국토해양부 고시 제2010-180호

교통카드 관련 장비의 전국호환성 인증요령을 다음과 같이 제정하여 고시합니다.

2010년 4월 6일

국토해양부장관

교통카드 관련 장비의 전국호환성 인증 요령

제1조(목적) 이 요령은 국토해양부장관이 교통카드·단말기 등 관련 장비(이하 "교통카드 관련 장비"라 한다)의 전국호환성을 확보하기 위하여, 「대중교통의 육성 및 이용 촉진에 관한 법률」(이하 "법률"이라 한다) 제10조의7에 따라 인증업무를 수행하는 데 필요한 세부사항을 정함을 목적으로 한다.

제2조(정의) 이 요령에서 사용하는 용어의 정의는 다음과 같다.

1. "교통카드"란 교통서비스 이용대가를 전자적으로 지불·결제하는데 사용되는 카드나 그 밖의 매체를 의미한다.

2. "지불보안응용모듈(SAM)"이란 소형 인증서버 역할을 수행하는 칩으로서, 지불단말기에 장착되어 암호 알고리즘 및 인증 알고리즘을 활용하여 지불거래 발생 시마다 교통카드의 데이터를 처리하는 장치를 말한다.

3. 지불단말기 : 교통카드의 인식 및 교통요금의 결제를 수행하는 장치를 말한다.

4. "전국호환성"이란 교통카드 관련 장비가 전국의 대중교통수단·시설에서 결제 및 정산 수단으로 기능할 수 있는 것을 말한다.

5. "전국호환성 인증"이란 교통카드 관련 장비가 전국호환성 인증기준을 준수한 장비임을 확인하는 행위를 말한다.

6. "적합성시험"이란 교통카드 관련 장비가 전국호환성 인증기준을 준수하였는지 여부를 검증하는 시험을 말한다.

7. "동일모델"이란 장비별로 다음 각 목에 해당하는 경우를 말한다.

가. 교통카드 : 크기나 외관 또는 형태(폐쇄형 또는 개방형)에 관계없이 동일 칩 및 동일 운영체계버전에 동일한 교통카드 프로토콜을 탑재한 제품

나. 지불보안응용모듈 : 크기나 외관 또는 형태(폐쇄형 또는 개방형)에 관계없이 동일 칩 및 동일 운영체계버전에 동일한 지불보안응용모듈 프로토콜을 탑재한 제품

다. 지불단말기 : 크기나 외관에 관계 없이 동일한 지불단말기 프로토콜을 탑재한 제품

8. "인증대행기관"이란 전국호환성 인증 업무의 효율적 추진을 위하여 법률 제10조의7제2항에 따라 국토해양부장관이 행하는 인증업무를 대행하도록 지정받은 기관이나 단체를 말한다.

제3조(인증대상) ①이 요령이 정하는 전국호환성 인증을 받아야 하는 교통

카드 관련 장비는 다음 각 호와 같다.

1. 교통카드

2. 지불보안응용모듈

3. 지불단말기

②전국호환성 인증은 제1항 각 호 장비의 동일모델별로 받아야 하며, 외관 및 구조·기능 등이 유사한 장비라도 동일모델에 해당하지 않는 경우에는 별도의 전국호환성 인증을 받아야 한다.

③국토해양부장관이 법률 제10조의5 및 제10조의7 규정에 따른 전국호환성 확보를 위하여 필요하다고 인정하는 경우에는 인증대상을 확대할 수 있다.

제4조(인증기준) 제3조제1항의 인증대상 장비에 대한 전국호환성 인증기준(이하 “인증기준”이라 한다)은 별표1과 같다.

제5조(인증대행기관의 요건) ①「대중교통의 육성 및 이용 촉진에 관한 법률 시행령」제11조의4제1호에 따라 인증대행기관이 갖추어야 하는 인력의 기준은 다음 각 호와 같다.

1. 책임자 : 교통·정보통신 등 관련 분야의 특급기술자(다음 각 목 중 어느 하나의 경우를 말한다)로서, 시스템보안·통제·시험인증 등 관련 분야의 경력이 4년 이상인 자

가. 기술자격기준 : 기사 자격 소지 후 경력 10년 이상(이하 동일 기준), 산업기사 13년 이상

나. 학력경험기준 : 박사 학위 소지 후 경력 3년 이상(이하 동일 기

준), 석사 9년 이상, 학사 12년 이상

2. 실무자(2인 이상) : 교통·정보통신 등 관련 분야의 중급기술자(다음 각 목 중 어느 하나의 경우를 말한다)로서, 시스템보안·통제·시험인증 등 관련 분야의 경력이 2년 이상인 자

가. 기술자격기준 : 기사 자격 소지 후 경력 4년 이상(이하 동일 기준), 산업기사 7년 이상

나. 학력경험기준 : 석사 학위 소지 후 경력 3년 이상(이하 동일 기준), 학사 6년 이상

②「대중교통의 육성 및 이용 촉진에 관한 법률 시행령」제11조의4제2호에 따라 인증대행기관이 갖추어야 하는 적합성시험 장비의 기준은 별표2와 같다.

제6조(인증대행기관의 지정) ①인증대행기관으로 지정받으려는 자는 별지 제1호 서식에 따른 신청서에 다음 각 호의 서류를 첨부하여 국토해양부장관에게 신청하여야 한다.

1. 법인등기부 등본(신청인이 법인 또는 법인의 부설기관인 경우에 한정한다)

2. 제5조에 따른 인력 및 장비 확보를 증명하는 서류

3. 인증업무 수행계획서(인증업무의 효율적 추진 및 공정성·보안성 확보 방안을 포함해야 한다)

4. 인증대행기관 운영에 관한 업무규정

②국토해양부장관이 제1항에 따라 인증대행기관 지정 신청을 받은 경우

에는 인력 및 장비 현황, 사업계획 등을 종합적으로 심사한 후 그 지정 여부를 결정한다.

③국토해양부장관은 인증대행기관 지정 내용을 별도 고시하며, 인증대행기관에 대해서는 별지 제2호 서식에 따른 지정서를 교부한다.

제7조(인증업무처리규정 등) ①인증대행기관은 이 요령의 내용에 따라 전국호환성 인증의 절차를 세부적으로 정한 인증업무처리규정을 제정·공고하여야 한다.

②인증대행기관은 인증대상 장비별 적합성시험의 방법과 절차를 세부적으로 정한 적합성시험규정을 제정·공고하여야 한다.

③인증대행기관이 인증업무처리규정 및 적합성시험규정을 제·개정하는 경우에는 국토해양부장관의 승인을 얻어야 한다.

④인증대행기관은 교통카드 전국호환에 필요한 기술적 사항에 대한 추가 규정 등을 국토해양부장관의 승인을 얻어 제정·공고할 수 있다.

제8조(인증대행기관의 비밀보호 의무) ①인증대행기관은 인증 및 적합성시험 업무 과정에서 알게 된 영업상 비밀에 해당하는 정보를 공개하거나 업무수행 목적 외에 이용할 수 없다.

②인증대행기관은 인증 및 적합성시험 업무의 보안대책을 수립하여 국토해양부장관에게 보고하고 이를 실행하여야 한다.

제9조(인증대행기관에 대한 관리) ①국토해양부장관이 인증업무의 적정성을 확보하기 위해 필요하다고 인정하는 경우에는 인증대행기관에 대한 지도·감독을 실시할 수 있다.

②인증대행기관은 인증업무와 관련된 문서 및 자료를 비치·보존하여야 한다.

③인증대행기관은 명칭, 소재지, 책임자 등 인증업무에 중대한 영향을 미치는 사항의 변경이 있는 경우에는 즉시 국토해양부장관에게 그 사실을 통지하고 변경내용을 증명하는 서류를 제출하여야 한다.

제10조(인증대행기관 지정의 취소) 다음 각 호의 어느 하나에 해당하는 사유가 있는 경우에는 국토해양부장관이 인증대행기관 지정을 취소할 수 있다.

