IBM Education Assistance for z/OS V2R3

XCF/XES CF Data Encryption
Element/Components: XCF/XES, RMF

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Session Summary
- Appendix

Trademarks

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

Session Objectives

As businesses and industry require more and more protection from outside intrusion, encryption of data is becoming more important.

This line item will provide support to secure customer information by encrypting customer data while it is being transferred to and from the coupling facility (CF) and while it resides in the coupling facility.

- Support will provide for encryption of all customer data in the CF and flowing on the CF link, at a CF structure level of granularity.
- With this capability, additional security against exposure of sensitive customer information can be achieved.

Overview

- Problem Statement / Need Addressed
  - Customer data that flows through the coupling link infrastructure and which is stored in CF structures is not protected by encryption and could be vulnerable to attack.
- Solution
  - Protect the data flowing over the coupling links and at rest in the CF with end-to-end host-based encryption. Individual CF structures can be designated in the CFRM policy as encrypted in which case the data will be encrypted.
- Benefit / Value
  - Improved security and protection against breaches involving sensitive customer data.

Overview

- Encryption of customer data in the CF will be controlled on a CF structure basis.
  - CFRM will manage the encryption capability of each structure. CFRM will enable encryption for a structure when all requirements are met.
  - The CFRM active policy must have ENCRYPT(YES) specified for each structure to enable encryption or ENCRYPT(NO) to disable encryption for that structure.
- The transition to or from encrypted for allocated structures will be via a structure rebuild process that encrypts or decrypts user data that is already stored in the allocated structure.
  - CF structure rebuild processing will be the mechanism for transitioning a structure and its data into or out of the secure mode, or changing the key with which the data is encrypted.
  - Allocated structure changes will remain pending until rebuild processing has completed encryption or decryption processing

Overview

- CF Encryption will support encryption of data from end-to-end. The data is never in the clear outside the host server.
  - The encryption facility that will be used is CPACF - CP Assist for Cryptographic Functions (host -based encryption), using AES-256 key encryption.
  - z/OS uses length-preserving encryption, as some of the storage areas used to send data to and from the coupling facility is defined by CF architecture.
- CFRM will also be responsible for managing and protecting the cryptographic keys that will be used to encrypt and decrypt the data.
  - CFRM will use ICSF services to request cryptographic keys generated on a structure basis.
  - A new ENCRYPTKEY option on the SETXCF MODIFY, STRNAME command will be provided to support a change key function request.

Overview

- Not all of the data transferred to an encrypted structure will need to be encrypted. Only actual customer data needs to be encrypted.
  - The control objects sent to the CF, such as the Message Command Block and control objects received from the CF, such as the Message Response blocks, Cross-Invalidates and List Notifications will not be encrypted.
- If the CFRM Policy indicates that the structure is to be encrypted, the data will be required to be moved to a fixed area managed and owned by XES before encrypting or decrypting.
  - Today, the connector or requestor buffers are used directly for data transfer to the CF structures.

Overview

- All CF structures that can contain customer data can be encrypted
  - Lock structures as well as Directory Only Cache Structures will not be encrypted
  - Adjunct data will be encrypted.
  - Customer data that may already be encrypted (by the application) will again be encrypted (by XES).
- Connectors must support rebuild.
  - System Managed duplexed structures will both be encrypted or both be not-encrypted
- CF Encryption requires software and hardware support for cryptographic services before enabling structure encryption.

Usage & Invocations

- Run the IXCMIAPU Administrative Policy Utility for CFRM policy data with structure parameters updated with ENCRYPT(YES) or ENCRYPT(NO)
- Issue SETXCF START to activate the updated CFRM Policy
  - Changes to allocated structures that require encryption or decryption will become pending
- Issue SETXCF START,REBUILD or SETXCF START,REALLOCATE
  - Structure data will be encrypted/decrypted and rebuilt to a new structure instance
- Issue D XCF,STR to display structure data to obtain structure encryption status
- Issue SETXCF MODIFY ENCRYPTKEY to request XCF obtain a new cryptographic key for specified structures

Usage & Invocation

Run the IXCMIAPU Administrative Data Utility for CFRM policy data with structure parameters updated with ENCRYPT(YES) or ENCRYPT(NO). When ENCRYPT is not specified, ENCRYPT(NO) is the default.

