한국ITS학회논문지
제2권, 제2호 (2003. 9 · 12)
pp.73~84

하이패스플러스카드 시스템을 위한 PSAM 시험 모듈 개발

Developing the Test Module of PSAM for Hipass^{PLUS} Card System

이 기 한* (Ki-Han, Lee) 서 현 교** (Hyun Kyo, Suh) 유 창 희*** (Chang Hee, Yoo) 이 승 환**** (Seung-Hwan, Lee)

요 약

한국도로공사는 기존 선불형 플라스틱카드에 문제가 많아서 이를 해결하기 위해서 하이패스플러스 카드인 스마트카드를 이용한 선불형 전자지불카드 시스템을 구현했다. 이 시스템에는 선불형 전자지불카드인 하이패스플러스카드로부터 가치를 지불 받을 수 있는 스마트카드인 PSAM이 필요하다. 그리고, PSAM은 PSAM에 저장된 거래내역을 정산하기 위해서 CSAM에 전달하여야 한다. 따라서, PSAM의 기능 및 보안이 완벽해야 한국도로공사의 전자지불시스템이 안전하다. 본 논문은 일반 가맹점, 하이패스, 또는 표준 SAM 기능에 의해서 하이패스플러스카드의 가치가 PSAM으로 지불되거나 PSAM에 저장된 거래내역을 CSAM에 전달하는 기능 및 보안성을 시험하기 위해서 시험 방법, 시험 표준항목, 그리고 시험 절차 등을 포함한 시험 모듈을 개발했다. 시험 모듈은 시험 검사표에 의한 시험 표준항목을 시험할 수 있는 방법 및 절차를 따라서 개발했다. PSAM의 시험 표준항목 및 시험 검사표는 한국도로공사 규격서에 준하여 ISO 표준에 적합한 시험 항목으로 선정했다. 시험은 한국도로공사에서 사용되는 PSAM을 이용하여 실행하였다. 본 시험 모듈은 PSAM의 기능뿐 아니라 보안성 및 적합성을 시험하였다. 시험 결과에 의하면, 한국도로공사에서 사용하는 PSAM은 기능 및 보안성이 시험인증 기준을 통과하였다.

Abstract

Due to the problems of existing prepaid plastic card issued by Korea Highway Company, the prepaid electronic payment system using a smart card, called HipassPLUS Card, was developed to overcome the problems. PSAM is one of the main component of the system, which can retrieve the value from HipassPLUS card, transmit the transaction data to CSAM, and store the accumulated account lists. For the safety of the electronic payment system, the functions of PSAM should be faultless. This paper developed a test module including the test method, the test checklist, and the test procedure. The test module examines the functionality and security of the payment mechanism to insure that the value stored in HipassPLUS card can be paid to PSAM by the merchants and the standardized SAM. The test module also inspects the transmission mechanism to send and store the transaction data from PSAM to CSAM correctly and safely. The module is designed to test the standard items using the test checklists for PSAM. The test items and the test checklists of PSAM was selected under the provision of the specification of Korea Highway Company and ISO standard. The evaluation on PSAM using the test module indicates that PSAM satisfies the evaluation criteria on the quality characteristics of the functionality, security, and compatibility.

Key Words : PSAM, HipassPLUS Card, LSAM, Test module, Function test, Security test

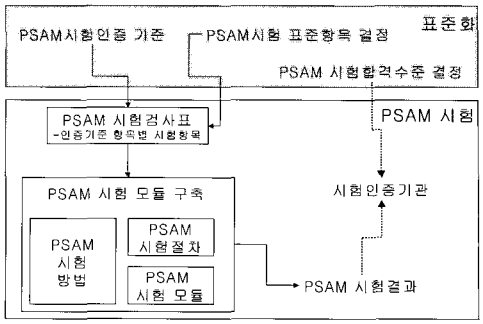
* 회 원 : 서울여자대학교 컴퓨터학과 부교수
** 비회원 : 한국도로공사 스마트웨이사업팀
*** 비회원 : 한국도로공사 스마트웨이사업팀 과장
**** 회 원 : 아주대학교 환경건설교통공학부 교수
† 논문접수일 : 2003년 8월 27일
¶ 본 논문은 2004년도 서울여자대학교 교내연구비의 지원으로 수행되었음.

