z/OS

Cryptographic Services Integrated Cryptographic Service Facility Messages

Version 2 Release 1

SC14-7509-02

Note
Before using this information and the product it supports, read the information in "Notices" on page 97.

This edition applies to ICSF FMID HCR77B0 and Version 2 Release 1 of z/OS (5650-ZOS) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this information

This information contains messages and their routing and descriptor codes for the Integrated Cryptographic Service Facility (ICSF).

Who should read this information

This information is for users who receive messages that have a prefix of *CSFxnnnn*.

This information is also for programmers who intend to alter codes that IBM programming assigns to messages.

How to use this information

This document contains ICSF messages with their prefixes organized in alphanumeric order.

Where to find more information

The ICSF library consists of the following books:

- *z/OS Cryptographic Services ICSF Overview*
- *z/OS Cryptographic Services ICSF System Programmer's Guide*
- *z/OS Cryptographic Services ICSF Administrator's Guide*
- *z/OS Cryptographic Services ICSF Application Programmer's Guide*
- *z/OS Cryptographic Services ICSF Writing PKCS #11 Applications*
- *z/OS Cryptographic Services ICSF Messages*

The TKE Workstation, which is an optional feature, is described in *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*.

Other documents that are referenced are:

- *z/OS DFSMS Macro Instructions for Data Sets*
- *z/OS DFSMS Access Method Services Commands*

- *S/390 PR/SM Planning Guide*
- *S/390 Support Element Operation Guide*
- *z/OS MVS System Codes*
- *z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG*
- *z/OS MVS IPCS User's Guide*
- *z/OS MVS Diagnosis: Reference*
- *z/OS DFSMSdfp Diagnosis*

IBM Crypto Education

The IBM Crypto Education community provides detailed explanations and samples pertaining to IBM cryptographic technology at https://www-304.ibm.com/connections/communities/community/crypto.

How to send your comments to IBM

We appreciate your input on this publication. Feel free to comment on the clarity, accuracy, and completeness of the information or provide any other feedback that you have.

Use one of the following methods to send your comments:

1. Send an email to mhvrcfs@us.ibm.com.
2. Send an email from the "Contact us" web page for z/OS (http://www.ibm.com/systems/z/os/zos/webqs.html).
3. Mail the comments to the following address:
   IBM Corporation
   Attention: MHVRCFS Reader Comments
   Department H6MA, Building 707
   2455 South Road
   Poughkeepsie, NY 12601-5400
   US
4. Fax the comments to us, as follows:
   From the United States and Canada: 1+845+432-9405
   From all other countries: Your international access code +1+845+432-9405

Include the following information:

- Your name and address.
- Your email address.
- Your telephone or fax number.
- The publication title and order number:
  z/OS ICSF Messages
  SC14-7509-02
- The topic and page number that is related to your comment.
- The text of your comment.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute the comments in any way appropriate without incurring any obligation to you.

IBM or any other organizations use the personal information that you supply to contact you only about the issues that you submit.

If you have a technical problem

Do not use the feedback methods that are listed for sending comments. Instead, take one of the following actions:

- Contact your IBM service representative.
- Call IBM technical support.
- Visit the IBM Support Portal at z/OS support page (http://www.ibm.com/systems/z/support/).

Summary of Changes

ICSF is an element of z/OS, but provides independent ICSF releases as web deliverables. These web deliverables are identified by their FMID. Each release of z/OS includes a particular ICSF FMID level as part of its base.

This document contains terminology, maintenance, and editorial changes to improve consistency and retrievability. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

Changes made in Cryptographic Support for z/OS V1R13 - z/OS V2R1 (FMID HCR77B0)

This document contains information previously presented in *z/OS ICSF Messages*, SC14-7509-01.

This document is for ICSF FMID HCR77B0. This release of ICSF runs on z/OS V1R13 and z/OS V2R1 and only on zSeries hardware.

New

The following messages are new.

- CSFG1034
- CSFG1042
- CSFH0030I
- CSFH0031E
- CSFH0032I
- CSFM645I
- CSFM653I
- CSFM654I
- CSFM655I
- CSFM657I
- CSFM659I
- CSFM660I
- CSFM661I
- CSFM662I
- CSFM663I
- CSFM664I
- CSFM665E
- CSFM673E
- CSFY0086

Changed

- CSFC0316
- CSFG0002
- CSFH0011I
- CSFM009I

- CSFM109I
- CSFM111I
- CSFM123E
- CSFM124I
- CSFM129I
- CSFM134I
- CSFM135E
- CSFM136I
- CSFM137E
- CSFM138I
- CSFM139I
- CSFM639I
- CSFM641I

Deleted

No content was removed from this information.

Changes made in Cryptographic Support for z/OS V1R13 - z/OS V2R1 (FMID HCR77A1) as updated June 2014

This document contains information previously presented in *z/OS ICSF Messages*, SC14-7509-00.

This document is for ICSF FMID HCR77A1. This release of ICSF runs on z/OS V1R13 and z/OS V2R1 and only on zSeries hardware.

New

The following messages are new.

CSFG0994
CSFG1004
CSFG1014
CSFG1024

Changed

The following messages are changed.

CSFG0224
CSFG0924
CSFM014I

Deleted

ICSF no longer issues the following message.

CSFM420E

Changes made in Cryptographic Support for z/OS V1R13 - z/OS V2R1 (FMID HCR77A1)

This document contains information previously presented in *z/OS ICSF Messages*, SA22-7523-16.

This document is for ICSF FMID HCR77A1. This release of ICSF runs on z/OS V1R13 and z/OS V2R1 and only on zSeries hardware.

New information

Changed information

Deleted information

Table 1. Deleted messages

Message number	Message number
• CSFC0254	• CSFM413E
• CSFC0266	• CSFM414I
• CSFC0306	• CSFM416I
• CSFG0604	• CSFM417I
• CSFG0886	• CSFM418E
• CSFM005A	• CSFM419E
• CSFM008I	• CSFM420E
• CSFM020I	• CSFM424I
• CSFM021I	• CSFM430I
• CSFM105E	• CSFM431I
• CSFM106A	• CSFM432I
• CSFM107E	• CSFM433E
• CSFM108I	• CSFM434E
• CSFM110I	• CSFM435I
• CSFM113E	• CSFM436I
• CSFM114E	• CSFM437E
• CSFM115E	• CSFM438I
• CSFM116I	• CSFM440I
• CSFM117I	• CSFM441I
• CSFM118E	• CSFM452I
• CSFM119E	• CSFM501E
• CSFM120E	• CSFM503E
• CSFM121E	• CSFM504E
• CSFM125I	• CSFM510E
• CSFM224I	• CSFM511E
• CSFM302A	• CSFM512E
• CSFM305A	• CSFM522E
• CSFM315I	• CSFM532I
• CSFM404A	• CSFM601I
• CSFM405A	• CSFM605I
• CSFM403I	• CSFM606I
• CSFM406A	• CSFM609I
• CSFM407A	• CSFM624I
• CSFM411I	• CSFM627I
• CSFM412I	• CSFM631I

Changes made in Cryptographic Support for z/OS V1R12-R13 (FMID HCR77A0)

This document contains information previously presented in *z/OS ICSF Messages*, SA22-7523-15.

This document is for ICSF FMID HCR77A0. This release of ICSF runs on z/OS V1R11, z/OS V1R12, and z/OS V1R13 and only on zSeries hardware.

New information

- CSFG0904
- CSFG0914
- CSFG0924
- CSFG0934
- CSFG0944
- CSFG0956
- CSFG0964
- CSFH0014I
- CSFH0015E
- CSFH0016E
- CSFM102I
- CSFM132I
- CSFM133I
- CSFM533I
- CSFM534I
- CSFM535I
- CSFM536I
- CSFM537I
- CSFM538I
- CSFM634I
- CSFM635I
- CSFM637I
- CSFM638I
- CSFM639I
- CSFM640I
- CSFM641I
- CSFM642I
- CSFM643I

Changed information

- CSFC0306
- CSFG0224
- CSFM012I
- CSFM014I
- CSFM015I
- CSFM108I
- CSFM109I
- CSFM110I
- CSFM111I
- CSFM123E
- CSFM124I
- CSFM129I
- CSFM131E

Changes made in Cryptographic Support for z/OS V1R11-R13 (FMID HCR7790)

This document contains information previously presented in *z/OS ICSF Messages*, SA22-7523-14.

This document is for ICSF FMID HCR7790. This release of ICSF runs on z/OS V1R11, z/OS V1R12, and z/OS V1R13 and only on zSeries hardware.

New information

- CSFC0316
- CSFG0876
- CSFG0886
- CSFG0896
- CSFH0010E
- CSFH0011I
- CSFH0012I
- CSFH0013I
- CSFM131E
- CSFM532I
- CSFM540I
- CSFM615I
- CSFM616I
- CSFM618I
- CSFM619I
- CSFM620I
- CSFM621I
- CSFM622I
- CSFM623I
- CSFM624I
- CSFM625I
- CSFM626I
- CSFM628I
- CSFM629I
- CSFM630I
- CSFM631I
- CSFM632I
- CSFM633I
- CSFM636I
- CSFU006I

Changed information

- CSFM108I
- CSFM110I
- CSFM111I
- CSFM122I
- CSFM128E

- CSFM400I
- CSFM409E

Chapter 1. Introduction

This book describes ICSF messages and their appropriate responses. ICSF writes messages to the ICSF job log, data sets, and consoles. You can view some messages immediately as they appear on the console and you can view messages in data sets.

Chapter 2. CSFBnnnn messages (Build control statement processing)

Chapter 2, "CSFBnnnn messages (Build control statement processing)" describes messages that ICSF issues while processing the installation options data set or key generator utility program (KGUP) control statements. These messages are sent to the ICSF job log using routing code 11.

CSFB0016 END OF THE INPUT RECORDS REACHED WHILE IN CONTINUATION STATEMENT.

Explanation: ICSF reached the end of the input file when it expected a continuation to another line.

System action: Processing ends.

User response:

- Check to see if there were physical records missing from the end of the input file or if a continuation character was misplaced in a previous record.
- Check for stray commas.

CSFB0026 STATEMENT EXCEEDS MAXIMUM LENGTH ALLOWED.

Explanation: The length of the logical record being built exceeds the maximum allowable by the application. The statement that contains the error precedes this message.

System action: Processing ends.

User response:

- Check to see if a continuation character was entered incorrectly.
- Check application guidelines to find out the maximum logical record length allowable.
- Check for stray commas.

CSFB0034 COMMENT ON RECORD FOR STATEMENT NOT CLOSED. PROCESSING CONTINUES WITH NEXT STATEMENT.

Explanation: A comment was opened (/*) but not closed (*/) on the same physical line.

System action: Processing of the statement ends. Normal processing of the input file continues.

User response: Check to see if the close comment delimiter (*/) is specified after column 71. Specify the close comment delimiter on the statement.

CSFB0044 COLUMN 72 NOT BLANK.

Explanation: Column 72 of the input control statement is not blank.

System action: ICSF ended processing for this control statement. Normal processing of the input file continues.

User response: Ensure that column 72 is blank.

CSFB0056 INPUT FILE EMPTY.

Explanation: The control statement input file is empty.

System action: Processing ends.

User response: Ensure that the input file contains statements for processing.

Chapter 3. CSFCnnnn messages (Cryptographic key data set processing)

Chapter 3, "CSFCnnnn messages (Cryptographic key data set processing)" describes messages that ICSF issues while processing the cryptographic key data set (CKDS), the PKA key data set (PKDS), or the token data set (TKDS). Most of these messages are sent to the ICSF job log using routing code 11. Messages warning that the CKDS or PKDS is full or nearly full are sent to the operator console or security console (routing codes 1 and 9).

CSFC0016 ABEND OCCURRED IN *routine*. **PSW =** *psw*, **COMPLETION CODE =** *code*.

Explanation: The key data set access module *routine* ended abnormally. The variable *psw* is the PSW at the time of the abnormal ending, and *code* is the system completion code.

System action: Processing ends.

System programmer response: Respond to the problem that is identified by the system completion code.

User response: Contact your system programmer.

Problem determination: In addition to the action that is specified for the system programmer:

- Make sure that the failing job step includes a SYSUDUMP DD statement.
- Run the EREP service aid for detailed reports of the system's error activity. Save the output.

CSFC0026 *Routine* **UNABLE TO ESTABLISH AN ESTAE.**

Explanation: The key data set access module that is indicated by *routine* could not establish an ESTAE environment.

While the conversion process is running, the system issues message CSFV0026 with a return code of 12 and a reason code of 6028.

System action: Processing ends.

System programmer response: Contact the IBM Support Center.

User response: Run the job again. If it still fails, contact your system programmer.

CSFC0036 ALLOCATE FAILED FOR DSNAME *dsname*, **RETURN CODE =** *retcode*, **REASON CODE =** *rsncode*.

Explanation: The key data set was being used by another user. In the message, *dsname* represents the data set name of the key data set. The failed dynamic allocation (SVC99) call returned the *retcode* and *rsncode*.

While the conversion process is running for the CSFCONV utility, the system issues message CSFV0026 with a return code of 12 and a reason code of 6032.

System action: Processing ends.

User response: Wait until the CKDS is available.

CSFC0046 UNABLE TO OPEN KEY DATASET *dsname*.

Explanation: The key data set, *dsname*, could not be opened.

A VSAM error message that further identifies the problem accompanies this message.

System action: Processing ends.

System programmer response: Correct the problem that is identified by the VSAM error message.

User response: Correct the problem that is identified by the VSAM error message. If you cannot resolve the problem, inform the system programmer.

CSFC0053 ROUTINE *routine* **FAILED. RETURN CODE =** *retcode*, **REASON CODE =** *rsncode*.

Explanation: A cryptographic service routine (*routine*) returned with an unexpected return code (*retcode*) and reason code (*rsncode*) combination.

While the conversion process is running, the system issues message CSFV0026 with a return code of 12 and a reason code of 6044.

System action: Processing ends.

System programmer response: Respond to the problem that is identified by the return and reason codes. If you cannot resolve the problem, contact the IBM Support Center.

User response: Contact your system programmer.

CSFC0064 UNABLE TO CLOSE KEY DATA SET *dsname*.

Explanation: The key data set, *dsname*, could not be closed.

A VSAM error message that further identifies the problem accompanies this message.

System action: Depending on the function that ICSF is performing, normal processing either continues or ends.

System programmer response: Contact the IBM Support Center.

User response: If the function ICSF is performing is not repetitive, no action is required.

If the problem persists, contact your system programmer.

CSFC0072 UNALLOCATE FAILED FOR DSNAME *dsname*, **RETURN CODE =** *retcode*, **REASON CODE =** *rsncode*.

Explanation: The CKDS access module could not deallocate the CKDS identified by *dsname*. The failed dynamic allocation (SVC99) call returned the *retcode* and *rsncode*.

While the conversion process is running, the system issues message CSFV0026 with a return code of 12 and a reason code of 6036.

System action: Depending on the function ICSF is performed, normal processing continues or ends.

System programmer response: Contact the IBM Support Center.

User response: If the function ICSF is performing is not repetitive, no action is needed.

If the problem persists, contact your system programmer.

CSFC0086 SYSTEM *syskey* **RECORD NOT FOUND IN CKT.**

Explanation: Either a system record was not found in the in-storage CKDS table (CKT) or the system MAC generation (MACGEN) key could not be found. *Syskey* is either CONTROL or MACGEN. This error can only occur when a new CKDS is being created from the in-storage image during CKDS creation, re-encipherment, or conversion.

While the conversion process is running, the system issues message CSFV0026 followed by a return code of 12 and a reason code of 6048.

System action: Processing ends.

System programmer response: Either correct the CKDS to be processed or use another CKDS.

User response: Ensure that the supplied CKDS being processed is valid. If you cannot use the CKDS, contact your system programmer.

CSFC0096 UNABLE TO UPDATE THE CKDS CONTROL RECORD.

Explanation: An I/O error occurred in writing the control record to the CKDS.

System action: Processing ends.

System programmer response: Ensure that the IDCAMS services can read the CKDS. If the problem persists, use a backup CKDS and rerun the job.

User response: Contact your system programmer.

CSFC0106 UNABLE TO RETRIEVE SYSTEM *keytype* **RECORD.**

Explanation: A system record of *keytype* is not in the CKDS.

System action: Processing ends.

System programmer response: Ensure that the CKDS has system records using IDCAMS services. Either add the system records or use another CKDS and rerun the job.

User response: Contact your system programmer.

CSFC0116 CONTROL BLOCK VALIDATION ERROR. RETURN CODE = *retcode*, **REASON CODE =** *rsncode*.

Explanation: The key data set access control block (CACB) is incorrect. The CACB is an ICSF internal control block. In the message, *retcode* indicates the return code, and *rsncode* indicates the reason code.

Return code: 08

Reason Code
Meaning

36 The key data set name is not a valid data set name.

System action: Processing ends.

System programmer response: Contact the IBM Support Center.

User response: Contact your system programmer.

CSFC0124 *Label-type* **BYPASSED BY THE** *exit-id* **EXIT** *routine*.

Explanation: An installation exit bypassed a record in the CKDS. *Label-type* is the CKDS VSAM key value for the bypassed CKDS record, *exit-id* is the installation options exit identifier, and *routine* is the installation exit module name.

System action: The conversion process bypassed the *Label-type* record, but continued the normal processing of the other records in the file.

User response: Ensure that the conversion process bypassed the correct record.

CSFC0136 *Exit-id* **EXIT** *routine* **ABENDED. PROCESSING TERMINATED.**

Explanation: The installation exit failed, and the conversion program ended processing as requested by the exit. The exit identifier is *exit-id*, and the installation exit module name is *routine.*

If the Single-record, read-write installation exit (*exit-id* is CSFSRRW) ends abnormally while the conversion process is running, ICSF issues message CSFV0026 with a return code of 12 and a reason code of 6020. If the conversion installation exit (*exit-id* is CSFCONV) ends abnormally ends, ICSF issues message CSFV0026 with a return code of 12 and a reason code of 9084.

System action: Processing ends.

System programmer response: Follow local procedures for errors that are detected in the installation exit.

CSFC0142 *Exit-id* **EXIT** *routine* **ABENDED. PROCESSING CONTINUES WITHOUT INVOKING EXIT.**

Explanation: The installation exit failed, and processing continued as requested by the exit. The exit identifier is *exit-id*, and the installation exit module name is *routine.*

System action: The conversion process does not call the installation exit module from the point of failure.

System programmer response: Follow local procedures for errors that are detected in the installation exit.

CSFC0156 NON-EMPTY DATA SET *dsname* CANNOT BE USED AS NEW KEY DATA SET.

Explanation: The output key data set that is identified by *dsname* must be empty.

System action: Processing ends.

User response: Use an empty output key data set.

CSFC0166 *Exit-id* EXIT *routine* CANNOT BE LOADED. RETURN CODE = *retcode*, REASON CODE = *rsncode*.

Explanation: The load module that is identified by *routine* cannot be loaded for the *exit-id* exit, where the return code and reason code are one of these combinations:

Return code: 04

Reason Code
Meaning

04 ICSF could not find the installation exit module.

Return code: 08

Reason Code
Meaning

08 ICSF found the installation exit module, but could not load it.

If the conversion process cannot load the Single-record, read-write installation exit (*exit-id* is CSFSRRW), ICSF issues message CSFV0026 with a return code of 12 and a reason code of 6040. If the conversion process cannot load the conversion installation exit (*exit-id* is CSFCONV), ICSF issues message CSFV0026 with a return code of 12 and a reason code of 9020.

System action: Processing ends.

System programmer response: Ensure that an installation exit module that can be loaded exists in a library directed to by the JCL or link list.

CSFC0172 *Exit-id* EXIT PROCESSING NOT IN EFFECT.

Explanation: The required installation exit, *exit-id*, could not be loaded.

System action: Normal processing continues without calling the installation exit.

System programmer response: Follow local procedures for errors that are detected in the installation exit.

CSFC0186 RETURN CODE *retcode* FROM *exit-id* EXIT *routine* NOT VALID.

Explanation: The installation exit returned a return code that was not valid. *Exit-id* is the exit identifier, and *routine* is the associated load module name.

If the Single-record, read-write installation exit (*exit-id* is CSFSRRW) is called during the conversion process, ICSF issues message CSFV0026 with a return code of 12 and a reason code of 6012. If the conversion installation exit (*exit-id* is CSFCONV) is called, ICSF issues message CSFV0026 with a return code of 12 and a reason code of 9076.

System action: Processing ends.

System programmer response: Follow local procedures for errors that are detected in the installation exit.

CSFC0196 CONTROL RECORD NOT FOUND ON CKDS *dsname*.

Explanation: The conversion process did not find the control record in the CKDS identified by *dsname*.

System action: Processing ends.

User response: Use a CKDS that has a control record.

CSFC0206 *Exit-id* **EXIT** *routine* **ABENDED. ICSF SHOULD BE TERMINATED.**

Explanation: The installation exit load module, *routine*, failed. The failure option for the *exit-id* exit specified that ICSF should also be ended.

If the Single-record, read-write installation exit (*exit-id* is CSFSRRW) is called during the conversion process, ICSF issues message CSFV0026 with a return code of 12 and a reason code of 6024. If the conversion installation exit (*exit-id* is CSFCONV) is called, ICSF issues message CSFV0026 with a return code of 12 and a reason code of 9080.

System action: Processing ends.

System programmer response: Follow local procedures for errors that are detected in the installation exit.

CSFC0216 **UNABLE TO FIND RECORD** *labelname* **FOR** *action* **ON DSNAME** *dsname***.**

Explanation: A record could not be found. The *action* is either READ or DELETE. The *dsname* is either CKDS or PKDS.

System action: Processing ends.

User response: Make sure that you specify the labelname that exists for the PKDS/CKDS.

CSFC0226 **MKVP** *mkvp* **SUPPLIED DOES NOT MATCH THE CKDS HEADER MKVP** *ckdsmkvp***.**

Explanation: The master key verification pattern *mkvp* for the CKDS record being updated didn't match the MKVP *ckdsmkvp* in the CKDS header record.

System action: Processing ends.

User response: Make sure the CKDS key token has the correct MKVP.

CSFC0236 **ATTEMPTED TO READ FROM EMPTY KEY DATA SET FOR DD** *ddname***.**

Explanation: An empty key data set, *dsname*, was specified for KGUP, a conversion program, or a refresh request. A minimum requirement is an initialized key data set.

System action: Processing ends.

User response: Make sure that you are using a fully initialized CKDS before rerunning the job.

CSFC0276 **UNABLE TO OPEN DATASET** *dsname***.**

Explanation: A attempt to open the cryptographic key data set *dsname* failed. The *dsname* is the TKDS.

System action: Processing ends.

User response: Make sure the TKDS is available for ICSF to open.

CSFC0286 **INCORRECT** *data-set-attribute* **FOR** *key-data-set-type* **DATASET** *dsname***.**

Explanation: The specified *data-set-attribute* does not have the expected value for the *key-data-set-type*. For example, the PKDS must have an LRECL of 3800.

This message is issued when ICSF start-up or refresh is attempted with a CKDS in KDSR format and ICSF is not at HCR77A1 or higher.

System action: Processing continues.

System programmer response: Follow the instructions to copy your existing key data set to a new VSAM data set with the correct data set attributes. Ensure that the options data set contains a statement with the correct key data set type and the new data set's name. Then restart ICSF.

User response: Contact your system programmer.

CSFC0316 REENCIPHER FAIL: RC = *retcode*, **RS =** *rsncode* **FOR ENTRY** *label*

Explanation: This message is no longer issued.

System action: None.

System programmer response: None.

CSFC0322 DUPLICATE TOKENS FOUND IN DATASET *dsname*.

Explanation: A key token in the key data set, dsname, was found stored under more than one label. This message was issued for the first duplicate token found. There may be more than one duplicate token in the key data set.

System action: Processing continues.

User response: The system security administrator should review the duplicate tokens using CSFDUTIL. Examine SMF type 82 subtype 24 records for the labels of the duplicate tokens.

CSFC0336 *Exit-id* **EXIT** *routine* **REQUESTED THAT PROCESSING BE TERMINATED.**

Explanation: The installation exit load module, routine, requested that the current CKDS operation (load, reencipher, or refresh) be terminated.

