

LOC	OBJECT CODE	ADDR1	ADDR2	STMT	
				2 *	
				3 *	Jurgen Winkelmann's MSA-5 'PRNO' instruction test
				4 *	
				5 *	This module tests the PRNO instruction
				6 *	in a standalone environment.
				7 *	
				8 *	Operation -
				9 *	
				10 *	PRNOTEST exercises PRNO QUERY, DRNG, and TRNG functions
				11 *	and does plausibility checks on the results.
				12 *	
				13 *	- If all tests pass, PRNOTEST enters a disabled wait state
				14 *	with a PSW address of X'0000000000000000' (all zeros).
				15 *	
				16 *	- If a test fails, the test sequence is aborted
				17 *	and a disabled wait state X'000000000000DEAD' is entered.
				18 *	
				19	PRINT OFF (register equates)
				36	PRINT ON
00000000		00000000	000007FF	37 PRNOTEST	CSECT
00000000		00000000		38	USING *,0
000001A0	00000001 80000000	00000000	000001A0	39	ORG PRNOTEST+X'1A0'
000001B0		000001B0	000001D0	40	DC X'00000001800000000000000000000200' # z/Arch restart PSW
000001D0	00020001 80000000	000001B0	000001D0	41	ORG PRNOTEST+X'1D0'
000001E0		000001E0	00000200	42	DC X'00020001800000000000000000000DEAD' # z/Arch pgm new PSW
				43	ORG PRNOTEST+X'200'
				44 ***	
				45 ***	QUERY
				46 ***	
00000200	C001 0000 0000			47	LGFI R0,0 R0->function code 0
00000206	D2EF 0480 0600	00000480	00000600	48	MVC PB(240),PBNUL clear parameter block
0000020C	4110 0480		00000480	49	LA R1,PB R1->parameter block
00000210	B93C 0024			50	PRNO R2,R4 perform random number operation
00000214	D50F 06F0 0480	000006F0	00000480	51	CLC ERQUERY(16),PB compare with expected result
0000021A	4780 0220		00000220	52	BE *+6 result OK
0000021E	0000			53	DC H'0' disabled wait DEAD if result invalid
				54 ***	
				55 ***	DRNG: FIPS known answer test
				56 ***	
00000220	C001 0000 0083			57	LGFI R0,131 R0->function code 3 with modifier: seed
00000226	D2EF 0480 0600	00000480	00000600	58	MVC PB(240),PBNUL clear parameter block
0000022C	4110 0480		00000480	59	LA R1,PB R1->parameter block
00000230	4120 0800		00000800	60	LA R2,F0 R2->first operand address
00000234	C031 0000 0000			61	LGFI R3,0 R3->first operand length
0000023A	4140 0570		00000570	62	LA R4,S0 R2->second operand address
0000023E	C051 0000 0040			63	LGFI R5,64 R3->second operand length
00000244	D23F 0570 0708	00000570	00000708	64	MVC S0(64),ENTROPY provide predefined entropy
0000024A	B93C 0024			65	PRNO R2,R4 perform random number seed operation
0000024E	C001 0000 0003			66	LGFI R0,3 R0->function code 3: generate
00000254	4110 0480		00000480	67	LA R1,PB R1->parameter block
00000258	4120 0800		00000800	68	LA R2,F0 R2->first operand address
0000025C	C031 0000 0040			69	LGFI R3,64 R3->first operand length
00000262	4140 0570		00000570	70	LA R4,S0 R2->second operand address
00000266	C051 0000 0000			71	LGFI R5,0 R3->second operand length
0000026C	B93C 0024			72	PRNO R2,R4 perform random number generate operation
00000270	D53F 0748 0800	00000748	00000800	73	CLC ERFIPS(64),F0 compare with expected result

