21 RACF

August 2000

update

In this issue

© Xephon plc 2000

RACF Update

Published by

Xephon
27-35 London Road
Newbury
Berkshire RG14 1JL
England
Telephone: 01635 38030
From USA: 01144 1635 38030
E-mail: fionah@xephon.com

North American office

Xephon
Post Office Box 350100
Westminster CO 80035-0100
USA
Telephone: (303) 410-9344

RACF Update on-line

You can download code from *RACF Update* from our Web site at http://www.xephon.com/racfupdate.html; you will need the user-id shown on your address label.

Subscriptions and back-issues

A year's subscription to *RACF Update*, comprising four quarterly issues, costs £190.00 in the UK; $290.00 in the USA and Canada; £196.00 in Europe; £202.00 in Australasia and Japan; and £200.50 elsewhere. In all cases the price includes postage. Individual issues, starting with the August 1995 issue, are available separately to subscribers for £50.50 ($77.50) each including postage.

Editor

Fiona Hewitt

Disclaimer

Readers are cautioned that, although the information in this journal is presented in good faith, neither Xephon nor the organizations or individuals that supplied information in this journal give any warranty or make any representations as to the accuracy of the material it contains. Neither Xephon nor the contributing organizations or individuals accept any liability of any kind howsoever arising out of the use of such material. Readers should satisfy themselves as to the correctness and relevance to their circumstances of all advice, information, code, JCL, and other contents of this journal before making any use of it.

Contributions

Articles published in *RACF Update* are paid for at the rate of £170 ($260) per 1000 words and £100 ($160) per 100 lines of code for the first 200 lines of original material. The remaining code is paid for at the rate of £50 ($80) per 100 lines. In addition, there is a flat fee of £30 ($50) per article. To find out more about contributing an article, without any obligation, please contact us at any of the addresses above and we will send you a copy of our *Notes for Contributors*, or you can download a copy from www.xephon.com/contnote.html

© Xephon plc 2000. All rights reserved. None of the text in this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior permission of the copyright owner. Subscribers are free to copy any code reproduced in this publication for use in their own installations, but may not sell such code or incorporate it in any commercial product. No part of this publication may be used for any form of advertising, sales promotion, or publicity without the written permission of the publisher. Copying permits are available from Xephon in the form of pressure-sensitive labels, for application to individual copies. A pack of 240 labels costs $36 (£24), giving a cost per copy of 15 cents (10 pence). To order, contact Xephon at any of the addresses above.

Printed in England.

RACHECK/RACDEF postprocessing exits

If the PROTECTALL option is set in RACF, datasets can be read or written to only if there is a matching RACF profile. The fact that this is also true for tape files can cause problems, particularly if a lot of tapes come from external sources.

The following two RACF exits enable you to prevent PROTECTALL from affecting tapes:

```
RACROUTE REQUEST=AUTH   (RACHECK) Postprocessing Exit  (ICHRCX02)

RACROUTE REQUEST=DEFINE (RACDEF ) Postprocessing Exit  (ICHRDX02)
```

If the following conditions are true

- Class DATASET
- Tape file
- No profile found

the RACHECK/RACDEF return and reason codes are set to values indicating that access is allowed.

NOTES

Reading from and writing to a tape yields a RACROUTE REQUEST=AUTH (RACHECK SVC) call; writing also involves a RACROUTE REQUEST=DEFINE (RACDEF SVC) call, because writing to tape always means the creation of a dataset, even if an identically named dataset is overwritten.

MANUALS

The following manuals are useful:

- *RACF System Programmer's Guide V2R2*, SC23-3725
- *External Security Interfaces (RACROUTE) Macro Reference V2R2*, GC23-3733
- *RACF Data Areas V2R2*, LY27-2636.

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

RACHECK/RACDEF POSTPROCESSING EXIT

```
TITLE 'ICHRCXØ2/ICHRDXØ2 - RACHECK/RACDEF POSTPROCESSING EXIT'
* REGISTER USAGE
*   RØ :
*   R1 : ADDRESS OF PARAMETER LIST
*   R2 : WORK
*   R3 : WORK
*   R4 : WORK
*   R5 :
*   R6 :
*   R7 :
*   R8 :
*   R9 :
*   R1Ø: WORK
*   R11:
*   R12: BASE
*   R13: ADDRESS OF SAVE AREA
*   R14: RETURN ADDRESS; WORK
*   R15: ENTRY ADDRESS; WORK; RETURN CODE
*********************************************************************
* RACROUTE REQUEST=AUTH POSTPROCESSING EXIT
*********************************************************************
         PRINT GEN                 MACRO EXPANSION VISIBLE
         YREGS ,                   REGISTER SYMBOLS
ICHRCXØ2 CSECT ,                   SUPERVISOR, KEY Ø; REUS, RENT, REFR
ICHRCXØ2 RMODE ANY
ICHRCXØ2 AMODE 31
         SAVE  (14,12),,'ICHRCXØ2 &SYSDATC &SYSTIME'
         LR    R12,R15
         USING ICHRCXØ2,R12
                                                              SPACE
         USING RCXPL,R1            ADDRESS PARAMETER LIST
         XR    R15,R15             VALUE Ø
         LA    R14,4               VALUE 4
                                                              SPACE
         L     R2,RCXCOMP          ADDRESS OF ABEND CODE
         CL    R15,Ø(,R2)          PENDING ABEND IN RACHECK ?
         BNE   LCEND                 YES, DO NOTHING
                                                              SPACE
         L     R2,RCXCLASS         ADDRESS OF CLASS
         CLC   KCLASS,Ø(R2)        CLASS DATASET ?
         BNE   LCEND                 NO, DO NOTHING
                                                              SPACE
         L     R2,RCXFLAG3         ADDRESS OF FLAGS
         TM    Ø(R2),RCXDTYPT      DSTYPE=T, IE TAPE FILE ?
         BZ    LCEND                 NO, DO NOTHING
                                                              SPACE
         L     R3,RCXRCODE         ADDRESS OF RACHECK RETURN CODE
         CL    R14,Ø(,R3)          RC = 4, NO PROFILE FOUND ?
```


© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

```
         BNE   LCEND                 NO, DO NOTHING
                                                                SPACE
         ST    R15,Ø(,R3)           RACHECK RET CODE Ø, ACCESS ALLOWED
LCEND    DS    ØH
         RETURN (14,12),,RC=(15)    RETURN WITH RETURN CODE Ø
         DROP  R12,R1
                                                                EJECT
*********************************************************************
* RACROUTE REQUEST=DEFINE POSTPROCESSING EXIT
*********************************************************************
ICHRDXØ2 DS    ØD
         ENTRY ICHRDXØ2             ALIAS
         SAVE  (14,12),,'ICHRDXØ2'
         LR    R12,R15
         USING ICHRDXØ2,R12
                                                                SPACE
         USING RDXPL,R1             ADDRESS PARAMETER LIST
         XR    R15,R15              VALUE Ø
         LA    R14,4                VALUE 4
         LA    R1Ø,8                VALUE 8
                                                                SPACE
         L     R2,RDXCOMP           ADDRESS OF ABEND CODE
         CL    R15,Ø(,R2)           PENDING ABEND IN RACDEF ?
         BNE   LDEND                  YES, DO NOTHING
                                                                SPACE
         L     R2,RDXISSUR          ADDRESS OF FLAG
         TM    Ø(R2),RDXICMND       RACDEF BECAUSE OF RACF COMMAND ?
         BO    LDEND                  YES, DO NOTHING
                                                                SPACE
         L     R2,RDXFLAG           ADDRESS OF FLAGS
         TM    Ø(R2),RDXTYPEV       TYPE=DEFINE (CREATION OF DATASET) ?
         BNZ   LDEND                  NO, DO NOTHING
                                                                SPACE
         L     R2,RDXCLASS          ADDRESS OF CLASS
         CLC   KCLASS,Ø(R2)         CLASS DATASET ?
         BNE   LDEND                  NO, DO NOTHING
                                                                SPACE
         L     R2,RDXFLAG2          ADDRESS OF FLAGS
         TM    Ø(R2),RDXDSTYT       DSTYPE=T, IE TAPE FILE ?
         BZ    LDEND                  NO, DO NOTHING
                                                                SPACE
         L     R3,RDXRCODE          ADDRESS OF RACDEF RETURN CODE
         CL    R1Ø,Ø(,R3)           RC = 8, ERROR ?
         BNE   LDEND                  NO, DO NOTHING
         L     R4,RDXREAS           ADDRESS OF RACDEF REASON CODE
         CL    R14,Ø(,R4)           4, NO PROFIL AND PROTECTALL ?
         BNE   LDEND                  NO, DO NOTHING
                                                                SPACE
         ST    R15,Ø(,R3)           RACDEF RET CODE Ø, ACCESS ALLOWED
         ST    R15,Ø(,R4)           REASON CODE Ø
```

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

```
LDEND    DS    ØH
         RETURN (14,12),,RC=(15)   RETURN WITH RETURN CODE Ø
         DROP  R12,R1
                                                                EJECT
*********************************************************************
* CONSTANTS
*********************************************************************
KCLASSØ  DC    AL1(7),C'DATASET'
KCLASS   EQU   KCLASSØ,*-KCLASSØ
         LTORG ,
         DC    ØD'Ø',32C'Z'        ZAP AREA
                                                                EJECT
*********************************************************************
* DSECTS
*********************************************************************
         PRINT NOGEN
         ICHRCXP ,                 RACHECK SVC EXIT PARAMETER LIST
                                                                EJECT
         ICHRDXP ,                 RACDEF SVC EXIT PARAMETER LIST
                                                                SPACE
         END   ICHRCXØ2
```

Walter Wiedemann
(Germany)

© Reserved 2000

Using REXX for RACF security checking

I have frequently written CLISTs and REXX EXECs that access datasets, volumes, and/or other secured resources to which a particular user might not have access. The security package usually issues a nasty message indicating that access is denied, and may even be configured to suspend the offending userid after a pre-defined number of violations.

When users run CLISTs or EXECs that access these restricted resources, they aren't usually aware of whether or not they have the necessary security level. I thought it would be nice to have a command that could be used to check their access to a resource before they actually attempted to access it. A number of vendor products have such a function built in, including various console automation packages and a few REXX language extension packages. The problem with

 © 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

automation packages, however, is that their security checking functions can be invoked only from within the automation environment. And both they and REXX extensions are expensive. I therefore decided to write a small REXX function to perform security checking using the IBM MVS standard RACROUTE security interface.

The function, RACAUTH, accepts up to three parameters:

- The first (required) parameter is the entity name on which to perform security checking, such as dataset name, volume name, SMS class name, etc.
- The second (optional) parameter is the level of access to check for. The valid levels are READ, UPDATE, CONTROL, or ALTER, with the default being READ.
- The third (optional) parameter is the class to which the entity belongs, with the default being DATASET. For a dataset name, the class would be DATASET; for an SMS storage class, it would be STORCLAS; for an MVS console command, it would be OPERCMDS; and so on. These class names are defined by the security product in use. For RACF, they are in the class descriptor table (CDT). For TopSecret, they are in the resource descriptor table (RDT) record.

RACAUTH sets the REXX RESULT variable to 0 to indicate that the user does not have access to the requested entity, or to 1 to indicate that the user does have access. RACAUTH can be invoked:

- As a REXX function, in which case a user-assigned variable will be given the proper RESULT value, but the RESULT variable itself will not be set.
- Via the REXX CALL statement, in which case RESULT is set appropriately.

The sample REXX EXEC shown below, called RACFTEST, demonstrates the various ways in which the RACAUTH function can be used. It can be invoked via the following commands:

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

```
%RACFTEST SYS1.PARMLIB READ DATASET
%RACFTEST SYS1.PARMLIB READ
%RACFTEST SYS1.PARMLIB
%RACFTEST SYSTEM       READ STORCLAS
```

RACFTEST – SAMPLE REXX EXEC

```
/*********************************REXX*********************************/
parse upper arg ent typ class rest
ent   = strip(ent,"B")
typ   = strip(typ,"B")
class = strip(class,"B")
say '****ent="'ent'"'|| ',typ="'typ'"'||',class="'class'"'

say ' '
call RACAUTH ent,typ,class
say 'call' rc result aa

say ' '
call RACAUTH ent,typ
say 'call' rc result aa

say ' '
aa=RACAUTH(ent,typ,class)
say 'func' rc result aa

say ' '
aa=RACAUTH(ent,typ)
say 'func' rc result aa

say ' '
aa=RACAUTH(ent)
say 'func' rc result aa

say ' '
aa=RACAUTH(ent,'READ','IBMFAC')
say ent typ class "RACAUTH("ent",'READ','IBMFAC')" rc result aa

say ' '
call RACAUTH ent,'READ','IBMFAC'
say ent typ class "call RACAUTH "ent",'READ','IBMFAC'" rc result aa
```

