MAINFRAME CRYPTO

Data Set Encryption – An Update

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 20+ 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 or Data Set Encryption?
- How it works
- Operational Stuff (Key Management and Performance)
- Summary

Pervasive Encryption – A suite of products and solutions

- 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)

Access Method Encryption

Standard Read/Write (BSAM/QSAM/VSAM)

vs

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

Access Authority for Dataset Encryption

User

Storage Admin

- Dataset
  - Access list
- Key Label
  - Access list, PERMIT CLASS(CSFKEYS) ID(*) ACCESS (READ) WHEN(CRITERIA(SMS(DSNENCRYPTION)))
- API Access (to CSNBKRR2)
  - CHECKAUTH(NO)
  - Access list - PERMIT CLASS(CSFSERV) ID(*)
    ACCESS(READ)

Configuration requirements

- Machines (CEX Coprocessors with AES-MK Loaded!)
  - z196/z114 w/CEX3C
  - zEC12/zBC12 w/CEX3C or CEX4Cz13/z13s w/CEX5C
  - z14/z14s w/CEX6C
  - z15/z15s w/CEX7C
  - 16/z16s w/CEX8C
- Operating System
  - z/OS 2.5
  - z/OS 2.4
  - 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
  - HCR77D2 (w/zOS2.5)
  - HCR77D1-HCR77C0
  - HCR77A0-HCR77B1 w/APAR OA50450

Supported filetypes

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

    DB2, IMS, logs
  - zFS

z/OS 2.4 Enhancements

- Basic & Large Format Data Sets (OA56622)
- PDSE (OA56324)
  - Data Set (not by member)

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)

Assigning the key (Key label)

- DFP Segment of the SAF data set profile
  - ALTDSD 'PROJECTA.DATA.*' UACC(NONE) DFP(DATAKEY(Key-Label for ProjectA))
- Manually at allocation
  - JCL, TSO Allocate (Dynamic Allocation)
    - DSKEYLBL=key-label
  - IDCAMS
    - DEFINE CLUSTER -
      (NAME(DSN1.EXAMPLE.ESDS1) -
      … -
      KEYLABEL (LABEL.FOR.DSN1))
- SMS Data Class

RDEFINE FACILITY STGADMIN.SMS.ALLOW.DATASET.ENCRYPT UACC(NONE)

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

PROD.CUSTDATA.**
ACCESS LIST

Cleartext file(s)

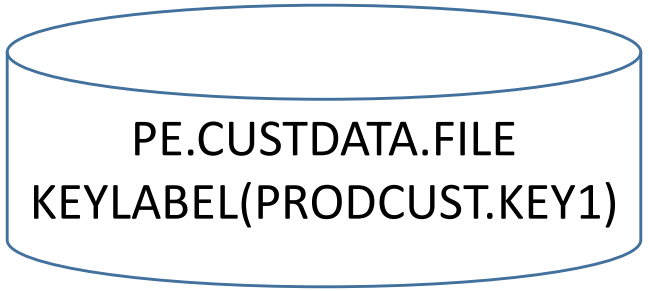
Creating a ciphertext copy of a file (2 of 5)

PROD.CUSTDATA.**
ACCESS LIST

PE. **
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEY1)

