ICSF Verify Key Check Value

In order to verify that a cryptographic key has been entered correctly many cryptographic implementations rely on "thumbprint calculation" called a Key Check Value (KCV). If someone wishes to verify that the key value entered is as expected and not incorrectly entered, one would check the KCV.

One widely used method for calculating a KCV is to use the Key in question to encipher an 8 byte HEX zero value. The resulting leftmost 4 digits (2 bytes) of the cryptogram are then called the Key Check Value (KCV).

Unlike many crypto systems ICSF and the Crypto Coprocessor Facility (CCF) do not have calculation of the KCV as an automated utility function. OS/390 ICSF V2R10 has an API that allows this same value to be created (CSNBKYT ENC-ZERO), but the API only executes on a PCICC feature not a CCF. Thus, prior OS/390 releases and systems without a PCICC adjunct coprocessor do not have this capability.

The KCV4ISPF program (callable from an ISPF panel) is a method of calculating the key check value without using a PCICC. The application does not rely on the presence of NOCV keys, nor does it ever expose or put any existing key into clear text form. It does, however, only work on keys stored in the CKDS.

The application externally consists of two ISPF panels and a message file. The assembler code uses the input from the panels and processes the key in a secure manner to provide a key check value. This sample application elements are:

Assembler Program (page 7)
- ✓ KCV4ISPF.ASM

ISPF Panels (page 4)
- ✓ KCVPAN01
- ✓ KCVPAN02

Message file (page 3)
- ✓ KCV00

CLIST (page 3)
- ✓ KCVALLOC

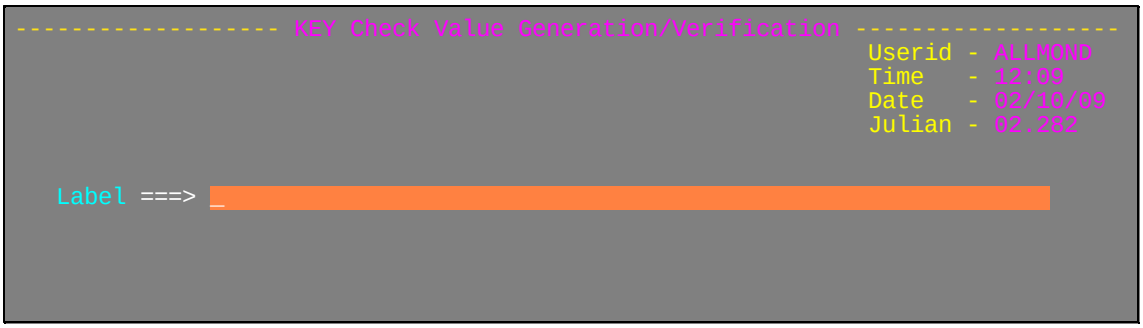
Documentation
- ✓ KCV4ISFP.DOC

Contents of each of the elements are listed in this documentation following the panel examples.

ICSF Verify Key Check Value

The first panel seen on invocation of the program requests the label of the key residing within the ICSF CKDS.

KCVPAN01 Figure 1.

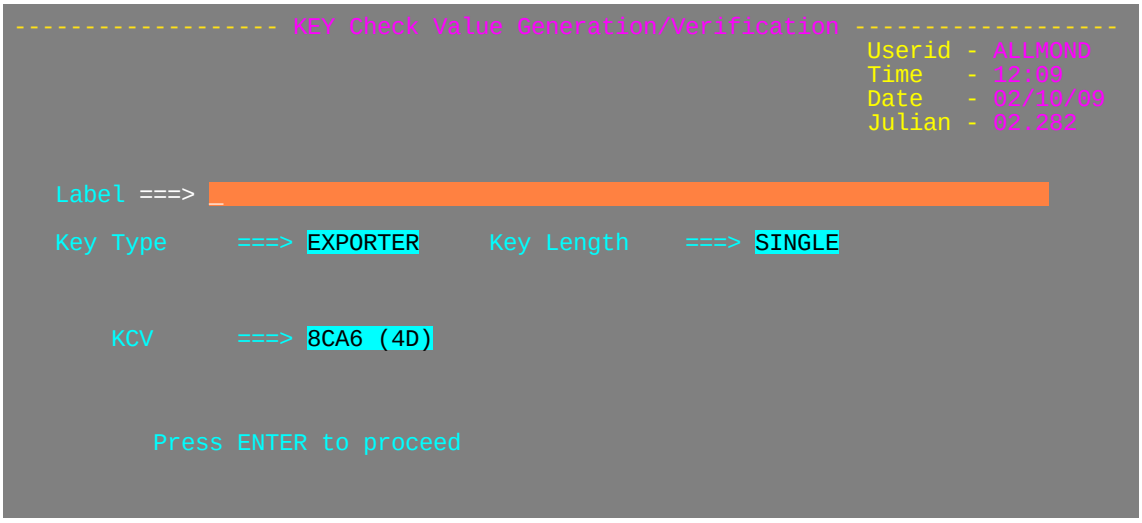


Type in the key label of the key value you wish to confirm with a KCV.

KCVPAN01 Figure 2.

