IBM Systems MEDIA

Crypto Statistics Monitor Watches Resource Usage

Crypto Statistics Monitor provides you with the means to assess your cryptographic usage and determine any areas that might need attention.

By Eysha Powers
Ronald Edick

11/06/2017

Security is a principle concern in today's world, and the secure handling of data is an essential component of security. Cryptographic Support for z/OS V2.1 to z/OS V2.3, also known as ICSF FMID HCR77C1 or web deliverable number 17, provides a means for the secure and reliable handling of data with Crypto Statistics Monitor. It helps security administrators and capacity planners monitor the use of cryptographic resources and shows which resources are being used, how much these resources are being used, and who is using these resources.

Cryptographic Usage Statistics (Subtype 31)

Cryptographic usage statistics are recorded in SMF data sets. ICSF writes subtype 31 whenever cryptographic

usage tracking is enabled. Each Integrated Cryptographic Services Facility (ICSF) instance can track the usage of cryptographic engines (ENG), cryptographic services (SRV) and cryptographic algorithms (ALG) for that LPAR. Subtype 31 contains information about the cryptographic user's HOME address space job ID, SECONDARY address space job name, HOME address space user ID, HOME task level user ID and ASID. This is an optional feature with ICSF FMID HCR77C1 and usage tracking algorithms can be turned on or off depending on your needs. Cryptographic options include:

- ENG: The cryptographic engines include Crypto Express (CEX*) coprocessors, Regional Cryptographic Servers, CP Assist for Cryptographic Functions (CPACF) and cryptographic software
- SRV: ICSF callable services and User Defined Extensions (UDXes) perform operations like encryption and decryption, or signature and verification
- ALG: Algorithms describe how data is being handled and the key or hash bit length used in the operation, such as SHA-256 hashing of a data block

Statistics are recorded for each SMF recording interval. The usage/interval recording allows you to determine usage over various time periods.

Setting up Cryptographic Usage Monitoring

First, configure SMF to record ICSF events and set the time interval for recording. ICSF must be configured to track the wanted usage statistics. You can set up SMF by using an SMF parameter member that is contained in the system PARMLIB. An example of an SMF parameter member is:

```
DSNAME(HLQ.SMF.MANA,HLQ.SMF.MANB)          /* SMF data sets                */
INTVAL(15)                                 /* INTERVAL =  15 MINUTES       */
SYNCVAL(00)                                /* SYNCHRONIZATION =  00 MINUTES */
SYS(TYPE(0,3,82(13:23,31,40:42),83,134))   /* Include subtype 31           */
```

The INTVAL(xx) parameter determines how often usage statistics are recorded. For example, a value of 15 triggers ICSF to record the usage every 15 minutes. The SYNCVAL(xx) parameter synchronizes the recording interval with the end of the hour on the TOD clock (e.g., a value of 00 triggers ICSF to start recording the usage at the end of the hour). The SYS(TYPE(*)) parameter specifies the type of records that are being recorded. These ICSF usage events are recorded in SMF type 82, subtype 31 records.

Next, set up the usage to be tracked in the ICSF installation options data set. There are two options that control usage tracking: STATS and STATSFILTERS. The STATS option enables usage tracking for various cryptographic statistics. Keywords may be combined to track multiple statistics. If the STATS option is not specified, usage tracking is not done. Syntax of the STATS and STATSFILTERS parameters are:

```
STATS(ENG,SRV,ALG)
STATSFILTERS(NOTKUSERID)
```

