교통카드 관련 장비의 전국호환성
프로토콜 적합성 시험 규정

2010. 6. 8. 제정

2010. 6. 7. 국토해양부장관 승인

한국건설교통기술평가원

목 차

서 문 ····· 1

1. 적용 범위 ····· 1

2. 인용 규격 ····· 1

3. 용어정의 ····· 2

4. 약 어 ····· 2

5. 시험 환경 ····· 3

6. 발급 데이터 ····· 4

6. 교통카드 프로토콜 적합성 시험 ····· 5

6.1. 교통카드 거래 프로토콜 ····· 5

6.2. 교통카드 재거래 프로토콜 ····· 5

6.3. 교통카드 직전거래 취소 프로토콜 ····· 5

6.4. Application 정보 조회 프로토콜 ····· 6

7. 지불SAM 프로토콜 적합성 시험 ····· 7

7.1. 지불SAM 거래 프로토콜 ····· 7

7.2. 지불SAM 재거래 프로토콜 ····· 7

7.3. 지불SAM 직전거래 취소 프로토콜 ····· 7

서 문

본 적합성 시험 규정은 교통카드 관련 장비의 프로토콜 적합성 여부를 시험하기 위한 방법과 절차를 정하는 규정이다.

1. 적용 범위

본 적합성 시험 규정은 "교통카드 관련 장비의 전국호환성 인증 요령"에서 정의된 각 요구 사항의 충족 여부를 확인하기 위해 필요한 항목들을 테스트하기 위한 사례를 기술하고 있다.

본 규정은 교통카드 관련 장비에 한정하며, 시험 방법 등에 대하여 적용한다.

2. 인용 규격

본 규정에서는 국제표준화기구(ISO)에서 제정한 카드관련 국제표준, 그리고 한국산업규격을 참조하여 작성함을 원칙으로 한다.

- 교통카드 관련 장비의 전국호환성 인증 요령, 2010.4.
- KS X 6923 - 1 비접촉식 전자화폐 단말기용 지불 보안응용모듈(SAM) 규격 제1부 : 지불 SAM의 물리적 특성 및 기본 구조, 2009.12.
- KS X 6923 - 2 비접촉식 전자화폐 단말기용 지불 보안응용모듈(SAM) 규격 제2부 : 명령어 및 프로토콜, 2009.12.
- KS X 6923 - 3 비접촉식 전자화폐 단말기용 지불 보안응용모듈(SAM) 규격 제3부 : 지불SAM의 암호 알고리즘, 2009.12.
- KS X 6923 - 4 비접촉식 전자화폐 단말기용 지불 보안응용모듈(SAM) 규격 제4부 : 지불SAM의 시험방법 및 관리, 2009.12.
- KS X 6924 - 1 선불IC카드 - KS X 6923 대응 사용자 카드 - 제1부 : 물리적 특성 및 기본 구조, 2009.12.
- KS X 6924 - 2 선불IC카드 - KS X 6923 대응 사용자 카드 - 제2부 : 명령어 및 프로토콜, 2009.12.
- KS X 6924 - 3 선불IC카드 - KS X 6923 대응 사용자 카드 - 제3부 : 암호 알고리즘, 2009.12.
- KS X 6924 - 4 선불IC카드 - KS X 6923 대응 사용자 카드 - 제4부 : 적합성 시험, 2009.12.
- ISO/IEC 7810, Identification cards - Physical characteristics
- ISO/IEC 7816, Identification cards - Integrated circuit cards
- ISO/IEC 10373, Identification cards - Test methods
- ISO/IEC 14443, Identification cards- Contactless integrated circuit(s) cards - Proximity cards

3. 용어정의

- 교통카드 : 교통서비스 이용대가를 전자적으로 지불 . 결제하는데 사용되는 카드나 그 밖의 매체를 의마한다.
- 지불보안응용모듈(SAM) : 소형 인증서버 역할을 수행하는 칩으로서, 지불단말기에 장착되어 암호 알고리즘 및 인증 알고리즘을 활용하여 지불거래 발생 시마다 교통카드의 데이터를 처리하는 장치를 말한다.
- 지불단말기 : 교통카드의 인식 및 교통요금의 결제를 수행하는 단말기를 말한다.
- 구매 키(Purchase Key) : 구매거래 시마다 사용하는 키를 의미한다.
- 서명(Sign) : 메시지 인증 코드인 MAC(Message Authentication Code)를 서명으로 사용한다.

4. 약 어

AID	Application Identifier
ALG	Algorithm Identifier
BAL	Balance
BCD	Binary Coded Decimal
CE	(SAM Application) Collection & Erase Key

CLA	Class Field
CT	Center Key
D_{EXP}	Date of Expiration
DP	Derivation Purchase key
EP	Electronic Purse
ID	Identifier/Identification
IND	Individual transaction key
INS	Instruction Field
M	Money of Transaction
MAC	Message Authentication Code
M_{PDA}	Money of Purchase Transaction
MP_{KEY}	Master Purchase Key
NC	Number of Collection
NI	Number of Individual transaction
NT_{EP}	Number of Transaction in EP
PDA	Purchase Device Application
S1, S2, S3	Sign1, Sign2, Sign3
SAM	Secure Application Module
SES	Session Key
SC	Status Code
SW	Status Word
T-DES	Triple Data Encryption Standard
TM	Total Amount Key
TRT	Transaction Type
VK	Version of Key

5. 시험 환경

별도의 언급이 없을 시, 시험환경은 다음과 같다.

가. 주위온도 : 23 ± 3℃

나. 상대습도 : 40 ~ 60%

다. 다음 조건의 미사용 카드를 시료로 한다.

