전자지불시스템에서 이용되는 스마트카드의 시험 모듈 구성에 대한 연구

A Study on Test Module of Smart Cards in Electronic Payment Systems

김윤정 (Yoonjeong Kim)*, 이기한 (Ki-Han Lee)*

초록

스마트카드는 전자지불시스템에서 인증 수단으로 유용하게 사용되는 도구로, 스마트카드 개발시 이의 기능이 올바로 동작하는지 테스트해 보는 것은 중요한 의미를 갖는다. 본 논문에서는 스마트카드의 기능을 테스트하기 위한 기존 연구 내용을 ISO/IEC 표준 문서 및 KS 표준 문서 그리고 한국도로공사 카드 품질시험인증서를 기반으로 살펴보고, 한국도로공사의 하이패스플러스 카드에 대한 기능 시험 결과를 제시한다. 하이패스플러스 카드에 시험 평가를 수행함으로써 안정적인 기능성과 보안성을 가진 카드 시스템을 확보할 수 있고 나아가 신뢰성 있는 보안 제품의 개발에 기여하리라 기대된다. 본 논문에서 제시하는 시험 방법과 결과는 시범서비스 중인 스마트카드에 대하여는 국내에서는 최초로 수행된 연구로, 향후 좀 더 보완된 시험 방안에 대한 연구의 기반을 제공하리라 기대된다.

Abstract

Smart card is a useful tool used in electronic payment systems and it is very important to test whether a smart card operates correctly. In this paper, we analyze previous researches on testing smart cards, such as ISO/IEC and KS standard documents, and Guideline of Card Quality Test. We also propose the functional test results done on the Highpassplus card of Korea Highway Corporation. By testing the Hipgpassplus card we can get card systems with reliable functionality and security. Furthermore, this can help developing more reliable security systems. The test results of the Highpassplus card proposed in this paper are the first research on testing smart cards in services in Korea and we expect that the test methods of smart card will be advanced based on our results.

키워드 : 스마트카드, ISO/IEC SC17, 스마트카드 - 테스트 방법
Smart Card, ISO/IEC SC17, Identification Cards - Test Methods

---

이 논문은 2003년도 서울여자대학교 교내특별과제 연구비 지원을 받았음.

* 서울여자대학교 정보통신공학부

1. 서 론

전자거래를 진행함에 있어서, 사용자 개인의 신분 확인 및 보안 유지가 중요한 문제로 대두되고 있다. 스마트카드는 기존 카드가 행할 수 없었던 양방향 통신, 정보의 보호 기능 등을 수행할 수 있으며, 개인을 확인할 수 있고 이동성이 뛰어나며 마그네틱 카드와 비교하여 복제가 어렵고, 암호 알고리즘을 카드 내부에서 수행하여 보안상 뛰어난 이점을 갖고 있다 [1,2,3]. 이렇게 전자 지불 시스템에서 유용하게 사용될 수 있는 스마트카드는 그 응용의 범위가 매우 광범위한데, 서비스 이용자들에게 카드가 발행된 후에 카드 자체의 불안정으로 인하여 문제가 발생할 경우 그 관리가 매우 어렵게 된다. 그러므로 카드가 생산되거나 발행되기 전에 카드에 정의된 기능 및 서비스의 수행 여부 및 예외 조건 처리 능력 등을 검증하기 위하여 미리 카드의 품질을 시험하는 것은 반드시 필요하다 [9].

스마트카드의 기능 시험에 대한 연구로는, ISO/IEC 표준화 단체에서 1998년경부터 표준 문서를 개발하는 작업을 진행하고 있고 [4-9], 국내에서는 한국표준협회에서 ISO/IEC 표준 문서를 번역한 KS 표준 문서를 작성 배포하였으며 [10-15], 한국정보보호진흥원 등에서 제품평가방법의 일환으로 지침에 대한 연구를 진행 중이다 [16,17]. 한편, 한국도로공사에서는 ISO/IEC 표준 문서에 기반한 자사의 하이패스플러스카드에 대한 시험인증지침서를 작성 보유하고 있다 [19].

본 논문에서는 스마트카드 기능 시험에 대한 기존 연구내용들을 살펴보고, 한국도로공사의 하이패스플러스카드에 대하여 기능 및 보안 시험을 수행한 내용을 소개한다. 우선, 하이패스플러스카드의 기능을 시험 평가하기 위한 시험 방법 및 절차와, 시험 방법에 맞는 시험 표준항목을 개발한 내용, 다음으로 선정된 시험 표준항목을 평가하기 위한 시험모듈 개발 내용, 그리고 이 모듈에 의해서 하이패스플러스카드를 시험하고 분석한 결과를 소개한다. 이와 같이, 하이패스플러스 카드에 시험 평가를 수행함으로써 안정적인 기능성과 보안성을 가진 카드 시스템을 확보할 수 있고 나아가 신뢰성 있는 보안 제품의 개발에 기여하리라 기대된다. 또한, 본 논문에서 소개하는 하이패스플러스 카드 시험은 국내에서는 최초로 수행된 스마트카드 시험에 대한 연구로, 향후 좀더 보완된 시험 방안에 대한 연구의 기반을 제공하리라 기대된다.

본 논문은 다음과 같이 구성되어 있다. 우선 2 장에서는 연구의 배경으로써, 스마트카드의 정의 및 개괄적인 내용과 하이패스플러스 카드의 활용법, 그리고 카드의 시험 방법에 대한 기존 연구 내용을 ISO/IEC 표준 문서 및 KS 표준 문서, 한국도로공사 카드 품질시험인증 지침서를 기반으로 살펴본다. 그리고, 한국도로공사 카드 품질시험인증 지침서에 기반한 시험 모듈 구성 및 시험 결과를 기술한다. 이의 세부 내용으로는 3 장에서 카드 시험 방법 및 절차를 기술하고 4 장에서 시험 항목 선정 결과를 5 장에서 시험 모듈 구성 내용을 6 장에서 시험 결과 및 이의 분석 내용을 기술하는 것이다. 끝으로 7 장에서 결론 및 향후 연구 내용을 소개한다.

