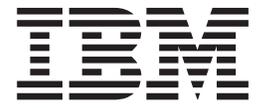


z/OS
Cryptographic Services
Integrated Cryptographic Service Facility



Messages

z/OS
Cryptographic Services
Integrated Cryptographic Service Facility



Messages

Note!

Before using this information and the product it supports, be sure to read the general information under "Notices" on page 65.

This edition applies to Version 1 Release 12 of z/OS (5694-A01) and to all subsequent releases and modifications until otherwise indicated in new editions. This edition applies to ICSF FMID HCR7780.

This edition replaces SA22-7523-13

© **Copyright IBM Corporation 1997, 2010.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Purpose of this information	v
Who should read this information.	v
How to use this information	v
Where to find more information	v
Using LookAt to look up message explanations	vii
Do You Have Problems, Comments, or Suggestions?	vii
Summary of Changes	ix
Chapter 1. Introduction	1
Chapter 2. CSFBnnnn Messages (Build Control Statement Processing)	3
Chapter 3. CSFCnnnn Messages (Cryptographic Key Data Set Processing)	5
Chapter 4. CSFEnnnn Messages (Exit Router)	9
Chapter 5. CSFGnnnn Messages (Key Generator Utility Processing)	11
Chapter 6. CSFHnnnn Messages (IBM Health Checker Processing)	21
Chapter 7. CSFInnnn Messages (Component Trace)	23
Chapter 8. CSFMnnnn Messages (ICSF Address Space)	25
Chapter 9. CSFOnnnn Messages (Installation Options Parameter Processing)	45
Chapter 10. CSFPnnnn Messages (Parse)	49
Chapter 11. CSFUnnnn Messages (ICSF Utility Processing)	51
Chapter 12. CSFVnnnn Messages (CKDS Conversion Processing)	53
Chapter 13. CSFYnnnn Messages (I/O Errors)	61
Appendix. Accessibility	63
Using assistive technologies	63
Keyboard navigation of the user interface	63
z/OS information	63
Notices	65
Trademarks	66

Purpose of this information

This information supports z/OS (5694-A01) and z/OS.e (5655-G52). It contains messages and their routing and descriptor codes for the Integrated Cryptographic Service Facility (ICSF), program number 5694-A01.

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

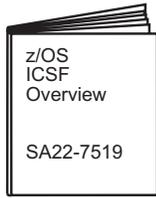
This document contains ICSF messages with their prefixes organized in alphanumeric order.

- Chapter 2, “CSFBnnnn Messages (Build Control Statement Processing)”
- Chapter 3, “CSFCnnnn Messages (Cryptographic Key Data Set Processing)”
- Chapter 4, “CSFEnnnn Messages (Exit Router)”
- Chapter 5, “CSFGnnnn Messages (Key Generator Utility Processing)”
- Chapter 6, “CSFHnnnn Messages (IBM Health Checker Processing)”
- Chapter 7, “CSFInnnn Messages (Component Trace)”
- Chapter 8, “CSFMnnnn Messages (ICSF Address Space)”
- Chapter 9, “CSFOnnnn Messages (Installation Options Parameter Processing)”
- Chapter 10, “CSFPnnnn Messages (Parse)”
- Chapter 11, “CSFUnnnn Messages (ICSF Utility Processing)”
- Chapter 12, “CSFVnnnn Messages (CKDS Conversion Processing)”
- Chapter 13, “CSFYnnnn Messages (I/O Errors)”
- “Accessibility,” on page 63 contains information on accessibility features in z/OS.
- “Notices” on page 65 contains notices and trademarks.

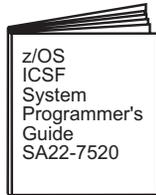
Where to find more information

For information about the referenced ICSF documents, see Figure 1.

Tasks



Evaluating
Planning



Customizing
Diagnosis
Installing
Operating



Application
Programming

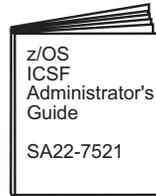


Application
Programming

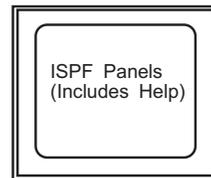
Tasks



Administrating
Application Programming
Diagnosis
Operating

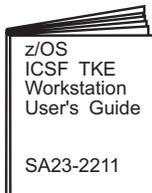


Administrating



Administrating

Optional Features



Available with the
Trusted Key Entry
Workstation
(TKE Version 7)



The ICSF Library,
Trusted Key Entry
Workstation User's
Guide and Encryption
Facility for z/OS
Planning and
Customizing are
included on the IBM
Online Library:
z/OS Collection Kit
SK3T-4269

Figure 1. The ICSF Library

Other documents that are referenced are:

- *z/OS DFSMS Macro Instructions for Data Sets*, SC26-7408

- *z/OS DFSMS Access Method Services for Catalogs*, SC26-7394
- *S/390 PR/SM Planning Guide*
- *S/390 Support Element Operations Guide*
- *z/OS MVS System Codes*, SA22-7626
- *z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG*, SA22-7610
- *z/OS MVS IPCS User's Guide*, SA22-7596
- *z/OS MVS Diagnosis: Reference*, GA22-7588
- *z/OS DFSMSdfp Diagnosis*, GY27-7618

Using LookAt to look up message explanations

LookAt is an online facility that lets you look up explanations for most of the IBM® messages you encounter, as well as for some system abends and codes. Using LookAt to find information is faster than a conventional search because in most cases LookAt goes directly to the message explanation.

You can use LookAt from these locations to find IBM message explanations for z/OS® elements and features, z/VM®, z/VSE, and Clusters for AIX® and Linux:

- The Internet. You can access IBM message explanations directly from the LookAt Web site at www.ibm.com/servers/eserver/zseries/zos/bkserv/lookat/.
- Your z/OS TSO/E host system. You can install code on your z/OS systems to access IBM message explanations using LookAt from a TSO/E command line (for example: TSO/E prompt, ISPF, or z/OS UNIX System Services).
- Your Microsoft Windows workstation. You can install LookAt directly from the *z/OS and Software Products DVD Collection* (SK3T-4271) and use it from the resulting Windows graphical user interface (GUI). The command prompt (also known as the DOS > command line) version can still be used from the directory in which you install the Windows version of LookAt.
- Your wireless handheld device. You can use the LookAt Mobile Edition from www.ibm.com/servers/eserver/zseries/zos/bkserv/lookat/lookatm.html with a handheld device that has wireless access and an Internet browser.

