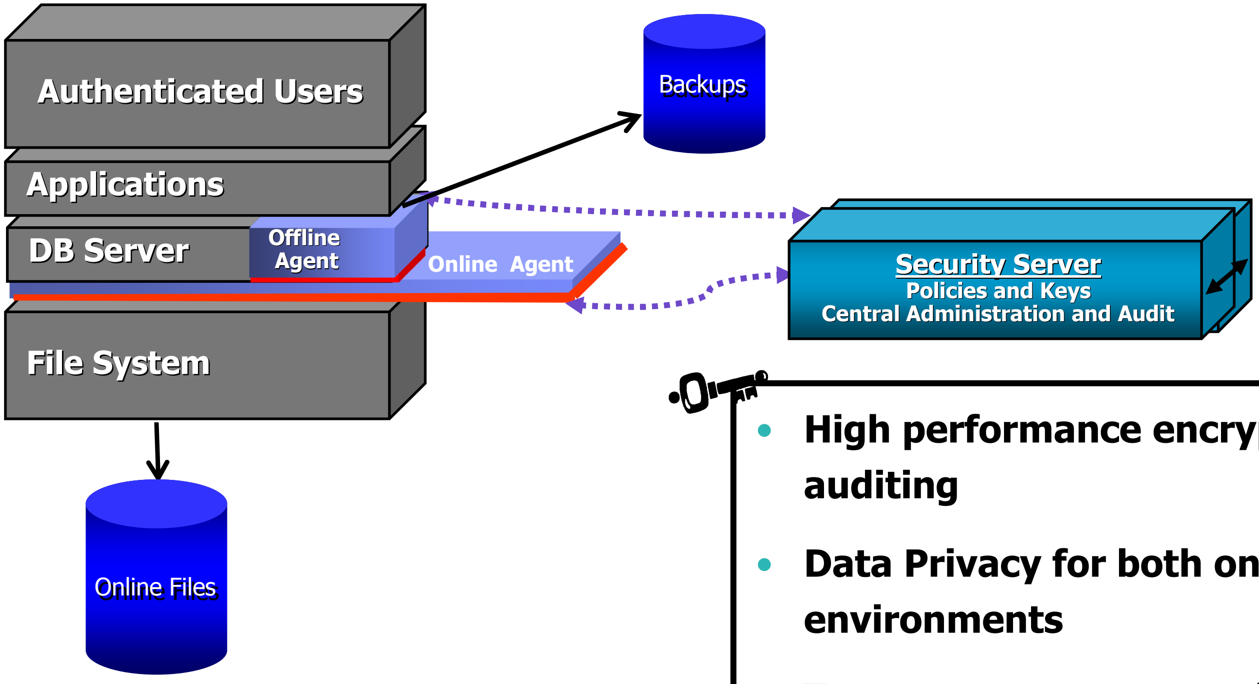
System z9 or later
z/OS CS V1R8 + PTFs
z/OS CS V1R9

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)**
  - 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
    - Establishing a new encryption key causes cryptographic erasure

- **Key attack vectors prevented:**
  - Disk removed (repair, or stolen)
  - Box removed (retire, or stolen)

Optim Encryption Expert – Data Encryption



UDB, IDS, and Others

- **High performance encryption, access control and auditing**
- **Data Privacy for both online and backup environments**
- **Transparency to users, databases, applications, storage**
  - No coding or changes to existing IT infrastructure
  - Protect data in any storage environment
  - User access to data same as before
- **Centralized administration**
  - Policy and key management
  - Audit logs
  - High Availability

