Government regulations: Securing DB2 and IMS data in the System z environment

Ernie Mancill
Executive IT Specialist
DB2 for z/OS Tools

Information Management software

Disclaimer

The information contained in this presentation has not been submitted to any formal IBM review and is distributed on an "As Is" basis without any warranty either express or implied. The use of this information is a customer responsibility.

The measurement results presented here were run in a controlled laboratory environment using specific workloads. While the information here has been reviewed by IBM personnel for accuracy, there is no guarantee that the same or similar results will be obtained elsewhere. Performance results depend upon the workload and environment. Customers attempting to adapt this data to their own environments do so at their own risk.

In addition, the material in this presentation may be subject to enhancements or Programming Temporary Fixes (PTFs) subsequent to general availability of the code.

Agenda

- Introduction
  - Regulatory Landscape
  - So, what does a security breach cost me?
  - Security Needs
- System Z – Secure Platform for an insecure world
  - Z9 Foundation for Security
  - Z9 and z/OS Support for Encryption
- DB2 on z/OS Security Support
  - DB2 on z/OS V8 Multi-Row Security
  - DB2 on z/OS V9 Trusted Context and Roles
- IBM Enterprise Data Governance Software
  - Design, Create, and Test
  - Secure and Protect
  - Retain and Decommission
  - Monitor and Audit

Introduction:

Regulatory Landscape
What does a Data Breach mean to me?
Security needs – different things to different folks

Information Management software

Life is not easy…..

- **Basel II - Improve measurement of total risk and strengthen ability to determine capital needed**
- **Sarbanes-Oxley - Strengthen financial reporting, internal controls by fixing responsibility within companies' management**
- **HIPAA - Secure medical records (lifetime), prove how they have been used & who has used them**
- **Patriot Act - Prevent usage of the financial system to support illegal activities, particularly terrorism**
- **Various anti-money laundering (AML) - Prevent the laundering of money derived from illegal activities**
- **Gramm-Leach-Bliley - Protection of personally identifiable financial information**
- **Department of Defense - 5015.2**
  - requires certified application or technology to manage records (retention)
- **SEC Rule 17a-4**
  - requires brokers to preserve communications with clients (6 years)
- **Corporate Information Security Accountability Act of 2003**
  - requires audit of IT security and reporting
  - security infrastructures meet minimum standards

…Nor Getting Easier

- **California Bill 1386**
  - a bill that protects data concerning California Residents in all computers across the United States
- **European Union**
  - various countries are working on proposed bills to protect data concerning EU residents
- VISA and Mastercard PIC
  - Requires among other things data encryption of cardholder account number, PIN, etc.
- **... and more to come**

The Bottom Line – Improving Internal Control

Regulators have multiple goals. . .

- ✓ Security of the national and international services infrastructure
- ✓ Improved risk management across the enterprise
- ✓ Integrity of financial reporting processes and related business practices
- ✓ Customer information security

. . . which drive investment in several areas

- People: Professionals with regulatory experience will be hired to enable firms to meet and anticipate new regulatory requirements
- Process: More robust processes and procedures will enable top management to monitor and enhance regulatory compliance
- Technology: Significant investment will be made to do the following:
  - **Encrypt sensitive data**
  - **Protect sensitive production data**
  - **Save data for future audits and to comply with retention rules**
  - **Auditiability - discover who did what, where and when**
    - **Real time**
    - **Historically**
  - **Engage in real-time monitoring of operations**

So, what does a security breach cost me?

- Forensics
  - Initial breach detection and investigation
  - Assessment of damage and affected customer population
- Triage
  - Reporting the breach to internal population
  - Short term reaction to ensure immediate reaction to breach
- Treatment
  - Notification of breach to external regulatory agencies
  - Communication to breach subjects
- Recovery
  - Redress provided to customers affected by breach
  - Penalties and remediation dictated by external agencies
  - Long term solution to resolve source of breach

Forensics

- **With inadequate audit reporting and controls, detection and isolation of the source of data breach can be sometimes difficult.**
- **Without good instrumentation, some breach events might require assumptions as to the size of the affected customer population, expanding the scope of the remediation.**
- **Delayed or incomplete damage assessment may in itself lead to a higher level of impact to the business.**
- **Many organizations incur additional expense in having to retain outside assistance in the forensic analysis of the data breach.**

Triage/Breach Notification

- **Participants of project team to address downstream activities need to be identified. Impacts will occur to ongoing activities and existing projects due to critical nature of threat response and the immediate project team involvement.**
- **Difficult orchestration between project team and department responsible for coordinating external communication and customer relations**
- **Preparation of customer-facing departments in notification delivery and subsequent customer interactions:**
  - Call Center scripting and procedures
  - Timely Delivery of notification to affected customer population might involve multiple campaigns (email, phone, mailings)
- **Engage external expertise to assist in these processes**

Recovery

- Tangible Costs to the enterprise
  - Cost of notification campaign to affected customer base
  - Fines and financial penalties levied by regulators
  - Credit reporting costs
  - Reissuing credit instruments
  - Acquisition of technology and processes to redress breach
  - Gifts and concessions (compensation) to exposed customers
- Intangible Costs
  - Customer relationships terminated due lost confidence due to the breach
  - Target customer population who would have otherwise entered into a business relationship
  - Erosion of shareholder confidence
  - Diminished competitive standing in the marketplace
  - Legal redress by disenfranchised customer base
- Bottom line
  - Much more financially responsible to invest in compliance technology and processes before the breach occurs

Different People have different "security" needs

- Chief Information Officer
  - Are my systems and data protected from inadvertent disclosure?
  - Are best practices deployed for security?
  - Should I build or buy security?
- Chief Financial Officer
  - Total cost of ownership – how much does "security" cost?
  - What return on investment does this spending deliver?
  - What risks/costs does it avoid?
- Chief Privacy Officer/Chief Information Security Officer
  - Can I meet Regulatory Compliance needs?
  - Are our processes auditable?
  - Are my IT Operations, Developers, End users/consumers educated on our security practices?
- Application Architects
  - Do we design "security" into the application architecture, add it after the fact or leave it up to the IT Operations staff?
- IT Operations
  - What products and technologies will best meet the needs/requirements of all the "executives" that have a security/compliance/audit focus in the business?

