# IBM Encryption Facility for z/OS and Other Platforms

Ernest Nachtigall cissp;cisa

Vanguard Session B11

July 11, 2006

# Trademarks

**The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.**

IBM*
IBM eServer*
IBM logo*
CICS*
DB2*
Domino*
FICON*

GDPS*
Geographically Dispersed Parallel Sysplex
HiperSockets
HyperSwap
IMS
MQSeries*
Parallel Sysplex*

RACF*
Rational*
Redbooks
Resource Link
System z9
Tivoli*
Virtualization Engine

WebSphere*
z/OS*
z/VM*
zSeries*

* Registered trademarks of IBM Corporation

**The following are trademarks or registered trademarks of other companies.**

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States, other countries or both.
Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries
Linux is a trademark of Linus Torvalds in the United States and other countries..
UNIX is a registered trademark of The Open Group in the United States and other countries.
Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries.

* 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 ar e 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.

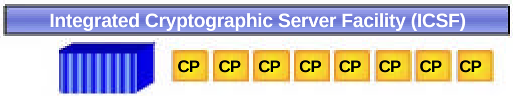
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products 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.

# Challenges

- Protecting the data from unauthorized access
  - RACF
  - Identification
    - PIN
    - Certificates
- Guarding the integrity of the data
  - Message authentication
  - HASHING
- Protecting disclosure of the information
  - Encryption

# Mainframe Encryption


Integrated Cryptographic Server Facility (ICSF)
CP
CP
CP
CP
CP
CP
CP
CP
Crypto Express2
CP Assist for Cryptographic Function

***Why IBM Mainframe encryption hardware?***

***To accelerate encryption and provide Secure Key services***

**Secure Key**

- For Secure Key exchanges
- Master keys in “tamper-resistant” package
- Dual control for Master Key management
- Important for banking functions
  - ✓ ATM support, Triple-DES, Trusted Key Entry
- Designed to comply with FIPS 140-2
- **CP Assist for Cryptographic Function** (z890, z990, z9-109)
- Support high levels of security for demanding applications
- Very high performance TDES, AES -128 (requires z9-109) and SHA-256 (requires z9-109)
  - ✓ SSL/TLS support

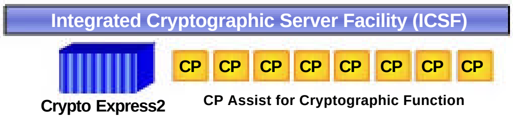
## Regulatory and Compliance Considerations

- Gramm-Leach-Bliley Financial Services Modernization Act (GLBA)
- Sarbanes Oxley (SOX)
- European Union Data Protection Directive (EUPA)
- International IT Security Standard (ISO 17799)
- California SB 1386
- New York Bill August 2005
- Ontario Bill 198
- PCI

## Examples:

- March 19, 2004 – CitiBank Japan loses tapes, put under government review
- February 28, 2005 – Bank of America loses tape with 1,200,000 accounts
- March 22, 2005 – Time Warner loses tape with information on 600,000 employees
- April 21, 2005 – Ameritrade loses tape with 200,000 clients information
- April 22, 2005 – Iron Mountain indicates 4 incidents of tape loss, suggests clients encrypt their tapes before archive
- January 2003 - IBM ISM reports theft of hard drive

## Mainframe Encryption


Integrated Cryptographic Server Facility (ICSF)
Crypto Express2
CP
CP
CP
CP
CP
CP
CP
CP
CP Assist for Cryptographic Function

***Why z/OS centralized key management?***

- Over a decade of production use

**Helps to protect and manage keys**

- Support of encryption standards
- Generates keys
- Manage based on customer policies
- Provides key recovery capabilities
- Uses tamper resistant hardware for “secure keys”

