



Specification for RFID Reader RS-232(serial) Interface



NESSLAB UHF RFID READER Protocol

July 2008

Revision 0.8.5

문서 버전

- 2006.06.30 Ver 0.1

프로토콜 초안 작성.

- 2006.08.11 Ver 0.2

2. Reader Sleep Mode 추가.

4.2 호 처리 관련 메시지 추가 및 수정.

- 2006.09.01 Ver 0.3

전체 문서 간략화 및 SST 1차 요청사항 수정.

- 2006.09.20 Ver 0.4

SST 2차 요청사항 수정 및 KTF 최종문서.

- 2006.10.17 Ver 0.5

ISO18000-6 Type B 추가.

- 2006.11.17 Ver 0.5.1

RES TAG READ COMMAND에 COMMAND COED(0xAE) 추가

- 2006.11.21 Ver 0.5.2

SET CONTROL COMMAND(0x6C) 추가

- 2007.1.5 Ver 0.5.3

SET CONTROL COMMAND의 'Scan Time' 항목 추가

- 2007.1.9 Ver 0.5.4

GET CONTROL COMMAND(0x6D) 추가

– 2007.2.21 Ver 0.6.0

1) SET/GET CONTROL COMMAND 관련

‘Continue Mode’, ‘Hopping Switch’, ‘Buzzer Switch’ 항목 추가

SET CONTROL COMMAND의 ‘Power Level Table’ 추가

SET CONTROL COMMAND의 ‘Q Value’의 Auto 기능 추가

2) REQ TAG READ 관련

‘WRITE USER MEMORY’, ‘BANK SELECT WRITE’ Data 길이 조정 가능하도록 수정

3) RES TAG READ 관련

TYPE C(Gen2)의 Variable EPC Length에 따른 패킷 길이 관련 사항 수정

– 2007.3.7 Ver 0.6.1

BANK SELECT LOCK COMMAND(0x6C) 추가

TAG KILL COMMAND(0x6B) 추가

– 2007.3.13 Ver 0.6.2

BANK SELECT READ/WRITE/LOCK ACCESS Password Parameter 추가

부록 추가

– 2007.7.4 Ver 0.6.9

1) TYPE C 256bits EPC Tag 까지 지원 (기존 96bits)

2) SET CONTROL COMMAND 관련

‘All Control Value’, ‘Default Setting’ 추가.

3) REQ TAG READ 관련

‘ONE TAG READ EPC_TAG SELECT’, ‘BANK SELECT READ/WRITE_TAG SELECT’ 추가.

– 2007.8.27 Ver 0.7.0

1) RF-200 (고정형) 관련 기능 추가

2) SET CONTROL COMMAMD 관련

‘Session Value’, ‘Antenna State(RF-200)’, ‘Antenna Change Value(RF-200)’ ,

‘Antenna Port View(RF-200)’ 추가.

– 2007.9.7 Ver 0.7.1

1) REQ TAG READ 관련

‘ONE TAG READ EPC_TAG SELECT’ 파라미터 수정, ‘ONE TAG READ

EPC_TAG SELECT ’ 추가.

– 2007.11.14 Ver 0.7.2

1) REQ TAG READ 관련

‘BANK SELECT READ/WRITE’ 파라미터 중 WordPtr의 범위를 0 ~ 127 에서 0 ~ 약 42M로 수정.

– 2007.12.21 Ver 0.7.3

1) REQ TAG READ 관련

‘BANK SELECT READ’ 파라미터 중 Length의 범위를 1 ~ 16 에서 1~255로 수정.

2) RES TAG READ 관련

‘255byte 이상의 패킷을 위한 COMMAND COED(0xA1)’ 추가

– 2008.01.07 Ver 0.7.4

1) SET/GET CONTROL COMMAMD 관련

LBT CH(일본형, 유럽형만 해당)을 User가 선택할 수 있도록 ‘CH State’ 추가.

– 2008.02. Ver 0.7.5~6

1) 펌웨어 문제점 수정

– 2008.02.26 Ver 0.7.7

1) REQ TAG READ 관련

- ‘USER MEMORY LOCK’(TYPE B) COMMAND 추가.
- USER MEMORY READ(TYPE B)의 파라미터 중 Length의 범위를 1~25에서 1~255 로 변경

– 2008.05.09 Ver 0.8.0

HITACHI POCOTOL 구현.

1) REQ TAG READ 관련

- ONE TAG READ EPC/MULTI TAG READ EPC의 Password Parameter 추가.
- HITACHI READ LOCK Command 추가.
- HITACHI GET SYSTEM INFO Command 추가.

2) RES TAG READ 관련

- HITACHI GET SYSTEM INFO Command의 응답 관련 사항 추가.

– 2008.05.16 Ver 0.8.1

1) REQ TAG READ 관련

- BANK SLELCT LOCK_TAG Sel Command 추가.
- TAG KILL_TAG Sel Command 추가.

– 2008.06.19 Ver 0.8.3

1) SET/GET CONTROL COMMAMD 관련

- LBT (일본형, 유럽형만 해당)경우, 채널 변경 시간을 조절 할 수 있도록 ‘LBT TIME’ 추가.

– 2008.07.10 Ver 0.8.5

NXP PROTOCOL 구현.

1) REQ TAG READ 관련

- NXP READ PROTECT Command 추가.
- NXP RESET READ PROTECT Command 추가.
- NXP CHANGE EAS Command 추가.
- NXP EAS ALARM Command 추가.

2) RES TAG READ 관련

- NXP EAS ALARM Command의 응답 관련 사항 추가.

목 차

1. 개 요	7
2. SIGNAL	8
3. 패 킷	9
4. COMMAND	10
5. 부 록	37

1 개 요

본 문서는 네스랩 리더와 연동되는 단말기에 대한 두 프로세서 사이의 통신 방식 및 메시지를 정의한다.



2 SIGNAL

리더와 접속되는 단말기는 TTL Level의 신호를 사용, MSB부터 전송한다. (115200 bps, Async, Full duplex, 8bits, No parity) 물리적 연결 상태는 그라운드를 공유하는 RX, TX선으로 독립적인 통신 선로를 사용한다.

3 패킷

3.1 패킷 구조

STX(1byte)	PL(1byte)	DATA(Variable)	CHECKSUM(1byte)	ETX(1byte)
------------	-----------	----------------	-----------------	------------

STX : 패킷의 시작 "0x7E". (1 byte)

PL : 패킷의 길이, DATA + CHECKSUM의 길이. (1 byte)

DATA : COMMAND를 포함한 데이터.(Command 1byte + data variable bytes).

