z/OS Cryptographic Services
Integrated Cryptographic Service Facility

Master Key Health Checks – APAR OA39489

(April 10, 2012)

Contents

Chapter 1. Overview

In versions of ICSF prior to FMID HCR7780, in order for a coprocessor to become active, a DES master key needed to be set on the coprocessor. Once the coprocessor was active, DES master key support, and the support of any other master key (an AES master key or an asymmetric master key) set on the coprocessor, would then be available.

Starting with ICSF FMID HCR7780, the activation procedure for non-CCF systems is designed to maximize the number of active coprocessors by selecting the set of master keys that are available on the majority of coprocessors. A DES master key is no longer required in order for a coprocessor to become active. Instead, any one of four master keys – the DES master key, the AES master key, the RSA master key (which in earlier releases was called the asymmetric master key), or the ECC master key – is enough for a coprocessor to become active.

- For systems running ICSF FMID HCR7751 or HCR7770, applying the PTF for APAR OA39489 provides the migration check ICSFMIG_MASTER_KEY_CONSISTENCY. The ICSFMIG_MASTER_KEY_CONSISTENCY check warns the user of potential problems with the states of the master keys before migrating from pre-HCR7780 releases of ICSF to HCR7780 or later. This check is inactive by default. In order to use this check, you must activate it.
- For systems running ICSF FMID HCR7780 or HCR7790, applying PTF for APAR OA39489 provides the heath check ICSF_MASTER_KEY_CONSISTENCY. The ICSF_MASTER_KEY_CONSISTENCY check detects inconsistencies in the states of the cryptographic coprocessor master keys. The check warns the user of potential problems with the states of the master keys. This check is an active periodic check.

Chapter 2. Update of z/OS Cryptographic Services ICSF Administrator's Guide, SA22-7521-16, information

This chapter contains updates to the document *z/OS Cryptographic Services ICSF Administrator's Guide*, SA22-7521-16. Specifically, it describes the new migration checks that are available by applying the PTF for APAR OA39489. Refer to "Chapter 20. Using ICSF Health Checks" of this source document if background information is needed.

ICSF_MASTER_KEY_CONSISTENCY

Type: Status

Initial State: Active

Interval: Periodic

This is a master key health check. The check detects inconsistencies in the states of the coprocessor master keys. The check is activated when the ICSF task is started and runs on a periodic (daily) basis. The check determines when the state of a master key on at least one coprocessor is not in accord with the state on the other coprocessors.

The master key states for the coprocessors are displayed on the ICSF Coprocessor Management panel. The states can be available ('A'), correct ('C'), error ('E'), uninitialized ('U') or not supported (-). Master keys are identified by Master Key Verification Pattern (MKVP).

Available
Indicates that the master key loaded on the Coprocessor matches the master key used in the CKDS/PKDS/TKDS and is available for use.

Correct
Indicates that the key matches the key used in the CKDS/PKDS/TKDS but is not available for use.

Error Indicates that the key does not match the key used in the CKDS/PKDS/TKDS.

Uninitialized
Indicates that the key has not been set.

The check is instituted to assist the user in maintaining master key functionality. The coprocessor activation algorithm maximizes the number of active cryptographic coprocessors. For non-CCF systems, any valid master key is acceptable for coprocessor activation. To activate the maximum number of coprocessors, the number of available master keys may be restricted.

The following table illustrates a configuration that would generate an inconsistency message by the check. In this scenario, three coprocessors are active. The AES and ECC master keys are available for use. The DES and RSA master keys are unavailable because they are not set on the relevant coprocessors. The DES master key is set on coprocessor G01, but not on G00 and G02. The RSA master key is set on coprocessor G00 and G01, but not G02.

Table 1. A configuration that would generate an inconsistency message by the check

Coprocessor / Master Key	AES	DES	ECC	RSA
G00	A	U	A	C
G01	A	C	A	C
G02	A	U	A	U

The ICSF_MASTER_KEY_CONSISTENCY health check detects the inconsistency in master key states and generates a health check exception messages indicating that the states of the DES and RSA master keys are not consistent across the coprocessors. If the DES and RSA master keys were set on all three coprocessors then both master keys would be available for use.

When the Health Check is run, one of the following messages is generated:

- The CSFH0014I message is generated if there are no problems.
- The CSFH0015E message is generated if there is a master key inconsistency.