2. 연구 배경

2.1 스마트카드

스마트카드는 신용카드와 같은 크기를 갖는 플라스틱 카드로, 마이크로 칩이 내장되어 있어서 데이터를 적재할 수 있으며 이 정보를 이용하여 전화 걸기나 전자지불시스템 등의 응용에 이용된다. 적재된 데이터는 추후의 이용을 위해 주기적으로 재충전 된다 [1,2,3].

스마트카드가 이용되는 응용은 다음과 같다.

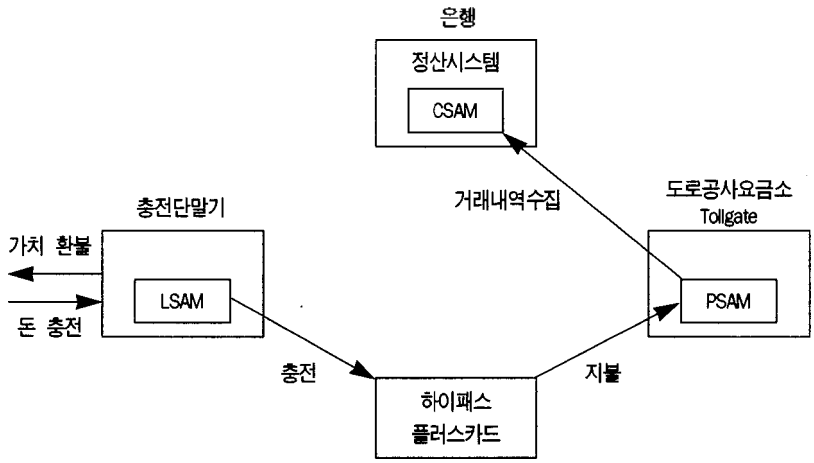
- 이동전화기를 이용하여 전화할 때 전화 호출 당 과금 정책 사용 시
- 인터넷 접속 공급자 (internet access provider)나 온라인 은행에 로그인할 경우
- 주차구역에 주차하거나, 지하철, 기차, 버스 등을 이용하여 요금 지불시
- 병원의 의사에게, 자신의 병력정보를 제출할 때
- 웹상의 전자 상점에서 물품을 구입할 때 (일종의 전자화폐로 이용됨)
- 가스 판매소에서 가스를 주입할 때.

현재 이미 전 세계적으로 10억 개 이상의 스마트카드가 사용되고 있으며, 연구기관들에 따르면 2005년까지는 265억 개 이상이 사용되리라 예측되고 있다. Compaq과 Hewlett-Packard는 스마트카드 슬롯을 내장한 키보드를 개발하고 있으며, Bull, Gemplus, Schlumberger 등은 스마트카드와 이를 읽을 수 있는 장치를 만드는 하드웨어를 개발하고 있다 [2].

스마트카드의 내부는 CPU, ROM, RAM, EEPROM으로 구성되어 있다. CPU는 8/16/32 비트 마이크로프로세서로, RSA 전용 프로세서 등의 cryptoprocessor를 옵션으로 보유한다. ROM에는 운영체제인 COS (Card Operating System)와 3DES 등의 보안 알고리즘이 적재되어 있으며 이들은 카드 제작시 저장되며 추후 수정은 불가하다. ROM의 용량은 16Kbytes, 32Kbytes 등이다. RAM은 임시 데이터 저장용으로 카드에 전력이 공급되는 동안 데이터의 보관이 가능하다. RAM의 용량은 4Kbits 이상이다. EEPROM에는 파일 시스템과 응용 프로그램, 키, 비밀번호 등이 저장되며 카드에 전력이 공급되지 않아도 데이터를 계속 보관할 수 있다. EEPROM의 용량은 4~16Kbytes 이다. 스마트카드의 CPU는 단일칩으로 구성되어 내부 시그널을 감지하기가 매우 어려우며 제작 단계에서 물리적/논리적으로 잠금되어 잠금을 풀어 내부구조를 재구성할 수가 없다.

2.2 한국도로공사 하이패스플러스카드

한국도로공사는 선불방식의 일회성 플라스틱 카드의 문제점을 극복하기 위해서, 스마트카드를 이용한 선불식 전자지불 시스템을 구축하고 있다. 스마트카드형 전자지불카드인 하이패스플러스카드의 가능은 기존의 선불기능과 하이패스 기능 뿐 아니라 일반 가맹점에서도 사용가능하도록 설계되었다. 한국형 전자지불 표준 SAM (Secure Application Module)과의 지불거래기능이 구현되어있어서 향후에 서울시에서 추진하는 지방자치단체카드뿐 아



〈그림 1〉 하이패스플러스카드를 이용한 충전/지불 방식

니라 여러 지방자치단체가 추진하는 카드와도 호환이 가능하다 [17]. 또한, 물리적으로는 하이패스플러스카드는 접촉식 및 비접촉식 기능이 가능하다.

하이패스플러스카드는 〈그림 1〉과 같이 LSAM (Load Secure Application Module)에 의해서 가치를 저장받고, PSAM (Purchase Secure Application Module)에 가치를 지불하는 방식이다. 지불된 가치는 CSAM (Check Secure Application Module)에 의하여 정산이 이루어진다. 따라서, 하이패스플러스카드의 시험 인증은 LSAM 및 PSAM과의 상호기능을 시험하면 된다 [17,18].

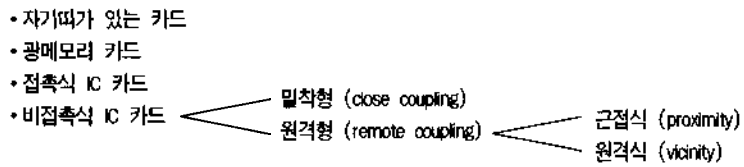
2.3 스마트카드 시험 방법

ISO/IEC에서는 식별카드(Identification Card)[1]의 시험 방법에 대한 문서를 제공하고 있으며 [4-9], 국내에서는 한국표준협회에서 이를 번역한 KS 표준 문서를 작성/배포하고 있다 [10-15]. 이들 시험 문서들은 일반특성시험과 카드 종류 별 시험 문서로 구성되어 있다.

일반특성시험 문서[4,10]는 외형의 평면성 변형이나 벗김 강도 (구조적으로 인접해 있는 층들을 분리할 때 이에 대한 카드의 저항 정도) 등 카드의 일반적인 특성에 대한 시험 내용을 기술한 것으로, ID카드의 생산업체나 ID카드를 이용하여 서비스를 제공하는 기관이나 업체에 적용될 수 있다.

