암호화 리더기 인터페이스 스펙

(KSNET)

Confidential

KSNET 단말기운영팀

문서 변경 이력

날짜	내 용	Version
2014.07.10	최초 문서 작성	V 0.1

Confidential

1 개요

문 본서는 암호화 리더기 와 POS(PC 포함)사이의 DATA 통신을 위한 인터페이스 규격이다.

2 적용범위

1. 본 규격은 암호화 리더기의 상태 정보 확인 및 상태 정보 변경 시 적용할 수 있다.
2. 본 규격은 암호화 리더기내부의 키 삭제 및 주입에 적용할 수 있다.
3. 본 규격은 암호화 리더기 펌웨어 업데이트 시 적용할 수 있다.

3 소프트웨어 인터페이스

3.1 통신방식

115,200 bps, No Parity, 8 bit Data, 1 stop bit

38,400 bps, No Parity, 8 bit Data, 1 stop bit

3.2 기본적인 전문 포맷

STX	Length	Command ID	Data Value	ETX	LRC
(1)	(2)	(1)	(n)	(1)	(1)

- STX : Start of Text (0x02)
- Length : Command ID 부터 ETX 까지의 바이트수
  예) 400 바이트 = 0x0190 (0x01 0x90)
- Command ID: 참고 1 참조
- Data Value : 전송할 데이터
- ETX : End of Text (0x03)
- LRC : Longitudinal Redundancy Check / STX 다음부터 ETX 까지의 XOR 값

3.3 COMMAND ID

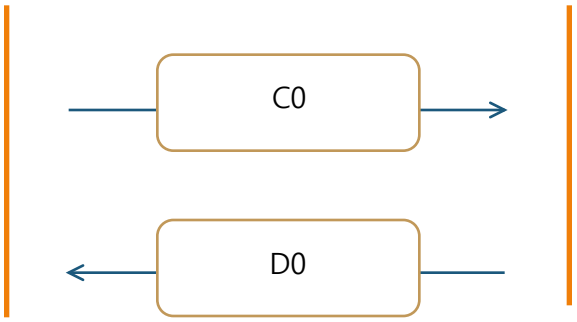
<참고 1> Command ID

내용	주체	Command ID	내용	주체	Command ID
상태정보 요청	PC	0xC0	상태 정보 응답	리더	0xD0
암호화 키 삭제 요청	PC	0xCA	암호화 키 삭제 응답	리더	0xDA
암호화 키 주입 요청	PC	0xCB	암호화 키 주입 결과 응답	리더	0xDB

4 통신절차

4-1 . POS 와 리더기 사이는 한번의 요청에 한번의 응답을 원칙으로 한다.

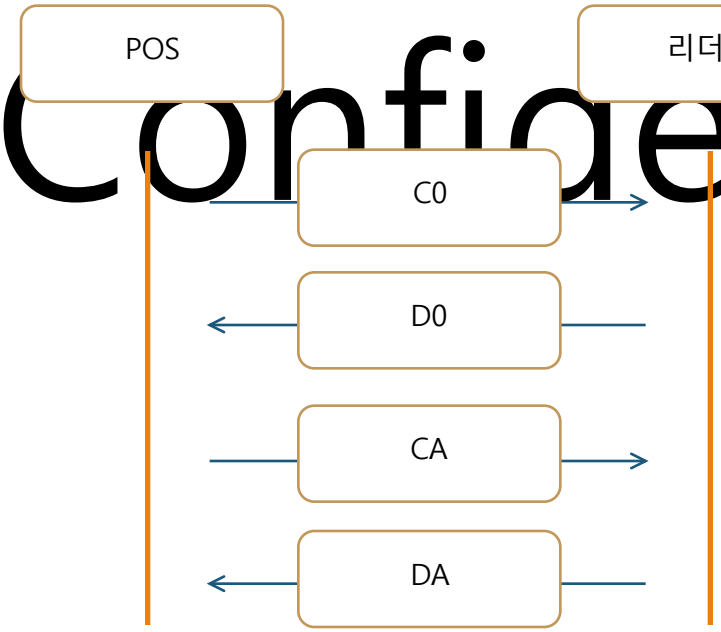
요청과 응답 사이의 타임 아웃은 1 초로 한다.