1. 거짓·부정한 방법으로 지정을 받은 경우
2. 제5조의 인증대행기관 요건에 적합하지 아니하게 된 경우
3. 인증의 기준 및 절차 등 이 요령의 중요내용을 위반한 경우
4. 정당한 사유 없이 인증업무를 중지하거나 인증을 거부한 경우

제11조(인증업무자문위원회) ①국토해양부장관은 인증업무의 공정성 및 전문성을 기하기 위하여 인증업무자문위원회(이하 “자문위원회”라 한다)를 구성하여 다음 각 호의 사항에 대한 자문을 의뢰할 수 있다.

1. 제6조에 따른 인증대행기관 지정 여부의 심사
2. 제7조에 따른 인증업무처리규정 및 적합성시험규정의 승인
3. 제9조에 따른 인증대행기관에 대한 관리
4. 제10조에 따른 인증대행기관 지정의 취소
5. 제15조에 따른 인증여부 판정에 대한 이의신청 심사
6. 제17조에 따른 인증 취소여부 심사

7. 기타 인증업무의 공정성 및 전문성을 확보하기 위해 국토해양부장관이 필요하다고 인정하는 사항

②자문위원회는 국토해양부장관이 위원으로 위촉하는 5인 이상의 교통카드 관련 전문가로 구성하며, 위원장은 국토해양부장관이 위원 중에서 지명한다.

③자문위원회 위원장이 제1항에 따라 자문하기 위하여 필요하다고 인정하는 경우에는 인증대행기관 또는 그 지정 신청자에 대하여 자료제출을 요구하거나 현장실사를 실시할 수 있다.

제12조(인증의 신청) ①대중교통운영자, 교통카드사업자 등 이 요령에 따라 전국호환성 인증을 받고자 하는 자(이하 “인증신청자”라 한다)는 인증대행기관에 인증을 신청하여야 한다.

②인증신청자는 별지 제3호 서식에 따른 신청서와 인증업무처리규정이 정하는 구비서류 및 자료를 인증대행기관에 제출하여야 한다.

제13조(인증수수료) 인증신청자가 인증을 신청하는 경우에는 국토해양부장관이 별도로 고시하는 인증수수료를 인증대행기관에 납부하여야 한다.

제14조(인증의 절차 등) ①인증대행기관은 다음 각 호의 절차에 따라 전국호환성 인증업무를 수행한다.

1. 인증 신청의 접수
2. 적합성시험 및 시험결과의 판정
3. 인증 결과의 통보
4. 인증서 교부

②인증대행기관은 적합성시험 결과에 따라 전국호환성 인증여부를 판정하며, 대상 장비가 인증에 적합하다고 인정하는 경우에는 인증신청자에게 국토해양부장관이 발행하는 별지 제4호 서식에 따른 전국호환성 인증서를 교부한다.

제15조(이의신청) ①제14조에 따른 인증여부 판정에 대하여 이의가 있는 인증신청자는 인증대행기관에 재심사를 신청할 수 있다.

②인증신청자가 재심사를 신청한 경우에는 인증수수료를 인증대행기관에 납부하여야 한다. 단, 이의신청 대상이 된 인증여부 판정에 대하여 인증대행기관에 과실이 있는 경우에는 재심사에 대한 인증수수료를 감면한다.

③인증여부 판정에 대해 분쟁이 있는 경우에 인증대행기관의 장은 그 판정의 당부에 대해 자문위원회에 자문을 의뢰할 수 있다.

제16조(인증의 유효기간) 전국호환성 인증의 유효기간은 인증서를 교부한 날로부터 3년으로 하며 유효기간 경과 후에는 동일모델이라도 다시 인증을 받아야 한다.

제17조(인증에 대한 사후관리) ①국토해양부장관은 다음 각 호의 하나에 해당하는 사유가 있는 경우에는 인증대행기관의 요청 또는 자문위원회의 자문을 받아 전국호환성 인증을 취소할 수 있다.

1. 인증의 근거나 전제가 되는 주요한 내용이 변경된 경우
2. 인증 신청 시 제공된 중요 자료가 거짓으로 판명된 경우
3. 인증 받은 장비와 동일모델이라 할 수 없는 장비를 전국호환성 인증

을 받은 장비로 제작·공급·설치한 사실이 있는 경우

4. 정당한 이유 없이 제2항에 따른 자료제출 요구를 계속하여 거부하는 경우

②인증대행기관은 제17조제1항제1호 내지 제3호에 해당하는 사실이 있는지 확인하기 위하여 인증신청자에게 필요한 자료의 제출 등을 요구할 수 있다.

③제1항에 따라 전국호환성 인증이 취소된 경우 인증신청자는 제14조제2항에 따른 인증서를 인증대행기관에 즉시 반납하여야 하며 인증에 관련된 용어 및 명칭 등의 사용을 중지하여야 한다.

부 칙

이 요령은 고시한 날로부터 시행한다.

[별표 1] 인증대상별 전국호환성 인증기준

제1장 교통카드 전국호환성 인증기준

제 1부 : 기본 구조

1. 적용범위 KS X 6924-1에 따른다.
2. 인용표준 KS X 6924-1에 따른다.
3. 용어와 정의 KS X 6924-1에 따른다.
4. 기호 및 약어 KS X 6924-1에 따른다.

5. 교통카드의 기능
5.1. 환경 조건 KS X 6924-1에 따른다.
5.2. 교통카드의 최소 요구 사항 KS X 6924-1에 따른다.

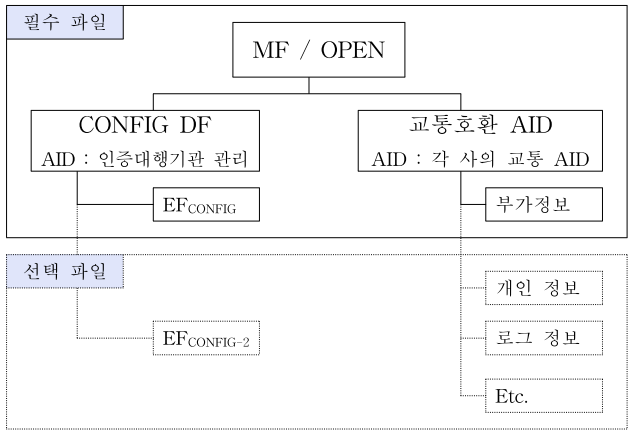
6. 특성
6.1 통신 방식 KS X ISO/IEC 14443-2에 따른다.
6.2 통신 거리 KS X ISO/IEC 14443-2에 따른다.
6.3 충돌 방지 KS X ISO/IEC 14443-3에 따른다.

7. 데이터
7.1 데이터 종류 KS X 6924-1에 따른다.
7.2 ID_{SAM} KS X 6924-1에 따른다.
7.3 NT_{SAM} KS X 6924-1에 따른다.
7.4 M_{PDA} KS X 6924-1에 따른다.
7.5 M_{MAX} KS X 6924-1에 따른다.
7.6 NT_{EP} KS X 6924-1에 따른다.
7.7 ID_{EP} KS X 6924-1에 따른다.
7.8 ID_{CENTER} KS X 6924-1에 따른다.
7.9 ALG_{EP} KS X 6924-1에 따른다.
7.10 VK_{DP_KEY} KS X 6924-1에 따른다.
7.11 BAL_{EP} KS X 6924-1에 따른다.

8. 파일 요구 사항

"교통카드"에서는 각사와의 호환사용을 위하여 다음 파일요구사항을 만족하여야 한다.

카드내의 파일에는 전용파일(DF) 및 요소파일(EF)이 있으며, 다음과 같은 디렉토리 구조의 계층구조(Tree Structure)를 가진다.



'선택파일'은 KS X 6924에서 정의된 명령어 및 거래에 필요한 파일이며, 이는 각 전자화폐사의 고유 규격에 따른다.

8.1 MF(Master File) 또는 OPEN

폐쇄형 카드에서는 Root Directory에 해당하는 Master File(이하 MF)이 최상위에 존재하며 개방형에서는 Open Platform Environment (이하 OPEN)이 최상위에 위치한다.

8.2 CONFIG DF

"교통카드"에서는 각 사와의 호환사용을 위하여 존재하는 ADF이며 "교통 카드"의 교통 호환 ADF의 정보를 저장하고 있다. 교통 호환 ADF의 정보를 외부에 제공하는 역할을 하며 최초의 거래시 필수적으로 CONFIG DF를 선택하여야 한다.

CONFIG DF의 AID는 아래와 같다.

