

z/OS



# Cryptographic Services Integrated Cryptographic Service Facility Messages

*Version 2 Release 3*

**Note**

Before using this information and the product it supports, read the information in "Notices" on page 121.

This edition applies to ICSF FMID HCR77C1 and Version 2 Release 3 of z/OS (5650-ZOS) and to all subsequent releases and modifications until otherwise indicated in new editions.

Last updated: November 19, 2018

© **Copyright IBM Corporation 1997, 2018.**

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

---

# Contents

<b>About this information . . . . .</b>	<b>v</b>	<b>Chapter 9. CSFOnnnn messages (Installation options parameter processing). . . . .</b>	<b>93</b>
Who should read this information . . . . .	v	<b>Chapter 10. CSFPnnnn messages (Parse) . . . . .</b>	<b>101</b>
How to use this information . . . . .	v	<b>Chapter 11. CSFUnnnn messages (ICSF utility processing) . . . . .</b>	<b>103</b>
Where to find more information. . . . .	v	<b>Chapter 12. CSFVnnnn messages (CKDS conversion processing). . . . .</b>	<b>105</b>
IBM Crypto Education. . . . .	vi	<b>Chapter 13. CSFYnnnn messages (I/O errors) . . . . .</b>	<b>113</b>
<b>How to send your comments to IBM . . . . .</b>	<b>vii</b>	<b>Appendix. Accessibility . . . . .</b>	<b>117</b>
If you have a technical problem . . . . .	vii	Accessibility features . . . . .	117
<b>Summary of changes. . . . .</b>	<b>ix</b>	Consult assistive technologies . . . . .	117
Changes made in Cryptographic Support for z/OS V2R1 - z/OS V2R3 (FMID HCR77C1) . . . . .	ix	Keyboard navigation of the user interface . . . . .	117
Changes made in Cryptographic Support for z/OS V2R1 - z/OS V2R2 (FMID HCR77C0) . . . . .	x	Dotted decimal syntax diagrams . . . . .	117
Changes made in Cryptographic Support for z/OS V1R13 - z/OS V2R2 (FMID HCR77B1) . . . . .	xi	<b>Notices . . . . .</b>	<b>121</b>
Changes made in Enhanced Cryptographic Support for z/OS V1R13 - z/OS V2R1 (FMID HCR77B0) . . . . .	xii	Terms and conditions for product documentation . . . . .	123
<b>Chapter 1. Introduction . . . . .</b>	<b>1</b>	IBM Online Privacy Statement. . . . .	124
<b>Chapter 2. CSFBnnnn messages (Build control statement processing) . . . . .</b>	<b>3</b>	Policy for unsupported hardware. . . . .	124
<b>Chapter 3. CSFCnnnn messages (Cryptographic key data set processing). 5</b>	<b>5</b>	Minimum supported hardware . . . . .	124
<b>Chapter 4. CSFEnnnn messages (Exit router) . . . . .</b>	<b>11</b>	Trademarks . . . . .	125
<b>Chapter 5. CSFGnnnn messages (Key generator utility processing) . . . . .</b>	<b>13</b>	<b>Index . . . . .</b>	<b>127</b>
<b>Chapter 6. CSFHnnnn messages (IBM Health Checker processing) . . . . .</b>	<b>29</b>		
<b>Chapter 7. CSFInnnn messages (Component trace). . . . .</b>	<b>37</b>		
<b>Chapter 8. CSFMnnnn messages (ICSF address space) . . . . .</b>	<b>39</b>		
Identification of cryptographic features . . . . .	39		



---

## About this information

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

---

## Who should read this information

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

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

---

## How to use this information

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

- Chapter 2, “CSFBnnnn messages (Build control statement processing),” on page 3
- Chapter 3, “CSFCnnnn messages (Cryptographic key data set processing),” on page 5
- Chapter 4, “CSFEnnnn messages (Exit router),” on page 11
- Chapter 5, “CSFGnnnn messages (Key generator utility processing),” on page 13
- Chapter 6, “CSFHnnnn messages (IBM Health Checker processing),” on page 29
- Chapter 7, “CSFInnnn messages (Component trace),” on page 37
- Chapter 8, “CSFMnnnn messages (ICSF address space),” on page 39
- Chapter 9, “CSFOnnnn messages (Installation options parameter processing),” on page 93
- Chapter 10, “CSFPnnnn messages (Parse),” on page 101
- Chapter 11, “CSFUnnnn messages (ICSF utility processing),” on page 103
- Chapter 12, “CSFVnnnn messages (CKDS conversion processing),” on page 105
- Chapter 13, “CSFYnnnn messages (I/O errors),” on page 113

---

## Where to find more information

The ICSF library consists of the following books:

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

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

Other documents that are referenced are:

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

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

## **IBM Crypto Education**

The IBM Crypto Education ([www.ibm.com/developerworks/community/groups/community/crypto](http://www.ibm.com/developerworks/community/groups/community/crypto)) community provides detailed explanations and samples pertaining to IBM cryptographic technology.

---

## How to send your comments to IBM

We invite you to submit comments about the z/OS<sup>®</sup> product documentation. Your valuable feedback helps to ensure accurate and high-quality information.

**Important:** If your comment regards a technical question or problem, see instead “If you have a technical problem.”

Submit your feedback by using the appropriate method for your type of comment or question:

### **Feedback on z/OS function**

If your comment or question is about z/OS itself, submit a request through the IBM RFE Community ([www.ibm.com/developerworks/rfe/](http://www.ibm.com/developerworks/rfe/)).

### **Feedback on IBM<sup>®</sup> Knowledge Center function**

If your comment or question is about the IBM Knowledge Center functionality, for example search capabilities or how to arrange the browser view, send a detailed email to IBM Knowledge Center Support at [ibmkc@us.ibm.com](mailto:ibmkc@us.ibm.com).

### **Feedback on the z/OS product documentation and content**

If your comment is about the information that is provided in the z/OS product documentation library, send a detailed email to [mhvrcfs@us.ibm.com](mailto:mhvrcfs@us.ibm.com). We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

To help us better process your submission, include the following information:

- Your name, company/university/institution name, and email address
- The following deliverable title and order number: z/OS ICSF Messages, SC14-7509-06
- The section title of the specific information to which your comment relates
- The text of your comment.

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

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

---

## If you have a technical problem

If you have a technical problem or question, do not use the feedback methods that are provided for sending documentation comments. Instead, take one or more of the following actions:

- Go to the IBM Support Portal ([support.ibm.com](http://support.ibm.com)).
- Contact your IBM service representative.
- Call IBM technical support.





---

## Summary of changes

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

ICSF publications can be obtained from:

- The Resource Link home page ([www.ibm.com/servers/resourcelink](http://www.ibm.com/servers/resourcelink)). (Select Publications and then select the release that you are interested in under ICSF Publications by FMID.)
- IBM z/OS downloads ([www.ibm.com/systems/z/os/zos/downloads](http://www.ibm.com/systems/z/os/zos/downloads)) for Cryptographic Support.

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

---

## Changes made in Cryptographic Support for z/OS V2R1 - z/OS V2R3 (FMID HCR77C1)

This document contains information previously presented in *z/OS ICSF Messages*, SC14-7509-05.

This document is for ICSF FMID HCR77C1. This release of ICSF runs on z/OS V2R1, V2R2, and V2R3 and only on zSeries hardware.

### New

The following messages are new.

- CSFG1054
- CSFG1064
- CSFG1074
- CSFG1084
- CSFG1094
- CSFG1124 (APAR OA54132)
- CSFG1134 (APAR OA55184)
- CSFH0041
- CSFM624I
- CSFM689I
- CSFM690I
- CSFM691E
- CSFM692E
- CSFM693E
- CSFM695I
- CSFM704I (APAR OA54509)
- CSFO001I

## Changed

The following messages are updated.

- CSFG0224
- CSFG0866 (APAR OA55184)
- CSFG0964 (APAR OA55184)
- CSFM109I
- CSFM111I
- CSFM123E
- CSFM124I
- CSFM129I
- CSFM134I
- CSFM135E
- CSFM136I
- CSFM137E
- CSFM138I
- CSFM139I

## Deleted

No content was removed from this information.

---

## Changes made in Cryptographic Support for z/OS V2R1 - z/OS V2R2 (FMID HCR77C0)

This document contains information previously presented in *z/OS ICSF Messages*, SC14-7509-04.

This document is for ICSF FMID HCR77C0. This release of ICSF runs on z/OS V2R1 and z/OS V2R2 and only on zSeries hardware.

## New

The following messages are new.

- CSFG1054 (APAR OA53817)
- CSFG1064 (APAR OA53817)
- CSFG1074 (APAR OA53817)
- CSFH0036I
- CSFH0037E
- CSFH0038I
- CSFH0039I
- CSFH0040E
- CSFM658I (APAR OA52806)
- CSFM687I
- CSFM688E
- CSFM704I (APAR OA54509)
- CSFO002I
- CSFO500I

- CSFO501I
- CSFO502I
- CSFO503I

### **Changed**

- CSFC0316
- CSFG0224 (APAR OA53817)
- CSFG0744
- CSFH0018I
- CSFM111I
- CSFM130I
- CSFM410E
- CSFM667I
- CSFM668I

### **Deleted**

ICSF no longer issues the following messages: CSFO0056 and CSFO0196.

---

## **Changes made in Cryptographic Support for z/OS V1R13 - z/OS V2R2 (FMID HCR77B1)**

This document contains information previously presented in *z/OS ICSF Messages*, SC14-7509-02.

This document is for ICSF FMID HCR77B1. This release of ICSF runs on z/OS V1R13, z/OS V2R1, and z/OS V2R2 and only on zSeries hardware.

### **New**

The following messages are new.

- CSFM666I
- CSFM667I
- CSFM668I
- CSFM669I
- CSFM670I
- CSFM674I
- CSFM676I
- CSFM677I
- CSFM678E
- CSFM679I
- CSFM680I
- CSFM681I
- CSFM682I
- CSFM683E
- CSFM684I
- CSFM685I
- CSFM686I

- CSFO0252

### **Changed**

- CSFM009I
- CSFM625I
- CSFM668I
- Terminology changed from open cryptographic services to regional cryptographic services.

### **Deleted**

ICSF no longer issues the following message: CSFC0086.

---

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

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

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

### **New**

The following messages are new.

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

### **Changed**

- CSFC0316
- CSFG0002
- CSFH0011I

- CSFM009I
- CSFM109I
- CSFM111I
- CSFM123E
- CSFM124I
- CSFM129I
- CSFM134I
- CSFM135E
- CSFM136I
- CSFM137E
- CSFM138I
- CSFM139I
- CSFM639I
- CSFM641I

### **Deleted**

No content was removed from this information.



---

## Chapter 1. Introduction

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





---

## Chapter 2. CSFBnnnn messages (Build control statement processing)

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

---

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

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

**System action:** Processing ends.

**User response:**

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

---

### CSFB0026 STATEMENT EXCEEDS MAXIMUM LENGTH ALLOWED.

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

**System action:** Processing ends.

**User response:**

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

---

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

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

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

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

---

### CSFB0044 COLUMN 72 NOT BLANK.

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

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

**User response:** Ensure that column 72 is blank.

---

### CSFB0056 INPUT FILE EMPTY.

**Explanation:** The control statement input file is empty.

**System action:** Processing ends.

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



---

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

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

---

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

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

**System action:** Processing ends.

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

**User response:** Contact your system programmer.

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

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

---

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

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

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

**System action:** Processing ends.

**System programmer response:** Contact the IBM Support Center.

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

---

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

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

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

**System action:** Processing ends.

**User response:** Wait until the CKDS is available.

---

**CSFC0046** UNABLE TO OPEN KEY DATASET *dsname*.

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

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

**System action:** Processing ends.

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

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

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

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

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

**System action:** Processing ends.

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

**User response:** Contact your system programmer.

---

**CSFC0064**    **UNABLE TO CLOSE KEY DATA SET** *dsname*.

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

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

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

**System programmer response:** Contact the IBM Support Center.

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

If the problem persists, contact your system programmer.

---

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

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

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

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

**System programmer response:** Contact the IBM Support Center.

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

If the problem persists, contact your system programmer.

---

**CSFC0096**    **UNABLE TO UPDATE THE CKDS CONTROL RECORD.**

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

**System action:** Processing ends.

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

**User response:** Contact your system programmer.

---

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

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

**System action:** Processing ends.

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

**User response:** Contact your system programmer.

---

---

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

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

**Return code:** 08

**Reason Code  
Meaning**

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

**System action:** Processing ends.

**System programmer response:** Contact the IBM Support Center.

**User response:** Contact your system programmer.

---

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

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

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

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

---

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

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

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

**System action:** Processing ends.

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

---

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

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

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

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

---

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

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

**System action:** Processing ends.

**User response:** Use an empty output key data set.

---

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

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

**Return code:** 04

## CSFC0172 • CSFC0206

### Reason Code Meaning

04 ICSF could not find the installation exit module.

Return code: 08

### Reason Code Meaning

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

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

**System action:** Processing ends.

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

---

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

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

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

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

---

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

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

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

**System action:** Processing ends.

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

---

### CSFC0196 CONTROL RECORD NOT FOUND ON CKDS *dsname*.

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

**System action:** Processing ends.

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

---

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

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

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

**System action:** Processing ends.

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

---

---

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

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

**System action:** Processing ends.

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

---

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

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

**System action:** Processing ends.

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

---

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

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

**System action:** Processing ends.

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

---

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

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

**System action:** Processing ends.

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

---

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

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

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

**System action:** Processing continues.

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

**User response:** Contact your system programmer.

---

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

**Explanation:** An error was encountered during the re-enciphering of one of the entries in the CKDS or PKDS. The label for the problem entry is specified in the message. See 'Using the ICSF Utility Program CSFEUTIL' and 'Using the ICSF Utility Program CSFPUTIL' in *z/OS Cryptographic Services ICSF Administrator's Guide* for the return and reason codes.

**System action:** Processing ends.

**System programmer response:** Investigate the entry specified by the CKDS or PKDS label to determine cause of problem. If you cannot resolve the problem, contact the IBM Support Center.

**User response:** Contact your ICSF administrator.

---

**CSFC0322**    **DUPLICATE TOKENS FOUND IN DATASET** *dsname*.

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

**System action:** Processing continues.

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

---

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

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

**System action:** Processing ends.

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

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

---

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

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

**System action:** Processing continues.

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



---

## Chapter 4. CSFEnnnn messages (Exit router)

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

---

### CSFE001I INSTALLATION EXIT *exit-name* NOT FOUND

**Explanation:** This is an informational message only.

**System action:** Processing continues.

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

---

### CSFE002A REQUIRED INSTALLATION EXIT *exit-name* NOT FOUND

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

**System action:** ICSF ends.

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



---

## Chapter 5. CSFGnnnn messages (Key generator utility processing)

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

---

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

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

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

### Return Code

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

**System action:** Processing ends.

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

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

## CSFG0014 • CSFG0064

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

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

---

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

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

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

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

---

### CSFG0024 NOCV SPECIFIED WITH TWO TRANSKEYS.

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

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

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

---

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

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

**System action:** Processing ends.

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

**User response:** Contact your system programmer.

**Problem determination:** In addition to the system programmer actions:

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

---

### CSFG0056 CKDS CONTROL RECORD NOT FOUND.

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

**System action:** Processing ends.

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

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

---

### CSFG0064 CONTROL STATEMENT VERB NOT VALID.

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

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

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

---

**CSFG0074 SYNTAX ERROR IN CONTROL STATEMENT.**

**Explanation:** A control statement was not valid.

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

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

---

**CSFG0084 SPECIFIED KEY VALUE IS NOT VALID.**

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

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

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

---

**CSFG0094 *keyword1* OR *keyword2* NOT SPECIFIED.**

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

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

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

---

**CSFG0104 *keyword1* AND *keyword2* BOTH SPECIFIED.**

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

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

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

---

**CSFG0124 RANGE LABEL PREFIXES NOT EQUAL.**

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

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

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

---

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

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

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

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

---

**CSFG0164 SAME KEY LABEL VALUES SPECIFIED FOR TRANSKEY.**

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

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

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

---

---

**CSFG0174 KEY VALUE AND TWO TRANSKEY LABELS SPECIFIED.**

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

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

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

---

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

**Explanation:** 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*. Probable causes are:

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

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

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

---

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

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

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

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

---

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

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

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

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

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

---

**CSFG0272 IMPORTED KEY DOES NOT HAVE ODD PARITY.**

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

**System action:** Processing continues.

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

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

---

**CSFG0284 BOTH TRANSPORT KEYS ARE EXPORTER TYPE WITH NOCV CAPABILITY.**

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

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

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

---

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

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

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

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

**User response:** Contact your system programmer.

---

**CSFG0302 STATEMENT NOT PROCESSED.**

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

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

**User response:** Investigate the previous diagnostic error messages.

---

**CSFG0313 STATEMENT PARTIALLY PROCESSED.**

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

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

**User response:** Investigate the previous diagnostic error messages.

---

**CSFG0321 STATEMENT SUCCESSFULLY PROCESSED.**

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

**System action:** Normal processing of the input file continues.

**User response:** None.

---

**CSFG0395 INSTALLATION EXIT MODULE REQUIRED BUT NOT AVAILABLE.**

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

**System action:** Processing ends.

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

**CSFG0402 INSTALLATION EXIT NOT LOADED.**

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

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

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

---

**CSFG0414 STATEMENT REJECTED BY INSTALLATION EXIT.**

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

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

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

---

**CSFG0425 KEY GENERATOR TERMINATED BY INSTALLATION EXIT.**

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

**System action:** Processing ends.

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

---

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

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

**System action:** Processing ends.

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

**User response:** Contact your system programmer.

---

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

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

**System action:** Processing ends.

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

**User response:** Contact your system programmer.

---

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

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

**System action:** Processing ends.

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

**User response:** Contact the programmer responsible for the exit.

---



---

**CSFG0465** INSTALLATION EXIT NOT AVAILABLE FOR PROCESSING SET STATEMENT.

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

**System action:** Processing ends.

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

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

---

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

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

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

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

---

**CSFG0484** TWO LABEL VALUES NOT SPECIFIED ON RENAME STATEMENT.

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

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

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

---

**CSFG0494** TOO MANY LABEL VALUES SPECIFIED.

**Explanation:** The control statement contains more than 64 labels.

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

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

---

**CSFG0504** INCORRECT NUMBER OF KEY VALUES SPECIFIED.

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

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

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

---

**CSFG0514** DUPLICATE LABEL VALUES SPECIFIED.

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

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

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

---

**CSFG0524** MORE THAN TWO TRANSKEY VALUES SPECIFIED.

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

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

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

---

**CSFG0544 KEY VALUE SPECIFIED NOT 16 CHARACTERS.**

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

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

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

---

**CSFG0554 TWO RANGE VALUES NOT SPECIFIED.**

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

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

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

---

**CSFG0575 CLEAR KEYWORD SPECIFIED WHILE SPECIAL SECURITY MODE DISABLED.**

**Explanation:** The CLEAR keyword requires special security mode.

**System action:** Processing ends.

**User response:** Contact your security administrator.

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

---

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

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

**System action:** Processing ends.

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

**User response:** Contact your system programmer.

---

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

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

**System action:** Processing ends.

**User response:** Correct the KGUP statement.

---

**CSFG0624 *Keyword* NOT VALID BECAUSE TYPE IS NULL.**

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

**System action:** Processing ends.

**User response:** Correct the KGUP statement.

---

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

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

**System action:** Processing ends.

**User response:** Correct the KGUP statement.

---

---

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

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

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

**User response:** Correct the KGUP statement.

---

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

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

**System action:** Processing ends.

**User response:** Correct the KGUP statement.

---

**CSFG0664** RANGE LABEL SUFFIXES ARE NOT THE SAME LENGTH.

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

**System action:** Processing ends.

**User response:** Correct the KGUP statement.

---

**CSFG0674** RANGE LABEL SUFFIX HAS TOO MANY DIGITS.

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

**System action:** Processing ends.

**User response:** Correct the KGUP statement.

---

**CSFG0684** RANGE LABEL HAS NO NUMERIC SUFFIX.

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

**System action:** Processing ends.

**User response:** Correct the KGUP statement.

---

**CSFG0704** UPDATE NOT ALLOWED FOR TYPE NULL.

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

**System action:** Processing ends.

**User response:** Correct the KGUP statement.

---

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

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

**System action:** Processing ends.

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

## CSFG0735 • CSFG0780

**User response:** Contact your system programmer.

---

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

**Explanation:** The LENGTH keyword on either an ADD or UPDATE statement contained a value that is not allowed for the key type and algorithm. The allowable lengths are defined in the explanation for the TYPE keyword in *z/OS Cryptographic Services ICSF Administrator's Guide*.

**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 cryptographic coprocessor specified.

**System action:** Processing for this statement ends.

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

---

### CSFG0754 LABEL NOT COMPLETE.

**Explanation:** The attempt to retrieve the key from the cryptographic coprocessor 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 cryptographic coprocessor was specified. If so, complete the key on the cryptographic coprocessor using the TKE workstation. Otherwise, correct the KGUP statement for the correct label and cryptographic coprocessor 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 cryptographic coprocessor 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 cryptographic coprocessor for the specified key label was successfully written to the CKDS. The ENC-ZERO verification pattern for the key is given.