System Z – A Secure Platform for an Insecure World

z9 - a Security Overview
zSeries Encryption Support

Information Management software

The Mainframe –
A History of Enterprise Security

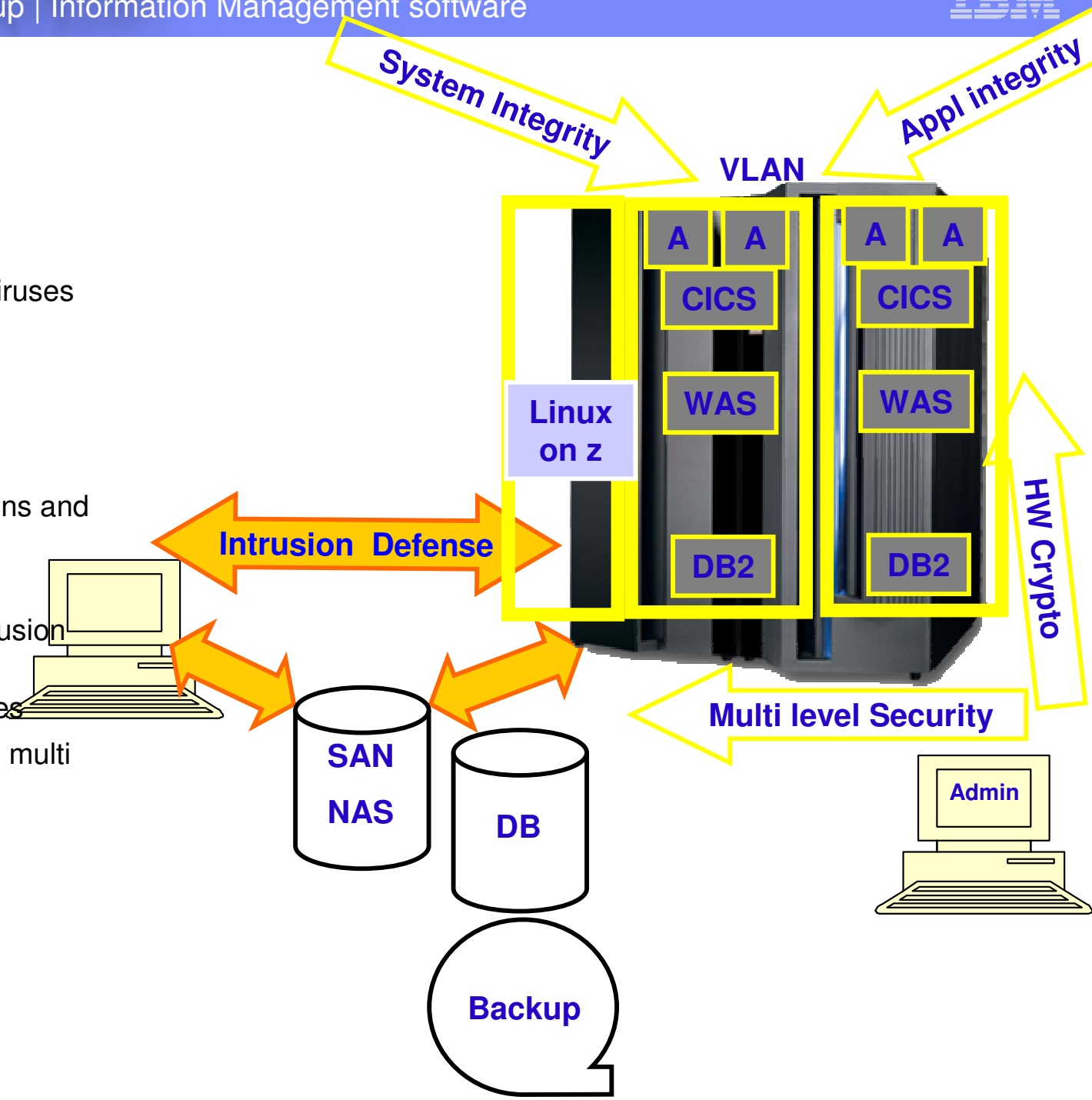
- Hardware Cryptography: 1970
- RACF: controls access to resources and applications – 1976
- Key management built into operating system (ICSF) – 1991
- Security Applications: Tivoli & Leading Software Vendors
- Intrusion Detection Services (IDS): 2001
- PKI: create digital certificates & act as Certificate Authority (CA) – 2002
- Multilevel Security (MLS): 2004
- Encryption Facility for z/OS: 2005
- Control Unit Tape Encryption – DR1120: 2006
- IPsec and assist with zIIP – Q3 2007

Protect sensitive information on line and off line
System z provides security without sacrificing responsiveness

- Protect the data
  - **End-to-end protection that helps keep data uncorrupted and uncompromised**
  - **Multiple Level Security for different levels of "need to know"**
- **Encrypt sensitive data**
- Prevent unauthorized access
  - **IBM Resource Access Control Facility – 25 years strong**
  - **Support for a variety of encryption algorithms**
  - **EAL5 and other security certifications**
- Secure and speed the transaction
  - **Specialized Cryptographic co-processor hardware**
- Monitor, manage, and control
  - **Centralized access and control helps lower security costs, meet compliance guidelines, and simplify audit trail.**
- Compliance with privacy/security legislation
  - **Auditability**
  - **Control**
  - **Recoverability**
- Solutions available
  - **DM tools from IBM**
  - **Tivoli Consul InSight**

zSeries Architecture value

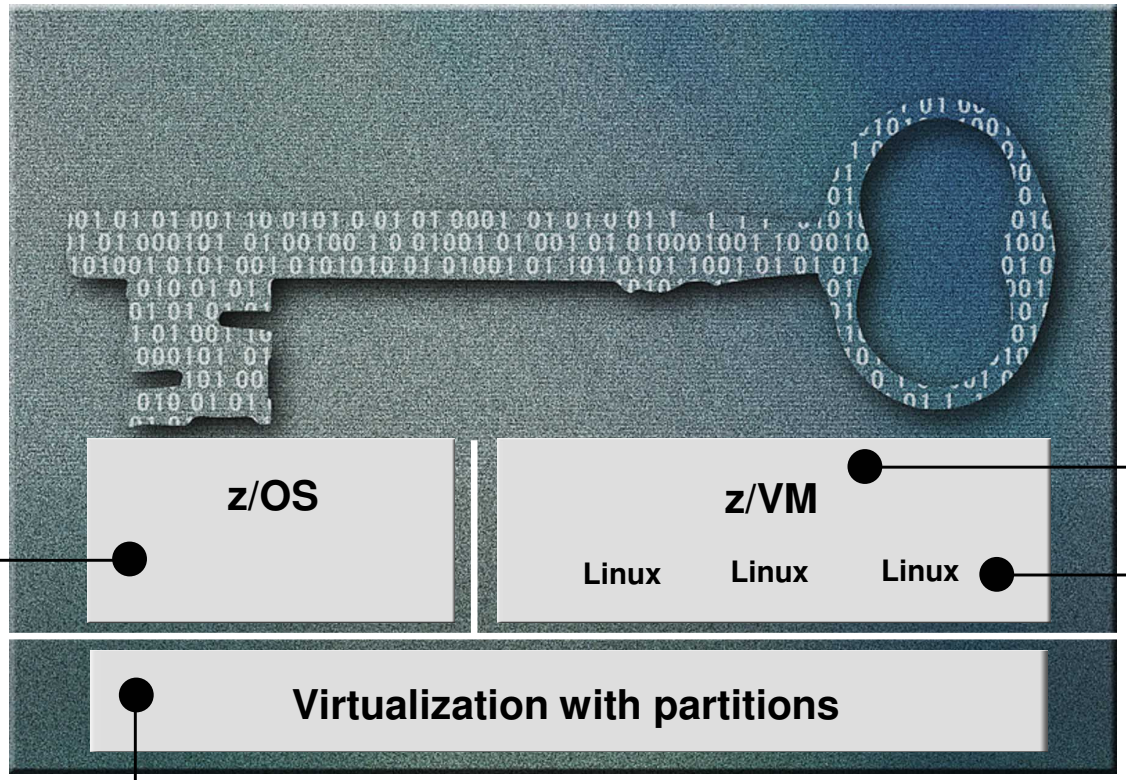
- System & Application Integrity
  - z/OS integrity statement
  - Inhibits trojan horses, worms & viruses via storage protection keys
  - Business Process Integration
  - Business Resilience
- Compartmentalization of work
  - Common Criteria certified partitions and guest isolation
  - Workload management
  - Virtual LANs reduce Security intrusion points
  - Middleware deployment processes
  - Row based security for DB2 and multi level security
- Data Confidentiality
  - Hardware encryption services
  - Encryption Key Management



