MAINFRAME CRYPTO

Policy-Based Data Set Encryption

Greg Boyd

gregboyd@mainframecrypto.com

www.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
- Key Management
- Configuration
- Performance

Announcement Letter 216-391

- IBM plans to deliver application transparent, policy-controlled dataset encryption in IBM z/OS. IBM DB2 for z/OS and IBM Information Management System (IMS) intend to exploit z/OS dataset encryption.

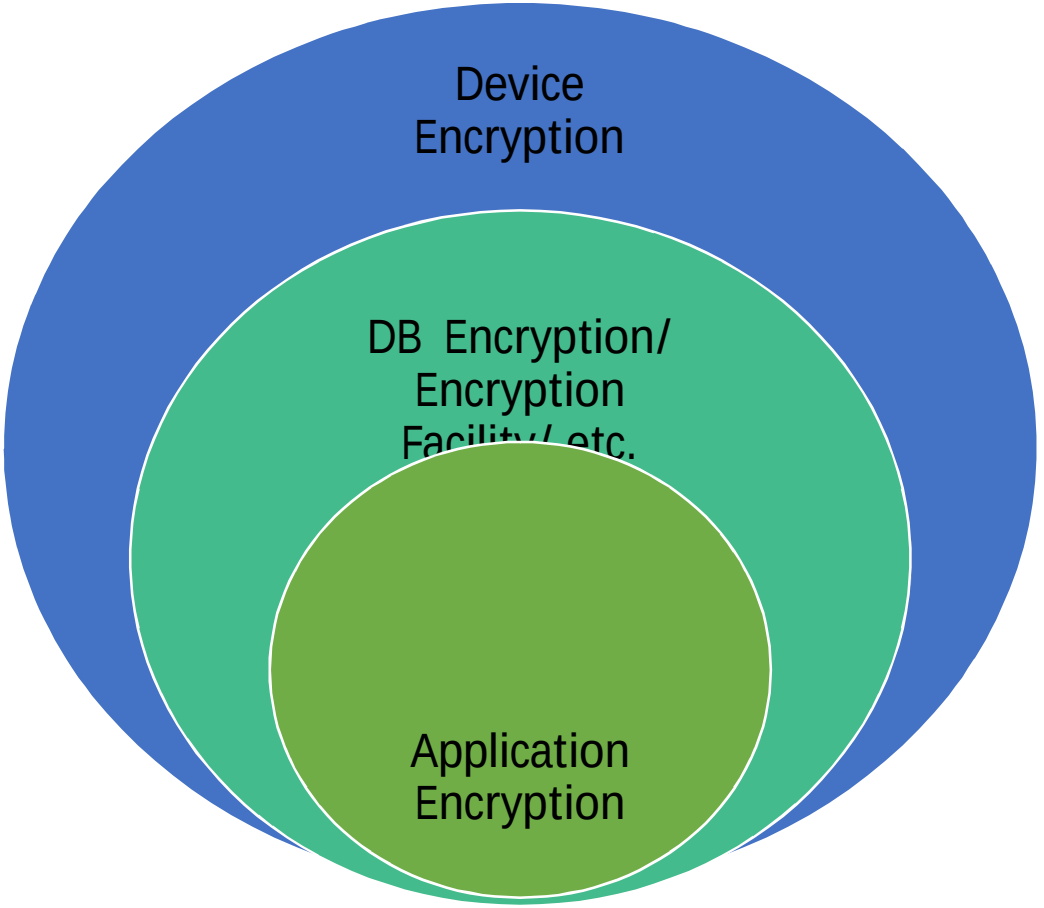
Announcement Letter 217-085

- z/OS V2.3 plans to replace application development efforts with transparent, policy-based data set encryption:
  - Planning enhanced data protection for z/OS data sets, zFS file systems, and Coupling Facility structures to give users the ability to encrypt data without needing to make costly application program changes.
  - Designing new z/OS policy controls to make it possible to use pervasive encryption to protect user data and simplify the task of compliance.
  - z/OS Communications Server will be designed to include encryption readiness technology to enable z/OS administrators to determine which TCP and Enterprise Extender traffic patterns to and from their z/OS systems meet approved encryption criteria and which do not.

