국제통용운전면허증의 보안성과 운용성 강화를 위한 상호인증 및 운용 기법에 관한연구

정회원 전 상 훈*, 전 문 석**

The Mutual Authentication and Operation Methodology for an Enhanced Security and Operation of the IDL

Sang-hoon Jeon*, Moon-suk Jun** ***Regular Members***

요 약

국가 간에 이동하는 인구가 급증하고 있는 현재, 국내·외 운전면허증은 쉽게 복제가 가능하며, 위조된 면허증을 감지하기 어려운 문제점을 갖고 있다. 그리고 국가 상호간에 운전자의 법규 위반 사항을 관리하고 통제하기 어려운 불편함이 증가되고 있다. 운전면허증은 대부분의 국가에서 개인 신분 증명 수단으로 사용되고 있기 때문에 보안성 및 안전성이 그 무엇보다도 중요하며, 분실, 도용 도난으로 인한 부정사용 방지가 요구되고 있다. 따라서 본 논문은 ISO/IEC 18013-3에서 정의하고 있는 ICC가반 국제통용운전면허증의 보안성 및 운용성을 강화하는 효율적인 상호인증 및 운용기법을 제안한다.

Key Words : IDL(ISO Compliant Driving Licence), IC card, Mutual Authentication, Biometric, Security

ABSTRACT

In the modern world, where the number of people moving from country to country is sharply increasing, domestic and international driver's licenses are easily fabricated or forged, and distinguishing if a driver's license is legitimate or not is often a difficult task. Furthermore, this would require different countries to mutually share and administer the driving records of individuals, making it a much more complex task. (Added to it is the complicated matter of countries having to mutually share and administer the driving records of individuals.) However, the authenticity and security of a driver's license has become the first priority since driver's licenses are also used as identification cards in most countries, thus requiring measures to prevent inappropriate uses arising from theft and embezzlement. In this paper, we propose the mutual authentication mechanism which, can provide enhanced security and efficient operation that is administration of personal information contained within ISO Compliant Driving licence(IDL).

Ⅰ. 서 론

글로벌 시대가 가속화되고 국가 간의 이동인구의 증가함에도 불구하고 현행 운전면허증은 플라스틱 형태의 위·변조에 취약한 형태이다. 쉽게 복제, 변경 등이 가능하며, 위조된 면허증을 감지하기 어려운 것이 현실이다. 또한 국제적으로 통용되지 않아 종이로 된 소책자 형태의 국제운전면허증을 추가로 발

* 숭실대학교 일반대학원 컴퓨터학과 컴퓨터통신 연구실(securelayer@ssu.ac.kr),
** 숭실대학교 컴퓨터학과(mjun@ssu.ac.kr)
논문번호 : KICS2008-10-480, 접수일자 : 2008년 10월 30일, 최종논문접수일자 : 2009년 2월 4일

급받아야 하는 번거로움이 있다. 운전면허증은 국내 DDP(Domestic Driving Permit)와 국제 IDP(International Driving Permit) 두 가지를 사용한다. 그러나 국내 운전면허 허가가 정지되거나 취소되면 국제 운전면허 허가가 동시에 취소되어야 하지만 현행 운전면허 시스템은 허가 및 자격여부, 위반사항 등을 실시간 업데이트할 수 없는 한계를 가지고 있다. 전자운전면허증은 국제표준기구인 ISO에서 규정하고 있는 국제적으로 통용 가능한 운전면허 증명서 기능과 기존 운전면허의 기능을 갖춘 운전면허증으로 IDL(ISO Compliant Driving License)[5],[6],[7]이라 한다. IDL은 위·변조를 방지하기 위해 IC카드를 기반으로 하여 경찰 터미널 등을 통해 전자적으로 정보를 판독 및 기록이 가능한 운전면허증을 의미한다. IDL은 ISO/IEC 7816[8]표준명령어에 의해 동작하며, PIN(Personal Identity Verification) 인증방법을 이용하여 소지자를 인증 및 식별한다. 그러나 이러한 패스워드 기반의 PIN 인증방식은 개인식별기능으로서 매우 취약하며, 도난, 분실 등으로 인한 부정사용을 방지 할 수 없는 단점을 가지고 있다[1],[2][3],[4]. IDL은 터미널을 통해 운용 및 관리된다. 현행 터미널 운용방식 또한 도난, 분실로 인한 부정사용에 매우 취약하며, 터미널 관리를 위해 터미널 ID와 SAM(secure application module)[10]을 관리해야 한다. 그리고 추가적인 터미널 분실 정책과 같은 보안정책이 요구된다. 뿐만 아니라 터미널이 항상 온라인 상태를 유지해야 하기 때문에 네트워크 장애 시, IDL 소지자의 정보를 유지 및 관리하기 어려운 취약점을 가지고 있다[6],[7].

따라서 본 연구는 ISO/IEC JTC1/SC17 WG10에서 규정하고 있는 IC카드기반 IDL과 터미널의 위·변조, 도난, 분실 및 부정사용을 방지하며, 터미널의 네트워크 연결이 온·오프라인 모두 지원이 가능한 강화된 보안성과 운용성을 제공하는 상호인증 및 운용 기법을 제시하고자 한다. 본 논문은 Ⅱ절에서 국내·외의 전자운전면허증의 기술현황과 문제점을 살펴보고 Ⅲ절에서는 보안성과 운용성을 강화하기 위해 설계한 제안 상호인증구조 및 운용기법을 설명한다. 그리고 Ⅳ절에서 제안기법을 실험하여 현행 IDL과 제안기법을 비교하여 성능을 평가한다. 마지막으로 향후 연구방향을 제시하고 결론을 맺는다.

Ⅱ. 관련연구

이 장에서는 현행 운전면허증 및 국내·외의 전자운전면허증 관련 기술과 현황, 그리고 ISO/IEC JTC1/SC17 WG10에서 정의하고 있는 IC카드기반 IDL의 문제점에 대해 살펴보도록 하겠다.

2.1 국내·외 전자운전면허증 기술과 현황

IC카드는 반도체 칩을 내장하고 있는 카드를 IC카드라 한다. 단말기와 카드가 통신을 위해 전원공급, 데이터 입출력 포트 등의 단자를 가지고 있는 카드를 접촉식 IC카드(IC Card with Contact)라 하고, 단말기와 카드가 선이 연결되지 않고 비 접촉으로 통신을 하는 카드를 비접촉식 IC카드(Contactless IC Card)라 한다. IC카드는 스마트카드와 메모리카드로 구분되는데, 스마트카드는 마이크로프로세서를 내장하고 COS(Chip Operating System) 명령과 암호 알고리즘에 의해 높은 보안성을 보장하는 카드이다. 접촉식 IC카드는 ISO 7816에서 정의하고 있는 반도체 칩을 8개의 접점을 갖고 있는 COB(Chip On Board)에 실장하여 0.76mm 두께와 신용카드 크기의 플라스틱카드에 내장한 카드로 반도체 칩에 마이크로프로세서와 칩 운영체제를 기반으로 동작하는 스마트카드와 CPU가 없는 메모리카드로 구분되는데, 본 연구에서 말하는 스마트카드는 접촉식 IC카드를 말하며, COS 운영체제 하에서 ISO 7816 명령어와 구조에 의해 동작한다[8],[9].

전자운전면허증은 DDP와 IDP를 통합한 면허증으로 사진 및 인적사항, 발급일자, 면허종류, 발행기관의 공통 정보를 포함하고 있으며, 단말기를 통해 읽을 수 있도록 기계 식별용 기록매체 ISO 7816자기 띠, ISO 7816 접촉식 IC카드, ISO 14443 비접촉식 IC카드, 바코드, 2D바코드 등의 다양한 기록매체를 사용할 수 있으며, 국제표준 운전면허는 ISO 18013에서 정의하고 있다. 주요 내용은 운전면허증의 물리적인 특성, 사진, 성명 및 인적사항, 면허번호 및 종류 등 육안식별용 기재사항에 대한 기초 데이터 셋과 이 데이터를 기계적으로 읽기 위한 기록 수단(접촉식 IC카드, 비접촉식 IC카드, 바코드, 자기띠)을 포함하고 있다[5],[6],[7].

현재 국내에서 발행하는 운전면허는 경찰청에서 정한 면허증 형식에 맞추어 각 지방 경찰청장 명의로 발행되고 있으며, 현행 시스템과 향후 국제표준을 기반 하는 시스템의 차이점과 개선점 등을 세부적으로 협의 중에 있다. 국내 전자운전면허증 기술은 각 분야에서 상당한 수준의 기술력을 보유하고 있으며, 각 기술 분야별로 물리규격요소, 논리규격요소, 보안규격요소를 표 1에 나타내었다.

