MAINFRAME CRYPTO

Pervasive Encryption – Are You Ready?

Greg Boyd (gregboyd@mainframecrypto.com)

Copyrights . . .

- Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 12 years

. . . And Trademarks

-
- All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. IBM, System z, zEnterprise and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.
- **THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY**. Greg Boyd and Mainframe Crypto, LLC assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will Greg Boyd or Mainframe Crypto, LLC be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if expressly advised in advance of the possibility of such damages.

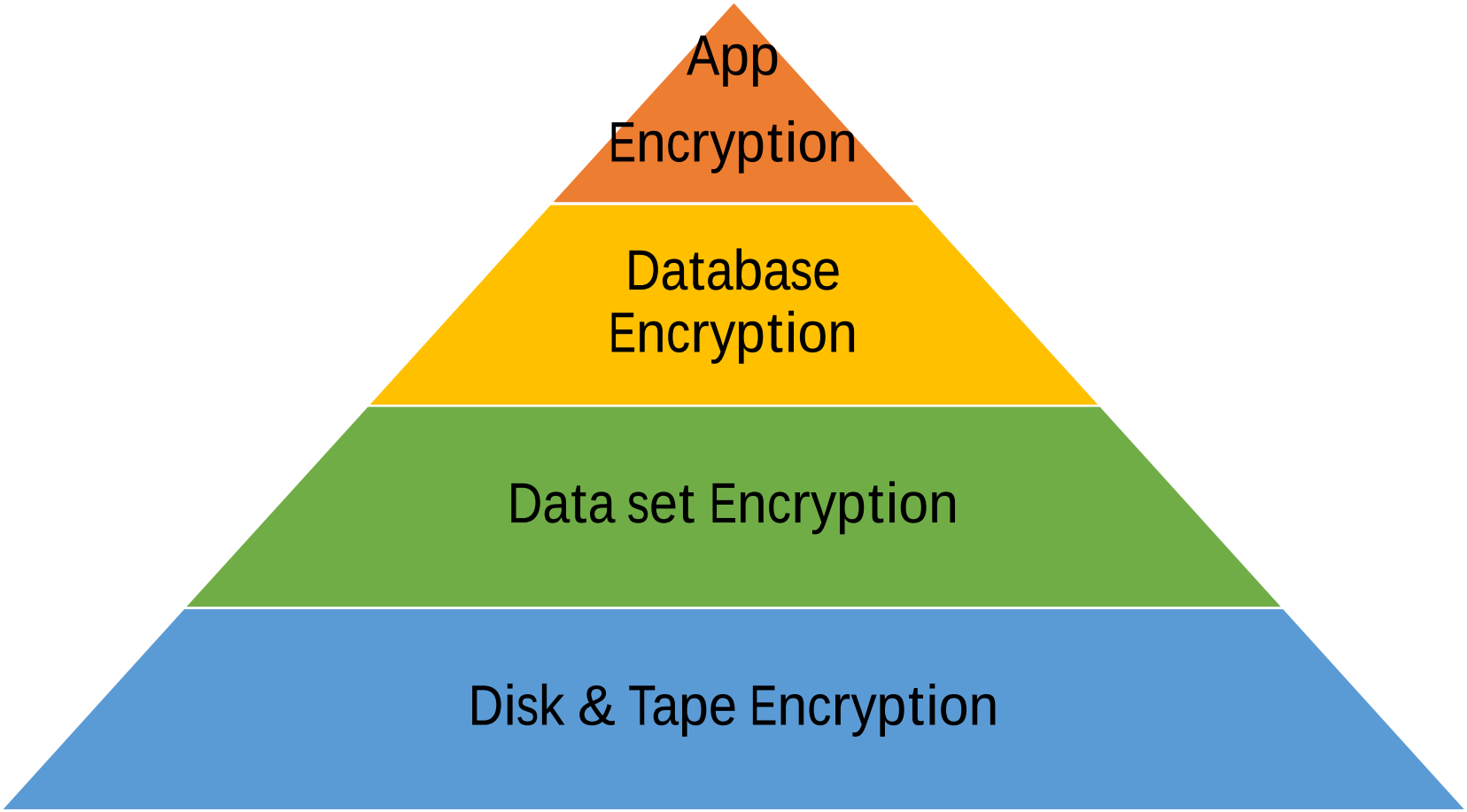
Agenda – Pervasive Encryption

- Introduction
- How it works
- Operational Stuff (Key Management and Performance)
- Coupling Facility
- Summary

An Apology – Just what is Pervasive Encryption?