**System action:** Processing continues.

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

---

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

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

**System action:** Processing continues.

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

---

**CSFG0791** KEYWORD *keyword* IS NO LONGER SUPPORTED.

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

**System action:** Processing continues.

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

---

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

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

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

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

---

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

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

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

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

---

**CSFG0824** ALGORITHM MISMATCH FOR UPDATE REQUEST.

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

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

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

---

**CSFG0834** ALGORITHM *keyword* NOT AVAILABLE ON SYSTEM.

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

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

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

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

---

**CSFG0856** CKDS IS NOT USABLE.

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

**System action:** Processing ends.

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

---

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

| **Explanation:** The entry with the key index *label* is a key token wrapped with an enhanced method that is  
| unsupported by this release of ICSF. Unsupported tokens cannot be deleted, updated, or renamed by KGUP.

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

| **User response:** Correct the KGUP statement so that the label is not for a key token that cannot be managed by this  
| release of ICSF.

---

---

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

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

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

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

---

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

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

**System action:** Processing for the OPKYLOAD statement ends.

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

---

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

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

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

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

---

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

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

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

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

---

**CSFG0924** KEYUSAGE VALUES ARE NOT CONSISTENT.

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

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

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

---

**CSFG0934** DUPLICATE TOKEN IN CKDS.

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

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

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

---

---

**CSFG0944 TRANSPORT KEY NOT COMPATIBLE WITH KEY TYPE AND ALGORITHM.**

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

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

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

---

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

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

**System action:** Processing ends.

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

---

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

**Explanation:** The length of the key specified by the LENGTH keyword or the number of key values supplied with the KEY keyword is not compatible with the *keyword*.

- The DOUBLEO keyword requires a key length of 16.
- \$TRIPLEO keyword requires a key length of 24.
- KEYMGT('COMP-TAG') keys must be double-length keys.

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

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

---

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

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

**System action:** Processing continues.

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

**User response:** Contact the programmer responsible for the exit.

---

**CSFG0986 CKDS IS NOT USABLE.**

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

**System action:** Processing ends.

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

---

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

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

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

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

---

**CSFG1004 DKYGENKYUSAGE VALUES ARE NOT CONSISTENT.**

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

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

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

---

**CSFG1014 ENCRYPTED KEY SUPPLIED FOR AES KEY.**

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

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

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

---

**CSFG1024 KEYUSAGE VALUES REQUIRE KEY OR TRANSKEY.**

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

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

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

---

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

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

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

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

---

**CSFG1042 TRANSKEY *label* HAS BAD METADATA.**

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

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

**System action:** Processing continues.

**User response:** None.

---

**CSFG1054 KEYMGT VALUE *value* SPECIFIED WITH *keytype* KEY TYPE FOR ALGORITHM *algorithm*.**

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

**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.



---

**CSFG1064 KEYMGT VALUES ARE NOT CONSISTENT.**

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

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

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

---

**CSFG1074 KEYMGT VALUE *value* SPECIFIED WITH *keyword*.**

**Explanation:** The KEYMGT *value* cannot be specified with the *keyword*. The usage is not allowed.

**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.

---

**CSFG1084 COMPLIANCE TAG REQUEST INCONSISTENT WITH TRANSPORT KEY.**

**Explanation:** When a request to generate a compliance-tagged key token (KEYMGT('COMP-TAG')) is in a ADD or UPDATED control statement, any transport keys specified must be compliance-tagged and cannot be marked NOCV. Also, compliance-tagged transport keys can be used to only generate compliance-tagged keys.

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

**User response:** Specify transport key or keys that match the type of key to be generated and rerun the key generator utility program.

---

**CSFG1094 TRANSKEY *label* TOO WEAK.**

**Explanation:** The transport key *label* that is specified in the control statement is too weak to wrap the key that is being generated or imported. DOUBLEO is specified for the requested key and the transport key is not DOUBLEO.

**System action:** Processing continues.

**User response:** Supply a transport key that is as strong or stronger than the requested key.

---

**CSFG1124 ENTRY *label* CONTAINS RCE REDIRECT METADATA. *verb* NOT PERFORMED.**

**Explanation:** An attempt was made to use KGUP to delete a record from a CKDS that contained redirect metadata used for Regional Cryptographic Server redirection. When RCE redirect metadata exists in a CKDS record, the record can only be deleted using the CSNBKRD callable service, which ensures that both the CKDS record and the associated TKDS entry are deleted.

*verb* Can be either UPDATE, DELETE, or RENAME.

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

**User response:** Use the CSNBKRD callable service to delete a CKDS record that contains RCE metadata.

---

**CSFG1134 KEY VALUES NOT UNIQUE.**

**Explanation:** The DOUBLEO or \$TRIPLEO keyword was specified in the control statement along with a clear key value with the KEY keyword. The 16-byte or 24-byte values for the key must be unique when the DOUBLEO and \$TRIPLEO keywords are specified.

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

**User response:** Supply unique keys values in the control statement.



---

## 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 (ICSE,ICSMIG7731\_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 (ICSE, ICSFMIG7731\_ICSF\_RETAINED\_RSAKEY) check found no apparent RSA key use on this system.

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

**System action:** Processing continues.

---

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

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

**System action:** There is no effect on the system.

**Operator response:** Report this exception to the system programmer.

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

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

---

**CSFH0010E** Coprocessor or Accelerator *ttmm* serial number *nnnnnnnn* has changed states from *xxxxxxxx* to *yyyyyyyy*

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

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

**Operator response:** Report this exception to the system programmer.

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

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

---

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

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

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

**Operator response:** Report this exception to the system programmer.

## CSFH0012I • CSFH0017I

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

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

---

**CSFH0012I (ICSE,ICSF\_COPROCESSOR\_STATE\_NEGCHANGE): Check performed with no problems found.**

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

**System action:** Processing continues.

---

**CSFH0013I (ICSE,ICSF\_DEPRECATED\_SERV\_WARNINGS): Check performed with no problems found.**

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

**System action:** Processing continues.

---

**CSFH0014I (ICSE,ICSF\_MASTER\_KEY\_CONSISTENCY): The master keys are consistent across the current set of coprocessors.**

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

**System action:** Processing continues.

**Operator response:** None

**User response:** None

---

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

**Explanation:** The current value for the specified master key is not consistent across the coprocessors. At least one coprocessor has the specified master key in a state that is not in agreement with the other coprocessors.

**System action:** Processing continues.

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

**User response:** Contact the ICSF administrator.

---

**CSFH0016E Unable to process request for Master Key consistency check.**

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

**System action:** Processing continues.

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

**User response:** Contact the ICSF administrator.

---

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

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

**System action:** There is no effect on the system.

**Operator response:** None.

**System programmer response:** None.

**Problem determination:** N/A

ICSF Administrator response: None.

**CSFH0018I (ICSE,ICSMIG77A1\_COPROCESSOR\_ACTIVE):**

**Active key stores:**

**CKDS:** *ckdsn*

**PKDS:** *pkdsn*

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

**System action:** There is no effect on the system.

**Operator response:** None.

**System programmer response:** None.

**Problem determination:** N/A

ICSF Administrator response: None.

**CSFH0019I (ICSE,ICSMIG77A1\_COPROCESSOR\_ACTIVE):**

**All CCA coprocessors will become active.**

**Explanation:** The state of the current master keys on each CCA cryptographic coprocessor was checked. All coprocessors have the required master keys loaded and the current master keys have the correct values. All coprocessors will be active and available for work when ICSF FMID HCR77A1 or newer is started.

**System action:** There is no effect on the system.

**Operator response:** None.

**System programmer response:** None.

**Problem determination:** N/A

ICSF Administrator response: None.

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

**CSFH0020E (ICSE,ICSMIG77A1\_COPROCESSOR\_ACTIVE):**

**Coprocessor *nn* serial number *sssssss* has mismatched *type* master keys.**

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

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

**System action:** There is no effect on the system.

**Operator response:** Contact the ICSF administrator.

**System programmer response:** None.

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

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

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

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

**CSFH0021E (ICSE,ICSMIG77A1\_COPROCESSOR\_ACTIVE):**  
**Unable to process request.**

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

**System action:** There is no effect on the system.

**Operator response:** Contact the ICSF administrator.

**System programmer response:** None.

**Problem determination:** None.

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

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

---

**CSFH0022E (ICSE,ICSMIG77A1\_UNSUPPORTED\_HW):**  
**Current processor (z800 or z900) will not be supported on a migration to ICSF HCR77A1. HCR77A1 is planned to require IBM zSeries z890, z990, or newer processors.**

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

**System action:** There is no effect on the system.

**Operator response:** Contact the ICSF administrator.

**System programmer response:** Contact the ICSF administrator.

**Problem determination:** None.

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

**Reference:** *z/OS Cryptographic Services ICSF Overview*

**Check Reason:** Detects systems that ICSF no longer supports.

---

**CSFH0023I (ICSE,ICSMIG77A1\_TKDS\_OBJECT):**  
**Active Token Data Set: *tkdsn***

**Explanation:** This informational message indicates which Token Data Set (TKDS) was used in the check.

**System action:** There is no effect on the system.

**Operator response:** None.

**System programmer response:** None.

**Problem determination:** None.

**ICSF Administrator response:** None.

---

**CSFH0024I (ICSE,ICSMIG77A1\_TKDS\_OBJECT):**  
**All TKDS objects are acceptable.**

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

**System action:** There is no effect on the system.

**Operator response:** None.

**System programmer response:** None.

**Problem determination:** N/A

**ICSF Administrator response:** None.

---

**CSFH0025E (ICSE,ICSMIG77A1\_TKDS\_OBJECT):**  
**TKDS objects were found that have too much data.**

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

The objects listed have information in the 'User data' field of the TKDS record which will be lost when running with ICSF FMID HCR77A1. The size of the object in the record is too large for the 'User data' field to be preserved with the new record format.

**System action:** There is no effect on the system.

**Operator response:** Contact the ICSF administrator.

**System programmer response:** Contact the ICSF administrator.

**Problem determination:** N/A

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

---

**CSFH0027I (ICSF):**  
**The check is not applicable in the current system environment.**

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

**System action:** There is no effect on the system.

**Operator response:** None.

**System programmer response:** None.

**Problem determination:** N/A

**ICSF Administrator response:** None.

---

**CSFH0030I Cryptographic records expiring in *nnn* days.**

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

**System action:** There is no effect on the system.

**Operator response:** None.

**Problem determination:** N/A

**ICSF Administrator response:** None.

---

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

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

**System action:** There is no effect on the system.

**Operator response:** Contact the ICSF administrator.

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

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

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

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

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

## CSFH0032I • CSFH0040E

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

*z/OS Cryptographic Services ICSF Application Programmer's Guide*

---

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

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

**System action:** There is no effect on the system.

---

**CSFH0036I (ICSE,ICSF\_OPTIONS\_CHECKS):**

**All the ICSF options checked were set to specified values.**

**Explanation:** This is an informational message indicating that the check found that all the ICSF installation options checked were set to the values indicated in the health check parameter.

**System action:** There is no effect on the system.

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

*z/OS Cryptographic Services ICSF System Programmer's Guide*

---

**CSFH0037E** Option *option* is set to *value*

**Explanation:** This check detected that the current value for the option is set to a value which does not match what was specified in the parameter or its default value. This may not be a issue, but should be investigated to ensure this setting was intended.

A YES value for this option has a possible negative impact on performance-sensitive cryptographic workloads.

**System action:** There is no effect on the system.

**Operator response:** Contact the ICSF administrator.

**ICSF Administrator response:** Investigate if the value specified for *option* was intended.

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

*z/OS Cryptographic Services ICSF System Programmer's Guide*

---

**CSFH0038I** Check for unsupported CCA cryptographic keys in CKDS and PKDS

**Explanation:** This informational message is the title of the check.

**System action:** There is no effect on the system.

---

**CSFH0039I** No unsupported CCA keys were found in the CKDS or PKDS

**Explanation:** This is an informational message indicating that the check did not detect any records in the key data sets that have unsupported CCA keys.

**System action:** There is no effect on the system.

---

**CSFH0040E** Unsupported CCA cryptographic keys in CKDS or PKDS were found.

**Explanation:** This check detected keys in the active key data sets that are not supported with the cryptographic features in use. The label of the records are listed.

These keys cannot be used by any ICSF service for any purpose. These keys may be removed if desired.

**System action:** There is no effect on the system.

**Operator response:** Contact the ICSF administrator.

**Problem determination:** If you are using the common record format (KDSR) of the CKDS and PKDS, you may be able to determine if the label is being used in an application.

If you have key reference tracking enabled, you can tell if the label has been referenced by an application using the



CSFKMDR callable service to read the last reference data metadata of the record.

If you do not have key reference tracking enabled, you can either enable key reference tracking or archive the record to see if the label is being used by an application.

**ICSF Administrator response:** Determine if the records specified in the output of the check can be deleted if desired. The records detected by this check have no effect on the operation of ICSF. They can be deleted if desired.

The CSNBKRD and CSNDKRD callable services are used to delete records from the key data sets.

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

*z/OS Cryptographic Services ICSF Application Programmer's Guide*

---

#### **CSFH0041I SAF authorization check for ICSF service *service* failed.**

**Explanation:** This is an informational message indicating that the check called the ICSF service and the caller is not authorized to the CSFSERV class profile for that service.

**System action:** There is no effect on the system.

**Operator response:** Contact the ICSF administrator.

**Problem determination:** The message indicates the service for which the user is not authorized.

**ICSF Administrator response:** Authorize the user to the service in the CSFSERV class indicated in the message. The userid may be the default userid for system address spaces or started tasks or a specified userid if one was defined for the Health Check address space.

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



---

## 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 (IPCSPRNT).

---

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

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

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

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

---

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

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

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

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

---

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

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

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

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



---

## Chapter 8. CSFMnnnn messages (ICSF address space)

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

---

### Identification of cryptographic features

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

Table 1. Cryptographic adapter identification

Cryptographic adapter	Prefix for FMIDs prior to HCR77B0	Prefix for FMID HCR77B0 and later
Crypto Express2 coprocessor	E	2C
Crypto Express2 accelerator	F	2A
Crypto Express3 coprocessor	G	3C
Crypto Express3 accelerator	H	3A
Crypto Express4 CCA coprocessor	SC	4C
Crypto Express4 EP11 coprocessor	SP	4P
Crypto Express4 accelerator	SA	4A

**Note:** All newer cryptographic adapters use the convention where  $n$  is the number in the adapter name. For regional cryptographic servers,  $n$  represents the generation number of the server:

- $nA$  Crypto Express $n$  accelerators.
- $nC$  Crypto Express $n$  CCA coprocessors.
- $nP$  Crypto Express $n$  EP11 coprocessors.
- $nR$  Regional cryptographic servers. Note: 2R requires ICSF FMID HCR77B1 with PTF OA49069 or later.

---

#### CSFM001I ICSF INITIALIZATION COMPLETE

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

**System action:** Processing continues.

**Operator response:** None.

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

---

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

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

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

**System action:** Processing continues.

**Operator response:** If appropriate, contact your system programmer.

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

---

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

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

**System action:** ICSF ends.

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

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

---

**CSFM004A ICSF TERMINATING. ICSF ALREADY ACTIVE.**

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

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

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

**Operator response:** If appropriate, contact your system programmer.

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

---

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

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

**System action:** ICSF ends.

**Operator response:** If necessary, contact your system programmer.

**System programmer response:** None.

---

**CSFM009I NO ACCESS CONTROL AVAILABLE FOR ICSF SERVICES OR KEYS**

**Explanation:** ICSF issues this message if it is unable to perform RACROUTE REQUEST=LIST for the classes CSFSERV, CSFKEYS, or XCSFKEY during initialization.

**System action:** Processing continues.

**Operator response:** Inform the system programmer.

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

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

---

---

**CSFM010E ICSF TERMINATING. PROCESSOR IS UNSUPPORTED.**

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

**System action:** ICSF ends.

**Operator response:** Inform your system programmer.

**System programmer response:** Contact the IBM Support Center.

---

**CSFM011I FASTAUTH IS NOT SUPPORTED BY THE INSTALLED SECURITY PRODUCT.**

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

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

**Operator response:** Notify your security administrator.

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

---

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

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

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

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

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

**Operator response:** Inform your system programmer.

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

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

---

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

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

**System action:** ICSF initialization terminates.

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

---

**CSFM014I FIPS 140 KNOWN ANSWER TEST FOR PKCS11 SERVICES FAILED.**

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

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

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

---

**CSFM015I FIPS 140 SELF CHECKS FOR PKCS11 SERVICES SUCCESSFUL.**

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

**System action:** ICSF initialization continues.

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

---

**CSFM016I FIPS 140 NOT SUPPORTED.**

**Explanation:** The ICSF installation option FIPSMODE(YES,FAIL(NO)) or FIPSMODE(COMPAT,FAIL(NO)) has been specified, indicating that the z/OS PKCS #11 services must operate in compliance with FIPS 140-2. However, one of the following is true:

- The current IBM Z<sup>®</sup> model type or the version/release of z/OS that is running on it does not support FIPS during initialization. The supported z/OS versions/releases are V1R10 and higher.
- FIPS known answer tests failed during initialization or FIPS continuous conditional testing failed and the SETICSF OPTIONS,REFRESH command was issued to update the FIPSMODE option.

**System action:** If the error occurred during ICSF initialization, initialization continues, but FIPSMODE mode is disabled. If the error occurred during processing of the SETICSF OPTIONS, REFRESH command, the command completes without enabling FIPSMODE.

**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:** This message is issued when the options data set keyword DEFAULTWRAP is specified with ENHANCED wrapping for symmetric keys and/or there are no coprocessors online that support the enhanced wrapping. All symmetric keys will be wrapped with the original wrapping until a coprocessor that supports enhanced wrapping comes online.

**System action:** Processing continues.

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

---

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

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

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

**System action:** Processing continues.

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

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

---



---

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

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

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

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

**Operator response:** Contact your system programmer.

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

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

---

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

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

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

**Operator response:** None

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

---

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

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

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

**Operator response:** Contact your system programmer.

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

---

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

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

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  - CRYPTO EXPRESS2 ACCELERATOR
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - CRYPTO EXPRESS6 ACCELERATOR
  - CRYPTO EXPRESS6 COPROCESSOR
  - PCI CRYPTO ACCELERATOR
  - PCI X CRYPTO COPROCESSOR
- *c* - the short name for the coprocessor type. Possible values are:
  - A (representing a PCICA)

## CSFM111I

- 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - 6A (representing a CEX6A)
  - 6C (representing a CEX6C)
  - 6P (representing a CEX6P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
  - *nnnnnnn* or N/A - the serial number for the cryptographic feature, or N/A when the feature is configured as an accelerator.

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

**Operator response:** None

**System programmer response:** Have the cryptographic feature brought online.

---

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

**Explanation:** The cryptographic feature is online and operational. When the cryptographic feature is a coprocessor, the ACTIVE message indicates that all of the MKVPs in the CKDS, PKDS, and TKDS match the current master key registers and ICSF services may be used. The substitution variables are:

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  - CRYPTO EXPRESS2 ACCELERATOR
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - CRYPTO EXPRESS6 ACCELERATOR
  - CRYPTO EXPRESS6 COPROCESSOR
  - PCI CRYPTO ACCELERATOR
  - PCI X CRYPTO COPROCESSOR
- *c* - the short name for the coprocessor type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)

- 5C (representing a CEX5C)
- 5P (representing a CEX5P)
- 6A (representing a CEX6A)
- 6C (representing a CEX6C)
- 6P (representing a CEX6P)
- X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnnnn* or N/A - the serial number for the cryptographic feature, or N/A when the feature is configured as an accelerator.

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

**Operator response:** None

**System programmer response:** None

#### CSFM122I PKA SERVICES WERE NOT ENABLED DURING ICSF INITIALIZATION.

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

**Note:** This message will not be issued when your system has no CCA coprocessors or your system has CEX3C or later CCA coprocessors (with the September 2011 or later LIC) online. The availability of RSA callable services will depend on the status of the RSA master key. The PKA callable services control will not be active. CSFM130I is issued when the RSA master key is active and RSA callable services are available.

**System action:** ICSF initialization continues.

**Operator response:** None.

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

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

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

- *mk* - master key. It identifies the master key that is in error. May have the value AES, DES, ECC, P11, or RSA.
- *coprocessor-name* - the type of cryptographic coprocessor. May have the value:
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - CRYPTO EXPRESS6 COPROCESSOR
  - PCI X CRYPTO COPROCESSOR
- *c* - the short name for the coprocessor type. May have the value:
  - 2C (representing a CEX2C)
  - 3C (representing a CEX3C)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - 6C (representing a CEX6C)

## CSFM124I • CSFM126I

- 6P (representing a CEX6P)
- X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic coprocessor is installed.
- *nnnnnnn* - the serial number for the cryptographic coprocessor.

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

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

**Operator response:** None.

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

---

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

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

- *mk* - master key. It identifies the master key that is in error. May have the value AES, DES, ECC, P11, or RSA.
- *coprocessor-name* - the type of cryptographic coprocessor. May have the value:
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - CRYPTO EXPRESS6 COPROCESSOR
  - PCI X CRYPTO COPROCESSOR
- *c* - the short name for the coprocessor type. May have the value:
  - 2C (representing a CEX2C)
  - 3C (representing a CEX3C)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - 6C (representing a CEX6C)
  - 6P (representing a CEX6P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic coprocessor is installed.
- *nnnnnnnn* - the serial number for the cryptographic coprocessor.