RACAUTH

```
RACAUTH  CSECT                         ESTABLISH CSECT
RACAUTH  AMODE 31
```


© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

```
RACAUTH  RMODE 24
         SAVE  (14,12),,RACAUTH-&SYSDATE
         YREGS                     REGISTER EQUATES
         LR    R12,R15             LOAD R12 W/EPA ADDRESS
         USING RACAUTH,R12         ESTABLISH ADDRESSABLITY
         LA    R15,SAVEAREA        LOAD A(MY SAVEAREA)
         ST    R15,8(,R13)         ST MY S/A ADDR IN CALLERS S/A
         ST    R13,4(,R15)         ST MY S/A ADDR IN CALLERS S/A
         LR    R13,R15             LOAD ADDR OF MY S/A IN R13
         ST    R1,EFPLADDR         SAVE A(EFPL)
         L     R1Ø,EFPLADDR        LOAD FOR LATER
         L     R1,EFPLARG-EFPL(,R1) LOAD A(EFPLARG)
         USING ARGTABLE_ENTRY,R1
         ST    R1,EFPLARGA         SAVE A(EFPLARG)
         SR    R15,R15             CLEAR R15 FOR COUNTER
ARGLOOP  DS    ØH
         CLC   ARGTABLE_ARGSTRING_PTR(L'ARGTABLE_END),ARGTABLE_END
         BE    ENDARGS             YES, R15 HAS # OF ARGS
         LA    R15,1(,R15)         ADD 1 TO ARG COUNTER
         LA    R1,L'ARGTABLE_NEXT(,R1) BUMP TO NEXT ENTRY
         B     ARGLOOP             LOOP TO SEE IF THERE ARE MORE ARGS
         DROP  R1
ENDARGS  DS    ØH
         L     R1,EFPLARGA         RESTORE A(EFPLARG)
         C     R15,=F'1'           IS THERE AT LEAST 1 ARG
         BL    ARGSERR             NO, THEN ERROR
         C     R15,=F'3'           ARE THERE MORE THAN 3 ARGS
         BH    ARGSERR             NO, THEN ERROR
         B     PARSARGS            ELSE, CHECK ARGS
ARGSERR  DS    ØH
         LA    RØ,MSG1             LOAD A(MESSAGE)
         ST    RØ,BUFRPTR          SAVE IN PLIST
         LA    RØ,L'MSG1           LOAD LENGTH(MESSAGE)
         ST    RØ,BUFRLEN          SAVE IN PLIST
         LA    R1,IRXSAYPL         LOAD A(PLIST)
         LINK  EP=IRXSAY           CALL SAY ROUTINE
         LA    RØ,2Ø               SET RETURN CODE
         STH   RØ,SAVERC           SAVE RETURN CODE
         B     RETURN              GO RETURN TO CALLER
PARSARGS DS    ØH
         STH   R15,NUMARGS         SAVE NUMBER OF ARGUMENTS
         L     R11,EFPLARGA        A(EFPLARGS)
         USING ARGTABLE_ENTRY,R11
         SR    R1,R1               CLEAR REGISTER
         SR    R14,R14             CLEAR REGISTER
         SR    R15,R15             CLEAR REGISTER
         CLC   =H'1',NUMARGS       ARE THERE NO ARGS
         BH    ARG1ERR             YES
```

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

```
         L     R14,ARGTABLE_ARGSTRING_LENGTH
         C     R14,=F'1'           IS LENGTH(ARG1) LESS THAN 1
         BL    ARG1ERR             YES
         C     R14,=F'44'          IS LENGTH(ARG1) MORE THAN 44
         BH    ARG1ERR             YES
         B     CHKARG2             ELSE
ARG1ERR  DS    ØH
         LA    RØ,MSG2             LOAD A(MESSAGE)
         ST    RØ,BUFRPTR          SAVE IN PLIST
         LA    RØ,L'MSG2           LOAD LENGTH(MESSAGE)
         ST    RØ,BUFRLEN          SAVE IN PLIST
         LA    R1,IRXSAYPL         LOAD A(PLIST)
         LINK  EP=IRXSAY           CALL SAY ROUTINE
         LA    RØ,2Ø               SET RETURN CODE
         STH   RØ,SAVERC           SAVE RETURN CODE
         B     RETURN              GO RETURN TO CALLER
CHKARG2  DS    ØH
         L     R2,ARGTABLE_ARGSTRING_PTR LOAD A(ARG1)
         L     R3,ARGTABLE_ARGSTRING_LENGTH LOAD LENGTH(ARG1)
         BCTR  R3,RØ               DECREMENT FOR EXECUTE
         EX    R3,EXMVCENT         EXECUTE MVC OF ARG1 TO ENTYNAME
         SR    R5,R5               CLEAR R5 FOR IC
         LA    R7,ATTRTABL         LOAD A(ATTR TRANSLATE TABLE)
         USING ATTRDSCT,R7
         IC    R5,ATTRHEX          SET DEFAULT ATTR OF READ (1ST ENTRY)
         CLC   =H'2',NUMARGS       ARE THERE LESS THAN 2 ARGS
         BH    CHKARG3             YES, GO CHECK ARG3
         CLC   ARGTABLE_ARGSTRING_LENGTH+L'ARGTABLE_NEXT(4),=F'Ø'
         CLC   ARGTABLE_ARGSTRING_LENGTH+8(4),=F'Ø' LEN(ARG2)=Ø?
         BE    CHKARG3             YES, WILL USE DEFAULT ATTR OF READ
ATTRLOOP DS    ØH
         CLC   ATTRTBND(TABENTLN),ATTRLEN ARE WE AT END OF TABLE
         BE    ARG2ERR             YES, ARG2 IN ERROR
         SR    R15,R15             CLEAR R15 FOR IC
         IC    R15,ATTRLEN         ELSE GET LENGTH OF EBCDIC ENTRY
         L     R1Ø,ARGTABLE_ARGSTRING_PTR+L'ARGTABLE_NEXT A(ARG3)
         L     R9,ARGTABLE_ARGSTRING_LENGTH+L'ARGTABLE_NEXT LEN(ARG3)
         CR    R9,R15              ARE LENGTHS EQUAL
         BNE   ATTRBUMP            NO, BUMP TO NEXT TABLE ENTRY
         BCTR  R15,RØ              DECREMENT R15 FOR EXECUTE
         EX    R15,EXCHKATR        EXECUTE CLC OF ARG3 TO TABLE ENTRY
         BE    GETATTR             IF MATCH, GET ATTR BYTE
ATTRBUMP DS    ØH
         LA    R7,ATTRTABL+TABENTLN ELSE BUMP TO NEXT TABLE ENTRY
         B     ATTRLOOP            LOOP TO CHECK NEXT TABLE ENTRY
GETATTR  DS    ØH
         SR    R5,R5               CLEAR REGISTER
         IC    R5,ATTRHEX          INSERT ATTR VALUE
         B     CHKARG3             GO CHECK ARG3
```


© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

```
ARG2ERR  DS    ØH
         LA    RØ,MSG3             LOAD A(MESSAGE)
         ST    RØ,BUFRPTR          SAVE IN PLIST
         LA    RØ,L'MSG3           LOAD LENGTH(MESSAGE)
         ST    RØ,BUFRLEN          SAVE IN PLIST
         LA    R1,IRXSAYPL         LOAD A(PLIST)
         LINK  EP=IRXSAY           CALL SAY ROUTINE
         LA    RØ,2Ø               SET RETURN CODE
         STH   RØ,SAVERC           SAVE RETURN CODE
         B     RETURN              GO RETURN TO CALLER
CHKARG3  DS    ØH
         SR    R1,R1               CLEAR REGISTER
         SR    R14,R14             CLEAR REGISTER
         SR    R15,R15             SET DEFAULT RETURN CODE
         CLC   =H'3',NUMARGS       ARE THERE LESS THAN 3 ARGS
         BH    DFLTCLAS            YES, GO USE DEFAULT CLASS
         CLC   ARGTABLE_ARGSTRING_LENGTH+L'ARGTABLE_NEXT*2,=F'Ø'
         BE    DFLTCLAS            YES
         L     R14,ARGTABLE_ARGSTRING_LENGTH+L'ARGTABLE_NEXT*2
         C     R14,=F'1'           IS LENGTH(ARG3) LESS THAN 1
         BL    ARG3ERR             YES
         C     R14,=F'8'           IS LENGTH(ARG3) MORE THAN 8
         BH    ARG3ERR             YES
         B     DFLTCLAS            ELSE
ARG3ERR  DS    ØH
         LA    RØ,MSG4             LOAD A(MESSAGE)
         ST    RØ,BUFRPTR          SAVE IN PLIST
         LA    RØ,L'MSG4           LOAD LENGTH(MESSAGE)
         ST    RØ,BUFRLEN          SAVE IN PLIST
         LA    R1,IRXSAYPL         LOAD A(PLIST)
         LINK  EP=IRXSAY           CALL SAY ROUTINE
         LA    RØ,2Ø               SET RETURN CODE
         STH   RØ,SAVERC           SAVE RETURN CODE
         B     RETURN              GO RETURN TO CALLER
DFLTCLAS DS    ØH
         LTR   R14,R14             IS THERE AN ARG2
         BNZ   SETCLAS             YES
         MVC   CLASSNAM,DATASET    ELSE ASSUME ARG2=DATASET
         MVI   CLASSLEN,7          SET CLASSNAM LENGTH
         B     SETREGS             GO CHECK AUTH
         B     CHEKAUTH            GO CHECK AUTH
SETCLAS  DS    ØH
         L     R2,ARGTABLE_ARGSTRING_PTR+16 LOAD A(ARG3)
         L     R3,ARGTABLE_ARGSTRING_LENGTH+16 LOAD LENGTH(ARG3)
         STCM  R3,1,CLASSLEN       SET CLASSNAM LENGTH
         BCTR  R3,RØ               DECREMENT FOR EXECUTE
         EX    R3,EXMVCCL          EXECUTE MVC OF ARG3 TO CLASSNAM
SETREGS  DS    ØH
         LA    R3,RACFWKA          LOAD A(RACF WORKAREA) FOR RACROUTE
```

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

```
         LA    R4,ENTYNAME        LOAD A(ENTITY NAME) FOR RACROUTE
         LA    R6,CLASSLEN        LOAD A(LEN,CLASS NAME) FOR RACROUTE
CHEKAUTH DS    ØH
         RACROUTE REQUEST=AUTH,WORKA=(R3),ATTR=(R5),                   X
               ENTITY=((R4)),CLASS=(R6),RACFIND=YES
         LTR   R15,R15            CHECK RETURN CODE
         BZ    AUTHOK             WAS RETURN CODE = Ø
         MVI   RESULT,C'Ø'        NO, SET RESULT
         B     SETRESLT           GO STORE RESULT
AUTHOK   DS    ØH
         MVI   RESULT,C'1'        SET RESULT
         B     SETRESLT           GO STORE RESULT
         MVI   RESULT,C'1'        ASSUME SUCCESS
         LTR   R15,R15            WAS IT
         BZ    SETRESLT           YES
         MVI   RESULT,C'Ø'        ELSE SET FAILURE
SETRESLT DS    ØH
         L     R14,EFPLADDR       LOAD A(EFPL)
         L     R14,EFPLEVAL-EFPL(,R14) LOAD A(A(EVALBLOCK))
         L     R14,Ø(,R14)        LOAD A(EVALBLOCK)
         USING EVALBLOCK,R14
         LA    R15,L'RESULT       GET LENGTH OF RESULT
         ST    R15,EVALBLOCK_EVLEN STORE LENGTH
         EX    R15,EXMVC          EXECUTE MVC OF RESULT
RETURN   DS    ØH
         LH    R15,SAVERC         LOAD RETURN CODE
         L     R13,SAVEAREA+4     LOAD R13 W/ADDR OF CALLERS S/A
         RETURN (14,12),RC=(15)   RETURN TO OS WITH RETCODE IN R15
SAVEAREA DS    18F                SHOULD BE FIRST IN WORKAREA
EFPLADDR DC    A(Ø)               A(EFPL)
EFPLARGA DC    A(Ø)               A(EFPLARG)
BUFRPTR  DC    A(Ø)               A(INPUT BUFFER)
BUFRLEN  DC    A(Ø)               LENGTH(INPUT BUFFER)
IRXSAYPL DC    A(WRITEERR)        A(FUNCTION)
         DC    A(BUFRPTR)         A(A(INPUT BUFFER))
         DC    A(BUFRLEN+X'8ØØØØØØØ') A(LENGTH(INPUT BUFFER))
NUMARGS  DC    H'Ø'               TOTAL NUMBER OF ARGUMENTS
SAVERC   DC    H'Ø'               SAVE AREA FOR RETURN CODE
RACFWKA  DC    512X'4Ø'           RACROUTE WORK AREA
ENTYNAME DC    CL256' '           ENTITY NAME
CLASSLEN DC    AL1(L'CLASSNAM) ----------| CLASSNAME LENGTH
CLASSNAM DC    CL8' ' -------------------| CLASSNAME
EXMVCENT MVC   ENTYNAME(Ø),Ø(R2)  EXECUTED MVC OF ARG1 TO ENTYNAME
EXMVCCL  MVC   CLASSNAM(Ø),Ø(R2)  EXECUTED MVC OF ARG3 TO CLASSNAM
EXCHKATR CLC   ATTRVAL(Ø),Ø(R1Ø)  EXECUTED CLC OF ARG3 TO TABLE ENTRY
EXMVC    MVC   EVALBLOCK_EVDATA(Ø),RESULT EXECUTED MVC OF RESULT
RESULT   DC    C' '               REXX RC
MSG1     DC    C'Minimum of 1 argument/maximum of 3 arguments needed.'
```


© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

```
MSG2     DC    C'Argument1 (entity) must be between 1-44 bytes long. '
MSG3     DC    C'Argument2 (auth) must be READ/UPDATE/CONTROL/ALTER. '
MSG4     DC    C'Argument3 (class) must be between 1-8 bytes long.   '
DATASET  DC    CL8'DATASET '      FOR DATASET CLASS CHECKING
ATTRTABL DS    ØF                 ATTRIBUTE TABLE---------------|
ATTRDFLT DC    AL1(4),CL8'READ    ',X'Ø2' DEFAULT ATTR          |
         DC    AL1(6),CL8'UPDATE  ',X'Ø4'                       |
         DC    AL1(7),CL8'CONTROL ',X'Ø8'                       |
         DC    AL1(5),CL8'ALTER   ',X'8Ø'                       |
ATTRTBND DC    X'FF',8X'FF',X'FF' END OF TABLE INDICATOR        |
TABENTLN EQU   *-ATTRTBND         LENGTH OF A TABLE ENTRY-------|
WRITEERR DC    C'WRITEERR'        IRXSAY FUNCTION
         LTORG
         IRXARGTB DECLARE=YES     MAPS REXX ARGUMENT TABLE
ATTRDSCT DSECT                    ATTRTABL MAPPING
ATTRLEN  DS    AL1                LENGTH OF EBCDIC ATTR
ATTRVAL  DS    CL8                EBCDIC ATTR VALUE
ATTRHEX  DS    X                  HEX EQUIVALENT OF EBCDIC ATTR
         PRINT NOGEN
         IRXEFPL                  MAPS REXX EXTERNAL FUNT PARM LIST
         IRXEVALB                 MAPS REXX EVALUATION BLOCK
         END
```

Systems programmer
(USA)

© Xephon 2000

Code from *RACF Update* articles

As a free service to subscribers and to remove the need to rekey the scripts, code from individual articles of *RACF Update* can be accessed on our Web site, at

http://www.xephon.com/racfupdate.html

You will need the user-id shown on your address label.