ID 카드의 종류는 〈그림 2〉와 같이 자기띠가 있는 카드, 광메모리 카드, 접촉식 IC카드, 비접촉식 IC카드 등으로 나눌 수 있고 비접촉식 IC카드는 다시 밀착형 (close coupling)과 원격형(remote coupling)으로 나뉘어지고 원격형은 접근거리에 따라 근접식(proximity)과 원격식(vicinity)으로 나뉜다. 각 카드 종류의 특성을 고려한 시험문서는

1) 식별카드란 자기띠 카드, 광카드, IC카드 등을 모두 포함하는 것으로, 이 중 마이크로 칩이 내장된 IC카드가 보통 스마트카드로 불린다.



〈그림 2〉 식별카드 종류

〈표 1〉 ID카드 시험방법 관련 표준 문서들

	ICO문서번호	ISO/IEC문서 번호
일반특성시험방법	KSXISOIEC 10373-1	ISO/IEC 10373-1
자기띠가 있는 카드 시험방법	KSXISOIEC 10373-2	ISO/IEC 10373-2
광메모리 카드 시험 방법	KSXISOIEC 10373-5	ISO/IEC 10373-5
접촉식 IC카드 시험방법	KSXISOIEC 10373-3	ISO/IEC 10373-3
비접촉식 원격형-근접식 IC카드 시험방법	KSXISOIEC 10373-6	ISO/IEC 10373-6
비접촉식 중 원격형-원격식 IC카드 시험방법	KSXISOIEC 10373-7	ISO/IEC 10373-7

카드 종류 별로 별도로 구성되어 있다. 이들 시험문서 구성을 도식화하여 표현하면 〈표 1〉과 같다.

한편, 한국도로공사에서는 ISO/IEC 10373-1과 ISO/IEC 10373-6에 근거한 카드 품질시험인증 지침서를 작성하였는데 [19], 이 문서에서는 품질 시험 항목을 물리 시험, 기능 시험, 보안 시험, 속도 시험의 4 가지로 구분하고 있다.

〈표 2〉에 이 지침서에서 정의하고 있는 시험 항목들이 나타나 있다. 본 논문에서는 이 지침안 중 하이패스플러스카드와 LSAM, PSAM 간의 기능 시험과 보안 시험 지침을 따르는 시험 모듈을 구성하고 시험을 수행한 결과를 제시한다.

3. 시험 방법 및 절차

하이패스플러스카드 시험은 ISO/IEC 10373-1과 ISO/IEC 10373-6에 근거한 카드 품질시험인증 지침서[19]에 기반하여 수행하였는데, 표 2의 시험 항목 들 중 *로 표시된 하이패스플러스카드와 PSAM 간의 기능 및 보안 시험, 하이패스플러스카드와 LSAM 간의 기능 및 보안 시험에 대하여 진행하였다.

하이패스플러스카드 기능 시험은 〈표 3〉과 같이 PSAM 및 LSAM과의 시험으로 구분하여 구성하였고, 보안 시험은 각 시험 중에 검사한다.

3.1 L2H (가치저장 기능 및 보안) 시험 방법 및 절차

〈표 2〉 한국도로공사 하이패스플러스카드 카드 품질시험 항목

대분류	중분류	소분류
물리시험		
기능 시험	하이패스플러스카드와 LSAM 기능시험	• 가치저장시험* (정상동작시험, 가치저장금액이 가치저장 한도 금액을 초과한 경우 시험, 비정상동작 시험) • 가치재저장시험 (정상동작시험, 가치저장금액이 가치환불한도 금액을 초과한 경우 시험, 비정상동작시험)
	하이패스플러스카드와 PSAM 기능시험	• 일반/하이패스 지불거래시험 (정상동작시험, 가치지불 금액이 가치지불한도금액을 초과한 경우 시험, 비정상동작시험) • 표준 SAM 지불거래 시험* (정상동작시험, 가치지불금액이 가치지불한도 금액을 초과한 경우 시험, 비정상동작 시험) • 표준 SAM 지불재거래 시험 (정상동작시험, 가치지불금액이 가치지불 한도 금액을 초과한 경우 시험) • 파라미터 갱신 시험 (정상동작시험, 비정상동작시험)
	하이패스플러스카드와 PPSAM 기능시험	• 가치저장시험 • 가치환불시험
	LSAM과 PPSAM 기능시험	• 가지저장시험 • 가치환불시험
	PSAM과 CSAM 기능시험	• 정상동작시험 • 비정상동작시험
보안 시험	하이패스플러스카드와 LSAM 보안시험	• 가치저장시험* (서명시험, 암호화/복호화시험) • 가치재저장시험 (서명시험, 암호화/복호화시험)
	하이패스플러스카드와 PSAM 보안시험	• 일반/하이패스 지불거래 시험 (서명시험, 암호화/복호화시험) • 표준SAM 지불거래 시험* (서명시험, 암호화/복호화시험) • 표준SAM 지불재거래 시험 (서명시험, 암호화/복호화시험) • 파라미터갱신시험 (서명시험, 암호화/복호화시험)
	하이패스플러스카드와 PPSAM 보안시험	• 가치저장시험 • 가치환불시험
	LSAM과 PPSAM 보안시험	• 가치저장시험 • 가치환불시험
	PSAM과 CSAM 보안시험	• 서명시험 • 암호화/복호화시험
속도시험		

LSAM (Load Secure Application Module)
PSAM (Purchase Secure Application Module)
PPSAM (Purse Provider Secure Application Module)
*본 논문에서 소개하는 시험 내용이다

〈표 3〉 하이패스플러스카드 시험종류

대분류	중분류	시험명
LSAM과의 시험	가치저장 시험 (LSAM에 의한 가치저장 시험)	L2H (가치저장)
PSAM과의 시험	비접촉식지불거래 시험 (비접촉식 표준SAM 지불거래 시험)	H2P (표준SAM)
보안 시험	서명 확인 시험	L2H 및 H2P 시험시 동시에 진행
	암호화 시험	

LSAM에 의해서 하이패스플러스카드에 가치가 저장되는 개략적인 흐름은 〈그림 3〉과 같다 [17,18]. 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 전달하는 지를 시험하는 서명확인 시험 방법 및 절차는 $A4_S$, $C4_S$, $C7_S$, $A8_S$, $A10_S$, $C9_S$, $C11_S$ 순으로 시험하며, LSAM과 하이패스플러스카드 간에 가치를 저장하는 동안에 LSAM과 하이패스플러스카드가 전달하는 정보가 정확하게 암호화 및 복호화가 이루어지는 지를 시험하는 암호화 시험 방법 및 절차는 $A3_C$, $C3_C$, $C6_C$, $A7_C$ 순으로 시험한다.