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

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

**Operator response:** None.

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

---

### CSFM126I CRYPTOGRAPHY - FULL CPU-BASED SERVICES ARE AVAILABLE.

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

**System action:** Processing continues.

**Operator response:** None.

**System programmer response:** None.

---

**CSFM127I CRYPTOGRAPHY - AES SERVICES ARE AVAILABLE.**

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

**System action:** Processing continues.

**Operator response:** None.

**System programmer response:** None.

---

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

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

**System action:** ICSF terminates.

**Operator response:** Contact your system programmer.

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

---

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

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

- *mk* - master key. It identifies the master key that is in error. May have the value AES, DES, ECC, P11 or RSA.
- *coprocessor-name* - the type of cryptographic coprocessor. May have the value:
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - CRYPTO EXPRESS6 COPROCESSOR
  - PCI X CRYPTO COPROCESSOR
- *c* - the short name for the coprocessor type. May have the value:
  - 2C (representing a CEX2C)
  - 3C (representing a CEX3C)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - 6C (representing a CEX6C)
  - 6P (representing a CEX6P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic coprocessor is installed.
- *nnnnnnnn* - 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 DES, RSA, or ECC. ICSF is up and remains started.

**System action:** Processing continues.

**Operator response:** None.

## CSFM131E • CSFM134I

**System programmer response:** None.

---

### CSFM131E CRYPTOGRAPHY - *mk* SERVICES ARE NOT AVAILABLE.

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

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

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

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

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

**Operator response:** Contact the system programmer.

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

---

### CSFM132I SECURE KEY PKCS11 SERVICES AVAILABLE.

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

**System action:** Processing continues.

**Operator response:** None.

**System programmer response:** None.

---

### CSFM133I THERE ARE NO ACTIVE PKCS11 COPROCESSORS.

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

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

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

**System programmer response:** None.

---

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

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

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  - CRYPTO EXPRESS2 ACCELERATOR
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - CRYPTO EXPRESS6 ACCELERATOR
  - CRYPTO EXPRESS6 COPROCESSOR

- PCI CRYPTO ACCELERATOR
- PCI X CRYPTO COPROCESSOR
- UNKNOWN FEATURE
- *c* - the short name for the cryptographic feature type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - 6A (representing a CEX6A)
  - 6C (representing a CEX6C)
  - 6P (representing a CEX6P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnnn* or *N/A* - the serial number for the cryptographic feature, or *N/A* when the feature is configured as an accelerator.
- *reason* - the reason the cryptographic feature is no longer active. Possible values are:

**Deactivated**

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

**Disabled by TKE**

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

**Offline**

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

**Busy**

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

**Being reconfigured**

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

**Initializing stage 1**

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

**Initializing stage 2**

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

**Initializing stage 3**

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

**No feature present**

No feature was detected at this index.

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

**Operator response:** None.

**System programmer response:** Contact the ICSF administrator.

---

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

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

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  - CRYPTO EXPRESS2 ACCELERATOR
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - CRYPTO EXPRESS6 ACCELERATOR
  - CRYPTO EXPRESS6 COPROCESSOR
  - PCI CRYPTO ACCELERATOR
  - PCI X CRYPTO COPROCESSOR
  - UNKNOWN FEATURE
- *c* - the short name for the cryptographic feature type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - 6A (representing a CEX6A)
  - 6C (representing a CEX6C)
  - 6P (representing a CEX6P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnnnn* or *N/A* - the serial number for the cryptographic feature, or *N/A* when the feature is configured as an accelerator.
- *reason* - the reason the cryptographic feature is no longer active. Possible values are:

**Master key incorrect**

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

**Hardware error**

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

**Hung user on feature**

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

**Bad feature response**

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



**Retry limit reached**

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

**Unknown response**

The feature has returned a return code reason code combination that ICSF does not recognize.

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

**Operator response:** Contact the ICSF administrator.

**System programmer response:** Contact the ICSF administrator.

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

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

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  - CRYPTO EXPRESS2 ACCELERATOR
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - CRYPTO EXPRESS6 ACCELERATOR
  - CRYPTO EXPRESS6 COPROCESSOR
  - PCI CRYPTO ACCELERATOR
  - PCI X CRYPTO COPROCESSOR
  - UNKNOWN FEATURE
- *c* - the short name for the cryptographic feature type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - 6A (representing a CEX6A)
  - 6C (representing a CEX6C)
  - 6P (representing a CEX6P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnnnn* or *N/A* - the serial number for the cryptographic feature, or *N/A* when the feature is configured as an accelerator.
- *oldreason* - the previous reason why the feature is inactive.
- *newreason* - the new reason why the feature is inactive. Possible values are:

## CSFM137E

### Deactivated

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

### Disabled by TKE

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

### Master key incorrect

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

### Offline

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

### Busy

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

### Being reconfigured

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

### Hardware error

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

### Initializing stage 1

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

### Initializing stage 2

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

### Initializing stage 3

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

### User hung on latch

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

### Bad feature response

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

### Retry limit reached

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

### No feature present

No feature was detected at this index.

### Unknown response

The feature has returned a return code reason code combination that ICSF does not recognize.

### Unknown feature type

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

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

**Operator response:** None.

**System programmer response:** Contact the ICSF administrator.

---

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

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

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

- CRYPTO EXPRESS3 ACCELERATOR
- CRYPTO EXPRESS3 COPROCESSOR
- CRYPTO EXPRESS4 ACCELERATOR
- CRYPTO EXPRESS4 COPROCESSOR
- CRYPTO EXPRESS5 ACCELERATOR
- CRYPTO EXPRESS5 COPROCESSOR
- CRYPTO EXPRESS6 ACCELERATOR
- CRYPTO EXPRESS6 COPROCESSOR
- PCI CRYPTO ACCELERATOR
- PCI X CRYPTO COPROCESSOR
- UNKNOWN FEATURE
- *c* - the short name for the cryptographic feature type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - 6A (representing a CEX6A)
  - 6C (representing a CEX6C)
  - 6P (representing a CEX6P)
  - X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnnnn* or *N/A* - the serial number for the cryptographic feature, or *N/A* when the feature is configured as an accelerator.
- *oldreason* - the previous reason why the feature is inactive.
- *newreason* - the new reason why the feature is inactive. Possible values are:

**Deactivated**

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

**Disabled by TKE**

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

**Master key incorrect**

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

**Offline**

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

**Busy**

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

**Being reconfigured**

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

## CSFM138I

### Hardware error

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

### Initializing stage 1

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

### Initializing stage 2

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

### Initializing stage 3

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

### User hung on latch

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

### Bad feature response

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

### Retry limit reached

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

### No feature present

No feature was detected at this index.

### Unknown response

The feature has returned a return code reason code combination that ICSF does not recognize.

### Unknown feature type

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

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

**Operator response:** Contact the ICSF administrator.

**System programmer response:** Contact the ICSF administrator.

---

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

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

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  - CRYPTO EXPRESS2 ACCELERATOR
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - CRYPTO EXPRESS6 ACCELERATOR
  - CRYPTO EXPRESS6 COPROCESSOR
  - PCI CRYPTO ACCELERATOR
  - PCI X CRYPTO COPROCESSOR
- *c* - the short name for the cryptographic feature type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)

- 3A (representing a CEX3A)
- 4A (representing a CEX4A)
- 4C (representing a CEX4C)
- 4P (representing a CEX4P)
- 5A (representing a CEX5A)
- 5C (representing a CEX5C)
- 5P (representing a CEX5P)
- 6A (representing a CEX6A)
- 6C (representing a CEX6C)
- 6P (representing a CEX6P)
- X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnnn* or *N/A* - the serial number for the cryptographic feature, or *N/A* when the feature is configured as an accelerator.

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

**Operator response:** None.

**System programmer response:** None.

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

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

- *coprocessor-name* - the cryptographic feature name and how it is configured. Possible values are:
  - CRYPTO EXPRESS2 ACCELERATOR
  - CRYPTO EXPRESS2 COPROCESSOR
  - CRYPTO EXPRESS3 ACCELERATOR
  - CRYPTO EXPRESS3 COPROCESSOR
  - CRYPTO EXPRESS4 ACCELERATOR
  - CRYPTO EXPRESS4 COPROCESSOR
  - CRYPTO EXPRESS5 ACCELERATOR
  - CRYPTO EXPRESS5 COPROCESSOR
  - CRYPTO EXPRESS6 ACCELERATOR
  - CRYPTO EXPRESS6 COPROCESSOR
  - PCI CRYPTO ACCELERATOR
  - PCI X CRYPTO COPROCESSOR
- *c* - the short name for the cryptographic feature type. Possible values are:
  - A (representing a PCICA)
  - 2C (representing a CEX2C)
  - 2A (representing a CEX2A)
  - 3C (representing a CEX3C)
  - 3A (representing a CEX3A)
  - 4A (representing a CEX4A)
  - 4C (representing a CEX4C)
  - 4P (representing a CEX4P)
  - 5A (representing a CEX5A)
  - 5C (representing a CEX5C)
  - 5P (representing a CEX5P)
  - 6A (representing a CEX6A)

## CSFM200I • CSFM301A

- 6C (representing a CEX6C)
- 6P (representing a CEX6P)
- X (representing a PCIXCC)
- *ii* - the index or position where the cryptographic feature is installed.
- *nnnnnnn* or *N/A* - the serial number for the cryptographic feature, or *N/A* when the feature is configured as an accelerator.
- *mm* - the number of minutes since the request was sent to the feature.
- *asid* - the address space ID of the caller's task.

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

**Operator response:** None.

**System programmer response:** None.

---

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

**Explanation:** This is an informational message only.

**System action:** Processing continues.

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

---

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

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

**System action:** ICSF ends.

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

---

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

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

**System action:** Processing continues.

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

---

### CSFM301A FAILURE UPDATING CKT AFTER CKDS UPDATE, RC = *return\_code*, RS = *reason\_code*. MANUAL REFRESH OF CKDS REQUIRED, MEMBER *member\_name*.

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

**System action:** ICSF processing will continue.

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

**System programmer response:** None.

---

---

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

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

**System action:** ICSF processing will continue.

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

**System programmer response:** None.

---

**CSFM304A** FAILURE UPDATING TKT AFTER TKDS UPDATE, RC = *return\_code*, RS = *reason\_code*. IN STORAGE TKDS NO LONGER CURRENT, MEMBER *member\_name*.

**Explanation:** The active TKDS in use by sysplex member *member\_name* has been successfully updated by a member of the sysplex. An attempt by sysplex member *member\_name* to update the TKDS record in its in-storage copy of the TKDS has failed with return code of *return\_code* and reason code of *reason\_code*. The in-storage TKDS is now out of sync with the DASD version of the TKDS. If the message specifies RC = none RS= none, the sysplex member that initiated the TKDS I/O update left the sysplex unexpectedly and the status of the TKDS DASD I/O operation is unknown. Message CSFM306E will also be issued to identify the handle of the record for which the in-storage TKDS update failed.

**System action:** ICSF processing will continue.

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

**System programmer response:** None.

---

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

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

**System action:** ICSF processing will continue.

**Operator response:** Refer to message CSFM304A.

**System programmer response:** None.

---

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

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

**System action:** ICSF processing will continue.

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

**System programmer response:** None.

---

**CSFM308I** MEMBER *member\_name* REPORTED *action* FROM SYSPLEX GROUP *group\_name*.

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

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

## CSFM314E • CSFM409E

**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.

---

### CSFM400I CRYPTOGRAPHY - SERVICES ARE NOW AVAILABLE.

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

**System action:** Processing continues.

**Operator response:** None.

**System programmer response:** None.

---

### CSFM401I CRYPTOGRAPHY - SERVICES ARE NO LONGER AVAILABLE.

**Explanation:** ICSF is stopping.

**System action:** ICSF ends.

**Operator response:** None.

**System programmer response:** None.

---

### CSFM402I DOMAIN INDEX IN THE OPTIONS DATASET WAS IGNORED.

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

**System action:** Processing continues.

**Operator response:** Contact your system programmer.

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

---

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

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

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

**System action:** ICSF ends.



**Operator response:** Contact your system programmer.

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

#### CSFM410E ERROR IN OPTIONS DATA SET.

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

**System action:** If the message is issued in response to a refresh options data set request, the request fails and ICSF continues. If issued during ICSF initialization, ICSF ends.

**Operator response:** Contact your system programmer.

**System programmer response:** Correct the error in the options data set and restart ICSF or use the options data set refresh function to correct the refreshable options.

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

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

*kds* will be either CKDS, PKDS, or TKDS.

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

**System action:** ICSF ends.

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

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

#### CSFM451E CRYPTOGRAPHIC COPROCESSOR *pp*, FAILED.

**Explanation:** This message is no longer issued.

**System action:** None.

**Operator response:** None.

**System programmer response:** None.

#### CSFM505I CRYPTOGRAPHY - THERE ARE NO ACTIVE CRYPTOGRAPHIC COPROCESSORS.

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

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

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

**System programmer response:** None.

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

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

- Domain is not specified on the LPAR activation panel.

## CSFM507I • CSFM533I

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

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

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

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

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

---

### CSFM507I CRYPTOGRAPHY - THERE ARE NO CRYPTOGRAPHIC COPROCESSORS ONLINE.

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

**System action:** The system continues processing.

**Operator response:** None.

**System programmer response:** None.

---

### CSFM508I CRYPTOGRAPHY - THERE ARE NO CRYPTOGRAPHIC ACCELERATORS ONLINE.

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

**System action:** The system continues processing.

**Operator response:** None.

**System programmer response:** None.

---

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

**Explanation:** This message is no longer issued.

**System action:** None.

**System programmer response:** None.

---

### CSFM531I MISSED I/O INTERRUPT HAS BEEN RECOVERED FOR *coprocessor-name cii*, SERIAL NUMBER *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, 3C (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.

---

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

**Explanation:** An unusable record was detected in a KDS dataset. This record will be skipped for further processing.

*kds-type* - Either CKDS or PKDS

*number* - The record number that was detected to be unusable

*record-type* - Label for CKDS and PKDS

*record-name* - Label name for CKDS and PKDS record

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

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

**System programmer response:** None.

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

**Explanation:** A record in a KDS dataset was detected as having excess length. The record length will be internally adjusted by ICSF in order to continue processing.

*kds-type* – Either CKDS, PKDS, or TKDS

*number* – The record number that was detected as having excess length

*record-type* – Label for CKDS, PKDS, and TKDS

*record-name* – Label name for CKDS, PKDS and TKDS record

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

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

**System programmer response:** None.

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

**Explanation:** Errors were detected in some of the KDS records.

*kds-type* – Either CKDS, PKDS, or TKDS

*log-type* – Log containing messages for record errors.

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

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

**System programmer response:** None.

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

**Explanation:** An unusable record was detected in a KDS dataset.

*kds-type* – TKDS

*number* – The record number that was detected to be unusable

*record-type* – Label for TKDS

*record-name* – Label name for TKDS record

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

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

**System programmer response:** None.

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

**Explanation:** While reading the TKDS, ICSF has found records for a previously deleted PKCS #11 token that have not yet been physically removed from the TKDS.

*kds-type* – The type of key data set.

*logtype* – Log containing messages for records found.

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

**Operator response:** None.

**System programmer response:** None.

---

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

**Explanation:** An object record belonging to a previously deleted PKCS #11 token was found in the TKDS data set. The record will be removed from the ICSF in-storage cache in order to continue processing.

*kds-type* – The type of key data set.

*number* – The number of the record that was detected

*record-type* – The type of TKDS record

*record-name* – Label name for the TKDS record

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

**Operator response:** None.

**System programmer response:** None.

---

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

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

**System action:** Processing continues.

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

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

---

**CSFM600I** CONNECTION ESTABLISHED TO ICSF SYSPLEX GROUP *group\_name*, MEMBER *member\_name*.

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

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

**System programmer response:** None.

---

**CSFM602E** CONNECTION BROKEN TO ICSF SYSPLEX GROUP *group\_name*, MEMBER *member\_name*.

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

**System action:** Sysplex member *member\_name* is disconnected from the ICSF sysplex group *group\_name*.

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

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

**System programmer response:** None.

---

**CSFM603E** FAILURE IN XCF SERVICE *xcf\_service* FOR MEMBER *member\_name*, GROUP *group\_name*. RETURN CODE = *return\_code*, REASON CODE = *reason\_code*.

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

In the message text:

*return\_code*

The hexadecimal return code from the IXCJOIN/IXCLEAVE macro.

*reason\_code*

The hexadecimal reason code from the IXCJOIN/IXCLEAVE macro.

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

For an IXCLEAVE failure: none.

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

**CSFM604E** FAILURE INITIALIZING ICSF CROSS-SYSTEM SERVICES ENVIRONMENT, FUNCTION = *code*, RETURN CODE = *return\_code*, REASON CODE = *reason\_code*.

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

In the message text:

*return\_code*

The hexadecimal return code from the IXCJOIN/ISGLCRT process.

*reason\_code*

The hexadecimal reason code from the IXCJOIN/ISGLCRT process.

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

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

**Operator response:** Contact the system programmer.

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

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

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

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

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

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

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

**System action:** Processing continues.

**Operator response:** None.

**System programmer response:** None.

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

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

The key policy controls that activate the CKDS key policy are the CSF.CKDS.TOKEN.CHECK.LABEL.WARN, the

## CSFM610I • CSFM612I

CSF.CKDS.TOKEN.CHECK.LABEL.FAIL, or the CSF.CKDS.TOKEN.CHECK.NODUPLICATES resources in the XFACILIT class.

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

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

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

**System action:** Processing continues.

**Operator response:** None.

**System programmer response:** None.

---

### CSFM610I GRANULAR KEYLABEL ACCESS CONTROL IS *state*.

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

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

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

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

**System action:** Processing continues.

**Operator response:** None.

**System programmer response:** None.

---

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

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

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

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

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

**System action:** Processing continues.

**Operator response:** None.

**System programmer response:** None.

---

### CSFM612I PKA KEY EXTENSIONS CONTROL IS *state*.

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

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

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

**System action:** Processing continues.

**Operator response:** None

**System programmer response:** None

**CSFM613E ICSF SHUTDOWN DUE TO NESTED ABEND ON ICSF SUBTASK.**

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

**System action:** ICSF ends.

**Operator response:** Inform your system programmer.

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

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

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

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

**System programmer response:** None.

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

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

**System action:** ICSF processing will continue.

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

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

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

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

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

**System action:** ICSF processing will continue.

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

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

If you are unable to determine the problem by looking up these values, contact the IBM Support Center. The *supplemental-return-code*, *supplemental-reason-code*, and *flags* show IBM internal diagnostic information. You may need to provide this information to the IBM Support Center.

---

**CSFM617I** COORDINATED *operation* ACTION COMPLETED SUCCESSFULLY.

**Explanation:** The coordinated KDS administration operation completed successfully. The *operation* may be CHANGE-MK, CONVERT-DS or REFRESH.

**System action:** ICSF processing will continue.

**System programmer response:** None.

---

**CSFM618I** *kds-type* DATA SET *data-set-name* RENAMED TO *new-data-set-name*

**Explanation:** The data set with *data-set-name* was renamed to the new data set name of *new-data-set-name*.

**System action:** ICSF processing will continue.

**System programmer response:** None.

---

**CSFM619I** DSN NOT CATALOGED, DIAG=*diagnostic-information* DSN=*data-set-name*

**Explanation:** The data set with data set name of *data-set-name* is not cataloged.

**System action:** ICSF processing will continue.

**System programmer response:** Catalog the data set with *data-set-name*. Once the data set is cataloged, notify the security administrator to retry the function that failed. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure.

---

**CSFM620I** COORDINATED *operation* MAINLINE PROCESSING FAILED BECAUSE *reason-for-failure*.

**Explanation:** A coordinated KDS administration operation failed because of the *reason-for-failure*. The operation may be CHANGE-MK, CONVERT-DS or REFRESH.

**System action:** ICSF processing will continue.

**System programmer response:** Notify the security administrator for help in determining the reason for the failure. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure. If unable to resolve the problem, contact the IBM Support Center.

---

**CSFM621I** COORDINATED *operation* BACK OUT PROCESSING FAILED BECAUSE *reason-for-failure*.

**Explanation:** Back out processing for a coordinated operation failed because of *reason-for-failure*. The operation may be CHANGE-MK, CONVERT-DS or REFRESH.

**System action:** Depending on the *reason-for-failure*, ICSF processing may continue or may shutdown across all instances of ICSF sharing the same active KDS.

**System programmer response:** Notify the security administrator for help in determining the reason for the failure. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure. If unable to resolve the problem, contact the IBM Support Center.

---

**CSFM622I** COORDINATED *operation* PROGRESS: *operation-progress*.

**Explanation:** This message indicates the progress of the coordinated operation. The operation may be CHANGE-MK, CONVERT-DS or REFRESH.

**System action:** ICSF processing will continue.

**System programmer response:** None.

---

**CSFM623I** CATALOG SEARCH FAILED. MODID=*module-id* RC=*return-code* RSN=*reason-code*.

**Explanation:** If this message is issued during ICSF startup, a problem occurred while retrieving catalog information about the active KDS. If this message is issued during a coordinated change master key or a coordinated refresh operation, a problem occurred while retrieving catalog information about the new KDS. The problem occurred in the module identified by *module-id*. The *return-code* and *reason-code* indicate what type of problem occurred.



