한국ITS학회논문지
제2권, 제2호 (2003. 9 · 12)
pp.31~42

하이패스플러스카드 시험 모듈 개발

Developing the Test Module of Hipass^{PLUS} Card

이 기 한* (Ki-Han, Lee) 이 대 규** (Dae-Kyu, Lee) 여 운 상*** (WoonSang, Yeo) 이 승 환**** (Seung-Hwan, Lee)

요 약

한국도로공사의 선불형 플라스틱카드는 사용자 측면이나 관리 측면에서 많은 문제를 야기하고 있다. 스마트카드 형태의 선불형 전자지불카드인 하이패스플러스카드는 기존 카드의 문제점들을 극복하고 현재 교통분야에 적용된 스마트카드 등과의 효율적인 연계가 가능하다. 하이패스플러스카드는 가치 저장 및 가지 지불에 사용되는 카드이다. 따라서, 하이패스플러스카드의 기능 및 보안이 철저해야 한국도로공사의 전자지불시스템이 안전하다. 본 논문은 하이패스플러스카드에 LSAM으로부터 가치를 저장받기위한 기능 및 보안 시험과 하이패스플러스카드로부터 PSAM에 가치를 지불하기 위한 기능 및 보안성을 시험하기 위한 시험 방법, 시험 표준항목, 그리고 시험 절차 등을 포함한 시험 모듈을 개발했다. 하이패스플러스카드의 시험 표준항목은 한국도로공사 규격서에 준하여 ISO 표준에 적합한 시험 항목으로 선정했으며, 시험 검사표는 시험 표준항목을 검사할 수 있는 기준에 의해서 작성했다. 시험 모듈은 시험 검사표에 의한 시험 표준항목을 시험할 수 있는 방법 및 절차를 따라서 개발했다. 시험은 한국도로공사에서 사용되는 하이패스플러스카드를 이용하여 실행하였다. 본 시험 모듈은 하이패스플러스카드의 기능뿐 아니라 보안성 및 적합성을 시험하였다. 시험 결과에 의하면 현재 사용중인 하이패스플러스카드의 보안성 및 기능은 기준을 통과하였으며, 보안 및 기능에 문제가 없다는 것이 입증되었다.

Abstract

Prepaid plastic card issued by Korea Highway Company had a lot of problems in end-user usage and management. HipassPLUS Card, which is a smart card used for a prepaid electronic payment, overcomes the problems of prepaid plastic card.

HipassPLUS Card is also designed be compatible to other cards such as public transportation card. Thus, for the safety of using the card in such environment, the functionality and the security of HipassPLUS card should be faultless. This paper developed a test module including the test method, the test checklist, and the test procedure to examine the functionality and security of the payment mechanism of HipassPLUS card. The test module contains the method and the procedure to test the standard items according to the test checklist of HipassPLUS card. The test items and the test checklist of HipassPLUS card was selected under the provision of the specification of Korea Highway Company and ISO standard. The results of evaluation on HipassPLUS card using the proposed test module indicates that the HipassPLUS card satisfied the criteria under the characteristics of the functionality, security, and compatibility.

Key Words : 지능형교통시스템, 구간통행시간, 주행차량 자동인식

* 회 원 : 서울여자대학교 컴퓨터공학과 교수
** 비회원 : 한국도로공사 스마트웨이팀 대리
*** 비회원 : 한국도로공사 스마트웨이팀 부장
**** 회 원 : 아주대학교 환경건설교통공학부 교수
† 논문접수일 : 2003년 7월 16일

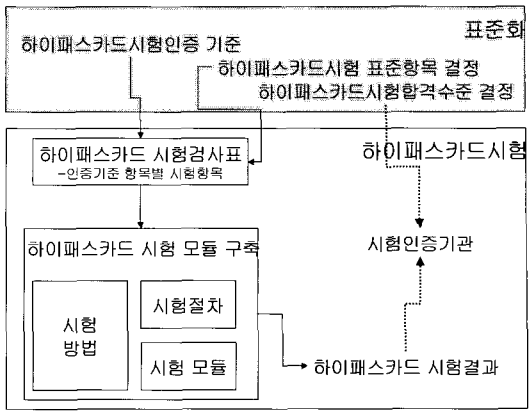
Ⅰ. 서 론

한국도로공사는 선불방식의 일회성 플라스틱 카드의 문제점을 극복하기 위해서, 스마트카드를 이용한 선불식 전자지불 시스템을 구축하고 있다. 스마트카드형 전자지불카드인 하이패스플러스카드의 기능은 기존의 선불기능과 하이패스기능뿐 아니라 일반 가맹점에서도 사용가능하도록 설계되었다. 한국형 전자지불 표준SAM과의 지불거래기능이 구현되어있어서 향후에 서울시에서 추진하는 지자체카드뿐 아니라 여러 지자체가 추진하는 카드와도 호환이 가능하다[1]. 또한, 물리적으로는 하이패스플러스카드는 접촉식 및 비접촉식 기능이 가능하다.

하이패스플러스카드의 기능 시험은 단순히 한국도로공사자체의 시험인증뿐 아니라 전국적인 인프라에 대한 시험인증과도 밀접한 연관 관계를 갖는다고 할 수 있다. 따라서, 하이패스플러스카드의 기능 및 보안성을 정확하게 시험 평가를 하는 것은 그 의미가 매우 크다고 본다.

