Cryptographic Services
Integrated Cryptographic Service Facility
ICSF Compliance Evidence
APAR OA61977

Chapter 1. Overview

This document describes changes to the Integrated Cryptographic Service Facility (ICSF) product for support for ICSF Compliance evidence collection using SMF Type 1154 Subtype 49 records upon the receipt of an ENF event code 86.

These changes are available through the application of the PTF for APAR OA61977 and apply to FMID HCR77D1 and HCR77D2. In addition to installing the PTF for APAR OA61977, you must be running on z/OS 2.4 and later and have the PTF for OA61444 installed to enable this support.

All the enhancements included in this document will also be documented in the FMID HCR77D2 release of the following ICSF publications:

- ICSF System Programmer's Guide SC14-7507
- ICSF Messages SC14-7509

The new abend code will be documented in the z/OS 2.5 release of the following publication:

- z/OS MVS System Codes SA38-0665-50

Chapter 2. z/OS Cryptographic Services ICSF System Programmer's Guide (SC14-7507) updates

Appendix B. ICSF SMF Records

Record type 1154 Subtype 49 – ICSF Compliance Evidence

Record type 1154 Subtype 49 is written to record ICSF compliance evidence when an ENF86 signal is received. Record type 1154 Subtype 49 is mapped by the CSFZ1154 macro.

Reference the MVS System Management Facilities (SMF) guide for a complete description of the SMF 1154 record and subtypes.

Record type 1154 Subtype 49 header

Table 1. Record type 1154 Subtype 49 header

Offsets	Name	Length	Format	Description
0 0	Smf1154_49_Trn	2	binary	Number of triplets: 2
2 2	Smf1154_49_Rsv1	2		Reserved (X'00')
4 4	Smf1154_49_1_Offset	4	binary	Offset to first data section 1
8 8	Smf1154_49_1_Length	2	binary	Length of data section 1
10 A	Smf1154_49_1_Number	2	binary	Number of repeated data section 1's: 1
12 C	Smf1154_49_2_Offset	4	binary	Offset to first data section 2
16 10	Smf1154_49_2_Length	2	binary	Length of data section 2
18 12	Smf1154_49_2_Number	2	binary	Number of repeated data section 2's: 1

Record type 1154 Subtype 49 Data section 1

Data section 1 reports various ICSF security settings for ICSF Key Data Sets, ICSF resource classes, Key Store Policy, and other configuration and audit options.

Table 2. Record type 1154 Subtype 49 Data section 1				
Offset	**Name**	**Length**	**Format**	**Description**
0 0	SMF1154_49_1_VERSION	2	Binary	Version of this section: 1
2 2	SMF1154_49_1_PROTECTALLFAIL	1	Binary	RACF PROTECTALL setting X'01' PROTECTALL(FAIL) X'00' PROTECTALL(WARN) or NOPROTECTALL
3 3	SMF1154_49_1_CHKAUTH	1	Binary	Setting of CHKAUTH keyword in ICSF options dataset.
4 4	SMF1154_49_1_RSV1	28		Reserved
32 20	SMF1154_49_1_XFACILIT_ACT	1	Binary	XFACILIT class status X'01' Active X'00' Not Active
33 21	SMF1154_49_1_XFACILIT_RACL	1	Binary	XFACILIT class RACLIST status X'01' Raclisted X'00' Not Raclisted
34 22	SMF1154_49_1_KSPCTOKCHKLBLWARN	1	Binary	CSF.CKDS.TOKEN.CHECK.LABEL.WARN Setting X'01' Enabled X'00' Not Enabled
35 23	SMF1154_49_1_KSPCTOKCHKLBLFAIL	1	Binary	CSF.CKDS.TOKEN.CHECK.LABEL.FAIL Setting X'01' Enabled X'00' Not Enabled
36 24	SMF1154_49_1_KSPPTOKCHKLBLWARN	1	Binary	CSF.PKDS.TOKEN.CHECK.LABEL.WARN Setting X'01' Enabled X'00' Not Enabled