AID	인증대행기관 관리

ConfigDF 아래에는 EF_{CONFIG}와 $EF_{CONFIG2}$가 있으며 EF_{CONFIG}는 교통 호환 정보를 저장하고 있으며 $EF_{CONFIG2}$는 선택 사항 파일로 하이패스 거래 시 필요한 데이터를 저장하고 있다.

ConfigDF 선택 시 응답으로 EF_{CONFIG}의 내용을 응답하는 경우 아래의 형태를 따른다.

FCI(File Control Information)

파일 구조					Lf			
파일 크기								
레코드 번호	**Tag**			**Length**	**항목**	**Value**	**비고**	**조건**
1	6F				FCI Template			필수

		84			DF Name			필수
		A5			FCI Proprietary Template			필수
			50	2	카드 규격 및 선후불 구분	01 00(선불) 11 00(후불)		필수
			47	2	지원 항목			필수
			43	1	ID_{CENTER}			필수
			11	5	잔액 조회 명령(선불 필수)			선택
			4F	5~16	교통 호환 ADF AID			필수
			9F10	3*N	부가 Data File 정보			필수
			45	1	카드 소지자(카드타입) 정보			필수
			5F24	2	유효기간			필수
			12	8	카드일련번호(후불 필수)			선택
			13	8	카드관리번호			선택
			BF0C	Var	FCI Issuer Discretionary Data			선택

8.3 EF_{CONFIG}

CONFIG DF 하위에 존재하며 실제 교통 호환용 Application 에 대한 정보를 저장하고 있다. Read Record 명령으로 파일 내용의 정보가 조회 가능하다.

EF_{CONFIG}를 통하여 얻을 수 있는 정보는 아래와 같다.

- 카드가 지원하는 "호환 카드"규격 버전
- "호환 카드" 규격 중 카드가 지원하는 항목
- 교통 호환 ADF의 AID
- 교통 호환 ADF에서의 존재하는 부가정보 파일의 정보
- 카드 소지자에 대한 정보
- 각 교통 호환 카드 사업자의 임의의 정보
- 카드 유효기간
- 잔액 조회 명령 (선택 사항)

EF_{CONFIG} 파일은 1개이상의 레코드로 구성되어 있으며 1번 레코드는 필수 항목이며 교통 호환을 위한 정보를 저장하고 있다. 2번 이하의 레코드는 선택 사항으로 발급사가 임의의 데이터를 저장할 수 있다. DF Select시 FCI로 조회하는 방법과 하위 EF파일을 조회하는 방법이 있다. FCI응답으로 EF_{CONFIG} 파일의 1번 레코드의 데이터를 포함하는 경우 FCI Proprietary Template Tag인 'A5' Tag에 포함 되어야한다.

파일 구조				Lf 또는 Lv		
파일 크기				Var.		
SFI				01		
읽기 권한				Free		
쓰기 권한				(주)		
레코드 번호	**Tag**	**Length**	**항 목**	**Value**	**비고**	**조건**

1	87			Config Data Template		교통호환 정보	필수
		50	2	카드 규격 및 선후불 구분	01 00(선불) 11 00(후불)		필수
		47	2	지원 항목			필수
		43	1	ID_{CENTER}			필수
		11	5	잔액 조회 명령(선불 필수)			선택
		4F	5~16	교통 호환 ADF AID			필수
		9F10	3*N	부가 정보 파일			필수
		45	1	카드 소지자(카드타입) 정보			필수
		5F24	2	유효기간			필수
		12	8	카드일련번호(후불 필수)			선택
		13	8	카드관리번호			선택
		BF0C	Var	카드 사업자 임의의 정보			선택

8.3.1 EF_{CONFIG} 구성

(주) 이 파일의 쓰기 권한은 각 교통 호환 사업자가 결정하며 16바이트 이상의 키에 의해서 보호 되거나 금지 되어 있어야 한다.

카드는 위의 정보의 항목을 상기의 순서로 저장한다.

EF_{CONFIG}의 정보는 CONFIG DF 선택시 FCI로 응답 할 수 있다.

8.3.2 교통호환 정보

교통호환 정보는 EF_{CONFIG} 파일의 1번 레코드에 저장 되며 필수 항목이다. 교통 호환을 위한 데이터를 저장하고 있다.

- 카드 규격 및 선후불 구분

카드가 지원하는 호환 카드의 규격의 버전 및 선후불 구분 코드를 저장한다. 최상위 4비트는 선불 및 후불 구분 코드로 사용되며 0의 경우 선불, 1의 경우 후불 카드를 나타낸다. 상위 바이트의 하위 4비트로 메이져 버전을 하위 바이트로 마이너 버전을 표시한다. 현재의 규격이 1.0이므로 선불카드의 경우 01 00의 값을 갖고 후불카드의 경우 11 00의 값을 갖는다.

- 지원 항목

카드가 규격의 일부만을 지원하는 경우 이를 표시하는 영역이다.

비트	사업자
b0	ISO 14443-3의 준수
b1	ISO 14443-4의 준수
b2	CONFIG DF의 준수
b3	Hipass의 지원 여부

b4 ~ b15	예비 영역

각 항목을 지원하는 경우 각 비트에 '1'의 값을 지원하지 않는 경우에는 '0'의 값을 설정한다.

- ID_{CENTER}

ID_{CENTER}는 한국전자지불산업협회에서 지정한 교통 사업자의 고유 번호이다. 교통호환 사업자는 고유의 ID_{CENTER}값을 가지고 있으며 이를 표시하는 영역이다. 자세한 사항은 한국전자지불산업협회(http://kepia.org/) 또는 ID_{CENTER} 관리기관의 전자화폐 고유 식별번호를 참조한다.

ID_{CENTER}	사업자
0x00	Reserved
0x01	금융결제원
0x02	에이캐시
0x03	마이비
0x04	Reserved
0x05	브이캐시
0x06	몬덱스코리아
0x07	한국도로공사
0x08	한국스마트카드
0x09	코레일네트웍스
0x0A	Reserved
0x0B	이비
0x0C	서울특별시버스운송사업조합
0x0D	카드넷

2009년 11월 한국전자지불산업협회에 등록된 전자화폐 고유 식별번호

- 잔액 조회 명령

단말기에서 카드의 잔액을 조회하기 위해 사용할 명령이다. 잔액 조회 명령에 표시 될수 있는 명령은 Case 2 명령으로 제한한다. 잔액 조회의 명령에 서명값 등 상수로 표현이 불가능한 경우에는 표시를 하지 않으며 또한 카드에서 잔액을 조회 할 수 있는 명령이 없는 경우 표시 하지 않는다. 또한 응답의 구조는 4바이트 이하의 16진수 값만이 가능하다.

- 교통 호환 ADF AID

교통 호환 사업자 별 고유의 ADF의 AID이다. 교통 호환 ADF를 선택하기 위해서 사용한다.

- 부가 정보 파일

교통 호환 사업자가 부가 서비스를 하기위하여 기록하는 부가 정보 파일의 정보를 가지고 있다. 부가 정보 파일의 종류, SFI 및 저장 가능한 최대 길이에 관한 정보를 나타낸다. 부가 정보 파일이 레코드 파일의 경우에는 길이에 Tag Length를 포함한 저장 가능한 최대 길이를 표시한다. 이 항목의 구성은 아래와 같다.

Tag	Length	Value

	'03' * N	File Type(3bit) || SFI(5bit) || Max Length(2byte) || [File Type(3bit) || SFI(5bit) || Max Length(2byte)]....

부가 정보 파일은 1개 이상 존재해야 하며, 파일 하나당 3바이트로 표현한다. 또한, 호환카드 규격 상 필요한 최대길이 이상을 포함한 정보 파일이 1개 이상 존재해야 하며 카드 발급 시 처음 기록된 부가 정보 파일에 교통호환정보를 기록한다.

(주)File Type이 Record의 경우 Max Length는 Tag Length를 포함한 저장 가능한 순수 데이터의 길이를 나타낸다.

부가 정보 파일은 아래의 파일 구조 중 하나를 지원해야 한다.

b8 b7 b6	File Type	지원 명령
0 0 0	RFU	-
0 0 1	Transparent	Read Binary
0 1 0	RFU	-
0 1 1	RFU	-
1 0 0	RFU	-
1 0 1	RFU	-
1 1 0	RFU	-
1 1 1	Cyclic Record	Read Record

- 소지자 정보

카드를 소지하고 있는 사람의 정보를 표시하며 자세한 사항은 아래와 같다.