스마트카드 시험에 관한 국제 표준은 ISO 10373에 규정하고 있다[2]. 스마트카드의 국제표준 시험인증은 일반적인 특성에 관한 시험[3], 접촉식 스마트카드의 시험인증[4], 그리고, 비접촉식 스마트카드의 시험인증[5,6,7,8,9]로 구분된다. 보안 분야는 국제적으로 CC/PP 시험인증과 국내에서는 정보화촉진기본법 제15조에 의한다[10,11]. 스마트카드를 시험하는 기구는 한국에서는 보안 및 기능에 관련되어서는 한국기술표준원이 ISO를 인증한 전자카드품질인증원과 한국정보보호진흥원이 있다[12].

하이패스플러스카드는 LSAM에 의해서 가치를 저장받고, PSAM에 가치를 지불하는 방식이다. 따라서, 하이패스플러스카드의 기능 시험인증은 LSAM 및 PSAM과의 기능을 시험하는 것이다. 하이패스플러스카드를 시험하기 위한 전체적인 시험 절차는 <그림 1>과 같다[13,14,15]. 본 논문에서는 하이패스플러스카드를 시험 평가하기 위해서 먼저, 시험 방법 및 절차를 정했고, 시험 방법에 맞는 시험 표준항목을 선정하였고, 선정된 시험 표준항목을 평가하기 위한 시험 모듈을 개발하였다. 이렇게 정해진



〈그림 1〉 하이패스플러스카드 시험 절차 구성

모듈에 의해서 실제 개발된 하이패스플러스카드를 시험하고 이를 분석하여 하이패스플러스카드가 원하는 기준을 통과하여 정확하게 동작하는 지를 분석했다.

Ⅱ. 시험 방법 및 절차

하이패스플러스카드 시험은 <표 1>과 같이 PSAM 및 LSAM과의 시험으로 구분한다. 보안 시험은 각 시험 중에 검사한다.

〈표 1〉 하이패스플러스카드 시험 종류

대분류	중분류	소분류	시험명
LSAM과의 시험	가치저장 시험	LSAM에 의한 가치저장 시험	L2H(가치저장)
PSAM과의 시험	비접촉식 지불거래 시험	비접촉식 일반/하이패스 지불거래 시험	H2P(일반/하이패스)
		비접촉식 표준SAM 지불거래 시험	H2P(표준SAM)
보안 시험	서명 확인 시험		
	암호화 시험		

1. L2H(가치저장) 시험 방법 및 절차

LSAM에 의해서 하이패스플러스카드에 가치가 저

장되는 개략적인 흐름은 <그림 2>와 같다[16]. 가치저장은 하이패스플러스카드와 LSAM이 상호 인증한 후, 선택된 금액만큼 LSAM 전자화폐에서 출금하여 하이패스플러스카드 소지자의 전자화폐로 이체되는 과정이다. 이 가치저장은 충전소의 충전단말기 등에서 이루어진다. LSAM에 저장되어 있는 금액 내에서만 하이패스플러스카드에 충전할 수 있다.

L2H(가치저장) 시험 중 기능 시험 방법 및 절차는 B3, A5, B4, C5, B5, A9, B6, C10, B7 순으로 시험하고, LSAM과 하이패스플러스카드간에 가치를 저장하는 동안에 LSAM과 하이패스플러스카드가 정확하게 정보를 전달되는 지를 시험하는 서명확인 시험 방법 및 절차는 A4, C4, C7, A8, A10, C9, C11 순으로 시험하며, LSAM과 하이패스플러스카드간에 가치를 저장하는 동안에 LSAM과 하이패스플러스카드가 전달하는 정보가 정확하게 암호화 및 복호화가 이루어지는 지를 시험하는 암호화 시험 방법 및 절차는 A3, C3, C6, A7 순으로 시험한다.

하이패스플러스카드	LDA	LSAM
	<- B1. 하이패스플러스카드 DF선택	
A1. 응답 ->		
	B2. M_{LDA}와 PIN입력	
	B3. Initialize 하이패스플러스(M_{LDA}, PIN)	
	<-	
A2. 난수생성		
A3. $KSES1_{하이패스플러스}$생성**(암호화)**		
A4. 서명 S1 생성**(서명확인)**		
A5. 거래내역 저장		
A6. 응답 ->		
	B4. Debit LSAM ->	
		C1. 난수 생성
		C2. 조건확인
		C3. KDL_{LSAM} 생성**(암호화)**
		C4. 서명S1검증**(서명확인)**
		C5. BAL_{LSAM} 차감
		C6. $KSES2_{LSAM}$ 생성**(암호화)**
		C7. 서명S2생성**(서명확인)**
		C8. 응답
	<- B5. Load 하이패스플러스(R_{LSAM},S2)	
A7. $KSES2_{하이패스플러스}$생성**(암호화)**		
A8. 서명S2검증**(서명확인)**		
A9. $BAL_{하이패스플러스}$증가		
A10. 서명S3생성**(서명확인)**		
A11. 거래내역저장		
A12. 응답 ->		
	B6. Complete Debit(S3) ->	
		C9. 서명S3검증**(서명확인)**
		C10. 충전내역저장
		C11. 서명S4생성**(서명확인)**
		C12. 응답
	B7. 저장 <-	

〈그림 2〉 LSAM과 하이패스플러스카드간의 가치저장 흐름도

2. H2P(일반/하이패스) 시험 방법 및 절차

H2P(일반/하이패스)은 PSAM과 하이패스플러스카드가 상호 인증한 후, 선택한 금액만큼 하이패스플러스카드에서 PSAM으로 전자적 가치가 이전되는 <그림 3>과 같은 과정을 시험한다[16]. 일반/하이패스 지불거래는 T-DES_F를 사용한다.