System action: Processing ends.

System programmer response: Ensure that the exit processing was supposed to request termination of processing.

User response: The system security administrator should review the duplicate tokens using CSFDUTIL. Examine SMF type 82 subtype 24 records for the labels of the duplicate tokens.

CSFC0343 CKDS KEY '*label-type***' AUTHENTICATION FAILED.**

Explanation: A message authentication code (MAC) verification for a CKDS key entry failed. If a system key (key with a label name of 64 bytes of X'00') fails authentication, the key-name field has the constant 'SYSTEM_KEY'.

System action: Processing continues.

System programmer response: Investigate the key entry to determine why the MAC verification failed.

Chapter 4. CSFEnnnn messages (Exit router)

Chapter 4, "CSFEnnnn messages (Exit router)" describes messages that ICSF exit router issues. These messages are sent to the ICSF job log using routing code 11.

CSFE001I INSTALLATION EXIT *exit-name* NOT FOUND

Explanation: This is an informational message only.

System action: Processing continues.

System programmer response: Determine if the exit that is named in *exit-name* is valid. Ensure that the name of the installation options data set matches the name in the module. If necessary, restart ICSF.

CSFE002A REQUIRED INSTALLATION EXIT *exit-name* NOT FOUND

Explanation: You specified an exit with a FAIL option for ICSF, and ICSF could not find it.

System action: ICSF ends.

System programmer response: Correct the name of the exit and restart ICSF.

Chapter 5. CSFGnnnn messages (Key generator utility processing)

Chapter 5, "CSFGnnnn messages (Key generator utility processing)" describes messages that the key generator utility program (KGUP) issues. These messages are sent to the KGUP diagnostic data set (CSFDIAG). For information about defining the CSFDIAG data set, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

CSFG0002 CRYPTOGRAPHIC KEY GENERATION - END OF JOB. RETURN CODE = *retcode*.

Explanation: The key generator utility program completed processing with a return code of *retcode*. The table lists all known return codes and their meanings.

Note: Not all of the return codes listed will be communicated via the CSFG0002 message in the CSFDIAG data sets; some will only be generated by the KGUP JCL job.

Return Code	Meaning
00	Successful processing.
04	The key generator utility program encountered warning conditions, but processed all transactions.
08	One or more control statements failed.
12	An error occurred as the key generator utility program was ending. The reason is in the CSFDIAG diagnostic data set.
16	Message queueing failed. The last message cannot be printed.
20	ESTAE macro failure.
24	An abnormal ending occurred in the key generator utility program.
28	ICSF is not started.
36	State of special secure mode on the coprocessor is not the same as the state that is specified in the PARM field of the EXEC JCL statement.
40	Unable to enqueue key generator resources.
44	Unable to run the specified installation exit module with the CSFKGUP exit identifier installation option.
48	EXEC PARM value is not valid. It must be blank, SSM, or NOSSM.
52	Unable to retrieve information from the CALL to the ICSF service routine.
56	Unable to obtain information from the ICSF service routine to issue the ENQ macro.
64	An OPEN error occurred for the CSFVRPT report data set. If you are using a pre-allocated data set, ensure that the record length is correct.
68	An I/O error occurred for the CSFVRPT report data set. An attempt to CLOSE the data set was tried, so check to see if there are meaningful messages in the data set.
72	The caller is not authorized to use the CSFKGUP utility.

System action: Processing ends.

System programmer response: Investigate previous diagnostic error messages and JCL log messages. If you can correct the error condition, rerun the key generator utility program. For problems that you cannot correct, contact the IBM Support Center.

User response: Review the return code and messages. A zero (0) return code indicates successful processing and requires no further analysis. If the return code is greater than zero (0), review the previous diagnostic messages for

errors. If errors occurred because of control statements that were not valid, make the necessary corrections and rerun the key generator utility program with the correct statements. When errors occurred from other than those on control statements, contact the system programmer.

If the return code is 72, contact your security administrator to obtain READ authority to the CSFKGUP profile in the CSFSERV class. The CSFSERV class will need to be SETR RACLIST(CSFSERV) REFRESH after authority is granted.

CSFG0014 SINGLE KEY SUPPLIED WITH TRANSKEY THAT DOES NOT PERMIT SINGLE KEY DECRYPTION.

Explanation: You supplied a single length key, but the TRANSKEY keyword specified an IMPORTER key that does not allow the decryption of a single length key. The key identifier of the CKDS record for the IMPORTER key must have the NOCV flag bit indicator set to 1 in order for a single length key to be decrypted when imported.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Either supply two key values or change the IMPORTER key to one that can be used to decrypt single length keys.

CSFG0024 NOCV SPECIFIED WITH TWO TRANSKEYS.

Explanation: You cannot specify the NOCV keyword with a TRANSKEY keyword that specifies two keys. The key generation utility program does not support the distribution of EXPORTER or IMPORTER keys that have NOCV capability to two sites.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Either remove the NOCV keyword or remove one of the TRANSKEY values and rerun the key generator utility program.

CSFG0035 ABEND DURING KEY GENERATION - PSW = *psw*, COMPLETION CODE = *code*.

Explanation: An abnormal ending occurred during key generator utility processing, where *psw* specifies the PSW at the time of the failure and *code* indicates the system completion code.

System action: Processing ends.

System programmer response: Respond to the problem that is identified by the PSW and the completion code, and any diagnostic messages that may have been issued prior to the abnormal end.

User response: Contact your system programmer.

Problem determination: In addition to the system programmer actions:

- Make sure that the failing job step includes a SYSUDUMP DD statement.
- Run the EREP service aid for detailed reports of the system's error activity. Save the output.

CSFG0056 CKDS CONTROL RECORD NOT FOUND.

Explanation: KGUP could not find the control record for the CKDS.

System action: Processing ends.

System programmer response: Either correct the CKDS or use another CKDS before running the key generator utility program again.

User response: Ensure that the CKDS is valid. If you cannot use the CKDS, contact your system programmer.

CSFG0064 CONTROL STATEMENT VERB NOT VALID.

Explanation: The control statement verb was not ADD, UPDATE, DELETE, RENAME or SET.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Supply a valid control statement verb of ADD, UPDATE, DELETE, RENAME, or SET and rerun the key generator utility program.

CSFG0074 SYNTAX ERROR IN CONTROL STATEMENT.

Explanation: A control statement was not valid.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Check the syntax of the control statement. Ensure that you specified the statement keywords and values correctly. For example, check for unpaired delimiters and missing or extraneous commas. Rerun the key generator utility program.

CSFG0084 SPECIFIED KEY VALUE IS NOT VALID.

Explanation: The specified value for the KEY keyword was not valid.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Check that the key values that you entered are valid hexadecimal values. The values should contain the characters A through F or the numerals 0 through 9. Rerun the key generator utility program.

CSFG0094 *Keyword1* **OR** *keyword2* **NOT SPECIFIED.**

Explanation: The control statement does not contain a required keyword, where *keyword1* and *keyword2* are the keywords.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Update the control statement with the required keyword and rerun the key generator utility program.

CSFG0104 *Keyword1* **AND** *keyword2* **BOTH SPECIFIED.**

Explanation: The control statement contains two mutually exclusive keywords, where *keyword1* and *keyword2* are the keywords.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Update the control statement with one of the keywords and rerun the key generator utility program.

CSFG0124 RANGE LABEL PREFIXES NOT EQUAL.

Explanation: The alphabetic prefixes of the starting and ending labels that you specified with the RANGE keyword are not the same.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Update the control statement by specifying equal prefixes for the starting and ending labels. Rerun the key generator utility program.

CSFG0144 END LABEL SUFFIX NOT GREATER THAN START LABEL SUFFIX FOR RANGE.

Explanation: The arithmetic value of the suffix for the ending label must be greater than the arithmetic value of the suffix for the starting label specified with the RANGE keyword.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Update the control statement so that the numeric value of the ending label suffix is greater than the numeric value of the starting label suffix. Rerun the key generator utility program.

CSFG0164 SAME KEY LABEL VALUES SPECIFIED FOR TRANSKEY.

Explanation: The TRANSKEY keyword specified two equal values for the key labels. Each key must have unique label values.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Update the control statement with unique key label values and rerun the key generator utility program.

CSFG0174 KEY VALUE AND TWO TRANSKEY LABELS SPECIFIED.

Explanation: You specified the KEY keyword and the TRANSKEY keyword with two labels together. Two TRANSKEY values are valid only when generating keys for distribution, so you cannot specify the KEY keyword in this case.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Either delete the key value or the second TRANSKEY label. Rerun the key generator utility program.

CSFG0204 KEY KEYWORD NOT SPECIFIED WITH KEY TYPE = *type*.

Explanation: When the key type is PINVER or MACVER, the control statement must contain the KEY keyword and its associated values.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Update the control statement with the KEY keyword and either supply the key values or change the key type. Rerun the key generator utility program.

CSFG0224 *keyword* SPECIFIED WITH TYPE *keytype*.

Explanation: There is a mismatch between *keyword* and *keytype*.

- If NOCV is specified, only key types EXPORTER or IMPORTER are allowed.
- KEYUSAGE may be specified only with key types with defined values as shown in the description for KEYUSAGE.
- DKYGENKYUSAGE may only be specified with key type DKYGENKY.
- If *keytype* CLRDES or CLRAES is specified, *keywords* CLEAR, OUTTYPE and TRANSKEY are not allowed.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Make sure that the keyword is valid for the key type. Rerun the key generator utility program.

CSFG0254 ENTRY *label type* FOUND ON CKDS. *verb* NOT PERFORMED.

Explanation: A CKDS entry with the key index *label type* was already on the CKDS. The key generator utility program could not perform the action (*verb*).

System action: KGUP bypassed the entry, but processed other valid labels or types on the control statement.

User response: Correct the label or key type on the control statement and rerun the key generator utility program.

CSFG0264 ENTRY *label type* NOT FOUND ON CKDS. *verb* NOT PERFORMED.

Explanation: A CKDS entry with the key index *label type* was not on the CKDS. KGUP could not perform the (*verb*) action. ICSF issues this message when one of these conditions occurs:

- An UPDATE, DELETE, or RENAME statement specified a key that did not exist.
- An ADD or UPDATE statement specified a key in the TRANSKEY keyword that did not exist. If you specify the KEY keyword, then the key type of the TRANSKEY will be IMPORTER; otherwise, the key type will be EXPORTER.

System action: KGUP bypassed the entry, but processed other valid labels or types on the control statement.

User response: Correct the label or key type on the control statement and rerun the key generator utility program.

CSFG0272 IMPORTED KEY DOES NOT HAVE ODD PARITY.

Explanation: A key with non-odd or mixed parity was imported.

System action: Processing continues.

User response: If your installation allows non-odd or mixed parity keys, no action is required.

Because you are importing the key value, you may need to check the key value for accuracy if you expected or require an odd parity key.

CSFG0284 BOTH TRANSPORT KEYS ARE EXPORTER TYPE WITH NOCV CAPABILITY.

Explanation: Both of the transport keys that you specified as label values with the TRANSKEY keyword are EXPORTER with the NOCV flag set on in the key identifier. The key generator utility program does not support distribution of a key to two sites that only process keys without control vectors.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Change one of the transport keys to one that is used to export keys with control vectors. Rerun the key generator utility program.

CSFG0293 ROUTINE *routine* FAILED. RETURN CODE = *retcode*, REASON CODE = *rsncode*.

Explanation: The cryptographic service routine *routine* returned with a return code of *retcode* and a reason code of *rsncode*, which is an unexpected combination.

System action: Depending on the severity of the error that caused the failure, KGUP either continues normal processing of the input control statements or ends processing.

This message appears if you are running KGUP on the IBM zSeries z990 and try to add a DATAXLAT key. You will get a return code of 8 and a reason code of 61.

System programmer response: If possible, correct the error that is indicated by the return code and the reason code combination for the cryptographic services. If you cannot correct error, contact the IBM Support Center.

User response: Contact your system programmer.

CSFG0302 STATEMENT NOT PROCESSED.

Explanation: This is the final message for a control statement that is not processed. ICSF issued diagnostic messages prior to this that contain specific information regarding the errors that have occurred.

System action: Depending on the severity of the error that caused the failure, KGUP either continues normal processing of the input control statements or ends processing.

User response: Investigate the previous diagnostic error messages.

CSFG0313 STATEMENT PARTIALLY PROCESSED.

Explanation: This is the final message for a control statement that KGUP has partially processed. This condition occurs when there is a mixture of unsuccessful and successful processing for control statements that specify more than one key to be processed; for example, RANGE(x,y) or LABEL(l1,l2,...,ln).

System action: Depending on the severity of the error that caused the failure, KGUP either continues processing of the input control statements or ends processing.

User response: Investigate the previous diagnostic error messages.

CSFG0321 STATEMENT SUCCESSFULLY PROCESSED.

Explanation: This is the final message for a control statement that is processed completely.

System action: Normal processing of the input file continues.

User response: None.

CSFG0395 INSTALLATION EXIT MODULE REQUIRED BUT NOT AVAILABLE.

Explanation: KGUP requires the installation exit module, but has not found it in any library that is specified in either the link list, or on a JOBLIB or STEPLIB DD JCL statement.

System action: Processing ends.

System programmer response: Link the installation exit module in one of the libraries that are designated in the system link list or in the JOBLIB or STEPLIB DD statement. The library must be APF-authorized. Rerun the key generator utility program.

CSFG0402 INSTALLATION EXIT NOT LOADED.

Explanation: An attempt to load the installation exit failed. You specify the load module name in the EXIT statement with the CSFKGUP exit identifier that is processed during ICSF initialization.

System action: Processing continues normally without calling the installation exit.

System programmer response: If the exit is required, specify a valid one.

CSFG0414 STATEMENT REJECTED BY INSTALLATION EXIT.

Explanation: The KGUP installation exit rejected a control statement. The rejected control statement precedes this message.

System action: Processing ends for this control statement. Normal processing of the input file continues.

System programmer response: Determine if the control statement was rejected because of an error or for other reasons. Follow local procedures for errors that are detected by your installation exit. If necessary, correct the error and rerun the job.

CSFG0425 KEY GENERATOR TERMINATED BY INSTALLATION EXIT.

Explanation: The key generator utility program ended at the request of the installation exit. The control statement KGUP was processing when this error occurred precedes this message in the diagnostic data set.

System action: Processing ends.

User response: Determine if processing ended normally, or because the KGUP installation exit encountered an error condition. If necessary, correct any errors in the control statements and rerun the key generator utility program.

CSFG0435 RETURN CODE *retcode* FROM INSTALLATION EXIT NOT VALID.

Explanation: The key generator utility installation exit returned a return code to the key generator utility program that is not valid. The control statement being processed precedes this message.

System action: Processing ends.

System programmer response: Check the installation exit to determine if there are problems in the module. Make any necessary corrections and re-link the installation exit.

User response: Contact your system programmer.

CSFG0445 INSTALLATION EXIT PREPROCESSING RETURN CODE = *retcode*. PROCESSING TERMINATED.

Explanation: The key generator utility program received a non-zero return code during the pre-processing phase of the exit.

System action: Processing ends.

System programmer response: Check the installation exit to determine if there are problems in the module. Make any necessary corrections and re-link the installation exit.

User response: Contact your system programmer.

CSFG0455 INSTALLATION EXIT POSTPROCESSING RETURN CODE = *retcode*. PROCESSING TERMINATED.

Explanation: The key generator utility program received a non-zero return code during the post-processing phase of the exit.

System action: Processing ends.

System programmer response: Check the installation exit to determine if there are problems in the module. Make any necessary corrections and re-link the installation exit.

User response: Contact the programmer responsible for the exit.

CSFG0465 INSTALLATION EXIT NOT AVAILABLE FOR PROCESSING SET STATEMENT.

Explanation: The installation exit was not available when processing the SET control statement.

System action: Processing ends.

System programmer response: Ensure that the installation exit resides in the appropriate library. If necessary, restart ICSF with the EXIT statement for CSFKGUP that is included in the installation options data set.

User response: If the SET control statement is required, contact the system programmer to make the exit available.

CSFG0474 *Keyword* **KEYWORD NOT SPECIFIED.**

Explanation: The control statement does not contain the required keyword, *keyword*.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Update the control statement with the required keyword and rerun the key generator utility program.

CSFG0484 TWO LABEL VALUES NOT SPECIFIED ON RENAME STATEMENT.

Explanation: The RENAME control statement does not contain two label values.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Update the control statement with two label values after the LABEL keyword. Rerun the key generator utility program.

CSFG0494 TOO MANY LABEL VALUES SPECIFIED.

Explanation: The control statement contains more than 64 labels.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Update the control statement with 1 to 64 label values and rerun the key generator utility program.

CSFG0504 INCORRECT NUMBER OF KEY VALUES SPECIFIED.

Explanation: The KEY keyword in the control statement contains an incorrect number of key values for the key type specified.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Update the control statement with the correct number of values (1, 2, 3 or 4) for the key type and rerun the key generator utility program.

CSFG0514 DUPLICATE LABEL VALUES SPECIFIED.

Explanation: The control statement contains duplicate label values for the LABEL keyword.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Update the control statement with unique label values and rerun the key generator utility program.

CSFG0524 MORE THAN TWO TRANSKEY VALUES SPECIFIED.

Explanation: The control statement contains more than two label values for the TRANSKEY keyword.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Update the control statement with two unique TRANSKEY label values and rerun the key generator utility program.

CSFG0544 KEY VALUE SPECIFIED NOT 16 CHARACTERS.

Explanation: The control statement contains a key value for the KEY keyword that is not 16 characters in length.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Specify 16 characters for the key value and rerun the key generator utility program.

CSFG0554 TWO RANGE VALUES NOT SPECIFIED.

Explanation: The control statement does not specify two label values with the RANGE keyword.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Update the control statement with starting and ending label values and rerun the key generator utility program.

CSFG0575 CLEAR KEYWORD SPECIFIED WHILE SPECIAL SECURITY MODE DISABLED.

Explanation: The CLEAR keyword requires special security mode.

System action: Processing ends.

User response: Contact your security administrator.

Programmer response: Make sure that SSM is enabled via the KGUP parameter, the Environment Control Mask, and system options. Then rerun the job.

CSFG0585 KEYS RETURNED FROM INSTALLATION EXIT DO NOT CONTAIN VALID HEXADECIMAL CHARACTERS.

Explanation: The key generator installation exit returned key values that are not valid. The values must be in hexadecimal characters.

System action: Processing ends.

System programmer response: Supply the correct hexadecimal values for the keys and re-link the installation exit.

User response: Contact your system programmer.

CSFG0614 OUTTYPE OF *outtype* NOT VALID WITH TYPE *type*.

Explanation: The OUTTYPE keyword specifies a key type that is not a valid complementary key type for the key type that is specified on the TYPE keyword. Refer to *z/OS Cryptographic Services ICSF Application Programmer's Guide* and *z/OS Cryptographic Services ICSF Administrator's Guide* for a list of valid TYPE and OUTTYPE combinations.

System action: Processing ends.

User response: Correct the KGUP statement.

CSFG0624 *Keyword* NOT VALID BECAUSE TYPE IS NULL.

Explanation: A keyword other than LABEL or RANGE was found with TYPE(NULL). The statement is not valid.

System action: Processing ends.

User response: Correct the KGUP statement.

CSFG0634 ONLY DOUBLE LENGTH KEY VALUES ALLOWED FOR KEY TYPES DATAM AND DATAMV.

Explanation: The control statement specifies a KEY with either a single-length or triple-length key value, but only a double-length key value is acceptable for the key type specified in the TYPE keyword.

System action: Processing ends.

User response: Correct the KGUP statement.

CSFG0643 SAME LABEL FOUND IN CKDS FOR TYPE *type1*. *Function* **NOT PERFORMED BECAUSE TYPE** *type2* **REQUIRES UNIQUE LABEL.**

Explanation: A KGUP control statement specifies ADD or RENAME, so KGUP is trying to place a new label on the CKDS. However, the same label name already exists on the CKDS for another key type (type1). Either the requested key type, or the key type of the existing CKDS entry, or both require a unique label.

System action: KGUP bypassed processing of the incorrect label. If this is a RANGE statement or a LABEL statement with multiple labels, processing of the other labels continues.

User response: Correct the KGUP statement.

CSFG0654 *Keyword* **NOT VALID FOR DELETE.**

Explanation: The specified keyword is not valid on a DELETE statement. The only valid keywords on a DELETE statement are TYPE and either LABEL or RANGE.

System action: Processing ends.

User response: Correct the KGUP statement.

CSFG0664 RANGE LABEL SUFFIXES ARE NOT THE SAME LENGTH.

Explanation: The two RANGE labels you specified do not have the same number of numeric digits after the last nonnumeric character in the label.

System action: Processing ends.

User response: Correct the KGUP statement.

CSFG0674 RANGE LABEL SUFFIX HAS TOO MANY DIGITS.

Explanation: You specified a RANGE label with more than 4 numeric digits after the last nonnumeric character. The maximum suffix value is 9999.

System action: Processing ends.

User response: Correct the KGUP statement.

CSFG0684 RANGE LABEL HAS NO NUMERIC SUFFIX.

Explanation: You specified a RANGE label with a nonnumeric character as its last character. A valid RANGE label must end with 1–4 numeric digits, which specifies a suffix value between 0 and 9999.

System action: Processing ends.

User response: Correct the KGUP statement.

CSFG0704 UPDATE NOT ALLOWED FOR TYPE NULL.

Explanation: An UPDATE statement specifies TYPE(NULL), which is allowed only in an ADD statement or DELETE statement.

System action: Processing ends.

User response: Correct the KGUP statement.

CSFG0715 INSTALLATION EXIT CHANGED THE <LABEL|TYPE> FOR *label type*.

Explanation: The installation exit changed the LABEL or TYPE of *label type* in the exit parameter block, which is not allowed.

System action: Processing ends.

System programmer response: Remove changes that the installation exit made to the type or label portion of the key.

User response: Contact your system programmer.

CSFG0735 INCORRECT VALUE OF LENGTH FOR KEY TYPE *type.*

Explanation: The LENGTH keyword on either an ADD or UPDATE statement contained a value greater than the maximum allowable length for the key type. For types MAC, MACVER, and DATAXLAT, the maximum allowable length is 8. For type DATA, the maximum is 24. For all other types, the maximum is 16.

System action: Processing for the ADD or UPDATE statement ends.

User response: Correct the KGUP statement so that the value of LENGTH does not exceed the maximum for the key type.

CSFG0744 LABEL NOT FOUND.

Explanation: The attempt to retrieve the key failed. The label was not found in the PCIXCC specified.

System action: Processing for this statement ends.

User response: Check that the correct label was specified and the correct serial number for the PCIXCC was specified. If so, create the key on the PCIXCC using the TKE workstation. Otherwise, correct the KGUP statement with the correct label and PCIXCC serial number.

CSFG0754 LABEL NOT COMPLETE.

Explanation: The attempt to retrieve the key from the PCIXCC failed. The label was found but the key is not complete.

System action: Processing for this statement ends.

User response: Check that the correct label was specified and the correct serial number for the PCIXCC was specified. If so, complete the key on the PCIXCC using the TKE workstation. Otherwise, correct the KGUP statement for the correct label and PCIXCC serial number.

CSFG0764 CONTROL VECTOR NOT VALID - *keycv*

Explanation: The attempt to retrieve the key failed. The control vector of the key on the specified PCIXCC is not valid. The control vector is returned.

System action: Processing for this statement ends.

User response: Check that the control vector was specified correctly. If not, clear the key part register for the label and reenter the key with the correct control vector using the TKE workstation.

CSFG0770 OPKYLOAD SUCCESSFUL, VERIFICATION PATTERN *keyvp*

Explanation: The key token retrieved from the PCIXCC for the specified key label was successfully written to the CKDS. The ENC-ZERO verification pattern for the key is given.

System action: Processing continues.

User response: Compare the verification pattern against the pattern generated when the key was completed at the TKE workstation to verify the key has the correct key value.

CSFG0780 A REFRESH OF THE IN-STORAGE CKDS IS NECESSARY TO ACTIVATE CHANGES MADE BY KGUP.

