NFC를 활용한 능동형 인증 방법

정회원 이 민 구*°, 김 동 완*, 손 진 수*

Active Authentication Method using NFC

Min-Gu Lee*°, Dong-Wan Kim*, Jin-Soo Sohn* ***Regular Members***

요 약

최근 NFC(Near Field Communcation) 기반 통신 기능을 채용한 스마트기기 및 OS 등이 확산됨에 따라 기존 RFID를 이용하던 다양한 응용 분야에 대하여 NFC로의 대체가 진행되고 있다. 대표적으로 출입 통제나, e-ticket, 전자 결제 등의 분야에서 NFC가 RFID를 대체하고 있다. 기존의 RFID는 수동적 통신 기능만 제공하여 충분히 안전한 인증 및 권한 검증 방법을 제시하지 못하였으나, 능동형 통신기능을 제공하는 NFC를 활용하면 보다 안전한 인증 방식을 제공하여 다양한 응용에서 요구하는 보안 요구사항을 만족시킬 수 있다. 그러므로 본 논문은 NFC의 능동형 통신 기능을 활용하여 신용카드 결제, 출입통제 시스템 등에 활용될 수 있는 능동형 인증 방식을 제공할 수 있는 방법으로 EAP(Extensible Authentication Protocol)과 AAA(Authentication. Authorization and Accounting) 규약을 활용하는 방법을 제안한다.

Key Words : NFC, Security, EAP, AAA, 인증

ABSTRACT

Since most of recently launched smart devices support NFC(Near Field Communication), RFID applications are tend to be replaced. For instance, previous RFID application areas such as entrance control, mobile e-ticket, electronic payment and et. al are subject to change using NFC. Due to the limitation of passive communication in RFID, it is impossible to cover all security requirements of authentication and authorization mechanism that wide areas of applications demand. Therefore authentication and authorization mechanism based on NFC is very attractive to such applications because active communication methods make it possible to be highly secure in authentication and authorization. In this paper, authors propose a new approach of secure authentication and authorization mechanism using NFC smart devices based on EAP(Extensible Authentication Protocol) and AAA(Authentication, Authorization and Accounting) protocols.

Ⅰ. 서 론

각 통신 응용에 적합한 통신 범위를 갖는 다양한 무선 통신 기술들이 지속적으로 발전하고 있다. 통신 범위를 기준으로 근접거리(proximity)에서만 통신이 가능한 RFID, NFC(Near Field Communication)[1]에서부터 개인 영역(Personal Area Network)에서의 Zigbee[2], Bluetooth[3] 등이 있으며, WLAN(Wireless Local Area Network) 등의 근거리 통신과 광대역 이동통신 서비스인 WCDMA, Mobile WiMAX 등이 있다. 이러한 통신 기술들은 각 응용에 적합한 방식으로 채택되고 있으며, 최근 출시되는 다양한 스마트기기 - Apple사의 iPhone 및 iPad 시리즈나, Android OS 채용 스마트 폰 및 스마트 패드, RIM

※ 본 연구는 지식경제 프론티어 기술개발사업의 일환으로 추진되고 있는 지식경제부의 유비쿼터스컴퓨팅및네트워크원천기반기술개발사업의 지원에 의한 것임(11C3-J1-20S)
* KT 종합기술원 ({mingu.lee;dongwan.kim;jinsoo.sohn}@kt.com), (° : 교신저자)
논문번호 : KICS2011-09-416, 접수일자 : 2011년 9월 27일, 최종논문접수일자 : 2012년 1월 30일

의 Blackberry 시리즈 등 - 는 이동 중 통신이 가능한 광대역 이동통신 기술과 함께 근거리에서 고속 통신이 가능한 WLAN 기술을 동시에 탑재하고 있다. 그러나 최근 근접거리 기반의 응용에 대한 요구가 급증함에 따라 각 스마트기기에서도 NFC를 지원하고 있으며, 2011년 초 출시된 Google과 삼성의 Nexus S는 NFC 기술을 채용하여 Google Wallet 등의 서비스를 출시하였고, 삼성의 Galaxy S II, RIM의 BlackBerry Bold 등 최근 출시되는 많은 스마트기기에서 NFC 기술을 채택하고 있다. NFC 채용 단말이 급증함에 따라 스마트기기 제조사 및 이동 통신 사업자, 서비스 제공자 등은 NFC 스마트기기를 활용하여 전자지갑, 출입통제, 명함 교환, 모바일 결제 등 다양한 분야의 응용 서비스를 추진하고 있다.