- Full Disk Encryption
- Integrated Crypto Hardware
- Network Encryption
- **Data set and File Encryption**
- **Coupling Facility Encryption**
- Secure Service Container
- Key Management (EKMF – Enterprise Key Management Foundation)

IBM's Encryption Pyramid



Access Method Encryption

Standard Read/Write (BSAM/QSAM/VSAM)

vs

Non-Standard Read/Write (Track/Cylinder level)

Access Authority for Dataset Encryption

- Dataset
  - Access list
- API Access (to CSNBKRR2)
  - Access list or
  - PERMIT ID(*) ACCESS(READ)?
- Key Label
  - Access list, PERMIT WHEN …

  (SYMCPACFWRAP / SYMCPACFRET)

User

Storage Admin

Configuration requirements

- Machine type
  - z196/z114 w/CEX3C (FC #0864)
  - zEC12/zBC12 w/CEX3C (FC #0864) or CEX4C (FC #0865)
  - z13/z13s w/CEX5C (FC #0890)
- Operating System
  - z/OS 2.3
  - z/OS 2.2 w/APAR OA50569
  - z/OS 2.1 w/APAR OA50569 (supports reading/writing an encrypted data set, but not creating an encrypted data set)
- ICSF
  - HCR77C1
  - HCR77C0
  - HCR77A0-HCR77B1 w/APAR OA50450

Supported filetypes

- Extended Format
  - Sequential BSAM/QSAM
  - VSAM (KSDS, ESDS, RRDS, VRRDS, LDS)

    DB2, IMS, logs
- zFS (not Extended Format)

Restricted data sets

- Restrictions
  - DFSMSdss REBLOCK ignored on COPY and RESTORE
  - DFSMSdss VALIDATE ignored when backing up encrypted indexed VSAM
- Data sets used during IPL
- Catalogs, SHCDS, HSM data sets, ICSF Keystores
- Temporary, SORTWKxx, BLKSIZE<16 (can’t be Extended Format)

Encryption enabled at allocation (by assigning a key label)

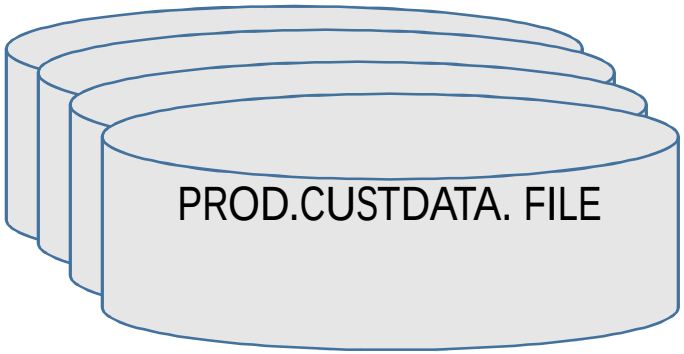
- DFP Segment of the SAF data set profile
  - ALTDSD 'PROJECTA.DATA.*' UACC(NONE)
    DFP(RESOWNER(iduser1)) DATAKEY(Key-Label for ProjectA))
- JCL, TSO Allocate (Dynamic Allocation)
  - DSKEYLBL=key-label
- IDCAMS
  - DEFINE CLUSTER -

