한국ITS학회논문지
제3권, 제1호 (2004. 3 · 6)
pp.1~12

하이패스플러스카드 시스템을 위한 LSAM 시험 및 모듈 개발

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

이 기 한*, 윤 현 탁**, 김 재 웅**, 이 승 환***
(Ki-Han, Lee), (Hyun-Tak, Yoon), (Jae-Uoong, Kim), (Seung-Hwan, Lee)

요 약

한국도로공사는 선불형 플라스틱카드를 스마트카드 형태의 선불형 전자지불카드인 하이패스플러스카드로 교체하여 사용하고 있다. 하이패스플러스카드를 전자지불에 사용하기 위해서는 하이패스플러스카드에 가치를 저장하여야 하는데 이를 수행하는 스마트카드가 LSAM이다. 또한, LSAM은 PPSAM에 의해서 가치를 저장 받거나 환불할 수 있도록 설계되어있다. 따라서, LSAM의 기능 및 보안이 철저해야 한국도로공사의 전자지불시스템이 안전하다. 본 논문은 PPSAM에 의한 LSAM의 가치저장, PPSAM에 의한 LSAM의 가치환불, 그리고, LSAM에 의한 하이패스플러스카드로의 가치저장 기능 및 보안을 시험하기 위한 시험 방법, 시험 표준항목, 그리고 시험 절차 등을 포함한 시험 모듈을 개발했다. LSAM의 기능 및 보안 시험에 관한 시험 표준항목 및 시험 검사표는 한국도로공사 규격서에 준하여 ISO 표준에 적합한 항목을 기준으로 선정했다. 본 시험 모듈은 LSAM의 기능뿐 아니라 보안성 및 적합성을 시험하였다. 시험은 한국도로공사에서 사용되는 LSAM을 이용하여 실행하였다. 시험결과에 의하면, 한국도로공사에서 사용되는 LSAM은 모든 시험 기준을 통과하여 보안성 및 기능성이 적합하다고 평가되었다.

Abstract

Recently, the Korea Highway Company is replacing their prepaid plastic cards with a smart card, called Hipass^{PLUS} Card. In order to use Hipass^{PLUS} Card in the prepaid payment system, LSAM, which is to store the value into Hipass^{PLUS} Card is needed. LSAM is also responsible to store or retrieve the value from PPSAM. For the safety of Korea Highway electronic payment system, the functionality and security of LSAM 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 loading the value from PPSAM to LSAM, retrieving the value from LSAM to PPSAM, and loading the value from LSAM to Hipass^{PLUS} Card. The test module contains the method and the procedure to test the standard items by the test checklists. The test items and test checklists of LSAM was selected under the provision of the specification of Korea Highway Company and ISO standard. The test module evaluates the functionality, the security and the compatibility of LSAM. After the evaluation test of LSAM using the test module, LSAM satisfied the characteristics of the functionality, security, and compatibility.

Key Words : LSAM, Hipass^{PLUS} Card, PPSAM, Test module, Function test, Security test

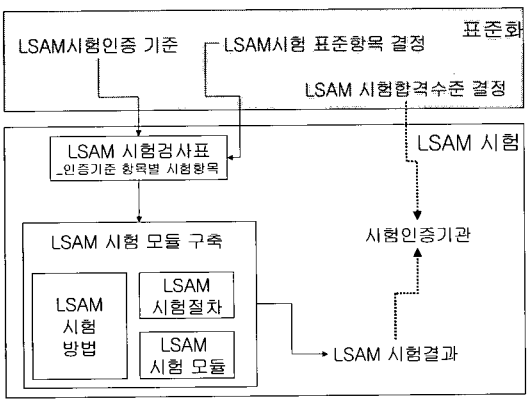
* 회 원 : 서울여자대학교 컴퓨터공학과 교수
** 비회원 : 한국도로공사 스마트웨이사업팀 대리
*** 비회원 : 한국도로공사 스마트웨이사업팀 과장
**** 회 원 : 아주대학교 환경건설교통공학부 교수
† 논문접수일 : 2003년 9월 26일

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, 먼저, 하이패스플러스카드에 금액이 충전되어있어야 한다. LSAM은 하이패스플러스카드에 금액을 충전시킬 수 있는 스마트카드로서, 매우 중요한 스마트카드이다. 따라서, LSAM이 정확하게 동작을 하지 않으면, 가치저장에 많은 문제를 야기할 수 있다. 그러므로, LSAM의 기능 및 보안성을 정확하게 시험평가를 하는 것은 그 의미가 매우 크다고 본다[1,2].

