MAINFRAME CRYPTO

Dataset Encryption – Just Do It!

Greg Boyd

Julie Bergh

August 2020

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 Intro

- **Recently 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

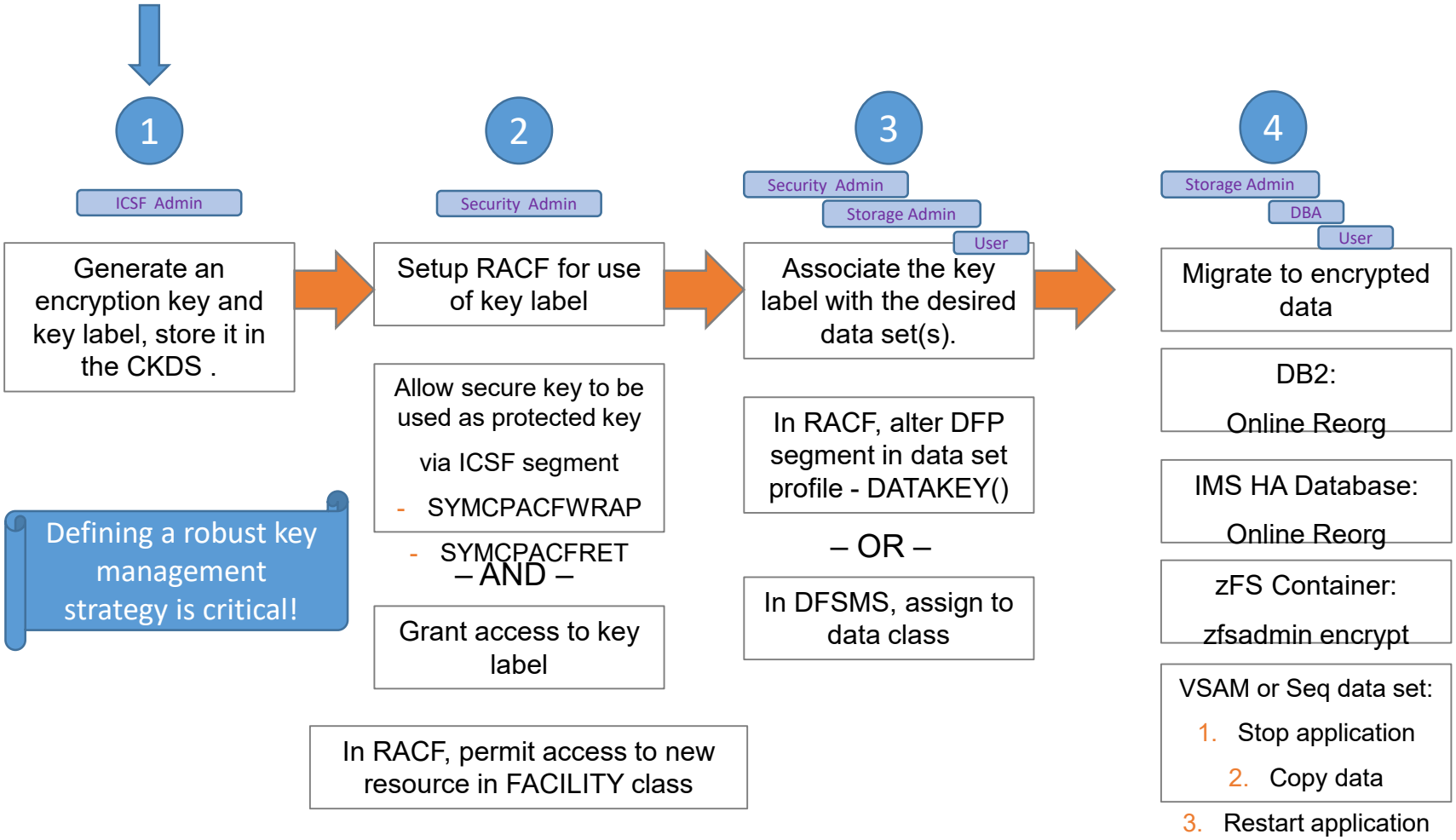
IBM Definition of Pervasive Encryption

- Full Disk Encryption
- Integrated Crypto Hardware
- Network Encryption
- Data Set and File Encryption
- Coupling Facility Encryption
- Secure Service Container
- Key Management (EKMF & TKE)
- z/OS 2.4 (JESSPOOL and PDS/E)