표 1. 국내 전자운전면허증 관련 기술현황

대분류	중분류	소분류	기술 현황
물리 규격 요소	IC카드 기술	IC카드 칩 기술	대용량 고성능 IC카드 칩을 개발하여 상용화하였음
		카드 외형기술	안테나 인레이 기술을 보유하고 있으나, 위조방지용 인쇄 기술 및 홀로그램 등의 기술은 주로 해외로부터 도입하고 있음
		단말기 기술	국내 몇몇 단말기 업체에서 다양한 단말기를 생산하고 있으며, 응용 서비스에 특화된 단말기들이 출시되고 있음
		서버 기술	외부 인터페이스 기술 및 인터넷 및 웹상 자료 처리 기술 등에서 지속적인 개발이 이루어지고 있음
	생체 인식 기술	생체정보 추출 기술 및 생체 정보 인식 기술	지문, 얼굴, 정맥 추출 단말기 및 복합 단말기에 대한 개발이 상당 부분 완료되었으며, 특히 지문 부분에서 국내 기업들의 기술 개발 수준이 높은 것으로 평가됨
논리 규격 요소	IC카드 기술	IC카드 COS 기술	다수의 국내 스마트카드 개발 회사에서 스마트카드 COS 및 Applet 기술을 보유하고 있으며, 응용 서비스 분야에서는 기술수준을 국제적으로 인정받고 있음
		단말기 처리 기술	국내 몇몇 단말기 업체에서 다양한 단말기를 생산하고 있으며, 응용 서비스에 특화된 단말기들이 출시되고 있음
		서버 및 시스템 운영 기술	발급 및 관리 시스템의 설계 및 구현에 경험이 많은 업체들이 있으며, 다양한 제품들이 출시되어 있음
	생체 인식 기술	생체정보 추출 기술 및 생체정보 인식 기술	추출 정보에 따른 템플릿 구성 기술, 생체인식 알고리즘 설계 기술에 대한 개발이 진행되어 지문 등에서는 이미 거의 완료된 상태이고, 최근에는 IC카드 상에서 생체정보를 인식하는 Match-on-Card 기술을 개발하고 있음
보안 규격 요소	물리 규격 요소	IC카드 칩 기술	암호처리용 보조연산기 설계 및 암호/인증 모듈 설계, 그리고 해킹방지 모듈 설계가 연구되고 있으며 부분적으로 구현되고 있음
		암호 처리 기술	
		인증 기술	
	논리 규격 요소	암호 처리 기술	암호 알고리즘 설계 기술 부분은 국내에서도 국제 표준인 SEED와 KS표준인 ARIA를 보유하고 있으며, 공개키 부분의 알고리즘의 구현기술도 보유하고 있음
		인증 기술	개인 인증 및 단말기/시스템 인증을 위한 다양한 기술이 개발되어 적용되고 있음. 생체인식 정보 및 PKD를 적용한 기술도 개발되고 있음
		시스템 운영 기술	시스템 차원의 보안 운영 기술은 침입 탐지 시스템 분야가 주도하고 있으며, 키 관리 및 개인정보 관리 기술 등은 지속적으로 개발되고 있음

표 2. 국외 전자운전면허증 표준기술 현황

대분류	중분류	유럽	미주	일본/호주	남아프리카	비고
물리규격요소	IC카드 기술	7810, 7816-1 7816-2, 18013-1	7810, 7811 18013-1,10536	7810 18013-1	18013-1	SC17
	생체인식 기술	-	-	18013-2 15444-1	-	SC17,27,37
논리규격요소	IC카드 기술	-	18013-2, 10918 11693, 11694 14443, 15693 15438, 15444-1	-	-	SC17,27
	생체인식 기술	7816-11, 7816-8	18033, 13335	-	-	SC17,27,37
보안기술	물리보안 기술요소	-	-	-	-	SC17,GSC-IS NICSS,AICF
	논리보안 기술요소	-	-	-	-	SC17

유럽의 국가들이 통합된 EU와 미국연방정부는 자유롭게 왕래가 용이한 여행객들이 교통법규를 위반한 경우에 조회가 불가능하고 국제면허증의 발행과 운용에 많은 문제점을 인식하여, 국제통용 가능한 제안하게 되었고 의결권을 갖고 있는 중국, 일본, 한국이 동의를 하여 국제통용 면허증의 표준작업반이 ISO/IEC JTC1/SC17산하에 WG10이 구성되어 전자운전면허증 표준기술을 연구 중에 있다. 현재 UN/ECE와 협력 하에 WG10에서 작업 중인 국제표준이 완성되면, 현행 국제면허관련 협약이 파기되고 WTO/TBT에 따라 ISO를 준수해야하기 때문에 국제표준을 따르는 국제통용 가능한 운전면허증을 준비해야 하는 상태이다.

따라서 각 국가는 ISO 표준기술을 준용하여 국제통용 가능한 전자운전면허증(IDL)을 개발하고 있으며, 국외에서 준용하고 있는 표준기술 현황을 표 2에 나타내었다. 국제통용운전면허증을 위한 보안기술은 ISO/IEC JTC1/SC27에서 다루며, 생체인식 기술부분은 ISO/IEC JTC1/SC37에서 각각 표준기술을 SC17과 협력하여 연구하고 있다. SC17 분과에서 IC카드의 물리적, 논리적 규격 요소를 다루고 있지만 앞서 서론에서 언급한 바와 같이 현행 IDL은 소지자의 인증 및 터미널 운용 기술에서 취약점들이 보고되고 있다. 따라서 본 연구에서 분석한 현행 운전면허증과 IDL의 취약점에 대해 살펴보기로 한다.

2.2 운전면허증과 IDL의 문제점

2.2.1 기존 운전면허증의 한계

현행 국내 운전면허증은 플라스틱 형태로 인쇄된 사용자 정보를 기준으로 취약하게 운영되고 있다.

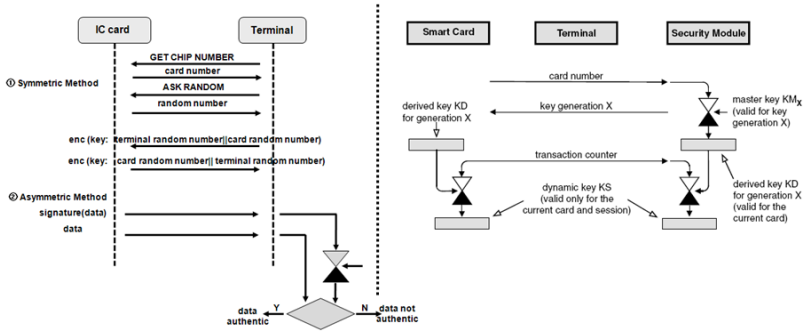

그림 1. 현행 IC카드와 터미널 인증기법

그리고 국내에서 발급받은 운전면허증은 DDP만을 가지고 있기 때문에, 국외에서 사용하기 위해서는 IDP를 추가로 발급받아야 하는 번거로움을 가지고 있다. 국제 운전면허증은 종이로 된 소책자 형태이기 때문에, 위·변조에 매우 취약하며, 감지하기도 어려운 것이 현실이다. 특히 DDP와 IDP의 실시간 관리가 불가능하다. 예를 들면, 국내에서 IDP를 받아 국외에서 사용하는 경우 또는 외국인이 IDP를 국내에서 사용하는 경우, 현행 국제운전면허증은 실시간 관리 및 위·변조 여부를 식별할 수 없을 뿐만 아니라 국제운전면허 허가를 받은 후, 국내운전면허 허가가 취소 또는 정지됨과 상관없이 IDP를 가지고 국외에서 사용될 수 있는 취약점을 가지고 있다. DDP, IDP 모두 동시에 실시간 취소 및 정지 등의 관리가 이루어져야하지만 사용자의 정보와 위반사항 등을 실시간 업데이트 할 수 없는 문제점이 기존 운전면허증의 한계이며 운용 시, 발생하는 문제점이다. 그리고 국제운전면허 허가를 가지고 있는 내국인이 국외 체류 중에 경찰이 면허증을 요구하는 경우나 국내에서 국제운전면허증을 소지하고 있는 외국인에게 면허증 제시를 요청하는 경우, 경찰이 합법적인 경찰임을 사용자는 식별할 수 없으며, 신뢰할 수 없다. 이러한 문제점은 국내 및 국제운전면허 허가가 실시간 관리 및 운용되지 못하고 관리자의 자격을 식별 및 검증할 수 없기 때문에, 발생하는 문제점이다[5],[6],[7].

2.2.2 IDL의 문제점

IDL(ISO Compliant Driving License)은 ISO/IEC 7816[8]표준명령어에 의해 동작한다. 그리고 ISO/IEC 18013-2[6]은 얼굴인식, 홍채, 지문 등의 생체정보로 개인식별기능을 강화할 수 있도록 선택사항으로 정의하고 있다.

IC카드를 제어하려면 터미널이 필요하다. 따라서 IC카드와 터미널간의 인증을 위한 키 협상 프로토콜을 필요로 한다. 일반적인 IC카드와 터미널간의 인증방법을 그림 1에 나타내었다. 좌측은 일반적인 IC카드의 고유번호로 키(PIN)를 생성하여 인증하는 방식으로 선택 암호기술에 따라 ①symmetric과 ② asymmetric 두 가지 방식을 사용하여 IC카드 소지자를 인증한다. 그리고 보안성을 강화시키기 위해 우측과 같이 SAM(secure application module)과 같은 보안 모듈에 의존하여 IDL은 인증 및 검증하는 방식의 프로토콜을 사용하고 있다[8],[9],[10]. 그러나 현행 IDL의 인증 및 운용 기술은 합당한 IDL 소지자와 터미널 운영자임을 검증하는데 매우 취약하며, IC카드 소지자의 인증을 위한 관점에 맞추어 설계되어 있다[6],[7]. 일반적으로 사용자는 기억하기 쉬운 패스워드를 사용하려고 하기 때문에 PIN과 같은 패스워드 기반 인증방법은 간단하게 유추하거나 쉽게 공유될 수 있는 단점을 가지고 있으며, PIN 인증방법은 사전공격, 부채널분석공격 등에 취약한 연구가 발표되고 있다[1],[2],[3],[4].