Create a new data set profile, referencing the new key label, PRODCUST.KEY1

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

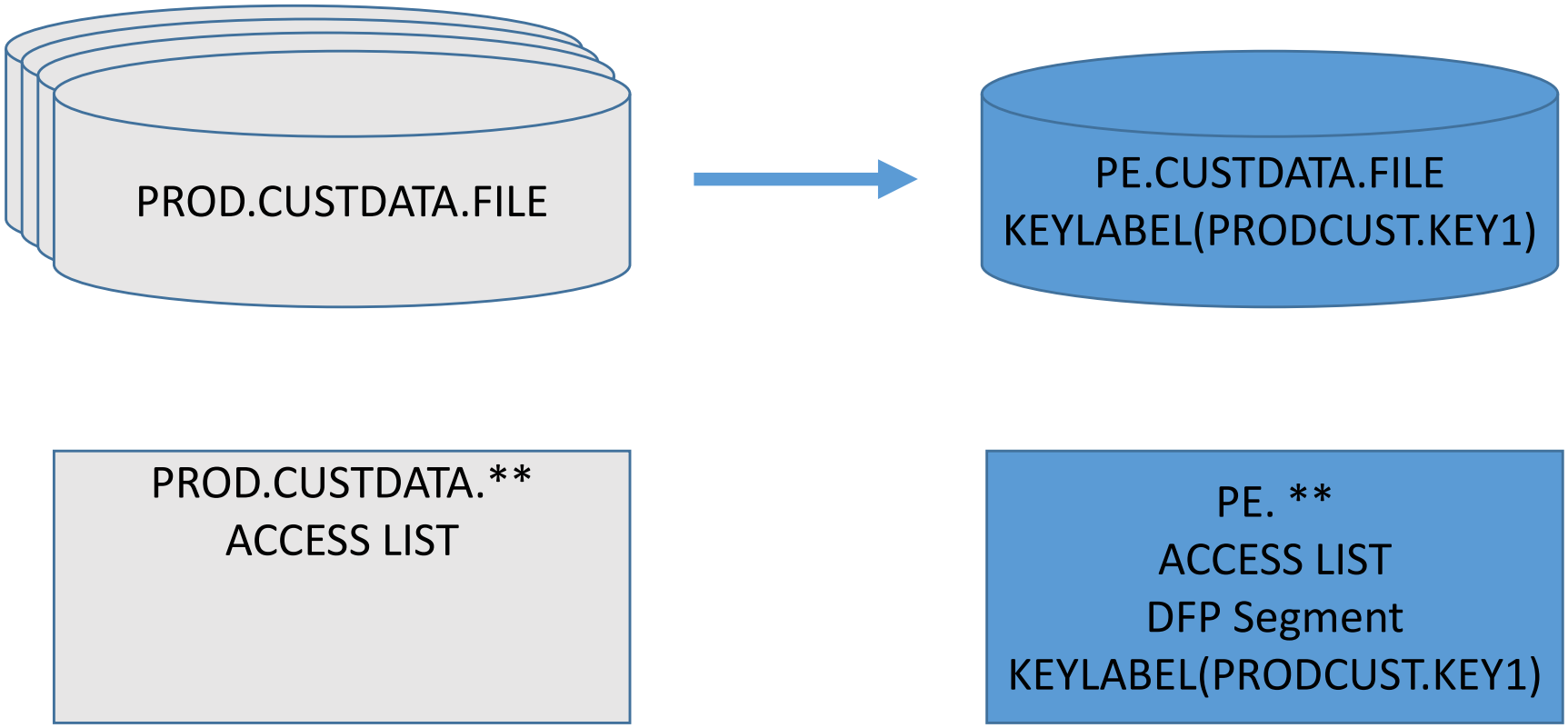


PROD.CUSTDATA.**
ACCESS LIST

PE. **
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEY1)

