MAINFRAME CRYPTO

Key Rotation – Which? When? Who? How?

Greg Boyd

gregboyd@mainframecrypto.com

www.mainframecrypto.com

Copyrights And Trademarks

Agenda – Key Rotation

- Why?
- When?
- Which?
- Who?
- How?

Why rotate keys?

- Because the standards say so

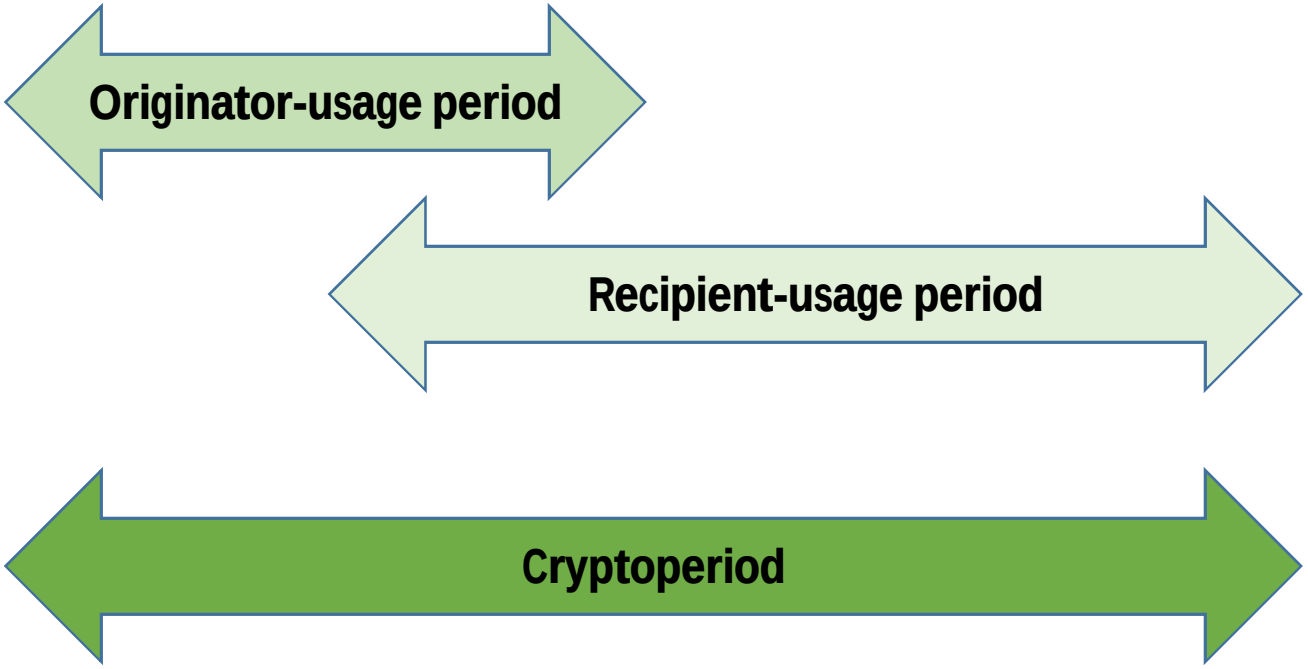
- Limit the amount of data (encrypted by a key)
- Key leakage

PCI DSS 3.6.4

- **Requirement**
  - **3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod** (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).
- Guidance
  - **A cryptoperiod is the time span during which a particular cryptographic key can be used for its defined purpose.** Considerations for defining the cryptoperiod include, but are not limited to, the strength of the underlying algorithm, size or length of the key, risk of key compromise, and the sensitivity of the data being encrypted.
  - Periodic changing of encryption keys when the keys have reached the end of their cryptoperiod is imperative to minimize the risk of someone's obtaining the encryption keys, and using them to decrypt data.

When to rotate keys?

- Whenever your security policy says ...