Explanation: KGUP has made changes to the disk copy CKDS defined on your CSFCKDS DD statement. In order to activate those changes to your in-storage CKDS, a refresh is needed.

System action: Processing continues.

User response: When you want to activate the changes made by this control card to your in-storage CKDS copy, use the refresh option from the ICSF panels or the CSFEUTIL Program. A refresh should be performed on all systems sharing the updated CKDS to ensure that they all utilize the updated CKDS records.

CSFG0791 KEYWORD *keyword* IS NO LONGER SUPPORTED.

Explanation: The keyword is not supported by CSFKGUP. The keyword is tolerated but ignored.

System action: Processing continues.

User response: Consider updating your control statement data sets and removing the unsupported keyword.

CSFG0804 KEY TYPE *keyword1* NOT VALID WITH ALGORITHM *keyword2*.

Explanation: The *keyword1* key type is not supported for ALGORITHM *keyword2*.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Select a supported key type for the algorithm specified. Re-run the key generator utility program.

CSFG0814 KEYWORD *keyword1* NOT VALID WITH ALGORITHM *keyword2*.

Explanation: The *keyword1* control statement keyword is not supported for ALGORITHM *keyword2*.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Correct the control statement and re-run the key generator utility program.

CSFG0824 ALGORITHM MISMATCH FOR UPDATE REQUEST.

Explanation: A request to update a key failed because the key is encrypted under a different master key than the one indicated by the ALGORITHM keyword. The algorithm of an existing key may not be changed.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Specify the correct ALGORITHM for the key. Re-run the key generator utility program.

CSFG0834 ALGORITHM *keyword* NOT AVAILABLE ON SYSTEM.

Explanation: The attempt to add or update a label in the key store failed. Possible reasons for the failure are:

1. The *keyword* algorithm is not available on your system in a cryptographic coprocessor, the CPACF or ICSF software
2. The master key for the algorithm is not loaded into the cryptographic coprocessors and key store.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Contact your system administrator to determine which system can process the requested algorithm and run your request on that system.

CSFG0856 CKDS IS NOT USABLE.

Explanation: The cryptographic key data set specified cannot be used by KGUP. Either the DES MKVP is not in the control record or record level authentication is off. This CKDS was initialized on a later release of ICSF and is not backwardly compatible.

System action: Processing ends.

User response: Specify a CKDS that is compatible with this release of ICSF.

CSFG0866 ENTRY *label* IS ENHANCED WRAPPED KEY TOKEN. *verb* NOT PERFORMED.

Explanation: The entry with the key index *label* is a key token wrapped with the enhanced X9.24 CBC method. Tokens with this wrapping cannot be deleted, updated, or renamed by KGUP.

System action: Processing for the UPDATE, DELETE, or RENAME statement ends.

User response: Correct the KGUP statement so that the label is not for a key token wrapped with the enhanced method.

CSFG0876 ENTRY *label* IS AN HMAC KEY TOKEN. *verb* NOT PERFORMED.

Explanation: The entry with the key index label is an HMAC key which cannot be deleted or updated by KGUP.

System action: Processing for the UPDATE, DELETE or RENAME statement ends.

User response: Correct the KGUP statement so that the label is not of a HMAC key.

CSFG0896 ENTRY IS A VARIABLE-LENGTH KEY TOKEN. *verb* NOT PERFORMED.

Explanation: The operational key specified is a variable-length symmetric key. The CKDS specified to KGUP contains only fixed-length records and cannot contain a variable-length symmetric key token.

System action: Processing for the OPKYLOAD statement ends.

User response: Correct the KGUP statement so that the label is not for a variable-length symmetric key token or specify a CKDS which can contain variable-length symmetric tokens.

CSFG0904 KEY TYPE *keytype* SPECIFIED WITH VERB *verb*.

Explanation: The *keytype* specified is not valid with the *verb* in the control statement.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Correct the control statement and rerun the key generator utility program.

CSFG0914 KEYUSAGE VALUE *value* SPECIFIED WITH *keytype* KEY TYPE FOR ALGORITHM *algorithm*.

Explanation: The KEYUSAGE *value* is not valid for the key type and algorithm specified in the control statement. The valid values are shown in the description for KEYUSAGE.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Check the syntax of the control statement. Ensure that you specified the statement keywords and values correctly. For example, check for unpaired delimiters and missing or extraneous commas. Rerun the key generator utility program.

CSFG0924 KEYUSAGE VALUES ARE NOT CONSISTENT.

Explanation: The KEYUSAGE values are not consistent. There may be more than one value specified where only one is allowed. Two or more values may have been specified which are not allowed to be used together. There may be one or more missing values. DKYUSAGE may not have been specified when the DKYGENKYUSAGE keyword was specified.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Check the syntax of the control statement. Ensure that you specified the statement keywords and values correctly. For example, check for unpaired delimiters and missing or extraneous commas. Rerun the key generator utility program.

CSFG0934 DUPLICATE TOKEN IN CKDS.

Explanation: A key token was either randomly generated or created from the value in the KEY keyword. The key token was not written to the CKDS because the XFACILIT resource CSF.CKDS.TOKEN.NODUPLICATES is enabled and the key token is the same as an existing token in the CKDS.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: If generating key tokens with random values, rerun the request. If a key value was supplied, the key token created cannot be written to the CKDS while the CSF.CKDS.TOKEN.NODUPLICATES resource is enabled.

CSFG0944 TRANSPORT KEY NOT COMPATIBLE WITH KEY TYPE AND ALGORITHM.

Explanation: A transport key was specified that cannot be used to wrap the key being generated. AES transport keys must be specified when processing AES keys and DES transport keys must be specified when processing DES keys.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Specify transport key or keys that are compatible with the key type and algorithm being processed.

CSFG0956 *ddname* **DOES NOT SUPPORT KEY TOKEN.**

Explanation: The key being processed cannot be written to the ddname data set. If you are generating an AES key that uses the variable-length token, the CKDS must be the variable-length record format. For the CSFKEYS data set, the LRECL must be large enough to accept a variable-length token. The LRECL should be at least 644.

System action: Processing ends.

User response: Specify a variable-length record format CKDS in the data set definitions. If you don't have a CKDS, contact your ICSF administrator. For the CSFKEYS data set, allocate a data set with a larger LRECL.

CSFG0964 KEY LENGTH NOT COMPATIBLE WITH *keyword***.**

Explanation: The length of the key specified by the LENGTH keyword or the number of key values supplied with the KEY keyword is not compatible with the *keyword*. The DOUBLE-O keyword requires a key length of 16.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Correct the length specified for the *keyword*.

CSFG0974 INSTALLATION EXIT IS NOT CALLED FOR RECORD POST-PROCESSING OF KDSR FORMAT RECORDS

Explanation: The key generator utility program has the CSFKGUP installation exit loaded and the CKDS is in KDSR format. The installation exit cannot be called during the post-processing phase for KDSR format records.

System action: Processing continues.

System programmer response: Verify that the installation exit is still required.

User response: Contact the programmer responsible for the exit.

CSFG0986 CKDS IS NOT USABLE.

Explanation: The cryptographic key data set specified cannot be used by KGUP. The master key verification patterns in the CKDS do not match the verification patterns of the active DES and AES master keys.

System action: Processing ends.

User response: Specify a CKDS that is compatible with this release of ICSF.

CSFG0994 DKYGENKYUSAGE VALUE *value* **SPECIFIED WITH** *keytype* **KEY TYPE FOR ALGORITHM** *algorithm***.**

Explanation: The DKYGENKYUSAGE *value* is not valid for the key type and algorithm specified in the control statement. The valid values are shown in the description for DKYGENKYUSAGE.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Check the syntax of the control statement. Ensure that you specified the statement keywords and values correctly. For example, check for unpaired delimiters and missing or extraneous commas. Rerun the key generator utility program.

CSFG1004 DKYGENKYUSAGE VALUES ARE NOT CONSISTENT.

Explanation: The DKYGENKYUSAGE values are not consistent. There may be more than one value specified where only one is allowed. Two or more values may have been specified which are not allowed to be used together. There may be one or more missing values.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Check the syntax of the control statement. Ensure that you specified the statement keywords and values correctly. For example, check for unpaired delimiters and missing or extraneous commas. Rerun the key generator utility program.

CSFG1014 ENCRYPTED KEY SUPPLIED FOR AES KEY.

Explanation: An encrypted key value was supplied to be imported to an AES key. This usage is not supported for AES as it is for DES.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Check the syntax of the control statement. Ensure that you specified the statement keywords and values correctly. Rerun the key generator utility program.

CSFG1024 KEYUSAGE VALUES REQUIRE KEY OR TRANSKEY.

Explanation: Certain KEYUSAGE values for a key type require the complementary key be generated or a key value be supplied. If, for example, an AES CIPHER key is generated with KEYUSAGE(ENCRYPT), the key can only be used for encrypting data. There is no key to decrypt the data. A key value can be supplied and a complementary key can be generated with the same key value. A complementary key can be generated and wrapped with a transport key. Complementary KEYUSAGE values are shown in the *z/OS ICSF Administrator's Guide* in the description for KEYUSAGE.

System action: Processing ends for this control statement. Normal processing of the input file continues.

User response: Check the syntax of the control statement. Decide whether to provide a key value or transport key or modify the KEYUSAGE values. Rerun the key generator utility program.

CSFG1034 TRANSKEY IS NOT USABLE. CKDS RECORD IS *state*.

Explanation: The transport key specified in the control statement is not active and cannot be used. The state of the record is either archived, pre-active, or deactivated.

System action: Processing for the UPDATE or ADD statement ends.

User response: Correct the KGUP statement so that the TRANSKEY is an active transport key.

CSFG1042 TRANSKEY *label* HAS BAD METADATA.

Explanation: The CKDS record for the transport key specified in the control statement has bad metadata. This is an informational message. The control statement will be processed.

The metadata for the CKDS record will be corrected when the CKDS is refreshed.

System action: Processing continues.

User response: None.

Chapter 6. CSFHnnnn messages (IBM Health Checker processing)

Chapter 6, "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.

CSFH0001I The (ICSF, ICSFMIG7731_ICSF_RETAINED_RSAKEY) check found no apparent retained RSA key use on this system because there are no online coprocessors that support retained keys.

Explanation: A migration check indicates that there is no apparent retained RSA key use on this system because there are no online processors.

System action: Processing continues.

CSFH0002I Cryptographic coprocessors were examined and the (ICSF, ICSFMIG7731_ICSF_RETAINED_RSAKEY) check found no apparent RSA key use on this system.

Explanation: A migration check indicates that there is no apparent retained RSA key use on this system.

System action: Processing continues.

CSFH0003E Cryptographic coprocessors were examined and found to possess retained RSA Keys.

Explanation: Online coprocessors possess one or more retained RSA keys, implying retained RSA keys are potentially being used on this system. ICSF is deprecating its retained RSA key support.

System action: There is no effect on the system.

Operator response: Report this exception to the system programmer.

System programmer response: Alert the installation security administrator and application and middleware administrators for this system.

Problem determination: Investigate the cryptographic services utilized by the workload executed on this system. Determine application and middleware products using retained RSA key services for key management use and depend upon the key labels listed in the report. Develop an immediate strategy to remove any dependencies on creating new ICSF-supported retained RSA keys prior to migration, and an eventual strategy to remove any dependencies on ICSF-supported retained key interfaces.

CSFH0010E Coprocessor or Accelerator *ttnn* **serial number** *nnnnnnn* **has changed states from** *xxxxxxxx* **to** *yyyyyyy*

Explanation: The Coprocessor or accelerator state has degraded since the last check. This has a possible negative impact on the operation of ICSF and the dependent cryptographic workload.

System action: There is no effect on the system. Processing continues.

Operator response: Report this exception to the system programmer.

System programmer response: Alert the installation security administrator to determine the impact of the change in coprocessor state.

Problem determination: Refer to the ICSF Coprocessor Management and hardware status panels and the support element (SE) panel for further information regarding the coprocessors.

CSFH0011I Cryptographic Service *name* **is currently used, but this service has been deprecated.**

Explanation: The specified callable service is not being supported. Workloads using the service will fail.

System action: There is no effect on the system. Processing continues.

Operator response: Report this exception to the system programmer.

System programmer response: Alert the installation security administrator and application/middleware administrators for this system.

Problem determination: Investigate applications using the service and determine appropriate actions to remove or replace the use of this service.

CSFH0012I (ICSF,ICSF_COPROCESSOR_STATE_NEGCHANGE): Check performed with no problems found.

Explanation: The current state of the cryptographic coprocessors and accelerators have been checked and no state degradation was found.

System action: Processing continues.

CSFH0013I (ICSF,ICSF_DEPRECATED_SERV_WARNINGS): Check performed with no problems found.

Explanation: A migration check verified that no services targeted for removal are being used.

System action: Processing continues.

CSFH0014I (ICSF, ICSF_MASTER_KEY_CONSISTENCY): 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.

System action: Processing continues.

Operator response: None

User response: None

CSFH0015E The state of the *xxx* master key is not consistent across all 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.

System action: Processing continues.

Operator response: Investigate the coprocessor states displayed on the coprocessor management panel. Master keys in a correct state (“C”), but not an active state ('A') are not available for work. Ensure specified master key is the desired state for all coprocessors.

User response: Contact the ICSF administrator.

CSFH0016E Unable to process request for Master Key consistency check.

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

System action: Processing continues.

Operator response: Investigate the coprocessor states displayed on the coprocessor management panel. Check the message logs and trace entries for problems.

User response: Contact the ICSF administrator.

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

Explanation: There are no cryptographic coprocessors applicable to this check on this system.

System action: There is no effect on the system.

Operator response: None.

System programmer response: None.

Problem determination: N/A

ICSF Administrator response: None.

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.

System programmer response: None.

Problem determination: N/A

ICSF Administrator response: None.

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.

System programmer response: None.

Problem determination: N/A

ICSF Administrator response: None.

Reference: *z/OS Cryptographic Services ICSF 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 is installed. The current type master key or keys loaded 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 DES, RSA, AES, and ECC.

System action: There is no effect on the system.

Operator response: Contact the ICSF administrator.

System programmer response: None.

Problem determination: The ICSF Coprocessor Management panel displays all cryptographic processors and their status. For FMID HCR7780 and newer, 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.

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.

Reference: *z/OS Cryptographic Services ICSF 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.

System programmer response: None.

Problem determination: None.

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

Reference: *z/OS Cryptographic Services ICSF 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.

System programmer response: Contact the ICSF administrator.

Problem determination: None.

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

Reference: *z/OS Cryptographic Services ICSF Overview*

Check Reason: Detects systems that ICSF no longer supports.

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.

System programmer response: None.

Problem determination: None.

ICSF Administrator response: None.

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.

System programmer response: None.

Problem determination: N/A

ICSF Administrator response: None.

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 be lost when running with ICSF HCR77A1. The size of the object in the record is too large for the 'User data' field to be preserved with the new record format.

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

Reference: *z/OS Cryptographic Services ICSF Administrator's Guide*

CSFH0027I (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.

System programmer response: None.

Problem determination: N/A

ICSF Administrator response: None.

CSFH0030I Cryptographic records expiring in *nnn* days.

Explanation: This informational message indicates the number of days used for the check.

System action: There is no effect on the system.

Operator response: None.

Problem determination: N/A

ICSF Administrator response: None.

CSFH0031E Records were detected that will expire within the next *nnn* days.

Explanation: This check detected records in the key data set that will reach their expiration date within the specified interval. When the keys reach their expiration date, the keys can no longer be used by the applications.

System action: There is no effect on the system.

Operator response: Contact the ICSF administrator.

Problem determination: The Key Data Set Metadata Read callable service can be used to read the key material validity dates for the labels specified in the output of the check. The Key Data Set Metadata Write callable service can be used to change or remove the key material validity dates for the records specified.

ICSF Administrator response: The administrator should determine if the records specified in the output of the check needs to be deleted, replaced, or have the key material validity end date adjusted. When a record is updated with new key material, the key material validity dates need to be reset.

The CKDS Key Record Delete, PKDS Key Record Delete and Token Record Delete callable services are used to delete records from the key data sets.

The Key Data Set Metadata Read callable service can be used to read the key material validity dates for the labels specified in the output of the check.

The Key Data Set Metadata Write callable service can be used to change or remove the key material validity dates for the records specified.

Reference: *z/OS Cryptographic Services ICSF Administrator's Guide*

z/OS Cryptographic Services ICSF Application Programmer's Guide

---

CSFH0032I No KDS records will expire within the next *nnn* days.

Explanation: This is an informational message indicating that the check did not detect any records in the key data sets that will reach their expiration date within the specified interval.

System action: There is no effect on the system.

Chapter 7. CSFInnnn messages (Component trace)

Chapter 7, "CSFInnnn messages (Component trace)" describes diagnostic messages that are issued only in an interactive problem control system (IPCS) environment. These messages are sent to the IPCS print file (IPCSPRNT).

CSFI002E *Module-name* **IPCS ERROR** *retcode*

Explanation: Module *module-name* encountered an IPCS service error. The return code is indicated in *retcode*.

System action: ICSF component trace formatting or control block formatting ends.

User response: Check the meaning of the return code in *z/OS MVS Diagnosis: Reference*.

CSFI003E *Module-name* **UNABLE TO LOCATE** *control-block* **- FOUND** *identifier*

Explanation: Either ICSF was not initialized, or module *module-name* was not able to locate the control block that is indicated in *control-block*. Instead, it found the identifier.

System action: ICSF component trace formatting or control block formatting ends.

User response: Either use the correct level of the formatter for the dump, take another up-level dump, or contact the IBM Support Center.

CSFI004E *Module-name* **UNABLE TO USE** *control-block*

Explanation: Either module *module-name* was not able to locate the control block following the control block *control-block* because the pointer to it from the *control-block* was zero, or ICSF was not initialized or was not running.

System action: ICSF component trace formatting or control block formatting ends.

User response: Either use the correct level of the formatter for the dump, take another up-level dump, or contact the IBM Support Center.

Chapter 8. CSFMnnnn messages (ICSF address space)

Chapter 8, "CSFMnnnn messages (ICSF address space)" describes messages that the Integrated Cryptographic Service Facility mainline task issues. Most of these messages are issued to the operator console or the security console (routing codes 1 and 9). Some are sent to the ICSF job log.

Identification of cryptographic features

Starting in ICSF release HCR77B0, the prefix used to identify Crypto Express2, Crypto Express3, and Crypto Express4 features has changed. Table 2 lists the prefix for these features for releases prior to HCR77B0 and the prefix for these features for HCR77B0 and later releases. This change applies to ICSF messages, panels, and publications. The TKE workstation uses this same identification starting with TKE release 8.0.

Table 2. Cryptographic feature identification

Cryptographic feature	Prefix for releases prior to HCR77B0	Prefix for HCR77B0 and later releases
Crypto Express2 coprocessor	E	2C
Crypto Express2 accelerator	F	2A
Crypto Express3 coprocessor	G	3C
Crypto Express3 accelerator	H	3A
Crypto Express4 CCA coprocessor	SC	4C
Crypto Express4 EP11 coprocessor	SP	4P
Crypto Express4 accelerator	SA	4A
Crypto Express5 CCA coprocessor	N/A	5C
Crypto Express5 EP11 coprocessor	N/A	5P
Crypto Express5 accelerator	N/A	5A

CSFM001I ICSF INITIALIZATION COMPLETE

Explanation: This is the normal message that is expected in response to a START CSF operator command. However, if ICSF services are not supported because the master key has not been validated yet, message CSFM400I may follow.

System action: Processing continues.

Operator response: None.

System programmer response: If ICSF services are not available, check to see if the master key has been validated.

CSFM002E ICSF STOP REQUEST OVERRIDDEN BY INSTALLATION EXIT *exit-name*.

Explanation: If installation exit CSFEXIT4 denies or overrides the STOP request, ICSF issues this message in response to an operator requested STOP (P CSF) command. The exit returned a return code of 4. For more information about CSFEXIT4, see the *z/OS Cryptographic Services ICSF System Programmer's Guide*.

The *exit-name* is the name of the routine.

System action: Processing continues.

Operator response: If appropriate, contact your system programmer.

System programmer response: Determine if the CSFEXIT4 installation exit is working properly.

CSFM003A ICSF TERMINATING. MUST BE RUN AS A STARTED TASK.

Explanation: ICSF must be started with a START CSF operator command. If ICSF is not a started task (for example, a batch job), this message is issued.

System action: ICSF ends.

Operator response: If appropriate, issue the START CSF command.

System programmer response: Determine why ICSF was not started as a started task.

CSFM004A ICSF TERMINATING. ICSF ALREADY ACTIVE.

Explanation: This message is issued if you try to start ICSF and one of these is true:

- You specified COMPAT(YES) mode, and PCF or CUSP is currently active.
- ICSF is currently active.

System action: If PCF or CUSP is active, ICSF ends. If ICSF is already active, the new call to ICSF ends, and ICSF remains active.

Operator response: If appropriate, contact your system programmer.

System programmer response: If PCF or CUSP is already active, you can start ICSF with either COMPAT(NO) or COMPAT(COEXIST) mode.

CSFM006A ICSF TERMINATING DUE TO INSTALLATION EXIT *exit-name***.**

Explanation: ICSF issues this message when an installation exit issues a request to stop ICSF. The *exit-name* indicates the name of the exit. CSFEXIT1, CSFEXIT2, CSFEXIT3, and CSFEXIT5 are the possible exits that can issue a request to stop ICSF. For more information about these exits, see the *z/OS Cryptographic Services ICSF System Programmer's Guide*.

System action: ICSF ends.

Operator response: If necessary, contact your system programmer.

System programmer response: None.

CSFM009I NO ACCESS CONTROL AVAILABLE FOR ICSF SERVICES OR KEYS

Explanation: ICSF issues this message if it is unable to perform RACROUTE REQUEST=LIST for any or all of the classes CSFSERV, CSFKEYS, CRYPTOZ, and XCSFKEYS during initialization. This results in ICSF not creating in-store profiles which affects performance, but the SAF checks are still performed.

System action: Processing continues.

Operator response: Inform the system programmer.

System programmer response: If the installation is using RACF for ICSF security, ensure that the correct level of RACF is installed. Also, check RACF to see that ICSF is setup (that the CSFSERV, CSFKEYS, CRYPTOZ, and XCSFKEYS classes have been defined for ICSF).

Programmer response: If the installation is using security exits instead of RACF for ICSF security, ensure that the ICSF OPTIONS data set contains EXIT statements that name those exits.

CSFM010E ICSF TERMINATING. PROCESSOR IS UNSUPPORTED.

Explanation: ICSF is being started on hardware that is not supported starting at release HCR77A1.

System action: ICSF ends.

Operator response: Inform your system programmer.

System programmer response: Contact the IBM Support Center.

CSFM011I FASTAUTH IS NOT SUPPORTED BY THE INSTALLED SECURITY PRODUCT.

Explanation: ICSF issues this message to notify users when it will not be issuing RACROUTE REQUEST=FASTAUTH requests due to the installed security product not supporting those requests.

System action: ICSF will continue processing. No checking will be performed before accessing ICSF services or the CKDS and PKDS.

Operator response: Notify your security administrator.

System programmer response: Contact your installed security product provider to see if an upgrade is available which supports RACROUTE REQUEST=FASTAUTH.

CSFM012I NO ACCESS CONTROL AVAILABLE FOR CRYPTOZ RESOURCES. ICSF PKCS11 SERVICES DISABLED.

Explanation: ICSF issues this message if it is unable to perform RACROUTE REQUEST=LIST for the class CRYPTOZ during initialization. It is issued only if CRYPTOZ processing is required based on the ICSF options specified:

- TKDSN(*tkds-data-set-name*) or
- FIPSMODE(COMPAT,FAIL(*fail-option*))

System action: Processing continues. However, ICSF PKCS #11 service functions that require CRYPTOZ processing are disabled.

- Persistent (TKDS) PKCS #11 objects are not available.
- FIPS compatibility mode reverts to FIPS standard mode.
- Key security decisions cannot be directed by setting permission to the CLEARKEY.token-label resource.

Operator response: Inform your system programmer.

