23

RACF

February 2001

In this issue

update

RACF Update

System symbols in the RACF database name table

With the advent of parallel sysplex, IBM introduced the concept of system symbols. A system symbol is a variable that can be defined and set to a certain value by the system programmer in parmlib concatenation members called IEASYMxx. Some naming standards apply: a system symbol starts with an ampersand and ends with a period. A number of symbols are set automatically to a default value – for example, &SYSCLONE., &SYSNAME., &SYSPLEX., or &SYSR1. Others are left to the inspiration of the customer. Most of the symbols are static, meaning that they can take on only one substituted value for the lifetime of the IPL. However, IBM defined some dynamic symbols that can be used for date and time functions. (See *OS/390 Initialization and Tuning Reference* [SC28-1752] for further details.)

System symbols came into existence to facilitate maintenance and dataset sharing in a parallel sysplex environment. By having each machine in the configuration set its identification in a different IEASYMxx member, for instance, it is possible to share one parmlib between different instances of the operating system. For example, imagine that machine A sets the system symbol &SYSTEMS. to 'A0', and system B sets the same variable to 'B0'. In the shared parmlib, different members could be activated by referring to them as <MEMBER PREFIX>&SYSTEMS.

While system symbols can be used in a variety of places – for instance, the parmlib concatenation, started procedure JCL, and system commands – there are still some places where they are not yet implemented by OS/390 designers, although they would certainly be useful.

One such place is the RACF database name table, ICHRDSNT. This is a load module that is assembled and link-edited into SYS1.LINKLIB (or its concatenation), which is static by nature. In our design, we wanted to have a RACF database that was shared among the members of a sysplex, but not between the different sysplex configurations. If

we could add the &SYSPLEX. symbol to the dataset name we would have eliminated the need for different SYS1.LINKLIB concatenations on the different sysplex resident volumes. This would make cloning and disaster recovery a lot easier.

Even if this specific problem is not relevant to your site, it is still valuable to see the way we tackled the problem, the coding itself, and the SMP/E implementation. This article therefore includes full details of the implementation, as well as reproducing the code.

The user modifications were tested on OS/390 Version 2 Release 4, Version 2 Release 7 and Version 2 Release 8. No changes were required.

Note that in the code below, everything that could be specific to our site – such as, for instance, the job class used to assemble a program – is printed in italics.

ALTERNATIVES

Basically, we found five possible solutions to the problem, as usual all with their own drawbacks. The options are described in turn below.

The master JCL

When ICHRDSNT is not found at IPL time, the system looks for a //SYSRACF DD statement in the master JCL. Although this would have resolved our problem in an easy-to-maintain parmlib concatenation member, the side effects were too great. The number of resident data blocks of the RACF database is reduced to ten when ICHRDSNT is not used, and, what's more, it's not possible to specify a name for the back-up database. These two limitations made us reject this option.

Operator reply

When ICHRDSNT is not found during IPL and there is no //SYSRACF DD statement in the master JCL, RACF will prompt the operator for the names of the primary and back-up databases to use. Although this would theoretically have resolved our problem, there are still drawbacks. For instance, the number of resident datablocks is again

reduced to ten. We also considered it too risky to allow operators to specify a reply that could influence the security of the entire sysplex.

The SAF nucleus initialization exit ICHRTX01

There is some documentation in *OS/390 Security Server External Security Interface (RACROUTE) Macro Reference* [GC28-1922-05] that alludes to the SAF router exits ICHRTX00 and ICHRTX01. ICHRTX01 is supposed to receive control immediately after SAF initialization. It could be that at that point in time RACF has not opened the databases, in which case this exit point could be used to translate the system symbols to their values. However, the documentation is rather vague, and we decided to keep this open as an option in case the other alternatives proved unfruitful.

Automated operator switch

Another solution would have been to start RACF with a minimum database and to switch over to the real one with 'RVARY' operator commands – containing &SYSPLEX. – as soon as the automated operator was up and running. Since RACF is used before the automated operator is active, this would have meant keeping certain RACF profiles up-to-date in both the mini and the real databases. This was considered too 'ugly', and too cumbersome to maintain.

System NIP modification

We investigated the possibility of somehow changing the logic of the nucleus initialization program, and finally selected this as our solution. It is described in the remainder of this article.

REVERSE ENGINEERING

ICHRDSNT is not the table that RACF will be using during normal operation. Rather, it is a place where RACF will look up some customer-specific values – such as the names of the databases – before building a control block in storage: the DSDT or Data Set Descriptor Table. According to the description of the DSDT in *OS/390 Security Server (RACF) Data Areas* [SY27-2640], the module responsible for

the construction of this control block is ICHSEC00. It seems therefore logical to look for a load or link SVC in this module. The designers of RACF often split out functionality between different modules, with, for example, one for the logic of the specification of the databases (operator prompt or ICHRDSNT or //SYSRACF DD statement in the master JCL). It came as no surprise that no trace of ICHRDSNT could be found in ICHSEC00. Link and load SVCs normally have the name of the entry point of the module they are going to bring in storage in them.

A quick and dirty scan in SYS1.LINKLIB on ICHRDSNT revealed that the loadmodule ICHSEC07 contained coding that could well be what we were looking for. ISPF browse gave us the displacement of 'ICHRDSNT' in the loadmodule. AMBLIST provided us with the name of the module inside ICHSEC07: ICHSEC08. The next step was to disassemble this module to check that our assumptions about its functionality were correct. The high-level Assembler toolkit was used to produce a rudimentary form of the program that was later assembled again to have the displacements in a listing. The job used for the disassembly/assembly is shown below:

```
//IBZZEX4X JOB (JAN),'JAN DE DECKER',CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID,
//             REGION=ØM,COND=(Ø,NE)
//*
//* DISASSEMBLY OF A MODULE
//*
//SØ       EXEC PGM=ASMDASM,PARM='COPYRIGHTOK'
//STEPLIB  DD DSN=ASMT.V1R2MØ.SASMMOD2,DISP=SHR
//SYSLIB   DD DSN=SYS1.LINKLIB,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSPUNCH DD DSN=&&ASM,DISP=(,PASS),UNIT=VIO,
//             SPACE=(CYL,(1,1),
//             DCB=(BLKSIZE=616Ø,LRECL=8Ø,RECFM=FB)
//SYSIN    DD *
ICHSECØ7 ICHSECØ8
/*
//*
//* ASSEMBLY
//*
//S1       EXEC PGM=ASMA9Ø,
//             PARM='NORENT,NODECK,NOOBJECT'
//SYSLIB   DD DISP=SHR,DSN=SYS1.MACLIB
//         DD DISP=SHR,DSN=SYS1.MODGEN
```

```
//         DD DISP=SHR,DSN=ASMT.SASMMAC2
//SYSUT1   DD UNIT=VIO,SPACE=(CYL,(1,1))
//SYSUT2   DD UNIT=VIO,SPACE=(CYL,(1,1))
//SYSUT3   DD UNIT=VIO,SPACE=(CYL,(1,1))
//SYSPRINT DD SYSOUT=*
//SYSIN    DD DSN=&&ASM,DISP=(OLD,DELETE)
//SYSPUNCH DD DUMMY,SYSOUT=*
```

The resulting code showed that ICHSEC08 was indeed what we were looking for. By wrapping a program around it, the logic of NIP regarding the RACF database names could be altered.

ICHSECXX, THE PROGRAM WRAPPED AROUND ICHSEC07

Once the critical module was identified, there were various ways in which we could proceed. We decided to do the following:

- Replace the entry point of ICHSEC08 with our own (ICHSECXX).

- Preload ICHRDSNT.

- Scan the database names for system symbols, and, if found, replace them with their substituted values for this particular system.

- Restore all registers as they were before our program executed.

- Transfer control to the old entry point.

ICHRDSNT

The design could work only if ICHRDSNT was not reloaded again by ICHSEC08. To prevent this, the linkage-editor was used to set the loadmodule as reentrant and reusable. This change must be reflected in SMP/E, which was done by the UCLIN below. Since this merely writes information in the CSI, a real linkage-edit was also needed to effectively change the characteristics of the module. If system symbols were going to be used, ICHRDSNT needed changing anyway, so the two steps were combined into one piece of JCL.

In order for an ampersand to be recognized as such, Assembler requires that there is a preceding ampersand. ICHSECXX recognizes a system symbol as anything that starts with an ampersand and ends

with a point. Imagine that &SYSPLEX. is set to 'PLX1' and the names
of the RACF databases are 'PLX1.RACF.P' and PLX1.RACF.B'; the
following could be coded in ICHRDSNT:

```
RACFPRIM DC CL44'&&SYSPLEX..RACF.P'
RACFBACK DC CL44'&&SYSPLEX..RACF.B'
```

The double ampersand counts as just one character. The two points,
however, could make the name with symbols longer than the actual
name. If this is the case, ICHSECXX could be adapted to load the
names from another module before overwriting the contents of
ICHRDSNT.

TESTS

During the development of ICHSECXX a built-in dummy ICHRDSNT
was used (label TESTDATA). The coding is left unchanged in the
sample below, but the assembly depends on the macro variable
COMPILE. If this is set to DEBUG, the internal table is used and the
program abends with register two pointing to the table after substitution.
This helped while writing the code using the system symbol interface
(ASASYMBM).

Real testing happened on a system programmer's test machine.
Besides checking whether or not everything behaved as expected, we
also tested for wrongly coded database name tables. As predicted, the
processing was exactly the same, regardless of wrongly coded symbols.
If the database is not found by the dynamic allocation SVC, for
instance, RACF prompts the operator for manual input.

SMP/E IMPLEMENTATION

A user modification is a method to make a change to vendor-supplied
software elements like modules, macros, sources, and so on, in a way
that SMP/E knows about the modification and the interactions that
possibly exist between the usermod and other installed elements.
There are several advantages to installing changes with SMP/E. Most
shops implement changes to elements that are known to
SMP/E as a usermod, but fail to do so for others. JES2 exits are a

notorious example of operating system coding that is often implemented without SMP/E assistance. The reason for this is that the manuals are not exactly clear about the way to accomplish this. For the more adventurous reader, I recommend the following material:

- *Software Delivery. Standard Packaging Rules for MVS-Based Products* (SC23-3695).

- *OS/390 SMP/E User's Guide* (SC28-1740).

At our shop, we implement all changes that become 'part' of the system as a usermod. Therefore, we package them all together in our own function (FMID) and just install this as part of a system upgrade. For this article, I separated the usermods from our function so that they become 'normal'sysmods on known functions.

For our program to work, we needed to do the following:

- Introduce three macros to SMP/E.

- Tell SMP/E that the linkage-editor attributes of ICHSEC07 and ICHRDSNT are changed.

- Introduce a new source (ICHSECXX).

- Re-link the original load module.

All of this was done in the one JCL below. To emulate a delivered usermod, we first copied the sources into a VIO temporary dataset. The target of the source was kept in the dataset JEDPLX1.JEDSRC, the DLIB version in JEDPLX1.AJEDSRC. We also needed a DLIB for the macros and the link-edited module. We used JEDPLX1.AJEDMAC and JEDPLX1.AJEDLINK. These datasets should be pre-allocated before the job is run. The targets for the macros was SYS1.MACLIB.

The job is coded to be re-executable. This is true if you remove the SMP/E REJECT and RESTORE statements for a first-time installation. All steps should produce a return code of zero except for S3, where 4 is expected accompanied by the message IEW2454W for the ICHSEC07 module.

```
//IBZZEX4X JOB (JAN),'JAN DE DECKER',CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID,
```

9

```
//              REGION=ØM
//*
//* PREPARATION: COPY THE SOURCES TO A TEMPORARY VIO DATASET
//*
//SØ        EXEC PGM=IEBUPDTE,PARM='NEW'
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
./ ADD NAME=ICHSECXX
*
* REGISTER EQUATES
*
RØ        EQU   Ø
R1        EQU   1
R2        EQU   2
R3        EQU   3
R4        EQU   4
R5        EQU   5
R6        EQU   6
R7        EQU   7
R8        EQU   8
R9        EQU   9
RA        EQU   1Ø
RB        EQU   11
RC        EQU   12
RD        EQU   13
RE        EQU   14
RF        EQU   15
          EJECT
          TITLE '** ICHSECXX: RACF NIP WRAPPER TO ALLOW SYSTEM SYMBOLS IX
                  N ICHRDSNT **'
*----------------------------------------------------------------------
*--JAN-DE-DECKER-JED:SP-NV-TIMMERHOUTKAAI-1-1ØØØ BRUSSEL-Ø75/52.65.11--
*----------------------------------------------------------------------
*
* NAME:          ICHSECXX
*
* PURPOSE:       SYSTEMS SYMBOLS CAN BE USED IN A LOT OF PLACES
*                BUT - AS FAR AS OS/39Ø V2R8 - NOT IN THE RACF
*                DATABASE NAME TABLE WHICH IS GENERATED FROM A
*                CUSTOMER MAINTAINED MODULE ICHRDSNT. TO ALLOW FOR
*                GREATER FLEXIBILITY AND TO ENHANCE THE NAMING
*                CONVENTIONS FOR SYSTEM DATASETS THIS SOLUTION WAS
*                DESIGNED. BASICALLY IT WRAPS AROUND THE RACF
*                MODULE THAT LOADS ICHRDSNT (ICHSECØ8) WHICH IS
*                CONTAINED IN THE ICHSECØ7 LOADMODULE. THE ACTUAL
*                CREATION OF THE IN-STORAGE DATABASE NAME TABLE IS
*                DONE BY YET ANOTHER MODULE (ICHSECØØ).
*                THIS PROGRAM REPLACES THE MAIN ENTRY POINT OF
```

```
*                      ICHSECØ7. IT LOADS ICHRDSNT ITSELF AND DOES A
*                      SUBSTITUTION FOR EVERY SYSTEM SYMBOL IT FINDS IN
*                      THE DATASETNAMES FOR THE RACF PRIMARY AND
*                      SECONDARY DATABASES. AFTERWARDS IT TRANSFERS
*                      CONTROL TO THE ORIGINAL MAIN ENTRY POINT.
*                      THIS IMPLIES THAT THE SECURITY OFFICER CAN USE
*                      SYSTEM SYMBOLS WHILE CREATING ICHRDSNT.
*                      SINCE THIS ALL HAPPENS DURING THE NUCLEUS
*                      INITIALIZATION PROGRAM (NIP) GREAT CARE MUST BE
*                      TAKEN WHEN THE SYSTEM IS UPGRADED.
*
* OS UPGRADE:          1. CHECK THE LAYOUT OF ICHRDSNT. IF THERE IS A
*                         DIFFERENCE WITH THE LAYOUT IN THE DSNT MACRO
*                         BELOW, ACTION SHOULD BE TAKEN.
*
*                      2. CHANGE THE LINKAGE EDIT CHARACTERISTICS OF
*                         ICHRDSNT TO REUSABLE WITH SMP/E, THEREBY
*                         COPYING ALL OTHER INFORMATION FROM THE IBM
*                         DELIVERED JCLIN.
*
*                      3. MAKE THIS MODULE (ICHSECXX) KNOWN TO SMP/E.
*
*                      4. CHANGE THE LINKAGE EDIT INSTREAM OF ICHSECØ7
*                         TO INCLUDE ICHSECXX AND TO MAKE IT ITS MAIN
*                         ENTRY POINT.
*
*                      THIS SEEMS WORSE THAN IT IS. ALL CAN BE DONE BY
*                      ONE UCLIN JOB THAT IS UNLIKELY TO CHANGE IN THE
*                      FUTURE.
*
* PARAMETERS:          IN ITSELF NONE BUT PASSED PARAMETERS MUST GO
*                      THROUGH TO THE ORIGINAL ENTRY POINT
*
* SYSTEM:              DEVELOPED AND TESTED ON OS/39Ø V2R6
*
* LINK:                TOGETHER WITH ICHSECØ7
*
* INTERFACES:          LOAD MACRO
*                      LINK MACRO
*                      ASASYMBM MODULE
*
* AUTHOR:              JAN
*
* SAMPLE:              N/A
*
* TEST:                THE MODULE IS WRITTEN AS A CONDITIONAL ASSEMBLY.
*                      BY ADAPTING THE VARIABLE &&COMPILE AT THE START
```