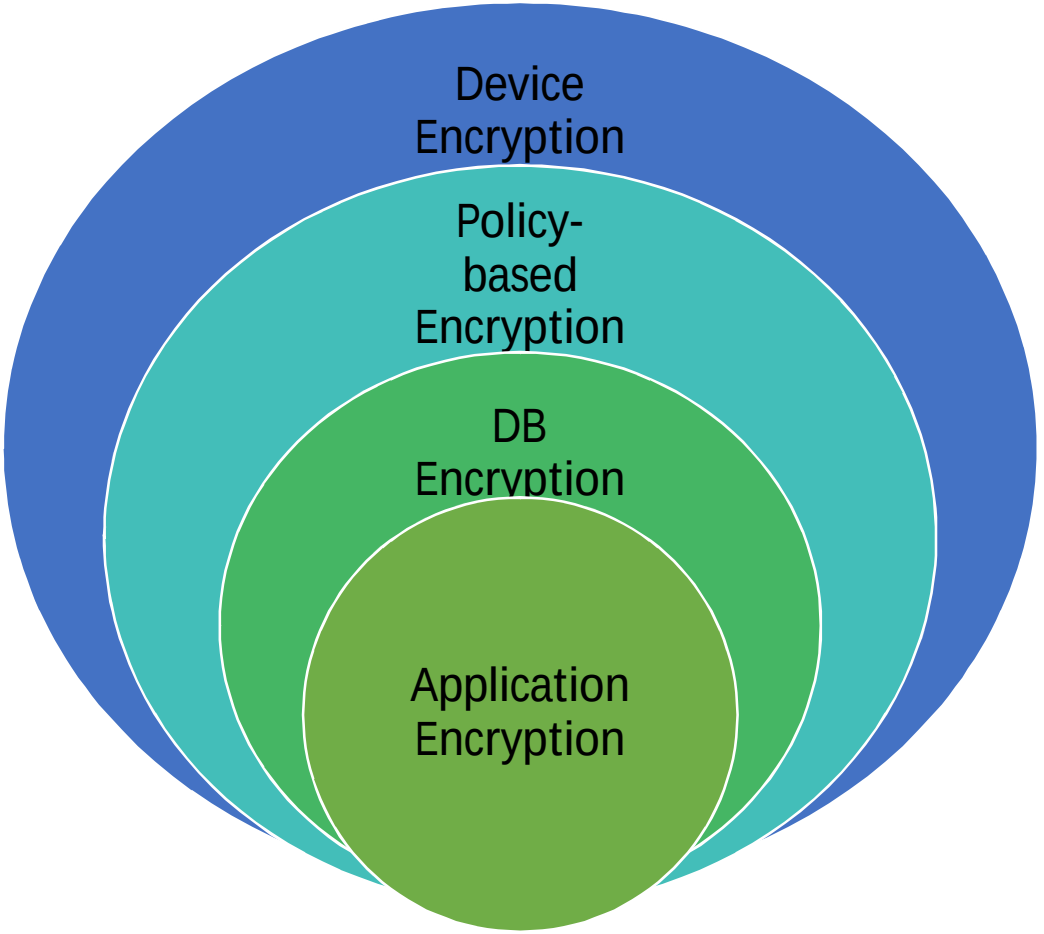
Coupling Facility

- Highlighted in z/OS V2.3 **preview announcement**
  - Plans to encrypt Coupling Facility list and cache structures
- Goal is to encrypt and decrypt CF data as it is sent to and returned from the CF protecting data in flight
- No application changes
- CFCC level 22 is recommended