Allocate the new file

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



Copy the file

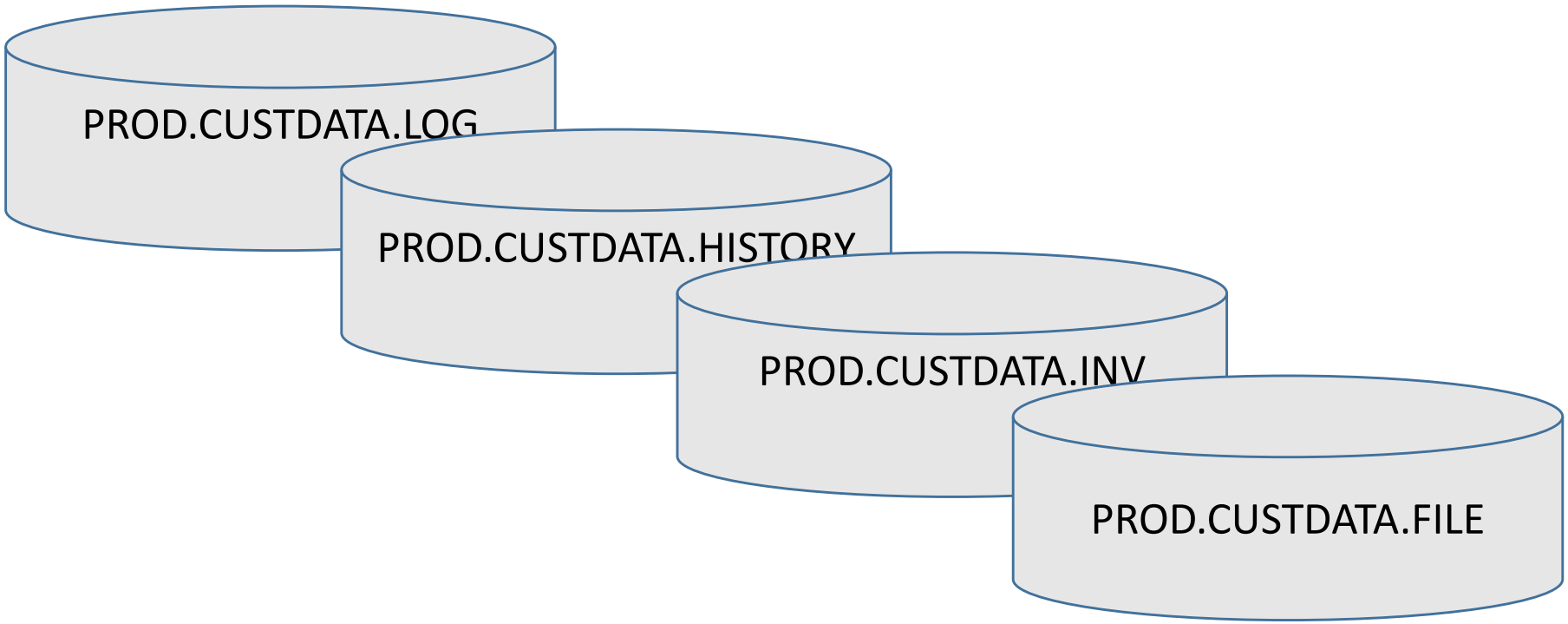
Creating a ciphertext copy of a file (5 of 5)

PROD.CUSTDATA.**
ACCESS LIST

PE. **
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEY1)