Value	설 명	Value	설 명
01	일 반	11	버 스
02	어 린 이	12	화 물 차
03	청 소 년	13	
04	경 로	14	
05	장 애 인	15	

- 유효기간

카드 유효기간 정보를 표시하며, 형식은 'YYMM'으로 한다.

- 카드일련번호

키 변형시 사용되는 카드번호 데이터 8자리를 기록한다. 거래 초기화시에 나오는 정보와 동일해야 한다.

- 카드관리번호

카드일련번호와 동일할 수도 동일하지 않을 수도 있으며 사업자가 관리하는 카드번호이다.

8.4 $EF_{CONFIG2}$

CONFIG DF 하위에 존재하며 하이패스 거래를 위한 정보를 저장하고 있다. 한국도로공사의 하이플러스 카드이외의 카드가 하이패스 거래가 가능한 경우에만 존재한다. Read Record 명령으로 파일 내용의 정보가 조회 가능하다.

8.4.1 $EF_{CONFIG2}$ 구성

파일 구조				Lf 또는 Lv		
파일 크기				Var.		
SFI				02		
읽기 권한				Free		
쓰기 권한				(주)		
레코드 번호	**Tag**	**Length**	**항 목**	**Value**	**비고**	**조건**
1	70	Var	5.4.2 표 참조		하이패스 정보	선택

'하이패스 정보'는 $EF_{CONFIG2}$ 파일의 1번 레코드에 저장한다.

8.4.2 하이패스 정보

"하이패스 정보" 항목에서 저장되는 데이터의 목록 및 형식은 아래와 같다.

항목		값	형식	길이	비고
Tag		70	Hex	1	하이패스 정보를 나타내는 Tag
Length			Hex	1	Data의 길이
Data	발행기관		BCD	3	키 변형 시 사용되는 카드 번호 데이터 8자리를 기록한다.
	일련번호		Hex	5	
	알고리즘 ID		Hex	1	SEED:00, DES:10
	만기일		BCD	4	카드의 만기일을 기록한다.
	카드정산센터 ID		BCD	1	ID_{CENTER}값을 기록한다.
	카드 서비스 ID		Hex	3	도로공사의 $P_{ER}SAM_{IDSERVICE}$를 통해서 값을 얻는다.
	소지자 지불정보	0100	BCD	2	도로공사 전자 카드 규격에서 정의된 카드소지자 정보파일의 소지자 지불 정보 항목이다. 선불거래로 값을 고정한다.
	카드관리번호		BCD	8	카드관리번호를 저장한다.
	차량번호		Ans.	10	'00'으로 10바이트를 기록한다.

하이패스 거래 시 사용되는 명령어 및 기능 요구 사항은 제3부 하이패스 기능을 참조한다.

8.5 교통 호환 DF(Dedicated File)

교통 호환 카드 Application 으로 Config DF 에 기록된 정보와 일치하여야 한다.

교통호환 ADF	각 사의 교통AID

8.5.1 부가정보파일

이 파일의 목적은 환승정보, 입구정보 등 거래 시 필요한 부가정보를 저장한다. 이 파일은 CONFIG DF에서 정의된 구조와 일치해야한다. 부가정보파일에 대한 조회에 관한 권한은 Free이며 기록에 관한 권한은 거래 프로토콜에서 정의한 절차에 의해서 가능하다. 그 외의 기록 권한은 16바이트의 키 이상의 보안 알고리즘으로 보호되어야 한다. 하지만 거래 프로토콜에 의한 기록 절차 이외에 기록 권한을 금지시킬 것을 권고한다.
각각의 부가 정보는 (레코드 파일의 경우 Tag Length 필드를 포함한) 순수 데이터의 길이가 최소 52바이트까지 저장 가능하여야 하며 레코드 형태의 파일 권고한다.

8.5.2 부가 정보 파일 구조

• Transparent

파일 구조	Transparent File	
접근조건	조회	Free
	기록	지불 거래 시
설 명	-Transparent 파일은 Read Binary 명령으로 조회할 수 있다. -저장은 지불 거래 시에 부가정보 처리로써 가능하며 잔액차감과 부가정보 기록은 일원화되어야 한다. -한 개의 부가정보를 기록 가능하다. -조회 시 Offset 0으로 조회한다	

• Record 파일 구조

파일 구조	Cyclic Record File	
접근조건	조 회	Free
	기 록	지불 거래 시
설 명	-Record파일은 Read Record 명령으로 조회할 수 있다. -저장은 지불 거래 시에 부가정보 처리로써 가능하며 잔액차감과 부가정보 기록은 일원화되어야 한다. -여러 개의 부가정보가 기록 가능하다. -최근의 부가 정보는 1번 레코드에 저장되며 레코드 번호가 증가 함에 따라 더 오래된 부가 정보도 조회 가능하다. -새로운 부가 정보를 기록하여 기존의 부가 정보를 유지 할 수 없는 경우 가장 오래된 정보를 삭제한다.	

8.5.3 부가 정보 파일 데이터 구조

부가 정보 파일의 데이터 구조는 각 교통 사업자가 필요한 정보를 임의로 기록할 수 있다.

8.5.4 부가 정보의 기록

부가 정보 파일이 Transparent 구조의 경우 부가 정보 파일에 기록할 데이터를 거래 명령에 추가 하여 보낸다. 부가 정보 파일이 Record 구조의 경우 부가 정보 파일에 기록할 데이터에 Tag와 Length 필드를 포함하여 거래 명령에 추가 하여 보낸다.
거래 명령에 부가 정보가 포함되는 경우에 APDU의 P2로 부가정보 파일을 지정하여야 한다. 이 때 Application은 P2의 정보가 내부에서 관리하는 부가정보 파일과 일치하는 경우에 부가정보를 기록하다.

• Tag의 구성

부가 정보 파일에 기록할 Tag의 경우 부가 정보 파일의 기록 주체를 확인할 수 있도록 거래 시 아래의 규칙에 따라 Tag를 구성한다. 또한 교통 호환 Application은 부가 정보 파일의 Tag를 값을 확인하거나 조작하지 않는다.

B8	B7	B6	B5	B4	B3	B2	B1	내용
1	1	0	-	-	-	-	-	교통 사업자의 구분

Tag는 B5~B1에 현재 거래를 하는 교통 사업자의 ID_{CENTER}값을 기록한다.
즉 ID_{CENTER}가 '01'의 경우 Tag를 'C1'로, '11'의 경우 Tag를 'D1'로 기록한다.

• Length 및 데이터의 기록

단말기는 카드의 부가 정보 파일 Max Length에 맞추어 카드에 부가 정보를 전송하며 이 때 추가로 기록되는 데이터는 '00'으로 처리한다.

제 2부 : 명령어 및 프로토콜

1. 적용범위 KS X 6924-2를 따른다
2. 인용표준 KS X 6924-2를 따른다
3. 용어와 정의 KS X 6924-2를 따른다
4. 기호 KS X 6924-2를 따른다

5. 명령어

5.1 관리 명령어
5.1.1 Select File KS X 6924-2를 따른다
5.1.2 Read Record KS X 6924-2를 따른다
5.1.3 Get Response KS X 6924-2를 따른다

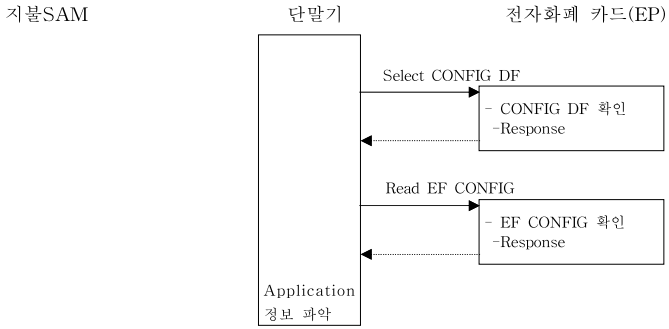
5.2 거래 명령어
5.2.1 Initialize Card(선불/후불) KS X 6924-2를 따른다
5.2.2 Purchase Card(선불/후불) KS X 6924-2를 따른다

6. 프로토콜

6.1 선불카드 거래 프로토콜 KS X 6924-2를 따른다
6.2 선불카드 재거래 프로토콜 KS X 6924-2를 따른다
6.3 선불카드 직전 거래 취소 프로토콜 KS X 6924-2를 따른다
6.4 후불카드 거래 프로토콜 KS X 6924-2를 따른다
6.5 후불카드 직전 거래 취소 프로토콜 KS X 6924-2를 따른다

6.6 Application 정보 조회 프로토콜

표준호환카드의 모든 거래는 거래 전 다음과 같은 프로토콜을 수행하여 Application 정보를 조회한다. 단 Application의 정보를 알고 있는 경우 생략 할 수도 있다.



