

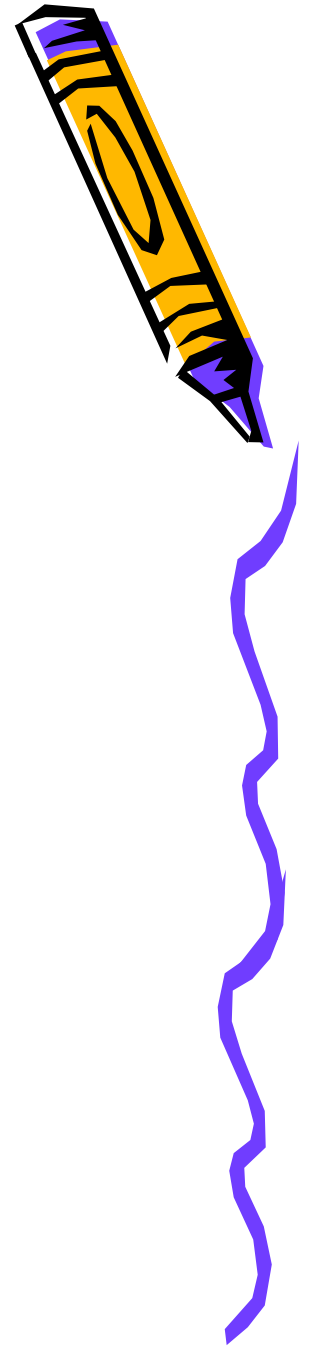
WAVV 2010

KEY15 vs KEYO
So Easy A Child Can Do It!

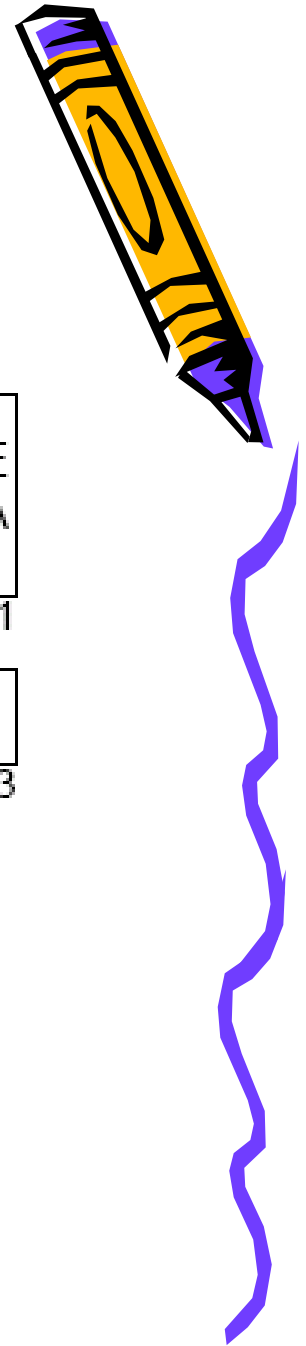


Storage Keys

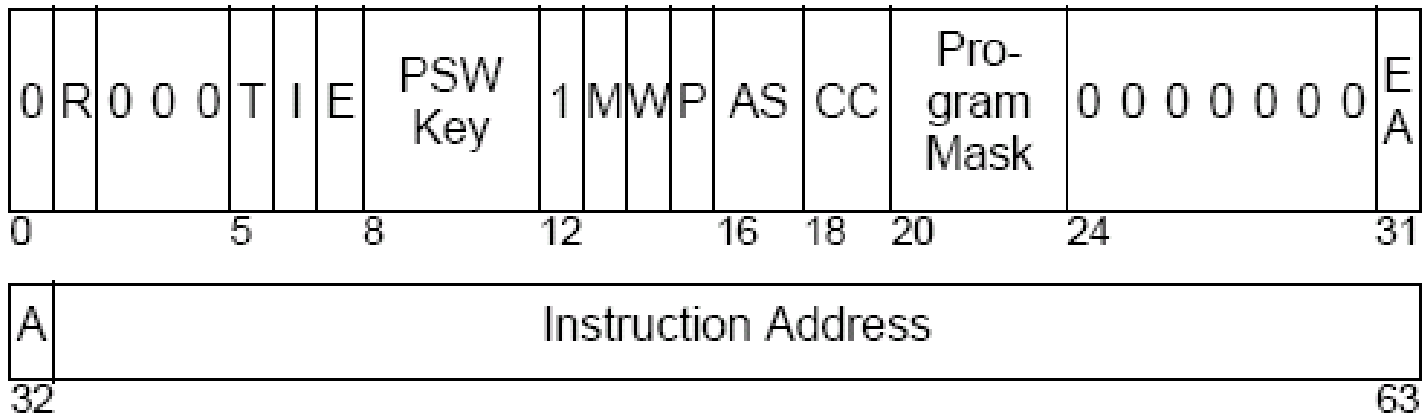
- Memory is protected by a storage key
- Protected on a 4K boundary
- Key 0 - highest protection
- Key 1 - BG
- Key 2 - FB
- Key 3-C - FA-F1
- Key D - Dynamic Partitions
- Key E and F - AFAIK Unused