The syntax of the CFRM structure parameters encryption are:

```
  . . . . .

 [ENCRYPT(NO | YES)]
```

- Specifies whether list and cache structure entry data and entry adjunct data written to the structure and residing in the structure should be encrypted.
- The structure entry and entry adjunct data is in an encrypted format while the data is being transferred to and from the coupling facility and while the data resides in the coupling facility structure.
- Encrypted data is decrypted when read from the structure.

Usage & Invocation

IXCMIAPU Administrative Policy Utility for CFRM policy data

When running the XCF Administrative Policy Utility (IXCMIAPU) service with structure statements that ***enable*** encryption, functions from ICSF (z/OS Integrated Cryptographic Service Facility) will be required:

- At least READ access to ICSF CSFSERV CSFKGN and CSFSERV CSFKYT resource profiles is required when running the utility for the purposes of specifying ENCRYPT(YES) on a structure definition.
- The Administrative Data Utility must be run on a system where ICSF is started.
- The AES master key where the utility is run must be the same AES master key as the target sysplex where encrypted structures will be allocated and connected to.

Usage & Invocation

- Issue SETXCF START,POL to activate the updated CFRM policy
- Allocated Structures
  - Structures will become policy change pending due to the encryption definition change
  - Rebuild processing is required to obtain the data from the CF, encrypt the data and store it back into the CF encrypted.
- Un-allocated Structures
  - Policy information will be updated to indicate this structure will be encrypted
- Structure display message IXC360I will indicate policy changes pending and encryption status

Usage & Invocation

- Issue SETXCF START,REBUILD or SETXCF START REALLOCATE
- Successful completion will resolve the pending change and encrypt the structure data
  - Structure display message IXC360I will indicate policy and encryption status
- A down level connection or an encryption error may prevent the structure from being rebuilt with encrypted data.
  - Message IXC576I will be issued indicating a system-managed rebuild could not make pending policy changes active due to a cryptography error
  - D XCF,STR command supports new filters: encmismatch, encrypted and notencrypted to help determine issues, if any

Usage & Invocation

- Issue D XCF, STR display structure to obtain structure encryption status

```
IXC360I  10.20.57  DISPLAY XCF
STRNAME: LIST02
 POLICY INFORMATION:
    ENCRYPT:  YES
 PENDING POLICY INFORMATION:
    ENCRYPTION KEY
    ENCRYPT        : NO
 ACTIVE STRUCTURE
   ENCRYPTION LEVEL:  AES-256 PROTECTED KEY
   ENCRYPTION LEVEL:  NOT APPLICABLE - NOT SUPPORTED FOR STRUCTURE TYPE
   ENCRYPTION LEVEL:  NOT ENCRYPTED
```

Usage & Invocation

- Issue SETXCF MODIFY ENCRYPTKEY to request XCF obtain a new cryptographic key for specified structure(s)
- SETXCF MODIFY, STRNAME = (strname | ALL), ENCRYPTKEY
  - Accepted message IXC562I
  - Status message IXC563I indicates immediate change for not-allocated structures or pending change for allocated structures
    - Allocated structures become policy change pending due to the encryption key change.. message IXC512I issued
    - Rebuild processing is required to obtain the data from the CF, re-encrypt the data and store it back into the CF
    - Error message IXC300I indicates command failure

Usage & Invocation

Health Check: XCF_CF_STR_ENCRYPT

This check verifies that structure data in an allocated structure is consistent with the effective ENCRYPT parameter and cryptographic encryption key for the structure (when the structure data is encrypted) in the CFRM policy.

XCF_CF_STR_ENCRYPT raises an exception when the current resident data format of structure data (encrypted or non-encrypted) in allocated structures is not consistent with the effective ENCRYPT parameter for the structure in the CFRM policy.

Additionally, the check will report an exception when a change to the cryptographic encryption key used for structure data encryption is pending for any allocated encrypted structure.   Cryptographic encryption key changes can be requested via the SETXCF MODIFY command for structures allocated with encrypted resident data.

