MAINFRAME CRYPTO

Key Labeling

Greg Boyd (gregboyd@mainframecrypto.com)

February 2023

Copyrights and Trademarks

- Copyright © 2023 Greg Boyd, Mainframe Crypto, LLC. All rights reserved.
- Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 30+ years

- 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 – Key Labeling

- Master Keys
- Operational Keys
  - Purpose of Key Labels
- Data Set Encryption

Master Keys / Operational Keys

- Master Keys
  - 4 CCA Master Keys (DES-MK, AES-MK, ECC-MK, RSA-MK) and 1 EP11 Master Key (P11-MK)
  - Encrypt other (operational) keys
- Operational Keys
  - Encrypt data (messages, data sets, ATM PINs, other keys)

Master Keys and Master Key Parts

- ~~Passphrase Initialization (a passphrase is used to generate 4 CCA master keys: AES-MK, DES-MK, ECC-MK and RSA-MK)~~
- ICSF Panels
  - Multiple key parts (i.e., random numbers) are loaded and combined to create each of the 4 CCA master keys)
  - Each key part must be securely stored and available for recovery purposes
- Trusted Key Entry Workstation
  - Multiple key parts (i.e., random numbers) are stored on a smart card, which is secured by the PIN technology of the smart card

Why do we need key labels

- Index into the VSAM KSDS keystore (to find the record)
- Security (to find the SAF profile in the CSFKEYS class)
- Key lifecycle management
  - Key rotation
  - Purpose or ownership

ICSF Key Labels

- 64 byte character string, left justified, right padded with blanks
- 1st character alphabetic or national (#, $, @)
- The rest can be alphanumeric, national or period (.)
- All alphabetic are upper case

