z/OS Cryptographic Services

Integrated Cryptographic Service Facility

ICSF HCR77A1 Migration Checks - APAR OA42011/OA43404

(November, 2013)

Table of Contents

Chapter 1. Overview

The PTFs for APAR OA42011 contain Migration Health Checks to aid customers preparing to migrate to ICSF FMID HCR77A1 – Cryptographic Support for z/OS V1R13 – z/OS V2R1.

Three migration checks are introduced in the APAR:

- **ICSFMIG77A1_COPROCESSOR_ACTIVE**
  The check will indicate which CCA coprocessors will not be active when HCR77A1 is installed.

- **ICSFMIG77A1_UNSUPPORTED_HW**
  The check will indicate whether the system where ICSF is currently running is supported by the HCR77A1 release.

- **ICSFMIG77A1_TKDS_OBJECT**
  The check will detect any PKCS #11 objects stored in the TKDS that is too large to allow the TKDS to be read into storage during ICSF initialization starting with ICSF FMID HCR77A1.

This document contains alterations to information previously presented in z/OS Cryptographic Services ICSF Administrator's Guide, SA22-7521 and z/OS Cryptographic Services ICSF Messages, SA22-7523.

Chapter 2. Update of z/OS Cryptographic Services ICSF Administrator's Guide, SA22-7521, information

Chapter 21. Using ICSF Health Checks

The IBM Health Checker for z/OS is used to identify potential problems before they impact availability or cause outages. The Health Checker outputs messages to notify the user of the problems and suggests actions to be taken. The messages can be merely informational, or they can indicate a risk to the operation of the product.

ICSF provides a set of health checks to inform the user of potential ICSF problems. The checks include both migration checks and status checks. A migration check is designed to warn of changes in a current or pending ICSF release that could negatively impact usage. A status check provides information on the current state of ICSF.

The ICSF health checks are:

- ICSFMIG7731_ICSF_RETAINED_RSAKEY
- ICSFMIG_DEPRECATED_SERV_WARNINGS
- ICSFMIG77A1_COPROCESSOR_ACTIVE
- ICSFMIG77A1_UNSUPPORTED_HW
- ICSFMIG77A1_TKDS_OBJECT
- ICSF_COPROCESSOR_STATE_NEGCHANGE
- ICSF_MASTER_KEY_CONSISTENCY

ICSFMIG77A1_COPROCESSOR_ACTIVE

Type: Migration

Initial State: Inactive

Interval: One Time

This is a migration check. If you are migrating to ICSF FMID HCR77A1 or a newer release, you should run this check on your system before installing the new release of ICSF.

The migration check detects CCA cryptographic coprocessors with master keys that don't match the CKDS and PKDS. A coprocessor that has master keys that don't match the CKDS and PKDS will not become active when HCR77A1 is started. This will affect the availability of coprocessors for cryptographic work.

Note: Coprocessors that have been deactivated from the ICSF Coprocessor Management panel will not be checked.

The method to decide which coprocessors become active has changed for HCR77A1 and newer releases. The master key verification pattern (MKVP) of the current master key register will be compared against the MKVPs in the header record of the CKDS and PKDS. If the MKVP is in the header record, the current master key must match that MKVP in order for the coprocessor to become active. This applies to all master keys that the coprocessor supports. When there is a MKVP in a key store and the coprocessor doesn't support that master key, it is ignored. When a MKVP is not in a key store, the master key is ignored. Note that if there are no MKVPs in any key store, the coprocessor will be active. Note that an initialized CKDS that has no MKVPs in the header record can't be used on a system that has online coprocessors.

This check will also check the new master key register if the current master key register doesn't match the MKVP from the key data set. The new master key will be set during ICSF initialization if the MKVP of the register matches the MKVP in the key data set.

When the Health Check is run, the following messages are generated:

The CSFH0017I message is generated if there are no CCA coprocessors.

The CSFH0018I message indicates the active key stores used in the check.

The CSFH0019I message is generated if all online CCA coprocessors will be activated.

The CSFH0020E message is generated for each of the coprocessors that will not become active.

The CSFH0021E message is generated if the request could not be processed.

