z/OS V2.5 IBM Education Assistant

Solution Name: ICSF Feistel-based encryption

Solution Element(s): RMF

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Objectives

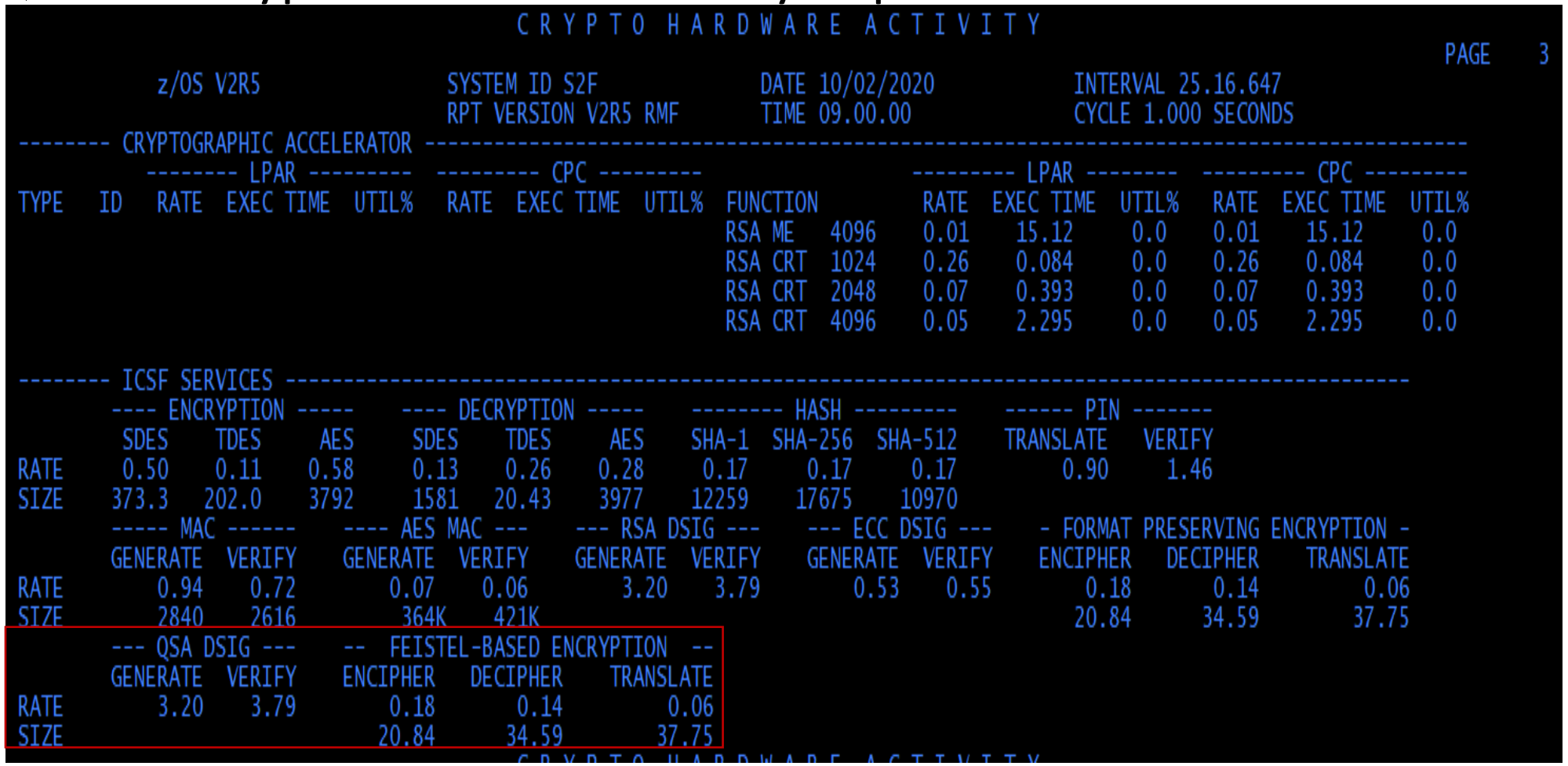
- Explain purpose/usage of RMF item
  - RMF Postprocessor
    - Introduce new Postprocessor reporting capabilities related to ICSF Feistel-based encryption and Quantum Safe Digital Signature.
    - Introduce new Postprocessor Overiew and Exception conditions related to ICSF Feistel-based encryption and Quantum Safe Digital Signature.