- ‘Node’ Separator, not required, but recommended

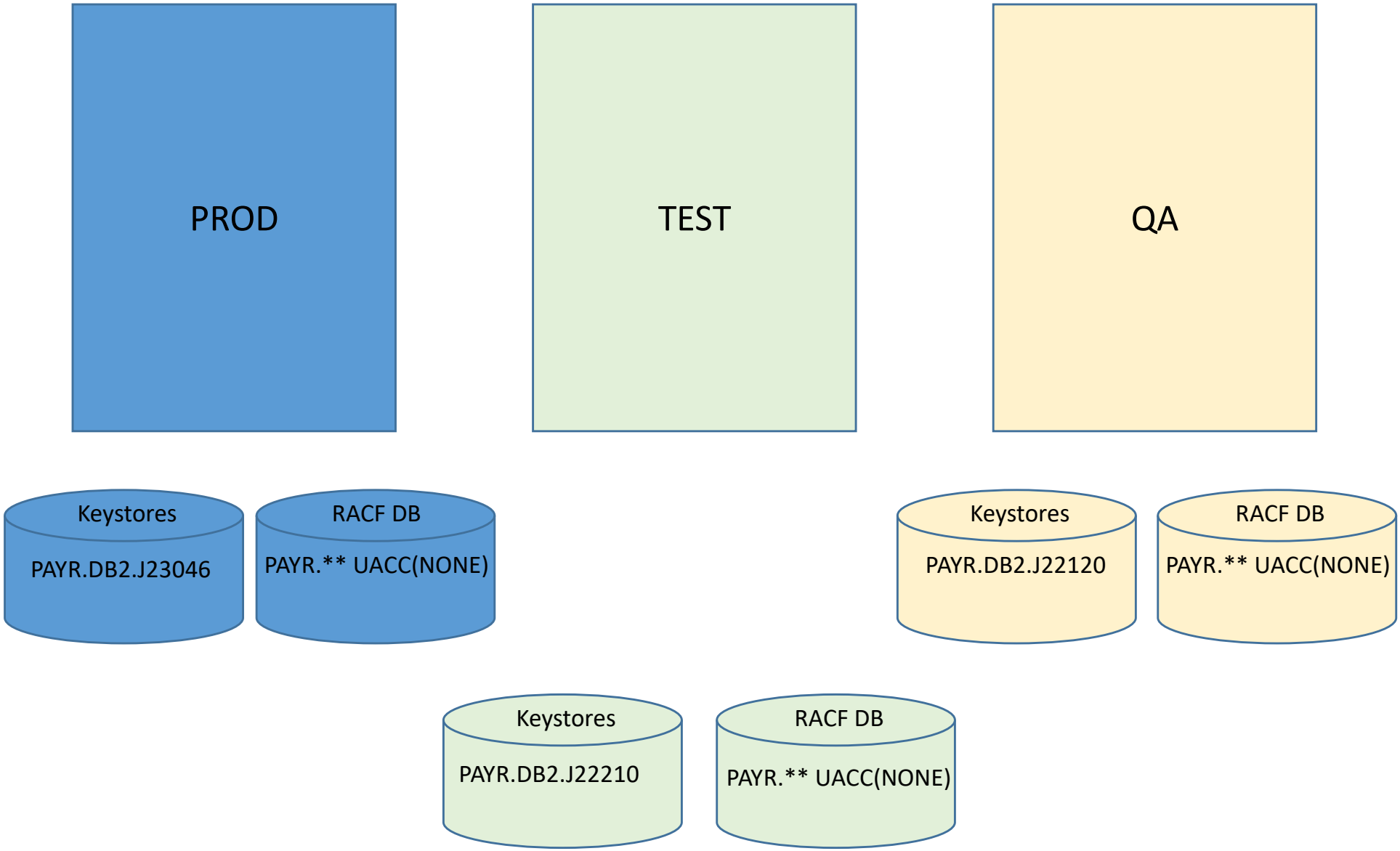
Key Labels and SAF profiles

- Bad Examples
  - THISISAREALLYLONGKEYLABELTHATHAS44CHARACTERS
  - MYKEY
  - X
- Good Examples
  - env.application.algorithm.date
    - PROD.APPX.AES256 .D180321 SAF(PROD.APPX.**)
  - env.businessunit.usage.algorithm.date
    - PROD.PERS.PAYROLL .D20180321 SAF(PROD.PERS.PAYROLL.*)
    - PROD.PERS.MEDICAL .D20180321 SAF(PROD.PERS.MEDICAL.*)
  - subsys.application. date.identifier.sequence
    - DB2.APPX.20180316. PAYROLL.V1 SAF(DB2.APPX.*.PAYROLL.*)
    - CICS.APPX.20180321.PARYOLL.V1 SAF(*.APPX.*PAYROLL.*)

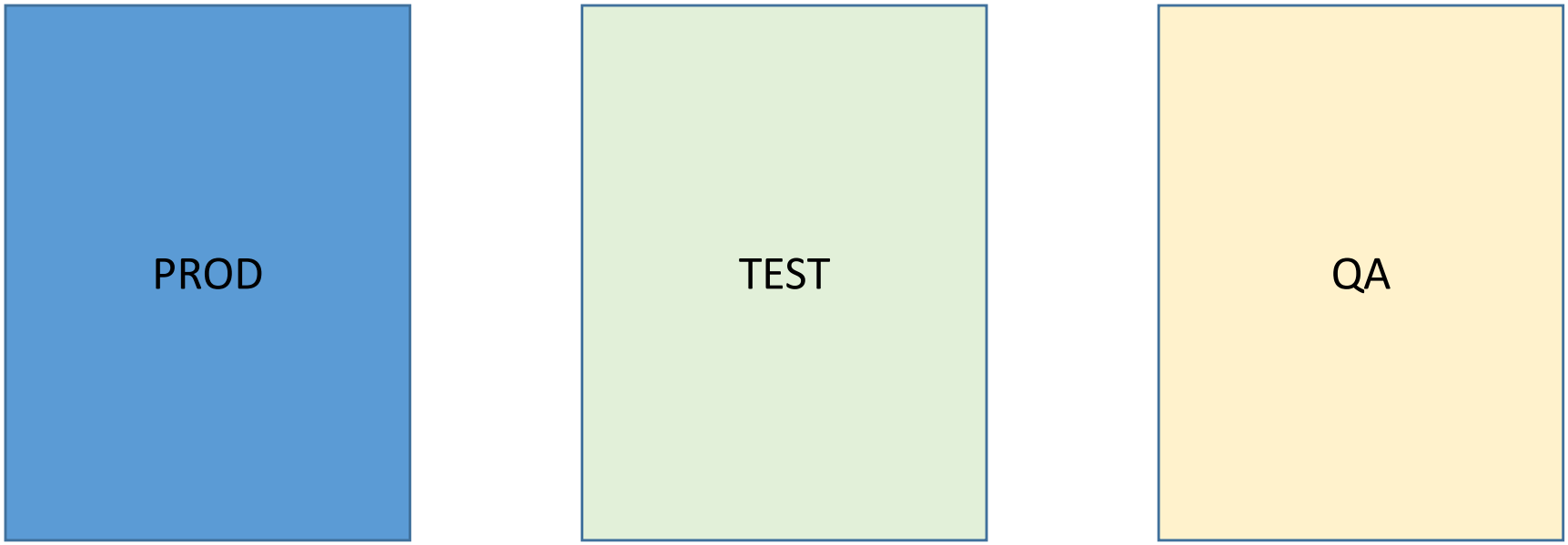
Qualifiers

- Userid – BOYDG, TS159876
- Environment – PROD, TEST, QA, SYSPROG
- Purpose – DSE, PE, ATM, GUARDium
- Organization/Business Unit – PERS, FIN, MFG
- Application – APPX, CostCenter, DB2
- Secondary Application – APPY
- Generation/Cycle – V01, 00001, 001
- Date – J23046, 20230215, D230215, D20230215