11

```
*                       OF THE PROGRAM, A VERSION IS GENERATED THAT WILL
*                       TRY TO DO THE REAL THING (&&COMPILE SETC NODEBUG)
*                       OR A VERSION THAT ASSEMBLES A PRIVATE COPY OF
*                       ICHRDSNT INTO ITS MAIN CODING.
*
* NOTES:                THE ASSEMBLER UNFORTUNATELY USES THE SAME
*                       QUALIFIER FOR VARIABLES AS THE SYSTEM SYMBOLS,
*                       NAMELY AN AMPERSAND. TO LET IT TELL THE
*                       DIFFERENCE BETWEEN ONE HAS TO SPECIFY A DOUBLE
*                       AMPERSAND.
*
* MODIFICATION LIST:
*
*-----------------------------------------------------------------------
*---FACSIMILE-Ø2/218.Ø9.69-E-MAIL-JAN@JEDSP.COM-HTTP://WWW.JEDSP.COM---
*-----------------------------------------------------------------------
         EJECT
ICHSECXX CSECT
ICHSECXX AMODE 31
ICHSECXX RMODE 24
&COMPILE SETC  'NODEBUG'
         PRINT GEN
         BAKR  RE,Ø                  SAVE REGISTERS
         LR    RC,RF                 RC -> CSECT
         USING ICHSECXX,RC           RC ADDRESSES CSECT
         LA    RD,SAVEAREA           RD -> OUR SAVEAREA
         EYECATCH
         AMODE31
         EJECT
*
* START OF PROCESSING
*
         AIF   ('&COMPILE' EQ 'DEBUG').LØØØØ
         LOAD  EP=ICHRDSNT           LOAD DATABASE NAME TABLE
         LTR   RF,RF                 LOAD OK?
         BZ    LØØØØ                 YES -> CONTINUE
         WTO   'ICHSECXX ØØ COULD NOT LOAD ICHRDSNT TABLE'
         B     THE_END
LØØØØ    DS    ØH
         LR    R2,RØ                 R2 -> MODULE
         AGO   .LØØ1Ø
.LØØØØ   ANOP
         LA    R2,TESTDATA           /* DEBUG                       */
.LØØ1Ø   ANOP
         USING DSNT,R2               R2 ADDRESSES THE DSNT
         XR    R3,R3                 R3 = Ø
         IC    R3,DSNTNUM            R3 = #(DATABASE ENTRIES)
         LA    R2,DSNTPRIM           R2 -> FIRST ENTRY
```

```
        DROP  R2                       DROP DSNT HEADER ADDRESSABILITY
        USING DSNTPRIM,R2              R2 ADDRESSES THE ENTRY
LØØ1Ø   DS    ØH
        LA    R4,DSNTPRIM              R4 -> PRIMARY
        BAL   RE,TRANSSYM              GO TRANSLATE
        LA    R4,DSNTSEC               R4 -> BACKUP ENTRY
        BAL   RE,TRANSSYM              GO TRANSLATE
        LA    R2,DSNTELEN(R2)          R2 -> NEXT ENTRY
        BCT   R3,LØØ1Ø                 LOOP FOR ALL ENTRIES
        AIF   ('&COMPILE' NE 'DEBUG').LØØ2Ø
        LA    R2,TESTDATA
        ABEND 666,DUMP
.LØØ2Ø  ANOP
        EJECT
*
* END OF PROCESSING
*
THE_END DS    ØH                       MY ONLY FRIEND, THE END
        WTO   'ICHSECXX SUBSTITUTION FINISHED'
        L     RF,=V(ICHSECØ7)
        EREG  RØ,RD
        BALR  RE,RF
        PR    .                        RETURN TO CALLER
        EJECT
*
* TRANSSYM PROCEDURE
* EXPECTS R4 TO POINT TO A DATASE NAME OF A RACF DATABASE
*
TRANSSYM DS   ØH
        BAKR  RE,Ø                     SAVE ALL REGISTERS
        MVI   DSNAME,C' '              BLANK OUT WORK ZONE DSNAME
        MVC   DSNAME+1(L'DSNAME-1),DSNAME
        LA    R3,L'DSNTPRIM            R3 = MAXIMUM LENGTH
        LR    R6,R4                    R6 -> START ICHRDSNT NAME
        LA    R5,DSNAME                R5 -> DSNAME WORK ZONE
LØØ2Ø   DS    ØH
        CLI   Ø(R4),C' '              BLANK (END OF DSNAME)?
        BE    LØØ6Ø                    YES -> GO COPY WORK TO ORIGINAL
        CLI   Ø(R4),C'&&'             AMPERSAND, START OF A SYMBOL?
        BNE   LØØ5Ø                    NO --> GO CHECK NEXT ONE
        EJECT
*
* THE START OF A SYMBOL IS FOUND AND R4 IS POINTING TO IT
*
        MVI   SYMBOL,C' '              BLANK OUT SYMBOL
        MVC   SYMBOL+1(L'SYMBOL-1),SYMBOL
        LA    R2,SYMBOL                R2 -> SYMBOL ZONE
        XR    R7,R7                    R7 WILL KEEP LENGTH SYMBOL
```

13

```
LØØ3Ø    DS    ØH
         MVC   Ø(1,R2),Ø(R4)           MOVE SYMBOL BYTE
         LA    R4,1(R4)               R4 -> NEXT ORIGINAL BYTE
         LA    R2,1(R2)               R2 -> NEXT FREE SYMBOL BYTE
         LA    R7,1(R7)               ++ L(SYMBOL)
         BCTR  R3,Ø                   -- L(ORIGINAL)
         CLI   Ø(R4),C'.'             END OF SYMBOL IN ORIGINAL?
         BNE   LØØ3Ø                  NO --> GO COPY NEXT BYTE
         LA    R4,1(R4)               R4 -> NEXT ORIGINAL BYTE
*                                     AFTER THE POINT WHICH IS
*                                     IGNORED
         BCTR  R3,Ø                   -- L(ORIGINAL) |POINT|
*
* RESOLUTION OF THE SYMBOL
*
         MVC   L_SUBST,=AL4(L'SUBST)  RESET (FILLED IN BY ASASYMBM)
         LA    R8,MYSYMBP             R8 -> PARAMETER LIST
         LA    R9,SUBST              R9 -> SUBSTITUTION FIELD
         LA    RA,L_SUBST            RA -> L(SUBSTITUTION FIELD)
         LA    RB,RETCODE           RB -> RETURN CODE FIELD
         USING SYMBP,R8              R8 ADDRESSES THE PARAMETER LIST
         XC    SYMBP(SYMBP_LEN),SYMBP SET PARAMETER LIST TO LOW VALUES
         MVC   SYMBPPATTERN@,A_SYMBOL SET -> TO SYMBOL
         ST    R7,SYMBPPATTERNLENGTH  SET L(SYMBOL)
*                                     SET -> TO SUBSTITUTION FIELD
         ST    R9,SYMBPTARGET@
*                                     SET -> L(SUBSTITUTION FIELD)
         ST    RA,SYMBPTARGETLENGTH@
*                                     SET -> RETURN CODE
         ST    RB,SYMBPRETURNCODE@
         DROP  R8                     FORGET THE PARAMETER LIST
         LINK  EP=ASASYMBM,           LINK TO SYMBOL RESOLUTION      X
               MF=(E,MYSYMBP)         WITH OUR PARAMETER LIST
         CLC   RETCODE,=F'Ø'          ALL WELL?
         BZ    LØØ4Ø                  YES -> CONTINUE
         AIF   ('&COMPILE' NE 'DEBUG').LØØ3Ø
         L     R2,RETCODE
         LA    R3,SYMBOL
         ABEND 999,DUMP
         AGO   .LØØ4Ø
.LØØ3Ø   ANOP
         WTO   'ICHSECXX Ø1 SYMBOL NOT RESOLVED'
         B     THE_END                RETURN TO CALLER
.LØØ4Ø   ANOP
*
* THE SYMBOL IS SUBSTITUTED, ADAPT THE DSNAME FIELD
*
LØØ4Ø    DS    ØH
         L     R2,L_SUBST             R2 = L(SUBSTITUTED SYMBOL)
```

```
        BCTR  R2,Ø                      --R2 |FOR EX INSTRUCTION|
        EX    R2,MVCSUBST               MOVE TO WORK ZONE
        AR    R5,R2                     ADJUST POINTER IN WORK ZONE
        LA    R5,1(R5)                  IN TWO STEPS
        LTR   R3,R3                     R3 AT END OF INPUT FIELD?
        BNE   LØØ2Ø                     NO --> CONTINUE
        B     LØØ6Ø                     YES -> GO LEAVE
        EJECT
LØØ5Ø   DS    ØH
        MVC   Ø(1,R5),Ø(R4)             MOVE BYTE TO WORK ZONE DSNAME
        LA    R4,1(R4)                  ++(ORIGIN DSNAME POINTER)
        LA    R5,1(R5)                  ++ WORK ZONE DSNAME POINTER
        BCT   R3,LØØ2Ø                  LOOP THROUGH ALL CHARACTERS
LØØ6Ø   DS    ØH
        MVC   Ø(L'DSNTPRIM,R6),DSNAME COPY WORK TO ORIGINAL
        PR    .                         RESTORE AND RETURN
        EJECT
*
* DATA AREA'S
*
SAVEAREA DS   F                         SAVEAREA FOR CALLED PROGRAMS
        DC    C'F1SA'                   WE USE THE LINKAGE STACK
        DS    16F
A_SYMBOL DC   AL4(SYMBOL)               A(SYMBOL)
SYMBOL  DS    CL1Ø                      L(&&) + L(SYMBOL) + L(.)
DSNAME  DS    CL(DSNTDBLN)              NAME WORK ZONE
L_SUBST DS    ØF                        KEEP WITH NEXT LINE
        DC    AL4(L'SUBST)              L(SUBSTITUTION FIELD)
SUBST   DS    CL8                       SUBSTITUTION FIELD
RETCODE DS    F                         RETURN CODE ASASYMBP
*
MYSYMBP DS    ØF                        KEEP TOGETHER WITH NEXT LINE!
        DS    CL(SYMBP_LEN)             PARAMETER LIST ASASYMBP
        EJECT
*
* EXECUTE TARGETS
*
MVCSUBST MVC  Ø(Ø,R5),SUBST             SUBSTITUTED SYMBOL TO WORK ZONE
        EJECT
        AIF   ('&COMPILE' NE 'DEBUG').LØØ5Ø
*
* TESTDATA
*
TESTDATA DS   ØF
        DC    AL1(2)
        DC    CL44'&&SYSNAME..&&SYSPLEX..PRIMARY'
        DC    CL44'&&SYSNAME..&&SYSR1..SECONDARY'
        DC    X'FF'
```

15

```
          DC    X'FF'
          DC    CL44'&&SYSNAME..&&SYSR1..&&HOSTID..PRIMARY'
          DC    CL44'SE.DATA.BASE.RACF.SECONDARY'
          DC    X'FF'
          DC    X'FF'
          EJECT
.LØØ5Ø    ANOP
*
* LITERAL POOL
*
          LTORG
          EJECT
*
* OS/39Ø PROVIDED DUMMY SECTIONS
*
          PRINT GEN
          ASASYMBP DSECT=YES
          EJECT
*
* OUR NEW DUMMY SECTIONS
*
          PRINT GEN
          DSNT
*
          END
./ ADD NAME=EYECATCH
*
* EYECATCHER MACRO
*
          MACRO
&LABEL    EYECATCH
          B     L&SYSNDX               SKIP AROUND DC'S
          DC    C'JAN DE DECKER --- JED:SP NV '
          DC    C'MODULE: '
          DC    CL8'&SYSECT'           MODULE NAME
          DC    C' ASM DATE: '
          DC    CL8'&SYSDATE'          DATE
          DC    C' ASM TIME: '
          DC    CL8'&SYSTIME'          TIME
L&SYSNDX  DS    ØH
          MEND
./ ADD NAME=AMODE31
*
* AMODE 31 MACRO
*
          MACRO
*
* THIS MACRO SETS THE AMODE TO 31
```

```
* THE CONTENT OF REGISTER 1 IS DESTROYED
*
&LABEL   AMODE31
         LA    R1,L&SYSNDX              R1 -> BRANCH ADDRESS
         O     R1,A&SYSNDX             SET FIRST BIT TO ON
         BSM   RØ,R1                    BRANCH AND SET MODE
A&SYSNDX DS    ØF                       BITMASK ALIGNMENT
         DC    X'8ØØØØØØØ'              BITMASK
L&SYSNDX DS    ØH
         MEND
./ ADD NAME=DSNT
*
* DSNT MAPPING DSECT
*
         MACRO
&NAME    DSNT
DSNT     DSECT
DSNTNUM  DS    AL1                     NUMBER OF DATABASES
DSNTPRIM DS    CL44                    PRIMARY NAME
DSNTDBLN EQU   *-DSNTPRIM              LENGTH OF DATABASE NAME
DSNTSEC  DS    CL(DSNTDBLN)            SECONDARY NAME
DSNTFLG1 DS    AL1                     FLAG BYTE
DSNTFLG2 DS    X                       FLAG BYTE
DSNTELEN EQU   *-DSNTPRIM              LENGTH OF AN ENTRY
         MEND
/*
//SYSUT2   DD  DSN=&&SRC,DISP=(NEW,PASS),
//             DCB=(DSORG=PO,LRECL=8Ø,BLKSIZE=661Ø),
//             UNIT=VIO,SPACE=(CYL,(1,1,1))
//*
//* COPY THE SOURCES TO THE DLIBS
//*
//S1       EXEC PGM=IEBCOPY
//SRC      DD  DISP=(OLD,PASS),DSN=&&SRC
//AMACLIB  DD  DISP=OLD,DSN=SPBPLX1.V2R7.ASPBMAC
//ASRCLIB  DD  DISP=OLD,DSN=SPBPLX1.V2R7.ASPBSRC
//SYSPRINT DD  SYSOUT=*
//SYSIN    DD  *
 COPY INDD=SRC,OUTDD=ASRCLIB
 SELECT M=(ICHSECXX)
 COPY INDD=SRC,OUTDD=AMACLIB
 SELECT M=(AMODE31,EYECATCH,DSNT)
/*
//*
//* PREPARATION: CREATE AN OBJECT DECK IN A TEMPORARY DATASET
//*
//S2       EXEC PGM=ASMA9Ø,PARM='OBJECT,NODECK'
//SYSLIB   DD  DSN=SYS1.MACLIB,DISP=SHR
//         DD  DSN=SYS1.MODGEN,DISP=SHR
```

```
//SYSUT1   DD  UNIT=VIO,SPACE=(17ØØ,(6ØØ,1ØØ))
//SYSUT2   DD  UNIT=VIO,SPACE=(17ØØ,(6ØØ,1ØØ))
//SYSUT3   DD  UNIT=VIO,SPACE=(17ØØ,(6ØØ,1ØØ))
//SYSPRINT DD  SYSOUT=*
//SYSPUNCH DD  DUMMY,SYSOUT=*
//SYSLIN   DD  DSN=&&OBJ(ICHSECXX),DISP=(NEW,PASS),
//             DCB=(DSORG=PO,LRECL=8Ø,BLKSIZE=616Ø),
//             UNIT=VIO,SPACE=(CYL,(1,1,1))
//SYSIN    DD  DISP=(OLD,PASS),DSN=&&SRC(ICHSECXX)
//*
//* PREPARATION: LINK THE OBJECT INTO THE DLIB
//*             EXPECT CONDIOTION CODE 4 (IEW2454W FOR ICHSECØ7)
//*
//S3       EXEC PGM=IEWL,PARM='NCAL'
//SYSLMOD  DD DISP=OLD,DSN=SPBPLX1.V2R7.ASPBLINK
//SYSPRINT DD SYSOUT=*
//SYSUT1   DD  UNIT=VIO,SPACE=(CYL,(1,1))
//SYSLIN   DD DISP=(OLD,PASS),DSN=&&OBJ(ICHSECXX)
//         DD *
 ENTRY ICHSECXX
 NAME ICHSECXX(R)
/*
//*
//* SMP/E STEP TO APPLY THE MACROS AND THE SOURCE
//*
//S4       EXEC PGM=GIMSMP
//SMPCSI   DD DISP=SHR,DSN=SMVS27ØS.GLOBAL.CSI
//SPBSRC   DD DISP=SHR,DSN=SPBPLX1.V2R7.SPBSRC
//ASPBSRC  DD DISP=SHR,DSN=SPBPLX1.V2R7.ASPBSRC
//ASPBLINK DD DISP=SHR,DSN=SPBPLX1.V2R7.ASPBLINK
//ASPBMAC  DD DISP=SHR,DSN=SPBPLX1.V2R7.ASPBMAC
//SYSLIB   DD DISP=SHR,DSN=SYS1.MACLIB
//MACLIB   DD DISP=SHR,DSN=SYS1.MACLIB
//SRC      DD DISP=(OLD,DELETE),DSN=&&SRC
//OBJ      DD DISP=(OLD,DELETE),DSN=&&OBJ
//SMPCNTL  DD  *
  SET BDY(MVST1ØØ) .
  UCLIN .
  REP LMOD(ICHSECØ7)
      NCAL
++LMODIN
      ENTRY    ICHSECXX
      ALIAS    ICHSECØ9
      ALIAS    ICHSEC9R
      NAME     ICHSECØ7(R)
++ENDLMODIN  .
  REP LMOD(ICHRDSNT)
      STD RENT .
```

```
        ENDUCL .
    SET BDY(MVST100).                        /* -> TARGET ZONE          */
     RESTORE S(GUMOD50                       /* RECEIVE IN GLOBAL ZONE  */
             GUMOD51                          /* AMODE31 MACRO           */
             GUMOD52                          /* DSNDT MACRO             */
             GUMOD53) .                       /* ICHSECXX SOURCE         */
    RESETRC .
    SET BDY(GLOBAL).                         /* -> GLOBAL ZONE          */
     REJECT  S(GUMOD50                       /* RECEIVE IN GLOBAL ZONE  */
             GUMOD51                          /* AMODE31 MACRO           */
             GUMOD52                          /* DSNDT MACRO             */
             GUMOD53) .                       /* ICHSECXX SOURCE         */
    RESETRC .
    SET BDY(GLOBAL).                         /* -> GLOBAL ZONE          */
     RECEIVE S(GUMOD50                       /* RECEIVE IN GLOBAL ZONE  */
             GUMOD51                          /* AMODE31 MACRO           */
             GUMOD52                          /* DSNDT MACRO             */
             GUMOD53)                         /* ICHSECXX SOURCE         */
           SYSMODS.
    SET BDY(MVST100).                        /* -> TARGET ZONE          */
     APPLY S(GUMOD50                         /* EYECATCH MACRO          */
           GUMOD51                            /* AMODE31 MACRO           */
           GUMOD52                            /* DSNDT MACRO             */
           GUMOD53)                           /* ICHSECXX SOURCE         */
                  .
/*
//SMPPTFIN DD DATA,DLM=##
++USERMOD(GUMOD50).
++VER(Z038) FMID(HBB6606).
++MAC(EYECATCH)                              /* NAME OF NEW MACRO       */
    DISTLIB(ASPBMAC)                          /* DDNAME OF DLIB          */
    TXLIB(SRC)                                /* SOURCE                  */
    SYSLIB(MACLIB) .                          /* DDNAME OF TARGET        */
++USERMOD(GUMOD51).
++VER(Z038) FMID(HBB6606).
++MAC(AMODE31)                               /* NAME OF NEW MACRO       */
    DISTLIB(ASPBMAC)                          /* DDNAME OF DLIB          */
    TXLIB(SRC)                                /* SOURCE                  */
    SYSLIB(MACLIB).                           /* DDNAME OF TARGET        */
++USERMOD(GUMOD52).
++VER(Z038) FMID(HBB6606).
++MAC(DSNT)                                  /* NAME OF NEW MACRO       */
    DISTLIB(ASPBMAC)                          /* DDNAME OF DLIB          */
    TXLIB(SRC)                                /* SOURCE                  */
    SYSLIB(MACLIB) .                          /* DDNAME OF TARGET        */
++USERMOD(GUMOD53).
++VER(Z038) FMID(HRF2260).
++SRC(ICHSECXX)                              /* NAME OF NEW SOURCE      */
    DISTLIB(ASPBSRC)                          /* DDNAME OF DLIB          */
```

