

REM(CRE) 1356 Series

Ceyon Access Protocol

Version 1.3S

<Revision History>

Date	Version	Name	Note
2004-10-18	CAP v1.3r0	Yongsoon Kim	Created
2004-12-12	CAP v1.4r0	***	Added and updated
2005-08-03	CAP v1.5r0	YoungSik Kim	Updated
2009-12-08	CAP v1.3S	JinDong Lee	Updated
2011-01-05	CAP v1.3S	SungMin Bae	Added the ErrorCode
2015-11-10	CAP v1.3S	s.i.Pack	Add Read UID
2016-05-27	CAP v1.3S	j.s.Nam	Add the Introduction

Contents

1	Introduction	4
2	Communication Protocol.....	4
3	교신 명령.....	5
3.1	교신 포맷.....	5
3.2	리더 운영 모드	8
3.3	Read 명령	9
3.4	Write 명령.....	10
3.5	기타	13
3.6	교신 에러 코드	14
4	Reader기의 환경 설정 Register.....	16
4.1	Registry 세부 설명	17
4.1.1	ERFCH.....	17
4.1.2	CFG1.....	17
4.1.3	CMD0.....	18
4.1.4	RTB	18
4.1.5	RTA	18
4.1.6	VTO	19
5	Appendix (ASCII 테이블)	20
6	Appendix (UID Format)	21

1 Introduction

이 문서는 세연테크놀로지(Ceyon Technology)의 HF RFID Reader와 Host간의 통신 규약을 정의합니다.

프로토콜의 명칭 및 버전은 CAP1.3S이며 Ceyon Reader Access Protocols v1.3S의 줄임 말입니다.


HF RFID Reader와 Host가 통신하기 위해서는 반드시 이 프로토콜 문서를 먼저 숙지 해야 하며 아울러 Reader의 속성을 이해 및 제어하기 위해서는 [<4 Reader기의 환경 설정 Register>](#)을 숙지하시기 바랍니다.

2 Communication Protocol

세연 장비와 통신하기 위한 방법은 시리얼통신(Serial)과 TCP통신(네트워크 모듈이 장착된 모델의 경우) 두 가지 입니다.

시리얼 통신을 하기 위한 규격은 하기와 같습니다.

Items	Descriptions
Baudrate	9600bps
Data & Stop Bi	8Bit / 1Bit
Flow Control	None
Parity Bit	None
Protocol	CAP1.3S

 모델에 따라서 일부 다를 수 있으므로 반드시 하드웨어 사양서를 참고하시기 바랍니다

유의사항

1. TCP/IP 통신 상태 체크

- Reader와 Host간의 통신상태가 정상 상태인지 확인하기 위해, 주기적으로 Reader에 [특정 레지스터](#)를 호출하여 통신상태를 확인 할 수 있게 설정해 주시기 바랍니다.
- 고정된 TCP/IP 사용시 중복된 IP를 사용하고 있는 곳이 없는지 확인 후 설정해주시기 바랍니다. 동일한 IP를 두 대의 리더에서 사용시 IP 충돌이 발생할 수 있습니다.

2. Reading 방법에 대한 가이드라인

- Reading 명령은 Tag값 또는 Timeout 값이 왔을 때 끝이 납니다.
- Reading 명령중에 또 다른 두번째 리딩 명령을 리더에 보내면 무시됩니다.
- 연속 동작을 하기 위해서는 반드시 Tag값 또는 Timeout 패킷을 받은 후 다음 리딩 동작을 시도해야 합니다.

3. 리더 에러코드

- Read 명령어는 [VTO]레지스터에서 정한 제한시간 동안 태그 인식 실패시 Timeout 메시지 및 에러 메시지가 발생합니다. 자세한 사항은 레지스터 [3.4 교신에러코드](#)를 참고 바랍니다
- ※ [VTO시간 + 1~2초] 동안 대기 후 리더기로부터 응답을 받고 Reading 명령을 다시 요청하기 바랍니다.