따라서 ISO/IEC 18013에서는 부가적으로 생체정보를 이용한 인증 방법을 선택사항으로 명시하고 있다. 그러나 소지자 인증 및 검증을 위한 현행 IDL의 PIN 인증방식은 합당한 터미널 운용자를 검증하는 기능을 가지고 있지 않기 때문에 터미널 운용자나 관리자 인증 및 검증 기법을 필요로 한다. 다시 말해, 사용자와 관리자간의 상호인증 및 검증 기능을 갖고 있지 않다[6],[7].

PC/SC(Personal Computer Smart Card) API(Application Program Interface)를 지원하는 터미널을 사용하면 지문과 같은 생체정보를 관리하는데 유용하며, 빠른 사용자 식별과 사용자의 프라이버시를 강화시킬 수 있는 장점을 가지고 있다. 그러나 지문과 같은 생

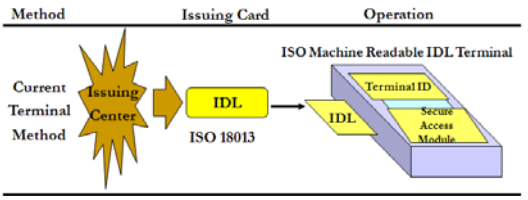

그림 2. 현행 IDL인증 및 터미널 운용

체정보 운용관리 시, 데이터베이스에 생체정보를 저장하고 터미널 애플리케이션으로 다시 로드하여 지문을 매칭하고 검증하는 방식은 보안 또는 관리 상, 항상 터미널이 연결되어 있어야 한다는 단점을 갖고 있으며, 네트워크 또는 데이터베이스 공격에 노출될 수 있는 취약점을 가지고 있다.

터미널은 터미널 ID를 통해 관리되며, 온라인으로 연결되어 있음을 전제로 하고 있다. 터미널이 오프라인인 경우, 현행 터미널 운용기법은 IC 카드와 터미널 간에 인증 및 검증하는데 문제점을 보이고 있다. 신뢰할 수 있는 IC카드 발급기관(Authoritative Entity)에 의해 발급된 서명을 검증하여, IC카드를 인증할 수 있지만, IC카드 내에 시간을 제어하는 클럭의 동기화[1]가 필요하다. 터미널이 오프라인의 경우, IC카드의 보다 신뢰할 수 있는 인증시점을 검증하기에 제한적인 단점[4]을 가지고 있다. 그리고 터미널 운용 시, 터미널 분실, 도난으로 인한 부정사용을 방지할 수 있는 방법이 전무한 상태이다. 터미널 ID를 부여하고 터미널을 인증하는 현행 터미널 운용방식[6],[7]은 운용성만을 고려하였기 때문에, 터미널 분실에 따른 추가적인 분실정책을 필요로 하며 관리 상, 번거로울 뿐만 아니라 오프라인 상태에서 IDL을 운용 관리할 수 없는 것이 현행 IDL의 문제점이기도 하다. 이처럼 현행 IDL은 소지자와 터미널 관리자를 온·오프라인 상태에서 실시간 상호인증 및 운용이 불가능하며, 강화된 상호인증 및 운용 기술과 정책을 필요로 하고 있음을 알 수 있다. 그리고 위·변조, 도난, 분실로 인한 부정사용 및 발급남용 방지를 위한 구성원의 기능과 보안 정책과 터미널 운용 정책이 요구됨을 알 수 있다. 더 나아가 국가 간의 IDL소지자 및 관리자를 상호인증 할 수 있는 국제통용운전면허증이 요구됨을 알 수 있다.

따라서 본 연구는 ISO/IEC 18013-2, 3 기반 하에 IDL과 터미널의 위·변조, 도난, 분실 및 부정사용을 방지하고 터미널의 온·오프라인 상태를 지원하도록 보안성과 운용성을 강화한 상호인증 및 운용기법을 제안하고자 한다.

Ⅲ. 제안하는 상호인증 및 운용기법 설계

3.1 제안하는 상호인증 및 운용구조

제안하는 상호인증구조는 ISO/IEC 7816, 18013-2를 준용하고 18013-3의 기계판독기술을 보완하기 위한 것으로, 본 연구에서 새로 도입한 전체 운용구조와 구성원을 그림 3에 나타내었다.

AD(Administrative Department)는 각 국가를 대표하며, 신뢰할 수 있는 기관을 말한다. PD(Police Department)는 경찰 또는 경찰청, DLA(Driving Licence Agency)는 운전면허 발급기관이라 총칭하고, 구성원(Players)은 발급자(MAIC), 관리자(MAMC), 사용자(IDL)로 구성된다. 발급 도메인(Mutual Authentication Issuing) 내의 AD는 MAIC, MAMC, IDL 발급 및 접근권한 또는 허가권한을 부여하는 기능을 하며, 하위등급의 MAIC, MAMC, IDL을 발급 및 운용 관리 기능을 갖고 있는 MAIC(Mutual Authentication Issuer Card)가 포함되어 있고 기능과 권한에 따라 MAIC(L1), MAIC(L2), MAIC(L3)로 구분하였다. 관리 도메인(Mutual Authentication Management) 내의 PD 또는 DLA는 IDL을 운영 및 관리하는 기능을 하는 MAMC(Mutual Authentication Management Card)를 포함하며, 발급자보다 낮은 권한의 구성원으로 MAMC(L1), MAMC(L2),MAMC(L3)으로 구분된다. 그리고 IDL(ISO compliant driving licence)은 DDP와 IDP를 갖고 있는 사용자를 말한다. MAIC는 구성원 발급 및 국가 간의 상호인증에 사용되며, MAMC는 IDL의 IDP, DDP를 정지, 갱신, 삭제, IDL 사용자의 위반사항과 같은 정보를 실시간 업데

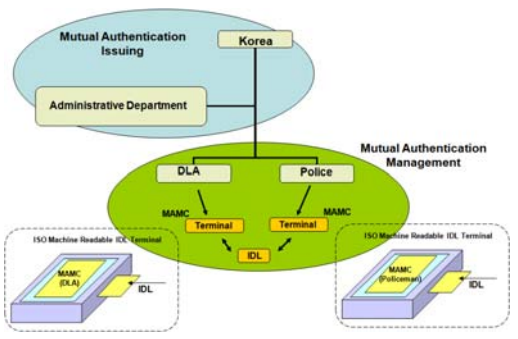

그림 3. 제안 상호인증 및 운용구조

이트하는 기능을 한다. MAIC에 의해 MAMC가 발급되고 MAMC는 권한에 따라 IDL의 정보를 네트워크를 통해 제어할 수 있다. 그림 3 우측하단에서 MAMC는 터미널을 이용하여 관리자임을 식별 또는 검증하여 터미널 관리자를 검증한 후, IDL 사용자를 인증 및 검증한다. IDL 인증 후, IDL의 위반사항 또는 정보를 운용 및 관리할 수 있도록 설계하고 오프라인 상태에서 IDL을 관리할 수 있도록 MAMC에 임시저장 기능을 추가하였다. 이 처럼 MAMC(관리자) 인증 및 검증을 선행 처리하는 것은 터미널 관리자를 선 검증하여, 터미널 관리자의 신뢰성을 확보하기 위한 것으로, IDL소지자 인증만을 수행하고 단지 터미널 ID와 SAM을 이용하여 IDL과 터미널의 통신 및 인증하는 현행 IDL의 보안성과 운용성을 향상시키기 위한 운용기법이다. 그리고 오프라인 상태에서 터미널 관리자와 터미널을 검증할 수 없고, 운용 및 관리가 불가능하여 터미널 도난, 분실에 따른 부정사용, 운용권한 남용을 방지할 수 없는 취약점을 보완하고 보안성과 운용성을 강화하기 위해, 각 구성원을 각각 기능과 권한에 따라 세분화하였다[11].

본 제안 기법에서 MAMC의 구성원을 이용하여 터미널 ID와 SAM을 대체하고 임시저장기능을 통해 운용 및 관리에 효율성을 제공하며, IDL, 터미널 그리고 IDL과 관리자(MAMC) 간에 상호인증 가능하도록 설계하였다. 새로 도입한 각 구성원(MAIC, MAMC, IDL)의 권한과 기능은 3.3에서 설명하도록 하겠다.

3.2 구성원과 터미널간의 제안 상호인증 및 운용 기법

IDL은 ISO/IEC 7816 기반 하에 PIN과 SAM에 의해 IC카드 소지자를 인증 및 검증하여 보안성을 제공하는 것을 그림 1에서 확인할 수 있다. 그러나 부정사용으로부터 안전하지 못하며, 터미널의 오프라인 상태에서 신뢰할 만한 사용자와 터미널 관리자임을 보장할 수 없는 한계를 앞서 언급하였다.