Enter

KCVPAN02 Figure 3.



ICSF Verify Key Check Value

The following is a CLIST (KCVALLOC) that will allocate the panels and message file for the current ISPF session:

```
concatd da(panels) fi(ispplib) after
concatd da(msgs) fi(ispmlib) after
```

The following is the ISPF message file (KCV00) for the application:

```
KCV001E 'INVALID KEY NAME'            .ALARM=YES
'KEY NAME NOT SPECIFIED'

KCV002E 'KEY LABEL NOT FOUND'         .ALARM=YES
'KEY LABEL NOT FOUND OR CKDS IN USE'
```

ICSF Verify Key Check Value

The following two panels (KCVPAN01 and KCVPAN02) are used by the application. KCVPAN01 is below and KCVPAN02 is on page 6. See page 2 for their visual display.

```
)ATTR
  /*****************************************/
  /**                                     **/
  /**             ISPF attribute symbols  **/
  /**                                     **/
  /*****************************************/
  ¢ TYPE(TEXT)  COLOR(YELLOW) INTENS(LOW)
  ¬ TYPE(TEXT)  COLOR(YELLOW) INTENS(HIGH)
  ¦ TYPE(TEXT)  COLOR(YELLOW) INTENS(HIGH) HILITE(REVERSE)
  } TYPE(TEXT)  COLOR(BLUE)   INTENS(HIGH) HILITE(REVERSE)
  + TYPE(TEXT)  COLOR(BLUE)   INTENS(LOW)
  @ TYPE(TEXT)  COLOR(BLUE)   INTENS(HIGH)
  { TYPE(TEXT)  COLOR(TURQ)   INTENS(LOW)
  # TYPE(TEXT)  COLOR(TURQ)   INTENS(HIGH) HILITE(REVERSE)
  ! TYPE(TEXT)  COLOR(GREEN)  INTENS(HIGH)
  $ TYPE(TEXT)  COLOR(RED)    INTENS(HIGH)
  ; TYPE(INPUT) COLOR(RED)    INTENS(HIGH) HILITE(REVERSE)
  % TYPE(TEXT)  COLOR(WHITE)  INTENS(LOW)
  ? TYPE(TEXT)  COLOR(WHITE)  INTENS(HIGH)
  \ TYPE(TEXT)  COLOR(PINK)   INTENS(HIGH)
  ~ TYPE(TEXT)  COLOR(PINK)   INTENS(LOW)
  ` TYPE(TEXT)
  | TYPE(TEXT)
  _ TYPE(INPUT) COLOR(RED)      INTENS(HIGH)
)BODY WIDTH(&ZSCREENW) EXPAND("")
¬"-"\KEY Check Value Generation/Verification¬"-"
$" "¢Userid -~&ZUSER  @
$" "¢Time   -~&ZTIME  @
$" "¢Date   -~&ZDATE  @
$" "¢Julian -~&ZJDATE @
$
$
  { Label%===>;KEYNM
    +
$
$
$
$
$
$
$
$
$
$
$
$
$
)INIT
  &KEYNM = ' '
  &KYTYPE = ' '
  &CKKEY = ' '
   VPUT (KEYNM) PROFILE
```

```
   VPUT (KYTYPE) PROFILE
   VPUT (CKKEY) PROFILE
)PROC
  VER (&KEYNM,NB,MSG=KCV001E)
  VPUT (KEYNM) PROFILE
)END
```

ICSF Verify Key Check Value

```
)ATTR
  /*****************************************/
  /**                                     **/
  /**             ISPF attribute symbols  **/
  /**                                     **/
  /*****************************************/
  ¢ TYPE(TEXT)  COLOR(YELLOW) INTENS(LOW)
  ¬ TYPE(TEXT)  COLOR(YELLOW) INTENS(HIGH)
  ¦ TYPE(TEXT)  COLOR(YELLOW) INTENS(HIGH) HILITE(REVERSE)
  } TYPE(TEXT)  COLOR(BLUE)   INTENS(HIGH) HILITE(REVERSE)
  + TYPE(TEXT)  COLOR(BLUE)   INTENS(LOW)
  @ TYPE(TEXT)  COLOR(BLUE)   INTENS(HIGH)
  { TYPE(TEXT)  COLOR(TURQ)   INTENS(LOW)
  # TYPE(OUTPUT)  COLOR(TURQ)   INTENS(HIGH) HILITE(REVERSE)
  ! TYPE(TEXT)  COLOR(GREEN)  INTENS(HIGH)
  $ TYPE(TEXT)  COLOR(RED)    INTENS(HIGH)
  ; TYPE(INPUT) COLOR(RED)    INTENS(HIGH) HILITE(REVERSE)
  % TYPE(TEXT)  COLOR(WHITE)  INTENS(LOW)
  ? TYPE(TEXT)  COLOR(WHITE)  INTENS(HIGH)
  \ TYPE(TEXT)  COLOR(PINK)   INTENS(HIGH)
  ~ TYPE(TEXT)  COLOR(PINK)   INTENS(LOW)
  ` TYPE(TEXT)
  | TYPE(TEXT)
  _ TYPE(INPUT) COLOR(RED)      INTENS(HIGH)
)BODY WIDTH(&ZSCREENW) EXPAND("")
¬"-"\KEY Check Value Generation/Verification¬"-"
$" "¢Userid -~&ZUSER  @
$" "¢Time   -~&ZTIME  @
$" "¢Date   -~&ZDATE  @
$" "¢Julian -~&ZJDATE @
$
$
  { Label%===>;KEYNM
    +
$
  { Key Type    %===>#KYTYPE  +  { Key Length   %===>#KYLEN +
$
$
$
$      {KCV     %===>#CKKEY    +
$
$
$
       $ {Press ENTER to proceed
$
)INIT
   VGET (KEYNM) PROFILE
)PROC
   VGET (KYTYPE) PROFILE
   VGET (KYLEN) PROFILE
   VGET (CKKEY) PROFILE
   VPUT (KEYNM) PROFILE
)END
```