Configuration requirements

- Machine type (z15/z15 T02, z14/z14s, z13/z13s, zEC12/zBC12)
  - With appropriate Crypto Express cards
  - With master keys loaded
- Operating System
  - 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
  - HCR77D1-HCR77C0
  - HCR77A0-HCR77B1 w/APAR OA50450

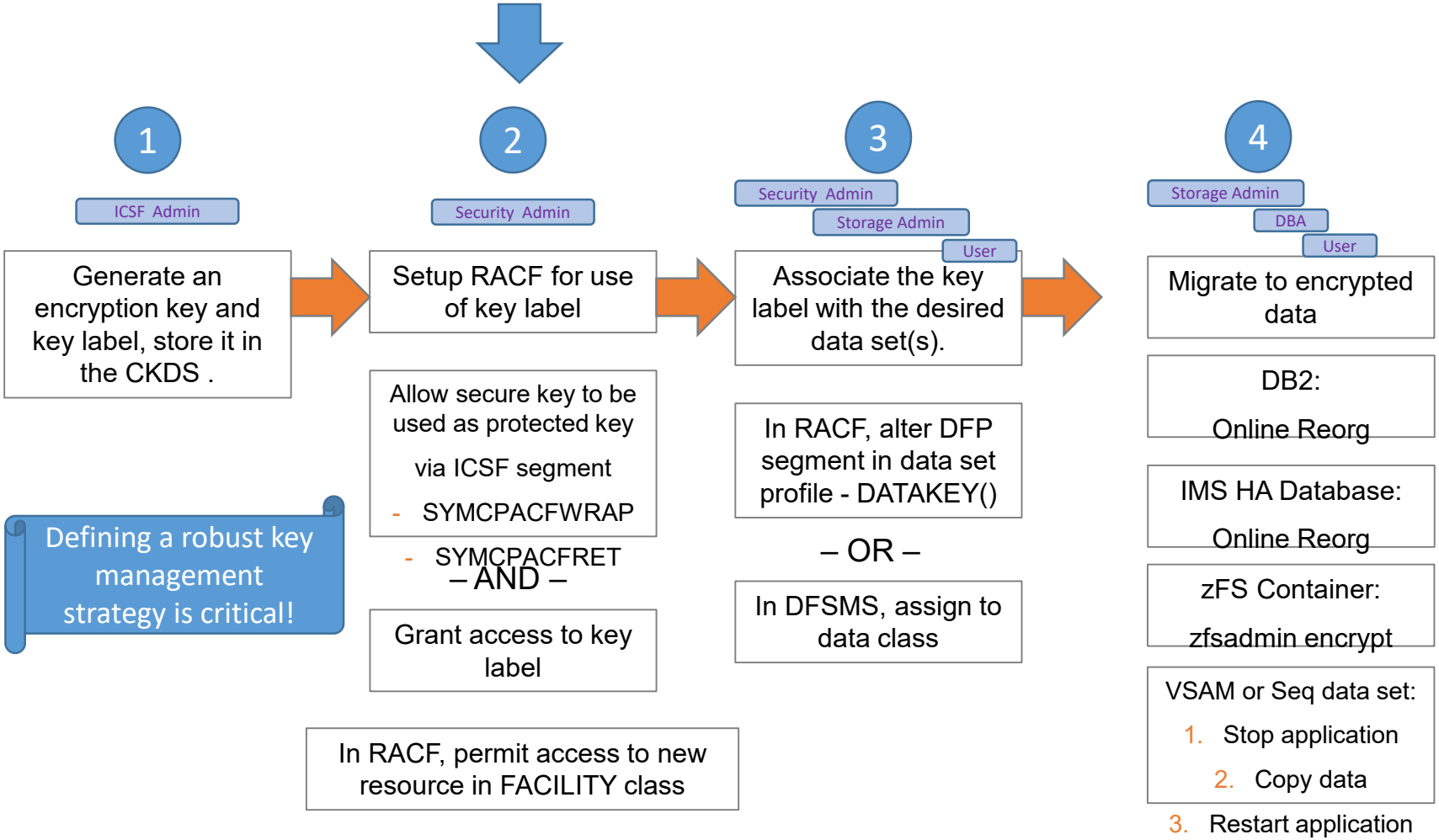
z/OS data set encryption – High Level Steps