Ⅰ. 서 론

한국도로공사에서 선불방식의 플라스틱 카드를 없애고, 스마트 칩이 내장된 스마트카드를 이용하여 선불식 전자지불 시스템을 구축하고 있다. 스마트카드에 의한 전자지불카드인 하이패스플러스카드를 이용하여 전자지불을 할 경우에, 하이패스플러스카드의 금액이 PSAM으로 지불되어야 한다. 따라서, PSAM은 하이패스플러스카드에 가치를 지불할 수 있는 스마트카드로서, 매우 중요한 스마트카드이다. PSAM이 정확하게 동작을 하지 않으면, 가치 지불에 많은 문제를 야기할 수 있다. PSAM은 한국형 전자지불 표준SAM과의 지불거래기능이 구현되어있어서 서울시를 비롯한 모든 카드와도 호환이 가능하다[1]. 그러므로, PSAM의 기능 및 보안성을 정확하게 시험 평가를 하는 것은 그 의미가 매우 크다고 본다[2].

스마트카드 시험에 관한 국제 표준은 ISO 10373에 규정하고 있다[3]. 스마트카드의 국제표준 시험인증은 일반적인 특성에 관한 시험[4]과 접촉식 스마트카드의 시험인증[5]으로 구분된다. 보안 분야는 국제적으로 CC/PP 시험인증과 국내에서는 정보화촉진기본법 제15조에 의한다[6,7]. 스마트카드를 시험하는 기구는 한국에서는 보안 및 기능에 관련되어서는 한국기술표준원이 ISO를 인증한 전자카드 품질인증원과 한국정보보호진흥원이 있다[8].

PSAM은 하이패스플러스카드에 의해서 가치를 지불받고, CSAM에 거래내역을 전달하는 방식이다. 따라서, PSAM의 기능 시험인증은 하이패스플러스카드 및 CSAM과의 기능을 시험하는 것이다. PSAM을 시험하기 위한 전체적인 시험 절차는 <그림 1>과 같다[2,7,9,10]. PSAM을 시험 평가하기 위해서 본 논문에서는 먼저, 시험 종류 및 방법을 정했고, 시험 방법에 맞는 시험 표준항목을 선정하였으며, 선정된 시험 표준항목을 평가하기 위한 시험 절차 및 모듈을 개발하였다. 이렇게 정해진 모듈에 의해서 실제 개발된 PSAM을 시험하고 이를 분석하여 PSAM이 원하는 기준을 통과하여 정확하게 동작하는 지를 분석했다.



〈그림 1〉 시험 절차 구성

〈표 1〉 PSAM 시험 종류

대 분 류	중 분 류	소분류 : 시험명
CSAM과의 시험	거래수집 시험	: P2C(거래수집)
하이패스플러스 카드와의 시험	지불거래 시험	일반/하이패스 지불거래 시험 : H2P(일반/하이패스)
		표준SAM 지불거래 시험 : H2P(표준SAM)
보안 시험	서명 확인 시험	
	암호화 시험	

Ⅱ. 시험 종류 및 방법

PSAM 시험은 <표 1>과 같이 PSAM과 CSAM간의 시험과 PSAM과 하이패스플러스 카드간의 시험으로 구분한다. 보안 시험은 각 시험 중에 실행한다.

1. P2C(거래수집) 시험 방법

거래수집은 <그림 2>와 같이 PSAM으로부터 CSAM으로 이루어지므로, P2C(거래수집) 시험은 PSAM과 CSAM사이에서의 거래 수집에 대한 시험을 한다[11]. 이 거래를 통해 PSAM에 저장된 총액과 개별구매거래내역이 전송되며, 전송이 완료되면 PSAM은 개별구매거래내역을 삭제한다.