PSW



ESA/390 PSW



PSW 07CD4007 00500346

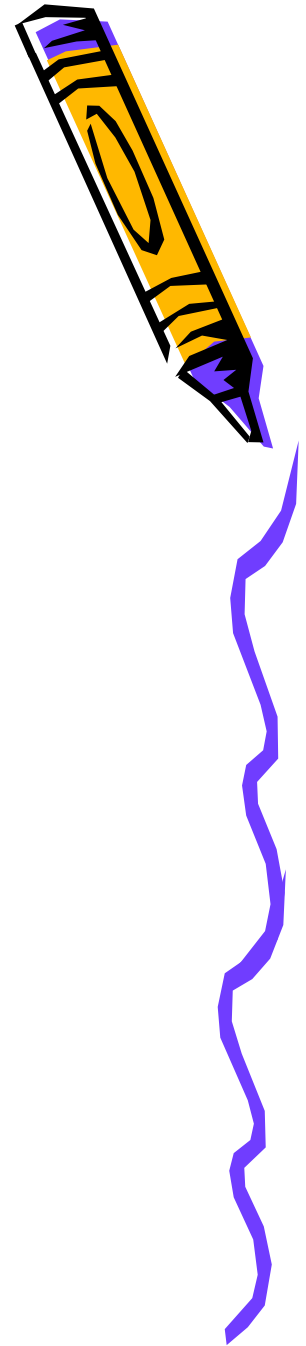


Changing Key

- **SVC** -
 - ICM R1,15,=X'FF000000' use for key 0
 - SVC 13

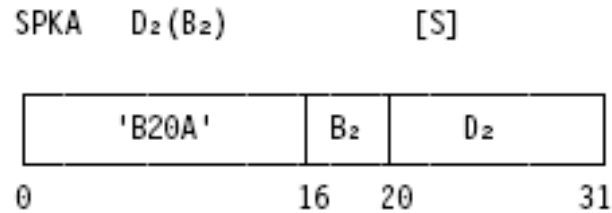
 - ICM R1,15,=X'FF0000FF' use for key user
 - SVC 12
- **MODESET** -
 - MODESET KEY=ZERO use for key 0
 - MODESET KEY=USER use for key user

OR...



- SPKA

SET PSW KEY FROM ADDRESS

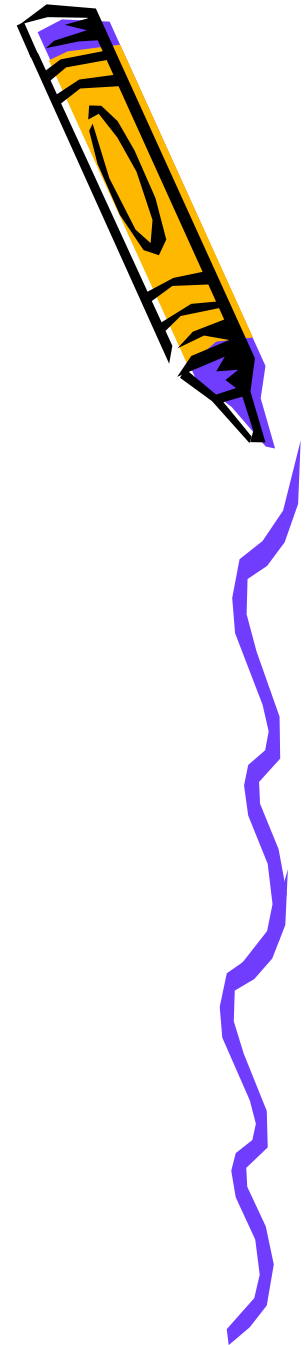


The four-bit PSW key, bits 8-11 of the current PSW, is replaced by bits 24-27 of the second-operand address.