Cryptoperiod - Symmetric

Key Type	Originator-Usage Period (OUP)	Recipient-Usage Period
Symmetric Authentication	<=2 years	<=OUP + 3 years
Symmetric Data Encryption	<=2 years	<=OUP + 3 years
Symmetric Key Wrapping	<=2 years	<=OUP + 3 years
Symmetric RBG	See SP800-90	--
Symmetric Master	About 1 year	--
Symmetric Key Agreement	1 to 2 years	

Table 1, Suggested cryptoperiods for key types

Recommendation for Key Management Part 1: General

NIST SP800-57 Part 1 Release 4

Cryptoperiod - Asymmetric

Key Type	Originator-Usage Period (OUP)	Recipient-Usage Period
Private Signature	1 to 3 years	--
Public Signature-Verification	Several years (depends on key size)	
Private Authentication	1 to 2 years	--
Public Authentication	1 to 2 years	--
Private Key Transport	<=2 years	
Public Key Transport	1 to 2 years	
Symmetric Key Agreement	1 to 2 years	
Private Static Key Agreement	1 to 2 years	
Public Static Key Agreement	1 to 2 years	
Private Ephemeral Key Agreement	One key-agreement transaction	
Public Ephemeral key Agreement	One key-agreement transaction	

Risks that affect Cryptoperiod

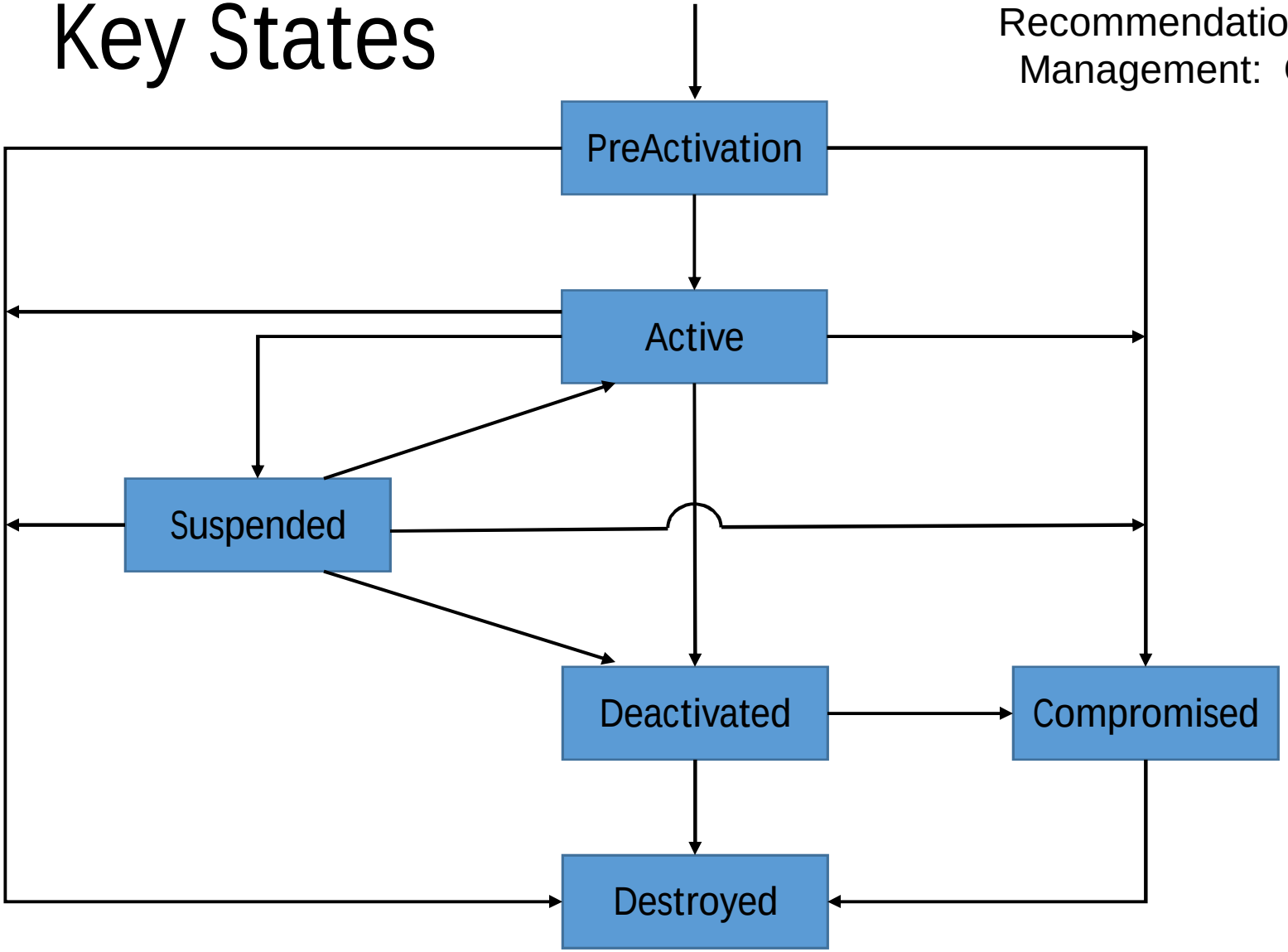
- Strength of the crypto mechanism (algorithm, key length, block length, mode)
- Security of the crypto module (FIPS 140 Level 4) vs software
- Operating environment (secure facility vs open office environment vs publicly accessible terminal)
- Volume of information (number of bytes or transactions)
- Lifecycle of the data
- Security function (data encryption, digital signature, key protection)
- Rekeying method (human intervention, vs PKI vs key management system)
- Key update or key-derivation process
- Number of nodes that share the key
- Number of copies of the key and the distribution process
- Personnel turnover
- Value of the data to attackers
- Threat to the data from new, disruptive technologies