CHECKSUM : DATA의 XOR 값.(1 byte)

ETX : 패킷의 끝 "0x7D". (1 byte)

※ 각 단위는 byte단위로 구성되고 형식은 네트워크 바이트 순서를 따른다.

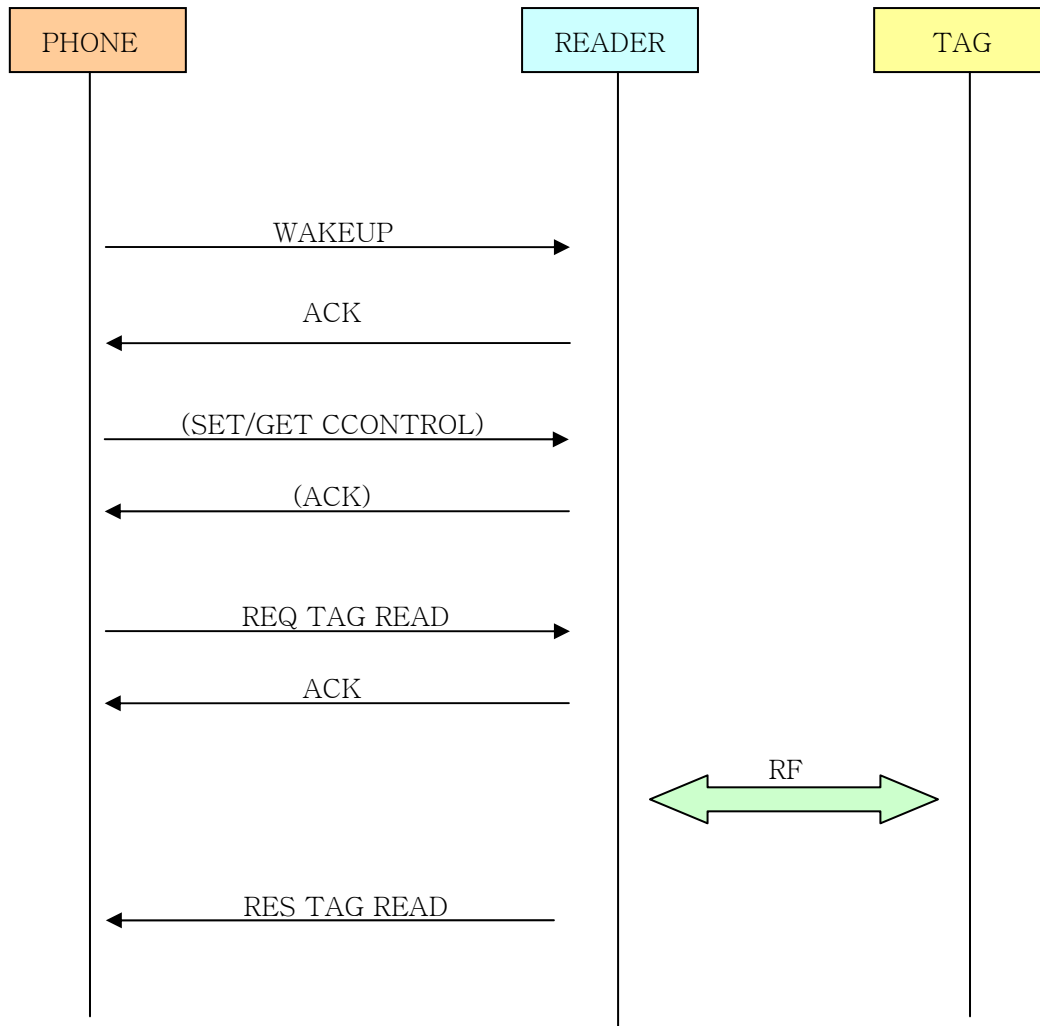
※ WAKE UP과 강제종료('#') 전송 시 STX, PL, CHECKSUM, ETX는 생략된다.

3.2 흐름제어

흐름제어 방식은 STOP & WAIT 방식을 사용하며 패킷을 하나 전송한 후에는 상대방으로부터 응답을 받을 때까지 대기한다. 1초 이내에 응답을 전혀 받지 못하는 경우 초기화되며, 메시지 오류인 경우에 한하여 3회까지 재전송한다.

상대방으로부터 NACK 메시지를 받은 경우는 해당 패킷을 재전송하고 3회 NACK를 받은 경우 초기화된다.

4 COMMAND



1) WAKE UP

리더는 Power On, TAG 응답 종료, 강제종료('#') 후에 항상 SLEEP MODE로

동작한다. WAKE UP은 리더 RX선으로 레벨 EVENT를 발생시키면 된다.

그러므로 WAKE UP은 유효한 패킷을 보내기 전에 임의의 코드를 전송하면 된다.

단, STX, PL, CHECKSUM, ETX 등은 생략 된다.

Octet	7	6	5	4	3	2	1	0
0	0xXX							

- 단말기 -> 리더
- 기능 : SLEEP MODE에 들어간 리더를 동작이 가능한 상태로 WAKE UP함.
- COMMAND CODE: 임의의 코드
- 응답 : ACK 메시지
- 예제) 00h

2) ACK

리더는 수신한 메시지에 대한 응답으로 메시지 수신이 정상적일 경우 ACK를 보낸다. ACK를 보내는 경우는 두 가지가 있다. 첫 번째 경우는 WAKE UP이 되었을 경우이며, 또 다른 경우는 REQ TAG READ 메시지를 정확하게 수신한 경우이다. 단 리더는 WAKE UP이 되고 1초간 패킷이 들어오지 않으면 다시 SLEEP MODE로 들어간다.

Octet	7	6	5	4	3	2	1	0
0	0x90							

- 단말기 <- 리더
- 기능 : 수신한 메시지에 대한 응답으로 메시지 수신이 정상적일 경우 응답을 보낸다.

- COMMAND CODE: 0x90
- 응답 : REQ TAG READ 메시지
- 예제) 7Eh 02h 90h 90h 7Dh

3) NACK

Octet	7	6	5	4	3	2	1	0
0	0x91							

- 단말기 <-> 리더
- 기능 : 수신한 메시지에 대한 응답으로 수신한 메시지에 오류가 있는 경우
응답을 보낸다.
- COMMAND CODE : 0x91
- 응답 : 보낸 메시지 재송신
- 예제) 7Eh 02h 91h 91h 7Dh

4) SET CONTROL

단말기에서 리더의 Control 값들을 변경하기 위한 명령어로 반복전송이 가능하며, 변경사항이 없으면 생략할 수 있다.