System programmer response: If the installation is using RACF for ICSF security, ensure that the correct level of RACF is installed. Check RACF to ensure that the CRYPTOZ class has been activated and RACLISTed.

Programmer response: If the installation is using security exits instead of RACF for ICSF security, ensure that the ICSF OPTIONS data set contains EXIT statements that name those exits.

CSFM013I ICSF CANNOT START. THERE NEEDS TO BE A PPT ENTRY FOR CSFINIT.

Explanation: ICSF requires a PPT entry for CSFINIT in order to start.

System action: ICSF initialization terminates.

System programmer response: Ensure that the proper PPT registration for CSFINIT is installed, and that the library containing the CSFINIT CSECT is APF authorized.

CSFM014I FIPS 140 KNOWN ANSWER TEST FOR PKCS11 SERVICES FAILED.

Explanation: As a part of FIPS 140-2 compliance, the ICSF z/OS PKCS #11 software services must perform a series of known answer cryptographic algorithm tests. This message indicates that at least one of the tests did not complete successfully.

System action: ICSF main or subtask initialization continues, but PKCS #11 services are disabled.

System programmer response: Ensure that feature code 3863 is installed. If the problem occurs with feature code 3863 installed, contact the IBM Support Center.

CSFM015I FIPS 140 SELF CHECKS FOR PKCS11 SERVICES SUCCESSFUL.

Explanation: ICSF z/OS PKCS #11 software services perform a series of self tests during initialization. This message indicates that all the tests have completed successfully.

System action: ICSF initialization continues.

System programmer response: This is an information message only. No response is required.

CSFM016I FIPS 140 NOT SUPPORTED.

Explanation: The ICSF installation option FIPSMODE(YES,FAIL(NO)) FIPSMODE(COMPAT,FAIL(NO)) has been specified, indicating that the z/OS PKCS #11 services must operate in compliance with FIPS 140-2. However, either the current IBM z Systems model type or the version/release of z/OS that is running on it does not support FIPS. The supported z/OS versions/releases are V1R10 and higher.

System action: ICSF initialization continues, but FIPSMODE mode is disabled.

System programmer response: None

CSFM022E ICSF TERMINATING. THE USE OF CSFINIT REQUIRED IN THE STARTED TASK PROCEDURE.

Explanation: An attempt was made to start ICSF using PGM=CSFMMAIN in the started procedure. As of HCR7770, the use of PGM=CSFINIT is required for ICSF to start.

System action: ICSF initialization terminates.

System programmer response: Change the started procedure to use PGM=CSFINIT

CSFM050I ENHANCED SYMMETRIC KEY WRAPPING IS NOT SUPPORTED.

Explanation: The options data set keyword DEFAULTWRAP was specified with ENHANCED wrapping for symmetric keys. There are no coprocessors online that support the enhanced wrapping. All symmetric keys will be wrapped with the original wrapping until a coprocessor that supports enhanced wrapping comes online.

System action: Processing continues.

System programmer response: Check that the correct coprocessors are available on this system.

CSFM051E UNABLE TO SET DEFAULT WRAPPING CONFIGURATION ON COPROCESSOR *cii*

Explanation: ICSF attempted to set the default wrapping configuration on a cryptographic coprocessor, but was unable to do so due to an error in the coprocessor code. To ensure symmetric keys are properly wrapped, this coprocessor will not be available for active work. The substitution variables are:

- *c* - the short name for the coprocessor type. For example, 3C (representing a CEX3C).
- *ii* - the index or position where the cryptographic feature is installed.

System action: Processing continues.

Operator response: Consider restarting ICSF. If the problem persists, contact the system programmer.

System programmer response: When there is a coprocessor with persistent error setting the default wrapping configuration, contact IBM.

CSFM100E CRYPTOGRAPHIC KEY DATA SET, *dsname* **IS NOT INITIALIZED.**

Explanation: ICSF detected a master key verification pattern that was not valid on the cryptographic key data set (CKDS). Either the CKDS was not initialized or the CKDS is not valid for this system.

It is normal to see this message the first time ICSF starts, as the CKDS has yet to be initialized.

System action: If the CKDS was not initialized, processing continues but cryptographic services are not enabled.

Operator response: Contact your system programmer.

System programmer response: If the CKDS was not initialized, initialize the CKDS through the ICSF panels. You may need to load the master key into the new master key register.

If the CKDS is unusable for the system, update the installation options data set with the correct CKDS and restart ICSF.

CSFM101E PKA KEY DATA SET, *dsname* IS NOT INITIALIZED.

Explanation: ICSF detected a master key verification pattern that was not valid on the PKA data set (PKDS). Either the PKDS was not initialized or the PKDS may not be valid for this system. It is normal to see this message the first time ICSF starts.

System action: The system continues processing but the PKA callable services are not enabled.

Operator response: None

System programmer response: The system administrator should enter the correct PKA master key and initialize the PKDS.

CSFM102I TOKEN DATA SET, *dsname* IS NOT INITIALIZED FOR SECURE KEY PKCS11.

Explanation: During ICSF start, ICSF detected a non-existent master key verification pattern on the token data set (TKDS) with Enterprise PKCS #11 coprocessors online. The TKDS was not initialized for secure key processing. It is normal to see this message the first time ICSF starts.

System action: Processing continues but secure key PKCS #11 services are not available.

Operator response: Contact your system programmer.

System programmer response: Initialize the TKDS through the ICSF panels. You may need to load the master key into the new master key register.

CSFM109I CRYPTOGRAPHIC FEATURE IS OFFLINE. *coprocessor-name cii*, SERIAL NUMBER *nnnnnnn*.

Explanation: A cryptographic feature is offline and cannot be used for any operation. The substitution variables are:

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  - CRYPTO EXPRESS2 ACCELERATOR
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - PCI CRYPTO ACCELERATOR
  - PCI X CRYPTO COPROCESSOR
- *c* - the short name for the coprocessor type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnnn* or N/A - the serial number for the cryptographic feature, or N/A when the feature is configured as an accelerator.

System action: The system will not use the cryptographic feature for cryptographic operations.

Operator response: None

System programmer response: Have the cryptographic feature brought online.

CSFM111I CRYPTOGRAPHIC FEATURE IS ACTIVE. *coprocessor-name cii*, **SERIAL NUMBER** *nnnnnnn*.

Explanation: The cryptographic feature is online and operational. When the cryptographic feature is a coprocessor, the ACTIVE message indicates that the master keys are active and ICSF services may be used. The substitution variables are:

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  - CRYPTO EXPRESS2 ACCELERATOR
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - PCI CRYPTO ACCELERATOR
  - PCI X CRYPTO COPROCESSOR
- *c* - the short name for the coprocessor type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnnn* or N/A - the serial number for the cryptographic feature, or N/A when the feature is configured as an accelerator.

System action: The system will use the cryptographic feature for cryptographic operations.

Operator response: None

System programmer response: None

CSFM122I PKA SERVICES WERE NOT ENABLED DURING ICSF INITIALIZATION.

Explanation: This message is issued during ICSF initialization and indicates that the PKA callable services control was not enabled. There are multiple reasons why ICSF would not have enabled the PKA services control. If the RSA Master Key set on the cryptographic coprocessor does not match the RSA Master Key verification pattern in the PKDS header record is a possibility. Once the PKA callable services control is enabled, this message is no longer highlighted and the message is allowed to scroll.

Note: This message will not be issued when your system has no CCA coprocessors or your system has CEX3C or later CCA coprocessors (with the September 2011 or later LIC) online. The availability of RSA callable services will

depend on the status of the RSA master key. The PKA callable services control will not be active. CSFM130I is issued when the RSA master key is active and RSA callable services are available.

System action: ICSF initialization continues.

Operator response: None.

System programmer response: Verify a valid RSA Master Key is set on the cryptographic coprocessor. Verify the active PKDS is initialized and contains a matching RSA Master Key verification pattern. Manually enable the PKA callable services control from the ICSF Utilities panel.

CSFM123E MASTER KEY *mk* **ON** *coprocessor-name cii*, **SERIAL NUMBER** *nnnnnnn*, **IN ERROR.**

Explanation: The cryptographic coprocessor has an incorrect master key. Specifically, the master key verification pattern (MKVP) in the CKDS/PKDS does not match the MKVP of the master key. The substitution variables are:

- *mk* - master key. It identifies the master key that is in error. May have the value AES, DES, ECC, P11, or RSA.
- *coprocessor-name* - the type of cryptographic coprocessor. May have the value:
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - PCI X CRYPTO COPROCESSOR
- *c* - the short name for the coprocessor type. May have the value:
  - 2C (representing a CEX2C)
  - 3C (representing a CEX3C)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic coprocessor is installed.
- *nnnnnnn* - the serial number for the cryptographic coprocessor.

This message is issued once for the master key that is determined to be in error.

System action: When a master key is incorrect, the cryptographic coprocessor cannot be used for secure operations until the system administrator has changed the master key.

Operator response: None.

System programmer response: Have the system administrator enter the correct master key.

CSFM124I MASTER KEY *mk* **ON** *coprocessor-name cii*, **SERIAL NUMBER** *nnnnnnn*, **NOT INITIALIZED.**

Explanation: The cryptographic coprocessor does not have the master key. The substitution variables are:

- *mk* - master key. It identifies the master key that is in error. May have the value AES, DES, ECC, P11, or RSA.
- *coprocessor-name* - the type of cryptographic coprocessor. May have the value:
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - PCI X CRYPTO COPROCESSOR
- *c* - the short name for the coprocessor type. May have the value:
  - 2C (representing a CEX2C)
  - 3C (representing a CEX3C)
  - 4C (representing a CEX4C)

- 4P (representing a CEX4P)
- 5C (representing a CEX5C)
- 5P (representing a CEX5P)
- X (representing a PCIXCC)

- *ii* - the index or position where the cryptographic coprocessor is installed.
- *nnnnnnn* - the serial number for the cryptographic coprocessor.

This message is issued once for the master key that is determined not to be initialized.

System action: When a master key is not set, then the cryptographic coprocessor may not be used for operations with the master key until the system administrator has provided the master key. This may be a normal situation for your installation.

Operator response: None.

System programmer response: Have the system administrator enter the correct master key if appropriate.

CSFM126I CRYPTOGRAPHY - FULL CPU-BASED SERVICES ARE AVAILABLE.

Explanation: This is an informational message. ICSF is up and remains started. This message indicates that the DES CPACF feature code is enabled. This allows clear key services to run in the CPACF.

System action: Processing continues.

Operator response: None.

System programmer response: None.

CSFM127I CRYPTOGRAPHY - AES SERVICES ARE AVAILABLE.

Explanation: This is an informational message and will only be issued if the AES master key is active. ICSF is up and remains started.

System action: Processing continues.

Operator response: None.

System programmer response: None.

CSFM128E CRYPTOGRAPHIC KEY DATA SET, *dsname*, CANNOT BE USED ON THIS SYSTEM.

Explanation: The cryptographic key data set (CKDS) cannot be used on this system. The CKDS was initialized on a system without cryptographic coprocessors, but the current system has cryptographic coprocessors.

System action: ICSF terminates.

Operator response: Contact your system programmer.

System programmer response: Update the ICSF installation options data set with the correct CKDS and restart ICSF.

CSFM129I MASTER KEY *mk* ON *coprocessor-name cii*, SERIAL NUMBER *nnnnnnn*, IS CORRECT.

Explanation: The cryptographic coprocessor has a correct master key. The substitution variables are:

- *mk* - master key. It identifies the master key that is in error. May have the value AES, DES, ECC, P11 or RSA.
- *coprocessor-name* - the type of cryptographic coprocessor. May have the value:
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - PCI X CRYPTO COPROCESSOR
- *c* - the short name for the coprocessor type. May have the value:
  - 2C (representing a CEX2C)
  - 3C (representing a CEX3C)

- 4C (representing a CEX4C)
- 4P (representing a CEX4P)
- 5C (representing a CEX5C)
- 5P (representing a CEX5P)
- X (representing a PCIXCC)

- *ii* - the index or position where the cryptographic coprocessor is installed.
- *nnnnnnn* - the serial number for the cryptographic coprocessor.

System action: The system will use the cryptographic coprocessor for the cryptographic operations that it supports.

Operator response: None.

System programmer response: None.

CSFM130I CRYPTOGRAPHY - *mk* SERVICES ARE AVAILABLE.

Explanation: This is an informational message and will only be issued if the *mk* master key is active. The variable *mk* can be RSA or ECC. ICSF is up and remains started.

System action: Processing continues.

Operator response: None.

System programmer response: None.

CSFM131E CRYPTOGRAPHY - *mk* SERVICES ARE NOT AVAILABLE.

Explanation: The *mk* master key is no longer active. Callable services that require the master key to be active will fail. This may occur because

- the master keys in an active coprocessor were cleared by the ICSF administrator.
- one or more coprocessors were activated or deactivated on the ICSF Coprocessor Management panel.

The master key validation routine found the *mk* master key was not available on all of the active coprocessors.

The variable *mk* can be AES, DES, ECC, RSA or SECURE KEY PKCS11.

System action: Processing continues. The callable services that require the master key to be active will fail.

Operator response: Contact the system programmer.

System programmer response: Work with the ICSF administrator to determine the reason for the inactive master key. See the migration chapter in the *z/OS Cryptographic Services ICSF System Programmer's Guide*. The *mk* master key should be loaded on all coprocessors.

CSFM132I SECURE KEY PKCS11 SERVICES AVAILABLE.

Explanation: This is an informational message and will only be issued if the P11 master key is active. ICSF is up and remains started. Secure key PKCS #11 services are available.

System action: Processing continues.

Operator response: None.

System programmer response: None.

CSFM133I THERE ARE NO ACTIVE PKCS11 COPROCESSORS.

Explanation: One or more errors or user actions has resulted in the disabling of all PKCS #11 coprocessors.

System action: The system continues processing. The system will not be able to perform any secure key PKCS #11 operations until an Enterprise PKCS #11 coprocessor is activated.

Operator response: Investigate the problem. Contact the system administrator to enter the master keys for any online Enterprise PKCS #11 coprocessors or to bring a new coprocessor online (if one is available).

System programmer response: None.

CSFM134I CRYPTOGRAPHIC FEATURE IS INACTIVE. *coprocessor-name cii*, **SERIAL NUMBER** *nnnnnnn* **RSN=***reason*.

Explanation: A cryptographic feature has become inactive and cannot be used for processing callable service requests. When the type of coprocessor could not be determined, a *coprocessor-name* of UNKNOWN FEATURE is used. The substitution variables are:

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  - CRYPTO EXPRESS2 ACCELERATOR
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - PCI CRYPTO ACCELERATOR
  - PCI X CRYPTO COPROCESSOR
  - UNKNOWN FEATURE
- *c* - the short name for the cryptographic feature type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnnn* or *N/A* - the serial number for the cryptographic feature, or N/A when the feature is configured as an accelerator.
- *reason* – the reason the cryptographic feature is no longer active. Possible values are:

  Deactivated
  The feature has been deactivated by the ICSF administrator from the Coprocessor Management panel or by the operator on the system console.

  TKE disabled
  The feature has been removed from service by the ICSF administrator on a TKE workstation.

  Offline
  The feature was configured offline at the support element. The feature is not available to ICSF.

  Busy The cryptographic feature is busy performing maintenance functions. This state may occur when the cryptographic feature is first brought online and is going through power-on reset. The cryptographic feature may also be in this state when new licensed internal code is being loaded or when the unit is going through recovery processing.

  Being reconfigured
  An error has been detected and the ICSF configuration task has been invoked to check the feature. The feature may become active if the error is resolved or may stay inactive if the error is not resolved.

Initializing stage 1
A newly online feature has been detected by ICSF and ICSF is starting the initialization process.

Initializing stage 2
A newly online feature or active feature is being reset by ICSF as part of the initialization process or recovery process.

Initializing stage 3
A newly online feature or inactive feature is being readied to process requests.

No feature present
No feature was detected at this index.

System action: ICSF will not use the cryptographic feature for cryptographic operations.

Operator response: None.

System programmer response: Contact the ICSF administrator.

CSFM135E CRYPTOGRAPHIC FEATURE IS INACTIVE. *coprocessor-name cii*, **SERIAL NUMBER** *nnnnnnn* **RSN=***reason*.

Explanation: A cryptographic feature has become inactive and cannot be used for processing callable service requests. When the type of coprocessor could not be determined, a *coprocessor-name* of UNKNOWN FEATURE is used. The substitution variables are:

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  - CRYPTO EXPRESS2 ACCELERATOR
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - PCI CRYPTO ACCELERATOR
  - PCI X CRYPTO COPROCESSOR
  - UNKNOWN FEATURE
- *c* - the short name for the cryptographic feature type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnnn* or *N/A* - the serial number for the cryptographic feature, or N/A when the feature is configured as an accelerator.
- *reason* – the reason the cryptographic feature is no longer active. Possible values are:

  Master key incorrect
  At least one master key is incorrect. When all master keys are correct, the feature will become active.

Hardware error
The feature has failed. Have the feature removed or replaced by your IBM customer engineer.

User hung on latch
A feature is not responding and the configuration task is attempting to obtain the feature latch so the feature can be reset. One or more users hold the latch.

Bad feature response
An unexpected response was received from a feature. The feature is unusable.

Retry limit reached
While initializing a feature, the limit of attempts to gather status/information was reached. The feature is unusable. ICSF will try again to acquire status.

Unknown response
The feature has returned a return code reason code combination that ICSF doesn't recognize.

System action: ICSF will not use the cryptographic feature for cryptographic operations.

Operator response: Contact the ICSF administrator.

System programmer response: Contact the ICSF administrator.

CSFM136I *coprocessor-name cii*, **SN** *nnnnnnn* **STATUS CHANGED FROM** *oldreason* **TO** *newreason*.

Explanation: A cryptographic feature is inactive and its status has changed. When the type of coprocessor could not be determined, a *coprocessor-name* of UNKNOWN FEATURE is used. The substitution variables are:

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  - CRYPTO EXPRESS2 ACCELERATOR
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - PCI CRYPTO ACCELERATOR
  - PCI X CRYPTO COPROCESSOR
  - UNKNOWN FEATURE
- *c* - the short name for the cryptographic feature type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnnn* or *N/A* - the serial number for the cryptographic feature, or N/A when the feature is configured as an accelerator.
- *oldreason* – the previous reason why the feature is inactive.

- *newreason* – the new reason why the feature is inactive. Possible values are:

  Deactivated
  The feature has been deactivated by the ICSF administrator from the Coprocessor Management panel or by the operator on the system console.

  TKE disabled
  The feature has been removed from service by the ICSF administrator on a TKE workstation.

  Master key incorrect
  At least one master key is incorrect. When all master keys are correct, the feature will become active.

  Offline
  The feature was configured offline at the support element. The feature is not available to ICSF.

  Busy The cryptographic feature is busy performing maintenance functions. This state may occur when the cryptographic feature is first brought online and is going through power-on reset. The cryptographic feature may also be in this state when new licensed internal code is being loaded or when the unit is going through recovery processing.

  Being reconfigured
  An error has been detected and the ICSF configuration task has been invoked to check the feature. The feature may become active if the error is resolved or may stay inactive if the error is not resolved.

  Hardware error
  The feature has failed. Have the feature removed or replaced by your IBM customer engineer.

  Initializing stage 1
  A newly online feature has been detected by ICSF and ICSF is starting the initialization process.

  Initializing stage 2
  A newly online feature or active feature is being reset by ICSF as part of the initialization process or recovery process.

  Initializing stage 3
  A newly online feature or inactive feature is being readied to process requests.

  User hung on latch
  A feature is not responding and the configuration task is attempting to obtain the feature latch so the feature can be reset. One or more users hold the latch.

  Bad feature response
  An unexpected response was received from a feature. The feature is unusable.

  Retry limit reached
  While initializing a feature, the limit of attempts to gather status/information was reached. The feature is unusable. ICSF will try again to acquire status.

  No feature present
  No feature was detected at this index.

  Unknown response
  The feature has returned a return code reason code combination that ICSF doesn't recognize.

  Unknown feature type
  A feature has a type that is not recognized by ICSF. The feature is unusable.

System action: ICSF will not use the cryptographic feature for cryptographic operations.

Operator response: None.

System programmer response: Contact the ICSF administrator.

CSFM137E *coprocessor-name cii*, **SN** *nnnnnnn* **STATUS CHANGED FROM** *oldreason* **TO** *newreason*.

Explanation: A cryptographic feature is inactive and its status has changed. When the type of coprocessor could not be determined, a *coprocessor-name* of UNKNOWN FEATURE is used. The substitution variables are:

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  – CRYPTO EXPRESS2 ACCELERATOR

  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - PCI CRYPTO ACCELERATOR
  - PCI X CRYPTO COPROCESSOR
  - UNKNOWN FEATURE
- *c* - the short name for the cryptographic feature type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnn* or *N/A* - the serial number for the cryptographic feature, or N/A when the feature is configured as an accelerator.
- *oldreason* – the previous reason why the feature is inactive.
- *newreason* – the new reason why the feature is inactive. Possible values are:

  Deactivated
  The feature has been deactivated by the ICSF administrator from the Coprocessor Management panel or by the operator on the system console.

  TKE disabled
  The feature has been removed from service by the ICSF administrator on a TKE workstation.

  Master key incorrect
  At least one master key is incorrect. When all master keys are correct, the feature will become active.

  Offline
  The feature was configured offline at the support element. The feature is not available to ICSF.

  Busy The cryptographic feature is busy performing maintenance functions. This state may occur when the cryptographic feature is first brought online and is going through power-on reset. The cryptographic feature may also be in this state when new licensed internal code is being loaded or when the unit is going through recovery processing.

  Being reconfigured
  An error has been detected and the ICSF configuration task has been invoked to check the feature. The feature may become active if the error is resolved or may stay inactive if the error is not resolved.

  Hardware error
  The feature has failed. Have the feature removed or replaced by your IBM customer engineer.

  Initializing stage 1
  A newly online feature has been detected by ICSF and ICSF is starting the initialization process.

Initializing stage 2
A newly online feature or active feature is being reset by ICSF as part of the initialization process or recovery process.

Initializing stage 3
A newly online feature or inactive feature is being readied to process requests.

User hung on latch
A feature is not responding and the configuration task is attempting to obtain the feature latch so the feature can be reset. One or more users hold the latch.

Bad feature response
An unexpected response was received from a feature. The feature is unusable.

Retry limit reached
While initializing a feature, the limit of attempts to gather status/information was reached. The feature is unusable. ICSF will try again to acquire status.

No feature present
No feature was detected at this index.

Unknown response
The feature has returned a return code reason code combination that ICSF doesn't recognize.

Unknown feature type
A feature has a type that is not recognized by ICSF. The feature is unusable.

System action: ICSF will not use the cryptographic feature for cryptographic operations.

Operator response: Contact the ICSF administrator.

System programmer response: Contact the ICSF administrator.

CSFM138I CRYPTOGRAPHIC FEATURE CONFIGURED ONLINE. *coprocessor-name cii*, **SERIAL NUMBER** *nnnnnnn*.

Explanation: A cryptographic feature has been configured online. The substitution variables are:

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  - CRYPTO EXPRESS2 ACCELERATOR
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - PCI CRYPTO ACCELERATOR
  - PCI X CRYPTO COPROCESSOR
- *c* - the short name for the cryptographic feature type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)
  - 5C (representing a CEX5C)

- 5P (representing a CEX5P)
- X (representing a PCIXCC)

- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnn* or *N/A* - the serial number for the cryptographic feature, or N/A when the feature is configured as an accelerator.

System action: The system will not use the cryptographic feature for cryptographic operations.

Operator response: None.

System programmer response: None.

CSFM139I STALL DETECTED ON *coprocessor-name cii*, **SERIAL NUMBER** *nnnnnnn*, **AFTER** *mm* **MINUTES, FOR ASID =** *asid*.

Explanation: A stalled job has been detected on a cryptographic feature. The feature will be checked to see that it is functional. The job will be routed to another feature. The substitution variables are:

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  - CRYPTO EXPRESS2 ACCELERATOR
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - PCI CRYPTO ACCELERATOR
  - PCI X CRYPTO COPROCESSOR
- *c* - the short name for the cryptographic feature type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnn* or *N/A* - the serial number for the cryptographic feature, or N/A when the feature is configured as an accelerator.
- *mm* - the number of minutes since the request was sent to the feature.
- *asid* - the address space ID of the caller's task.