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 정보화 촉진기본법 제15조에 의한다[6,7]. 스마트카드를 시험하는 기구는 한국에서는 보안 및 기능에 관련되어서는 한국기술표준원이 ISO를 인증한 전자카드품질인증원과 한국정보보호진흥원이 있다[8].

LSAM은 PPSAM에 의해서 가치를 저장받고, 하이패스플러스카드에 가치를 전달 및 저장하는 방식이다. 따라서, LSAM의 기능 시험인증은 PPSAM 및 하이패스플러스카드와의 기능을 시험하는 것이다. LSAM을 시험하기 위한 전체적인 시험 절차는 <그림 1>과 같다[1,2,9]. LSAM을 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 LSAM을 시험하고 이를 분석하여 LSAM이 원하는 기준을 통과하여 정확하게 동작하는 지를 분석했다.



〈그림 1〉 시험 절차 구성

Ⅱ. 시험 방법 및 절차

LSAM 시험은 <표 1>과 같이 LSAM과 PPSAM 그리고 LSAM과 하이패스플러스카드간의 시험으로 나누어진다. LSAM과 PPSAM간의 시험은 PPSAM의 가치를 LSAM으로 저장하는 PP2L(가치저장) 시험, LSAM의 가치를 PPSAM으로 환불하는 L2PP(가치환불) 시험, 그리고 PPSAM에 의해서 LSAM의 파라미터를 갱신하는 PP2L(파라미터갱신) 시험으로 구분한다. LSAM과 하이패스플러스카드간의 시험은 LSAM의 가치를 하이패스플러스카드로 저장하는 L2H(가치저장) 시험으로 구분한다.

〈표 1〉 LSAM 시험 종류

대분류	중분류	시험명
LSAM과 PPSAM간 시험	가치저장 시험	PP2L(가치저장)
	가치환불 시험	L2PP(가치환불)
LSAM과 하이패스플러스 카드간 시험	가치저장 시험	L2H(가치저장)
보안 시험	서명 확인 시험	
	암호화 시험	

1. PP2L(가치저장) 시험 방법 및 절차

PPSAM에 있는 가치를 LSAM으로 저장하는 PP2L(가치저장)시험은 PPSAM에 있는 가치가 LSAM에

정확하게 저장되는 지를 확인하기 위한 시험이다. LSAM의 가치저장을 위한 잔액 파일 구조는 <표 2>와 같다[10].

PPSAM에 의해서 LSAM에 가치가 저장되는 개략적인 흐름은 다음 <그림 2>와 같다[10]. 가치저장은 PPSAM과 LSAM이 상호인증 한 후, 선택된 금액만큼 한국도로공사 LSAM소지자의 주계좌에서 LSAM로 이체된다.

〈표 2〉 LSAM 잔액 파일(EF_{BAL})

파일식별자	EF03		
항목	크기	내용	형식
BAL_{LSAM}	4	LSAM에 남아있는 금액	Hex
CKS_{BAL}	1	LSAM에 남아있는 금액의 Check Sum	Hex
$BBAL_{LSAM}$	4	잔액에 대한 BACK-UP	Hex
CKS_{BBAL}	1	잔액에 대한 BACK-UP의 Check Sum	Hex
BAL_{MAX_LSAM}	4	한국도로공사 LSAM의 최대 저장 한도 금액	Hex
M_{MAX_LSAM}	4	1회에 출금할 수 있는 최대 금액	Hex
NT_{LSAM}	4	한국도로공사 LSAM 카드 거래일련번호	Hex

LSAM	LDA	PPSAM
	B1. 한국도로공사LSAM DF선택	
	B2. PIN/M_{LDA} 입력	
	<- B3. Initialize LSAM (M_{LDA}, PIN)	
A1. 난수생성		
A2. 조건확인		
A3. $KSES1_{LSAM}$ 생성(암호화)		
A.4 서명S1생성(서명확인)		
A5. 거래내역저장		
A6. 응답		
	B4. Debit PPSAM ->	
		C1. 난수 생성
		C2. 조건확인
		C3. $KDLL_{PPSAM}$ 생성(암호화)
		C4. $KSES1_{PPSAM}$ 생성(암호화)
		C5. 서명S1검증(서명확인)
		C6. BAL_{PPSAM} 차감
		C7. $KSES2_{PPSAM}$ 생성(암호화)
		C8. 서명S2생성
		C9. 응답
	<- B5. Load LSAM(R_{PPSAM},S2)	
A7. $KSES2_{LSAM}$생성(암호화)		
A8. 서명검증(S2)(서명확인)		
A9. BAL_{LSAM} 증가		
A10. 서명S3생성(서명확인)		
A11. 거래내역저장		
A12. 응답		
	-> B6. 저장	