You can obtain code to install LookAt on your host system or Microsoft Windows workstation from:

- The *z/OS and Software Products DVD Collection* (SK3T-4271).
- The LookAt Web site (click **Download** and then select the platform, release, collection, and location that suit your needs). More information is available in the LOOKAT.ME files available during the download process.

Do You Have Problems, Comments, or Suggestions?

Your suggestions and ideas can contribute to the quality and the usability of this document. If you have problems using this document, or if you have suggestions for improving it, complete and mail the Reader's Comment Form found at the back of the document.

Summary of Changes

Summary of changes for SA22-7523-14 z/OS Version 1 Release 11

This document contains information previously presented in *z/OS ICSF Messages*, SA22-7523-13, which supports z/OS Version 1 Release 11.

This document is for ICSF FMID HCR7780. This release of ICSF runs on z/OS V1R9, z/OS V1R10, and z/OS V1R11 and only on zSeries hardware.

New information

- CSFG0866
- CSFM050I
- CSFM051E
- CSFM130I
- CSFM420E
- CSFM530I
- CSFM531I
- CSFM614I
- CSFO0236
- CSFV0560

Deleted information

- CSFC0254
- CSFC0266
- CSFC0294

Summary of changes for SA22-7523-13 z/OS Version 1 Release 11

This document contains information previously presented in *z/OS ICSF Messages*, SA22-7523-12, which supports z/OS Version 1 Release 10.

This document is for ICSF FMID HCR7770. This release of ICSF runs on z/OS V1R7, z/OS V1R8, z/OS V1R9, z/OS V1R10, and z/OS V1R11 and only on zSeries hardware.

New information

- CSFC0226
- CSFC0276
- CSFM013I
- CSFM014I
- CSFM015I
- CSFM016I
- CSFM022E
- CSFM108I

- CSFM109I
- CSFM110I
- CSFM111I
- CSFM307E
- CSFM308I
- CSFM612I
- CSFO0220
- CSFO0230

Changed information

- CSFC0156
- CSFM012I
- CSFM119E
- CSFM123E
- CSFM124I
- CSFM129I
- CSFM419E
- CSFM611I
- CSFM613I
- Build Control Statement Processing messages, which used to be sent to the CSFDIAG data set, are now sent to the ICSF job log.
- Cryptographic Key Data Set Processing messages, which used to be sent to the CSFDIAG or CSFVRPT data sets, are now sent to the ICSF job log.
- Exit Router messages, which used to be sent to the CSFLIST data set, are now sent to the ICSF job log.
- Installation Option Parameter Messages, which used to be sent to the CSFLIST data set, are now sent to the ICSF job log.
- CKDS Conversion Processing messages, which used to be sent to the CSFVRPT data set, are now sent to the ICSF job log.
- I/O Errors, which used to be sent to the CSFDIAG or CSFVRPT data sets, are now sent to the ICSF job log.

Deleted information

- CSFC0246
- CSFG0385
- CSFG0534
- CSFG0725
- CSFG0846
- CSFH0004I
- CSFH0005E
- CSFI001E
- CSFO0086
- CSFO0116
- CSFO0186
- CSFV0066
- CSFV0402
- CSFY0016

- CSFY0046
- CSFY0066

In addition, the following messages are no longer issued. The information for these messages has been modified to reflect this.

- CSFM005A
- CSFM008I
- CSFM010E
- CSFM020I
- CSFM021I
- CSFM403I
- CSFM406A
- CSFM407A
- CSFM431I
- CSFM432I
- CSFM433E
- CSFM434E
- CSFM435I
- CSFM436I
- CSFM437E
- CSFM438I
- CSFM441I
- CSFM452I
- CSFM601I
- CSFM605I
- CSFM606I
- CSFM609I

**Summary of changes
for SA22-7523-012
z/OS Version 1 Release 10**

The document contains information previously presented in *z/OS ICSF Messages*, SA22-7523-11, which supports z/OS Version 1 Release 9.

This release of ICSF, HCR7751, runs on z/OS V1R7, V1R8 and V1R9 and only on zSeries hardware.

New information

- CSFC0294
- CSFC0306
- CSFC0322
- CSFG0791
- CSFG0804
- CSFG0814
- CSFG0824
- CSFG0834
- CSFG0846

- CSFG0856
- CSFH001I
- CSFH002I
- CSFH003E
- CSFH004I
- CSFH005E
- CSFM123E
- CSFM124I
- CSFM125I
- CSFM126I
- CSFM127I
- CSFM128E
- CSFM129I
- CSFM314E
- CSFM315I
- CSFM606I
- CSFM607I
- CSFM608I
- CSFM609I
- CSFM610I
- CSFM611I
- CSFO0212
- CSFU001I
- CSFU002I

Changed information

- CSFG0002
- CSFG0534
- CSFG0725
- CSFM400I
- CSFM406I
- CSFM407A
- CSFM431I
- CSFM434E

**Summary of changes
for SA22-7523-011
z/OS Version 1 Release 9**

The document contains information previously presented in *z/OS ICSF Messages*, SA22-7523-10, which supports z/OS Version 1 Release 9.

This release of ICSF, HCR7750, runs on z/OS V1R7, V1R8 and V1R9 and only on zSeries hardware.

Changed information

- CSFM122I

**Summary of changes
for SA22-7523-010
z/OS Version 1 Release 9**

The document contains information previously presented in *z/OS ICSF Messages*, SA22-7523-09, which supports z/OS Version 1 Release 9.

This release of ICSF, HCR7750, runs on z/OS V1R7, V1R8 and V1R9 and only on zSeries hardware.

New information

- CSFC0286
- CSFG0780
- CSFM122I

This document has been enabled for the following types of advanced searches in the online z/OS Library Center: examples, tasks, concepts, and references.

You may notice changes in the style and structure of some content in this document—for example, headings that use uppercase for the first letter of initial words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our documents.

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

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.

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.

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.

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) or public key data set (PKDS). 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.

User response: Contact your system programmer.

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

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.

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

System programmer response: Contact the IBM Support Center.

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.

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

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

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.

User response: Contact your system programmer.

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.

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.

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

If the problem persists, contact your system programmer.

System programmer response: Contact the IBM Support Center.

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.

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

If the problem persists, contact your system programmer.

System programmer response: Contact the IBM Support Center.

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.

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

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

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.

User response: Contact your system programmer.

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

CSFC0106 UNABLE TO RETRIEVE SYSTEM *keytype* RECORD.

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

System action: Processing ends.

User response: Contact your system programmer.

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.

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.

User response: Contact your system programmer.

System programmer response: Contact the IBM Support Center.

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, 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** *dsname*.