PSAM의 거래내역이 CSAM에 전달되어 저장되는지를 시험하는 P2C(거래수집) 시험은 B1, B2, B3, A4, B4, C8, B5, A9, B6 순으로 시험하고, PSAM과 CSAM간에 거래내역을 전달하는 동안에 정확하게 정보를 전달되는 지를 시험하는 서명확인시험은 C5,

PSAM	PDA	CSAM
	<- B1. Initialize PSAM	
A1. 응답		
	<- B2. Initialize CSAM	
		C1. 난수생성 (R) C2. 조건확인 C3. $KDCOMP_{CSAM}$ 생성**(암호화)** C4. KSESCSAM 생성**(암호화)** C5. 서명S1 생성**(서명확인)** C6. 응답
	<- B3. Total Collect PSAM	
A2. $KSES_{PSAM}$ 생성**(암호화)** A3. 서명S1검증**(서명확인)** A4. 거래내역생성 A5. 서명S2 생성**(서명확인)** A6. 응답		
	B4. Collect to CSAM ->	
		C7. 서명S2검증**(서명확인)** C8. 거래내역저장 C9. 서명S3 생성**(서명확인)** C10. 응답
	<- B5. Complete Collect PSAM	
A7. 서명S3검증**(서명확인)** A8. 서명S4생성**(서명확인)** A9. 거래내역저장 A10. Erase Total(TMPP) A11. 응답		
	B6. Complete CSAM ->	
		C11. 서명S4검증**(서명확인)** C12. 응답

〈그림 2〉 PSAM과 CSAM의 거래수집 흐름도

A3, A5, C7, C9, A7, A8, C11 순으로 시험하며, PSAM과 CSAM간에 거래내역을 전달하는 동안에 전달되는 정보가 정확하게 암호화 및 복호화가 이루어지는 지를 시험하는 암호화시험은 C3, C4, A2 순으로 시험한다.

2. H2P(일반/하이패스)

H2P(일반/하이패스)은 PSAM과 하이패스플러스 카드가 상호 인증한 후, 선택한 금액만큼 하이패스플러스 카드에서 PSAM으로 전자적 가치가 이전되는 <그림 3>과 같은 과정을 시험한다[11]. 일반/하이패스 지불거래는 T-DES_F를 사용한다.

하이패스플러스 카드의 가치가 PSAM에 정확하게 저장되는 지를 시험하는 H2P(일반/하이패스) 시험은 B1, A1, A4, B2, C1, C6, B3, A7, A9, B4, C8, C10, B5, A11, A12, B6, C12, C13, B7 순으로 시험하고, 하이패스플러스 카드와 PSAM간에 가치를 저장하는 동안에 정확하게 정보를 전달되는 지를 시험하는 서명확인시험은 A3, C3, C5, A6, A8, C7, C9, A10, C11 순으로 시험하며, 하이패스플러스 카드와 PSAM간에 가치를 저장하는 동안에 전달하는 정보가 정확하게 암호화 및 복호화가 이루어지는 지를 시험하는 암호화시험은 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. KDCSAM 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 PSAMB6. Com plete CSAM ->	
		C11. 서명S4검증(**서명확인**) C12. 개별거래내역저장 C13. 응답
	B7. 개별거래내역저장 ->	

〈그림 3〉 PSAM과 하이패스플러스 카드의 일반/하이패스지불거래 흐름도

3. H2P(표준SAM)

H2P(표준SAM)은 <그림 4>와 같이 비접촉식 교통 표준SAM과의 거래를 시험한다. 표준SAM 지불거래는 다른 지불거래와 같이 취소 거래도 가능하지만 T-DES를 사용한다[11].

하이패스플러스 카드의 가치가 PSAM에 정확하게 저장되는 지를 시험하는 H2P(표준SAM) 시험은 B1, A1, A4, B2, C1, C6, B3, A7, A9, B4, C8, C9, C10, B5 순으로 시험하고, 하이패스플러스 카드와 PSAM간에 가치를 저장하는 동안에 정확하게 정보를 전달되는 지를 시험하는 서명확인시험은 A3, C3, C5, A6, A8, C7 순으로 시험하며, 하이패스플러스 카드와 PSAM간에 가치를 저장하는 동안에 전달하는 정보가 정확하게 암호화 및 복호화가 이루어지는 지를 시험하는 암호화시험은 A2, C2, C4, A5 순으로 시험한다.

