Helping to Secure your Enterprise
IBM Mainframe Encryption

IMS-DB2
Data Encryption
with IBM Data Encryption for IMS and DB2 V1.1
(5799-GWD)

Ernie Mancill
Certified DB2 Technical Sales Specialist

James J Catchpole
IBM IMS Advanced Technical Support

ON DEMAND BUSINESS™

Agenda

Why Encrypt Your Data I

Security Headlines Daily

Is Anything More Important to the Success and Survival of Your Business?

More Than 90% Of Companies Regularly Expose Employee And Customer Data[1]

FBI – Businesses Reluctant To Report Cyber Attacks[2]

One In Four Identity-Theft Victims Never Fully Recover[3]

PCI: Card Associations Unite to Fight Fraud With Collaborative Standard[4]

1) Reconnex Insider Threat Index August 2005
2) 2005 CSI/FBI Computer Crime and Security Survey
3) Nationwide Mutual Insurance Co. Survey July 2005
4) Green Sheet Inc. August 2005 Issue 2

Why Encrypt Your Data II

Regulatory and Compliance Considerations

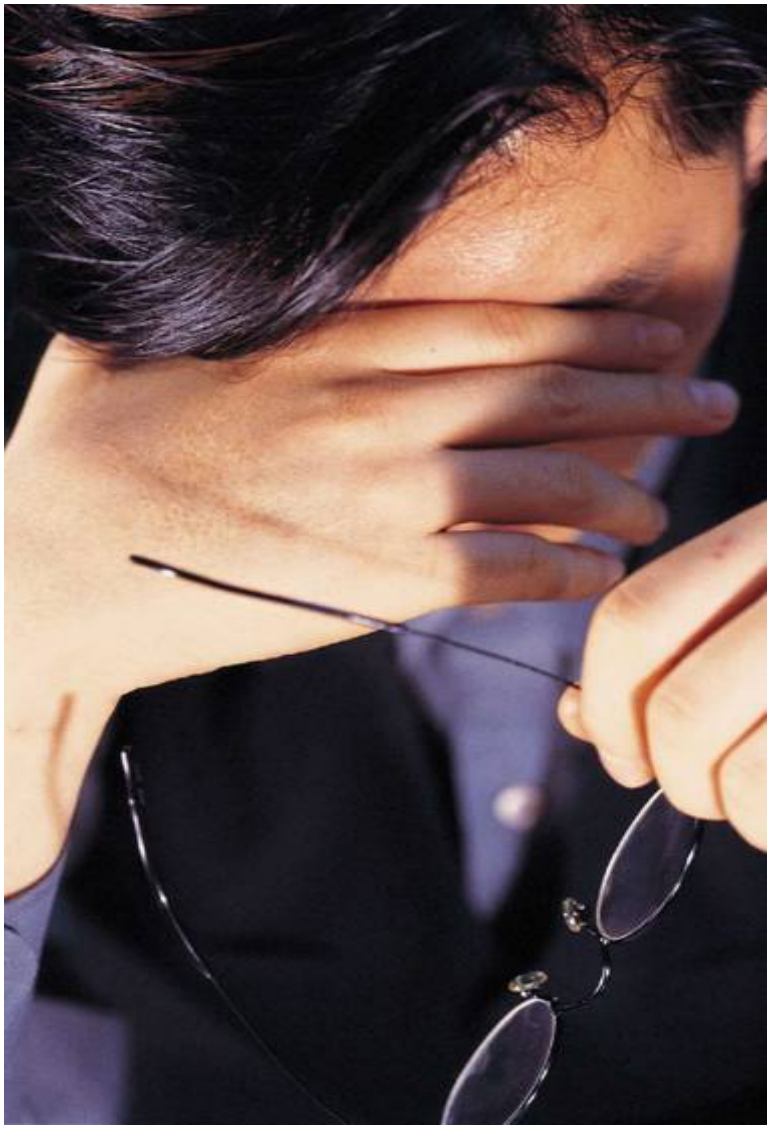
- Gramm-Leach-Bliley Financial Services Modernization Act (GLBA)
- Sarbanes Oxley (SOX)
- European Union Data Protection Directive (EUPA)
- International IT Security Standard (ISO 17799)

Why Encrypt Your Data III

Potential Costs of A Security Breach

- $ Cost of research and recovery
- $ Cost to notify customers
- $ Lost customers/business
- $ Problem solution or remediation
- $ Claims from trusted vendors and business partners

$$ Damage to Brand Image



Concepts of Cryptography I

- **Cryptography Scrambles or Disguises Information**
- **Available to Persons | Programs that can Unscramble the Information**