37 25	SMF1154_49_1_KSPPTOKCHKLBLFAIL	1	Binary	CSF.PKDS.TOKEN.CHECK.LABEL.FAIL Setting X'01' Enabled X'00' Not Enabled
38 26	SMF1154_49_1_KSPCTOKCHKDFLTLBL	1	Binary	CSF.CKDS.TOKEN.CHECK.DEFAULT.LABEL Setting X'01' Enabled X'00' Not Enabled
39 27	SMF1154_49_1_KSPPTOKCHKDFLTLBL	1	Binary	CSF.PKDS.TOKEN.CHECK.DEFAULT.LABEL Setting X'01' Enabled X'00' Not Enabled
40 28	SMF1154_49_1_KSP_CTOKNODUPS	1	Binary	CSF.CKDS.TOKEN.NODUPLICATES Setting X'01' Enabled X'00' Not Enabled
41 29	SMF1154_49_1_KSP_PTOKNODUPS	1	Binary	CSF.PKDS.TOKEN.NODUPLICATES Setting X'01' Enabled X'00' Not Enabled
42 2A	SMF1154_49_1_KSP_XKEYENABLEAES	1	Binary	CSF.XCSFKEY.ENABLE.AES Setting X'01' Enabled X'00' Not Enabled
43 2B	SMF1154_49_1_KSP_XKEYENABLEDES	1	Binary	CSF.XCSFKEY.ENABLE.DES Setting X'01' Enabled X'00' Not Enabled
44 2C	SMF1154_49_1_KSP_KEYSAUTHWARN	1	Binary	CSF.CSFKEYS.AUTHORITY.LEVELS.WARN Setting X'01' Enabled X'00' Not Enabled

45 2D	SMF1154_49_1_KSP_KEYSAUTHFAIL	1	Binary	CSF.CSFKEYS.AUTHORITY.LEVELS.FAIL Setting X'01' Enabled X'00' Not Enabled
46 2E	SMF1154_49_1_KSP_ARCHUSE	1	Binary	CSF.KDS.KEY.ARCHIVE.USE Setting X'01' Enabled X'00' Not Enabled
47 2F	SMF1154_49_1_KSP_ARCHDATADEC	1	Binary	CSF.KDS.KEY.ARCHIVE.DATA.DECRYPT Setting X'01' Enabled X'00' Not Enabled Note: This field is reserved (X'00') on HCR77D1.
48 30	SMF1154_49_1_KSP_KGUPAUTHCHK	1	Binary	CSF.KGUP.CSFKEYS.AUTHORITY.CHECK Setting X'01' Enabled X'00' Not Enabled
49 31	SMF1154_49_1_KSP_ECCPVTKEYNAME	1	Binary	CSF.CSFKEYS.ECC.PRIVATEKEYNAME.ENABLE Setting X'01' Enabled X'00' Not Enabled Note: This field is reserved (X'00') on HCR77D1.
50 32	SMF1154_49_1_RSV2	16		Reserved
66 42	SMF1154_49_1_AKL_CLBL	1	Binary	AUDITKEYLIFECKDS(LABEL()) X'01' YES X'00' NO
67 43	SMF1154_49_1_AKL_CTOK	1	Binary	AUDITKEYLIFECKDS(TOKEN()) X'01' YES X'00' NO
68 44	SMF1154_49_1_AKL_PLBL	1	Binary	AUDITKEYLIFEPKDS(LABEL())

				X'01' YES X'00' NO
69 45	SMF1154_49_1_AKL_PTOK	1	Binary	AUDITKEYLIFEPKDS(TOKEN()) X'01' YES X'00' NO
70 46	SMF1154_49_1_AKL_TTOKO	1	Binary	AUDITKEYLIFETKDS(TOKENOBJ()) X'01' YES X'00' NO
71 47	SMF1154_49_1_AKL_TSESSO	1	Binary	AUDITKEYLIFETKDS(SESSIONOBJ()) X'01' YES X'00' NO
72 48	SMF1154_49_1_RSV3	8		Reserved
80 50	SMF1154_49_1_AKU_CLBL	1	Binary	AUDITKEYUSGCKDS(LABEL()) X'01' YES X'00' NO
81 51	SMF1154_49_1_AKU_CTOK	1	Binary	AUDITKEYUSGCKDS(TOKEN()) X'01' YES X'00' NO
82 52	SMF1154_49_1_AKU_PLBL	1	Binary	AUDITKEYUSGPKDS(LABEL()) X'01' YES X'00' NO
83 53	SMF1154_49_1_AKU_PTOK	1	Binary	AUDITKEYUSGPKDS(TOKEN()) X'01' YES X'00' NO
84 54	SMF1154_49_1_AKU_P11TOKO	1	Binary	AUDITPKCS11USG(TOKENOBJ()) X'01' YES X'00'