Key Management

- TKE – Trusted Key Entry
- EKMF – Enterprise Key Management Facility
- EKMF Web - Enterprise Key Management Facility Web
- IBM SKLM 4.0 for Docker running in a z/OS Container Extensions – Announcement Letter 219-514
- ICSF – Integrated Cryptographic Services Facility

z/OS data set encryption – High Level Steps



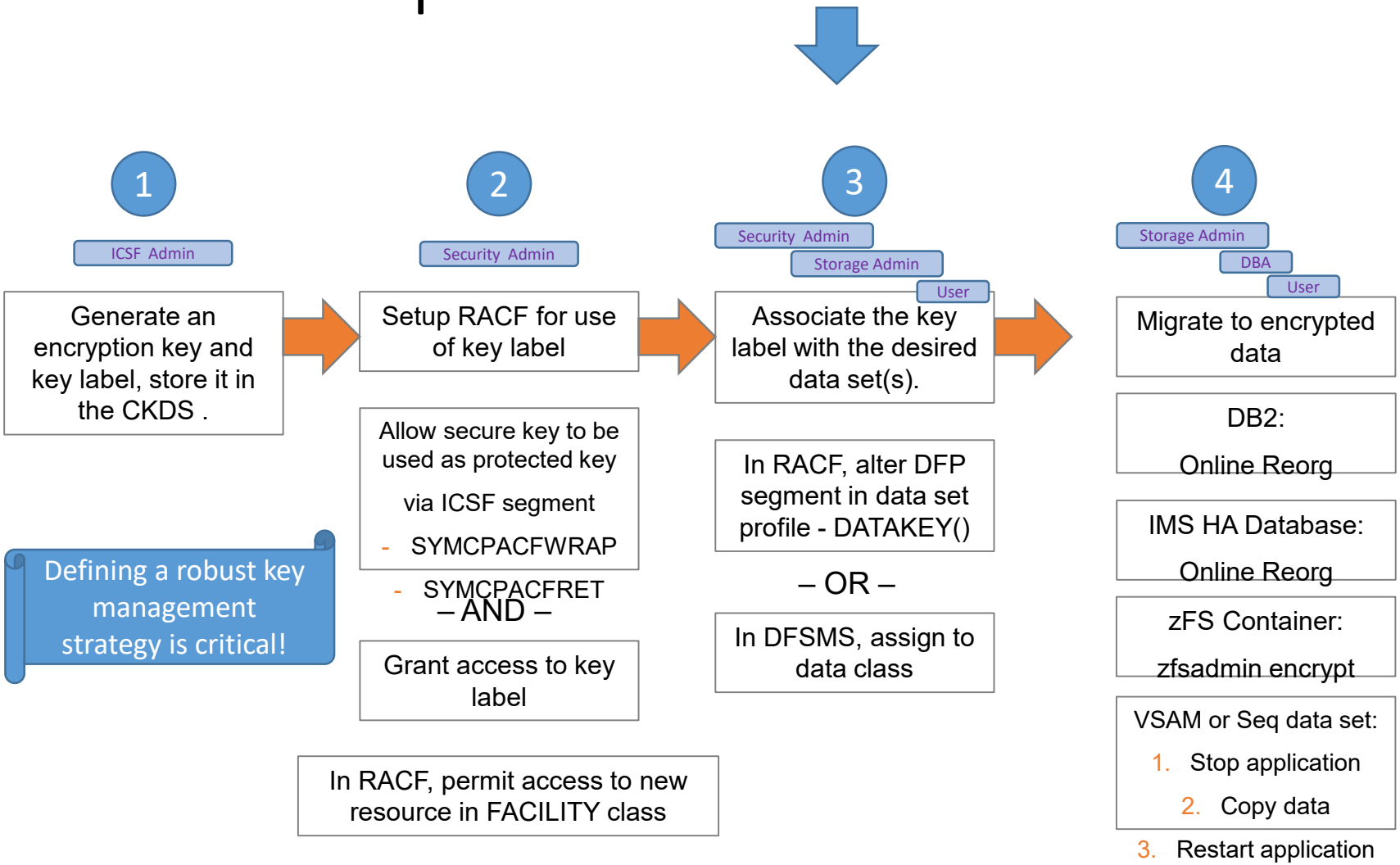
RACF Classes

- CSFKEYS
- CSFSERV
- FACILITY
- OPERCMDS
- XFACILIT
  - ICSF – key store policies additional support – strongly implement. For example prohibit duplicate keys.
- DFP Segment
- ICSF Segment

Encryption enabled at allocation

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

z/OS data set encryption – High Level Steps



How do you rotate keys?