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

RACF internals

This article offers general background information on the structure and facilities available in RACF, from the perspective of an MVS systems programmer. It covers the following topics:

- RACF database structure
- Resident data blocks
- RACF buffer synchronization
- Grouping profiles
- RACROUTE REQUEST=LIST processing
- Sysplex communication
- Sysplex data sharing
- RACGLIST class
- Recent RACF enhancements.

THE RACF DATABASE STRUCTURE

The RACF database is formatted into 4096 byte blocks. The first block in the database is the Inventory Control Block (ICB), and provides the beginning pointers for all other block types. The ICB also contains:

- RBA of the highest level index block
- Number of BAM blocks in the RACF dataset
- BAM high water mark
- The RBA of the first block of the INDEX sequence set
- Change count arrays
- SETROPTS options
- Audit options
- CLASS masks.

© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

There is also an in-storage copy of the ICB located in ESCA storage subpool 231 key 0, pointed to by field DSDEHRD in the DSDT data area.

The first byte of each block in the RACF database contains a block identifier as follows:

- X'00' – BAM
- X'02' – segment table
- X'83' – data block
- X'8A' – index block
- X'C3' – empty block.

Logical view of the RACF database

The logical view of the RACF database is very similar to a VSAM KSDS in that there is always a level 1 (L1) or sequence set in the index structure, and, depending on the number of profiles, there may be two (L2), three (L3), or more levels of index above the sequence set (there can be up to ten levels on a RACF database). The sequence set or level 1 index entries contain the RBAs of the actual security profiles. IBM has used index-entry compression to save space on the RACF database. The types of compression are:

- Front-end compression
- Upper-level compression.

The forward and backward pointers between the higher level and lower index blocks allow RACF to find the next block in sequence. All of the pointers are given by relative byte address (RBA) from byte zero of the ICB. If the required information is not in-storage, each profile access will require an access to the ICB information and the information within one block at each level of the index structure, plus an access to the data block desired. Each index block contains a 14-byte header followed by the index entries.

The structure of the index block header is shown in Figure 1.

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

Byte position	Description
1	The index block identifier (X'8A')
2-3	The length of the index block (X'1000')
4	An index block identifier (X'4E')
5	Format identifier (X'00')
6	The index level number
7-8	The offset to the last entry in the index block
9-10	The offset to free space in the index block
11-12	The offset to a table of index-entry offsets
13-14	A count of entries in the table of index-entry offsets

Figure 1: Index block header structure

At the logical end of each block, there is a one-byte end-of-block delimiter, which is set to X'0C'. The end of the index entries is identified by a level-1 block consisting of 255 bytes of X'FF'.

IBM provides a utility program called BLKUPD which can be used to examine or modify any BAM, index, or data block on a RACF database. It's an extremely powerful utility, and should be used only when directed by the IBM support centre. For a systems programmer or RACF administrator to run the BLKUPD utility, at least UPDATE authority is required to the RACF database.

Figure 2 shows the logical view of the RACF database.

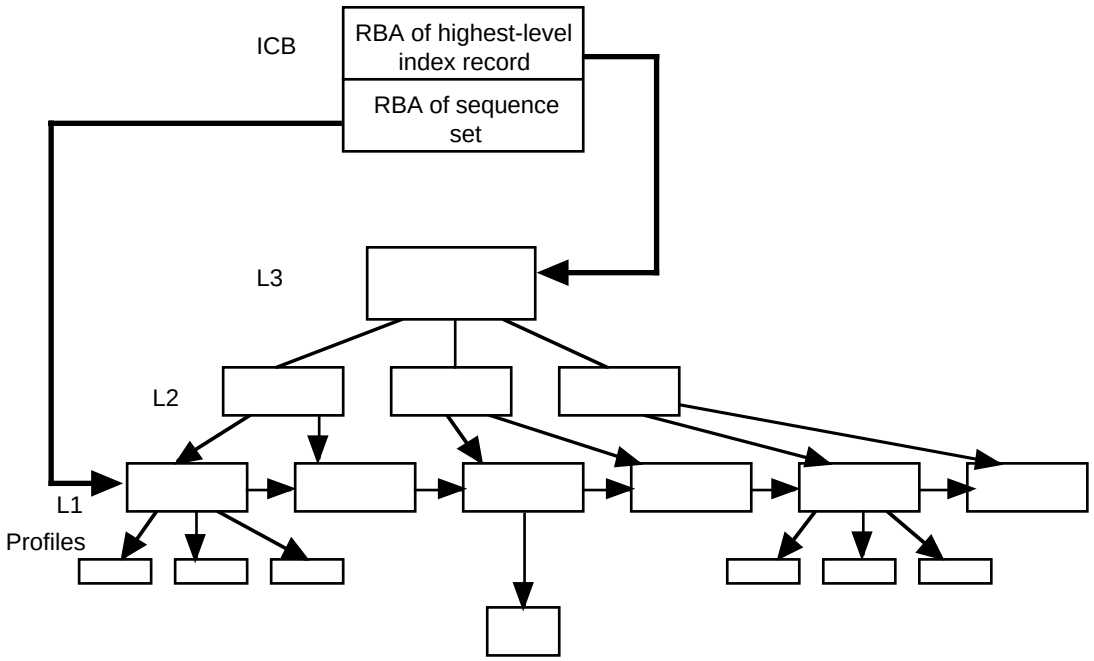

Figure 2: RACF logical dataset structure

© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

Template blocks

The blocks that follow the ICB will contain templates. These are maps of how profiles are structured, and normally vary between different releases of RACF. The number of template blocks will vary between different release levels of RACF because of reserved fields being used for new functions. RACF provides a template for each type of profile (user, group, dataset, and general resource). Internally, the template maps the fields that are contained in each segment of the profile by describing the field name and length.

Segment table block

The segment table block physically follows the template blocks. This block contains mappings of individual profile segments from within templates.

Block Availability Map

The block availability map (BAM), which physically follows the segment table block, contains bit structures representing parts of blocks in the RACF database and are on or off depending on whether the block contains information or is free (if a bit is set to 1, the corresponding slot is free). Each 4096 byte data block is broken down into sixteen parts, each 256 bytes long. One BAM bit represents one of the 256 byte parts. It takes two bytes to map a 4096 byte block. Each BAM block contains header information followed by the block masks. The header contains the information shown in Figure 3.

A maximum of 2038 blocks ((4096-20)/2), each of length 4096, can be defined by one BAM block.

Contained within the ICB is the BAM high-water mark. This field

Byte position	Description
1-6	The RBA of the previous BAM block (or 0 if this is the first block)
7-12	The RBA of the next BAM block (or 0 if this is the last block)
13-18	The RBA of the first block whose space this BAM block defines.
19-20	The number of blocks whose space this BAM block defines.

Figure 3: Header information

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

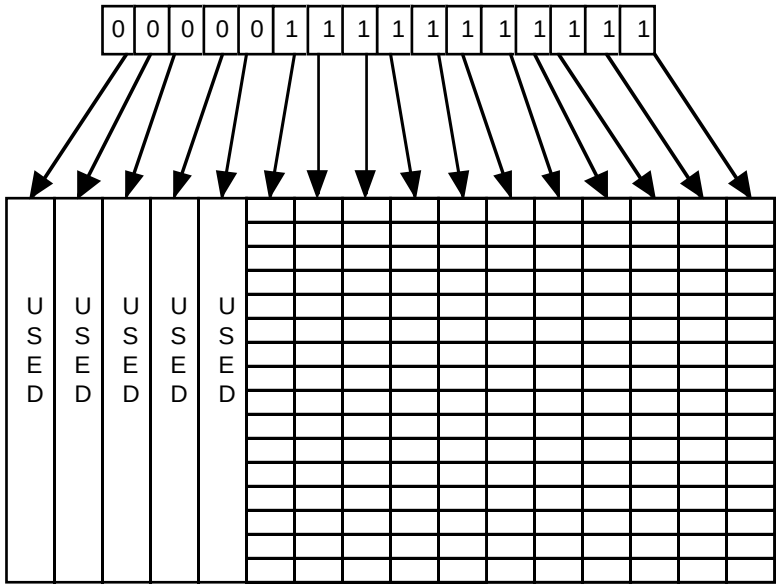

Figure 4: BAM blocks

contains the address of the BAM block that was last used to allocate or de-allocate space within the RACF database. When space is required in the RACF database for a new profile, the BAM high-water mark is used as the starting position. For instance, in Figure 4 the first five slots are in use and the next eleven are available for allocation.

Security profiles

The security profiles are made up of:

- USER profiles
- GROUP profiles
- Dataset profiles
- RESOURCE profiles.

A profile can be made up of a number of segments. Segments that make up a profile are stored as individual elements and are not necessarily stored in contiguous positions in the RACF database. The

© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

Field	Description
Record identifier	A one-byte field containing the identifier X'83'
Logical record length	A four-byte field containing the length of the actual data portion contained in the physical record
Physical record length	A four-byte field containing the physical record length
Segment name	An eight-byte field containing the name of the segment
Key length	A two-byte field containing the length of the profile name
Reserved	A one-byte reserved field
Record key	The profile name
Data fields	One or more segment data fields

Figure 5: Record header fields

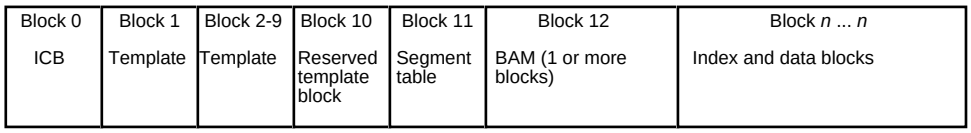

Figure 6: The physical RACF database view

level-one index entry for a profile has a count of and pointers to all segments that make up a profile. For example, the user profile has a base segment and may also have a TSO segment, an OMVS segment, a DFP segment, an OPERPARM segment, a CICS segment, a NetView segment, or a WORKATTR segment.

The RACF database profiles consist of a header record followed by segments that are made up of fields and repeat groups. The record header is made up of the fields shown in Figure 5.

Physical view of the RACF database

The RACF database may be made up of multiple datasets, and each may have a mirror copy called a duplex. The number of RACF datasets is controlled by creating a RACF dataset name table and placing it as member ICHRDSNT in a link list library. The systems programmer can also use the Database Range Table (ICHRRNG) to determine the RACF database on which to place each security profile. The Database Range Table must reside in an LPA or MLPA library.

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

From the physical viewpoint, an index or data record/block can be located anywhere in the RACF database.

The structure of the RACF physical database is shown in Figure 6.

RESIDENT DATA BLOCKS

RACF provides an option to keep the active portions of the RACF database in storage. This is accomplished by specifying the number of resident data blocks for each primary RACF database in the RACF Database Name Table (ICHRDSNT). During the IPL procedure, RACF obtains the storage for the specified number of buffers from the extended common storage area (ECSA). It is recommended that this value be set to 255 (the maximum that can be specified) as RACF will work most efficiently when the maximum number is given to it.

The following RACF data blocks can be kept in the resident data blocks:

- RACF profiles
- Block availability blocks
- Database index blocks

Depending on whether the RACF database environment is shared or non-shared, RACF will use a different technique to synchronize the various RACF local buffers, as described below.

Shared RACF database

When resident data blocks are used for a shared RACF database, synchronization for local buffers in all systems sharing the RACF database is performed by using change count arrays in the inventory control block (ICB). The change count in the ICB, corresponding to the block type (profile or index), is updated whenever a block is updated. Index block buffers and profile buffers are marked out-of-date if the change count in the ICB differs from the change count in the in-storage buffer. Before the resident data blocks are searched, the ICB must be read and the change count arrays compared. If a count differs, all blocks for one level or all data blocks are invalidated.

© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

When a profile or index block needs to be read by a sharing CPU, RACF will see whether the ICB has been refreshed in storage within the last two seconds. If it has, the in-storage copy will be used; otherwise, the DASD copy of the ICB will be brought into storage before it accesses other information. If RACF is performing I/O to the RACF database (writing a profile or index block), the ICB is always refreshed.

If all the space has been used and a profile is needed which is not in storage, a Least Recently Used (LRU) algorithm will be used to identify which block to purge in order to provide the needed space.

Non-shared RACF database

For a non-shared RACF database, RACF will first search the resident data blocks to find a copy of the needed block. If this block is not found in the resident data blocks, RACF will obtain an in-storage buffer from the pool of buffers from within the resident data blocks, read the data block from the RACF database into that buffer, and retain the data block in storage for future references. When updating a profile, RACF searches the in-storage buffers for a copy of the block that contains the profile. If it doesn't find one, it obtains an in-storage buffer from the pool of buffers. When a block is updated , RACF always performs an I/O operation to store the new data block on the RACF database to ensure that the database has an up-to-date version of the block. When getting a buffer from the pool, RACF attempts to get a buffer that is empty. If it can't find an empty buffer, RACF takes the buffer containing the least-recently-used block.

GROUPING PROFILES

A facility in RACF permits the association of a name with a single profile through the use of a resource name group facility. This is referred to in RACF terminology as a grouping class. The resource managers of CICS and IMS use this facility through

```
RACROUTE REQUEST=LIST
```

and

```
RACROUTE REQUEST=FASTAUTH
```

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

In CICS, the default grouping class is GCICSTRN. RACF grouping classes are associated with a member class which could have a single RACF profile per transaction. The default member class for transaction names in CICS is TCICSTRN.

In MVS environments, CICS uses RACF's fast authorization checking mechanism to minimize I/Os during transaction processing. To use the fast authorization check (RACROUTE REQUEST=FASTAUTH), CICS will build transaction profiles in storage at initialization time by using the RACROUTE REQUEST=LIST macro (RACLIST). The space needed for the RACLISTed profiles can be minimized by grouping transactions which have like security requirements under a unique name in the appropriate grouped class.