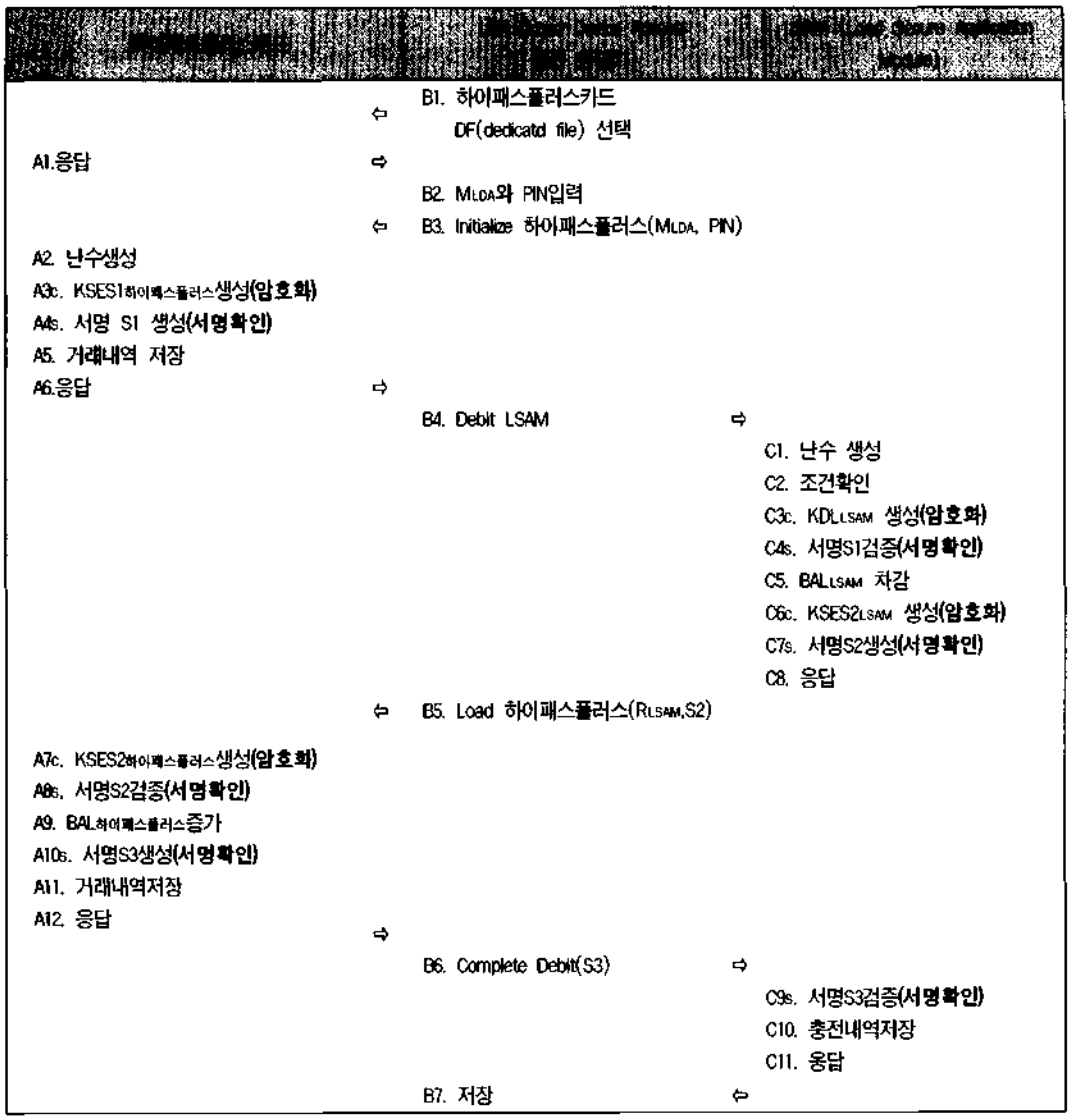
3.2 H2P (표준 SAM 기능 및 보안) 시험 방법 및 절차

H2P (표준SAM)은 〈그림 4〉와 같이 비접촉식 교통 표준 SAM과의 거래를 시험한다 [17,18].

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 PSAM 간에 가치를 저장하는 동안에 정확하게 정보를 전달되는 지를 시험하는 서명확인 시험 방법 및 절차는 $A3_S$, $C3_S$, $C5_S$, $A6_S$, $A8_S$, $C7_S$ 순으로 시험하며, 하이패스플러스카드와 PSAM 간에 가치를 저장하는 동안 전달하는 정보가 정확하게 암호화 및 복호화가 이루어지는 지를 시험하는 암호화 시험 방법 및 절차는 $A2_C$, $C2_C$, $C4_C$, $A5_C$ 순으로 시험한다.

