

BaphCorp



KDSLIST

User's Guide

Version 3.3

March 2024

Alain Barthélemy

Table of contents

HOW DOES KDSLIST WORK	4
KDSLIST NEEDS	4
<i>Using KDSLlist</i>	4
The DDnames	4
The Syntax	5
Return Codes.....	5
USAGE ENVIRONMENTS	6
<i>KDSLlist under TSO</i>	6
<i>KDSLlist in Batch</i>	6
RESULTS OBTAINED	7
KDSLlist of a CKDS	7
KDSLlist of a PKDS.....	8
KDSLlist of a TKDS	8

Figures

<i>Figure 1 : Calling KDSL</i> LIST in TSO online.....	6
<i>Figure 2 : Calling KDSL</i> LIST in Batch.....	6

How does KDSLIS work

KDSLIS is a utility written in Rexx allowing you to list the contents of an ICSF KDS (CKDS, PKDS or TKDS). It has the particularity of being able to work on an "offline" file, that is to say non-active (for example a backup) while the ICSF browser only works on active databases. KDSLIS only lists a small part of the KDS information, its role is above all to have a quick idea of the content of a KDS file and to see if the keys are in line with the right MasterKey used to create the KDS.

KDSLIS needs

KDSLIS expects a sequential file as input, but KDS are VSAM files, it may be therefore necessary to flatten the file before submitting it to KDSLIS. If you don't, KDSLIS will issue an IDCAMS REPRO itself on a temporary file before starting processing (This option is easier and recommended).

In its process KDSLIS automatically detects the type of KDS (CKDS, PKDS or TKDS) as well as its format (Fixed, Variable, KDSR or KDSRL). Note that the KDSRL format is not distinguishable from KDSR if you use a sequential file on input.

Using KDSLIS

When called, KDSLIS accepts two optional parameters: a Dsname and the expected output format. The Dsname can be replaced by an asterisk in which case KDSLIS will use the Dsname associated with the DDname KDS.

KDSLIS can be called either in Batch (the most common) or directly in TSO online.

In TSO online the input file (sequential or VSAM) must previously exist.

The DDnames

KDSLIS uses the following DDnames :

KDS : This is the KDS file in VSAM or its sequential copy. (Optional)
OUT : File which will contain the report (necessary for the *Long* format).
SYSTSPRT: Standard Sysout (replaces the OUT file if it is not defined)

The Syntax

KDSLIST [*Dsname Format*]

Description

Dsname As a general rule, it is the name of the file which will appear at the top of the list. This allows you to indicate the real name of the KDS cluster when you provide a sequential file to KDSLIST.

However, in certain situations its use may change :

- If the KDS DDname is not defined, the Dsname will be that of the KDS in VSAM or in sequential which will be taken as input to KDSLIST.
(Ex: When calling with TSO online)
- If the Dsname is replaced by an asterisk (*) the Dsname taken into account will be that of the file associated with the DDname KDS.

Format Requested output format (**Short**, **Medium** or **Long**). Each format can be indicated with at least 1 character.

For the **Long** format you need a minimum Lrecl of 201, for the **Medium** format an Lrecl of 132 and for the **Short** format, you need 80.

The default value is **Short** in TSO online, **Medium** in Batch, this being weighted by the Lrecl of the OUT file.

Notes :

- The **Dsname** parameter is mandatory during a TSO online call.
- The format is automatically adapted if it does not correspond to the output used : In TSO online **Short** is imposed and **Medium** replaces **Long** if you omit the DDname OUT.
- If you want to indicate only the format, **Dsname** can be replaced by "*" which represents the default value.

Return Codes

0	Report ended correctly.
4	VSAM file not supported as output (DDname OUT).
6	The DDname indicated is an <i>instream</i> file, it's not supported.
12	DDname not allocated.
14	Lrecl of the OUT file is too short for the requested format.
24	The file indicated doesn't exist (OUT or KDS).
27	File unusable (OUT or KDS).
29	I/O Error on KDS file.

Usage Environments

KDSLST under TSO

KDSLST may be called under TSO by typing KDSLST in front of the KDS file or its sequential version. The Rexx named KDSLST (example below) must be stored in one of the libraries defined in the DDname SYSEXEC or SYSPROC under ISPF.

The result obtained is succinct because it will necessarily be the *Short* format.

```
/* Rexx : Calling KdsList */
  Address TSO
  "EXEC 'SCSF.ICSF.EXEC(KDSLST)'  '"translate(arg(1)," ","'")'"
  Return Rc
```

Figure 1 : Calling KDSLST in TSO online

KDSLST in Batch

For a Batch call, the following example shows the two possibilities, either flattening the KDS or using it directly on the VSAM file (better).