3 교신 명령

3.1 교신 포맷

송신과 수신은의 기본 통신 포맷은 그림1과 같다. HOST와 Reader기는 기본적으로 ASCII 통신을 한다. 교신 명령은 읽기 요구와 쓰기 요구로 나뉘어진다. HOST에서 보내는 명령은 읽기/쓰기 요구에 관계없이 동일한 포맷을 갖는다. 기기로부터의 응답 포맷은 그림1과 같이 읽기/쓰기 성공/실패에 따라 그림1과 같이 다른 형태를 가지게 된다.

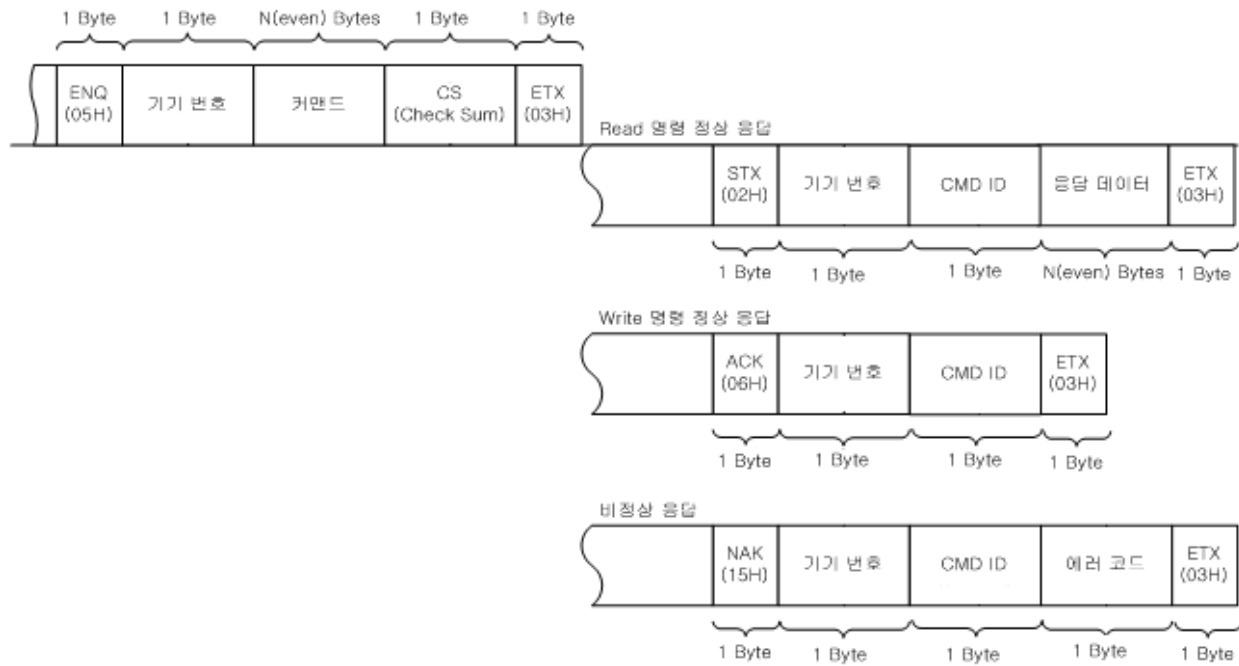


그림1 기본 통신 포맷

■ ASCII통신(CAP1.3S Protocol) 이란?

CAP1.3S Protocol은 기본적으로 ASCII통신을 한다.

ASCII통신 이란 HOST에서 리더로 명령어를 전송할 때 바이너리 1바이트를 두 개의 ASCII 바이트로 나누어 전송 및 수신하는 것을 의미한다.

예를 들면, 리더의 '0B' 레지스터 값을 조회하는 커맨드가 아래와 같다면

ENQ	Reader ID	Command	Address	Len	Check Sum
0x05	0x01	0x08	0x0b	01	?