Explanation: The master key verification pattern *mkvp* for the CKDS record being updated didn't match the MKVP in the *dsname* 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, starting with HCR7750, the PKDS must have an LRECL of 3800.

System action: Processing continues.

User response: Contact your system programmer.

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.

CSFC0306 **PKDS FULL. NO UPDATES ALLOWED.**

Explanation: The PKDS data space for the in-storage copy is full.

System action: No updates to the PKDS will be allowed.

User response: Request security administrator to do a REFRESH of the PKDS. This increases the size of the data space for the PKDS.

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.

Chapter 4. CSFEnnn Messages (Exit Router)

Chapter 4, “CSFEnnn 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 or the cryptographic coprocessor is not active (CCF or PCIXCC/CEX2C).
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.

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.

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.

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.

User response: Contact your system programmer.

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.

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.

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

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

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*. *Keyword* values can be NOCV or DES. If NOCV is specified, only key types EXPORTER or IMPORTER are allowed. If DES is specified, only key types EXPORTER, IMPORTER, or DATA are allowed.

If *keytype* CLRDES 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 @server zSeries 990 and try to add a DATAxLAT key. You will get a return code of 8 and a reason code of 61.

User response: Contact your system programmer.

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.

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.

User response: Contact your system programmer.

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.

**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.

User response: Contact your system programmer.

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.

**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.

User response: Contact the programmer responsible for the exit.

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.

**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.

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

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.

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.

User response: Contact your system programmer.

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

CSFG0604 DOUBLE LENGTH KEY VALUE IS NOT VALID FOR KEY TYPE *type*.

Explanation: The control statement specifies KEY(key_value,ikey_value), but TYPE specifies a short key type that can accept only KEY(key_value).

System action: Processing ends.

User response: Correct the KGUP statement.

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 ON THE CKDS FOR TYPE *type1*. Function NOT PERFORMED BECAUSE TYPE *type2* REQUIRES A 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 <LABELTYPE> 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.

User response: Contact your system programmer.

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

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 DATA, 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 can not 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 can not 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.

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 keys 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.

Chapter 7. CSFIxxxx Messages (Component Trace)

Chapter 7, “CSFIxxxx 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 (IPCSPRINT).

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.

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.

CSFM005A ICSF TERMINATING. PREREQUISITE SOFTWARE IS NOT INSTALLED.

Explanation: This message is no longer issued.

System action: None.

Operator response: None.

System programmer response: None.

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.

CSFM008I AN ABEND OCCURRED IN THE ICSF MAINLINE. PSW = *psw*, abend code = *abend-code*, reason = *rsncode*.

Explanation: This message is no longer issued.

System action: None.

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 the classes CSFSERV and/or CSFKEYS during initialization.

System action: Processing continues.

Operator response: Inform system programmer.

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.

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 and CSFKEYS classes have been defined for ICSF).

CSFM010E ICSF TERMINATING. PROCESSOR IS UNSUPPORTED.

Explanation: This message is no longer issued.

System action: None.

Operator response: None.

System programmer response: None.

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

PKCS11 service functions that require CRYPTOZ processing are disabled.

- Persistent (TKDS) PKCS11 objects are not available
- FIPS compatibility mode reverts to FIPS standard mode.

Operator response: Inform your system programmer.

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.

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 RACLSTed.

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: The ICSF installation option FIPSMODE(YES,FAIL(NO)) or FIPSMODE(COMPAT,FAIL(NO)) has been specified, indicating that the z/OS PKCS #11 services must operate in compliance with FIPS 140-2. As a part of this 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 initialization continues, but FIPSMODE mode is disabled.

System programmer response: Contact the IBM Support Center.

CSFM015I FIPS 140 SELF CHECKS FOR PKCS11 SERVICES SUCCESSFUL.

Explanation: The ICSF installation option FIPSMODE(YES,FAIL(*fail-option*)) or FIPSMODE(COMPAT,FAIL(*fail-option*)) has been specified, indicating that the z/OS PKCS #11 services must operate in compliance with FIPS 140-2. As a part of this compliance, the ICSF z/OS PKCS #11 software services must perform a series of self tests. 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 system z model type or the version/release of z/OS that is running on it does not support FIPS. The supported model types are: z890/z990 and newer. The supported z/OS versions/releases are V1R10 and higher.

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

System programmer response: None

**CSFM020I AN ABEND OCCURRED IN CSFMLFDT.
PSW *psw* COMPLETION CODE
abend-code, REASON = *rsncode*.**

Explanation: This message is no longer issued.

System action: None.

System programmer response: None.

**CSFM021I CSFMLFDT WAS UNABLE TO
ESTABLISH RECOVERY. RETURN
CODE *return-code* FROM THE ESTAE
MACRO.**

Explanation: This message is no longer issued.

System action: None

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, G (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 authentication 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 hash 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.

CSFM105E CRYPTOGRAPHY - DOMAIN '*domain*' IS NOT ACCESSIBLE.

Explanation: The value of the DOMAIN parameter in the installation options file has specified a cryptographic domain that this operating system cannot access. Either the number was incorrect, or the PR/SM definition tables do not allow access.

For more information about the number of domains that your processor supports, see either the *S/390 PR/SM Planning Guide* or the *IBM ES/9000 and ES/3090 Processor Complex PR/SM Planning Guide*.

System action: ICSF ends.

Operator response: Contact your system programmer.

System programmer response: Ensure that the specified DOMAIN is valid for your processor. If you are running in logically partitioned (LPAR) mode, ensure that the DOMAIN has been assigned to your LPAR mode. If neither of these conditions resolve the problem, contact the IBM Support Center.

CSFM106A CRYPTOGRAPHY - PKA MASTER KEYS ARE NOT VALID.

Explanation: One or both of the PKA master keys are not valid. This occurs if a PKA master key is not installed in all cryptographic units, or if the PKA master keys on all the cryptographic units are not the same. It is normal to see this message the first time ICSF starts.

System action: Processing continues, but PKA callable services are not enabled.

Operator response: Notify your security administrator to install the PKA master keys.

System programmer response: None.

CSFM107E CRYPTOGRAPHY - CRYPTO UNITS CONFIGURED DIFFERENTLY.

Explanation: The Cryptographic Configuration Control (CCC) installed on the cryptographic units is not the same. The Processor Controller installs the CCC from the Cryptographic Configuration diskette.

System action: ICSF abends.

Operator response: Notify your system programmer.

System programmer response: Verify that the correct Cryptographic Configuration diskettes were used to initialize the cryptographic units and that the Processor Controller initialization completed successfully. If the diskettes are incorrect, contact IBM.