For example, the coprocessor installed at index 01 doesn't have the correct AES master key, the health check will generate the following exception:

```
CHECK(IBMICSF,ICSFMIG77A1_COPROCESSOR_ACTIVE)
START TIME: 04/18/2013 09:54:22.127981
CHECK DATE: 20130301  CHECK SEVERITY: MEDIUM

CSFH0018I (ICSF,ICSFMIG77A1_COPROCESSOR_ACTIVE): Active key
stores:

CKDS: CSF.CKDS

PKDS: CSF.PKDS

* Medium Severity Exception *

CSFH0020E (ICSF,ICSFMIG77A1_COPROCESSOR_ACTIVE):
Coprocessor 39 serial number 93X06008 has mismatched
AES master keys.
```

Explanation: The coprocessor installed with the specified index has master keys that don't match the active key stores. The coprocessor will not become active.

The ICSF administrator should load the correct master keys as indicated using the ICSF master key entry panels or the TKE workstation. The master keys are set using the SETMK panel utility on the Master Key Management panel.

System Action: There is no effect on the system.

Operator Response: Contact the ICSF administrator.

System Programmer Response: Contact the ICSF administrator.

Problem Determination: If the indicated master key is not loaded on the coprocessor, it is possible that the CKDS or PKDS was updated with a new master key and the value of that master key was not saved. If the master key in question is not being used, the CKDS or PKDS must be fixed. Contact ICSF service for instruction on how to clear the MKVP from the header record of a key data set.

Source: n/a

Reference Documentation: z/OS Cryptographic Services Integrated Cryptographic Service Facility: Administrators Guide.

Automation: n/a

Check Reason: Detects CCA coprocessors that will not be active.

ICSFMIG77A1_UNSUPPORTED_HW

Type: Migration

Initial State: Inactive

Interval: One Time

This is a migration check. If you are migrating to ICSF FMID HCR77A1 or newer release, you should run this check on your system before installing the new release of ICSF.

The HCR77A1 release does not support IBM Eserver zSeries 800 and 900 systems. This migration check will indicate if your system is not supported by HCR77A1 and newer releases.

When the Health Check is run, the following messages are generated:

The CSFH0022I message is generated if your system is not supported.

For example, the system zSeries 800 and 900:

```
CHECK(IBMICSF,ICSFMIG77A1_UNSUPPORTED_HW)
START TIME: 04/18/2013 09:12:47.938778
CHECK DATE: 20130301  CHECK SEVERITY: MEDIUM

* Medium Severity Exception *

CSFH0022E (ICSF,ICSFMIG77A1_UNSUPPORTED_HW):
Current processor (z800 or z900) will not be supported on a
migration to ICSF HCR77A1. HCR77A1 is planned to require IBM
zSeries z890, z990, or newer processors.

  Explanation:  The processor this check was executed on will
not be supported by ICSF FMID HCR77A1.  HCR77A1 will not start
on zSeries 900 and 800 processors.  All releases of ICSF prior
to HCR77A1 support the zSeries 900 and 800 processors.

  System Action:  There is no effect on the system.

  Operator Response:  Contact the ICSF administrator.

  System Programmer Response:  Contact the ICSF administrator.

  Problem Determination:  n/a

  Source:  n/a
```

Reference Documentation: z/OS Cryptographic Services Integrated Cryptographic Service Facility: Overview.

Automation: n/a

Check Reason: Detects systems that ICSF no longer supports.

ICSFMIG77A1_TKDS_OBJECT

Type: Migration

Initial State: Inactive

Interval: One Time

This is a migration check. If you are migrating to ICSF FMID HCR77A1 or a newer release, you should run this check on your system before installing the new release of ICSF.

Note: If you do not have a Token Data Set (TKDS) with PKDS #11 objects in it, there is no need to run this check.

In the HCR77A1 release, ICSF is introducing a common key data set record format for CCA key tokens and PKCS #11 tokens and objects. This new format of the record adds new fields for key utilization and metadata. Because of the size of the new fields, some exisitng PKCS #11 objects in the TKDS may cause ICSF to fail to start.