이렇게 주목받고 있는 NFC의 주요 응용 분야 중 많은 응용에서 요구되는 핵심 기반 기술은 사용자의 인증으로, 기존의 RFID 태그의 주요 응용 분야인 출입통제나, 교통카드 등을 NFC로 대체하여 NFC 스마트기기를 이용하여 서비스 인증을 수행하고, 인증이 완료된 경우 사용자에게 서비스를 제공하는 분야의 응용에서 RFID를 대체하고 있다. 일례로 KT텔레캅은 기존 RFID의 주요 응용 분야인 출입통제 시스템을 NFC 스마트기기로 대체하여 개발[4]하였으며, MasterCard의 PayPass와 VISA의 Blink NFC Payment Card를 지원하는 신용카드 결제 앱(App)인 CHARGE Anywhere[5]는 NFC 스마트기기를 스마트 신용카드 결제 기능을 제공하는 이동형 판매시점정보관리 장치(Point of Sales - POS)로 사용하도록 하는 응용이다.

NFC 스마트기기를 이용하여 인증 서비스를 제공하는 경우에 보안은 매우 중요한 이슈이다. 그러나 NFC 기술은 기존의 RFID 기반 스마트카드와 마찬가지로 근접거리 통신방식의 특성에 기반하여 중간자 공격(man-in-the-middle attack)등의 보안 위협에 취약할 수 있다. 마그네틱 신용카드나 RFID 스마트카드에서 발생하는 스키밍(skimming) 등이 주로 악의적인 리더기를 활용하여 카드 정보를 복제하여 발생하는 것을 고려하면, NFC 기반 전자 지갑, 전자 결재, 출입 통제 등의 응용에서도 악의적 NFC 리더기를 사용하는 해킹 수법에 노출 될 가능성이 크다. 이러한 인증의 보안 이슈를 해소하기 위하여 본 논문은 NFC의 능동 통신 모드를 활용하여 안전한 인증을 제공할 수 있는 방법을 제시한다. 본 논문의 구성은 2장에서 NFC의 특징 및 보안 위협과 보안 위협을 해소하기 위한 관련연구를 살펴보고, 3장에서는 기존 RFID와 차별화된 NFC 만의 장점을 기반으로 안전한 인증 방법에 필요한 요구사항을 기반으로 기존 응용들에서는 제공할 수 없었던 안전한 인증방식을 제공하는 새로운 방법을 제시하고, 4장에서 결론을 맺는다.

Ⅱ. NFC 개요 및 인증의 보안 위협

2.1. NFC 개요

NFC는 13.56MHz 대역의 통신 주파수에서 106Kbps에서 424Kbps의 통신 속도를 제공하는 통신범위 약 10cm 이내의 근접거리 무선 통신 기술이다. NFC는 네트워크 설정에 필요한 시간이 약 0.1초 수준으로, 기존의 Bluetooth 등과 차별화된 즉시 응답성이 필요한 형태의 응용에 매우 적합하다. NFC는 두 단말의 안테나를 통하여 유도기전력을 기반으로 통신하는 기술로 각 단말의 전자기장의 생성 여부에 따라 수동 통신(passive communication) 모드와 능동 통신(active communication) 모드로 동작한다. 능동 통신 모드는 단말이 캐리어 주파수에 전자기장을 생성하여 다른 단말에 유도기전력을 공급하여 통신을 수행하는 모드로 일반적으로 전원이 필요한 모드이다. 수동 통신 모드는 단말이 스스로의 전자기장을 생성하지 않고, 능동 통신 모드의 단말이 생성한 전자기장으로부터 유도되는 전력을 이용하여 통신을 수행하는 모드를 말한다. 이러한 2개 모드를 활용하면 NFC 단말은 다음과 같은 3가지 형태의 동작 모드로 통신을 수행할 수 있다.

- 카드 모사: NFC 단말의 수동 통신 모드 동작으로, RFID 태그처럼 내부 전원 없이 외부의 리더기/기록기에 NFC 카드의 정보를 제공하여, 기존 RFID의 응용을 지원할 수 있다. 이 모드는 ISO/IEC 14443[6]의 표준을 준수하여 기존 스마트카드에서 사용하던 모바일 결제 서비스 등을 사용할 수 있으며, 그 외에 출입통제, 교통카드 등의 응용에 사용 가능하다.
- RFID 리더기/기록기 모드: NFC 단말의 능동 통신 모드의 동작으로 외부의 수동 통신 모드의 NFC 및 RFID의 정보를 읽거나 쓰는 역할을 수행한다. 이 모드는 NFC 단말을 통하여 외부의 스마트 포스터나 쿠폰 등의 정보를 읽거나, 전자지갑에서 이용 요금을 지불하는 등의 응용에 주로 사용되며, 기존 RFID를 활용하여 사용자에게 제공하지 못하던 새로운 응용을 제공할 수 있다.

• 동등 계층 통신(Peer-to-Peer) 모드: 두 단말이 모두 능동 통신 모드로 통신하여 두 단말의 각자의 전자기장을 생성하여 상호 통신을 수행하는 모드이다. 이 모드를 활용하면 스마트기기 간 정보를 능동적으로 상호간 송수신 할 수 있어 명함 교환이나, 사진, 동영상 등의 교환이 가능하며, 전자 지갑의 일환으로 동등 계층간 자금 이체 등이 가능하다.