이것을 ASCII 바이트로 변환하면 패킷의 구조는 아래 같다.

ENQ	Reader ID	Command	Address	Len	Check Sum
0x05	0x01	0x08	0x0B	0x01	0x1A

※ Check Sum은 ASCII 바이트로 모두 변환한 후 ENQ + Reader ID + Command + Address + Len을 모두 더한 값임

※ ENQ, STX, ETX, NAK등 패킷의 시작과 끝을 의미하는 것을 제외한 모든 패킷은 ASCII로 구성되어야 하므로 패킷의 시작과 끝 그리고 데이터 영역을 정확하게 구분할 수 있다.

■ 바이너리 통신(CAP1.3S Protocol) 지원

본 RFID리더는 기본적으로 상기의 ASCII통신포맷(CAP1.3 Protocol)으로 통신을 하지만 컨베이어와 같은 PLL인터페이스를 위해 ASCII통신 대신 바이너리 통신(CAP1.3S Protocol)을 지원한다.

바이너리 통신(CAP1.3S Protocol)을 적용하면 위의 예제 패킷은 아래와 같은 구조로 구성된다.

ENQ	Reader ID	Command	Address	Len	Check Sum
0x05	0x01	0x08	0x0B	0x01	0x1A

※ Check Sum은 Check Sum을 제외한 모든 패킷의 합이므로 0x1A

☞ CAP1.3 프로토콜을 CAP1.3S 프로토콜로 변경하기 위해서는 CFG1레지스터를 참고한다

3.2 리더 운영 모드

리더의 운영모드는 아래와 같이 두 가지 모드로 동작하게 되며 운영모드의 변경은 리더의 레지스터(CFG1)의 값을 셋팅하여 전환한다.

■ Verbose Mode

리더가 명령어 대기 상태로 있으며 HOST로부터 Tag Read Command를 수신하면 리더는 VTO(Verbose Timeout)동안 태그를 읽어 HOST로 응답한다. 이때, VTO시간 전에 태그 데이터를 읽으면 VTO시간 전에 응답하고 다시 명령어 대기 상태로 돌아간다. (VTO 레지스터 참고)

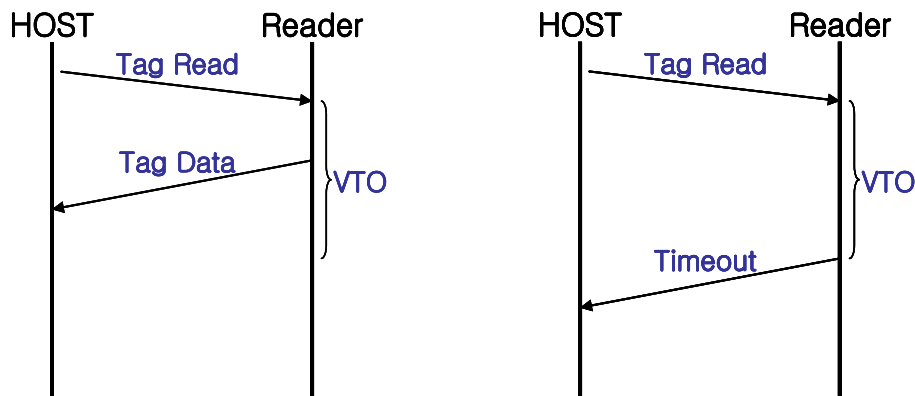


그림2 Verbose Mode Sequence

■ Continuous Mode

리더의 모드가 Continuous Mode의 경우 리더는 태그의 유무를 계속 감시하며 RF필드 내에 태그가 감지되면 태그데이터를 읽어 HOST로 송신한다. 태그데이터를 송신한 이후에도 동일한 태그가 RF필드 내에 계속 머무르면 주기적으로 태그데이터를 읽어 HOST로 송신하게 된다.(RTA, RTB레지스터 참고)