    (NAME(DSN1.EXAMPLE.ESDS1) -

    ... -

    KEYLABEL (LABEL.FOR.DSN1))
- SMS Data Class

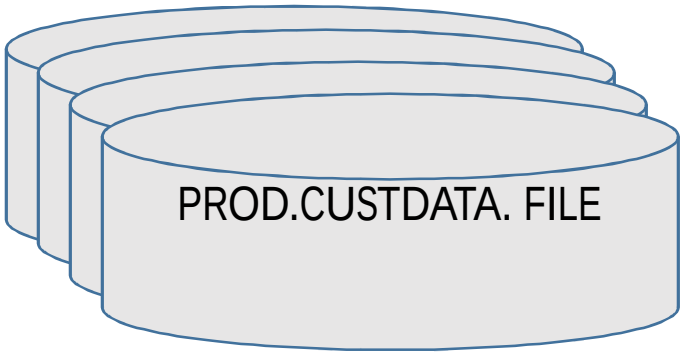
Creating a ciphertext copy of a file (1 of 5)



PROD.CUSTDATA.**
ACCESS LIST

Cleartext file(s)

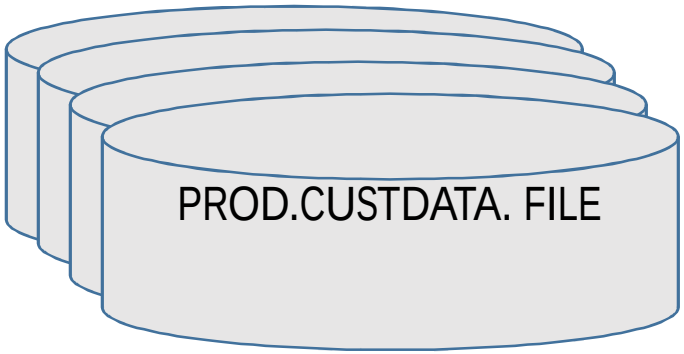
Creating a ciphertext copy of a file (2 of 5)



PROD.CUSTDATA.**
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEY1)

Specify the key label in the DFP Segment of the data set profile

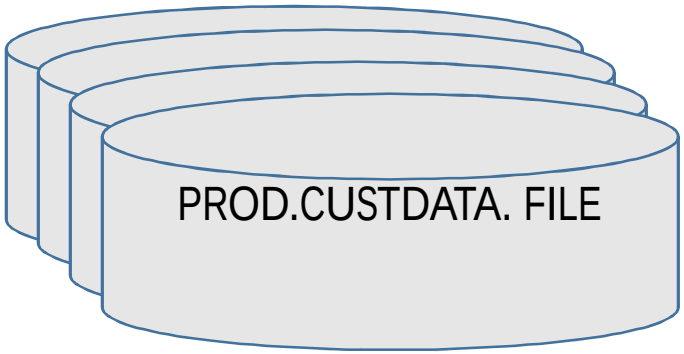
Creating a ciphertext copy of a file (3 of 5)



PROD.CUSTDATA.**
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEY1)

Allocate the new file

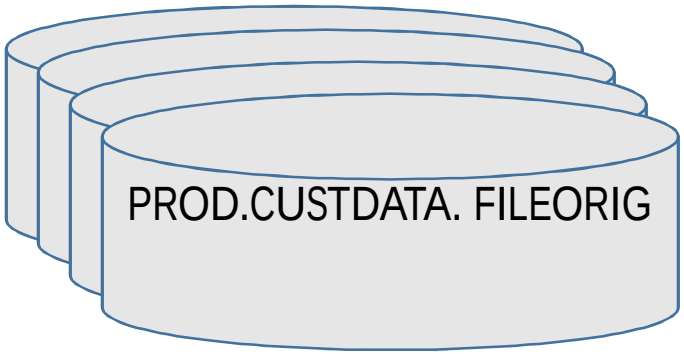
Creating a ciphertext copy of a file (4 of 5)



PROD.CUSTDATA.**
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEY1)

Copy the file

Creating a ciphertext copy of a file (5 of 5)



Rename the two files

Reencipher a file (1 of 5)

PROD.CUSTDATA.**
ACCESS LIST

Ciphertext file, protected by PRODCUST.KEY1

Reencipher a file (2 of 5)