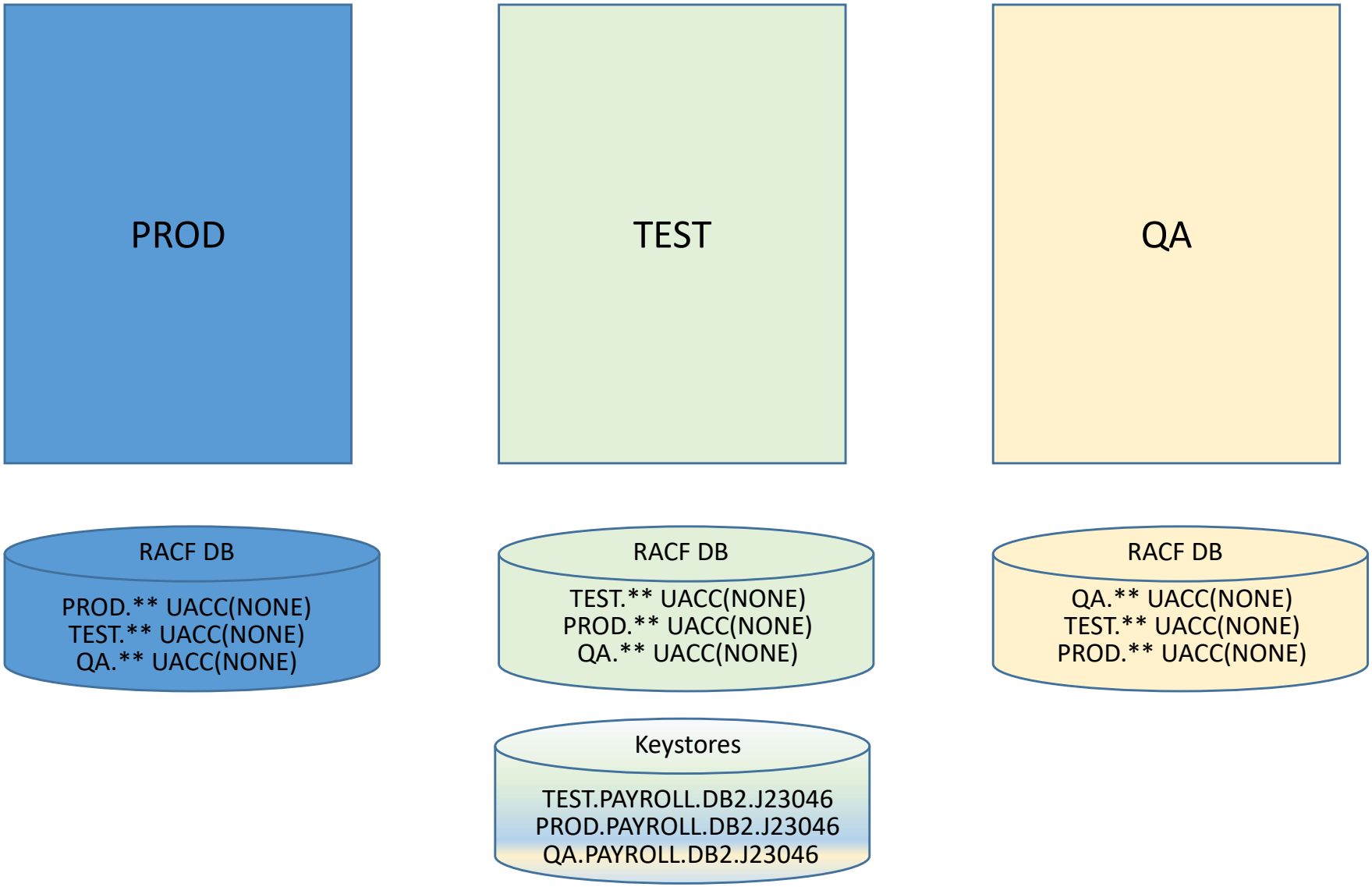
Isolated Environments



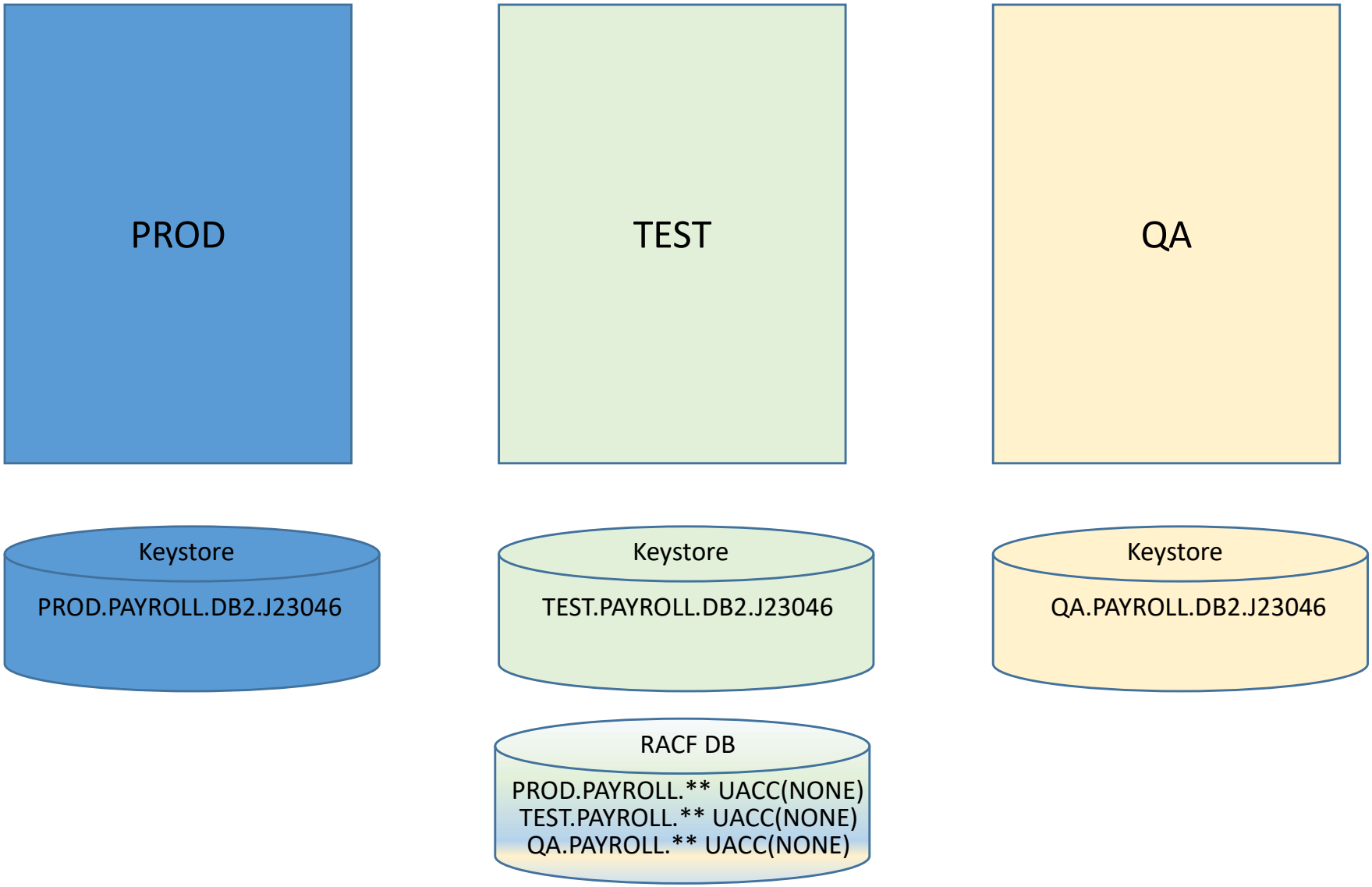