19

```
       TXLIB(SRC)                              /* DDNAME OF INPUT SOURCE    */
       DISTMOD(ASPBOBJ) .                      /* DLIB FOR OBJECT           */
++JCLIN .
//*
//* JCLIN TO FORCE COPY FROM THE DLIB TO THE TARGET LIBRARY
//* FOR THE ASSEMBLER SOURCE
//* ASSEMBLY AND LINK IS DONE AUTOMATICALLY BY SMP/E
//*
//SMPESØ   EXEC PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
//SPBSRC   DD DISP=SHR,DSN=SPBPLX1.V2R7.SPBSRC
//ASPBSRC  DD DISP=SHR,DSN=SPBPLX1.V2R7.ASPBSRC
//SYSIN    DD *
 COPY INDD=ASPBSRC,OUTDD=SPBSRC TYPE=SRC
 SELECT M=(ICHSECXX)
/*
++MOD(ICHSECXX)                               /* NAME OF NEW MODULE        */
     DISTLIB(ASPLINK)                         /* DDNAME OF DLIB            */
     TXLIB(OBJ)                               /* DDNAME OF INPUT OBJECT    */
     LMOD(ICHSECØ7) .                         /* RELATED LOADMODULE        */
##
//
```

SYSTEM UPGRADE CHECKLIST

In the event of a system upgrade:

• Check the layout of ICHRDSNT. If necessary adapt the macro DSNT – instream in the SMP/E job above – to reflect the modifications.

• Check the SMP/E user modifications and adapt changes to the FMID or the DISTLIB.

• List the linkage-edit attributes of ICHRDSNT and ICHSEC07 and, if necessary, adapt the usermods.

• Reinstall the usermods.

CONCLUSION

It is possible to use system symbols in the RACF database name table if you accept that the NIP modules are changed. By using SMP/E for the full implementation, and by producing a well-documented upgrade checklist, the risks are kept to a minimum. At some time, there will be

an IPL for the upgraded system in a test environment where it will become immediately clear whether something is wrong with the names of the RACF databases.

I predict that IBM will allow the usage of system symbols for more and more variables in the near future. Meanwhile, the solution proposed here could be used to decrease maintenance and synchronization efforts between RACF databases on different images of the operating system.

Jan de Decker
JED:SP NV (Belgium)   © Xephon 2001

Need help with a RACF problem or project?

Do you need help with a RACF problem or project? Maybe we can help:

- If it's on a topic of interest to other subscribers, we'll commission an article on the subject, which we'll publish in *RACF Update*, and which we'll pay for – it won't cost you anything.

- If it's a more specialized, or more complex, problem, you can advertise your requirements (including one-off projects, freelance contracts, permanent jobs, etc) to the hundreds of RACF professionals who visit *RACF Update*'s home page every month. This service is also free of charge.

Visit the *RACF Update* Web site:

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

and follow the link to *Suggest a topic* or *Opportunities for RACF specialists*.

Confirming a COBOL transaction using RACF

The following procedure can be used to confirm a COBOL transaction, for example by a supervisor or a partner:

1   Display a CICS panel asking for the userid and password.

2   The COBOL program checks whether the userid belongs to the group of authorized userids (eg managerial group).

3   The COBOL program calls an Assembler program and passes the userid and password to it.

4   The Assembler program asks RACF whether the password passed is a correct one for the userid passed. RACROUTE REQUEST=VERIFY is used.

5   If the password is OK, a return code of 0 is passed to the COBOL routine.

6   If the password is invalid, a non-zero return code is passed to the COBOL routine.

Note that the PRINTDCB references are included in the code for testing purpose only, and can be removed if wished.

SOURCE

```
//YOUR JOB CARD
//*         BATCH TESTING ENVIRONMENT
//ASM     EXEC PGM=IEV9Ø,PARM=(NODECK,OBJECT)
//SYSLIB  DD DSN=SYS1.MACLIB,DISP=SHR
//        DD DSN=SYS1.AMODGEN,DISP=SHR
//SYSUT1  DD  DSN=&SYSUT1,SPACE=(1Ø24,(12Ø,12Ø),,,ROUND),UNIT=VIO,
//            DCB=BUFNO=1
//SYSPUNCH DD  DUMMY
//SYSPRINT DD  SYSOUT=T
//SYSLIN  DD  DSN=&OBJ,SPACE=(CYL,(2,1),,,ROUND),UNIT=VIO,
//            DISP=(NEW,PASS)
//SYSIN   DD *
RØ       EQU  Ø
................
R15      EQU  15
PASSVERI CSECT
         USING *,R1Ø,R11          ESTABLISH ADDRESSABILITY
```

```
        STM    R14,R12,12(R13)     SAVE3 REGISTERS
        LR     R1Ø,R15             SET FIRST BASE REGISTER
        LA     R11,2Ø48(R1Ø)       SET SECOND BASE REGISTER
        LA     R11,2Ø48(R11)       AND INCREMENT TO PROPER VALUE
        LR     R12,R13             STORE PREVIOUS SA ADDRESS
        LR     R2,R1  (R2) = POINTER TO ADDRESS OF THE PARM LIST
        LA     R13,SAVE3           LOAD ADDRESS OF THIS SAVE3 AREA
        ST     R12,SAVE3+4         CHAIN BACKWARDS
        ST     R13,8(R12)          CHAIN FORWARD
        ST     R9,R9SAVE
        OPEN   (PRINTDCB,(OUTPUT))
        L      R3,Ø(R2)
        LA     R1,USERID           MOVE USERID PARM
        MVC    Ø(8,R1),Ø(R3)
        L      R3,4(R2)
        LA     R1,USERPASS         MOVE USERPASS PARM
        MVC    Ø(8,R1),Ø(R3)
        LA     R4,USERID               (R4) = ADDRESS OF USERID
        BAL    R8,COUNTLEN             COUNT LENGTH
        MVC    USERNAME(1),LENGTH+3    STORE LENGTH OF USERID
        LA     R4,USERPASS             (R4) = ADDRESS OF PASSWORD
        BAL    R8,COUNTLEN             COUNT LENGTH
        MVC    PASSWORD(1),LENGTH+3    STORE LENGTH OF PASSWORD
        RACROUTE REQUEST=VERIFY,ENVIR=CREATE,RELEASE=2.6,              *
               MF=(E,LEXTGENE)
        ST     RØ,RZEROSAV    STORE REASON CODE
        ST     R1,MEMBRESP    STORE ADDRESS OF THE RESPONSE
        ST     R15,R15SAV     STORE SAF RETURN CODE
        LTR    R15,R15        SAF RETURN CODE = Ø ?
        BZ     OKRACFS1       YES- OK.
        MVI    PRINT,C' '
        MVC    PRINT+1(L'PRINT-1),PRINT
        MVC    PRINT+1(28),=C'RACROUTE VERIFY CREATE ERROR'
        PUT    PRINTDCB,PRINT
        MVC    PRINT(133),BLANK
        MVC    PRINT+1(8),USERID               MOVE USERID
        PUT    PRINTDCB,PRINT
*  DISPLAY SAF AND RACF RETURN CODES AND REASON CODE:
*  SEE: OS/39Ø 2.6 SECURITY SERVER RACROUTE MACRO REFERENCE
*  ALL RETURN AND REASON CODES ARE SHOWN IN HEXADECIMAL
        LA     R7,LEXTGENE
        USING  SAFP,R7        EST. ADDRESSABILITY FOR SAF RC
        MVC    PRINT(133),BLANK
        MVC    PRINT+1(8),USERID               MOVE USERID
        MVC    PRINT+19(7),=C'SAF RC='
        MVC    NUMBER(4),R15SAV
        BAL    R8,CONTOHEX
        MVC    PRINT+26(2),RESULT1Ø+8          MOVE SAF RETURN CODE
        MVC    PRINT+35(11),=C', SAFPRRET='
        MVC    NUMBER(4),SAFPRRET
        BAL    R8,CONTOHEX
```

```
        MVC    PRINT+46(2),RESULT1Ø+8            MOVE RACF RETURN CODE
        MVC    PRINT+54(11),=C', SAFPRREA='
        MVC    NUMBER(4),SAFPRREA
        BAL    R8,CONTOHEX
        MVC    PRINT+65(2),RESULT1Ø+8            MOVE REASON CODE
        PUT    PRINTDCB,PRINT
        DROP   R7
        L      R7,R15SAV
        B      FREEM
OKRACFS1 EQU   *
        RACROUTE REQUEST=VERIFY,ENVIR=DELETE,ACEE=ACEEADR,              *
               RELEASE=2.6,WORKA=WORKAREA,MF=S
        ST     RØ,RZEROSAV    STORE REASON CODE
        ST     R1,MEMBRESP    STORE ADDRESS OF THE RESPONSE
        ST     R15,R15SAV     STORE RETURN CODE
*    TEST THE RETURN CODE FROM RACROUTE REQUEST=VERIFY,ENVIR=DELETE
        L      R15,R15SAV     LOAD  RETURN CODE FROM RACXTRT
        LTR    R15,R15        RC FROM RACXTRT = Ø ?
        BZ     FREEM          YES- OK.
        L      R1,R15SAV      STORE RETURN CODE
        CVD    R1,PACKFIEL
        MVC    COPYPATE(1Ø),PATTERN
        ED     COPYPATE(1Ø),PACKFIE2
        MVI    PRINT,C' '
        MVC    PRINT+1(L'PRINT-1),PRINT
        MVC    PRINT+1(28),=C'RACROUTE VERIFY DELETE ERROR'
        PUT    PRINTDCB,PRINT
        MVI    PRINT,C' '
        MVC    PRINT+1(L'PRINT-1),PRINT
        MVC    PRINT+1(11),=C'DELETE  RC='
        MVC    PRINT+13(8),COPYPATE+2
        MVC    PRINT+23(11),=C'REASON CODE'
        L      R1,RZEROSAV
        CVD    R1,PACKFIEL
        MVC    COPYPATE(1Ø),PATTERN
        ED     COPYPATE(1Ø),PACKFIE2
        MVC    PRINT+35(8),COPYPATE+2
        PUT    PRINTDCB,PRINT
FREEM    EQU   *
        MVC    USERID(8),BLANK
        MVC    USERPASS(8),BLANK
        CLOSE  (PRINTDCB)
        L      R13,4(R13)
        LR     R15,R7
        RETURN (14,12),RC=(15)
LEXTGENE RACROUTE REQUEST=VERIFY,ENVIR=CREATE,ACEE=ACEEADR,             *
               USERID=USERNAME,RELEASE=2.6,PASSCHK=YES,                 *
               PASSWRD=PASSWORD,                                        *
               WORKA=WORKAREA,MF=L
COUNTLEN EQU   *
        LA     R12,8
```

```
        LA    R2,PARM           (R2)  = ADDRESS OF THE PARM FIELD
*                               (R4)  = ADDRESS OF THE PARM FIELD
*                               (R12) = LENGTH OF THE PARM FIELD
        MVC   PARM(8),BLANK
        XR    R5,R5             EST. PARM COUNTER
        LA    R5,1
LOOPPARM EQU  *
        C     R5,=F'9'          TEST IF MORE THAN 8 CHARACTERS?
        BL    CONTPARM
        MVC   PRINT(133),BLANK
        MVC   PRINT+1(27),=C'LENGTH OF PARM GT 8 ERROR '
        PUT   PRINTDCB,PRINT
        B     INVALIDP
CONTPARM EQU  *
        MVC   Ø(1,R2),Ø(R4)  MOV ONE CHARACTER
        CLI   Ø(R2),C' '
        BNE   NOTBLANK
        B     INVALIDP
NOTBLANK EQU  *
        LA    R1,1
        AR    R2,R1
        AR    R4,R1
        AR    R5,R1
        BCT   R12,LOOPPARM
INVALIDP EQU  *
        XR    R1,R1
        LA    R1,1
        SR    R5,R1
        ST    R5,LENGTH
        BR    R8
CONTOHEX EQU  *
        XC    CHARACTE,CHARACTE
        MVC   CHARACTE(4),NUMBER
        UNPK  CHARACTE,CHARACTE(5)
        TR    CHARACTE+7(8),HEXTABLE
        MVC   RESULT1Ø+2(8),CHARACTE+7
        BR    R8
*   CONSTANTS AND STORAGE
SAVE3    DS   18F
NUMBER   DS   F
R9SAVE   DS   F
LENGTH   DS   F
RZEROSAV DS   F
R15SAV   DS   F
ACEEADR  DS   F
MEMBRESP DS   F
PARM     DS   CL8
RESULT1Ø DS   CL1Ø
PRINT    DS   CL133
BLANK    DC   CL133' '
CHARACTE DS   CL16
```

```
HEXTABLE DC      24ØCL1'?',C'Ø123456789ABCDEF'
PATTERN  DC      XL1Ø'4Ø2Ø2Ø2Ø2Ø2Ø2Ø2Ø212Ø'
         DS      ØD
PACKFIEL DS      ØPL8
         DS      PL3
PACKFIE2 DS      PL5
COPYPATE DS      CL1Ø
WORKAREA DS      512X'ØØ'
PASSWORD DS      XL1    LENGTH
USERPASS DS      CL8    PASSWORD
USERNAME DS      XL1    LENGTH
USERID   DS      CL8    USERID
         DS      ØD
PRINTDCB DCB     MACRF=PT,RECFM=FBA,LRECL=133,BLKSIZE=133,DSORG=PS,      *
                 DDNAME=PRINTOUT
         LTORG
LICHSAFP ICHSAFP            RACF RETURN CODE MAPPING MACRO
         END
//*
//*----------------------------------------------------------------
//LINK     EXEC PGM=IEWL,COND=(5,LT,ASM),PARM='REUS,LET,XREF,AC=1'
//SYSLMOD  DD DSN=FSS2.LINKLIB,DISP=SHR
//SYSUT1   DD UNIT=VIO,SPACE=(CYL,(1,1))
//SYSPRINT DD  SYSOUT=T
//SYSLIN   DD DSN=&&OBJ,DISP=(OLD,DELETE)
//       DD  *
  NAME PASSVERI(R)
//*  IBM COBOL FOR MVS & VM
//*  COMPILE AND LINK EDIT A COBOL PROGRAM
//COBOL  EXEC PGM=IGYCRCTL,REGION=2Ø48K
//STEPLIB  DD  DSNAME=SYS1.IGY.SIGYCOMP,DISP=SHR
//SYSPRINT DD  SYSOUT=*
//SYSLIN   DD  DSNAME=&&LOADSET,UNIT=SYSDA,
//    DISP=(MOD,PASS),SPACE=(TRK,(3,3)),DCB=(BLKSIZE=32ØØ)
//SYSUT1   DD  UNIT=SYSDA,SPACE=(CYL,(1,1))
//SYSUT2   DD  UNIT=SYSDA,SPACE=(CYL,(1,1))
//SYSUT3   DD  UNIT=SYSDA,SPACE=(CYL,(1,1))
//SYSUT4   DD  UNIT=SYSDA,SPACE=(CYL,(1,1))
//SYSUT5   DD  UNIT=SYSDA,SPACE=(CYL,(1,1))
//SYSUT6   DD  UNIT=SYSDA,SPACE=(CYL,(1,1))
//SYSUT7   DD  UNIT=SYSDA,SPACE=(CYL,(1,1))
//SYSIN DD *
       IDENTIFICATION DIVISION.
       PROGRAM-ID.  COBRACF.
       AUTHOR. S. KOWALSKI.
       DATE-WRITTEN.  JAN 2ØØØ.
       ENVIRONMENT DIVISION.
       CONFIGURATION SECTION.
       INPUT-OUTPUT SECTION.
       FILE-CONTROL.
       DATA DIVISION.
```

```
        FILE SECTION.
        WORKING-STORAGE SECTION.
       * DEFINE STORAGE FOR PARMS*
        Ø1  USERID    PIC X(8)        VALUE 'XXXXXXXX'.
        Ø1  USERPASS  PIC X(8)        VALUE 'YYYYYYYY'.
        LINKAGE SECTION.
        PROCEDURE DIVISION.
            MOVE 'XXXXX  '  TO USERID.
            MOVE 'M2ØØØ1 '  TO USERPASS.
            CALL 'PASSVERI' USING USERID USERPASS.
            DISPLAY RETURN-CODE.
            MOVE '        '  TO USERID.
            MOVE '        '  TO USERPASS.
            STOP RUN.
//LKED   EXEC PGM=HEWL,PARM='REUS,LET,XREF,AC=1'
//SYSPRINT DD  SYSOUT=*
//SYSLMOD  DD DSN=YOUR.APF.AUTHORIZED.LIBRARY,DISP=SHR
//SYSLIB   DD  DSNAME=SYS1.CEE.SCEELKED,DISP=SHR
//         DD  DISP=SHR,DSN=YOUR.APF.AUTHORIZED.LIBRARY
//SYSUT1   DD  UNIT=SYSDA,SPACE=(TRK,(1Ø,1Ø))
//SYSLIN   DD  DSNAME=&&LOADSET,DISP=(OLD,DELETE)
//      DD  *
  NAME COBRACF(R)
//ST1      EXEC PGM=COBRACF
//STEPLIB  DD DISP=SHR,DSN=YOUR.APF.AUTHORIZED.LIBRARY
//OUTPUT1   OUTPUT DEFAULT=YES
//PRINTOUT  DD SYSOUT=*
```