4. 시험 표준항목 선정

3. 시험 종류 및 방법에서 결정된 사항에 의하여 하이패스플러스카드의 PSAM과의 연관 기능을 시험하고 평가하기 위해서 다음과 같

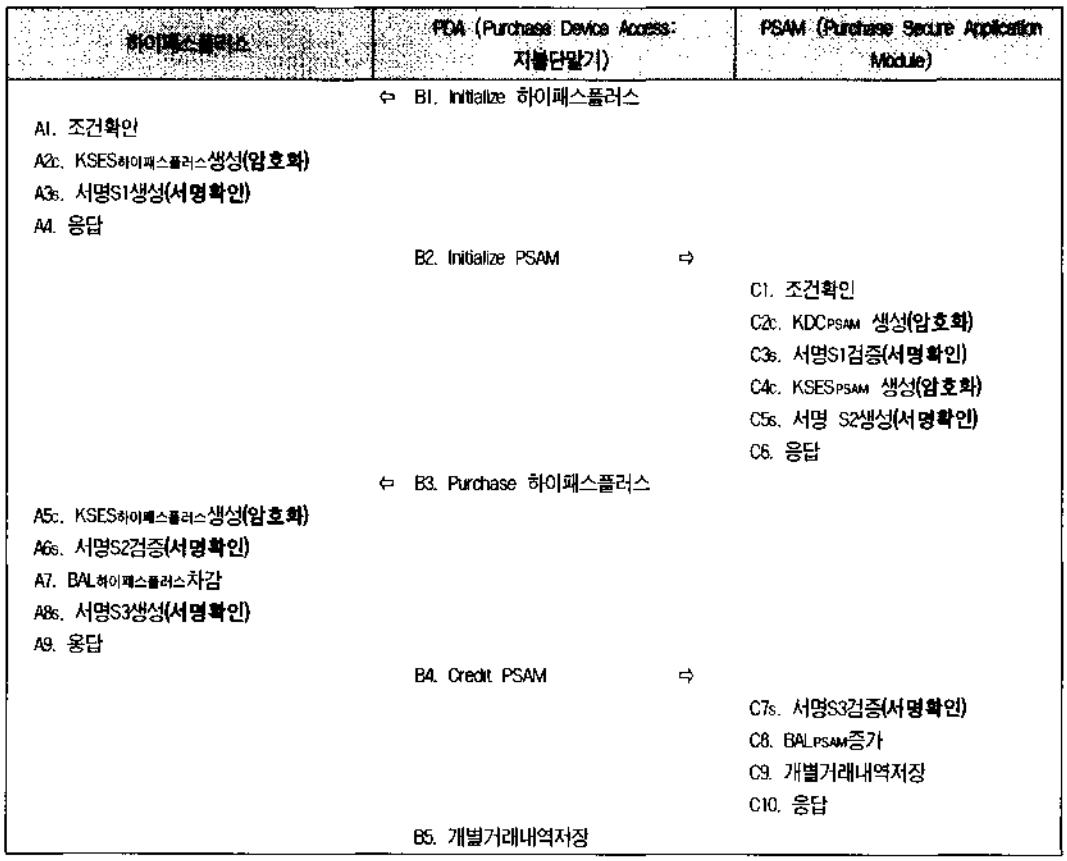


〈그림 3〉 LSAM과 하이패스플러스카드 간의 가치저장 흐름도

은 시험 표준항목을 결정하였다.

4.1 L2H (가치저장 기능 및 보안) 시험 표준 항목

〈그림 3〉에서 L2H(가치저장) 시험은 A1부터 A12, B1부터 B7, 그리고 C1부터 C12까지의 모든 항목에 걸쳐서 이루어진다. 이 중, B1과 B2는 B3에 의해서 검증되므로, B1, B2, B3를 대표해서 B3를 시험한다. 또한, $A2_C$는 $A3_S$과 A4에서 사용되는 것으로 별도의 시험이 필요없고, $A3_S$은 A4에 의해서 검



〈그림 4〉 PSAM과 하이패스플러스카드의 표준 SAM 지불거래 흐름도

증되므로 $A2_c$, $A3_s$, A4를 대표해서 A4를 시험한다. 마찬가지로 A7은 $A8_s$에 의해서 검증되므로 A7, $A8_s$을 대표해서 $A8_s$을 검증한다. C1과 $C2_c$는 $C3_s$과 $C4_c$에 의해서 검증되므로 시험할 필요가 없고, $C3_s$는 $C4_c$에 의해서 검증되므로 전체적으로 C1, $C2_c$, $C3_s$, $C4_c$를 대표해서 $C4_c$ 기능을 시험한다. 또한, C6은 $C7_s$에 의해서 검증되므로 C6, $C7_s$을 대표해서는 $C7_s$를 시험한다. 이와 같이, 시험 순서에 따른 주요 표준항목들은 〈표 4〉와 같다:

4.2 H2P (표준 SAM 기능 및 보안) 시험 표준 항목

〈그림 4〉에서 H2P(표준SAM) 시험은 A1부터 A9, B1부터 B5, 그리고 C1부터 C10까지의 모든 항목에 걸쳐서 이루어진다. 하지만, 이 모든 과정 중에서 A1과 $A2_c$는 $A3_s$에 의해서, A4는 B2에 의해서, C1,$C2_c$, $C3_s$, 그리고 $C4_c$는 $C5_s$에 의해서, C6은 B3에 의해서, $A5_c$, $A6_s$은 $A8_s$에 의해서, A9는 B4에 의해서, C10은 B5에 의해서 각각 검증되므로 주요항목만 시험하면 된다. 이와 같이,

시험 순서에 따른 표준항목들은 〈표 5〉와 같다.

5. 시험 모듈 개발

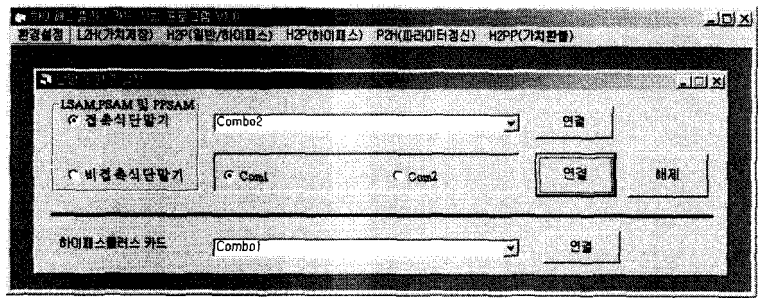
3 장 및 4 장에서 결정된 시험 방법 및 시험 표준항목을 이용하여 하이패스플러스카드를 시험하고 평가하기 위해서 다음과 같은 시험 모듈을 개발하였다. 개발에 사용한 언어는 Visual Basic 6.0이다.