하이패스플러스	PDA	PSAM
	<- B1. Initialize 하이패스플러스	
A1. 조건확인 A2. KSES하이패스플러스 생성(암호화) A3. 서명S1생성(서명확인) A4. 응답		
	<- B2. Initialize PSAM	
		C1. 조건확인 C2. KDCSAM 생성(암호화) C3. 서명S1검증(서명확인) C4. KSESPSAM 생성(암호화) C5. 서명 S2생성(서명확인) C6. 응답
	<- B3. Purchase 하이패스플러스	
A5. KSES하이패스플러스 생성(암호화) A6. 서명S2검증(서명확인) A7. BAL하이패스플러스차감 A8. 서명S3생성(서명확인) A9. 응답		
	B4. Credit PSAM ->	
		C7. 서명S3검증(서명확인) C8. BALPSAM증가 C9. 서명S4생성(서명확인) C10. 응답
	<- B5. 개별거래내역저장	

〈그림 4〉 PSAM과 하이패스플러스 카드의 표준SAM 지불거래 흐름도

III. 시험 표준항목 선정

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

1. P2C(거래수집) 시험 표준항목

<그림 2>에서 P2C(거래수집) 시험은 A1부터 A11, B1부터 B6, 그리고 C1부터 C12까지의 모든 항목에 걸쳐서 이루어진다. 하지만, 이 모든 과정 중에서 A1은 B2에 의해서 검증되고, A2는 A3에 의해서 검증되고, A6은 B4에 의해서 검증되고, A7은 A8에 의해서 검증되며, A11은 B6에 의해서 검증되므로 시험할 필요가 없다. C1과 C2, 그리고 C3는 C4에 의해서 검증되고, C6은 B3에 의해서 검증되고, C10은 B5에 의해서 검증되고, C12은 종료이므로 시험할 필요가 없다. 따라서, 시험 순서에 따른 표준항목 및 선정기준은 다음 <표 2>와 같다[10,11].

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 없

다. 따라서, 시험 순서에 따른 표준항목 및 선정기준은 다음 <표 3>과 같다[10,11].

〈표 2〉 P2C(거래수집) 시험 순서에 따른 기준 및 표준항목

시험기준	시험 표준항목
기능시험	B1. Initialize PSAM
기능시험	B2. Initialize CSAM
보안시험	C5. 서명S1생성
기능시험	B3. Total Collect PSAM
기능시험	A4. 거래내역생성
보안시험	A5. 서명S2생성
기능시험	B4. Collect to CSAM
기능시험	C8. 거래내역저장
보안시험	C9. 서명S3생성
기능시험	B5. Complete Collect PSAM
보안시험	A8. 서명S4생성
기능시험	A9. 거래내역저장
기능시험	A10. Erase Total(TMPP)
기능시험	B6. Complete CSAM

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

시험기준	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

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, C10은 B5에 의해서 각각 검증되므로 시험할 필요가 없다. 따라서, 시험 순서에 따른 표준항목 및 선정기준은 다음 <표 4>와 같다[10,11].

〈표 4〉 H2P(표준SAM) 시험 순서에 따른 기준 및 표준항목

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

IV. 시험 모듈 개발

II.장 및 III.장에서 결정된 시험 방법 및 시험 표준항목을 이용하여 PSAM을 시험하고 평가하기 위해서 다음과 같은 시험 모듈을 개발하였다. 시험 모듈은 Visual Basic 6.0으로 개발했다.

1. 시험 환경설정 모듈

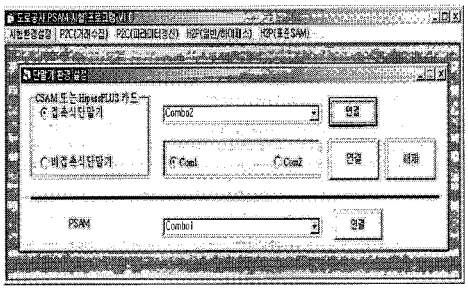
<그림 5>는 PSAM을 시험하기 위해서 PSAM과 CSAM 및 하이패스플러스 카드를 연결하기 위한 환경을 설정하기 위한 모듈이다. PSAM은 Combo1에 삽입하고, CSAM 및 하이패스플러스 카드는 Combo2에 삽입하여 시험한다.