System action: The system will not use the cryptographic feature for cryptographic operations.

Operator response: None.

System programmer response: None.

CSFM200I INSTALLATION SERVICE *service-name* **NOT FOUND**

Explanation: This is an informational message only.

System action: Processing continues.

System programmer response: Determine if the name of the service that is indicated in *service-name* is valid. If it is wrong, correct it and restart ICSF.

CSFM201A REQUIRED INSTALLATION SERVICE *service-name* **NOT FOUND**

Explanation: You specified a service with option FAIL(ICSF) in the installation options data set, and ICSF could not find the service.

System action: ICSF ends.

System programmer response: Correct the name of the service and restart ICSF.

CSFM300I CKDS KEY '*key-name key-type***' AUTHENTICATION FAILED.**

Explanation: A message authentication code (MAC) verification for a CKDS key entry failed. If a system key (key with a label name of 64 bytes of X'00') fails authentication, the *key-name* field has the constant SYSTEM_KEY.

System action: Processing continues.

System programmer response: Investigate the key entry to determine why the MAC verification failed.

CSFM301A FAILURE UPDATING CKT AFTER CKDS UPDATE, RC = *return_code***, RS =** *reason_code***. MANUAL REFRESH OF CKDS REQUIRED, MEMBER** *member_name***.**

Explanation: The active CKDS in use by sysplex member *member_name* has been successfully updated by a member of the sysplex. An attempt by sysplex member *member_name* to update the corresponding key token in its in-storage copy of the CKDS has failed with return code of *return_code* and reason code of *reason_code*. The in-storage CKDS is now out of sync with the DASD version of the CKDS. If the message specifies RC = none, RS= none the sysplex member that initiated the CKDS I/O update left the sysplex unexpectedly and the status of the CKDS DASD I/O operation is unknown. CSFM303E will also be issued to identify the label of the record for which the in-storage CKDS update failed.

System action: ICSF processing will continue.

Operator response: The operator should attempt to refresh the CKDS on sysplex member *member_name* using the ICSF TSO panels.

System programmer response: None.

CSFM303E CKT UPDATE FAILED, LABEL *label***.**

Explanation: The active CKDS has been successfully updated by a member of the ICSF sysplex group. An attempt by the local system to update the key token with label *label* in its in-storage copy of the CKDS has failed. The in-storage CKDS is now out of sync with the DASD version of the CKDS. Refer to message CSFM301A for further information about this error.

System action: ICSF processing will continue.

Operator response: The operator should attempt to refresh the CKDS on sysplex member *member_name* using the ICSF TSO panels.

System programmer response: None.

CSFM304A FAILURE UPDATING TKT AFTER TKDS UPDATE, RC = *return_code***, RS =** *reason_code***. IN STORAGE TKDS NO LONGER CURRENT, MEMBER** *member_name***.**

Explanation: The active TKDS in use by sysplex member *member_name* has been successfully updated by a member of the sysplex. An attempt by sysplex member *member_name* to update the TKDS record in its in-storage copy of the TKDS has failed with return code of *return_code* and reason code of *reason_code*. The in-storage TKDS is now out of sync with the DASD version of the TKDS. If the message specifies RC = none RS= none, the sysplex member that

initiated the CKDS I/O update left the sysplex unexpectedly and the status of the TKDS DASD I/O operation is unknown. Message CSFM306E will also be issued to identify the handle of the record for which the in-storage TKDS update failed.

System action: ICSF processing will continue.

Operator response: In order to synchronize the in-storage copy of the TKDS on sysplex member *member_name*, ICSF must be stopped and restarted.

System programmer response: None.

CSFM306E TKT UPDATE FAILED, HANDLE *handle***.**

Explanation: The active TKDS has been successfully updated by a member of the ICSF sysplex group. An attempt by the local system to update the TKDS record with handle *handle* in its in-storage copy of the TKDS has failed. The in-storage TKDS is now out of sync with the DASD version of the TKDS. Refer to message CSFM304A for further information about this error.

System action: ICSF processing will continue.

Operator response: Refer to message CSFM304A.

System programmer response: None.

CSFM307E PKT UPDATE FAILED, LABEL *label***.**

Explanation: The active PKDS has been successfully updated by a member of the ICSF sysplex group. An attempt by the local system to update the key token with label *label* in its in-storage copy of the PKDS has failed. The in-storage PKDS is now out of sync with the DASD version of the PKDS. Refer to message CSFM314E for further information about this error.

System action: ICSF processing will continue.

Operator response: The operator should attempt to refresh the PKDS on sysplex member *member_name* using the ICSF TSO panels.

System programmer response: None.

CSFM308I MEMBER *member_name* **REPORTED** *action* **FROM SYSPLEX GROUP** *group_name***.**

Explanation: Sysplex group member *member_name* is no longer participating in sysplex group *group_name*. This is due to one of two possibilities:

- The ICSF started task on member *member_name* has stopped, or
- the system was reported or detected as gone from the sysplex.

System action: ICSF sysplex processing will continue with the remaining members of the sysplex group.

Operator response: The operator should verify that *member_name* leaving *group_name* was intentional.

System programmer response: None.

CSFM314E FAILURE UPDATING PKT AFTER PKDS UPDATE, RC = *return_code***, RS =** *reason_code***. IN STORAGE PKDS NO LONGER CURRENT, MEMBER** *member_name***.**

Explanation: The active PKDS in use by sysplex member *member_name* has been successfully updated by a member of the sysplex. An attempt by sysplex member *member_name* to update the PTKDS record in its in-storage copy of the PKDS has failed with return code of *return_code* and reason code of *reason_code*. The in-storage PKDS is now out of sync with the DASD version of the PKDS. If the message specifies RC = none RS= none, the sysplex member that initiated the PKDS I/O update left the sysplex unexpectedly and the status of the PKDS DASD I/O operation is unknown. Message CSFM602E will also be issued to identify the handle of the record for which the in-storage PKDS update failed.

System action: ICSF processing will continue.

Operator response: In order to synchronize the in-storage copy of the PKDS on sysplex member *member_name* ICSF must be stopped and restarted.

System programmer response: None.

CSFM400I CRYPTOGRAPHY - SERVICES ARE NOW AVAILABLE.

Explanation: This is an informational message. ICSF is up and the DES master key is active. DES application services are available.

System action: Processing continues.

Operator response: None.

System programmer response: None.

CSFM401I CRYPTOGRAPHY - SERVICES ARE NO LONGER AVAILABLE.

Explanation: Either ICSF is stopping, or access to a cryptographic processor is no longer possible. For example, the last processor is in a 'DISABLED' state.

System action: ICSF ends.

Operator response: Contact your system programmer.

System programmer response: Investigate the sequence of error messages prior to this message to help you resolve the problem.

CSFM402I DOMAIN INDEX IN THE OPTIONS DATASET WAS IGNORED.

Explanation: ICSF detected a changed domain parameter in the options data set and COMPAT(YES) was specified, but there was no intervening IPL. The specified index in the domain installation option was ignored. The index was set to the value that was stored in the cryptographic communications vector table (CCVT) when ICSF was last started.

System action: Processing continues.

Operator response: Contact your system programmer.

System programmer response: If the cryptographic domain index needs to be changed, re-IPL the system.

CSFM409E MULTIPLE DOMAINS AVAILABLE. SELECT ONE IN OPTIONS DATA SET.

Explanation: Multiple domains are available for this LPAR or native system. Select the domain using the DOMAIN parameter in the options data set.

If this error is generated even though the DOMAIN parameter is specified, it indicates that the DOMAIN parameter specifies an invalid value. Valid values are 0-15 (in decimal).

System action: ICSF ends.

Operator response: Contact your system programmer.

System programmer response: Add the DOMAIN parameter to the options data set (or verify that it is set to a valid value) and restart ICSF.

CSFM410E ERROR IN OPTIONS DATA SET.

Explanation: Some keywords or parameters are not valid in the options data set. Check the CFLIST data set for the specific error messages.

System action: ICSF ends.

Operator response: Contact your system programmer.

System programmer response: Correct the error in the options data set and restart ICSF.

CSFM450E UNEXPECTED ERROR PROCESSING *kds*, RETURN CODE = *rc*, REASON CODE = *rs*.

Explanation: An error occurred during processing of the kds (CKDS, PKDS, or TKDS) during initialization of ICSF. This may have occurred during allocation, open, read or write.

kds will be either CKDS, PKDS, or TKDS.

For an explanation of the *rc* and *rs* values, refer to the Return and Reason Codes in either the *z/OS Cryptographic Services ICSF Application Programmer's Guide* or *z/OS DFSMS Macro Instructions for Data Sets*. If the error occurred during data set allocation, the reason code is a combination of the dynamic allocation error code and an ICSF-assigned reason code for dynamic allocation error. Message CSFC0036 precedes this message and gives more useful information in this case.

System action: ICSF ends.

Operator response: Attempt to start ICSF again, and contact the system programmer.

System programmer response: Correct the problem as appropriate for any error messages that precede this one. Start ICSF again with an empty or error-free CKDS, PKDS, or TKDS.

CSFM451E CRYPTOGRAPHIC COPROCESSOR *pp*, FAILED.

Explanation: This message is no longer issued.

System action: None.

Operator response: None.

System programmer response: None.

CSFM505I CRYPTOGRAPHY - THERE ARE NO ACTIVE CRYPTOGRAPHIC COPROCESSORS.

Explanation: One or more errors or user actions has resulted in the disabling of all cryptographic coprocessors.

System action: The system will not be able to use a CCA cryptographic coprocessor for cryptographic operations until a coprocessor is activated.

Operator response: Investigate the problem. Contact the system administrator to enter the master keys for any online coprocessors or to bring a new cryptographic coprocessor online (if one is available).

System programmer response: None.

CSFM506I CRYPTOGRAPHY - THERE IS NO ACCESS TO ANY CRYPTOGRAPHIC COPROCESSORS OR ACCELERATORS.

Explanation: ICSF does not have access to any cryptographic coprocessors or accelerators. This message is issued when:

- Domain is not specified on the LPAR activation panel.
- Domain in the ICSF options data set does not match the usage domain on the Support Element LPAR activation panel.
- There are no coprocessors defined in LPAR candidates lists.

It is a normal message if only the CP assist instructions are being exploited. If cryptographic coprocessors are required, then update the Options Data Set or reconfigure the partition correctly and restart ICSF.

System action: The system continues processing and only a limited subset of ICSF services are available.

Operator response: Contact your system programmer; this may be an error.

System programmer response: The Options Data Set may need to be updated.

CSFM507I CRYPTOGRAPHY - THERE ARE NO CRYPTOGRAPHIC COPROCESSORS ONLINE.

Explanation: During ICSF initialization, there were no online cryptographic coprocessors detected. This may be the desired configuration.

System action: The system continues processing.

Operator response: None.

System programmer response: None.

CSFM508I CRYPTOGRAPHY - THERE ARE NO CRYPTOGRAPHIC ACCELERATORS ONLINE.

Explanation: During ICSF initialization, there were no online cryptographic accelerators detected. This may be the desired configuration.

System action: The system continues processing.

Operator response: None.

System programmer response: None.

CSFM530I I/O INTERRUPT SUPPORT HAS BEEN ENABLED FOR *coprocessor-name cii*, **SERIAL NUMBER** *nnnnnnn*.

Explanation: This message is no longer issued.

System action: None.

System programmer response: None.

CSFM531I MISSED I/O INTERRUPT HAS BEEN RECOVERED FOR *coprocessor-name cii*, **SERIAL NUMBER** *nnnnnnn*.

Explanation: ICSF has discovered and recovered from a missed I/O Interrupt from either a cryptographic accelerator or coprocessor. The substitution variables are:

- *coprocessor-name* - the type of cryptographic coprocessor.
- *c* - the short name for the coprocessor type. For example, 3C (representing a CEX3C).
- *ii* - the index or position where the cryptographic coprocessor is installed.
- *nnnnnnn* - the serial number for the cryptographic coprocessor.

System action: This instance of ICSF will continue to operate with cryptographic accelerator and coprocessor I/O interrupt capability.

System programmer response: None.

CSFM533I *kds-type* **RECORD** *number* **UNUSABLE AND SKIPPED,** *record-type record-name*.

Explanation: An unusable record was detected in a KDS dataset. This record will be skipped for further processing.
kds-type – Either CKDS or PKDS
number – The record number that was detected to be unusable
record-type – Label for CKDS and PKDS
record-name – Label name for CKDS and PKDS record

System action: ICSF processing will continue. This record will be skipped.

Operator response: The operator should contact the ICSF administrator to determine if the record can be restored.

System programmer response: None.

CSFM534I *kds-type* **RECORD** *number* **EXCESS LENGTH DETECTED AND ADJUSTED,** *record-type record-name*.

Explanation: A record in a KDS dataset was detected as having excess length. The record length will be internally adjusted by ICSF in order to continue processing.
kds-type – Either CKDS, PKDS, or TKDS
number – The record number that was detected as having excess length
record-type – Label for CKDS, PKDS, and TKDS
record-name – Label name for CKDS, PKDS and TKDS record

System action: ICSF processing will continue. The length of this record will be internally adjusted in order to continue processing. This length adjustment will not be written back out to the KDS dataset.

Operator response: The operator should contact the ICSF administrator to determine if the record can be restored or the excess length can be removed.

System programmer response: None.

CSFM535I ERRORS WERE DETECTED IN SOME *kds-type* RECORDS, CHECK THE *log-type* JOBLOG.

Explanation: Errors were detected in some of the KDS records.
kds-type – Either CKDS, PKDS, or TKDS
log-type – Log containing messages for record errors.

System action: For CKDS and PKDS records with detected errors, ICSF processing will continue. Records with excess length will be internally adjusted for further processing. Records that have been determined unusable will be skipped. For TKDS records, records with excess length will be internally adjusted for further processing. If an unusable record is detected it will NOT be skipped and ICSF processing will issue an 18F'x / 458'x abend and stop processing.

Operator response: The operator should contact the ICSF administrator to determine if the records with detected errors can be restored.

System programmer response: None.

CSFM536I *kds-type* RECORD *number* UNUSABLE, *record-type record-name*.

Explanation: An unusable record was detected in a KDS dataset.
kds-type – TKDS
number – The record number that was detected to be unusable
record-type – Label for TKDS
record-name – Label name for TKDS record

System action: ICSF processing will issue an 18F'x / 458'x abend and stop processing.

Operator response: The operator should contact the ICSF administrator to determine if the record can be restored.

System programmer response: None.

CSFM537I DEFERRED DELETION OF *kds-type* RECORDS RESUMED, CHECK THE *logtype* JOBLOG.

Explanation: While reading the TKDS, ICSF has found records for a previously deleted PKCS #11 token that have not yet been physically removed from the TKDS.
kds-type – The type of key data set.
logtype – Log containing messages for records found.

System action: ICSF resumes the deletion of the TKDS records and continues. No action is required.

Operator response: None.

System programmer response: None.

CSFM538I PREVIOUSLY DELETED *kds-type* RECORD *number* DISCARDED, *record-type record-name*.

Explanation: An object record belonging to a previously deleted PKCS #11 token was found in the TKDS data set. The record will be removed from the ICSF in-storage cache in order to continue processing.
kds-type – The type of key data set.
number – The number of the record that was detected
record-type – The type of TKDS record
record-name – Label name for the TKDS record

System action: ICSF processing will continue. No action is required.

Operator response: None.

System programmer response: None.

CSFM540I COPROCESSOR AT INDEX *nn* ENCOUNTERED CONDITION CODE = *cc* WITH STATUS WORD *statword* – COPROCESSOR BYPASSED.

Explanation: A failing response was encountered from a coprocessor during ICSF initialization. The coprocessor is bypassed and is unavailable for work.

System action: Processing continues.

Operator response: Operator should check support element. Contact the system programmer.

System programmer response: Have the ICSF administrator investigate the coprocessor response to determine cause of problem. Contact system hardware support for assistance. If problem is not resolved, contact the IBM Support Center.

CSFM600I CONNECTION ESTABLISHED TO ICSF SYSPLEX GROUP *group_name*, MEMBER *member_name*.

Explanation: Sysplex member *member_name* has successfully established a connection to the ICSF sysplex group *group_name*.

System action: This system will participate in sysplex-wide consistency for the specified ICSF resource (CKDS or TKDS).

System programmer response: None.

CSFM602E CONNECTION BROKEN TO ICSF SYSPLEX GROUP *group_name*, MEMBER *member_name*.

Explanation: The ICSF Cross-System Services task on sysplex member *member_name* has terminated abnormally.

System action: Sysplex member *member_name* is disconnected from the ICSF sysplex group *group_name*.

In releases of ICSF prior to HCR7770, ICSF processing will continue and this system will no longer participate in sysplex-wide consistency for the specified ICSF resource (CKDS or TKDS).

Starting in HCR7770, ICSF recovery processing attempts to restart the subtask, and sysplex member *member_name* will rejoin the sysplex as if ICSF has been restarted. If ICSF recovery processing cannot restart the subtask, ICSF terminates.

System programmer response: None.

CSFM603E FAILURE IN XCF SERVICE *xcf_service* FOR MEMBER *member_name*, GROUP *group_name*. RETURN CODE = *return_code*, REASON CODE = *reason_code*.

Explanation: A failure occurred in either the IXCJOIN processing when sysplex member *member_name* attempted to join the ICSF sysplex group *group_name*, or in the IXCLEAVE processing when sysplex member *member_name* attempted to leave the ICSF sysplex group *group_name*.

In the message text:

return_code
The hexadecimal return code from the IXCJOIN/IXCLEAVE macro.

reason_code
The hexadecimal reason code from the IXCJOIN/IXCLEAVE macro.

System action: For an IXCJOIN failure: the system action depends upon the specification of the SYSPLEXCKDS or SYSPLEXTKDS option in the ICSF Installation Options Data Set. If FAIL(NO) was specified, ICSF initialization will continue and this system will not be notified of updates to the ICSF Key Data Set (CKDS or TKDS) by other sysplex members. If FAIL(YES) was specified, ICSF will abend with abend code X'18F', reason code 84 (X'54').

For an IXCLEAVE failure: none.

System programmer response: Examine the return code and reason code from the IXCJOIN or IXCLEAVE operation to determine if an environmental condition relating to XCF can be corrected.

CSFM604E FAILURE INITIALIZING ICSF CROSS-SYSTEM SERVICES ENVIRONMENT, FUNCTION = *code*, **RETURN CODE =** *return_code*, **REASON CODE =** *reason_code*.

Explanation: A failure occurred while setting up the ICSF cross-system services environment. The *function code* identifies the process that failed. If *code* is 1, an error occurred in IXCJOIN processing when attempting to join the ICSF sysplex group. If *code* is 2, a failure occurred when attempting to create the latch set for either the CKDS or TKDS.

In the message text:

return_code
The hexadecimal return code from the IXCJOIN/ISGLCRT process.

reason_code
The hexadecimal reason code from the IXCJOIN/ISGLCRT process.

For a failure in IXCJOIN, message CSFM603E will also be issued.

System action: The system action depends upon the specification of the SYSPLEXCKDS or SYSPLEXTKDS option in the ICSF Installation Options Data Set. If FAIL(NO) was specified, ICSF initialization will continue and this system will not be notified of updates to the ICSF Key Data Set (CKDS or TKDS) by other sysplex members. If FAIL(YES) was specified, ICSF will abend with abend code X'18F', reason code 84 (X'54' or 85 (X'55').

Operator response: Contact the system programmer.

System programmer response: Examine the return code and reason code from the IXCJOIN or ISGLCRT operation to determine if an environmental condition relating to the failure can be corrected.

CSFM607I A *key-data-set* **KEY STORE POLICY IS NOT DEFINED.**

Explanation: None of the key policy controls that activate the key policy for the specified *key-data-set* are defined. Possible key-data-sets are CKDS or PKDS.

The key policy controls that activate the CKDS key policy are the CSF.CKDS.TOKEN.CHECK.LABEL.WARN, the CSF.CKDS.TOKEN.CHECK.LABEL.FAIL, or the CSF.CKDS.TOKEN.CHECK.NODUPLICATES resources in the XFACILIT class.

The key policy controls that activate the PKDS key policy are the CSF.PKDS.TOKEN.CHECK.LABEL.WARN, the CSF.PKDS.TOKEN.CHECK.LABEL.FAIL, or the CSF.PKDS.TOKEN.CHECK.NODUPLICATES resources in the XFACILIT class.

RACF commands may be used to define, change, list or delete the profiles that cover these resources in the XFACILIT class.

This message may be issued during ICSF initialization or when ICSF detects that the key policy is deactivated.

System action: Processing continues.

Operator response: None.

System programmer response: None.

CSFM608I A *key-data-set* **KEY STORE POLICY IS DEFINED.**

Explanation: One or more of the key policy controls that activate the key policy for the specified *key-data-set* is defined. Possible key-data-sets are CKDS or PKDS.

The key policy controls that activate the CKDS key policy are the CSF.CKDS.TOKEN.CHECK.LABEL.WARN, the CSF.CKDS.TOKEN.CHECK.LABEL.FAIL, or the CSF.CKDS.TOKEN.CHECK.NODUPLICATES resources in the XFACILIT class.

The key policy controls that activate the PKDS key policy are the CSF.PKDS.TOKEN.CHECK.LABEL.WARN, the CSF.PKDS.TOKEN.CHECK.LABEL.FAIL, or the CSF.PKDS.TOKEN.CHECK.NODUPLICATES resources in the XFACILIT class.

RACF commands may be used to define, change, list or delete the profiles that cover these resources in the XFACILIT class.

This message may be issued during ICSF initialization or when ICSF detects that the key policy is deactivated.

System action: Processing continues.

Operator response: None.

System programmer response: None.

CSFM610I GRANULAR KEYLABEL ACCESS CONTROL IS *state*.

Explanation: If *state* is DISABLED, neither of the profiles that activate the granular keylabel access controls are defined. If *state* is ENABLED, either or both of the profiles are defined.

The profiles that activate the granular keylabel access controls are the CSF.CSFKEYS.AUTHORITY.LEVELS.FAIL and CSF.CSFKEYS.AUTHORITY.LEVELS.WARN resources in the XFACILIT class.

RACF commands may be used to define, change, list or delete the profiles that cover these resources in the XFACILIT class.

This message may be issued during ICSF initialization or when ICSF detects that the key policy is deactivated.

System action: Processing continues.

Operator response: None.

System programmer response: None.

CSFM611I XCSFKEY EXPORT CONTROL FOR *algorithm* IS *state*.

Explanation: *algorithm* can be DES or AES. If *state* is DISABLED, the profile that activates the Symmetric Key Label Access control for that algorithm is not defined. If *state* is ENABLED, the profile is defined.

The profiles that activate the Symmetric Key Label Access control for CSNDSYX are the CSF.XCSFKEY.ENABLE.AES and CSF.XCSFKEY.ENABLE.DES resources in the XFACILIT class.

RACF commands may be used to define, change, list or delete the profiles that cover these resources in the XFACILIT class.

This message may be issued during ICSF initialization or when ICSF detects that the key policy is deactivated.

System action: Processing continues.

Operator response: None.

System programmer response: None.

CSFM612I PKA KEY EXTENSIONS CONTROL IS *state*.

Explanation: If *state* is DISABLED, the profile that enables the PKA Key Management Extensions control is not defined. If *state* is ENABLED, the profile is defined.

The existence of a profile for the CSF.PKAEXTNS.ENABLE resource in the XFACILIT class enables the PKA Key Management Extensions control. RACF commands can be used to define, change, list, or delete the profiles that cover this resource in the XFACILIT class.

This message may be issued during ICSF initialization or when ICSF detects that the policy is either activated or deactivated.

System action: Processing continues.

Operator response: None

System programmer response: None

CSFM613E ICSF SHUTDOWN DUE TO NESTED ABEND ON ICSF SUBTASK.

Explanation: ICSF has encountered recursive ABENDs in one or more subtasks and can no longer remain operational.