Szczepan Kowalski
The Johannesburg Stock Exchange (South Africa)   © Xephon 2001

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.

A glossary of RACF and security terminology

Recent developments in the IT industry, coupled with a flurry of acquisitions, make it harder than ever to keep track of the fast-growing area of computer security. As a special feature this issue, the glossary presented below explains RACF and security terms, acronyms, and product names, and terms and products from other areas where RACF professionals most frequently find themselves involved. An accompanying article (*RACF-related organizations and products –* see pages 57-63) contains information on security companies and other relevant organizations.

READER'S GUIDE

First, some notes about the way the glossary is formatted:

- Terms defined elsewhere in the glossary are in **bold,** with the one exception of 'RACF'. This is partly because it is used so frequently, but also because, when the word following it is in bold, it would be unclear whether the term is listed alone or preceded by RACF. For example, "...a **RACF dataset** found..." could indicate that **RACF** and **dataset** are separate entries in the glossary, or, as is in fact the case, that there is a two-word entry '**RACF dataset**' under R.

- Some acronyms are self-explanatory once you know what they stand for. These definitions are only listed (and not in bold).

- Because the changes are so recent and most readers are more familiar with the old terms, the following IBM product names are used:

    - **OS/390** for z/OS (and MVS)

    - **System/390** for IBM eserver zSeries

    - **AS/400** for IBM eserver iSeries 400

    - **RS/6000** for IBM eserver pSeries

    - **OS/400** and **AIX** have not undergone a name change.

- Where relevant, pronunciation is shown in parentheses and *italics*. Where spaces are shown, instead of hyphens, a short pause is indicated, as would normally occur between words.

- Finally, recognizing RACF's EBCDIC environment, numeric entries are listed *at the end* of the alphabet, rather than at the beginning, as in the ASCII world of publishing.

GLOSSARY

AAC – **Khephren 2000 Application Framework's Authentication and Access Control Facility**.

abuse – any behaviour violating security procedures.

access authority – the level of access allowed to a **protected resource** for a specific user. Levels in RACF are NONE, EXECUTE, READ, UPDATE, CONTROL, and ALTER.

access control – enforcing rules governing the use of computer resources, by restricting both the use and type of use to authorized individuals and the computer resources they are responsible for.

access list – **standard access list**, not the **conditional access list**.

access token – **authenticator**.

Accessor Environment Element (ACEE) – a RACF control block that describes the current user's security environment.

ACE/Agents – client software from **RSA Security** that communicates with **ACE/Server** to verify **SecurID** authentication requests. It runs in OS/390, Windows NT/2000, Lotus Domino, Netscape, AS/400, NetWare, Unnix, and Compaq VAX/VMS environments.

ACE/Server – server software that verifies **SecurID** authentication requests. It runs in Windows NT/2000 Advanced Server, Solaris, HP/UX, and AIX environments.

ACEE – **ACcessor Environment Element**.

ACF/2 – see **CA-ACF2**.

ACL for MVS – audit software from **ACL Services** for OS/390.

ACL for Windows – audit software from **ACL Services** for Windows 9*x*/NT/2000.

ActivPack for IBM OS390/RACF – a hardware/software solution from **ActivCard** that adds **smart card** security to RACF.

ADABAS SAF Security – software from **Software AG** that gives ADABAS a security interface to RACF, **CA-ACF2**, **CA-Top Secret**, and any other security package that supports **SAF**.

ADAU – **Automatic Direction of Application Updates**.

ADSP – **Automatic DataSet Protection**.

ADSP attribute – a **user attribute** that ensures that all DASD datasets created by the user are protected by RACF.

algorithm – a detailed non-programming-language-specific procedure that can be used to solve a problem or perform a specific task.

ANSI *(ann-see)* – **American National Standards Institute**.

anti-virus software – software that can scan memory, files, and magnetic media for viruses, remove them (when possible), and protect a running system from **virus** attacks.

APF-authorized – programs permitted to use sensitive system functions by the OS/390 Authorized Program Facility (APF).

APFCHECK – security software from **Goldis Consulting Services** that audits the use of **APF authorization**.

API – **Application Programming Interface**.

Application Programming Interface (API) – documented programming procedures to access a given piece of software, eg an entry point name and parameter list.

application user identity – an alternative name by which a RACF user can be known to an application.

ASPG – **Advanced Software Products Group**.

asymmetric algorithm – an **encryption** method that uses one key to encrypt and a second to decrypt.

attribute – see **user attribute** and **group-related user attribute**.

audit – a thorough and systematic review of procedures, their implementation, and the results.

Audit Central – a software product from Platinum that is now part of **eTrust** from **Computer Associates**.

AUDIT request – a resource manager program would code the **RACROUTE macro** specifying REQUEST=AUDIT to access RACF.

audit trail – detailed logging of individual security-related activities, allowing a specific event to be traced from beginning to end.

AUDITOR attribute – a **user attribute** that permits use of the RACF **audit** features.

AUDITRE – **audit** software from **Treehouse Software** that uses the ADABAS protection log to identify changes to data.

AUTH request *(ahh-th)* – checks a user's authorization to a **RACF-protected** resource via the **RACROUTE macro** with REQUEST=AUTH specified.

authentication – verify a user identity, message **integrity**, or a user is permitted to access a resource in the manner requested.

authentication token – **authenticator**.

authenticator – a hand-held electronic device (or software that emulates it) that can be identified because each device generates a unique set of characters at a fixed point in time.

authority – the right to access resources, objects, or functions.

authorization checking – checking **authority** using the RACF **RACROUTE macro**, with REQUEST= parameters such as **AUTH**, **FASTAUTH**, and **VERIFY**.

automatic command direction – the automatic routing of commands to remote **RRSF nodes**.

Automatic DataSet Protection (ADSP) – see **ADSP attribute**.

automatic direction – see **automatic command direction**, **automatic direction of application updates,** and **automatic password direction**.

automatic direction of application updates (ADAU) – **RRSF**'s ability to route RACF database update requests, using the **ICHEINTY** and **RACROUTE macros**, to remote **RRSF nodes**.

automatic password direction – **RRSF**'s ability to change the **password** for a **user ID** on remote **RRSF nodes** whenever the password is changed on the local system.

automatic profile – the tape volume profile created by RACF when a RACF-defined user protects a tape dataset.

BAAS – **Blockade Authentication and Authorization Services**.

back door – **trap door**.

back-up dataset – a dataset in the **back-up RACF database**.

back-up RACF database – a **RACF database** defined in the dataset name table (ICHRDSNT) that is kept current with the **primary RACF database**. No IPL is required to switch to the back-up should the primary fail.

Baltimore Enterprise Crypto System (ECS) – encryption hardware/software from **Baltimore Technologies** that supports Compaq Non Stop (Tandem), OS/390, OS/400, AIX, Solaris, HP-UX, Linux, and Windows NT. It consists of three components: the standalone hardware-based ECS Server, the thin-client ECS Software Adapter, and ECS Desktop hardware or software.

base segment – the **segment** within the RACF **profile** that contains the most fundamental information.

BCS – **Blockade Certificate Support**.

BESS – **Blockade Enterprise Security System**.

BETA 88 RACF Manager – management software for RACF from **Beta Systems Software** that monitors RACF and provides its own user interface to RACF.

BETA 89 Automated Security Auditor – real-time security monitor software from **Beta Systems Software**.

BGS – **Blockade Gateway Server**.

biometrics – identification through the use of any human attribute that is unique to each individual.

block cipher – **algorithms** that **encrypt** data a chunk (eg 64 bits) at a time, rather than as a continuous stream of bits (**stream cipher**).

block update command (BLKUPD) – a RACF diagnostic command to view and change records in a **RACF dataset**.

Blockade Authentication and Authorization Services (BAAS) – a component of **Extended Access Control (EAC).**

Blockade Certificate Support (BCS) – a component of **Extended Access Control (EAC)**.

Blockade Enterprise Security System (BESS) – a component of **Extended Access Control (EAC).**

Blockade Gateway Server (BGS) – a component of **Blockade Enterprise Security System (BESS)**, which is a component of **Extended Access Control (EAC)**.

Blockade Password Synchronization Services – security software from **Blockade Systems** that ensures password changes are reflected on all platforms where the user ID exists.

Blockade SNA Support (BSNAS) – a component of **Extended Access Control (EAC)**.

Blockade Synchronization Services (BSS) – a component of **Extended Access Control (EAC)**.

Blockade Web Support (BWS) – a component of **Extended Access Control (EAC)**.

BSAFE Cert-C – certificate handling Software Developer Kit (SDK) from **RSA Security** for creating C programs that integrate into a **public key infrastructure (PKI)**.

BSAFE Cert-J – certificate handling Software Developer Kit (SDK) from **RSA Security** for creating Java programs that integrate into a **public key infrastructure (PKI)**.

BSAFE Crypto-C – Software Developer Kit (SDK) from **RSA Security** providing **encryption** components with a C language **API**.

BSAFE Crypto-J – Software Developer Kit (SDK) from **RSA Security** providing Java **encryption** components with its own **API** as well as support for the Java Security API.

BSAFE S/MIME-C – Software Developer Kit (SDK) from **RSA Security** providing security protocol components for C programs.

BSAFE SSL-C – Software Developer Kit (SDK) from **RSA Security** that simplifies implementation of **SSL** in C programs.

BSAFE SSL-J – Software Developer Kit (SDK) from **RSA Security** that simplifies implementation of **SSL** in Java programs.

BSAFE WTLS-C – Software Developer Kit (SDK) from **RSA Security** providing **APIs** for C language implementations of the **Wireless Transport Layer Security (WTLS).**

Bsafe/DB2 Security Server – software from **BSafe Software Solutions** that provides DB2 security in the CICS environment.

BSNAS – **Blockade SNA Support**.

BSS – **Blockade Synchronization Services**.

BWS – **Blockade Web Support**.

C2 – a security classification level set by the US **National Security Agency**. There are other levels within the Trusted Computer System Evaluation Criteria (TCSEC).

CA – **certification authority**.

CA – **Computer Associates International**.

CA-ACF2 – security software from **Computer Associates International** that competes with RACF.

CA-ALERT for VM – security software from **Computer Associates** that controls user access with a menu-driven user interface.

cache structure – a **Coupling Facility** structure that contains data shared by systems in a sysplex.

CA-PanAudit Plus – mainframe and PC **audit** software from **Computer Associates** that provides file interrogation functions as well as the complete CA-Easytrieve Plus product.

CA-ProAudit for DB2 – audit software from **Computer Associates** that accesses **SMF** data, and DB2 catalogue and log data.

CA-ProSecure for DB2 – security software from **Computer Associates** for OS/390 DB2.

category – see **security category**.

CA-Top Secret – security software from **Computer Associates** that competes with RACF.

CA-VM:Secure – security software from **Computer Associates** that competes with **RACF for VM**.

CDMF – **Commercial Data Masking Facility**.

CDT – **Class Descriptor Table**.

certificate – **digital certificate**.

certificate name filter – created by the RACDCERT MAP command, a mapping of **digital certificates** to multiple **user IDs**.

certificate store – a storage location for **digital certificates**, Certificate Revocation Lists, and **Certificate Trust Lists**.

Certificate Trust List (CTL) – a predefined list of items that have been signed by a **certification authority**.

certificate-authority certificate – RACF-managed **digital certificate** associated with a **certification authority**, used to verify signatures in other certificates.

certification – see **digital certificate**.

certification authority (CA) – any trusted entity that follows established procedures when requested to issue a **digital certificate** by an individual, organization, or machine.

CFSizer – **System/390 Coupling Facility Structure Sizer Tool**.

checksum – a mathematical calculation made on data in a file, database, or transmission, used to check the **integrity** of the data.

cipher text – a message that has been **encrypted**.

class – a collection of RACF-defined entities with similar characteristics.

class authority (CLAUTH) – a user attribute specifying the **classes**, if any, where the user may create RACF **profiles**.

Class Descriptor Table (CDT) – a RACF table containing entries for each class, except USER, GROUP, and DATASET.

CLAUTH attribute – see **class authority**.

command direction – **RRSF**'s ability for users to issue a command and specify that it must run on a local or remote RACF, on their own or another user ID.