이 절에서는 취약점을 개선하기 위한 보안성과 운용성을 강화하는 상호인증 및 운용기법을 설명하겠다. 본 연구의 제안기법은 인증 및 검증 대상이 터미널, 관리자(MAMC), 사용자(IDL)로서 각 객체를 4회 인증 및 검증 프로세스를 수행하도록 보안성을 강화하였다. 각 구성원은 단계별 인증을 통해 검증한 후, 다음 단계의 인증을 수행하도록 설계하여, 각 단계에서 검증이 실패하면 다음 단계의 인증

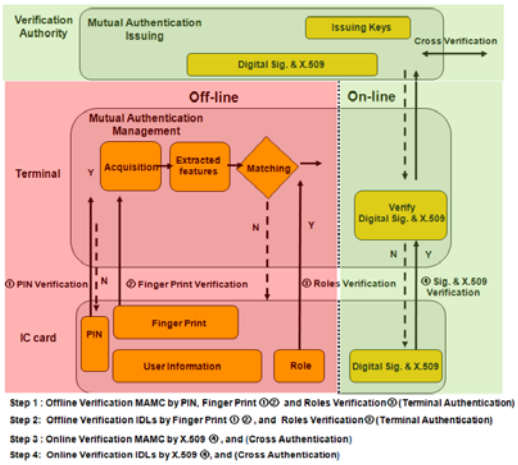

그림 4. 4단계 제안 인증 및 검증 프로세스

을 수행하지 않으며 운용이 불가능하다. 따라서 신뢰할 수 있는 터미널 관리자인 MAMC와 IDL 인증 및 검증을 수행하므로 강화된 구성원의 개인식별 기능 및 인증과 검증된 관리자에 의해 터미널 운용이 가능하도록 기능을 강화하였다. 신뢰할 수 있는 MAIC에 의해 MAMC와 IDL이 발급되며, MAMC와 IDL 기능과 권한에 따라 PIN, 지문, 권한등급, 인증서 4가지의 보안 요소를 각각 저장하여 발급한다. 터미널을 통해 IDL을 운용하려면, 반드시 터미널 관리자인 MAMC 검증이 선행 처리되어야 한다. 이는 터미널 도난 분실에 따른 부정사용을 방지하고 신뢰할 수 있는 관리자임을 검증하기 위함이다. ①PIN, ②지문, ③권한, ④인증서 검증을 통해 MAMC 검증을 선행 처리한 후, 동일한 방식으로 IDL을 검증한다. 그림 4의 음영영역으로 표시된 부분은 터미널이 오프라인 상태에서도 수행 가능한 인증과정으로서, 발급 시 부여하였던 ①PIN은 표준 명령어[8] "INS=20" AUTHENTICATE 명령에 의해 수행된다. PIN 인증은 현행 IDL과 동일한 방식을 따르고 있다[6],[7]. ②지문정합[12],[13],[14] 검증은 발급 시 저장된 지문과 즉석에서 터미널을 이용하여 추출한 지문을 정합하여 소지자를 검증하는 방식이다. 이 방식은 일반적으로 사용하는 네트워크에 연결된 서버로부터 지문정보를 로드하여 지문정보를 정합하는 현행 방법과 달리 신뢰성 있는 식별이 가능한 장점이 있다. ③단계의 검증은 터미널에 삽입되어 있는 MAMC의 터미널 운용 및 IDL 운용 권한을 확인하는 검증단계이다. 따라서 ①, ②, ③검증단계에서 터미널이 오프라인 상태이더라도 MAMC가 신뢰할 수 있는 관리자임을 실시간 확인할 수 있다.

그림 4에서 온라인 영역에 나타낸 ④검증은 온라인 상태에서만 가능한 실시간 검증단계로 인증서(X.509)를 검증한다[18]. 만약 PIN이 노출되고 지문 정합 오류로 인해 권한 단계까지 터미널이 승인되었다 하여도 마지막 실시간 인증서 검증을 거쳐야 하므로 강력한 보안성과 신뢰성을 제공할 수 있다. 그리고 인증서는 실시간 국가 간의 크로스 인증이 가능하여, 관리자와 사용자 상호인증에 효율적으로 사용할 수 있다. 제안 인증기법의 ②는 추가적인 지문정보 관리를 위한 데이터베이스를 구축할 필요가 없어 비용절감에 효율성을 제공한다. ③은 터미널이 오프라인 상태이며 ①, ②의 인증 실패에도 터미널 관리자를 검증하고 권한에 따라 IDL의 정보를 관리하는 권한을 식별할 수 있어, 부정사용 또는 남용으로부터 안전하다. 그리고 ④는 공인인증서를 사용하는 모든 서비스에 확대 적용시킬 수 있는 장점을 가지고 있다.

제안기법의 인증단계는 Step1에서 MAMC의 PIN과 지문 그리고 권한을 검증하고 Step2에서 IDL을 Step1과 동일한 검증방법으로 사용자를 검증하는 단계이다. Step3는 온라인 상태만을 지원하는 단계로 MAMC의 인증서 검증 단계이며, Step4는 IDL의 인증서를 검증하는 단계를 그림 4에 나타내었다. 본 연구는 ②, ③, ④ 단계를 추가하여 구성원의 보안성 기능을 강화하도록 설계하였다. 현재 국가 간의 크로스 인증을 위한 보안기술을 ISO/IEC JTC1 SC27에서 다루고 있기 때문에, 본 연구의 범위에서 벗어나는 것으로 본 연구에 포함시키지 않고 현행 X.509 인증서를 응용하였다[17].

터미널의 운용방법을 설명하기 전에, 제안기법의 오프라인 영역과 온라인 영역으로 인증 및 검증영역이 구분되어 있음을 그림 4에서 확인할 수 있다. 터미널은 온라인과 오프라인 상태로 구분할 수 있다. 터미널이 온·오프라인 상태에서 ①, ②, ③ 인증 및 검증을 수행하며, 그림 5의 Step1, Step2에 해당한다. 그림 5의 Step1은 터미널 관리자인 MAMC가 ①PIN, ②지문, ③권한 검증을 수행하는 단계이며, Step2는 Step1과 동일한 검증방법으로 IDL을 인증 및 검증하는 단계이다. Step1을 수행하여 터미널 관리자를 확인하고 Step2에서 IDL 사용자를 검증하는 오프라인 상태의 운용절차를 그림 5에서 확인할 수 있다. 터미널이 오프라인 상태에서 IDL을 관리해야 하는 경우, MAMC에 IDL의 임시정보를 저장할 수 있도록 설계하여, 위반사항, 벌점 등의 IDL 정보를 임시저장하고 터미널이 온라인 재개 시 데이터베이스와 같은 관리서버로 업데이트를 할 수 있다. 따라서 오프라인 상태의 관리가 불가능한 현행 IDL 보다 효율적이다.

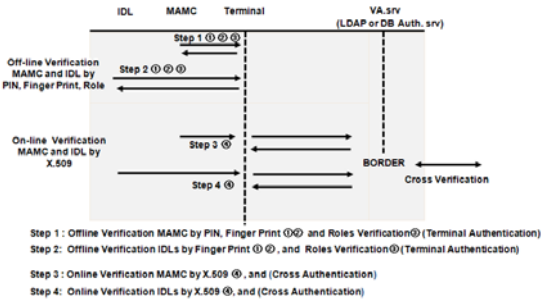

그림 5. 제안 터미널 단계별 운용절차

터미널이 온라인 상태에서 추가적인 그림 4의 온라인 영역에서 나타내고 있는 ④검증은 그림 5의 Step3, Step4에 해당한다. Step3 단계에서 관리자인 MAMC를 검증한 후, Step4에서 IDL을 검증하는 운용절차를 그림 5에 나타내었다. Step3, Step4단계는 공인인증서(X.509)를 검증하는 단계로, 현 단계에서 신뢰할 수 있는 인증서가 탑재되어 있는 국내·외의 터미널 관리자를 검증할 수 있다. 제 3국에서 면허증 제시를 요청하는 경찰 또는 관리자를 신뢰할 수 없는 현행 IDL의 단점을 보완하기 위함이다. 또한 동일한 검증방법으로 국외에 체류 중인 내국인이나 국내에 체류 중인 외국인이 사용하는 IDL을 인증 및 검증이 가능하여 효율적인 운용성과 신뢰성을 제공한다.

본 연구에서는 RFC3280 준용하여 인증기관(CA)를 구축하여 C=KR, O=National Police Department, OU=Seoul Police Department, CN=Mr Jeon, 서명알고리즘=sha1RSA, 공개키= RSA(2048btis) 인증서를 그림 8와 같이 발급하여 각 구성원에 저장할 수 있도록 설계하였다.

3.3 제안하는 구성원의 기능과 권한

IDL은 반드시 국제통용 가능해야 하며, 국내·외에서 발생하는 IDL과 관련된 사건 또는 정보의 효율적인 운용 및 관리가 필요하며, 부정사용 또는 권한 남용으로부터 안전해야 한다. 따라서 제안구조 내의 구성원을 기능과 권한에 따라 RBAC(Role-Based Access Control)을 기반 하여 각 등급을 세분화하였다[11].