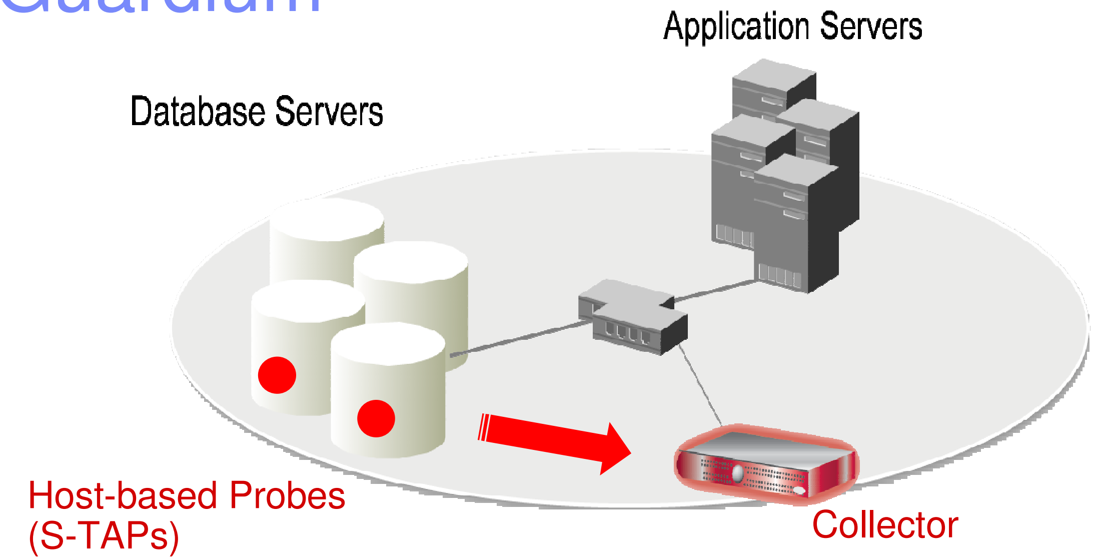
Why auditing is important in a RACF controlled environment

- **RACF provides significant controls to protect access to resources, but does little in the way of meaningful access reporting**
  - RACF does two things:
    - Prevents people from accessing a resource that is not essential or appropriate for their jobs
    - Allows people access to the necessary data to do their jobs
  - But RACF does NOT:
    - prevent a malicious update if the user has authority to the data.
    - prevent an authorized user from accessing sensitive data that is ***NOT*** within the scope of their job.E.g. a bank teller looks up the CEOs bank balance or personal customer information
    - provide meaningful information about access to protected DB2 resources (authorized or not).
- **DB2 Audit trace will do nothing to protect data, but provides data to help understand what type of access has occurred.**
    - Auditing is about ensuring that the appropriate controls are in place to identify inappropriate access and use of production data
    - You need some form of audit facility to watch your privileged users who have RACF and/or DB2 authority and users that have access to sensitive data within the scope of their job
    - Understanding how trusted (privileged) users access sensitive information is essential to ensuring that data is indeed protected

Auditing the Privileged Database User

- **DB2 trace based processes are managed by DBA's**
  - The DBA's are responsible for generating audit data with which they are in turn audited, this constitutes a significant security risk and exposure
  - Trace data collection can be interfered with or turned off completely
    - DBA can issue –DSN Stop Trace
    - Use IFASMFDMP to selectively filter SMF data based on timestamp
    - Use DB2PM (Or Equivalent) filter such as DATE/TIME/EXCLUDE to filter selected records
  - Having the DBA involved in the collection of audit data is viewed as weak from a compliance and control perspective
- **Security and Auditors with system privileges**
  - Also viewed as problematic from a compliance perspective
  - Requires additional technical skills not within their core competencies
  - Misuse of privileges without coordination can result in performance and availability issues
    - Turning on traces without proper filtering to reduce overhead or quantity of trace data collected
    - Altering objects to AUDIT without ensuring that plan/package invalidation is not an issue