Certification of mainframe products and components

Certifications on System z

The Common Criteria program developed by NIST and NSA establishes an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles



z/OS

- **Common Criteria** EAL4+ with CAPP and LSPP
  - z/OS 1.7 + RACF
- **IdenTrust™** certification for z/OS PKI Services

z/VM

- **Common Criteria** EAL3+ with CAPP and LSPP
  - **z/VM 5.1 + RACF**

Linux on System z

- **Common Criteria** EAL4+ with CAPP and LSPP
  - **SUSE LES9 certified**
- **Common Criteria** EAL3+ with CAPP and LSPP
  - **Red Hat EL3 certified at EAL3+**
  - **Red Hat EL4 EAL4+ in progress**

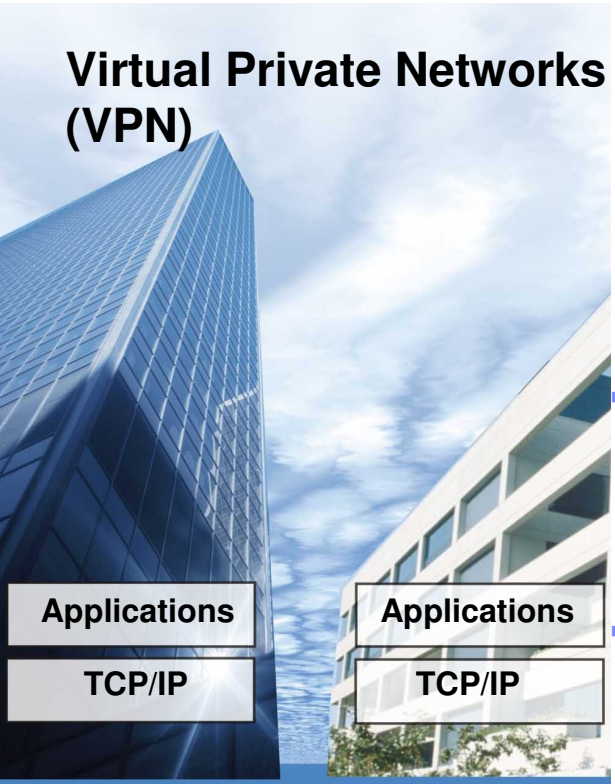
System z EC and other System z servers

- **Common Criteria** EAL5 with specific Target of Evaluation
  - **Logical partitions**
- FIPS 140-2 level 4
  - Crypto Express 2

See: www.**ibm.com**/security/standards/st_evaluations.shtml

Network security – encryption over the Internet

Help secure access from the Internet



- Application-layer encryption with SSL and TLS
  - Encryption acceleration provided in each engine on System z server
    - Support for up to 6000 SSL handshakes per second*
  - Help reduce development complexity and costs with Application Transparent TLS (z/OS 1.7)
    - Define a TLS or SSL secured connection with no anticipated changes to existing applications
  - DB2 V9 DRDA requestors encryption exploitation
- Network layer encryption with IPsec
  - Allows secure tunnel between two locations (Virtual Private Network)
  - Improved scale and performance in z/OS 1.7
- Simpler and consistent configuration of the above technologies
  - *z/OS Network Security Configuration Assistant*

*** In a recent test using a System z9 with four CPs and both PCI-X adapters configured as accelerators with the Crypto Express2 feature**

Mainframe uses latest technologies to help protect exchanges over the Internet

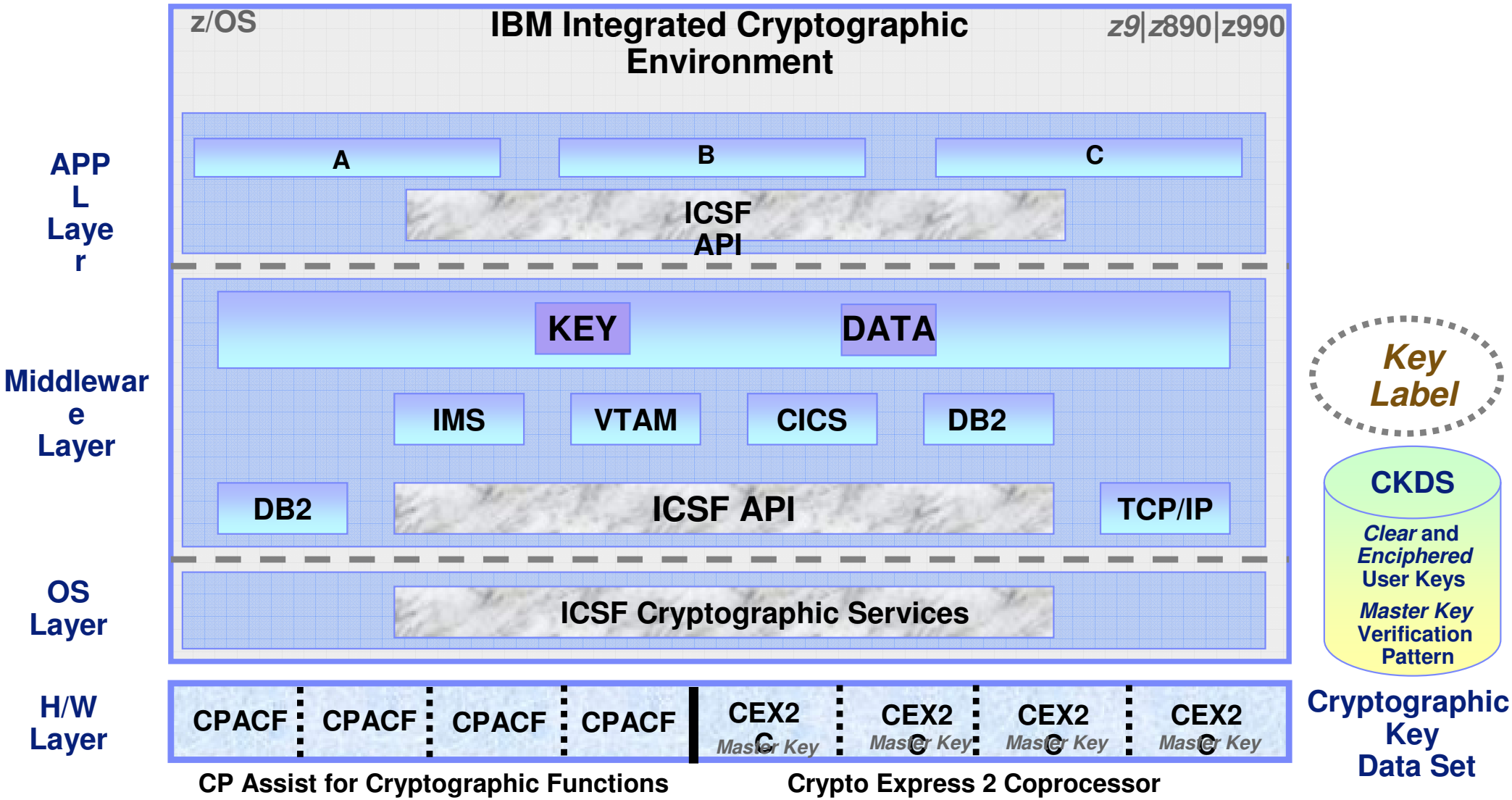
IBM z Series Encryption Support

Encrypt sensitive data

Integrated Cryptographic Service Facility (ICSF)