System action: ICSF ends.

Operator response: Inform your system programmer.

System programmer response: Collect any documentation that precedes this message, including messages and dumps, and contact the IBM Support Center.

CSFM614I ICSF SUBTASK *routine* **HAS TERMINATED. RECOVERY WILL BE ATTEMPTED.**

Explanation: And ICSF subtask routine terminated. ICSF will attempt to perform recovery.

System action: This instance of ICSF will attempt recovery on a terminated subtask.

System programmer response: None.

CSFM615I COORDINATED CHANGE-MK FAILED. NEW MASTER KEYS INCORRECT ON *sysname***. RC =** *return-code***, RSN =** *reason-code***.**

Explanation: The Coordinated Change Master Key operation failed due to incorrect new master key values on system *sysname*. The return code and reason code provide a more specific reason for the failure.

System action: ICSF processing will continue.

System programmer response: Contact the security administrator to ensure that the new master key values on system *sysname* match the new master key values on all other systems sharing the same active Key Data Set (KDS). Once all systems sharing the same active KDS contain the same new master key values, the coordinated change master key operation may be executed again.

For more information on the *return-code* and *reason-code*, refer to the *z/OS Cryptographic Services ICSF Application Programmer's Guide* or the information on the CSFEUTIL program in the *z/OS Cryptographic Services ICSF Administrator's Guide*.

Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure.

CSFM616I COORDINATED *operation* **FAILED, RC=***return-code* **RS=** *reason-code* **SUPRC=** *supplemental-return-code* **SUPRS=** *supplemental-reason-code* **FLAGS=** *flags***.**

Explanation: The coordinated KDS administration operation failed. The *operation* may be CHANGE-MK, CONVERT-DS or REFRESH. *return-code* and *reason-code* indicate the primary return code and reason code for the failure. *supplemental-return-code* and *supplemental-reason-code* indicate the supplemental return code and reason code for the failure. *flags* indicate additional internal diagnostic information about the failure.

System action: ICSF processing will continue.

System programmer response: Contact the security administrator for help determining the problem. Use the *return-code*and *reason-code* for problem determination. For more information on the *return-code* and *reason-code*, refer to the *z/OS Cryptographic Services ICSF Application Programmer's Guide* or the information on the CSFEUTIL program in the *z/OS Cryptographic Services ICSF Administrator's Guide*.

Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure.

If you are unable to determine the problem by looking up these values, contact the IBM Support Center. The *supplemental-return-code*, *supplemental-reason-code*, and *flags* show IBM internal diagnostic information. You may need to provide this information to the IBM Support Center.

CSFM617I COORDINATED *operation* **ACTION COMPLETED SUCCESSFULLY.**

Explanation: The coordinated KDS administration operation completed successfully. The *operation* may be CHANGE-MK, CONVERT-DS or REFRESH.

System action: ICSF processing will continue.

System programmer response: None.

CSFM618I *kds-type* **DATA SET** *data-set-name* **RENAMED TO** *new-data-set-name*

Explanation: The data set with *data-set-name* was renamed to the new data set name of *new-data-set-name*.

System action: ICSF processing will continue.

System programmer response: None.

CSFM619I DSN NOT CATALOGED, DIAG=*diagnostic-information* **DSN=***data-set-name*

Explanation: The data set with data set name of *data-set-name* is not cataloged.

System action: ICSF processing will continue.

System programmer response: Catalog the data set with *data-set-name*. Once the data set is cataloged, notify the security administrator to retry the function that failed. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure.

CSFM620I COORDINATED *operation* **MAINLINE PROCESSING FAILED BECAUSE** *reason-for-failure***.**

Explanation: A coordinated KDS administration operation failed because of the *reason-for-failure*. The operation may be CHANGE-MK, CONVERT-DS or REFRESH.

System action: ICSF processing will continue.

System programmer response: Notify the security administrator for help in determining the reason for the failure. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure. If unable to resolve the problem, contact the IBM Support Center.

CSFM621I COORDINATED *operation* **BACK OUT PROCESSING FAILED BECAUSE** *reason-for-failure***.**

Explanation: Back out processing for a coordinated operation failed because of *reason-for-failure*. The operation may be CHANGE-MK, CONVERT-DS or REFRESH.

System action: Depending on the *reason-for-failure*, ICSF processing may continue or may shutdown across all instances of ICSF sharing the same active KDS.

System programmer response: Notify the security administrator for help in determining the reason for the failure. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure. If unable to resolve the problem, contact the IBM Support Center.

CSFM622I COORDINATED *operation* **PROGRESS:** *operation-progress***.**

Explanation: This message indicates the progress of the coordinated operation. The operation may be CHANGE-MK, CONVERT-DS or REFRESH.

System action: ICSF processing will continue.

System programmer response: None.

CSFM623I CATALOG SEARCH FAILED. MODID=*module-id* **RC=***return-code* **RSN=***reason-code***.**

Explanation: If this message is issued during ICSF startup, a problem occurred while retrieving catalog information about the active KDS. If this message is issued during a coordinated change master key or a coordinated refresh operation, a problem occurred while retrieving catalog information about the new KDS. The problem occurred in the module identified by *module-id*. The *return-code* and *reason-code* indicate what type of problem occurred.

System action: If this message is issued during ICSF startup, the KDS sysplex group will convert to the sysplex communication protocol used prior to HCR7790, and coordinated KDS administrative functions will be unavailable. If this message is issued during a coordinated change master key or a coordinated refresh operation, the operation will fail. In either case, ICSF processing will continue.

System programmer response: If this message is issued during ICSF startup, ensure that the active KDS is correctly cataloged on the system. If this message is issued during a coordinated change master key or a coordinated refresh operation, notify the security administrator and make sure the new target data set is correctly cataloged on the system.

Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure.

CSFM625I SET *key-type* **MASTER KEY FAILED FOR COPROCESSOR SERIAL NUMBER** *serial-number***.**

Explanation: A failure occurred when attempting to set a new *key-type* master key for the coprocessor with serial number *serial-number*. *key-type* may be DES or AES. *serial-number* is the serial number of the coprocessor that experienced the failure.

System action: ICSF processing will continue.

System programmer response: Notify the security administrator to ensure that the new master key register for *key-type* is correctly loaded. If sharing the KDS across a sysplex and performing a coordinated change master key operation, the security administrator should ensure all instances of ICSF sharing the same active KDS have the same new master key value loaded into the new master key register for *key-type*. After correcting the new master key register or registers, the security administrator should retry the operation.

Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure.

CSFM626I COORDINATED *operation* **COMPLETE, RC=***return-code* **RSN=***reason-code***. CANCEL RSN=***cancel-reason-code***.**

Explanation: The coordinated operation has completed. The *operation* may be CHANGE-MK, CONVERT-DS or REFRESH. If a failure occurred during the operation, the *return-code*, *reason-code*, and *cancel-reason-code* may be used to determine the cause of the failure.

System action: ICSF processing will continue.

System programmer response: In the case of a failure, an explanation of the *return-code*, *reason-code*, and *cancel-reason-code* values can be found in the 'Return and Reason Codes' section of the *z/OS Cryptographic Services ICSF Application Programmer's Guide*. Alternatively, refer to the return and reason code information for the CSFEUTIL program described in the *z/OS Cryptographic Services ICSF Administrator's Guide*.

CSFM628I SYSTEM *system-name* **HAS MISSED A** *kds-type* **UPDATE. DIAG=***diagnostic-information***.**

Explanation: The system with *system-name* has missed a sysplex KDS update. *kds-type* indicates which type of KDS update was missed. *diagnostic-information* contains additional diagnostic information about the failure.

diagnostic-information may be the following:

- PREP - This indicates that an internal ICSF sysplex message was missed. This message is used during internal KDS I/O processing in a sysplex environment.
- '10'X - This indicates that a sysplex KDS record create was missed. This message is used to notify sysplex members of a KDS record create.
- '11'X - This indicates that a sysplex KDS record update was missed. This message is used to notify sysplex members of a KDS record update.
- '13'X - This indicates that a sysplex KDS record delete was missed. This message is used to notify sysplex members of a KDS record delete.

System action: ICSF processing continues, however the system indicated in this message by *system-name* has missed a KDS update. This system's in-storage KDS will now be out of sync with other members in the sysplex group sharing the same active KDS. The next time a KDS update is processed against this systems active KDS, ICSF will recognize that its in-storage KDS is out of sync and will perform an internal KDS refresh to get back in sync.

Operator response: None.

System programmer response: Notify the security administrator to perform a single-system KDS refresh on the system where the KDS is out of sync.

CSFM629I *IDCAMS-processor-message***.**

Explanation: This message is used to route IDCAMS processor messages to the job log. This message is used during the rename step of a coordinated change master key or coordinated refresh operation.

System action: ICSF processing continues.

System programmer response: If this message indicates a failure, notify the security administrator for help in determining the reason for the failure. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure. If unable to resolve the problem, contact the IBM Support Center.

CSFM630I *kds-type* **RENAME FAILED:** *original-name* **TO** *new-name*

Explanation: The rename step of the a coordinated change master key or coordinated refresh operation failed. *kds-type* indicates which KDS this rename was being performed for. *original-name* indicates the original name of the KDS. *new-name* indicates the new name of the KDS.

System action: ICSF processing continues.

System programmer response: Notify the security administrator for help in determining the reason for the failure. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure. If unable to resolve the problem, contact the IBM Support Center.

CSFM632I CRITICAL ICSF SUBTASK *name* **CAN NOT BE RESTARTED. ICSF WILL BE TERMINATED.**

Explanation: The ICSF subtask specified by *name* experienced a problem that ICSF tried to recover. ICSF recovery was unable to restart this subtask. This subtask is critical to ICSF processing. ICSF will terminate without this subtask.

System action: ICSF terminates.

System programmer response: Restart ICSF. If this problem reoccurs, contact the IBM Support Center.

CSFM633I ICSF SUBTASK *subtask* **CAN NOT BE RESTARTED. ICSF CAPABILITIES REDUCED.**

Explanation: The ICSF subtask specified by *name* experienced a problem that ICSF tried to recover. ICSF recovery was unable to restart this subtask. This subtask is not critical to ICSF processing. ICSF processing will continue with limited capabilities.

System action: ICSF continues processing with limited capabilities.

System programmer response: Restart ICSF. If this problem reoccurs, contact the IBM Support Center.

CSFM634I *log-type* **UPDATE TIMED OUT WAITING FOR ENQ** *resource***.**

Explanation: The I/O subtask for the *kds-type* timed out waiting for an exclusive ENQ on the *resource* specified. At least one member of the ICSF *kds-type* sysplex group has not relinquished its ENQ on the *resource*.

System action: ICSF processing will continue. The internal *kds-type* cache will be refreshed.

Operator response: The operator should issue D GRS,RES=*resource* from the message to determine which system or systems hold the *resource*. The operator should determine if action should be taken to cause the holding system to release its ENQ on the *kds-type resource*.

System programmer response: None.

CSFM635I *kds-type* **CACHE ERROR DETECTED. AUTOMATIC REFRESH IN PROGRESS.**

Explanation: An error was detected in the in-storage cache of the *kds-type* dataset. The error will be corrected internally by automatically refreshing the internal *kds-type* cache.

System action: ICSF processing will continue. The internal *kds-type* cache will be refreshed.

Operator response: None.

System programmer response: None.

CSFM636I SYSTEM *system-name* **FAILURE FOR COORDINATED** *kds-type* **ACTIVITY. MSGTYPE=***message-type* **RC=***return-code* **RSN=***reason-code***.**

Explanation: The system identified by *system-name* experienced a failure performing coordinated KDS activity. A *reason-code* of C3A indicates that the system *system-name* is not being responsive to the originator of the coordinated KDS function.

- *system-name* - Name of the system which either detected a problem or failed to respond.
- *kds-type* - KDS type for the coordinated activity.
- *message-type* - Internal diagnostic information.
- *return-code* - Return code either returned by the remote system or set by the originating system in case of timeout.
- *reason-code* - Reason code either returned by the remote system or set by the originating system in case of timeout.

System action: ICSF processing continues.

System programmer response: Notify the security administrator for help in determining the reason for the failure. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure.

CSFM637I FAILURE UPDATING *kds-type* **CACHE, RC =** *return-code***, RS =** *reason-code***. AUTOMATIC REFRESH OF** *kds-type* **DRIVEN BY SYSTEM** *system-name***.**

Explanation: A failure occurred while updating the in-storage cache of the *kds-type* dataset. The *kds-type* update operation will be failed with *return-code*/*reason-code*. System *system-name* will internally correct the problem by automatically refreshing the internal *kds-type* cache.

System action: ICSF processing will continue. The internal kds-type cache will be refreshed.

Operator response: None.

System programmer response: None.

CSFM638I *kds-type* **IS UNUSABLE DUE TO MISSING RECORDS. DSN=***dataset-name***.**

Explanation: *kds-type* IS UNUSABLE DUE TO MISSING RECORDS, DSN=*dataset-name*.
kds-type - CKDS, PKDS or TKDS
dataset-name – The name of the dataset that is missing records.

System action: ICSF will shut down.

Operator response: Contact the ICSF administrator to restore the missing records.

System programmer response: None.

CSFM639I ICSF COMMUNICATION LEVEL FOR *kds-type* **CHANGED FROM** *previous-level* **TO** *new-level***.**

Explanation: The ICSF sysplex communication level for the *kds-type* changed from the *previous-level* to the *new-level*. *previous-level* may be 0, 2, or 3. *new-level* may be 0, 2, or 3. The coordinated change master key and coordinated refresh utilities are only available when all ICSF instances in the sysplex are at ICSF sysplex communication level 2 or higher for the *kds-type*. The coordinated convert utility (convert KDS to KDSR format) is only available when all ICSF instances in the sysplex are at ICSF sysplex communication level 3 or higher for the *kds-type*.

kds-type – CKDS, PKDS or TKDS
previous-level – 0, 2, or 3
new-level – 0, 2, or 3

ICSF release level	CKDS communication level	PKDS communication level	TKDS communication level
HCR7780 and earlier releases	0	0	0
HCR7790	2	0	0
HCR77A0	2	2	2

ICSF release level	CKDS communication level	PKDS communication level	TKDS communication level
HCR77A1 and later releases	3	3	3

System action: ICSF processing will continue. ICSF will process KDS updates using the communication level indicated by this message.

Operator response: None.

System programmer response: None.

CSFM640I ICSF RELEASE FMID=*fmid*.

Explanation: This message indicates the ICSF release FMID that is currently started.

System action: Processing continues.

Operator response: None

System programmer response: None.

CSFM641I INCORRECT MKVP DETECTED IN *kds-type* RECORD *name*.

Explanation: This message is no longer issued.

System action: None.

System programmer response: None.

CSFM642I UNEXPECTED *kds-type* REENCIPHER TERMINATED IN MID-REENCIPHER. RETURN CODE = *return-code*, REASON CODE = *reason-code*.

Explanation: An unexpected failure occurred while reenciphering the KDS specified by kds-type.

System action: The reencipher will fail.

Operator response: Contact the ICSF administrator to analyze the return and reason codes returned for the reencipher failure.

System programmer response: None.

CSFM643I CRITICAL ICSF SUBTASK FAILURE. ICSF WILL BE TERMINATED.

Explanation: An ICSF subtask has suffered a failure that has caused ICSF to terminate.

System action: ICSF will Terminate.

Operator response: Contact the ICSF administrator to analyze the ICSF job log and determine what has caused this failure. If the ICSF joblog does not indicate the problem, contact the IBM support center.

System programmer response: None.

CSFM644E DOMAIN INDEX IN THE OPTIONS DATASET IS NOT SPECIFIED IN THE ACTIVATION PROFILE.

Explanation: The value of the DOMAIN parameter in the installation options specifies a cryptographic usage domain that this LPAR cannot access because it is not in the LPAR Activation Profile.

System action: ICSF ends.

Operator response: Contact your system programmer.

System programmer response: Ensure that the specified Usage Domain has been assigned to your LPAR. If this does not resolve the problem, contact the IBM Support Center.

CSFM645I INCORRECT METADATA DETECTED IN *kds-type* **RECORD** *label***.**

Explanation: A *kds-type* KDS record in storage was detected as having damage in the KDSR metadata area.

kds-type is one of CKDS, PKDS, or TKDS.

label is the label name (for CKDS or PKDS) or handle (for TKDS).

System action: ICSF will ABEND the unit of work.

Operator response: None.

System programmer response: Notify the ICSF administrator.

CSFM649I SPECIAL SECURE MODE IS *setting*

Explanation: This message is written to the system console and ICSF joblog each time the Special Secure Mode (SSM) setting changes. The initial SSM setting is based on the SSM option in the installation options dataset.

setting is either ENABLED or DISABLED

System action: When the setting is DISABLED, operations requiring SSM to be enabled will fail. When the setting is ENABLED, ICSF will attempt to process requests requiring that SSM be enabled.

Operator response: None.

System programmer response: Examine the content of the message and if unexpected, see the *z/OS Cryptographic Services ICSF System Programmer's Guide* for information on how to change the SSM setting.

CSFM650I CSFSERV AUTHORIZATION CHECK FOR *service* **IS** *setting*

Explanation: This message is written to the system console and ICSF joblog each time the setting changes. By default, the setting is ENABLED. It tells the installation whether or not CSFSERV SAF authorization checks may be performed for the set of services indicated.

service is either ONE-WAY HASH SERVICES or RANDOM NUMBER GENERATE SERVICES
setting is either ENABLED or DISABLED

The ONE-WAY HASH SERVICES include CSNBOWH, CSNEOWH, CSNBOWH1, CSNEOWH1, CSFPOWH, and CSFPOWH6. The RANDOM NUMBER GENERATE SERVICES include CSNBRNG, CSNERNG, CSNBRNGL, CSNERNGL, CSFPPRF, and CSFPPRF6.

System action: When the setting is DISABLED, no CSFSERV SAF checks will be performed for the services indicated. When the setting is ENABLED, normal CSFSERV SAF authorization checking will be attempted for the services indicated.

Operator response: None.

System programmer response: Examine the content of the message and if unexpected, see the *z/OS Cryptographic Services ICSF System Programmer's Guide* for information on how to change whether or not the CSFSERV SAF check will be performed for the indicated services.

CSFM651I THE FOLLOWING SYSTEMS ARE PREVENTING A COORDINATED *operation***:** *list-of-systems*

Explanation: The coordinated change master key and coordinated refresh operations may only be performed when all systems in the KDS sysplex group are at the ICSF HCR7790 release level or higher. The coordinated conversion operation may only be performed when all systems in the KDS sysplex group are at the ICSF HCR77A1 release level or higher. If an instance of ICSF joins the KDS sysplex group at a level lower than the ICSF HCR7790 release level, then, regardless of active KDS, the coordinated change master key and coordinated refresh operations will be unavailable.

operation may be CHANGE-MK, CONVERT-DS or REFRESH, and indicates whether a coordinated change master key, coordinated conversion, or coordinated refresh operation was requested.

list-of-systems indicates the systems containing an instance of ICSF at lower than the HCR7790 release level.

System action: ICSF processing continues.

System programmer response: In order to perform a coordinated change master key or coordinated refresh operation, systems running a release of ICSF lower than HCR7790 must be removed from the KDS sysplex group or upgraded to the HCR7790 release or higher. In order to perform a coordinated conversion, systems running a release of ICSF lower than HCR77A1 must be removed from the KDS sysplex group or upgraded to the HCR77A1 release or higher. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure.

CSFM652I *kds-type* **IS UNUSABLE.**
DSN = *dataset-name*, **REASON =** *reason-code*

Explanation: This message is no longer issued.

System action: None.

Operator response: None.

System programmer response: None.

CSFM653I *kds* **LOADED** *num_record* **RECORDS WITH AVERAGE SIZE** *average_size*

Explanation: This informational message is provided to assist in optimizing VSAM record sizes. A key data set was loaded into memory by ICSF. The data set has *num_record* records in it and the average size of the records is *average_size*. The *kds* may be CKDS, PKDS or TKDS.

System action: Processing continues.

Operator response: None.

System programmer response: None.

CSFM654I KEY ARCHIVING USE CONTROL IS *state*.

Explanation: The key store policy key archiving use control is currently in the specific *state*. The *state* may be ENABLED or DISABLED.

The profile that activates the key archive use control is the CSF.KDS.KEY.ARCHIVE.USE resource in the XFACILIT class.

RACF commands may be used to define, change, list, or delete the profiles that cover these resources in the XFACILIT class.

This message may be issued during ICSF initialization and when ICSF detects that the key store policy is changed.

System action: Processing continues.

Operator response: None.

System programmer response: None.

CSFM655I AN ARCHIVED RECORD *label* **IN THE ACTIVE** *key-data-set* **WAS REFERENCED.**

Explanation: An attempt to use an archived record *label* occurred. The *key-data-set* can be CKDS, PKDS, or TKDS. The results of the request for the archived record will depend on the key archive use policy. An SMF type 82 audit record was produced.

This message is only issued for the first attempt to use a record. Subsequent attempts will produce an audit record only.

System action: Processing continues.

Operator response: None.

System programmer response: Notify the ICSF administrator.

CSFM657I FAILURE ON CSVDYNEX FOR EXIT *exitname* **RETURN CODE =** *return-code*, **REASON CODE =** *reason-code*.

Explanation: An invocation of CSVDYNEX for the exit *exitname* failed with *return-code* and *reason-code*. See *MVS Programming Authorized Assembler Services Reference Vol 1 (ALESERV-DYNALLOC)* for the explanation of possible CSVDYNEX return codes and reason codes.

This message is issued if an invocation of CSVDYNEX fails for a exit.

System action: Processing continues. The exit is disabled.

Operator response: Contact your system programmer.

System programmer response: Contact the IBM Support Center.

CSFM659I FIPS 140 KNOWN ANSWER TEST FAILED. FEATURE CODE 3863 IS NOT INSTALLED.

Explanation: The FIPS 140 tests failed because the CPACF feature (code 3863) is not installed or enabled. ICSF requires feature code 3863 be installed and enabled.

System action: ICSF terminates.

Operator response: None.

System programmer response: Enable the CPACF feature.

CSFM660I *key-data-set* **RECORD** *label* **FAILED: RC =** *nnnnnnnn*, **RS =** *nnnnnnnn*

Explanation: An attempt to validate or reencipher a *key-data-set* record was unsuccessful. The *key-data-set* can be CKDS or PKDS.

This message is issued for each failing label.

For CKDS, the *label* is the CKDS label and type concatenated with a slash between them. For PKDS, the *label* is just the PKDS label.

System action: Processing continues.

Operator response: None.

System programmer response: Notify the ICSF administrator.

CSFM661I *key-data-set* **RECORD** *label*: *validation-message*

Explanation: An attempt to validate or reencipher a *key-data-set* record detected a problem. The *key-data-set* can be CKDS or PKDS.

For CKDS, the *label* is the CKDS label and type concatenated with a slash between them. For PKDS, the *label* is just the PKDS label.

This message is issued for each record where a problem was detected. If *validation-message* begins with 'ERROR', the problem detected will cause a reencipher of the CKDS or PKDS to fail.

System action: Processing continues.

Operator response: None.

System programmer response: Notify the ICSF administrator.

CSFM662I *kds-type* **RECORD** *number* **METADATA DAMAGE DETECTED,** *record-type record-name*

Explanation: A record in a KDS dataset was detected as having damage in the KDSR metadata area. The KDSR metadata area will be reset to initial state.

kds-type is one of CKDS, PKDS, or TKDS.

number is the record number that was detected as having damage in the KDSR metadata area.

record-type is LABEL (for CKDS or PKDS) or HANDLE (for TKDS).

record-name is the label name (for CKDS or PKDS) or handle (for TKDS).

System action: ICSF processing continues. The KDSR metadata area and length of this record will be internally adjusted in order to continue processing. These adjustments will not be written back out to the KDS dataset immediately, but instead on the next update to the record or on the next Coordinate Change Master Key operation.

Operator response: None.

System programmer response: None.