Real-Time Database Monitoring with InfoSphere Guardium

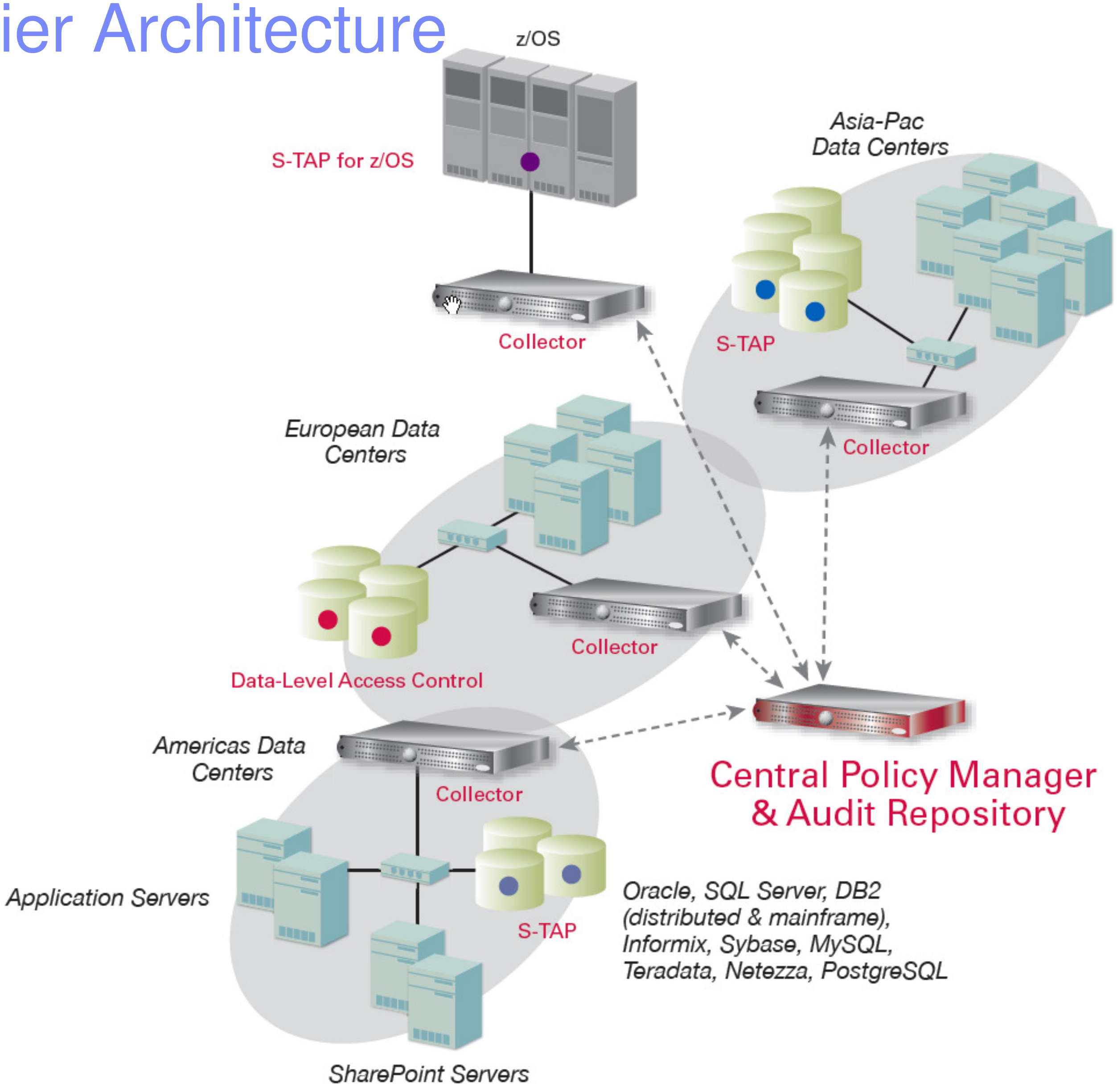


ORACLE
IBM DB2
Microsoft Office SharePoint
TERADATA
Microsoft SQL Server
PostgreSQL
NETEZZA
MySQL
IBM Informix
SYBASE