The problem exists for TKDS object records with large objects. The 'User data' field in the existing record can not be stored in the new record format if the object size is greater that 32,520 bytes. The TKDSREC_LEN field in the record has the size of the object. If the 'User data' field is not empty and the size of the object is greater than 32,520 bytes, the TKDS can not be loaded.

This migration check will detect any TKDS object that is too large to allow the TKDS to be loaded when ICSF is started.

The problem can be corrected by

- modifying the attributes of the object to make it smaller, if possible.
- removing the information in the 'User data' field of the object. The 'User data' field must be all zeros for it to be ignored.
- copying the object using PKCS #11 services and deleting the old object.
- deleting the object.

Note: ICSF does not provide any interface to modify the 'User data' field in the TKDS object record. The field can only be modified by editing the record.

The TKDS object record is documented in the ICSF System Programmer's Guide.

When the Health Check is run, the following messages are generated:

The CSFH0023I message indicates the active TKDS that was checked.

The CSFH0024I message is generated if there are no TKDS objects that failed the check

The CSFH0025E message is generated if there are TKDS objects that failed the check.
For example,

```
CHECK(IBMICSF,ICSFMIG77A1_TKDS_OBJECT)
START TIME: 04/18/2013 08:54:38.293403
CHECK DATE: 20130301  CHECK SEVERITY: MEDIUM

CSFH0023I Active Token Data Set: CSF.TKDS

The following TKDS objects are too large:
SAMPLE.TOKEN                    00000006T
SAMPLE.TOKEN                    00000005T

* Medium Severity Exception *

CSFH0025E TKDS objects were found that have too much data.

  Explanation:  This message indicates which objects failed this
check. The handle of each object is listed.

  System Action:  There is no effect on the system.

  Operator Response:  Contact the ICSF administrator.

  System Programmer Response:  Contact the ICSF administrator.

  Problem Determination:  n/a

  Source:  n/a

  Reference Documentation:  z/OS Cryptographic Services
Integrated Cryptographic Service Facility: Writing PKCS #11
Applications.

  Automation:  n/a

  Check Reason:  Detects objects in the TKDS that will prevent
ICSF from loading the TKDS during initialization.
```

Chapter 3. Update of z/OS Cryptographic Services ICSF Messages, SA22-7523 , information

Chapter 6. CSFHnnnn Messages (IBM Health Checker Processing)

CSFH0017I (ICSF):
The check is not applicable in the current system environment.

Explanation: The migration check could not be executed because the system environment is not subject to the check. Possible explanations are no coprocessors to check or no active key data set.

System action: There is no effect on the system.

Operator response: None.

ICSF Administrator response: None.

Problem Determination: N/A

CSFH0018I (ICSF, ICSFMIG77A1_COPROCESSOR_ACTIVE):
Active key stores:
CKDS: *ckdsn*
PKDS: *pkdsn*

Explanation: This informational message indicates which key stores were used in the check. The master key verification patterns in the header record of the key store is used to decide whether a CCA coprocessor becomes active.

System action: There is no effect on the system.

Operator response: None.

ICSF Administrator response: None.

Problem Determination: N/A

CSFH0019I (ICSF, ICSFMIG77A1_COPROCESSOR_ACTIVE):
All CCA coprocessors will become active.

Explanation: The state of the current master keys on each CCA cryptographic coprocessor was checked. All coprocessors have the required master keys loaded and the current master

keys have the correct values. All coprocessors will be active and available for work when ICSF FMID HCR77A1 or newer is started.

System action: There is no effect on the system.

Operator response: None.

ICSF Administrator response: None.

Problem Determination: N/A

Reference Documentation:
z/OS Cryptographic Services Integrated Cryptographic Service Facility: Administrator's Guide.

CSFH0020E (ICSF, ICSFMIG77A1_COPROCESSOR_ACTIVE):
Coprocessor *nn* **serial number** *ssssssss* **has mismatched** *type* **master keys.**

Explanation: The coprocessor installed with index *nn* with serial number *ssssssss* will not become active when ICSF FMID HCR77A1 or newer release is installed. The current *type* master key(s) on the coprocessor does not have the same value (as indicated by the master key verification pattern (MKVP)) as stored in the CKDS or PKDS.