When issued in verbose mode, the check reports on all allocated structures, the effective ENCRYPT value for the structure from the CFRM policy, the current resident data format and an indicator as to whether a change is pending for the cryptographic encryption key used for the structure.

Usage & Invocation

Structure Dumping:

Encrypted structure data will be decrypted before moving the data to dump data sets.

Accounting & Measurement (IXLMG service)

New fields in the List and Cache Structure records will report on statistics related to the amount of data moved to and from the CF for each structure. These measurements are useful for estimating the overhead of encryption as these statistics will be gathered for both encrypted and non-encrypted structures.

A new AMDALEVEL = 3 is required to obtain the data read/write statistics. This support will be rolled down to V2.2. RMF support is planned to report these new measurements per CF structure in the SMF 74 subtype 4 record. In addition the RMF V2R3 Postprocessor and Monitor III CF reports are enhanced to indicate whether a CF structure is encrypted or not.

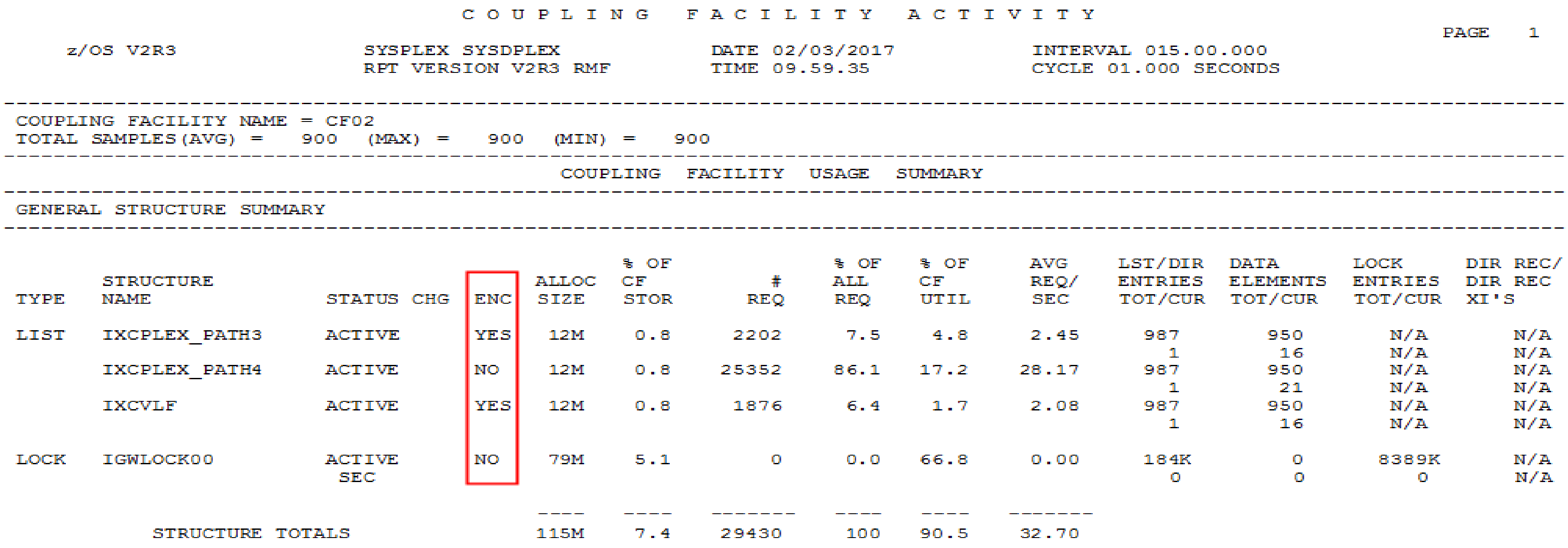
XCF Query

New fields will be reported in the IXCYQUAA structure data to indicate encryption status.

A new field in the FEATURES bits will indicate whether the support for the Accounting and Measurement structure data read/write statistics is installed on this system.

