
MAINFRAME CRYPTO

# Two Nerds Talking about Pervasive Encryption

Greg Boyd

Julie Bergh

# Greg Boyd

gregboyd@mainframecrypto.com

www.mainframecrypto.com

240-772-1539

**Greg Boyd** is a Certified Information Systems Security Specialist (CISSP). Greg retired from IBM in 2014 and started his own consulting firm, Mainframe Crypto, to provide consulting and technical assistance for implementing cryptographic solutions. Prior to leaving IBM, Greg spent the last 10 years providing technical marketing support for the System z Cryptographic hardware and software for IBM's Washington Systems Center. In that role, he assisted customers with installation and technical questions on the cryptographic products, and regularly presented at conferences such as SHARE, IBM's zTechnical University and the Vanguard Security and Compliance Conference.

# Julie Bergh

- **Retired from IBM,** I provided technical leadership and sales support activities to achieve competitive security product take-outs in North America, and promotes sales of additional security product components.
- CISSP-ISSMP, CBCP
- Experienced Security Professional
- Years creating / architecting security solutions on z Systems
- RACF, CA ACF2, CA Top Secret
- Systems Programmer
- IT Management
- Application Programmer
- Audit Director

# IBM Definition of Pervasive Encryption

- Full Disk Encryption
- Integrated Crypto Hardware
- Network Encryption
- Data Set and File Encryption
- Coupling Facility Encryption
- Secure Service Container
- Key Management (EKMF & TKE)

# Configuration requirements

- Machine type
  - zEC12/zBC12 w/CEX3C (FC #0864) or CEX4C (FC #0865)
  - z13/z13s w/CEX5C (FC #0890)
  - Z14
- 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
  - HCR77D1-HCR77C0
  - HCR77A0-HCR77B1 w/APAR OA50450

# Supported File Types

- 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

# Encryption enabled at allocation

- DFP Segment of the SAF data set profile
- JCL, TSO Allocate (Dynamic Allocation)
- IDCAMS
- SMS Data Class

# Crypto Security

- CSFSERV - CSNBKRR2 API
- CSFKEYS - Key Label

- ICSF Keystore Policies
- Healthchecks

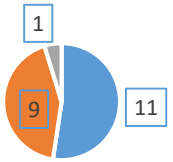
# Key Management

- Key Labels / Naming Standards
- KDSR Format
- Key Rotation
  - Archived data sets
- Key Management Tools
  - TKE
  - EKMF
  - OEM
  - Roll your own

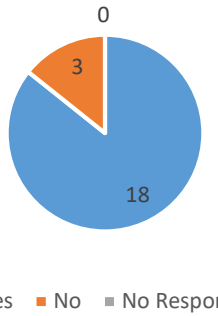
# Questions?

# Survey Results (1 of 2)

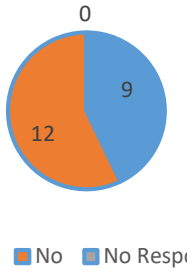
1. Do you have crypto cards, configured in coprocessor mode?



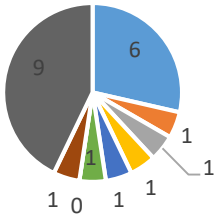

2. Are you using SMS?



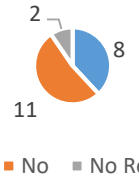

3. Have you identified your PII data?




4. If your answer to question 3 is yes, how much of your PII data is in extended format datasets?

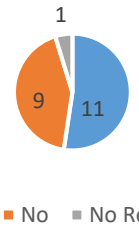



5. Have you implemented your ICSF keystores in KDSR (Key Data Set Reformat)?

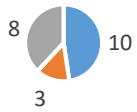


# Survey Results (2 of 2)

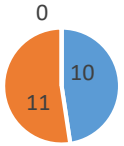
6. Is ESM security set up for using the CSFSERV class?




7. If your answer to question 6 is yes, is it more than just in warning mode?

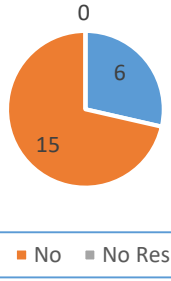



8. Is ESM security set up for using the CSFKEYS class?




9. If your answer to question 8 is yes, is it more than just in warning mode.


10. Do you have a key management policy?




11. Do you have a key management tool? Feel free to name your tool in the Comments box.