NFC는 RFID의 리더기/기록기 모드로의 동작과 동등 계층 통신의 지원으로 기존 RFID에서 제공하지 못하던 새로운 응용을 제공하거나, 기존 RFID에서 가지고 있던 보안상의 이슈를 해소하는 등의 장점을 얻을 수 있다. 이러한 특징을 활용하여 안전하고 편리하고 다양한 상황에서 사용 가능한 범용적 인증 방식을 도입하면 다양한 응용에서 NFC 스마트기기 사용자가 NFC 채택 단말 하나만 소지하고 다니는 것으로 해당 서비스를 활용할 수 있도록 지원이 가능해진다.

2.2. NFC의 잠재적 보안 위험

기본적으로 NFC는 근거리 무선 통신이므로 SSL(Secure Socket Layer)등의 별도 무선구간 보안을 확보하지 않는 한 도청 등의 위험에 취약[7]하다. 이러한 무선구간 통신의 보안 위협을 해소하기 위하여 NFC의 표준화 단체에서는 NFC-SEC[8] 보안 규약을 정의하고 있다. NFC-SEC의 NFCIP-1(Near Field Communication Interface Protocol - 1) 보안 규약은 각 NFC 장치간 통신에서 공유 비밀키 기반의 보안 통신 방법을 제공한다. NFC 각 장치는 공개키와 개인키를 가지고 키 생성 규약을 따르게 되며, 그에 따라 생성된 마스터키를 기반으로 기밀성 키(KE)와 무결성 키(KI)를 생성하여 AES-CTR 암복호화 및 AES-CBC를 통한 무결성 검증을 수행[9]한다. 그러므로 사전 공유된 비밀키가 없어도 단말 사이의 무선 구간에서의 안전한 통신의 지원이 가능하다. 이는 기존 RFID와 달리 공유된 비밀키가 없어도 상호간 보안이 유지되는 통신 지원이 가능하여 보다 다양한 서비스의 제공이 가능하도록 한다. 또한 SN(sequence number)를 활용하여 무선구간의 통신을 도청을 통한 재생 공격(replay attack)을 방지할 수 있도록 하고 있다.

NFC는 이처럼 다양한 기법의 무선 구간의 보안성 확보를 위하여 노력하였지만 기존 RFID의 표준인 ISO/IEC 14443을 지원하고 있어 기존 ISO/IEC14443 표준을 따르는 응용 시스템을 지속 지원할 수 있다. 그러나 해당 표준에서 별도의 보안

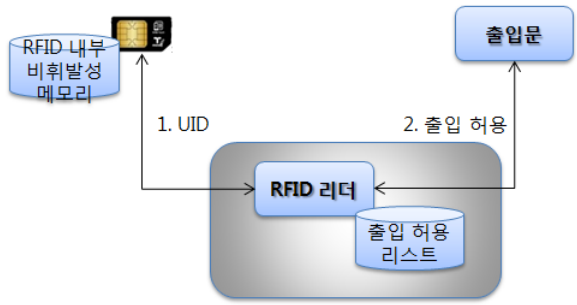

그림 1. RFID 출입통제의 구성
Fig. 1. Structure of RFID entrance control

규약을 정의하지 않아서 각 응용 시스템에서 자체적인 보안 규약을 구현하여 발생한 보안 취약성을 그대로 가지게 된다. 특히 무선 통신을 채택한 스마트카드는 비접촉식 통신이라는 특성으로 기존의 마그네틱 카드보다 쉽게 정보 노출이 가능[10]하여 그 문제가 더욱 크며, RFID의 가장 대표적인 솔루션인 NXP의 Mifare classic[11] 카드의 경우에는 역공학(reverse engineering)을 통한 다양한 해킹 방법이 노출되어 해당 솔루션을 사용한 스마트 신용카드 및 국내 외의 다양한 교통카드들의 보안 취약성이 노출[12-14]되었다. 또한 RFID를 활용한 각종 스마트카드 형태의 신용카드들에 대한 보안 위험성[15]이 연구되었으며, 전자 여권 역시 다양한 보안 위협에 의하여 개인 정보가 노출될 수 있음이 확인[16,17] 되었다. 이러한 위험은 여권이나 신용카드의 주요 정보를 비접촉식 RFID 리더기만 가지고도 무단으로 획득할 수 있어 악의적 해커가 신용카드 및 여권 등을 복제하여 악의적으로 이용할 수 있는 심각한 보안 문제를 나타낸다. 그러므로 이러한 문제를 원천적으로 해소하기 위해서 비접촉식 카드에 저장된 정보는 반드시 리더기 해킹에 대한 대비가 필요하다.