제 3부 : 하이패스 기능

1. 용어정의

용어	정의
SAM	키를 저장하고 그 키에 연관된 암호연산까지도 수행함으로써 보안부분을 담당하는 논리적·물리적으로 안전한 모듈
전자적 가치	실제적인 화폐를 대신하여 도로공사 선불카드 시스템 내에서 유통되는 가치
PSAM	구매단말기에서 사용되는 SAM
거래유형	거래유형에 대한 구분자로 도로공사 선불카드의 구매거래, 가치저장거래, 취소거래/에러 복구 및 파라미터 갱신 거래 등을 구분

2. 기호, 약어 및 데이터 요소

IEP	Inter-sector Electronic Purse
PAN	Primary Account Number
PDA	Purchase Device Application
PPSAM	Purse Provider SAM
PSAM	Purchase SAM
PTS	Protocol Type Selection
SAM	Secure Application Module
SECP	Security Protocol

[데이터 요소]

ALG_{COMP}	각 구성요소들이 사용하고 있는 알고리즘의 종류
BAL_{COMP}	각 구성요소에 저장된 금액
BAL_{MAX_IEP}	IEP의 최대저장한도금액
BAL_{TEMP}	후불 전자카드용 일시적인 카드잔액
CC_{COMP}	각 구성요소가 전송하는 거래에 대한 완료코드
COMP	도로공사 선불카드 시스템의 구성요소
$DEXP_{COMP}$	각 구성요소들의 만료일
IND	개별구매거래데이터
$KSES_{COMP}$	각 구성요소가 통신시 상호인증을 위해 일시적으로 생성하여 사용하는 암호 키
$KUSES_{COMP}$	파라메터 업데이트시의 세션키
Lf	Record File 종류
Lv	Record File 종류
M_{COMP}	선불카드 거래금액
M_{MAX_IEP}	IEP의 최대출금한도금액
$MTOT_{COMP}$	연속구매거래시의 구매총액
NC	거래수집 일련번호
NI	한 NC내에 존재하는 개별구매거래내역의 개수
NT_{COMP}	거래일련번호
NV	파라미터 갱신을 위해 필요한 새로운 값
PAR	파라미터 ID
PV	파라미터 버전

SN	암호화 키를 이용하여 생성한 서명
TM_{COMP}	총액
TRT	거래유형
VK_{COMP}	암호 키의 버전

3. 파일구조

3.1 고속도로 입구정보 파일

이 파일은 일종의 시스템 Cyclic 파일로서 Read HighPass Info/Read Record 명령으로 조회할 수 있으며 Update HighPass Info 명령으로 저장할 수 있다. 조회는 Free이며, 저장은 구매 키에 의한 Session Key 즉, Initialize IEP 명령 후에 저장된다. 폐쇄식의 경우 입구에서 기록되나 경유지 정보가 필요한 개방식에서도 이용될 수 있다. 이 파일에 저장하기 위해서는 Session Key에 의한 MAC을 생성해야 하는데, 이 MAC 생성은 하이패스(터치패스) SAM에 의해서만 가능하다.

Read Hipass-info 명령에 의해서는 가장 최근에 저장된 입구정보에 대하여 Tag, Length 제외한 값을 읽어온다.

파일 식별자			01		
파일 구조			CR		
접근조건			읽기	Free	
			쓰기	Forbidden	
파일 크기			26byte * N		
항목	크기	Value		비고	조건
날짜	4	YYYYMMDD		BCD	필수
시간	3	HHMMSS		BCD	필수
운영기관	1	운영기관 코드 (한국도로공사 : 0x01)		BCD	필수
영업소 번호	2	1 ~ 9999		BCD	필수
지불유형	0.5	0 : 전자 지불, 1:하이패스		BCD	필수
차선유형	0.5	0 : 개방식 상행, 1 : 개방식 하행 2 : 폐쇄식 입구, 3 : 폐쇄식 출구		BCD	필수
차로번호	1	1 ~ 99		BCD	필수
근무번호	1	1 ~ 99		BCD	필수
처리번호	2	1 ~ 65,535		HEX	필수
원 통행요금	3	1 ~ 16,777,215		HEX	필수
징수금액	3	1 ~ 16,777,215		HEX	필수
차종	1	1 ~ 9		BCD	필수
차량번호	2	0000 ~ 9999 (부정방지용)		BCD	필수

* 고속도로 입구 정보 파일의 레코드 개수의 초기값은 10개로 한다.

3.2 고속도로 요금징수 내역 파일

이 파일은 Read/Update/Append Record 명령으로 조회/저장할 수 있다. 단, 구매 거래 완료 시 구매키(Local #1 Key)에 의한 인증이 된 것으로 간주되므로 별도의 인증 절차 없이 갱신이 가능해야 한다.

파일 식별자				02	
파일 구조				CR	
접근조건				읽기	Free
				쓰기	Local #1 Key
파일 크기				50Bytes × N	
구분	항목	크기	Value	비고	조건
입구	입구 날짜	4	YYYYMMDD	BCD	
	입구 시간	3	HHMMSS	BCD	
	입구 운영기관	1	운영기관 코드 (한국도로공사 : 0x01)	BCD	
	입구 영업소번호	2	1 ~ 9999	BCD	
	입구 차로번호	1	1 ~ 99	BCD	
	입구 근무번호	1	1 ~ 99	BCD	
	입구 처리번호	2	1 ~ 65,535	HEX	
	차종	1	1 ~ 9	BCD	
출구	출구 날짜	4	YYYYMMDD	BCD	
	출구 시간	3	HHMMSS	BCD	
	출구 운영기관	1	운영기관 코드 (한국도로공사 : 0x01)	BCD	
	출구 영업소번호	2	1 ~ 999	BCD	
	출구 차로번호	1	1 ~ 99	BCD	
	출구 근무번호	1	1 ~ 99	BCD	
	출구 처리번호	2	1 ~ 65,535	HEX	
	징수전 잔액	3	1 ~ 16,777,215	HEX	
	징수금액	3	1 ~ 16,777,215	HEX	
	OBU 일련번호	8	1 ~ 9999-9999-9999-9999	BCD	
	입구 OBU 상태	1	0x00 ~ 0xff	HEX	
	입구 카드상태	1	0x00 ~ 0xff	HEX	
	출구 OBU 상태	1	0x00 ~ 0xff	HEX	
	출구 카드 상태	1	0x00 ~ 0xff	HEX	
	예비(선택사용)	1		HEX	

* 미 정의된 Data Format들은 시스템 사업자와의 협의를 거쳐 "도로공사 발급지침서"에 별도 정의한다.

4. 하이패스 전용 명령어

4.1 INITIALIZE IEP

- 하이패스 거래를 하기 전에 거래를 초기화하는 명령이다

4.1.1 Command Message

코 드	내 용
CLA	90
INS	50
P1	01 : PURCHASE IEP거래를 위한 초기화
P2	02 : PURCHASE IEP HIGHPASS (접촉/비접촉 HighPass거래)
Lc	NONE
Data	M_{LDA} 지불거래 금액(4Byte)
Le	23

4.1.2 Response Message

이 름	내 용	길 이
ALG_{IEP}	도로공사 선불카드에서 사용되는 알고리즘	1
VK_{IEP_KDP}	키 버젼	1
NT_{IEP}	도로공사 선불카드 거래일련번호	4

R_{IEP}	도로공사 선불카드에서 생성한 난수	8
PP_{IEP}	도로공사 선불카드 발행자 ID	3
IEP	도로공사 선불카드 ID	5
BAL_{IEP}	도로공사 선불카드잔액	4
ID_{center}	도로공사의 고유식별번호(통합SAM : "01")	1
$ID_{SERVICE}$	카드 서비스 ID	3
S1	도로공사 선불카드에서 계산한 SIGNATURE	4
CKS	Checksum(ALG_{IEP} ~ S1)	1
SW1, SW2	COMPLETION CODE	2

* CKS 계산시 모든 바이트에 대한 Exclusive OR 결과가 사용된다.