〈그림 2〉 PPSAM과 LSAM의 가치저장 흐름도

PPSAM의 가치가 LSAM에 정확하게 저장되는지를 시험하는 가치저장 시험은 B3, A5, B4, C5, B5, A9, B6 순으로 시험하고, PPSAM과 LSAM간에 가치를 저장하는 동안에 PPSAM과 LSAM이 정확하게 정보를 전달되는 지를 시험하는 서명확인시험은 A4, C5, C8, A8, A10 순으로 시험하면, PPSAM과 LSAM간에 가치를 저장하는 동안에 PPSAM과 LSAM이 전달하는 정보가 정확하게 암호화 및 복호화가 이루어지는 지를 시험하는 암호화시험은 A3, C3, C4, C7, A7 순으로 시험한다.

2. L2PP(가치환불) 시험 방법 및 절차

가치환불은 <그림 3>과 같이 PPSAM과 LSAM이 상호인증 한 후, 선택된 금액만큼 한국도로공사 LSAM에서 출금하여 HOST(원장)로 이체되는 과정이다[10].

LSAM에 있는 가치를 PPSAM으로 정확하게 환불되는 지를 시험하는 가치환불 시험은 B3, A5, B4, C2, C4, B5, A9, B6, C10, B7, A13, B8 순으로 시험하고, LSAM과 PPSAM간에 가치를 환불하는

LSAM	LDA	PPSAM
	B1. 한국도로공사LSAM DF선택	
	B2. M_{LDA}와 PIN입력	
	B3. Initialize LSAM(M_{LDA}, PIN) <-	
A1. 난수생성		
A2. 조건확인		
A3. $KSES1_{LSAM}$생성(암호화)		
A4. 서명 S1 생성(서명확인)		
A5. 거래내역 저장		
A6. 응답 ->		
	B4. Initialize PPSAM ->	
		C1. 난수 생성
		C2. 조건확인
		C3. $KDLL_{PPSAM}$ 생성(암호화)
		C4. 서명S1검증(서명확인)
		C5. BAL_{PPSAM} 증가
		C6. $KSES2_{LSAM}$ 생성(암호화)
		C7. 서명S2생성(서명확인)
		C8. 응답
	<- B5. Load LSAM(R_{PPSAM},S2)	
A7. $KSES2_{LSAM}$생성(암호화)		
A8. 서명S2검증(서명확인)		
A9. BAL_{LSAM} 차감		
A10. 서명S3생성(서명확인)		
A11. 거래내역저장		
A12. 응답 ->		
	B6. Credit PPSAM(S3) ->	
		C9. 서명S3검증(서명확인)
		C10. 응답
	<- B7. Complete Transaction	
A13. 응답		
	-> B8. 저장	

〈그림 3〉 PPSAM과 LSAM간의 가치환불 흐름도

동안에 LSAM과 PPSAM이 정확하게 정보를 전달되는 지를 시험하는 서명확인시험은 A4, C5, C7, A8, A10, C9 순으로 시험하며, LSAM과 PPSAM간에 가치를 저장하는 동안에 LSAM과 PPSAM이 전달하는 정보가 정확하게 암호화 및 복호화가 이루어지는 지를 시험하는 암호화시험은 A3, C3, C6, A7 순으로 시험한다.

3. L2H(가치저장) 시험 방법 및 절차

LSAM에 의해서 하이패스플러스카드에 가치가 저장되는 개략적인 흐름은 다음 <그림 4>와 같다 [10]. 가치저장은 하이패스플러스카드와 LSAM이 상호 인증한 후, 선택된 금액만큼 LSAM 전자화폐에서 출금하여 하이패스플러스카드 소지자의 전자화폐로 이체되는 과정이다. 이 가치저장은 충전소의 충전단말기에서 이루어진다. LSAM에 저장되어 있는 금액 내에서 하이패스플러스카드에 충전할 수 있다.