PROD.CUSTDATA.**
ACCESS LIST

PE. **
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEY2)

Create a new data set profile, referencing the new key label, PRODCUST.KEY2

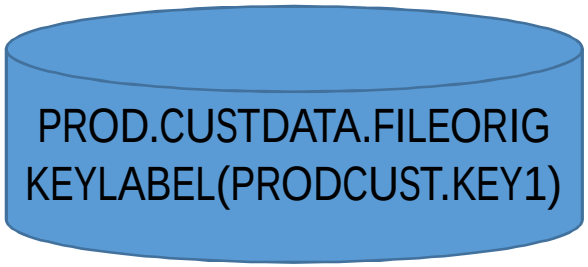
Reencipher a file (3 of 5)

Allocate

Reencipher a file (4 of 5)

Copy the file

Reencipher a file (5 of 5)



PROD.CUSTDATA.**
ACCESS LIST

PE. **
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEY2)

Rename the two files

Data set lifecycle

- Backups, Replication
  - Still encrypted
- Migrated (in the storage hierarchy)
  - It's still encrypted!

Key Management Tools

- HCR77C1 – CKDS Browser
  - Proof of Concept
- Key Generation Utility Program
  - Comes with ICSF
  - Low volume of keys
- Trusted Key Entry (TKE) Workstation
  - Priced product
  - Must be managed
  - Additional benefits
  - Mid volume of keys
- Enterprise Key Management Foundation
  - Priced product
  - Must be managed
  - High volume of keys

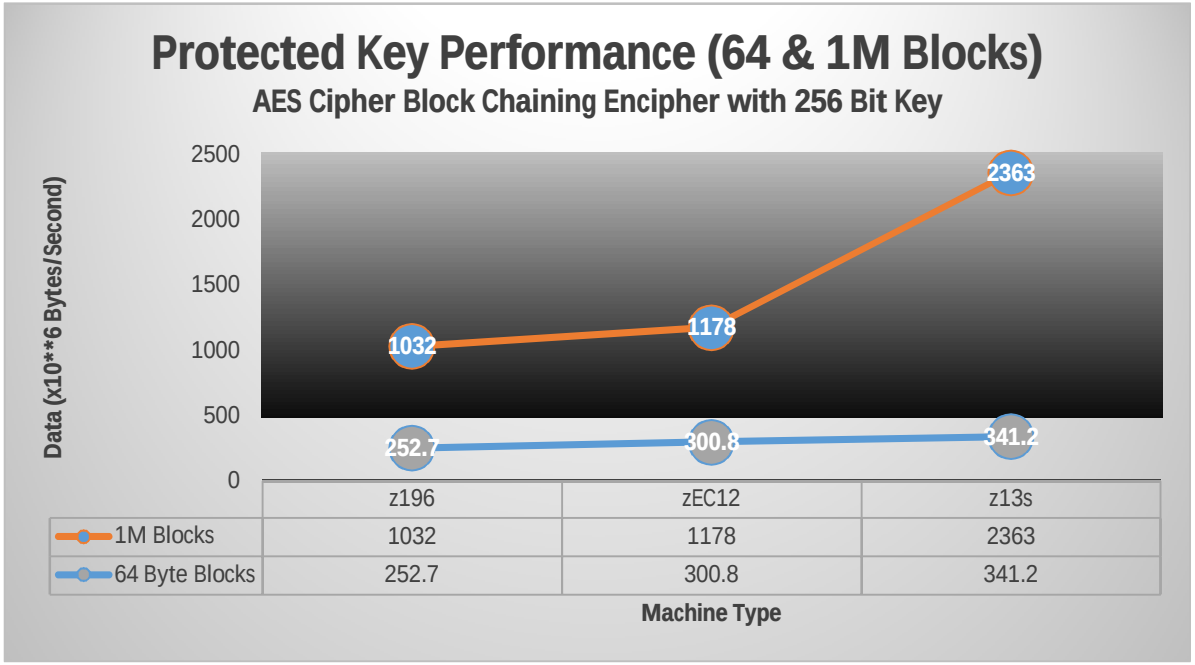
Compression

- Encryption still impacts compression
  - May impact space savings
  - Compress, then encrypt
- Compression
  - Generic – uses system supplied dictionary building blocks
  - Tailored – system generated compression dictionary
  - zEDC – uses zEnterprise Data Compression functionality (Required or Preferred)
- IBM recommends compressing all data sets before encrypting