ICSF Verify Key Check Value

Following is the ASM source code for the application:

```
        TITLE 'KCV4ISPF'                                                00010000
KCV4ISPF AMODE 31                                                       00020000
KCV4ISPF RMODE ANY                                                      00030000
*****************************************************************       00040000
* TITLE: KCV4ISPF                                               *       00050000
*                                                               *       00060000
* FUNCTION: PRODUCE KCV FOR AN ICSF CKDS KEY RECORD             *       00070000
*                                                               *       00080000
*                                                               *       00090000
*****************************************************************       00100000
R0       EQU   0                                                        00110000
R1       EQU   1                                                        00120000
R2       EQU   2                                                        00130000
R3       EQU   3                                                        00140000
R4       EQU   4                                                        00150000
R5       EQU   5                                                        00160000
R6       EQU   6                                                        00170000
R7       EQU   7                                                        00180000
R8       EQU   8                                                        00190000
R9       EQU   9                                                        00200000
R10      EQU   10                                                       00210000
R11      EQU   11                                                       00220000
R12      EQU   12                                                       00230000
R13      EQU   13                                                       00240000
R14      EQU   14                                                       00250000
R15      EQU   15                                                       00260000
        EJECT                                                           00270000
KCV4ISPF CSECT                                                          00280000
        USING KCV4ISPF,R12,R11        SET UP BASE REGISTER              00290000
        LA    R2,4095                       SET INCREMENT 4K            00300000
        LA    R2,1(R2)                                                  00310000
        STM   R14,R12,12(R13)         SAVE REGISTERS                    00320000
        LR    R12,R15                 SET UP ADDRESSABILITY             00330000
        LA    R11,0(R2,R12)                 SET SECOND BASE REG         00340000
        LA    R2,SAVEAREA                                               00350000
        ST    R13,4(R2)               SET UP SAVE AREA CHAIN            00360000
        LR    R13,R2                                                    00370000
        B     START                   BRANCH AROUND CONSTANT            00380000
        DC    C'** KCV4ISPF **'       MODULE                            00390000
        DC    C'** &SYSDATE **'       ASM DATE                          00400000
        DC    C'** &SYSTIME **'       ASM TIME                          00410000
        DC    C'**CREATED 10/25/00 **'                                  00420000
        DC    C'** E.H. NACHTIGALL **' AUTHOR                           00430000
*                                                                       00440000
START    DS    0H                                                       00450000
*    /* LOGIC: GET OUR VARIABLES FROM ISPF.                    */      00460000
        CALL  ISPLINK,                          DISPLAY PANEL          X00470000
              (DISPLAY,KCVPAN01,BLANK),VL                               00480000
        LTR   R15,R15                                                   00490000
        BNZ   END                                                       00500000
KRRLABEL DS    0H                                                       00510000
        MVC   COPYLEN(4),LEN60                                          00520000
        MVC   KEYNM(64),=CL64' '    CLEAN OUT KEY LABEL                 00530000
        CALL  ISPLINK,                GET KEY LABEL                    X00540000
```