Overview

- Who (Audience)
  - z/OS Performance Analysts
- What (Solution)
  - Introduce new Monitor III and Postprocessor measurements to monitor:
    - ICSF Feistel-based encryption
    - Quantum Safe Digital Signature
- Wow (Benefit / Value, Need Addressed)
  - Capability to analyze the performance of new Integrated Cryptographic Service Facility (ICSF) functionality

Usage & Invocation

- Enhanced Crypto Hardware Activity Report



```
                                C R Y P T O   H A R D W A R E   A C T I V I T Y
                                                                                                                PAGE    3

          z/OS V2R5              SYSTEM ID S2F           DATE 10/02/2020          INTERVAL 25.16.647
                                 RPT VERSION V2R5 RMF    TIME 09.00.00            CYCLE 1.000 SECONDS
-------- CRYPTOGRAPHIC ACCELERATOR ----------------------------------------------------------------------------------------
          -------- LPAR ---------  --------- CPC ---------                  --------- LPAR --------  --------- CPC ---------
TYPE   ID   RATE  EXEC TIME  UTIL%   RATE  EXEC TIME  UTIL%  FUNCTION         RATE  EXEC TIME  UTIL%   RATE  EXEC TIME  UTIL%
                                                             RSA ME   4096     0.01    15.12     0.0    0.01    15.12     0.0
                                                             RSA CRT  1024     0.26    0.084     0.0    0.26    0.084     0.0
                                                             RSA CRT  2048     0.07    0.393     0.0    0.07    0.393     0.0
                                                             RSA CRT  4096     0.05    2.295     0.0    0.05    2.295     0.0


-------- ICSF SERVICES ----------------------------------------------------------------------------------------------------
        ---- ENCRYPTION -----     ---- DECRYPTION -----     -------- HASH ---------     ------ PIN -------
         SDES    TDES     AES     SDES    TDES     AES     SHA-1  SHA-256  SHA-512    TRANSLATE   VERIFY
RATE     0.50    0.11    0.58     0.13    0.26    0.28      0.17     0.17     0.17         0.90      1.46
SIZE    373.3   202.0    3792     1581   20.43    3977     12259    17675    10970
        ----- MAC ------     ---- AES MAC ---     --- RSA DSIG ---     --- ECC DSIG ---     - FORMAT PRESERVING ENCRYPTION -
        GENERATE  VERIFY     GENERATE  VERIFY     GENERATE  VERIFY     GENERATE  VERIFY     ENCIPHER   DECIPHER    TRANSLATE
RATE        0.94    0.72         0.07    0.06         3.20    3.79         0.53    0.55         0.18       0.14         0.06
SIZE        2840    2616          364K    421K                                              20.84      34.59        37.75
        --- QSA DSIG ---     --  FEISTEL-BASED ENCRYPTION  --
        GENERATE  VERIFY     ENCIPHER   DECIPHER    TRANSLATE
RATE        3.20    3.79         0.18       0.14         0.06
SIZE                            20.84      34.59        37.75
                                C R Y P T O   H A R D W A R E   A C T I V I T Y
```

Usage & Invocation

- New conditions for Overview and Exception reporting

Condition	Condition Name	Qualifier	Source	Algorithm
QSA digital signature generation rate	CRYIDQGR	none	R702DQGC SMF70INT	DQGC/INT
QSA digital signature verify rate	CRYIDQVR	none	R702DQVC SMF70INT	DQVC/INT
FFX encipher rate	CRYIFXER	none	R702FXEC SMF70INT	FXEC / INT
FFX encipher size	CRYIFXES	none	R702FXEB R702FPEC	FXEB / FXEC
Number of instructions used to encipher data using FFX	CRYIFXEI	none	R702FXEI	Value or comparison
FFX decipher rate	CRYIFXDR	none	R702FXDC SMF70INT	FXDC / INT
FFX decipher size	CRYIFXDS	none	R702FXDB R702FXDC	FXDB / FXDC
Number of instructions used to decipher data using FFX	CRYIFXDI	none	R702FXDI	Value or comparison
FFX translate rate	CRYIFXTR	none	R702FXTC SMF70INT	FXTC / INT
FFX translate size	CRYIFXTS	none	R702FXTB R702FXTC	FXTB / FXTC
Number of instructions used to translate data using FFX	CRYIFXTI		R702FXTI	Value or comparison

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - None

Upgrade & Coexistence Considerations

- None

Installation & Configuration

- This support is included in the GA shipment of the z/OS V2.5 RMF (HRM77D0) deliverable.

Summary

- Introduced enhanced Crypto Hardware Activity Postprocessor report with ICSF Feistel-based Encryption and Quantum Safe Digital Signatures
- Introduced new Overview and Exception condition fields

Appendix

- RMF - https://github.com/IBM/IBM-Z-zOS/tree/master/zOS-RMF
  - Contains Product information, presentations, etc.

- Documentation and news
  - RMF Report Analysis, SC34-2665
  - RMF User‘s Guide, SC34-2664
  - RMF Programmer‘s Guide, SC34-2667
  - Latest version of PDF files can be downloaded from: http://www.ibm.com/systems/z/os/zos/bkserv/