H2P(일반/하이패스) 시험 중 기능 시험 방법 및 절차는 B1, A1, A4, B2, C1, C6, B3, A7, A9, B4, C8, C10, B5, A11, A12, B6, C12, C13, B7 순으로 시험하고, 하이패스플러스카드와 PSAM간에 가치를 저장하는 동안에 정확하게 정보를 전달되는 지를 시험하는 서명확인 시험 방법 및 절차는 A3, C3, C5, A6, A8, C7, C9, A10, C11 순으로 시험하며, 하이패스플러스카드와 PSAM간에 가치를 저장하는 동안에 전달하는 정보가 정확하게 암호화 및 복호화가 이루어지는 지를 시험하는 암호화 시험 방법 및 절차는 A2, C2, C4, A5 순으로 시험한다.

하이패스플러스	PDA	PSAM
	<- B1. Initialize 하이패스플러스	
A1. 조건확인 A2. $KSES_{하이패스플러스}$생성**(암호화)** A3. 서명S1생성**(서명확인)** A4. 응답		
	B2. Initialize PSAM ->	
		C1. 조건확인 C2. KDC_{PSAM}생성**(암호화)** C3. 서명S1검증**(서명확인)** C4. $KSES_{PSAM}$생성**(암호화)** C5. 서명 S2생성**(서명확인)** C6. 응답
	<- B3. Purchase 하이패스플러스	
A5. $KSES_{하이패스플러스}$생성**(암호화)** A6. 서명S2검증**(서명확인)** A7. $BAL_{하이패스플러스}$차감 A8. 서명S3생성**(서명확인)** A9. 응답		
	B4. Credit PSAM ->	
		C7. 서명S3검증**(서명확인)** C8. BAL_{PSAM}증가 C9. 서명S4생성**(서명확인)** C10. 응답
	<- B5. Complete Purchase 하이패스플러스	
A10. 서명S4생성**(서명확인)** A11. 거래내역저장 A12. 응답		
	B6. Complete Purchse PSAM ->	
		C11. 서명S4검증**(서명확인)** C12. 개별거래내역저장 C13. 응답
	B7. 개별거래내역저장	

〈그림3〉 PSAM과 하이패스플러스카드의 일반/하이패스지불거래 흐름도

3. H2P(표준SAM) 시험 방법 및 절차

H2P(표준SAM)은 <그림 4>와 같이 비접촉식 교통 표준SAM과의 거래를 시험한다[1,17]. 표준SAM 지불거래는 다른 지불거래와 같이 취소 거래도 가능하지만 T-DES를 사용한다.

H2P(표준SAM) 시험 중 기능 시험 방법 및 절차는 B1, A1, A4, B2, C1, C6, B3, A7, A9, B4, C8, C9, C10, B5 순으로 시험하고, 하이패스플러스카드와 PSAM간에 가치를 저장하는 동안에 정확하게 정보를 전달되는 지를 시험하는 서명확인 시험 방법 및 절차는 A3, C3, C5, A6, A8, C7 순으로 시험하며, 하이패스플러스카드와 PSAM간에 가치를 저장하는 동안에 전달하는 정보가 정확하게 암호화 및 복호화가 이루어지는 지를 시험하는 암호화 시험 방법 및 절차는 A2, C2, C4, A5 순으로 시험한다.

III. 시험 표준항목 선정

II.장 시험 종류 및 방법에서 결정된 시험 방법에 의해서 PSAM을 시험하고 평가하기 위해서 다음과 같은 시험 표준항목을 결정하였다.

1. L2H(가치저장) 시험 표준항목

<그림 2>에서 L2H(가치저장) 시험은 A1부터 A12, B1부터 B7, 그리고 C1부터 C12까지의 모든 항목에 걸쳐서 이루어진다. 하지만, 이 모든 과정 중에서 B1과 B2는 B3에 의해서 검증되므로 시험할 필요가 없다. A2는 A3과 A4에 의해서 검증되므로 시험할 필요가 없고, A3은 A4에 의해서 검증되므로 시험할 필요가 없으며, A7은 A8에 의해서 검증되므로 시험할 필요가 없다. C1과 C2는 C3과 C4에 의