Octet	7	6	5	4	3	2	1	0
0	0x6C							

1	READER COMMAND
2	0X20
3	PARAMETER 1

- 단말기 -> 리더

- 기능 : 리더의 주요 Control 값을 변경하기 위한 명령어

- COMMAND CODE : 0x6C

- READER COMMAND/PARAMETER

CODE (char)	CODE (HEX)	COMMAND	PARA METER	DEFAULT
p	0x70	Power Control	0~255 (0x30~0x323535)	0
q	0x71	Q Value (TYPE C)	0~15(0x30~0x3135)	0 (AUTO)
t	0x74	Scan Time	0 ~ 60 (0x30~0x3630)	0
c	0x63	Continue Mode	0(0x30), 1(0x31)	0 (OFF)
f	0x66	Hopping Select	0(0x30)~4(0x34)	0(KORE A FHSS)
b	0x62	Buzzer switch	0(0x30), 1(0x31)	1(ON)
a	0x61	All Control Value	Code + Parameter	X
d	0x64	Default Setting	X	X
s	0x73	Session Value	1(0x31), 2(0x32)	1
i	0x69	Antenna State	0~255	1

			(0x30~0x323535)	
j	0x6A	Antenna Change Value	1~255 (0x31~0x323535)	5
k	0x6B	Antenna Port View	0(0x30), 1(0x31)	0
r	0x72	LBT CH State	1(0x31) ~ MAX	254(JA) ,15(EU)
g	0x67	LBT TIME	0(0x31) ~ 4000(0x34303030)	4000 (ms)

Antenna State, Antenna Change Value, Antenna Port View는
NL-RF200만 해당

※ CH State는 NL-RM100J(일본향), NL-RM100E(유럽향)만 해당

1) Power Control : 리더 송신 파워 레벨을 변경한다.

※ Power Level TABLE

Power Level (Parameter)	0	1	2	...	31
Power(dBm)	Full (약 28dBm)	- 1dB	- 2dB	...	-31dB

※ 즉, Power Level (Parameter)는 Full Power를 감쇄 시킬 값을 나타낸다. Ex) Power Level = 3 이면, 실제 Power Level은 25dBm이 된다.

2) Q Value : Type C Multi Read에 사용되는 Q Range를 결정하는 Q 값 변경. (Gen2만 해당)

※ Mobile Reader 권장 Q Value

Q (Parameter)	0	1	2	3	4	5
------------------	---	---	---	---	---	---

Multi TAG 갯수	AUTO	2~4	4~10	10~20	20~40	40~80
-----------------	------	-----	------	-------	-------	-------

3) Scan Time : 리더의 Read Command 실행 시간을 변경한다.

※ Scan Time은 초(sec)단위이며, '0'이면 무제한(STOP COMMAND ' #'을 받을 때까지) 실행한다.

Parameter	0	1 ~ 60
Scan Time	∞	1 ~ 60 sec

4) Continue Mode : One Tag Read EPC(Type C)/UID(Type Command를 실행 시에 Continue Mode가 ON('1')인 경우 Tag를 한번 읽었더라도 리더는 자동으로 동작을 멈추지 않고 STOP Command(' #')를 받을 때까지 계속 읽어서 TAGID를 단말기로 송신한다.

Parameter	0	1
Continue Mode	Off	On

5) Hopping Select : 국가별 사용 주파수 범위와 호핑 방식을 설정한다.

Hopping Select (Parameter)	0	1	2	3	4	5	6
국 가	KOREA	KOREA	JAPAN	EURO	USA	TEST	CHINA
호핑방식	FHSS	LBT	LBT	LBT	FHSS	TEST	FHSS

6) Buzzer Switch : Buzzer On/Off를 설정한다.

Parameter	0	1
Buzzer Switch	Off	On

7) All Control Value : 여러 개의 Control Value를 한번에 Setting 한다.

Parameter	Code1+Value1	Code2+Value2	...
-----------	--------------	--------------	-----

※ Parameter (CodeX+ValueX)의 갯수는 상관없이 있으며, 구분자 ' ' (0x20)는 All Control Value를 나타내는 'a'(0x61) 다음에만 사용하고, Parameter들 사이에는 사용하지 않는다.

Ex) "a p1q2"(7Eh 08h 6Ch 61h 20h 70h 31h 71h 32h 2F 7Dh)

8) Default Setting : 모든 Control Value를 Default Setting 한다.

※ Parameter는 없다.

9) Session Value : Session Value를 지정해서 Type C Multi Read 시에

TAG의 Inventoried Flag를 선택할 수 있다. (Gen2 만 해당)

Session Value (Parameter)	1	2
Inventoried Flag Reset	Tag는 약 0.5초 마다 Reset	Tag는 Power가 OFF되고 약 30초 후 Reset
사용 환경	일정 시간 간격으로 TAG 들을 반복해서 읽고자 할 때	읽지 않은 TAG만 읽고 자 할 때
특징	언제 다시 읽더라도 모든 TAG들이 잘 응답하며, 실시간으로 TAG들을 확인 할 수가 있음. 반복적으로 읽으므로 다수의 TAG를	한번 읽었던 TAG는 읽지 않으므로 다수의 TAG들을 가장 빠른 속도로 읽을 수가 있음. 리더를 끄고 30초 이상

	읽을 경우 속도는 다소 떨어짐	지나지 않은 상태에서 다시 읽으면 응답하지 않는 TAG가 있을 수 있음.
--	------------------	--

※

Session 2 로 설정하면 반복적으로 읽는 것을 최소화하는 것이지만 반드시 읽지 않는 것은 아니므로 응용 Level 에서 중복 TAG Read 상황에 대한 처리를 해 줄 것을 권장함.

10) Antenna State : Antenna Port를 설정 한다. (RF-200 만 해당)

ANT 8	ANT ...	ANT 2	ANT 1	VALUE
OFF	OFF	OFF	ON	1
OFF	OFF	ON	OFF	2
OFF	OFF	ON	ON	3
...
ON	ON	ON	ON	255

11) Antenna Change Value : Antenna Switching 주기 즉, Inventory Round 수를 나타낸다. 예를 들어 Q가 2일 때 TAG를 읽기 위해 4번의 Query 명령을 보내게 되는데 이 4번을 Inventory Round라 한다. 이때, Antenna Change Value가 5라면 한 안테나에서 Inventory Round를 5번 반복한 뒤 다음 안테나로 바꾸게 된다. (RF-200 만 해당)

Parameter	1 ~ 255
Antenna Change Value	1 ~ 255 (Inventory Rounds)

12) Antenna Port View : ON일 경우, TAG를 읽은 ANT Port 번호를 TAGID 앞에 포함하여 전송. (RF-200 만 해당)

Parameter	0	1
Buzzer Switch	Off	On

13) LBT CH State : 사용할 LBT CH을 사용자가 구성한다. (NL-RM100J/E 만 해당)

CH ...	CH 3	CH 2	CH 1	VALUE
OFF	OFF	OFF	ON	1
OFF	OFF	ON	OFF	2
OFF	OFF	ON	ON	3
OFF	ON	OFF	OFF	4
...