Layers of Encryption



Layers of Encryption



Segregate roles and duties

- Data Owner
  - Required authority
    - Data Set
    - Key Label

- Storage Administrator
  - Required authority
    - Data Set

Supported filetypes

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

    DB2, IMS, zFS, logs

- Restrictions
  - DFSMSdss REBLOCK ignored on COPY and RESTORE
  - DFSMSdss VALIDATE ignored when backing up encrypted indexed VSAM

Restricted data sets

- Data sets used during IPL
- Catalogs, SHCDS, HSM data sets, ICSF Keystores
- Temporary, SORTWKxx, BLKSIZE<16 (can’t be Extended Format)

Data set lifecycle

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

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
    - Only works for DASD devices
- IDCAMS
  - DEFINE CLUSTER -
    (NAME(DSN1.EXAMPLE.ESDS1) -
    ... -
    KEYLABEL (LABEL.FOR.DSN1))
- SMS Data Class

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)
- Extended Format
  - Sequential support generic, tailored, or zEDC compression
  - VSAM support generic compression

Key labels – business as usual

- Key must be in the CKDS
- Further segregate across line of business, or application or …
  - Unique key per data set
  - Unique key by HLQ
  - Unique key per any qualifier
  - Or any combination thereof

Key Management – the hard part of crypto

- Key Volume
  - Naming Conventions
  - Key administrators – need access to KGUP
  - Tools – EKMF, TKE or …
- Key Criticality
  - Master Keys
  - Process & Procedure
- Key Security
- Operational Key Change
  - Define a new key with new key label
  - Create/copy the data to a new data set

Utilities and Control Blocks

- LISTCAT
  - Encryption Data Section
    - Data Set Encryption (Yes or No)
    - Data Set Key Label
- LISTVTOC
  - Encryption Attribute in SMS.IND field
- ISMF
  - DASD Data Set Level Encryption Management
    - Data Set Key Label
  - Data Set List
    - Encryption Indicator

The Players

- Sysprog – Implement and support ICSF
- ICSF Administrator – Manage the ICSF environment
- Master Key Officers – Own responsibility for the care of master keys
- Key Administrators – define and manage operational (symmetric) keys
- Security Administrator – setup the rules or profiles for securing crypto resources and associating keys with data set profiles
- Storage Administrator – update data classes via ISMF, update ACS routines to associate key labels with data sets
- User – needs the access to the resources, and probably cares the most about the data
- Security Auditor – monitors all of the above

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
  - HCR77C0
  - HCR77A0-HCR77B1 w/APAR OA50450

ICSF Support

- ICSF Segment of the CSFKEYS profile
  - SYMCPACFWRAP(YES) – key is eligible to be used as protected key
  - SYMCPACFRET(YES) – key is eligible to be returned to the caller in wrapped format (RACF APAR OA50367)
- ICSF APIs
  - CKDS Key Record Read2 (CSNBKRR2) – now can return the wrapped key to a caller
- Keylabel – AES-256 bit key