〈표 4〉 L2H (가치저장) 시험 순서에 따른 기준 및 표준항목

지침서 시험 기준 [19]	시험 표준항목
기능시험	B3. Initialize 하이패스플러스
[illegible]	[illegible]
기능시험	B4. Debit LSAM
기능시험	C5. BALLSAM
[illegible]	[illegible]
기능시험	B5. Load 하이패스플러스
기능시험	A9. BAL하이패스플러스
[illegible]	[illegible]
기능시험	B7. 저장

〈표 5〉 H2P (표준SAM) 시험 순서에 따른 기준 및 표준항목

지침서 시험 기준 [19]	시험 표준항목
기능시험	B1. Initialize 하이패스플러스
[illegible]	[illegible]
기능시험	B2. Initialize PSAM
[illegible]	[illegible]
기능시험	B3. Purchase 하이패스플러스
기능시험	A7. BAL하이패스플러스차감
[illegible]	[illegible]
기능시험	B4. Credit PSAM
기능시험	C9s. 개별거래내역저장
기능시험	B5. 개별거래내역저장



〈그림 5〉 하이패스플러스 카드 시험환경 사용자인터페이스 화면

5.1 시험 환경 설정 모듈

하이패스플러스카드를 시험하기 위해서 LSAM과 PSAM을 연결하기 위한 환경을 설정하기 위한 모듈을 구성하였는데, 하이패스플러스카드는 Combo1에 삽입하고, LSAM과 PSAM은 Combo2에 삽입하여 시험하도록 하였다. 〈그림 5〉는 이렇게 구성한 환경설정 모듈의 사용자 인터페이스 화면이다.

5.2 L2H (가치저장 기능 및 보안) 시험 모듈

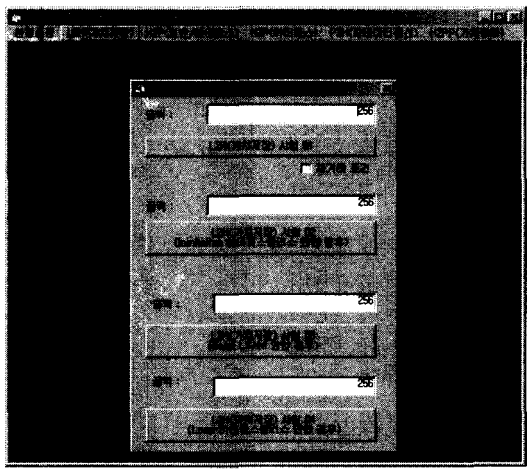
LSAM에서 하이패스플러스카드에 가치를 저장하는 L2H(가치저장) 시험 모듈은 원하는 가치가 정상적으로 저장되는 지를 시험하기 위한 모듈이다. L2H(가치저장) 시험의 시험 모듈은 Initialize 하이패스플러스가 하이패스플러스카드에서 수행되고 이에 의해서 서명S1이 생성되며, Debit LSAM이 LSAM에 전달되고, BAL_{LSAM}이 원하는 가치만큼 감소되며, 서명S2가 생성되고, Load 하이패스플러스가 하이패스플러스카드에 전달되어 $BAL_{하이패스플러스}$가 원하는 가치만큼 증가되며, 서명S3이 생성되는 지를 검사한다. 〈그림 6〉은 이의 슈도 코드이며 〈그림 7〉은 LSAM에서 하이패스플러스카드에 가치를 저장하는 시험을 위해 구현한 모듈의 사용자 인터페이스 화면이다.

5.3 H2P (표준 SAM 기능 및 보안) 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 $BAL_{하이패스플러스}$가 지정된 가치만큼 감소되며, 서명 S3가 생성되고, Credit PSAM이 PSAM에 전달되어 BAL_{PSAM}이 지정된 가치만큼 증가되며, 개별거래내역이 저장되는 지를 검사한다. 〈그림 8〉은 이의 슈도 코드이며 〈그림 9〉는 하이패스플러스카드에서 PSAM에 가치를 지불하는 시험을 위해 구현한 모듈의 사용자인터페이스 화면이다.

```
시험 모듈 L2H
// L2H (가치저장 기능 및 보안) 시험 모듈 슈도 코드
[하이패스플러스카드] LDA의 요청에 의하여 hiphpassplus 카드 초기화
[하이패스플러스카드] 서명 S1 생성
[LSAM]              Debit LSAM 요청을 받음
[LSAM]              BALLSAM이 원하는 가치만큼 감소됨
[LSAM]              서명 S2 생성
[하이패스플러스카드] Load 하이패스플러스가 하이패스플러스카드에 전달됨
[하이패스플러스카드] BAL하이패스플러스가 원하는 가치만큼 증가됨
[하이패스플러스카드] 서명 S3 생성
```

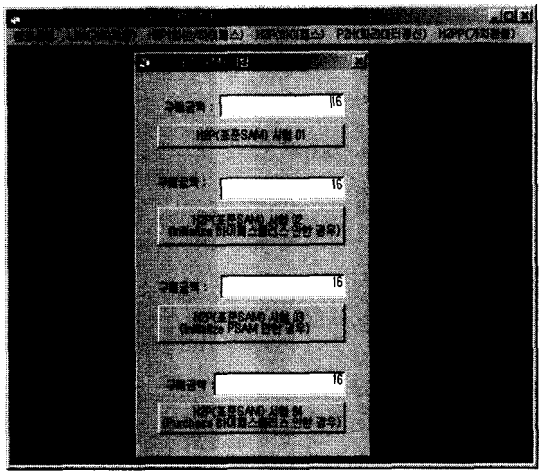
〈그림 6〉 L2H (가치저장 기능 및 보안) 시험 모듈 슈도 코드



〈그림 7〉 L2H (가치저장) 시험 모듈 사용자인터페이스 화면

```
시험 모듈 H2P
// H2P (표준 SAM 기능 및 보안) 시험 모듈 슈도 코드
[하이패스플러스카드] PDA의 요청에 의하여 hiphpassplus 카드 초기화
[하이패스플러스카드] 서명 S1 생성
[PSAM]              Initialize PSAM 요청을 받음
[PSAM]              서명 S2 생성
[하이패스플러스카드] Purchase 하이패스플러스가 하이패스플러스카드에 전달됨
[하이패스플러스카드] BAL하이패스플러스가 지정된 가치만큼 감소됨
[하이패스플러스카드] 서명 S3 생성
[PSAM]              Credit PSAM 요청을 받음
[PSAM]              BALPSAM이 지정된 가치만큼 증가
[PSAM]              개별거래내역 저장
```

〈그림 8〉 H2P (표준SAM) 시험 모듈 슈도 코드



〈그림 9〉 H2P (표준SAM) 시험 모듈 사용자인터페이스 화면

6. 시험 결과 및 분석, 평가

하이패스플러스카드, LSAM, PSAM 등은 한국도로공사에 사용하는 카드를 이용하였고, 시험 모듈은 5 장에서 기술한 개발 모듈을 이용하여, 하이패스플러스 카드의 기능 시험을 수행하였다. 본 시험은 상온에서 시행한다.