- z/OS Integrated Software Support for Data Encryption
- Enhanced Key Management (Cryptographic Key Data Set (CKDS) Key Repository)
  - Key Creation and Distribution
    - Public and Private Keys
    - Secure and Clear Keys
    - Master Keys
  - Unique *Key Label* (Key Alias) Indexes each Key stored in the CKDS
- Access Control for CKDS via Security Access Facility (SAF)
  - Control access to ICSF Callable Services
  - Control access to *Key Labels* (Key Alias) stored in the CKDS
- ICSF Software Implementation of AES (z9 CPACF)
- Operating System S/W API Interface to Cryptographic Hardware
- Procedures for creating Installation-Defined Callable Services (UDX)

IBM Encryption Flow



CP Assist for Cryptographic Functions

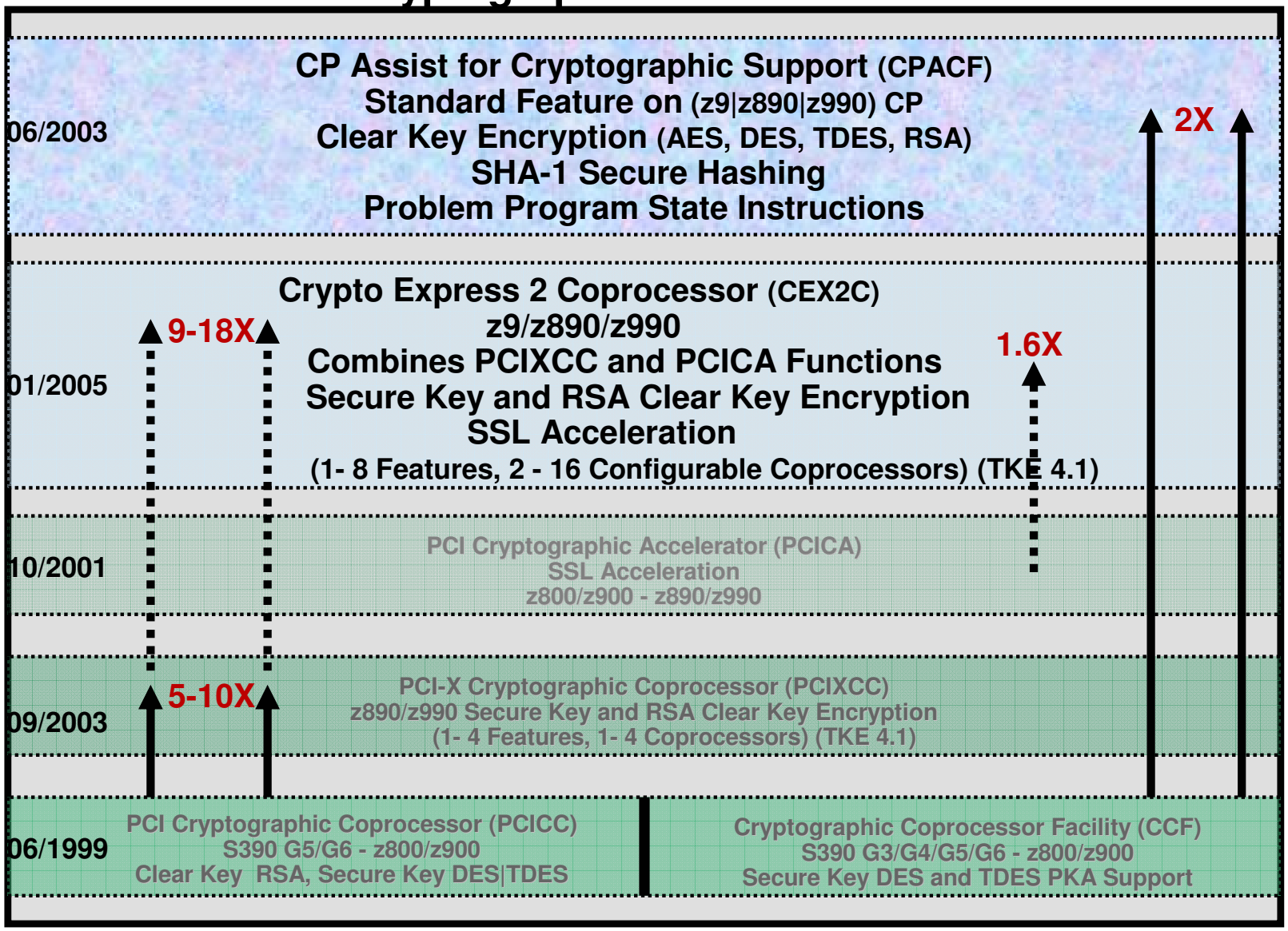
- Problem State Instructions
- Clear Keys Only
- DES/TDES Encryption
- AES (128 Bit)
- SHA-1 (256 on z9)

Crypto Express 2 Coprocessor

- ICSF Access Only (Key 0)
- Master Key Stored Within Boundary of Crypto Express 2 Feature
- Secure Key DES/TDES Encryption
- SSL Accelerator
- Tamper Resistant