※ 일본향의 CH은 2번부터 8번까지 사용가능 하다. (7개 채널만 사용가능)

< 일본향 채널 표)

CH No.	Frequency	지원 여부
1	952.2 (MHz)	사용 불가
2	952.4	사용 가능
3	952.6	사용 가능
4	952.8	사용 가능
5	953	사용 가능
6	953.2	사용 가능
7	953.4	사용 가능
8	953.6	사용 가능
9	953.8	사용 불가

※ 유럽향의 CH은 1번부터 4번까지 사용가능 하다. (4개 채널만 사용가능)

< 유럽향 채널 표)

CH No.	Frequency	지원 여부
1	865.7 (MHz)	사용 가능
2	866.3	사용 가능
3	866.9	사용 가능
4	867.5	사용 가능

14) LBT TIME : 한 채널을 점유하여 TAG를 Read하는 시간을 설정한다. 단위는 ms이며, 전파 규정상 최대 점유시간인 4초를 초과할 수 없다.

Parameter	0 ~4000
Duration Time	0 ~ 4000 ms

※ LBT TIME을 ‘0’ 으로 설정 했다고 해서 전혀 동작을 하지 않는 것은 아니며, 일단 채널을 점유한 뒤 최소한의 시간 동안 READ 한 뒤 다음 채널로 이동하게 된다.

- 응답 : ACK or NACK

- 예제) 7Eh 07h 6Ch 70h 20h 32h 31h 30h 0Fh 7Dh (“p 210”)

5) GET CONTROL

단말기에서 리더의 Control 값들을 읽어오기 위한 명령어로 반복전송이

가능하며, 생략할 수 있다.

폰 -> 리더 (Command)

Octet	7	6	5	4	3	2	1	0
0	0x6D							
1	READER COMMAND							

리더 -> 폰 (Reply)

Octet	7	6	5	4	3	2	1	0
0	0x6E							
1	READER COMMAND 1							
2	Control Value 1 (variable)							
3	...							
4	READER COMMAND 2							
5	Control Value 2 (variable)							
6	...							
7	READER COMMAND X							
8	Control Value X (variable)							
9	...							

단말기 <-> 리더

- 기능 : 리더에 현재 설정되어 있는 Control 값을 읽어 오기 위한 명령어

- COMMAND CODE : 0x6D, 0x6E

- READER COMMAND

CODE (char)	CODE (HEX)	COMMAND
a	0x61	All Control Value
p	0x70	Power Control
q	0x71	Q Value (TYPE C)
t	0x74	Scan Time
v	0x76	Protocol Ver. Info
c	0x63	Continue Mode
f	0x66	Hopping Select
b	0x62	Buzzer Switch
s	0x73	Session Value
i	0x69	Antenna State
j	0x6A	Antenna Change Value
k	0x6B	Antenna View
r	0x72	LBT CH State

g	0x67	LBT TIME
---	------	----------

1) All Control Value : 현재 리더에 설정되어 있는 모든 User Control Value를 읽어온다.

※ 리더는 RF-200을 기준으로 모든 Control Value를 전송.

2) 그 외 : 현재 설정 되어 있는 각 COMMAND의 값을 읽어 온다.

- 응답 : 리더는 해당 각 READER COMMAND 뒤에 현재 설정되어 있는 Control Value를 붙여서 응답한다.

1) All Control Value : 모든 User Control Value를 응답한다. 'v' + 'value' + 'p' + 'value' + 'q' + 'value' + 't' + 'value' + ...

2) 그 외 : 각 Command의 코드와 Value를 응답한다. Ex) 'p' + 'value'

- 예제) GetControl Command : 7Eh 03h 6Dh 70h 1Dh 7Dh ("p")

Reply : 7Eh 07h 6E 70h 31h 32h 30h 2Dh 7Dh ("p120")

6) REQ TAG READ

단말기는 리더가 수행해야 할 명령어를 전송한다. 리더는 실행 할 수 있는 명령어를 각 프로토콜 Type 별로 제공한다.

첫 번째로 ONE TAG READ UID/EPC이며, 이 명령어는 TAG가 오직 한 개 존재 할 경우에 UID(Type B) 또는 EPC(Type C)를 READ할 때 사용된다. 두 번째는 MULTI TAG READ UID/EPC이다. 복수개의 TAG가 존재 할 경우 TAG들이 동시에 응답하게 되어 발생하는 충돌을 방지하지 하여 READ하기 위한 명령어이다. 세 번째는 READ USER MEMORY/BANK SELECT READ인데, 이 명령어는 2~4가지의 파라미터를 함께 사용하여, 지정된 TAG 메모리 위치의 정보를 읽고자 할 때 사용된다. 네 번째

명령어인 WRITE USER MEMORY/BANK SELECT WRITE는 2~4가지의 파라미터를 함께 사용하여, 지정된 메모리 위치에 DATA를 쓰고자 할 때 사용된다. 단, Type B인 경우에는 2byte 단위(아스키코드 기준)로, Type C인 경우에는 4byte 단위(아스키 코드 기준)로 Data를 Write 할 수가 있다. 이 외에 리더는 TYPE C의 BANK SELECT LOCK 과 TAG KILL 명령어를 제공한다. BANK SELECT LOCK 명령어는 TAG의 Access Password를 알고 있는 사용자만이 BANK SELECT READ/WRITE/LOCK 명령어를 사용할 수 있도록 설정하는 명령어이다. 사용자가 LOCK된 TAG를 Access 하고자 할 때는 각 명령어의 마지막 파라미터에 Password를 포함시키면 된다. TAG KILL 명령어는 TAG가 어떤 명령어로도 더 이상 응답 할 수 없도록 할 때 사용하는 명령어이다. 한번 KILL이 되면 더 이상 변경할 수 없으므로 주의하여야 한다. (LOCK, KILL의 자세한 사항은 부록을 참조바람)

REQ TAG READ에 대한 응답으로 리더는 먼저 ACK를 보내고 각 명령어에 해당되는 RES TAG READ 메시지를 보낸다.