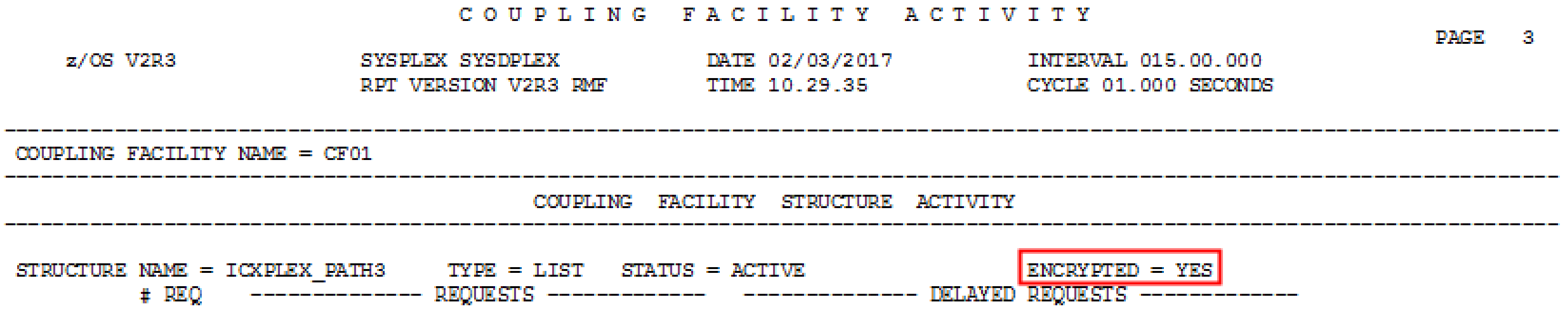
Usage & Invocation

RMF Postprocessor CF Report - Usage Summary section



```
                                   C O U P L I N G   F A C I L I T Y   A C T I V I T Y
                                                                                                   PAGE    1
       z/OS V2R3                SYSPLEX SYSDPLEX           DATE 02/03/2017             INTERVAL 015.00.000
                                RPT VERSION V2R3 RMF       TIME 09.59.35               CYCLE 01.000 SECONDS

 ----------------------------------------------------------------------------------------------------------------
 COUPLING FACILITY NAME = CF02
 TOTAL SAMPLES(AVG) =    900   (MAX) =    900   (MIN) =    900
 ----------------------------------------------------------------------------------------------------------------
                                         COUPLING  FACILITY  USAGE  SUMMARY
 ----------------------------------------------------------------------------------------------------------------
 GENERAL STRUCTURE SUMMARY
 ----------------------------------------------------------------------------------------------------------------

                                                        % OF               % OF   % OF     AVG    LST/DIR  DATA     LOCK      DIR REC/
       STRUCTURE                               ALLOC   CF         #        ALL    CF      REQ/    ENTRIES  ELEMENTS ENTRIES   DIR REC
 TYPE  NAME                STATUS CHG  ENC     SIZE    STOR      REQ       REQ    UTIL    SEC     TOT/CUR  TOT/CUR  TOT/CUR   XI'S

 LIST  IXCPLEX_PATH3       ACTIVE      YES     12M     0.8      2202       7.5    4.8     2.45      987      950       N/A       N/A
                                                                                                      1       16       N/A       N/A
       IXCPLEX_PATH4       ACTIVE      NO      12M     0.8     25352      86.1   17.2    28.17      987      950       N/A       N/A
                                                                                                      1       21       N/A       N/A
       IXCVLF              ACTIVE      YES     12M     0.8      1876       6.4    1.7     2.08      987      950       N/A       N/A
                                                                                                      1       16       N/A       N/A

 LOCK  IGWLOCK00           ACTIVE      NO      79M     5.1         0       0.0   66.8     0.00     184K        0     8389K       N/A
                            SEC                                                                       0        0         0       N/A

                                               ----    ----   -------     ----   ----   -------
           STRUCTURE TOTALS                    115M     7.4     29430      100   90.5    32.70
```