Don't forget that the OUT file must have a minimum LRECL of 201, the better way is to set a RECFM VB and an LRECL of 512 so you will be ready for future developments.

```
//KDSLST1 JOB (BAPH), 'List Icsf KDS',MSGCLASS=S,CLASS=A,
//          MSGLEVEL=(1,1),NOTIFY=&SYSUID,REGION=8M
//*
//*   - List the content of an ICSF KDS -
//*
//          SET PKDS=SCSF.ICSF.PKDS          ) Vsam
//          SET CKDS=SCSF.ICSF.CKDS          ) files
//*
//* - Copy the CKDS on a flat file -
//COPYKDS EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//FILEIN  DD DISP=SHR,DSN=&CKDS.
//FILEOUT DD DISP=(,PASS),DSN=&&TMP,UNIT=3390,
//          SPACE=(CYL,(100,50),RLSE),RECFM=VB,LRECL=32756
//SYSIN   DD *
//          REPRO IFILE(FILEIN) OFILE(FILEOUT)
//*
//* - Analysis of CKDS file -
//LISTCKDS EXEC PGM=IKJEFT1B,PARM='%KDSLST &CKDS. Long'
//SYSEXEC DD DISP=SHR,DSN=SCSF.ICSF.EXEC
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD DUMMY
//KDS     DD DISP=(OLD,PASS),DSN=&&TMP    < Flat file
//OUT     DD DISP=SHR,DSN=TZSSY03.RESULT.LISTE(CKDSLST)
//*
//* - Analysis of PKDS file directly -
//LISTPKDS EXEC PGM=IKJEFT1B,PARM='%KDSLST * Long'
//SYSEXEC DD DISP=SHR,DSN=SCSF.ICSF.EXEC
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD DUMMY
//KDS     DD DISP=SHR,DSN=&PKDS.          < VSAM file
//OUT     DD DISP=SHR,DSN=TZSSY03.RESULT.LISTE(PKDSLST)
//
```

Figure 2 : Calling KDSLST in Batch

Results obtained

The columns have a meaningful title, however some information should be noted.

- The MKVP of the header is the one which corresponds to the MasterKey present on the crypto card, the one in the column named **Mkvp**, is the MKVP of the MasterKey that encrypted the key; these two pieces of information should be identical, if this is the case the **Mk?** column will be filled with **Ok**, otherwise it will indicate **Err**. If the **Mk?** column indicates a dash it means that the MKVP of the key is not present on this record.
- The last three columns are only populated in KDSR or KDSRL files if the STATS(SRV) option is active.
- Quantum keys Kyber and Dilithium are supported.

KDSLlist of a CKDS

26 Mar 2024 * * K d s L i s t (3.2) * * 19:04:04 (Long)												
- Creation - * * C K D S * * - Last update -												
14-02-2024 18:31:58												
> PAPPER.CSF.CKDS <												
Format : KdsrL												
Mkvp : DES=6789B754F366D500 - AES=AC5A2B16E70B0978												
Label	Type	Algo	Size	Mkvp	Mk?	CreDate	CreTime	Arch Date	End Valid	Last Use	Last Service	
CLEF.APPAC.ZT50.GUICHET.V0001	DATA	AES	256	AC5A2B16E70B0978	Ok	28-02-2024	11:01:59	-	-	28-02-2024	CSFKRR2	
CLEF.APPCP.ZT50.COMPTA.V0001	DATA	AES	256	AC5A2B16E70B0978	Ok	28-02-2024	11:02:15	-	-	28-02-2024	CSFKRR2	
CLEF.APPGA.ZT50.RH.V0001	DATA	AES	256	AC5A2B16E70B0978	Ok	28-02-2024	11:02:30	-	-	-	-	
CLEF.PRDCSF.QSAFAES	CIPHER	AES	-	AC5A2B16E70B0978	Ok	03-03-2024	15:45:57	-	-	09-03-2024	CSFPKE	
CLEF.PRDCSF.ZT51.TEST2	DATA	AES	256	AC5A2B16E70B0978	Ok	27-02-2024	16:35:34	-	-	05-03-2024	CSFKRR2	
CLEF.PRDJES.SPOOL	DATA	AES	256	AC5A2B16E70B0978	Ok	26-02-2024	14:22:33	-	-	26-02-2024	CSFKRR2	
CLEF.PRDRAC.ZT50.BASESECU	DATA	AES	256	AC5A2B16E70B0978	Ok	25-02-2024	11:36:17	-	-	06-03-2024	CSFKRR2	
PASSTICKET.HMAC.KEY	MAC	HMAC	-	-	-	27-02-2024	16:16:20	-	-	-	-	
8 Keys read												



KDSLlist of a PKDS

26 Mar 2024	* * K d s L i s t (3.2) * *	19:03:42	(Long)
- Creation -	* * P K D S * *	- Last update -	
14-02-2024 18:32:36			
	> PAPPER.CSF.PKDS <		
Format : KdsrL			
Mkvp : RSA=4F4214F7E1F74BE8 - ECC=FC87505E9A066845			
2D81F694B9898883			
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+			
Label	Algorithm	Type	Size Mkvp Mk? CreDate CreTime End Valid Last Use Last Service
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+			
CLEF.PRDCSF.KYBER	Kyber_r2	1024	- FC87505E9A066845 Ok 02-03-2024 19:58:54 - 09-03-2024 CSFPKE
CLEF.PRDCSF.TEST	RSA	-	2048 FC87505E9A066845 Ok 01-03-2024 14:22:16 - 09-03-2024 CSFPKE
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+			
2 Keys read			

KDSLlist of a TKDS

29 Jun 2023	* * K d s L i s t (2.6) * *	15:50:50	(Long)
- Creation -	* * T K D S * *	- Last update -	
05-06-2023 19:53:01			
	> PAPPER.CSF.TKDS <		
Format : Kdsr			
Mkvp : P11=.	- RCS=.		
.			
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+			
! Label	! SeqNum	! Att	! Token ! Type ! Size ! Relate ! CreDate ! CreTime ! End Valid ! Last Use ! Last Service !
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+			
! TOKEN.PRDMFA.BIZPLEX1.KEYS	! -	! -	! TOKN ! - ! - ! HCR77D2 ! 06-06-2023 ! 00:21:55 ! - ! - ! - !
! TOKEN.PRDMFA.BIZPLEX1.KEYS	! 00000002	! C1r	! SECK ! AES ! 256 ! AZFTOTP.AESKEY ! 06-06-2023 ! 13:52:45 ! - ! - ! - !
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+			
2 Keys read			