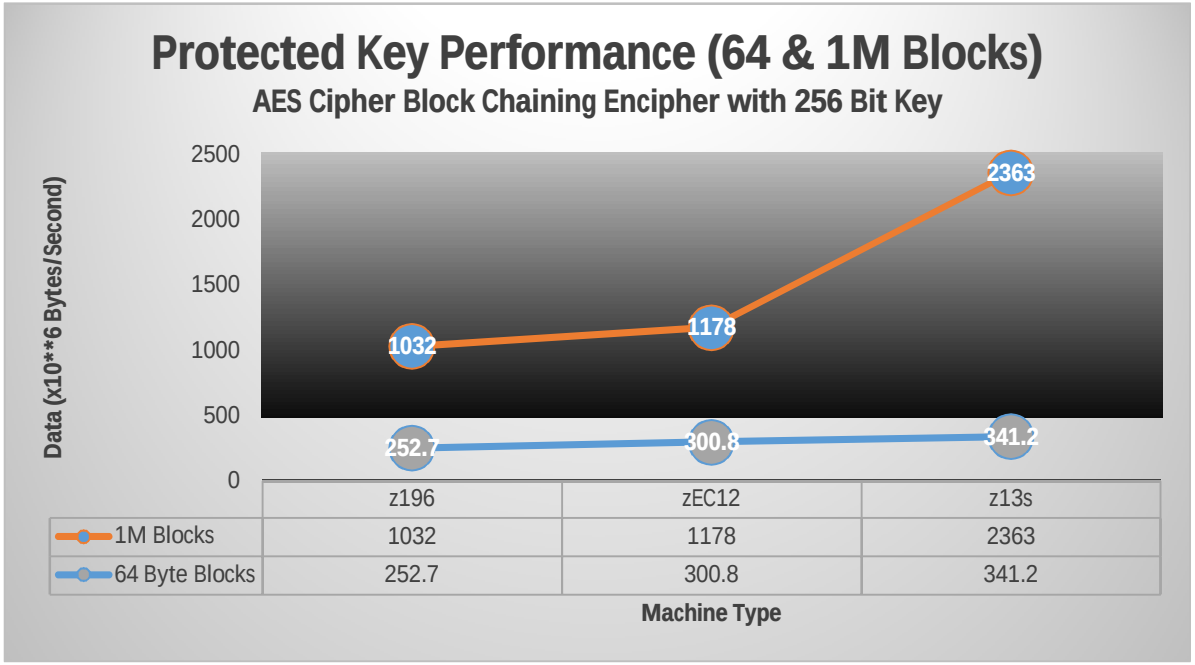
SAF Rules – CSFSERV Class

- CSFSERV
  - CSNBKRR2
    - RDEFINE CSFSERV * UACC(NONE)
    - RDEFINE CSFSERV CSFKRR2 UACC(NONE)
    - PERMIT CSFKRR2 CLASS(CSFSERV) ID(*) ACCESS(READ)

SAF Rules – CSFKEYS Class

- By default, access to key material should be highly restricted!
  - RDEFINE CSFKEYS * UACC(NONE)
  - RDEFINE CSFKEYS keylabel UACC(NONE)
- But, any user that needs the data in the clear must have access to the key label
  - PERMIT keylabel CLASS(CSFKEYS) ID(groupid/userid) ACCESS(READ)
  - PERMIT key-label CLASS(CSFKEYS) ID(*) ACCESS(READ) WHEN(CRITERIA(SMS(DSENCRYPTION)))

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)

IBM z Systems Batch Network Analyzer (zBNA) Tool

- Is being enhanced to help clients estimate the impact of enabling encryption
  - PC Based
  - Analyzes SMF data

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

SMF Records

- Type 14/15 (Sequential data sets)
  - SMF14DEF – Indicator (data set encrypted)
  - SMF14DET – Encryption type
  - SMF14DKL – Key label
- Type 62 (VSAM data sets)
  - SMF62DEF – Indicator (data set encrypted)
  - SMF62DET – Encryption type
  - SMF62DKL – Key label
- DFSMS DCOLLECT

Summary

- From a crypto perspective, there's nothing new here, except:
  - Criticality of keys
  - Volume of keys
- From an operational perspective, there is a lot going on
  - Assigning key labels via RACF, or ISMF or JCL
  - Concept of assigning a key label at data set allocation, not when you create the data
  - Performance impact
  - Potential data set conversion (i.e. making sure PII data sets are extended format)

Pervasive Encryption

- Policy-based – your organization can define a policy that will protect the data using DFSMS constructs
  - Simple (relatively speaking)
  - Automatic (encryption is enabled before the data is created)
  - Bulk encryption
  - Application transparent

References

- Announcement Letters
  - 216-392, Oct. 4, 2016
  - 217-085, Feb. 21, 2017
- 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*

- 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

More references

- *IBM z Systems Webcast, March 7, 2017*

Protection Begins with Data at the Center: Encrypt it all with z Systems Pervasive Encryption - Security Architect Michael Jordan

https://securityintelligence.com/events/protection-begins-with-data-at-the-center-encrypt-it-all-with-z-systems-pervasive-encryption/

Questions?