ICSF Verify Key Check Value

```
         (VCOPY,CKEYNM,COPYLEN,KEYNM,MOVE),VL                          00550000
      MVC  KEYNMSAV(64),KEYNM    SAVE CURRENT LABEL                    00560000
      MVC  KYTYPE(8),=CL8' '       CLEAN OUT KEY TYPE                  00570000
      CALL CSNBKRR,              GET RECORD                           X00580000
         (RETCODE,RESCODE,EXITLEN,EXITDATA,KEYNM,WORKTOKE)             00590000
      CLC  RETCODE(4),=F'0'      FOUND?                                00600000
      BNE  KRRERROR                                                    00610000
      CLC  WORKEY3(8),=D'0'                                            00620000
      BNE  KEY3                                                        00630000
      CLC  WORKEYR(8),=D'0'                                            00640000
      BNE  KEY2                                                        00650000
      MVC  KEYLENG(8),SINGLE                                           00660000
      B    DORNG                                                       00670000
KEY3   DS   0H                                                         00680000
      MVC  KEYLENG(8),TRIPLE                                           00690000
      B    DORNG                                                       00700000
KEY2   DS   0H                                                         00710000
      MVC  KEYLENG(8),DOUBLE                                           00720000
DORNG  DS   0H                                                         00730000
      CALL CSNBRNG,              GENERATE A RANDOM IMPORTER           X00740000
         (RETCODE,RESCODE,EXITLEN,EXITDATA,FORMODD,IMPORTL)            00750000
      CALL CSNBRNG,                                                   X00760000
         (RETCODE,RESCODE,EXITLEN,EXITDATA,FORMODD,IMPORTR)            00770000
      CALL CSNBSKI,              CREATE IMPORTER                      X00780000
         (RETCODE,RESCODE,EXITLEN,EXITDATA,IMPORTKY,IMPTYPE,          X00790000
         FORMOP,ZERO,WORKIMP)                                          00800000
      CALL CSNBCKI,              CREATE DATA KEY, HEX ZEROES          X00810000
         (RETCODE,RESCODE,EXITLEN,EXITDATA,ZERO,DATAZERO)              00820000
      CLC  WORKCVL(4),=F'0'       DATA KEY?                            00830000
      BE   GOTDATA                                                     00840000
      CLC  WORKCVL(2),CVMAC       MAC?                                 00850000
      BE   GOTMAC                                                      00860000
      CLC  WORKCVL(2),CVXLAT      DATAXLAT?                            00870000
      BE   GOTXLAT                                                     00880000
      CLC  WORKCVL(2),CVIPIN      IPINENC?                             00890000
      BE   GOTIPE                                                      00900000
      CLC  WORKCVL(2),CVOPIN      OPINENC?                             00910000
      BE   GOTOPE                                                      00920000
      CLC  WORKCVL(3),CVPINVER    PINVER?                              00930000
      BE   GOTPVER                                                     00940000
      CLC  WORKCVL(3),CVPINGEN    PINGEN?                              00950000
      BE   GOTPGEN                                                     00960000
      CLC  WORKCVL(2),CVEXP       EXPORTER?                            00970000
      BE   GOTEXP                                                      00980000
      CLC  WORKCVL(2),CVIMP       IMPORTER?                            00990000
      BE   GOTIMP                                                      01000000
      MVC  KYTYPE(8),=CL8'UNKNOWN'                                     01010000
      B    MAKEXP                  ?????                               01020000
GOTIPE  DS   0H                                                        01030000
      MVC  KYTYPE(8),IPINENC                                           01040000
      B    MAKEXP                                                      01050000
GOTOPE  DS   0H                                                        01060000
      MVC  KYTYPE(8),OPINENC                                           01070000
      B    MAKEXP                                                      01080000
GOTPVER DS   0H                                                        01090000
      MVC  KYTYPE(8),PINVER                                            01100000
      B    MAKEXP                                                      01110000
```

ICSF Verify Key Check Value

```
GOTPGEN  DS    0H                                                       01120000
         MVC   KYTYPE(8),PINGEN                                         01130000
         B     MAKEXP                                                   01140000
GOTEXP   DS    0H                                                       01150000
         MVC   KYTYPE(8),EXPTYPE                                        01160000
         B     MAKEXP                                                   01170000
GOTIMP   DS    0H                                                       01180000
         MVC   KYTYPE(8),IMPTYPE                                        01190000
MAKEXP   DS    0H                                                       01200000
*  HERE WE EFFECTIVELY STRIP OFF THE CONTROL VECTORS (LEFT AND RIGHT)   01210000
*       AND BASE THE RESULTING ENCRYPTED KEY ON RANDOM IMPORTER          01220000
         MVC   EXPLEFT(8),IMPORTL                                       01230000
         XC    EXPLEFT(8),WORKCVL                                       01240000
         MVC   EXPRIGHT(8),IMPORTR                                      01250000
         XC    EXPRIGHT(8),WORKCVL                                      01260000
         CALL  CSNBSKI,         MAKE THIS AN EXPORTER (LEFT)           X01270000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,EXPORTKY,EXPTYPE,      X01280000
               FORMOP,ZERO,WORKEXPL)                                    01290000
         MVC   EXPLEFT(8),IMPORTL                                       01300000
         XC    EXPLEFT(8),WORKCVR                                       01310000
         MVC   EXPRIGHT(8),IMPORTR                                      01320000
         XC    EXPRIGHT(8),WORKCVR                                      01330000
         CALL  CSNBSKI,         MAKE THIS AN EXPORTER (RIGHT)          X01340000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,EXPORTKY,EXPTYPE,      X01350000
               FORMOP,ZERO,WORKEXPR)                                    01360000
         XC    WORKTOKE(4),WORKTOKE                                     01370000
         CALL  CSNBKEX,         EXPORT THE LABEL                       X01380000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,KYTYPE,KEYNM,          X01390000
               WORKEXPL,WORKTOKE)                                       01400000
         MVC   ENCLEFT(8),WORKEYL      LEFT HALF NOW UNDER RANDOM KEY   01410000
         XC    WORKTOKE(4),WORKTOKE                                     01420000
         CALL  CSNBKEX,                                                 X01430000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,KYTYPE,KEYNM,          X01440000
               WORKEXPR,WORKTOKE)                                       01450000
*   KTB, THEN IMPORT USING WORKIMP                                      01460000
         CLC   ENCLEFT(8),WORKEYR      SAME CRYPTOGRAM?                 01470000
         BNE   NOTSINGL                                                 01480000
         MVC   KEYLENG(8),SINGLE       YES, THEREFORE SINGLE LENGTH     01490000
NOTSINGL DS    0H                                                       01500000
         MVC   EXPLEFT(8),IMPORTL                                       01510000
         XC    EXPLEFT(8),WORKCVL                                       01520000
         XC    EXPLEFT(8),CVEXPL                                        01530000
         MVC   EXPRIGHT(8),IMPORTR                                      01540000
         XC    EXPRIGHT(8),WORKCVL                                      01550000
         XC    EXPRIGHT(8),CVEXPL                                       01560000
         CALL  CSNBSKI,         MAKE THIS AN EXPORTER (LEFT)           X01570000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,EXPORTKY,EXPTYPE,      X01580000
               FORMOP,ZERO,WORKEXPL)                                    01590000
         MVC   EXPLEFT(8),IMPORTL                                       01600000
         XC    EXPLEFT(8),WORKCVR                                       01610000
         XC    EXPLEFT(8),CVEXPR                                        01620000
         MVC   EXPRIGHT(8),IMPORTR                                      01630000
         XC    EXPRIGHT(8),WORKCVR                                      01640000
         XC    EXPRIGHT(8),CVEXPR                                       01650000
         CALL  CSNBSKI,         MAKE THIS AN EXPORTER (RIGHT)          X01660000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,EXPORTKY,EXPTYPE,      X01670000
               FORMOP,ZERO,WORKEXPR)                                    01680000
```