NFC 스마트기기에 저장된 정보를 리더기에 제공하는 것 외에도 출입 통제, 신용카드 결제와 같은 종류의 응용들은 사용자가 정상적으로 서비스를 이용할 수 있는지 여부를 검증하는 인증 절차가 필요하다. 예를 들어 기존의 단순 출입 통제만 수행하는 시스템을 생각해 보자. 단순 출입 통제 시스템의 경우 그림 1처럼 출입할 사람 혹은 차량의 신분을 나타내는 RFID 태그와, 사람 혹은 차량의 신분을 파악하여 출입 여부를 결정하는 RFID 리더기, 그리고 실제 사람 혹은 차량의 출입이 이뤄지는 출입문으로 구성된다. RFID 리더기는 전자기장을 생성하여 RFID 태그의 접근을 대기하며, RFID 태그가 접근

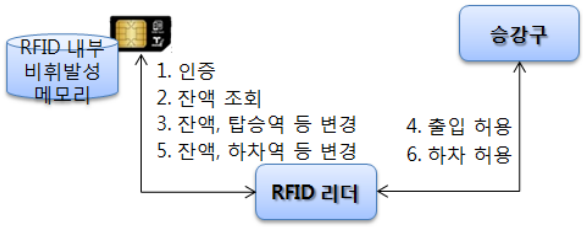

그림 2. 교통카드 응용의 구성
Fig. 2. Structure of RFID public transportation payment

하여 통신이 가능해지면 해당 태그에 기록되어 있는 유일한 신분 정보를 읽어 출입 허용 목록에 들어있는지 판단하고, 허용 리스트에 포함된 경우 출입구를 개방하고, 포함되지 않은 경우 출입을 거부하는 형태로 동작한다. 이 모델은 다양한 RFID 기반의 출입 통제 시스템에서 활용되고 있으며, 실제 아파트 주차장이나 건물 내 주차 카드 등의 응용에 사용 되고 있다. 위에서 논의한대로 NFC의 수동통신 모드는 RFID 태그 기능을 지원하므로, 최근 NFC 스마트폰을 이용하여 유사한 응용 시스템이 만들어지고 있다. 그러나 이러한 방식은 카드 정보의 해킹(RFID 태그의 신분 정보 복제 혹은 RFID 태그의 신분 정보 임의 생성 등의 방식)에 취약하여 보안이 중요한 응용에는 사용이 적합하지 않다.

기존 RFID 태그의 신분 정보만을 이용하여 구축하는 이런 모델의 보안 위험성을 극복하기 위하여 Mifare classic 카드는 단말과 리더기간 상호 인증을 통하여 보안성을 확보하는 기능을 제공하며, 이 보안 기능을 기반으로 국내외 여러 국가에서 교통카드로 사용되고 있다. 보안이 중요한 RFID 응용의 대표적인 예제인 교통 카드 응용은 그림 2처럼 RFID 태그 내부의 비휘발성 메모리 영역에 카드의 잔액 정보를 기록하고, 대중 교통 이용시, 탑승 역 정보, 탑승 시각 등을 기록하고, 대중 교통의 이용이 종료될 때 다시 해당 정보를 읽어 최종 이용 금액을 잔액 정보에서 삭감하는 형태로 동작한다. 그러므로 RFID 태그 내부의 비휘발성 메모리 영역에는 잔액 정보 및 이용 요금 정산을 위한 탑승 역 및 탑승 시각 등의 중요 정보가 기록되어 있으므로 반드시 합법적인 RFID 리더기만 읽기와 쓰기가 가능해야 한다. 그러므로 Mifare classic 카드 솔루션은 RFID 리더기와 RFID 태그 사이에 상호 인증을 수행하여 신뢰 관계가 생성하여야만 RFID 태그 내부 정보로의 접근을 허용하는 솔루션을 제공하고 있으며, 이를 이용하여 그림 2와 같은 형태의 교통카드 응용의 필요 기능을 수행한다. 그러나 그림 2의 모델에서 잔액의 갱신 및 조회 등의 요구의 주체는 RFID 리더기로, RFID는 근접한 RFID 태그의 정보를 평문으로 파악하게 된다. 그러므로 악의적 해커는 RFID 태그에 대한 해킹이 아닌 RFID 리더기에 대한 해킹을 시도하여, 해킹된 리더기를 이용하는 사용자들의 중요 정보를 탈취/조작할 수 있게 된다. 이러한 RFID의 위험은 RFID 리더기에서 요청하는 메시지에 대하여 일정 수준의 검증(공유 비밀키 등) 후 응답을 보내는 형식의 규약만 사용하는 것으로는 충분한 검증이 불가능하게 되어 발생하는 문제이다.