The second-operand address is not used to address data; instead, bits 24-27 of the address form the new PSW key. Bits 0-23 and 28-31 of the second-operand address are ignored.

Special Conditions

In the problem state, the execution of the instruction is subject to control by the PSW-key mask in control register 3. When the bit in the PSW-key mask corresponding to the PSW-key value to be set is one, the instruction is executed successfully. When the selected bit in the PSW-key mask is zero, a privileged-operation exception is recognized. In the supervisor state, any value for the PSW key is valid.



SPKA

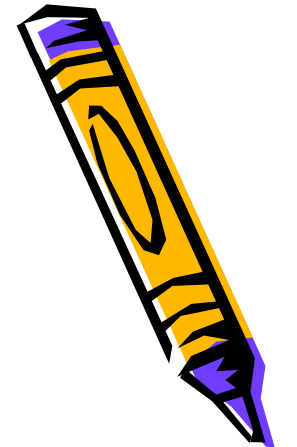
Control Registers

3	32-47	PSW-key mask	Instruction authorization
	48-63	Secondary ASN	Address spaces

```
MODESET KEY=ZERO
MODESET MODE=SUP
STCTL R3,R3,WORK
OC  WORK(2),=X'0003' ALLOW KEY E AND F
LCTL R3,R3,WORK
MODESET KEY=USER
MODESET MODE=PROB
ORG *-32
DC X'00000008'
ORG
```



SPKA



A minor modification to this:

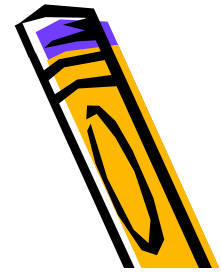
```
          DC      CL8'MODESET '           EYECATCHER
          DC      CL8'07/24/97'
MODESET  DS      OH                       SERVICE ENTRY POINT
*        AMODESW  SET, AMODE=31, WR=(R4)   GET AMODE 31
          LA      R4, DMS0396A             SET ADDRESS FOR BSM
          O       R4, BITOOMSK            TURN ON AMODE 31
          DC      OH'0', X'0B', AL.4(0, R4)
DMS0396A EQU  *
*        SET UP MODE AND KEY FIELDS
          SR      R3, R3                   NO PUBL. STOR. KEY
```

To

```
MODESET  DS      OH
          SAM31
          LA      R3, X'0003'
          SLL    R3, 16
          NOPR   0, 0
```



SPKA



```
// JOB KEYPREP
// EXEC DTRIATTN,PARM='ALTER 188E8'
// EXEC IESWAIT,PARM='01'
// EXEC DTRIATTN,PARM='15 IGNORE  '
// EXEC IESWAIT,PARM='01'
// EXEC DTRIATTN,PARM='15 010D41300003893000100700'
```

original code is here (from console)

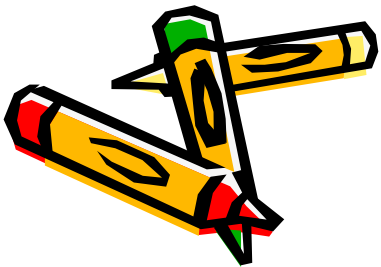
```
OLD DATA: 4140D688 5640081C 0B041B33 5820026C
```

We made a permanent patch to the supervisor.
Must have one dummy MODESET MODE=PROB
per program execute. Job control resets it.

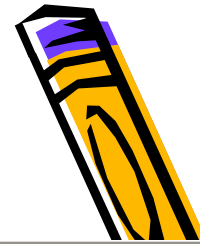


Protection Key Caveat

- IBM has made a special exception for protection key 9 (user key for F4). Any memory with KEY 9 can be touched without having KEY 9 set in the PSW. This was designed for CICS/TS.