**Provides information for:**

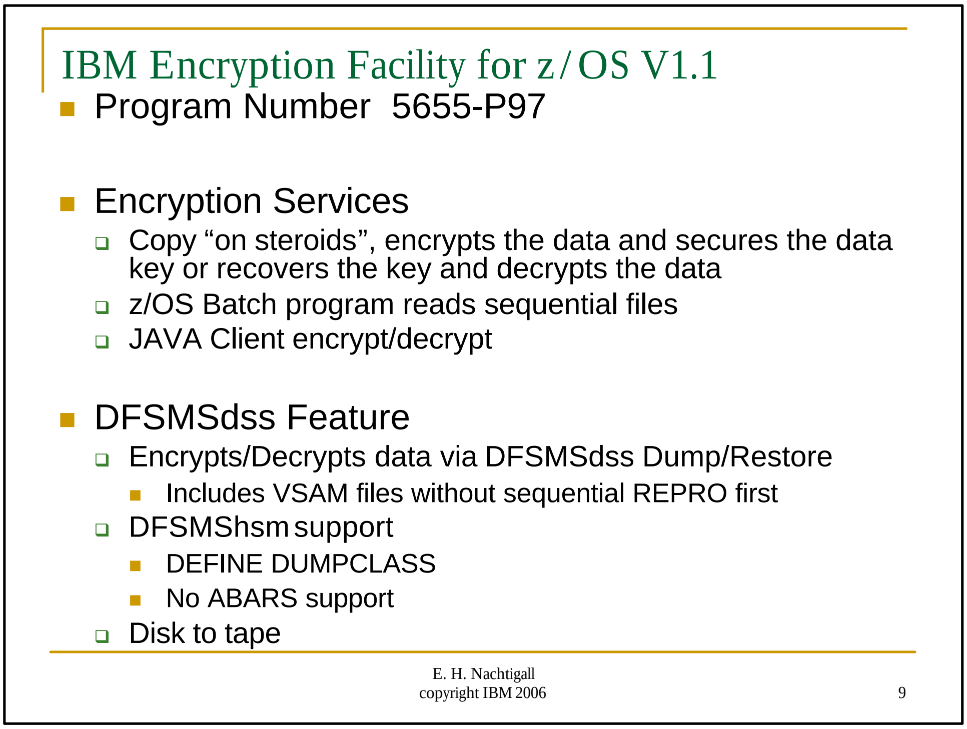
- Audit Compliance
- Management Controls
- Access Controls

**Integrates with z/OS security features:**

- z/OS  Digital Certificate hosting services
    - Customer can be their own certificate authority
    - Identrus certified  (z/OS 1.5)
- z/OS RACF for authorization, authentication