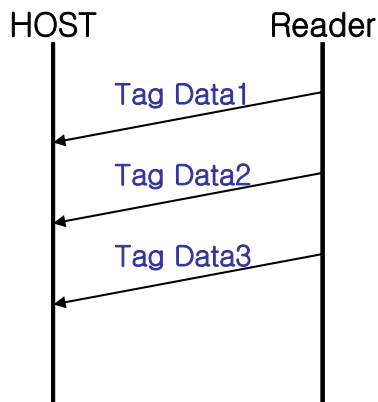


그림3 Continuous Mode Sequence

3.3 Read 명령

Read 명령은 Reader기의 환경설정(Register) 그리고 채널 별 RF TAG를 읽기 위한 명령으로 구분된다. 각각의 명령 코드는 아래와 같다.

명령 ID	Operation	Note
08H	Read System Register	Reader기의 환경설정 상태를 읽어 온다.
80H	Read RF Tag	각 채널별 RF TAG의 값을 읽어 온다. 채널의 선택은 하위4bit를 이용한다. (ex. 채널4번의 RF TAG 값을 읽기위한 명령 ID는83H)
	Read UID	Read RF Tag 명령과 동일하고 Packet의 Address와 Length를 0xFF로 설정한다. Channel No는 Read RF Tag와 동일

표 1 읽기 명령 코드

READ 명령 FORMAT은 아래 그림과 같고, 1Byte 에서 최대 112 Byte를 읽을 수 있다.

Host		Reader
[ENQ][RID][CMD][DATA][LEN][CS]	→	
정상 응답	←	[STX][RID][CMD][DATA][ETX]
비정상 응답	←	[NAK][RID][CMD][ERCD][ETX]

RID: 리더기의 기기번호는 H30 H31로 고정

CMD : 명령어(Command ID)

DATA : Request

CMD Type	Field #1	Field #2
08H (2 Bytes)	Length (1Byte)	Register (1Byte)
80H (2 Bytes)	Address (1Byte)	Length (1Byte)

DATA : Request

CMD Type	Field #1	Field #2	Field #3
08H (2 Bytes)	Length (1Byte)	Register (1Byte)	Value (1Byte)
80H (2 Bytes + N Data)	Address (1Byte)	Length (1Byte)	Data (N Byte)
80H (2 Bytes + 8Bytes)	Address (1Byte)	Length (1Byte)	UID (8 Bytes)

ERCD : 에러 코드

LEN : 데이터 사이즈

CS : 체크섬

■ 시스템 레지스트리 읽기

리더의 h0B 레지스터를 읽을 경우의 정상적인 동작의 예를 들면 아래와 같다.

CMD : 0x08

DATA : 0x0B – CFG1 레지스터

LEN : 0x01 – DATA의 사이즈

[HOST → READER]

h05[ENQ] h01[RID] h08[CMD] h0B[DATA] h01[LEN] h1A[CS]

– DATA는 읽고자 하는 레지스트리의 주소(번지)가 됨

[HOST ← READER]

h02[STX] h01[RID] h08[CMD] hDE[DATA] h03[ETX]

– DATA는 요청한 레지스터의 주소의 값(value)이 됨

■ 태그 읽기

1번 채널에서 Tag Address 0번지에서 8 Byte를 읽는 명령의 예이다.(Verbose mode 상태에서 가능하다)

CMD : 0x80

DATA : 0x00[ADD] 0x08[LEN]

[HOST → READER]

h05[ENQ] h01[RID] h80[CMD] h00 h08[DATA] h8E[CS]

– DATA는 태그를 읽을 시작 주소(h00)과 시작 주소로부터 읽을 사이즈(h08)로 구성

– 2번 채널의 경우의 CMD는 h81이며 하위비트(h1)는 채널을 의미함

[HOST ← READER] 정상적으로 태그를 읽은 경우

h02[STX] h01[RID] h80[CMD] h31 h32 h33 h34 h35 h36 h37 h38[DATA] h03[ETX]

– DATA는 태그의 0번지부터 8바이트를 읽은 데이터이며 ASCII로 “12345678”을 나타냄

☞ continuous mode에서 태그를 읽었을 때 올라오는 data의 포맷은 상기의 포맷과 동일하지만 CMD가 채널 별로 0xA0, 0xA1, 0xA2, 0xA3, 0xA4로 구성되어 진다.