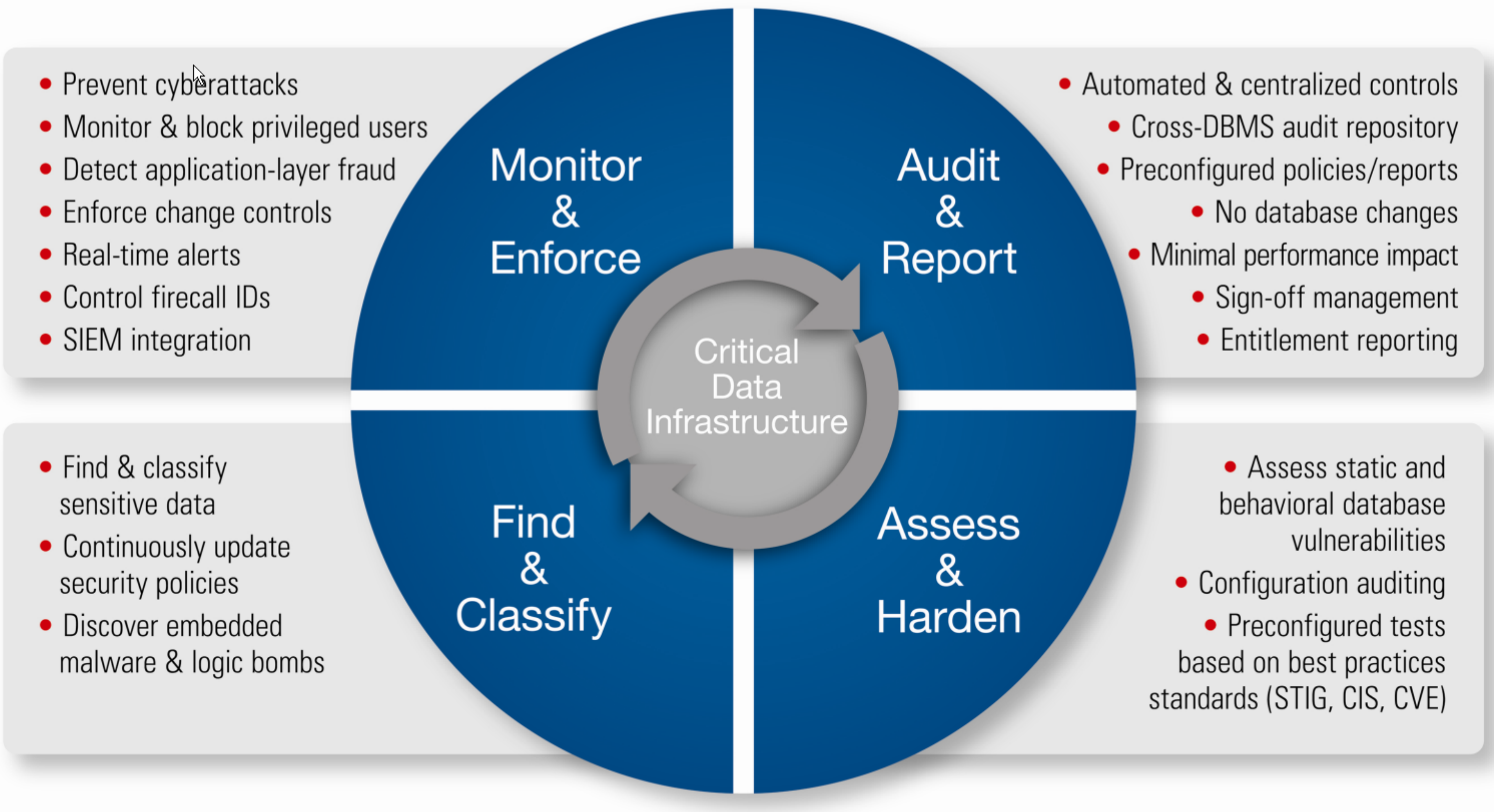
- Non-invasive architecture
  - Outside database
  - Minimal performance impact
  - No DBMS or application changes
- Cross-DBMS solution
- 100% visibility including local DBA access