Shared Environments



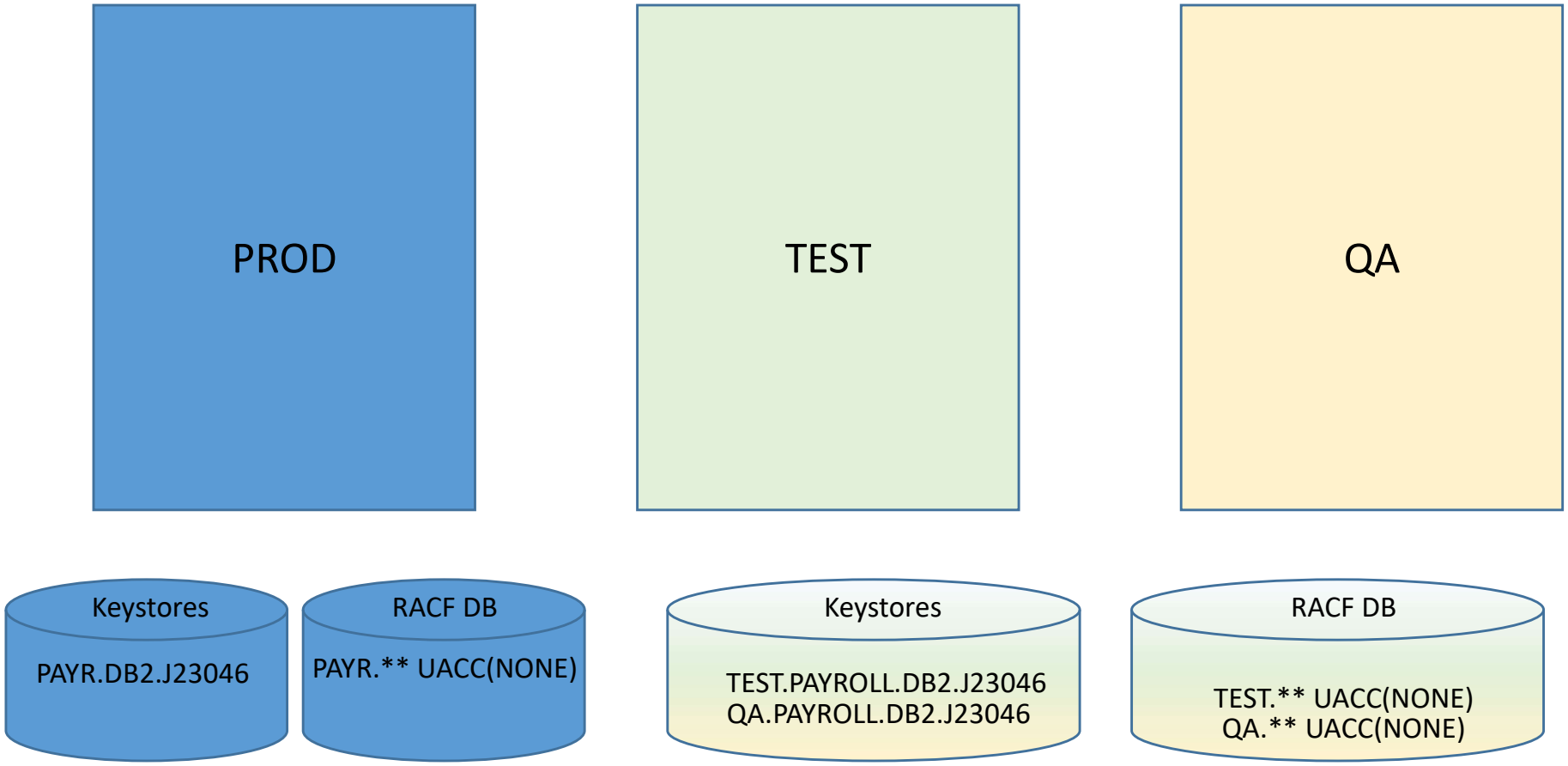
Shared Keystore/Unique RACF DB



Shared RACF DB / Unique Keystore