ICSF Verify Key Check Value

```
         XC    WORKTOKE(4),WORKTOKE                                      01690000
         CALL  CSNBKEX,          EXPORT THE LABEL                       X01700000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,KYTYPE,KEYNM,          X01710000
               WORKEXPL,WORKTOKE)                                        01720000
         MVC   ENCLEFT(8),WORKEYL      LEFT HALF NOW UNDER RANDOM KEY    01730000
         XC    WORKTOKE(4),WORKTOKE                                      01740000
         CALL  CSNBKEX,                                                 X01750000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,KYTYPE,KEYNM,          X01760000
               WORKEXPR,WORKTOKE)                                        01770000
*   KTB, THEN IMPORT USING WORKIMP                                      01780000
         MVC   ENCRIGHT(8),WORKEYR     RIGHT HALF NOW UNDER RANDOM KEY   01790000
BLDTOKEN DS    0H                                                       01800000
         XC    IMPORTL(8),IMPORTL      ERASE IMPORTER                    01810000
         XC    IMPORTR(8),IMPORTR                                        01820000
         MVC   EXTYPFLG(1),=XL1'02'    FORM IT INTO AN EXTERNAL TOKEN    01830000
         MVC   EXFLAG(1),=XL1'C0'                                        01840000
         MVC   CVL(8),CVEXPL           EXPORTER KEY TYPE                 01850000
         MVC   CVR(8),CVEXPR                                             01860000
         SR    R3,R3                   CALCULATE NEW TVV                 01870000
         L     R4,EXTOKEN                                                01880000
         AR    R3,R4                                                     01890000
         L     R4,EXTOKEN+4                                              01900000
         AR    R3,R4                                                     01910000
         L     R4,EXTOKEN+8                                              01920000
         AR    R3,R4                                                     01930000
         L     R4,EXTOKEN+12                                             01940000
         AR    R3,R4                                                     01950000
         L     R4,EXTOKEN+16                                             01960000
         AR    R3,R4                                                     01970000
         L     R4,EXTOKEN+20                                             01980000
         AR    R3,R4                                                     01990000
         L     R4,EXTOKEN+24                                             02000000
         AR    R3,R4                                                     02010000
         L     R4,EXTOKEN+28                                             02020000
         AR    R3,R4                                                     02030000
         L     R4,EXTOKEN+32                                             02040000
         AR    R3,R4                                                     02050000
         L     R4,EXTOKEN+36                                             02060000
         AR    R3,R4                                                     02070000
         L     R4,EXTOKEN+40                                             02080000
         AR    R3,R4                                                     02090000
         L     R4,EXTOKEN+44                                             02100000
         AR    R3,R4                                                     02110000
         L     R4,EXTOKEN+48                                             02120000
         AR    R3,R4                                                     02130000
         L     R4,EXTOKEN+52                                             02140000
         AR    R3,R4                                                     02150000
         L     R4,EXTOKEN+56                                             02160000
         AR    R3,R4                                                     02170000
         ST    R3,TVV                                                    02180000
         CALL  CSNBKIM,               IMPORT THIS NEW EXPORTER          X02190000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,EXPTYPE,EXTOKEN,       X02200000
               WORKIMP,TARGET)                                           02210000
         XC    WORKTOKE(8),WORKTOKE                                      02220000
         CALL  CSNBKEX,                EXPORT HEX ZEROES                 X02230000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,TYPEDATA,DATAZERO,     X02240000
               TARGET,WORKTOKE)                                          02250000
```