Other Factors (related to cryptoperiod)

- Operational Impact
  - Cost of an outage
    - Guardium Tool, Pervasive Encryption (non-DB2)
      - An outage is required
    - Pervasive Encryption (DB2)
      - Supports dynamic key rotation
- DoS Risk
  - How complicated is the key change process? (How long does it take?)
  - What is the risk if there is a problem?

Key States

From SP800-57 Part 1 Recommendation for Key Management: General



Which keys?

- All keys … but the cryptoperiod will be different
  - Symmetric Keys
  - Signing Keys
  - Key Management Keys

- Only master keys?
  - No, a master key is just a data key, where the encrypted data is … other keys

Who? And How?

- Depends on the implementation
  - Guardium Infosphere
    - DBA
  - Pervasive Encryption
    - Owner?
    - Storage Admin?
  - Application Encryption
    - Application coder
  - Digital Certificates

Data Set Encryption - Reencipher (1 of 5)

PROD.CUSTDATA.**
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEYX)

Ciphertext file, protected by PRODCUST.KEY1

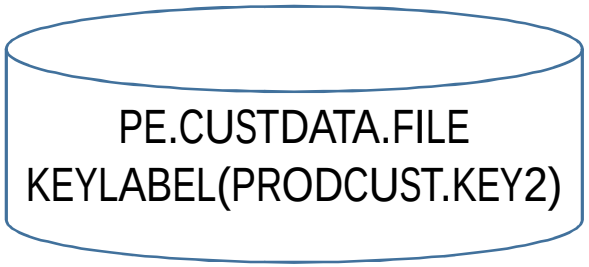
Data Set Encryption - Reencipher (2 of 5)

PROD.CUSTDATA.**
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEYX)

PE. **
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEY2)

Create a new data set profile, referencing the new key label, PRODCUST.KEY2

Data Set Encryption - Reencipher (3 of 5)