In RACF, the systems programmer maintains a table called the Class Descriptor Table (CDT). This table describes how resources in the class are to be named, and how they are to be administered. It also allows resources with the same name to be distinguished from each other. For each class defined in the CDT, the following information can be specified:

- Name of the resource class
- Default return code when no profile exists for the resource that is being accessed
- GENLIST option
- Grouping class name
- Member class name
- POSIT number
- RACLIST option
- Default UACC
- Class name format.

As can be seen from the previous information, the CDT also specifies when grouping of profiles is to be used, and which class is the grouping class and which the member class. The definitions for the

 © 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

Class Name	Parameters
GCICSTRN	POSIT=5 OTHER=ANY MAXLNTH=13 DFTUACC=NONE **MEMBER=TCICSTRN** OPER=NO FIRST=ANY ID=13
TCICSTRN	POSIT=5 OTHER=ANY MAXLNTH=13 DFTUACC=NONE **GROUP=GCICSTRN** OPER=NO FIRST=ANY ID=12

In the entity or member class, the profile name is the name of the resource against which the authorization request will be made. In the corresponding grouping class the profile name has no application significance. It is merely chosen as a convenient name to refer to the group of resource names that are added as "members". These member names are the resource names against which requests will be made. Generic names can be defined as the profile name in the entity or member class or as member names in any of the grouping class profiles. Generic profiles cannot be used with the resource name grouping facility.

Figure 7: Definitions for GCICSTRN and TCICSTRN classes

GCICSTRN and TCICSTRN classes are as shown in Figure 7 (CDT entry for grouping class will be paired with member class entry).

During CICS initialization, the CICS Resource Manager requests the service of RACLIST by invoking the RACROUTE REQUEST=LIST macro. RACLIST determines that the TCICSTRN class is grouped by the GCICSTRN class by looking at the CDT and reads the GCICSTRN records first. RACLIST will build the in-storage profiles in two pools. The two pools are pointed to by an anchor element. The anchor element varies in size depending on whether generic or non-generic profiles are defined. The first pool contains fixed information such as UACC and AUDIT flags. It also contains the access list, either USERID or GROUP names. The second pool contains the index. Every entry in the member list will have an entry in the index. The index is built from the following sources:

- The transaction named by the ADDMEM keyword of the GCICSTRN definition.

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

- The transaction named in the definition in the TCICSTRN class.

The index entries contain fields that are used to provide the binary search capability of RACF FRACHECK in response to a RACROUTE REQUEST=FASTAUTH. When the GCICSTRN records have been exhausted, RACLIST starts processing the records from the TCICSTRN class.

The following examples show CICS transaction security definitions. The examples use grouping profiles, generic profiles, and discrete profiles:

```
RDEFINE  GCICSTRN  TG1 UACC(NONE)
                   ADDMEM(TRN1,TRN2,TRN3,TRN4,TRN5)

PERMIT   TG1  CLASS(GCICSTRN)  ID(U1,U2,U3,U4,U5) ACCESS(READ)

RDEFINE  GCICSTRN  TG2 UACC(NONE)
                   ADDMEM(TRN6,TRN7,TRN8,TRN9,TRNA)

PERMIT   TG2  CLASS(GCICSTRN)  ID(U6,U7,U8,U9) ACCESS(READ)

RDEFINE  TCICSTRN  T*  UACC(NONE)

PERMIT   T* CLASS(TCICSTRN)  ID(U1Ø,U11,U12,U13,U14,U15,U16)
ACCESS(READ)

RDEFINE TCICSTRN TRNZ UACC(NONE)

PERMIT   TRNZ  CLASS(TCICSTRN)  ID(UQ,UY,UZ) ACCESS(READ)
```

It is never necessary to define the name of any resource for which RACF control is desired in more than one RACF profile, but there is nothing preventing you from doing so. In general, all of the CICS or IMS resources that you wish to control can be defined, via the ADDMEM parameter, as members of profiles defined within the grouping class used for each CICS or IMS resource type. It is not necessary (and is in fact undesirable because of the additional processing required during RACLIST processing) to define these same CICS or IMS resource names individually as profiles in the member class. Whenever a single resource name appears in more than one profile, RACF is forced to merge these multiple profiles during RACLIST processing to provide the correct response for any authorization request that may be issued for any such resource name. The net effect of the profile merge processing is to construct a profile in memory such that the response to any particular resource name

 © 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

would be the same as processing each profile within which the resource name appears, allowing the least restrictive access defined for any of the profiles.

A resource manager that uses grouping profiles would probably issue the following RACF macro services:

- During initialization:

```
RACROUTE REQUEST=LIST,CLASS=class_name,ENVIR=CREATE, ....
```

- For each authorization request:

```
RACROUTE REQUEST=FASTAUTH,CLASS=class_name,ACEE=acee_addr, ....
```

- To REFRESH in-storage profiles:

```
RACROUTE REQUEST=LIST,CLASS=class_name,ENVIR=DELETE, ....

RACROUTE REQUEST=LIST,CLASS=class_name,ENVIR=CREATE, ....
```

Recent enhancements to RACROUTE REQUEST=LIST have provided the option of specifying GLOBAL=YES on the request. When this option is specified, the results of the REQUEST=LIST are stored in a dataspace which can shared by other applications that issue the same request. The main benefit of this new option is that the RACF administrator can issue a

```
SETROPTS RACLIST(classname) REFRESH
```

which deletes the existing dataspace and loads the discrete and generic profiles into a new dataspace, and that all applications that have issued

```
REQUEST=LIST,GLOBAL=YES
```

for the same class will therefore be automatically connected to the new dataspace. This saves applications from having to issue the

```
RACROUTE REQUEST=LIST,CLASS=class_name,ENVIR=DELETE
```

followed by a

```
RACROUTE REQUEST=LIST,CLASS=class_name,ENVIR=CREATE
```

to refresh the in-storage profiles. In the case of CICS, the CICS administrator does not have to issue the CEMT PERFORM SECURITY REBULID command.

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

GLOBAL ACCESS TABLE

An important tuning option in RACF is the global access table. This table allows an installation to define a set of named resources and a level of access at which anyone may access them. A global table may be created for any resource class.

The global access table is built at IPL time or when a refresh is performed by a security administrator, and is maintained in central storage. Once built, there is no I/O performed for security checking if there is an entry in the table which grants access to the resources being checked. The global access table entries will be used for regular authorization checking, such as OPEN, unless the class of resources has had all of its profiles built in shared storage, using SETROPTS RACLIST.

The global access table is not used for fast authorization checking (RACROUTE REQUEST=FASTAUTH). For example, CICS uses FASTAUTH checking for transaction authorization for the TCICSTRN class.

To add a resource class to the global access table, use the RDEFINE GLOBAL class_name command. To allow global access checking for a specific resource, use the RALTER GLOBAL class_name ADDMEM command. To delete an entry from the global access table, use the RALTER GLOBAL class_name DELMEM command. To list the global access table, issue the RLIST GLOBAL class_name command (see Figure 8).

Note the following conditions for global access checking:

RDEFINE GLOBAL DATASET	Add a resource class to the global access table
RALTER GLOBAL DATASET ADDMEM('SYS1.HELP'/READ)	Allow global access checking for a specific resource
SETROPTS GLOBAL (DATASET) REFRESH	Rebuild the global access table
RLIST GLOBAL class_name	List entries in a particular class
SETROPTS GLOBAL(DATASET)	Activate global access checking for a class
SETROPTS NOGLOBAL(class_name)	Stop global access checking for a specific class

Figure 8: Global access table

© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

```
Enhanced Generic Names is in effect.
      &RACGPID.**/READ
      &RACUID.**/ALTER
      CATALOG.MASTER.**/READ
      ISF.**/READ
      ISP.**/READ
      SYS1.BRODCAST/UPDATE
      SYS1.RACF*/NONE
      SYS1.LPALIB/NONE
      SYS1.PARMLIB/NONE
      SYS1.**/READ

      &RACGPID  Represents the group that a user has signed on with at the time that
                the resource access check is being made.
      &RACUID   Represents the userid that the user has signed on with at the time of
                the authorization check.
      NONE      None implies that the given name is not to be included in the broader
                security definition further down the list.
```

Figure 9: Example global access table

- Global access checking is used for authorization processing invoked by the RACROUTE REQUEST=AUTH macro. It is not used for authorization processing invoked by the RACROUTE REQUEST=FASTAUTH macro.
- When access is granted through the global access table, no logging to SMF will occur at authorization checking time.
- When access is granted through the global access table, RACF maintains no statistics.
- RACF bypasses global access checking if the PROFILE, CSA, or PRIVATE operand is specified on the RACROUTE REQUEST=AUTH request.
- Fully qualified names of resources as well as generic names may be placed in the global access table.

Figure 9 illustrates what a global access table might look like when displayed in response to a RLIST GLOBAL DATASET. The display is in the sequence that RACF will build the table in storage.

SYSPLEX COMMUNICATION

When RACF is enabled for RACF communication, it uses the cross-

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

system coupling facility (XCF) to join the RACF data sharing group, IRRXCF00. There is only one data sharing group per system. RACF sysplex communication can be enabled only by modifying the flag byte (Bit 4 - Enable RACF Sysplex communication) of the first entry in the RACF database name table (ICHRDSNT). Activating this modification requires an IPL of the systems.

An essential requirement is that the RACF database name table and the class descriptor table (ICHRRCDE) must be compatible on all systems, and the database range table (ICHRRNG) must be the same on all systems.

Once RACF sysplex communication has been activated, RACF can be in one of the following modes:

- Non-data sharing
- Data sharing
- Read-only.

When RACF is enabled for sysplex communication, it propagates SETROPTS RACLIST Class_name or SETROPTS RACLIST Class_name REFRESH commands issued from any one system to the other systems in the data sharing group, if the command is successful on the system on which it was entered. The full list of commands that are propagated through the sysplex are as follows:

- RVARY SWITCH
- RVARY ACTIVE
- RVARY INACTIVE
- RVARY DATASHARE
- RVARY NODATASHARE
- SETROPTS RACLIST(classname)
- SETROPTS RACLIST(classname) REFRESH
- SETROPTS NORACLIST(classname)
- SETROPTS GLOBAL(classname)

 © 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

- SETROPTS GLOBAL(classname) REFRESH
- SETROPTS GENERIC(classname) REFRESH
- SETROPTS WHEN(PROGRAM)
- SETROPTS WHEN(PROGRAM) REFRESH

RACF DATA SHARING.

RACF uses a Coupling Facility (CF) cache structure for data sharing, and implements CF cache structures as a store through cache for the RACF primary and back-up databases (see Figure 10). It is used to keep frequently-referenced information located in the RACF database so that security information can be accessed quickly by all sharing RACF systems. The structures act like a buffer for the RACF read activity. Whenever you make changes to RACF, the DASD version is always updated before the structure. One cache structure is created for each dataset that makes up the primary and back-up RACF databases.

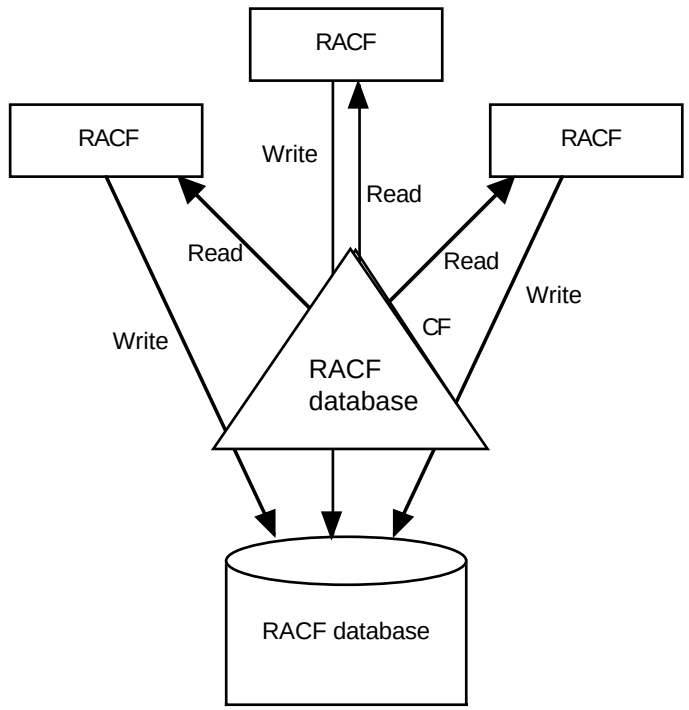

Figure 10: RACF data sharing

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

Structure type	Naming conventions
CACHE	IRRXCF00_ayyy Where: a = P/B for primary/backup yyy = RACF database sequence number The sequence number is retrieved from the RACF dataset descriptor table (ICHPDSDT). This table describes the primary and back-up RACF dataset and is created at IPL time with information from the customer provided load module database name table (ICHRDSNT). The sequence number is assigned by RACF in the dataset descriptor table according to the sequence in which the RACF datasets are defined in the dataset name table. Both sequence numbers, for the primary and back-up, should start with 001.

Figure 11: RACF cache structure name definitions

These cache structures are shared with all systems in the coupling facility. RACF uses non-persistent cache structures, which means that buffers get deallocated when all systems have disconnected from them.

RACF sysplex data sharing is enabled by setting bit 5 (Bit 5 - Enable RACF sysplex data sharing) of the RACF database name table (ICHRDSNT) flag byte. RACF sysplex communication must also be enabled.

The RACF cache structure name definitions are shown in Figure 11.

In order to exploit RACF data sharing the following are required:

- RACF Version 2 Release 2 or later must be installed on all sharing systems.
- All sharing systems must have access to the same coupling facility.
- All sharing systems must be enabled for sysplex communication.
- Only members of the multi-system sysplex can share the RACF database.
- The major names SYSZRACF and SYSZRAC2 cannot be in the GRS exclusion RNL.

© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

- The database must reside on shared DASD.
- The database name table (ICHRDSNT) must be compatible for all sharing systems.
- The database range table (ICHRRNG) must be identical on all sharing systems.
- The class descriptor table (ICHRRCDE) must be compatible for all sharing systems.
- RACF sysplex communication must be enabled via bit setting in the RACF database name table (ICHRDSNT).

When implementing RACF data sharing, all systems in the parallel sysplex that are in data sharing mode must share the same RACF database. Other systems within the parallel sysplex that are not in data sharing mode can use their own RACF database.

RACF support for data sharing mode can be characterized as follows:

- Use of GRS ENQ/DEQ protocol, rather than the use of RESERVE/RELEASE for serialization. This protocol uses GLOBAL ENQs to protect the integrity of RACF data in the RACF database.
- Use of XCF signalling for communication.
- Use of the coupling facility for sharing the RACF database.
- When data sharing is initiated, the RACFDS (data sharing) address space is started automatically and stays active until the next IPL, even if RACF is placed back into non-RACF sysplex data sharing mode. The RACFDS address space is started with a high dispatching priority.

The following steps are required to enable RACF sysplex data sharing:

- Enable RACF sysplex communication.
- Define the coupling facility structures.
- Activate the coupling facility structures.

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

- Activate RACF sysplex data sharing mode by issuing the following RACF command:

  ```
  #RVARY DATASHARE
  ```

  (where # is the RACF subsystem prefix character).

- Default to RACF sysplex data sharing mode. To enable RACF to initialize automatically in RACF sysplex data sharing mode at IPL time, the flag byte of the first entry in the RACF dataset name table (ICHRDSNT) may be modified.

RACGLIST CLASS

RACGLIST was designed specifically for the parallel sysplex environment, to improve the performance of RACLIST processing, and ensures that all members have exactly the same copy of the profiles. RACGLIST provides a single image for security when the installation is using

```
RACROUTE REQUEST=LIST,ENVIR=CREATE,GLOBAL=YES,
```

or

```
SETROPTS RACLIST(class_name)
```

on multiple systems in a sysplex. Installations that use RACGLIST classes should see decreased accesses to the RACF database when performing sysplex-wide SETROPTS RACLIST REFRESH operations or during initialization when an initial RACLIST is performed

RACF uses the RACGLIST class to save the results of in-storage profiles that have been RACLISTed to a RACLIST dataspace, when using one of the following commands:

- SETROPTS RACLIST(Class_name)
- SETROPTS RACLIST(Class_name) REFRESH
- RACROUTE REQUEST=LIST,GLOBAL=YES

When a SETROPTS RACLIST(Class_name) is issued on a system in a sysplex and the RACGLIST class has been activated, the system will

 © 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

read every profile in the class from the RACF database, build the RACLIST tree of profiles for the RACLIST dataspace, and write a copy of the whole tree into one or more RACGLIST profiles in the RACF database. The other systems will read the RACGLIST profile and copy them into their own dataspace. The RACGLIST class profiles are stored in a structure similar to the structure that is finally stored in the RACLIST dataspace.

RACF uses the RACGLIST profiles to build the RACLIST dataspace for the following events:

- SETROPTS RACLIST(class_name) during an IPL
- `RACROUTE REQUEST=LIST,ENVIR=CREATE,GLOBAL=YES`
- Propagates SETROPTS RACLIST or SETROPTS RACLIST(class_name) REFRESH

To enable RACF to use the RACGLIST class, you need to activate RACGLIST by using

```
SETROPTS CLASSACT(RACGLIST)
```

and prime RACGLIST for a specific class by issuing the RDEFINE RACGLIST Class_name command. RACF will then build additional profiles and store them in the RACF database. For example, if the RACGLIST class name profile is REMCLASS, RACF creates profiles named:

- REMCLASS_00001
- REMCLASS_00002
- REMCLASS_00003, etc.

RECENT RACF ENHANCEMENTS

Password management

The following password management enhancements are provided by APAR OW26060:

- As of Release 2.6, a help desk administrator can reset passwords and resume user ids that have been revoked without requiring

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

excessive RACF privilege. This means you avoid the requirement for help desk personnel to have the SPECIAL or GROUP SPECIAL attribute, or to own the affected USER PROFILE. Also, the home-grown Assembler and REXX add-ons can now be removed. Password management is implemented by defining a profile that will protect resource IRR.PASSWORD.RESET in the FACILITY class. If the profile does not exist, the standard privileges apply when RACF determines whether the command issuer is authorized. Users who are permitted to this rule with READ permission can reset passwords for all userids except userids which have SPECIAL, OPERATIONS, or AUDITOR.

The command syntax is:

```
RDEFINE FACILITY IRR.PASSWORD.RESET UACC(NONE) OWNER(OWNGROUP)
PERMIT IRR.PASSWORD.RESET CLASS(FACILITY) ACC(READ) ID(HELPDESK)
```

- The ability to reset a password without marking the new password as expired, so that the next time the user logs on, he or she does not need to change the password.

  The commands syntax is

  ```
  ALU userid NOEXPIRED Password(password)
  ```

- The ability to list information in the base RACF segment of a user profile without requiring SPECIAL, GROUP SPECIAL, or ownership of the profile.

The previous two enhancements can be delegated to help desk personnel by permitting them to a FACILITY class rule named IRR.LISTUSER. A user or group with READ or higher permission to this rule can issue the LISTUSER command for all userids except those userids with SPECIAL, OPERATIONS, or AUDITOR. A user with UPDATE or higher permission to this rule can issue ALTUSER userid NOEXPIRED for any userid except those with SPECIAL, OPERATIONS, or AUDITOR.

To enable a help desk user to issue the LU and ALU userid NOEXPIRED, the following RACF commands can be issued:

```
RDEFINE FACILITY IRR.LISTUSER UACC(NONE) OWNER(OWNGROUP)
PERMIT IRR.LISTUSER CLASS(FACILITY) ACC(UPDATE) ID(HELPDESK)
```


© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

The UNIXMAP class

RACF has used the facilities of Virtual Lookaside Facility (VLF) to map UIDs to user IDs and GIDs to group names for verification of OS/390 Unix system service requests. For RACF to begin using VLF for UID and GID mapping, you must define the IRRUMAP and IRRGMAP class to VLF in the COFVLFxx member of SYS1.PARMLIB as follows. Although not required, IBM strongly recommends this action:

```
CLASS NAME(IRRUMAP)
EMAJ(UMAP)

CLASS NAME(IRRGMAP)
EMAJ(GMAP)
```

A performance problem has been encountered when RACF is invoked to look up a RACF userid when given an OMVS UID, or when RACF is invoked to look up a RACF group name when given an OMVS GID. If VLF is not active or VLF is active but a UID or GID is not found in a VLF data space, requests for UID-to-USERID mapping and GID-to-GROUP mapping default to searching the RACF database on each request. Even more serious are environments that use Network File System (NFS) or Distributed File System (DFS) to mount external file systems from systems where the UIDs and GIDs are not kept in synch with the mounting system. In this case, the UIDs and GIDs will not be found in VLF, and then the entire RACF database is searched in order to determine that the UID or GID is unknown, resulting in poor performance.

To resolve this problem, IBM has provided the UNIXMAP class. This is used to map UIDs to user IDs and GIDs to group names. This allows RACF to tell whether a UID or GID is unknown by doing one I/O operation to the RACF database. This new function will automatically keep the new class in synch with user and group information in the RACF database. It does this by modifying the UNIXMAP class profile appropriately when ADDUSER, ALTUSER, DELUSER, ADDGROUP, or DELGROUP commands are issued.

The new support still uses VLF as follows: when a UID or GID mapping is not found in VLF, the UID or GID is looked up in the new UNIXMAP class. If it is found, the UID or GID is added to VLF.

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

There are two types of profile in the UNIXMAP class:

- UID mapping profiles. The profile names are of the form U*xxxxxxxxxx*, where *xxxxxxxxxx* is the UID in EBCDIC.
- GID mapping profiles. The profile names are of the form G*yyyyyyyyyy*, where *yyyyyyyyyy* is the GID in EBCDIC.

Where one UID is allowed to map to multiple user ids (for example, UID=1 for system programmers), there would be multiple entries on the access list of UNIXMAP profile U1. The look-up routine will return the first user ID on the access list.

The RACF FMID

As of OS/390 Version 2 Release 6, RACF is a component of the OS/390 Security Server. Security Server (RACF) has a new FMID HRF22260. Because RACF is a component of the OS/390 Security Server, it no longer has a version, release, and modification level of its own. To provide compatibility with previous releases and versions of RACF, the ICHEINTY, ICHEACTN, ICHETEST, and RACROUTE macros accept the RELEASE=2.6 keyword. The RACF Vector Table (RCVT) contains the value 2060 to identify the RACF level. In essence, the FMID HRF2260 is presented as Version 2.6.0

R F Perretta
Millenium Computer Consultancy (UK)
© Xephon 2000

Leaving? You don't have to give up *RACF Update*

You don't have to lose your subscription when you move to another location – let us know your new address, and the name of your successor at your current address, and we will send *RACF Update* to both of you, for the duration of your subscription. There is no charge for the additional copies.

 © 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

Checking the authorization of JCL parameters

THE PROBLEM

We wanted to restrict the output class in JCL to certain permitted classes. We also wanted certain users to be allowed only certain classes. The authorizations are defined in RACF.

OUR SOLUTION

Checking permitted output classes takes place in JES2 user exit 6 (converter exit). The exit extracts the following from the converted JCL (the converter/interpreter text):

- The MSGCLASS parameter from the JOB card '//... JOB... ,MSGCLASS=X,...'. This is the output class when SYSOUT=* in DD card.
- The first sub-parameter of the SYSOUT parameter from the DD card '//... DD... ,SYSOUT=(X,...),...'.
- The CLASS parameter from the OUTPUT card '//... OUTPUT... ,CLASS=X,...'.

This creates the following RACF resource names to check RACF authorization in class FACILITY:

- @JCL.JOB.MSGCLASS.x
- @JCL.DD.SYSOUT.CLASS.x
- @JCL.OUTPUT.CLASS.x.

where 'x' is the output class.

Note that the exit is executing as a subtask in the JES2 address space, but with an ACEE for the job user. This means that RACF checking is possible for the job user.

An output class is allowed if the user has at least READ authority for the matching RACF profile, or if there is no profile. If the user is not

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

authorized, the job terminates with a JCL error and the following message appears in the joblog:

```
IEFC452I jobname - JOB NOT RUN - JCL ERROR
```

The job is also shown as not executed in BETA92.

INSTALLATION

The following steps are necessary to install this solution:

- Install the USREX006 load module in SYS1.LINKLIB, preferably by SMP.
- Define the exit in JES2 parameters:

```
LOAD(USREX006) STORAGE=PVT
EXIT(006)  ROUTINE=UEX006,
           STATUS=ENABLED,
           TRACE=NO
```

- Create profiles in RACF class FACILITY, for example, using @JCL.** with UACC(READ), @JCL.JOB.MSGCLASS.x, @JCL.DD.SYSOUT.CLASS.x, @JCL.OUTPUT.CLASS.x with the necessary UACC and entries in access lists (eg @JCL.**.*CLASS.x is also possible).
- To turn off the exit, use the following JES2 command:

```
$T EXIT(6),STATUS=DISABLED
```

  It can be reactivated using:

```
$T EXIT(6),STATUS=ENABLED
```

EXTENDING THE EXIT

This exit can be easily extended for any parameter of the JOB, EXEC, DD, and OUTPUT card (it makes little sense to check the remaining JCL statements) – see the program logic (the JCL parameter table) and the commentary of the source program below.

The RACF resource names are defined as follows:

© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

```
@JCL.statement.parameter.value
```

if the JCL parameter has no sub-parameters, and:

```
@JCL.statement.parameter.subparameter.value
```

if the JCL parameter has sub-parameters.

Additional background information can be obtained from the *JES2 Installation Exits* manual, SC28-1463, and from the *MVS C/I Text Processing* chapter in *MVS/ESA Installation Exits*, SC28-1459. It would also be useful to review SYS1.SAMPLIB(HASX06A).