Rename the two files

RACF Profile Coverage



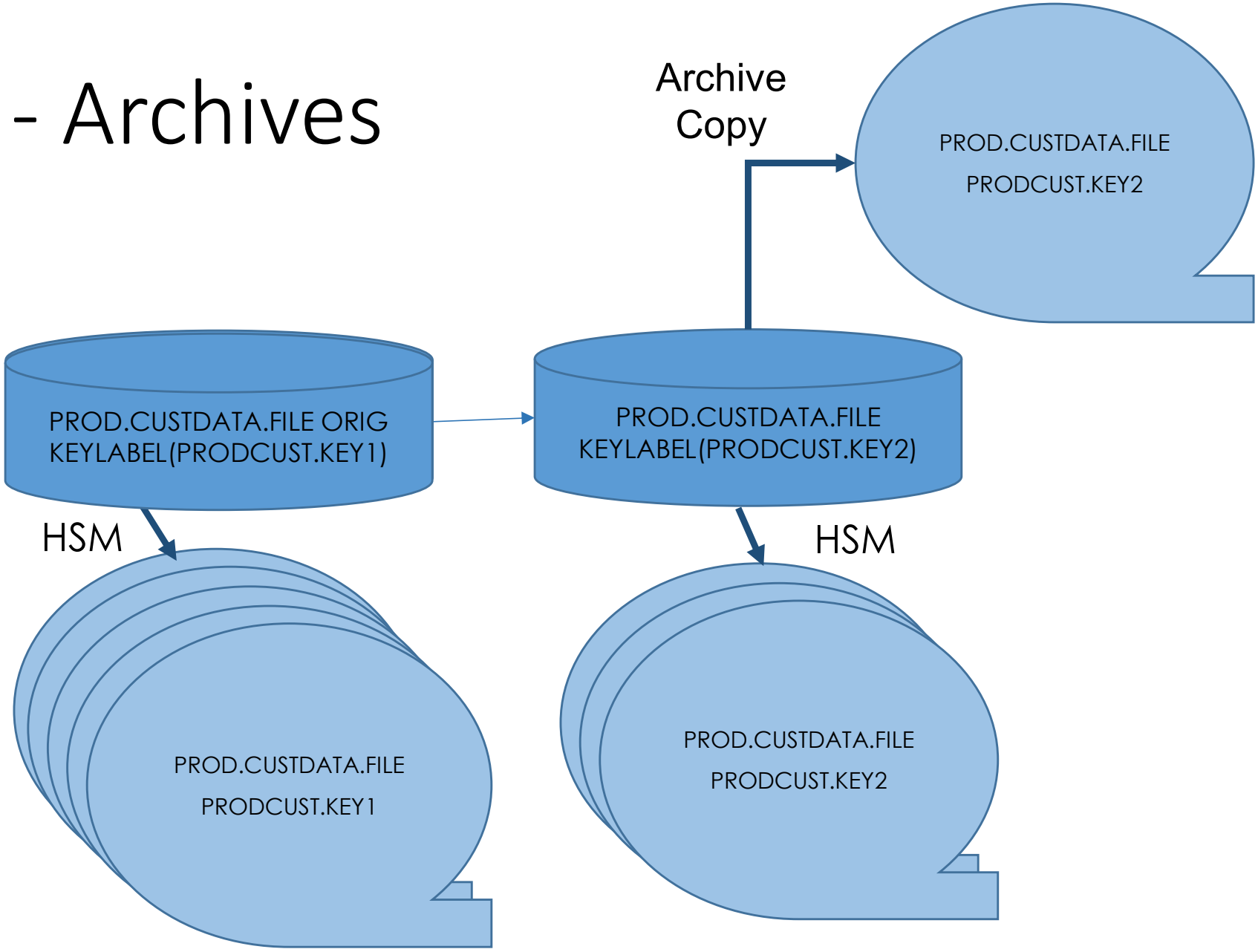
PROD.CUSTDATA.**
ACCESS LIST

DFP Segment
KEYLABEL(PRODCUST.KEY1)