Commercial Data Masking Facility (CDMF) – part of the IBM Common Cryptographic Architecture, **40-bit encryption** used by RACF to mask the data portion of **RRSF** transaction processing message packets.

conditional access list – users and **groups** permitted access only when a specified condition is true. For example, access to a dataset may be permitted only when executing a specific program.

Consistent Sign-On (CSO) – a feature of both **Blockade Password Synchronization Services** and **Extended Access Control (EAC)** that ensures that a user ID has the same **password** across all platforms.

Consul/Audit for ACF/2 – security auditing software from **CONSUL Risk Management** for **CA-ACF2**.

Consul/Audit for RACF – security auditing software from **CONSUL Risk Management**.

Consul/CVO – security software from **CONSUL Risk Management** that enforces security **policy** by controlling the use of RACF commands.

Consul/Enterprise Audit – multi-platform security monitoring software from **CONSUL Risk Management**.

Consul/RACF – software from **CONSUL Risk Management** that streamlines the use of RACF.

Consul/RACF Administrator for Windows – software from **CONSUL Risk Management** that provides a RACF Windows NT user interface.

content policy – rules within an organization regarding what type of material may not be stored on computers, eg pornography.

content security – enforcement of **content policy**.

contingency planning – any cost-effective preparations for negative future circumstances.

CONTROL-SA – security management software from **BMC Software** that centralizes control and a view of security, with some security audit functions.

CONTROL-SA/Links – security event management software from **BMC Software** for **CONTROL-SA**.

CONTROL-SA/PassPort – Web-based interface from **BMC Software** that enables **password** change and reset by end-users.

CONTROL-SA/Workflow – Web-based interface from **BMC Software** that manages

the **access authority** process.

coordinator system – the system in a **RACF data sharing group** where a RACF command is entered by a system operator or administrator and is propagated to the entire group.

Coupling Facility (CF) – hardware from IBM where common tables can be shared in a sysplex, most notably for update locking.

CRL – Certificate Revocation List.

cryptanalysis – interpreting **cipher text** without being given the key.

CRYPTOAdmin – centralized user authentication software from **CRYPTOCard**.

cryptoanalysis – less common spelling for **cryptanalysis**.

CRYPTOCard RB-1 Challenge-Response Token – a credit card sized **authenticator** from **CRYPTOCard**.

cryptography – designing an **algorithm** for **cipher text**.

cryptology – the mathematics behind **cryptography** and **cryptanalysis**.

CSI – **Computer Security Institute**.

CSO – **Consistent Sign-On**.

CTL – **Certificate Trust List**.

current connect group – the RACF **group** assigned to the user at log-on.

current security label – the RACF **security label** assigned to the user at log-on.

CUTPWHIS – a free utility from **IBM** that removes non-usable **passwords** from the RACF password history.

CyberArmor – personal **firewall** from **InfoExpress**.

CyberFUSION – file transfer software from **Proginet** that provides **encryption** and compression for use across the Internet and within corporate networks.

Data Encryption Standard (DES) – originally developed by **IBM**, now an **NIST** standard first published in 1977. A **block cipher** that encrypts 64 bits at a time using a **symmetric algorithm**.

data integrity – the assurance that information has been unaltered during transmission or storage.

Data Security Monitor (DSMON) – a RACF **auditing** tool.
dataset profile – a **profile** used by RACF to protect one or more datasets.

DBSYNC *(dee-bee-sync)* – a free utility from **IBM** that compares two RACF **databases** and generates the RACF commands to make them similar.

DCE Security Server – a component of **SecureWay Security Server for OS/390** that is integrated with RACF and provides a fully functional **OSF** DCE security server for OS/390 Unix System Services (USS).

decode – translating an **encoded** object back to its original form.

decryption – converting **cipher text** to plain text.

default group – the **group** specified in the RACF **user profile** that becomes the

current connect group unless another group is specified at log-on.

DEFINE request – adds or deletes a **resource profile** via the **RACROUTE macro** with REQUEST=DEFINE specified.

delegation – giving **groups** or users the **authority** to use some security administrator functions of RACF.

DES *(dess)* – **Data Encryption Standard**.

DH – **Diffie-Hellman algorithm**.

Diffie-Hellman algorithm (DH) – a **public key algorithm** used for secure key exchange.

digital certificate – a digital document containing the owner's public key and a **digital signature** that **authenticates** the owner because it is issued by a **certification authority**.

digital signature – a digital string used to **authenticate** the message it is *attached* to, verify that it has not been tampered with, and, optionally, identify the sender.

DIRAUTH request *(derr-oth)* – checks security authorization of the receiver of a message via the **RACROUTE macro** with REQUEST=DIRAUTH specified.

Direct/7 – a software product from Platinum, later renamed **Enterprise Security Administrator** and now part of **eTrust** from **Computer Associates**.

directed command – a RACF command specifying AT or ONLYAT, issued from a **user ID** on an **RRSF node**.

Disaster Recovery Plan (DRP) – a documented set of procedures to be used in the event of a major computer outage.

discrete profile – a **resource profile** that provides RACF protection for a single resource.

discretionary access control – the resource owner defines who can access the resource.

Distributed Key Management System (DKMS) – security management software from **IBM** that provides central management of **encryption** keys.

DKMS – **Distributed Key Management System**.

DMS – **Delegated Management Services**.

DRP – **Disaster Recovery Plan**.

DSA – **Digital Signature Algorithm**.

DSMON *(dee-ess-monn)* – **Data Security Monitor**.

DSS – **Digital Signature** Standard.

E0, **E1**, **E2**, **E3**, **E4**, **E5**, **E6** – **ITSEC** certification of software products based on security assurance levels, **E0** being inadequate.

EAC – **Extended Access Control**.

Easy RACF Query (ERQ) – components from **Advanced Software Products Group (ASPG)** for programmers writing CLIST and REXX programs requiring

information from RACF.

ECS – **Baltimore Enterprise Crypto System**.

EDP – Electronic Data Processing, now more commonly known as Information Technology.

EFC (Essential Format Commands) – now part of **Easy RACF Query (EFQ)**.

E-HelpDesk – a VTAM application from **EKC Products** that allows end users to reset their own **RACF** and **CA-ACF2 passwords**.

EIR (Essential Information Retrieval) – now part of **Easy RACF Query (EFQ)**.

ELP (Essential List Parsing) – now part of **Easy RACF Query (EFQ)**.

Embedded Security Subsystem – a security chip and client security software from **IBM** for NetVista, PC 300 PL, and IntelliStation systems.

encode – convert data into a stream of bits so that it can be transmitted over a serial line.

encryption – an attempt to translate data (**plain text**) into a form where the only practical way to reconstruct it is by knowing a specific algorithm (fixed) and a key (can vary).

ENTACT!Admin – user security administration software from **Entact Information Security**.

ENTACT!API – an **API** from **Entact Information Security** that provides enterprise-wide access to RACF, **CA-ACF2,** and **CA-Top Secret** security services.

ENTACT!Audit – Windows-based security software from **Entact Information Security** that reports on user privileges across multiple platforms.

ENTACT!Request – intranet security workflow application from **Entact Information Security** focused on user access requests and approval.

ENTACT!Reset – Web-based software from **Entact Information Security** that allows users to reset their own **passwords**.

ENTACT!Role – role definition methodology and Windows-based software from **Entact Information Security** that grants security privileges based on a defined role.

ENTACT!UniPass – security software from **Entact Information Security** that provides selected users with enterprise-wide **passwords** administered by OS/390 RACF, **CA-ACF2**, or **CA-Top Secret**.

Enterprise Security Administrator – a software product from Platinum that is now part of **eTrust** from **Computer Associates**.

Enterprise Security Server (ESS) – a component of **Blockade Enterprise Security System (BESS)**, which is a component of **Extended Access Control (EAC)**.

Entire Security SAF Gateway – software from **Software AG** that allows RACF, **CA-ACF2**, or **CA-Top Secret** to control remote data access to ADABAS.

EntireX Security – software from **Software AG** that protects applications using EntireX Broker and Broker Services.

entity – a user, **group**, or resource defined to RACF.

ENVR object – a transportable format for **ACEE** data that allows the ACEE to be recreated without referencing the RACF database.

ERQ – **Easy RACF Query**.

e-security – security for electronic commerce on the Internet.

E-SRF Reporting Facility – security reporting software from **EKC Products** that provides RACF and **CA-ACF2** access analysis and event reporting.

ESS – **Enterprise Security Server**.

ETF/A – security software from **EKC Products** that simplifies and enhances the use of **CA-ACF2**.

ETF/R Firecall – security software from **EKC Products** that provides emergency RACF facilities.

ETF/T Firecall – security software from **EKC Products** that provides emergency **CA-Top Secret** facilities.

eTrust – an e-Business security software family from **Computer Associates**.

Extended Access Control (EAC) – a number of software components from **Blockade Systems** that extend RACF, **CA-ACF2**, or **CA-Top Secret** security to non-mainframe platforms.

EXTRACT request – **encodes** specific data, or gets or replaces certain fields in a RACF **profile** via the **RACROUTE macro** with REQUEST=EXTRACT specified.

ezRESET *(easy-reset)* – Web-based software from **Vanguard Integrity Professionals** that allows authorized users to reset their own **password**.

failsoft processing – a state when no datasets in the **primary RACF database** are available, **RVARY** INACTIVE has been specified, or a serious system error has occurred.

FASTAUTH request *(fast-ahh-th)* – uses in-**storage** profiles to check a user's authorization to a **RACF-protected** resource or function via the **RACROUTE macro** with REQUEST=FASTAUTH specified.

field-level access checking – a RACF facility that can be used to control access to **segments** of a RACF **profile**, and fields within those segments.

FileSecure – **encryption** software from **Baltimore Technologies** that runs as a Windows NT service.

FireWalker Suite – remote access hardware/software suite from **InfoExpress**, integrating **CyberArmor** personal **firewall**, **VTCP VPN**, and **VTCP** extranet client.

firewall – security software, often with a stand-alone computer system, that controls all of an organization's incoming traffic from the Internet at one location, most notably **viruses** and unauthorized access attempts.

FISC *(fisk)* – **Fischer International Systems** Corporation.

FormSecure – software components from **Baltimore Technologies** that allows programmers to add **encryption** security to Web forms.

FRACHECK function *(fra-check)* – replaced by **FASTAUTH request**.

FTPalert *(eff-tee-pee-alert)* – security software from **William Data Systems** to manage OS/390 ftp usage.

fully-qualified generic profile – a **dataset profile** defined to RACF as generic, but

with a dataset name specified, ie without any **generic characters**.

GCS – **Goldis Consulting Services**.

general resource – anything defined in the **Class Descriptor Table (CDT)**.

general resource profile – a **profile** used by RACF to protect a **general resource**.

general user – a RACF user with no security administration privileges beyond logging on, access to certain resources, and control over owned datasets.

generic character – special pattern-matching characters, such as the asterisk ('*'), known as *wildcard* characters in other operating systems, that are invalid in dataset names but are used in **generic profiles** to specify all dataset names that match the specified pattern.

generic profile – a **resource profile** that protects zero or more resources having the same RACF security requirements.

GID *(gidd)* – OS/390 Unix Group Identifier.

global access checking – a RACF performance feature that allows certain resources to be security checked against an **in-storage** table.

globally RACLISTed profiles – **in-storage profiles** for RACF-defined resources that are shared with other RACF nodes. See also **RACLISTed profile**, **locally RACLISTed profiles**.

granularity – level of detail.

group – zero or more users defined with the same security requirements for specified RACF resources.

group authority – which functions a user can perform on a **group**: USE, CREATE, CONNECT, or JOIN.

group dataset – a dataset with a qualifier with the same name as a RACF **group name**. Normally, the high-level qualifier, but installations can choose another qualifier.

group ID – now known as **group name**.

group name – one to eight characters that uniquely identifies a **group** to RACF.

group profile – the RACF **profile** that defines a **group**.

grouping profile – a RACF **profile** in a **resource group class**.

group-related user attribute – allows a user to control RACF security for a **group** and its subgroups.

GRPACC attribute – gives all RACF users in a **group** UPDATE **authority** to any group datasets created by any user in the group.

hacker – anyone purposely attempting unauthorized access to a computer system, without the organization's permission.

Halo – OS/390 and Windows NT **password** management software from **NEON Systems**.

hashing algorithm – a method used to transform a record's key into a location within a file where the record will be stored.

HFS – Hierarchical File System of OS/390 Unix System Services and Unix-based

operating systems.

IBM eserver zSeries and IBM System/390 Cryptographic Coprocessor – **encryption** hardware.

IBM eserver zSeries and IBM System/390 PCI Cryptographic Coprocessor (PCICC) – **encryption** hardware.

IBM Network Security Auditor – software included with every IBM **firewall**.

IBM Payment Registry – server software from **IBM** that manages and stores **certificates**.

IBM SecureWay Boundary Server – component of **Tivoli SecureWay FirstSecure**.

IBM SecureWay Firewall – **firewall** hardware/software.

IBM SecureWay Toolbox – security and **encryption** tools for developers.

IBM SmartCard Security Kit – security hardware/software that prevents unauthorized **access** to a workstation.

ICB – **Inventory Control Block**.

ICHEINTY – a macro providing a direct interface to the **RACF database**, to locate or update a **profile**.

ICHRIN03 – the RACF started procedures table.

ICU...MVS – security software from **JANUS Associates** that focuses on identifying access control exposures; ICU is Integrity Concerns Uncovered.

INCompliance *(inn-compliance)* – Web-based audit security software from **Technologic Software Concepts** that identifies RACF security vulnerabilities.

INCONTROL for Security Management *(inn-control)* – a multi-platform security software suite from **BMC Software** based on CONTROL-SA.

insider – anyone authorized to use an organization's computing resources.

in-storage – resident in memory, not in a dataset or database.

integrity – measures whether something, typically data, is intact, with nothing missing; uncorrupted.

intrusion detection – to discover unauthorized **access** to computing resources.

Inventory Control Block (ICB) – the first block in a **RACF database**.

IP – **Internet Protocol**.

IP hijacking – see **IP splicing**.

IP splicing – a **hacker** technique: take over an active, established Internet session.

IP spoofing – a **hacker** technique: attempt access by impersonating an authorized **IP** address.

IRRHFSU – a free utility from **IBM** that unloads and reformats **HFS** file security information into RACF IRRDBU00 format.

IT Service Vision – multi-platform performance management software from **SAS Institute**.

ITSEC *(eye-tee-sek)* – IT Security Evaluation and Certification Scheme (UK).

KCA – **Key Certification Authority**.

KEA – Key Exchange **Algorithm**.

Keon *(key-onn)* – a **PKI** software family from **RSA Security** that manages **digital certificates**.

Kerberos *(kurr-burr-oss)* – a Unix security system derived from work done at Massachusetts Institute of Technology (MIT).

key – although it has several security-related meanings, it may also refer to an **authenticator**.

key pair – a **private key** and its related **public key**.

key ring – a named collection of **digital certificates**.

KeyTools – a suite of **e-security** tools for developers from **Baltimore Technologies**.

Khephren 2000 Application Framework's Authentication and Access Control Facility (AAC) *(keff-renn)* – a run-time environment with **API** from **ADDC InfoTech** for programmers writing Java CORBA enterprise servers.

KMIGRATE *(kay-migrate)* – a free software tool from **IBM** that migrates existing DCE and OS/390 users to **Kerberos**.

KT-1 Key Chain Token – an **authenticator** from **CRYPTOCard** that attaches to a key chain and fits in a pocket.

LDAP *(ell-dapp)* – **Lightweight Directory Access Protocol**.

Lightweight Directory Access Protocol (LDAP) – Internet security standard for user **access** to network resources.

LIST request – builds **in-storage profiles** for a RACF **general resource class** via the **RACROUTE macro** with REQUEST=LIST specified.

list-of-groups checking – the RACF SETROPTS GRPLIST option that searches all **groups** of which the current user is a member, rather than just the **current connect group**, to determine the user's access to a requested resource.

local mode – an **RRSF node** operating without a logical connection to any other RRSF node.

locally RACLISTed profiles – **in-storage profiles** for RACF-defined resources that are not shared with other RACF nodes. See also **RACLISTed profile**, **globally RACLISTed profiles**.

LockStar – software from **LockStar** that provides end-to-end security from mainframe to Web browser. LockStar Enabler resides on the mainframe and LockStar Forwarder on the Web server.

log retention – how long **audit trail** logs are kept.

logging – recording of data about specific events, creating an **audit trail**.