이러한 문제는 비단 RFID뿐만 아니라 NFC응용에서도 동일하게 발생할 수 있다. NFC 리더기에 인증/승인 로직을 구현하는 경우 악의적 사용자가 NFC 리더기를 해킹된 리더기로 변경하거나, 허가되지 않은 악의적 리더기를 설치해 놓아 타 사용자의 카드 정보를 확보하여 악의적 이용(카드 복제 등)이 가능할 수 있다. 이러한 중간자 공격 형태를 활용한 중요 정보의 노출 위험은 NFC 리더기에서 NFC 카드 중요 정보에 대한 접근 허용이 근본 원인이다. 즉, 전자 결제 응용에 있어 카드 내의 결제 잔액이나, 출입 통제에 있어 카드의 인증 번호 및 비밀번호 등을 NFC 리더기가 확보하여 서비스를 제공하게 되면, NFC 리더기의 해킹을 통해 중요 정보가 노출되거나 잘 못 갱신될 수 있게 된다. 그러므로 NFC 리더기는 NFC 응용에 사용되는 NFC 스마트기기의 중요 정보를 직접 접근할 수 없도록 하는 것이 최선이다. 이러한 보안 위협을 극복하기 위한 방법으로 NFC의 동등 계층 통신 모드를 사용하여 정보 제공을 요청하는 장치를 사전에 검증함으로써 보안 위험의 극복을 시도할 수 있다. 즉, 리더기의 신호에 의하여 반응하는 수동적 인증이 아닌, 능동적으로 자신에 정보를 요청하는 장치에 대하여 직접 인증을 수행하여 악의적으로 해킹된 리더기의 접근을 사전에 차단할 수 있어야 한다. 그러므로 NFC 스마트기기는 능동적으로 자신이 정보를 요청하는 시스템을 검증하여 기존 RFID에서는 어려웠던 안전한 능동형 인증 방식을 제공할 수 있도록 해야 한다.

2.3. 관련 연구

기존의 RFID 기반 스마트카드의 결제 및 현재의 NFC 기반 스마트카드는 ISO14443 표준을 기반으로 RFID/NFC 태그의 보안 모듈을 이용하여, 내부 저장소의 접근을 위한 비밀키 등을 이용하여 인

증이 완료된 경우에 접근을 허용하는 형태이다. 그러나 이러한 방법에 대하여 이미 앞에서 언급한대로 다양한 해킹 방법이 알려져 보안상의 위험을 노출하였다. NFC는 리더기/기록기 모드를 제공하므로 위의 Charge Anywhere처럼 NFC 스마트기기를 판매시점정보관리 장치로 활용이 가능하게 되었고, 그에 따라 스마트카드를 접근하기 위한 비밀키에 대한 관리의 중요성이 대두되었다. 그러므로 H-C. Cheng 등[18]은 NFC 스마트기기를 이동형 판매시점정보관리 장치로 활용하기 위한 공유비밀키 정보를 안전하게 관리하기 위한 다양한 방법을 분석하고, 공유비밀키 정보를 장치에 저장하는 것이 아닌 서버에 저장하고 장치에는 필요시 서버로부터 받아오는 방법을 제시하였다. 그러나 이 방법은 NFC 내부의 중요 정보를 리더기가 접근할 수 있다는 기존의 단점을 그대로 가지고 있어, 해킹된 리더기를 통한 NFC 접근에 대한 대응으로는 부족하다.

S. Tamrakar 등[19]은 NFC 탑재 이동전화를 이용하여 대중교통의 매표(ticketing)를 위한 신분 확인 방법을 제시하였다. NFC에 단순화된 인증서를 설치하고, 해당 인증서를 기반으로 교통수단의 출입구에 설치되는 NFC 리더기에서 인증을 수행하고 교통수단 이용 내역을 기록하고, 이용 내역에 대한 부인봉쇄 등의 방법을 제시하였다. 그러나 이 방법은 위의 H-C. Cheng 등의 연구와 마찬가지로 인증을 NFC 리더기 에서 수행하여 해킹된 리더기를 통한 NFC의 내부 주요 정보 탈취에 취약한 단점이 있다.

W. Chen 등[20]은 사용자의 인증서를 기반으로 하는 NFC 전자 결제 방법을 제시하였다. 영국 정부에서 발행하는 사용자 인증서를 사용자의 NFC 이동전화 및 이동전화 사업자와 사용자 인증서간 전자 결제를 위한 자격 정보를 연동하는 절차를 수행하여 각 이동전화 사업자와 NFC 단말간 공유 비밀키를 공유한다. 이후 실제 결제 과정에서 NFC 신용카드 결제기는 인증에 필요한 공유 비밀키 등의 핵심 보안 정보를 파악하지 못한 상태에서 메시지 전달자 역할만 수행하여 안전하게 전자 결제를 수행할 수 있는 방법을 제시하였다. 그러나 이 방법은 국가적인 사용자 인증서라는 인프라의 구축이 필요하고, 사전에 자격정보 연계 절차가 필요하며, 전자 결제의 수행시 국가에서 관리하는 신분 정보가 같이 활용되어 개인 사생활을 침해할 수 있는 문제를 야기할 수 있는 단점이 있다.