MAIC(L1)은 하위의 MAIC(L2)를 MAIC(L2)는 하위 MAIC(L3)의 발급권한을 가지며, MAIC(L1)는

표 3. MAIC, MAMC, IDL 보안정책 및 관리기능

		상호인증정책	발급 및 관리기능	접근권한	인증	발급	읽기	쓰기	삭제
MAIC	L1	높음	발급 및 관리 (MAIC,MAMC,IDL)	제한 없음	필요	Y	Y	Y	Y
	L2	높음	발급 및 관리(국제) (MAIC,MAMC,IDL)	제한 없음	필요 (국제)	Y	Y	Y	N
	L3	중간	발급(국내용) MAIC,MAMC,IDL관리	제한적 (국내)	필요	Y	Y	Y	Y
MAMC	L1	높음	IDL 관리 발급(국내용)	제한적	필요	Y (국내)	Y	Y	Y
	L2	중간	IDL 관리	제한적	필요 (국제)	N	Y	Y	N
	L3	중간	IDL 관리	제한적	필요	N	Y	Y	N
IDL		낮음	없음	제한적	필요	N	N	N	N

표 4. 구성원 접근 권한 및 허가 권한

B8	B7	B6	B5	B4	B3	B2	B1	Meaning
x	x	x	x	x	x	x	x	TYPE
–	–	–	–	0	1	0	0	MAIC '4'
–	–	–	–	0	0	1	0	MAMC '2'
–	–	–	–	1	1	1	1	IDL 'F' 국제가능-국내가능-사용가능
–	–	–	–	1	0	1	1	IDL 'B' 국제정지-국내가능-사용가능
–	–	–	–	1	0	0	0	IDL '8' 국제정지-국내정지-사용불가능
LEVEL								
–	–	–	–	1	1	1	0	L1 'E'
–	–	–	–	0	1	1	0	L2 '6'
–	–	–	–	0	1	0	0	L3 '4'
–	–	–	–	0	0	0	0	IDL '0'
ACCESS CONTROL PERMISSION								
–	–	–	–	1	1	1	1	ISSUING 'F'
–	–	–	–	1	1	1	0	WRITE 'E'
–	–	–	–	1	1	0	0	DELETE 'C'
–	–	–	–	0	1	1	1	READ '7'

표 5. EF.DF11, IDL 위반데이터

접근 조건			읽기	MAIC/MAMC	
			쓰기	MAIC/MAMC	
자료그룹	이름		EF 단축 식별자	EFID	태그
DG11	선택적 국내 자료		'0B'	'000B'	'73'
태그	내용	고정적/유동적	필드형식/길이/타입	형식	
'5F24'	위반날짜	F	8N	YYYYMMDD	
'5F1B'	위반항목	V	10AN	A2B06	
'5F02'	벌금	V	8N	40000	
'5F03'	벌점	V	3N	100	

구성원 중에 최고의 권한을 가지며 국가 대표한다. MAIC(L1), (L2), L(3)는 MAMC와 IDL의 발급과 기록, 읽기, 삭제 가능한 관리기능을 갖는다. MAIC(L2)는 국가 간의 호환성을 위한 상호인증정책을 포함하며, 외국인이 소지한 IDL 관리에 사용되지만 외국인의 원 정보를 삭제할 수 없고 위반사항과 같은 정보를 읽기, 쓰기만 가능하도록 IDL의 정보 관리에 제약을 포함한 것을 표 3에서 확인할 수 있다. 이것은 제3국에서 IDL정보가 삭제되는 것을 방지하기 위함이다. MAIC(L3)는 국내에서 사용하는 보안정책 및 관리기능을 포함한다. MAMC(L1), (L2), (L3)는 IDL을 관리하는 기능과 보안정책을 포함한다. MAMC(L1)은 긴급 또는 분실상황을 고려한 제한적 임시 발급기능을 포함한다. MAMC(L2)는 국가 간의 크로스 인증정책을 필요로 하며, 외국인이 소지한 IDL의 원 정보를 삭제할 수 없는 보안정책과 기능을 포함한다. 그리고 MAMC(L3)도 삭제 권한이 없다. 이는 관리자의 권한남용을 방지하기 위한 것으로 IDL 소지자의 해당국의 DLA 내의 MAMC(L1) 이상의 구성원만이 IDL의 원 정보를 삭제시킬 수 있도록 한 것이다. IDL은 관리 기능을 포함하고 있지 않다. DDP와 IDP의 허가 정보만을 포함하며, 표 4에서 국제 및 국내 사용가능, 사용불가능의 면허 허가 여부를 확인할 수 있다. 그리고 표 4에 나타낸 구성원의 접근 권한은 본 연구에서 각 구성원을 식별 및 검증하는

표 6. EF.DF14, 조건적 접근제어 권한

접근 조건			읽기	MAIC/MAMC	
			쓰기	MAIC/MAMC	
자료그룹	이름		EF 단축 식별자	EFID	태그
DG14	조건적 접근 제어		'0D'	'000D'	'6F'
태그	내용	고정적/유동적	필드형식/길이/타입	형식	
'5F01'	MAIC L1	F	8N	'4EFEC7'	
'5F02'	MAIC L2	F	8N	'46FEC7'	
'5F03'	MAIC L3	F	8N	'44FEC7'	
'5F04'	MAMC L1	F	8N	'2EFEC7'	
'5F05'	MAMC L2	F	8N	'260E07'	
'5F06'	MAMC L3	F	8N	'240E07'	
'5F07'	IDL	F	8N	'100000'	

식별자로 사용되며, 각 권한은 EF.DF14에 표 6과 같이 HEX로 표기 및 저장된다.

3.3.1 구성원의 데이터 및 파일구조

제안기법을 위한 구성원의 데이터 구조는 ISO 18013-2[6]기반 하에 설계하였으며, 각 데이터 그룹(Data Group)에 포함하는 정보에 대해 설명하도록 하겠다.

IDL의 데이터는 EF.DG1에 저장되는 필수 데이터 요소는 성, 이름, 생년월일, 발행일, 만기일, 발행국, 발행기관, 면허번호, 차량의 카테고리/제한사항/조건은 하나 이상의 결합된 데이터 객체를 포함하는 템플릿으로써 인코딩되며, [카테고리];[발행일];[만기일];[제한/조건코드];[제한/조건서명];[제한/조건값]과 같은 형식을 취한다. EF.DG2는 선택적인 면허소지자의 세부사항으로 성별, 키, 몸무게, 눈동자색, 머리카락 색, 출생지, 거주지 7개의 데이터요소로 구성된다. EF.DG3은 IDL이나 발급 기관에 대한 추가적인 세부사항을 제공하며, 관리번호, 문서 판별자(추가적인 면허들 또는 실제 문서와 같은 번호를 가지고 발행된 이중문서 구별하기 위해 발행 기관에 의해 할당된 번호), 데이터 판별자(물리적 문서에 대한 다른 기계 판독 데이터 집합을 구별하기 위해 발행 기관에 의해 할당된 번호), ISO 발행자 ID번호(ISO 번호는 발행 국가 또는 면허 발급 기관에 할당)로 4개의 선택적인 요소로 구성되어 있다. EF.DG7은 생체인식 정보 중에, 지문정보 데이터가 저장된다. ISO/IEC 19794[12],[13],[14]을 따르는 지문정보 데이터를 탑재하고 TLV(Tag-Length -Value) 형식으로 부호화 되며, 생체인식 교환파일 형식(CBEFF: Common Biometric Exchange File Format)[14] 구조를 사용하여 카드에 저장된다. EF.DG11은 국내 사용자를 위한 데이터 그룹으로 국내의 특징적인 정보를 저장할 수 있는 파일 요소이다. IDL사용자의 위반 항목, 벌금, 벌점 등 위반 정보를 저장하기 위한 것이며, 형식은 표 5에 나타내었다.

EF.DG13은 능동적 인증을 위한 데이터 그룹으로 SubjectPublicKeyInfo를 DER형식으로 저장하며, ISO/IEC 9796-2 디지털 서명기법[15]에 따라 계산하여, 구성원의 전자서명을 통해 검증이 가능하며, 서명 또는 인증서는 SCVP(Server-based Certificate Validation Protocol) 프로토콜을 사용하여 실시간 검증이 가능하기 때문에, 강력한 보안성을 제공할 수 있다[18].

```
ActiveAuthenticationPublicKeyInfo::=
    SubjectPublicKeyInfo
SubjectPublicKeyInfo::= SEQUENCE {
    algorithm AlgorithmIdentifier,
    subjectPublicKey BIT STRING }
AlgorithmIdentifier::= SEQUENCE {
    algorithm OBJECT IDENTIFIER,
    parameters ANY DEFINED BY
    algorithm OPTIONAL}
```

EF.DG14는 구성원의 PIN과 지문 인증을 마친 후, 권한을 검증할 때 사용되는 데이터로서 각 구성원의 발급, 읽기, 쓰기, 수정, 삭제 권한을 명시하고 있는 데이터 그룹이며 구성원을 식별하는 식별자 기능을 한다. 예를 들어 '2EFEC7'의 '2'는 MAMC, 'E'는 Level1, 'F'는 발급권한, 'E'쓰기, 'C'삭제, '7'읽기 권한을 의미하여 MAMC(L1)임을 표 4에서 확인할 수 있다. MAIC의 EF.DF1은 필수 데이터 요소로 IDL과 동일한 형식을 따른다. 표 8에 나타낸 파일구조와 동일하며, '관리번호'를 추가하였다. MAMC는 표 7에서 관리자를 식별하기 위해 'Police Number'를 추가하였다. DLA의 관리자라면, DLA Number와 같이 관리자식별자를 추가할 수 있

표 7. MAMC의 EF.DF1

접근 조건			읽기	MAIC/MAMC		
			쓰기	MAIC/MIMC		
자료그룹	이름			EF 단축 식별자	EFID	태그
DG1	필수 자료			01	0001	'61'
이름	내용	고정적/유동적	필드형식/길이/타입	형식		태그
Family name	성	V	36AS	Jeon		'5F60'
Given names	이름	V	36AS	Sanghoon		'5F61'
Data of Birth	생년월일	F	8N	YYYYMMDD		'5F2B'
Date of Issue	발행일	F	8N	YYYYMMDD		'5F26'
Issuing Country	발행국	F	3A	KOR (ISO/IEC 3166-1)		'5F28'
Issuing Authority	발행기관	V	65ANS	KPD		'5F62'
Police Number	경찰번호	V	25AN	MAMC 00001		'5A'