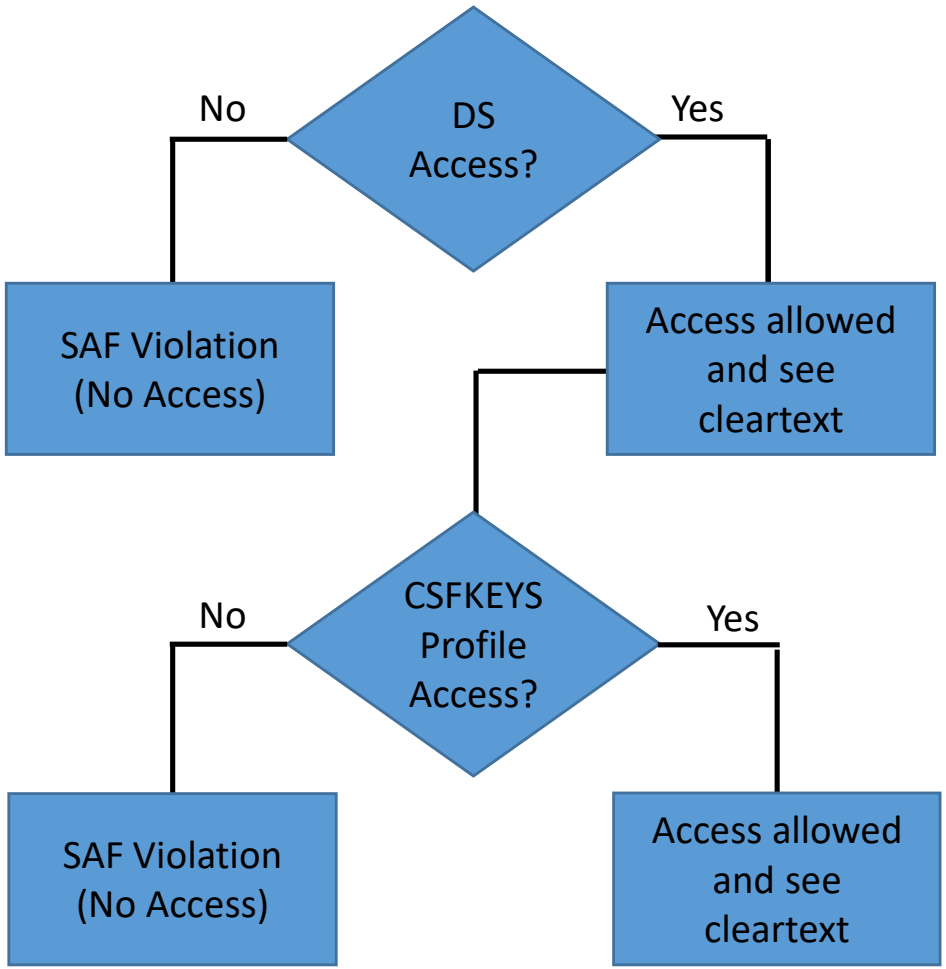


Shared Environments

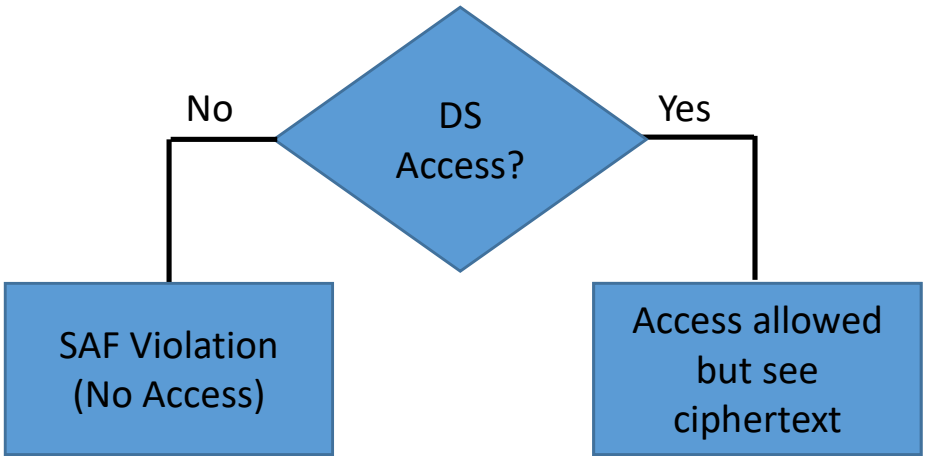