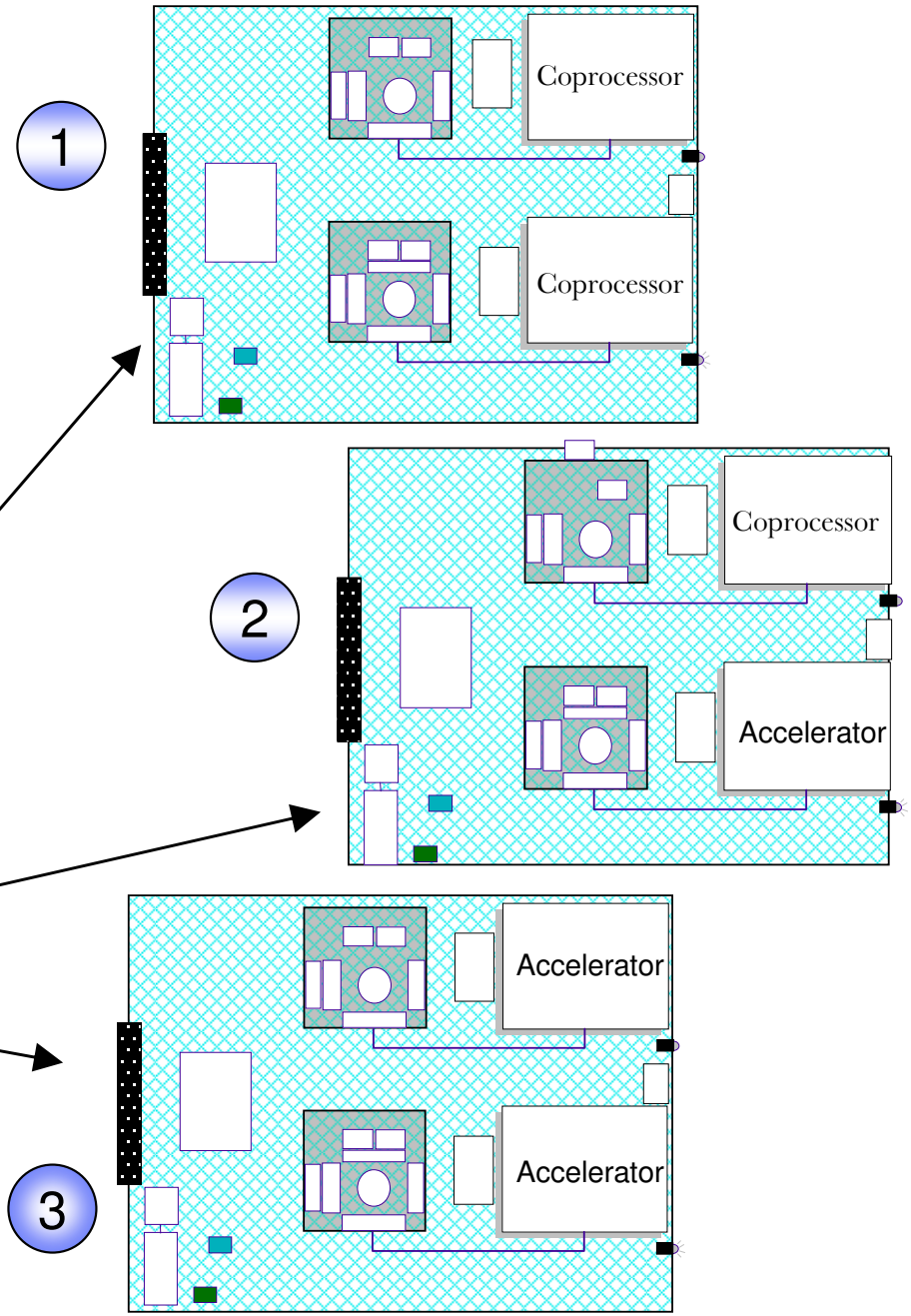
zSeries H/W Support for Data Encryption

zSeries Cryptographic Functional Evolution



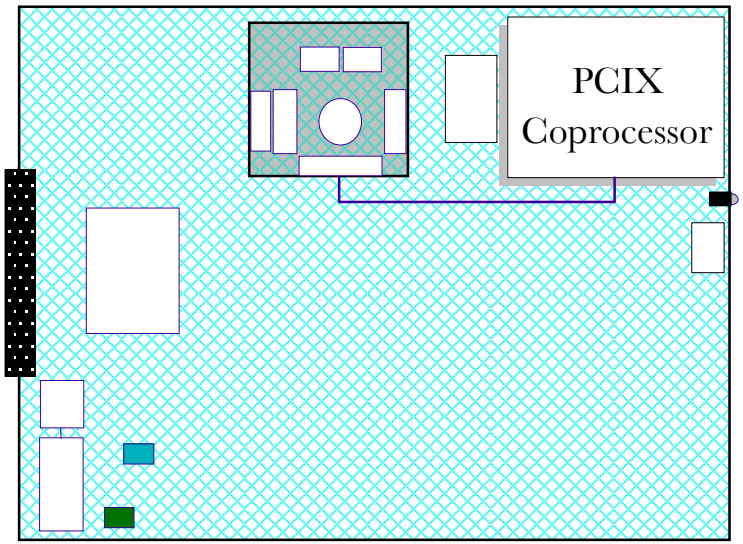
System z9 Cryptographic Support Summary

- **CP Assist for Cryptographic Function (CPACF)**
  - Standard on every CP and IFL
  - Supports DES, TDES and SHA-1
  - New to System z9
    - Advanced Encryption Standard (AES)
    - Secure Hash Algorithm – 256 (SHA-256)
    - Pseudo Random Number Generation (PRNG)
- **Crypto Express2**
  - Two configuration modes
    - Coprocessor (default)
      - Federal Information Processing Standard (FIPS) 140-2 Level 4 certified
    - Accelerator (configured from the HMC)
  - Three configuration options
    - Default set to Coprocessor
- **TKE workstation with 5.0 level of LIC**
  - Supports configurable Crypto Express2 feature
  - New Graphical User Interface (GUI)
  - Smart Card Reader



System z9 BC Crypto Express2-1P

- **Single Integrated Cryptographic Coprocessor**
  - Configurable on the HMC as:
    - Secure Coprocessor (default), designed to provide both "Secure key" and "Public key" function
    - Accelerator designed to provide only "Public key" function with enhanced performance
  - Applications expected to run without change
- **Secure Coprocessor mode is fully programmable and supports User Defined Extensions (UDX)**
- **Scalable (no CP affinity) –**
  - Model S07 supports 0, 2, 3, 4, 5, 6, 7, or 8 Crypto Express2 features (but NOT 1 feature)
    Model R07 supports no more than 4 features
  - Single and dual Crypto Express2 features can be mixed
    - Two feature minimum can be one of each or two of either
  - Plugs into an I/O card slot (no external cables)
- **Designed for FIPS 140-2 Level 4 Certification**



FC #0870

Note: Can not be carried forward from a z9 BC Model S07 on an upgrade to a z9 EC

Mainframe Innovation: Specialty Engines

IBM System z9 Integrated Information Processor (IBM zIIP) 2006

Eligible for zIIP:

- DB2® remote access and BI/DW
- ISVs
- New! IPSec encryption
- z/OS XML (SOD)*

System z Application Assist Processor (zAAP) 2004

Eligible for zAAP:

- Java™ execution environment
- z/OS XML (SOD)*

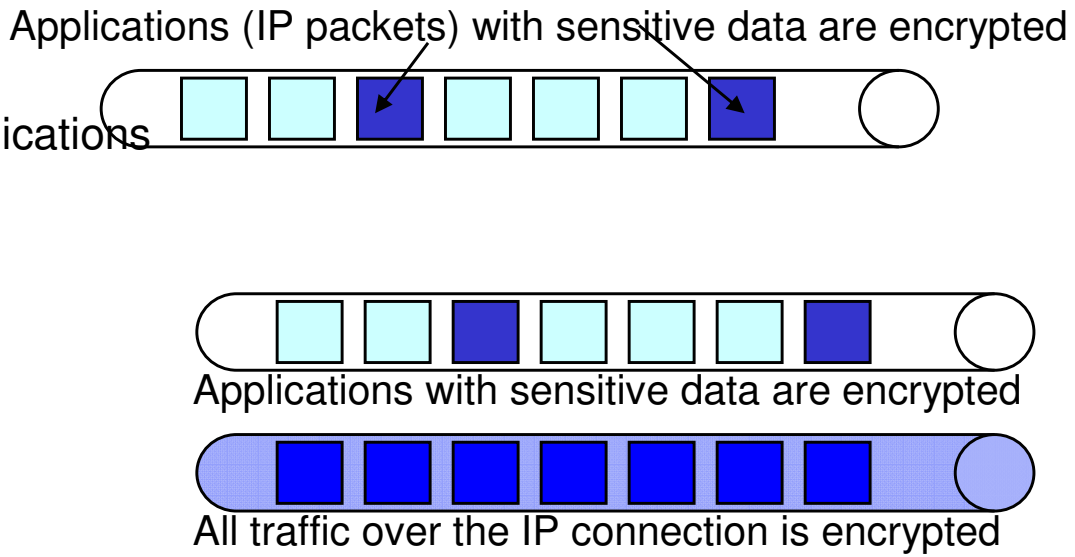
Integrated Facility for Linux (IFL) 2000

Internal Coupling Facility (ICF) 1997

What is IPSec?