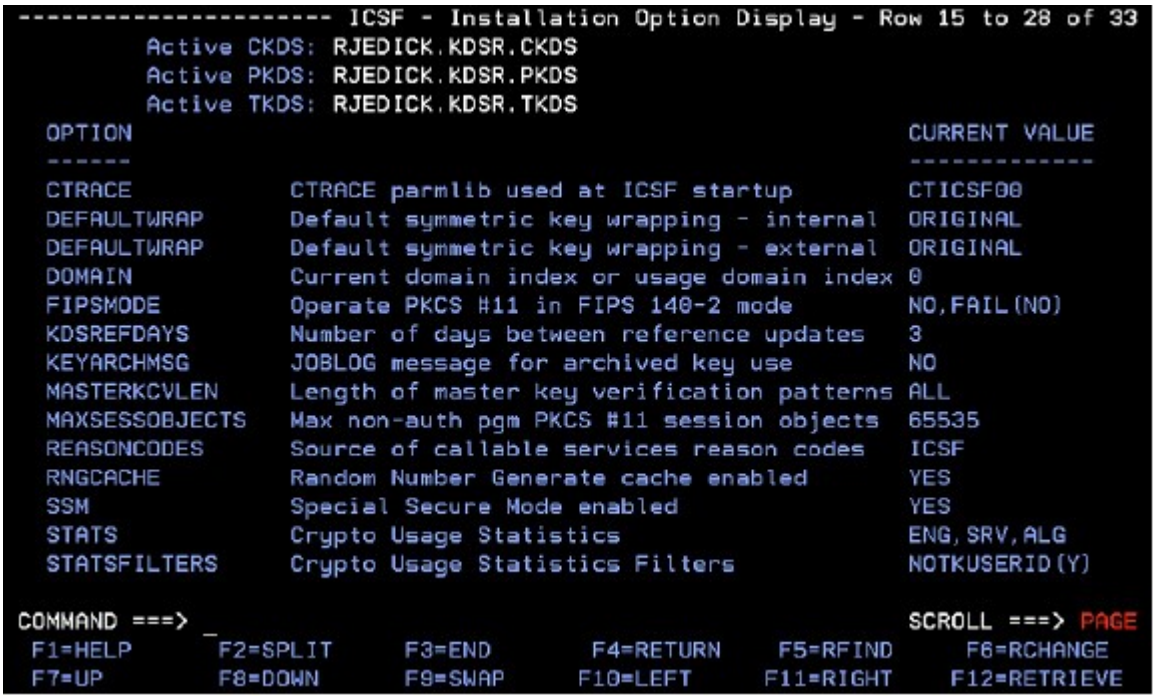
ENG enables usage tracking of cryptographic engines and supports Crypto Express cards, regional cryptographic servers, CPACF and software. SRV enables usage tracking of cryptographic services and supports ICSF callable services and UDXes only. ALG enables usage tracking of cryptographic algorithms and supports cryptographic algorithms that are referenced in cryptographic operations. There’s limited support for key generation, key derivation and key import.

STATSFILTERS controls the identifier that’s used to collect usage information. Usage is tracked by unique user and job identifiers. The user identifier consists of an address space userid and a task level userid. For applications such as CICS, which generate a unique task level userid for each transaction, a large number of

SMF records can be generated. To prevent this problem, use the STATSFILTER(NOTKUSERID) option. Specifying STATSFILTER(NOTKUSERID) ignores the task level userid and uses only the address space userid when creating the job/user identifier. STATSFILTER(NOTKUSERID) reduces the number of SMF records written.

Displaying Usage Settings

You can view the current usage settings from either the ICSF Installation Option Display panel or from the MVS console. In Figure 1, all usage (i.e., engines, services and algorithms) is tracked.



STATS information can also be obtained by issuing the Display ICSF command (D ICSF,OPT) from the MVS console. The below example shows that all usage is being tracked. STATSFILTERS information isn't displayed.

```
CSFM668I 11.06.42 ICSF OPTIONS 744
  SYSNAME = SY1          ICSF LEVEL = HCR77C1
    LATEST ICSF CODE CHANGE = 05/02/17
     .
     .
     .
   STATS:
     SY1       ENG, SRV, ALG
```

Modifying Usage Monitoring

The SETICSF command can be used to dynamically change cryptographic usage tracking options. Note: STATSFILTERS isn't supported.

To change the cryptographic usage settings to monitor only crypto engine usage across a sysplex, issue the SETICSF OPT,STATS=(ENG),SYSPLEX=YES command.

To stop all cryptographic usage tracking, issue the SETICSF OPT,STATS=NONE,SYSPLEX=YES command.