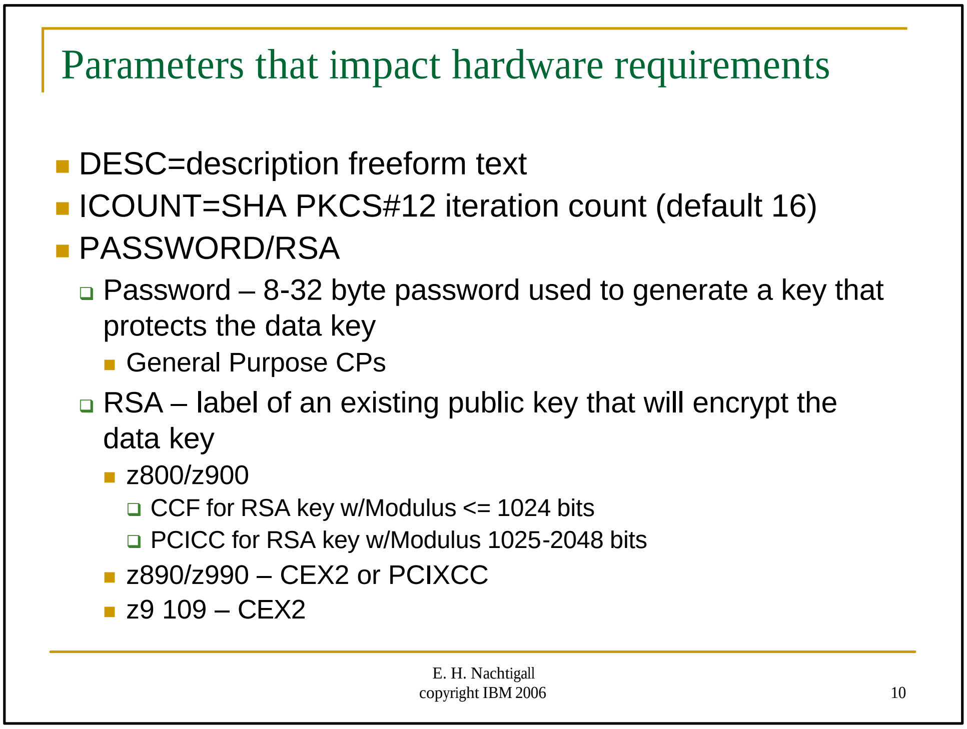
## Data Base Encryption

- **IBM** Data **Encryption** for **IMS** and **DB2** Databases 5655-P03
    - Encrypt DB2 rows and IMS segments
- DB2 V8
    - Encrypt DB2 columns



## IBM Encryption Facility for z/OS V1.1

- Program Number  5655-P97
- Encryption Services
  - Copy “on steroids”, encrypts the data and secures the data key or recovers the key and decrypts the data
  - z/OS Batch program reads sequential files
  - JAVA Client encrypt/decrypt
- DFSMSdss Feature
  - Encrypts/Decrypts data via DFSMSdss Dump/Restore
    - Includes VSAM files without sequential REPRO first
  - DFSMShsm support
    - DEFINE DUMPCLASS
    - No ABARS support
  - Disk to tape



## Parameters that impact hardware requirements

- DESC=description freeform text
- ICOUNT=SHA PKCS#12 iteration count (default 16)
- PASSWORD/RSA
  - Password – 8-32 byte password used to generate a key that protects the data key
    - General Purpose CPs
  - RSA – label of an existing public key that will encrypt the data key
    - z800/z900
      - CCF for RSA key w/Modulus <= 1024 bits
      - PCICC for RSA key w/Modulus 1025-2048 bits
    - z890/z990 – CEX2 or PCIXCC
    - z9 109 – CEX2