(리더기 상태 정보 요청 및 응답 전문은 연결 상태 확인 용으로 수시 사용 가능)

4-2. 필요에 의해서 두 가지 요청 및 응답을 순서대로 진행할 수 있다.

단, POS 는 원칙적으로 첫 번째 요청의 응답이 없으면 두 번째 요청을 수행하지 않는다.



5 COMMAND ID 와 해당 전문포맷 설명

5.1 리더기 상태정보요청 (POS 와 리더기의 연결상태를 확인하는 용도로 사용 가능)

<STX><Length><0xC0><ETX><LRC>

5.1-1 리더기 상태정보 응답전문

<STX><Length><0xD0><Data><ETX><LRC>

항목		길이	속성	내용
STX		1	Bin	0x02
Length		2	Bin	Command ID 부터 ETX 까지의 길이
Command ID		1	Bin	0xD0
DATA	**랜덤키**	**16**	**Char**	**단말기에서 생성한 랜덤키 (Well512 알고리즘)**
	제품시리얼번호	13	Char	KSR01YYMMXXXX 초기값 " all "0"
	S/W 버전	3	Char	100 (1.00 ~ 시작)
	암호화 키 존재 유무	1	Char	O : 키 정상 , X : 키 없음
	통신 속도	3	Char	"384" (통신속도 기본값은 38400 bps)
	KEY Data 갱신일자	6	Char	YYMMDD "000000"
	EMV Data 갱신일자	6	Char	YYMMDD "000000"
ETX		1	Bin	0x03
LRC		1	Bin	Length ~ ETX 까지 XOR 한 값

오류 시 <STX><Length><0xD0><에러코드><ETX><LRC>

리더기는 상태정보 응답과 동시에 초기상태로 대기

POS 는 연결상태를 확인하는 용도로 사용함.

5.2 리더기 키 삭제 요청

<STX><Length><0xCA><DATA ><ETX><LRC>

항목	길이	속성	내용
STX	1	Bin	0x02
Length	2	Bin	Command ID 부터 ETX 까지의 길이
Command ID	1	Bin	0xCA

DATA	KEY 제거	3	Char	"DEL"
ETX		1	Bin	0x03
LRC		1	Bin	Length ~ ETX 까지 XOR 한 값

5.3-1 리더기 삭제 상태 응답

<STX><Length><0xDA><Data><ETX><LRC>

항목		길이	속성	내용
STX		1	Bin	0x02
Length		2	Bin	Command ID 부터 ETX 까지의 길이
Command ID		1	Bin	0xDA
DATA	응답 코드 또는 에러코드	2	Char	성공 "00" , 실패 시 에러코드 : 01 ~ 99
ETX		1	Bin	0x03
LRC		1	Bin	Length ~ ETX 까지 XOR 한 값

5.4 리더기 키 주입 요청 전문

<STX><Length><0xCB><Data><ETX><LRC>

항목	길이	속성	내용
STX	1	Bin	0x02
Length	2	Bin	Command ID 부터 ETX 까지의 길이
Command ID	1	Bin	0xCB

DATA	IPEK + KSN	848	Bin	암호화 된 데이터
	해쉬값	32	Bin	M-Key 의 해쉬 값 (SHA256)
	암호화된 M-Key	24	Bin	M-Key 를 리더기의 랜덤키로 HIGHT 암호화 함.
	현재 시간	12	Char	YYMMDDhhmmss
ETX		1	Bin	0x03
LRC		1	Bin	Length ~ ETX 까지 XOR 한 값

- M-Key = 암호화된 IPEK 를 복호화 하는데 사용하는 암호키이다.
  - 키주입툴: 단말기로부터 받은 랜덤키를 가지고 M-Key 를 HIGHT 암호화 함
  - 단말기: 암호화된 M-Key 를 랜덤키를 사용하여 복호화 한다.

5.4-1 리더기 키 주입 결과 응답 전문

<STX><Length><0xDB><Data><ETX><LRC>

항목		길이	속성	내용
STX		1	Bin	0x02
Length		2	Bin	Command ID 부터 ETX 까지의 길이
Command ID		1	Bin	0xDB
DATA	응답 코드 또는 에러코드	2	Char	응답 : 00 , 실패 시 에러코드 : 01 ~ 99
ETX		1	Bin	0x03
LRC		1	Bin	Length ~ ETX 까지 XOR 한 값