2. P2C(거래수집) 시험 모듈

1) P2C(거래수집) 시험 절차

PSAM에서 CSAM으로 거래내역을 전달하는 시험 모듈은 원하는 거래내역이 정상적으로 전달되는 지

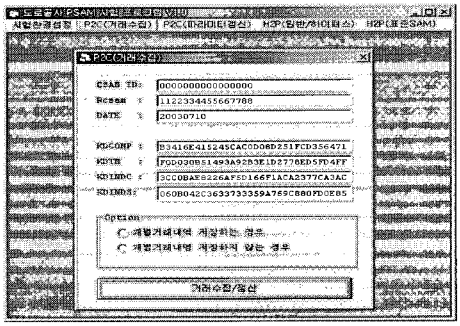
를 시험하기 위한 모듈이다. 시험 절차는 <그림 2>와 같이 Initialize PSAM이 PSAM에서 수행되고, Initialize CSAM이 CSAM에서 수행되어 서명S1이 생성되며, Total Collect PSAM이 PSAM에서 수행되어 거래내역이 생성되고 서명S2가 생성되며, Collect to CSAM이 CSAM에서 수행되어 거래내역이 저장되고 서명 S3이 생성되며, Complete Collect PSAM이 PSAM에서 수행되어 서명 S4가 생성되고 거래내역이 저장되고 모든 거래내역이 삭제되며, Complete CSAM이 CSAM에서 처리되는 과정을 시험한다.



〈그림 5〉 시험 환경설정 모듈

2) P2C(거래수집) 시험 모듈

<그림 6>은 CSAM에서 PSAM의 거래내역을 저장하는 시험을 위해 구현한 모듈이다.



〈그림 6〉 P2C(거래수집) 시험 모듈

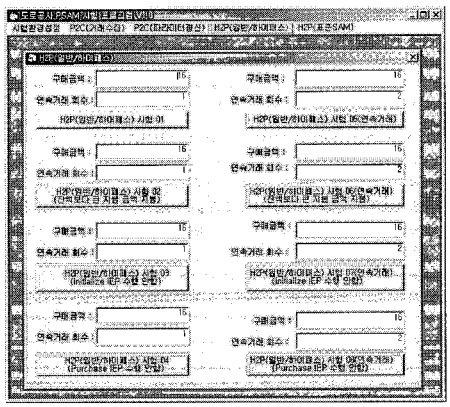
3. H2P(일반/하이패스) 시험 모듈

1) H2P(일반/하이패스) 시험 절차

H2P(일반/하이패스) 시험 모듈은 하이패스플러스 카드에서 PSAM에 지정된 가치가 지불되는 지를 시험하기 위한 모듈이다. 시험 절차는 Initialize 하이패스플러스 가 하이패스플러스 카드에서 수행되고 서명S1이 생성되며, Initialize PSAM이 PSAM에 전달되고, 서명S2가 생성되고, Purchase 하이패스플러스 가 하이패스플러스 카드에 전달되어 BAL하이패스플러스가 지정된 가치만큼 감소되며, 서명S3가 생성되고, Credit PSAM이 PSAM에 전달되어 BALPSAM이 지정된 가치만큼 증가되며, 서명S4가 생성되고, Complete Purchase 하이패스플러스 가 하이패스플러스 카드에 전달되어 거래내역이 저장되고, Complete Purchase PSAM이 PSAM에 전달되어 개별 거래내역이 저장되는 지를 검사한다.

2) H2P(일반/하이패스) 시험 모듈

<그림 7>은 PSAM의 파라미터를 CSAM에 의해서 갱신하는 시험을 위해 구현한 모듈이다.