Data set lifecycle vs Key lifecycle

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

DSE - Archives

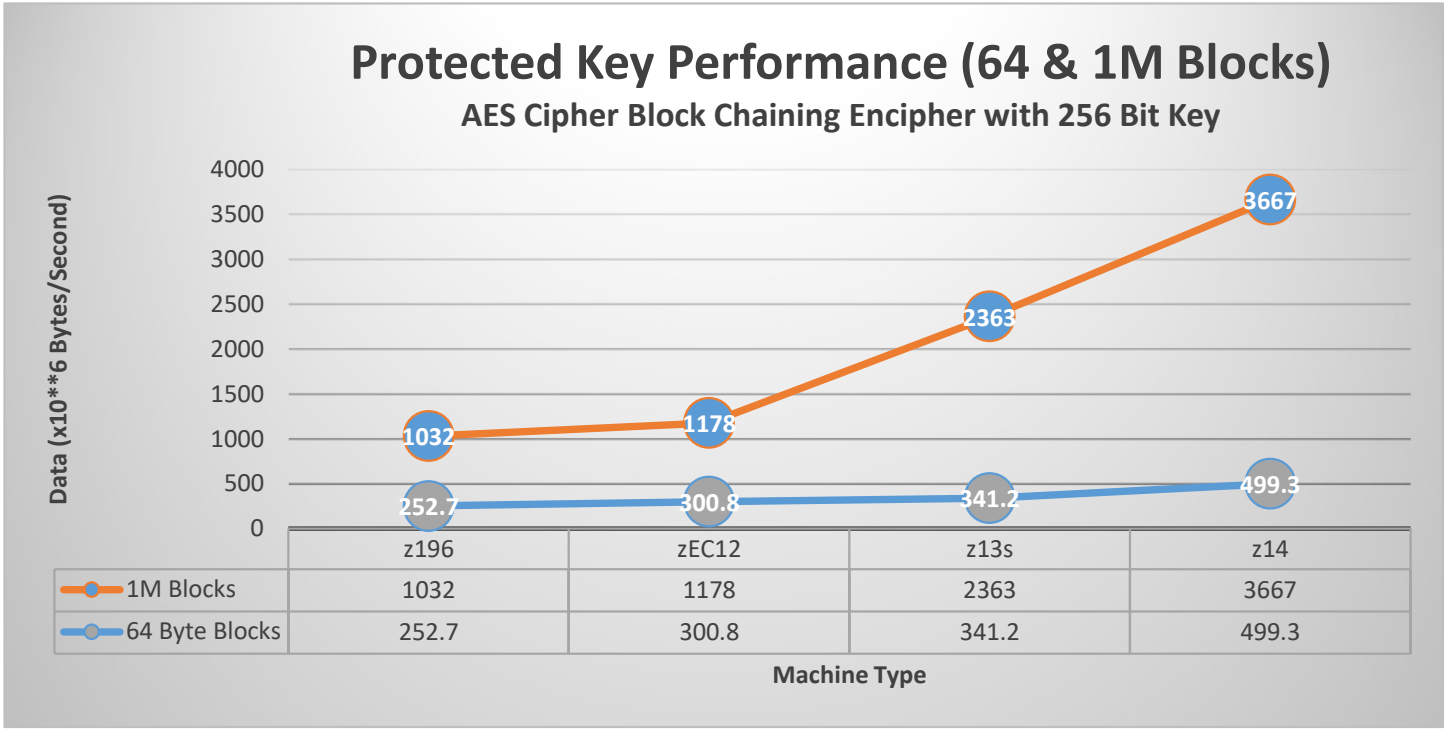


Compression

- Encryption impacts compression
  - May impact space savings
  - Compress, then encrypt