A couple of other things

- Data set encryption breaks deduplication
- Shared (or replicated) DASD – be careful
  - Encryption enabled on LPAR1
  - Encryption not enabled on LPAR2
  - Not good
- Restricting
  - STGADMIN.SMS.ALLOWED.DATASET.ENCRYPT UACC(NONE)
  - If FIELD Class is active, DATASET.DFP.DATAKEY

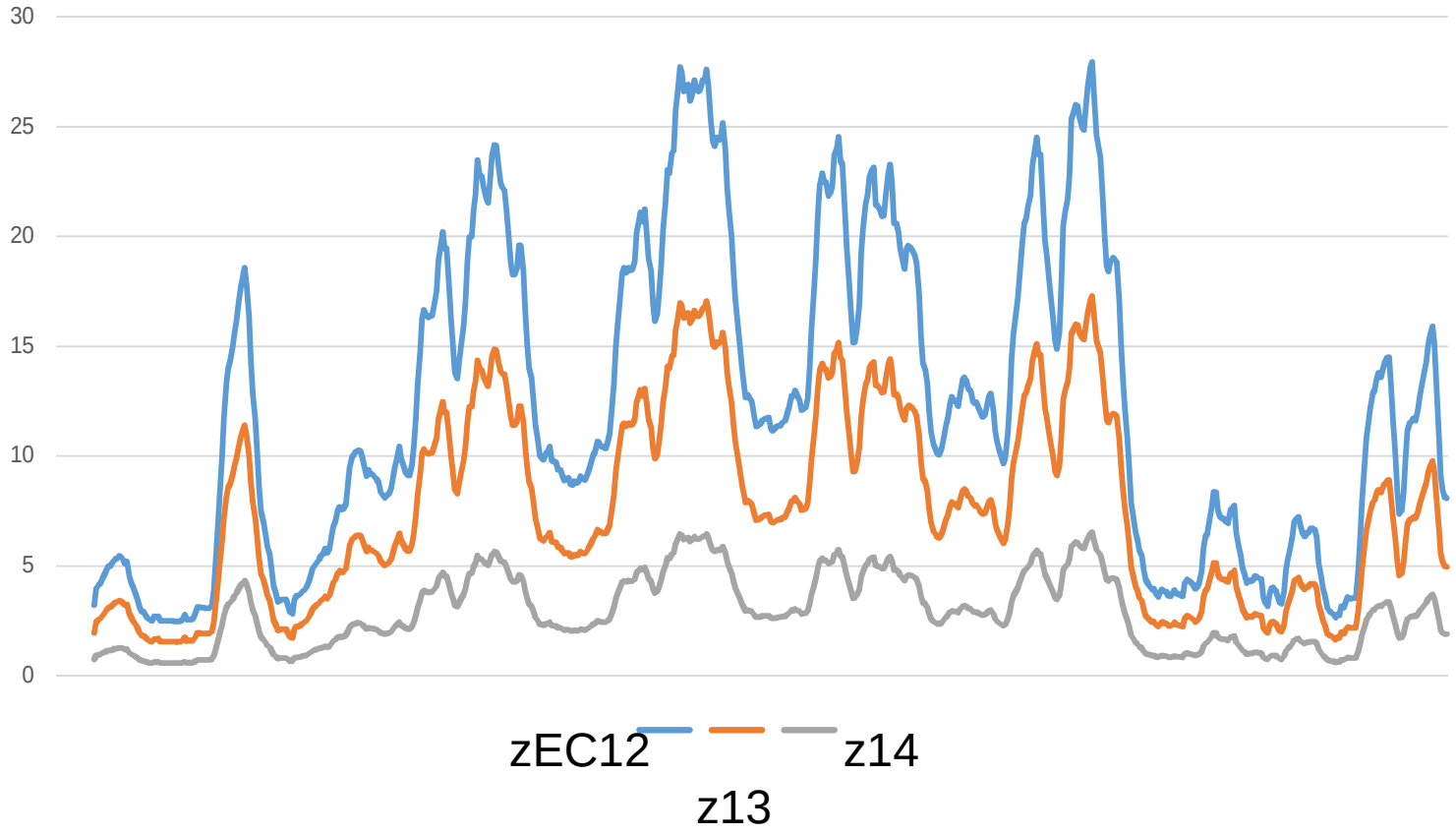
Performance



- IBM z13 Performance of Cryptographic Operations (Cryptographic Hardware: CPACF, CEX5S)