〈그림 7〉 H2P(일반/하이패스)시험 모듈

4. H2P(표준SAM) 시험 모듈

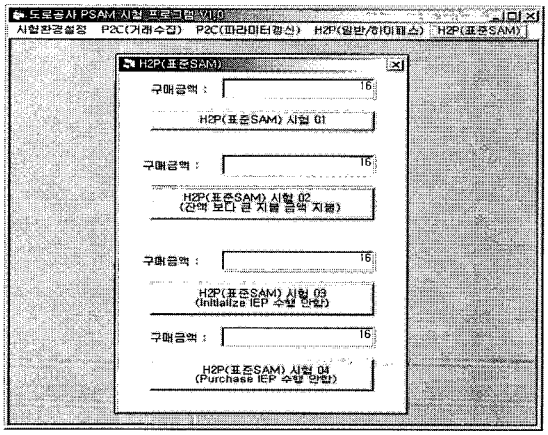
1) H2P(표준SAM) 시험 절차

H2P(표준SAM) 시험 모듈은 하이패스플러스 카드에서 PSAM에 지정된 가치가 지불되는 지를 시험하기 위한 모듈이다. 시험 절차는 Initialize 하이패스플러스 가 하이패스플러스 카드에서 수행되고 서명S1이 생성되며, Initialize PSAM이 PSAM에 전달

되고, 서명S2가 생성되고, Purchase 하이패스플러스가 하이패스플러스 카드에 전달되어 BAL하이패스플러스가 지정된 가치만큼 감소되며, 서명S3가 생성되고, Credit PSAM이 PSAM에 전달되어 BALP SAM이 지정된 가치만큼 증가되며, 개별거래내역이 저장되는 지를 검사한다.

2) H2P(표준SAM) 시험 모듈

<그림 8>은 PSAM에서 하이패스플러스 카드에 가치를 저장하는 시험을 위해 구현한 모듈이다.



〈그림 8〉 H2P(표준SAM)시험 모듈

V. 시험 결과 및 분석, 평가

1. 시험 환경

CSAM과 하이패스플러스 카드, PSAM은 한국도로공사에 납품하는 H 회사에서 개발한 카드를 이용하여 시험했다. 본 시험은 상온에서 시행한다. IV장에서 개발된 시험 모듈을 이용하여 다음과 같이 PSAM을 시험하였다.

2. P2C(거래수집) 시험 결과 및 분석, 평가

1) P2C(거래수집) 시험 결과

P2C(거래수집) 시험 결과는 다음 <표 5>와 같다.

2) P2C(거래수집) 시험 분석 및 평가

기능시험 B1. Initialize PSAM이 정상적으로 수행되었으며, 기능시험 B2. Initialize CSAM이 정상적으로 수행되었다. 보안시험 C5. 서명S1생성에 의해서 서명 S1의 값 9AF234DFHEX이 생성되었다. 기능시험 B3. Total Collect PSAM 및 기능시험 A4. 거래내역생성이 정상적으로 수행되었다. 보안시험 A5. 서명S2생성에 의해서 서명S2값 6071E9AAHEX이 생

〈표 5〉 P2C(거래수집) 시험 결과

시험절차	시험 표준항목	예상SW	예상결과	결과SW	측정결과
기능시험	B1. Initialize PSAM	9000		9000	
기능시험	B2. Initialize CSAM	9000		9000	
보안시험	C5. 서명S1생성	9000		9000	9AF234DF
기능시험	B3. Total Collect PSAM	9000		9000	
기능시험	A4. 거래내역생성	9000		9000	
보안시험	A5. 서명S2생성	9000		9000	6071E9AA
기능시험	B4. Collect to CSAM	9000		9000	
기능시험	C8. 거래내역저장	9000		9000	
보안시험	C9. 서명S3생성	9000		9000	63DB2EBE
기능시험	B5. Complete Collect PSAM	9000		9000	
보안시험	A8. 서명S4생성	9000		9000	6267B24C4
기능시험	A9. 거래내역저장	9000		9000	
기능시험	A10. Erase Total(TMPP)	9000		9000	
기능시험	B6. Complete CSAM	9000		9000	