표 8. MAMC EF.DF11, 임시저장

접근 조건			읽기	MAIC/MAMC		
			쓰기	MAIC/MAMC		
자료그룹	이름			EF 단축 식별자	EFID	태그
DG11	선택적 국내 자료			'0B'	'000B'	'73'
태그	내용	고정적/유동적	필드형식/길이/타입	형식		
'5F04'	IDL사용자 면허번호	V	25AN	A290654395164273X		
'5F24'	위반 날짜	F	8N	YYYYMMDD		
'5F1B'	위반 항목	V	10AN	A2B06		
'5F02'	벌금	V	8N	40000		
'5F03'	벌점	V	3N	100		

다. MAIC와 MAMC의 EF.DF2는 각각 EF.DF1의 상세정보를 포함하고 있다. EF.DF3은 발급기관의 세부사항으로 발급기관의 정보를 포함한다. EF.DF7의 MAIC와 MAMC 정보는 IDL과 동일한 지문 정보를 저장하며, EF.DF13은 신뢰할 수 있는 인증기관으로부터 발급받은 인증서는 IDL과 동일한 형태로 저장된다. EF.DF14는 표 6의 파일구조를 따르며, 표4에서 나타내고 있는 MAIC, MAMC의 접근 권한이 각각 저장된다. EF.DF11은 터미널이 오프라인인 경우, IDL에 의해 발생될 수 있는 이벤트를 MAMC의 EF.DF11에 기록하여 IDL의 효율적으로 운용 및 관리하기 위한 임시저장 기능의 데이터 그룹으로 실시간 데이터 업데이트가 불가능한 경우에 사용 가능하다. 터미널의 온라인 재개된 후, 관리서버로 임시 저장된 정보를 업데이트할 수 있으며 표 8에서 MAMC의 파일구조를 확인할 수 있다.

Ⅳ. 보안성 및 운용성 실험과 성능분석

본 연구의 실험의 PIN 인증 기법은 현행 IDL 인증방식과 동일한 ISO/IEC 18013, 7816을 준용하며, 지문은 ISO/IEC 19794-2, 3을 준용한다. 권한은 RBAC을 응용하여 설계한 권한을 사용하였다[12]. 인증서의 검증을 위해 RFC 3280, 5019, 5055를 준용한 인증기관(CA)과 SCVP, OCSP 서버를 구축하여 인증기법을 강화하였다. 그리고 MAIC와 MAMC의 구성원을 설계하여 강화된 개인식별기능과 터미널 및 터미널 관리자간의 강화된 상호인증 및 운용 기법을 실험하여 제안기법의 우수성을 증명하도록 하겠다. 실험은 발급, 구성원 인증 및 검증, 운용 및 관리 세 가지를 시험한다.

첫째, 현행 IDL 인증의 취약점을 개선하기 위해, PIN 인증, 지문, 권한검증, 인증서 4가지의 보안요소를 저장하여 구성원 발급을 확인한다. 둘째, MAIC와 MAMC의 등급과 권한을 부여하여 합당한 터미널 관리자임을 식별하고 부정사용 및 터미널 분실에 따른 부정사용을 방지하기 위해, 사용자 인증 및 권한을 검증한다. 셋째, 터미널 운용방법을 개선하기 위한 MAMC의 임시저장 기능을 확인한다.

실험을 위해 T=0 프로토콜을 사용하는 접촉식 IC카드를 이용하며, ISO/IEC 7816 표준명령어 사용 가능한 터미널을 이용하여 본 시스템을 구현하였으며, 사용된 시스템은 다음과 같다.

·Operating System:Windows 2000 Server, Windows XP
·Development Software : Visual C++, MS-SQL, IIS, ASP, JAVA
·Finger Print Sensor: Input Method(Optical), Resolution(500dpi/256 Gray), Input Area (14.6x16.3mm), FAR(≤0.0001%), FRR(≤0.1%)
·Smart Card: EMV Level 1 Compliant Supports ISO 7816, T=0 & T=1, Supports high speed smart card interface with transfer data rates of up to 115kbps

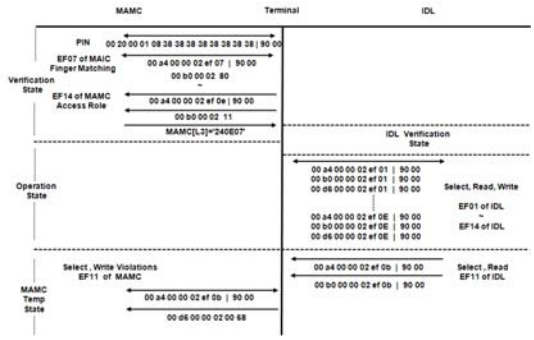

그림 6. 인증 및 검증, 관리, 임시저장 표준명령어

4.1 보안성 및 운용성 성능실험

· 검증 상태: MAIC는 IDL 발급을 위해 MAIC의 PIN='88888888', 지문, 권한을 검증해야 한다. 필요에 따라 추가로 인증서를 검증할 수 있다. 그림 6에서 MAIC의 PIN과 MAIC의 EF 07에 저장된 지문을 검증하는 표준명령어를 확인할 수 있다. MAIC의 권한과 인증서 검증은 생략하였고 대신 MAMC의 EF14에 저장된 권한 'MAMC(L3)=240E07' 검증을 수행하는 명령어를 나타내었다.

· 운영 및 관리 상태: EF01~EF14 내의 정보를 운영 및 관리하는 상태로 IDL의 정보를 선택, 읽기, 쓰기 등을 수행하는 표준명령어를 나타내고 있다.

· 임시저장 상태: MAMC의 임시저장 상태는 앞서 언급한바와 같이 IDL에 저장된 EF11내의 정보를 읽고 MAMC 임시공간에 위반날짜 또는 위반 항목, 벌점과 같은 새로운 정보를 기록하는 상태를 나타내고 있다.

터미널의 온·오프라인 상태 모두를 지원할 수 있는 제안기법을 실험하여 운용성과 보안성을 강화할 수 있음을 그림 6에 나타낸 표준명령어의 흐름을 통해 확인할 수 있다. 본 실험을 더욱 구체화하기 위해 구현 시스템으로 실험을 확인하겠다.

4.1.1 발급 및 보안성 실험

그림 7에서 MAIC가 IDL 발급을 위해, MAIC의 PIN='88888888', 지문정합='Match OK', 권한등급 'L2'과 상세정보가 검증됨을 확인할 수 있다. 검증된 MAIC에 의해 IDL을 발급한다. 표 3, 표 4에 따라 MAMC 또는 IDL의 IC카드를 초기화하여 발급한다.

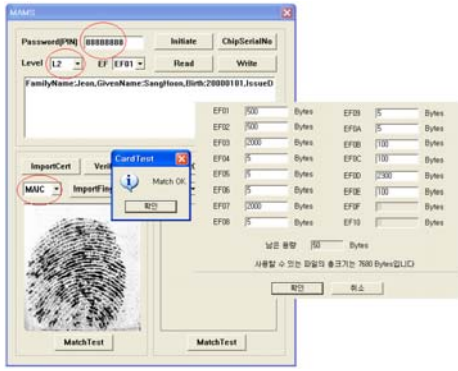

그림 7. MAIC 검증 및 IDL 발급과정

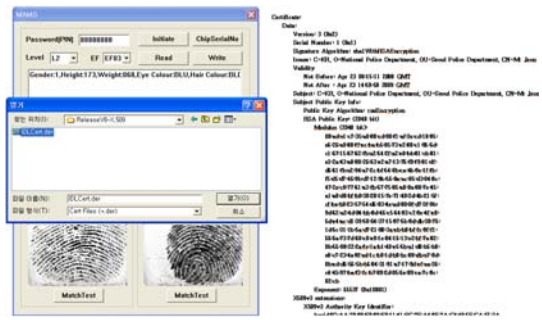

그림 8. IDL발급을 위한 인증서 저장

제안기법을 실험하기 위해, EF.DF1, 2, 3, 7, 11, 12, 13, 14를 임의의 크기로 설정하여 초기화한 후, 그림 8과 같이 사용자의 정보, 지문, 신뢰할 수 있는 기관으로부터 서명 또는 인증서를 저장하여 발급한다. 동일한 절차에 의해 MAMC도 발급할 수 있다.

제안하는 상호인증구조의 AD, PD가 존재함을 가정하고 인증정책을 포함하여 구축한 인증기관(CA)으로부터 인증서를 발급하였지만, 제안한 AD와 PD가 실재 존재하지 않기 때문에, 인증서 검증 실험에서는 SCVP, OCSP 서버를 구축하여, 현재 사용하고 있는 공인인증서를 사용하여 검증 실험을 하였다. 그림 9에 붉은 선으로 표시한 것과 같이, 'IDL 사용자=전상훈', '인증서 발급기관=yessignCA', 최고 '루트기관=KISA'의 검증경로를 확인할 수 있다. 따라서 신뢰할 수 있는 제안 상호인증구조의 AD와 PD가 존재한다면, 'IDL 사용자=전상훈', '인증서 발급기관=PD', 최고 '루트기관=KOREA'과 같이 제안 상호인증구조가 이루어 질 것이다.