USREX006

```
TITLE '— USREXØØ6 — JES2 USER EXIT 6 —'
* REGISTER USAGE
*   RØ : WORK
*   R1 : WORK
*   R2 : WORK
*   R2 : ADDRESS OF 1ST ENTRY FOR KEY FOUND IN KEY TABLE
*   R3 : ADDRESS OF ENTRY IN KEY TABLE
*   R4 : LENGTH OF KEY PARAMETER OR KEY SUBPARAMETER
*   R5 : # OF KEY SUBPARAMETER
*   R6 : KEY SUBPARAMETER COUNT
*   R7 : # OF KEY PARAMETER
*   R8 : KEY PARAMETER COUNT
*   R9 : CURRENT POINTER TO C/I TEXT
*   R1Ø: ADDRESS OF 16 BYTES WORK AREA
*   R11: ADDRESS OF $HCT
*   R12: BASE
*   R13: ADDRESS OF WORK AREA = ADDRESS OF SAVE AREA
*   R14: WORK
*   R15: WORK
*********************************************************************
* JES2 ENVIRONMENT AND DSECTS
*********************************************************************
         PRINT NOGEN
         COPY  $HASPGBL            HASP GLOBALS
                                                          EJECT
USREXØØ6 $MODULE ENVIRON=SUBTASK,  SUBTASK IN JES2 ADDRESS SPACE      +
               RMODE=ANY,          THEREFORE AMODE=31                 +
               SYSP=(NOGEN,NOGEN,NODATA,NOGEN,NOGEN), (*,EX,*,MVS,JES) +
               CNMB,               CONVERTER MESSAGE BUFFER           +
               (KEYS,GEN),         IEFVKEYS, TABLE OF C/I KEYS        +
               (TEXT,GEN),         IEFTXTFT, C/I TEXT FORMAT          +
```

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

```
               $DTE,              DAUGHTER TASK ELEMENT              +
               $HASPEQU,          GENERAL EQUATES                    +
               $HCCT,             COMMON STORAGE COMMUNICATION TABLE +
               $HCT,              COMMUNICATION TABLE  <- R11        +
               $JCT               JOB CONTROL TABLE
                                                          EJECT
         PUSH  PRINT
         PRINT GEN
DOKEY    DSECT ,                  DYNAMIC OUTPUT KEYS (// OUTPUT ...)
         IEFDOKEY ,
         POP   PRINT
                                                          EJECT
XPL      DSECT ,                  EXIT PARAMETER LIST, NOT IN $XPL
X00 6WORK DS    A                 ADDRESS OF 16 BYTES WORK AREA
X00 6TEXT DS    A                 ADDRESS OF C/I TEXT
X00 6DTE  DS    A                 ADDRESS OF $DTE
X00 6JCT  DS    A                 ADDRESS OF $JCT
X00 6CNMB DS    A                 0, POSSIBLY ADDR OF CNMB AT RETURN
                                                          SPACE
WK16     DSECT ,                  16 BYTES WORK AREA
WK1616   DS    0XL16
WK16R3   DS    F                 SAVED R3
WK16R14  DS    F                 SAVED R14
WK16@DYN DS    A                 ADDRESS OF WORKING STORAGE
WK16IND  DS    B
WK16IND1   EQU   B'10000000'     KEY TO SEARCH FOUND IN C/I TEXT
         DS    (WK16+16-*)B      UNUSED
                                                          SPACE
WORK     DSECT ,                  WORKING STORAGE
         DS    18F               SAVE AREA (FOR RACROUTE)
WORK@SAH EQU   WORK+4,4          ADDRESS OF HIGHER SAVE AREA
WORKR13  DS    F                 SAVED R13
WORKRN   DS    0H                ENTITYX STRUCTURE
WORKRNL  DS    H                 RESOURCE NAME BUFFER LENGTH
WORKRNA  DS    H                 TRUE LENGTH OF RESOURCE NAME
WORKRNM  DS    CL(5*9-1)         RESOURCE NAME (MAX 5 QUALIFIERS)
         DS    0F
WORKRAU  DS    XL(RAUPL)         RACROUTE PAR LIST FOR AUTH CHECK
         DS    0F
WORKSAFW DS    XL512             SAF WORK AREA
         DS    0D
WORKL    EQU   *-WORK            LENGTH OF WORKING STORAGE
                                                          SPACE
KEY_     DSECT ,                  TAB OF KEYS TO PROCESS IN C/I TEXT
KEY_KEY  DS    AL1               KEY
*                                  (SEE MACRO IEFVKEYS)
KEY_OUTP DS    AL2               KEY FOR OUTPUT (0 WHEN JOB/EXEC/DD)
*                                  (SEE MACRO IEFDOKEY)
```


© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

```
KEY_#PAR DS    AL1                 # OF KEY PARAMETER
KEY_#SUB DS    AL1                 # OF KEY SUBPARAMETER
*                                    (Ø WHEN NO KEY SUBPARAMETER)
KEY_IND  DS    B
KEY_CONT  EQU   1                  ANOTHER TAB ENTRY FOR THE SAME KEY
*                                    FOLLOWS BUT WITH A DIFFERENT KEY
*                                    PARAMETER OR KEY SUBPARAMETER
KEY_@PRO DS    AL4                 ADDRESS OF RACF PROFILE
*                                    (1 BYTE LENGTH FIELD IS 1ST BYTE)
KEY_L    EQU   *-KEY_              LENGTH OF TABLE
                                                                SPACE
&J2SECTN &J2SECTT ,                AGAIN CSECT OR RSECT
                                                                EJECT
         TITLE '── USREXØØ6 ── JES2 USER EXIT 6 ──'
*********************************************************************
* PROLOGUE
*********************************************************************
UEXØØ6   $ENTRY BASE=R12           REUS, RENT, REFR; KEY 1; SUPERVISOR
         $SAVE ,                   SAVE CALLER'S REGISTERS
         LR    R12,R15             LOAD BASE REGISTER
         USING XPL,R1
         L     R1Ø,XØØ6WORK        ADDRESS OF 16 BYTES WORK AREA
         USING WK16,R1Ø
         XC    WK1616,WK1616       CLEAR 16 BYTES WORK AREA
         LTR   RØ,RØ               4 = CONVERTER FINISHED ?
         BNZ   RETURN                YES, LAST CALL, NOTHING TO DO
         L     R2,XØØ6TEXT         ADDRESS OF C/I TEXT
         USING TEXT,R2
         DROP  R1
                                                                SPACE
         LA    R3,KEYSJOB          KEYS TO PROCESS IF JOB CARD
         LA    R9,STRJKEY          ADDR OF 1ST KEY IN C/I TEXT IF JOB
         TM    STRINDCS,JOBSTR     JOB CARD ?
         BO    CIT                   YES
         LA    R3,KEYSEXEC         KEYS TO PROCESS IF EXEC CARD
         LA    R9,STREKEY          ADDR OF 1ST KEY IN C/I TEXT IF EXEC
         TM    STRINDCS,EXECSTR    EXEC CARD ?
         BO    CIT                   YES
         LA    R3,KEYSDD           KEYS TO PROCESS IF DD CARD
         LA    R9,STRDKEY          ADDR OF 1ST KEY IN C/I TEXT IF DD
         TM    STRINDCS,DDSTR      DD CARD ?
         BO    CIT                   YES
         LA    R3,KEYSOUTP         KEYS TO PROCESS IF OUTPUT CARD
         LA    R9,STRSKEY          ADDR OF 1ST KEY IN C/I TEXT IF OUTP
         TM    STRINDCS,JDVBSTR    OUTPUT/CNTL/ENDCNTL CARD ?
         BZ    RETURN                NO
         CLI   STRSKEY,JDTVERBK    OUTPUT/CNTL/ENDCNTL CARD ?
         BNE   RETURN                NO
```

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

```
         CLC   COUTPUT,STRSKEY+2   OUTPUT CARD ?
         BE    CIT                   YES
         B     RETURN              OTHER JCL CARDS NOT PROCESSED
         DROP  R2
         USING KEY_,R3
                                                              EJECT
CIT      DS    ØH
         CLI   KEY_KEY,ETEND       ANY KEYS TO PROCESS ?
         BE    RETURN                NO
         ST    R3,WK16R3           SAVE ADDRESS OF TABLE OF KEYS
         XR    R8,R8               KEY PARAMETER COUNT
         XR    R6,R6               KEY SUBPARAMETER COUNT
         XR    R4,R4               LENGTH OF KEY PAR OR KEY SUBPAR
                                                                SPACE
* ******** NOTE **********    ***************** EXAMPLES ***************
* JCL           C/I TEXT      // JOB (X,Y),..  // DD SPACE=(..,(1,2)),.
* ————          ————————      ——————————————   ————————————————————
* PARAMETER <-> KEY           POSITION PARAM   'SPACE'
* SUBPAR    <-> KEY PAR       ACCOUNT          PRIM+SEC
* SUBSUBPAR <-> KEY SUBPAR    'X' , 'Y'        '1' , '2'
                                                              SPACE
CITLKEY  DS    ØH                  LOOP: ALL KEYS
         CLI   Ø(R9),ENDK          END OF C/I TEXT ?
         BE    RETURN                YES
         NI    WK16IND,255-WK16IND1  KEY NOT FOUND
         XR    RØ,RØ
         XR    R1,R1
         CLI   Ø(R9),JDTKWDK       KEY FOR OUTPUT ?
         BNE   CITNKEYO              NO
         BCTR  RØ,Ø                KEY FOR OUTPUT WITHOUT KEY PARAMETER
         LA    R1,3                SKIP KEY FOR OUTPUT
CITNKEYO DS    ØH
                                                              SPACE
         L     R3,WK16R3           AGAIN ADDR OF BEGIN OF TABLE OF KEYS
         LA    R14,KEY_L           LENGTH OF A TABLE ENTRY
         SLR   R3,R14
CITSKEY  DS    ØH                  LOOP: TABLE OF KEYS
         ALR   R3,R14              TO NEXT TABLE ENTRY
         CLI   KEY_KEY,ETEND       END OF TABLE ?
         BE    CITNKEY               YES, NOT ONE OF THE KEYS SEARCHED
         CLC   KEY_KEY,Ø(R9)       THE KEY SEARCHED ?
         BNE   CITSKEY               NO
                                                              SPACE
         CLI   Ø(R9),JDTKWDK       KEY FOR OUTPUT TO SEARCH ?
         BNE   CITNOUT               NO
         CLC   KEY_OUTP,3(R9)      IS IT THE KEY FOR OUTPUT SEARCHED ?
         BNE   CITSKEY               NO
CITNOUT  DS    ØH
                                                              SPACE
```


© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

```
         OI    WK16IND,WK16IND1    KEY FOUND
CITNKEY  DS    ØH
         IC    R8,1(,R9)           KEY PARAMETER COUNT
         AR    R8,RØ               POSSIBLY ONE LESS IF KEY FOR OUTPUT
         XR    R7,R7               # OF KEY PARAMETER
         LA    R9,2(R1,R9)         ADDRESS OF LENGTH OF KEY PARAMETER
         LTR   R8,R8               NO KEY PARAMETERS ?
         BZ    CITLKEY               YES, ALREADY AT NEXT KEY
                                                          SPACE
CITLPAR  DS    ØH                  LOOP: ALL KEY PARAMETERS OF A KEY
         LA    R7,1(,R7)           # OF KEY PARAMETER
         TM    Ø(R9),X'8Ø'         KEY SUBPAR SEQUENCE, NOT KEY PAR ?
         BZ    CITXSUB               NO
         IC    R6,Ø(,R9)           KEY SUBPARAMETER COUNT
         LA    R15,X'FF'-X'8Ø'
         NR    R6,R15              KEY SUBPAR COUNT WITHOUT SUBPAR BIT
         XR    R5,R5               # OF KEY SUBPARAMETER
         LA    R9,1(,R9)           ADDR OF LENGTH OF KEY SUBPARAMETER
                                                            SPACE
CITLSUB  DS    ØH                  LOOP: ALL KEY SUBPAR OF A KEY PAR
         LA    R5,1(,R5)           # OF KEY SUBPARAMETER
         ICM   R4,B'ØØØ1',Ø(R9)    LENGTH OF KEY SUBPAR; LENGTH ZERO ?
         BZ    CITISUB               YES, KEY SUBPAR NOT EXISTING
         TM    WK16IND,WK16IND1    THE KEY SEARCHED ?
         BZ    CITISUB               NO
         LR    R2,R3               SAVE ADDR OF 1ST TABLE ENTRY FOR KEY
CIT#SUB  DS    ØH
         CLM   R7,B'ØØØ1',KEY_#PAR  THE KEY PARAMETER SEARCHED ?
         BNE   CITCSUB                NO
         CLM   R5,B'ØØØ1',KEY_#SUB  THE KEY SUBPARAMETER SEARCHED ?
         BE    CITFSUB                YES
CITCSUB  DS    ØH
         TM    KEY_IND,KEY_CONT    ANOTHER KEY PARAMETER FOR SAME KEY ?
         BZ    CITNSUB               NO
         LA    R3,KEY_L(,R3)       ADDR OF NEXT TAB ENTRY FOR SAME KEY
         B     CIT#SUB
                                                          SPACE
CITFSUB  DS    ØH
         BAS   R14,RACF            CHECK KEY SUBPARAMETER VALUE BY RACF
         B     *+4(R15)
         B     CITNSUB             VALUE IS VALID
         B     RETURN              NO DECISION, NO FURTHER CHECKING
         B     CANCEL              VALUE IS INVALID
CITNSUB  DS    ØH
         LR    R3,R2               AGAIN ADDR OF 1ST TAB ENTRY FOR KEY
                                                          SPACE
CITISUB  DS    ØH
         LA    R9,1(R4,R9)         ADDRESS BEHIND KEY SUBPARAMETER
```

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

```
         BCT   R6,CITLSUB          ANOTHER KEY SUBPARAMETER ?
         BCT   R8,CITLPAR            NO, ANOTHER KEY PARAMETER ?
         B     CITLKEY                     NO, NEXT KEY
CITXSUB  DS    ØH
                                                              SPACE
         ICM   R4,B'ØØØ1',Ø(R9)    LENGTH OF KEY PAR; LENGTH ZERO ?
         BZ    CITIPAR               YES, KEY PARAMETER NOT EXISTING
         TM    WK16IND,WK16IND1    THE KEY SEARCHED ?
         BZ    CITIPAR               NO
         LR    R2,R3               SAVE ADDR OF 1ST TAB ENTRY FOR KEY
CIT#PAR  DS    ØH
         CLM   R7,B'ØØØ1',KEY_#PAR  THE KEY-PARAMETER SEARCHED ?
         BNE   CITCPAR               NO
         CLI   KEY_#SUB,1          NO KEY SUBPAR OR THE FIRST ONE ?
         BNH   CITFPAR               YES
* NO KEY SUBPAR AND THE 1ST KEY SUBPAR ARE SYNONYMOUS, EG:
* SPACE=(TRK,1)     : PRIMARY SPACE IS KEY PARAMETER, NO KEY SUBPAR
* SPACE=(TRK,(1,Ø)) : PRIMARY SPACE IS 1ST KEY SUBPARAMETER
CITCPAR  DS    ØH
         TM    KEY_IND,KEY_CONT    ANOTHER KEY PAR FOR THE SAME KEY ?
         BZ    CITNPAR               NO
         LA    R3,KEY_L(,R3)       ADDR OF NEXT TAB ENTRY FOR SAME KEY
         B     CIT#PAR
                                                              SPACE
CITFPAR  DS    ØH
         BAS   R14,RACF            CHECK KEY PARAMETER VALUE BY RACF
         B     *+4(R15)
         B     CITNPAR             VALUE IS VALID
         B     RETURN              NO DECISION, NO FURTHER CHECKING
         B     CANCEL              VALUE IS INVALID
CITNPAR  DS    ØH
         LR    R3,R2               AGAIN ADDR OF 1ST TAB ENTRY FOR KEY
                                                              SPACE
CITIPAR  DS    ØH
         LA    R9,1(R4,R9)         ADDRESS BEHIND KEY PARAMETER
         BCT   R8,CITLPAR          ANOTHER KEY PARAMETER ?
         B     CITLKEY               NO, NEXT KEY
                                                              EJECT
*********************************************************************
* EPILOGUE
*********************************************************************
CANCEL   DS    ØH
         LA    R2,8                CANCEL JOB
         B     RETURNX
RETURN   DS    ØH
         XR    R2,R2               OK
RETURNX  DS    ØH
         L     R1,WK16@DYN         ADDRESS OF WORKING STORAGE
         XC    WK1616,WK1616       RESET 16 BYTES WORK AREA
```


© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

```
         LTR   R1,R1               WORKING STORAGE EXISTING ?
         BZ    RETURNY               NO
         USING WORK,R1
         L     R13,WORKR13         RESTORE R13 OF CALLER
* $RETURN NEEDS R13 OF CALLER IN SPITE OF REGISTERS BEING IN STACK!
* (OTHERWISE SØF7 REASON X'58')
         DROP  R1
         LA    RØ,WORKL            LENGTH OF WORKING STORAGE
         STORAGE RELEASE,LENGTH=(Ø),ADDR=(1),SP=Ø  FREE STORAGE
RETURNY  DS    ØH
         $RETURN RC=(R2)
                                                                    EJECT
*********************************************************************
* SUBROUTINE
* CHECK BY RACF IF JCL PARAMETER IS ALLOWED FOR USER
* OUT: R15 = Ø: JCL PARAMETER ALLOWED FOR USER
*          = 4: RACF CLASS NOT ACTIVE OR NO PROFILE
*          = 8: JCL PARAMETER NOT ALLOWED FOR USER
*********************************************************************
RACF     DS    ØH
         ST    R14,WK16R14         SAVE R14
         ICM   R1,B'1111',WK16@DYN  WORKING STORAGE ALREADY OBTAINED ?
         BNZ   RACFDYN               YES
         LA    RØ,WORKL            LENGTH OF DYNAMIC WORKING STORAGE
         STORAGE OBTAIN,LENGTH=(Ø),LOC=BELOW,SP=Ø
         ST    R1,WK16@DYN         KEEP ADDRESS IN MIND
         LR    RØ,R1
         LA    R1,WORKL
         XR    R15,R15
         MVCL  RØ,R14              CLEAR DYNAMIC WORKING STORAGE
         L     R1,WK16@DYN
         USING WORK,R1
         ST    R13,WORKR13         SAVE ADDRESS OF CALLER'S SAVE AREA
         DROP  R1
         LR    R13,R1              ADDR OF OWN SAVE AREA = ADDR DYN STG
         USING WORK,R13
         MVC   WORK@SAH,=C'F1SA'   REGS IN STACK INSTEAD OF SAVE AREA
         LA    RØ,L'WORKRNM        TOTAL LENGTH OF RESOURCE NAME
         STH   RØ,WORKRNL
         MVC   WORKRNM(L'RHIQ),RHIQ  1ST QUALIFIER OF RESOURCE NAME
RACFDYN  DS    ØH
                                                                   SPACE
         LA    R1,WORKRNM+L'RHIQ   ADDR BEHIND 1ST QUAL OF RSRC NAME
         MVI   Ø(R1),C' '          PAD RESOURCE NAME WITH BLANKS
         MVC   1(L'WORKRNM-L'RHIQ-1,R1),Ø(R1)
         ICM   R14,B'1111',KEY_@PRO  ADDRESS OF RACF PROFILE FOR KEY
         XR    R15,R15
         IC    R15,Ø(,R14)         LENGTH OF PROFILE
```

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

```
         BCTR  R15,Ø               MINUS 1 BECAUSE OF EX
         EX    R15,EXMVC1          RACF PROF FOR KEY TO RESOURCE NAME
         LA    R1,1(R15,R1)        ADDRESS BEHIND RESOURCE NAME
         MVI   Ø(R1),C'.'
         LR    R15,R4              LENGTH OF JCL PARAMETER (VALUE)
         BCTR  R15,Ø               MINUS 1 BECAUSE OF EX
         EX    R15,EXMVC2          JCL PARAM (VALUE) TO RESOURCE NAME
         EX    R15,EXTR2           '*' & '&' IN RSRC NAME NOT ALLOWED
                                                          SPACE
         MVC   WORKRAU,RAUP        RACROUTE PROTOTYPE TO DYNAMIC AREA
         RACROUTE REQUEST=AUTH,    CHECK AUTHORIZATION BY RACF         +
               WORKA=WORKSAFW,                                         +
               CLASS=RCLS,         (LENGTH OF CLASS + CLASS)           +
               ENTITYX=WORKRN,                                         +
               RELEASE=1.9,                                            +
               MF=(E,WORKRAU)
         LA    RØ,8
         CLR   R15,RØ              JCL PARAMETER NOT ALLOWED FOR USER ?
         BE    RACFCNMB              YES
         L     R14,WK16R14         SAVED R14
         LA    RØ,4
         CLR   R15,RØ              CLASS NOT ACTIVE OR NO PROFILE ?
         BER   R14                   YES
         XR    R15,R15             ALLOWED, OR ANY ERROR
         BR    R14
                                                          SPACE
RACFCNMB DS    ØH
         LA    RØ,CNMBSIZE         LENGTH OF CNMB
         STORAGE OBTAIN,LENGTH=(Ø),LOC=BELOW,SP=CNMBSP,                +
               CALLRKY=YES         BECAUSE KEY 1 REQUIRED FOR STORAGE!
* RELEASE OF STORAGE OF CNMB DONE BY CONVERTER!
         LR    R15,R1
         USING CNMB,R15
         LA    R1,3                MODIFIABLE AREA OF STACK REQUESTED
         ESTA  RØ,R1               GET RØ AND R1 FROM STACK
         USING XPL,R1
         ST    R15,XØØ6CNMB        RETURN ADDR VIA PARAMETER ADDR LIST
         DROP  R1
         XC    CNMB(CNMBSIZE),CNMB  CLEAR ALL FIELDS
         MVC   CNMBID,=AL4(CNMBCID)  ID OF CONTROL BLOCK
         MVI   CNMBVER,CNMBCVER    VERSION OF CONTROL BLOCK
         MVI   CNMBSUBP,CNMBSP     SUBPOOL OF CONTROL BLOCK
         LA    RØ,CNMBSIZE
         STH   RØ,CNMBLEN          LENGTH OF CONTROL BLOCK
         OI    CNMBOPTS,CNMBFJOB   INDICATE JCL ERROR
* PUTS MESSAGE "IEFC452I ........ - JOB NOT RUN - JCL ERROR" TO JOBLOG;
* IMPORTANT FOR BETA92: OTHERWISE JCL ERROR OF JOB NOT RECOGNIZED
         DROP  R15
```


© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

```
         LA    R15,8               JCL PARAMETER NOT ALLOWED FOR USER
         L     R14,WK16R14         SAVED R14
         BR    R14
                                                                    EJECT
*********************************************************************
* CONSTANTS
*********************************************************************
CNMBSP   EQU   23Ø                 SUBPOOL OF CNMB
EXMVC1   MVC   Ø(1,R1),1(R14)      RACF PROFILE FOR KEY TO RSRC NAME
EXMVC2   MVC   1(1,R1),1(R9)       JCL PARAM (VALUE) TO RESOURCE NAME
EXTR2    TR    1(1,R1),TTAB        REPLACE '*' & '&' IN VALUE BY '?'
RHIQ     DC    C'@JCL.'            1ST QUALIFIER OF RACF PROFILE
                                                                    SPACE
         DC    AL1(6),C'OUTPUT'    IDENT IN C/I TEXT FOR OUTPUT CARD
COUTPUT  EQU   *-6-1,1+6,C'C'
                                                                    SPACE
TTAB     DC    256AL1(*-TTAB)      TRANSLATION TABLE '*' & '&' TO '?'
         ORG   TTAB+C'*'           '*' & '&' ARE NOT ALLOWED IN
         DC    C'?'                  RESOURCE NAME, REPLACE BY '?'
         ORG   TTAB+C'&&'
         DC    C'?'
         ORG   ,
                                                                    SPACE
         DC    AL1(8)              LENGTH OF RACF CLASS NAME
RCLSN    DC    CL8'FACILITY'       RACF CLASS
RCLS     EQU   RCLSN-1,1+L'RCLSN,C'C'
                                                                    SPACE
RAUP     RACROUTE REQUEST=AUTH,    RACROUTE PROTOTYPE FOR AUTH CHECK   +
               ATTR=READ,          READ AUTHORITY SUFFICIENT           +
               RELEASE=1.9,                                            +
               MF=L
RAUPL    EQU   *-RAUP              LENGTH OF RACROUTE PROTOTYPE
                                                                    EJECT
* KEYS TO PROCESS IN C/I TEXT (SEE DSECT KEY_)
* NOTE: LINES FOR THE SAME KEY HAVE TO BE DIRECTLY CONSECUTIVE AND
*       THE CONCATENATION INDICATOR HAS TO BE SET,
*       EXCEPT IN THE LAST LINE!
KEYSJOB  DS    ØX                  FOR JOB CARD
         DC    AL1(MSGCLAJK+Ø),AL2(Ø),AL1(1,Ø,Ø),AL4(PRØØ1-1)
         DC    AL1(CLASSJK+ØØ),AL2(Ø),AL1(1,Ø,Ø),AL4(PRØØ4-1)
         DC    AL1(ETEND)          INDICATE END OF TABLE
KEYSEXEC DS    ØX                  FOR EXEC CARD
         DC    AL1(ETEND)          INDICATE END OF TABLE
KEYSDD   DS    ØX                  FOR DD CARD
         DC    AL1(SYSOUTK+ØØ),AL2(Ø),AL1(1,Ø,Ø),AL4(PRØØ2-1)
         DC    AL1(ETEND)          INDICATE END OF TABLE
KEYSOUTP DS    ØX                  FOR OUTPUT CARD
         DC    AL1(JDTKWDK),AL2(DOCLASS+ØØ),AL1(1,Ø,Ø),AL4(PRØØ3-1)
         DC    AL1(ETEND)          INDICATE END OF TABLE
                                                                    SPACE
```

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

```
* RACF PROFILES BELONGING TO THE KEYS
* (WITHOUT FIXED 1ST QUALIFIER AND LAST QUALIFIER = VALUE)
         DC    AL1(L'PR00001)
PR00001  DC    C'JOB.MSGCLASS'
         DC    AL1(L'PR00002)
PR00002  DC    C'DD.SYSOUT.CLASS'
         DC    AL1(L'PR00003)
PR00003  DC    C'OUTPUT.CLASS'
         DC    AL1(L'PR00004)
PR00004  DC    C'JOB.CLASS'
                                                                EJECT
*********************************************************************
* END JES2 ENVIRONMENT
*********************************************************************
         DROP  R13,R10,R3
         $MODEND ,
         END   ,
```

Walter Wiedemann
Consultant (Germany)

© Reserved 2000

Call for papers

Why not share your expertise, and earn money at the same time?

RACF Update is looking for REXX EXECs, macros, program code, etc, that experienced RACF users have written to make their lives, or the lives of their users, easier. We also publish longer, analytical pieces, and 'hints and tips' type articles.

Your article will be vetted by our expert panel, and we'll send you a cheque when it's published. Articles can be short or long, and can be sent or e-mailed to Fiona Hewitt at any of the addresses shown on page 2.

Why not call now for a free copy of our *Notes for Contributors*, or look on our Web site, at

www.xephon.com/contnote.html

 © 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

Cursor-sensitive LISTDSD EDITOR command

When you're creating a new JCL member, or changing an existing one, you may need to know how a dataset is protected. Although you can often find this information by using the RACF ISPF dialog or by issuing a TSO LISTDSD command, both methods can give the wrong answer if a dataset name is misspelled. In addition, the RACF ISPF dialog requires an extra logical screen – the LISTDSD TSO command presents the most important information, UACC and access list, on different screens.

You can avoid these problems by using the simple ELDB EDIT macro presented here. This enables you to find out how a dataset is protected simply by entering ELDB on the EDIT (or VIEW) command line, positioning the cursor on the first character of the dataset name, and pressing ENTER. Note that you will need ISPF (any supported release) and TSO (any supported release) in order to use this macro.

HOW ELDB WORKS

After the dataset name has been extracted, an "LD DATASET(dsn) GENERIC ALL" command is issued. The resulting output is OUTTRAPped in the stem variable SOL. A VIO dataset is allocated to a logical screen dependent DD statement.

The really interesting parts of the LISTDSD command output are:

- The profile name, owner, and UACC, which are contained in lines 1 to 6.
- The access list, starting around line 45 (depending on other segments).

These are copied to the VIO dataset and displayed using the ISPF BROWSE service (see sample output below).

Using a VIO dataset instead of a disk dataset removes the need to code

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

complex recovery, since it will be automatically cleaned up at TSO LOGOFF or TIMEOUT.