Concepts of Cryptography II

Only Cryptographic Services can Provide the Required

- **Identity and Authentication**
- **Data Confidentiality**
- **Non-Repudiation — assures that the appropriate individual sent the message**

Concepts of Cryptography III

- ***Enciphering*** **(Encryption) is converting *plaintext* into *cipher-text***
- ***Deciphering*** **(Decryption) converts *cipher-text* back into *plaintext***

Concepts of Cryptography IV

- **Most practical Cryptographic Systems combine two elements:**
  - **A *Process or Algorithm*: A set of rules that specify the steps needed to Encipher or Decipher Data**
  - **A *Cryptographic Key*: A string of numbers or characters used to select the *Algorithm* for Encrypting or Decrypting *Plaintext* and *Cipher-text***

Concept of Keys I

- ***Cryptographic Keys*** **are used for Encrypting and Decrypting** ***Plaintext*** **and** ***Cipher-Text***
- ***Cryptographic Keys are used*** **for Encrypting and Decrypting**
  - **Files, Databases, Logs, Image Copies, Backups, etc**
  - **Network Transmissions**

Concept of Keys II

Secret Keys

- Used when two parties (Person - Person, Program - Program, etc) want to exchange data
- Both parties must have access to the Secret Key
- IBM IMS|DB2 Data Encryption Tool Uses Secret Keys

Concept of Keys III

Public Keys (Asymmetric Keys)

- Each party in a *Public Key Cryptography System* has a pair of keys
- One key is *Public* and is published, the other key is *Secret*, known only to the owner
- Sending party looks up the receiving party's *Public Key* and uses it to encipher the data
- Receiving party uses its *Secret Key* to decipher the data

Concept of Keys IV

Clear - Secure Keys

- ***Clear Key*** **describes an unprotected Key Value; it is visible or exposed in some manner during the Encryption | Decryption process: (Example: System Memory)**
- ***Secure Key*** **describes a Key Value that must have its value protected from view during the Encryption | Decryption process**
- **A *Master Key* is used to Encipher | Decipher all *Secure Keys***

Concept of Keys Summary I

- ***Key Management*** **is required to ensure the integrity of Encrypted Data**
- ***Public Key*** **is published and Accessible to All**
- **Secret Key is known only to Owner and Authorized User**
- **Public-Key Encryption consists of a Secret Key and a Published Public Key**

Concept of Keys Summary II

- ***Clear Key*** **is an** ***Un-Enciphered Key*** **that is** ***Visible*** **during an Encryption | Decryption Process**
- ***Secure Key*** **is an** ***Enciphered Key*** **that is** ***Not-Visible*** **during an Encryption | Decryption Process**
- ***Master Key*** **is used to Encipher | Decipher all** ***Secure Keys***
- ***Master Key*** **is stored within a Secure, Tamper Resistant H/W Device**

Integrated Cryptographic Service Facility I (ICSF)

z/OS Integrated Software Support for H/W Data Encryption

- **Enhanced Key Management (Cryptographic Key Data Set (CKDS))**
  - **Key Creation and Distribution**
    - **Public and Secret Keys**
    - **Secure and Clear Keys**
    - **Master Keys in "Tamper-Resistant" Device**
    - **Key Recovery Capabilities**
  - **Unique *Key Labels* (Key Alias) Index stored in the CKDS**
  - **Digital Certificate API Support**

Integrated Cryptographic Service Facility II (ICSF)

z/OS Integrated Software Support for H/W Data Encryption

- 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
- S/W API Interface to Cryptographic Hardware
- Installation-Defined Callable Services (UDX)

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

- **Fast Implementation**
- **Requires no changes to Applications**
- **All Supported IMS | DB2 Versions**
- **Pre-Coded IMS Segment | Edit Compression Exit Used for Accessing Cryptographic Functions**
- **Pre-Coded DB2 EDITPROC Used for Accessing Cryptographic Functions**

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

- Encryption | Decryption occurs at the IMS Segment Level
- Encryption | Decryption occurs at the DB2 Table Level
- Exploits z/OS Integrated Cryptographic Service Facility (ICSF)
- Exploits zSeries Cryptographic H/W

IBM Encryption Facility for zOS
(z800 | z900 | z890 | z990 | z9)