**System action:** If this message is issued during ICSF startup, the KDS sysplex group will convert to the sysplex communication protocol used prior to ICSF FMID HCR7790, and coordinated KDS administrative functions will be unavailable. If this message is issued during a coordinated change master key or a coordinated refresh operation, the operation will fail. In either case, ICSF processing will continue.

**System programmer response:** If this message is issued during ICSF startup, ensure that the active KDS is correctly cataloged on the system. If this message is issued during a coordinated change master key or a coordinated refresh operation, notify the security administrator and make sure the new target data set is correctly cataloged on the system.

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

**CSFM624I** *compmode compstat* **COMPLIANCE MODE IS REQUIRED TO COMPLETE THE REENCIPHER OPERATION**

**Explanation:** There are keys in the key data set that are being checked or reenciphered that require an active compliance mode to be reenciphered. There are no coprocessors active in the compliance mode required.

*compmode*

The compliance mode. Possible values are:

- PCI-HSM (representing the Payment Card Industry-Hardware Security Module compliance mode).

*compstat*

The state of the compliance mode. Possible values are:

- 2016 (The compliance mode is active at 2016 level).

The value of *compstat* is dependent on *compmode*. Possible *compmode-compstat* combinations are:

*Table 2. compmode-compstat combinations*

<i>compmode</i>	<i>compstat</i>	Description
PCI-HSM	2016	PCI-HSM 2016 mode.

**System action:** The operation fails.

**System programmer response:** Configure one or more coprocessors in the required compliance mode.

**CSFM625I** SET *key-type* MASTER KEY FAILED FOR COPROCESSOR SERIAL NUMBER *serial-number*.

**Explanation:** A failure occurred when attempting to set a new *key-type* master key for the coprocessor with serial number *serial-number*. *key-type* may be DES, AES, RSA, ECC, P11, or RCS. *serial-number* is the serial number of the coprocessor that experienced the failure.

**System action:** ICSF processing will continue.

**System programmer response:** Notify the security administrator to ensure that the new master key register for *key-type* is correctly loaded. If sharing the KDS across a sysplex and performing a coordinated change master key operation, the security administrator should ensure all instances of ICSF sharing the same active KDS have the same new master key value loaded into the new master key register for *key-type*. After correcting the new master key register or registers, the security administrator should retry the operation.

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

**CSFM626I** COORDINATED *operation* COMPLETE, RC=*return-code* RSN=*reason-code* CANCEL RSN=*cancel-reason-code*.

**Explanation:** The coordinated operation has completed. The *operation* may be CHANGE-MK, CONVERT-DS or REFRESH. If a failure occurred during the operation, the *return-code*, *reason-code*, and *cancel-reason-code* may be used to determine the cause of the failure.

**System action:** ICSF processing will continue.

**System programmer response:** In the case of a failure, an explanation of the *return-code*, *reason-code*, and

## CSFM628I • CSFM632I

*cancel-reason-code* values can be found in the Return and Reason Codes of *z/OS Cryptographic Services ICSF Application Programmer's Guide*. Alternatively, refer to the return and reason code information for the CSFEUTIL program described in the *z/OS Cryptographic Services ICSF Administrator's Guide*.

---

**CSFM628I** SYSTEM *system-name* HAS MISSED A *kds-type* UPDATE. DIAG=*diagnostic-information*.

**Explanation:** The system with *system-name* has missed a sysplex KDS update. *kds-type* indicates which type of KDS update was missed. *diagnostic-information* contains additional diagnostic information about the failure.

*diagnostic-information* may be the following:

- PREP - This indicates that an internal ICSF sysplex message was missed. This message is used during internal KDS I/O processing in a sysplex environment.
- '10'X - This indicates that a sysplex KDS record create was missed. This message is used to notify sysplex members of a KDS record create.
- '11'X - This indicates that a sysplex KDS record update was missed. This message is used to notify sysplex members of a KDS record update.
- '13'X - This indicates that a sysplex KDS record delete was missed. This message is used to notify sysplex members of a KDS record delete.

**System action:** ICSF processing continues, however the system indicated in this message by *system-name* has missed a KDS update. This system's in-storage KDS will now be out of sync with other members in the sysplex group sharing the same active KDS. The next time a KDS update is processed against this systems active KDS, ICSF will recognize that its in-storage KDS is out of sync and will perform an internal KDS refresh to get back in sync.

**Operator response:** None.

**System programmer response:** Notify the security administrator to perform a single-system KDS refresh on the system where the KDS is out of sync.

---

**CSFM629I** IDCAMS-processor-message.

**Explanation:** This message is used to route IDCAMS processor messages to the job log. This message is used during the rename step of a coordinated change master key or coordinated refresh operation.

**System action:** ICSF processing continues.

**System programmer response:** If this message indicates a failure, notify the security administrator for help in determining the reason for the failure. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure. If unable to resolve the problem, contact the IBM Support Center.

---

**CSFM630I** *kds-type* RENAME FAILED: *original-name* TO *new-name*

**Explanation:** The rename step of the a coordinated change master key or coordinated refresh operation failed. *kds-type* indicates which KDS this rename was being performed for. *original-name* indicates the original name of the KDS. *new-name* indicates the new name of the KDS.

**System action:** ICSF processing continues.

**System programmer response:** Notify the security administrator for help in determining the reason for the failure. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure. If unable to resolve the problem, contact the IBM Support Center.

---

**CSFM632I** CRITICAL ICSF SUBTASK *name* CAN NOT BE RESTARTED. ICSF WILL BE TERMINATED.

**Explanation:** The ICSF subtask specified by *name* experienced a problem that ICSF tried to recover. ICSF recovery was unable to restart this subtask. This subtask is critical to ICSF processing. ICSF will terminate without this subtask.

**System action:** ICSF terminates.

**System programmer response:** Restart ICSF. If this problem reoccurs, contact the IBM Support Center.

---

---

**CSFM633I** ICSF SUBTASK *subtask* CAN NOT BE RESTARTED. ICSF CAPABILITIES REDUCED.

**Explanation:** The ICSF subtask specified by *name* experienced a problem that ICSF tried to recover. ICSF recovery was unable to restart this subtask. This subtask is not critical to ICSF processing. ICSF processing will continue with limited capabilities.

**System action:** ICSF continues processing with limited capabilities.

**System programmer response:** Restart ICSF. If this problem reoccurs, contact the IBM Support Center.

---

**CSFM634I** *log-type* UPDATE TIMED OUT WAITING FOR ENQ *resource*.

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

**System action:** ICSF processing will continue. The internal *kds-type* cache will be refreshed.

**Operator response:** The operator should issue D GRS,RES=*resource* from the message to determine which system or systems hold the *resource*. The operator should determine if action should be taken to cause the holding system to release its ENQ on the *kds-type resource*.

**System programmer response:** None.

---

**CSFM635I** *kds-type* CACHE ERROR DETECTED. AUTOMATIC REFRESH IN PROGRESS.

**Explanation:** An error was detected in the in-storage cache of the *kds-type* dataset. The error will be corrected internally by automatically refreshing the internal *kds-type* cache.

**System action:** ICSF processing will continue. The internal *kds-type* cache will be refreshed.

**Operator response:** None.

**System programmer response:** None.

---

**CSFM636I** SYSTEM *system-name* FAILURE FOR COORDINATED *kds-type* ACTIVITY. MSGTYPE=*message-type* RC=*return-code* RSN=*reason-code*.

**Explanation:** The system identified by *system-name* experienced a failure performing coordinated KDS activity. A *reason-code* of C3A indicates that the system *system-name* is not being responsive to the originator of the coordinated KDS function.

- *system-name* - Name of the system which either detected a problem or failed to respond.
- *kds-type* - KDS type for the coordinated activity.
- *message-type* - Internal diagnostic information.
- *return-code* - Return code either returned by the remote system or set by the originating system in case of timeout.
- *reason-code* - Reason code either returned by the remote system or set by the originating system in case of timeout.

**System action:** ICSF processing continues.

**System programmer response:** Notify the security administrator for help in determining the reason for the failure. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure.

---

**CSFM637I** FAILURE UPDATING *kds-type* CACHE, RC = *return-code*, RS = *reason-code*. AUTOMATIC REFRESH OF *kds-type* DRIVEN BY SYSTEM *system-name*.

**Explanation:** A failure occurred while updating the in-storage cache of the *kds-type* dataset. The *kds-type* update operation will be failed with *return-code/reason-code*. System *system-name* will internally correct the problem by automatically refreshing the internal *kds-type* cache.

**System action:** ICSF processing will continue. The internal *kds-type* cache will be refreshed.

**Operator response:** None.

**System programmer response:** None.

**CSFM638I** *kds-type* IS UNUSABLE DUE TO MISSING RECORDS. DSN=*dataset-name*.

**Explanation:** *kds-type* IS UNUSABLE DUE TO MISSING RECORDS, DSN=*dataset-name*.

*kds-type* - CKDS, PKDS or TKDS

*dataset-name* - The name of the dataset that is missing records.

**System action:** ICSF will shut down.

**Operator response:** Contact the ICSF administrator to restore the missing records.

**System programmer response:** None.

**CSFM639I** ICSF COMMUNICATION LEVEL FOR *kds-type* CHANGED FROM *previous-level* TO *new-level*.

**Explanation:** The ICSF sysplex communication level for the *kds-type* changed from the *previous-level* to the *new-level*. *previous-level* may be 0, 2, or 3. *new-level* may be 0, 2, or 3. The coordinated change master key and coordinated refresh utilities are only available when all ICSF instances in the sysplex are at ICSF sysplex communication level 2 or higher for the *kds-type*. The coordinated convert utility (convert KDS to KDSR format) is only available when all ICSF instances in the sysplex are at ICSF sysplex communication level 3 or higher for the *kds-type*.

*kds-type* - CKDS, PKDS or TKDS

*previous-level* - 0, 2, or 3

*new-level* - 0, 2, or 3

ICSF FMID	CKDS communication level	PKDS communication level	TKDS communication level
HCR7780 and earlier	0	0	0
HCR7790	2	0	0
HCR77A0	2	2	2
HCR77A1 and later	3	3	3

**System action:** ICSF processing will continue. ICSF will process KDS updates using the communication level indicated by this message.

**Operator response:** None.

**System programmer response:** None.

**CSFM640I** ICSF RELEASE FMID=*fmid*.

**Explanation:** This message indicates the ICSF release FMID that is currently started.

**System action:** Processing continues.

**Operator response:** None

**System programmer response:** None.

**CSFM641I** INCORRECT MKVP DETECTED IN *kds-type* RECORD *name*.

**Explanation:** This message is no longer issued.

**System action:** None.

**System programmer response:** None.

**CSFM642I** UNEXPECTED *kds-type* REENCIPHER TERMINATED IN MID-REENCIPHER. RETURN CODE = *return-code*, REASON CODE = *reason-code*.

**Explanation:** An unexpected failure occurred while reenciphering the KDS specified by *kds-type*.

**System action:** The reencipher will fail.

**Operator response:** Contact the ICSF administrator to analyze the return and reason codes returned for the reencipher failure.

**System programmer response:** None.

---

**CSFM643I CRITICAL ICSF SUBTASK FAILURE. ICSF WILL BE TERMINATED.**

**Explanation:** An ICSF subtask has suffered a failure that has caused ICSF to terminate.

**System action:** ICSF will Terminate.

**Operator response:** Contact the ICSF administrator to analyze the ICSF job log and determine what has caused this failure. If the ICSF joblog does not indicate the problem, contact the IBM support center.

**System programmer response:** None.

---

**CSFM644E DOMAIN INDEX IN THE OPTIONS DATASET IS NOT SPECIFIED IN THE ACTIVATION PROFILE.**

**Explanation:** The value of the DOMAIN parameter in the installation options specifies a cryptographic usage domain that this LPAR cannot access because it is not in the LPAR Activation Profile.

**System action:** ICSF ends.

**Operator response:** Contact your system programmer.

**System programmer response:** Ensure that the specified Usage Domain has been assigned to your LPAR. If this does not resolve the problem, contact the IBM Support Center.

---

**CSFM645I INCORRECT METADATA DETECTED IN *kds-type* RECORD *label*.**

**Explanation:** A *kds-type* KDS record in storage was detected as having damage in the KDSR metadata area.

*kds-type* is one of CKDS, PKDS, or TKDS.

*label* is the label name (for CKDS or PKDS) or handle (for TKDS).

**System action:** ICSF will ABEND the unit of work.

**Operator response:** None.

**System programmer response:** Notify the ICSF administrator.

---

**CSFM649I SPECIAL SECURE MODE IS *setting***

**Explanation:** This message is written to the system console and ICSF joblog each time the Special Secure Mode (SSM) setting changes. The initial SSM setting is based on the SSM option in the installation options dataset.

*setting* is either ENABLED or DISABLED

**System action:** When the setting is DISABLED, operations requiring SSM to be enabled will fail. When the setting is ENABLED, ICSF will attempt to process requests requiring that SSM be enabled.

**Operator response:** None.

**System programmer response:** Examine the content of the message and if unexpected, see the *z/OS Cryptographic Services ICSF System Programmer's Guide* for information on how to change the SSM setting.

---

**CSFM650I CSFSERV AUTHORIZATION CHECK FOR *service* IS *setting***

**Explanation:** This message is written to the system console and ICSF joblog each time the setting changes. By default, the setting is ENABLED. It tells the installation whether or not CSFSERV SAF authorization checks may be performed for the set of services indicated.

*service* is either ONE-WAY HASH SERVICES or RANDOM NUMBER GENERATE SERVICES

*setting* is either ENABLED or DISABLED

## CSFM651I • CSFM654I

The ONE-WAY HASH SERVICES include CSNBOWH, CSNEOWH, CSNBOWH1, CSNEOWH1, CSFPOWH, and CSFPOWH6. The RANDOM NUMBER GENERATE SERVICES include CSNBRNG, CSNERNG, CSNBRNGL, CSNERNGL, CSFPPRF, and CSFPPRF6.

**System action:** When the setting is DISABLED, no CSFSERV SAF checks will be performed for the services indicated. When the setting is ENABLED, normal CSFSERV SAF authorization checking will be attempted for the services indicated.

**Operator response:** None.

**System programmer response:** Contact your security administrator to examine the content of the message, and if unexpected, see *z/OS Cryptographic Services ICSF Administrator's Guide* for information on how to change whether or not the CSFSERV SAF check will be performed for the indicated services.

---

### CSFM651I THE FOLLOWING SYSTEMS ARE PREVENTING A COORDINATED *operation: list-of-systems*

**Explanation:** The coordinated change master key and coordinated refresh operations may only be performed when all systems in the KDS sysplex group are at the ICSF FMID HCR7790 release level or higher. The coordinated conversion operation may only be performed when all systems in the KDS sysplex group are at the ICSF FMID HCR77A1 release level or higher. If an instance of ICSF joins the KDS sysplex group at a level before the ICSF FMID HCR7790 release level, then, regardless of active KDS, the coordinated change master key and coordinated refresh operations will be unavailable.

*operation* may be CHANGE-MK, CONVERT-DS or REFRESH, and indicates whether a coordinated change master key, coordinated conversion, or coordinated refresh operation was requested.

*list-of-systems* indicates the systems containing an instance of ICSF at a previous level than the HCR7790 release level.

**System action:** ICSF processing continues.

**System programmer response:** In order to perform a coordinated change master key or coordinated refresh operation, systems running a release of ICSF before FMID HCR7790 must be removed from the KDS sysplex group or upgraded to FMID HCR7790 or higher. In order to perform a coordinated conversion, systems running a release of ICSF before FMID HCR77A1 must be removed from the KDS sysplex group or upgraded to FMID HCR77A1 or higher. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure.

---

### CSFM652I *kds-type* IS UNUSABLE. DSN = *dataset-name*, REASON = *reason-code*

**Explanation:** This message is no longer issued.

**System action:** None.

**Operator response:** None.

**System programmer response:** None.

---

### CSFM653I *kds* LOADED *num\_record* RECORDS WITH AVERAGE SIZE *average\_size*

**Explanation:** This informational message is provided to assist in optimizing VSAM record sizes. A key data set was loaded into memory by ICSF. The data set has *num\_record* records in it and the average size of the records is *average\_size*. The *kds* may be CKDS, PKDS or TKDS.

**System action:** Processing continues.

**Operator response:** None.

**System programmer response:** None.

---

### CSFM654I KEY ARCHIVING USE CONTROL IS *state*.

**Explanation:** The key store policy key archiving use control is currently in the specific *state*. The *state* may be ENABLED or DISABLED.

The profile that activates the key archive use control is the CSF.KDS.KEY.ARCHIVE.USE resource in the XFACILIT class.

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

This message may be issued during ICSF initialization and when ICSF detects that the key store policy is changed.

**System action:** Processing continues.

**Operator response:** None.

**System programmer response:** None.

**CSFM655I AN ARCHIVED RECORD *label* IN THE ACTIVE *key-data-set* WAS REFERENCED.**

**Explanation:** An attempt to use an archived record *label* occurred. The *key-data-set* can be CKDS, PKDS, or TKDS. The results of the request for the archived record will depend on the key archive use policy. An SMF type 82 audit record was produced.

This message is only issued for the first attempt to use a record. Subsequent attempts will produce an audit record only.

**System action:** Processing continues.

**Operator response:** None.

**System programmer response:** Notify the ICSF administrator.

**CSFM657I FAILURE ON CSVDYNEX FOR EXIT *exitname* RETURN CODE = *return-code*, REASON CODE = *reason-code*.**

**Explanation:** An invocation of CSVDYNEX for the exit *exitname* failed with *return-code* and *reason-code*. See *MVS Programming Authorized Assembler Services Reference Vol 1 (ALESERV-DYNALLOC)* for the explanation of possible CSVDYNEX return codes and reason codes.

This message is issued if an invocation of CSVDYNEX fails for a exit.

**System action:** Processing continues. The exit is disabled.

**Operator response:** Contact your system programmer.

**System programmer response:** Contact the IBM Support Center.

| **CSFM658I INCOMPLETE CLIENT CLEANUP. JOB=*jobname* SERVICE=*service-name*.**

| **Explanation:** This is a recovery message. The processing of an ICSF ENQ failed to release the ENQ and recovery  
| was initiated. ICSF client cleanup has released the ENQ for the client identified for the job *jobname*. The ICSF callable  
| service in use at the time was *service-name*.

| **System action:** ICSF processing continues.

| **System programmer response:** None.

| **ICSF Administrator response:** If this message is issued multiple times, set the following SLIP trap and contact IBM  
| Support Center:

| SLIP SET,MSGID=CSFM658I,A=SVCD,SDATA=(CSA,SQA,RGN,TRT,SUM),AL=(H,P,S),END

**CSFM659I FIPS 140 KNOWN ANSWER TEST FAILED. FEATURE CODE 3863 IS NOT INSTALLED.**

**Explanation:** The FIPS 140 tests failed because the CPACF feature (code 3863) is not installed or enabled. ICSF requires feature code 3863 be installed and enabled.

**System action:** ICSF terminates.

**Operator response:** None.

**System programmer response:** Enable the CPACF feature.

---

**CSFM660I** *key-data-set* **RECORD label FAILED: RC = nnnnnnnnn, RS = nnnnnnnnn**

**Explanation:** An attempt to validate or reencipher a *key-data-set* record was unsuccessful. The *key-data-set* can be CKDS, PKDS, or TKDS.

This message is issued for each failing label.

For CKDS, the *label* is the CKDS label and type concatenated with a slash between them. For PKDS, the *label* is just the PKDS label. For TKDS, the *label* is the TKDS handle.

**System action:** Processing continues.

**Operator response:** None.

**System programmer response:** Notify the ICSF administrator.

---

**CSFM661I** *key-data-set* **RECORD label: validation-message**

**Explanation:** An attempt to validate or reencipher a *key-data-set* record detected a problem. The *key-data-set* can be CKDS or PKDS.

For CKDS, the *label* is the CKDS label and type concatenated with a slash between them. For PKDS, the *label* is just the PKDS label.

This message is issued for each record where a problem was detected. If *validation-message* begins with 'ERROR', the problem detected will cause a reencipher of the CKDS or PKDS to fail.

**System action:** Processing continues.

**Operator response:** None.

**System programmer response:** Notify the ICSF administrator.

---

**CSFM662I** *kds-type* **RECORD number METADATA DAMAGE DETECTED**, *record-type record-name*

**Explanation:** A record in a KDS dataset was detected as having damage in the KDSR metadata area. The KDSR metadata area will be reset to initial state.

*kds-type* is one of CKDS, PKDS, or TKDS.

*number* is the record number that was detected as having damage in the KDSR metadata area.

*record-type* is LABEL (for CKDS or PKDS) or HANDLE (for TKDS).

*record-name* is the label name (for CKDS or PKDS) or handle (for TKDS).

**System action:** ICSF processing continues. The KDSR metadata area and length of this record will be internally adjusted in order to continue processing. These adjustments will not be written back out to the KDS dataset immediately, but instead on the next update to the record or on the next Coordinate Change Master Key operation.