Octet	7	6	5	4	3	2	1	0
0	0x60							
1	READER COMMAND							
2	0X20							
3	PARAMETER 1(VARIABLE)							
4	0X20							
5	PARAMETER 2(VARIABLE)							

6	0X20
7	PARAMETER 3(VARIABLE)
8	0X20
9	PARAMETER 4(VARIABLE)

- 단말기 -> 리더

- 기능 : 리더가 TAG에게 수행 할 명령어

- COMMAND CODE : 0x60

- READER COMMAND

CODE (char)	CODE (HEX)	COMMAND	PROTOCOL TYPE	PARA METER
a	0x61	ONE TAG READ UID	B	(1)
b	0x62	MULTI TAG READ UID	B	(1)
c	0x63	READ USER MEMORY	B	1, 2
d	0x64	WRITE USER MEMORY	B	1, 2
n	0x6E	LOCK USER MEMORY	B	1, 2
e	0x65	ONE TAG READ EPC	C	X
f	0x66	MULTI TAG READ EPC	C	X
r	0x72	BANK SELECT READ	C	1, 2, 3, (4)
w	0x77	BANK SELECT WRITE	C	1, 2, 3, (4)

I	0x6C	BANK SELECT LOCK	C	1, 2, (3)
K	0x6B	TAG KILL (Select Tag)	C	1,(2)
J	0x6A	ONE TAG READ EPC (Select Tag)	C	1, 2, 3
Y	0x79	MULTI TAG READ EPC (Select Tag)	C	1, 2, 3
m	0x6D	BANK SELECT READ (Select Tag)	C	1, 2, 3, 4, (5)
q	0x71	BANK SELECT WRITE (Select Tag)	C	1, 2, 3, 4, (5)
z	0x7A	BANK SELECT LOCK (Select Tag)	C	1, 2, 3, (4)
0	0x30	HITACHI READ LOCK	HC	1, 2, (3)
1	0x31	HITACHI GET SYS INFO	HC	X
4	0x34	NXP READ PROTECT	NC	1
5	0x35	NXP RESET READ PROTECT	NC	1
6	0x36	NXP CHANGE EAS	NC	2

7	0x37	NXP EAS ALARM	NC	X
---	------	---------------	----	---

※ op : Optional

– ‘ (0x20) : SPACE

– PARAMETER

COMMAND	PARA 1	PARA 2	PARA 3	PARA 4
READ USER MEMORY (TYPE B)	Memory Address '0'(0x30)~'255' (0x323535)	Length '1'(0x31) ~ "255"(0x323535)	X	X
WRITE USER MEMORY (TYPE B)		Write Data (2 ~ 100 Byte) Ex) "12" (0x3132)	X	X
LOCK USER MEMORY (TYPE B)	Memory Address '0'(0x30)~'255' (0x323535)	Length '1'(0x31) ~ "255"(0x323535)	X	X
ONE TAG READ EPC	(Access Password) (8 Byte)	X	X	X
MULTI TAG READ EPC	(Access Password) (8 Byte)	X	X	X
BANK SELECT READ (TYPE C)	MemBank '0'(0x30) : Reserved '1'(0x31) : EPC '2'(0x32) : TID '3'(0x33) : User	WordPtr '0'(0x30) ~ 'MAX'	Length '1'(0x31)~ '255'(0x323 535)	(Access Password) (8 Byte)
BANK SELECT WRITE (TYPE C)			Write Data (4 ~ 100 Byte) Ex) "1234" (0x3132333	(Access Password) (8 Byte) Ex) "12345678" (0x31323333

			4)	435363738)
BANK SELECT LOCK (TYPE C)	MASK (4 Byte) Ex) “0030” (0x30303330)	ACTION (4 Byte) Ex) “0020” (0x30303230)	(Access Password) (8 Byte)	X
TAG KILL or TAG KILL_Tag Sel (TYPE C)	KILL PASSWORD (8 Byte) Ex) “12345678” (0x31323334353 63738)	(EPC(TagID)) Ex) “00001111” (0x303030303131 3131)	X	X
ONE TAG READ EPC _Tag Sel (TYPE C)	MemBank ‘0’(0x30) : Reserved ‘1’(0x31) : EPC ‘2’(0x32) : TID ‘3’(0x33) : User	BitPtr ‘0’(0x30) ~ ‘MAX’	MASK (1 Byte 이상) Ex) “12345” (0x3132333 435))	X
MULTI TAG READ EPC _Tag Sel (TYPE C)				X
BANK SELECT READ_Tag Sel (TYPE C)	PARA1~3		PARA4	PARA5
BANK SELECT WRITE_Tag Sel (TYPE C)	PARA1~3은 BANK SELECT READ/WRITE와 동일		EPC(TagID) Ex) “00001111” (0x3030303 031313131)	(Access Password) (8 Byte)

BANK SELECT LOCK_Tag Sel (TYPE C)	MASK (4 Byte) Ex) "0030" (0x30303330)	ACTION (4 Byte) Ex) "0020" (0x30303230)	EPC(TagID) Ex) "00001111" (0x3030303031313131)	(Access Password) (8 Byte)
HITACHI READ LOCK	MASK (4 Byte) Ex) "0030" (0x30303330)	ACTION (4 Byte) Ex) "0020" (0x30303230)	(Access Password) (8 Byte)	X
NXP READ PROTECT	Access Password (8 Byte)	X	X	X
NXP RESET READ PROTECT	Access Password (8 Byte)	X	X	X
NXP CHANGE EAS	SET/RESET (1 Byte) SET '1'(0x31) RESET '0'(0x30)	Access Password (8 Byte)	X	X

※ WRITE USER MEMORY(TYPE B)는 2byte 단위(ex 31h 32h)로 Write가 가능하며, BANK SELECT WRITE(TYPE C)는 4byte 단위(ex 31h 32h 33h 34h)로 Write가 가능함. (아스키 코드 기준) 두 Command 모두 Data의 길이를 따로 지정할 필요가 없이 쓸 data만큼 각 단위에 맞게 Parameter에 넣어주면 된다. WRITE DATA는 100Byte(TAG 기준 50byte data)를 넘지 않도록 한다.

※ Access Password는 생략 가능 함.

※ Tag Select Command는 특정 Tag만 선택하여 Read/Write하기 위해 사용 한다.

※ ONE/MULTI TAG READ EPC_Tag Sel의 파라미터 중 BitPtr은 비트단위를 나타낸다. 예를 들면 WordPtr이 1이면 BitPtr은 16이며, WordPtr이 2이면 BitPtr은

32가 된다.

