

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 *	Fish 2025-09-02:
				20 *	1. Do each test for each addressing mode too
				21 *	2. Added GitHub #765 test ==> Addresssing Exception
				22 *	
				23	PRINT OFF (register equates)
				40	PRINT ON
00000000		00000000	000007FF	41 PRNOTEST	CSECT
00000000		00000000		42	USING *,0
000001A0	00000000 00000000	00000000	000001A0	43	ORG PRNOTEST+X'1A0' # z/Arch restart PSW
				44 RSTRTNEW	DC X'000000000000000000000000000000200' # z/Arch restart PSW (24-bit mode)
				45 **	DC X'000000008000000000000000000000200' # z/Arch restart PSW (31-bit mode)
				46 **	DC X'000000018000000000000000000000200' # z/Arch restart PSW (64-bit mode)
000001B0		000001B0	000001D0	47	ORG PRNOTEST+X'1D0' # z/Arch pgm new PSW
000001D0	00020000 00000000			48 PROGNEW	DC X'000200000000000000000000000000DEAD' # z/Arch pgm new PSW (24-bit mode)
				49 **	DC X'000200008000000000000000000000DEAD' # z/Arch pgm new PSW (31-bit mode)
				50 **	DC X'000200018000000000000000000000DEAD' # z/Arch pgm new PSW (64-bit mode)
000001E0		000001E0	00000200	51	ORG PRNOTEST+X'200'
				52 ***	
				53 ***	QUERY
				54 ***	
00000200	C001 0000 0000			55	LGFI R0,0 R0->function code 0
00000206	D2EF 0480 0600	00000480	00000600	56	MVC PB(240),PBNUL clear parameter block
0000020C	4110 0480		00000480	57	LA R1,PB R1->parameter block
00000210	B93C 0024			58	PRNO R2,R4 perform random number operation
00000214	D50F 06F0 0480	000006F0	00000480	59	CLC ERQUERY(16),PB compare with expected result
0000021A	4780 0220		00000220	60	BE *+6 result OK
0000021E	0000			61	DC H'0' disabled wait DEAD if result invalid
				62 ***	
				63 ***	DRNG: FIPS known answer test
				64 ***	
00000220	C001 0000 0083			65	LGFI R0,131 R0->function code 3 with modifier: seed
00000226	D2EF 0480 0600	00000480	00000600	66	MVC PB(240),PBNUL clear parameter block
0000022C	4110 0480		00000480	67	LA R1,PB R1->parameter block
00000230	4120 0800		00000800	68	LA R2,F0 R2->first operand address
00000234	C031 0000 0000			69	LGFI R3,0 R3->first operand length
0000023A	4140 0570		00000570	70	LA R4,S0 R2->second operand address
0000023E	C051 0000 0040			71	LGFI R5,64 R3->second operand length
00000244	D23F 0570 0708	00000570	00000708	72	MVC S0(64),ENTROPY provide predefined entropy
0000024A	B93C 0024			73	PRNO R2,R4 perform random number seed operation

LOC	OBJECT CODE	ADDR1	ADDR2	STMT			
0000024E	C001 0000 0003			74	LGFI	R0,3	R0->function code 3: generate
00000254	4110 0480		00000480	75	LA	R1,PB	R1->parameter block
00000258	4120 0800		00000800	76	LA	R2,F0	R2->first operand address
0000025C	C031 0000 0040			77	LGFI	R3,64	R3->first operand length
00000262	4140 0570		00000570	78	LA	R4,S0	R2->second operand address
00000266	C051 0000 0000			79	LGFI	R5,0	R3->second operand length
0000026C	B93C 0024			80	PRNO	R2,R4	perform random number generate operation
00000270	D53F 0748 0800	00000748	00000800	81	CLC	ERFIPS(64),F0	compare with expected result
00000276	4780 027C		0000027C	82	BE	*+6	result OK
0000027A	0000			83	DC	H'0'	disabled wait DEAD if result invalid
				84	***		
				85	***	DRNG: Reseed and generate	
				86	***		
0000027C	C001 0000 0083			87	LGFI	R0,131	R0->function code 3 with modifier: reseed
00000282	4110 0480		00000480	88	LA	R1,PB	R1->parameter block
00000286	4120 0800		00000800	89	LA	R2,F0	R2->first operand address
0000028A	C031 0000 0000			90	LGFI	R3,0	R3->first operand length
00000290	4140 0570		00000570	91	LA	R4,S0	R2->second operand address
00000294	C051 0000 0040			92	LGFI	R5,64	R3->second operand length
0000029A	D23F 0570 0491	00000570	00000491	93	MVC	S0(64),PB+17	steal seed material (ignored by Hercules)
000002A0	B93C 0024			94	PRNO	R2,R4	perform random number reseed operation
000002A4	C001 0000 0003			95	LGFI	R0,3	R0->function code 3: generate
000002AA	4110 0480		00000480	96	LA	R1,PB	R1->parameter block
000002AE	4120 0800		00000800	97	LA	R2,F0	R2->first operand address
000002B2	C031 0001 0000			98	LGFI	R3,65536	R3->first operand length
000002B8	4140 0570		00000570	99	LA	R4,S0	R2->second operand address
000002BC	C051 0000 0000			100	LGFI	R5,0	R3->second operand length
000002C2	B93C 0024			101	PRNO	R2,R4	perform random number generate operation
000002C6	D53F 0800 0600	00000800	00000600	102	CLC	F0(64),PBNUL	first 64 bytes zero ..