CSFM663I *kds-type* **CLUSTER ID ERROR:** *kdsold, kdsnew***.**

Explanation: This system attempted to use KDS *kdsnew* which has a KDS cluster identifier that matches KDS *kdsold*. The KDS cluster identifier is based on the location of the KDS within the volume. This means that *kdsold* was moved without a restart of all ICSF instances sharing *kdsold* and so ICSF continues to use the original cluster identifier for *kdsold*. *kdsnew* now resides in the exact location on the volume previously occupied by *kdsold*, causing the cluster identifiers to not be unique. A KDS cluster is made up of all the systems sharing a KDS in the sysplex. The KDS cluster identifier determines the ICSF instances which make up a KDS cluster and must be unique for each KDS.

kds-type is one of CKDS, PKDS, or TKDS.

kdsold is the active KDS for one or more ICSF instances.

kdsnew is the KDS that an ICSF instance is attempting to use.

System action: The current operation ends. If this error is detected at ICSF startup, ICSF terminates.

Operator response: Contact the system programmer.

System programmer response: You may either:

1. Move *kdsnew* to a different volume and retry the operation
2. Move *kdsnew* to a different location on the volume and retry the operation. One way to ensure *kdsnew* ends up at a different location is:
   a. Allocate a temporary KDS, *kdstmp*, on the volume.
   b. If *kdsnew* is not empty, copy the contents of *kdsnew* to *kdstmp*.
   c. Delete *kdsnew*.
   d. Rename *kdstmp* to *kdsnew*.
3. Shutdown all ICSF instances that are sharing *kdsold*. Once all instances are down, restart those instances and retry the operation.

CSFM664I ICSF ENCOUNTERED CONTINUOUS ISGQUERY FAILURES: *kds-type dsname* **RC=***rc* **RS=***rs*

Explanation: During a user-initiated KDS operation (for example, KDS Refresh, Change Master Key), ICSF was unable to complete the operation due to continuous failures from the ISGQUERY service. This error is often associated with an inability to communicate with other systems in the sysplex.

kds-type is one of CKDS, PKDS, or TKDS.

dsname is the name of the KDS that was being processed as part of the operation.

rc is the return code from the ISGQUERY service in hexadecimal.

rs is the reason code from the ISGQUERY service in hexadecimal.

System action: The current operation ends.

Operator response: Look for signs of communication problems among systems in the sysplex and resolve them. Some indications of a communication problem include issuance of one or more of the following messages: IXC402D, ISG378I (z/OS V1R13 and above). If there are no signs of a communication problem, contact the IBM Support Center. Once the issue is resolved, the operation can be retried.

System programmer response: None.

CSFM665E ICSF WAITING FOR RESOLUTION TO ISGQUERY FAILURES: *kds-type dsname* **RC=***rc* **RS=***rs*

Explanation: ICSF cannot continue because of continuous failures from the ISGQUERY service. This error is often associated with an inability to communicate with other systems in the sysplex. Until the issue is resolved, some of ICSF's functionality will be affected.

kds-type is one of CKDS, PKDS, or TKDS.

dsname is the name of the active KDS.

rc is the return code from the ISGQUERY service in hexadecimal.

rs is the reason code from the ISGQUERY service in hexadecimal.

System action: ICSF waits for the issue to be resolved. Once the issue is resolved, ICSF processing continues.

Operator response: Look for signs of communication problems among systems in the sysplex and resolve them. Some indications of a communication problem include issuance of one or more of the following messages: IXC402D, ISG378I (z/OS V1R13 and above). If there are no signs of a communication problem, contact the IBM Support Center.

System programmer response: None.

CSFM673E COORDINATED CHANGE MASTER KEY IS WAITING FOR FINAL VERIFICATION OF THE CONFIGURATION

Explanation: After the master key has been changed on each cryptographic coprocessor, the master key verification patterns (MVKPs) from each coprocessor are read and compared to the MKVPs in the KDS header. ICSF must be able to complete these requests for each coprocessor in order to mark them as either available or unavailable.

If there is an exceptionally heavy workload or there is a hung user request, this message persists.

When the processing completes, this message is deleted.

System action: ICSF continues to wait for all coprocessor requests to complete.

Operator response: None.

System programmer response: If the message is not deleted in a reasonable amount of time, you may need to obtain a console dump of ICSF for diagnosis and then stop and restart ICSF.

Chapter 9. CSFOnnnn messages (Installation options parameter processing)

Problems encountered during the processing of installation option parameters are written to the ICSF job log.

CSFO0016 ERROR OCCURRED OPENING OPTIONS FILE.

Explanation: ICSF could not open the options parameter file that is specified on the CSFPARM DD statement in the JCL.

System action: Processing ends.

User response: Ensure that the options parameter file that is defined by the DD statement is valid. Correct the DD statement and restart ICSF.

CSFO0026 ERROR OCCURRED CLOSING OPTIONS FILE.

Explanation: ICSF could not close the options parameter file.

System action: Processing ends.

System programmer response: Check other messages. If you cannot correct the error, contact the IBM Support Center.

User response: Contact your system programmer.

CSFO0036 SYNTAX ERROR IN OPTION STATEMENT.

Explanation: The statement that immediately precedes this message has at least one syntax error.

System action: Processing ends.

User response: Check the syntax of the option statement. Check for unpaired delimiters and missing or extraneous commas and ensure that the statement does not exceed position 71. Correct the error and restart ICSF.

CSFO0046 PARTITIONED DATA SET NOT ALLOWED FOR THE CKDS, PKDS, OR TKDS.

Explanation: The CKDSN, PKDSN or TKDSN keyword on an option statement specified a member name for a data set. The CKDS, PKDS, or TKDS must be a VSAM data set.

System action: Processing ends.

User response: Correct the data set name and restart ICSF.

CSFO0056 CKDS DSNAME MISSING.

Explanation: The options parameter file did not include a statement that contains the CKDSN keyword and value.

System action: Processing ends.

User response: Ensure that the options parameter file contains a statement with the CKDSN keyword and its value, and restart ICSF.

CSFO0066 *Keyword* **VALUE NOT IN RANGE.**

Explanation: The specified value for the keyword is not within the allowable range. *z/OS Cryptographic Services ICSF System Programmer's Guide* describes the allowable range for the keyword. The statement that contains the error precedes this message.

System action: Processing ends.

User response: Specify an allowable range for the keyword and restart ICSF.

CSFO0076 *Keyword* **KEYWORD SPECIFIED WITH MISSING VALUE.**

Explanation: A keyword value is missing for the *keyword* variable. The statement that contains the error precedes this message.

System action: Processing ends.

User response: Specify a value for the keyword and restart ICSF.

CSFO0096 SERVICE NUMBER VALUE NOT IN RANGE.

Explanation: The specified service number for the SERVICE and UDX keywords must be from 1 to 32767. The statement containing the error precedes this message.

System action: Processing ends.

User response: Specify a service number value between 1 and 32767 and restart ICSF.

CSFO0106 *Keyword* **KEYWORD AND VALUE MISSING.**

Explanation: The *keyword* keyword and its value are missing from the option statement. The statement that contains the error precedes this message.

System action: Processing ends.

User response: Specify the keyword and its value and restart ICSF.

CSFO0126 ERROR OCCURRED OPENING WAITLIST FILE.

Explanation: ICSF could not open the Wait List file specified by the WAITLIST parameter in the ICSF Installation Options data set.

System action: Processing continues. The ICSF default CICS Wait List file will be used.

System programmer response: Ensure that the Wait List file specified in the Installation Options data set is valid.

User response: Contact your system programmer.

CSFO0136 ERROR OCCURRED CLOSING WAITLIST FILE.

Explanation: ICSF could not close the Wait List file specified by the WAITLIST parameter in the ICSF Installation Options data set.

System action: Processing continues.

System programmer response: Check for other messages. If you cannot correct the error, contact the IBM Support Center.

User response: Contact your system programmer.

CSFO0146 ERROR OCCURRED ALLOCATING WAITLIST FILE.

Explanation: ICSF could not allocate the Wait List file specified by the WAITLIST parameter in the ICSF Installation Options data set.

System action: Processing continues. The ICSF default CICS Wait List will be used.

System programmer response: Ensure that the Wait List file specified in the Installation Options data set is valid.

User response: Contact your system programmer.

CSFO0156 ERROR OCCURRED FREEING WAITLIST FILE.

Explanation: ICSF could not deallocate the Wait List file specified by the WAITLIST parameter in the ICSF Installation Options data set.

System action: Processing continues.

System programmer response: Check other messages. If you cannot correct the error, contact the IBM Support Center.

User response: Contact your system programmer.

CSFO0166 DEFAULT CICS WAIT LIST WILL BE USED.

Explanation: The default ICSF CICS Wait List file will be used for ICSF processing because:

1. There was no Wait List file specified in the Installation Options data set.
2. ICSF could not open or allocate the Wait List file specified.
3. The specified Wait List file contained more entries than allowed.

System action: Processing continues. The default ICSF CICS Wait List file will be used during ICSF processing.

System programmer response: If use of the ICSF default CICS Wait List file is the desired ICSF processing option, no action is required. Otherwise, ensure that the Wait List file specified in the Installation Options data set is valid.

User response: Contact your system programmer.

CSFO0176 SERVICE NAME *routine* NOT VALID AND WILL BE SKIPPED.

Explanation: The service name specified (*routine*), which is contained in the Wait List file, is not a valid name of an ICSF service or of an installation-defined service. The specified service name will not be placed in the Wait List.

System action: Processing continues. The specified service name will not be placed in the Wait List.

System programmer response: Check the contents of the Wait List file specified by the WAITLIST option of the Installation Options data set. Check the spelling of the service names in the file. Each record must be the name of an ICSF service or of a current installation-defined service or UDX service. Syntax rules for the CICS Wait List file are discussed in *z/OS Cryptographic Services ICSF System Programmer's Guide*.

User response: Contact your system programmer.

CSFO0196 PKDS DSNAME MISSING.

Explanation: The options parameter file did not include a statement that contains the PKDSN keyword and value.

System action: Processing ends.

System programmer response: Ensure that the options data set contains a statement with the PKDSN keyword and its value, and restart ICSF.

User response: Contact your system programmer.

CSFO0206 TKDSN OPTION NOT SPECIFIED. SYSPLEXTKDS OPTION IGNORED.

Explanation: The SYSPLEXTKDS option was specified without the TKDSN option in the installation options data set. No PKCS #11 processing is possible and the SYSPLEXTKDS option will have no effect.

System action: Processing ends.

System programmer response: Ensure that the SYSPLEXTKDS option is specified with the TKDSN option in the installations options data set or no PKCS #11 processing is possible and the SYSPLEXTKDS option will have no effect.

User response: Contact your system programmer.

CSFO0212 *Keyword* **KEYWORD NO LONGER SUPPORTED.**

Explanation: The keyword, *keyword*, is no longer supported by ICSF. The keyword was parsed, but has no affect.

System action: Processing continues.

System programmer response: Remove the keyword from the options data set if appropriate. Older releases of ICSF may still support the keyword.

CSFO0220 *Keyword* **VALUE NOT IN RANGE.**

Explanation: The specified value for the keyword is not within the allowable range. The default value for the keyword will be used in place of the value specified. *z/OS Cryptographic Services ICSF System Programmer's Guide* describes the allowable range for the keyword. The statement that contains the error precedes this message.

System action: Processing continues.

User response: Update the options data set with an allowable range for the keyword.

CSFO0230 *ICSF_option*

Explanation: This message is issued once for each option in the ICSF Options Data Set. This message is informational only. No action is required.

CSFO0236 BEGIN-END KEYWORD ERROR. ERROR CODE = *errcode*

Explanation: An error was detected with the BEGIN(FMID) and END keywords. The error code indicates the error.

1. There was no END for a BEGIN(FMID).
2. Unknown FMID. The FMID specified is not valid. For information on the z/OS ICSF FMIDs, see the *z/OS Cryptographic Services ICSF System Programmer's Guide*.
3. There was not matching BEGIN(FMID) for an END.

System action: Processing ends.

System programmer response: Check the syntax of the option statements.

User response: Contact your system programmer.

CSFO0240 EXIT NAME *exit-name* **NOT VALID AND WILL BE SKIPPED.**

Explanation: The installation exit name exit-name is not valid. Chapter 5 (Installation Exits) in the *z/OS Cryptographic Services ICSF System Programmer's Guide* lists the valid installation exit names.

System action: The exit for *exit-name* will not be loaded. Processing continues.

System programmer response: None.

User response: Update the options data set.

CSFO0404 CTRACE OPTION *text_value* **IS NOT VALID.**

Explanation: This message is issued when an incorrect trace option is specified in either the ICSF CTRACE configuration PARMLIB member or in the REPLY to a TRACE CT operator command.

System action: If this error occurs during ICSF startup, the default or specified PARMLIB member contains an incorrect option, and will not be used. ICSF CTRACE will attempt to use the default CTICSF00 PARMLIB member. If the CTICSF00 PARMLIB member is absent or contains an incorrect option, ICSF CTRACE will perform tracing using an internal default set of trace options. By default, ICSF CTRACE support will trace with the KdsIO, CardIO, and SysCall filters using a 2M buffer.

If this error occurs during a TRACE CT operator command, ICSF CTRACE will ignore the command and continue to use the current active options.

ICSF will continue processing.

System programmer response: Correct the ICSF CTRACE configuration PARMLIB member if one was specified and

reset ICSF CTRACE to use it using either the TRACE CT command or by restarting ICSF. If this error occurred during a TRACE CT operator command, correct the command syntax and reissue the command.

User response: Contact your system programmer.

CSFO0414 CTRACE PARMLIB MEMBER *member_name* COULD NOT BE USED. SWITCHING TO MEMBER CTICSF00.

Explanation: This message is issued when the PARMLIB member specified for the ICSF CTRACE configuration PARMLIB member is unusable.

System action: During ICSF startup, if the specified PARMLIB member is absent or contains an incorrect option, ICSF CTRACE will attempt to use the default CTICSF00 PARMLIB member. If the CTICSF00 PARMLIB member is absent or contains an incorrect option, ICSF CTRACE will perform tracing using an internal default set of trace options. By default, ICSF CTRACE support will trace with the KdsIO, CardIO, and SysCall filters using a 2M buffer.

ICSF will continue processing.

System programmer response: Correct the ICSF CTRACE configuration PARMLIB member and reset ICSF CTRACE to use it by using either the TRACE CT command or restarting ICSF.

User response: Contact your system programmer.

CSFO0424 CTRACE PARMLIB MEMBER CTICSF00 COULD NOT BE USED. SWITCHING TO DEFAULT SETTINGS.

Explanation: This message is issued at ICSF startup when the default CTICSF00 ICSF CTRACE configuration PARMLIB member is unusable.

System action: ICSF will use default CTRACE configuration settings and continue processing. By default, ICSF CTRACE support will trace with the KdsIO, CardIO, and SysCall filters using a 2M buffer.

System programmer response: Correct the unusable CTICSF00 PARMLIB member and reset ICSF CTRACE by using either the TRACE CT command or by restarting ICSF to use either the CTICSF00 PARMLIB member or another PARMLIB member containing valid ICSF CTRACE configuration options.

User response: Contact your system programmer.

Chapter 10. CSFPnnnn messages (Parse)

The following parse message is written to the ICSF job log.

CSFP0016 COULD NOT CREATE PARSE ENVIRONMENT.

Explanation: ICSF or the key generator utility program initialization process could not create an environment suitable for parsing of the options parameter statements or the key generator control statements.

System action: Processing ends for this request.

System programmer response: Ensure that there is enough space to create parse related control blocks. Check if the valid level of TSO/E is installed in accordance with the installation instructions in the OS/390 Program Directory. If it is valid, contact the IBM Support Center.

User response: Contact your system programmer.

Chapter 11. CSFUnnnn messages (ICSF utility pocessing)

Chapter 11, "CSFUnnnn messages (ICSF utility pocessing)" describes messages issued by the ICSF utilities. These messages are written to the ICSF job log using routing code 11.

CSFU001I THE ACTIVATE KEYWORD IS NO LONGER SUPPORTED. USE REFRESH INSTEAD.

Explanation: The CSFPUTIL utility no longer supports the ACTIVATE keyword. Use the REFRESH keyword instead.

System action: Processing ends.

System programmer response: Change the parameters on the CSFPTUIL job or program to use REFRESH or REFRESH followed by the new PKDS data set name. Re-run the job.

CSFU002I *utility* **COMPLETED, RETURN CODE =** *rc*, **REASON CODE =** *rs*.

Explanation: The return and reason codes are contained in the message.

System action: Processing ends.

System programmer response: Look up the ICSF utility in the *z/OS Cryptographic Services ICSF Administrator's Guide* and check the meaning for the return and reason codes. Make the necessary corrections and run the job again.

CSFU003E *keyword1* **WAS SPECIFIED, BUT** *keyword2* **WAS ALREADY SPECIFIED.**

Explanation: In parsing a set of options, both keyword1 and keyword2 were specified, when only one or the other was expected.

System action: Processing ends.

System programmer response: Review the options provided to the utility. Make the necessary corrections and run the job again.

CSFU004E SYNTAX ERROR ON LINE *linenum* **OF** *dsname*.

Explanation: In parsing a set of options from dsname, a syntax error was encountered on line *linenum*. The *dsname* provided will be in the form of DD:ddname where ddname is the name of the DD which provides the options to the utility.

System action: Processing ends.

System programmer response: Review the option provided to the utility on the line indicated. Make the necessary corrections and run the job again.

CSFU005E *kwdclass* **NOT SPECIFIED.**

Explanation: After parsing all options, no keyword from the class *kwdclass* was provided.

System action: Processing ends.

System programmer response: options provided to the utility. Make the necessary corrections and run the job again.

CSFU006I *operation* **FEEDBACK: RC=***return-code* **RS=***reason-code* **SUPRC=***supplemental-return-code* **SUPRS=***supplemental-reason-code* **FLAGS=***flags*.

Explanation: The coordinated KDS administration operation failed. The *operation* may be CHANGE-MK or REFRESH. *return-code* and *reason-code* indicate the primary return code and reason code for the failure. *supplemental-return-code* and *supplemental-reason-code* indicate the supplemental return code and reason code for the failure. *flags* indicate additional internal diagnostic information about the failure.

System action: ICSF processing continues.

System programmer response: Contact the security administrator for help determining the problem. Use the *return-code* and *reason-code* for problem determination. For more information on the *return-code* and *reason-code*, refer to the *z/OS Cryptographic Services ICSF Application Programmer's Guide* or the information on the CSFEUTIL program in the *z/OS Cryptographic Services ICSF Administrator's Guide*. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure. If you are unable to determine the problem by looking up these values, contact the IBM Support Center. The *supplemental-return-code*, *supplemental-reason-code*, and *flags* show IBM internal diagnostic information. You may need to provide this information to the IBM Support Center.

Chapter 12. CSFVnnnn messages (CKDS conversion processing)

CSFVnnnn Messages (CKDS Conversion Processing) describes messages that ICSF issues during the cryptographic key data set (CKDS) conversion process. These messages are written to the ICSF job log using routing code 11.

CSFV0012 CONVERSION PROCESSING COMPLETED. RETURN CODE = *retcode*.

Explanation: The CUSP/PCF CKDS to ICSF CKDS conversion program has completed successfully.

System action: Processing ends.

User response: Review the return codes and their meanings:

Return Code
Meaning

00 Successful processing.

04 The conversion process encountered warning conditions, but completed processing of all transactions. Review preceding messages for the warning conditions.

CSFV0026 CONVERSION TERMINATED. RETURN CODE = *retcode*, **REASON CODE =** *rsncode*.

Explanation: An error occurred in the conversion program that caused ICSF to end processing. See the list of return and reason codes to determine the cause of the error.

Return code: 12

Reason Code
Meaning

6004 The conversion program selected a CKDS access function that is not valid.

The valid CKDS access functions are:

- READ
- READUP
- WRITE
- REWRITE

6008 A service routine failed. ICSF sets the reason code after issuing message CSFG0293.

The service routines are:

- CSFMGN
- CSFMVR
- CSFMKVR

6012 The installation exit returned a return code greater than 4. ICSF sets the reason code after issuing message CSFC0186.

6016 A failure or error occurred in an I/O routine. ICSF sets the reason code after the I/O routine issues a CSFYnnnn message.

6020 The installation exit ended abnormally and the service processing has ended. ICSF sets the reason code after issuing message CSFC0136.

6024 The installation exit ended abnormally and the service processing has ended. ICSF sets the reason code after issuing message CSFC0206.

6028 An ESTAE environment could not be established. ICSF sets the reason code after issuing message CSFC0026.

6032 The dynamic allocation for the supplied CKDS failed. ICSF sets the reason code after issuing message CSFC0036.

6036 The dynamic unallocation for the supplied CKDS failed. ICSF sets the reason code after issuing message CSFC0072.

6040 The required installation exit could not be loaded to be run. ICSF sets the reason code after issuing message CSFC0166.

6044 A call to CSFINF1 failed, and the error was not caused by ICSF not being active. ICSF sets the reason code after issuing message CSFC0053.

6048 ICSF could not find the system keys while attempting to write a complete CKDS. ICSF sets the reason code after issuing message CSFC0086.

9000 The IMPORTER label that is specified for the PARM keyword of the EXEC JCL statement is not valid. The length of the label must be eight characters or less, all non-blank character must be alphanumeric, and the first character must be alphabetic. ICSF sets the reason code after issuing message CSFV0036.

9004 ICSF could not find the IMPORTER record on the supplied ICSF CKDS for the label that is specified with the PARM keyword on the EXEC JCL statement. ICSF sets the reason code after issuing message CSFV0046.

9008 The CUSP/PCF CKDS that was input to the conversion process is not valid. ICSF sets the reason code after issuing message CSFV0056.

9016 The conversion process attempted to use a non-empty output ICSF CKDS. The output ICSF CKDS that is specified by DD statement CSFVNEW must be empty when running the conversion process. ICSF sets the reason code after issuing message CSFV0056.

9020 The required conversion installation exit could not be loaded. This may be caused by one of these conditions. The EXIT keyword in the options file specifies an incorrect load module name. The load module does not exist in any library in the link list being used. The load module does not exist in the library specified in a JOBLIB or STEPLIB DD statement. ICSF sets the reason code after issuing message CSFC0166.

9024 The record type of a source CUSP/PCF CKDS entry is not valid. The record type must be either LOCAL, REMOTE, or CROSS. ICSF sets the reason code after issuing message CSFV0266.

9028 The conversion program encountered a second explicit override entry when an explicit override entry already pertains to all types within the label. ICSF sets the reason code after issuing message CSFV0256.

9032 The conversion program encountered a third global override entry. The conversion process allows for a total of two global override entries as input. ICSF sets the reason code after issuing message CSFV0276.

9036 The conversion program encountered a second global override entry when the first global override entry pertains to all types. ICSF sets the reason code after issuing message CSFV0286.

9040 An override entry consists of all blanks.

9044 An override entry is out of sequence. The override entries should be in sequence by LABEL and OLD_TYPE. ICSF sets the reason code after issuing message CSFV0316.

9048 An override entry duplicates another override entry within LABEL and OLD_TYPE. ICSF sets the reason code after issuing message CSFV0326.

9056 An override entry's NEW_TYPE is not valid. If the OLD_TYPE is LOCAL, the NEW_TYPE must be EXPORTER, OPINENC, or blank. If the OLD_TYPE is REMOTE, the NEW_TYPE must be IMPORTER, IPINENC, or blank. ICSF sets the reason code after issuing message CSFV0346.

9060 An override entry's OLD_TYPE is not valid. The OLD_TYPE must be LOCAL, REMOTE, or blank. ICSF sets the reason code after issuing message CSFV0356 or CSFV0366.

9064 An override entry's BYPASS_FLAG is not valid. The BYPASS_FLAG must be Y, N, or blank. Blank is equivalent to N. ICSF sets the reason code after issuing message CSFV0376.

9068 The pre-processing installation exit call has failed with a return code greater than 8. ICSF sets the reason code after issuing message CSFV0506. Follow local procedures for installation exit problems.

9072 The post-processing installation exit call has failed with a return code greater than 8. ICSF sets the reason code after issuing message CSFV0516. Follow local procedures for installation exit problems.