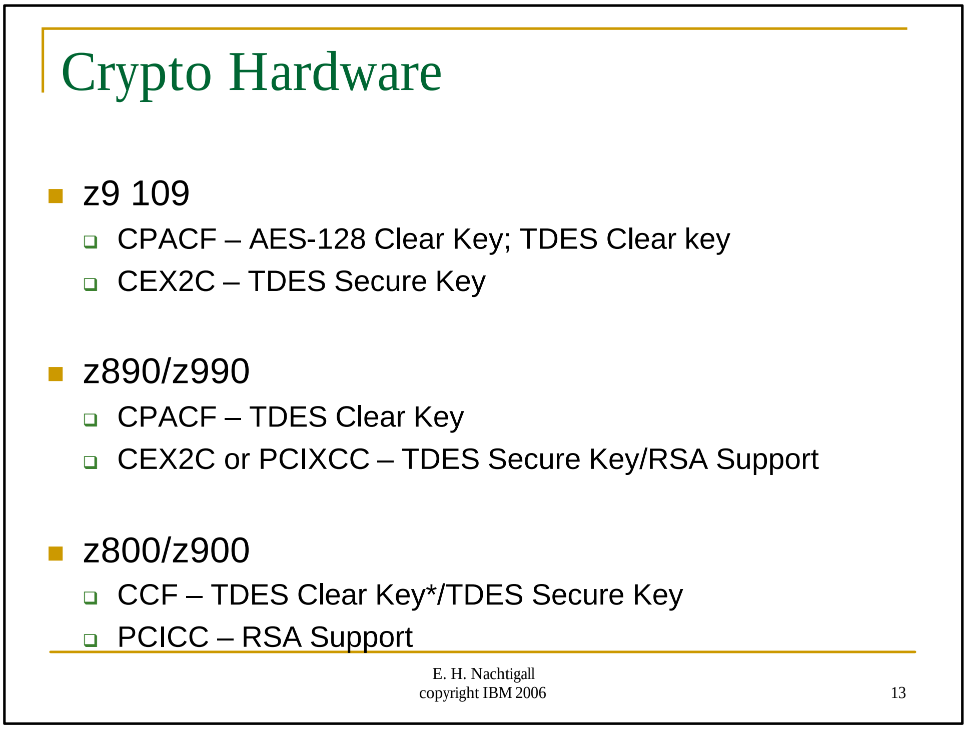
# Parameters that affect performance

## Compression

- Yes
  - Uses General Purpose CPs to do the compression
  - Requires approx 50% more tapes than compressing at the drive
- No
  - No compression workload on the General Purpose CPs
  - Requires 2-3 times more tapes than compressing at the drive

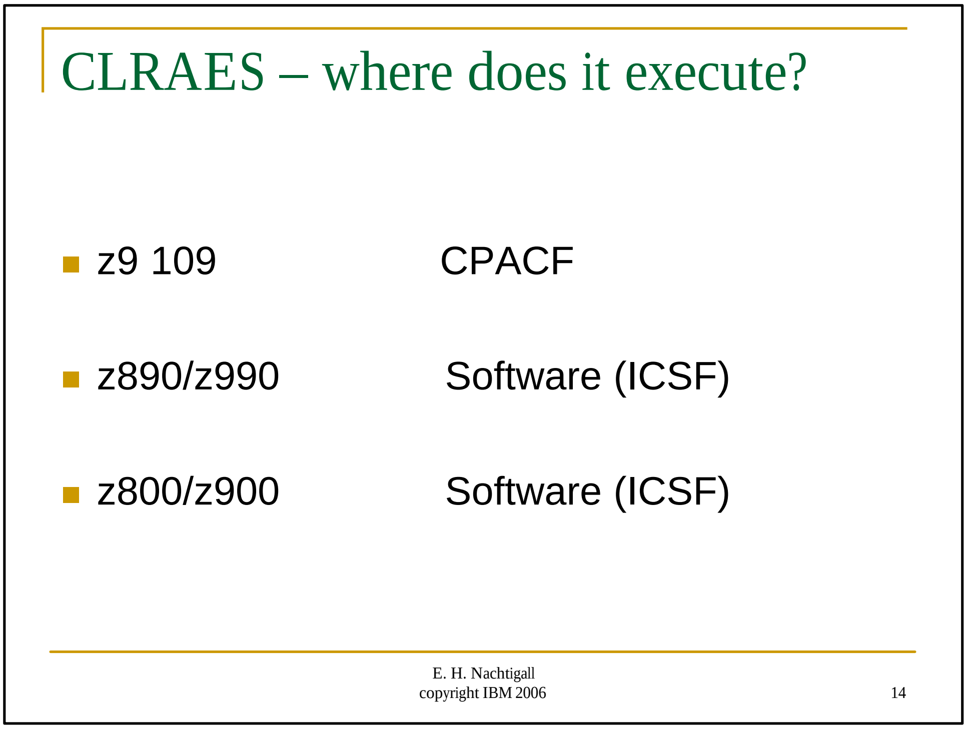
# Parameters that affect performance

- Encryption Algorithm to protect the data
  - CLRAES – AES-128 Bit Clear Key
  - CLRTDES – TDES Clear Key
  - ENCTDES – TDES Secure Key