**CSFM108I CRYPTOGRAPHIC FEATURE IS BUSY.
coprocessor-name cii, SERIAL NUMBER
nnnnnnn.**

Explanation: A 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. The substitution variables are:

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
 - CRYPTO EXPRESS2 COPROCESSOR
 - CRYPTO EXPRESS2 ACCELERATOR
 - CRYPTO EXPRESS3 COPROCESSOR
 - CRYPTO EXPRESS3 ACCELERATOR
- *c* - the short name for the coprocessor type. Possible values are:
 - E (representing a CEX2C)
 - F (representing a CEX2A)
 - G (representing a CEX3C)
 - H (representing a CEX3A)
- *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 retry the cryptographic feature until it is no longer busy.

Operator response: None

System programmer response: None

CSFM109I CRYPTOGRAPHIC FEATURE IS OFFLINE. *coprocessor-name cij*, **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 COPROCESSOR
 - CRYPTO EXPRESS2 ACCELERATOR
 - CRYPTO EXPRESS3 COPROCESSOR
 - CRYPTO EXPRESS3 ACCELERATOR
- *c* - the short name for the coprocessor type. Possible values are:
 - E (representing a CEX2C)
 - F (representing a CEX2A)
 - G (representing a CEX3C)
 - H (representing a CEX3A)
- *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.

CSFM110I CRYPTOGRAPHIC FEATURE FAILED. *coprocessor-name cij*, **SERIAL NUMBER** *nnnnnnn*.

Explanation: The cryptographic feature failed. The substitution variables are:

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
 - CRYPTO EXPRESS2 COPROCESSOR
 - CRYPTO EXPRESS2 ACCELERATOR
 - CRYPTO EXPRESS3 COPROCESSOR
 - CRYPTO EXPRESS3 ACCELERATOR
- *c* - the short name for the coprocessor type. Possible values are:
 - E (representing a CEX2C)
 - F (representing a CEX2A)
 - G (representing a CEX3C)
 - H (representing a CEX3A)
- *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 removed or replaced by your IBM customer engineer.

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

Explanation: The cryptographic feature is online and operational. When the Cryptographic feature is a coprocessor, the ACTIVE message indicates that the symmetric master key is set and ICSF services requiring the use of a symmetric master key may be used. The substitution variables are:

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
 - CRYPTO EXPRESS2 COPROCESSOR
 - CRYPTO EXPRESS2 ACCELERATOR
 - CRYPTO EXPRESS3 COPROCESSOR
 - CRYPTO EXPRESS3 ACCELERATOR
- *c* - the short name for the coprocessor type. Possible values are:
 - E (representing a CEX2C)
 - F (representing a CEX2A)
 - G (representing a CEX3C)
 - H (representing a CEX3A)
- *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

CSFM113E CRYPTOGRAPHY - *cryptographic_module_id* **MODULE NOT INITIALIZED.**

Explanation: The cryptographic module that the message identifies has not been initialized.

System action: If neither cryptographic module has been initialized, then ICSF ends; no cryptographic function is possible. If either cryptographic module has been successfully initialized, ICSF continues initialization processing.

Operator response: Notify your system programmer.

System programmer response: The Service Processor needs to initialize the cryptographic module

from a diskette. Use the cryptographic module identifier in the message to identify the correct diskette to use. The restart ICSF.

CSFM114E CRYPTOGRAPHY - ALL ASYNCHRONOUS COPROCESSORS NOT AVAILABLE.

Explanation: The processing that is required to pass work to the asynchronous coprocessor is not available.

System action: Processing continues, but services that are using the asynchronous coprocessor will not function.

Operator response: Notify your system programmer.

System programmer response: Check that the proper domain is specified in the Installation Options Data Set. The domain must agree with the PR/SM usage domain specification. If you cannot resolve the problem, contact the IBM Support Center.

CSFM115E CRYPTOGRAPHY - *cryptographic_module_id* RANDOM NUMBER GENERATOR NOT INITIALIZED.

Explanation: The random number generator of the cryptographic module that the message identifies has not been initialized.

System action: This is most likely a hardware error. If the random number generator has not been initialized on either cryptographic module, ICSF ends; no cryptographic function is possible. If the random number generator on either cryptographic module has been successfully initialized, ICSF continues the initialization processing.

Operator response: Notify your system programmer.

System programmer response: Contact the IBM Support Center.

CSFM116I BOTH MASTER KEYS CORRECT ON PCI CRYPTOGRAPHIC COPROCESSOR *Ppp*, SERIAL NUMBER *nn-nnnn*.

Explanation: The PCI cryptographic coprocessor with serial number *nn-nnnn* is online and operational. It is installed at position *pp*.

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

CSFM117I PCI CRYPTOGRAPHIC COPROCESSOR *Ppp*, SERIAL NUMBER *nn-nnnn*, OFFLINE.

Explanation: The PCI cryptographic coprocessor with serial number *nn-nnnn* is offline and cannot be used for any operation. It is installed at position *pp*.

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

System programmer response: Have the PCI cryptographic coprocessor brought online.

CSFM118E PCI CRYPTOGRAPHIC COPROCESSOR *Ppp*, SERIAL NUMBER *nn-nnnn*, FAILED.

Explanation: The PCI cryptographic coprocessor with serial number *nn-nnnn*, installed at position *pp*, has failed and cannot be used for any operation.

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

System programmer response: Have the PCI cryptographic coprocessor removed or replaced by your IBM Customer Engineer.

CSFM119E INCORRECT MASTER KEY (*mk*) ON PCI CRYPTOGRAPHIC COPROCESSOR *Ppp*, SERIAL NUMBER *nnnnnnn*.

Explanation: The PCI cryptographic coprocessor with serial number *nnnnnnn*, installed at position *pp*, 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 variable *mk* will specify either SYM-MK or ASYM-MK or BOTH. This message may be issued at initialization or when a new PCI cryptographic coprocessor unit comes online.

System action: The system will not use the PCI cryptographic coprocessor for cryptographic operations until the security administrator changes its master key.

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

CSFM120E PUBLIC KEY SECURE CABLE (PKSC) FACILITY IS NOT ENABLED.

Explanation: There are several functions that must be enabled on the PR/SM definition. They are Enable cryptographic functions and Enable public key secure cable (PKSC) and integrated cryptographic service facility (ICSF). These boxes must be checked on the Crypto page of **Customize/Delete Activation Profiles**. *These options are selected on the Support Element panels.*

See *PR/SM Planning Guide*.

System action: ICSF ends.