DSE and Access Methods

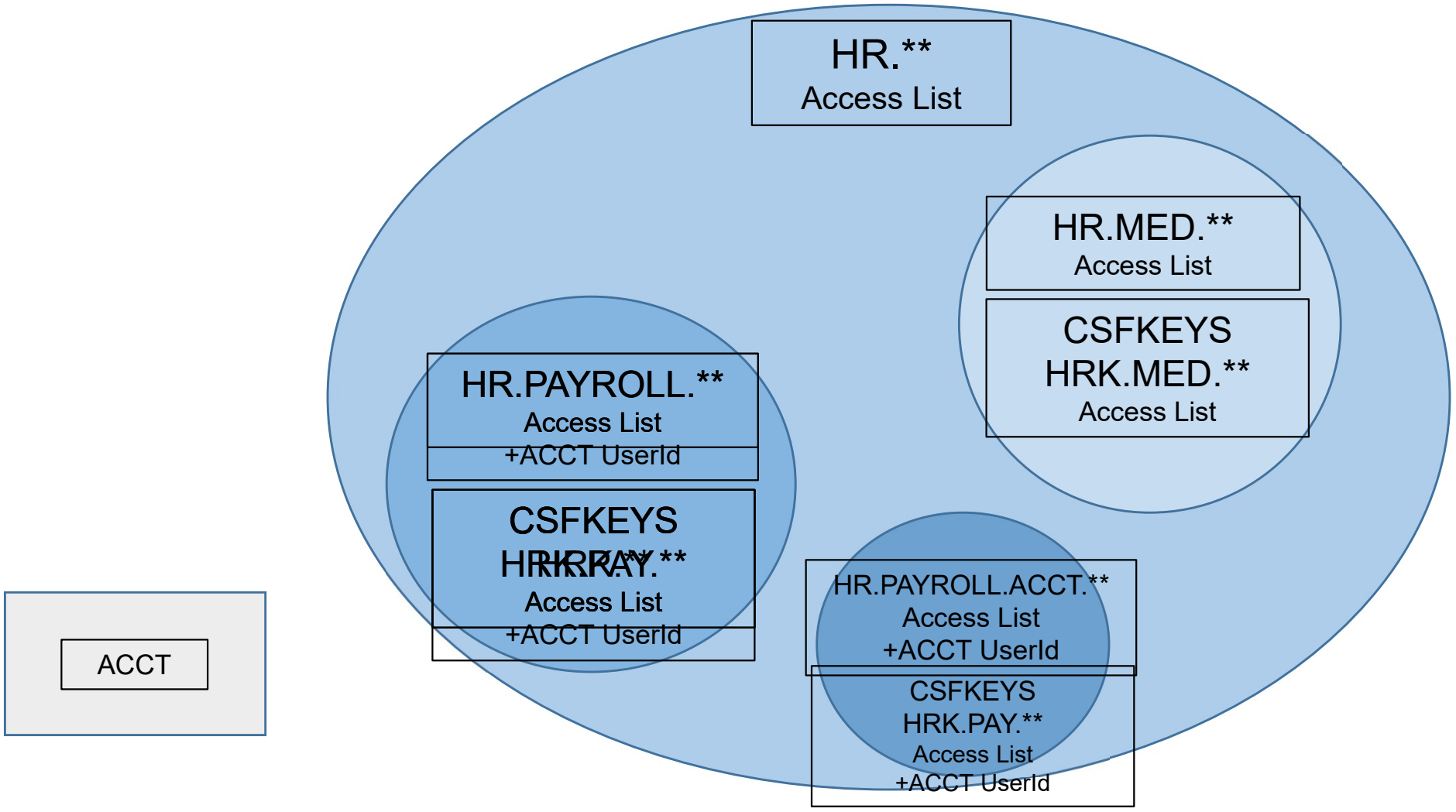
Standard Access Method
and
data set flagged for encryption