LRA – **Local Registration Authority**.

LSA – **Local Security Authority**.

LU – VTAM Logical Unit.

MAC *(mack)* – Mandatory Access Control or Message Authentication Code **algorithm**.

MailSecure – an e-mail plug-in or client (depending on the e-mail system) from **Baltimore Technologies** that provides **encryption**, **digital signatures**, and **digital certificates**.

main system – the system designated to receive most of the **RRSF** communications on a multisystem **RRSF node**.

managed user ID association – relationship between two **user IDs**, where the managing ID can run RACF commands under the authority of the managed ID, but not vice versa.

master primary dataset – the first dataset activated in the **primary RACF database**.

MD2, MD4, and MD5 algorithms – **hashing algorithms** developed by **RSA Data Security** to create a 128-bit hash value from a 64-bit block.

MegaCryption – OS/390 **encryption** software from **Advanced Systems Product Group** (ASPG) that is compatible with encryption software on other platforms.

member – a user belonging to a **group**.

member profile – RACF **profile** storing the **security level** information for, and definition of, a **member**.

member system – any OS/390 system image in a multisystem **RRSF node**.

MFsafe – software from **BSafe Software Solutions** that enhances existing security, including **access control** down to the record and field levels for databases and **VSAM**.

MIMEsweeper – **content security** software from **Baltimore Technologies** to manage and enforce **content policy** enterprise-wide.

modelling – see **profile modelling**.

M-Tech – **Mercury Information Technology**.

multiple-subsystem scope – DB2 classes with the subsystem ID as part of the **resource** name.

multisystem node – see **multisystem RRSF node**.

multisystem RRSF node – an **RRSF node** with multiple OS/390 system images that share the same **RACF database**.

NCSC – National Computer Security Center, part of the **National Security Agency** (NSA).

Netlock – a network security software suite from **Netlock Technologies** that provides central administrator control.

NetMagic Pro – **user ID**/**password** management software from **NetMagic Systems** for user self-service and Help Desk staff.

NetSec – **Computer Security Institute** annual conference.

Network Trusted Computing Base (NTCB) – all security components within a network system.

Nigel's RACF Utilities – PC software from Nigel **Pentland** that processes a RACF

file downloaded from the mainframe, and creates reports or JCL.

node – see **RRSF node**.

non-automatic profile – a tape volume profile that RACF deletes only when an RDELETE command is issued. The profile must have been created with an RDEFINE command or when tape dataset protection was not active.

nonce *(nahh-ss)* – a randomly-generated value to protect against **hackers** using replay techniques.

non-data sharing mode – RACF **sysplex communication** without using the **Coupling Facility**.

NTCB – **Network Trusted Computing Base**.

one-time password – a **password** that can be used only once, to protect against **hackers** using replay techniques.

Open Cryptographic Services Facility – a feature of OS/390 Unix System Services.

OPERATIONS attribute – a **user attribute** that gives ALTER authority to any resource that a user or **group** has not been given explicit **access authority**.

operator identification card (OIDCARD) – a card with an encoded magnetic stripe used to identify terminal operators to RACF.

OS390ART *(oh-ess-three-ninety-art)* – free DB2-based **audit** software from **IBM**.

OSF – Open Software Foundation.

owner – the user or **group** specified in the owner field of a profile, usually whoever created the profile.

PADS – **Program Access to DataSets**.

PassTicket – an alternative to the RACF **password**, to avoid sending passwords across the network.

password – a string of characters, intended to be kept secret, that a user enters with his user ID to confirm his/her identity.

password cracker – software (often used by hackers) that rapidly and repeatedly retries a log-on sequence by cycling through possible **passwords**.

password synchronization – an option during RACF **peer user ID association** that automatically changes the **password** on one ID when the other is changed.

PasswordCourier – self-serve **password** management software from **Courion**.

PCICC – **IBM eserver zSeries and IBM System/390 PCI Cryptographic Coprocessor**.

peer system – any system in a **RACF data sharing group** to which RACF commands are propagated.

peer user ID association – definition of a relationship between two **user IDs** that allows either ID to run RACF commands under the authority of the other.

perimeter-based security – a term borrowed from physical security, defining a network security method of controlling access to all entry and exit points of the network.

permission bits – part of OS/390 Unix System Services security controls for directories and files stored in the **HFS**.

persistent verification (PV) – a VTAM sign-on/sign-off capability between two **LUs** that transmits a **password** only once, during sign-on, rather than on each attach.

physical security – protection of equipment, real estate, hard copy records, and other physical assets from theft, damage, or intrusion.

PIN *(pinn)* – Personal Identification Number, normally numeric and usually four digits, such as the password required when using a magnetic striped card in a banking machine.

PKCS – **Public-Key Cryptography Standards**.

PKI – **public key infrastructure**.

PKISERV – free sample Web application from **IBM** that uses RACF **digital certificate** support to create and retrieve certificates from a Web browser.

plain text – data that is not **encrypted**.

policy – a set of rules, often with enforcement methods, intended to implement an organization's decisions in a given area, such as security policy.

Policy Compliance Manager – a software product from **Computer Associates** that is now part of **eTrust**.

POSIT – a field of bit flags specifying RACF processing options for each **class** in the **CDT**.

PRF – pseudo-random function.

primary dataset – a dataset in the **primary RACF database**.

primary RACF database – the **RACF database** specified in the dataset name table (ICHRDSNT) or specified at IPL time, which contains the RACF **profiles** to be used for **authorization checking**.

Prio! – meta directory software from **Fischer International Systems**, including a **PKI** toolkit and meta agents for RACF and other platforms.

private key – a key known only to the sender or receiver of an encrypted message.

procedural security – security methods relying solely on human action.

profile – RACF's information about a user, **group**, or computer resource, stored in a **base segment** and zero or more other **segments**.

profile list – an **in-storage** index of **dataset profiles** (sorted by name) or **general resources** (sorted by **class**).

profile modelling – any definition of a new **profile** where RACF copies attributes from another profile.

ProfileBuilder – software from **Courion** that allows self-service update of employee information.

Program Access to DataSets (PADS) – defining **access** to a dataset based on the program being executed and who is running it.

program control – defining who can run a program.

protected resource – any resource for which RACF controls access.

protected user ID – a **user ID** that cannot be **revoked**, but can be used only to start a task, or other situation where a **password** is not required.

ProtectIT – comprehensive multi-platform security software from **Computer Associates**.

protocol – definition of the communications between two pieces of hardware or software, typically across a network: format of each transmission, allowable responses, and perhaps even timing.

proxy server – a server that receives and fulfils requests intended for another server.

P-Synch *(pee-sink)* – **password** management software from **Mercury Information Technology (M-Tech)**.

PT-1 Palm Organizer Token – software from **CRYPTOCard** that turns the 3Com Palm Organizer into a **one-time password** generator.

PTKTGEN – free **PassTicket** software from Thierry **Falissard**.

public key – a published key value used as one of the two keys in **public-key encryption**.

Public Key Infrastructure (PKI) – a combination of hardware, software, policy, and procedures to create secure communications using **digital certificates**.

Public-Key Cryptography Standards (PKCS) – **public-key encryption** procedures, including signing data, exchanging keys, requesting **certificates,** and, of course, actually encrypting and decrypting the data.

public-key encryption – **encryption** using an **asymmetric algorithm** with one key for encryption and another for decryption. One is a **public key** and the other a **private key**.

PV – **persistent verification**.

PWCHECK *(pee-doubleyou-chekk)* – a **password** quality **audit** tool for RACF environments from **Goldis Consulting Services**.

PWCHECK-PRO – **PWCHECK** with a **password cracker** and other features added; also from **Goldis Consulting Services**.

QS/390 (Quality Security/390 Suite) – one of various names for **Vanguard Administrator**, Analyzer, Enforcer, and Advisor integrated together by SmartLink, Find-it-Fix-it-Fast, RiskMinder, SmartAssist, and eDistribution technologies from **Vanguard Integrity Professionals**.

Quality Security Solution Suite – see **QS/390**.

Quality Security/390 Suite – see **QS/390**.

RA/2 – RACF administrative, auditing and reporting software from **Software Engineering of America (SEA)**.

RA/7 – a RACF report generator from **Software Engineering of America (SEA)**.

RA/8 – RACF security software from **Software Engineering of America (SEA)** that manages the assignment of users to **groups**.

RAC *(rack)* – a free utility from **IBM** that executes RACF commands in an OS/390 Unix System Services environment.

RAC/PACK *(rack-pack)* – **RA/2**, **RA/7**, and **RA/8**.

RACDEF request *(rack-deff)* – has been replaced by the **DEFINE** request.

RACF *(rack-eff)* – **Resource Access Control Facility**.

RACF dataset – one of up to 90 datasets in the **RACF database**.

RACF data sharing group – multiple instances of RACF, each sysplex-defined to XCF.

RACF database – RACF's security information repository.

RACF for VM – a RACF implementation for VM from **IBM**.

RACF manager – the routines within RACF that provide access to the **RACF database**.

RACF remote sharing facility (RRSF) – RACF's ability to communicate with other **RRSF nodes**.

RACF remove ID utility – a program supplied with RACF that generates RACF commands to remove all references to deleted **user ID**s and **group names**. Alternatively, it can generate commands to remove all references to a specified user ID or group name.

RACF Report Writer (RACFRW) – though still provided for compatibility with previous RACF versions, replaced by the **RACF SMF unload utility (IRRADU00)**.

RACF segment – renamed **base segment**.

RACF SMF data unload utility (IRRADU00) – a program supplied with RACF that creates a sequential file of the **SMF** RACF records.

RACF/DB2 external security module – a RACF exit point that receives control from the DB2 **access control** authorization exit point (DSNX@XAC) to handle DB2 **authorization checks**.

RACFDB2 – a free utility from **IBM** that helps migrate DB2 access control to RACF.

RACFICE *(rack-eff-ice)* – free analysis software from **IBM** that uses DFSORT ICETOOL to process output from the RACF DataBase Unload Utility and RACF SMF Data Unload Utility.

RACF-indicated – an attribute of a dataset with the RACF indicator on. The dataset can be used only if RACF is installed and either a RACF **profile** or entry in the **global access checking** table exists for the dataset.

RACF-protected – a RACF **profile** applies to this resource; datasets must also be **RACF-indicated**.

RACFRW – **RACF Report Writer**.

RACHECK request *(rack-check)* – has been replaced by the **AUTH request**.

RACINIT request *(rack-inn-itt)* – has been replaced by the **VERIFY request**.

RACLIST request *(rack-list)* – has been replaced by the **LIST request**.

RACLISTed profile – an **in-storage profile** for a RACF-defined resource created

by **LIST requests**.

RACROUTE macro *(rack-root)* – an Assembler macro used to call RACF for security functions.

RACSTAT request *(rack-statt)* – has been replaced by the **STAT request**.

RACTRACE *(rack-trace)* – free software from **IBM** that traces calls made to RACF through the **SAF** interface.

RACXTRT request *(rack-ex-tract)* – has been replaced by the **EXTRACT request**.

Radius – see **Steel-Belted Radius**.

RB-1 – see **CRYPTOCard RB-1 Challenge-Response Token**.

RC/Secure – security software from **Computer Associates** for DB2 in OS/390 environments.

read-only mode – a recovery mode of operation when RACF is enabled for sysplex communication that does not allow updates (except certain statistics) to the **RACF database**.

residual authority – references in the **RACF database** to deleted **user IDs** and **group names**.

residual group name – references in the **RACF database** to a deleted **group name**.

residual user ID – references in the **RACF database** to a deleted **user ID**.

Resource Access Control Facility (RACF) – security software from **IBM**, available either as part of **SecureWay Security Server for OS/390** or as a stand-alone product for OS/390 or VM.

resource group profile – a **general resource profile** in a **resource grouping class**.

resource grouping class – a RACF **class** in which **resource group profiles** can be defined.

resource profile – RACF **profiles** other than USER, GROUP, and CONNECT, protecting one or more resources.

RESTRICTED attribute – a **user attribute** that prevents the **user ID** from gaining access to protected resources that would otherwise be accessible through **global access checking**, **UACC**, or an ID(*) entry in the access list.

REVOKE attribute – a user attribute that does not allow the **user ID** any access to RACF-protected resources.

revoked user ID – a **user ID** with the **REVOKE attribute** set.

REXXTOOLS for VSE/ESA – software from **Open Software Technologies** that extends the functionality of REXX.

REXXTOOLS/MVS – software from **Open Software Technologies** that extends the functionality of REXX.

rights – **access authority**.

RioVision – Windows-based security administration software from **Vanguard Integrity Professionals** for RACF and DB2.

risk management – risk analysis, risk assessment, and actually dealing with the threat, be it reactive, proactive, or preventative action.

rogue program – intended to damage programs or data. **Trojan horses** are one example.

role – in **Tivoli** products, a functional grouping of user authorizations.

RRSF – **RACF Remote Sharing Facility**.

RRSF logical node connection – a state where two **RRSF nodes** can communicate with each other.

RRSF network – two or more **RRSF nodes** communicating with each other via an **RRSF logical node connection**.

RRSF node – one or more OS/390 system images sharing a **RACF database**, defined to RACF with a TARGET command.

RSA encryption – using the **encryption algorithm** invented by and named after Ron Rivest, Adi Shamirm, and Leonard Adleman, founders of **RSA Security**.

RTOKEN *(are-token)* – the RACF resource **security token**.

RtoR *(are-2-are)* – software from **Open Software Technologies** that provides REXX developers with **APIs** and templates for RACF access and other security functionality.

RUG *(rugg)* – RACF User Group.

RVARY *(are-very)* – the command an OS/390 system console operator would use to communicate with RACF.

System/390 Coupling Facility Structure Sizer Tool (CFSizer) – a free Web service from **IBM** that calculates storage usage within a **Coupling Facility** for, among other software, RACF.

SAF *(saff)* – **System Authorization Facility**.

SafeWord – **authentication** software from **Secure Computing**.

SAM *(samm)* – **Security Administration Manager**.

SAS *(sass)* – Statistical Analysis System.

SAS/C – C programming language compiler and run-time environment from **SAS Institute**.

SAS/CPE – now **IT Service Vision**.

SDS – **Safe Data System (SDS)**.

SDS Access One – a static-only Radius and Tacacs+ **authentication** server from **Safe Data System (SDS)**.

SDS Card Device – a credit-card-size **authenticator** from **Safe Data System (SDS)**.

SDS E-Access – an **authentication** server from **Safe Data System (SDS)** that can protect Web access to specific URLs.

SDS ikey *(eye-kk-ee)* – an **authenticator** from **Safe Data System (SDS)** that fits on a key chain and can be plugged into a USB port.

SDS Remote Access – a dynamic and static Radius and Tacacs+ **authentication** server from **Safe Data System (SDS)** that **authenticates** remote users.

SDS Smart Card – a **smart card** from **Safe Data System (SDS)**.

SDS Soft – software from **Safe Data System (SDS)** that acts as an **authenticator**.

SEA – **Software Engineering of America**.

Secure Sockets Layer (SSL) – a security protocol using **encryption** for network communication, indicated in Web browsers by the use of http<u>s</u>://.

secured sign-on – a RACF function that provides an alternative to a password.

SecureWay Security Server for OS/390 – security software from **IBM** that includes RACF, **DCE Security Server**, OS/390 **Firewall** Technologies, and **LDAP** Server.

SecurID 1100 Smart Card *(secure-eye-dee)* – a **smart card** from **RSA Security** that is no longer actively marketed.

SecurID 3100 Smart Card – a **smart card** from **RSA Security** that supports **Keon**.

SecurID Authenticator – any of several sizes and formats of hardware and software **authenticators** from **RSA Security**.

SecurID for the Palm Computing Platform – authentication software from **RSA Security**.

SecurID Key Fob (SD600) – a hardware **authenticator** from **RSA Security** that fits on a key chain.

SecurID PINPAD Card (SD520) *(pin-pad)* – a credit card-sized hardware **authenticator** from **RSA Security** with numeric entry keys.

SecurID Software Token – Windows-based **authentication** software from **RSA Security**.

SecurID Standard Card (SD200) – a credit card-sized hardware **authenticator** from **RSA Security** for the 3Com Palm Organizer.

SECURITRE *(secure-itree)* – an ADABAS and NATURAL security interface to RACF, **CA-ACF2**, and **CA-Top Secret from Treehouse Software (TSI)**.

Security Administration Manager (SAM) – multi-platform security management software from **SYSTOR Security Solutions**.