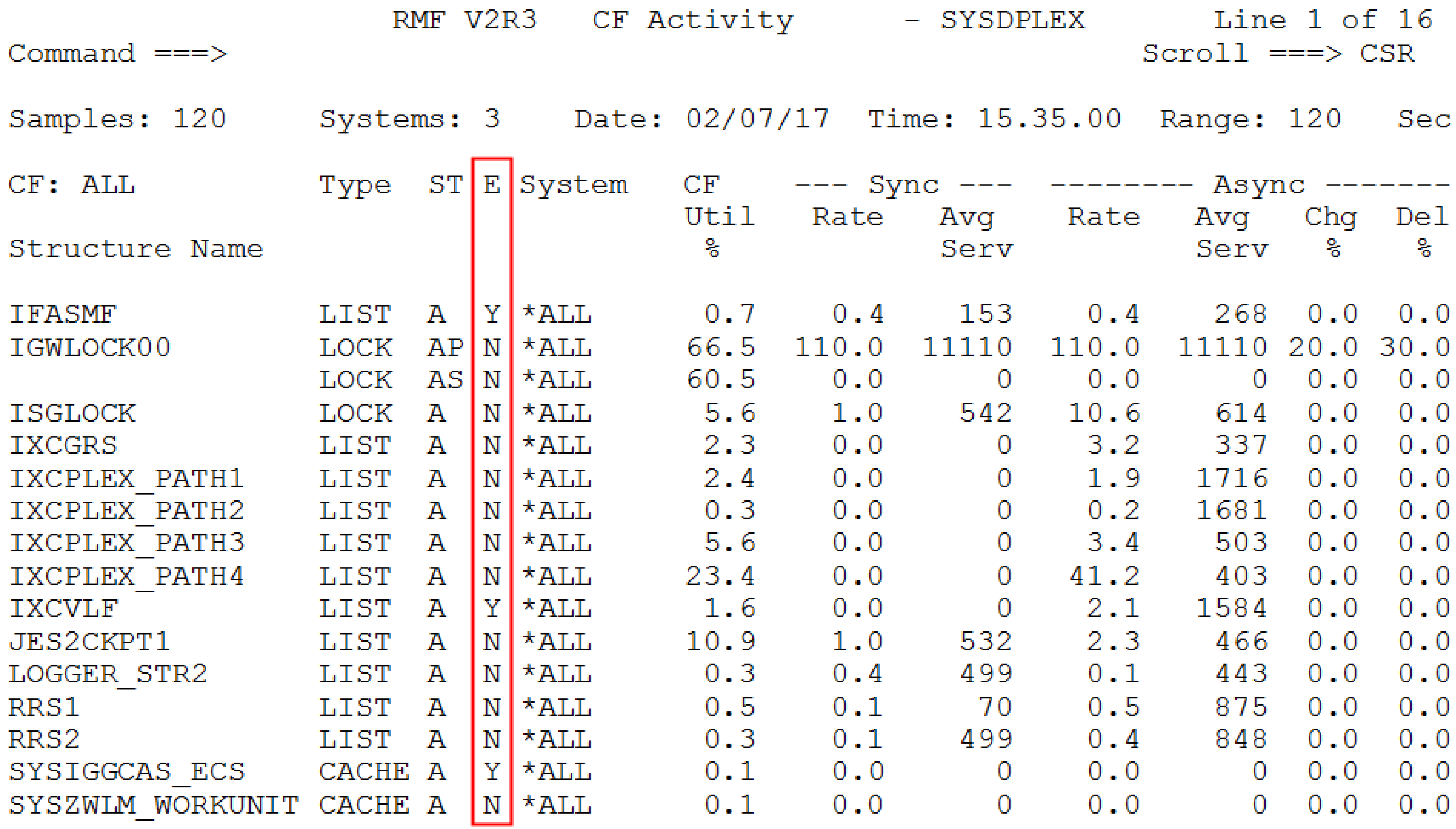
RMF Postprocessor CF Report – Structure Activity section



```
                                 C O U P L I N G   F A C I L I T Y   A C T I V I T Y
                                                                                          PAGE    3
      z/OS V2R3              SYSPLEX SYSDPLEX          DATE 02/03/2017          INTERVAL 015.00.000
                             RPT VERSION V2R3 RMF      TIME 10.29.35            CYCLE 01.000 SECONDS

 ---------------------------------------------------------------------------------------------------
 COUPLING FACILITY NAME = CF01
 ---------------------------------------------------------------------------------------------------
                                   COUPLING  FACILITY  STRUCTURE  ACTIVITY
 ---------------------------------------------------------------------------------------------------

 STRUCTURE NAME = ICXPLEX_PATH3     TYPE = LIST   STATUS = ACTIVE               ENCRYPTED = YES
           # REQ     -------------- REQUESTS -------------   -------------- DELAYED REQUESTS -------------
```