  - https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSW03283USEN
- IBM zEnterprise EC12 Performance of Cryptographic Operations (Cryptographic Hardware: CPACF, CEX4S)
- IBM zEnterprise 196 Performance of Cryptographic Operations (Cryptographic Hardware: CPACF, CEX3C, CEX3A)

4-Hour Rolling Average

Customer Encryption Overhead



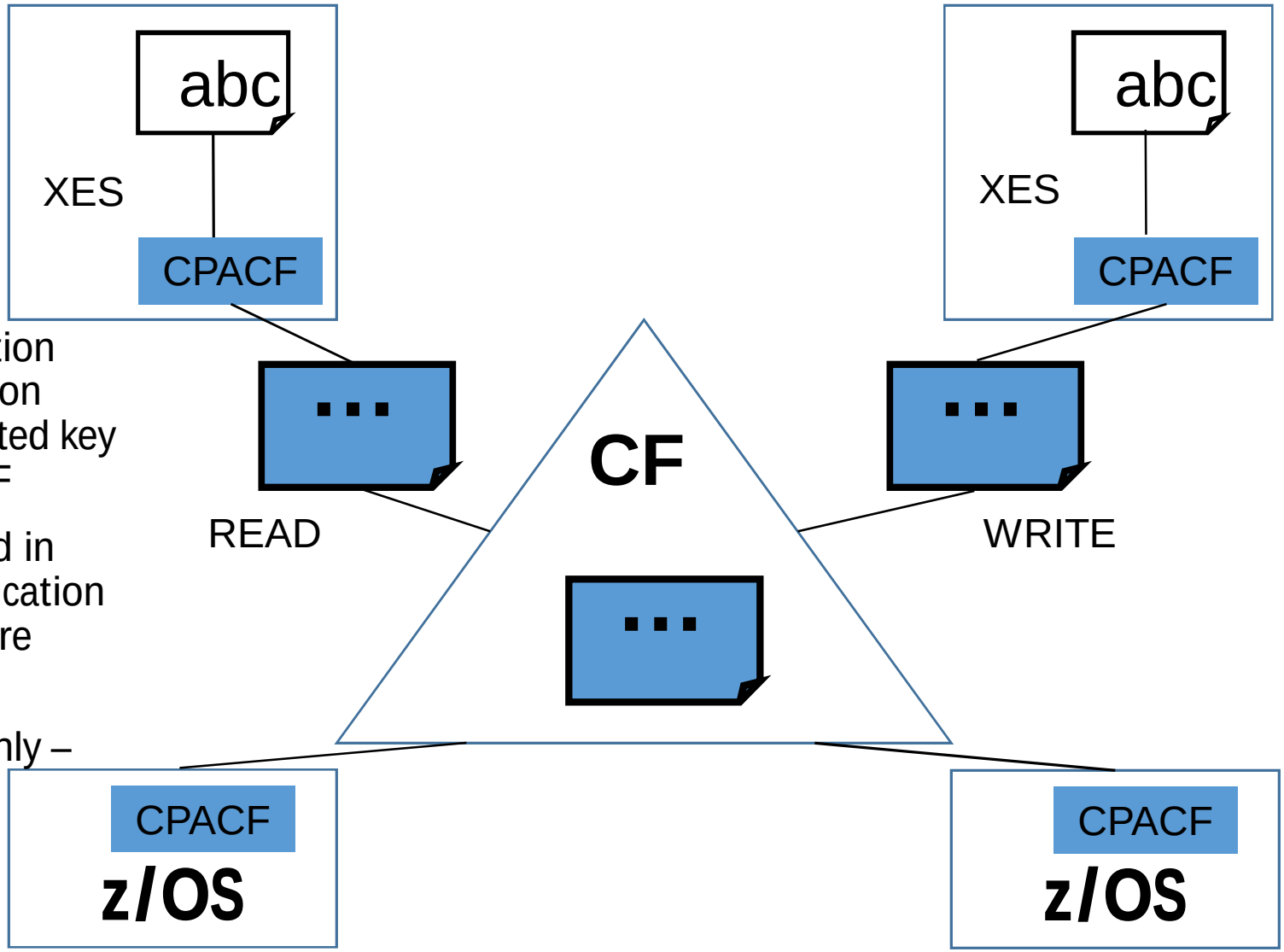
IBM z Systems Batch Network Analyzer (zBNA) Tool

