ICHRCX02 – Erase temporary data sets – Version 2

# Purpose

IBM introduced Pervasive Encryption of data sets for a limited set of data sets. Those capable of being encrypted had to conform to the following criteria,

* Disk based data sets
* Permanent data sets
* SMS managed data sets
* Extended format data sets
* Data sets accessed using the QSAM or VSAM access methods

Tape data (clearly not encrypted) sets can be avoided or, if used for backups, can be populated using block-copy based tools such as DFSMSdss which copy the encrypted data set with decryption.

However, a large class of data sets which are not covered are temporary data sets. As temporary data sets are deleted at the end of the step in which they are last used, they are not normally accessible. However, the data contained in those data sets will still reside on the storage disk unless those data sets are specifically erased.

IBM supply a mechanism to erase temporary data sets, but it must be set system-wide and it will apply to all disk data sets, whether temporary or permanent. No facility is available to erase only temporary data sets, nor is there any selectivity for those data sets.

This version of the RACF post-processing exit ICHRCX02 is intended to fill that gap in capability.

# ICHRCX02

ICHRCX02 is called during processing of each RACF security check (RACROUTE REQUEST=AUTH) against a RACF resource. By alteration of the return and reason codes of the RACROUTE service, it is possible to request DFSMS to erase the data set in question.

# Logic

The supplied code first checks that the RACF check is not about to fail (i.e. deny access) or to abend. If so, then it simply returns to its caller without any change.

It then checks that the return code that is about to be returned to the caller of the RACROUTE REQUEST=AUTH is 0, 4 or 8. If any other code is present then the exit simply return to its caller, with nothing modified.

The code then checks that the caller has specified STATUS=ERASE. This is normally used by DFSMS to determine whether to erase the data set in question. If this has not been requested, the exit returns to its caller, with nothing modified.

Next, the exit checks that the caller has not specified DSTYPE=T (normally used for TAPE data sets). If this is the case, then the exit simply returns to the caller, with nothing modified.

If the resource class for the request is not “DATASET” then the exit returns to the caller with nothing modified.

After all the above checks have been completed the exit obtains a work area. It then calls an internal routine (EOS0000) to perform the checking for Erase-On-Scratch processing.

## EOS0000

This routine checks that the data set name conforms to the format of temporary data sets. This requires that the name is formatted as follows,

SYSnnnnn.Tnnnnn.RA000.\*\*

where,

“n” is any numeric value, and  
“\*\*” is an unspecified number of unchecked qualifiers.

If the name does not conform to these standards then it is not a temporary data set name and control returns to the mainline of ICHRCX02 with making any changes.

At this point we have established that we have a request for access to a temporary data set that has requested the ERASE status. Normally this status is decided by flags in the RACF resource protecting the data set. But temporary data sets have no profiles to protect them, so there is nowhere to store such information.

At this point this exit performs a local check for READ access to a resource in the FACILITY class. Included in the check is a request that the caller’s access to the resource be returned. The resource is named,

#EOS.sysplex.system.TEMPDSN

In the above resource name, “sysplex” is character name of the sysplex, with a maximum of 8 bytes, and “system” is the character name of the system, also with a maximum of 8 bytes.

This naming of the resource being checked is set up so that different systems and/or sysplexes that are managed using a common RACF database can be manipulated differently.

Decisions as to what actions are taken are made based on the access level to the resource from the current environment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Access to #EOS.sysplex.system.TEMPDSN*** | **NONE**, or resource not defined. | **READ** | **UPDATE** | **CONTROL** or higher |
| **Action taken** | No change to processing. EOS not requested. | No change to processing. EOS not requested.  Messages issued to show what would have happened if access was UPDATE. | Flags set to request EOS processing for this data set.  Messages issued to show what has happened. | Flags set to request EOS processing for this data set.  No messages issued. |

# How the exit is intended to be used

If the exit is active, but the resource #EOS.sysplex.system.TEMPDSN is not defined, no change to security processing will take place.

Once the resource check finds a profile to match, the application can be granted access to the #EOS.sysplex.system.TEMPDSN resource. If no access is granted then there will still be no change to security processing.

If READ access is granted, then messages will be issued as follows, showing the data sets which could be erased.

RCX02001I DSN=dddddddd.dddddddd.dddddddd.dddddddd.dddddddd

RCX02002I Current: RACFrc=rcrcrcrc, RACFrs=rsrsrsrs

RCX02003I #EOS.sysplex.system.TEMPDSN ,xxxx.xxxx.xxxx.xxxx

RCX02004I SAFrc=srsrsrsr ,RACFrc=rcrcrcrc, RACFrs=rsrsrsrs

The RCX02001I message shows the name of the data set being processed. The RCX02002I message shows the RACF return code and RACF reason code for the temporary data set resource after RACF mainline has checked the user’s access.

The RCX02003I message shows the name of the resource being checked, with the actual sysplex and system names in use, and the profile (shown as xxxx.xxxx.xxxx.xxxx above) which was used to perform the check.

The RCX02004I shows the SAF return code, the RACF return code and the RACF reason code found when checking the user’s access to the resource.

If the user’s access to the resource is increased to UPDATE then the above messages will be issued together with the message,

RCX02005I Erase-On-Scratch selected

The expectation is that the user running the application in question be granted first READ access, so that the data sets in question can be identified, then UPDATE access so the data sets can be erased.

Once the application is running as required, the access can be increased to CONTROL so that the messages are no longer issued.

# Installation

The exit will need to be assembled and then linked with the attributes RENT, REFR and placed in a suitable LPA library. A system IPL will be required to install the exit.

(Dynamic methods are available, but these will require specialist code and great care. See the author for more details.)

Lennie Dymoke-Bradshaw, RSM Partners  
04 June 2019 (Revised 06 April 2021)