				NO
85 55	SMF1154_49_1_AKU_P11SESSO	1	Binary	AUDITPKCS11USG(SESSIONOBJ()) X'01' YES X'00' NO
86 56	SMF1154_49_1_RSV4	32		Reserved
118 76	SMF1154_49_1_CC_SERVICES	1	Binary	Existence of installation defined services in the ICSF Installation Options Dataset. X'01' At least one SERVICE() entry specified in ICSF Installation Options Dataset X'00' No SERVICE() entries are defined in the ICSF Installation Options Dataset
119 77	SMF1154_49_1_CC_EXITS	1	Binary	Existence of installation exits in the ICSF Installation Options Dataset X'01' At least one EXIT() entry specified in ICSF Installation Options Dataset X'00' No EXIT() entries in ICSF Installation Options Dataset
120 78	SMF1154_49_1_RSV5	4		Reserved
124 7C	SMF1154_49_1_KDSFORMAT	3	Binary	ICSF Key Data Set (KDS) Format. Byte **1** CKDS Format **2** PKDS Format **3** TKDS Format Byte meaning when set X'00' Not defined X'01' Empty KDS X'02' Non KDSR Format X'03' KDSR Format X'04' KDSRL Format (Note: This value is applicable only on HCR77D2.)

127 7F	SMF1154_49_1_CLASS	292 * 4		ICSF class information. 4 contiguous instances each mapped by SMF1154_49_CLASS definition in Table X. The first instance is CSFSERV class profile access information. The second instance is CSFKEYS class profile access information. The third instance is CRYPTOZ class profile access information. The fourth instance is XCSFKEY class profile access information.
1295 50F	SMF1154_49_1_DFLTLBL	292 * 2		Default label checking for CKDS and PKDS. 2 contiguous instances each mapped by SMF1154_49_DL_CLASS definition in Table Y. The first instance is CKDS default label access controls. The second instance is PKDS default label access controls.
1879 757	SMF1154_49_1_KDS	327 * 3		CKDS, PKDS, and TKDS protection settings. 3 contiguous instances each mapped by Smf1154_49_Kds KDS Access Controls in Table Z. The first instance is CKDS access controls. The second instance is PKDS access controls. The third instance is TKDS access controls.

Table X: SMF1154_49_CLASS Profile access

Offset	Name	Length	Format	Description
0 0	SMF1154_49_CLS_NAME	8	EBCDIC	Class Name. CSFSERV, CSFKEYS, CRYPTOZ, and XCSFKEY.

8 8	SMF1154_49_CLS_ACTIVE	1	Binary	Class ACTIVE X'01' YES X'00' NO
9 9	SMF1154_49_CLS_RACLISTED	1	Binary	Class RACLISTed? X'01' YES X'00' NO
10 A	SMF1154_49_CLS_PROFLEN	1	Binary	Length of profile name
11 B	SMF1154_49_CLS_PROF	246	Char	Profile name '*' or '**'
257 101	SMF1154_49_CLS_PROFUACC	1	Binary	Profile UACC setting Bit Meaning when set 0 ALTER access 1 CONTROL access 2 UPDATE access 3 READ access 4 EXECUTE access 5–6 Reserved for IBM®'s use 7 NONE access.
258 102	SMF1154_49_CLS_PROFWARN	1	Binary	Profile WARN setting. Identifies the data set as having (bit 0 or 7 is on) or not having the WARNING attribute.
259 103	SMF1154_49_CLS_PROFIDSPLAT	1	Binary	ID(*) Setting X'01' ID(*) Access X'00' ID(*) not defined
260 104	SMF1154_49_CLS_RSV	32		Reserved

Table Y: SMF1154_49_DL_CLASS KDS Default Label Access Controls

Offset	Name	Length	Format	Description
0 0	SMF1154_49_DL_CLS_NAME	8	EBCDIC	Class name CSFKEYS
8 8	SMF1154_49_DL_CLS_ACTIVE	1	Binary	Class ACTIVE? X'01' YES X'00'