6.1 L2H (가치저장) 시험 결과 및 분석 평가

6.1.1 L2H (가치저장) 시험 결과

L2H (가치저장) 시험 결과는 〈표 6〉과 같다.

6.1.2 L2H (가치저장) 시험 분석 평가

- [기능시험] B3. Initialize 하이패스플러스
  저장하고자 하는 가치는 10진수로는 256_{DEC} 또는 16진수로 100_{HEX}이다. 가치저장 전 LSAM 값은 16진수로 $0FFFDC50_{HEX}$이며, 하이패스플러스카드의 값은 00000320_{HEX}이다. 시험결과 Initialize 하이패스플러스가 정상적으로 수행됨을 확인하였다.
- [보안시험] $A4_S$. 서명 S1생성
  서명S1의 16진수값 $F4A87659_{HEX}$이 생성되었다.
- [기능시험] B4. Debit LSAM, 기능시험 C5. BAL_{LSAM} 차감
  Debit LSAM, BAL_{LSAM} 차감 기능에 의하여 LSAM의 가치가 $0FFFDB50_{HEX}$가 정상적으로 바뀌었다.
- [보안시험] $C7_S$. 서명 S2생성
  서명 S2 생성에 의하여 서명 S2는 16 진수값 B0D95A07가 생성되었다.
- [기능시험] B5. Load 하이패스플러스
  Load 하이패스플러스가 정상적으로 수행되었다.
- [기능시험] A9. $BAL_{하이패스플러스}$ 증가
  $BAL_{하이패스플러스}$ 증가에 의해서 $BAL_{하이패스플러스}$가 00000320_{HEX}에서 00000420_{HEX}으로 증가

하였다.

- [보안시험] $A10_S$. 서명 S3생성
  서명S3생성에 의해서 서명 S3의 16진수 값 A605231C이 생성되었다. 또한, B3, B4, B5가 잘못된 경우에는 실행이 중단되었다.

이상과 같이, L2H (가치저장) 시험을 수행한 결과, 한국도로공사에서 사용하는 하이패스플러스카드는 L2H (가치저장) 시험을 통과함을 확인할 수 있다.

6.2 H2P (표준 SAM) 시험 결과 및 분석 평가

6.2.1 H2P (표준 SAM) 시험 결과

H2P (표준 SAM) 시험 결과는 〈표 7〉과 같다.

6.2.2 H2P (표준 SAM) 시험 분석 평가

- [기능시험] B1. Initialize 하이패스플러스
  지불 금액은 10진수 16_{DEC}이고 16진수로는 10_{HEX}인 값을 지불하고자 한다. 'Initialize 하이패스플러스'를 실행한 결과, 하이패스플러스카드의 $NT_{하이패스플러스}(4)$는 $000000AE_{HEX}$이고, $BAL_{하이패스플러스}(4)$는 $000004A0_{HEX}$이다. 따라서, 시험을 종료한 후의 $NT_{하이패스플러스}(4)$는 $000000AF_{HEX}$이고, $BAL_{하이패스플러스}(4)$는 $000004B0_{HEX}$이 되어야 한다.
- [보안시험] $A3_S$. 서명 S1 생성
  서명S1의 값은 $AB8B81B0_{HEX}$이 생성되었다.
- [기능시험] B2. Initialize PSAM
  'Initialize PSAM'을 실행한 결과, NT_{PSAM}

〈표 6〉 L2H(가치저장) 시험 결과

시험절차	시험 프로토콜	시험 목표 (기준값)	시험 결과
가정	가치저장전 금액(LSAM)	0FFFDC50	
	가치저장전 금액(하이패스플러스)	00000320	
기능시험	B3. Initialize 하이패스플러스	NT하이패스플러스(4) R하이패스플러스(8)	00000092 95682235849FC2AC
[redacted]			
기능시험	B4. Debit LSAM		
기능시험	C5. BAL_{LSAM} 차감	가치저장후 금액	0FFFDB50
[redacted]			
기능시험	B5. Load 하이패스플러스		
기능시험	A9. $BAL_{하이패스플러스}$ 증가	00000420	00000420
[redacted]			
기능시험	B7. 저장		

은 0000006B$_{HEX}$이고, PSAM의 가치저장 전 금액은 00001158$_{HEX}$이었다. 따라서, 시험이 종료된 후의 NT$_{PSAM}$은 0000006C$_{HEX}$이고, PSAM의 가치저장 전 금액은 00001168$_{HEX}$이 되어야 한다.

- [보안시험] C5$_S$. 서명 S2 생성
  서명S2은 57E5656B$_{HEX}$이 생성되었고, NT$_{PSAM}$은 0000006C$_{HEX}$이고, PSAM의 가치저장 전 금액은 00001168$_{HEX}$이 되어서, 예상한 결과와 일치하였다.
- [기능시험] A7. BAL$_{하이패스플러스}$ 차감
  'BAL$_{하이패스플러스}$ 차감' 결과, NT$_{하이패스플러스}$(4)는 000000AF$_{HEX}$이 되었고, BAL$_{하이패스플러스}$(4)은 000004B0$_{HEX}$이 되어서 예상한 결과와 일치하였다.
- [보안시험] A8$_S$. 서명 S3 생성
  서명S3은 846843F0이 생성되었다. 또한, B1, B2, B3, 그리고 B4를 실행하지 못한 경우에는 시험이 중단되어서 원하는 결과와 일치하였다.

이상과 같이, H2P (표준SAM) 시험을 수행한 결과, 시험이 정상적으로 이루어졌고, 한국도로공사에서 사용하는 하이패스플러스카드는 H2P(표준 SAM) 시험을 통과함을 확인할 수 있다.