Usage & Invocation

RMF Monitor III CF Report



```
                     RMF V2R3   CF Activity      - SYSDPLEX      Line 1 of 16
Command ===>                                                Scroll ===> CSR

Samples: 120     Systems: 3    Date: 02/07/17  Time: 15.35.00  Range: 120   Sec

CF: ALL          Type  ST E System    CF   --- Sync ---   -------- Async -------
                                     Util  Rate   Avg    Rate    Avg   Chg   Del
Structure Name                        %           Serv           Serv   %     %

IFASMF           LIST  A  Y *ALL      0.7   0.4    153    0.4    268   0.0   0.0
IGWLOCK00        LOCK  AP N *ALL     66.5 110.0  11110  110.0  11110  20.0  30.0
                 LOCK  AS N *ALL     60.5   0.0      0    0.0      0   0.0   0.0
ISGLOCK          LOCK  A  N *ALL      5.6   1.0    542   10.6    614   0.0   0.0
IXCGRS           LIST  A  N *ALL      2.3   0.0      0    3.2    337   0.0   0.0
IXCPLEX_PATH1    LIST  A  N *ALL      2.4   0.0      0    1.9   1716   0.0   0.0
IXCPLEX_PATH2    LIST  A  N *ALL      0.3   0.0      0    0.2   1681   0.0   0.0
IXCPLEX_PATH3    LIST  A  N *ALL      5.6   0.0      0    3.4    503   0.0   0.0
IXCPLEX_PATH4    LIST  A  N *ALL     23.4   0.0      0   41.2    403   0.0   0.0
IXCVLF           LIST  A  Y *ALL      1.6   0.0      0    2.1   1584   0.0   0.0
JES2CKPT1        LIST  A  N *ALL     10.9   1.0    532    2.3    466   0.0   0.0
LOGGER_STR2      LIST  A  N *ALL      0.3   0.4    499    0.1    443   0.0   0.0
RRS1             LIST  A  N *ALL      0.5   0.1     70    0.5    875   0.0   0.0
RRS2             LIST  A  N *ALL      0.3   0.1    499    0.4    848   0.0   0.0
SYSIGGCAS_ECS    CACHE A  Y *ALL      0.1   0.0      0    0.0      0   0.0   0.0
SYSZWLM_WORKUNIT CACHE A  N *ALL      0.1   0.0      0    0.0      0   0.0   0.0
```

Interaction & Dependencies

- Software Dependencies
  - Full Support is provided via z/OS V2.3
    - Toleration support is provided on z/OS V2.1, V2.2 via APAR OA52060 for fall back scenarios
  - Before enabling structure encryption, ensure all systems in the sysplex are on z/OS V2.3
  - Structure read/write accounting and measurements metrics roll down available via APAR OA51879
- Hardware Dependencies
  - CPACF Protected Key Support
  - CryptoExpress3 or later Coprocessor
- Exploiters
  - No explicit application exploitation is needed for this function. CF Structures can be transparently encrypted without application awareness or involvement.

Migration & Coexistence Considerations

- **Migration Considerations:** None
- **Coexistence Considerations:**
  - Systems running on a lower level of z/OS (V2R2 or below) in the sysplex are unaware of the ENCRYPT parameter and unable to encrypt and decrypt structure data.
  - A structure allocated by a connector from a system running at a lower level release will be allocated as if the encryption parameter specified ENCRYPT(NO). Connection requests from a lower level system to an already allocated structure containing encrypted data will not be allowed.
- **Toleration Considerations**:
  - Before enabling encryption in the sysplex, a toleration APAR (OA52060) must be applied to the lower level systems. This is required to prevent the lower level system from corrupting cryptographic information in the CFRM active policy.