SMF Crypto Statistics Records

Cryptographic usage statistics are recorded in SMF data sets. If there were usage events, usage records are created at the end of each SMF recording interval. The usage data that is collected is based on unique job/user identification. The record contains the job/user identifiers, information about the time interval, and the cryptographic usage counts associated with the event.

```
An example of a crypto usage record is:

Subtype=001F Crypto Usage Statistics
   TME... 002E0D35 DTE... 0117118F SID... SP21    SSI... 00000000 STY... 001F
   INTVAL_START.. 04/28/2017 12:20:15.604977
   INTVAL_END.... 04/28/2017 12:25:15.376901
   USERID_AS..... USERABC
   USERID_TK.....
   JOBID......... J0000192
   JOBNAME....... TCPKS009
   JOBNAME2......
   PLEXNAME...... LOCAL
   DOMAIN........ 0
   ENG...CARD...5P59/97006060... 5
   ENG...SOFTW   ... 6
   ALG...ECCBP160... 2
   SRV...CSF1TRC.... 3
   SRV...CSF1TRD.... 3
   SRV...CSF1PKS.... 1
   SRV...CSF1PKV.... 1
```

The above example shows that the usage event that is recorded is for job/user=J0000192/USERABC. It occurred on system SP21 and used crypto domain 0. The time interval for the event is between 12:20 and 12:25 on 28 April. In the event, the CSF1PKS (Private Key Sign) and CSF1PKV (Public Key Verify) services were each called once. There were two ECC 160 bit Brain Pool algorithm counts (one for each service). The event required five cryptographic card calls and six cryptographic software calls.

```
Subtype=001F Crypto Usage Statistics
  TME... 002E0D35 DTE... 0117118F SID... SP21    SSI... 00000000 STY... 001F
  INTVAL_START.. 04/28/2017 12:20:15.604977
  INTVAL_END.... 04/28/2017 12:25:00.376901
  USERID_AS..... USERABC
  USERID_TK.....
  JOBID......... J0000166
  JOBNAME....... TCOWH001
  JOBNAME2......
  PLEXNAME...... LOCAL
  DOMAIN........ 0
  ENG...CARD...5P59/97006060... 5
  ENG...CPACF   ... 2
  ALG...RSA1024.... 2
  ALG...SHA1....... 2
  SRV...CSF1TRC.... 3
  SRV...CSF1TRD.... 3
  SRV...CSF1OWH.... 2
```

The above example shows that the usage event that is recorded is for job/user= J0000166/USERABC. It also occurred on system SP21 and used crypto domain 0. The time interval for the event is between 12:20 and 12:25 on 28 April. In the event, the CSF1OWH (One Way Hash) service was called twice. The event required the use of the RSA 1024 bit algorithm twice and the SHA1 algorithm twice. The event required five cryptographic card calls and two CPACF calls.

Displaying Card Usage

You can find the total number of cryptographic engine requests by issuing the Display ICSF command with one of the two options: For CEX* hardware (D ICSF,CARDS) or for Regional Cryptographic servers (D ICSF,RD). The cryptographic engine requests is an aggregate number that shows the total number of requests over the entire time span that ICSF has been active. It displays only the cryptographic hardware requests. It doesn't display CPACF or software requests. The request that is filed does not require STATS to be enabled.

```
D ICSF,CARDS command is:

  CSFM668I 09.17.58 ICSF CARDS 222
  ACTIVE DOMAIN = 000
  CRYPTO EXPRESS5 ACCELERATOR 5A40
    STATUS=Active
    REQUESTS=0000000015  ACTIVE=0000
  CRYPTO EXPRESS5 COPROCESSOR 5C49
    STATUS=Active               SERIAL#=99EA6020 LEVEL=5.2.27z
    REQUESTS=0000000144  ACTIVE=0000
```

The above example shows that there have been 15 requests to the CEX5A and 144 requests to the CEX5C since ICSF initialization.

Securing the Way

Crypto Statistics Monitor provides you with the means to assess your cryptographic usage and determine any areas that might need attention. By determining which applications are using which cryptographic engines, services and algorithms, you can ensure that you're operating in the most secure manner. Using the Crypto Statistics Monitor can also help you tune your systems for optimal performance.

Rita M. Beisel contributed to the technical and editorial review of this article.

About the author
Eysha Powers is a cryptographic software designer and developer for the z/OS Integrated Cryptographic Services Facility.

Ronald Edick is a developer/tester for the z/OS Integrated Cryptographic Services Facility.