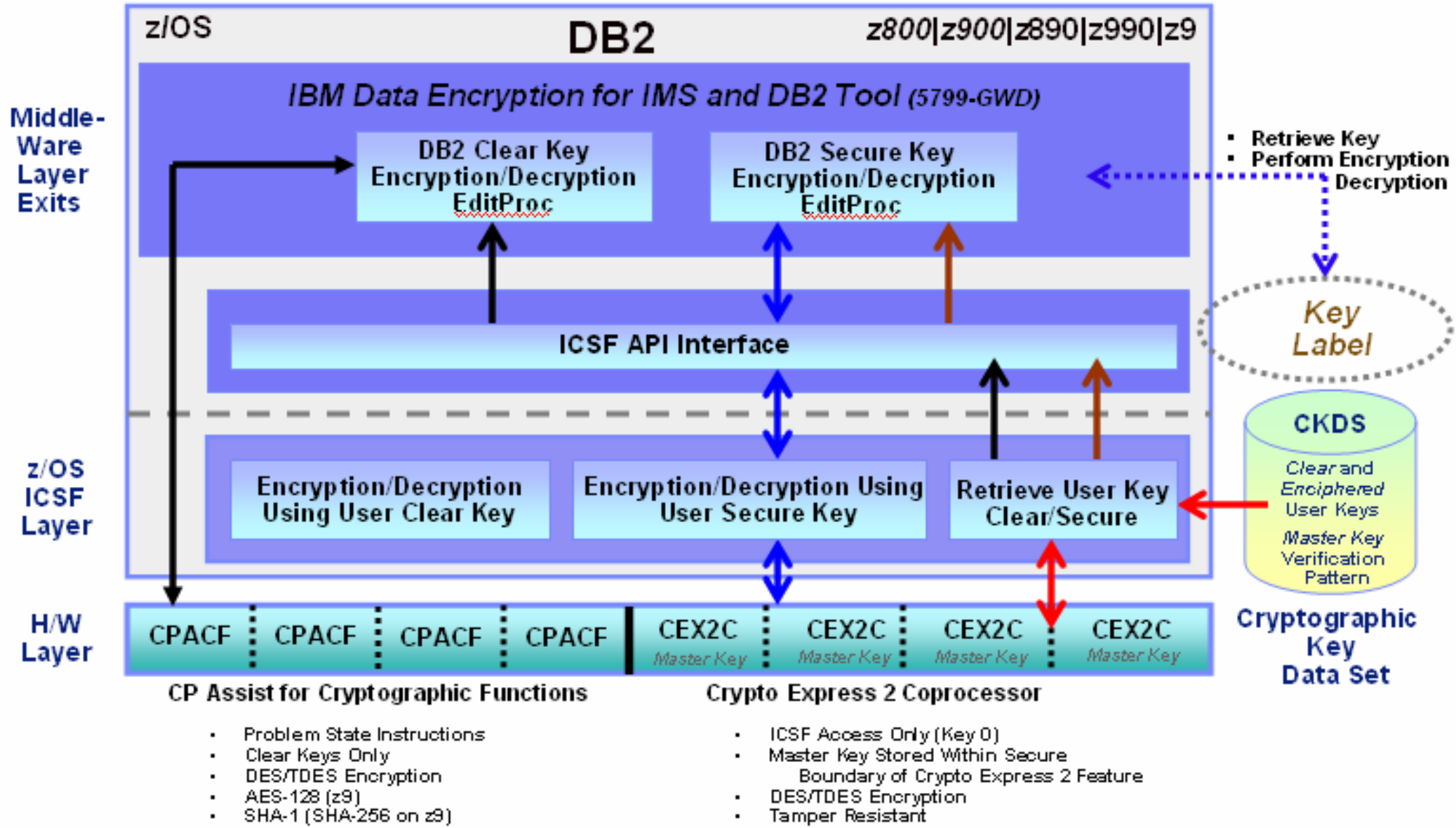
Enabling Encryption to Tape and Disk

- **Encryption Services**
  - Exploits ICSF Centralized Key Management
  - Encrypting | Decrypting 'Data at Rest'
    - Tapes
    - Disks
    - Encryption Facility Client (JAVA) allows Exchange of Tapes across Multiple Platforms
    - Compression and Encryption on zOS
    - PKI Key Support
    - Passwords
- **DFSMSxxx Encryption**
  - Encrypts | Decrypts Dump Data Set (Along with Compression)