**Operator response:** None.

**System programmer response:** None.

---

**CSFM663I** *kds-type* **CLUSTER ID ERROR: kdsold, kdsnew.**

**Explanation:** This system attempted to use KDS *kdsnew* which has a KDS cluster identifier that matches KDS *kdsold*. The KDS cluster identifier is based on the location of the KDS within the volume. This means that *kdsold* was moved without a restart of all ICSF instances sharing *kdsold* and so ICSF continues to use the original cluster identifier for *kdsold*. *kdsnew* now resides in the exact location on the volume previously occupied by *kdsold*, causing the cluster identifiers to not be unique. A KDS cluster is made up of all the systems sharing a KDS in the sysplex. The KDS cluster identifier determines the ICSF instances which make up a KDS cluster and must be unique for each KDS.

*kds-type* is one of CKDS, PKDS, or TKDS.

*kdsold* is the active KDS for one or more ICSF instances.

*kdsnew* is the KDS that an ICSF instance is attempting to use.

**System action:** The current operation ends. If this error is detected at ICSF startup, ICSF terminates.



**Operator response:** Contact the system programmer.

**System programmer response:** You may either:

1. Move *kdsnew* to a different volume and retry the operation
2. Move *kdsnew* to a different location on the volume and retry the operation. One way to ensure *kdsnew* ends up at a different location is:
  - a. Allocate a temporary KDS, *kdstmp*, on the volume.
  - b. If *kdsnew* is not empty, copy the contents of *kdsnew* to *kdstmp*.
  - c. Delete *kdsnew*.
  - d. Rename *kdstmp* to *kdsnew*.
3. Shutdown all ICSF instances that are sharing *kdsold*. Once all instances are down, restart those instances and retry the operation.

**CSFM664I ICSF ENCOUNTERED CONTINUOUS ISGQUERY FAILURES:** *kds-type dsname RC=rc RS=rs*

**Explanation:** During a user-initiated KDS operation (for example, KDS Refresh, Change Master Key), ICSF was unable to complete the operation due to continuous failures from the ISGQUERY service. This error is often associated with an inability to communicate with other systems in the sysplex.

*kds-type* is one of CKDS, PKDS, or TKDS.

*dsname* is the name of the KDS that was being processed as part of the operation.

*rc* is the return code from the ISGQUERY service in hexadecimal.

*rs* is the reason code from the ISGQUERY service in hexadecimal.

**System action:** The current operation ends.

**Operator response:** Look for signs of communication problems among systems in the sysplex and resolve them. Some indications of a communication problem include issuance of one or more of the following messages: IXC402D, ISG378I (z/OS V1R13 and higher). If there are no signs of a communication problem, contact the IBM Support Center. Once the issue is resolved, the operation can be retried.

**System programmer response:** None.

**CSFM665E ICSF WAITING FOR RESOLUTION TO ISGQUERY FAILURES:** *kds-type dsname RC=rc RS=rs*

**Explanation:** ICSF cannot continue because of continuous failures from the ISGQUERY service. This error is often associated with an inability to communicate with other systems in the sysplex. Until the issue is resolved, some of ICSF's functionality will be affected.

*kds-type* is one of CKDS, PKDS, or TKDS.

*dsname* is the name of the active KDS.

*rc* is the return code from the ISGQUERY service in hexadecimal.

*rs* is the reason code from the ISGQUERY service in hexadecimal.

**System action:** ICSF waits for the issue to be resolved. Once the issue is resolved, ICSF processing continues.

**Operator response:** Look for signs of communication problems among systems in the sysplex and resolve them. Some indications of a communication problem include issuance of one or more of the following messages: IXC402D, ISG378I (z/OS V1R13 and higher). If there are no signs of a communication problem, contact the IBM Support Center.

**System programmer response:** None.

**CSFM666I** *kds-type DATASET dsname mode FOR I/O.*

**Explanation:** In response to a SETICSF ENABLE or DISABLE command when the SYSPLEX=YES option is in effect, a KDS has been enabled or disabled for updates. This message appears on every participating member in the sysplex group when the state of the KDS has changed (for example, changed from enabled to disabled).

In the message text:

## CSFM667I

*kds-type* The key data set type, either CKDS, PKDS, or TKDS.

*dsname* The dataset name of the KDS.

*mode* The action performed on the KDS, either ENABLED or DISABLED.

**System action:** The system continues processing.

**Operator response:** None.

**System programmer response:** None.

---

**CSFM667I** *hh:mm:ss* SETICSF *type* [*idr*] *text*

**Explanation:** In response to a SETICSF command where *type* is the SETICSF command being processed.

In the message text:

*hh:mm:ss*

The time when the message was issued, in hours (00 through 23), minutes (00 through 59), and seconds (00 through 59).

*type* One of the following:

- Activate
- Add
- Check
- DeAct
- Delete
- IO Cntl
- Options
- Restart

*idr* A 3-digit decimal identifier. This identifier is used with the CONTROL C,D command to cancel status displays that are:

- Written on typewriter or display consoles.
- Displayed in-line (not in a display area) on display (CRT) consoles.

This identifier does not appear when the display is presented in a display area on a display console.

*text* The local system's response to the SETICSF command:

- SETICSF ACTIVATE,RD:  
SERIAL NUMBER=*nnnnnnn* PORT=*nnnn* LEVEL=*level*  
HOST/IP@=*hhhhh*  
*cii*  
*sysname state Sockets=number-sockets*
- SETICSF ADD,RD:  
SERIAL NUMBER=*nnnnnnn* PORT=*nnnn* LEVEL=*level*  
HOST/IP@=*hhhhh*  
*cii*  
*sysname state Sockets=number-sockets*
- SETICSF CHECK,RD:  
SERIAL NUMBER=*nnnnnnn* PORT=*nnnn* LEVEL=*level*  
HOST/IP@=*hhhhh*  
*cii*  
*sysname state Sockets=number-sockets*
- SETICSF ENABLE or SETICSF DISABLE:  
I/O *mode* ON *sysname* FOR *kdstype*  
*dsname*
- SETICSF DEACTIVATE:

- ```

coprocessor-name cii SERIALNR=nnnnnnnn
sysname state
mk MASTER KEY IS NO LONGER AVAILABLE ON SYSTEMS:
sysname sysname sysname ...

```
- SETICSF DEACTIVATE,RD:

```

SERIAL NUMBER=nnnnnnnn PORT=nnnn LEVEL=level
HOST/IP@=hhhhh
cii
sysname state Sockets=number-sockets

```
  - SETICSF DELETE,RD:

```

SERIAL NUMBER=nnnnnnnn PORT=nnnn LEVEL=level
HOST/IP@=hhhhh
cii
sysname state Sockets=number-sockets

```
  - SETICSF OPTIONS:

```

refoption in seconds: xxxxxxx
MASTERKCVLEN set to m1en
adoption

```
  - SETICSF OPTIONS,REFRESH may contain one of the following:
    - All supported changes accepted.
    - An ABEND occurred while processing options.
    - Check ICSF joblog for unsupported changes.
    - Error processing option data set.
    - Error trying to build the CICS wait list.
    - No changes detected to supported options.
    - Some changes accepted. Check ICSF joblog.
    - Syntax error. Check ICSF joblog.
    - Unable to allocate the option data set.
    - Unable to retrieve option data set attrs.
  - SETICSF RESTART:

```

coprocessor-name cii SERIALNR=nnnnnnnn
sysname state

```
  - SETICSF RESTART,RD:

```

SERIAL NUMBER=nnnnnnnn PORT=nnnn LEVEL=level
HOST/IP@=hhhhh
cii
sysname state Sockets=number-sockets

```

where:

*kds-type* The key data set type, either CKDS, PKDS, or TKDS.

*dsname* The dataset name of the KDS.

*mode* The action performed on the KDS, either ENABLED or DISABLED.

*sysname*

The name of the sysplex member that took part in the SETICSF command.

*mk* Identifies the master key that is no longer available and may have the value of AES, DES, ECC, P11, or RSA.

*coprocessor-name*

The type of cryptographic coprocessor and may have the value of:

- PCI CRYPTOGRAPHIC ACCELERATOR
- CRYPTO EXPRESS2 COPROCESSOR
- CRYPTO EXPRESS2 ACCELERATOR
- CRYPTO EXPRESS3 COPROCESSOR
- CRYPTO EXPRESS3 ACCELERATOR

## CSFM667I

- CRYPTO EXPRESS4 COPROCESSOR
- CRYPTO EXPRESS4 ACCELERATOR
- CRYPTO EXPRESS5 COPROCESSOR
- CRYPTO EXPRESS5 ACCELERATOR
- CRYPTO EXPRESS6 ACCELERATOR
- CRYPTO EXPRESS6 COPROCESSOR
- PCI X CRYPTO COPROCESSOR

*c* The short name for the server. For example, 1R (representing a first generation remote regional cryptographic server).

*ii* The index or position where the cryptographic coprocessor is installed.

*mlen* The new MASTERKCVLEN setting.

*nnnnnnn*

The serial number for the cryptographic coprocessor.

*refoption*

The ICSF reference date option that was changed. May have the value:

Reference date interval in seconds: xxxxxxxx

Reference date period in seconds: xxxxxxxx

*audoption*

The ICSF key usage audit option that was changed. May be one of the following:

AUDITKEYLIFECKDS: Audit CCA symmetric key lifecycle events

| SYSNAME | LABEL | TOKEN |
|---------|-------|-------|
| sysname | yn    | yn    |

AUDITKEYLIFEPKDS: Audit CCA asymmetric key lifecycle events

| SYSNAME | LABEL | TOKEN |
|---------|-------|-------|
| sysname | yn    | yn    |

AUDITKEYLIFETKDS: Audit PKCS #11 key lifecycle events

| SYSNAME | TOKOBJ | SESSOBJ |
|---------|--------|---------|
| sysname | yn     | yn      |

AUDITKEYUSGCKDS: Audit CCA symmetric key usage events

| SYSNAME | LABEL | TOKEN | Interval | Days/HH.MM.SS |
|---------|-------|-------|----------|---------------|
| sysname | yn    | yn    |          | ddd/hh.mm.ss  |

AUDITKEYUSGPKDS: Audit CCA asymmetric key usage events

| SYSNAME | LABEL | TOKEN | Interval | Days/HH.MM.SS |
|---------|-------|-------|----------|---------------|
| sysname | yn    | yn    |          | ddd/hh.mm.ss  |

AUDITPKCS11USG: Audit PKCS #11 usage events

| SYSNAME | TOKOBJ | SESSOBJ | NOKEY | Interval | Days/HH.MM.SS |
|---------|--------|---------|-------|----------|---------------|
| sysname | yn     | yn      | yn    |          | ddd/hh.mm.ss  |

*xxxxxxx*

The new option setting, in seconds.

*yn* The current setting of the option. May have the value of Yes or No.

**System action:** The system continues processing. If the message, *mk NO LONGER AVAILABLE ON SYSTEMS: sysname*, is displayed, callable services that require that master key will fail.

**Operator response:** If the message, *mk NO LONGER AVAILABLE ON SYSTEMS: sysname*, is displayed, contact your system programmer.

**System programmer response:** If the message, *mk NO LONGER AVAILABLE ON SYSTEMS: sysname*, is displayed, work with the ICSF administrator to determine the reason for the inactive master key. See the migration topic in *z/OS Cryptographic Services ICSF System Programmer's Guide*. The *mk* master key should be loaded on all coprocessors.

**CSFM668I** *hh:mm:ss ICSF command [idr] text*

**Explanation:** In response to a DISPLAY ICSF command where *command* is the DISPLAY ICSF command being processed.

In the message text:

*hh:mm:ss*

The time when the message was issued, in hours (00 through 23), minutes (00 through 59), and seconds (00 through 59).

*command*

One of the following:

- CARDS
- MKS
- KDS
- OPTIONS
- LIST
- RD

*idr*

A 3-digit decimal identifier. This identifier is used with the CONTROL C,D command to cancel status displays that are:

- Written on typewriter or display consoles.
- Displayed in-line (not in a display area) on display (CRT) consoles.

This identifier does not appear when the display is presented in a display area on a display console.

*text*

The local system's response to the DISPLAY ICSF command:

- For DISPLAY ICSF,CARDS:

```
ACTIVE DOMAIN = domain
coprocessor-name cii
STATUS=status SERIAL#=nnnnnnnn LEVEL=level CLIC=CLIC level (if applicable)
REQUESTS ACTIVE=nnnn
compmode1, compmode2, ... ,compmodeN (if applicable)
```

- For DISPLAY ICSF,LIST:

```
Systems supporting SETICSF and DISPLAY ICSF commands:
sysname fmid DOMAIN = domain
```

- For DISPLAY ICSF,MKS:

```
SYSNAME: sysname DOMAIN: domain CPC Name: cpc_name
FEATURE# SERIAL# STATUS AES DES ECC RSA P11
cii nnnnnnn status S S S S S
```

- For DISPLAY ICSF,KDS:

```
CKDS dsname
FORMAT=format SYSPLEX=sysplex MKVPs=mkvplist
PKDS dsname
FORMAT=format SYSPLEX=sysplex MKVPs=mkvplist
TKDS dsname
FORMAT=format SYSPLEX=sysplex MKVPs=mkvplist
```

- For DISPLAY ICSF,OPTIONS:

```
SYSNAME = sysname ICSF LEVEL = fmid
LATEST ICSF CODE CHANGE = builddate
Refdate update interval in Days/HH.MM.SS = ddd/hh.mm.ss
Refdate update period in Days/HH.MM.SS = ddd/hh.mm.ss
MASTERKCVLEN = display mlen digits
AUDITKEYLIFEKDS: Audit CCA symmetric key lifecycle events
SYSNAME LABEL TOKEN
sysname yn yn
AUDITKEYLIFEPKDS: Audit CCA asymmetric key lifecycle events
SYSNAME LABEL TOKEN
sysname yn yn
AUDITKEYLIFETKDS: Audit PKCS #11 key lifecycle events
```

## CSFM668I

```

SYSNAME  TOKOBJ  SESSOBJ
sysname  yn      yn
AUDITKEYUSGCKDS: Audit CCA symmetric key usage events
SYSNAME  LABEL   TOKEN   Interval Days/HH.MM.SS
sysname  yn      yn      ddd/hh.mm.ss
AUDITKEYUSGPKDS: Audit CCA asymmetric key usage events
SYSNAME  LABEL   TOKEN   Interval Days/HH.MM.SS
sysname  yn      yn      ddd/hh.mm.ss
AUDITPKCS11USG: Audit PKCS #11 usage events
SYSNAME  TOKOBJ  SESSOBJ  NOKEY Interval Days/HH.MM.SS
sysname  yn      yn      yn      ddd/hh.mm.ss
```

- For DISPLAY ICSF,RD:  
TKDS = *tkds-name*  
RCS MKVP FROM TKDS = *rscmkvp*  
SERIAL NUMBER=*nnnnnnnn* PORT=*port* LEVEL=*level*  
HOST/IP@=*hhhhh*  
REGIONAL CRYPTO SRV *cii*  
*sysname status* Sockets=*number-sockets*  
REQUESTS ACTIVE=*mmm*  
NMK = *nmkvp* State = *nmkstate*

where:

*builddate*

The latest executable build date for the active ICSF instance.

*c*

The short name for the server. For example, 1R (representing a first generation remote regional cryptographic server).

*coprocessor-name*

The type of cryptographic device and may have the value of:

- PCI CRYPTOGRAPHIC ACCELERATOR
- CRYPTO EXPRESS2 COPROCESSOR
- CRYPTO EXPRESS2 ACCELERATOR
- CRYPTO EXPRESS3 COPROCESSOR
- CRYPTO EXPRESS3 ACCELERATOR
- CRYPTO EXPRESS4 COPROCESSOR
- CRYPTO EXPRESS4 ACCELERATOR
- CRYPTO EXPRESS5 COPROCESSOR
- CRYPTO EXPRESS5 ACCELERATOR
- CRYPTO EXPRESS6 ACCELERATOR
- CRYPTO EXPRESS6 COPROCESSOR
- PCI X CRYPTO COPROCESSOR

*cpc\_name*

The name of the CPC.

*domain*

The active domain of the ICSF instance.

*dsname*

The dataset name of the KDS.

*fmid*

The FMID of the active ICSF instance.

*format*

The record format of a KDS. May have values of:

- FIXED
- VARIABLE
- KDSR

*hhhh*

The host name or IP address of the regional cryptographic server.

*ii*

The index or position where the server is installed.

*level*

The firmware level installed on the cryptographic device.

- mkvplist* List of master key verification patterns initialized in the KDS header. May have values of:
- AES, DES, or both for CKDS
  - RSA, ECC, or both for PKDS
  - P11, RCS, or both for TKDS
- mlen* The number of master key verification pattern digits to be displayed.
- nmkstate* The state of the RCS new master key register. The state may be EMPTY, FULL UNCOMMITTED, or FULL COMMITTED.
- nmkvp* The regional cryptographic server master key verification pattern from the NMK register when the NMK register is full.
- mmmm* The current number of active regional cryptographic server requests.
- nnnnnnnn* The serial number for the cryptographic device.
- optional diagnostic information* Displays the regional cryptographic server MKVP when the master key verification pattern does not match what is in the TKDS.
- rcsmkvp* The regional cryptographic server master key verification pattern from the TKDS. Note: All MKVPs are displayed in a shortened format (6 hex digits only).
- s* The state of the master keys in the coprocessor. The state can be:
- U** The current master key register is empty.
  - C** The current master key matches the MKVP in the key data set, but the master key is not active.
  - A** The master key is active and requests using this master key will be processed by the coprocessor.
  - E** The current master key does not match the MKVP in the key data set.
  - I** The MKVP is not in the key data set.
- A hyphen (-) in the state area indicates the key type is not supported. For additional information on crypto device status, see *z/OS Cryptographic Services ICSF Administrator's Guide*.
- status* The status of the server.
- sysname* The name of the sysplex member that took part in the SETICSF command.
- sysplex* Sysplex sharing indicator (Y or N).
- yn* The current setting of the option. May have the value of Yes or No.
- System action:** The system continues processing.
- Operator response:** None.
- System programmer response:** None.

**CSFM669I DISPLAY ICSF command failed:** *error\_text*

**Explanation:** The DISPLAY ICSF command encountered an error and *error\_text* is diagnostic information.

*error\_text* may have the value of:

**REMOTEDevice support not active**

The DISPLAY ICSF,REMOTEDevice command requires the specification of at least one REMOTEDevice entry in the ICSF installation options data set. In addition, the machine type must be IBM zEnterprise EC12 or later.

**System action:** Processing ends for the DISPLAY ICSF command.

**Operator response:** Review the *error\_text*, make any necessary changes, and reissue the command.

## CSFM670I • CSFM674I

If *error\_text* contains 'REMOTEDevice support not active', make sure that the machine type is an IBM zEnterprise EC12 or later. If it is, add a REMOTEDevice entry to the ICSF installation options data set. You may also have to allocate a TKDS and add the TKDSN entry as well, if not already done. Restart ICSF when complete.

**System programmer response:** None.

---

**CSFM670I SETICSF command failed:** *error\_text*

**Explanation:** The SETICSF command encountered an error and *error\_text* is diagnostic information.

*error\_text* may contain one of the following:

**REMOTEDevice support not active**

The SETICSF *action*,REMOTEDevice command requires the specification of at least one REMOTEDevice entry in the ICSF installation options data set. In addition, the machine type must be IBM zEnterprise EC12 or later.

**Specified RD not defined locally**

The SETICSF *action*,REMOTEDevice,INDEX=*nn* command requires that a regional cryptographic server be defined at the specified index on the system where the command was entered.

**Requested Regional Crypto servers not found on any system**

The SETICSF *action*,REMOTEDevice,SN=*nn* command was entered. No regional cryptographic server with the specified serial number was found either locally (when SYSPLEX=NO was specified or defaulted) or within the SYSPLEX (when SYSPLEX=YES was specified).

**System action:** Processing ends for the SETICSF command.

**Operator response:** Review the *error\_text*, make any necessary changes, and reissue the command.

If *error\_text* contains 'REMOTEDevice support not active', 'Specified RD not defined locally', or 'Requested Regional Crypto servers not found on any system', contact your system programmer.

**System programmer response:** If *error\_text* contains 'REMOTEDevice support not active', make sure that the machine type is an IBM zEnterprise EC12 or later. If it is, add a REMOTEDevice entry to the ICSF installation options data set. You may also have to allocate a TKDS and add the TKDSN entry as well, if not already done. Restart ICSF when completed.

If *error\_text* contains 'Specified RD not defined locally' or 'Requested Regional Crypto servers not found on any system', check that you have entered the correct index or serial number value. Reissue the command with any necessary changes.

---

**CSFM673E COORDINATED CHANGE MASTER KEY IS WAITING FOR FINAL VERIFICATION OF THE CONFIGURATION**

**Explanation:** After the master key has been changed on each cryptographic coprocessor, the master key verification patterns (MVKPs) from each coprocessor are read and compared to the MKVPs in the KDS header. ICSF must be able to complete these requests for each coprocessor in order to mark them as either available or unavailable.

If there is an exceptionally heavy workload or there is a hung user request, this message persists.

When the processing completes, this message is deleted.

**System action:** ICSF continues to wait for all coprocessor requests to complete.

**Operator response:** None.

**System programmer response:** If the message is not deleted in a reasonable amount of time, you may need to obtain a console dump of ICSF for diagnosis and then stop and restart ICSF.