- Enforces separation of duties
- Does not rely on DBMS-resident logs that can easily be erased by attackers, rogue insiders
- Granular, real-time policies & auditing
  - *Who, what, when, how*
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)

Scalable Multi-Tier Architecture



Addressing the Complete Database Security and Compliance Lifecycle



- Prevent cyberattacks
- Monitor & block privileged users
- Detect application-layer fraud
- Enforce change controls
- Real-time alerts
- Control firecall IDs
- SIEM integration

Monitor & Enforce

Audit & Report

- Automated & centralized controls
- Cross-DBMS audit repository
- Preconfigured policies/reports
- No database changes
- Minimal performance impact
- Sign-off management
- Entitlement reporting

Critical Data Infrastructure

Find & Classify

- Find & classify sensitive data
- Continuously update security policies
- Discover embedded malware & logic bombs

Assess & Harden

- Assess static and behavioral database vulnerabilities
- Configuration auditing
- Preconfigured tests based on best practices standards (STIG, CIS, CVE)

Closing Thoughts

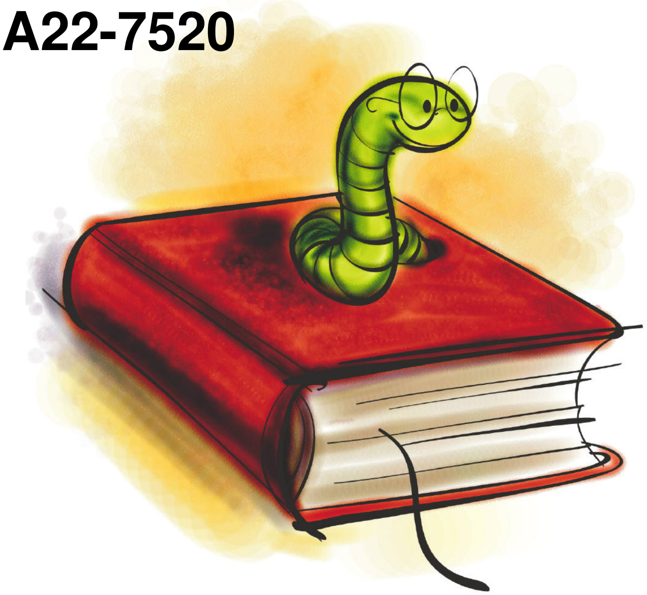
- **Encryption has a cost**
  - Crypto hardware more efficient with large blocks of data
- **Secure Key on a PCI Card – longer pathlength**
- **Clear Key exists in the DB2 Address Space, Protected Key and Secure Key are too, but they are stored encrypted under the Wrapping Key or Master Key**

References

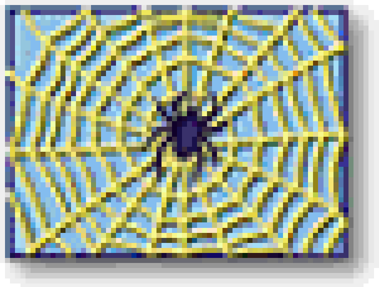
- **Cryptography Books**
  - Bruce Schneier, 'Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in "C"', Addison Wesley Longman, Inc., 1997
  - Simon Singh, 'The Code Book', Anchor Books, 1999
  - Niels Ferguson, Bruce Schneier, 'Practical Cryptography', Wiley Publishing, Inc. 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 System z10 Enterprise Class Technical Guide, SG74-7516
  - IBM System z10 Enterprise Class Configuration Setup, SG24-7571
  - IBM System z10 Business Class Technical Overview, SG24-7632
- **ATS TechDocs Web Site www.ibm.com/support/techdocs (Search All Documents for keyword of ‘Crypto’)**
  - WP100810 – A Synopsis of zSeries 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