SAMPLE OUTPUT

```
****************************** Top of Data ******************************
INFORMATION FOR DATASET USERØ1.RJ.** (G)

LEVEL  OWNER    UNIVERSAL ACCESS   WARNING   ERASE
-----  -------- ----------------   -------   -----
 ØØ    USERØ1          NONE          NO       NO


   ID     ACCESS
--------  -------
GROUPØ5    READ
USER52     ALTER
USERØ1     ALTER
GROUP22    READ

   ID    ACCESS   CLASS                ENTITY NAME
-------- ------- -------- ---------------------------------------
NO ENTRIES IN CONDITIONAL ACCESS LIST
***************************** Bottom of Data ****************************
```

ELDB SOURCE CODE

```
/* REXX LISTDSD EDITOR COMMAND POINT AND SHOOT                      */

 ADDRESS ISREDIT
 "MACRO "                              /* MUST BE 1ST STATEMENT      */

 "(ELDBLIN,ELDBCOL) = CURSOR"          /* RETRIEVE  CURSOR POSITION  */

 "(ELDBDSN) = LINE "ELDBLIN            /* COPY EDITOR LINE           */

 ELDBLEN = LENGTH(ELDBDSN)             /* LENGTH OF LINE             */
                                       /* REST OF LINE STARTING AT   */
                                       /* CURSOR POSITION            */
 ELDBDSN = SUBSTR(ELDBDSN,ELDBCOL,(ELDBLEN-ELDBCOL+1))

 I1= INDEX(ELDBDSN,' ')                /* SEARCH FOR FIRST BLANK     */
 IF I1 = Ø THEN I1 = 999               /* OR FIRST COMMA. OTHER      */
 I2= INDEX(ELDBDSN,',')                /* DELIMITERS MAY BE ADDED.   */
 IF I2 = Ø THEN I2 = 999               /* WHATEVER COMES FIRST, DE-  */
```


© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

```
LPOS = MIN(I1,I2) - 1                /* LIMITS THE DATASET NAME    */
                                     /*                            */

ELDBDSN = SUBSTR(ELDBDSN,1,LPOS)     /* EXTRACT DATASET NAME       */

ADDRESS TSO                          /*                            */

A = OUTTRAP(SOL.,5ØØ)     /* MAXIMAL 5ØØ SYSOUT LINES IN STEM SOL. */

"LD DATASET('"ELDBDSN"') GENERIC ALL"   /* IMPORTANT : SINGLE QUOTE*/

IM = SOL.Ø

ADDRESS ISPEXEC  'VGET ZSCREEN'      /* RETRIEVE  SCREEN-ID        */
                                     /* ALLOCATE A VIO DATASET     */
ADDRESS TSO 'ALLOCATE DD(LDB'ZSCREEN') NEW UNIT(VIO)' ||,
         ' RECFM(V B) LRECL(133) BLKSIZE(4127) REUSE'

                      /* COPY THE FIRST 6 LINES TO THE VIO DATASET */
'EXECIO 6 DISKW LDB'ZSCREEN' (STEM SOL. )'

A = OUTTRAP(OFF)                     /* SWITCH OFF SYSOUTTRAPPING  */

J = Ø                                /* COPY ALL LINES STARTING AT */
DO  I = 45 TO IM                     /* LINE  45 TO   STEM LINE.   */
    J = J + 1
    LINE.J =  SOL.I
END

                     /* WRITE COPIED LINES TO THE VIO DATASET      */
'EXECIO ' J ' DISKW LDB'ZSCREEN' (STEM LINE. FINIS)'

ADDRESS ISPEXEC                      /* DEFAULT IS  ISPEXEC        */

'LMINIT DATAID(COM'ZSCREEN'DID)',    /* CALL LMINIT SERVICE        */
    '  DDNAME(LDB'ZSCREEN') ENQ(SHR) ORG(PS) '

A = 'COM' || ZSCREEN || 'DID'        /* RETRIEVE  DATAID           */
DXD =  VALUE( A )

'BROWSE  DATAID('DXD')'              /* CALL BROWSE SERVICE        */
ADDRESS TSO 'FREE DD(LDB'ZSCREEN')'  /* FREE VIO DATASET           */

EXIT
```

Karl Reinhard Blatt
(Germany)

© Xephon 2000

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

Information point – reviews

MANUALS

IBM offers RACF manuals on-line in the System/390 Library. The entry point is

http://www.s390.ibm.com/library

and there will be detailed discussion of exactly what's there in future issues of *RACF Update*. In the meantime, don't forget that the OS/390 implementation of RACF is now part of the SecureWay Security Server for OS/390, and the RACF name is slowly disappearing.

RACF users often need to look at ACF2 and Top Secret manuals. Surprisingly enough, Top Secret manuals are included in the IBM VSE Collection, and can be found by using the *Search Titles* feature.

Computer Associates offers manuals on-line in Adobe Acrobat format for both products from its Support site, at

http://support.cai.com

Note that manuals aren't currently provided for certain implementations, most notably VM.

In the *Support by Product* section of the page, select CA-ACF2 or CA-Top Secret from the selection list. In the *Technical Information by Product* section, click on the implementation (operating system or database) of the product you're interested in. In the *General Technical Information* section, click on *Manuals*.

You'll now see a complete list of manuals. In some cases, multiple lists will appear, one for each of the currently supported versions of the product. Clicking on a manual title will download the complete manual before displaying it with the Adobe Acrobat. A free reader can be installed from

http://www.adobe.com/products/acrobat/readstep.html

© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

These manuals aren't small (for example, the *ACF2 Administrator Guide* is 4MB), so how long you wait will depend on your Internet access. If you plan to use the same manual even occasionally, a download may be a better idea. For Microsoft Internet Explorer, right mouse click the manual and select *Save Target As* from the menu that appears.

TECHCRAWLER

New (to me) at

http://www.techcrawler.com

TechCrawler is a computing portal that knows how to spell Mainframe. It divides the world into:

- Hardware and systems
- IT management
- Networking and telecommunications
- Software development.

One section of *IT Management* is *Security*, and *Security* is further sub-divided into:

- Vendors – 22
- Associations – 5
- Research – 4
- News – 10
- Resources – 4.

The number following each category is the current number of links listed. If the site is as new as I think it is, the number of categories and links is likely to grow in the months ahead.

In *Resources*, you'll find *AspEncrypt Crypto 101*, which leads to a Web page on the AspEncrypt product. At the bottom of this page,

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

you'll find a link to Crypto 101. Follow that link to find an easy-to-read on-line book with six short chapters covering the basics of cryptography. If you can't be bothered navigating, the direct URL is:

http://www.aspencrypt.com/crypto101.html

Search

In the middle of any TechCrawler page, you'll find a Search box that allows you to search just the section you're in, or the entire site. There are also options to search all of parent company EarthWeb's sites, as well as the entire Internet.

A search for RACF across all of TechCrawler returned 547 matching pages from 80 different sources. Listed first, with 99% confidence level, was the IBM search page for *RACF for VM* on-line manuals. The second, at 98% confidence, was Computer Associates' product information page for the RACF option of Unicenter TNG. Next up came:

3 Eric Loriaux's System/390 home page

4 An Amdahl security management page

5 A Counterpane list of sensors they support

6 IBM security overview page

7 StorageTek's Library Station software.

Each entry has two additional options. You can list all the other search results from the same source. Or you can *monitor* the page. You can even monitor the top ten search results in a single mouse click.

Monitoring notifies you when a given Web page changes, but it does require that you create a (free) log-in ID and password with TechCrawler. Optionally, a cookie can be used to save you repeatedly typing in your ID and password.

© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

CISSP

If you've heard about the CISSP, but aren't quite sure what it is, why not go to the source – the organization that controls it? The Certified Information Systems Security Practitioner (CISSP) designation can be used legally only by people who have been certified by the International Information Systems Security Certification Consortium. This is quite a mouthful for an organization name, but they've somehow managed to figure out a clever acronym: $(ISC)^2$. The somewhat mathematically flawed concept is that if you take the square of ISC, you get IISSCC.

With that in mind, it makes sense that the home page is at

http://isc2.org

And the site is kept current. When I last checked, it had been updated less than two hours before I looked at it.

This site has lots of great information resources, but if you're just looking for the CISSP Examination Study Guide, you'll find a link to it on the home page near the top on the left side. Unfortunately, however, it's not quite that easy. Although the guide is free, you must fill out an electronic form to get the URL where the guide can be downloaded. And because it's a security organization, the electronic form is SSL-secured with 128-bit encryption.

Further down the page, below the electronic form, there's a list of some of the major references used to create the questions on the exam, including a two-volume set published this year specifically for the CISSP, though not published or endorsed by ISC^2.

Finally, there's an additional list of books at the bottom of the page that are described as being part of the ISC^2 Reference Library. Unlike the previous set of references, no links are provided to on-line sources where you can purchase the books.

From the ISC^2 home page, the *CISSP Examination* link gets you to a page with links to detailed information on exams:

- Locations and dates

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

- Fees (about US$450)
- Exam overview
- Applicant requirements
- Registration forms.

But note that passing the exam isn't the end of it. Every three years, 120 Continuing Professional Education (CPE) credits are required to maintain CISSP certification.

CBK

If you spend any time at all on this site, you're likely to run into the CBK acronym. It stands for Common Body of Knowledge, which refers to the scope of subject areas that the CISSP exam is intended to test.

The *CBK Review Seminar* link on the ISC^2 home page provides details on:

- Locations and dates
- Fees
- Registration forms.

Note that the seminar fees include the examination fee, presumably meaning that you would do the exam at the end of the review seminar, although that's not clear from the information on the site.

Finally, note that the registration forms for both the exam and seminars are currently available only in hard copy. There are plans to automate the registration process.

IS LIBRARY

If you haven't looked at Xephon's own Web site recently, you may not be aware of the new IS Library. To get there directly, go to

http://www.xephon.com/is_library.html

© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

You'll find more than 300 articles listed, almost half of which are available free. All are extracted from published Xephon consulting reports. The free ones can be read on-line or downloaded without so much as a prompt for your subscriber ID and password. All are in Adobe Acrobat format. Details on obtaining the free Adobe reader are included near the end of *Manuals* section above.

You'll find 'Integrating RACF and Distributed Security Systems' and 'Managing the OS/390 Security Server (RACF) with Tivoli' in the *New Technologies and Applications* section, 'An Introduction to CA-ACF2' under *System/390*, and 'Authorization Checking for RACF and AIX' as *Other Systems*. Of these, only the ACF2 article is not available for on-line viewing.

There are also a significant number of articles on security, scattered amongst the sections. To find them quickly, use your Web browser's search function, specifying 'secur' as the search string. For example, in Microsoft Internet Explorer, hit Ctrl-F or select Edit from the Menu bar, then Find from the drop-down menu, type the string, and hit the Find Next button.

Because this Web site is frames-based, you must move to the frame before doing the Find. An easy way to do this is to select some text with the mouse near the top of the right side of the page: position the mouse, hold down the left mouse button and move the mouse a few characters horizontally. Then do the Find.

Search

Another new feature of the Xephon site at

http://www.xephon.com

is the Search function, located in the red sidebar on the left of the screen. Because this is a frames site, the red sidebar, and therefore the Search function, follow you wherever you go on the site.

The search looks through the 10,000 pages of free material on the site, plus the titles and summaries of subscriber-only pages. You have a

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

choice of an All Words or Any Words keyword search. Note that if an All Words search fails, you should look carefully for a very small print 'No pages found that include all search words' message, after which you'll see the results of an Any Words search.

Jon E Pearkins
(Canada)

© Xephon 2000

Free weekly news by e-mail

Xephon has four weekly news services covering the following subject areas:

- Data centre
- Distributed systems
- Networks
- Software.

Each week, subscribers receive, by e-mail, a short news bulletin consisting of a list of items; each item has a link to the page on our Web site that contains the corresponding article. Each news bulletin also carries links to the main industry news stories of the week.

To subscribe to one or more of these news services, or review recent articles, point your browser at

http://www.xephon.com/news.htm

© 2000. Xephon UK telephone 01635 33848, fax 01635 38345. USA telephone (303) 410 9344, fax (303) 438 0290.

Contributing to *RACF Update*

In addition to *RACF Update*, the Xephon family of *Update* publications now includes *CICS Update*, *MVS Update*, *TCP/SNA Update*, *VSAM Update*, *DB2 Update*, *AIX Update*, *Domino Update*, *MQ Update*, *NT Update*, *Oracle Update*, *SQL Server Update*, and *TSO/ISPF Update*. Although the articles published are of a very high standard, the vast majority are not written by professional writers, and we rely heavily on our readers themselves taking the time and trouble to share their experiences with others. Many have discovered that writing an article is not the daunting task that it might appear to be at first glance.

They have found that the effort needed to pass on valuable information to others is more than offset by our generous terms and conditions and the recognition they gain from their fellow professionals. Often, just a few hundred words are sufficient to describe a problem and the steps taken to solve it.

If you have ever experienced any difficulties with RACF, or made an interesting discovery, you could receive a cash payment, a free subscription to any of our *Updates*, or a credit against any of Xephon's wide range of products and services, simply by telling us all about it. For a copy of our *Notes for Contributors*, which explains the terms and conditions under which we publish articles, please write to the editor, Fiona Hewitt, at any of the addresses shown on page 2, or e-mail her at fionah@xephon.com

© 2000. Reproduction prohibited. Please inform Xephon of any infringement.

William Data Systems has now announced FTPalert Version 1.1, an OS/390 application that interfaces to FTP and enables reporting of all FTP activity, showing both successful and failed file transfers, the users' ID and IP addresses, and the transfer rates achieved.

With FTPalert, all FTP activities can be defined to RACF and other security systems as secure resources, making FTP as secure as all other mainframe services.

For further information, contact:
William Data Systems, 5 High Street, Old Oxted, Surrey, RH8 9LN, UK.
Tel (01883) 723 999
URL: http://www.willdata.com

* * *

Blockade Systems has announced a partnership with enCommerce, a provider of software and services for managing secure access to e-business portals. The partnership means Blockade's OS/390 security products for authentication, authorization, and auditing will be integrated with the enCommerce getAccess portal management software through a specialized getAccess pluggable authentication and authorization module (PAAM).

For further information, contact:
Blockade Systems, 2200 Younge Street, Number 1400, Toronto, ON, M4S 2C6, Canada.
Tel: (416) 482 8400.
URL: http://www.blockade.com

* * *

InfoExpress has announced CyberArmor Suite 1.1, a software suite to help establish enterprise personal firewalls, enabling corporations to extend policy-based security to remote users connecting from home computers.

In a separate announcement, InfoExpress has appointed Network Utilities as the sole provider of its marketing and technical support in the UK market.

For further information, contact:
InfoExpress, 425 First Street, Suite E, Los Altos, CA 94022, USA.
Tel: (650) 947 7880
URL: http://www.infoexpress.com
Network Utilities, Liberty House, 158a Ewell Road, Surbiton, Surrey, KT6 6HE, UK.
Tel: (020) 8390 9911
URL: http://www.netutils.com