				NO
9 9	SMF1154_49_DL_CLS_RACLISTED	1	Binary	Class RACLISTed? X'01' YES X'00' NO
10 A	SMF1154_49_DL_CLS_PROFLEN	1	Binary	Length of profile name
11 B	SMF1154_49_DL_CLS_PROF	246	EBCDIC	Profile name CSF-CKDS-DEFAULT and CSF-PKDS-DEFAULT
257 101	SMF1154_49_DL_CLS_PROFUACC	1	Binary	UACC setting Bit Meaning when set 0 ALTER access 1 CONTROL access 2 UPDATE access 3 READ access 4 EXECUTE access 5–6 Reserved for IBM®'s use 7 NONE access.
258 102	SMF1154_49_DL_CLS_PROFWARN	1	Binary	WARN setting. Identifies the data set as having (bit 0 or 7 is on) or not having the WARNING attribute.
259 103	SMF1154_49_DL_CLS_PROFIDSPLAT	1	Binary	ID(*) setting: X'01' ID(*) Access X'00' ID(*) not defined
260 104	SMF1154_49_DL_CLS_RSV	32		Reserved

Table Z: Smf1154_49_Kds KDS Access Controls				
Offset	**Name**	**Length**	**Format**	**Description**
0 0	SMF1154_49_KDS_TYPE	1	Binary	The KDS type X'00' Not defined X'01' CKDS X'02' PKDS X'03' TKDS

1 1	SMF1154_49_KDS_NAME	44	EBCDIC	KDS name
45 2D	SMF1154_49_KDS_PROFLEN	1	Binary	Length of profile protecting KDS. If X'00', no profile has been defined to protect the KDS.
46 2E	SMF1154_49_KDS_PROF	246	EBCDIC	The name of the profile protecting the KDS
292 124	SMF1154_49_KDS_PROFUACC	1	Binary	UACC Settings Bit Meaning when set 0 ALTER access 1 CONTROL access 2 UPDATE access 3 READ access 4 EXECUTE access 5–6 Reserved for IBM®'s use 7 NONE access.
293 125	SMF1154_49_KDS_PROFWARN	1	Binary	WARN Settings identifies the data set as having (bit 0 or 7 is on) or not having the WARNING attribute.
294 126	SMF1154_49_KDS_PROFIDSPLAT	1	Binary	ID(*) Settings
295 127	SMF1154_49_KDS_RSV	32		Reserved

Record type 1154 Subtype 49 Data section 2

Data section 2 reports the algorithm names and their counts used in ICSF services since the last ENF86 signal was received. You must have Cryptographic algorithm (ALG) usage statistics enabled for data section 2 to be included in the SMF type 1154 Subtype 49 record.

Table 3: Record type 1154 Subtype 49 Data section 2

Offset	Name	Length	Format	Description
0 0	Smf1154_49_2_Version	2	Binary	Version of this section: 1
2 2	Smf1154_49_2_Rsv1	2		Reserved
4 4	Smf1154_49_2_AlgsCount	4	Binary	Number of entries in Smf1154_49_2_Alg
8 8	Smf1154_49_2_Alg	16 * Smf1154_49_2_AlgsCount		Algorithm count information since the ENF86 signal was received. Each instance is mapped by table A: Smf1154_49_2_Alg algorithm count information.

Table A: Smf1154_49_2_Alg algorithm count information				
Offset	**Name**	**Length**	**Format**	**Description**
0 0	Smf1154_49_2_Alg_Func	8	EBCDIC	Algorithm name. See table “SMF82STAT_ALG algorithm names” in the ICSF System Programmer’s Guide.
8 8	Smf1154_49_2_Alg_Count	8	Binary	Number of times algorithm was used during ENF86 interval.

Chapter 3. z/OS Cryptographic Services ICSF Messages (SC14-7509) updates

Chapter 8. CSFMnnnn messages (ICSF address space)

CSFM733E ENFREQ LISTEN FOR ENF 86 FAILED RC=*rc*. SMF TYPE 1154 SUBTYPE 49 WILL NOT BE LOGGED.

Explanation
The ENFREQ ACTION=LISTEN for ENF event code 86 has failed. SMF Type 1154 Subtype 49 ICSF compliance evidence records will not be logged. Your system does not have the required pre-requisite APARs installed to enable this support.
SMF Type 1154 requires z/OS 2.4 and later and must have the PTF for OA61444 installed.

In the message text:
rc
The return code from the ENFREQ macro.

System action

Processing continues**.**

System programmer response
Determine the cause of the failure by looking up the return code in the z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG. Ensure that the PTF for OA61444 is installed. Once installed, ICSF must be restarted.

Chapter 4. z/OS MVS System Codes (SA38-0655-50) updates

Chapter 2 System Completion Codes

18F

48E An error occurred during ATTACH of the CSFMICMP task.