ICSF Verify Key Check Value

```
         MVC   KCVHEX(8),WORKEYL       ENCRYPTED KEY IS KCV             02260000
         B     FORMKCV                                                  02270000
GOTMAC   DS    0H                                                       02280000
* CREATE KEY CHECK VALUE                                               02290000
         CLC   WORKCVL(3),CVMACVER                                      02300000
         BNE   DOMACVER                                                 02310000
         MVC   KYTYPE(8),MAC           JUST MACGEN HEX ZEROES           02320000
         CALL  CSNBMGN,                                                X02330000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,WORKTOKE,LEN8,ZERO,    X02340000
               RAC0,ZERO,CV,KCVHEX)                                     02350000
         B     FORMKCV                                                  02360000
DOMACVER DS    0H                                                       02370000
         MVC   KYTYPE(8),MACVER        FORMAT SINGLE LENGTH MACVER      02380000
         MVC   EXPLEFT(8),IMPORTL         INTO DOUBLE LENGTH EXPORTER   02390000
         XC    EXPLEFT(8),WORKCVL                                       02400000
         XC    EXPLEFT(8),CVEXPL                                        02410000
         MVC   EXPRIGHT(8),IMPORTR                                      02420000
         XC    EXPRIGHT(8),WORKCVL                                      02430000
         XC    EXPRIGHT(8),CVEXPL                                       02440000
         CALL  CSNBSKI,                CREATE EXPORTER LEFT             X02450000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,EXPORTKY,EXPTYPE,      X02460000
               FORMOP,ZERO,WORKEXPL)                                    02470000
         MVC   EXPLEFT(8),IMPORTL                                       02480000
         XC    EXPLEFT(8),WORKCVL                                       02490000
         XC    EXPLEFT(8),CVEXPR                                        02500000
         MVC   EXPRIGHT(8),IMPORTR                                      02510000
         XC    EXPRIGHT(8),WORKCVL                                      02520000
         XC    EXPRIGHT(8),CVEXPR                                       02530000
         CALL  CSNBSKI,                CREATE EXPORTER RIGHT            X02540000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,EXPORTKY,EXPTYPE,      X02550000
               FORMOP,ZERO,WORKEXPR)                                    02560000
         XC    WORKTOKE(4),WORKTOKE                                     02570000
         CALL  CSNBKEX,                EXPORT THE KEY (LEFT)            X02580000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,KYTYPE,KEYNM,          X02590000
               WORKEXPL,WORKTOKE)                                       02600000
         MVC   ENCLEFT(8),WORKEYL                                       02610000
         XC    WORKTOKE(4),WORKTOKE                                     02620000
         CALL  CSNBKEX,               EXPORT THE KEY (RIGHT)            X02630000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,KYTYPE,KEYNM,          X02640000
               WORKEXPR,WORKTOKE)                                       02650000
*   KTB, THEN IMPORT USING WORKIMP                                      02660000
         MVC   ENCRIGHT(8),WORKEYL    SINGLE LENGTH TO KEY RIGHT        02670000
         B     BLDTOKEN               BUILD AN EXTERNAL EXPORTER        02680000
GOTXLAT  DS    0H                                                       02690000
* HERE WE CREATE A CRYPTOGRAM OF HEX ZEROES, KNOWN DATAXLAT IN KEY      02700000
         MVC   KYTYPE(8),DATAXLAT                                       02710000
         CALL  CSNBECO,                                                X02720000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,ZERO,ZERO,WORKECO)     02730000
         CALL  CSNBSKI,                CREATE KNOWN IN DATAXLAT         X02740000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,ZERO,DATAXLAT,         X02750000
               FORMOP,ZERO,XLATIN)                                      02760000
         CALL  CSNBCTT,                TRANSLATE HEX ZEROES FOR KCV     X02770000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,XLATIN,WORKTOKE,       X02780000
               LEN8,WORKECO,ZERO,ZERO,KCVHEX)                           02790000
         B     FORMKCV                                                  02800000
GOTDATA  DS    0H                                                       02810000
* CREATE KEY CHECK VALUE                                               02820000
```