The index may have a value of 00-63. The type of master key may be any or all of AES, DES, ECC, and RSA.

System action: There is no effect on the system.

Operator response: Contact the ICSF administrator.

ICSF Administrator response: The administrator should load the correct master keys as indicated in the message using the ICSF master key entry panels or the TKE workstation. The master keys are set using the SETMK panel utility on the Master Key Management panel. Rerun this migration check after all master keys have been processed.

Problem Determination: The ICSF Coprocessor Management panel displays all cryptographic processors and their status. For HCR7780 and newer releases, the state of the master key is also displayed. For HCR7770, the hardware status panel can be used to get the MKVPs of the master keys.

If the indicated master key is not loaded on the coprocessor, it is possible that the CKDS or PKDS was updated with a new master key and the value of that master key was not saved. If the master key in question is not being used, the CKDS or PKDS must be fixed. Contact ICSF service for instruction on how to clear the MKVP from the header record of a key data set.

Reference Documentation:

z/OS Cryptographic Services Integrated Cryptographic Service Facility: Administrator's Guide.

CSFH0021E (ICSF, ICSFMIG77A1_COPROCESSOR_ACTIVE):
Unable to process request.

Explanation: An error was encountered during processing for the health check and the request could not be completed.

System action: There is no effect on the system.

Operator response: Contact the ICSF administrator.

ICSF Administrator response: Investigate the coprocessor states displayed on the ICSF Coprocessor Management panel. Check the message logs and trace entries for problems.

Problem Determination: None

Reference Documentation:
z/OS Cryptographic Services Integrated Cryptographic Service Facility: Administrator's Guide.

CSFH0022E (ICSF, ICSFMIG77A1_UNSUPPORTED_HW):
Current processor (z800 or z900) will not be supported on a migration to ICSF HCR77A1. HCR77A1 is planned to require IBM zSeries z890, z990, or newer processors.

Explanation: The processor this check was executed on will not be supported by ICSF FMID HCR77A1. HCR77A1 will not start on zSeries 900 and 800 processors. All releases of ICSF prior to HCR77A1 support the zSeries 900 and 800 processors.

System action: There is no effect on the system.

Operator response: Contact the ICSF administrator.

ICSF Administrator response: Access your need to migrate to the HCR77A1 or newer releases.

Problem Determination: None

Reference Documentation:
z/OS Cryptographic Services Integrated Cryptographic Service Facility: Overview.

CSFH0023I (ICSF, ICSFMIG77A1_TKDS_OBJECT):
Active Token Data Set: *tkdsn*

Explanation: This informational message indicates which Token data set (TKDS) was used in the check.

System action: There is no effect on the system.

Operator response: None.

ICSF Administrator response: None.

Problem Determination: N/A

CSFH0024I (ICSF, ICSFMIG77A1_TKDS_OBJECT):
All TKDS objects are acceptable.

Explanation: This informational message indicates that no object failed this check.

System action: There is no effect on the system.

Operator response: None.

ICSF Administrator response: None.

Problem Determination: N/A

CSFH0025E (ICSF, ICSFMIG77A1_TKDS_OBJECT):
TKDS objects were found that have too much data.

Explanation: This message indicates which objects failed this check. The handle of each object is listed.

The objects listed have information in the 'User data' field of the TKDS record which will cause the TKDS not to be loaded when running with ICSF HCR77A1. The size of the object in the record is too large and the 'User data' field is not hex zero.

System action: There is no effect on the system.

Operator response: Contact the ICSF administrator.

ICSF System Programmer Response: Contact the ICSF administrator.

Problem Determination: N/A

Reference Documentation:
z/OS Cryptographic Services Integrated Cryptographic Service Facility: Writing PKCS #11 Applications.

CSFH0028I (ICSF):
The check is not applicable in the current system environment.

Explanation: There is no Token Data Set (TKDS) specified in the installation options data set.

System action: There is no effect on the system.

Operator response: None.

ICSF Administrator response: None.

Problem Determination: N/A