하이패스플러스	PDA	PSAM
	<- B1. Initialize 하이패스플러스	
A1. 조건확인 A2. $KSES_{하이패스플러스}$생성**(암호화)** A3. 서명S1생성**(서명확인)** A4. 응답		
	B2. Initialize PSAM ->	
		C1. 조건확인 C2. KDC_{PSAM}생성**(암호화)** C3. 서명S1검증**(서명확인)** C4. $KSES_{PSAM}$생성**(암호화)** C5. 서명 S2생성**(서명확인)** C6. 응답
	<- B3. Purchase 하이패스플러스	
A5. $KSES_{하이패스플러스}$생성**(암호화)** A6. 서명S2검증**(서명확인)** A7. $BAL_{하이패스플러스}$차감 A8. 서명S3생성**(서명확인)** A9. 응답		
	B4. Credit PSAM ->	
		C7. 서명S3검증**(서명확인)** C8. BAL_{PSAM}증가 C9. 개별거래내역저장 C10. 응답
	B5. 개별거래내역저장	

〈그림 4〉 PSAM과 하이패스플러스카드의 표준SAM 지불거래 흐름도

해서 검증되므로 시험할 필요가 없고, C3은 C4에 의해서 검증되므로 시험할 필요가 없고, C6은 C7에 의해서 검증되므로 시험할 필요가 없다. 따라서, 시험 순서에 따른 표준항목 및 선정기준은 다음 <표 2>와 같다.

〈표 2〉 L2H(가치저장) 시험 순서에 따른 기준 및 표준 항목

시험 기준	시험 표준항목
기능시험	B3. Initialize 하이패스플러스
보안시험	A4. 서명S1생성
기능시험	B4. Debit LSAM
기능시험	C5. BALLSAM
보안시험	C7. 서명S2생성
기능시험	B5. Load 하이패스플러스
기능시험	A9. BAL하이패스플러스
보안시험	A10. 서명S3생성
기능시험	B7. 저장

2. H2P(일반/하이패스) 시험 표준항목

<그림 3>에서 H2P(일반/하이패스) 시험은 A1부터 A12, B1부터 B7, 그리고 C1부터 C13까지의 모든 항목에 걸쳐서 이루어진다. 하지만, 이 모든 과정 중에서 A1과 A2는 A3에 의해서, A4는 B3에 의해서, C1과 C2는 C3에 의해서, C4는 C5에 의해서, C6은 B3에 의해서, A5는 A6에 의해서, A9는 B4에 의해서, C10은 B5에 의해서, A12는 B6에 의해서, C13은 B7에 의해서 각각 검증되므로 시험할 필요가 없다. 따라서, 시험 순서에 따른 표준항목 및 선정기준은 다음 <표 3>과 같다.

3. H2P(표준SAM) 시험 표준항목

<그림 4>에서 H2P(표준SAM) 시험은 A1부터 A9, B1부터 B5, 그리고 C1부터 C10까지의 모든 항목에 걸쳐서 이루어진다. 하지만, 이 모든 과정 중에서 A1과 A2는 A3에 의해서, A4는 B2에 의해서, C1,C2, C3, 그리고 C4는 C5에 의해서, C6은 B3에 의해서, A5, A6은 A8에 의해서, A9는 B4에 의해서,

〈표 3〉 H2P(일반/하이패스) 시험 순서에 따른 기준 및 표준항목

시험 기준	시험 표준항목
기능시험	B1. Initialize 하이패스플러스
보안시험	A3. 서명S1생성
기능시험	B2. Initialize PSAM
보안시험	C5. 서명S2생성
기능시험	B3. Purchase 하이패스플러스
기능시험	A7. BAL하이패스플러스감소
보안시험	C5. 서명S3생성
기능시험	B4. Credit PSAM
기능시험	C8. BALPSAM증가
보안시험	C5. 서명S4생성
기능시험	B3. Complete Purchase 하이패스플러스
기능시험	A11. 거래내역저장
기능시험	B6. Complete Purchase PSAM
기능시험	C12. 개별거래내역저장
기능시험	B7. 개별거래내역저장

C10은 B5에 의해서 각각 검증되므로 시험할 필요가 없다. 따라서, 시험 순서에 따른 표준항목 및 선정기준은 다음 <표 4>와 같다:

〈표 4〉 H2P(표준SAM) 시험 순서에 따른 기준 및 표준 항목

시험기준	시험 표준항목
기능시험	B1. Initialize 하이패스플러스
보안시험	A3. 서명S1생성
기능시험	B2. Initialize PSAM
보안시험	C5. 서명S2생성
기능시험	B3. Purchase 하이패스플러스
기능시험	A7. BAL하이패스플러스차감
보안시험	A8. 서명S3생성
기능시험	B4. Credit PSAM
기능시험	C9. 개별거래내역저장
기능시험	B5. 개별거래내역저장

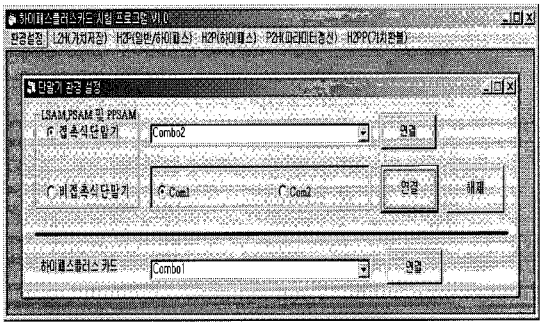
IV. 시험 모듈 개발

2장 및 3장에서 결정된 시험 방법 및 시험 표준 항목을 이용하여 PSAM을 시험하고 평가하기 위해

서 다음과 같은 시험 모듈을 개발하였다. 시험 모듈은 Visual Basic 6.0으로 개발했다.