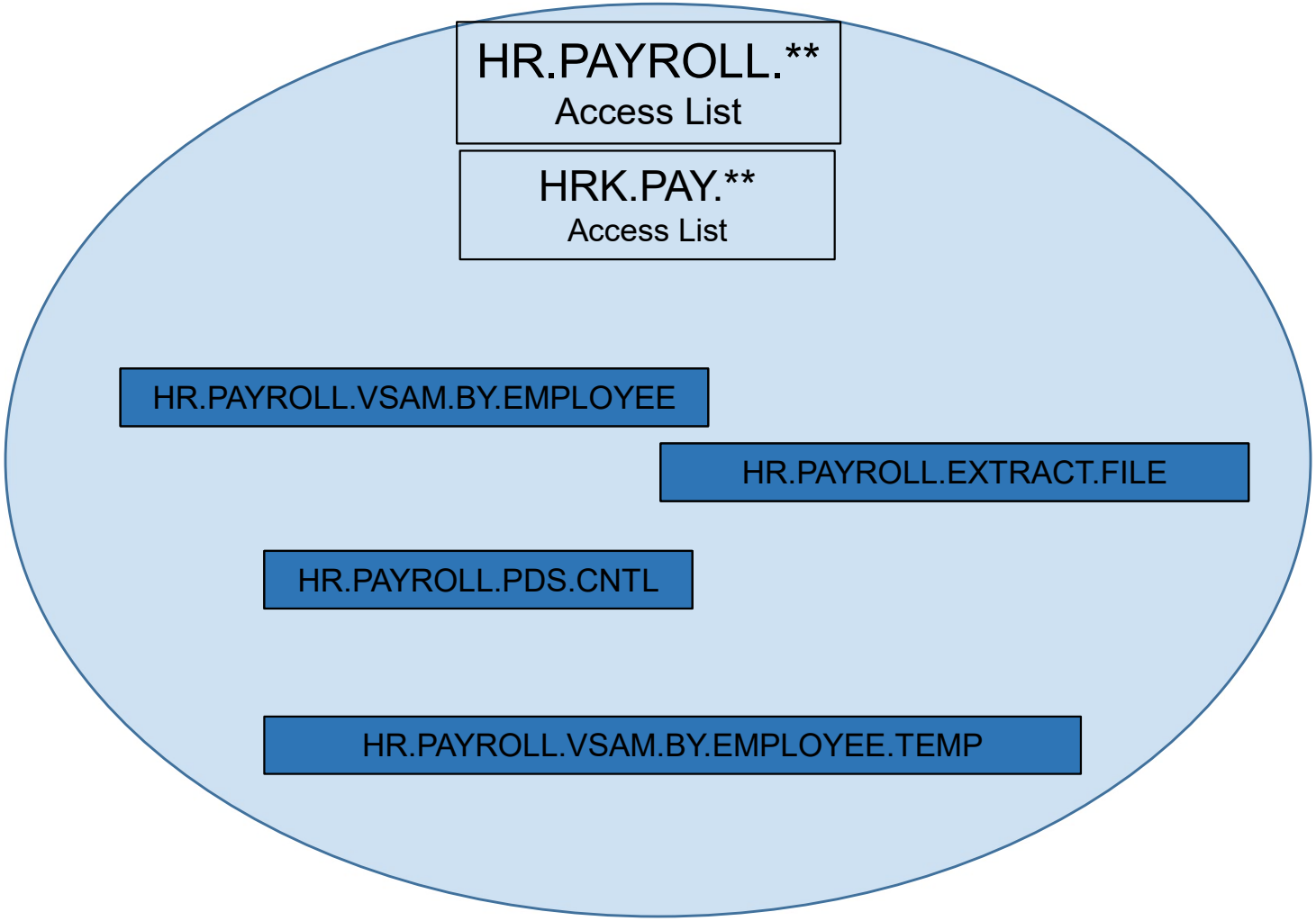
Non-Standard Access Method
and
data set flagged for encryption