There are two types of key rotation that you can perform on IBM Z:

- Master Key Rotation
- Operational Key Rotation

Master Keys	Operational Keys
Master keys are used only to encipher and decipher keys.	Operational keys are used in various cryptographic operations (e.g. encryption).
Master keys are stored in secure, tamper responding hardware.	Operational keys may be stored in a key store (e.g. data set, file, database) or returned back to the caller.

Operational keys may be encrypted by a Master Key to be considered secure keys.

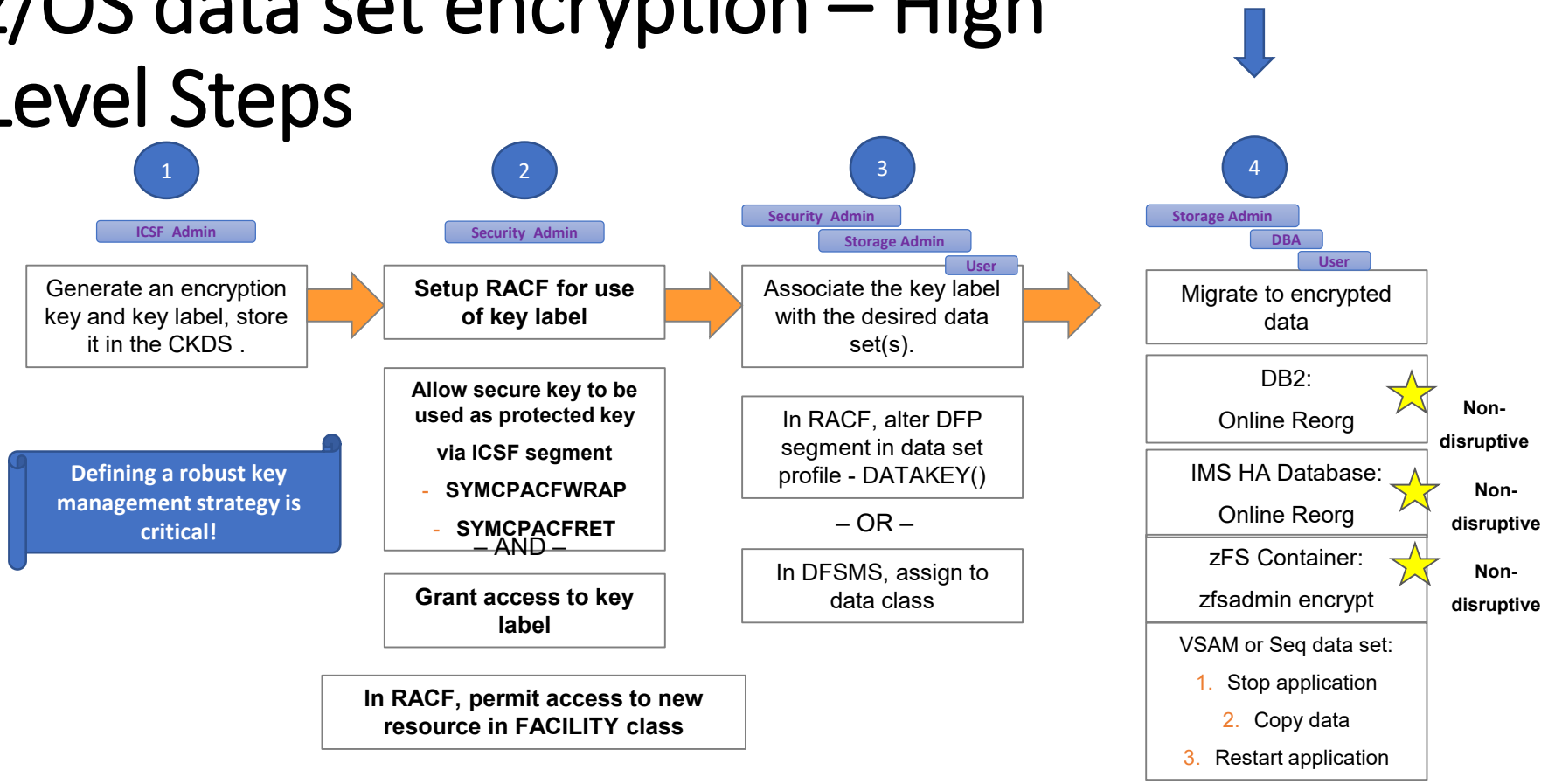
When can you delete an operational key used with data set encryption?

Life of data set = Life of key

NIST SP800-57 Recommendation
for Key Management

Part 1-3

z/OS data set encryption – High Level Steps



z/OS Data Set Encryption

Questions?