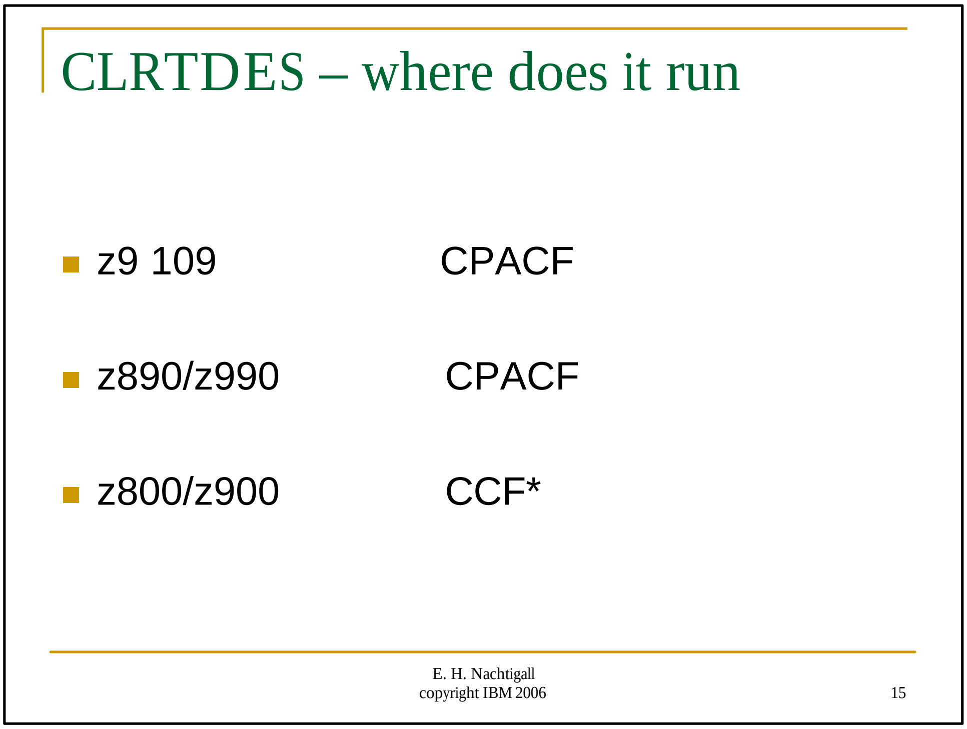
## Crypto Hardware

- z9 109
  - CPACF – AES-128 Clear Key; TDES Clear key
  - CEX2C – TDES Secure Key
- z890/z990
  - CPACF – TDES Clear Key
  - CEX2C or PCIXCC – TDES Secure Key/RSA Support
- z800/z900
  - CCF – TDES Clear Key*/TDES Secure Key
  - PCICC – RSA Support



## CLRAES – where does it execute?

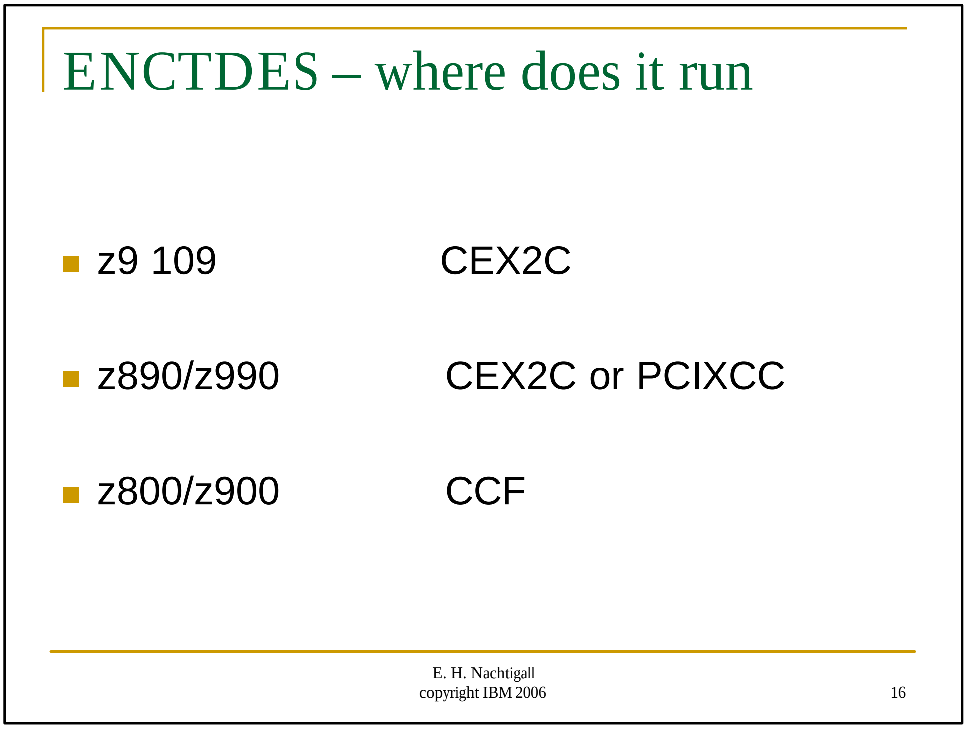
| | |
|---|---|
| z9 109 | CPACF |
| z890/z990 | Software (ICSF) |
| z800/z900 | Software (ICSF) |