LSAM의 가치가 하이패스플러스카드에 정확하게 저장되는 지를 시험하는 가치저장 시험은 B3, A5, B4, C5, B5, A9, B6, C10, B7 순으로 시험하고,

하이패스플러스카드	LDA	LSAM
	<- B1. 하이패스플러스카드 DF 선택	
A1. 응답 ->		
	B2. M_{LDA}와 PIN입력	
	B3. Initialize 하이패스플러스(M_{LDA},	
	<- PIN)	
A2. 난수생성		
A3. KSES1 하이패스플러스생성(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 Hi-pass^{PLUS} (R_{LSAM},S2)	
A7. KSES2 하이패스플러스생성(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 4〉 LSAM과 하이패스플러스카드간의 가치저장 흐름도

LSAM과 하이패스플러스카드간에 가치를 저장하는 동안에 LSAM과 하이패스플러스카드가 정확하게 정보를 전달되는 지를 시험하는 서명확인시험은 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 암호화시험은 A3, C3, C6, A7 순으로 시험한다.

Ⅲ. 시험 표준항목 선정

II.장에서 결정된 시험 방법에 의해서 LSAM을 시험하고 평가하기 위해서 다음과 같은 시험 표준항목을 결정하였다.

1. PP2L(가치저장) 시험 표준항목

<그림 2>에서 PP2L(가치저장) 시험은 A1부터 A12, B1부터 B6, 그리고 C1부터 C9까지의 모든 항목에 걸쳐서 이루어진다. 하지만, 이 모든 과정 중에서 B1과 B2는 B3에 의해서 검증되므로 시험할 필요가 없다. A1과 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 의해서 검증되므로 시험할 필요가 없고, C3과 C4는 C6에 의해서 검증되므로 시험할 필요가 없고, C7은 C8에 의해서 검증되므로 시험할 필요가 없다. 따라서, 시험 순서에 따른 표준항목 및 선정기준은 다음 <표 2>와 같다[6,7].

2. L2PP(가치환불) 시험 표준항목

<그림 3>에서 L2PP(가치환불) 시험은 A1부터 A13, B1부터 B8, 그리고 C1부터 C10까지의 모든 항목에 걸쳐서 이루어진다. 하지만, 이 모든 과정 중에서 B1과 B2는 B3에 의해서 검증되므로 시험할 필요가 없다. A1과 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 의해서 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 3>과 같다[6,7].

〈표 2〉 PP2L(가치저장) 시험 순서에 따른 기준 및 표준항목

시험기준	시험 표준항목
기능시험	B3. Initialize LSAM
보안시험	A4. 서명S1생성
기능시험	B4. Debit PPSAM
기능시험	C5. BAL_{PPSAM}
보안시험	C8. 서명S2생성
기능시험	B5. Load LSAM
기능시험	A9. BAL_{LSAM}
보안시험	A10. 서명S3생성
기능시험	B6. 저장

〈표 3〉 L2PP(가치환불) 시험 순서에 따른 기준 및 표준항목

시험기준	시험 표준항목
기능시험	B3. Initialize LSAM
보안시험	A4. 서명S1생성
기능시험	B4. Initialize PPSAM
기능시험	C5. BAL^{PPSAM}
보안시험	C7. 서명S2생성
기능시험	B5. Load LSAM
기능시험	A9. BAL^{LSAM}
보안시험	A10. 서명S3생성
기능시험	B6. Credit PPSAM
기능시험	B7. Complete Transaction
기능시험	B8. 저장

3. L2H(가치저장) 시험 표준항목

<그림 4>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 의해서 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 4>와 같다[6,7].

〈표 4〉 L2H(가치저장) 시험 순서에 따른 기준 및 표준 항목

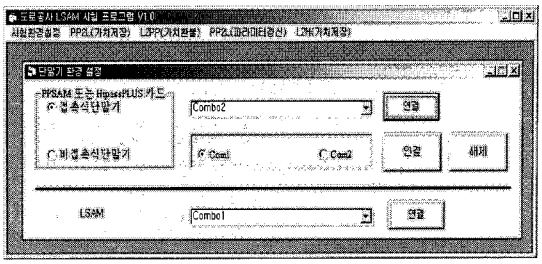
시험기준	시험 표준항목
기능시험	B3. Initialize 하이패스플러스
보안시험	A4. 서명S1생성
기능시험	B4. Debit LSAM
기능시험	C5. BAL_{LSAM}
보안시험	C7. 서명S2생성
기능시험	B5. Load 하이패스플러스
기능시험	A9. $BAL_{하이패스플러스PLUS}$
보안시험	A10. 서명S3생성
기능시험	B7. 저장