Installation

- Hardware and Software dependencies are required
  - Details in Appendix
- CFRM Policy updates are required to define structure encryption parameter
- SETXCF START policy and rebuild procedures are required
- Planning considerations
  - Enable on test configuration
  - Determine which structures require encryption
- Use D XCF,STR command and health check to validate expected structure encryption status

Session Summary

- As businesses and industry require more and more protection from outside intrusion, encryption of data is becoming more important.
- This line item will provide support to secure customer information by encrypting customer data while it is being transferred to and from the Coupling Facility and while it resides in the Coupling Facility Structure
- Protect the data flowing over the coupling links and at rest in the CF with end-to-end host-based encryption. Individual CF structures can be designated in the CFRM policy as encrypted in which case the data will be encrypted.

Appendix

- Publication references
  - IBM Health Checker for z/OS User's Guide (SC23-6843-xx)
  - z/OS V2R3 MVS Setting up a Sysplex
  - z/OS V2R3 MVS Sysplex Services Guide
  - z/OS V2R3 MVS Sysplex Services Reference
  - z/OS V2R3 MVS Data Areas Volume 3 (SDRSN)
  - z/OS V2R3 MVS Data Areas Volume 4 (IXC and IXL data areas)
  - z/OS V2R3 MVS Messages Vol. 6 (IEA911E)
  - z/OS V2R3 MVS Messages Vol. 10 (IXC and IXL messages)

Appendix

IXCMIAPU Administrative Data Utility for CFRM policy data – Status Messages

IXC747I CRYPTOGRAPHIC KEY TOKENS [GENERATED / REGENERATED / REENCIPHERED] UNDER THE CURRENT MASTER KEY FOR STRUCTURES SPECIFYING DATA ENCRYPTION

Explanation: This is a status message issued to indicate that the XCF Administrative Data Utility added or updated cryptographic key data for structure definitions that specify data encryption

IXC748I CRYPTOGRAPHIC KEY TOKENS ENCIPHERED UNDER THE CURRENT MASTER KEY FOR STRUCTURES SPECIFYING DATA ENCRYPTION

Explanation: This is a status message issued to indicate that secure key tokens for structures specifying ENCRYPT(YES) in the CFRM administrative data set are encrypted under the current master key.

IXC749I CRYPTOGRAPHIC KEY TEST SERVICE TO VERIFY THE SECURE VERIFICATION PATTERN OF ENCRYPTED STRUCTURE KEYS WAS NOT AVAILABLE

Explanation: The message is issued to indicate that the secure verification pattern of encrypted key tokens for structures specifying ENCRYPT(YES) in the CFRM administrative data set could not be verified due to the ICSF Key Test callable service not being available.

Appendix

IXCMIAPU Administrative Data Utility for CFRM policy data – Error Messages

IXC735I XCF ADMINISTRATIVE DATA UTILITY ENCOUNTERED AN ERROR: *error_text*

USER NOT AUTHORIZED TO USE ICSF SERVICES

The user of the administrative data utility was not authorized to use Integrated Cryptographic Service Facility (ICSF) services to generate cryptographic keys for structures defined with the data encryption attribute.

ICSF IS NOT AVAILABLE

The Integrated Cryptographic Service Facility (ICSF) is not available. ICSF is not started.

CRYPTOGRAPHIC COPROCESSOR CONFIGURATION ERROR

ICSF is started, but the AES-MK is not defined. ICSF is started, but the requested function is not available or the required hardware is not installed.

UNEXPECTED KEY TOKEN FOUND

The Administrative data utility program found a structure key token in the administrative data set that does not contain a valid master key verification pattern.

MASTER KEY CHANGE IN PROGRESS

ICSF was in the process of performing a coordinated master key change while the XCF administrative data utility was using ICSF services to generate cryptographic keys for structures defined with the data encryption attribute.