DB2 Version 8 Built-In-Functions Data Encryption

- **Standard Feature of DB2 UDB Version 8**
- **Addresses Open Standards Requirements**
- **Built in Encryption Primitives for Application Programmer**
- **Requires Application Changes (Not Transparent)**
- **Encryption at the Column or Cell (Value) Level**

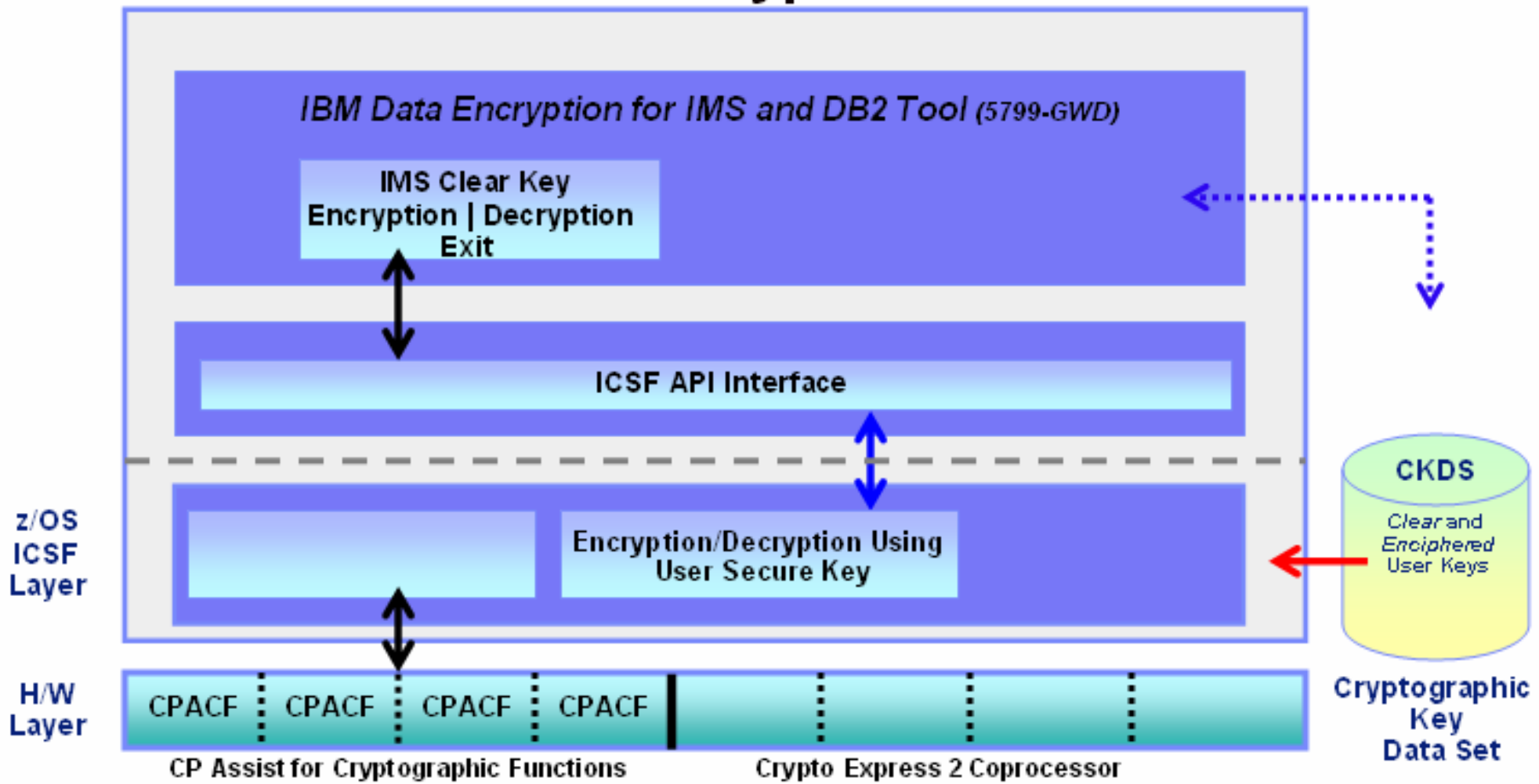
DB2 Data Encryption Flow



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

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

IMS Data Encryption Flow

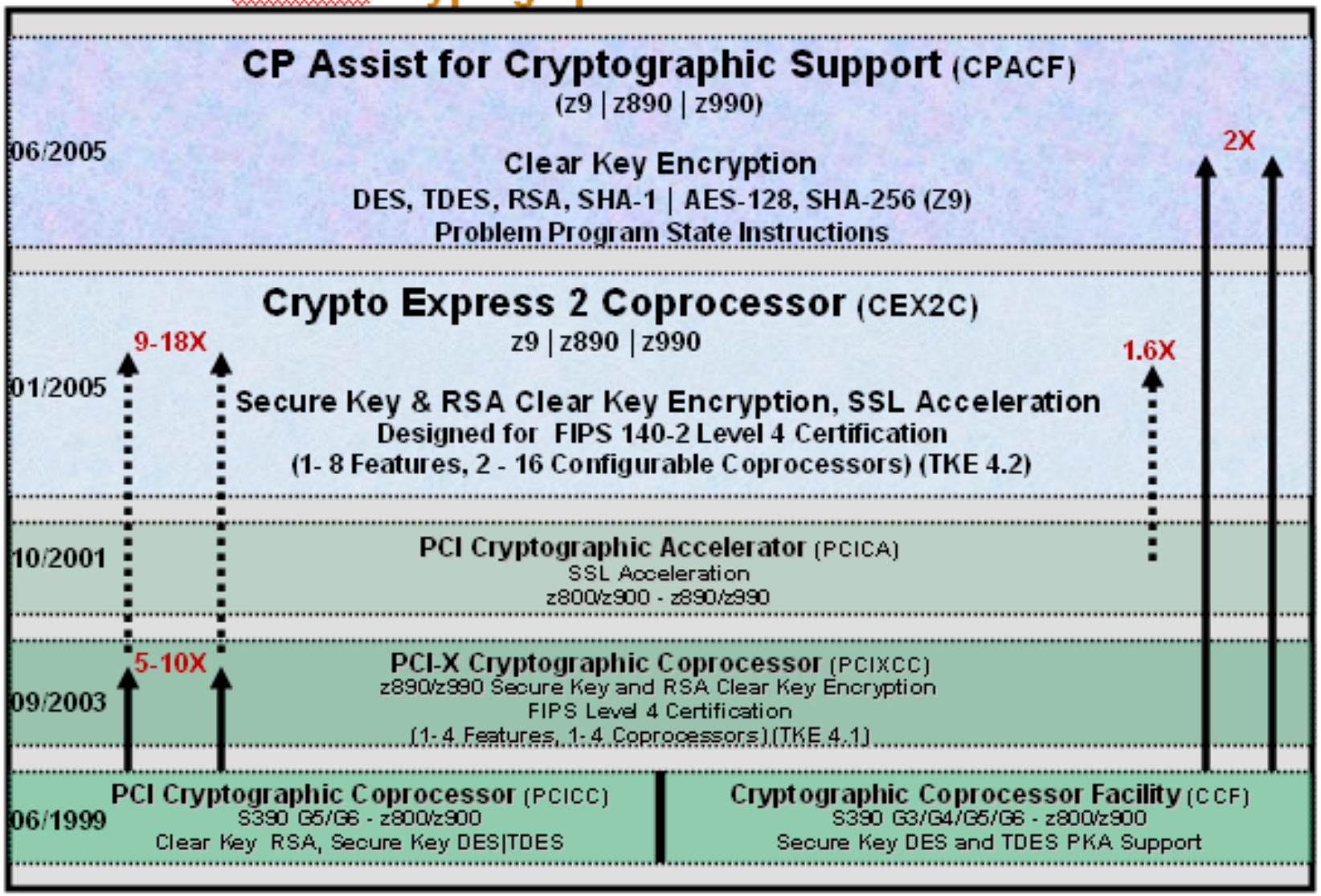


- Problem State Instructions
- Clear Keys Only
- DES/TDES Encryption
- AES-128 (z9)
- SHA-1 (SHA-256 on z9)

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

zSeries H/W Support for Data Encryption

zSeries Cryptographic Functional Evolution



IBM zSeries Cryptography Product Matrix

Features	Description	z9	z890	z990	z800	z900	s390
CPACF	CP Clear Key Encryption DES, TDES, RSA, SHA-1	X	X	X			
CPACF	CP Clear Key Encryption + AES-128, SHA-256	X					
CEX2C	Secure Key, SSL Tamper Resistant FIPS 140-2 Level 4	X	X	X			
PCIXCC	Secure Key Tamper Resistant FIPS 140-2 Level 4		X	X			
PCICC	Clear Key Encryption Secure Key encryption				X	X	X
PCICA	SSL Acceleration		X	X	X	X	
CCF	Secure Key Encryption				X	X	X