Ⅳ. 시험 모듈 개발

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

1. 시험 환경설정 모듈

<그림 5>는 LSAM을 시험하기 위해서 LSAM과



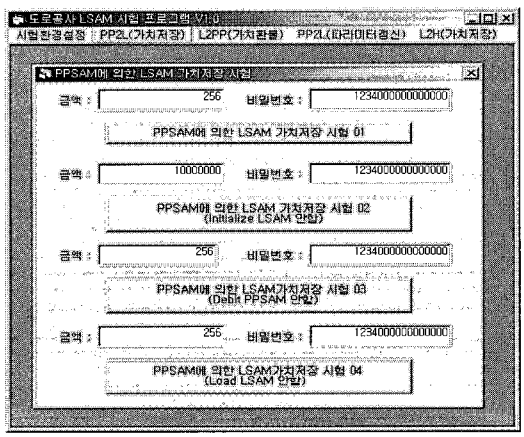
〈그림 5〉 시험 환경설정 모듈

PPSAM 및 하이패스플러스카드를 연결하기 위한 환경을 설정하기 위한 모듈이다. LSAM은 Combo1에 삽입하고, PPSAM 및 하이패스플러스카드는 Combo2에 삽입하여 시험한다.

2. PP2L(가치저장) 시험 모듈

1) PP2L(가치저장) 시험 절차

PPSAM에서 LSAM에 가치를 저장하는 시험 모듈은 원하는 가치가 정상적으로 저장되는 지를 시험하기 위한 모듈이다. 시험 절차는 Initialize LSAM이 LSAM에서 수행되고 이에 의해서 서명S1이 생성되며, Debit PPSAM이 PPSAM에 전달되고, BAL_{PPSAM}이 원하는 가치만큼 감소되며, 서명S2가 생성되고, Load LSAM이 LSAM에 전달되어 BAL_{LSAM}이 원하는 가치만큼 증가되며, 서명S3이 생성되는지를 검사한다.



〈그림 6〉 PP2L(가치저장)시험 모듈

2) PP2L(가치저장) 시험 모듈

<그림 6>은 PPSAM에서 LSAM에 가치를 저장하는 시험을 위해 구현한 모듈이다.

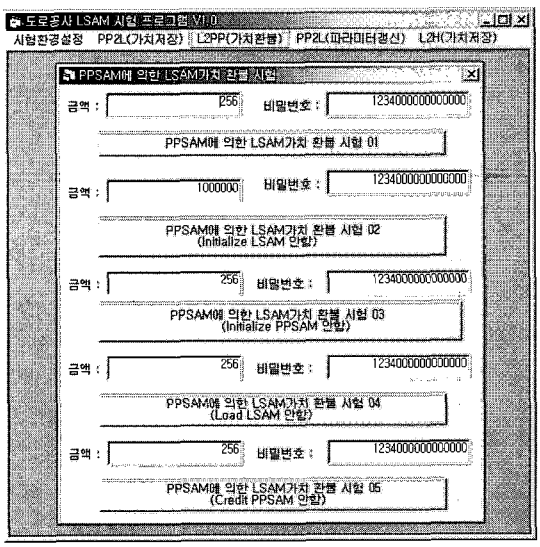
3. L2PP(가치환불) 시험 모듈

1) L2PP(가치환불) 시험 절차

LSAM의 가치를 PPSAM에 환불하는 시험 모듈은 원하는 가치가 정상적으로 환불되는 지를 시험하기 위한 모듈이다. 시험 절차는 Initialize LSAM이 LSAM에서 수행되고 이에 의해서 서명S1이 생성되며, Initialize PPSAM이 PPSAM에 전달되고, BAL_{PPSAM}이 원하는 환불가치만큼 증가되며, 서명S2가 생성되고, Load LSAM이 LSAM에 전달되어 BAL_{LSAM}이 원하는 환불가치만큼 감소되며, 서명S3이 생성되고, Credit PPSAM이 PPSAM에 전달되고 Complete Transaction이 LSAM에 전달되어 그 정보가 LDA에 저장되는 지를 검사한다.

2) L2PP(가치환불) 시험 모듈

<그림 7>은 LSAM에서 PPSAM에 가치를 환불하는 시험을 위해 구현한 모듈이다.