- Enhanced to estimate the impact of enabling data set encryption
  - PC Based
  - Analyzes SMF data

- http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS5132

Coupling Facility Encryption

- Host encryption and decryption using protected key on the CPACF
- Implemented in XES, no application or middleware
- List & Cache Structures only – No locks



Coupling Facility Structure Encryption

- CFRM Policy Keyword
  - ENCRYPT(NO) – the default
  - ENCRYPT(YES)
- Encryption performed when the structure is written
  - New structure with ENCRYPT(YES) as it's built
  - Existing structure with rebuild
- Neither the Coupling Facility nor the CF Links do encryption/decryption – it's done on the CPACF
- Encryption is transparent

Coupling Facility Structures

- All entry and adjunct data moving between z/OS and the Coupling Facility is encrypted
  - Control info & metadata is not encrypted

- Cache Structure
- Serialized List Structure
- CF Lock Structure – not encrypted

Requirements for running policy utility with ENCRYPT(YES)

- ICSF must be active on the system where the job runs
- Job must have READ access to CSFSERV CSFKGN and CSFKYT resource profiles
- AES master key must be the same where the job is run and where the encrypted structures are used

Summary (of Data Set Encryption)

- Traditional access methods
  - Allocation will flag a data set for pervasive encryption and assign a key to that data set
  - If that flag is on,
    - Access to the Data set is not sufficient
    - Also need access to CSNBKRR2 and the key associated with the data set
- Non-Traditional access methods (Utilities that manage the data set, not the data work differently)
  - Work on the ciphertext

Summary (operational impact)

- From a crypto perspective, business as usual, but …
  - Criticality of keys
  - Volume of keys
  - Performance
- From an operational perspective
  - Potential data set conversion (i.e. making sure PII data sets are extended format)
  - Assigning key labels
  - Key assigned at allocation
  - Performance impact

References

- Share Presentations
  - **Securing Your Environment With Encryption**, *Session Number 20564 Speaker: Julie Bergh & Greg Boyd*
  - **Protect Your Data at Rest with z/OS Data Set Encryption**, *Session 20612 Speaker: Cecilia Carranza Lewis*
- Other presentations (Google 'IBM Encryption' and the speaker)
  - Eysha Powers
  - Mark Brooks
- Redbook – coming …

References

- OA50569 Data Set Encryption PDF
  http://publibz.boulder.ibm.com/zoslib/pdf/OA50569.pdf

- TechDocs – IBM z Systems Batch Network Analyzer (zBNA) Tool A PC-based tool for estimating elapsed time
  - http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS5132
- IBM DeveloperWorks
  - https://www.ibm.com/developerworks/community/groups/community/crypto

Questions?