---

**CSFM674I REGIONAL CRYPTO SUPPORT DISABLED. UNABLE TO DUB. RETURN CODE = *return\_code*, REASON CODE = *reason\_code***

**Explanation:** During ICSF start, when the REMOTEDevice ICSF installation option is specified, ICSF initialization attempts to DUB the address space in preparation for using z/OS UNIX System Services. The DUB failed. The return and reason codes received from the BPX1SDD service are displayed.

**System action:** ICSF ends.



**Operator response:** Contact your system programmer.

**System programmer response:** Look up the return and reason codes in *z/OS UNIX System Services Messages and Codes* and read the usage notes for the BPX1SDD service in *z/OS UNIX System Services Programming: Assembler Callable Services Reference*. Additionally, ensure you have properly set up the OMVS segment of the user ID assigned to the ICSF started procedure. For additional details, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

**CSFM676I** *server-name* *cii*, **SERIAL NUMBER** *nnnnnnnn* **IS** *state*

**Explanation:** ICSF is attempting to connect to a regional cryptographic server. The connection was successful. The server information is displayed:

*server-name*

The regional cryptographic server name (for example, REGIONAL CRYPTO SRV).

*c*

The short name for the server (for example, 1R represents a first generation remote regional cryptographic server).

*ii*

The index or position where the server is logically located.

*nnnnnnnn*

The serial number for the server.

*state*

The current state of the server. Possible values are:

**Active** The server is fully active. All sockets opened successfully.

**Active Partial**

The server is partially active. At least one socket opened successfully.

**System action:** Processing continues.

**Operator response:** Contact your system programmer when *state* = Active Partial.

**System programmer response:** When *state* = Active Partial, consult the documentation supplied by the vendor of your regional cryptographic server for the recommended number of sockets to be opened. Update either the REMOTEDEVICE ICSF installation option or use the SETICSF DELETE, RD console command to remove the remote device and then reissue the SETICSF ADD, RD console command to update the number of sockets to the recommended value. For additional details, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

**CSFM677I** *server-name* *cii*, **SN** *nnnnnnnn* **STATUS CHANGED FROM** *old\_state* **TO** *new\_state*.

**Explanation:** A regional cryptographic server is inactive and its status has changed. The server information is displayed:

*server-name*

The regional cryptographic server name (for example, REGIONAL CRYPTO SRV).

*c*

The short name for the server (for example, 1R represents a first generation remote regional cryptographic server).

*ii*

The index or position where the server is logically located.

*nnnnnnnn*

The serial number for the server.

*old\_state*

The previous state of the server.

*new\_state*

The current state of the server. Possible values are:

**Initializing stage 1**

A newly online regional cryptographic server has been detected by ICSF and ICSF is starting the initialization process.

**Deleted**

The regional cryptographic server was deleted by the operator on the system console.

## CSFM678E

### Being reconfigured

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

### Deactivated

The regional cryptographic server has been deactivated by the operator on the system console.

**System action:** Processing continues. ICSF will not use the regional cryptographic server in this state.

**Operator response:** Contact your system programmer if the problem does not resolve when *new\_state* = Being reconfigured.

**System programmer response:** If the problem does not resolve when *new\_state* = Being reconfigured, try restarting the regional cryptographic server using the SETICSF RESTART,REMOTEDEVICE console command. For additional details, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

---

CSFM678E *server-name* *cii*, SN *nnnnnnnn* STATUS CHANGED FROM *old\_state* TO *new\_state*.

**Explanation:** A regional cryptographic server is inactive and its status has changed. The server information is displayed:

*server-name*

The regional cryptographic server name (for example, REGIONAL CRYPTO SRV).

*c*

The short name for the server (for example, 1R represents a first generation remote regional cryptographic server).

*ii*

The index or position where the server is logically located.

*nnnnnnnn*

The serial number for the server.

*old\_state*

The previous state of the server.

*new\_state*

The current state of the server. Possible values are:

### Bad hostname or IP

The specified hostname or IP address and port is not valid.

### Bad server response

The regional cryptographic server returned either an unexpected response or no response. The server is not usable.

### Duplicate serial#/port

Another regional cryptographic server was found with the same serial number and the same port in its definition. This regional cryptographic server will not be made active.

### Failed authentication

The server failed to authenticate properly. Check the failure reason identified in the accompanying message CSFM681I.

### Hardware error

The regional cryptographic server has failed. Contact the vendor of your regional cryptographic server for support.

### Incompatible gen

The regional cryptographic server reported a generation number greater than what is supported by ICSF. The server is not usable.

### Master key incorrect

The master key on the regional cryptographic server is missing or incorrect.

### Repeat failures

A regional cryptographic server has been permanently disabled due to repeated failures.

**Retry limit reached**

While initializing a regional cryptographic server, the limit of attempts to gather status or information was reached. The server is not usable. ICSF will try again to acquire status.

**Unable to connect**

ICSF was unable to open a socket with the regional cryptographic server. Check the return and reason codes and the failing service name identified in the accompanying message CSFM680I.

**Unknown geo code**

The regional cryptographic server reported a geography code not recognized by ICSF. The server is not usable.

**System action:** Processing continues. ICSF will not use the regional cryptographic server in this state.

**Operator response:** Contact your system programmer.

**System programmer response:****If *new\_state* = 'Bad hostname or IP' or 'Unable to connect':**

Look up the failure codes in *z/OS UNIX System Services Messages and Codes* that are identified in the accompanying message CSFM680I. The most common error is return code = 00000468 (ECONNREFUSED) returned from BPX4CON. This indicates that the regional cryptographic server is not reachable at the hostname (or IP address) using the port number specified. It may be that the server is not online, in which case the problem will resolve itself once the server comes online. It may also mean that the hostname (or IP address), the port number, or both were incorrectly specified. In this case, determine the correct values to use and update the REMOTEDEVICE ICSF installation option (Note: This requires a restart of ICSF) or use the SETICSF DELETE,REMOTEDEVICE console command to remove the incorrect server definition and then reissue the SETICSF ADD,REMOTEDEVICE console command with the correct information. For additional details, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

**If *new\_state* = 'Bad server response':**

Check accompanying message CSFM680I. If the service is CSFENOCX and the return and reason codes are 0000000C and 00000D30, the regional cryptographic server did not respond to a request. Report the problem to the regional cryptographic server administrator. For all other return and reason codes, contact the IBM Support Center.

**For all other failures:**

Contact the IBM Support Center.

**CSFM679I ICSF UNABLE TO START. REMOTEDEVICE REQUIRES A TKDS DATA SET.**

**Explanation:** When the REMOTEDEVICE ICSF installation option is specified, ICSF uses the TKDS to store information about the regional cryptographic servers. The TKDS has not been defined.

**System action:** ICSF ends.

**Operator response:** Contact your system programmer.

**System programmer response:** Allocate a TKDS using a IDCAMS DEFINE CLUSTER and add the TKDSN keyword entry to the ICSF Options data set. For additional details, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

**CSFM680I** *server-name cii, SN nnnnnnnn: service-name FAILED: RC = return\_code, RS = reason\_code*

**Explanation:** ICSF manages connections to regional cryptographic servers using z/OS UNIX System Services. Either a call to one of these services or a call to a related ICSF internal service has returned an error. The server and service information is displayed:

*server-name*

The regional cryptographic server name (for example, REGIONAL CRYPTO SRV).

*c*

The short name for the server (for example, 1R represents a first generation remote regional cryptographic server).

*ii*

The index or position where the server is logically located.

*nnnnnnnn*

The serial number for the server.

## CSFM681I

### *service-name*

The name of the z/OS UNIX System Service or ICSF internal service that failed.

### *return\_code*

The hexadecimal return code from the failing service.

### *reason\_code*

The hexadecimal reason code from the failing service.

**System action:** Processing continues.

**Operator response:** Contact your system programmer.

**System programmer response:** If the *service-name* begins with CSF, look up the description for the return and reason codes displayed in the message in the Appendix of *z/OS Cryptographic Services ICSF System Programmer's Guide*.

See accompanying message CSFM678E and follow its recommendations.

---

## CSFM681I *server-name cii*, SN *nnnnnnnn* FAILED AUTHENTICATION, *failure-reason*

**Explanation:** ICSF is attempting to connect to a regional cryptographic server. The connection was not successful because the server failed the authentication process. The server and failure information is displayed:

### *server-name*

The regional cryptographic server name (for example, REGIONAL CRYPTO SRV).

### *c*

The short name for the server (for example, 1R represents a first generation remote regional cryptographic server).

### *ii*

The index or position where the server is logically located.

### *nnnnnnnn*

The serial number for the server.

### *failure-reason*

The descriptive reason for the failure. Possible values are:

#### **Unable to parse server certificate**

The server returns a X.509 certificate as part of the authentication process. The certificate has an unknown format and cannot be parsed.

#### **Server certificate expired**

The server returns a X.509 certificate as part of the authentication process. The certificate has expired.

#### **Server certificate not issued by IBM**

The server returns a X.509 certificate as part of the authentication process. The certificate was not issued by the IBM authority used for this purpose.

#### **Server certificate failed validation**

The server returns a X.509 certificate as part of the authentication process. The certificate signature failed to verify.

#### **Server handshake failed validation**

The server and ICSF perform a cryptographic handshake intended to prove the server owns the certificate that the server presented. The handshake signature failed to verify.

#### **Required mechanisms missing**

Regional cryptographic servers need to support a minimum set of mechanisms (algorithms). The server is missing at least one of these mechanisms.

#### **Known answer tests failed**

ICSF performs known answer tests of the mechanisms offered by a regional cryptographic server. At least one of these tests failed.

**System action:** Processing continues.

**Operator response:** Contact your system programmer.

**System programmer response:** Contact the IBM Support Center.

---

**CSFM682I REGIONAL CRYPTOGRAPHIC SERVICES ARE AVAILABLE.**

**Explanation:** This is an informational message and will only be issued if at least one regional cryptographic server is activated.

**System action:** Processing continues.

**Operator response:** None.

**System programmer response:** None.

---

**CSFM683E REGIONAL CRYPTOGRAPHIC SERVICES ARE NOT AVAILABLE.**

**Explanation:** No regional cryptographic servers are active. This may occur because:

- ICSF was unable to connect to the remote device or devices specified through the REMOTEDEVICE installation option or the SETICSF ADD,REMOTEDEVICE operator command.
- The remote devices or devices do not have the correct RCS master key set or are otherwise configured incorrectly.
- The last active regional cryptographic server has been deactivated by the SETICSF DELETE,REMOTEDEVICE or SETICSF DEACTIVATE,REMOTEDEVICE operator command.

**System action:** Processing continues. Callable services that require regional cryptographic services will fail.

**Operator response:** Contact your system programmer.

**System programmer response:** Check for additional failure information displayed on accompanying messages CSFM677I, CSFM678E, CSFM680I, or CSFM681I. Follow recommendations for those messages.

---

**CSFM684I ICSF IS BEING TERMINATED: *termination-reason***

**Explanation:** ICSF has experienced a problem that requires it to end. The *termination-reason* is as follows:

**ABEND in subtask while holding ENQ**

An ICSF subtask detected that it ABENDED while holding serialization to a key data set (KDS). The termination is necessary to ensure complete cleanup of the serialization.

**System action:** ICSF ends and restarts. Cryptographic services may be temporarily unavailable.

**Operator response:** Contact your system programmer.

**System programmer response:** Contact the IBM Support Center to diagnose the problem that caused the initial ABEND.

---

**CSFM685I SOCKET UNEXPECTEDLY CLOSED: DEV=*cii* S=*s* HOST=*ip-addr-or-hostname:port*  
LASTACT=*YYYYMMDDhhmmssst***

**Explanation:** ICSF is submitting a request to a regional cryptographic server. Either the request resulted in the failure of the server and the closing the socket, or the socket was found to be closed already. This message is written to the ICSF joblog only. The server and failure information is displayed:

*c* The short name for the server (for example, 1R represents a first generation remote regional cryptographic server).

*ii* The index or position where the server is logically located.

*s* The socket number that detected the error.

*ip-addr-or-hostname*

The IP address or hostname of the regional cryptographic server.

*port* The port number of the regional cryptographic server.

*YYYYMMDDhhmmssst*

The UTC date and time that the socket was last known to be active.

**System action:** The request is re-queued for sending to another server or another socket on the same server.

ICSF also attempts to restore the bad socket connection. If this is successful, no other messages are issued. If the restore attempt fails, ICSF issues a message about the change in state for the server.

## CSFM686I • CSFM689I

**Operator response:** Contact your system programmer.

**System programmer response:** The error could be the result of an intermittent network issue which may have already been resolved. In that case, multiple sockets, perhaps on multiple devices, may be closed. ICSF should be able to recover the lost socket or sockets and no action is needed. If this error reoccurs regularly, contact the IBM Support Center or the vendor of your regional cryptographic server to diagnose the reason for the socket failure.

---

### CSFM686I *CCMK-processing-message*

**Explanation:** This message is used to indicate error conditions detected during CCMK processing. This message is used during the initial step of a coordinated change master key operation.

**System action:** CCMK processing will terminate.

**Operator response:** Contact your system programmer.

**System programmer response:** Notify the security administrator for help in determining the reason for the failure. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated KDS administration failure. If unable to resolve the problem, contact the IBM Support Center.

---

### CSFM687I **NO ACTIVE *kdstype* SPECIFIED.**

**Explanation:** The options parameter file did not include a statement that contains the CKDSN or PKDSN keyword and value. *kdstype* is either CKDS or PKDS. When *kdstype* is CKDS, secure symmetric CCA key services is unavailable. When *kdstype* is PKDS, secure asymmetric CCA key services is unavailable.

**System action:** Processing continues.

**Operator response:** Contact your system programmer.

**System programmer response:** Notify the security administrator. If secure CCA key services are required, define a CKDS, a PKDS, or both as appropriate and restart ICSF.

---

### CSFM688E **ICSF KDS I/O REQUIRES CICSVR TO BE STARTED.**

**Explanation:** The KDS I/O request requires that the CICS VSAM Recovery (CICSVR) product is running.

**System action:** The KDS I/O request fails. After CICSVR is started and the next KDS I/O request succeeds, this message is DOMed.

**Operator response:** Contact your system programmer.

**System programmer response:** If you plan on using VSAM replication, start the CICSVR product. Ensure that the CICSVR product is started before ICSF is started. Otherwise, use IDCAMS ALTER to remove the replication settings from the key data sets.

---

### CSFM689I *coprocessor-name cii, SN nnnnnnnn compmode COMPLIANCE MODE IS compstat.*

**Explanation:** This message is issued when the cryptographic feature is first detected as being in an active compliance mode and is reissued each time a compliance state change is detected. The substitution variables are:

*coprocessor-name*

The cryptographic feature name and how it is configured. Possible values are:

- CRYPTO EXPRESS6 COPROCESSOR

*c* The short name for the coprocessor type. Possible values are:

- 6C (representing a CEX6C)

*ii* The index or position where the cryptographic feature is installed.

*nnnnnnn*

The serial number for the cryptographic feature.

*compmode*

The compliance mode. Possible values are:

- MIGRATION (representing migration compliance mode).

- PCI-HSM (representing the Payment Card Industry-Hardware Security Module compliance mode).

*compstat*

The state of the compliance mode. Possible values are:

- INACTIVE (The compliance mode is inactive).
- ACTIVE (The compliance mode is active).
- 2016 (The compliance mode is active at the 2016 level).

The value of *compstat* is dependent on *compmode*. Possible *compmode-compstat* combinations are:

*Table 3. compmode-compstat combinations*

| <i>compmode</i> | <i>compstat</i> | Description                 |
|-----------------|-----------------|-----------------------------|
| MIGRATION       | INACTIVE        | Migration mode is inactive. |
| MIGRATION       | ACTIVE          | Migration mode is active.   |
| PCI-HSM         | INACTIVE        | PCI-HSM mode is inactive.   |
| PCI-HSM         | 2016            | PCI-HSM 2016 mode.          |

**System action:** The cryptographic feature changes its processing to comply with the compliance setting.

**Operator response:** None.

**System programmer response:** None.

**CSFM690I** SYSTEM *compmode* COMPLIANCE MODE IS *compstat*

**Explanation:** This message is issued when the system first detects that a compliance mode is available and is reissued each time the system compliance mode changes. The substitution variables are:

*compmode*

The compliance mode. Possible values are:

- MIGRATION (representing migration compliance mode).
- PCI-HSM (representing the Payment Card Industry-Hardware Security Module compliance mode).

*compstat*

The state of the compliance mode. Possible values are:

- INACTIVE (The compliance mode is inactive).
- ACTIVE (The compliance mode is active).
- 2016 (The compliance mode is active at the 2016 level).

The value of *compstat* is dependent on *compmode*. Possible *compmode-compstat* combinations are:

*Table 4. compmode-compstat combinations*

| <i>compmode</i> | <i>compstat</i> | Description                                       |
|-----------------|-----------------|---------------------------------------------------|
| MIGRATION       | INACTIVE        | No coprocessor is in migration mode.              |
| MIGRATION       | ACTIVE          | At least one coprocessor is in migration mode.    |
| PCI-HSM         | INACTIVE        | No coprocessor is in a PCI-HSM mode.              |
| PCI-HSM         | 2016            | At least one coprocessor is in PCI-HSM 2016 mode. |

**System action:** None.

**Operator response:** None.

**System programmer response:** Confirm that the compliance mode and state specified is expected. Otherwise, requests requiring a given compliance mode may fail.

---

**CSFM691E COMPLIANCE WARN MODE REQUIRES AN ACTIVE *coprocessor-name*. WARN MODE DISABLED FOR: *comp-std*.**

**Explanation:** This message is issued whenever a requested compliance warn mode is disabled because the level of cryptographic coprocessor required is not available. The substitution variables are:

*coprocessor-name*

The type of coprocessor. Possible values are:

- CEX6C (representing a CRYPTO EXPRESS6 COPROCESSOR).

*comp-std*

The compliance standard. Possible values are:

- PCI-HSM 2016 (representing the Payment Card Industry-Hardware Security Module 2016 standard).

**System action:** The requested compliance warn mode is disabled.

**Operator response:** Contact the system programmer.

**System programmer response:** If compliance warning events are wanted, define an active coprocessor of the type specified to ICSF. Otherwise, disable the option in the installation options data set and refresh the options using the SETICSF OPT,REFRESH command.

---

**CSFM692E CRYPTO USAGE STATISTICS ARE REQUESTED BUT SMF TYPE 82, SUBTYPE 31 RECORDS ARE NOT BEING LOGGED.**

**Explanation:** Cryptographic usage statistics were requested, but SMF is not logging the type 82, subtype 31 records.

**System action:** ICSF continues to collect statistic data even if SMF records are not logged.

**Operator response:** Contact your system programmer.

**System programmer response:** Update the SMFPRMxx parmlib member to record SMF type 82, subtype 31 records, issue the SET SMF=xx operator command to start SMF recording with the new options, and issue the command SETICSF OPT,STATS=yyy operator command to trigger the update to ICSF. Alternatively, issue the command SETICSF OPT,STATS=NONE to disable cryptographic usage statistics collection.

For more information, see 'Monitoring users and jobs that perform cryptographic operations' in *z/OS Cryptographic Services ICSF Administrator's Guide*.

This message is deleted when:

- ICSF is stopped, or
- Cryptographic usage statistics is disabled, or
- SMF starts logging type 82, subtype 31 records and either:
  - The current SMF interval has ended, or
  - SETICSF OPT,STATS=xxx has been issued.

---

**CSFM693E COMPLIANCE WARN MODE IS REQUESTED BUT SMF TYPE 82, SUBTYPE 48 RECORDS ARE NOT BEING LOGGED.**

**Explanation:** This message is issued whenever a compliance warn mode is requested, but logging of the SMF type 82 subtype 48 record is disabled.

**System action:** Compliance warn mode is disabled.

**Operator response:** Contact the system programmer.

**System programmer response:** If compliance warning events are wanted, enable logging of the SMF type 82 subtype 48 record. Otherwise, disable compliance warnings in the installation options data set and refresh the options using the SETICSF OPT,REFRESH command.



---

**CSFM695I ICSF TERMINATION DUE TO ABEND *aaa* WHILE INITIALIZING COPROCESSOR AT INDEX *nn***

**Explanation:** During ICSF initialization of the cryptographic coprocessors, an unexpected ABEND caused ICSF to terminate.

*aaa* The ABEND that occurred.

*nn* The index for the cryptographic coprocessor that was being processed at the time of the ABEND. N/A appears if the ABEND occurred while not processing a specific coprocessor.

**System action:** ICSF initialization stops and ICSF terminates. A dump will usually accompany the abend, but may be suppressed by SLIP or DAE.

**System programmer response:** Attempt to start ICSF again. If the problem persists, consult the documentation for the ABEND code to see if it explains the problem.

You can also try to configure the coprocessor offline before restarting ICSF to see if that allows ICSF to be started. If this works, you can try to configure the coprocessor online after ICSF is up.

If the problem persists, contact the IBM Support Center.

---

**CSFM704I RSA CRT KEY COMPONENTS CORRECTED IN PKDS RECORD *label***

**Explanation:** While loading the PKDS, a record with label *label* was found containing a clear RSA CRT private key with prime *p* less than prime *q*, which is in violation of the standard. The key material was corrected.

**System action:** ICSF processing continues. The RSA CRT key token in this record is updated for the in-store copy of the PKDS.