W. Chen 등[21]은 NFC 채용 단말기의 인증 및 모바일 결제를 GSM 네트워크의 구성 요소들을 활용하여 제공할 수 있는 방법을 제시하였다. GSM 네트워크에서의 인증은 시도-응답(challenge-response) 방식과 전송 구간내 암호화 기능을 제공하여, GSM 단말과 네트워크 인증 서버간의 공유 비밀키 등의 정보를 인증자 등에 노출하지 않으면서 안전한 인증을 제공하고 있다. 이 인증 방식을 NFC에 적용하는 방법을 제시하였으나, NFC의 인증을 수행하는 NFC 리더기 (예를 들어 상점의 판매시점정보관리 장치)와 NFC 단말이 모두 같은 통신사업자의 네트워크를 사용해야만 인증이 가능한 문제를 가지고 있다. 그러나 일반적인 경우, 전자 결제를 수행하는 NFC 리더기는 유선네트워크에 연계되어 있거나, 타 통신사업자의 이동 통신 네트워크를 사용할 수 있어 충분한 서비스를 제공할 수 없다. 저자들은 GSM 뿐만 아니라 3G네트워크를 사용하는 경우에도 유사한 방식을 제시[22]하였으나, 역시 마찬가지로 동일한 사업자의 3G네트워크를 사용하는 경우에만 서비스가 가능하다는 공통된 한계가 있다. 또한 향후 전산 자원의 발전에 따라 보안 위협이 새롭게 대두되는 경우, 기존에 구축된 인프라에 대하여 새로운 인증 방식을 적용하는 것이 어렵다는 공통된 단점을 가지고 있다. 그러므로 NFC 인증 인프라를 구축하게 되면 현재의 인증방식 뿐만 아니라, 향후 추가될 새로운 인증방식도 지원할 수 있는 유연한 구조가 필요하다.

Ⅲ. NFC 기반의 능동형 인증 방법

NFC 리더기는 지역적으로 분산되고, 악의적 해커에 의한 해킹이 가능할 수 있으므로 인증 및 결제 등에 필요한 주요 정보에 접근이 불가능해야 한다. 그러므로 리더기에서 인증/결제 등을 직접 처리하는 그림 2의 구조는 리더기 해킹에 대응이 불가능하므로, 주요 정보를 보안성 확보가 용이한 중앙의 인증시스템과 실제 단말에서 수행하는 그림 3 형태의 모델 도입이 필요하다. 그림 3 모델에서의 NFC 리더기는 NFC 스마트기기로부터의 인증 요청에 대하여 직접 인증을 수행하는 것이 아니라 중앙의 인증 서버로 단순 전달하여 중앙의 인증서버에서 인증을 수행할 수 있도록 지원하는 형태로 인증 요청자와 인증 서버간 인증 결과를 신뢰된 인증 서버로부터 전달받아 서비스를 제공할 수 있도록 장치를 제어하는 모델이다. 이 모델에 따르면 인증에 사용되는 공유비밀키 등의 주요 정보를 리더기에 배포하지 않아도 서비스의 제공을 위한 인증이

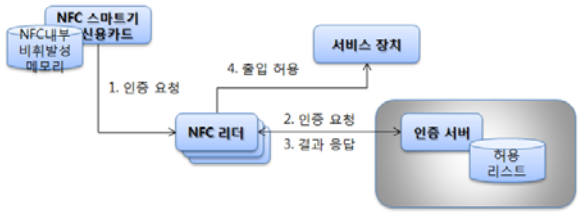

그림 3. 중앙의 인증 서버를 사용하는 NFC 인증 모델
Fig. 3. Structure of NFC authentication with central authentication server

가능하므로, 신용카드 결제기, 출입통제기 등 지역적으로 분산된 많은 수의 인증자가 필요한 응용에 매우 적합하다. 만약 그림 3의 인증 모델을 따르지 않으면 인증 대상 리스트를 지역적으로 분산된 모든 NFC 리더기에 동기화 시켜야 정상적으로 서비스가 가능하게 되는 난관에 봉착하게 된다.

3.1. 안전한 인증 지원을 위한 필요 사항

2장에서 간략히 살펴본 단순 주차장 출입 통제 응용에서부터, 매우 높은 보안성을 요구하는 신용카드, 전자결제 등의 응용까지 NFC 기반의 인증을 활용하는 다양한 응용들이 존재한다. 특히 마그네틱 기반의 신용카드의 카드 번호 등의 주요 정보를 손쉽게 파악할 수 있는 단점을 해소하기 위하여 도입된 스마트카드는 RFID를 사용하여 보다 안전한 결제 방법을 제공한다. 신용카드 리더기는 스마트카드로부터 실제 카드의 번호와 유효기간 등의 정보를 확보하기 위하여 스마트카드의 내부 정보를 읽기/쓰기 모드로 접근할 수 있는 비밀키를 가지고 있음을 증명하고, 확보된 접근 권한으로 실제 카드 번호(혹은 카드번호와 매핑될 수 있는 다른 주요 정보)와 유효기간 등의 정보를 확보하여, 신용카드 승인 서버에 제공하여 결제하고자 하는 신용카드를 소지하고, 제시하였음을 인증(authentication)하고, 신용카드 승인 서버는 해당 카드의 한도 초과 여부, 분실 카드 여부 등의 권한 검증(authorization)을 수행하여 모든 것이 정상적인 경우 카드 승인 요청에 대한 승인 완료 응답을 보내야 한다. 그러므로 기본적으로 제시되는 NFC 카드를 인증하여야 하고, 해당 카드에 대한 이용 권한을 제어할 수 있어야 한다.