3.4 Write 명령

Write 명령은 Reader기의 환경설정(Register) 그리고 채널 별 RF TAG를 쓰기 위한 명령으로

구분된다. 각각의 명령 코드는 아래와 같다.

명령 ID	Operation	Note
18H	Write System Register Byte	Reader기의 환경설정 상태를 Byte단위로 쓴다.
90H	Write RF Tag	각 채널별 RF TAG에 값을 쓴다. 채널의 선택은 하위4bit를 이용한다. (ex. 채널4번의 RF TAG에 값을 쓰기위한 명령 ID는93H)

표 2 쓰기 명령 코드

WRITE 명령 FORMAT은 아래와 같고, 1 Byte에서 최대 112Byte를 쓸 수 있다.

Host	Reader
[ENQ][RID][CMD][DATA][CS]	→
정상 응답	← [ACK][ADD][CMD][ETX]
비정상 응답	← [NAK][ADD][CMD][ERCD][ETX]

RID : 리더기의 기기번호는 H30 H31(0x01)로 고정

CMD : 명령어(Command ID)

DATA : 데이터(레지스트리 값을 변경하는 경우는 ADD + LEN + VAL로 구성)

ADD : 레지스트리 주소(번지)

VAL : 레지스트리 값(Value)

LEN : 데이터 사이즈(VAL의 사이즈)

ERCD : 에러 코드

CS : 체크섬

■ 시스템 레지스트리 쓰기

리더의 h0B 레지스터의 값을 변경하여 리더의 동작상태를 verbose mode로 변경하는 경우의 정상적인 동작의 예를 들면 아래와 같다.

CMD : 0x18

ADD : 0x0B – CFG1 레지스터

LEN : 0x01 (VAL의 사이즈)

VAL : 0x9E – 레지스터에 쓸 값

[HOST → READER]

h05[ENQ] h01[RID] h18[CMD] h0B[ADD] h01[LEN] h5E[VAL] h88[CS]

– 레지스트리 ADD번지에 VAL값을 0x5E로 변경함

[HOST ← READER]

h06[ACK] h01[RID] h18[CMD] h03[ETX]

– 성공적으로 레지스트리의 값을 변경한 경우

■ 태그 쓰기

1번 채널에서 Tag Address 0번지에서 8 Byte를 쓰는 명령의 예이다.(Verbose mode 상태에서 가능하다)

CMD : 0x9x – 0번 채널의 경우 h90, 1번 채널의 경우 h91

ADD : 0x00 – 태그의 Writing할 시작 주소(번지)

LEN : 0x08 – Writing할 데이터 사이즈

DATA : Writing할 실제 데이터(아래 예제의 경우 “12345678”을 Writing함)

[HOST → READER]

h05[ENQ] h01[RID] h90[CMD] h00[ADD] h08[LEN] h31 h32 h33 h34 h35 h36 h37 h38[DATA] h42[CS]

– 태그에 데이터를 쓸 시작 주소(h00과 시작 주소로부터 Writing할 사이즈(h08) 그리고 실제 Writing할 데이터[DATA]로 구성됨

– 2번 채널로 Writing할 경우의 CMD는 h91이며 하위비트(h1)는 채널을 의미함

[HOST ← READER] 정상적으로 태그에 데이터를 쓴 경우

h06[ACK] h01[RID] h90[CMD] h03

3.5 기타

■ Make Check Sum

체크섬(CS)은 CS필드를 제외한 나머지 모든 패킷의 값을 더한 값을 의미한다.