ICSFMIG_MASTER_KEY_CONSISTENCY

Type: Migration

Initial State: Inactive

Interval: Onetime

This is a migration check. The check detects inconsistencies in the states of the cryptographic coprocessor master keys. The check is intended to warn the user of potential problems when migrating from pre-HCR7780 releases of ICSF to more current releases. The check is inactive when ICSF is started. When activated, it performs a one time check on the states of the coprocessor master keys. If a master key is not consistent across the available coprocessors, then a problem condition is assumed and a health checker exception message is generated for the administrator's attention.

The following master key states are defined for use in describing this migration health check: available ('A'), correct ('C'), error ('E'), uninitialized ('U') or not supported (-).

Available
Indicates that the master key matches the key used in the CKDS/PKDS and is available for use.

Correct
Indicates that the key matches the key used in the CKDS/PKDS but is not available for use.

Error Indicates that the key does not match the key used in the CKDS/PKDS.

Uninitialized
Indicates that the key has not been set.

The following tables illustrate a problem scenario. The pre-HCR7780 releases of ICSF require a DES master key. For these releases the G01 coprocessor will be active since it has the DES master key set, but the G00 and G02 coprocessors will

not be active since they do not have the DES master key set. Since all 4 master keys are valid for the G01 coprocessor, all 4 master keys are available.

Table 2. Coprocessor/Master Key configuration on a pre-HCR7780 system

Coprocessor / Master Key	Coprocessor State	AES	DES	ECC	RSA
G00	Online	C	U	C	C
G01	Active	A	A	A	A
G02	Online	C	U	C	U

When a non-CCF system is migrated to the HCR7780 or later release of ICSF, the master states will change. The migrated system will have all three coprocessors active, however all master keys will not be available. The DES and RSA master keys will not be available. These keys are unavailable since they are not set on all active coprocessors.

Table 3. Coprocessor/Master Key configuration on a HCR7780 or later system

Coprocessor / Master Key	Coprocessor State	AES	DES	ECC	RSA
G00	Active	A	U	A	C
G01	Active	A	C	A	C
G02	Active	A	U	A	U

The ICSFMIG_MASTER_KEY_CONSISTENCY health check detects problem states and generates health check exception messages indicating a problem with the DES and RSA master keys because these keys are not consistent across the coprocessors.

When the Health Check is run, one of the following messages is generated:

- The CSFH0014I message is generated if there are no problems.
- The CSFH0015E message is generated if there is a potential master key problem.
- The CSFH0016E message is generated if the system is unable to process the requested check.

Chapter 3. Update of z/OS Cryptographic Services ICSF Messages, SA22-7523-15, information

This chapter contains updates to the document *z/OS Cryptographic Services ICSF Messages*, SA22-7523-15. Specifically, it describes the new IBM Health Checker Processing messages that may be issued when running ICSF with the PTF for APAR OA39489 applied. Refer to this source document if background information is needed.

CSFHnnnn Messages (IBM Health Checker Processing)

CSFHnnnn Messages (IBM Health Checker Processing) describes messages that ICSF issues while processing health checks. See *IBM Health Checker for z/OS: User's Guide* for more information.

CSFH0014I (ICSF, *health_check*) check: The master keys are consistent across the current set of coprocessors.

Explanation: The state of the current master keys on each coprocessor was checked. The master keys on each coprocessor are in the same state, and thus are consistent across the available coprocessors. The *health_check* is either ICSF_MASTER_KEY_CONSISTENCY or ICSFMIG_MASTER_KEY_CONSISTENCY.

System action: Processing continues.

User response: User response: none.

CSFH0015E (ICSF, *health_check*) check: The state of the xxx master key is not consistent across the coprocessors.

Explanation: The current value for the specified master key is not consistent across the coprocessors. At least one coprocessor has the specified master key in a state that is not in agreement with the other coprocessors. This may result in application failing after migration due to loss of master key availability. The *health_check* is either ICSF_MASTER_KEY_CONSISTENCY or ICSFMIG_MASTER_KEY_CONSISTENCY.

System action: Processing continues.

User response: Have your ICSF administrator investigate the coprocessor states displayed on the Coprocessor Hardware Status panel to ensure the current master key verification pattern is consistent across the available coprocessors. If problem is not resolved, contact the IBM Support Center.

CSFH0016E (ICSF, *health_check*) check: Unable to process request.

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

System action: Processing continues.

User response: Have your ICSF administrator. investigate the coprocessor states displayed on the coprocessor management panel. Check the message logs and trace entries for problems.