추가적으로 특정 응용에서는 신용카드 결제 등의 경우와 달리, 서비스를 사용하는 동안 지속적으로 세션을 유지해야 하는 경우도 존재한다. 예를 들어 차량 임대사업에서 NFC 스마트폰을 차량의 스마트키를 활용하면, NFC 스마트기기를 차량이 운행되는 동안 지속적으로 세션이 유지 되어야 한다. 그러므로 특정 유형의 응용에서는 인증에 대한 관리가 세션 기반으로 이뤄져야 한다. 또한 차량 임대사업의 경우, 차량의 제어기능, 정산기능 및 관리기능 등이 필수적으로 요구[23]된다. 차량의 제어기능이란 기본적으로 현재 차량을 사용하고자 하는 사람이 정말 그 사람이 맞는지를 판단하는 인증 기능과 차량의 예약 정보와 사용자의 일치성 확인, 차량의 예약 시간에 따른 이용 권한 등을 확인하여 차량의 사용 허가 여부를 결정하는 권한제어 기능 등을 의미하며, 정산 기능이란 차량의 이용시간, 주행거리, 차량의 위치, 속도 등의 정보를 중앙 제어 서버로 전달하는 사용정보 수집(accounting) 및 처리 기능 등을 의미한다. 이러한 응용은 사용 세션 동안 지속적으로 권한에 대한 제어가 이뤄져야 한다. 예를 들어 차량의 초기 인증 시점에는 적합한 권한을 소유하고 있었으나, 차량을 운행하던 중 예약 기간을 초과하거나, 주행거리 한계를 초과하는 등의 특정 사유 발생시 추가 이용을 차단하는 등의 제어 기능이 필요하다.

이러한 부분들을 종합하면 다양한 응용에서 사용할 NFC 스마트기기를 기반으로 하는 인증 체계에 요구되는 특징들을 살펴보면 다음과 같다. ① 인증자인 NFC 리더기의 해킹에 대한 대비를 위하여 NFC 리더기는 사용자의 NFC 스마트기기 내부의 공유비밀키 등의 주요 정보 파악이 불가능해야 하며, ② 인증 서버는 NFC 스마트기기 내부의 정보를 이용하여 안전한 인증을 수행하여 서비스 제공 여부를 제어할 수 있어야 하고, ③ 인증 절차에 있어 NFC 내부의 공유비밀키 등의 주요 정보를 인증 서버에 제공하기 이전에 NFC 스마트기기가 인증을 요청하는 인증 서버를 먼저 검증할 수 있도록 상호 인증 기능을 제공해야하며, ④ NFC 스마트기기 내부의 유효한 정보를 기반으로 요청하는 서비스의 제공 여부를 판단하는 권한 관리가 가능해야 하고, ⑤ 세션 기반의 인증 및 서비스 제공이 가능할 수 있어야 하며, ⑥ 지역적으로 분산된 많은 수의 인증자인 NFC 리더기에 대하여 일관적인 서비스 제공이 가능해야 하고, ⑦ 향후 발생할 수 있는 새로운 보안 위협에 대비하여 다양한 보안 규약의 확장이 가능해야 한다. 이러한 특징들은 적법한 사용자에 한해 서비스를 허용(authentication & authorization)하고, 서비스 이용 정보를 수집하여 이용료를 부과(accounting)하고, 세션에 대한 실시간 관리가 이뤄지는 네트워크의 접속 및 인증체계(Authentication, Authorization and Accounting - AAA)[24]와 유사

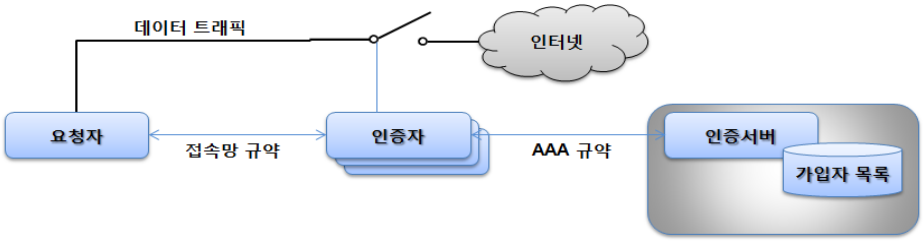

그림 4. 네트워크 접속 인증 체계
Fig. 4. Generalized structure of network authentication, authorization and accounting

한 속성을 가진다.