Operator response: Contact your system programmer.

System programmer response: Update the PR/SM panels and restart ICSF.

CSFM121E CRYPTO MODULES HAVE NOT BEEN INITIALIZED.

Explanation: The Cryptographic Configuration Control (CCC) has not been installed on the cryptographic units. The Processor Controller installs the CCC from the Cryptographic Configuration diskettes.

System action: ICSF terminates.

Operator response: Notify your system programmer.

System programmer response: Ensure the Processor Controller installation of the CCC is successful.

CSFM122I PKA SERVICES WERE NOT ENABLED DURING ICSF INITIALIZATION.

Explanation: This message is issued during ICSF initialization and indicates PKA services (RSA services) were not enabled. There are multiple reasons why ICSF would not have enabled PKA services. Not having an RSA Master Key set on the cryptographic coprocessor or having an RSA Master Key on the cryptographic coprocessor which does not match the RSA Master Key hash pattern in the PKDS header record are possibilities. Once PKA services are enabled, this message is no longer highlighted and the message is allowed to scroll.

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 hash pattern. Manually enable PKA services 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, RSA, or ECC.
- *coprocessor-name* - the type of cryptographic coprocessor. May have the value:
 - CRYPTO EXPRESS2 COPROCESSOR
 - CRYPTO EXPRESS3 COPROCESSOR
- *c* - the short name for the coprocessor type. May have the value:
 - E (representing a CEX2C)
 - G (representing a CEX3C)

- *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 first master key that is determined to be in error.

System action: When a master key is incorrect, then the cryptographic coprocessor may not be used for operations with the master key 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, RSA, or ECC.
- *coprocessor-name* - the type of cryptographic coprocessor. May have the value:
 - CRYPTO EXPRESS2 COPROCESSOR
 - CRYPTO EXPRESS3 COPROCESSOR
- *c* - the short name for the coprocessor type. May have the value:
 - E (representing a CEX2C)
 - G (representing a CEX3C)
- *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 first 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.

CSFM125I CRYPTOGRAPHY - LIMITED CPU-BASED SERVICES ARE AVAILABLE.

Explanation: This is an informational message. ICSF is up and remains started. Only SHA-1 and SHA-2 services are available. The DES CPACF feature code is not enabled.

System action: Processing continues.

Operator response: None.

System programmer response: None.

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. This support is available on z890, z990, z9 BC, z9 EC, z10 EC, z10 BC, and z196.

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. Secure AES key services are available if you are on a z9 BC, z9 EC, z10 EC, z10 BC, or z196.

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. There are several reasons for this occurring.

1. Some of the keys required by this system are missing from the CKDS. This can occur when a CKDS is initialized on a system that requires fewer system keys. For a z900 or z800 system, the CKDS must be initialized on a z900 or z800.
2. 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, RSA, or ECC.
- *coprocessor-name* - the type of cryptographic coprocessor. May have the value:
 - CRYPTO EXPRESS2 COPROCESSOR
 - CRYPTO EXPRESS3 COPROCESSOR
- *c* - the short name for the coprocessor type. May have the value:
 - E (representing a CEX2C)
 - G (representing a CEX3C)
- *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.

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.

CSFM224I PCI CRYPTOGRAPHIC COPROCESSOR
Ppp, SERIAL NUMBER nn-nnnn, BUSY.

Explanation: This state may occur when the PCI cryptographic coprocessor is first brought online and is going through power-on reset. The PCI cryptographic coprocessor may also be in this state when new licensed internal code is being loaded or when the unit is going through recovery processing.

System action: The system will retry the PCI cryptographic coprocessor until it is no longer busy.

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.

CSFM302A TIMED OUT WAITING FOR RESOURCE
SYSZCKDS.*ckdsdsn*. CKDS UPDATE
FAILED.

Explanation: The CKDS I/O subtask timed out waiting for an exclusive ENQ on the SYSZCKDS.*ckdsdsn* resource. At least one member of the ICSF sysplex group has not relinquished its ENQ on the resource.

System action: ICSF processing will continue. The CKDS update operation will be failed with return code 12, reason code 3005 (X'BBD').

Operator response: The operator should issue D GRS,RES=*nnnnn* from the message to determine which system(s) hold the resource. The operator should determine if action should be taken to cause the holding system to release its ENQ on the CKDS resource.

nnnnn

The CKDS resource name.

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.

CSFM305A TIMED OUT WAITING FOR RESOURCE SYSZTKDS.tkdsdsn. TKDS UPDATE FAILED.

Explanation: The TKDS I/O subtask timed out waiting for an exclusive ENQ on the *SYSZTKDS.tkdsdsn* resource. At least one member of the ICSF sysplex group has not relinquished its ENQ on the resource.

System action: ICSF processing will continue. The TKDS update operation will be failed with return code 12, reason code 3005 (X'BBD').

Operator response: The operator should issue D GRS,RES=(*,nnnnn) (where nnnn is the TKDS resource name from the message) to determine which system or systems hold the resource. Then the operator should determine if action should be taken to cause the holding system to release its ENQ on the TKDS resource.

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 PKDS 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.

CSFM315I TIMED OUT WAITING FOR RESOURCE SYSZPKDS.pkdsdsn. PKDS UPDATE FAILED.

Explanation: The PKDS I/O subtask timed out waiting for an exclusive ENQ on the *SYSZPKDS.pkdsdsn* resource. At least one member of the ICSF sysplex group has not relinquished its ENQ on the resource.

System action: ICSF processing will continue. The PKDS update operation will be failed with return code 12, reason code 3005 (X'BBD').

Operator response: The operator should issue D GRS,RES=(*,nnnnn) (where *nnnn* is the PKDS resource

name from the message) to determine if a system or systems hold the resource. Then the operator should determine if action should be taken to cause the holding system to release its ENQ on the PKDS resource.

System programmer response: None.

CSFM400I CRYPTOGRAPHY - SERVICES ARE NOW AVAILABLE.

Explanation: This is an informational message. ICSF is up and remains started. 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 unit is no longer possible. For example, the last unit 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.

CSFM403I CSFMIOST WAS UNABLE TO ESTABLISH RECOVERY. RETURN CODE *return_code* FROM THE ESTAE MACRO.

Explanation: This message is no longer issued.

System action: None.

User response: None.

System programmer response: None.

CSFM404A PKA HASH PATTERN IN PKDS HEADER RECORD DOES NOT MATCH SYSTEM PKA HASH PATTERN.