Security Bridge for LDAP – OS/390 Unix System Services software from **Security Integration** that allows controlled integration of **LDAP** with RACF, **CA-ACF2**, or **CA-Top Secret**.

Security Bridge for OS/390 – a security API from **Security Integration** that allows programmers to integrate applications with RACF, **CA-ACF2**, or **CA-Top Secret**.

security category – the name defined to RACF for a department or area within an organization whose members have similar security requirements.

security classification – use of a **security category** or **security level** to increase protection of sensitive resources.

security label – the name defined to RACF for a **security level** containing zero or more **security categories**.

security level – the name defined to RACF for a numeric security level, where the larger the number, the higher the security level.

Security Server – **SecureWay Security Server for OS/390**.

Security Solution Suite – see **QS/390**.

security token – a collection of identification and security information.

SecurPass *(secure-pass)* – security administration software from **Proginet** that integrates Windows NT security with other platforms' security, including RACF, **CA-ACF2**, and **CA-Top Secret**.

segment – the portion of a RACF **profile** defined by one template.

session – multiple transmissions protected by the same **encryption** key(s).

session stealing – **IP splicing**.

SETROPTS RACLISTed profiles *(sett-are-opts)* – **globally RACLISTed profiles**.

SideWinder – a network **access control** gateway from **Secure Computing**.

signature files – stored information on known viruses used by **anti-virus software**.

signed-on-from list – used for **persistent verification**, a list of users with a session in progress between two LUs.

SIGNON request – **RACROUTE macro** with REQUEST=SIGNON specified.

Single Sign-On (SSO) – a software product from **Computer Associates** that is now part of **eTrust**.

single-subsystem scope – DB2 classes with the subsystem ID as part of the **class** name.

single-system node – **single-system RRSF node**.

single-system RRSF node – an **RRSF node** consisting of one OS/390 system image.

site certificate – a RACF-managed **digital certificate** associated with a server, or network entity.

SiteMinder – security software for enterprise portals from **Netegrity**.

smart card – credit-card-sized **authenticator**.

SmartFilter – software from **Secure Computing** that monitors and restricts user access to Web sites.

SMF – **System Management Facilities**.

social engineering – a **hacker's** technique of impersonating a staff member in an attempt to deceive other staff, to gain access to an organization's computing resources.

Software Publishing Certificate (SPC) – a **PKCS** #7 signed-data object containing **X.509 digital certificates**.

SOLVE:Access – network security software for SNA networks from **Computer Associates**.

SonicWALL PRO – a 100Mbps Ethernet **firewall** from SonicWALL that also

provides **VPN encryption** for up to 100 branch offices.

SonicWALL PRO-VX – a 100Mbps Ethernet **firewall** from **SonicWALL** that also provides **VPN encryption** for up to 1,000 branch offices.

SonicWALL SOHO2 *(so-ho-2)* – a 100Mbps Ethernet **firewall** from SonicWALL, available in 10 and 50 user models, with optional **VPN encryption**.

SonicWALL TELE2 *(tell-ee-2)* – a 100Mbps Ethernet **firewall** for up to five users from **SonicWALL** that also provides **VPN encryption**.

SonicWALL XPRS2 *(ex-press-2)* – a 100Mbps Ethernet **firewall** from **SonicWALL** for organizations with public Web servers. **VPN encryption** is optional.

source user ID – the first of a pair of **user IDs** in functions such as **password synchronization**, where RACF changes the password of the **target user ID** whenever the source user ID's password changes.

SPC – **Software Publishing Certificate**.

SPECIAL attribute – a **user attribute** providing full control over all of the **profiles** in the **RACF database** and allows use of all commands, except **auditing**.

split database – a **RACF database** stored in more than one dataset.

spoofing – **IP spoofing**, or, alternatively, processing by an intermediate network node on behalf of the final destination node.

SSG – **Systems Support Group**.

SSL – **Secure Sockets Layer** protocol.

SSO – **Single Sign-On**, a software product from **Computer Associates** that is now part of **eTrust**.

ST-1 Software Token – software from **CRYPTOCard** that emulates a hardware **authenticator**.

standard access list – the portion of a **resource profile** that specifies the users and **groups** that may access the resource and, for each, the level of access.

started procedures table (ICHRIN03) – a list of started procedure names and the **user ID** or **group** that RACF assigns to each, as well as a generic entry indicating what to assign to started procedures not listed in the table.

STAT request *(statt)* – checks whether RACF is active or whether a specific **resource class** is defined to RACF and active, via the **RACROUTE macro** with REQUEST=STAT specified.

Steel-Belted Radius – a family of Radius **authentication** servers from **Funk Software**.

STOKEN *(ess-tt-oh-kenn)* – a **UTOKEN** associated with a user who has submitted work.

stream cipher *(ss-eye-ferr)* – **algorithms** that **encrypt** data as a continuous stream of bits.

structure – **cache structure**.

subject's distinguished name (SDN) – the **X.509**-defined name of the owner in a **digital certificate**.

superuser *(super-user)* – a **user ID** with minimal security restrictions.

SurfinGate – security software from **Finjan Software** that protects against Web content containing malicious ActiveX, Java, Visual Basic Script, and JavaScript code.

SurfinGuard – free security software from **Finjan Software** that protects against .exe and VBScript **worms** and **trojan horses**.

SurfinShield Corporate – security software from **Finjan Software** that monitors downloaded code for malicious behaviour.

symmetric algorithm – an **encryption** method that uses the same key to encrypt and decrypt.

System Authorization Facility (SAF) – an OS/390 **access control** interface that software can call without knowing whether RACF, **CA-ACF2**, or **CA-Top Secret** is installed.

System Management Facilities (SMF) – an OS/390 component that creates log entries (SMF records) detailing system resource usage, including RACF-specific information.

tape volume table of contents (TVTOC) – dataset names and other information for each tape file stored by RACF in the tape volume profile.

target node – the **RRSF node** that a given RRSF node is connected to via the TARGET command.

target user ID – the second of a pair of **user IDs** in functions such as **password synchronization**, where RACF changes the password of the target user ID whenever the **source user ID's** password changes.

template – defines the format of **profiles** in the **RACF database**.

three-phase key-exchange protocol – a **protocol** that creates an **authenticated encrypted** connection across a non-secure network.

Tivoli NetView Access Services – session manager from **Tivoli Systems** that provides hot-key swapping between multiple OS/390 on-line applications.

Tivoli Remote Control – software from **Tivoli Systems** that allows help desk staff to operate workstations and servers at a distance, effectively taking over the keyboard and mouse.

Tivoli SecureWay FirstSecure – security hardware/software from **Tivoli Systems** consisting of **Tivoli SecureWay Policy Director**, **IBM SecureWay Boundary Server**, Tivoli SecureWay **Public Key Infrastructure**, Symantec Norton AntiVirus, and **IBM SecureWay Toolbox**.

Tivoli SecureWay Global Sign-On – security software from **Tivoli Systems** that provides one ID and **password** across multiple platforms.

Tivoli SecureWay Policy Director – security software from **Tivoli Systems** that provides consistent **access control** across Web, TCP/IP, and other applications.

Tivoli SecureWay Policy Director for MQSeries – MQSeries **access control** software from **Tivoli Systems**.

Tivoli SecureWay Privacy Manager – security software from **Tivoli Systems** that

extends **Tivoli SecureWay Policy Director** to protect confidential customer information in e-Business applications.

Tivoli SecureWay Public Key Infrastructure – software from **Tivoli Systems** that uses **digital certificates** to secure Web applications.

Tivoli SecureWay Risk Manager – security software from **Tivoli Systems** that monitors for threats, provides detail information, and manages the response.

Tivoli SecureWay Security Manager – security software from **Tivoli Systems** centralizes management of **access control policy**.

Tivoli SecureWay User Administration – user administration software from **Tivoli Systems**.

Tivoli Virtual Private Network Manager – software from **Tivoli Systems** that automates the deployment of **VPN**.

TLS – **Transport Layer Security protocol**.

Token – **authenticator**.

TOKENBLD request – builds a **UTOKEN** via the **RACROUTE macro** with REQUEST=TOKENBLD specified.

TOKENMAP request – maps a **UTOKEN** in internal or external format, providing access to individual fields within the UTOKEN; coded as a **RACROUTE macro** with REQUEST=TOKENMAP specified.

TOKENXTR request – gets a **UTOKEN** via the **RACROUTE macro** with REQUEST=TOKENXTR specified.

Top Secret (TSS) – see **CA-Top Secret**.

tranquillity – keeping a **security classification** constant while in use.

Transaction Security System (TSS) – **IBM encryption** support software for transaction systems.

transport layer – the network layer responsible for quality of service and accurate delivery of information, ie error detection/correction occurs here.

Transport Layer Security protocol (TLS) – protects network communication between two applications.

trap door – a hidden method of avoiding security within an application.

triple DES – a **block cipher symmetrical algorithm** that encrypts data three times, with three keys.

trojan horse – hiding malicious code inside a useful program.

trust provider – software that decides whether to accept a file based on the **digital certificate** attached to it.

TSI – **Treehouse Software** (Inc).

TSS – **CA-Top Secret** or **Transaction Security System**.

TVTOC *(Ttee-vee-tock)* – **tape volume table of contents**.

two-factor authentication – **access** based on something a user knows and something a user has.

UACC – **Universal Access Authority**.

UADS *(you-adds)* – **User Attribute DataSet**.

UID – OS/390 Unix System Services user identification.

Unicenter TNG RACF Option – software from **Computer Associates** to integrate RACF with Unicenter TNG.

UniCERT *(you-ni-sir-t)* – a **certificate** management system from **Baltimore Technologies**.

Universal Access Authority (UACC) – the default access authority to a resource when a user or group has not been given explicit access authority to that resource. UACC is overridden by the **OPERATIONS** and **RESTRICTED** user attributes.

user attribute – special RACF privileges assigned to a user.

User Attribute DataSet (UADS) – TSO's **access control** file: a Partitioned DataSet (PDS) with a member for each user.

user certificate – a **digital certificate** associated with a RACF **user ID** that **authenticates** the user's identity.

user dataset – any dataset named with a RACF **user ID** as a high-level qualifier, though an installation can choose another qualifier level.

user ID – RACF's identification for a person using computer resources, usually no more than seven characters in length (a TSO restriction), beginning with a letter or '#', '$', or '@'.

user ID association – a relationship between two **user IDs** defined by the RACLINK command.

user identification – **user ID**.

user identification and verification – securely associating a user with a process, eg identification during log-on or batch job initiation by looking up the **user ID**; verification by checking the password.

user name – the 1-20 character name RACF stores for each **user ID**, typically including the surname of the user.

user profile – where RACF stores information specific to a single **user ID**.

UTOKEN *(you-token)* – the RACF user **security token**.

Vanguard Administrator – RACF administration and reporting software from **Vanguard Integrity Professionals**.

Vanguard Advisor – security event detection, analysis, and reporting software from **Vanguard Integrity Professionals** that combines information from RACF and **SMF**.

Vanguard Analyzer – RACF system integrity verification and **audit** software from **Vanguard Integrity Professionals**.

Vanguard Enforcer – RACF security **policy** management software from **Vanguard Integrity Professionals**.

verification – see **user identification and verification**.

VERIFY request – verifies the authority of a user to enter work into the system, via the **RACROUTE macro** with REQUEST=VERIFY specified.

VERIFYX request *(verify-ex)* – verifies a user and builds a **UTOKEN**, via the **RACROUTE macro** with REQUEST=VERIFYX specified.

virtual store – a **certificate store** that is a logical collection of other certificate stores.

Virus – any unauthorized code that propagates itself to (infect) other computers.

VM:Secure – see **CA-VM:Secure**.

VPN – **Virtual Private Network**.

VSAM *(vee-samm)* – Virtual Storage Access Method, a System/390 file access method capable of creating datasets that can be accessed sequentially, by record number or by key.

VTCP – a remote access **VPN** from **InfoExpress**.

WAP *(wapp)* – **Wireless Application Protocol**.

Web Single Sign-On (Web SSO) – a software agent from **Blockade Systems** that allows a user in a Web browser to log on once to gain access to multiple systems.

Web-Reset – Web-based self-serve **password** reset software from **Blockade Systems**.

WebSecure – Java software from **Baltimore Technologies** that runs on both a Web server and browser to provide **128-bit encryption**.

Wireless Application Protocol (WAP) – a set of **transport**, security, transaction, session, and application layer **protocols** that creates end-to-end secure connections for mobile communications.

Wireless Transport Layer Security (WTLS) – a **protocol** that provides the security layer of **WAP**.

workspace datasets – **VSAM** datasets used by RACF for queuing requests between **RRSF nodes**.

worm – a **virus** that creates multiple versions of itself in a computer's memory, effectively forcing other programs out.

WTLS – **Wireless Transport Layer Security**.

X.509 *(ex-dot-five-oh-nine)* – an international standard that defines the contents of **digital certificates**.

128-bit encryption – **DES encryption** using a 16-byte key that would require 3.4 x 10^{38} attempts to guess. In theory, this would require at least 5.4 x 10^{18} years for 1,000 2GHz processors.

40-bit encryption – **DES encryption** using a five-byte key that would require 10^{12} attempts to guess. Possible in a reasonable time with today's computers. Until recently, the most secure form of **DES** that could be exported outside the US and Canada.

4758 – **encryption** coprocessor from **IBM**, with models available for personal computers, RS/6000, AS/400, and System/390.

MISSING IN ACTION?

Did we miss any products, companies, or terms? Of course we did. Let us know what, and we'll research them for inclusion in a future issue.

Please contact the editor, Fiona Hewitt, at any of the addresses shown on page 2, or e-mail her at fionah@xephon.com

Roy Linnell
(Canada)   © Xephon 2001

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,* 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.

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

RACF-related organizations and products

This article stands alongside the *RACF glossary* published earlier in this issue (pages 28-56). It contains an alphabetical list of RACF-related software and hardware companies, standards organizations, and security user groups, and even a few individuals offering free software. Along with contact information, the entry for each software/hardware company also includes a list of relevant products. A brief description of each product can be found in the *RACF glossary*.

Some of the products listed overlap. Typically, the manufacturer has packaged several products together as an integrated solution or product family, and given the grouping another name.

Web site URL, address, and phone numbers are included for each company and organization. To find an appropriate e-mail address or a local office/distributor that handles your area, follow a *Contact*, *About Us,* or *Company Information* link on the Web site home page.

IBM

As so often happens, IBM is a special case. First, you undoubtedly already know how to find your local IBM office (check the *Yellow Pages*), which is really the best point of contact for information about the products listed here. Second, the IBM Web site is so large that more direct URLs are required to find product information on-line. The key IBM URLs are listed below. See also see Tivoli Systems (later in this article).

http://www.ibm.com/security/products
4758 Cryptographic Coprocessor
DCE Security Server
Distributed Key Management System (DKMS)
Embedded Security Subsystem
IBM eserver zSeries and IBM S/390 Cryptographic Coprocessor
IBM eserver zSeries and IBM S/390 PCI Cryptograhic Coprocessor (PCICC)
IBM Payment Registry
IBM SecureWay Firewall
IBM SmartCard Security Kit
RACF
SecureWay Security Server for OS/390
Transaction Security System (TSS)

http://www.tivoli.com/products/index/secureway_firstsecure ibm_secureway_bound_serve.html
IBM SecureWay Boundary Server

http://www.tivoli.com/products/index/secureway_firstsecure/ ibm_secureway_toolbox.html
IBM SecureWay Toolbox

http://www.s390.ibm.com/products/racf/vm.html
RACF for VM

http://s390.ibm.com/cfsizer/racf.html
S/390 Coupling Facility Structure Sizer Tool

http://www.s390.ibm.com/products/racf/goodies.html
CUTPWHIS
DBSYNC
IRRHFSU
KMIGRATE
OS390ART
PKISERV
RAC
RACFDB2
RACFICE
RACTRACE

NON-IBM

The list below gives contact and product details for non-IBM companies in the RACF environment.

ACL Services – http://www.acl.com
575 Richards St., Vancouver, B.C. V6B 2Z5, Canada. Tel: (888) 669 4225.
Products: ACL for MVS; ACL for Windows

ActivCard – http://www.activcard.com
6531 Dumbarton Circle, Fremont, CA 94555, USA. Tel: (800) 529 9499.
Products: ActivPack for IBM OS390/RACF

ADDC InfoTech – http://www.addc.com
Rauenmattenweg 7, CH-3225 Müntschemier, Switzerland. Tel: +41 32 313 4581.
Products: Khephren 2000 Application Framework – Authentication and Access Control Facility (AAC)

Advanced Software Products Group (ASPG) – http://www.aspg.com
3185 Horseshoe Drive South, Naples, FL 34104-6138, USA. Tel: (800) 662 6090.
Products: Easy RACF Query (ERQ); MegaCryption

American National Standards Institute (ANSI) – http://www.ansi.org
1819 L Street, NW, 6th Fl., Washington, DC, 20036. Tel: (202) 293 8020.