## CLRTDES – where does it run

| | |
|---|---|
| z9 109 | CPACF |
| z890/z990 | CPACF |
| z800/z900 | CCF* |

E. H. Nachtigall



## ENCTDES – where does it run

| | |
|---|---|
| z9 109 | CEX2C |
| z890/z990 | CEX2C or PCIXCC |
| z800/z900 | CCF |

E. H. Nachtigall

# Performance Expectations

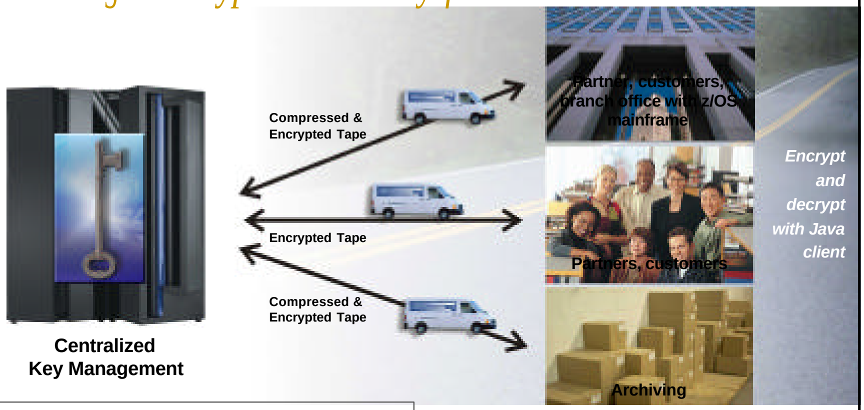
- CLRAES is best done on a z9 109 because its supported on the hardware
- ENCTDES on z890/z990/z9 109 uses less CPU than CLRTDES, but takes substantially longer wall-clock
- ENCTDES on a z800/z900 is as good as or better than CLRTDES BUT if the customer moves to a z890/z990/z9 109, secure key crypto moves to the PCI cards in the I/O cage

# Encryption Options by Machine Type

| | z800 z900 | z890 z990 | z9-109 |
|---|---|---|---|
| CLRTDES | CCF Hardware<br>(25MB second) | CPACF Instruction<br>(150MB second) | CPACF instruction<br>(200MB second) |
| ENCTDES | CCF Hardware<br>(25MB second) | PCI Hardware<br>(5MB second. Longer path length) | PCI Hardware (5MB second. Longer path length) |
| CLRAES | General purpose CP<br>(CPU intensive) | General purpose CP<br>(CPU intensive) | CPACF<br>(250-290MB second) |