9076 The record processing installation exit call has failed with a return code greater than 8. ICSF sets the reason code after issuing message CSFC0186. Follow local procedures for installation exit problems.

9080 The installation exit has ended abnormally, and ICSF should be stopped. ICSF sets the reason code after issuing message CSFC0206. Check the installation exit for errors.

9084 The installation exit has ended abnormally, and the conversion process has ended. ICSF sets the reason code after issuing message CSFC0136. Check the installation exit module for errors.

9088 The installation exit has requested the ending of the conversion process. ICSF sets the reason code after issuing message CSFV0546.

9092 A data set that was input to the conversion process is not a valid ICSF/MVS Version 1 Release 1 CKDS. ICSF sets the reason code after issuing message CSFV0066.

9096 ICSF detected a duplicate label that is not valid. Processing would have resulted in more than one key on the target CKDS with the same label. This condition is not valid when one of the keys is a DATA, MAC, MACVER, DATAXLAT, or NULL key. ICSF sets the reason code after issuing message CSFV0396.

Return code: 16

Reason Code
Meaning

0000 Could not open the output report data set. Ensure that a JCL DD statement exists for the CSFVRPT report data set in the conversion process jobstream. If you cannot resolve the problem, see your system programmer.

Return code: 20

Reason Code
Meaning

0000 Could not establish an ESTAE recovery environment. Attempt to run the job again. If it still fails, contact the IBM Support Center.

Return code: 24

Reason Code
Meaning

0000 An abnormal ending has occurred. Respond to the problem that is identified in the associated error message.

Return code: 64

Reason Code
Meaning

0000 An OPEN error occurred for the CSFVRPT report data set. If it is a pre-allocated data set, ensure that the record length is correct.

Return code: 68

Reason Code
Meaning

0000 An I/O error occurred for the CSFVRPT report data set. An attempt to CLOSE the data set was tried, so check to see if there are meaningful messages in the data set.

System action: Processing ends.

System programmer response: Respond to the problem that is identified by the return and reason codes. Rerun the conversion program.

User response: Determine the cause of the error, correct the problem, and rerun the conversion program. If you cannot resolve the problem, contact your system programmer.

CSFV0036 IMPORTER KEY LABEL NOT VALID.

Explanation: The IMPORTER key label that is specified with the PARM keyword on the EXEC JCL statement is not valid. The label must be 64 or fewer characters in length.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9000. Processing ends.

User response: Ensure that the label that is specified is correct and matches the IMPORTER label on the supplied ICSF CKDS. Rerun the conversion program.

CSFV0046 *label* **IMPORTER KEY NOT FOUND ON INPUT ICSF CKDS.**

Explanation: The conversion program could not find the record for the IMPORTER key with the *label* label in the supplied ICSF CKDS. The label was specified with the PARM keyword on the EXEC JCL statement.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9004. Processing ends.

User response: Ensure that the specified *label* is correct or that the IMPORTER label in the supplied ICSF CKDS is correct. Rerun the conversion program.

CSFV0056 CSFVSRC DATA SET NOT A CUSP OR PCF CKDS.

Explanation: The data set that is named in the CSFVSRC DD statement is not a CUSP/PCF CKDS.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9008. Processing ends.

User response: Ensure that the CSFVSRC DD statement specifies the correct data set name for a CUSP/PCF CKDS. Rerun the conversion program.

CSFV0152 TYPE FOR ALL *type* **KEY ENTRIES CONVERTED TO** *new-type***.**

Explanation: A global override entry specified that all *type* key entries on the CUSP/PCF CKDS are to be converted to *new-type* key entries on the new ICSF CKDS.

System action: Processing continues.

User response: None.

CSFV0172 ALL *type* **KEY ENTRIES BYPASSED.**

Explanation: A global override entry specified to bypass all entries on the CUSP/PCF CKDS with a type of *type*.

System action: Processing continues.

User response: None.

CSFV0182 INSTALLATION DATA FOR ALL *type* **KEY ENTRIES SET TO** *installation-data***.**

Explanation: A global override entry specified that all key entries in the CUSP/PCF CKDS with a type of *type* are to have the value *installation-data* set in the INSTALLATION_DATA field of the entries on the new ICSF CKDS.

System action: Processing continues.

User response: None.

CSFV0192 TYPE FOR KEY ENTRY *label type* **CONVERTED TO** *new-type***.**

Explanation: An override entry specified that the type for the key entry in the CUSP/PCF CKDS identified as *label type* is to be changed to *new-type* on the new ICSF CKDS.

System action: Processing continues.

User response: None.

CSFV0212 KEY ENTRY *label type* **BYPASSED.**

Explanation: An override entry specified to bypass the key entry in the CUSP/PCF CKDS identified as *label type* and not include it in the new ICSF CKDS.

System action: Processing continues.

User response: None.

CSFV0222 KEY ENTRY *label type* **NOT BYPASSED.**

Explanation: An override entry specified not to bypass the key entry in the CUSP/PCF CKDS identified as *label type* and to include it in the new ICSF CKDS.

System action: Processing continues.

User response: None.

CSFV0232 INSTALLATION DATA FOR KEY ENTRY *label type* **SET TO** *installation-data***.**

Explanation: An override entry specified that the INSTALLATION_DATA for the key entry in the CUSP/PCF CKDS identified as *label type* is to be set to *installation-data* on the new ICSF CKDS.

System action: Processing continues.

User response: None.

CSFV0256 OVERRIDE ENTRY FOR KEY ENTRY *label* **NOT VALID. PREVIOUS OVERRIDE ENTRY HAD BLANK OLD_TYPE.**

Explanation: An override entry specified the same key label (*label*) as a previous override entry, which had a blank OLD_TYPE specified. Only one override entry is allowed with a blank OLD_TYPE because it applies to all entries with a matching label.

System action: The system issues message CSFV0026 with return code of 12 and a reason code of 9028. Processing ends.

User response: Either remove the second override entry from the override data set or ensure that the first override entry has a value for OLD_TYPE. Rerun the conversion program.

CSFV0266 CUSP/PCF KEY ENTRY *label* **TYPE NOT VALID.**

Explanation: The CUSP/PCF CKDS entry with LABEL *label* has a type that is not LOCAL, REMOTE, or CROSS.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9024. Processing ends.

User response: Specify LOCAL, REMOTE, or CROSS for the CUSP/PCF CKDS entry type. Rerun the conversion program.

CSFV0276 MORE THAN TWO GLOBAL OVERRIDE ENTRIES SPECIFIED.

Explanation: The override data set contains more than two global entries. The maximum number of global entries is two; one for each type, LOCAL and REMOTE.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9032. Processing ends.

User response: Remove the extraneous global override entries. Rerun the conversion program.

CSFV0286 GLOBAL OVERRIDE ENTRY NOT VALID. PREVIOUS GLOBAL OVERRIDE ENTRY HAD BLANK OLD_TYPE.

Explanation: A second global override entry was present when the first global override entry had no value specified for OLD_TYPE. Because the first global override entry is to be applied to all entries, the second global override entry is redundant.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9036. Processing ends.

User response: Ensure that the override data set contains the proper global override entries. Rerun the conversion program.

CSFV0292 NO KEY ENTRY FOUND FOR *label type***.**

Explanation: An override entry specified a key entry of *label type* that was not present in the CUSP/PCF CKDS. The conversion program ignored the override entry.

System action: Processing continues.

User response: If the *label type* specification was incorrect, change it. A global override entry may be required to bypass all entries on the CUSP/PCF CKDS. Rerun the conversion program.

CSFV0306 BLANK OVERRIDE ENTRY.

Explanation: The override data set contains an entry that is all blanks, which is not valid.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9040. Processing ends.

User response: Remove the blank override entry and rerun the conversion program.

CSFV0316 OVERRIDE ENTRY NOT IN SEQUENCE.

Explanation: The override data set has an entry that is not in ascending sequence on LABEL and OLD_TYPE.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9044. Processing ends.

User response: Ensure that the override data set is in ascending sequence on LABEL and OLD_TYPE. Rerun the conversion program.

CSFV0326 DUPLICATE OVERRIDE ENTRY FOR KEY ENTRY *label type***.**

Explanation: The override data set contained an entry that specified the same key entry (*label type*) as a previous override entry.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9048. Processing ends.

User response: Remove one of the duplicate override entries. Rerun the conversion program.

CSFV0346 CANNOT CHANGE TYPE TO *new-type* **FOR KEY ENTRY** *label type***.**

Explanation: An override entry specified that the type for the key entry *label type* in the CUSP/PCF CKDS be converted to *new-type* in the new ICSF CKDS. This is not valid. If the source type is LOCAL, the new type must be EXPORTER or OPINENC. If the source type is REMOTE, the new type must be IMPORTER or IPINENC.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9056. Processing ends.

User response: Either change the new type or delete the override entry. Rerun the conversion program.

CSFV0356 OLD_TYPE REQUIRED WHEN NEW_TYPE SPECIFIED ON OVERRIDE ENTRY.

Explanation: An override entry specified a value for NEW_TYPE, but did not specify a value for OLD_TYPE.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9060. Processing ends.

User response: Either specify a value for the OLD_TYPE or remove the supplied NEW_TYPE. Rerun the conversion program.

CSFV0366 OLD_TYPE *type* SPECIFIED ON OVERRIDE ENTRY NOT VALID.

Explanation: An override entry specified an old type of *type*, which is not valid. The OLD_TYPE must be LOCAL, REMOTE, or blank.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9060. Processing ends.

User response: Specify LOCAL, REMOTE, or blank for the OLD_TYPE field. Rerun the conversion program.

CSFV0376 BYPASS_FLAG VALUE SPECIFIED ON OVERRIDE ENTRY NOT VALID.

Explanation: An override entry specified a value in the BYPASS_FLAG field that is not valid. The valid values are Y, N, or blank. Blank is equivalent to N.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9064. Processing ends.

User response: Specify Y, N, or blank for the BYPASS_FLAG field. Rerun the conversion program.

CSFV0382 ADD/CHANGE SPECIFICATIONS IGNORED ON OVERRIDE ENTRY. BYPASS_FLAG VALUE IS "Y".

Explanation: An override entry specified a value of Y in the BYPASS_FLAG field. This caused the conversion program to bypass the CUSP/PCF CKDS entry. However, the override entry had non-blank values specified in one or more of the fields that are used to specify additions or changes to the new ICSF CKDS entry. The conversion program did not apply thes non-blank values because it pypassed the CUSP/PCF CKDS entry.

System action: Processing continues.

User response: If you do not want the conversion program to bypass the CUSP/PCF CKDS entry, change the value in the BYPASS_FLAG field to N or blank. It may require the use of a global override entry to bypass all entries on the CUSP/PCF CKDS. Rerun the conversion program.

CSFV0396 UNIQUE *label type* FOUND ON INPUT ICSF/MVS CKDS. CANNOT CONVERT *label* RECORD FROM PCF/CUSP SOURCE.

Explanation: The conversion program detected a duplicate label that is not valid. The CUSP/PCF label was the same as a label on the target ICSF CKDS and processing would have resulted in more than one key on the target CKDS with the same label. This condition is not valid for keys that require unique labels (DATA, DATAXLAT, MAC, MACVER, or NULL keys).

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9096. Processing ends.

User response: Resolve the label conflict in the input, merged, and target CKDS, or update the conversion override file to bypass conversion of *label* from the input PCF/CUSP CKDS. Then rerun the conversion program.

CSFV0506 CONVERSION INSTALLATION EXIT PREPROCESSING FAILED. RETURN CODE = *retcode*.

Explanation: The pre-processing installation exit has failed with a return code of *retcode*.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9068. Processing ends.

System programmer response: Follow local procedures for correcting errors that are found in the installation exit. Rerun the conversion process.

CSFV0516 CONVERSION INSTALLATION EXIT POSTPROCESSING FAILED. RETURN CODE = *retcode*.

Explanation: The post-processing installation exit has failed with a return code of *retcode*.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9072. Processing ends.

System programmer response: Follow local procedures for correcting errors that are found in the installation exit. Rerun the conversion process.

CSFV0522 CONVERSION INSTALLATION EXIT ATTEMPT TO CHANGE LABEL OR TYPE IGNORED.

Explanation: The record processing installation exit has attempted to change the LABEL or TYPE key entry, which is not allowed. The conversion program ignored the attempt.

System action: Processing continues.

System programmer response: Follow local procedures for correcting errors that are found in the installation exit. Rerun the conversion program.

CSFV0546 *exit-id* **INSTALLATION EXIT** *routine* **REQUESTED TERMINATION OF PROCESSING.**

Explanation: The *exit-id* installation exit and the *routine* load module requested that the conversion program be ended.

System action: The system issues message CSFV0026 with a return code of 12 and a reason code of 9088. Processing ends.

System programmer response: Follow local procedures for the installation exit termination request.

CSFV0552 KEY ENTRY *label* **WILL BE CONVERTED BUT MAY NOT BE USABLE IN ICSF SERVICES.**

Explanation: The first character of the *label* is not a valid character for ICSF labels. ICSF services will not accept labels formed incorrectly.

System action: Processing continues.

User response: Notify the security administrator of the error so corrective action can be taken.

CSFV0560 *utility* **COMPLETED, RETURN CODE =** *retcode*, **REASON CODE =** *rsncode*.

Explanation: The utility *utility* completed processing with a return code of *retcode* and reason code of *rsncode*.

System action: Processing ends.

System programmer response: Look up the ICSF utility in the *z/OS Cryptographic Services ICSF Administrator's Guide* and check the meaning for the return and reason codes. Make the necessary corrections and run the job again.

Chapter 13. CSFYnnnn messages (I/O errors)

Chapter 13, "CSFYnnnn messages (I/O errors)" describes messages that the ICSF Input/Output (I/O) routine issues. These messages are written to the ICSF job log using routing code 11.

CSFY0026 ERROR OCCURRED PROCESSING DD *ddname*. RETURN CODE = *retcode*, REASON CODE = *rsncode*.

Explanation: *Ddname* indicates the DD statement for the data set that was being processed when the error occurred. *Retcode* indicates the return code, and *rsncode* indicates the reason code. See the list of return and reason codes to determine the cause of the error.

For QSAM files:
Return code: 04

Reason Code
Meaning

128 An error occurred closing the data set. No action is necessary. The data set will close when the job ends.

Return code: 12

Reason Code
Meaning

100 Could not acquire the storage that the DCB and I/O buffers require. Increase the region size.

104 Logical record length for the data set is incorrect. If pre-allocated, redefine with the correct record length. If defined on a DD statement, correct the LRECL value.

108 An error occurred while running SYNADAF. A message is printed, but some information may be missing. Asterisks represent the missing information.

112 An error occurred while running SYNADRLS. No action is necessary. The macro releases the space when the job ends. Register 13 will not point to the save area the SYNADAF macro provided, resulting in an improper chaining of the save areas. Further errors may result.

116 An error occurred opening the data set. Ensure that the JCL DD statement for the data set is present and that it defines the correct data set.

For VSAM files:
Return code: 04

Reason Code
Meaning

196 An error occurred closing the data set. Run an IDCAMS verify to reset the data set's catalog pointers.

Return code: 12

Reason Code
Meaning

160 Could not acquire the storage the I/O buffer requires. Increase the region size.

164 Could not generate the exit list.

168 Could not generate the access control block (ACB).

172 An error occurred running an AMS SHOWCB macro.

176 Could not generate the request parameter list (RPL).

180 The supplied logical record length does not agree with the record length that is defined for the data set. Redefine the data set with the correct record length.

184 An error occurred running an AMS MODCB macro.

192 An error occurred opening the file. This can be normal if concurrent instances of ICSF are being started on different systems for a shared data set. In this case, ICSF initialization logic is constructed to overcome the error. If this is not a situation where concurrent instances of ICSF are starting and sharing the data set, then ensure that the JCL DD statement for the data set is present and that it defines the correct data set.

200 An error occurred attempting to change the RPL for keyed access.

204 An error occurred attempting to change the RPL for update access.

208 An error occurred attempting to change the RPL for non-update access.

316 A VSAM logical error occurred. Message CSFY0076 shows the ddname for the data set and the VSAM feedback code.

3078 The CKDS was created with an unsupported LRECL.

System action: Processing ends.

System programmer response: Respond to the problem that is identified by the return and reason codes. If you cannot resolve the problem, contact the IBM Support Center.

User response: Contact your system programmer.

CSFY0036 Synad message (for VSAM or non-VSAM file).

Explanation: A physical error occurred while processing a VSAM or QSAM file.

For a QSAM file, the format and explanation of the message is in the SYNADAF macro instruction description.

For a VSAM file, the format and explanation of the message is in the Physical-Error Message Format figure.

System action: Processing ends.

System programmer response: See the appropriate document for the explanation of the message. Correct the problem and rerun the job. If you cannot resolve the problem, contact the IBM Support Center.

User response: Contact your system programmer.

CSFY0056 I/O ROUTINE UNABLE TO ESTABLISH AN ESTAE.

Explanation: The ICSF I/O routine could not establish an ESTAE environment.

System action: Processing ends.

System programmer response: Contact the IBM Support Center.

User response: Attempt to run the job again. If it still fails, contact your system programmer.

CSFY0076 VSAM ERROR OCCURRED PROCESSING DD *ddname***. VSAM FEEDBACK CODE =** *fdbkcode*

Explanation: A VSAM logical error occurred while processing the data set that is specified by the *ddname* DD statement. The VSAM RPL Feedback Word *fdbkcode* indicates which error occurred.

System action: Processing ends.

System programmer response: If you cannot resolve the error, contact the IBM Support Center.

User response: Check the VSAM RPL Feedback Word as documented in the *z/OS DFSMSdfp Diagnosis*. If you cannot correct the error, contact your system programmer.

CSFY0086 VSAM ERROR OCCURRED PROCESSING DD *ddname*. OUT OF EXTENTS.

Explanation: A VSAM error has occurred processing a data set that is specified by the *ddname* DD statement. The data set is out of extents. The data set must be on a volume that has enough space for the data.

System action: Processing ends.

System programmer response: If you cannot resolve the error, contact the IBM Support Center.

User response: Contact your system programmer.

Appendix. Accessibility

Accessible publications for this product are offered through the z/OS® Information Center, which is available at www.ibm.com/systems/z/os/zos/bkserv/.

If you experience difficulty with the accessibility of any z/OS information, please send a detailed message to mhvrcfs@us.ibm.com or to the following mailing address:

IBM® Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
USA

Accessibility features

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:

- Use assistive technologies such as screen readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size.

Using assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using such products to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to *z/OS TSO/E Primer*, *z/OS TSO/E User's Guide*, and *z/OS ISPF User's Guide Vol I* for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

Dotted decimal syntax diagrams

Syntax diagrams are provided in dotted decimal format for users accessing the z/OS Information Center using a screen reader. In dotted decimal format, each syntax element is written on a separate line. If two or more syntax elements are always present together (or always absent together), they can appear on the same line, because they can be considered as a single compound syntax element.

Each line starts with a dotted decimal number; for example, 3 or 3.1 or 3.1.1. To hear these numbers correctly, make sure that your screen reader is set to read out punctuation. All the syntax elements that have the same dotted decimal number (for example, all the syntax elements that have the number 3.1) are mutually

exclusive alternatives. If you hear the lines 3.1 USERID and 3.1 SYSTEMID, you know that your syntax can include either USERID or SYSTEMID, but not both.

The dotted decimal numbering level denotes the level of nesting. For example, if a syntax element with dotted decimal number 3 is followed by a series of syntax elements with dotted decimal number 3.1, all the syntax elements numbered 3.1 are subordinate to the syntax element numbered 3.

Certain words and symbols are used next to the dotted decimal numbers to add information about the syntax elements. Occasionally, these words and symbols might occur at the beginning of the element itself. For ease of identification, if the word or symbol is a part of the syntax element, it is preceded by the backslash (\) character. The * symbol can be used next to a dotted decimal number to indicate that the syntax element repeats. For example, syntax element *FILE with dotted decimal number 3 is given the format 3 * FILE. Format 3* FILE indicates that syntax element FILE repeats. Format 3* * FILE indicates that syntax element * FILE repeats.

Characters such as commas, which are used to separate a string of syntax elements, are shown in the syntax just before the items they separate. These characters can appear on the same line as each item, or on a separate line with the same dotted decimal number as the relevant items. The line can also show another symbol giving information about the syntax elements. For example, the lines 5.1*, 5.1 LASTRUN, and 5.1 DELETE mean that if you use more than one of the LASTRUN and DELETE syntax elements, the elements must be separated by a comma. If no separator is given, assume that you use a blank to separate each syntax element.

If a syntax element is preceded by the % symbol, this indicates a reference that is defined elsewhere. The string following the % symbol is the name of a syntax fragment rather than a literal. For example, the line 2.1 %OP1 means that you should refer to separate syntax fragment OP1.

The following words and symbols are used next to the dotted decimal numbers:

- ? means an optional syntax element. A dotted decimal number followed by the ? symbol indicates that all the syntax elements with a corresponding dotted decimal number, and any subordinate syntax elements, are optional. If there is only one syntax element with a dotted decimal number, the ? symbol is displayed on the same line as the syntax element, (for example 5? NOTIFY). If there is more than one syntax element with a dotted decimal number, the ? symbol is displayed on a line by itself, followed by the syntax elements that are optional. For example, if you hear the lines 5 ?, 5 NOTIFY, and 5 UPDATE, you know that syntax elements NOTIFY and UPDATE are optional; that is, you can choose one or none of them. The ? symbol is equivalent to a bypass line in a railroad diagram.
- ! means a default syntax element. A dotted decimal number followed by the ! symbol and a syntax element indicates that the syntax element is the default option for all syntax elements that share the same dotted decimal number. Only one of the syntax elements that share the same dotted decimal number can specify a ! symbol. For example, if you hear the lines 2? FILE, 2.1! (KEEP), and 2.1 (DELETE), you know that (KEEP) is the default option for the FILE keyword. In this example, if you include the FILE keyword but do not specify an option, default option KEEP will be applied. A default option also applies to the next higher dotted decimal number. In this example, if the FILE keyword is omitted, default FILE(KEEP) is used. However, if you hear the lines 2? FILE, 2.1, 2.1.1!

(KEEP), and 2.1.1 (DELETE), the default option KEEP only applies to the next higher dotted decimal number, 2.1 (which does not have an associated keyword), and does not apply to 2? FILE. Nothing is used if the keyword FILE is omitted.

- * means a syntax element that can be repeated 0 or more times. A dotted decimal number followed by the * symbol indicates that this syntax element can be used zero or more times; that is, it is optional and can be repeated. For example, if you hear the line 5.1* data area, you know that you can include one data area, more than one data area, or no data area. If you hear the lines 3*, 3 HOST, and 3 STATE, you know that you can include HOST, STATE, both together, or nothing.

  Note:

  1. If a dotted decimal number has an asterisk (*) next to it and there is only one item with that dotted decimal number, you can repeat that same item more than once.
  2. If a dotted decimal number has an asterisk next to it and several items have that dotted decimal number, you can use more than one item from the list, but you cannot use the items more than once each. In the previous example, you could write HOST STATE, but you could not write HOST HOST.
  3. The * symbol is equivalent to a loop-back line in a railroad syntax diagram.

- + means a syntax element that must be included one or more times. A dotted decimal number followed by the + symbol indicates that this syntax element must be included one or more times; that is, it must be included at least once and can be repeated. For example, if you hear the line 6.1+ data area, you must include at least one data area. If you hear the lines 2+, 2 HOST, and 2 STATE, you know that you must include HOST, STATE, or both. Similar to the * symbol, the + symbol can only repeat a particular item if it is the only item with that dotted decimal number. The + symbol, like the * symbol, is equivalent to a loop-back line in a railroad syntax diagram.

Notices

This information was developed for products and services offered in the U.S.A. or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

Site Counsel
IBM Corporation
2455 South Road
Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

COPYRIGHT LICENSE:

This information might contain sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Policy for unsupported hardware

Various z/OS elements, such as DFSMS, HCD, JES2, JES3, and MVS™, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted

for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (http://www.ibm.com/software/support/systemsz/lifecycle/)
- For information about currently-supported IBM hardware, contact your IBM representative.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Index

Printed in USA

SC14-7509-02