MAINFRAME CRYPTO

Unscrambling the Complexity of Crypto!

Key Rotation – Who? What? When? Where? Why? (But not necessarily in that order) Greg Boyd gregboyd@mainframecrypto.com

NY/ Tampa RUG

Copyrights and Trademarks

NY/Tampa RUG

© 2023

- 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 Rotation

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

© 2023

• Where/How?

Why rotate keys?

NY/Tampa RUG

• Because the standards say so!

PCI DSS v4.0 Section 3.7.4

Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following:

- A defined cryptoperiod for each key type in use.
- A process for key changes at the end of the defined cryptoperiod.
- Guidance

C 2023

- A cryptoperiod is the time span during which a cryptographic key can be used for its defined purpose. Cryptoperiods are often defined in terms of
 - the period for which the key is active and/or
 - the amount of cipher-text that has been produced by the key.

Risks that affect Cryptoperiod

- Strength of the crypto mechanism (algorithm, key length, block length, mode)
- Security of the crypto module (HSM) 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

Tampa RUG

- 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

2023

- Value of the data to attackers
- Threat to the data from new, disruptive technologies

NIST SP 800-57 Part 1 Revision 5 Recommendation for Key Management Part 1 - General

NY/Tampa RUG - Key Rotation

NY/Tampa RUG

© 2023



NIST SP 800-57 Part 1 Revision 5 Recommendation for Key Management Part 1 - General

NY/Tampa RUG - Key Rotation

© 2023

Cryptoperiod - Symmetric

Кеу Туре	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/Key Derivation Key	About 1 year	
Symmetric Key Agreement	1 to 2 years	
Symmetric Authorization	<=2 years	

Table 1, Suggested cryptoperiods for key typesNIST SP800-57 Part 1 Revision 5Recommendation for Key Management: Part 1 - General

Cryptoperiod - Asymmetric

Кеу Туре	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		
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		
Private Authorization	<=2 years		
Public Authorization	<=2 years		

When? (Other factors)

- Operational/Cost Impact
 - Outage required?

NY/Tampa RUG

© 2023

- Performance impact?
- What if there is a problem?

© MAINER



Which keys?

Tampa RUG

© 2023

- 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? It Depends ...

- On the 'owner' of the data
 - DB2 databases DBAs
 - Application files

NY/Tampa RUG

- Data Set Encryption
 - Application owner
 - Production control
 - Storage Admins
- Application encrypted Application owner
- Public/private keys (Digital certificates)
 - PKI

© 2023

• Security Admin

© 2023

How (Utility)?

- Data set type
 - Sequential IEBGENER
 - PDSE IEBCOPY
 - VSAM IDCAMS
 - Application encryption Local application

How (Operationally)?

- How is the data used
 - Output files
 - Online

NY/Tampa RUG

• Batch

© 2023

Output Files (1 of 2)





DAILY.REPORT.FILE.*

ACCESS LIST

DFP Segment KEYLABEL(REPORT.KEY1)

© 2023

DAILY.REPORT.FILE.G031V000 KEYLABEL(REPORT.KEY1) DAILY.REPORT.FILE.G030V000 G029V000 KEYLABEL(REPORT.KEY1) T.KEY1)

Page 15

(C) MAINFE

Output Files (2 of 2)





DAILY.REPORT.FILE.*

ACCESS LIST

DFP Segment KEYLABEL(REPORT.KEY2)

© 2023

DAILY.REPORT.FILE.G032V000 KEYLABEL(REPORT.KEY2) DAILY.REPORT.FILE.G031V000 G030V000 KEYLABEL(REPORT.KEY1) T.KEY1)

Page 16

(C) MAINER

NY/Tampa RUG

© 2023

Unscrambling the Complexity of Crypto!



DFP Segment KEYLABEL(PRODCUST.KEY2)

Page 17

© MAI

NY/Tampa RUG

Unscrambling the Complexity of Crypto!

DB2 Databases - Reorg







Wrap-Up

- Key Management Policies
 - Which keys apply to which data
 - Key label conventions
 - Key lifecycles
 - By application
 - By key type
 - By audit requirement
 - Key rotation

© 2023

- Routine
- Non-routine
- Key rotation processes
 - By application? By data set?

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
- PCI DSS 4.0

C 2023

NY/Tampa RUG

- <u>https://www.pcisecuritystandards.org/document_library</u>
- 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
- RACF-L 'Key Management' post
 - <u>https://listserv.uga.edu/scripts/wa-UGA.exe?A2=RACF-L;7cc763d7.2204&S=</u>

NY/Tampa RUG

© 2023

Unscrambling the Complexity of Crypto!

© MAINFRAME