※ TAG KILL/TAG KILL_TAG Sel은 명령어는 같으나 2번째 파라미터(EPC)가 생략되면 TAG KILL이며, 두번째 파라미터로 1byte이상의 EPC data를 전송하면 TAG KILL_TAG Sel 명령어가 된다.

- 응답 : ACK, RES TAG READ

- 예제)

1) ONE TAG READ EPC : 7Eh 03h 60h 65h 05h 7Dh (“e”)

2) MULTI TAG READ EPC : 7Eh 03h 60h 66h 06h 7Dh (“f”)

3) BANK SELECT READ : 7Eh 09h 60h 72h 20h 31h 20h 32h 20h 31h 00h
7Dh(“r 1 2 1”)

4) BANK SELECT WRITE :

7Eh 18h 60h 77h 20h 31h 20h 34h 20h 31h 31h 31h 31h 32h 32h 32h 32h
33h 33h 33h 33h 34h 34h 34h 34h 32h 7Dh (“w 1 4 1111222233334444”)

5) BANK SELECT LOCK/HITACHI READ LOCK :

7Eh 0Ch 60h 6Ch 20h 30h 30h 33h 30h 20h 30h 30h 32h 30h 0Dh 7Dh
(“l 0030 0020”)

6) TAG KILL :

7Eh 0Bh 60h 6Bh 20h 31h 32h 33h 34h 35h 36h 37h 38h 23h 7Dh
(“k 12345678”)

7) BANK SELECT WRITE + Access Password

7Eh 15h 60h 77h 20h 31h 20h 34h 20h 31h 31h 31h 31h 20h 31h 32h 33h
34h 35h 36h 37h 38h 1Ah 7Dh(“w 1 4 1111 12345678”)

8) ONE TAG READ EPC_TAG SELECT

“j 1 32 000011112222333344445555”

9) MULTI TAG READ EPC_TAG SELECT

“y 1 32 1234” -> EPC가 1234로 시작되는 TAG들만 응답

10) BANK SELECT READ _TAG SELECT

“m 1 2 2 000011112222333344445555”

11) BANK SELECT WRITE _TAG SELECT

“q 1 4 1111 000011112222333344445555”

12) HITACHI READ LOCK :

7Eh 0Ch 60h 6Ch 20h 30h 30h 32h 30h 20h 30h 30h 32h 30h XXh 7Dh

(“0 0020 0020”)

13) HITACHI GET SYS INFO : 7Eh 03h 60h 31h XXh 7Dh (“1”)

14) BANK SELECT LOCK_TAG SELECT :

“z 0020 0020 000011112222333344445555”

15) TAG KILL_TAG SELECT :

“k 12345678 000011112222333344445555”

※ TYPE B의 경우도 위의 예제와 유사함.

7) RES TAG READ

리더가 TAG에 수행한 명령어에 대한 응답으로 TAG를 READ하였을 경우는 이에 해당하는 TAGID를 문자열로 전송한다. 단, 수행 한 명령어가 MULTI TAG READ UID/EPC인 경우는 여러 개의 TAGID를 전송해야 할 경우가 발생하는 데, 이 때는 리더가 TAG를 읽을 때마다 TAGID를 전송한 뒤 마지막에 종료 메시지(“FF”)를 전송한다. TAG를 WRITE를 하였을 경우는 성공하였을 때는 Success(“01”)코드를 전송하며, TAG로부터 에러 코드를 받았을 때는 이를 그대로 메시지로 전송한다.

리더는 TAG를 DETECT하였을 경우 항상 BUZZ를 울리고, TAGID 및 응답코드를

전송한 뒤 자동으로 종료하게 된다. 단, MULTI TAG READ EPC 명령어 일 때는 반드시 설정된 시간(Scan Time) 동안 계속 수행 한 뒤 종료 된다. TAG를 DETECT하지 못하였을 경우는 모든 TAG명령어를 설정된 시간(Scan Time)동안 수행하고 에러코드를 전송한 뒤 자동으로 종료한다. 종료된 다음 리더는 곧 바로 SLEEP MODE로 들어가게 된다.

Octet	7	6	5	4	3	2	1	0
0	0xA0 or 0xA1 or 0xAE							
1	DATA1							
2	DATA2							
...	..							

- 단말기 <- 리더
- 기능 : REQ TAG READ에 대한 응답 메시지
- COMMAND CODE : TAG ID Data 와 TAG Response Code를 구분

1) 0xA0

리더가 보내는 DATA가 TAG Memory의 data인 경우.

예) EPC, TID, UID, USER MEMORY 등..

2) 0xA1

리더가 보내는 DATA가 TAG Memory의 data인 경우에 패킷의 길이(PL)가 255byte가 넘을 경우. 이 때 PL은 실제 패킷 길이에 255를 뺀 값을 나타낸다. 즉, PL = 총 패킷 Length - 255 가 된다.

예제) 7Eh XXh A1h (30h 31h... 30h) XXh 7Dh
 └───> 254byte

3) 0xAE

리더가 보내는 DATA가 ERROR 코드이거나 TAG로부터 수신한 응답 코드일 경우

- DATA : REQ TAG READ의 READER COMMAND에 따라 각각 응답

1) ONE TAG READ UID

TAGID의 UID(64bits)를 16 Octet으로 전송

예제) 7Eh 1Ah A0h (30h 31h... 30h) 00h 7Dh
 └─── 16 Octet(UID)

※ TAG(TYPE B)는 8byte로 구성 되지만 리더에서 단말기로 전송 할 때에는 TAGID를 아스키 문자로 변환하여 전송하므로 2배가 늘어난 TAGID(16byte)가 된다. (예제 “01” -> “3031”)

2) MULTI TAG READ UID

TAGID를 16 Octet로 계속 전송. 즉 data길이가 17 Octet(COMMAND CODE 포함)인 패킷을 TAG의 응답이 있을 때 마다 전송하고 지정된 시간(Scan Time)이 지나거나 STOP Command('#')를 받으면 종료 코드(“FF”)를 전송한다.

예제) 7Eh 1Ah A0h 30h 31h... 30h 00h 7Dh

7Eh 1Ah A0h 30h 32h... 33h 01h 7Dh

.

.

7Eh 1Ah A0h 34h 35h... 36h 02h 7Dh

7Eh 04h AEh 46h 46h AEh 7Dh(“FF”(0x4646) : 종료코드)

※ 종료코드는 TAG Memory Data가 아니므로 COMMAND CODE는 ‘AEh’이다.

3) ONE TAG READ EPC

EPC Bank의 PC(16bits)와 EPC(0~256bits)를 포함한 TAGID를 전송

※ TYPE C(Gen2.)의 EPC는 TAG에 따라 길이가 다양하므로 리더는 TAG의 응답에 따라 PC(16bits)와 함께 0~256bit의 EPC를 전송한다.