**Operator response:** None.

**System programmer response:** None required. If the PKDS is in KDSR format, the updated record can be hardened by being referenced (using reference date processing) or by updating any metadata. If the PKDS is in non-KDSR format, the updated record can be written to the DASD copy by reading and then writing the token back to the label.

---

**CSFM721I *kds-type* RECORD *number* *dmgttype* DAMAGE DETECTED, *record-type* *record-name***

**Explanation:** A record in a KDS was detected as being damaged. ICSF's action depends on the type of damage detected.

In the message text:

*kds-type*

Either CKDS, PKDS, or TKDS.

*number*

The record number that was detected as being damaged.

*dmgttype*

The type of damage detected. Either KEY, ATTRIBUTE, or KEY AND ATTRIBUTE.

*record-type*

LABEL for CKDS, PKDS, and TKDS.

*record-name*

The label of the CKDS, PKDS, and handle of the TKDS record.

**System action:** ICSF processing continues.

• When *dmgttype* is ATTRIBUTE, all variable-length attributes have been removed from the record in memory.

• When *dmgttype* is KEY, there is no key value in the record.

• When *dmgttype* is KEY AND ATTRIBUTE, both the variable-length attributes and the key value have been removed from the record in memory.

The modified records in memory are written to the KDS if a master key change occurs.

**Operator response:** None.

**System programmer response:** Notify the ICSF administrator.



---

## Chapter 9. CSFOnnnn messages (Installation options parameter processing)

Problems encountered during the processing of installation option parameters are written to the ICSF job log.

---

**CSFO001I** z/OS V2R3 or a later release is required for CICSAUDIT. The function is not enabled.

**Explanation:** The CICS audit support requires support from the security product (for example, z/OS Security Server (RACF)) that is provided in z/OS V2R3 and higher releases. CICS auditing is disabled until the base release of z/OS supports the LOGSTRX option on RACROUTE calls.

**System action:** Processing of the ICSF options at startup or during SETICSF OPT,REFRESH continues.

**User response:** Change your ICSF options to CICSAUDIT(NO) until you are running on z/OS V2R3 or higher so that you do not see this message on each ICSF startup. Upgrade to z/OS 2.3 if you need the CICS auditing of ICSF services.

---

**CSFO002I** *kdsn* OPTION NOT SPECIFIED. *plexkds* OPTION IGNORED.

**Explanation:** The *plexkds* option was specified without the corresponding *kdsn* option in the installation options data set. The *plexkds* option will have no effect. *kdsn* is either CKDSN or PKDSN. *plexkds* is either SYSPLEXCKDS or SYSPLEXPKDS.

**System action:** Processing continues.

---

**CSFO0016** ERROR OCCURRED OPENING OPTIONS FILE.

**Explanation:** ICSF could not open the options parameter file that is specified on the CSFPARM DD statement in the JCL.

**System action:** Processing ends.

**User response:** Ensure that the options parameter file that is defined by the DD statement is valid. Correct the DD statement and restart ICSF.

---

**CSFO0026** ERROR OCCURRED CLOSING OPTIONS FILE.

**Explanation:** ICSF could not close the options parameter file.

**System action:** Processing ends.

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

**User response:** Contact your system programmer.

---

**CSFO0036** SYNTAX ERROR IN OPTION STATEMENT.

**Explanation:** The statement that immediately precedes this message has at least one syntax error.

**System action:** Processing ends.

**User response:** Check the syntax of the option statement. Check for unpaired delimiters and missing or extraneous commas and ensure that the statement does not exceed position 71. Correct the error and restart ICSF.

---

---

**CSFO0046 PARTITIONED DATA SET NOT ALLOWED FOR THE CKDS, PKDS, OR TKDS.**

**Explanation:** The CKDSN, PKDSN or TKDSN keyword on an option statement specified a member name for a data set. The CKDS, PKDS, or TKDS must be a VSAM data set.

**System action:** Processing ends.

**User response:** Correct the data set name and restart ICSF.

---

**CSFO0066** *Keyword* **VALUE NOT IN RANGE.**

**Explanation:** The specified value for the keyword is not within the allowable range. *z/OS Cryptographic Services ICSF System Programmer's Guide* describes the allowable range for the keyword. The statement that contains the error precedes this message.

**System action:** Processing ends.

**User response:** Specify an allowable range for the keyword and restart ICSF.

---

**CSFO0076** *Keyword* **KEYWORD SPECIFIED WITH MISSING VALUE.**

**Explanation:** A keyword value is missing for the *keyword* variable. The statement that contains the error precedes this message.

**System action:** Processing ends.

**User response:** Specify a value for the keyword and restart ICSF.

---

**CSFO0096** **SERVICE NUMBER VALUE NOT IN RANGE.**

**Explanation:** The specified service number for the SERVICE and UDX keywords must be from 1 to 32767. The statement containing the error precedes this message.

**System action:** Processing ends.

**User response:** Specify a service number value between 1 and 32767 and restart ICSF.

---

**CSFO0106** *Keyword* **KEYWORD AND VALUE MISSING.**

**Explanation:** The *keyword* keyword and its value are missing from the option statement. The statement that contains the error precedes this message.

**System action:** Processing ends.

**User response:** Specify the keyword and its value and restart ICSF.

---

**CSFO0126** **ERROR OCCURRED OPENING WAITLIST FILE.**

**Explanation:** ICSF could not open the Wait List file specified by the WAITLIST parameter in the ICSF Installation Options data set.

**System action:** Processing continues. The ICSF default CICS Wait List file will be used.

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

**User response:** Contact your system programmer.

---

**CSFO0136** **ERROR OCCURRED CLOSING WAITLIST FILE.**

**Explanation:** ICSF could not close the Wait List file specified by the WAITLIST parameter in the ICSF Installation Options data set.

**System action:** Processing continues.

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

**User response:** Contact your system programmer.

---

**CSFO0146 ERROR OCCURRED ALLOCATING WAITLIST FILE.**

**Explanation:** ICSF could not allocate the Wait List file specified by the WAITLIST parameter in the ICSF Installation Options data set.

**System action:** Processing continues. The ICSF default CICS Wait List will be used.

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

**User response:** Contact your system programmer.

---

**CSFO0156 ERROR OCCURRED FREEING WAITLIST FILE.**

**Explanation:** ICSF could not deallocate the Wait List file specified by the WAITLIST parameter in the ICSF Installation Options data set.

**System action:** Processing continues.

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

**User response:** Contact your system programmer.

---

**CSFO0166 DEFAULT CICS WAIT LIST WILL BE USED.**

**Explanation:** The default ICSF CICS Wait List file will be used for ICSF processing because:

1. There was no Wait List file specified in the Installation Options data set.
2. ICSF could not open or allocate the Wait List file specified.
3. The specified Wait List file contained more entries than allowed.

**System action:** Processing continues. The default ICSF CICS Wait List file will be used during ICSF processing.

**System programmer response:** If use of the ICSF default CICS Wait List file is the desired ICSF processing option, no action is required. Otherwise, ensure that the Wait List file specified in the Installation Options data set is valid.

**User response:** Contact your system programmer.

---

**CSFO0176 SERVICE NAME *routine* NOT VALID AND WILL BE SKIPPED.**

**Explanation:** The service name specified (*routine*), which is contained in the Wait List file, is not a valid name of an ICSF service or of an installation-defined service. The specified service name will not be placed in the Wait List.

**System action:** Processing continues. The specified service name will not be placed in the Wait List.

**System programmer response:** Check the contents of the Wait List file specified by the WAITLIST option of the Installation Options data set. Check the spelling of the service names in the file. Each record must be the name of an ICSF service or of a current installation-defined service or UDX service. Syntax rules for the CICS Wait List file are discussed in *z/OS Cryptographic Services ICSF System Programmer's Guide*.

**User response:** Contact your system programmer.

---

**CSFO0206 TKDSN OPTION NOT SPECIFIED. SYSPLEXTKDS OPTION IGNORED.**

**Explanation:** The SYSPLEXTKDS option was specified without the TKDSN option in the installation options data set. No PKCS #11 processing is possible and the SYSPLEXTKDS option will have no effect.

**System action:** Processing ends.

**System programmer response:** Ensure that the SYSPLEXTKDS option is specified with the TKDSN option in the installations options data set or no PKCS #11 processing is possible and the SYSPLEXTKDS option will have no effect.

**User response:** Contact your system programmer.

---

---

**CSFO0212** *Keyword* **KEYWORD NO LONGER SUPPORTED.**

**Explanation:** The keyword, *keyword*, is no longer supported by ICSF. The keyword was parsed, but has no affect.

**System action:** Processing continues.

**System programmer response:** Remove the keyword from the options data set if appropriate. Older releases of ICSF may still support the keyword.

---

**CSFO0220** *Keyword* **VALUE NOT IN RANGE.**

**Explanation:** The specified value for the keyword is not within the allowable range. The default value for the keyword will be used in place of the value specified. *z/OS Cryptographic Services ICSF System Programmer's Guide* describes the allowable range for the keyword. The statement that contains the error precedes this message.

**System action:** Processing continues.

**User response:** Update the options data set with an allowable range for the keyword.

---

**CSFO0230** *ICSF\_option*

**Explanation:** This message is issued once for each option in the ICSF Options Data Set. This message is informational only. No action is required.

---

**CSFO0236** **BEGIN-END KEYWORD ERROR. ERROR CODE = *errcode***

**Explanation:** An error was detected with the BEGIN(FMID) and END keywords. The error code indicates the error.

1. There was no END for a BEGIN(FMID).
2. Unknown FMID. The FMID specified is not valid. For information on the z/OS ICSF FMIDs, see the *z/OS Cryptographic Services ICSF System Programmer's Guide*.
3. There was not matching BEGIN(FMID) for an END.

**System action:** Processing ends.

**System programmer response:** Check the syntax of the option statements.

**User response:** Contact your system programmer.

---

**CSFO0240** **EXIT NAME *exit-name* NOT VALID AND WILL BE SKIPPED.**

**Explanation:** The installation exit name *exit-name* is not valid. Chapter 5 (Installation Exits) in the *z/OS Cryptographic Services ICSF System Programmer's Guide* lists the valid installation exit names.

**System action:** The exit for *exit-name* will not be loaded. Processing continues.

**System programmer response:** None.

**User response:** Update the options data set.

---

**CSFO0252** *option* **INSTALLATION OPTION IGNORED DUE TO MACHINE TYPE.**

**Explanation:** The ICSF installation option specified is not supported while running on the current machine type. The ICSF installation option is ignored.

In the message text:

*option*

**REMOTEDEVICE**

This option requires an IBM zEnterprise EC12 or later machine type.

**System action:** Processing continues, but the option is not processed.

**System programmer response:** Remove the option from the ICSF installation options data set to prevent this message from being issued in the future.

**User response:** Contact your system programmer.

---

**CSFO0404** CTRACE OPTION *text\_value* IS NOT VALID.

**Explanation:** This message is issued when an incorrect trace option is specified in either the ICSF CTRACE configuration PARMLIB member or in the REPLY to a TRACE CT operator command.

**System action:** If this error occurs during ICSF startup, the default or specified PARMLIB member contains an incorrect option, and will not be used. ICSF CTRACE will attempt to use the default CTICSF00 PARMLIB member. If the CTICSF00 PARMLIB member is absent or contains an incorrect option, ICSF CTRACE will perform tracing using an internal default set of trace options. By default, ICSF CTRACE support will trace with the KdsIO, CardIO, and SysCall filters using a 2M buffer.

If this error occurs during a TRACE CT operator command, ICSF CTRACE will ignore the command and continue to use the current active options.

ICSF will continue processing.

**System programmer response:** Correct the ICSF CTRACE configuration PARMLIB member if one was specified and reset ICSF CTRACE to use it using either the TRACE CT command or by restarting ICSF. If this error occurred during a TRACE CT operator command, correct the command syntax and reissue the command.

**User response:** Contact your system programmer.

---

**CSFO0414** CTRACE PARMLIB MEMBER *member\_name* COULD NOT BE USED. SWITCHING TO MEMBER CTICSF00.

**Explanation:** This message is issued when the PARMLIB member specified for the ICSF CTRACE configuration PARMLIB member is unusable.

**System action:** During ICSF startup, if the specified PARMLIB member is absent or contains an incorrect option, ICSF CTRACE will attempt to use the default CTICSF00 PARMLIB member. If the CTICSF00 PARMLIB member is absent or contains an incorrect option, ICSF CTRACE will perform tracing using an internal default set of trace options. By default, ICSF CTRACE support will trace with the KdsIO, CardIO, and SysCall filters using a 2M buffer.

ICSF will continue processing.

**System programmer response:** Correct the ICSF CTRACE configuration PARMLIB member and reset ICSF CTRACE to use it by using either the TRACE CT command or restarting ICSF.

**User response:** Contact your system programmer.

---

**CSFO0424** CTRACE PARMLIB MEMBER CTICSF00 COULD NOT BE USED. SWITCHING TO DEFAULT SETTINGS.

**Explanation:** This message is issued at ICSF startup when the default CTICSF00 ICSF CTRACE configuration PARMLIB member is unusable.

**System action:** ICSF will use default CTRACE configuration settings and continue processing. By default, ICSF CTRACE support will trace with the KdsIO, CardIO, and SysCall filters using a 2M buffer.

**System programmer response:** Correct the unusable CTICSF00 PARMLIB member and reset ICSF CTRACE by using either the TRACE CT command or by restarting ICSF to use either the CTICSF00 PARMLIB member or another PARMLIB member containing valid ICSF CTRACE configuration options.

**User response:** Contact your system programmer.

---

**CSFO500I** Option *option* not changed. *reason\_text*.

**Explanation:** The option updated in the installation options data set was not changed by the refresh function.

In the message text:

*option*

The installation options data set option parameter.

*reason\_text*

'Domain change requires a reIPL'

This is issued if the DOMAIN option was different in the options data set from the current domain.

## CSFO501I • CSFO502I

**'Use TRACE CT,COMP=(CSF) to change trace.'**

This is issued if the CTRACE option value is different than the value that ICSF was started with.

**'Restart required to change this option.'**

This is issued if the option is not supported by the refresh and the value for the option is different than the value that ICSF was started with.

**System action:** Processing continues.

**Operator response:** Contact your system programmer.

**System programmer response:** If the DOMAIN option change is needed, reIPL.

If the CTRACE option change is needed, use TRACE CT,COMP=(CSF) to change trace.

If any other specified option changes are needed, restart ICSF.

**Problem determination:** Check the options supported for REFRESH in *z/OS Cryptographic Services ICSF System Programmer's Guide*.

---

### CSFO501I Option *option* WARNING. *reason\_text*

**Explanation:** The option in the installation options data set was not changed by the refresh function because the option can only be changed with a restart of ICSF. In addition, the specified value in the option does not match that of the currently active setting on the system.

In the message text:

*option*

The installation options data set option parameter.

*reason\_text*

**Specified KDS does not match active CKDS**

This is issued if the CKDS specified in the CKDSN option does not match the active CKDS.

**Specified KDS does not match active PKDS**

This is issued if the PKDS specified in the PKDSN option does not match the active PKDS.

**Specified KDS does not match active TKDS**

This is issued if the TKDS specified in the TKDSN option does not match the active TKDS.

**SSM option overridden by SAF profile**

This is issued if the CSF.SSM.ENABLE profile is defined.

**System action:** Processing continues.

**Operator response:** Contact your system programmer.

**System programmer response:** The *option* in the installation options data set should be updated before the next restart of ICSF if you want to keep the currently active KDS after restarting ICSF.

The requested SSM option has been saved and will be used if the CSF.SSM.ENABLE profile is deleted in the future.

**Problem determination:** Check the active KDSs using either the ICSF - Installation Option Display panel set or the DISPLAY ICSF,KDS command against the values in the current installation options data set.

---

### CSFO502I Option *option* changed by option refresh processing.

**Explanation:** The option in the installation options data set was successfully updated by the refresh function.

In the message text:

*option*

The installation options data set option parameter.

**System action:** Processing continues.



---

**CSFO503I** Option *option* ignored for option refresh.

**Explanation:** The option specified is not supported by refresh processing.

In the message text:

*option*

The installation options data set option parameter.

**System action:** Processing continues.

**Operator response:** Contact your system programmer.

**System programmer response:** A restart of ICSF is required to change this option.



---

## Chapter 10. CSFPnnnn messages (Parse)

The following parse message is written to the ICSF job log.

---

**CSFP0016**    **COULD NOT CREATE PARSE ENVIRONMENT.**

**Explanation:** ICSF or the key generator utility program initialization process could not create an environment suitable for parsing of the options parameter statements or the key generator control statements.

**System action:** Processing ends for this request.

**System programmer response:** Ensure that there is enough space to create parse related control blocks. Check if the valid level of TSO/E is installed in accordance with the installation instructions in the OS/390 Program Directory. If it is valid, contact the IBM Support Center.

**User response:** Contact your system programmer.



---

## Chapter 11. 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 CSFPUTIL 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.

---

**CSFU006I** *operation* FEEDBACK: RC=*return-code* RS=*reason-code* SUPRC=*supplemental-return-code*  
SUPRS=*supplemental-reason-code* FLAGS=*flags*.

**Explanation:** The coordinated KDS administration utility completed. The *operation* may be CHANGE-MK or REFRESH. *return-code* and *reason-code* indicate the primary return code and reason code for the utility. In the case of a failure, the *supplemental-return-code* and *supplemental-reason-code* indicate the supplemental return code and reason code for the failure. *flags* indicate additional internal diagnostic information about the failure.

**System action:** ICSF processing continues.

**System programmer response:** In the case of a failure, contact the security administrator for help determining the problem. Use the *return-code* and *reason-code* for problem determination. For more information on the *return-code* and *reason-code*, refer to the *z/OS Cryptographic Services ICSF Application Programmer's Guide* or the information on the CSFEUTIL program in the *z/OS Cryptographic Services ICSF Administrator's Guide*. Refer to the *z/OS Cryptographic Services ICSF Administrator's Guide* for information on recovering from a coordinated CKDS administration failure. If you are unable to determine the problem by looking up these values, contact the IBM Support Center. The *supplemental-return-code*, *supplemental-reason-code*, and *flags* show IBM internal diagnostic information. You may need to provide this information to the IBM Support Center.

---

## Chapter 12. CSFVnnnn messages (CKDS conversion processing)

CSFVnnnn Messages (CKDS Conversion Processing) describes messages that ICSF issues during the cryptographic key data set (CKDS) conversion process. These messages are written to the ICSF job log using routing code 11.

---

**CSFV0012 CONVERSION PROCESSING COMPLETED. RETURN CODE = *retcode*.**

**Explanation:** The CUSP/PCF CKDS to ICSF CKDS conversion program has completed successfully.

**System action:** Processing ends.

**User response:** Review the return codes and their meanings:

**Return Code**

**Meaning**

- |    |                                                                                                                                                            |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 00 | Successful processing.                                                                                                                                     |
| 04 | The conversion process encountered warning conditions, but completed processing of all transactions. Review preceding messages for the warning conditions. |

---

**CSFV0026 CONVERSION TERMINATED. RETURN CODE = *retcode*, REASON CODE = *rsncode*.**

**Explanation:** An error occurred in the conversion program that caused ICSF to end processing. See the list of return and reason codes to determine the cause of the error.

**Return code:** 12

**Reason Code**

**Meaning**

- |      |                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6004 | The conversion program selected a CKDS access function that is not valid.<br>The valid CKDS access functions are: <ul style="list-style-type: none"><li>• READ</li><li>• READUP</li><li>• WRITE</li><li>• REWRITE</li></ul> |
| 6008 | A service routine failed. ICSF sets the reason code after issuing message CSFG0293.<br>The service routines are: <ul style="list-style-type: none"><li>• CSFMGN</li><li>• CSFMVR</li><li>• CSFMKVR</li></ul>                |
| 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.                                                                                                                    |

## CSFV0026

- 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.
- 9000 The IMPORTER label that is specified for the PARM keyword of the EXEC JCL statement is not valid. The length of the label must be eight characters or less, all non-blank character must be alphanumeric, and the first character must be alphabetic. ICSF sets the reason code after issuing message CSFV0036.
- 9004 ICSF could not find the IMPORTER record on the supplied ICSF CKDS for the label that is specified with the PARM keyword on the EXEC JCL statement. ICSF sets the reason code after issuing message CSFV0046.
- 9008 The CUSP/PCF CKDS that was input to the conversion process is not valid. ICSF sets the reason code after issuing message CSFV0056.
- 9016 The conversion process attempted to use a non-empty output ICSF CKDS. The output ICSF CKDS that is specified by DD statement CSFVNEW must be empty when running the conversion process. ICSF sets the reason code after issuing message CSFV0056.
- 9020 The required conversion installation exit could not be loaded. This may be caused by one of these conditions. The EXIT keyword in the options file specifies an incorrect load module name. The load module does not exist in any library in the link list being used. The load module does not exist in the library specified in a JOBLIB or STEPLIB DD statement. ICSF sets the reason code after issuing message CSFC0166.
- 9024 The record type of a source CUSP/PCF CKDS entry is not valid. The record type must be either LOCAL, REMOTE, or CROSS. ICSF sets the reason code after issuing message CSFV0266.
- 9028 The conversion program encountered a second explicit override entry when an explicit override entry already pertains to all types within the label. ICSF sets the reason code after issuing message CSFV0256.
- 9032 The conversion program encountered a third global override entry. The conversion process allows for a total of two global override entries as input. ICSF sets the reason code after issuing message CSFV0276.
- 9036 The conversion program encountered a second global override entry when the first global override entry pertains to all types. ICSF sets the reason code after issuing message CSFV0286.
- 9040 An override entry consists of all blanks.
- 9044 An override entry is out of sequence. The override entries should be in sequence by LABEL and OLD\_TYPE. ICSF sets the reason code after issuing message CSFV0316.
- 9048 An override entry duplicates another override entry within LABEL and OLD\_TYPE. ICSF sets the reason code after issuing message CSFV0326.
- 9056 An override entry's NEW\_TYPE is not valid. If the OLD\_TYPE is LOCAL, the NEW\_TYPE must be EXPORTER, OPINENC, or blank. If the OLD\_TYPE is REMOTE, the NEW\_TYPE must be IMPORTER, IPINENC, or blank. ICSF sets the reason code after issuing message CSFV0346.
- 9060 An override entry's OLD\_TYPE is not valid. The OLD\_TYPE must be LOCAL, REMOTE, or blank. ICSF sets the reason code after issuing message CSFV0356 or CSFV0366.
- 9064 An override entry's BYPASS\_FLAG is not valid. The BYPASS\_FLAG must be Y, N, or blank. Blank is equivalent to N. ICSF sets the reason code after issuing message CSFV0376.
- 9068 The pre-processing installation exit call has failed with a return code greater than 8. ICSF sets the reason code after issuing message CSFV0506. Follow local procedures for installation exit problems.
- 9072 The post-processing installation exit call has failed with a return code greater than 8. ICSF sets the reason code after issuing message CSFV0516. Follow local procedures for installation exit problems.
- 9076 The record processing installation exit call has failed with a return code greater than 8. ICSF sets the reason code after issuing message CSFC0186. Follow local procedures for installation exit problems.