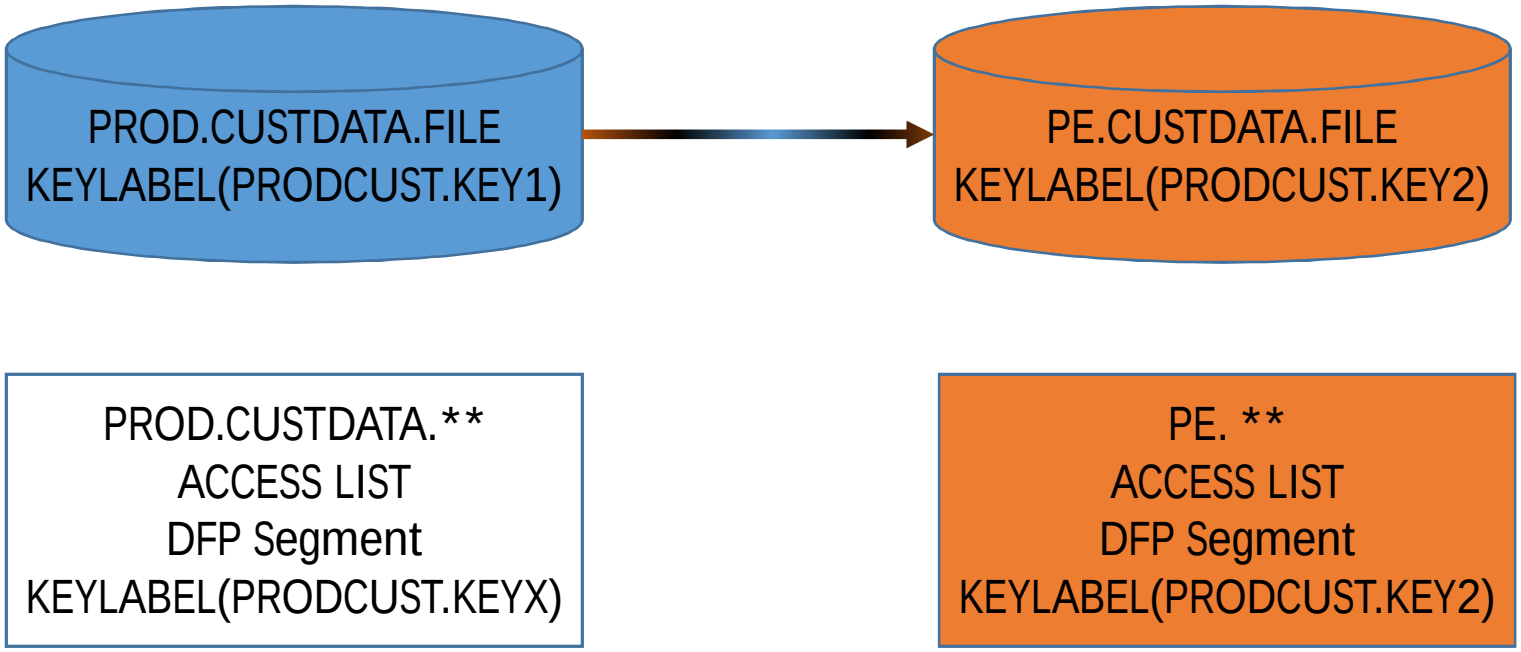


PROD.CUSTDATA.**
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEYX)

PE. **
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEY2)

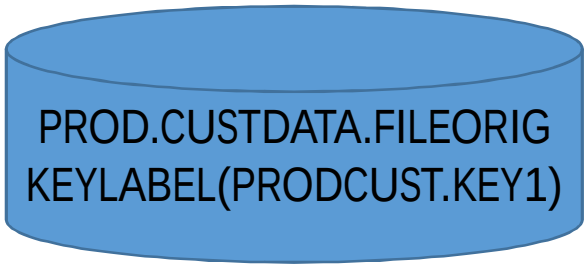
Allocate

Data Set Encryption - Reencipher (4 of 5)



Copy the file

Data Set Encryption - Reencipher (5 of 5)