ICSF Verify Key Check Value

```
         MVC   KYTYPE(8),TYPEDATA                                        02830000
         CALL  CSNBENC,                JUST ENCIPHER HEX ZEROES         X02840000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,WORKTOKE,LEN8,ZERO,    X02850000
               IV,RAC1,RACENC,PAD,CV,KCVHEX)                            02860000
FORMKCV  DS    0H                                                       02870000
*                                                                       02880000
*        FORMAT KEY CHECK VALUE TO CHARACTER                            02890000
         MVC   COPYLEN(4),LEN3                                          02900000
         CALL  CSNBXBC,                                                 X02910000
               (RETCODE,RESCODE,EXITLEN,EXITDATA,COPYLEN,KCVHEX,        X02920000
               CHARKCV,XBCTABLE)                                        02930000
         MVC   CKKEY(4),CHARKCV                                         02940000
         MVC   CKKEY+6(2),CHARKCV+4                                     02950000
*                                                                       02960000
*                                                                       02970000
IMPORT   DS    0H                                                       02980000
*    /* LOGIC: REPLACE ISPF VARIABLES WITH OURS                  */     02990000
         MVC   COPYLEN(4),LEN9                                          03000000
         CALL  ISPLINK,                SET KCV                          X03010000
               (VREPLACE,CCKKEY,COPYLEN,CKKEY,MOVE),VL                  03020000
         MVC   COPYLEN(4),LEN8                                          03030000
         CALL  ISPLINK,                SET KEY TYPE                     X03040000
               (VREPLACE,CKYLEN,COPYLEN,KEYLENG,MOVE),VL                03050000
         MVC   COPYLEN(4),LEN8                                          03060000
         CALL  ISPLINK,                SET KEY TYPE                     X03070000
               (VREPLACE,CKYTYPE,COPYLEN,KYTYPE,MOVE),VL                03080000
         CALL  ISPLINK,                DISPLAY PANEL                    X03090000
               (DISPLAY,KCVPAN02,BLANK),VL                              03100000
         LTR   R15,R15                                                  03110000
         BNZ   END                                                      03120000
         MVC   COPYLEN(4),LEN60                                         03130000
         CALL  ISPLINK,                NEW LABEL ENTERED?               X03140000
               (VCOPY,CKEYNM,COPYLEN,KEYNM,MOVE),VL                     03150000
         LTR   R15,R15                                                  03160000
         BNZ   END                     PF3?                             03170000
         CLC   KEYNMSAV(64),KEYNM      NEW LABEL?                       03180000
         BE    START                   NO, BACK TO INITIAL PANEL        03190000
         B     KRRLABEL                YES, PROCESS                     03200000
*                                                                       03210000
KRRERROR DS    0H                                                       03220000
         MVC   ERRMSG(8),=CL8'KCV002E' CKDS BUSY, OR NO RECORD          03230000
GOTERROR DS    0H                                                       03240000
*                                                                       03250000
         CALL  ISPLINK,                           DISPLAY MESSAGE       X03260000
               (SETMSG,ERRMSG),VL                                       03270000
         MVC   ERRCODE(4),=F'8'        SET ERROR RETURN CODE            03280000
         B     START                                                    03290000
ABEND1   DS    0H                                                       03300000
         ABEND 1,DUMP                                                   03310000
ABEND2   DS    0H                                                       03320000
         ABEND 2,DUMP                                                   03330000
ABEND3   DS    0H                                                       03340000
         ABEND 3,DUMP                                                   03350000
ABEND4   DS    0H                                                       03360000
         ABEND 4,DUMP                                                   03370000
ABEND5   DS    0H                                                       03380000
         ABEND 5,DUMP                                                   03390000
```

```
ABEND6   DS    0H                                                      03400000
         ABEND 6,DUMP                                                  03410000
ABEND7   DS    0H                                                      03420000
         ABEND 7,DUMP                                                  03430000
ABEND8   DS    0H                                                      03440000
         ABEND 8,DUMP                                                  03450000
END      DS    0H                                                      03460000
*                                                                      03470000
         L     R15,ERRCODE           SET ANY ERROR CODE                03480000
         L     R13,4(R13)            RESTORE SAVE POINTERS             03490000
         ST    R15,16(R13)                                             03500000
         LM    R14,R12,12(R13)       RESTORE REGISTERS                 03510000
         LA    R0,0                  SET REASON CODE 0                 03520000
         BR    R14                   RETURN TO CALLER                  03530000
         LTORG                                                         03540000
*                                                                      03550000
SAVEAREA DS    18F                                                     03560000
*                                                                      03570000
ERRCODE  DC    F'0'                                                    03580000
ZERO     DC    2D'00'                                                  03590000
DATAXLAT DC    CL8'DATAXLAT'                                           03600000
MAC      DC    CL8'MAC'                                                03610000
MACVER   DC    CL8'MACVER'                                             03620000
EXPTYPE  DC    CL8'EXPORTER'                                           03630000
IMPTYPE  DC    CL8'IMPORTER'                                           03640000
TYPETOKE DC    CL8'TOKEN'                                              03650000
TYPEDATA DC    CL8'DATA'                                               03660000
IPINENC  DC    CL8'IPINENC'                                            03670000
OPINENC  DC    CL8'OPINENC'                                            03680000
PINVER   DC    CL8'PINVER'                                             03690000
PINGEN   DC    CL8'PINGEN'                                             03700000
DISPLAY  DC    CL8'DISPLAY'                                            03710000
KCVPAN01 DC    CL8'KCVPAN01'                                           03720000
KCVPAN02 DC    CL8'KCVPAN02'                                           03730000
BLANK    DC    CL8' '                                                  03740000
ERRMSG   DC    CL8' '                                                  03750000
VDEFINE  DC    CL8'VDEFINE'                                            03760000
VCOPY    DC    CL8'VCOPY'                                              03770000
VGET     DC    CL8'VGET'                                               03780000
ASIS     DC    CL8'ASIS'                                               03790000
VREPLACE DC    CL8'VREPLACE'                                           03800000
VPUT     DC    CL8'VPUT'                                               03810000
CHAR     DC    CL8'CHAR'                                               03820000
SETMSG   DC    CL8'SETMSG'                                             03830000
HEX      DC    CL8'HEX'                                                03840000
MOVE     DC    CL8'MOVE'                                               03850000
CKEYNM   DC    CL8'KEYNM'                                              03860000
CCKKEY   DC    CL8'CKKEY'                                              03870000
CKYTYPE  DC    CL8'KYTYPE'                                             03880000
CKYLEN   DC    CL8'KYLEN'                                              03890000
FORMOP   DC    CL8'OP'                                                 03900000
FORMODD  DC    CL8'ODD'                                                03910000
KEYLENG  DC    CL8' '                                                  03920000
SINGLE   DC    CL8'SINGLE'                                             03930000
DOUBLE   DC    CL8'DOUBLE'                                             03940000
TRIPLE   DC    CL8'TRIPLE'                                             03950000
RAC0     DC    F'0'                                                    03960000
```