000002CC	4770 02D2		000002D2	103	BNE	*+6	.. is not plausible
000002D0	0000			104	DC	H'0'	disabled wait DEAD if first 64 bytes zero
000002D2	C031 0001 07C1			105	LGFI	R3,FODISP+65536-63	last 64 bytes ..
000002D8	D53F 3000 0600	00000000	00000600	106	CLC	0(64,R3),PBNUL	.. zero ..
000002DE	4770 02E4		000002E4	107	BNE	*+6	.. is not plausible
000002E2	0000			108	DC	H'0'	disabled wait DEAD if last 64 bytes zero
				109	***		
				110	***	TRNG Query	
				111	***		
000002E4	C001 0000 0070			112	LGFI	R0,112	R0->function code 112
000002EA	D2EF 0480 0600	00000480	00000600	113	MVC	PB(240),PBNUL	clear parameter block
000002F0	4110 0480		00000480	114	LA	R1,PB	R1->parameter block
000002F4	B93C 0024			115	PRNO	R2,R4	perform random number operation
000002F8	D507 0700 0480	00000700	00000480	116	CLC	TRQUERY(8),PB	compare with expected result
000002FE	4780 0304		00000304	117	BE	*+6	result OK
00000302	0000			118	DC	H'0'	disabled wait DEAD if result invalid
				119	***		
				120	***	TRNG	
				121	***		
00000304	C001 0000 0072			122	LGFI	R0,114	R0->function code 114: TRNG
0000030A	4120 0800		00000800	123	LA	R2,F0	R2->first operand address
0000030E	C031 0000 0040			124	LGFI	R3,64	R3->first operand length
00000314	4140 0570		00000570	125	LA	R4,S0	R4->second operand address
00000318	C051 0000 0040			126	LGFI	R5,64	R5->second operand length
0000031E	9500 0413		00000413	127	CLI	GH765,0	normal test?
00000322	4780 0332		00000332	128	BE	PRNO	yes, continue
00000326	E350 0400 0004		00000400	129	LG	R5,=X'050505050000040'	#765 salva-rczero

LOC	OBJECT CODE	ADDR1	ADDR2	STMT				
0000032C	D203 01DC 0408	000001DC	00000408	130	MVC	PROGNEW+12(4),=AL4(0)	Program Intgerrupt handler	
				131	*		(Addr Exception expected!)	
00000332	B93C 0024			132	PRNO	PRNO R2,R4	perform random number generate operation	
00000336	9500 0413		00000413	133	CLI	GH765,0	Normal run?	
0000033A	4780 0360		00000360	134	BE	CONT	Yes, continue	
0000033E	9540 0412		00000412	135	CLI	AM,64	64-bit addressing mode?	
00000342	4770 0360		00000360	136	BNE	CONT	No, continue	
00000346	B2B2 0350		00000350	137	FAIL765	LPSWE PSW765	WTF?! We should have Program Checked!!	
00000350	00020001 80000000			138	PSW765	DC 0D'0',X'0002000180000000000000000000765'	GH765 FAILURE!	
00000360	D53F 0800 0600	00000800	00000600	139	CONT	CLC FO(64),PBNUL	first operand zero ..	
00000366	4770 036C		0000036C	140	BNE	*+6	.. is not plausible	
0000036A	0000			141	DC	H'0'	disabled wait DEAD if first operand zero	
0000036C	D53F 0570 0600	00000570	00000600	142	CLC	SO(64),PBNUL	seconf operand zero ..	