Explanation: The PKA Hash Pattern, which is part of the PKDS header record, does not match the PKA Hash Pattern currently in use by ICSF. This can occur if the PKA master keys are changed and ICSF is ended before writing any PKDS records. In this situation, the PKDS header record is not updated. When ICSF is restarted it detects a mismatch in the PKDS header record. This can also occur if the PKDS being used is not associated with the ICSF being started or the PKDS is back level or empty.

System action: ICSF continues the initialization process, but marks the PKDS services as unavailable.

User response: None.

System programmer response: If the PKDS is usable, use the ICSF panels to invoke the User Control functions and enable PKDS Read Access and PKDS Write, Create, and Delete Access. If the PKDS is unusable, correct the condition (if possible), stop ICSF, and restart with appropriate or fixed PKDS.

CSFM405A AUTHENTICATION CODE IN PKDS HEADER RECORD DOES NOT MATCH COMPUTED VALUE.

Explanation: The authentication code is a hash value computed using all the data in the record. It is stored in the header record when it is written, and is used as an integrity check. Subsequently, when ICSF read the record and recomputed the authentication code, it did not match the one in the record. This may mean that the record has been altered since it was written to the PKDS.

If the PKDS is empty when you start ICSF, it is normal to see this message. This message will no longer appear at start up once you have written to the PKDS.

System action: ICSF continues the initialization process, but marks the PKDS services as unavailable.

User response: None.

System programmer response: If the PKDS is usable, use the ICSF panels to invoke the User Control functions and chose the options to allow PKDS Read Access and PKDS Write, Create, and Delete Access. If the PKDS is unusable, correct the condition (if possible), stop ICSF, and restart with fixed PKDS.

CSFM406A UNEXPECTED ERROR PROCESSING PKDS HEADER RECORD. FUNCTION = *function*, RETURN CODE = *rc*, REASON CODE = *rs*.

Explanation: This message is no longer issued.

System action: None.

User response: None.

System programmer response: None.

CSFM407A PKDS *dsname* IS UNAVAILABLE.

Explanation: This message is no longer issued.

System action: None.

User response: None.

System programmer response: None.

**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.

System action: ICSF ends.

Operator response: Contact your system programmer.

System programmer response: Add the Domain parameter to the options data set 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.

**CSFM411I PCI CRYPTOGRAPHIC ACCELERATOR
Aaa IS ACTIVE**

Explanation: The PCI cryptographic accelerator is online and operational. It is installed at position *aa*.

System action: The system will use the PCI cryptographic accelerator.

**CSFM412I PCI CRYPTOGRAPHIC ACCELERATOR
Aaa IS OFFLINE**

Explanation: The PCI cryptographic accelerator is offline. It is installed at position *aa*.

System action: The system will not use the PCI cryptographic accelerator.

System programmer response: Have the PCI cryptographic accelerator brought online.

**CSFM413E PCI CRYPTOGRAPHIC ACCELERATOR
Aaa FAILED**

Explanation: The PCI cryptographic accelerator installed at position *Aaa* has failed.

System action: The system will not use the PCI cryptographic accelerator.

System programmer response: Have the PCI cryptographic accelerator removed or replaced by your IBM Customer Engineer.

**CSFM414I PCI CRYPTOGRAPHIC ACCELERATOR
Aaa IS BUSY**

Explanation: This state may occur when the PCI cryptographic accelerator is first brought online and is going through power-on reset. The PCI cryptographic accelerator may also be in this state when new licensed internal code is being loaded or when the unit is going through recovery processing.

System action: The system will retry the PCI cryptographic accelerator until it is no longer busy.

**CSFM416I BOTH MASTER KEYS CORRECT ON
PCI X CRYPTOGRAPHIC
COPROCESSOR *Xpp*, SERIAL NUMBER
nnnnnnn.**

Explanation: The PCI X Cryptographic Coprocessor with serial number *nnnnnnn* is online and operational. It is installed at position *pp*.

System action: The system will use the PCI X Cryptographic Coprocessor for cryptographic operations

Operator response: None

System programmer response: None

**CSFM417I PCI X CRYPTOGRAPHIC
COPROCESSOR *Xpp*, SERIAL NUMBER
nnnnnnn, OFFLINE**

Explanation: The PCI X Cryptographic Coprocessor with serial number *nnnnnnn* is offline and cannot be used for any operation. It is installed at position *pp*.

System action: The system will not use the PCI X Cryptographic Coprocessor for cryptographic operations

Operator response: None

System programmer response: Have the PCI X Cryptographic Coprocessor brought online.

**CSFM418E PCI X CRYPTOGRAPHIC
COPROCESSOR *Xpp*, SERIAL NUMBER
nnnnnnn, FAILED**

Explanation: The PCI X Cryptographic Coprocessor with serial number *nnnnnnn* has failed and cannot be used for any operation. It is installed at position *pp*.

System action: The system will not use the PCI X Cryptographic Coprocessor for cryptographic operations

Operator response: None

System programmer response: Have the PCI X Cryptographic Coprocessor removed or replaced by your IBM customer engineer.

CSFM419E INCORRECT MASTER KEY (*mk*) ON PCI X CRYPTOGRAPHIC COPROCESSOR *Xpp*, SERIAL NUMBER *nnnnnnn*.

Explanation: The PCI X Cryptographic Coprocessor with serial number *nnnnnnn*, installed at position *pp*, 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 variable *mk* will specify SYM, ASYM, or BOTH. This message may be issued at initialization or when a new cryptographic coprocessor unit comes online.

System action: If the SYM-MK is valid, then the PCI X Cryptographic Coprocessor may be used for DES operations, else the system will not use the PCI X Cryptographic Coprocessor for cryptographic operations until the security administrator has changed its master keys.

Operator response: None

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

CSFM420E PKDS NOT USABLE ON THIS SYSTEM - ECC ONLY MK

Explanation: The PKDS contains only an ECC MKVP. The header record of the PKDS has been checked and only an ECC MKVP was found. The valid states are: no MKHP/MKVPs, both RSA MKHP and ECC MKVPs, or only an RSA MKHP. The PKDS specified for this system must be changed to match one of the valid states. This message is issued at initialization.

System action: ICSF ends.

Operator response: Notify the security administrator. The PKDS must be changed or modified for use on this system.

System programmer response: None

CSFM424I PCI X CRYPTOGRAPHIC COPROCESSOR *Xpp*, SERIAL NUMBER *nnnnnnn*, BUSY.

Explanation: This state may occur when the PCI X Cryptographic Coprocessor is first brought online and is going through power-on reset. The PCI X Cryptographic Coprocessor may also be in this state when new licensed internal code is being loaded or when the unit is going through recovery processing.