ICSF Verify Key Check Value

```
RAC1     DC    F'1'                                                    03970000
IV       DC    D'0'                                                    03980000
RACENC   DC    CL8'CBC'                                                03990000
PAD      DC    XL1'00'                                                 04000000
CV       DC    XL18'00'                                                04010000
WORKECO  DS    XL8                                                     04020000
CVMAC    DC    XL2'0005'                                               04030000
CVMACVER DC    XL3'00054D'                                             04040000
CVXLAT   DC    XL2'0006'                                               04050000
CVIPIN   DC    XL2'0021'                                               04060000
CVOPIN   DC    XL2'0024'                                               04070000
CVPINVER DC    XL3'002242'                                             04080000
CVPINGEN DC    XL3'00227E'                                             04090000
CVEXP    DC    XL2'0041'                                               04100000
CVIMP    DC    XL2'0042'                                               04110000
CVEXPL   DC    XL8'00417D0003410000'   CV EXPORTER LEFT                04120000
CVEXPR   DC    XL8'00417D0003210000'   CV EXPORTER RIGHT               04130000
XBCTABLE DC    CL16'0123456789ABCDEF'                                  04140000
IMPORTKY DC    XL16'01010101010101010101010101010101'                  04150000
         ORG   IMPORTKY                                                04160000
IMPORTL  DS    XL8                                                     04170000
IMPORTR  DS    XL8                                                     04180000
         ORG   ,                                                       04190000
RETCODE  DC    F'0'                                                    04200000
RESCODE  DC    F'0'                                                    04210000
EXITLEN  DC    F'0'                                                    04220000
EXITDATA DC    F'0'                                                    04230000
CHARKCV  DS    XL6                                                     04240000
KCVHEX   DS    XL8                                                     04250000
KEYNM    DC    CL64' '                 KEY LABEL                       04260000
XLATIN   DC    XL64'00'                                                04270000
KEYNMSAV DC    CL64' '                                                 04280000
WORKTOKE DC    XL64'00'                                                04290000
         ORG   WORKTOKE                                                04300000
         DS    CL16                                                    04310000
WORKEYL  DS    CL8                                                     04320000
WORKEYR  DS    CL8                                                     04330000
WORKCVL  DS    CL8                                                     04340000
WORKCVR  DS    CL8                                                     04350000
WORKEY3  DS    CL8                                                     04360000
         DS    CL8                                                     04370000
         ORG   ,                                                       04380000
WORKEXPL DC    XL64'00'                                                04390000
WORKEXPR DC    XL64'00'                                                04400000
EXPORTKY DC    XL16'00'                                                04410000
         ORG   EXPORTKY                                                04420000
EXPLEFT  DS    XL8                                                     04430000
EXPRIGHT DS    XL8                                                     04440000
         ORG   ,                                                       04450000
         DS    0D                                                      04460000
EXTOKEN  DC    XL64'00'                                                04470000
         ORG   EXTOKEN                                                 04480000
EXTYPFLG DS    XL1                                                     04490000
         DS    XL5                                                     04500000
EXFLAG   DS    XL1                                                     04510000
         DS    XL9                                                     04520000
ENCLEFT  DS    XL8                                                     04530000
```

ICSF Verify Key Check Value

```
ENCRIGHT DS    XL8                                                    04540000
CVL      DS    XL8                                                    04550000
CVR      DS    XL8                                                    04560000
         DS    XL12                                                   04570000
TVV      DS    XL4                                                    04580000
         ORG   ,                                                      04590000
WORKIMP  DC    XL64'00'                                               04600000
TARGET   DC    XL64'00'                                               04610000
DATAZERO DC    XL64'00'                                               04620000
CKKEY    DC    CL9'     (  )'          KEY CHECK VALUE NNNN (NN)      04630000
KYTYPE   DC    CL8' '                                                 04640000
LEN3     DC    F'3'                                                   04650000
LEN8     DC    F'8'                                                   04660000
LEN9     DC    F'9'                                                   04670000
LEN60    DC    F'60'                                                  04680000
COPYLEN  DC    F'0'                                                   04690000
         END                                                          04700000
```