DUMPER SHOWS KEY



JOBNAME=GIL DATE=04/07/2010 TIME=15:33:33 CPUID=00097AC2 20988000 COMP=5686CF806C

OS01I THE OPERATOR CANCELED THE JOB
OS00I JOB GIL CANCELED
OS07I PROBLEM PROGRAM PSW = 07DD0000 80843706

SYMPTOM RECORD

00509120	00000001	E2D9F2F0	F9F8F0F9	F7C1C3F2	F1F57AF3	F37AF3F3	7AF0F0F1	F061F0F4	00SR209809
00509140	61F0F7F1	F47AF3F3	7AF3F37A	F0F0F5F6	F8F6C3C6	F8F0F6F0	F1C30000	E2C3D7D9		/0714:33:33:
00509160	C5D84040	00000000	00000000	003F0074	000000B3	002B00B3	000000DE	00000000		EQ
00509180	00000000	00000000	00000000	00000000	00000000	00000000	C1C261E2	F2F4F0F0	
005091A0	40D9C5C7	E261C6C6	C6C6C640	D9C5C7E2	61F0C4F4	C2F640D4	E261F0E2	F0F1C940		REGS/FFFF
005091C0	D9C9C4E2	61C7C9D3	40D6C6C6	E261F0F0	F3F0F3F7	F0F640D1	D6C26DD5	C1D4C57E		RIDS/GIL OFF
005091E0	C7C9D340	40404040	40C4E4D4	D7C5C46D	C4C1E3C1	7ED7F160	D7C1D9E3	C9E3C9D6		GIL DUM
00509200	D540									N

PSW AND REGISTERS OF ENDING TASK

PSW 07DD0000 80843706

GR 0-7 00000150 00837380 072AE6C8 005416D8 00000000 005487F4 00000000 00842000
8-F 000D0C22 00837380 00542094 0084401C 0084301C 00744250 80843702 00000000

AR 0-7 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
8-F 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

FP 0-3 40404040 40404040 40404040 40404040 40404040 40404040 40404040 40404040

CR 0-7 0D00EE50 01218000 6749C600 0007000E 0000000E 010BDB80 10000000 01218000
8-F 00010000 80800000 0053CDE8 00540E08 00000000 01218000 C00810BB 07287C10

P1 - PARTITION ADDRESS IS 00540000 LENGTH IS 005C0000

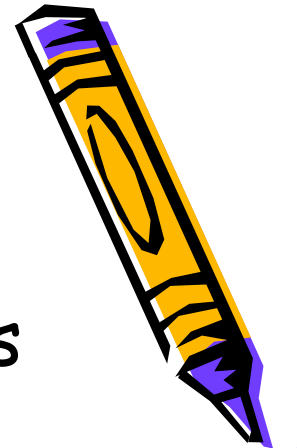
00540000	C2C1E3C3	C8C4C5C2	07DD0000	80843706	00837380	00542094	0084401C	0084301C	DO	BATCHDEB....
00540020	00744250	80843702	00000000	00000150	00837380	072AE6C8	005416D8	00000000		...&.d.....
00540040	005487F4	00000000	00842000	000D0C22	0000C5CB	6BA8E9B6	40404040	40404040		..g4.....d..



SHOW COMMAND

The show command on the console displays the protection key.

```
SHOW 1D2FB0.30
AR 0015  DATA  FOUND AT 001D2FB0
V001D2FB0 00040000 00000000 C4C4D4C9 D6D9E340 06 *.....DDMIORT * R00A27FB0
V001D2FC0 F0F9D0F1 F4C0F0F9 F1F2F1F2 F2F00000 06 *09}14{09121220..* R00A27FC0
V001D2FD0 22510001 47FF0008 001D2FB8 90ECD00C 06 *.....}.* R00A27FD0
AR 0015 1I40I  READY
F3 0071 OC0001 GIL      GILS      6:45:31
SHOW F4,500000.30
AR 0015  DATA  FOUND AT 00500000
V00500000 D4C1C9D5 E3C1E2D2 079C0000 80502452 96 *MAINTASK.....&..* R0135A000
V00500010 00502F60 00505D1C 00501F60 00500F60 96 *.&.-.&)..&.-.&.-* R0135A010
V00500020 0078E1A0 0050244C 00000000 0000001C 96 *.....&.<.....* R0135A020
```