System action: The system will retry the PCI X Cryptographic Coprocessor until it is no longer busy.

Operator response: None

System programmer response: None

CSFM430I CRYPTO EXPRESS2 COPROCESSOR *Epp*, SERIAL NUMBER *nnnnnnn*, IS BUSY.

Explanation: This message is no longer issued.

System action: None

Operator response: None

System programmer response: None

CSFM431I BOTH MASTER KEYS CORRECT ON CRYPTO EXPRESS2 COPROCESSOR *Epp*, SERIAL NUMBER *nnnnnnn*.

Explanation: This message is no longer issued.

System action: None.

Operator response: None

System programmer response: None

CSFM432I CRYPTO EXPRESS2 COPROCESSOR *Epp*, SERIAL NUMBER *nnnnnnn*, OFFLINE.

Explanation: This message is no longer issued.

System action: None.

Operator response: None.

System programmer response: None.

CSFM433E CRYPTO EXPRESS2 COPROCESSOR *Epp*, SERIAL NUMBER *nnnnnnn*, FAILED.

Explanation: This message is no longer issued.

System action: None.

Operator response: None

System programmer response: None.

CSFM434E INCORRECT MASTER KEY *mk* ON CRYPTO EXPRESS2 COPROCESSOR *Epp*, SERIAL NUMBER *nnnnnnn*.

Explanation: This message is no longer issued.

System action: None.

Operator response: None

System programmer response: None.

**CSFM435I CRYPTO EXPRESS2 ACCELERATOR
F&index. IS ACTIVE.**

Explanation: This message is no longer issued.

System action: None.

Operator response: None.

System programmer response: None.

**CSFM436I CRYPTO EXPRESS2 ACCELERATOR
F&index. IS OFFLINE.**

Explanation: This message is no longer issued.

System action: None

Operator response: None.

System programmer response: None.

**CSFM437E CRYPTO EXPRESS2 ACCELERATOR
F&index. FAILED.**

Explanation: This message is no longer issued.

System action: None.

Operator response: None.

System programmer response: None.

**CSFM438I CRYPTO EXPRESS2 ACCELERATOR
F&index. IS BUSY.**

Explanation: This message is no longer issued.

System action: None.

Operator response: None.

System programmer response: None.

**CSFM440I PCI X CRYPTOGRAPHIC
COPROCESSOR X_{pp}, SERIAL NUMBER
nnnnnnnn, ACTIVE.**

Explanation: The symmetric-keys master key has been set on PCI X Cryptographic Coprocessor with serial number *nnnnnnnn*. The coprocessor is able to process service requests for services requiring the symmetric-keys master key.

System action: The system will use the PCI X Cryptographic Coprocessor for cryptographic operations.

Operator response: None.

System programmer response: None.

**CSFM441I CRYPTO EXPRESS2 COPROCESSOR
E_{pp}, SERIAL NUMBER nnnnnnnn,
ACTIVE.**

Explanation: This message is no longer issued.

System action: None.

Operator response: None.

System programmer response: None.

**CSFM450E UNEXPECTED ERROR PROCESSING
kds, RETURN CODE = xxxx, REASON
CODE = yyyy.**

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: A cryptographic coprocessor is checkstopped and cannot be used for any operation. It is installed at position *pp*.

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

Operator response: None.

System programmer response: Have the cryptographic coprocessor removed or replaced by your IBM customer engineer.

**CSFM452I CSFMIOTT WAS UNABLE TO
ESTABLISH RECOVERY. RETURN
CODE &RC. FROM THE ESTAE
MACRO.**

Explanation: This message is no longer issued.

System action: None.

Operator response: None.

System programmer response: None.

CSFM501E CRYPTOGRAPHY - HARDWARE FAILURE ON COPROCESSOR
coprocessor-id, CPU cpu-id.

Explanation: A cryptographic instruction has ended, indicating a cryptographic hardware failure. ICSF disables the failing CPU for cryptographic operations. An SMF82 record is written.

System action: The CPU is disabled for cryptography.

Operator response: Contact your system programmer.

System programmer response: Contact the IBM Support Center.

CSFM503E CRYPTOGRAPHY - TAMPERING DETECTED ON COPROCESSOR
coprocessor-id, CPU cpu-id.

Explanation: A tamper condition occurred. The cryptographic feature has zeroed the master key registers in the indicated *coprocessor-id* and *cpu-id*.

System action: The CPU alarm sounds. The CPU is disabled for cryptography. ICSF generates an SMF type 82 record.

Operator response: See *S/390 Support Element Operations Guide*.

System programmer response: Contact the IBM Support Center.

CSFM504E CRYPTOGRAPHY - THERE ARE NO ONLINE CPUS WITH ACCESS TO A COPROCESSOR.

Explanation: A sequence of error messages has resulted in the disabling of all cryptographic CPUs.

System action: The CPU is disabled for cryptographic services. They will be restored when at least one CPU is made available for cryptographic functions.

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

If you cannot resolve the problem, contact the IBM Support Center.

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 continues processing. The system will not be able to use a PCI X Cryptographic Coprocessor or Crypto Express2

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.

CSFM510E CRYPTOGRAPHY - VERIFICATION FAILED ON COPROCESSOR
coprocessor-id, CPU cpu-id.

Explanation: The master key authentication pattern is not valid.

System action: The CPU is disabled for cryptography.

Operator response: Contact your system programmer.

System programmer response: Ensure that the CKDS is valid for the master key that is installed for that CPU.

CSFM511E CRYPTOGRAPHY - MASTER KEY ON COPROCESSOR
coprocessor-id, CPU cpu-id IS NOT VALID.

Explanation: The cryptographic unit has a zero master key.

System action: The CPU is disabled for cryptography.

System programmer response: Determine why the master key is zeroed. You need to re-install the correct key before using the CPU for cryptographic services. If you cannot resolve the problem, contact the IBM Support Center. It is normal to see this message the first time ICSF starts.

CSFM512E CRYPTOGRAPHY - PKA MASTER KEYS ON COPROCESSOR
coprocessor-id ARE NOT VALID.

Explanation: A new cryptographic unit has come online, but the PKA master key is not valid or does not agree with the PKA master key of the cryptographic unit already online.

System action: Processing continues, but PKA callable services are not enabled on the new unit.

Operator response: Notify your security administrator to install the correct PKA master key on the new unit.

System programmer response: None.

CSFM522E CRYPTOGRAPHY - COPROCESSOR
coprocessor-id, CPU cpu-id IS DISABLED.

Explanation: Cryptographic functions are disabled in the Environment Control Mask (ECM). This can only be done from the TKE workstation.