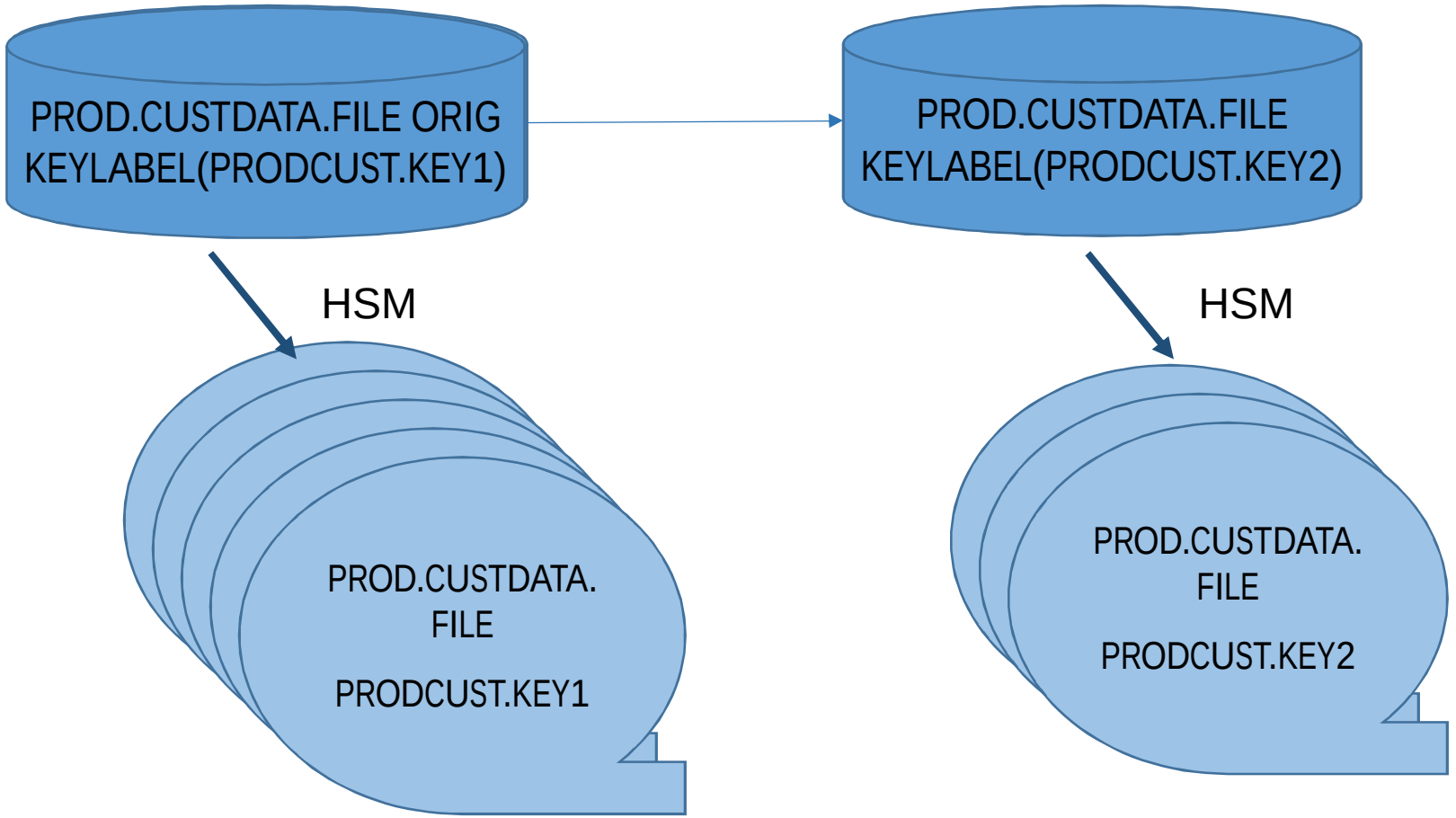


PROD.CUSTDATA.**
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEYX)

PE. **
ACCESS LIST
DFP Segment
KEYLABEL(PRODCUST.KEY2)

Rename the two files

Data Set Encryption - Archives



zDMF

- IBM z/OS Dataset Mobility Facility V3.4
  - Announcement letter 218-533, Oct. 23, 2018
  - Support for encryption of extended format data sets during migration
- December 2018
  - zDMF encrypts EF data sets while in use
- 2Q2019
  - zDMF converts basic/large format data sets to EF data sets and encrypts at the same time
  - zDMF will reencipher the data set
- Future
  - Support additional data set types
  - Dynamic data set compression option

When to rotate keys

- Routine
  - Whenever your standards call for key rotation
- Non-routine
  - In case of emergency

References

- NIST SP 800-57 Part 1 Rev 4 Recommendation for Key Management, Part 1: General
  - https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final
- PCI DSS 3.2.1
  - https://www.pcisecuritystandards.org/document_library
- zDMF Announcement
  - https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=897/ENUS218-533&infotype=AN&subtype=CA
  - Or Google IBM zDMF Announcement
- NIST SP 800-90A Rev. 1 Recommendations for Random Number Generation Using Deterministic Random Bit Generators
  - https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final