1. 시험 환경설정 모듈

<그림 5>는 하이패스플러스카드를 시험하기 위해서 LSAM과 PSAM을 연결하기 위한 환경을 설정하기 위한 모듈이다. 하이패스플러스카드는 Combo1에 삽입하고, LSAM과 PSAM은 Combo2에 삽입하여 시험한다.



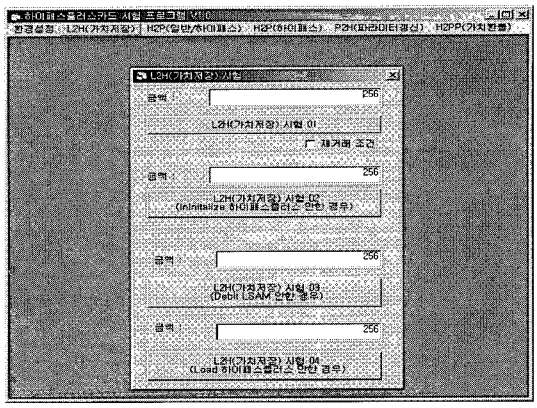
〈그림 5〉 하이패스플러스카드 시험환경

2. L2H(가치저장) 시험 모듈

LSAM에서 하이패스플러스카드에 가치를 저장하는 L2H(가치저장) 시험 모듈은 원하는 가치가 정상적으로 저장되는 지를 시험하기 위한 모듈이다. L2H(가치저장) 시험은 Initialize 하이패스플러스가 하이패스플러스카드에서 수행되고 이에 의해서 서명S1이 생성되며, Debit LSAM이 LSAM에 전달되고, BALLSAM이 원하는 가치만큼 감소되며, 서명S2가 생성되고, Load 하이패스플러스가 하이패스플러스카드에 전달되어 BAL하이패스플러스가 원하는 가치만큼 증가되며, 서명S3이 생성되는 지를 검사한다. <그림 6>은 LSAM에서 하이패스플러스카드에 가치를 저장하는 시험을 위해 구현한 모듈이다.

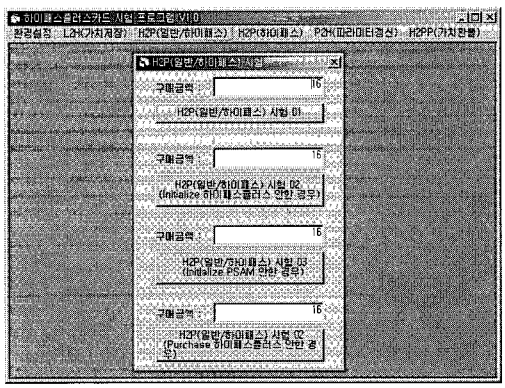
3. H2P(일반/하이패스) 시험 모듈

H2P(일반/하이패스) 시험 모듈은 하이패스플러스



〈그림 6〉 L2H(가치저장)시험 모듈

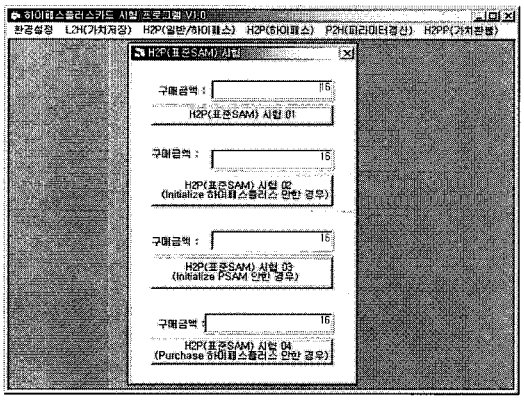
카드에서 PSAM에 지정된 가치가 지불되는 지를 시험하기 위한 모듈이다. 시험 모듈은 Initialize 하이패스플러스가 하이패스플러스카드에서 수행되고 서명S1이 생성되며, Initialize PSAM이 PSAM에 전달되고, 서명S2가 생성되고, Purchase 하이패스플러스가 하이패스플러스카드에 전달되어 BAL하이패스플러스가 지정된 가치만큼 감소되며, 서명S3가 생성되고, Credit PSAM이 PSAM에 전달되어 BALPSAM이 지정된 가치만큼 증가되며, 서명S4가 생성되고, Complete Purchase 하이패스플러스가 하이패스플러스카드에 전달되어 거래내역이 저장되고, Complete Purchase PSAM이 PSAM에 전달되어 개별거래내역이 저장되는 지를 검사한다. <그림 7>은 하이패스플러스카드의 가치를 PSAM에 지불하는 시험을 위해 구현한 모듈이다.



〈그림 7〉 H2P(일반/하이패스)시험 모듈

4. H2P(표준SAM) 시험 모듈

H2P(표준SAM) 시험 모듈은 하이패스플러스카드에서 PSAM에 지정된 가치가 지불되는 지를 시험하기 위한 모듈이다. 시험 모듈은 Initialize 하이패스플러스가 하이패스플러스카드에서 수행되고 서명S1이 생성되며, Initialize PSAM이 PSAM에 전달되고, 서명S2가 생성되고, Purchase 하이패스플러스가 하이패스플러스카드에 전달되어 BAL하이패스플러스가 지정된 가치만큼 감소되며, 서명S3가 생성되고, Credit PSAM이 PSAM에 전달되어 BALPSAM이 지정된 가치만큼 증가되며, 개별거래내역이 저장되는 지를 검사한다. <그림 8>는 하이패스플러스카드에서 PSAM에 가치를 지불하는 시험을 위해 구현한 모듈이다.