〈그림 7〉 PP2L(가치환불)시험 모듈

4. L2H(가치저장) 시험 모듈

1) L2H(가치저장) 시험 절차

LSAM에서 하이패스플러스카드에 가치를 저장하는 시험 모듈은 원하는 가치가 정상적으로 저장되는 지를 시험하기 위한 모듈이다. 시험 절차는 Initialize 하이패스플러스 가 하이패스플러스카드에서 수행되고 이에 의해서 서명S1이 생성되며,. Debit LSAM이 LSAM에 전달되고, BAL_{LSAM}이 원하는 가치만큼 감소되며, 서명S2가 생성되고, Load 하이패스플러스가 하이패스플러스카드에 전달되어 $BAL_{하이패스플러스}$가 원하는 가치만큼 증가되며, 서명S3이 생성되는 지를 검사한다.

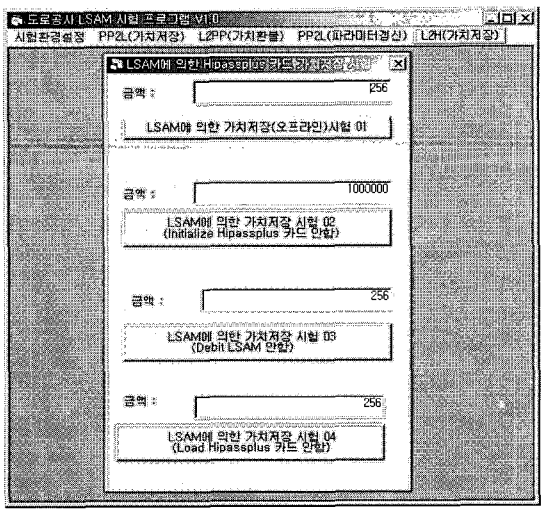
2) L2H(가치저장) 시험 모듈

<그림 8>은 LSAM에서 하이패스플러스카드에 가치를 저장하는 시험을 위해 구현한 모듈이다.

V. 시험 결과 및 분석

1. 시험 환경

PPSAM과 하이패스플러스카드, LSAM은 한국도



〈그림 8〉 L2H(가치저장)시험 모듈

〈표 5〉 PP2L(가치저장) 시험 순서에 따른 기준 및 표준항목

시험절차	시험 표준항목	예상SW	예상결과	측정SW	측정결과
가정	가치저장전금액(LSAM)	0FFFBD50			
	가치저장전금액(PPSAM)	0FF00256			
기능시험	B3. Initialize LSAM	9050		9050	
보안시험	A4. 서명S1생성	9050		9050	9886739A
기능시험	B4. Debit PPSAM	903C		903C	
기능시험	C5. BAL_{PPSAM}차감	9000	0FF00000	9000	0FF00000
보안시험	C8. 서명S2생성	903C		903C	6BE23345
기능시험	B5. Load LSAM	9052		9052	
기능시험	A9. BAL_{LSAM}증가	9000	0FFFBFA6	9000	0FFFBFA6
보안시험	A10. 서명S3생성	9052		9052	C4DBE0D6
기능시험	B6. 저장	9052		9052	

로공사에서 개발한 카드를 이용하여 시험했다.

본 시험은 상온에서 시행한다. III.장에서 개발된 시험 모듈을 이용하여 다음과 같이 LSAM을 시험하였다.

2. PP2L(가치저장) 시험 결과 및 분석, 평가

1) PP2L(가치저장) 시험 결과

시험 결과는 다음 <표 5>와 같다.

2) PP2L(가치저장) 시험 분석 및 평가

저장하고자 하는 가치는 16진수로는 256_{HEX}이다. 가치저장전 LSAM 값은 16진수로 $0FFFBD50_{HEX}$이고, PPSAM의 값은 $0FF00256_{HEX}$이다. 이는 기능시험 B3. Initialize 하이패스플러스를 실행하고, 보안기능 A4. 서명S1생성에 의해서 서명S1의 16진수값 $9886739A_{HEX}$이 생성되었다. 기능시험 B4.Debit PPSAM이 PPSAM에 전달되었다. 기능시험 C5. BAL_{PPSAM}차감에 의해서, PPSAM의 예상 값이 $0FF00000_{HEX}$인데, 수행한 결과 정확하게 감소하였다. 또한, 보아시험 C5. 서명S2생성에 의해서 서명 S2가 $6BE23345_{HEX}$가 생성되었다. 기능시험 B5. Load LSAM이 LSAM에 전달되었고, 기능 시험 A9. BAL_{LSAM}증가에 의해서 예상되는 BAL_{LSAM}값은 0FFFBFA6HEX이었는데, 수행한 결과 정확하게 증가되었다. 보안 시험 A10. 서명S3생성에 의해서 서명 S3의 16진수값 $C4DBE0D6_{HEX}$이 생성되었다. 그리고, B3, B4, B5가 잘못된 경우에는 실행이 중단되었다. 따라서, PP2L(가치저장) 시험이 정상적으로 이루어졌고, 한국도로공사에서 사용하는 LSAM은 PP2L(가치저장) 시험을 통과하였다.