성되었다. 기능시험 B4. Collect to CSAM 및 기능시험 C8. 거래내역저장이 정상적으로 수행되었다. 보안시험 C9. 서명S3생성에 의해서 서명S3값 63DB2EBEHEX이 생성되었다. 기능시험 B5. Complete Collect PSAM이 정상적으로 수행되었다. 보안시험 A8. 서명S4생성에 의해서 서명S4값 6267B24C4HEX이 생성되었다. 기능시험 A9. 거래내역저장, 기능시험 A10. Erase Total(TMPP) 및 기능시험 B6. Complete CSAM이 정상적으로 수행되었다. 또한, 기능시험 B1. Initialize PSAM, 기능시험 B2. Initialize CSAM, 기능시험 B3. Total Collect PSAM, 기능시험 B4. Collect to CSAM, 기능시험 B5. Complete Collect PSAM, 그리고 기능시험 B6. Complete CSAM이 실행되지 않은 경우에는 실행을 중단하였다. 따라서, P2C(거래수집) 시험이 정상적으로 이루어졌고, 한국도로공사에서 사용하는 PSAM은 P2C(거래수집) 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 하이패스플러스를 실행한 결과, R하이패스플러스는 F72 DD067E8342ED2HEX, 그리고 BAL하이패스플러스는 00000520HEX이다. 따라서, 시험 결과 후, 가치지불 후 금액인 BAL하이패스플러스는 00000510 HEX이 되어야 한다. 하이패스플러스카드는 서명 S1이 C24FDA26HEX인 16진수값을 생성하였고, B2. Initialize PSAM을 실행한 결과, PSAM의 가치저장 전 금액인 BALPSAM은 0000009AHEX였다. 따라서, 시험 결과 후, PSAM의 가치저장 후 금액인 BALP SAM은 000000AAHEX이 되어야 한다. C5. 서명S2생성에 의해서 서명S2는 D9CBE586HEX이 생성되었다. B3.Purchase 하이패스플러스를 실행하고, A7. BAL하이패스플러스 감소를 실행한 결과, BAL하이패스플러스는 00000510HEX이 되어서, 예상한 결과와 일치하였다. 서명 S3은 6197A09EHEX이 생성되었다. B4. Credit PSAM 및 C8. BALPSAM증가 시험 결과, PSAM의 가치저장 후 금액인 BALPSAM은 000000 AAHEX이 되

〈표 6〉 H2P(일반/하이패스) 시험 결과

시험절차	시험 표준항목	예상SW	예상결과	결과SW	측정결과
가정	가치저장전금액(하이패스플러스카드) 가치저장전금액(PSAM)		00000520 0000009A		
기능시험	B1. Initialize 하이패스플러스	9000	$R_{하이패스플러스}$(8)	9000	F72DD067E8342ED2
보안시험	A3. 서명S1생성	9000	S1(4)	9000	C24FDA26
기능시험	B2. Initialize PSAM	9000		9000	
보안시험	C5. 서명S2생성	9000	S2(4)	9000	D9CBE586
기능시험	B3. Purchase 하이패스플러스	9000		9000	
기능시험	A7. $BAL_{하이패스플러스}$ 감소	9000	00000510	9000	00000510
보안시험	C5. 서명S3생성	9000	S3(4)	9000	6197A09E
기능시험	B4. Credit PSAM	9000		9000	
기능시험	C8. BAL_{PSAM}증가	9000	000000AA	9000	000000AA
보안시험	C5. 서명S4생성	9000	S4(4)	9000	D9F231BF
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	