※ 리더는 2byte 이상의 Hex값을 아스키 코드로 변환하여 전송되므로 실제 전송량은 2배가 늘어나므로 4byte 이상의 TAGID를 전송함.

예제) PC 16bits“0800” + EPC 32bits(“12345678”) ->

7Eh 0Eh A0h 30h 38h 30h 30h 31h 32h 33h 34h 35h 36h 37h 38h A0h
7Dh



PC+ EPC

4) MULTI TAG READ EPC

PC와 EPC를 포함한 여러 개의 TAGID를 연속적으로 전송. 즉, 패킷을 TAG의 응답이 있을 때 마다 전송하고 설정된 시간(Scan Time)이 지나거나 STOP Command(‘#’)를 받으면 종료 코드(“FF”)를 전송한다.

예제) 7Eh 1Ah A0h 30h 31h... 30h 00h 7Dh

7Eh 1Ah A0h 30h 32h... 33h 01h 7Dh

.

.

7Eh 1Ah A0h 34h 35h... 36h 02h 7Dh

7Eh 04h AEh 46h 46h AEh 7Dh(“FF”(0x4646) : 종료코드)

※ 종료코드는 TAG Memory Data가 아니므로 COMMAND CODE는 ‘AEh’이다.

※ 각기 다른 EPC 길이를 가진 TAG가 응답할 수 있으므로 DATA길이는 가변적임.

5) USER MEMORY READ/BANK SELECT READ

각 PARAMETER로 지정한 LENGTH의 DATA를 전송

예제) 7Eh XXh A0h (30h 31h... 30h) XXh 7Dh
 variable length data

6) USER MEMORY WRITE/BANK SELECT WRITE/BANK SELECT LOCK/TAG

KILL/USER MEMORY LOCK/HITACHI READ LOCK/NXP READ PROTECT

```
/NXP RESET READ PROTECT/NXP CHANGE EAS
```

TAG의 응답 코드를 전송(2 Octet)

“01”(0x3031) : Success

“00”(0x3030) : Other error

“03”(0x3033) : Memory overrun

“04”(0x3034) : Memory locked

“0B”(0x3042) : Insufficient power

“0F”(0x3046) : Non-specific error

예제) 7Eh 04h AEh 30h 31h AFh 7Dh(Success)

※ LOCK 되어 있는 TAG가 리더로부터 틀린 Access Password를 받았을 경우 어떤 응답도 하지 않는다. 단, Access Password 없이 Access할 경우 Memory locked로 응답 함.

7) HITACHI GET SYS INFO

HITACHI PROTOCOL 중 GetSystemInformation Command에 대한 응답으로 15 BYTE DATA를 전송.

예제) 7Eh 20h A0h 46h 46h 38h 30h 31h 30h 31h . . . 30h 30h XXh 7Dh
(FF801011046007083000000000000000)

8) NXP EAS ALARM

NXP PROTOCOL 중 EAS ALARM Command에 대한 응답으로 8 BYTE DATA(EAS CODE)를 전송.

Octet	7	6	5	4	3	2	1	0
0	Info Flags							
1								
2	Reserved							
3	UII(EPC)							
4	TID							
5	User							
6	Set Attenuate Level							
7	Bank Lock							
8								
9	Block Read Lock							
10								

11	Block Read/Write Lock
12	
13	Block Write Lock
14	

< Get System Information Command Response >

※ 응답 DATA의 15byte는 Header, Length, RN, CRC-16을 제외한 DATA임.

※ 응답 DATA의 자세한 내용은 HITACHI PROTOCOL 문서 참조.

8) ERROR CODE

“05”(0x3035) : Not Detect

“06”(0x3036) : Data error

예제) 7Eh 04h AEh 30h 35h ABh 7Dh(Not Detect)

- 응답 : 없음.

8) STOP

리더가 TAG명령어를 수행하고 있는 동안 종료해야 할 경우가 필요 할 때 쓰는 메시지이다. 단, STX, PL, CHECKSUM, ETX는 생략되고 오직 ‘#’ (0x23) 만 전송한다.

Octet	7	6	5	4	3	2	1	0
0	0x23							

- 단말기 -> 리더

- 기능 : TAG명령어를 강제 종료하는 메시지.
- '#'(0x23) : STOP(강제종료)
- 강제종료의 패킷은 STX, PL, CHECKSUM, ETX가 생략되고 오직 '#'(0x23)만 전송한다.
- 응답 : 없음.
- 예제) 23h('#')

5 부 록

BANK SELECT LOCK

- BANK SELECT LOCK Command 사용하기:

'l [Mask(4byte)] [Action(4byte)]'(6Ch 20h XXh XXh XXh 20h XXh XXh XXh XXh)

* Mask :

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
						Kill Pwd		AccessPwd		EPC		TID		User	
						pwd	lock	pwd	lock	pwd	lock	pwd	lock	pwd	Lock

Bit 0 : Lock bit를 변경하지 않음.

Bit 1 : Lock bit를 변경.

* Action :

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
						Kill Pwd		AccessPwd		EPC		TID		User	
						pwd	lock	pwd	lock	pwd	lock	pwd	lock	pwd	Lock

Pwd Bit 0 : Read/Write시에 Password가 필요없음.

Pwd Bit 1 : Read/Write시에 Password가 필요함.

Lock Bit 0 : Pwd Bit를 변경할 수가 있음.(단, AccessPwd를 알고있거나, Accesspwd가 0으로 설정되어 있어야함.)

Lock Bit 1 : Read/Write을 영구적으로 할 수가 없으며, Pwd Bit와 Lock Bit를 변경할 수 없음.

※ Lock Command 는 AccessPwd가 '0'이거나 AccessPwd를 알고있어야 실행 할수있음.

※ Kill Pwd, AccessPwd는 Read/Write에 대한 pwd/lock 기능을 가지며, 나머지는 Write에 대한 pwd/lock 기능을 가짐.(결국 Kill Pwd, AccessPwd를 제외한 모든 메모리는 어떠한 상태에서 Read가 가능함)

※ Lock Bit를 한번 1로 변경하면 다시 0으로 변경할 수가 없음.

※ Mask, Action을 리더로 전송 할 때에는 다른 명령어와 마찬가지로 아스키 코드로 인코딩하여 리더로 전송 해야 함. Ex) Mask가 "0030" 일 경우 "0x30303330"으로 변환해 주어야 함.