〈그림 8〉 H2P(표준SAM)시험 모듈

V. 시험 결과 및 분석, 평가

1. 시험 환경

하이패스플러스카드, LSAM, PSAM 및 PPSAM은 한국도로공사에 사용하는 카드를 이용하여 시험했다. 본 시험은 상온에서 시행한다. IV장에서 개발된 시험 모듈을 이용하여 다음과 같이 하이패스플러스카드를 시험하였다.

2. L2H(가치저장) 시험 결과 및 분석, 평가

1) L2H(가치저장) 시험 결과

L2H(가치저장) 시험 결과는 다음 <표 5>와 같다.

2) L2H(가치저장) 시험 분석 및 평가

저장하고자 하는 가치는 10진수로는 256DEC 또는 16진수로 100HEX이다. 가치저장전 LSAM 값은 16진수로 0FFFDC50HEX이며, 하이패스플러스카드의 값은 00000320HEX이다. 기능시험 B3. Initialize 하이패스플러스가 정상적으로 수행되었으며, 보안시험 A4. 서명S1생성에 의해서 서명S1의 16진수값 F4A87659HEX이 생성되었으며, 기능시험 B4. Debit-LSAM이 LSAM에 전달되고, 기능시험 C5. BAL-LSAM 차감에 의해서 예상되는 LSAM의 가치인 0FFFDB50HEX가 정상적으로 바뀌어야 한다. 보안시험 C7. 서명S2생성에 의해서 서명S2는 16진수값 B0D95A07가 생성되었다. 기능시험 B5. Load 하이패스플러스가 정상적으로 수행되었으며, 기능시험 A9. BAL하이패스플러스 증가에 의해서 BAL하이패스플러스이 00000320HEX에서 00000420HEX으로 증가하였다. 보안시험 A10. 서명S3생성에 의해서 서명 S3의 16진수값 A605231C이 생성되었다. 또한, B3, B4, B5가 잘못된 경우에는 실행이 중단되었다. 따라서, L2H(가치저장) 시험이 정상적으로 이루어졌고, 한국도로공사에서 사용하는 하이패스플러스카드는 L2H(가치저장) 시험을 통과하였다.

3. H2P(일반/하이패스) 시험 결과 및 분석, 평가

1) H2P(일반/하이패스) 시험 결과

H2P(일반/하이패스) 시험 결과는 다음 <표 6>과 같다.

2) H2P(일반/하이패스) 시험 분석 및 평가

지불 금액은 10진수 16DEC이고 16진수로는 10HEX인 값을 지불하고자 한다. B1. Initialize 하이패

〈표 5〉 L2H(가치저장) 시험 결과

시험절차	시험 표준항목	예상SW	예상결과	측정SW	측정결과
가정	가치저장전 금액(LSAM)	0FFFDC50			
	가치저장전 금액(하이패스플러스)	00000320			
기능시험	B3. Initialize 하이패스플러스	9000	NT하이패스플러스(4) R하이패스플러스(8)	9000	00000092 95682235849FC2AC
보안시험	A4. 서명S1생성	9000	S1(4)	9000	F4A87659
기능시험	B4. Debit LSAM	9000		9000	
기능시험	C5. BALLSAM 차감	9000	가치저장후 금액	9000	0FFFDB50
보안시험	C7. 서명S2생성	9000	S2(4)	9000	B0D95A07
기능시험	B5. Load 하이패스플러스	9000		9000	
기능시험	A9. BAL하이패스플러스 증가	9000	00000420	9000	00000420
보안시험	A10. 서명S3생성	9000	S3(4)	9000	A605231C
기능시험	B7. 저장	9000		9000	

〈표 6〉 H2P(일반/하이패스) 시험 결과

시험절차	시험 표준항목	예상SW	예상결과	결과SW	측정결과
가정	가치저장전금액(하이패스플러스카드) NTPSAM 가치저장전금액(PSAM)		000004E0 00000067 00001118		
기능시험	B1. Initialize 하이패스플러스	9000	NT하이패스플러스(4) R하이패스플러스(8)	9000	000000A8 F4AC4A095F37CD96
보안시험	A3. 서명S1생성	9000	S1(4)	9000	4A171968
기능시험	B2. Initialize PSAM	9000		9000	
보안시험	C5. 서명S2생성	9000	S2(4)	9000	D78C992C
기능시험	B3. Purchase 하이패스플러스	9000		9000	
기능시험	A7. BAL하이패스플러스 감소	9000	000004D0	9000	000004D0
보안시험	C5. 서명S3생성	9000	S3(4)	9000	A7B69A33
기능시험	B4. Credit PSAM	9000		9000	
기능시험	NTPSAM C8. BALPSAM증가	9000	00000068 00001128	9000	00000068 00001128
보안시험	C5. 서명S4생성	9000	S4(4)	9000	C1C14425
기능시험	B5. Complete Purchase 하이패스플러스	9000		9000	
기능시험	A11. 거래내역저장	9000		9000	
기능시험	B6. Complete Purchase PSAM	9000		9000	
기능시험	C12. 개별거래내역저장	9000		9000	
기능시험	B7. 개별거래내역저장	9000		9000	