Usage & Invocation

SMF record type 74 subtype 4 – Request Data Section

Offset		Name	Len	Format	Description
25	19	R744SFLG	1	binary	**Status Flag** **0** Structure was connected to the system at the end of the interval. **1** Structure became active during the interval. **2** Structure is capable to participate in asynchronous duplexing. **3** Structure is in the duplexing active state. **4** Structure is primary instance of an asynchronously duplexed structure. **5** Structure is secondary instance of an asynchronously duplexed structure. **6** Structure is encrypted. **7** Reserved.
425	1A9	R744SXFL	1	binary	**Bit Meaning When Set** **0** Data for primary instance of asynchronous duplexed structure is valid **1** Data for secondary instance of asynchronous duplexed structure is valid **2** Data for Write and Read Request Measurements is valid **3-7** Reserved.
426	1AA		2		Reserved.
428	1AC	R744SWDR	4	binary	Number of requests to write data to the CF structure. (Valid if bit 2 of R744SXFL is set.)
432	1B0	R744SWAC	4	binary	Number of adjunct areas written to the CF structure. (Valid if bit 2 of R744SXFL is set.)
436	1B4	R744SRDR	4	binary	Number of requests to read data from the CF structure. (Valid if bit 2 of R744SXFL is set.)
440	1B8	R744SRAC	4	binary	Number of adjunct areas read from the CF structure. (Valid if bit 2 of R744SXFL is set.)

Usage & Invocation

SMF record type 74 subtype 4 – Request Data Section

Offset		Name	Len	Format	Description
444	1BC	R744SWEC	4	binary	Number of data entries with data elements that have been written to the CF structure. Include both single and multi entry write requests. (Valid if bit 2 of R744SXFL is set.)
448	1C0	R744SREC	4	binary	Number of data entries with data elements that have been read from the CF structure. Include both single and multi entry read requests. (Valid if bit 2 of R744SXFL is set.)
452	1C4		4		Reserved.
456	1C8	R744SWED	8	binary	Sum of 256 byte increments accumulated for entry data with data elements written to the CF structure. (Valid if bit 2 of R744SXFL is set.)
464	1D0	R744SWES	8	binary	Square of summed number of 256 byte increments accumulated for entry data with data elements written to the CF structure. (Valid if bit 2 of R744SXFL is set.)
472	1D8	R744SRED	8	binary	Sum of 256 byte increments accumulated for entry data with data elements read from the CF structure. (Valid if bit 2 of R744SXFL is set.)
480	1E0	R744SRES	8	binary	Square of summed number of 256 byte increments accumulated for entry data with data elements read from the CF structure. (Valid if bit 2 of R744SXFL is set.)
488	1E8		60		Reserved.

Interactions & Dependencies

Software Dependencies - Details

- Ensure all systems in the sysplex are at z/OS V2.3 before activating a CFRM Policy that has been updated with the structure encryption parameter (ENCRYPT(YES)) that will enable encryption for a CF Structure.

- Activating the ICSF address space is mandatory. XCF needs ICSF to be started with a CKDS (Cryptographic Key Data Set) and the AES master key needs to be active.

- Installations should ensure a sysplex ICSF CKDS configuration so that XCF is using the same CKDS across all systems in the sysplex for encrypting and decrypting structure data. Using the same CKDS will ensure that the AES master key is consistent as well. See "Running in a Sysplex Environment" in the *ICSF Administrator's Guide*

- The Administrative Policy Utility (IXCMIAPU) must be run with the proper resource access authority and on a system with the same AES Master Key as the target sysplex or run on a system in the target sysplex.

- XCF will require functions from ICSF to generate and wrap secure key tokens. These services will require RACF or equivalent System Authority Facility access. The XCFAS should be defined as a **TRUSTED** user to allow access to the ICSF services protected by the CSFSERV general resource class.

Interactions & Dependencies

Hardware Dependencies - Details

- Each system should be operating on servers with the cryptographic hardware configured and activated to perform cryptographic functions and hold Advanced Encryption Standard (AES) master keys within a secure boundary.
  - Cryptographic hardware features available on the required servers that support cryptographic functions and AES master keys include: IBM zBC12 and zEC12 with the
    Crypto Express3 Coprocessor (CEX3C) or Crypto Express4 Coprocessor (CEX4C) or IBM z13 and z13s with the Crypto Express5 Coprocessor (CEX5C)
  - Note: Feature 3863, CPACF DES/TDES Enablement must be installed to use features CEX3C, CEX4C or CEX5C.
- AES master key must be active. Customers will need to define and initialize an ICSF CKDS (Cryptographic Key Data Set) to set the AES master key. The AES master key must be set on all servers used as z/OS systems in a sysplex using CF encryption. The AES master key must be the same for all z/OS systems in the sysplex.