- **What is IPSec?**
  - IPSec (IP security) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream. IPSec also includes protocols for cryptographic key establishment.
  - IPSec helps enable secure tunnels between two IP entities –Virtual Private Network.
  - Helps provide end-to-end network encryption

- **Why is it important?**
  - Some encryption technologies are application-specific
    - SSL, Open SSH, AT-TLS encrypt applications with sensitive data
  - IPSec is designed to encrypt specific applications
  - OR IPSec can encrypt all traffic over an IP connection :
    - Server, client, printer, disk, remote data center, to branch office... to any IP node that is IPSec compliant



IBM Data Encryption for IMS and DB2 Databases (5799-GWD)

Standard DB2 EDITPROC for Accessing Cryptographic Functions

- All Supported DB2 Versions
- Member of IBM IMS | DB2 Tools Family of Products
- Pre-coded EDITPROC for encryption of DB2® Data
- Encryption/Decryption occurs at the DB2 Row Level
- Unique EDITPROC can be defined for each DB2 Table
- Exploits z/OS Integrated Cryptographic Service Facility (ICSF)
- Exploits zSeries CPACF Cryptographic Hardware Directly
- Requires no changes to your applications
- Fast implementation

Edit Procedures (EDITPROC) are Programs That:

- Transform Data on INSERT | UPDATE | LOAD
- Restore Data to Original Format on SELECT
- Transformations on Entire ROW
- Supported by Utilities
- Implemented via Create Table specification
- Requires unload/load of data

EDITPROC – Definition

- **Edit procedures are simply programs that transform data on insertion and convert the data to its original format on subsequent retrieval. One edit procedure for compressing data, DSN8HUFF, is supplied with DB2. Additional EDITPROCs must be developed by the DB2 user. They are ideal for implementing data compression routines and data encryption.**

- **Implemented via Create Table Statement:**

```
CREATE TABLE DSN8710.EMP
    ....
    EDITPROC DSN8EAE1
    IN DSN8D71A.DSN8S71E
    CCSID EBCDIC;
```

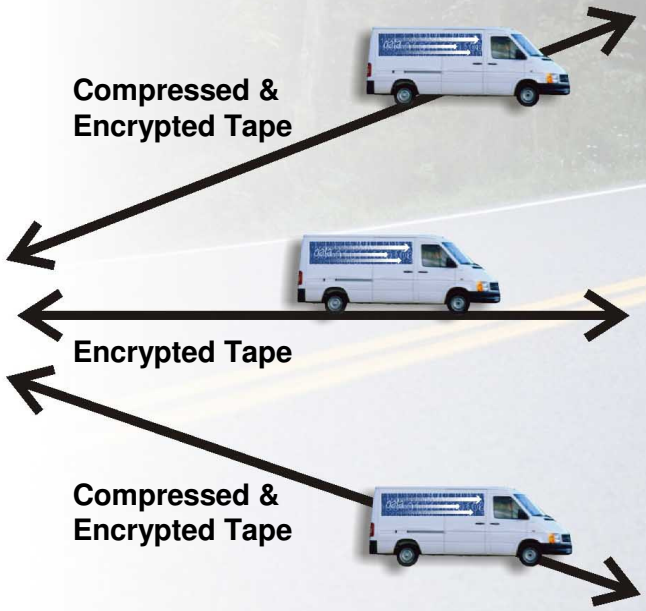
IBM Data Encryption for IMS and DB2 Databases Summary

- Configure the Integrated Cryptographic Service Facility (ICSF)
- Enable Crypto Express 2 Coprocessor Feature(s) (CEX2C) (z9/z890/z990)
  (This Feature subject to US Export Restrictions)
- Generate and store in the Cryptographic Key Data Set (CKDS) Key Labels
- Build the IMS User Exit or DB2 EDITPROC
  - For IMS use the Sample JCL Provided or the ISPF Panels
  - For DB2 use the ISPF Panels
  - For IMS Custom Built Exits follow Instructions outlined in:
    - ICSF Application Programmers Guide (SA22-7522)
    - IMS Customization guide (SC18-7817)
    - IMS Utilities Reference System (SC18-7834)
- Back - Up and Unload Databases
- Create Exits for IMS or EDITPROCS for DB2
- Reload the Databases: Data Bases will be Encrypted
- Validate your Output

Extending Mainframe Encryption

Encryption Facility for z/OS V1.2

Centralized
Key Management




Partner, customers, branch office with z/OS mainframe


Partners, customers


Archiving

Encrypt and decrypt with Java client

Mainframe Encryption Services

Encryption hardware

Centralized key management

Encryption standards (AES, TDES, SHA-256)

IBM Encryption Facility for z/OS, 1.2

Licensed Program Product
MSU-based pricing*

Runs on the following servers: System z9 109 (z9-109), or equivalent
zSeries z900 or z990, or equivalent
zSeries z800 or z890, or equivalent

Requires: z/OS V1.4 or higher z/OS.e V1.4 or higher

Feature: *Encryption Services*

Optional Priced Feature*

Encryption Facility Client

Web download

Feature: *DFSMSdss Encryption*

Optional Priced Feature*

- **Supports encrypting and decrypting of data at rest (tapes, disk)**
- **Supports either Public Key/Private keys or passwords to create highly-secure exchange between partners**
- **Java technology-based code that allows client systems to decrypt and encrypts data for exchange with z/OS systems**
- **Allows encryption and compression of DUMP data sets created by DFSMSdss**
- **Supports decryption and decompression during RESTORE**

* Variable Workload License Charges (VWLC), Entry Workload License Charges (EWLC), zSeries Entry License Charges™ (zELC), Parallel Sysplex License Charges (PSLC)

DB2 V8 on z/OS : Multi-row Security
DB2 V9 on z/OS : Trusted Context and Roles

Access for “need to know” only

Multilevel Security

Provide access to data based on need to know

REQUIREMENT:

Data shared between people/organizations with different "need to know"

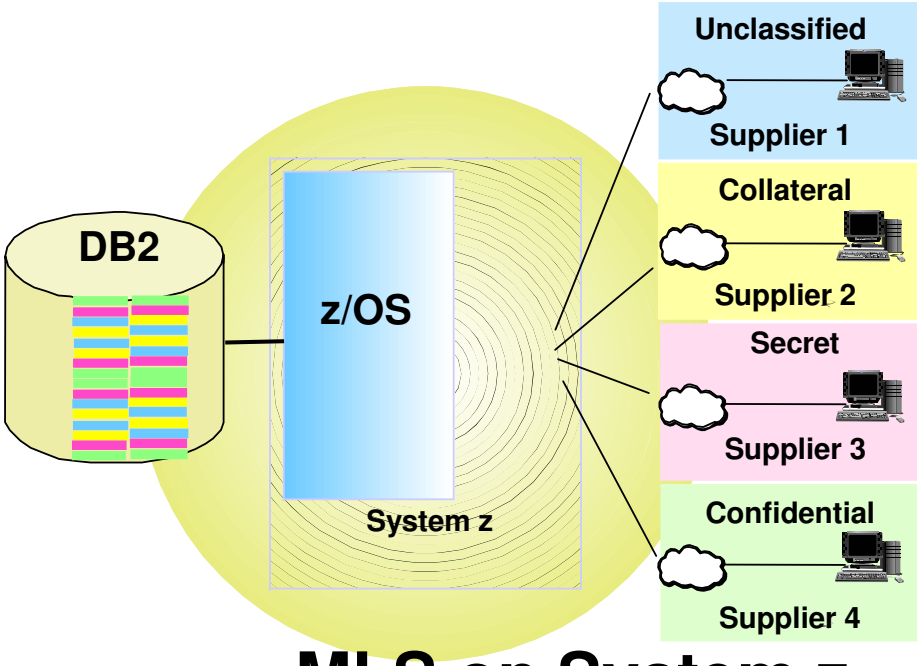
System z solution:

- **Highly secure access to DB2 databases**
- **Security labeling at the row-level of DB2**
- **With RACF as single security manager for both z/OS and DB2**