3. L2PP(가치환불) 시험 결과 및 분석, 평가

1) L2PP(가치환불) 시험 결과

시험 결과는 다음 <표 6>과 같다.

2) L2PP(가치환불) 시험 분석 및 평가

환불하고자 하는 가치는 16진수로는 256_{HEX}이다. 가치환불전 LSAM 값은 16진수로 $1FFFC6A8_{HEX}$이며, PPSAM의 값은 $1FFED5B3_{HEX}$이다. 기능시험 B3. Initialize 하이패스플러스를 실행 결과한 $BAL_{하이패스플러스}$를 수행한 후, 보안시험 A4.서명S1생성에 의해서 서명S1의 16진수값 $04718EC2_{HEX}$이 생성되었다. 기능 시험 B4. Initialize PPSAm이 수행되고, 기능 시험 C5. BAL_{PPSAM}증가에 의해서 예상되는 결과는 $1FFED35D_{HEX}$인데, 수행한 결과 일치하였다. 보안 시험 C7. 서명S2생성에 의해서 서명 값

E0895EF6이 생성되었다. 기능 시험 B5. Load LSAM가 수행되었고, 기능시험 A9. BAL_{LSAM}감소에 의해서 예상되는 LSAM값인 $1FFFC452_{HEX}$이, 수행 결과와 일치하였다. 보안시험 A10. 서명S3생성에 의해서 서명 S3이 $0844BE0E_{HEX}$로 생성되었다. 기능시험 B6. Credit PPSAM, B7. Complete Transaction, 그리고 B8. 저장이 정상적으로 수행되었다. 또한, B3, B4, B5, B6, 그리고 B7이 잘못된 경우에는 실행이 중단되었다. 따라서, L2PP가치환불) 시험이 정상적으로 이루어졌고, 한국도로공사에서 사용하는 LSAM은 L2PP(가치환불) 시험을 통과하였다.

4. L2H(가치저장) 시험 결과 및 분석, 평가

1) L2H(가치저장) 시험 결과

L2H(가치저장) 시험 결과는 다음 <표 7>과 같다.

〈표 6〉 L2PP(가치환불) 시험 순서에 따른 기준 및 표준항목

시험절차	시험 표준항목	예상SW	예상결과	측정SW	측정결과
가정	가치환불전금액(LSAM)	1FFFC6A8			
	가치환불전금액(PPSAM)	1FFED5B3			
기능시험	B3. Initialize LSAM	9050		9050	
보안시험	A4. 서명S1생성	9050		9050	04718EC2
기능시험	B4. Initialize PPSAM	9038		9038	
기능시험	C5. BAL_{PPSAM}증가		1FFED35D		1FFED35D
보안시험	C7. 서명S2생성				E0895EF6
기능시험	B5. Load LSAM	9054		9054	
기능시험	A9. BAL_{LSAM}감소		1FFFC452		1FFFC452
보안시험	A10. 서명S3생성				0844BE0E
기능시험	B6. Credit PPSAM	905E		905E	
기능시험	B7. Complete Transaction	905E		905E	
기능시험	B8. 저장	905E		905E	

〈표 7〉 L2H(가치저장) 시험 결과

시험절차	시험 표준항목	예상SW	예상결과	측정SW	측정결과
가정	가치저장전 금액(LSAM)	0FFFDC**50**			
	가치저장전 금액(하이패스플러스)	00000**320**			
기능시험	B3. Initialize 하이패스플러스	9000	$NT_{하이패스플러스}$(4) $R_{하이패스플러스}$(8)	9000	00000092 95682235849FC2AC
보안시험	A4. 서명S1생성	9000	S1(4)	9000	F4A87659
기능시험	B4. Debit LSAM	9000		9000	
기능시험	C5. BAL_{LSAM} 차감	9000	가치저장후 금액	9000	0FFFD**B50**
보안시험	C7. 서명S2생성	9000	S2(4)	9000	B0D95A07
기능시험	B5. Load 하이패스플러스	9000		9000	
기능시험	A9. $BAL_{하이패스플러스}$ 증가	9000	00000420	9000	00000**420**
보안시험	A10. 서명S3생성	9000	S3(4)	9000	A605231C
기능시험	B7. 저장	9000		9000	