IBM Data Encryption Summary I

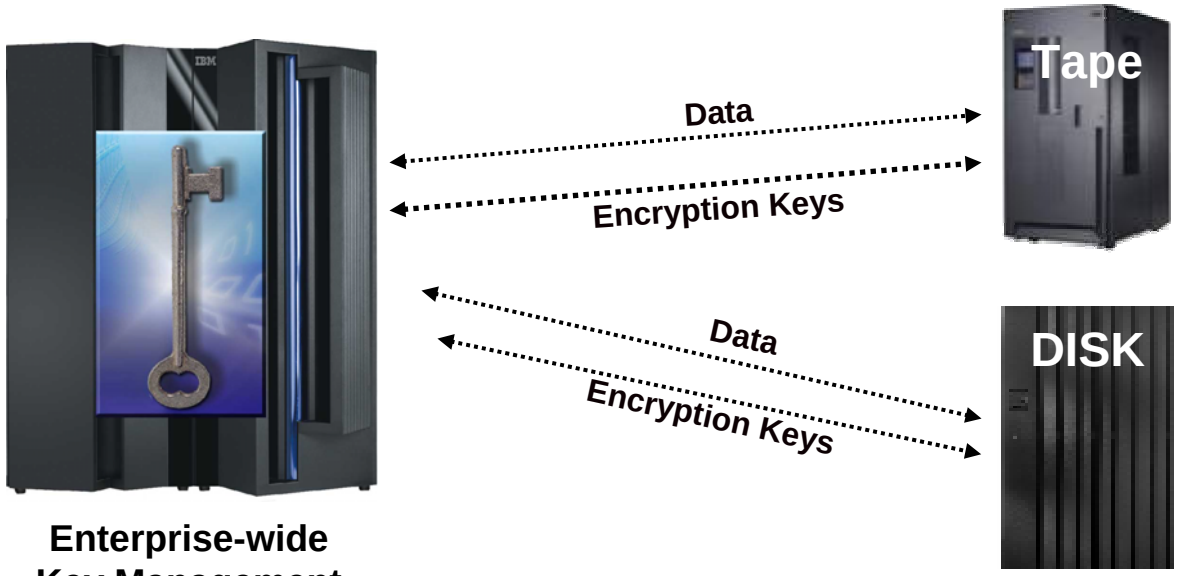
IBM has Long History of Cryptographic H/W and S/W

- zSeries z800 | z900 | z890 | z990 | z9 Continue H/W Evolution
- IBM Data Encryption IMS and DB2 Databases (5799-GWD)
- Integrated Cryptographic Service Facility (ICSF)
  - Key Management Functions
  - Access to H/W | S/W Encryption Facilities
- IBM Encryption Facility for zOS V1.1
- DB2 UDB V8 Built-In-Functions Data Encryption

IBM Data Encryption Summary II

Future Directions: Extending Encryption to IBM TotalStorage

- **Statement of Direction:**
  - **IBM is announcing a statement of direction for the development, enhancement and support of encryption capabilities within storage environments, such that the capability does not require the use of host server resources.**
  - **This includes the intent to offer, among other things, capabilities for products within the IBM TotalStorage portfolio to support outboard encryption and to leverage the centralized key management functions planned for z/OS ICSF.**



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

Publications

- IBM Data Encryption for IMS and DB2 Databases User's Guide (SC18-7336-02)
- IMS Version 8 Customization Guide (SC27-1294-05)
- IMS Version 9 Customization Guide (SC18-7817-00)
- DB2 UDB Version 8 for z/OS Administration Guide (SC18-7413-02)
- DB2 UDB Version 8 Application Programming and SQL Guide (SC18-7415-02)
- z/OS V1R6 ICSF Cryptographic Overview (SA22-7519-06)
- z/OS V1R6 ICSF Administrator's Guide (SA22-7521-07)
- z/OS V1R6 ICSF System Programmer's Guide (SA22-7520-07)
- z/OS V1R6 ICSF Application Programmer's Guide (SA22-7522-06)
- z/OS V1R6 ICSF TKE Workstation User's Guide (SA22-7524-07)
- Exploiting S/390 Hardware Cryptography with Trusted Key Entry (SG24-5455-00)