〈표 7〉 H2P (표준SAM) 시험 결과

시험절차	시험 표준항목	시험 목표 (기준값)	시험 결과
가정	가치저장전금액(하이패스플러스카드) NTPSAM 가치저장전금액(PSAM)	000004A0 0000006B 00001158	
기능시험	B1. Initialize 하이패스플러스	NT하이패스플러스(4) BAL하이패스플러스(4)	000000AE 000004A0
[redacted]	[redacted]	[redacted]	[redacted]
기능시험	B2. Initialize PSAM		
[redacted]	[redacted]	[redacted]	[redacted]
기능시험	NTPSAM B3. Purchase 하이패스플러스	0000006C 00001168	0000006C 00001168
기능시험	A7. BAL하이패스플러스차감	NT하이패스플러스(4):000000AF BAL하이패스플러스(4):000004B0	NT하이패스플러스(4):000000AF BAL하이패스플러스(4):000004B0
[redacted]	[redacted]	[redacted]	[redacted]
기능시험	B4. Credit PSAM		
기능시험	C9. 개별거래내역저장		
기능시험	B5. 개별거래내역저장		

7. 결 론

본 논문에서는, 전자지불 시스템에서 유용하게 사용될 수 있는 스마트카드를 시험하기 위한 기존 ISO/IEC 표준 문서 및 KS 표준 문서들의 내용을 살펴보고, 이들 표준 문서에 기반한 한국도로공사 카드 품질시험인증 지침서에 따른 한국도로공사 하이패스플러스 카드의 시험 모듈을 구성하고 시험을 수행한 결과를 제시하였다. 하이패스플러스 카드에 시험 평가를 수행함으로써 안정적인 기능성과 보안성을 가진 카드 시스템을 확보할 수 있고 나아가 신뢰성 있는 보안 제품의 개발에 기여하리라 기대된다.

하이패스플러스 카드의 기능 시험은 국내에서는 최초로 수행된 스마트카드에 대한 시험으로 향후 스마트카드 시험 방안에 대한 연구기반을 제공하리라 기대된다. 향후 좀더 체계적인 시험을 위하여 시험 절차 및 방법에 대한 표준화 연구 및 시험 결과를 인증하는 기준 및 절차에 대한 연구가 필요할 것으로 보인다.

참 고 문 헌

[1] 황선태, 이 형, "스마트카드 모델의 기준에 관한 연구", 한국 CALS/EC 학회지 제 4권 제 3호 1999.

[2] smart card - www.whatis.com, 2003.

[3] (주) 스마트카드연구소, 스마트카드 기술 동향 및 활용사례, 2001.

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

[5] ISO/IEC 10373-2. Identification cards - Test methods: Part 2. Cards with magnetic strips, 1998.

[6] ISO/IEC 10373-3. Identification cards - Test methods: Part 3. Integrated circuit(s) cards with contacts and related interfacc devices, 2001.

[7] ISO/IEC 10373-5. Identification cards - Test methods: Part 5. Optical memory cards, 1998.

[8] ISO/IEC 10373-6. Identification cards - Test methods: Part 6. Proximity cards. 2001.

[9] ISO/IEC 10373-7. Identification cards - Test methods: Part 7. Vicinity cards, 2001.

[10] KSXISOIEC 10373-1. ID 카드 - 시험 방법 - 제 1부: 일반 특성 시험, 1999.12.29

[11] KSXISOIEC 10373-2. ID 카드 - 시험 방법 - 제 2부: 자기 띠가 있는 카드, 1999. 12. 29.

[12] KSXISOIEC 10373-3. ID 카드 - 시험 방법 - 제 3부: 접촉식 IC 카드와 관련 인터페이스 장치, 2002. 12. 23

[13] KSXISOIEC 10373-5. ID 카드 - 시험 방법 - 제 5부: 광메모리 카드, 1999. 12. 29

[14] KSXISOIEC 10373-6. ID 카드 - 시험 방법 - 제 6부: 근접식 카드 (proximity card), 2002. 12. 23.

[15] KSXISOIEC10373-7. ID 카드 -시험 방법 - 제 7부: 원격식 카드 (vicinity card), 2002. 12. 23.

[16] 이태승, 신규평가대상제품평가방안, 한국정보보호진흥원, 2003. 9.

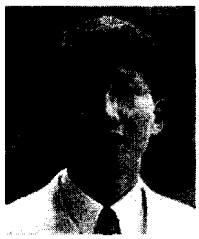
[17] 한국전자지불포럼단체표준, 비접촉식 전자화폐 판독기용 지불 SAM 규격(개정용-Issue 2.0), 2003. 8.

[18] 한국도로공사, 도로공사 전자카드 규격서 v 1.1, 2003. 12.

[19] 한국도로공사, 한국도로공사 하이패스 플러스카드 카드 품질시험인증 지침서, 2003. 12.

저 자 소 개

김윤정	(E-mail : yjkim@swu.ac.kr)
1991.	서울대학교 컴퓨터공학과 졸업(공학사)
1993.	서울대학교 대학원 컴퓨터학과 졸업(공학석사)
2000.	서울대학교 대학원 전기컴퓨터공학부 졸업(공학박사)
2000 ~ 2001.	(주) 앤써커뮤니티 제품개발연구소 차장
2001 ~ 2002.	(주) 데이타게이트 인터내셔널 보안기술연구소 차장
2002 ~ 현재	서울여자대학교 정보통신대학 정보통신공학부 교수
관심 분야	암호학, 시스템 보안, 암호 응용



이기한	(E-mail : knight@swu.ac.kr)
1987.	서강대학교 컴퓨터 공학과 졸업(학사)
1989.	서울대학교 대학원 컴퓨터공학과(공학석사)
1993.	서울대학교 대학원 컴퓨터공학과(공학박사)
1995 ~ 1999.	서울여자대학교 컴퓨터학과 조교수
1999 ~ 현재	서울여자대학교 컴퓨터학과 부교수
1998 ~ 현재	ISO/TC215 건강카드 대표위원
2001 ~ 현재	ISO/SC27 보안 전문위원
2002 ~ 현재	ISO/SC17 스마트카드 전문위원
관심 분야	스마트카드, 보안, 의료 정보, Bio-infomatics