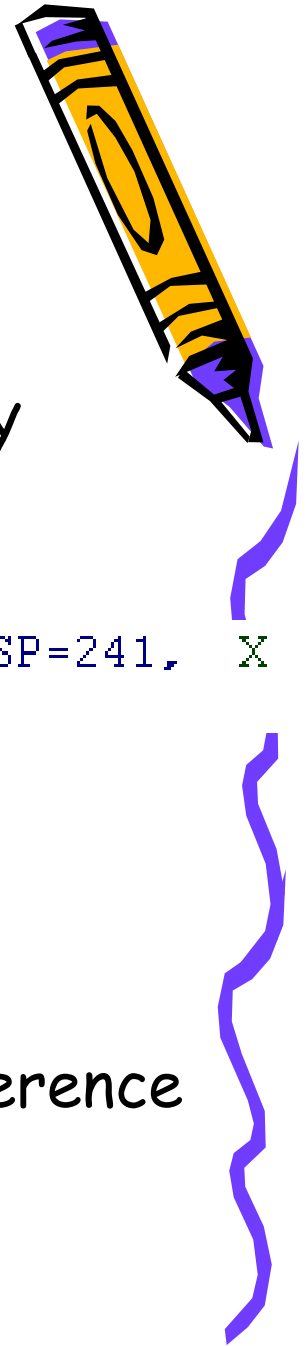


Getting the User Key

- To get the User Key for the partition you are running in, use the IPK instruction. This puts the protection key in general register 2. Then it may be saved off and used with the SPKA instruction to get back to the user key.



Getting Storage In KEYF



There are various ways to get the storage in KEY F. The easiest is using the STORAGE macro:

```
STORAGE OBTAIN,LENGTH=(R4),BNDRY=PAGE,KEY=15,LOC=ANY,SP=241, X  
COND=YES
```

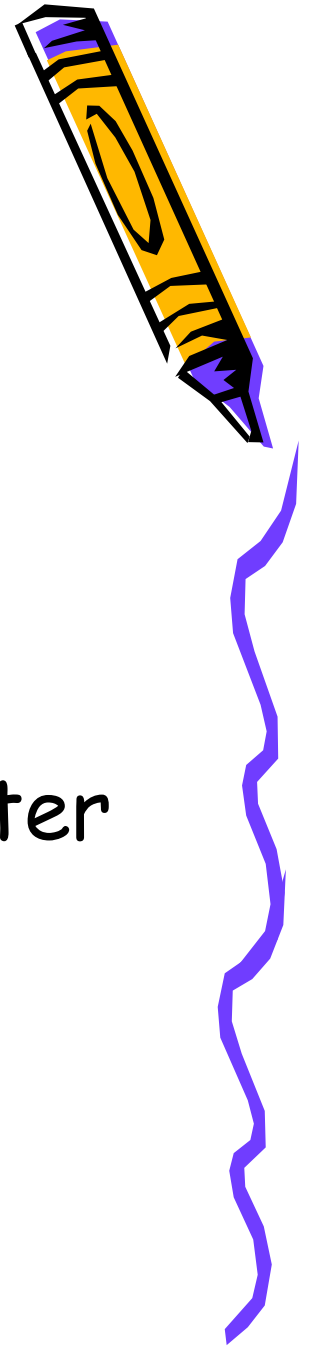
Note the subpool of 241. This is for System Getvis.

OS/390 V2.R10.0 MVS Assembler Services Reference



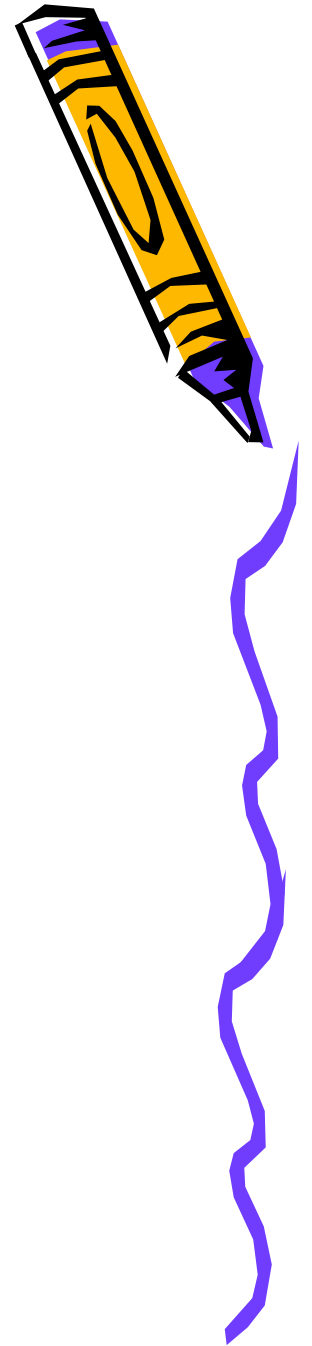
Performance Stats

- To do 500,000 KEYO and KEYU
- MODESET 33.7 sec
- SVC 30.3 sec faster
- SPKA 0.004 sec MUCH faster



GOTCHAS

- Reentrant programs.
- Must do `MODESET MODE=PROB` with each execute.



Questions?