# Extending Mainframe Encryption to Tape

*Introducing: Encryption Facility for z/OS V1*



**Mainframe Encryption Services**

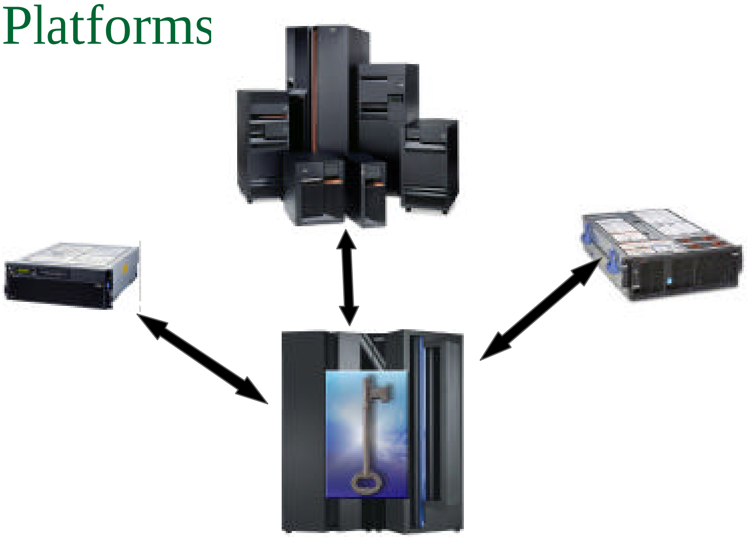
**Encryption hardware**

**Centralized key management**

**Encryption standards (AES, TDES, SHA-256)**

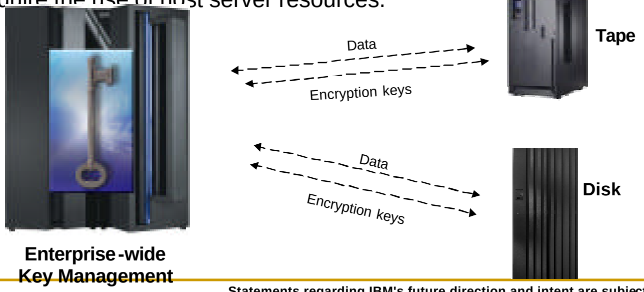
- IBM Encryption Facility for z/OS :
  - •Encryption Services – 28 Oct, 2005
  - •DFSMSdss Encryption - 2 Dec, 2005

# Encrypted Data Shared Across Platforms

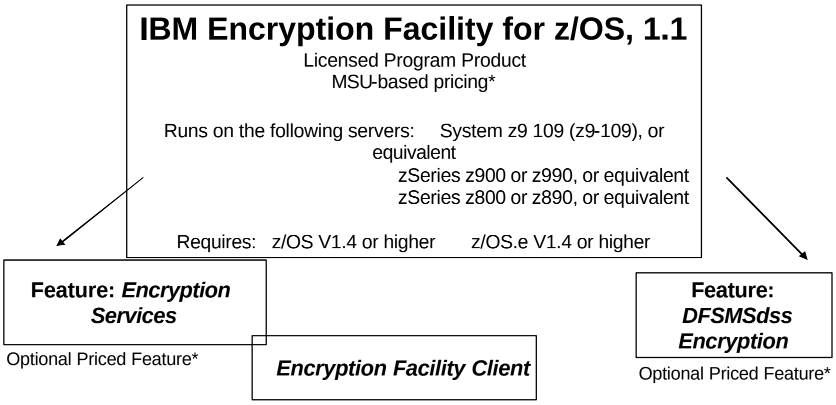


# Future Directions – Extending Encryption to IBM TotalStorage

- Statement of Direction:
  - 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.
  - To address customers' growing concern with data security, 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.



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



## IBM Encryption Facility for z/OS, 1.1

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*

- **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**

***Encryption Facility Client***

Web download

- **Java technology-based code that allows client systems to decrypt and encrypts data for exchange with z/OS systems**

**Feature: *DFSMSdss Encryption***

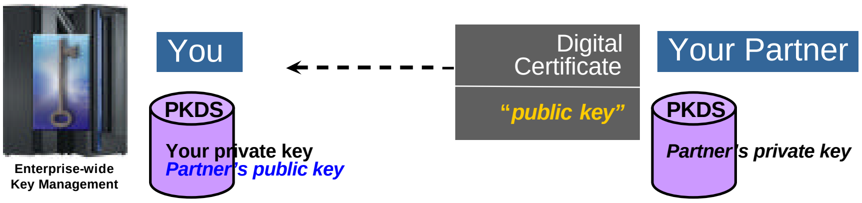
Optional Priced Feature*

- **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)

## Establishing a Trusted Exchange with Your Partners

**Key Exchange –**
- **Digital Certificates or passwords can be used to identify and authenticate**



**Options for Partners to acquire a Digital Certificate:**
1. z/OS customer can generate a certificate for the partner
   - z/OS can be a Digital Certificate Authority using z/OS PKI Services
2. Partner may already have a Digital Certificate
3. Partner may use third party Digital Certificate Authority