본 인증서 검증 실험은 개인식별기능을 강화시켜 실시간 인증, 부인방지, 부정사용 등의 보안 서비스를 제공할 수 있으며, 국가 간의 상호인증이 가능함

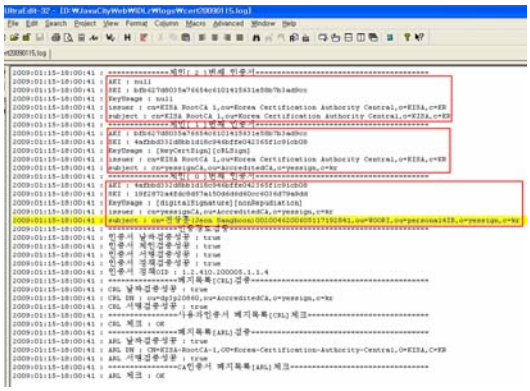

그림 9. SCVP를 이용한 인증서 검증경로

을 제시하고 있다. 뿐만 아니라 주민등록증을 대신한 개인식별 ID로 대체할 수 있으며, 공인인증서를 사용하고 있는 다양한 서비스에 확대 적용 가능함을 보여주고 있다.

4.1.2 IDL 운용성 실험

그림 10(a)은 MAMC의 PIN과 지문 검증 후, 표 4, 표 6에서 정의된 EF.DF14에 저장되어 있는 MAMC(L3)의 '240E07' 권한을 확인하는 과정을 나타내고 있다. Type은 MAMC='2', Level은 L3='4', Issuing='0'으로 발급 권한이 없는 것을 의미하며, Write=E, Delete=0, Read=7으로 쓰기, 읽기가 가능한 권한을 가진 등급3의 MAMC(L3)임을 확인할 수 있다. 이처럼 터미널 운용 권한이 승인된 MAMC(PIN='12345678', 지문(좌)='Match OK', 등급=3)에 의해 IDL 운용 및 관리가 가능하다. 그림 10(b)와 같이 터미널 운용자인 MAMC 검증 후, 동일한 검증방법으로 IDL사용자가 입력한 PIN='11111111'과 발급 시, 저장된 사용자의 지문정보와 터미널에서 추출한 지문정보를 즉석에서 정합하여, IDL을 검증한다. 사용자를 식별한 후, MAMC에 의해 IDL 정보를 조회하고 갱신할 수 있다. 터미널이 오프라인 상태일 때, IDL사용자의 정보를 추가로 저장해야하는 경우, PIN, 지문, 등급의 3단계 검증을 거쳐 후, 터미널이 오프라인 상태에서 IDL정보 업데이트를 위해 EF.DF11에 표8에서 정의한 파일형식에 따라 그림 10(c)과 같이 MAMC의 EF.DF11의 임시저장 공간에 IDL의 임시 데이터를 저장한다. 그리고 터미널이 온라인으로 재개된 후, 관리서버로 업데이트를 할 수 있기 때문에, IDL 사용자 운용 및 관리에 효율적이다.

4.2 제안기법 성능분석 비교

4.2.1 IDL 보안성 및 운용성 성능분석

음영영역으로 나타낸 현행 IDL 인증기법으로 IDL과 터미널간의 인증과 음영영역을 포함한 구성원 전체(IDL, MAMC, MAIC)가 제안하는 상호인증 영역을 그림 11에서 나타내고 있다. 현행 IDL은 ISO 7816-4에 준하는 인증방식에 의해 IDL사용자 중심의 인증방식을 채택하고 있으며, 생체정보 검증 방법을 선택사항[5],[6],[7]으로 정의하고 있다. ISO 7816을 준용하는 현행 PIN 인증방식은 사전공격, 부채널분석공격 등과 같은 공격에 노출될 수 있는 연구[1],[2],[3],[4]가 보고되고 있고, 일반적으로 쉬운 패스워드를 사용하려는 사용자의 특성과 쉽게 공유 또는 유추될 수 있는 취약점 가지고 있다. 따라서

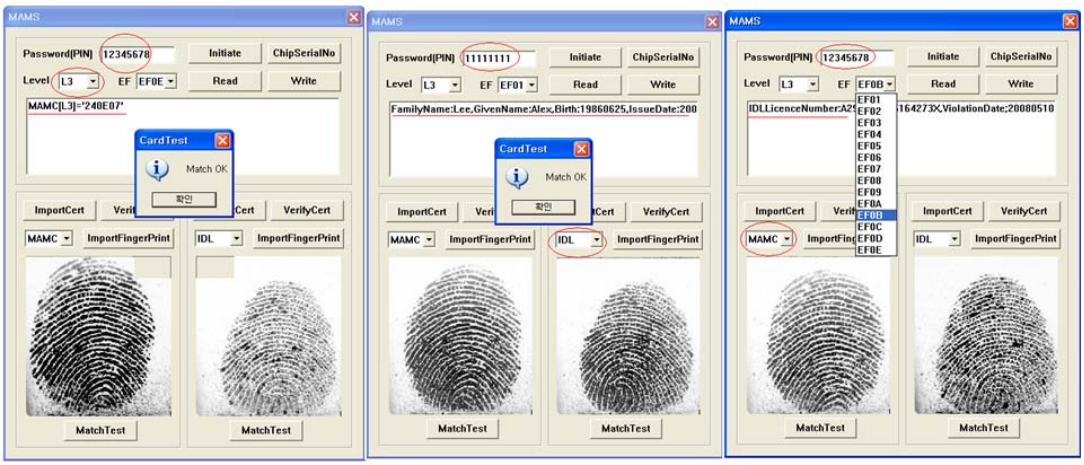

그림 10. EF.DF14 MAMC의 권한 검증(a), 검증된 IDL 사용자 정보조회(b), MAMC에 IDL정보 임시저장(c)

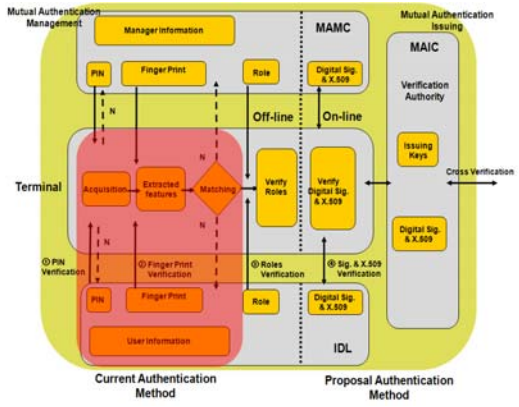

그림 11. 보안성 강화를 위한 현행 및 제안 상호인증기법 비교

보안모듈을 기반 하는 PIN인증 방법은 효율적이지 못하며, 선택사항으로 정의한 생체정보를 이용한 국가 간의 사용자를 상호인증하기 위해서는 막대한 비용과 관리 서버가 요구될 것이다. 현행 IDL의 인증방법을 그림 11에 붉은 영역 내의 ①PIN, ②지문 해당한다.

본 제안 기법은 보안성을 강화하기 위해 그림 11와 같이 음영영역의 현행 IDL의 ①PIN인증 방식과 선택사항인 생체정보를 이용한 인증기법을 적용하였다. 그러나 현행 IDL의 정합 방법과 달리, 지문 관리 서버에서 사용자의 지문을 로드하여 정합하는 방식이 아닌, 본 연구에서 개발한 터미널 시스템을 이용하여 발급 시, 저장하였던 지문정보 템플릿과 즉석에서 획득한 IDL사용자의 지문과 정합하여 ② 일대일(one-to-one) 인증방식으로 사용자와 관리자를 식별 및 검증하는 방식을 사용하기 때문에, 현행 IDL 인증방식보다 향상된 보안성과 관리에 용이한 장점을 확인할 수 있다. 그리고 ③권한과 ④인증서로 사용자 또는 관리자를 검증하는 인증방식을 사용하므로 보다 안전하고 신뢰할 수 있다. 뿐만 아니라 터미널 부정사용을 방지하고 합당한 관리자만이 터미널을 운용할 수 있도록 검증된 관리자인 MAMC와 MAIC라는 구성원을 도입하여 IDL사용자와 MAMC 터미널 관리자를 상호인증 하는 방식을 채택하여, 보다 신뢰성을 향상시킬 수 있다. 또한 ④인증서 검증은 외국인이나 내국인이 외국에 체류 중에도 실시간 IDL사용자를 검증할 수 있는 인증기능으로서, 국가 간의 크로스 인증이 가능함을 제시하였다. 현행 IDL은 ① 인증방식만을 지원하고 오프라인 상태의 인증기능을 지원하지 않는다. 반면에, 제안기법은 오프라인 상태에서 ①, ②, ③의 인증기법을 지원하며, 온라인 상태에서 ④까지 지원 가능함을 실험하여 강화된 보안성을 확인할 수 있었다.