4.1.3 에러 코드

코 드	내 용
SW1-SW2	SUCCESS : 90 00/61 XX ERROR 69 84 Key/PIN이 Write되지 않음, 9개 필수 파일이 Block, Key/PIN파일이 Block되어 있음 91 01 BAL_{IEP}의 Check Sum 에러 6A 81 후불 전자카드인 경우, 지원되지 않는 기능

4.2 PURCHASE IEP

- 전자 지갑 내에 가치를 차감하는 명령이다.
- 거래를 위한 초기화가 행해져야 한다.

4.2.1 Command Message

코 드	내 용
CLA	90
INS	54
P1	00 : 첫번째 구매거래 03 : IEP Complete Purchase
P2	P1 = 00 일 때, P2 = 02 : PURCHASE IEP HIGHPASS (접촉/비접촉 HighPass거래) P1 = 03 일 때, P2 = 00 : IEP Complete Purchase
Lc	P1 = 00 , P2 = 02 : 18 P1 = 03 : P2 = 00 : 04
DATA	(주) 참조
Le	P1 = 00, P2 = 02일 때 05 P1 = 03일 때 NONE

주 : PURCHASE IEP 거래시의 Data

P1		이 름	의 미	길 이
	P2			
00	02	PP_{PSAM}	PSAM 발행자	3
		PSAM	PSAM의 ID	8
		NT_{PSAM}	PSAM의 거래 일련 번호	4

		M_{PDA}	거래 금액	4
		S2	PSAM에서 계산한 서명	4
		CKS	Checksum(PP_{PSAM}~S2)	1
03	00	DATE	거래 일자	4

* CKS 계산시 모든 바이트에 대한 Exclusive OR 결과가 사용된다.

4.2.2 Response Message

이 름	내 용	길 이
S3[CKS]	도로공사 선불카드에서 계산한 서명[Checksum]	4[1]
SW1, SW2	COMPLETION CODE	2

* CKS는 S3에 대한 Exclusive OR 결과가 사용된다.

4.2.3 에러 코드

코 드	내 용
SW1-SW2	SUCCESS : 90 00/61 XX ERROR 94 03 거래 금액 잔액 초과($BAL_{IEP} \leq M_{PDA}$) 거래 금액 한도 초과($M_{MAX\_IEP} \leq M_{PDA}$)

4.3 READ HiPass Info

- 고속도로 입구정보파일을 읽기 위한 전용명령이다.
- 입구정보파일 구조가 Cyclic 구조로 변경되었으나 하위규격과의 호환성을 유지하여야 한다.
- 읽어온 데이터는 가장 최근에 기록된 데이터의 Tag, Length를 제외한 값이다.

4.3.1 Command message

코 드	내 용
CLA	90
INS	C6
P1	00
P2	00
Lc	None
Data	None
Le	18

4.3.2 Response Message

	내 용	길 이
	Response Data는 파일 구조 참조	

4.3.3 에러 코드

코 드	내 용
SW1-SW2	Success : 90 00 Error 6A 81 - 지원되지 않는 기능 6A 82 - 존재하지 않는 파일 6A 86 - 오류 파라미터 P1-P2 6A 87 - P1 P2와 일치되지 않는 Lc

4.4 UPDATE HiPass Info

- 고속도로 입구정보파일에 기록하기 위한 전용 명령이다.
- Initialize IEP 명령에 의해 생성된 Session Key가 존재해야 한다.
- 입력데이터는 입구정보외의 Tag, Length는 제외한다.

4.4.1 Command message

코 드	내 용
CLA	94
INS	C8
P1	00 : 입구정보파일
P2	00
Lc	18 + 4
Data	Data Block + Mac
Le	None

* Data Block은 입구정보 파일 참조

5. 하이패스 거래 프로토콜

5.1 접촉식 하이패스 거래

선택한 금액만큼 IEP에서 PSAM으로 전자적 가치가 이전되는 과정이다. 이 거래는 하이패스 차로 거래에 이용될 수 있다. 하이패스 거래는 취소거래를 할 수 없으므로, 사용자 카드 및 PSAM은 마지막 구매 거래 내역파일을 생성할 필요가 없다.

IEP	PDA	PSAM
- 난수 생성(R_{IEP}) - $MTOT_{IEP}$ = 0 - NT_{IEP} = NT_{IEP} + 1 - $KSES_{IEP}$ 생성 FEA_CBC(NT_{IEP}||R_{IEP}, KDP_{IEP}) - 서명S1 생성 FEA_CBC(PP_{IEP}||IEP||BAL_{IEP}, $KSES_{IEP}$) - Response (ALG_{IEP},VK_{IEP_KDP},NT_{IEP},R_{IEP},PP_{IEP}, IEP,BAL_{IEP},ID_{CENTER},$ID_{SERVICE}$,S1)	<- Initialize IEP	
	Initialize PSAM -> (ALG_{IEP},VK_{IEP_KDP},NT_{IEP},R_{IEP},PP_{IEP}, IEP,BAL_{IEP},ID_{CENTER}, S1)	- 조건확인 (ALG_{IEP},VK_{IEP_KDP},PP_{IEP},IEP, $ID_{SERVICE}$) - TRT_{PSAM} 생성 - NT_{PSAM} = NT_{PSAM} + 1 - $MTOT_{PSAM}$ = 0 - KDP_{PSAM} 생성 3DES_CBC(ID_{CENTER}||ID_{IEP}, KMP_{PSAM}) - $KSES_{PSAM}$ 생성 FEA_CBC(NT_{IEP}||R_{IEP}, KDP_{PSAM}) - 서명검증(S1) - 서명S2 생성 FEA_CBC(PP_{PSAM}||PSAM||NT_{PSAM}, $KSES_{PSAM}$) - Response(PP_{PSAM}, PSAM, NT_{PSAM}, S2)
	M_{PDA} 입력	
- 조건확인(BAL_{IEP} ≥ M_{PDA})	<- Purchase IEP	

- 조건확인(M_{MAX_IEP} ≥ M_{PDA})
- 서명검증(S2)
- $MTOT_{IEP}$ = $MTOT_{IEP}$ + M_{PDA}
- if(소지자지불정보==후불)
BAL_{TEMP} = BAL_{IEP} - M_{PDA}
else
BAL_{IEP} = BAL_{IEP} - M_{PDA}
- 서명S3 생성
if(소지자지불정보==후불) {
FEA_CBC(PSAM||NT_{PSAM}||BAL_{TEMP} $KSES_{IEP}$)
} else {
FEA_CBC(PSAM||NT_{PSAM}||BAL_{IEP}, $KSES_{IEP}$)
}
- Response(S3)
	(PP_{PSAM}, PSAM, NT_{PSAM}, M_{PDA}, S2)	

	Credit PSAM(M_{PDA}, S3, $ID_{SERVICE}$) ->	- $MTOT_{PSAM}$=$MTOT_{PSAM}$+M_{PDA} - BAL_{IEP}=BAL_{IEP}-M_{PDA} - 서명검증(S3) - TM_{PP} = TM_{PP} + M_{PDA} - Response(MAC)

- 거래내역저장
if(소지자지불정보==후불) {
(Data,TRT,NT_{IEP},$MTOT_{IEP}$,BAL_{TEMP}, PP_{PSAM},PSAM,NT_{PSAM},CC_{IEP})
} else {
(Data,TRT,NT_{IEP},$MTOT_{IEP}$,BAL_{IEP}, PP_{PSAM},PSAM,NT_{PSAM},CC_{IEP})
}
- Response()
	<- IEP Complete purchase (Date)	