## Performance Considerations

- **Performance measurements for Encryption Facility for z/OS are available at**
  - **http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100700**
- **Performance will vary based on a number of factors including:**
  - Server type
  - Cryptographic features available on server
  - Data type
  - Type of encryption
    - FICON/ESCON/TAPE contention
  - Compression
- **z9-109 provides advanced encryption services (AES-128 and SHA-256) and is provides the highest cryptographic performance among IBM mainframes.**

# z990 Sample Run Times

your mileage may vary….

| Option | Size | Elapsed Time | TCB Time |
|---|---|---|---|
| CLRTDES | 80MB<br>DCB 80*5120 | 00:00:10.42 | 00:00:00.84 |
| CLRTDES | 523MB<br>DCB 125*1632 | 00:01:57.67 | 00:00:05.35 |
| CLRTDES | 523MB<br>DCB (U) 27998 | 00:00:38.15 | 00:00:04.26 |
| CLRTDES<br>COMPRESS | 80MB<br>DCB 80*5120 | 00:00:09.16 | 00:00:01.26 |
| CLRTDES<br>COMPRESS | 523MB<br>DCB 125*1632 | 00:01:50.25 | 00:00:09.89 |

These figures are from a LAB run and do not necessarily represent values you may achieve.

# 1.5GB Sample Run Times

your mileage may vary….

| System | Clear Key Triple-DES | Clear Key Triple-DES w/ Compression | Clear Key AES | Clear Key AES w/ Compression | Secure Key Triple-DES | Secure Key Triple-DES w/ Compression |
|---|---|---|---|---|---|---|
| z9-109 | 143 MBytes/CPU sec | 64 MBytes/CPU sec | 167 MBytes/CPU sec | 67 MBytes/sec | 52 Mbytes/CPU sec | 42 Mbytes/CPU sec |
| z990 | 104 | 44 | 33 | 29 | 34 | 29 |
| z890 | 78 | 33 | 25 | 21 | 26 | 23 |
| z900 | 27 | 20 | 15 | 15 | 27 | 20 |
| z800 | 20 | 15 | 11 | 11 | 20 | 15 |

These figures are from a LAB run and do not necessarily represent values you may achieve.

# Additional Information

- http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100700
- http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS1666
- http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS1601
- Or http://www.ibm.com/support/techdocs
  - search on key words crypto or encryption facility

# Encryption Facility Requests

- PGP support
- Certificate create/import without RACF (OA15156)
- Encrypted file destined for multiple sites/keys

**IBM System z9 109 (z9-109)**

These are a sample of requests by customers. IBM makes no representation as to whether these requests will be addressed.

# ICSF Utility Menu OA15156

```
------------------------------------------ ICSF - Utilities ----------------------------------
OPTION ===>
 Enter the number of the desired option.
  1 ENCODE           - Encode Data
  2 DECODE           - Decode Data
  3 RANDOM           - Generate a random number
  4 CHECKSUM         - Generate a checksum and verification and hash
                       pattern
  5 PPKEYS           - Generate master key values from a pass phrase
  6 PKDSKEYS         - Manage keys in the PKDS

Press ENTER to go to the selected option.
Press END   to exit to the previous menu.
```

# ICSF PKDS Key Management

```
CSFPKY00----------------------------------- ICSF – PKDS Keys ---------------------------
Enter the PKDS record’s label for the actions below ===>
Select one of the following actions then press Enter to process:
   _  Generate a new PKDS key pair record
       Enter the key length ===>                512, 1024 or 2048
       Enter Private Key Name (optional)
       ===>
   _  Delete the existing public key or key pair PKDS record
   _  Export the PKDS record’s public key to a certificate data set
      Enter the DSN ===>
      Enter the desired subject’s common name (optional)
      CN ===>
   _  Create a PKDS public key record from an input certificate.
      Enter the DSN ===>

Press ENTER to go to the selected option.
Press END   to exit to the previous menu.
```

# Questions