2) L2H(가치저장) 시험 분석 및 평가

저장하고자 하는 가치는 10진수로는 256_{DEC} 또는 16진수로 100_{HEX}이다. 가치저장전 LSAM 값은 16진수로 $0FFFDC50_{HEX}$이며, 하이패스플러스카드의 값은 00000320_{HEX}이다. 기능시험 B3. Initialize 하이패스플러스가 정상적으로 수행되었으며, 보안시험 A4. 서명S1생성에 의해서 서명S1의 16진수값 $F4A87659_{HEX}$이 생성되었으며, 기능시험 B4. Debit LSAM이 LSAM에 전달되고, 기능시험 C5. BAL_{LSAM} 차감에 의해서 예상되는 LSAM의 가치인 $0FFFDB50_{HEX}$가 정상적으로 바뀌어야 한다. 보안시험 C7. 서명S2생성에 의해서 서명S2는 16진수값 $B0D95A07_{HEX}$가 생성되었다. 기능시험 B5. Load 하이패스플러스가 정상적으로 수행되었으며, 기능시험 A9. $BAL_{하이패스플러스}$ 증가에 의해서 $BAL_{하이패스플러스}$이 00000320_{HEX}에서 00000420_{HEX}으로 증가하였다. 보안시험 A10. 서명S3생성에 의해서 서명 S3의 16진수값 $A605231C_{HEX}$이 생성되었다. 또한, B3, B4, B5가 잘못된 경우에는 실행이 중단되었다. 따라서, L2H(가치저장) 시험이 정상적으로 이루어졌고, 한국도로공사에서 사용하는 하이패스플러스카드는 L2H(가치저장) 시험을 통과하였다.

Ⅵ. 결 론

본 논문에서 제시한 시험 방법 및 절차는 한국도로공사 규격서 및 국제 ISO 표준에 의거하여 개발하였다. 시험에 사용된 LSAM은 한국도로공사에서 현재 사용 중인 LSAM을 시험하였다. LSAM은 한국도로공사 전자지불시스템에서 사용되는 매우 중요한 요소이므로 LSAM의 기능뿐 아니라 보안성의 시험 인증은 매우 중요한 의미를 갖는다. 따라서, 본 시험에서 제시한 방법 및 절차에 의거한 LSAM의 시험은 한국도로공사 전자지불시스템의 적합성 및 안정성, 품질 향상을 증가시킬 수 있다.

본 논문에서 제시한 시험 표준항목의 선정은 국제표준 및 한국도로공사의 규격서에 의해서 이루어졌다. 시험 방법 및 절차는 국내 표준 및 국제 표준 시험 방법을 적용하여 연구되었다.

본 논문에서 실행한 LSAM 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.

참고문헌

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

[2] 이태승, 신규평가대상제품평가방안, 한국정보보호진흥원, 2003.9.

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

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

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

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

[7] 임낙희, 신규평가대상제품확대추진계획, 정보통신부, 2003.9.

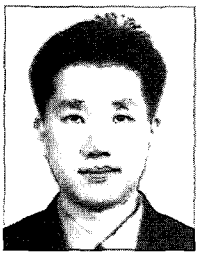
[8] 김재성, 평가대상제품평가준비지원방안, 한국정보보호진흥원, 2003.9.

[9] 한국도로공사, 도로공사 LSAM 시험인증 규격서 V1.1, 2003.

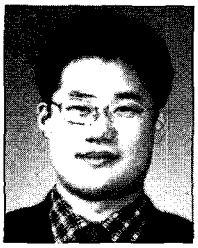
[10] 한국도로공사, 도로공사 LSAM V1.1, 2003.

〈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



윤 현 탁(Hyun-Tak, Yoon)
2002년 8월 : 동국대학교 전자공학과 학사
2003년 3월~현재 : 아주대학교 산업대학원 교통공학과 재학
2002년 2월~현재 : 한국도로공사 스마트웨이사업팀 대리



김 재 웅(Jae-Uoong, Kim)
1996년 2월 : 전남대학교 경영학과 학사
2003년 8월 : 경희대학교 경영대학원 마케팅공학과 석사
1995년 10월~현재 : 한국도로공사 스마트웨이사업팀 과장

이 승 환 (Seung-hwan, Lee)
Polytech University 교통공학 박사
아주대학교 환경건설교통공학부 교수
아주대학교 ITS대학원 대학원장
현 한국ITS학회 회장