예를 들면 리더로 보내는 패킷이 아래와 같다면

h05[ENQ] h01[RID] h08[CMD] h1B[DATA] h01[LEN]

모든 패킷을 더하여 CS값을 구한 후(hA1) 두개의 ASCII로 변환한다.

(h05 + h01 + h08 + h0B + h01 = hA1)

CS값을 추가한 최종 완성 패킷은 아래와 같다.

h05[ENQ] h01[RID] h08[CMD] h0B[DATA] h01[LEN] h1A[CS]

3.6 교신 에러 코드

표 3은 읽기/쓰기 교신중 발생할 수 있는 에러코드 리스트이다.

Error Code	Error Contents
0x00	No Error
0x01	Unknown Command ID
0x02	Not Yet Implemented Command ID
0x03	Invalid Destination Address(Device ID)
0x04	Invalid System Register Address
0x05	Timeout Error
0x06	Invalid SLRC Register Address
0x07	Out of System Register Address Range
0x08	Out of SLRC Register Address Range
0x09	Out of RF Channel Number
0x0A	Out of Bit Range
0x0B	Invalid Bit Value
0x0C	Check Sum Error
0x0D	Write Command Fail
0x0E	Read Command Fail
0x0F	Long Data Length (max 32 bytes)
0x10	RF Channel Disabled
0x11	SLRC Reset Error
0x12	SLRC Parallel Bus Error
0x13	Max Timeslot Error(max 255)
0x14	Not Supported RF Protocol
0x15	ICODE Wrong Command Parameter
0x16	ICODE Timeout, ICODE No Tag
0x17	ICODE No Tag
0x18	ICODE CRC Error
0x19	ICODE Collision Error
0x1A	ICODE SNR Error
0x1B	ICODE Count Error
0x1C	RFU
0x1D	ICODE Invalid Quit Value

0x1E	ICODE Weak Collision Error
0x1F	ICODE Write Fail
0x20	ICODE Halt Fail
0x21	ICODE Not implemented Error
0x22	RFU
0x23	RFU
0x24	RFU
0x25	RFU
0x26	RFU
0x27	Family Code Mismatch
0x28	Application Code Mismatch
0x29	ICODE Framing Error
0x2A	Carrier Disabled
0xA1	Write 동작 중 Write or Read 명령 수신 시
0xA2	Read 동작 중 Write or Read 명령 수신 시
0xA3	Write Data의 개수가 112 Byte를 초과하는 경우
0xA4	Length와 Data의 개수가 틀린 경우

표 3 에러코드 리스트

* 회색으로 되어있는 error code의 발생이유는 TAG는 있는데, Field를 통해 보낸 명령이나 혹은 받은 data가 불안정한 경우이다. 안테나 주위에 TAG가 하나 이상 존재하는지 확인 해 보거나, 다시 명령을 시도해 본다.

4 Reader기의 환경 설정 Register

Reader기는 내부 Register에 Reader기의 동작의 설정상태를 저장하고 있다. Register는 EEPROM에 저장되어 있으므로, Reader기에 전원을 공급하지 않아도 설정 상태가 지워지지 않는다. 표4는 Register의 구조이다.

Register Address	Default Value	Name	용도
03H	0x03	ERFCH	RF Channel을enable/disable
0AH	0x00	CFG0	System configuration register 0
0BH	0x86	CFG1	System configuration register 1
18H	0x00	CMD0	Command 0 register0
1BH	0x0F	RTB	Continuous mode시 Read Tag byte size
1CH	0x11	RTA	Continuous mode시 Read tag address
1DH	0x1E	VTO	Verbose mode read시 timeout 값으로 100ms단위로 셋팅. 디폴트는 3초(1E)