- 개인화 또는 시험 작업을 거치지 않은 상태
- 5 ~ 30℃의 온도 및 10 ~ 90%의 상대습도에서 보관된 상태
- 열충격 및 48시간 이상의 직사광선에 노출되지 않은 상태

시료가 사전 조건을 만족해야 할 경우 상기의 시험 환경에서 24시간 이상 유지한다.

6. 발급 데이터

가. 적합성 시험을 위한 발급 데이터는 아래와 같다.

ID_{CENTER}	MP_{KEY}	VK	비고
01	01010101010101010101010101010101	01	
02	02020202020202020202020202020202	01	
03	03030303030303030303030303030303	01	
04	04040404040404040404040404040404	01	
05	05050505050505050505050505050505	01	
06	06060606060606060606060606060606	01	
07	07070707070707070707070707070707	01	
08	08080808080808080808080808080808	01	
09	09090909090909090909090909090909	01	
0A	0A0A0A0A0A0A0A0A0A0A0A0A0A0A0A0A	01	
0B	0B0B0B0B0B0B0B0B0B0B0B0B0B0B0B0B	01	
0C	0C0C0C0C0C0C0C0C0C0C0C0C0C0C0C0C	01	
0D	0D0D0D0D0D0D0D0D0D0D0D0D0D0D0D0D	01	
0E	0E0E0E0E0E0E0E0E0E0E0E0E0E0E0E0E	01	예비
0F	0F0F0F0F0F0F0F0F0F0F0F0F0F0F0F0F	01	예비
10	10101010101010101010101010101010	01	예비
11	11111111111111111111111111111111	01	예비
12	12121212121212121212121212121212	01	예비
13	13131313131313131313131313131313	01	예비
14	14141414141414141414141414141414	01	예비
15	15151515151515151515151515151515	01	예비
16	16161616161616161616161616161616	01	예비
17	17171717171717171717171717171717	01	예비

나. CONFIG DF의 AID는 아래와 같다.

AID	A0 00 00 04 52 00 01

7. 교통카드 프로토콜 적합성 시험

7.1. 교통카드 거래 프로토콜

7.1.1. Initialize CARD Command

KS X 6924-4 7.1.1 Initialize CARD Command 적합성 시험에 따른다.

7.1.2. Purchase CARD Command

KS X 6924-4 7.1.2 Purchase CARD Command 적합성 시험에 따른다.

7.2. 교통카드 재거래 프로토콜

7.2.1. Re-Initialize CARD Command

KS X 6924-4 7.2.1 Re-Initialize CARD Command 적합성 시험에 따른다.

7.2.2. Re-Purchase CARD

KS X 6924-4 7.2.2 Re-Purchase CARD Command 적합성 시험에 따른다.

7.3. 교통카드 직전거래 취소 프로토콜

7.3.1. Initialize CARD For Cancellation Command

KS X 6924-4 7.3.1 Initialize CARD For Cancellation Command 적합성 시험에 따른다.

7.3.2. Cancellation CARD Command

KS X 6924-4 7.3.2 Cancellation CARD Command 적합성 시험에 따른다.

7.4. Application 정보 조회 프로토콜

7.4.1. Application 정보 조회 프로토콜 적합성 시험

Test No	내용	Status	평가목표
7.4.1.1	정상조회	9000	Read Record EF_{CONFIG} 수행 시 정상적인 응답Data와 SW("9000") 반환 여부 확인

7.4.1.1. Read Record

목적	Read Record EF_{CONFIG} 수행 시 정상적인 응답Data와 SW("9000") 반환 여부 확인
적합성시험 절차	① Select CONFIG DF ② Read Record EF_{CONFIG}
적합성시험 APDU	CLA: 00 / INS: B2 / P1: 01 / P2: 0C / Lc: Empty / DATA: <input> / Le: 00
<input>	NONE
적합성시험 방법	적합성시험 APDU값과 DATA를 사용하여 Read Record EF_{CONFIG}를 정상적으로 수행시킨다.
합격 기준	SW1-SW2 = "9000" Response Data 확인

Response Data

Tag	길이	Value
50	2	카드 규격(선불 : 01 00 , 후불 : 11 00)
47	2	지원 항목
43	1	ID_{CENTER}
11	5	잔액 조회 명령 (선택)
4F	5~16	교통 호환 ADF AID
9F10	3*N	부가 정보 파일
45	1	카드 소지자(카드타입) 정보
5F24	2	유효기간
12	8	카드일련번호 (선택)
13	8	카드관리번호 (선택)
BF0C	Var	카드 사업자 임의의 정보 (선택)

8. 지불SAM 프로토콜 적합성 시험

8.1. 지불SAM 거래 프로토콜

8.1.1. Initialize SAM Command

KS X 6923-4 7.1.1 Initialize SAM Command 적합성 시험에 따른다.

8.1.2. Credit SAM Command

KS X 6923-4 7.1.2 Credit SAM Command 적합성 시험에 따른다.

8.2. 지불SAM 재거래 프로토콜

8.2.1. Re-Initialize SAM Command

KS X 6923-4 7.2.1 Re-Initialize SAM Command 적합성 시험에 따른다.

8.2.2. Re-Credit SAM Command

KS X 6923-4 7.2.2 Re-Credit SAM Command 적합성 시험에 따른다.

8.3. 지불SAM 직전거래 취소 프로토콜

8.3.1. Initialize SAM For Cancellation Command

KS X 6923-4 7.3.1 Initialize SAM For Cancellation Command 적합성 시험에 따른다.

8.3.2. Cancellation SAM Command

KS X 6923-4 7.3.2 Cancellation SAM Command 적합성 시험에 따른다.