00000372	4770 0378		00000378	143	BNE	*+6	.. is not plausible	
00000376	0000			144	DC	H'0'	disabled wait DEAD if second operand zero	
00000378	9518 0412		00000412	145	CLI	AM,24	AM24 done?	
0000037C	4780 0392		00000392	146	BE	AM31	Yes, Then test AM31	
00000380	951F 0412		00000412	147	CLI	AM,31	AM31 done?	
00000384	4780 03A6		000003A6	148	BE	AM64	Yes, Then test AM64	
00000388	9540 0412		00000412	149	CLI	AM,64	AM64 done?	
0000038C	4780 03BA		000003BA	150	BE	TRY765	Yes, Do GitHub #765 test if we haven't yet	
00000390	0000			151	DC	H'0'	WTF?!	
00000392	D201 01A3 040C	000001A3	0000040C	152	AM31	MVC RSTRTNEW+3(2),=XL2'0080'	Switch to AM31	
00000398	D201 01D3 040C	000001D3	0000040C	153	MVC	PROGNEW+3(2),=XL2'0080'	Switch to AM31	
0000039E	921F 0412		00000412	154	MVI	AM,31	Switch to AM31	
000003A2	B2B2 01A0		000001A0	155	LPSWE	RSTRTNEW	Do all in AM31	
000003A6	D201 01A3 040E	000001A3	0000040E	156	AM64	MVC RSTRTNEW+3(2),=XL2'0180'	Switch to AM64	
000003AC	D201 01D3 040E	000001D3	0000040E	157	MVC	PROGNEW+3(2),=XL2'0180'	Switch to AM64	
000003B2	9240 0412		00000412	158	MVI	AM,64	Switch to AM64	
000003B6	B2B2 01A0		000001A0	159	LPSWE	RSTRTNEW	Do all in AM64	
000003BA	9500 0413		00000413	160	TRY765	CLI GH765,0	First time here?	
000003BE	4770 03DA		000003DA	161	BNE	BAD765	No?! WTF?!	
000003C2	92FF 0413		00000413	162	MVI	GH765,X'FF'	Remember what we're doing	
000003C6	9218 0412		00000412	163	MVI	AM,24	Switch back to AM24 again	
000003CA	D201 01A3 0410	000001A3	00000410	164	MVC	RSTRTNEW+3(2),=XL2'0000'	Switch back to AM24 again	
000003D0	D201 01D3 0410	000001D3	00000410	165	MVC	PROGNEW+3(2),=XL2'0000'	Switch back to AM24 again	
000003D6	B2B2 01A0		000001A0	166	LPSWE	RSTRTNEW	Do all AM tests all over again	
000003DA	4DE0 0346		00000346	167	BAD765	BAS R14,FAIL765	GH #765 FAILURE	
000003DE		000003DE	00000400	168	ORG	PRNOTEST+X'400'		
00000400				169	LTORG	,	Literals pool	
00000400	05050505 00000040			170		=X'0505050500000040'		
00000408	00000000			171		=AL4(0)		
0000040C	0080			172		=XL2'0080'		
0000040E	0180			173		=XL2'0180'		
00000410	0000			174		=XL2'0000'		
00000412	18			175	AM	DC AL1(24)	current addressing mode	
00000413	00			176	GH765	DC X'00'	FF = try GH #765 test, 00 = don't	
00000414		00000414	00000480	177	ORG	PRNOTEST+X'480'		
00000480	00000000 00000000			178	PB	DS XL240	current parameter block	
00000570	00000000 00000000			179	SO	DS XL64	second operand	
000005B0		000005B0	00000600	180	ORG	PRNOTEST+X'600'		
00000600	00000000 00000000			181	PBNUL	DC 240X'00'	empty parameter block	
000006F0	90000000 00000000			182	ERQUERY	DC X'90000000000000000000000000A000'	expected query reslt	
00000700	000000C0 00000020			183	TRQUERY	DC X'000000C000000020'	expected Hercules TRNG query result	
00000708	3295117F 02371270			184	ENTROPY	DC X'3295117F02371270'	predefined entropy for	
00000710	105A3783 CFE0BF5A			185	DC	X'105A3783CFE0BF5A'	FIPS known answer test	





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 **
```