Baltimore Technologies – http://www.baltimore.com
Parkgate Street, Dublin 8, Ireland. Tel: +353 1 881 6000.
Products: Baltimore Enterprise Crypto System (ECS); FileSecure; FormSecure; KeyTools; MailSecure; MIMEsweeper; UniCERT; WebSecure

BETA Systems Software – http://www.betasystems.com
Alt-Moabit 97a,10559 Berlin, Germany. Tel: +49 30 399 26 0.
Products: BETA 88 RACF Manager; BETA 89 Automated Security Auditor; e-Security

Beyond Software – now part of NEON Systems.

Blockade Systems – http://www.blockade.com
2200 Yonge Street, Suite 1400, Toronto, Ontario M4S 2C6, Canada. Tel: (888) 898 9949.
Products: Blockade Authentication and Authorization Services (BAAS); Blockade Certificate Support (BCS); Blockade Enterprise Security System (BESS); Blockade Gateway Server (BGS); Blockade Password Synchronization Services; Blockade SNA Support (BSNAS); Blockade Synchronization Services (BSS); Blockade Web Support (BWS); Consistent Sign-On (CSO); Enterprise Security Server (ESS); Extended Access Control (EAC); Web Single Sign-On (Web SSO); Web-Reset

BMC Software – http://www.bmc.com
2101 City West Blvd., Houston, TX 77042-2827, USA. Tel: (800) 841 2031.
Products: CONTROL-SA; CONTROL-SA/Links; CONTROL-SA/PassPort; CONTROL-SA/Workflow; INCONTROL for Security Management

BSafe Software Solutions – http://www.bsafesolutions.com
Industrial & Business Park, P.O. Box 12325, Hertzlia, Israel. Tel: +972 9 952 5480.
Products: Bsafe/DB2 Security Server; MFsafe

CCITT – now ITU

CERT (Computer Emergency Response Team) – http://www.cert.org
CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA. Tel: (412) 268 7090.

Cole Software – http://www.colesoft.com
2256 Loma Rica Drive, Prescott, AZ 86303. Tel: (800) 932 5150.
Products: XDC/SE

Computer Associates International (CA) – http://www.cai.com
One Computer Associates Plaza, Islandia, NY 11749, USA. Tel: (800) 225 5224.
Products: CA-ACF2, CA-ALERT for VM, CA-ProAudit for DB2, CA-PanAudit Plus, CA-ProSecure for DB2, CA-Top Secret, CA-VM:Secure, eTrust, ProtectIT, RC/Secure, SOLVE:Access, Unicenter TNG RACF Option

Computer Security Institute (CSI) – http://www.gocsi.com
600 Harrison Street, San Francisco, CA 94107, USA. Tel: (415) 905 2626.
Products: NetSec

CONSUL Risk Management – http://www.consul.com
Marshalllaan 2, 2625 GZ Delft, Netherlands. Tel: +31 15 2513333.
Products: Consul/Audit for ACF/2, Consul/Audit for RACF, Consul/CVO, Consul/Enterprise Audit, Consul/RACF, Consul/RACF Administrator for Windows

Content Technologies – now part of Baltimore Technologies

Courion – http://www.courion.com
1881 Worcester Road, Framingham, MA 01701-5409, USA. Tel: (866) COURION.
Products: PasswordCourier; ProfileBuilder

CRYPTOCard – http://www.cryptocard.com
300 March Road, Suite 304, Kanata, Ontario K2K 2E2, Canada. Tel: (800) 307 7042.
Products: CRYPTOAdmin; CRYPTOCard RB-1 Challenge-Response Token; KT-1 Key Chain Token; PT-1 Palm Organizer Token; ST-1 Software Token

EKC Products (Eberhard Klemens) – http://www.ekcinc.com
10400 West Higgins Rd, Rosemont, IL 60018, USA. Tel: (847) 296 8010.
Products: E-HelpDesk; E-SRF Reporting Facility; ETF/A; ETF/R Firecall; ETF/T Firecall

Entact Information Security – http://www.entactinfo.com
5300 Six Forks Road, Suite 213, Raleigh, NC 27609, USA. Tel: (877) 368 2281.
Products: ENTACT!Admin; ENTACT!API; ENTACT!Audit; ENTACT!Request; ENTACT!Reset; ENTACT!Role; ENTACT!UniPass

Essential Software & Services – sold their products to ASPG, who combined them and renamed them ERQ.
Products: EIR (Essential Information Retrieval); ELP (Essential List Parsing); EFC (Essential Format Commands)

Falissard, Thierry – http://os390-mvs.hypermart.net/passtkt.htm
Products: PTKTGEN

Finjan Software – http://www.finjan.com
2860 Zanker Road, Suite 201, San Jose, CA 95134, USA. Tel: (888) 346 5268.
Products: SurfinGate; SurfinGuard; SurfinShield Corporate

Fischer International Systems (FISC) – http://www.fisc.com
3584 Mercantile Avenue, Naples, Florida 34104, USA. Tel: (941) 643 1500.
Products: Prio!

Funk Software – http://www.funk.com
222 Third Street, Cambridge, MA 02142, USA. Tel: (800) 828 4146.
Products: Steel-Belted Radius

Goldis Consulting Services (GCS) – http://www.goldisconsulting.com
100 Memorial Drive, Suite 11-3B, Cambridge, MA 02142, USA. Tel: (617) 492 4364.
Products: APFCHECK; PWCHECK; PWCHECK-PRO

IETF (The Internet Engineering Task Force) – http://www.ietf.org
(part of the Internet Society)

InfoExpress – http://www.infoexpress.com
170 S. Whisman Road, Suite B, Mountain View, CA 94041, USA. Tel: (650) 623 0260.
Products: CyberArmor, FireWalker Suite, VTCP

International Computer Security Association (ICSA) – now TruSecure Corporation

Internet Society – http://www.isoc.org
11150 Sunset Hills Road, Suite 100, Reston, VA 20190-5321, USA. Tel: (703) 326 9880.

ISO (International Standards Organization) – http://www.iso.ch
1, rue de Varembé, Case postale 56, CH-1211 Geneva 20, Switzerland. Tel: +41 22 749 01 11.

ISSA (International Systems Security Association) – http://www.issa.org
7044 S. 13th Street, Oak Creek, WI 53154, USA. Tel: (414) 768-8000.

ITSEC (UK IT Security Evaluation & Certification Scheme) – http://www.itsec.gov.uk
P.O. Box 152, Cheltenham, Gloucester GL52 5UF, UK. Tel: +44 1242 238739.

ITU (International Telecommunication Union) – http://www.itu.int
Place des Nations, CH-1211 Geneva 20, Switzerland. Tel: +41 22 730 5111.

JANUS Associates – http://www.janusassociates.com
1010 Summer Street, Stamford, CT 06905, USA. Tel: (203) 251-0200.
Products: I.C.U...MVS

LockStar – http://www.lockstar.com
1200 Wall Street West, Third Floor, Lyndhurst, NJ 07071, USA. Tel: (201) 508 3200.
Products: LockStar

Mercury Information Technology (M-Tech) – http://psynch.com
735 12th Ave. SW, Suite 203, Calgary, Alberta T2R 1J7, Canada. Tel: (403) 233 0740.
Products: P-Synch

National Bureau of Standards – renamed (1988) to National Institute of Standards and Technology (NIST)

NCSC (National Computer Security Center) – part of the National Security Agency (NSA)

NEON Systems – http://www.neonsys.com
14100 Southwest Fwy., Suite 500. Sugar Land, TX 77478, USA. Tel: (800) 505 NEON.
Products: Halo

Netegrity – http://www.netegrity.com
52 Second Ave, Waltham, MA 02451, USA. Tel: (800) 325 9870.
Products: Delegated Management Services (DMS); SiteMinder

Netlock Technologies – http://www.netlock.com
3230 E. Imperial Hwy., Suite 250, Brea, CA 92821, USA. Tel: (714) 792 1800.
Products: Netlock

NetMagic Systems – http://www.netmagicinc.com
One Erin Lane, Suite 200, Chestnut Ridge, NY 10977, USA. Tel: (877) 638 6244.
Products: NetMagic Pro

NIST (National Institute of Standards and Technology) – http://www.nist.gov

NSA (National Security Agency) – http://www.nsa.gov

Open Software Technologies – http://www.open-softech.com
P.O. Box 162652, Altamonte Springs, FL 32716-2652, USA. Tel: (407) 788 7173.
Products: REXXTOOLS for VSE/ESA; REXXTOOLS/MVS; RtoR

Pentland, Nigel – http://www.cairnleck.co.uk/nigel/readme.htm
Products: Nigel's RACF Utilities

Platinum – now part of CA

Proginet – http://www.proginet.com
200 Garden City Plaza, Suite 220, Garden City, NY 11530, USA. Tel: (516) 248 2000.
Products: CyberFUSION; SecurPass

RSA Security – http://www.rsa.com
20 Crosby Drive, Bedford, MA 01730, USA. Tel: (877) RSA 4900.
Products: ACE/Agents; ACE/Server; BSAFE Cert-C; BSAFE Cert-J; BSAFE Crypto-C; BSAFE Crypto-J; BSAFE S/MIME-C; BSAFE SSL-C; BSAFE SSL-J; BSAFE WTLS-C; Keon; SecurID 1100 Smart Card; SecurID 3100 Smart Card; SecurID for the Palm Computing Platform; SecurID Key Fob (SD600); SecurID PINPAD Card (SD520); SecurID Software Token; SecurID Standard Card (SD200)

Safe Data System (SDS) – http://www.safedata.com
67 rue Guillaume Dupuytren, Parc Euromédecine Bât Sienne, 34000 Montpellier, France. Tel: +33 467 91 71 05.
Products: SDS Access One; SDS Card Device; SDS E-Access; SDS ikey; SDS Remote Access; SDS Smart card; SDS Soft

SafeWord – now part of Secure Computing Corporation

SAS Institute – http://www.sas.com
SAS Campus Drive, Cary, NC 27513-2414, USA. Tel: (919) 677 8000.
Products: IT Service Vision; SAS/C

Schumann Security Software – now SYSTOR Security Solutions

SYSTOR Security Solutions – http://www.systor.com/index_e.html
6411 Ivy Lane, Suite 610, Greenbelt, MD 20770, USA . Tel: (301) 486 4600.
Products: Security Administration Manager (SAM)

Secure Computing – http://www.securecomputing.com
One Almaden Boulevard, Suite 400, San Jose, CA 95113, USA. Tel: (800) 692 5625.
Products: SafeWord; SideWinder; SmartFilter

Security Dynamics – now part of RSA Security

Security Integration – http://www.securityintegration.com
One Forbes Road, Lexington, MA 02421, USA. Tel: (800) 888-5031.
Products: Security Bridge for LDAP; Security Bridge for OS/390

Security Solutions – now part of JANUS

Software AG – http://www.softwareag.com
Uhlandstr. 12, 64297 Darmstadt, Germany. Tel: +49 6151 92 0.
Products: ADABAS SAF Security; Entire Security SAF Gateway; EntireX Security

Software Engineering of America (SEA) – http://www.seasoft.com
1230 Hempstead Turnpike, Franklin Square, NY 11010, USA. Tel: (800) 272 7322.
Products: RA/2; RA/7; RA/8; RAC/PACK

SonicWALL – http://www.sonicwall.com
1160 Bordeaux Drive, Sunnyvale, CA 94089-1209, USA. Tel: (888) 222 6563.
Products: SonicWALL PRO; SonicWALL PRO-VX; SonicWALL SOHO2; SonicWALL TELE2; SonicWALL XPRS2

SOS Data & Software – now part of Entact

Sterling – now part of CA

Systems Support Group (SSG) – now part of Vanguard

Technologic Software Concepts – http://www.technologic.com
4199 Campus Drive, Irvine, CA 92612, USA. Tel: (949) 509 5000.
Products: INCompliance

Tivoli Systems (an IBM company) – http://www.tivoli.com
9442 Capital of Texas Highway North, Arboretum Plaza One, Austin, Texas 78759, USA. Tel: (800) 284 8654.
Products: Tivoli NetView Access Services; Tivoli Remote Control; Tivoli SecureWay FirstSecure; Tivoli SecureWay Global Sign-On; Tivoli SecureWay Policy Director; Tivoli SecureWay Policy Director for MQSeries; Tivoli SecureWay Privacy Manager; Tivoli SecureWay Public Key Infrastructure; Tivoli SecureWay Risk Manager; Tivoli SecureWay Security Manager; Tivoli SecureWay User Administration; Tivoli Virtual Private Network Manager

Treehouse Software (TSI) – http://www.treehouse.com
409 Broad Street, Suite 140, Sewickley, PA 15143, USA. Tel: (412) 741 1677.
Products: AUDITRE. SECURITRE

Vanguard Integrity Professionals – http://www.go2vanguard.com
180 S. Anita Drive, Orange, CA 92868-3306, USA. Tel: (714) 939 0377.
Products: ezRESET; QS/390 (Quality Security/390 Suite); Quality Security Solution Suite; RioVision; Security Solution Suite; Vanguard Administrator; Vanguard Advisor; Vanguard Analyzer; Vanguard Enforcer

VeriSign – http://www.verisign.com
1350 Charleston Road, Mountain View, CA 94043, USA. Tel: (650) 961 7500.

William Data Systems – http://www.willdata.com
Arch House, 5 High Street, Old Oxted, Surrey, RH8 9LN, UK. Tel: +44 1 883 723 999.
Products: FTPalert

Roy Linnell
(Canada)
© Xephon 2001

Free weekly Enterprise IS News

A weekly enterprise-oriented news service is available free from Xephon. Each week, subscribers receive an e-mail listing around 40 news items, with links to the full articles on our Web site. The articles are copyrighted by Xephon – they are not syndicated, and are not available from other sources.

To subscribe to this newsletter, send an e-mail to news-list-request@xephon.com, with the word subscribe in the body of the message. You can also subscribe to this and other Xephon e-mail newsletters by visiting Xephon's home page, which contains a simple subscription form: see http://www.xephon.com

RACF news

Technologic has introduced its INCompliance audit software, which performs 200 checks for compliance against RACF best practices. As well as a Web-based Detail View of any non-compliance, it also provides instant e-mail notification of high-exposure changes or exceptions to your policy standards or rules.

For further information, contact:
Technologic Software Concepts, 4199 Campus Drive, Irvine, CA 92612, USA.
Tel: (949) 509 5000.
URL: http://www.technologic.com.

* * *

GCS is offering APFCHECK to audit the use of the z/OS, OS/390, and MVS Authorized Program Facility (APF). It's provided free with the company's PWCHECK and PWCHECK-PRO products. Both products audit the quality of passwords in a RACF environment, with PWCHECK-PRO adding a password cracker that combines educated guesses with a brute force approach.

For further information, contact:
Goldis Consulting Services (GCS), 100 Memorial Drive, Suite 11-3B, Cambridge, MA 02142, USA.
Tel: (617) 492 4364.
URL: http://www.goldisconsulting.com.

* * *

Tivoli e-Marketplace Manager Version 3.7 adds new features to enforce privacy policies, and to assess and manage security risks and vulnerabilities.

For further information, contact:
Tivoli Systems, 9442 Capital of Texas Highway North, Arboretum Plaza One, Austin, Texas 78759, USA.
Tel: (800) 284 8654.
URL: http://www.tivoli.com.

* * *

SAS has released Version 2.3 of IT Service Vision. New to this release is support for SAS Version 8 and inclusion of the Webhound product. Webhound can read and analyse all major Web server log formats.

For further information, contact:
SAS Institute, SAS Campus Drive, Cary, NC 27513-2414, USA.
Tel: (919) 677 8000.
URL: http://www.sas.com.

* * *

ASPG has announced version 4.2 of Megacryption, which enables any file in the MVS environment to be encrypted or decrypted. The main new feature is the support of public-key encryption.

For further information, contact:
ASPG, 3185 Horseshoe Drive South, Naples, FL 34104-6138, USA.
Tel: (800) 662 6090.
URL : http://www.aspg.com.
URL: http://www.megacryption.com.