어서 예상 결과와 일치하였다. 나머지, 항목들도 시험 예상결과와 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 10HEX인 값을 지불하고자 한다. B1.Initialize 하이패스플러스를 실행한 결과, 하이패스플러스카드의 BAL 하이패스플러스(4)는 00000460HEX이다. 따라서, 시험을 종료한 후의 BAL하이패스플러스(4)는 00000450HEX이 되어야한다. A3. 서명S1의 값은 9AF234DFHEX이 생성되었다. B2. Initialize PSAM을 실행한 결과, NTPSAM은 000000A2HEX이고, PSAM의 가치저장 전 금액은 00001198HEX이었다. 따라서, 시험이 종료된 후의 NTPSAM은 000000A3HEX이고, PSAM의 가치저장 후 금액은 000011A8HEX이 되어야 한다. C5. 서명S2은 6071E9AAHEX이 생성되었고, NTPSAM은 000000A3HEX이고, PSAM의 가치저장 후 금액은 000011A8HEX이 되어서, 예상한 결과와 일치하였다. A7. BAL하이패스플러스차감 결과, NT하이패스플러스(4)는 000000AFHEX이 되었고, BAL하이패스플러스(4)은 00000450HEX이 되어서 예상한 결과와 일치하였다. A8. 서명S3은 0A1BDA3C이 생성되었다. 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 시험 방법 및 절차는 한국도로공사 규격서 및 국제 ISO 표준에 의거하여 개발하였다. 시험에 사용된 PSAM은 한국도로공사에서 사용 중인 PSAM을 시험하였다. PSAM은 한국도로

〈표 7〉 H2P(표준SAM) 시험 결과

시험절차	시험 표준항목	예상SW	예상결과	결과SW	측정결과
가정	가치저장전금액(하이패스플러스카드)		00000460		
	가치저장전금액(PSAM)		00001198		
	NT_{PSAM}		000000A2		
기능시험	B1. Initialize 하이패스플러스	9000	$NT_{하이패스플러스}$(4)	9000	000000B3
보안시험	A3. 서명S1생성	9000	S1(4)	9000	9AF234DF
기능시험	B2. Initialize PSAM	9000		9000	
보안시험	C5. 서명S2생성	9000	S2(4)	9000	6071E9AA
기능시험	NT_{PSAM} B3. Purchase 하이패스플러스	9000	000000A3 000011A8	9000	000000A3 000011A8
기능시험	A7. $BAL_{하이패스플러스}$차감	9000	00000450	9000	00000450
보안시험	A8. 서명S3생성	9000	S3(4)	9000	0A1BDA3C
기능시험	B4. Credit PSAM	9000		9000	
기능시험	C9. 개별거래내역저장	9000		9000	
기능시험	B5. 개별거래내역저장	9000		9000	

공사 전자지불시스템에서 사용되는 매우 중요한 요소이므로 PSAM의 기능뿐 아니라 보안성의 시험 인증은 매우 중요한 의미를 갖는다. 따라서, 본 시험에서 제시한 방법 및 절차에 의거한 PSAM의 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 PSAM 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] 임낙희, 신규평가대상제품확대추진계획, 정보통신부, 2003.9.

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

[4] ISO/IEC 10373-1, Identification cards-Test me thods - Part 1 : General characteristics tests, 1998. 12.

[5] ISO/IEC 10373-3, Identification cards-Test me thods - Integrated circuit(s) cards - Part 3 : Inte grated circuit(s) cards with contacts, 2001.2.

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

[7] 김재성, 평가대상제품평가준비지원방안, 한국정보보호진흥원, 2003.9.

[8] 이태승, 신규평가대상제품평가방안, 한국정보보호진흥원, 2003.9.

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

[10] 한국도로공사, 도로공사 PSAM 시험인증 규격서 V1.1, 2003.

[11] 한국도로공사, 도로공사 PSAM 규격서 V1.1, 2003.

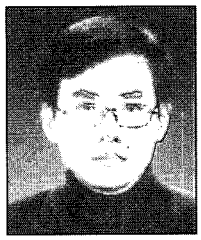
〈저자소개〉

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

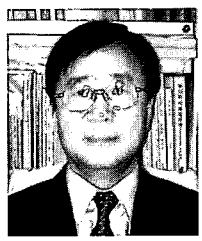
서 현 교 (Hyun Kyo, Suh)

1999. 2 : 서강대학교 경영학과 학사
2003. 8 : 서울대학교 경영대학 경영학과 대학원 석사
2003. 7~현재 : 한국도로공사 스마트웨이사업팀 근무



유 창 희 (Chang Hee, Yoo)

1994. 2 : 성균관대학교 경제학과 졸업
1995 : 한국도로공사 입사
2004~현재 : 스마트웨이사업팀 카드사업부 과장



이 승 환 (Seung-Hwan, Lee)

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