스플러스를 실행한 결과, NT하이패스플러스(4)는 000000A8HEX, R하이패스플러스(8)는 F4AC4A095 F37CD96HEX, 그리고 BAL하이패스플러스(4)는 000 004E0HEX이다. 따라서, 시험 결과 후, 가치지불 후 금액인 BAL하이패스플러스(4)는 000004D0HEX이 되어야 한다. 하이패스플러스카드는 서명 S1이 4A 171968HEX인 16진수값을 생성하였고, B2.Initi alize-PSAM을 실행한 결과, NTPSAM은 00000067 HEX이고, PSAM의 가치저장 전 금액인 BALPSAM은 00001118HEX였다. 따라서, 시험 결과 후, NTPSAM

은 00000068HEX이고, PSAM의 가치저장 후 금액인 BALPSAM은 00001128HEX이 되어야 한다. B3.Purchase 하이패스플러스를 실행하고, A7. BAL하이패스플러스 감소를 실행한 결과, BAL하이패스플러스(4)는 000004D0HEX이 되어서, 예상한 결과와 일치하였다. 서명 S3은 A7B69A33HEX이 생성되었다. B4.Credit PSAM 및 C8. BALPSAM증가 시험 결과, NTPSAM은 00000068HEX이고, PSAM의 가치저장 후 금액인 BALPSAM은 00001128HEX이 되어서 예상 결과와 일치하였다. 나머지, 항목들도 시험 예상 결과와 일치하였다. 또한, B1, B2, B3, B4, B5 그리고 B6을 실행하지 못한 경우에는 시험이 중단되어서 원하는 결과와 일치하였다. 따라서, H2P(일반/하이패스) 시험이 정상적으로 이루어졌고, 한국도로공사에서 사용하는 하이패스플러스카드는 H2P (일반/하이패스) 시험을 통과하였다.

4. H2P(표준SAM) 시험 결과 및 분석, 평가

1) H2P(표준SAM) 시험 결과

H2P(표준SAM) 시험 결과는 다음 <표 7>과 같다.

2) H2P(표준SAM) 시험 분석 및 평가

지불 금액은 10진수 16DEC이고 16진수로는 10EX인 값을 지불하고자 한다. B1.Initialize 하이패스플러스를 실행한 결과, 하이패스플러스카드의 NT하이패스플러스(4)는 000000AEHEX이고, BAL하이패스플러스(4)는 000004A0HEX이다. 따라서, 시험을 종료한 후의 NT하이패스플러스(4)는 000000 AFHEX이고, BAL하이패스플러스(4)는 000004B0HEX이 되어야한다. A3. 서명S1의 값은 AB8B81B0HEX이 생성되었다. B2. Initialize PSAM을 실행한 결과, NTPSAM은 0000006BHEX이고, PSAM의 가치저장 전 금액은 00001158HEX이었다. 따라서, 시험이 종료된 후의 NTPSAM은 0000006CHEX이고, PSAM의 가치저장 전 금액은 00001168HEX이 되어야 한다.

C5. 서명S2은 57E5656BHEX이 생성되었고, NTPSAM은 0000006CHEX이고, PSAM의 가치저장 전 금액은 00001168HEX이 되어서, 예상한 결과와 일치하였다. A7. BAL하이패스플러스차감 결과, NT하이패스플러스(4)는 000000AFHEX이 되었고, BAL하이패스플러스(4)은 000004B0HEX이 되어서 예상한 결과와 일치하였다. A8. 서명S3은 846843F0이 생성되었

<표 7> H2P(표준SAM) 시험 결과

시험절차	시험 표준항목	예상SW	예상결과	결과SW	측정결과
가정	가치저장전금액(하이패스플러스카드) NT_{PSAM} 가치저장전금액(PSAM)		000004**A0** 0000006**B** 00001158		
기능시험	B1. Initialize 하이패스플러스	9000	$NT_{하이패스플러스(4)}$ $BAL_{하이패스플러스(4)}$	9000	000000AE 000004A0
보안시험	A3. 서명S1생성	9000	S1(4)	9000	AB8B81B0
기능시험	B2. Initialize PSAM	9000		9000	
보안시험	C5. 서명S2생성	9000	S2(4)	9000	57E5656B
기능시험	NT_{PSAM} B3. Purchase 하이패스플러스	9000	0000006C 00001168	9000	0000006**C** 00001168
기능시험	A7. $BAL_{하이패스플러스}$차감	9000	$NT_{하이패스플러스(4)}$:000000AF $BAL_{하이패스플러스(4)}$:000004B0	9000	$NT_{하이패스플러스(4)}$:000000**AF** $BAL_{하이패스플러스(4)}$:000004**B0**
보안시험	A8. 서명S3생성	9000	S3(4)	9000	846843F0
기능시험	B4. Credit PSAM	9000		9000	
기능시험	C9. 개별거래내역저장	9000		9000	
기능시험	B5. 개별거래내역저장	9000		9000	

다. 또한, B1, B2, B3, 그리고 B4를 실행하지 못한 경우에는 시험이 중단되어서 원하는 결과와 일치하였다. 따라서, H2P(표준SAM) 시험이 정상적으로 이루어졌고, 한국도로공사에서 사용하는 하이패스플러스카드는 H2P(표준SAM) 시험을 통과하였다.