※ Lock 시나리오 1 :

Pwd Bit : 1 , Accesspwd : 0

해당 메모리에 Write/Password Read를 하는 것은 불가능 하지만 Pwd Bit를 0 으로 변경하고 다시 Write/Password Read를 할 수가 있음. 즉, 1차적으로 Write/Password Read를 할 수 없도록 할 수는 있으나 Pwd Bit를 0으로 변경한다면 누구나 Write/Password Read를 할 수가 있음.

※ Lock 시나리오 2 :

Pwd Bit : 1 , Accesspwd : 00이 아닌 값

해당 메모리에 Write/Password Read를 하기 위해선 반드시 Accesspwd를 알고 있어야 함.
각 명령어(BANK SELECT READ/WRITE/LOCK)의 마지막 파라미터에 TAG의 Access Password(아스키코드 기준 8 Byte)를 포함하면 가능함.

- BANK SELECT READ Command 를 이용해 TAG에 설정되어 있는 Lock Bit 를 읽어오기

: TAG의 Lock bit를 읽어 오려면 Bank Select Read Command “r 0 4 1”명령어를 이용하면 됨. 응답되는 16bits중 상위 10bits가 이에 해당 됨.

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Kill Pwd		AccessPwd		EPC		TID		User							
pwd	lock	pwd	lock	pwd	lock	pwd	lock	pwd	lock						

Ex) Reader Reply : “0300”(0x30333030) -> TID Pwd, Lock Enable

※ “r 0 4 1”, “0300” 은 패킷의 DATA부분 중 중요 부분만 표현 한 것 임. 아래 설명들도 동일한 표현을 적용함. 정식 표현은 본문 참조바람.

- BANK SELECT READ Command 를 이용해 TAG의 AccessPwd 를 읽어오기

: “r 0 2 2 (XXXXXXXX)” 명령어를 이용하면 됨. Pwd Enable 된 TAG는 Access Password 8Byte (XXXXXXXX)를 포함 하여야함.

Ex) Reader Reply : “00000000”(0x3030303030303030) -> AccessPwd가 ‘0’이므로 Lock Command를 Password 없이 실행시킬 수 있음

- BANK SELECT WRITE Command를 이용하여 AccessPwd 변경하기

: “w 0 2 XXXXXXXX (XXXXXXXX)”를 이용하면 됨

※ AccessPwd 의 Lock bit중 Pwd가 Enable 되어 있을 경우 기존 Pwd를 BANK SELECT WRITE Command의 파라미터 4에 포함하여 새 Pwd로 바꿀 수 있으나 이때는 한번에 2byte씩 해야 하며, 통신환경에 따라 Write는 되었으나 응답이 제대로 오지 않을 수가 있음. 그러므로 이 방법은 권장하지 않음. 이 경우에는 AccessPwd 의 Lock bit중 Pwd를 Disable 시킨 뒤 실행 할 것을 권장함.

- Access Password를 이용하여 TAG Access를 제한하기의 예

1. BANK SELECT WRITE로 data를 입력한다. Ex) w 1 2 11112222333344445555
2. BANK SELECT WRITE로 ACCESS Password를 입력한다. Ex) w 0 2 12345678
3. ACCESS Password를 포함한 BANK SELECT LOCK로 ACCESS Password, EPC BANK pwd를 enable 한다. Ex) l 00a0 00a0 12345678
4. ACCESS Password를 포함한 BANK SELECT WRITE로 data를 변경 할 수 있다.

Ex) w 1 2 6666777788889999aaaa 12345678

※ 위 방법은 한가지의 예로서 다른 방법을 사용할 수도 있음.

🔑 TAG KILL

– TYPE C KILL Command 사용하기:

'k [password(8byte)]'(6Bh XXh XXh XXh XXh XXh XXh XXh XXh)

* password : KILL Password는 Reserved Memory(MemBank 0) 0번지(상위), 1번지(하위)에 저장된다. KILL Password가 모두 '0'일 경우는 KILL을 할 수 없으므로 KILL을 하기 위해선 반드시 '0'이 아닌 KILL Password가 저장되어 있어야 한다. KILL Password는 Bank Select Write를 이용하여 저장할 수 있으며, Bank Select Read를 이용해 읽을 수 있다.

Ex1) KILL Password 읽어오기 : “r 0 0 2 (XXXXXXXX)” -> 리더 응답 : “00000000”

Ex2) KILL Password 저장하기 : “w 0 0 12345678 (XXXXXXXX)” -> 리더응답 : “01”

Ex3) KILL 하기 : “k 12345678(0x6B203132333435363738)” -> 리더응답 : “01”

※ KILL Command에 대한 응답은 “01”이 들어와야 하지만 통신환경에 따라 KILL이 되었지만 응답이 오지 않을 수 있으므로 이때는 응답을 계속적으로 기다리는 것 보다 Read하여 확인할 것을 권장함.

※ 한번 KILL된 TAG는 다시 변경 할 수 없으므로 사용시 주의해야 함.

🔑 HITACHI READ LOCK

– HITACHI READ LOCK Command 사용하기 :

'0 [Mask(4byte)] [Action(4byte)]'(6Ch 20h XXh XXh XXh XXh 20h XXh XXh XXh XXh)

* Mask :

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
										UID(EPC)		TID		User	
										pwd	lock	pwd	lock	pwd	Lock

Bit 0 : Lock bit를 변경하지 않음.

Bit 1 : Lock bit를 변경.

* Action :

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
										UID(EPC)		TID		User	
										pwd	lock	pwd	lock	pwd	Lock

Pwd Bit 0 : Read/Write시에 Password가 필요없음.

Pwd Bit 1 : Read/Write시에 Password가 필요함.

Lock Bit 0 : Pwd Bit를 변경할 수가 있음.(단, AccessPwd를 알고있거나, Accesspwd가 0으로 설정되어 있어야함.)

Lock Bit 1 : Read/를 영구적으로 할 수가 없으며, Pwd Bit와 Lock Bit를 변경할 수 없음.

- ※ Lock Command 는 AccessPwd가 '0'이거나 AccessPwd를 알고있어야 실행 할수있음.
- ※ Lock Bit를 한번 1로 변경하면 다시 0으로 변경할 수가 없음.
- ※ Mask, Action을 리더로 전송 할 때에는 다른 명령어와 마찬가지로 아스키 코드로 인코딩하여 리더로 전송 해야 함. Ex) Mask가 "0030" 일 경우 "0x30303330"으로 변환해 주어야 함.
- ※ Lock Bit 에 1을 Setting 하면 해당 영역의 메모리는 영구적으로 Read할 수가 없으므로 주의해야 함.