표4 System Register

4.1 Registry 세부 설명

4.1.1 ERFCH

ERFCH(03H R/W)							
D7	D6	D5	D4	D3	D2	D1	D0
–	–	–	CH5	CH4	CH3	CH2	CH1

CH1~CH5 : ENABLE RF CHANNEL

4.1.2 CFG1

CFG1(0BH R/W)							
D7	D6	D5	D4	D3	D2	D1	D0
EBZ	CAP	–	TRC	–	–	VRM	–

EBZ : ENABLE BUZZER

1: ENABLE, 0: DISABLE

ENABLE 시에는 TAG정보가 있을때만 부저의 작동을 말함

CAP : Ceyon Access Protocol

1 : CAP1.3S Protocol(PLL연동을 위한 바이너리 패킷 통신)

0 : CAP1.3 Protocol(ASKII 통신)

TRC: Tag Read in Continuous mode

1 : Reading Tag User Memory

0 : Reading Tag UID

VRM : Enable Verbose Mode

1 : ENABLE VERBOSE MODE, 0: DISABLE VERBOSE MODE(Continuous Mode)

4.1.3 CMD0

CMD0(18H R/W)							
D7	D6	D5	D4	D3	D2	D1	D0
-	SFD	CSE	-	-	-	-	-

SFD : Set Factory Default

공장초기화(Factory Default) 상태로 복구

CSE : COMMAND SAVE EEPROM

현재의 최종 레지스터 값을 저장함으로써 리더가 리셋 되더라도 레지스터 값을 유지함
상기의 비트는 실행후 지워짐

4.1.4 RTB

RTB(1BH R/W)							
D7	D6	D5	D4	D3	D2	D1	D0

READ TAG BYTE

Continuous Mode를 사용할 때 유효하며 새로운 TAG EVENT가 있을 때 RTA에서 부터 RTB에 설정된 바이트 만큼 전송한다.

4.1.5 RTA

RTA(1CH R/W)							
D7	D6	D5	D4	D3	D2	D1	D0

READ TAG ADDRESS

Continuous Mode를 사용할 때 유효하며 새로운 TAG EVENT가 있을 때 전송할 TAG의 시작 ADDRESS를 설정한다.

4.1.6 VTO

VTO (1DH R/W)							
D7	D6	D5	D4	D3	D2	D1	D0

VTO(Verbose mode Time Out)

Verbose mode일 때 Reading Time out을 설정한다.

단위는100ms이며 VTO값을 1E로 설정하였다면 Time out은 3초가 되며 3초가 넘어서도 Tag ID가 검출되지 않으면 Time out 에러가 발생한다.

5 Appendix (ASCII 테이블)

HN LN	0	1	2	3	4	5	6	7
0	NUL	DLE	Space	0	@	P	'	p
1	SOH	DC1	!	1	A	Q	a	q
2	STX	DC2	"	2	B	R	b	r
3	ETX	DC3	#	3	C	S	c	s
4	EOT	DC4	\$	4	D	T	d	t
5	ENQ	NAK	%	5	E	U	e	u
6	ACK	SYN	&	6	F	V	f	v
7	BEL	ETB	'	7	G	W	g	w
8	BS	CAN	(8	H	X	h	x
9	HT	EM)	9	I	Y	i	y
A	LF	SUB	*	:	J	Z	j	z
B	VT	ESC	+	;	K	[k	{
C	FF	FS	,	<	L	₩	l	
D	CR	GS	-	=	M	}	m]
E	SO	RS	.	>	N	^	n	~
F	SI	US	/	?	O	_	o	DEL

표 5 ASCII 코드표

6 Appendix (UID Format)

The VICCs are uniquely identified by a 64 bits unique identifier (UID). This is used for addressing each VICC uniquely and individually, during the anticollision loop and for one-to-one exchange between a VCD and a VICC.

The UID shall be set permanently by the IC manufacturer in accordance with figure 1.

MSB				LSB			
64	57	56	49	48			1
'E0'		IC Mfg code		IC manufacturer serial number			

Figure 1 — UID format

The UID comprises

- The 8 MSB bits shall be 0xE0,
- The IC manufacturer code, on 8 bits according to ISO/IEC 7816-6/AM1,
- A unique serial number on 48 bits assigned by the IC manufacturer.