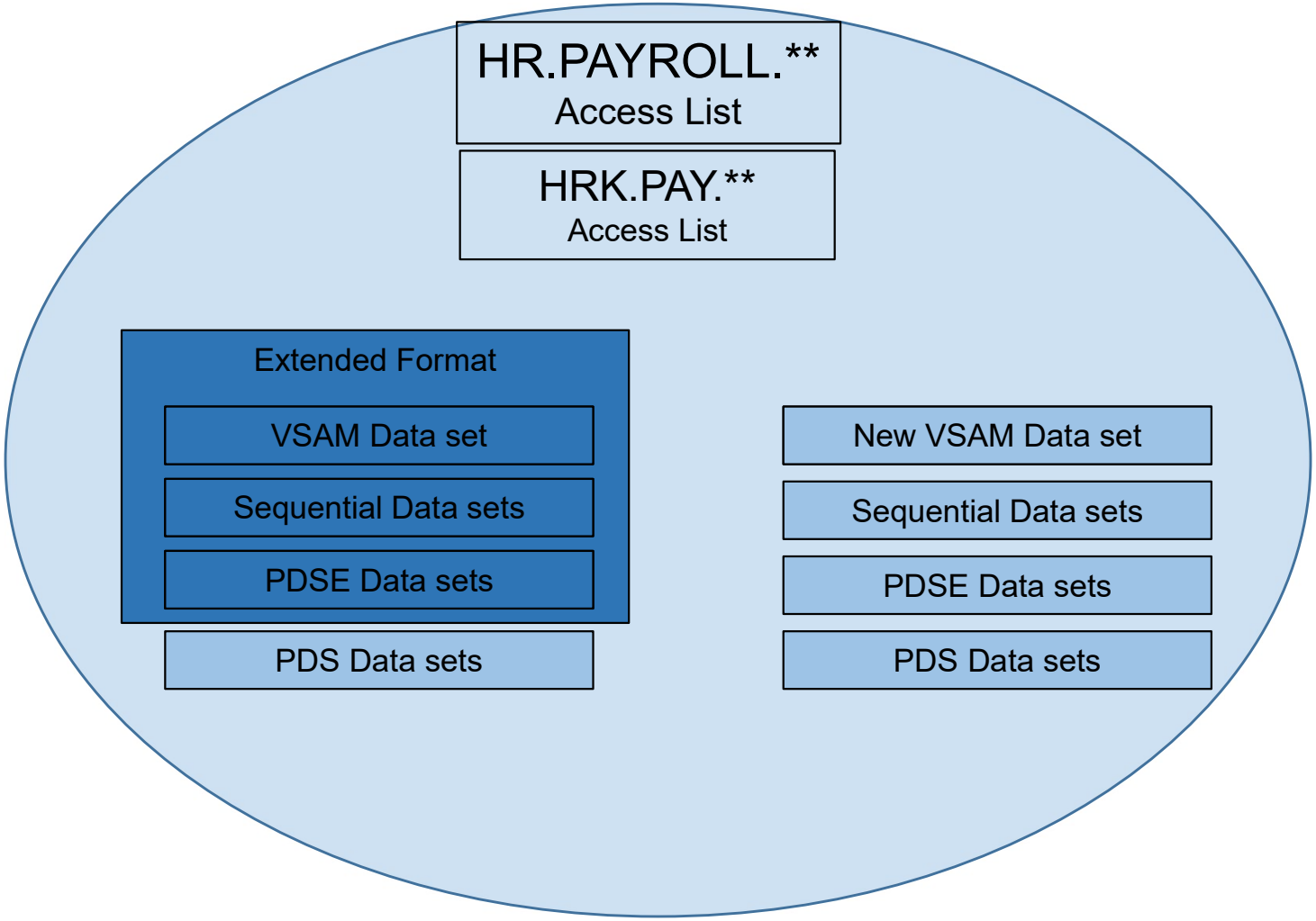
Key Label Access



PII vs non-PII Data Sets



Eligible Data Sets



READ ACCESS to FACILITY Profile

STGADMIN.SMS.FAIL.INVALID.DSNTYPE.ENC

Summary

- Secure your keys
- Key management is important; Use your key labels to
  - Know the purpose/owner
  - Know where the key is, in it's lifecycle
- Start small, with the number of keys

References

- NIST SP 800-57 Part 1 Rev 5 Recommendation for Key Management, Part 1: General
  - https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final
- ICSF Manuals
  - SC14-7507 ICSF System Programmer's Guide
  - SC14-7506 ICSF Administrator's Guide
  - SC14-7508 ICFS Application Programmer's Guide
- Redbook
  - SG24-8410 Getting Started with z/OS Data Set Encryption

Questions?