	PSAM Complete Purchase(Date) ->	- NI_{PP}=NI_{PP}+1 - 서명S_{INDC}생성(Date||TRT_{PSAM}||PP_{IEP}||IEP||NT_{IEP}||NT_{PSAM}||$MTOT_{PSAM}$||NI_{PP}||NC||VK_{PSAM_KDINDC},$KDINDC_{PSAM}$) - 서명S_{INDS}생성(Date||TRT_{PSAM}||PP_{IEP}||IEP||NT_{IEP}||NT_{PSAM}||$MTOT_{PSAM}$||NI_{PP}||NC||VK_{PSAM_KDINDC}||S_{INDC}||VK_{PSAM_KDINDS},$KDINDS_{PSAM}$) - Response($MTOT_{PSAM}$,NI_{PP},NC, VK_{PSAM_KDINDC},S_{INDC},VK_{PSAM_KDINDS},S_{INDS})
	<- Update Hipass Info (입구정보파일,MAC) 입구정보파일 업데이트 <- Append Record (요금징수내역파일) 요금징수내역파일 기록 Write	

	(Date,TRT_{PSAM},PP_{IEP},IEP,NT_{IEP}, NT_{PSAM},$MTOT_{PSAM}$,NI_{PP},NC, VK_{PSAM_KDINDC},S_{INDC}, VK_{PSAM_KDINDS},S_{INDS})	

5.2 비접촉식 하이패스 거래

선택한 금액만큼 IEP에서 PSAM으로 전자적 가치가 이전되는 과정이다. 이 거래는 하이패스 차로 거래에 이용될 수 있다. 하이패스 거래는 취소거래를 할 수 없으므로, 사용자 카드 및 PSAM은 마지막 구매 거래 내역파일을 생성할 필요가 없다.

IEP	PDA	PSAM
- 난수 생성(R_{IEP}) - $MTOT_{IEP}$ = 0 - NT_{IEP} = NT_{IEP} + 1 - $KSES_{IEP}$ 생성 FEA_CBC(NT_{IEP}||R_{IEP}, KDP_{IEP}) - 서명S1 생성 FEA_CBC(PP_{IEP}||IEP ‖ BAL_{IEP}, $KSES_{IEP}$) -Response(ALG_{IEP},VK_{IEP_KDP},NT_{IEP}, R_{IEP},PP_{IEP},IEP,BAL_{IEP}, ID_{CENTER},$ID_{SERVICE}$,S1)	<- Initialize IEP	
	Initialize PSAM -> (ALG_{IEP},VK_{IEP_KDP},NT_{IEP},R_{IEP},PP_{IEP}, IEP,BAL_{IEP},ID_{CENTER}, S1)	- 조건확인 (ALG_{IEP},VK_{IEP_KDP},PP_{IEP},IEP, $ID_{SERVICE}$) - TRT_{PSAM} 생성 - NT_{PSAM} = NT_{PSAM} + 1 - $MTOT_{PSAM}$ = 0 - KDP_{PSAM} 생성 3DES_CBC(ID_{CENTER}||ID_{IEP}, KMP_{PSAM}) - $KSES_{PSAM}$ 생성 FEA_CBC(NT_{IEP}||R_{IEP}, KDP_{PSAM}) - 서명검증(S1) - 서명S2 생성 FEA_CBC(PP_{PSAM}||PSAM||NT_{PSAM} , $KSES_{PSAM}$) - Response (PP_{PSAM}, PSAM, NT_{PSAM}, S2)
	M_{PDA} 입력	
- 조건확인(BAL_{IEP} ≥ M_{PDA}) - 조건확인(M_{MAX_IEP} ≥ M_{PDA}) - 서명검증(S2) - $MTOT_{IEP}$ = $MTOT_{IEP}$ + M_{PDA} - if(소지자지불정보==후불) BAL_{TEMP} = BAL_{IEP} - M_{PDA} else	<- Purchase IEP (PP_{PSAM}, PSAM, NT_{PSAM}, M_{PDA}, S2)	

BAL_{IEP} = BAL_{IEP} - M_{PDA}
- 서명S3 생성
if(소지자지불정보==후불) {
FEA_CBC(PSAM||NT_{PSAM}||BAL_{TEMP}
$KSES_{IEP}$)
} else {
FEA_CBC(PSAM||NT_{PSAM}||BAL_{IEP},
$KSES_{IEP}$)
}
- Response(S3)		

	Credit PSAM(M_{PDA}, S3, $ID_{SERVICE}$) ->	- $MTOT_{PSAM}$=$MTOT_{PSAM}$+M_{PDA} - BAL_{IEP}=BAL_{IEP}-M_{PDA} - 서명검증(S3) - TM_{PP} = TM_{PP} + M_{PDA} - Response(MAC)

- 거래내역저장
if(소지자지불정보==후불) {
(Data,TRT,NT_{IEP},$MTOT_{IEP}$,BAL_{TEMP},
PP_{PSAM},PSAM,NT_{PSAM},CC_{IEP})
} else {
(Data,TRT,NT_{IEP},$MTOT_{IEP}$,BAL_{IEP},
PP_{PSAM},PSAM,NT_{PSAM},CC_{IEP})
}
R6:Reponse()
	<- IEP Complete purchase (Date)	

	PSAM Complete Purchase(Date) ->	- NI_{PP} = NI_{PP} + 1 - 서명S_{INDC}생성(Date||TRT_{PSAM}|| PP_{IEP}||IEP||NT_{IEP}||NT_{PSAM}|| $MTOT_{PSAM}$||NI_{PP}||NC|| VK_{PSAM_KDINDC},$KDINDC_{PSAM}$) - 서명S_{INDS}생성(Date||TRT_{PSAM}|| PP_{IEP}||IEP||NT_{IEP}||NT_{PSAM}|| $MTOT_{PSAM}$||NI_{PP}||NC|| VK_{PSAM_KDINDC}||S_{INDC}|| VK_{PSAM_KDINDS},$KDINDS_{PSAM}$) - Response($MTOT_{PSAM}$,NI_{PP},NC, VK_{PSAM_KDINDC},S_{INDC},VK_{PSAM_KDINDS},S_{INDS})
	<- Update Hipass Info (입구정보파일,MAC) 입구정보파일 업데이트 <- Append Record (요금징수내역파일) 요금징수내역파일 기록 Write (Date,TRT_{PSAM},PP_{IEP},IEP,NT_{IEP}, NT_{PSAM},$MTOT_{PSAM}$,NI_{PP},NC, VK_{PSAM_KDINDC},S_{INDC},	

	$VK_{PSAM\_KDINDS,S_{INDS}}$	

부속서 A(참고) 응답 코드

A.1 응답 코드 KS X 6924-2를 따른다

제2장 지불SAM 전국호환성 인증기준

제1부 : 지불 SAM의 기본 구조

1. 적용범위 KS X 6923-1에 따른다.
2. 인용표준 KS X 6923-1에 따른다.
3. 용어와 정의 KS X 6923-1에 따른다.
4. 기호 및 약어 KS X 6923-1에 따른다.

5. 지불 SAM의 기능
5.1. 환경 조건 KS X 6923-1에 따른다.
5.2 지불 SAM의 논리적 구조 KS X 6923-1에 따른다.
5.3 지불 SAM의 최소 요구 사항 KS X 6923-1에 따른다.

6. 특 성
6.1 통신 방식 및 통신 속도 KS X 6923-1에 따른다.
6.2 전송 프로토콜 KS X 6923-1에 따른다.
6.3 통신상 오류 발생 시 응답 구조 KS X 6923-1에 따른다.
6.4 지불 SAM의 명령 KS X 6923-1에 따른다.
6.5 지불 SAM의 응답 KS X 6923-1에 따른다.

7. 데이터 구조
7.1 데이터 종류 KS X 6923-1에 따른다.
7.2 ALG_{SAM} KS X 6923-1에 따른다.
7.3 AV_{SAM} KS X 6923-1에 따른다.
7.4 AID(RID + PIX) KS X 6923-1에 따른다.
7.5 $DEXP_{SAM}$ KS X 6923-1에 따른다.
7.6 $DISS_{SAM}$ KS X 6923-1에 따른다.
7.7 ID_{SAM} KS X 6923-1에 따른다.
7.8 NT_{SAM} KS X 6923-1에 따른다.
7.9 SC_{SAM} KS X 6923-1에 따른다.
7.10 $TYPE_{SAM}$ KS X 6923-1에 따른다.
7.11 LC_{SAM} KS X 6923-1에 따른다.
7.12 M_{PDA} KS X 6923-1에 따른다.
7.13 NT_{EP} KS X 6923-1에 따른다.
7.14 ID_{EP} KS X 6923-1에 따른다.
7.15 ID_{CENTER} KS X 6923-1에 따른다.
7.16 ALG_{EP} KS X 6923-1에 따른다.
7.17 VK_{XX_KEY} KS X 6923-1에 따른다.
7.18 BAL_{EP} KS X 6923-1에 따른다.
7.19 TRT KS X 6923-1에 따른다.
7.20 NI_{SAM} KS X 6923-1에 따른다.