VI. 결론

본 논문에서 제시한 하이패스플러스카드의 시험 방법 및 절차는 한국도로공사 규격서 및 국제 표준에 의거하여 개발하였으며, 한국도로공사에서 사용중인 하이패스플러스카드를 시험하였다. 하이패스플러스카드는 한국도로공사 전자지불시스템에서 사용되는 매우 중요한 요소이므로 하이패스플러스카드의 기능뿐 아니라 보안성의 시험 인증은 매우 중요한 의미를 갖는다. 따라서, 본 시험에서 제시한 방법 및 절차에 의거한 하이패스플러스카드의 시험은 한국도로공사 전자지불시스템의 적합성 및 안정성, 품질 향상을 증가시킬 수 있다. 본 논문에서 제시한 시험 표준항목의 선정은 국제 표준 및 한국도로공사의 규격서에 의해서 이루어졌다. 시험 방법 및 절차는 국내 표준 및 국제 표준 시험 방법을 적용하여 연구되었다.

본 논문에서 실행한 하이패스플러스카드 시험은 국내에서는 최초로 수행된 연구이므로, 앞으로도 많은 연구 및 수정이 필요하다. 특히, 보다 체계적인 시험을 위해서는 시험 절차 및 방법에 관한 표준화 연구가 더욱 필요다. 또한, 시험 결과를 인증하는 기준 및 절차에 관한 연구도 필요하다.

참 고 문 헌

[1] 한국전자지불포럼단체표준, 비접촉식 전자화폐 판독기용 지불SAM 규격(개정용-Issue 2.0), 2003.8.

[2] http://www.sc17.com, ISO/IEC JTC1/SC17 N2183.

[3] ISO/IEC 10373-1, Identification cards-Test methods - Part 1 : General characteristics tests, 1998.12.

[4] ISO/IEC 10373-3, Identification cards-Test methods - Integrated circuit(s) cards - Part 3 : Integrated circuit(s) cards with contacts, 2001.2.

[5] ISO/IEC 10373-6, Test methods-Proximity card, 2001.5.

[6] ISO/IEC 10373-6/AM1, Test methods-Proximity card- Amendment 1 : Additional PICC test methods, 2002.7.

[7] ISO/IEC 10373-6/AM1, Test methods-Proximity card- Amendment 2 : Improved RF test methods, 2002.7.

[8] ISO/IEC 10373-7, Test methods-Vicinity cards, 2001.5.

[9] ISO/IEC 10373-6, Identification cards- Contactless integrated circuit(s) cards- Part2 : Dimensions and location of coupling areas,1995.12.

[10] Wrankl & Effing, Translated by Kenneth Cox, "Smart card HandBook second edition", John wiely&Sons, 2000.

[11] 임낙희, 신규평가대상제품확대추진계획, 정보통신부, 2003.9.

[12] 김재성, 평가대상제품평가준비지원방안, 한국정보보호진흥원, 2003.9.

[13] 이태승, 신규평가대상제품평가방안, 한국정보보호진흥원, 2003.9.

[14] 산업자원부 기술표준원, 2003년 산업용 소프트웨어 국제표준 적합성 시범인증 설명회, 2003.3.

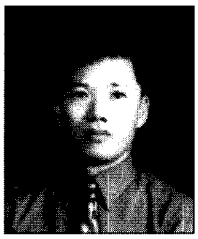
[15] 한국도로공사, 도로공사 전자카드 시험인증 규격서 V1.1, 2003.12.

[16] 한국도로공사, 도로공사 전자카드 규격서 V1.1, 2003.12.

〈저자소개〉

이 기 한 (Ki-Han, Lee)

1987년 서강대학교 컴퓨터 공학과 졸업 (학사)
1989년 서울대학교 대학원 컴퓨터공학과 (공학석사)
1993년 서울대학교 대학원 컴퓨터공학과 (공학박사)
1995년~1999년 : 서울여자대학교 컴퓨터학과 조교수
1999년~현재 : 서울여자대학교 컴퓨터학과 부교수
1998년~현재 : ISO/TC215 건강카드 대표위원
2001년~현재 : ISO/SC27 보안 전문위원
2002년~현재 : ISO/SC17 스마트카드 전문위원
<관심분야> 스마트카드, 보안, 의료 정보, Bio-infomatics



이 대 규 (Dae-Kyu, Lee)

1992. 2 : 한양대학교 전자공학과 학사
1998. 9 : 한국도로기술대학원 정보통신공학과 석사
1994. 7~현재 : 한국도로공사 스마트웨이사업팀 대리

여 운 상 (WoonSang, Yeo)

1984. 2 : 전남대학교 경영학과 학사
1998. 9 : 한양대 산업경영대학원 교통공학과 석사
1987. 1~현재 : 한국도로공사 스마트웨이사업팀 부장

이 승 환 (Seung-Hwan, Lee)

Polytech University 교통공학 박사
아주대학교 환경건설교통공학부 교수
아주대학교 ITS대학원 대학원장
현 한국ITS학회 회장