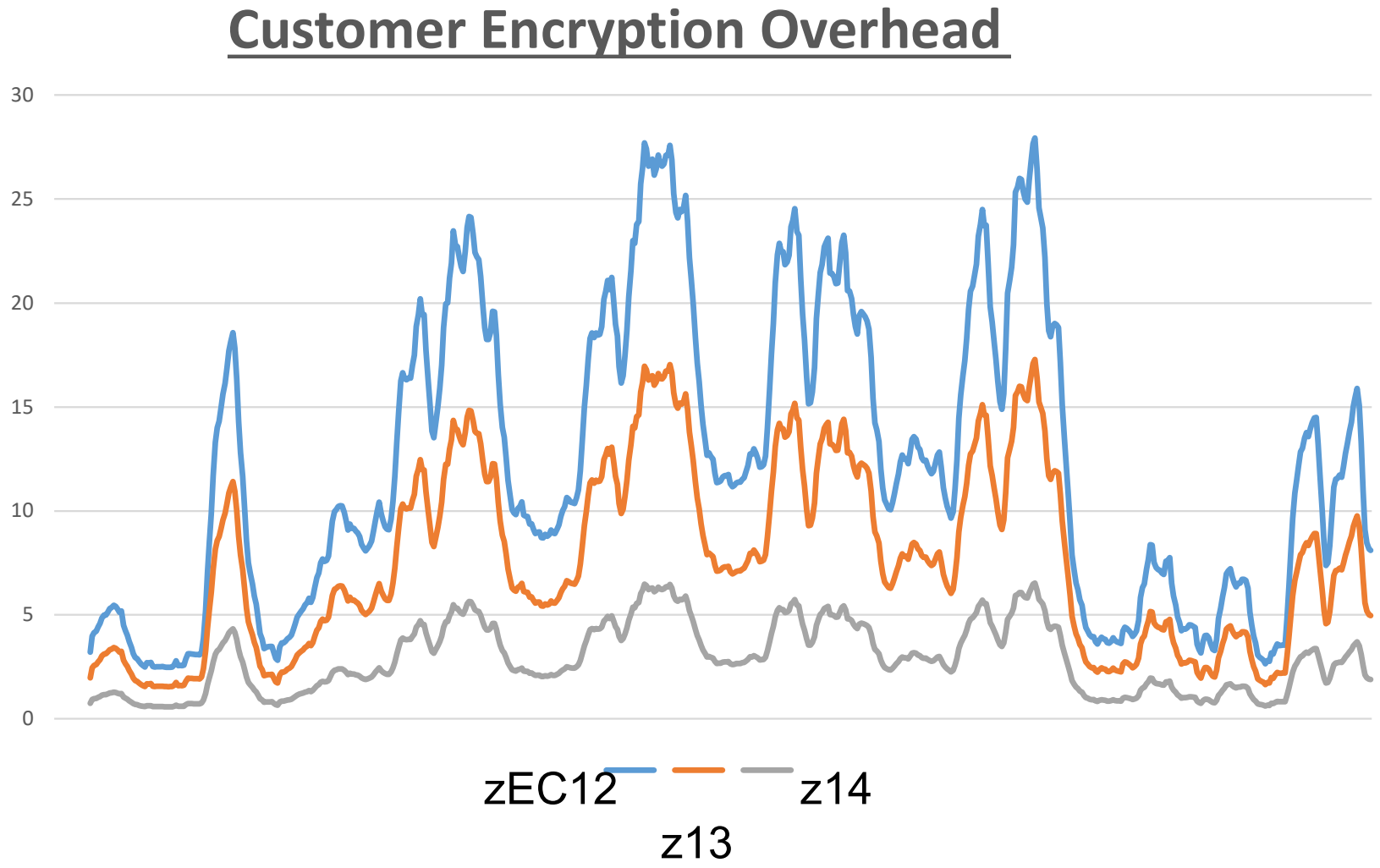
- IBM recommends compressing all data sets before encrypting

Performance



- IBM z14 Performance of Cryptographic Operations (Cryptographic Hardware: CPACF, CEX6S)
  - https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSL03607USEN
- 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



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

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 label 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

How do I get there?

Crypto Config
- ICSF Options
- STC Always Up
- Keystore Layout
- RACF Security
  - CSFKEYS
  - CSFSERV
  - Keystore Policies
- MKs Loaded/Recoverable

Identify Target data sets
- Compression enabled?
- Extended Format
- Convert to Extended Format
- Basic/Large Format
- Identify RACF Profiles

Develop
- Key labeling conventions
- Key rotation policies
- Key management procedures

→ Enable DSE & Test

References

- OA50569 Data Set Encryption PDF

http://publibz.boulder.ibm.com/zoslib/pdf/OA50569.pdf

- OA56622 Data set encryption for for seq basic and large format data sets

https://public.dhe.ibm.com/eserver/zseries/zos/DFSMS/ENCRYPTION/OA56622/OA56622.pdf

- IBM Community

https://community.ibm.com/community/user/home

- Redbook

SG24-8410 Getting Started with z/OS Data Set Encryption

Questions?