4.2.2 터미널 보안성 및 운용성 성능분석

현행 IDL의 터미널 운용기법과 제안기법을 그림 12에서 비교하고 있다. 현행 IDL 운용기법은 ISO/IEC 18013을 준용하는 IDL을 ISO 기계판독 가능한 터미널을 이용하여, 운용 및 관리하고 있다. 그리고 터미널 ID와 SAM을 탑재하고 있다. SAM을 이용하여 IDL의 인증기능을 강화하고, 온라인 상태에서 터미널 ID를 통해 터미널을 인증하는 방식이다. 이러한 현행 방식은 터미널 ID와 SAM의 관리를 위한 시스템을 요구하며, 터미널이 오프라인 상태에서는 사용 불가능한 단점을 가지고 있다. 뿐만 아니라 터미널 분실대한 추가적인 정책이 필요하며, 관리해야 하는 번거로움이 있다. 그리고 도난, 분실, 부정사용 방지 대책과 오프라인 상태의 검증 방법에 대한 방안이 없어 매우 취약하다. 따라서 터미널 관리자를 신뢰할 수 없다.

본 제안 기법은 표 3에서 제시하고 있는 세분화된 정책을 적용하여 터미널을 이용한 운용권한 남용으로 부터 방지할 수 있으며, 분실과 부정사용으로부터 안전함을 확인할 수 있다. 그리고 MAMC가 터미널 ID와 SAM의 기능을 대체하기 때문에, 터미널로 인해 부가되는 추가적인 관리 서버 없이, 터미널 관리자 검증이 가능함을 확인할 수 있다. 신뢰할 수 있는 관리자에 의해 터미널이 동작하기 때문에, 분실과 부정사용으로부터 안전할 뿐만 아니라 터미널이 오프라인 상태에도 관리자인 MAMC의 ①PIN, EF.DF7내의 ②지문정합, EF.DF11 내의 접근제어 ③권한을 검증이 이루어지므로 현행 기법보다 국내·외에서 관리자를 신뢰할 수 있는 장점과 터미널이 오프라인 상태에서도 MAMC의 임시저장 기능을 통해, IDL을 관리할 수 있어 효율적인 운용성을 확인하였다.

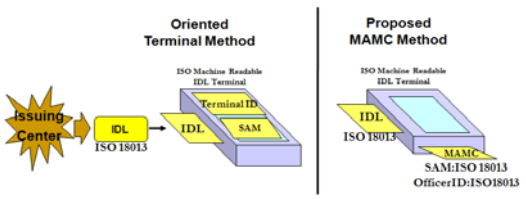

그림 12. 터미널 운용 기법비교

표 9. 보안성 및 운용성 강화 요소 비교

	보안 및 운용요소	현행 IDL	현행 터미널	제안 IDL	제안 터미널
IC 카드	PIN	사용	-	사용	-
	생체정보	선택사항	-	사용	-
	권한	-	-	사용	-
	인증서	-	-	사용	터미널(사용가능)
	임지저장기능	-	-	사용	-
	크로스인증	-	-	가능	가능
터미널	온라인	지원	지원	지원	지원
	오프라인	불가	불가	지원	지원
	SAM	-	사용	(사용가능)	MAMC(사용가능)
	터미널 ID	-	사용	(사용가능)	MAMC(사용가능)
	인증 방식	IDL인증	터미널 ID	IDL,MAMC 상호인증	MAIC, MAMC 상호인증
관리 서버	키, 지문	-	필요	-	필요없음
	터미널 ID	-	필요	-	필요없음
	분실정책 관리	-	필요	-	필요없음

따라서 본 제안기법을 실험하여 현행 IDL과 터미널 운용기법 보다 강화된 신원식별 기능과 제안 터미널 운용기법을 통해, IDL과 MAMC간에 보안성과 운용성이 강화된 상호인증기법임을 확인할 수 있었다. 표 9에서는 보안성을 제공하는 인증기능과 운용성을 제공하는 터미널과 관리 서버를 비교하여 본 연구에서 제공하는 기법의 우수성을 비교하였다.

V. 결 론

플라스틱이나 종이책자 형태의 기존 운전면허증의 취약점을 보완하고 국제통용가능한 운전면허증 표준을 위해, ISO/IEC JTC1/SC17에서 국제표준 기술 연구가 활발히 진행되고 있으며, 현재 ISO/IEC 18013-3은 CD단계로 표준 제정이 완료되지 않은 상태이다. 그러나 현행 IDL과 터미널 운용방식은 보안성과 운용성 측면에 앞서 언급한바와 같이 많은 취약점과 보완해야 할 점들을 본 연구를 통해 확인할 수 있었다.

본 연구에서 IDL과 MAMC 간의 상호인증 기능을 통해 위·변조, 분실, 도난에 따른 부정사용을 방지하고, 터미널 온·오프라인 상태에서 국제통용 가능한 보안 및 운용정책을 적용하여 도입한 구성원 간의 상호인증 및 운용기법과 검증 실험을 통해 현행 인증 기법보다 강화된 보안성을 제공할 수 있음을 제안기법을 통해 확인하였다. 그리고 임시저장 기능과 터미널의 ID와 SAM을 대체하는 MAMC의 기능을 통해 관리기능의 효율성을 향상시켜 강화된 운용성을 확인하였다. 그리고 본 연구에서 PKI 응용기술을 적용하여 IDL과 터미널 관리자를 실시간 인증 및 검증을 실험하여 국가 간의 크로스 인증이 가능함을 제시하였고 개인식별기능 및 증명수단으로 사용될 수 있는 국제통용운전면허증은 본 연구를 통해 은행, 국세청, 공공서비스 등에 확대 적용 및 활용될 수 있음을 제시하여 본 연구의 우수성을 확인하였다.

향후, 국제 호환 가능한 IDL을 위해서는 보다 체계적인 상호인증 정책 및 운용관리 정책이 수립되어야 할 것이다. 그리고 IC카드에 대한 부채널분석 공격과 같은 취약점이 발표되고 있는 현 시점에, IC 카드 내에 저장되는 정보를 보호하기 위한 암호기술 또는 전자서명 등의 대비책을 마련해야 할 것이다. 마지막으로 전자여권, 전자사증, 의료카드, 선원카드 등과 같은 IC카드 기반 응용기술에 본 제안 기법을 확대 적용하면, 개인식별부분에 강화된 상호인증기능을 제공하고 운용 및 관리에 효율적일 것으로 사료된다.

참 고 문 헌

[1] P.Kocher, “Timing Attacks on Implementation of Diffie-Hellman, RSA, DSS, and Other Systems,” CRYPT’96, LNCS 1109, pp.104-113, Springer-Verlag, 1996.

[2] P.Kocher, J. Jaffe and B.Jun, “Differential Power Analysis,” CRYPT’99, LNCS 1666, pp.388-397, Springer-Verlag, 1999.

[3] H.Yoo, herbst, S. mangard, E. Oswald, and S. Moon, “investigations of Power Analysis Attacks and Countermeasures for ARIA,” WISA’06, LNCS 4298, pp.160-172, Springer-Verlag, 2007.

[4] ChangKyun Kim, IIHwan Park, “Investigation of side channel analysis attacks on financial IC cards”, KIISC, 18-1 pp.31-35, KIISC, 2008

[5] ISO 18013-1, Information technology-Personal

identification-ISO-compliant driving licence-Part 1: Physical characteristics and basic data set, ISO, 2005.

[6] ISO 18013-2, Information technology-Personal identification-ISO-compliant driving licence-Part 2: Machine-readable technologies, ISO, 2007.

[7] ISO 18013-3: Information technology-Personal identification-ISO-compliant driving licence-Part 3: Access control, authentication and integrity validation, ISO, 2006.

[8] ISO 7816-4: Identification cards-Integrated circuit(s) cards with contacts-Part 4: Interindustry commands for interchange, ISO, 2005.

[9] ISO 7816-8: Identification cards-Integrated circuit(s) cards with contacts-Part 8: Security related interindustry commands, ISO, 2004

[10] ISO 10202-4: Financial transaction cards-Security architecture of financial transaction systems using integrated circuit cards-Part 4: Secure application modules, ISO, 1996.

[11] Richard Fernandez. enterprise Dynamic Access Control(EDAC) Compliance with the Role-Based Access Control(RBAC) Standard ANSI/INCITS 359-2004, 2005.

[12] ISO 19794-2, Information Technology-Biometric Data Interchange Formats-Part 2: Finger Minutiae Data, ISO, 2005.

[13] ISO FDIS 19794-3, Information Technology-Biometric Data Interchange Formats-Part 3: Finger Pattern Spectral Data, ISO, 2006.

[14] ISO 19785-1, Information technology-Common Biometric Exchange Formats Framework-Part 1: Data element specification, ISO, 2006

[15] ISO 9796-2, Information technology-Security techniques-Digital signature schemes giving message recovery-Part 2: Integer factorization based mechanisms, ISO, 2002.

[16] ISO 8825-1:2002: Information technology-ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), ISO, 2000.

[17] R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, 2002.

[18] T.Freeman,R.Housley,A."Serverbased Certificate Validation Protocol (SCVP)", RFC 5055, 2007.

전 상 훈 (Sang-hoon Jeon) 정회원

2000년 2월 한신대학교 정보통신학 (이학사)

2002년 8월 숭실대학교 컴퓨터학 (공학석사)

2005년 8월 숭실대학교 컴퓨터학 (박사수료)

<관심분야> 네트워크 보안, 암호학, 스마트카드,

전 문 석 (Moon-suk Jun) 정회원

1981년 숭실대학교 전산학 학사

1986년 Univ. of Maryland 전산학(석사)

1989년 Univ. of Maryland 전산학(박사)

1991년 3월~현재 숭실대학교 정교수

<관심분야> 네트워크 보안, 암호학, 스마트카드