- 9080** The installation exit has ended abnormally, and ICSF should be stopped. ICSF sets the reason code after issuing message CSFC0206. Check the installation exit for errors.
- 9084** The installation exit has ended abnormally, and the conversion process has ended. ICSF sets the reason code after issuing message CSFC0136. Check the installation exit module for errors.
- 9088** The installation exit has requested the ending of the conversion process. ICSF sets the reason code after issuing message CSFV0546.
- 9092** A data set that was input to the conversion process is not a valid ICSF/MVS Version 1 Release 1 CKDS. ICSF sets the reason code after issuing message CSFV0066.
- 9096** ICSF detected a duplicate label that is not valid. Processing would have resulted in more than one key on the target CKDS with the same label. This condition is not valid when one of the keys is a DATA, MAC, MACVER, DATAXLAT, or NULL key. ICSF sets the reason code after issuing message CSFV0396.

**Return code:** 16

**Reason Code**  
**Meaning**

- 0000** Could not open the output report data set. Ensure that a JCL DD statement exists for the CSFVRPT report data set in the conversion process jobstream. If you cannot resolve the problem, see your system programmer.

**Return code:** 20

**Reason Code**  
**Meaning**

- 0000** Could not establish an ESTAE recovery environment. Attempt to run the job again. If it still fails, contact the IBM Support Center.

**Return code:** 24

**Reason Code**  
**Meaning**

- 0000** An abnormal ending has occurred. Respond to the problem that is identified in the associated error message.

**Return code:** 64

**Reason Code**  
**Meaning**

- 0000** An OPEN error occurred for the CSFVRPT report data set. If it is a pre-allocated data set, ensure that the record length is correct.

**Return code:** 68

**Reason Code**  
**Meaning**

- 0000** An I/O error occurred for the CSFVRPT report data set. An attempt to CLOSE the data set was tried, so check to see if there are meaningful messages in the data set.

**System action:** Processing ends.

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

**User response:** Determine the cause of the error, correct the problem, and rerun the conversion program. If you cannot resolve the problem, contact your system programmer.

---

**CSFV0036**    **IMPORTER KEY LABEL NOT VALID.**

**Explanation:** The IMPORTER key label that is specified with the PARM keyword on the EXEC JCL statement is not valid. The label must be 64 or fewer characters in length.

**System action:** The system issues message CSFV0026 with a return code of 12 and a reason code of 9000. Processing ends.

**User response:** Ensure that the label that is specified is correct and matches the IMPORTER label on the supplied ICSF CKDS. Rerun the conversion program.

---

**CSFV0046**    *label* **IMPORTER KEY NOT FOUND ON INPUT ICSF CKDS.**

**Explanation:** The conversion program could not find the record for the IMPORTER key with the *label* label in the supplied ICSF CKDS. The label was specified with the PARM keyword on the EXEC JCL statement.

**System action:** The system issues message CSFV0026 with a return code of 12 and a reason code of 9004. Processing ends.

**User response:** Ensure that the specified *label* is correct or that the IMPORTER label in the supplied ICSF CKDS is correct. Rerun the conversion program.

---

**CSFV0056**    **CSFVSRC DATA SET NOT A CUSP OR PCF CKDS.**

**Explanation:** The data set that is named in the CSFVSRC DD statement is not a CUSP/PCF CKDS.

**System action:** The system issues message CSFV0026 with a return code of 12 and a reason code of 9008. Processing ends.

**User response:** Ensure that the CSFVSRC DD statement specifies the correct data set name for a CUSP/PCF CKDS. Rerun the conversion program.

---

**CSFV0152**    **TYPE FOR ALL *type* KEY ENTRIES CONVERTED TO *new-type*.**

**Explanation:** A global override entry specified that all *type* key entries on the CUSP/PCF CKDS are to be converted to *new-type* key entries on the new ICSF CKDS.

**System action:** Processing continues.

**User response:** None.

---

**CSFV0172**    **ALL *type* KEY ENTRIES BYPASSED.**

**Explanation:** A global override entry specified to bypass all entries on the CUSP/PCF CKDS with a type of *type*.

**System action:** Processing continues.

**User response:** None.

---

**CSFV0182**    **INSTALLATION DATA FOR ALL *type* KEY ENTRIES SET TO *installation-data*.**

**Explanation:** A global override entry specified that all key entries in the CUSP/PCF CKDS with a type of *type* are to have the value *installation-data* set in the INSTALLATION\_DATA field of the entries on the new ICSF CKDS.

**System action:** Processing continues.

**User response:** None.

---

**CSFV0192**    **TYPE FOR KEY ENTRY *label type* CONVERTED TO *new-type*.**

**Explanation:** An override entry specified that the type for the key entry in the CUSP/PCF CKDS identified as *label type* is to be changed to *new-type* on the new ICSF CKDS.

**System action:** Processing continues.

**User response:** None.

---

**CSFV0212** KEY ENTRY *label type* **BYPASSED.**

**Explanation:** An override entry specified to bypass the key entry in the CUSP/PCF CKDS identified as *label type* and not include it in the new ICSF CKDS.

**System action:** Processing continues.

**User response:** None.

---

**CSFV0222** KEY ENTRY *label type* **NOT BYPASSED.**

**Explanation:** An override entry specified not to bypass the key entry in the CUSP/PCF CKDS identified as *label type* and to include it in the new ICSF CKDS.

**System action:** Processing continues.

**User response:** None.

---

**CSFV0232** INSTALLATION DATA FOR KEY ENTRY *label type* **SET TO** *installation-data*.

**Explanation:** An override entry specified that the INSTALLATION\_DATA for the key entry in the CUSP/PCF CKDS identified as *label type* is to be set to *installation-data* on the new ICSF CKDS.

**System action:** Processing continues.

**User response:** None.

---

**CSFV0256** OVERRIDE ENTRY FOR KEY ENTRY *label* **NOT VALID. PREVIOUS OVERRIDE ENTRY HAD BLANK OLD\_TYPE.**

**Explanation:** An override entry specified the same key label (*label*) as a previous override entry, which had a blank OLD\_TYPE specified. Only one override entry is allowed with a blank OLD\_TYPE because it applies to all entries with a matching label.

**System action:** The system issues message CSFV0026 with return code of 12 and a reason code of 9028. Processing ends.

**User response:** Either remove the second override entry from the override data set or ensure that the first override entry has a value for OLD\_TYPE. Rerun the conversion program.

---

**CSFV0266** CUSP/PCF KEY ENTRY *label* **TYPE NOT VALID.**

**Explanation:** The CUSP/PCF CKDS entry with LABEL *label* has a type that is not LOCAL, REMOTE, or CROSS.

**System action:** The system issues message CSFV0026 with a return code of 12 and a reason code of 9024. Processing ends.

**User response:** Specify LOCAL, REMOTE, or CROSS for the CUSP/PCF CKDS entry type. Rerun the conversion program.

---

**CSFV0276** MORE THAN TWO GLOBAL OVERRIDE ENTRIES SPECIFIED.

**Explanation:** The override data set contains more than two global entries. The maximum number of global entries is two; one for each type, LOCAL and REMOTE.

**System action:** The system issues message CSFV0026 with a return code of 12 and a reason code of 9032. Processing ends.

**User response:** Remove the extraneous global override entries. Rerun the conversion program.

---

**CSFV0286** GLOBAL OVERRIDE ENTRY NOT VALID. PREVIOUS GLOBAL OVERRIDE ENTRY HAD BLANK OLD\_TYPE.

**Explanation:** A second global override entry was present when the first global override entry had no value specified for OLD\_TYPE. Because the first global override entry is to be applied to all entries, the second global override entry is redundant.

## CSFV0292 • CSFV0356

**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.

## CSFV0522 • CSFV0560

**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).

## CSFY0036 • CSFY0076

- 180 The supplied logical record length does not agree with the record length that is defined for the data set. Redefine the data set with the correct record length.
- 184 An error occurred running an AMS MODCB macro.
- 192 An error occurred opening the file. This can be normal if concurrent instances of ICSF are being started on different systems for a shared data set. In this case, ICSF initialization logic is constructed to overcome the error. If this is not a situation where concurrent instances of ICSF are starting and sharing the data set, then ensure that the JCL DD statement for the data set is present and that it defines the correct data set.
- 200 An error occurred attempting to change the RPL for keyed access.
- 204 An error occurred attempting to change the RPL for update access.
- 208 An error occurred attempting to change the RPL for non-update access.
- 316 A VSAM logical error occurred. Message CSFY0076 shows the ddname for the data set and the VSAM feedback code.
- 3078 The CKDS was created with an unsupported LRECL.

**System action:** Processing ends.

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

**User response:** Contact your system programmer.

---

### CSFY0036 Synad message (for VSAM or non-VSAM file).

**Explanation:** A physical error occurred while processing a VSAM or QSAM file.

For a QSAM file, the format and explanation of the message is in the SYNADAF macro instruction description.

For a VSAM file, the format and explanation of the message is in the Physical-Error Message Format figure.

**System action:** Processing ends.

**System programmer response:** See the appropriate document for the explanation of the message. Correct the problem and rerun the job. If you cannot resolve the problem, contact the IBM Support Center.

**User response:** Contact your system programmer.

---

### CSFY0056 I/O ROUTINE UNABLE TO ESTABLISH AN ESTAE.

**Explanation:** The ICSF I/O routine could not establish an ESTAE environment.

**System action:** Processing ends.

**System programmer response:** Contact the IBM Support Center.

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

---

### CSFY0076 VSAM ERROR OCCURRED PROCESSING DD *ddname*. VSAM FEEDBACK CODE = *fdbkcode*

**Explanation:** A VSAM logical error occurred while processing the data set that is specified by the *ddname* DD statement. The VSAM RPL Feedback Word *fdbkcode* indicates which error occurred.

**System action:** Processing ends.

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

**User response:** Check the VSAM RPL Feedback Word as documented in the *z/OS DFSMSdfp Diagnosis*. If you cannot correct the error, contact your system programmer.



---

**CSFY0086** VSAM ERROR OCCURRED PROCESSING DD *ddname*. OUT OF EXTENTS.

**Explanation:** A VSAM error has occurred processing a data set that is specified by the *ddname* DD statement. The data set is out of extents. The data set must be on a volume that has enough space for the data.

**System action:** Processing ends.

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

**User response:** Contact your system programmer.



---

## Appendix. Accessibility

Accessible publications for this product are offered through IBM Knowledge Center ([www.ibm.com/support/knowledgecenter/SSLTBW/welcome](http://www.ibm.com/support/knowledgecenter/SSLTBW/welcome)).

If you experience difficulty with the accessibility of any z/OS information, send a detailed email message to [mhvrcfs@us.ibm.com](mailto:mhvrcfs@us.ibm.com).

---

### Accessibility features

Accessibility features help users who have physical disabilities such as restricted mobility or limited vision use software products successfully. The accessibility features in z/OS can help users do the following tasks:

- Run assistive technology such as screen readers and screen magnifier software.
- Operate specific or equivalent features by using the keyboard.
- Customize display attributes such as color, contrast, and font size.

---

### Consult assistive technologies

Assistive technology products such as screen readers function with the user interfaces found in z/OS. Consult the product information for the specific assistive technology product that is used to access z/OS interfaces.

---

### Keyboard navigation of the user interface

You can access z/OS user interfaces with TSO/E or ISPF. The following information describes how to use TSO/E and ISPF, including the use of keyboard shortcuts and function keys (PF keys). Each guide includes the default settings for the PF keys.

- *z/OS TSO/E Primer*
- *z/OS TSO/E User's Guide*
- *z/OS ISPF User's Guide Vol I*

---

### Dotted decimal syntax diagrams

Syntax diagrams are provided in dotted decimal format for users who access IBM Knowledge Center with a screen reader. In dotted decimal format, each syntax element is written on a separate line. If two or more syntax elements are always present together (or always absent together), they can appear on the same line because they are considered a single compound syntax element.

Each line starts with a dotted decimal number; for example, 3 or 3.1 or 3.1.1. To hear these numbers correctly, make sure that the screen reader is set to read out punctuation. All the syntax elements that have the same dotted decimal number (for example, all the syntax elements that have the number 3.1) are mutually exclusive alternatives. If you hear the lines 3.1 USERID and 3.1 SYSTEMID, your syntax can include either USERID or SYSTEMID, but not both.

The dotted decimal numbering level denotes the level of nesting. For example, if a syntax element with dotted decimal number 3 is followed by a series of syntax

elements with dotted decimal number 3.1, all the syntax elements numbered 3.1 are subordinate to the syntax element numbered 3.

Certain words and symbols are used next to the dotted decimal numbers to add information about the syntax elements. Occasionally, these words and symbols might occur at the beginning of the element itself. For ease of identification, if the word or symbol is a part of the syntax element, it is preceded by the backslash (\) character. The \* symbol is placed next to a dotted decimal number to indicate that the syntax element repeats. For example, syntax element \*FILE with dotted decimal number 3 is given the format 3 \\* FILE. Format 3\* FILE indicates that syntax element FILE repeats. Format 3\* \\* FILE indicates that syntax element \* FILE repeats.

Characters such as commas, which are used to separate a string of syntax elements, are shown in the syntax just before the items they separate. These characters can appear on the same line as each item, or on a separate line with the same dotted decimal number as the relevant items. The line can also show another symbol to provide information about the syntax elements. For example, the lines 5.1\*, 5.1 LASTRUN, and 5.1 DELETE mean that if you use more than one of the LASTRUN and DELETE syntax elements, the elements must be separated by a comma. If no separator is given, assume that you use a blank to separate each syntax element.

If a syntax element is preceded by the % symbol, it indicates a reference that is defined elsewhere. The string that follows the % symbol is the name of a syntax fragment rather than a literal. For example, the line 2.1 %OP1 means that you must refer to separate syntax fragment OP1.

The following symbols are used next to the dotted decimal numbers.

**? indicates an optional syntax element**

The question mark (?) symbol indicates an optional syntax element. A dotted decimal number followed by the question mark symbol (?) indicates that all the syntax elements with a corresponding dotted decimal number, and any subordinate syntax elements, are optional. If there is only one syntax element with a dotted decimal number, the ? symbol is displayed on the same line as the syntax element, (for example 5? NOTIFY). If there is more than one syntax element with a dotted decimal number, the ? symbol is displayed on a line by itself, followed by the syntax elements that are optional. For example, if you hear the lines 5 ?, 5 NOTIFY, and 5 UPDATE, you know that the syntax elements NOTIFY and UPDATE are optional. That is, you can choose one or none of them. The ? symbol is equivalent to a bypass line in a railroad diagram.

**! indicates a default syntax element**

The exclamation mark (!) symbol indicates a default syntax element. A dotted decimal number followed by the ! symbol and a syntax element indicate that the syntax element is the default option for all syntax elements that share the same dotted decimal number. Only one of the syntax elements that share the dotted decimal number can specify the ! symbol. For example, if you hear the lines 2? FILE, 2.1! (KEEP), and 2.1 (DELETE), you know that (KEEP) is the default option for the FILE keyword. In the example, if you include the FILE keyword, but do not specify an option, the default option KEEP is applied. A default option also applies to the next higher dotted decimal number. In this example, if the FILE keyword is omitted, the default FILE(KEEP) is used. However, if you hear the lines 2? FILE, 2.1, 2.1.1! (KEEP), and 2.1.1 (DELETE), the default option KEEP applies only to the next higher dotted

decimal number, 2.1 (which does not have an associated keyword), and does not apply to 2? FILE. Nothing is used if the keyword FILE is omitted.

**\* indicates an optional syntax element that is repeatable**

The asterisk or glyph (\*) symbol indicates a syntax element that can be repeated zero or more times. A dotted decimal number followed by the \* symbol indicates that this syntax element can be used zero or more times; that is, it is optional and can be repeated. For example, if you hear the line 5.1\* data area, you know that you can include one data area, more than one data area, or no data area. If you hear the lines 3\* , 3 HOST, 3 STATE, you know that you can include HOST, STATE, both together, or nothing.

**Notes:**

1. If a dotted decimal number has an asterisk (\*) next to it and there is only one item with that dotted decimal number, you can repeat that same item more than once.
2. If a dotted decimal number has an asterisk next to it and several items have that dotted decimal number, you can use more than one item from the list, but you cannot use the items more than once each. In the previous example, you can write HOST STATE, but you cannot write HOST HOST.
3. The \* symbol is equivalent to a loopback line in a railroad syntax diagram.

**+ indicates a syntax element that must be included**

The plus (+) symbol indicates a syntax element that must be included at least once. A dotted decimal number followed by the + symbol indicates that the syntax element must be included one or more times. That is, it must be included at least once and can be repeated. For example, if you hear the line 6.1+ data area, you must include at least one data area. If you hear the lines 2+, 2 HOST, and 2 STATE, you know that you must include HOST, STATE, or both. Similar to the \* symbol, the + symbol can repeat a particular item if it is the only item with that dotted decimal number. The + symbol, like the \* symbol, is equivalent to a loopback line in a railroad syntax diagram.



---

## Notices

This information was developed for products and services that are offered in the USA or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
United States of America*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

This information could include missing, incorrect, or broken hyperlinks. Hyperlinks are maintained in only the HTML plug-in output for the Knowledge Centers. Use of hyperlinks in other output formats of this information is at your own risk.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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:

*IBM Corporation  
Site Counsel  
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 document 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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.



## COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

---

## Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

### Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

### Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

### Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

### Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY,

## IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s name, email address, phone number, or other personally identifiable information for purposes of enhanced user usability and single sign-on configuration. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at [ibm.com/privacy](http://ibm.com/privacy) and IBM’s Online Privacy Statement at [ibm.com/privacy/details](http://ibm.com/privacy/details) in the section entitled “Cookies, Web Beacons and Other Technologies,” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at [ibm.com/software/info/product-privacy](http://ibm.com/software/info/product-privacy).

---

## Policy for unsupported hardware

Various z/OS elements, such as DFSMS, JES2, JES3, and MVS™, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

---

## Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS ([www.ibm.com/software/support/systemsz/lifecycle](http://www.ibm.com/software/support/systemsz/lifecycle))

- For information about currently-supported IBM hardware, contact your IBM representative.

---

## Trademarks

IBM, the IBM logo, and [ibm.com](http://ibm.com)<sup>®</sup> 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 ([www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)).

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.



---

## Index

### A

accessibility 117  
  contact IBM 117  
  features 117  
assistive technologies 117

### C

contact  
  z/OS 117  
crypto education vi

### F

feedback vii

### K

keyboard  
  navigation 117  
  PF keys 117  
  shortcut keys 117

### N

navigation  
  keyboard 117

### S

sending to IBM  
  reader comments vii  
shortcut keys 117

### U

user interface  
  ISPF 117  
  TSO/E 117

### V

V2R1 changed information FMID  
  HCR77B0 xii  
V2R1 deleted information FMID  
  HCR77B0 xiii  
V2R1 new information FMID  
  HCR77B0 xii  
V2R2 changed information FMID  
  HCR77B1 xii  
V2R2 changed information FMID  
  HCR77C0 xi  
V2R2 deleted information FMID  
  HCR77B1 xii  
V2R2 deleted information FMID  
  HCR77C0 xi

V2R2 new information FMID  
  HCR77B1 xi  
V2R2 new information FMID  
  HCR77C0 x  
V2R3 changed information FMID  
  HCR77C1 x  
V2R3 deleted information FMID  
  HCR77C1 x  
V2R3 new information FMID  
  HCR77C1 ix







Printed in USA

SC14-7509-06