LOC	OBJECT CODE	ADDR1	ADDR2	STMT			
00000276	4780 027C		0000027C	74	BE	*+6	result OK
0000027A	0000			75	DC	H'0'	disabled wait DEAD if result invalid
				76	***		
				77	***	DRNG: Reseed and generate	
				78	***		
0000027C	C001 0000 0083			79	LGFI	R0,131	R0->function code 3 with modifier: reseed
00000282	4110 0480		00000480	80	LA	R1,PB	R1->parameter block
00000286	4120 0800		00000800	81	LA	R2,F0	R2->first operand address
0000028A	C031 0000 0000			82	LGFI	R3,0	R3->first operand length
00000290	4140 0570		00000570	83	LA	R4,S0	R2->second operand address
00000294	C051 0000 0040			84	LGFI	R5,64	R3->second operand length
0000029A	D23F 0570 0491	00000570	00000491	85	MVC	S0(64),PB+17	steal seed material (ignored by Hercules)
000002A0	B93C 0024			86	PRNO	R2,R4	perform random number reseed operation
000002A4	C001 0000 0003			87	LGFI	R0,3	R0->function code 3: generate
000002AA	4110 0480		00000480	88	LA	R1,PB	R1->parameter block
000002AE	4120 0800		00000800	89	LA	R2,F0	R2->first operand address
000002B2	C031 0001 0000			90	LGFI	R3,65536	R3->first operand length
000002B8	4140 0570		00000570	91	LA	R4,S0	R2->second operand address
000002BC	C051 0000 0000			92	LGFI	R5,0	R3->second operand length
000002C2	B93C 0024			93	PRNO	R2,R4	perform random number generate operation
000002C6	D53F 0800 0600	00000800	00000600	94	CLC	F0(64),PBNUL	first 64 bytes zero ..
000002CC	4770 02D2		000002D2	95	BNE	*+6	.. is not plausible
000002D0	0000			96	DC	H'0'	disabled wait DEAD if first 64 bytes zero
000002D2	C031 0001 07C1			97	LGFI	R3,FODISP+65536-63	last 64 bytes ..
000002D8	D53F 3000 0600	00000000	00000600	98	CLC	0(64,R3),PBNUL	.. zero ..
000002DE	4770 02E4		000002E4	99	BNE	*+6	.. is not plausible
000002E2	0000			100	DC	H'0'	disabled wait DEAD if last 64 bytes zero
				101	***		
				102	***	TRNG Query	
				103	***		
000002E4	C001 0000 0070			104	LGFI	R0,112	R0->function code 112
000002EA	D2EF 0480 0600	00000480	00000600	105	MVC	PB(240),PBNUL	clear parameter block
000002F0	4110 0480		00000480	106	LA	R1,PB	R1->parameter block
000002F4	B93C 0024			107	PRNO	R2,R4	perform random number operation
000002F8	D507 0700 0480	00000700	00000480	108	CLC	TRQUERY(8),PB	compare with expected result
000002FE	4780 0304		00000304	109	BE	*+6	result OK
00000302	0000			110	DC	H'0'	disabled wait DEAD if result invalid
				111	***		
				112	***	TRNG	
				113	***		
00000304	C001 0000 0072			114	LGFI	R0,114	R0->function code 114: TRNG
0000030A	4120 0800		00000800	115	LA	R2,F0	R2->first operand address
0000030E	C031 0000 0040			116	LGFI	R3,64	R3->first operand length
00000314	4140 0570		00000570	117	LA	R4,S0	R2->second operand address
00000318	C051 0000 0040			118	LGFI	R5,64	R3->second operand length
0000031E	B93C 0024			119	PRNO	R2,R4	perform random number generate operation
00000322	D53F 0800 0600	00000800	00000600	120	CLC	F0(64),PBNUL	first operand zero ..
00000328	4770 032E		0000032E	121	BNE	*+6	.. is not plausible
0000032C	0000			122	DC	H'0'	disabled wait DEAD if first operand zero
0000032E	D53F 0570 0600	00000570	00000600	123	CLC	S0(64),PBNUL	seconf operand zero ..
00000334	4770 033A		0000033A	124	BNE	*+6	.. is not plausible
00000338	0000			125	DC	H'0'	disabled wait DEAD if second operand zero
0000033A	B2B2 0400		00000400	126	LPSWE	WAITPSW	load enabled wait PSW
0000033E		0000033E	00000400	127	ORG	PRNOTEST+X'400'	
00000400	00020001 80000000			128	WAITPSW	DC	X'00020001800000000000000000000000' SUCCESS wait PSW
00000410		00000410	00000480	129	ORG	PRNOTEST+X'480'	

MACRO DEFN REFERENCES

No defined macros

DESC	SYMBOL	SIZE	POS	ADDR
------	--------	------	-----	------

Entry: not defined

Image	IMAGE	2048	000-7FF	000-7FF
Region		2048	000-7FF	000-7FF
CSECT	PRNOTEST	2048	000-7FF	000-7FF

STMT

FILE NAME

```
1 C:\Users\Fish\Documents\Visual Studio 2008\Projects\MyProjects\ASMA-0\PRNO\PRNO.asm
```

**** NO ERRORS FOUND ****