System action: The CPU is disabled for cryptography.

System programmer response: Enable cryptographic functions for the cryptographic unit in the ECM using the TKE workstation.

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

Explanation: ICSF initialization determined that system conditions were sufficient for operating with the cryptographic accelerator and coprocessor I/O interrupt capability, and therefore enabled this functionality. The substitution variables are:

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

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

System programmer response: None.

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

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, G (representing a CEX3C).
- *ii* - the index or position where the cryptographic coprocessor is installed.
- *nnnnnnnn* - 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.

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.

**CSFM601I CONNECTION DISABLED TO ICSF
SYSPLEX GROUP *group_name*,
MEMBER *member_name*.**

Explanation: This message is no longer issued.

System action: None.

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.

**CSFM605I SYSTEM &*sys*. NOT IN MULTI-SYSTEM
SYSPLEX. ICSF CROSS-SYSTEM
SERVICES ENVIRONMENT NOT
ESTABLISHED.**

Explanation: This message is no longer issued.

System action: None.

CSFM606I **ICXMSGO FAILURE BROADCASTING MESSAGE TO GROUP** *sysplex-group*
RETURN CODE = *return_code*, **REASON CODE =** *reason_code*.

Explanation: This message is no longer issued.

System action: None.

Operator response: None.

System programmer response: None.

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

Explanation: None of the key policy controls that activate the key policy for the specified key-data-store are defined. Possible key-data-stores 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-store KEY STORE POLICY IS DEFINED.**

Explanation: One or more of the key policy controls that activate the key policy for the specified key-datastore is defined. Possible key-data-stores 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.

CSFM609I **IXCMSGI FAILURE RECEIVING MESSAGE FROM GROUP** *group*.
RETURN CODE = *return_code*. **REASON CODE =** *reason_code*.

Explanation: This message is no longer issued.

System action: None.

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.

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.

User response: Contact your system programmer.

System programmer response: Check other messages. If you cannot correct the error, contact the IBM Support Center.

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.

User response: Contact your system programmer.

System programmer response: Ensure that the Wait List file specified in the Installation Options data set is valid.

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.

User response: Contact your system programmer.

System programmer response: Check for other messages. If you cannot correct the error, contact the IBM Support Center.

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.

User response: Contact your system programmer.

System programmer response: Ensure that the Wait List file specified in the Installation Options data set is valid.

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.

User response: Contact your system programmer.

System programmer response: Check other messages. If you cannot correct the error, contact the IBM Support Center.

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.

User response: Contact your system programmer.

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.

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.

User response: Contact your system programmer.

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*.

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.

User response: Contact your system programmer.

System programmer response: Ensure that the options data set contains a statement with the PKDSN keyword and its value, and restart ICSF.

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 PKCS11 processing is possible and the SYSPLEXTKDS option will have no effect.

System action: Processing ends.

User response: Contact your system programmer.

System programmer response: Ensure that the SYSPLEXTKDS option is specified with the TKDSN option in the installations options data set or no PKCS11 processing is possible and the SYSPLEXTKDS option will have no effect.

- | 3. There was not matching BEGIN(FMID) for an END.
- | **System action:** Processing ends.
- | **User response:** Contact your system programmer.
- | **System programmer response:** Check the syntax of the option statements.

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*.

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.

User response: Contact your system programmer.

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.

Chapter 11. CSFUxxxx Messages (ICSF Utility Processing)

Chapter 11, “CSFUxxxx Messages (ICSF Utility Processing)” 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 *kwclass* NOT SPECIFIED.

Explanation: After parsing all options, no keyword from the class *kwclass* was provided.

System action: Processing ends.

System programmer response: options provided to the utility. Make the necessary corrections and run the job again.

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: <ul style="list-style-type: none"> • READ • READUP • WRITE • REWRITE
6008	A service routine failed. ICSF sets the reason code after issuing message CSFG0293. The service routines are: <ul style="list-style-type: none"> • 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.	9040	An override entry consists of all blanks.
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.	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.
9008	The CUSP/PCF CKDS that was input to the conversion process is not valid. ICSF sets the reason code after issuing message CSFV0056.	9048	An override entry duplicates another override entry within LABEL and OLD_TYPE. ICSF sets the reason code after issuing message CSFV0326.
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.	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.
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.	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.
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.	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.
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.	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.
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.	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.
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.	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, DATA LAT, 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.

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.

System programmer response: Respond to the problem that is identified by the return and reason codes. Rerun the conversion program.

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 these non-blank values because it bypassed 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. 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. For more information, see *MVS/DFP: Managing VSAM Data Sets*.

| **3078** The CKDS was created with an unsupported LRECL.
 |

System action: Processing ends.

User response: Contact your system programmer.

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.

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 in the *MVS/ESA Data Administration: Macro Instruction Reference*.

For a VSAM file, the format and explanation of the message is in the Physical-Error Message Format figure in the *MVS/DFP: Managing VSAM Data Sets*.

System action: Processing ends.

User response: Contact your system programmer.

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.

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.

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

System programmer response: Contact the IBM Support Center.

**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.

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.

System programmer response: If you cannot resolve the error, contact the IBM Support Center.

Appendix. Accessibility

Publications for this product are offered in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when using PDF files, you may view the information through the z/OS Internet Library Web site or the z/OS Information Center. If you continue to experience problems, send an e-mail to mhvrcfs@us.ibm.com or write to:

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
U.S.A.

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.

z/OS information

z/OS information is accessible using screen readers with the BookServer or Library Server versions of z/OS books in the Internet library at:

<http://www.ibm.com/systems/z/os/zos/bkserv/>

Notices

This information was developed for products and services offered in the U.S.A.

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.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 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.

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.

Readers' Comments — We'd Like to Hear from You

**z/OS
Cryptographic Services
Integrated Cryptographic Service Facility
Messages**

Publication No. SA22-7523-14

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:

- Send your comments to the address on the reverse side of this form.
- Send your comments via email to: mhvrcfs@us.ibm.com

If you would like a response from IBM, please fill in the following information:

Name

Address

Company or Organization

Phone No.

Email address



Fold and Tape

Please do not staple

Fold and Tape



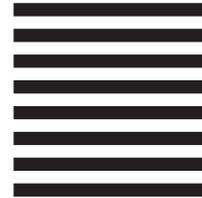
NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Department 55JA, Mail Station P384
2455 South Road
Poughkeepsie, NY 12601-5400



Fold and Tape

Please do not staple

Fold and Tape



Program Number: 5694-A01

Printed in USA

SA22-7523-14