Public Sector: Hierarchical security

Commercial opportunities:

- Hosting similar applications
- Single database
  - **hosting subsidiaries**
  - **hosting partners**



MLS on System z

DB2 MLS

- **Rows in a DB2 table have a security label associated with them by means of a special column of the table that contains only the 8-character security label that defines the security classification of each row in that table.**
- **New attribute 'AS SECURITY LABEL'**
- **Table has column defined AS SECURITY LABEL**
  - Each row value has a specific security label
  - Get security labels from RACF
  - Save in rows for INSERT, UPDATE, LOAD, ...
- **Check for each new seclabel value accessed**
  - If access is allowed, then normal access
  - If access is not allowed, data not returned
- **Runtime user to data checking**
- **Seclabel values are cached to minimize cpu**
- **Requires z/OS V1R5 and Security Server (RACF)**

Role and Trusted Context - Existing challenges

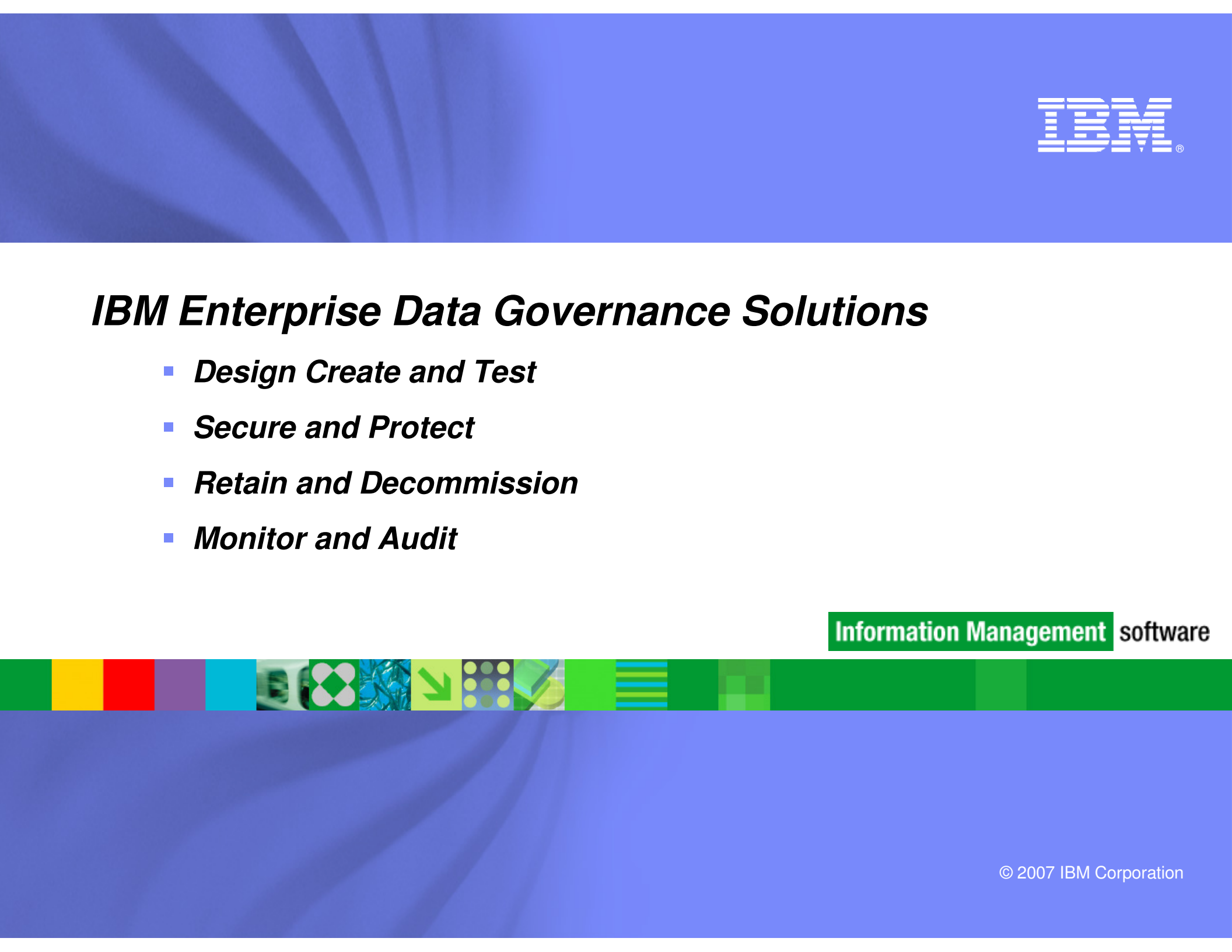
- **Single ID has all privileges (administrative + Business User). If stolen significant exposure**
- **As Business user authentication done by middleware, DB2 does not know who does what, e.g. “admin” vs “end user”. Lack of accountability/auditability**
- **Trust all connection requests?**
  - Parm applies to all, means no authentication, not practical
  - Lack of already verified option inhibited migration from SNA to TCP/IP
- **Shared SYSADM ID or DBADM ID to avoid cascading effect when someone leaves unit**
  - **Create view for another but cannot alter it**
  - **Privileges granted can be exercised from anywhere**
  - **Full time DBA access to all prod data AND sensitive/private data**
  - **Privileges always available to DBA**
  - **Dual responsibilities (prod + dev) can lead to mistakes**

Trusted context functional overview

- Trusted context addresses the problem of establishing a trusted relationship between DB2 and an external entity, such as a middleware server.
- A series of trust attributes are evaluated at connect time to determine if a specific connection is to be trusted.
- The relationship between a connection and a trusted context is established when a connection to the server is first created
- Once established, a trusted connection provides the ability to:
  - Use the trusted connection for a different user without authentication.
  - Acquire special set of privileges by an authorization ID, that are not available to it outside the trusted context. This is accomplished by associating a role with the trusted context.
  - Allow a role to own objects, if objects are created in a trusted context with role defined as the owner.
- Trusted context provides:
  - User accountability
  - Improved Security and Manageability
  - Ability of DBADM to perform DDL on behalf of others via database role

Database role functional overview

- Can optionally be the owner of DB2 objects. A ROLE can be dropped if it owns no objects
- Removing a person's ROLE does not cause the objects to be cascade deleted
- Role is independent of it's creator. Allows a DBA to have privileges to create objects and manage them for a time, even though ownership is to be another id.
- Without roles, transferring ownership implies drop/recreate
- Implement on weekend, privileges no longer available on Monday morning
- Roles are a way to allow multiple DBA authids to have ownership of an object at the same time or at different times
- An example, how to secure privliged access via ROLE:
  - Grant DBA privileges to a ROLE
  - At the point where an application change needs to be implemented by DBA:
  - Assign DBA ROLE to DBA via trusted context
  - Via V9 audit trace filtering, start audit trace of the ROLE
  - DBA is performs necessary object change activity to support application change
  - Revoke Trusted Context assigned to DBA
  - Turn off audit trace and generate audit trace report
  - Review and store the audit trace report as necessary for compliance