7.21 NC_{SAM} KS X 6923-1에 따른다.
7.22 TOT_{SAM} KS X 6923-1에 따른다.
7.23 SN_{SAM} KS X 6923-1에 따른다.

8. 키 구조
8.1 키의 종류 KS X 6923-1에 따른다.
8.2 CT_{KEY} KS X 6923-1에 따른다.
8.3 MP_{KEY} KS X 6923-1에 따른다.
8.4 TM_{KEY} KS X 6923-1에 따른다.
8.5 IND_{KEY} KS X 6923-1에 따른다.
8.6 CE_{KEY} KS X 6923-1에 따른다.
8.7 DP_{KEY} KS X 6923-1에 따른다.

제2부 : 명령어 및 프로토콜

1. 적용범위 KS X 6923-2에 따른다.
2. 인용표준 KS X 6923-2에 따른다.
3. 용어와 정의 KS X 6923-2에 따른다.
4. 기호 및 약어 KS X 6923-2에 따른다.

5. 명령어
5.1 Initialize_SAM(선불/후불) KS X 6923-2에 따른다.
5.2 Credit_SAM(선불/후불) KS X 6923-2에 따른다.
5.3 Re-initialize_SAM KS X 6923-2에 따른다.
5.4 Re-credit_SAM KS X 6923-2에 따른다.
5.5 Initialize_SAM_for_Cancellation(선불/후불) KS X 6923-2에 따른다.
5.6 Cancellation_SAM(선불/후불) KS X 6923-2에 따른다.

7. 프로토콜
7.1 선불카드 거래 프로토콜 KS X 6923-2에 따른다.
7.2 선불카드 재거래 프로토콜 KS X 6923-2에 따른다.
7.3 선불카드 직전 거래 취소 프로토콜 KS X 6923-2에 따른다.
7.4 후불카드 거래 프로토콜 KS X 6923-2에 따른다.
7.5 후불카드 직전 거래 취소 프로토콜 KS X 6923-2에 따른다.

부속서 A(참고) 응답 코드
A.1 응답 코드 KS X 6923-2에 따른다.

제3장 지불단말기 전국호환성 인증기준

1. 적용범위 KS X 6925-2에 따른다
2. 인용표준 KS X 6925-2에 따른다
3. 용어와 정의 KS X 6925-2에 따른다
4. 기호 KS X 6925-2에 따른다

5. 지불단말기의 특성 및 구조
5.1 통신 방식 KS X ISO/IEC 14443-2에 따른다.
5.2 통신 거리 KS X ISO/IEC 14443-2에 따른다.
5.3 충돌 방지 KS X ISO/IEC 14443-3에 따른다.

6. 프로토콜
6.1 선불카드 거래 프로토콜 KS X 6925-2에 따른다.
6.2 선불카드 재거래 프로토콜 KS X 6925-2에 따른다.
6.3 선불카드 직전 거래 취소 프로토콜 KS X 6925-2에 따른다.
6.4 후불카드 거래 프로토콜 KS X 6925-2에 따른다.
6.5 후불카드 직전 거래 취소 프로토콜 KS X 6925-2에 따른다.
6.6 Application 정보 조회 프로토콜 제1장 교통카드 전국호환성 인증기준에 따른다.

[별표 2] 인증대행기관의 적합성시험 장비 기준

장비명	용도 및 목적	사양
통신거리측정기	시료의 접촉 각도에 따른 통신거리 검증	거리: 10cm이내 각도: 0~90°
충돌방지측정기	복수 개의 시료 존재 시 충돌방지 검증	Anti-Collision 알고리즘 모듈
교통카드 프로토콜 적합성시험 모듈	CONFIG DF 및 EF CONFIG 규격 준수 여부 검증	거래 적합성시험 모듈
	거래 프로토콜 준수 여부 검증	
	재거래 프로토콜 준수 여부 검증	재거래 적합성시험 모듈
	직전거래취소 프로토콜 준수 여부 검증	직전거래취소 적합성시험 모듈
	거래/재거래/직전거래취소 프로토콜 중 서명(MAC) 검증 절차 준수 여부 검증	보안 적합성시험 모듈
지불SAM 프로토콜 적합성시험 모듈	거래 프로토콜 준수 여부 검증	거래 적합성시험 모듈
	재거래 프로토콜 준수 여부 검증	재거래 적합성시험 모듈
	직전거래취소 프로토콜 준수 여부 검증	직전거래취소 적합성시험 모듈
	거래/재거래/직전거래취소 프로토콜 중 서명(MAC) 검증 절차 준수 여부 검증	보안 적합성시험 모듈

[별지 제1호 서식] 인증대행기관 지정 신청서

인증대행기관 지정 신청서

선청인	기 관 명		사업자등록번호	
	대표자명		생 년 월 일	
	소 재 지			
	전화번호	TEL / FAX		
설 립 목 적				
설립 연월일				

국토해양부 고시 제2010-180호 교통카드 관련 장비의 전국호환성 인증 요령에 의거하여 교통카드 관련 장비에 대한 전국호환성 인증대행기관 지정을 신청합니다.

년 월 일

신청인 (서명 또는 인)

국토해양부장관 귀하

<구비서류>

1. 법인등기부등본 1 부
2. 인력 및 장비 확보를 증명하는 서류 5부
3. 인증업무 수행계획서 5부
4. 인증대행기관 운영에 관한 업무규정 5부

비고 : “인증업무 수행계획서”는 지정신청자의 일반현황, 인증업무의 효율성·공정성·보안성 확보방안, 업무수행 일정계획을 포함하여 작성한다.

[별지 제2호 서식] 인증대행기관 지정서

제 호

인증대행기관 지정서

기 관 명

사업자등록번호

대 표 자 명

소 재 지

국토해양부 고시 제2010-180호 교통카드 관련 장비의 전국호환성 인증 요령에 따라 위 기관을 교통카드 관련 장비에 대한 전국호환성 인증대행기관으로 지정합니다.

년 월 일

국토해양부장관

[별지 제3호 서식] 인증신청서

전국호환성 인증 신청서

신청인	기 관 명 (상 호 명)		사업자등록번호	
	대표자명		생 년 월 일	
	소 재 지			
	전화번호	TEL / FAX		
신청 구분	☐ 신규인증 ☐ 재시험 ☐ 유효기간 만료에 따른 재인증			
신청 장비	인증대상	☐ 교통카드 ☐ 지불보안응용모듈 ☐ 지불단말기 ☐ 기타 ( )		
	제 품 명			
	제품상세 (모 델 명)			

국토해양부 고시 제2010-180호 교통카드 관련 장비의 전국호환성 인증요령에 의거하여 교통카드 관련 장비의 전국호환성 인증을 신청합니다.

년 월 일

신청인 : (서명 또는 날인)

국토해양부장관 귀하

<구비서류>

1. 사업자등록증 사본 1부
2. 인증대상 시료 5대
3. 시료 설명서 1부
4. 기타 인증대행기관 요구 자료

[별지 제4호 서식] 인증서

전국호환성 인증서

인증대상	:	□교통카드 □지불보안응용모듈 □지불단말기 □기타( )
기 관 명 (상 호 명)	:	
대 표 자	:	
제 품 명	:	
제품상세 (모 델 명)	:	
인증번호	:	
인증연월일	:	
인증유효기간	:	

「대중교통의 육성·이용촉진에 관한 법률」 제10조의7의 규정 및 「교통카드 관련 장비의 전국호환성 인증 요령」에 의하여 위와 같이 교통카드 등 관련 장비를 인증합니다.

년 월 일

국토해양부장관