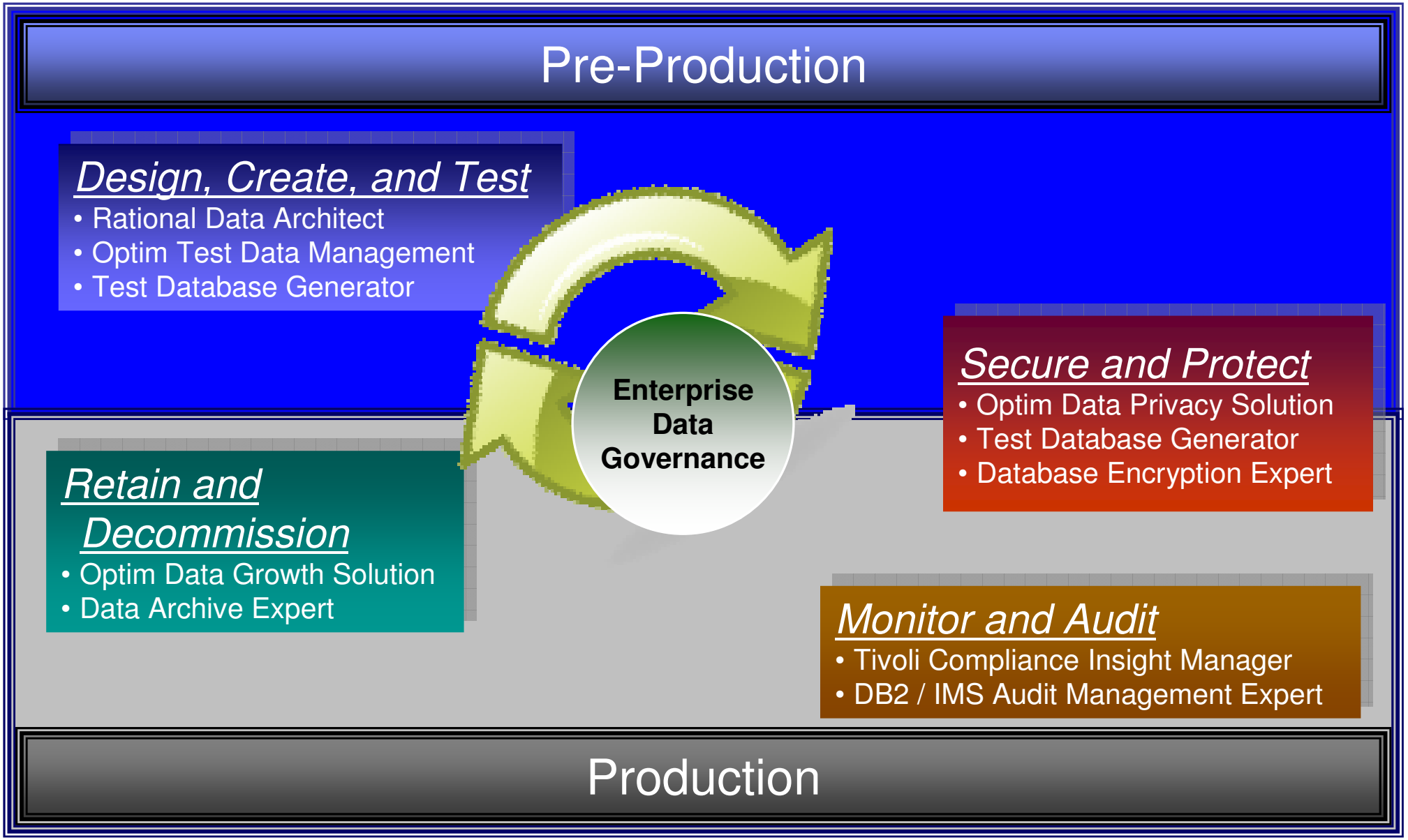


IBM Enterprise Data Governance Solutions

- *Design Create and Test*
- *Secure and Protect*
- *Retain and Decommission*
- *Monitor and Audit*

Information Management software

IBM Enterprise Data Governance Software



Enterprise Data Governance Solutions

- Design, Create and Test
  - Enterprise Data Governance begins at design
  - Design requires classifying, modeling and assigning stewardship
  - Testing requires cost-effective methods to obtain realistic test data

Design, Create, and Test
- ***Rational Data Architect***
- ***Optim Test Data Management***
- ***Test Database Generator***

- Rational Data Architect
  - Enables discovery, modeling and visualization of data assets
- Optim Test Data Management
  - Produce accurate testing results using the realistic test business objects for heterogeneous databases and/or packaged application environments
- DB2 Test Database Generator
  - Produce accurate testing results using the realistic test business objects for DB2

Enterprise Data Governance Solutions

- Secure and Protect
  - Preventing unauthorized access is critical to Enterprise Data Governance
  - Privacy protection ensures confidential and sensitive data is protected regardless of how the data is obtained

Secure and Protect
- Optim Data Privacy Solution
- Test Database Generator
- IBM Encryption Tool for DB2 and IMS Databases

- Optim Data Privacy Solution
  - Reduce the liability risk of exposing sensitive or confidential test data across heterogeneous databases and/or packaged application environments

- DB2 Test Database Generator
  - Reduce the liability risk of exposing sensitive or confidential DB2 test data

- IBM Encryption Tool for DB2 and IMS Databases
  - Prevents theft of confidential or sensitive DB2 data

Enterprise Data Governance Solutions

- Monitor and Audit
  - Prevent unauthorized access by monitoring database activity to identify any 'out of policy' situations
  - Support ongoing compliance procedures or special investigations by providing audit reports

Monitor and Audit
- Tivoli Compliance Insight Manager
- DB2 / IMS Audit Management Expert

- Tivoli Compliance Insight Manager
  - Enable compliance requirements with comprehensive auditing across the enterprise

- DB2 / IMS Audit Management Expert
  - Enable compliance requirements with detailed database auditing

Enterprise Data Governance Solutions

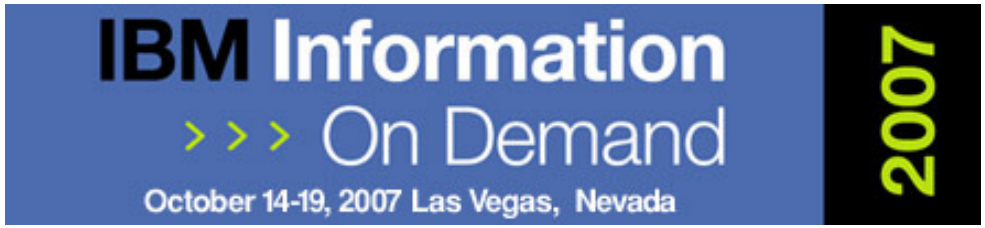
- Retain, Retrieve, Retire
  - Cost-effectively manage data growth
  - Ensure inactive data is not effecting performance of the active data

Retain and Decommission
- Optim Data Growth Solution
- Data Archive Expert

- Optim Data Growth Solution
  - Lower storage costs and improve performance by separating inactive from active data in heterogeneous databases and/or packaged application environments

- DB2 Data Archive Expert
  - Lower storage costs and improve performance by separating inactive from active DB2 data

Some sessions of interest



- *1019 Best Practices in DB2 Security - Roger Miller*
- *1148 Audit and Compliance for DB2 on z/OS and LUW - Dave Schwartz*
- *1346 A Deep Dive into the Mechanisms of DB2 9 for z/OS Security Enhancements - Dave Romack*
- *2317 DB2 for z/OS, IMS and Tools: Spotlight Keynote*
- *2293 DB2 and IMS Data Encryption Round Table - Ernie Mancill, et. al.*
- *1130 How to Secure IMS Resources - Maida Snapper*

Thank You for Joining Us today!

Go to **www.ibm.com/software/systemz** to:

- Replay this teleconference
- Replay previously broadcast teleconferences
- Register for upcoming events