3.2. 능동형 인증 체계

네트워크 접속 인증 체계는 그림 4의 모델을 따라 구성되며. 이 모델은 그림 3의 모델과 매우 유사하다. 요청자(supplicant)는 네트워크의 접속 권한을 요청하는 사용자로 그림 3의 NFC 스마트기기에 해당되며, 인증자(authenticator)는 네트워크의 접속을 허용하거나 차단하는 스위치 제어 기능과 사용량, 사용시간 등의 세션 이용 정보를 추출하여 인증서버(authentication server)로 전달하는 역할을 수행하는 장치로 그림 3의 NFC 리더기에 해당한다. 인증 서버는 가입자 목록을 가지고 실제 인증 로직을 수행하며 권한 제어를 수행하는 장치로, 인증자에서 보내는 세션 기반 사용량 정보 등을 처리하고, 정책의 변경 등의 이벤트를 인증자로 전달하여 서비스에 반영되도록 하는 시스템으로 그림 3의 인증서버에 해당한다. 이 모델에 따르면 지역적으로 분산되어 있는 다수의 인증자는 서비스 제공 여부를 결정하는 스위치 제어 역할을 수행하며, 실제 인증 처리는 요청자와 인증 서버간 수행하도록 되어 있고, 인증서버는 요청자에 대한 권한 검증을 수행하여 최종 인증 완료 여부를 인증자에게 제공하므로 NFC 기반 인증의 요구사항의 ②와 ④를 만족시킬 수 있다. 또한 인증자는 기존의 네트워크 인증에서와 마찬가지로 지역적으로 분산 설치가 가능하고, 다수의 인증자와가 인증 서버와의 안전한 연동이 가능하므로 지역적으로 분산된 다수의 NFC 리더기를 사용하는 응용에 적합한 구조로 특징 ⑥을 만족시킨다. 더욱이 인증자는 인증서버와 접속한 단말에 대한 세션 제어를 수행할 수 있어 특징 ⑤를 만족시킬 수 있다. 이러한 네트워크 접속 및 인증체계 모델은 이미 유선 초고속 인터넷, 와이브로, WiFi 같은 무선 상용 통신 시스템에서 성공적으로 사용되고 있어 그 안전성과 효용성은 충분히 입증되었다.

그림 4의 인증 모델은 데이터 트래픽의 허용 여부를 결정하기 위한 인증에 필요한 규약(protocol)으로 접속망 규약과 AAA 규약으로 구성되어 있다. AAA 규약은 주로 RADIUS[25]와 Diameter[26]를 사용하여 인증자와 인증 서버 사이의 통신을 지원한다. RADIUS와 Diameter 등의 AAA 규약은 중앙의 인증 서버와 인증자 사이에 공유비밀키 등을 활용한 방법을 통하여 상호간 보안 채널을 생성하여 통신을 수행하므로 메시지의 안전한 전달을 보장한다. 네트워크 접속 인증 방식은 각 응용의 요구사항에 따라 다양한 지원이 가능하도록 하기 위하여 다양한 확장이 가능하도록 속성-값 쌍 형태로 메시지를 송/수신 하도록 되어 있으며, 회사별 명령어(vendor specific command)를 지원하여 다양한 요구 사항에 대응할 수 있다. AAA규약은 기본적으로 요청자와 인증 서버 사이의 인증을 위한 비밀번호 인증 규약(password authentication protocol - PAP)[27]이나 시도-응답 비밀번호 인증 규약(challenge-handshake password authentication protocol - CHAP)[27] 등의 기본적인 인증 규약을 지원한다. 표 1은 이러한 특징을 갖는 AAA 규약인 RADIUS와 Diameter의 특징을 비교하여 보여준다.

RADIUS와 Diameter를 통한 인증 방식에 있어 기존 PAP이나 CHAP 등의 보안 규약은 그 보안 정도가 낮아 충분히 안전한 인증을 제공하기 어렵다. 그러므로 인증 규약은 보다 강력한 보안 기능을 확보하기 위하여 지속적으로 개발되어 상용 네트워크 시스템에 적용되고 있다. 그러나 이러한 규약의 신규 적용시마다 인증자의 변경이 필요하다면 그 비용이 매우 크므로 실제 상용 시스템으로의 사용이 어렵다. 예를 들어 높은 보안성을 제공하기 위하여 GSM 및 WCDMA 네트워크의 인증 규약인 인증 키 동의(Authenication Key Agreement - AKA) 인증 방식을 기존 네트워크에 적용하려면 기존에 PAP과 CHAP만 제공하던 모든 인증자에 AKA 인증을 위한 추가 기능을 적용시켜야 한다. 그러나 지역적으로 분산된 다수의 인증자에 AKA 기능을 적

용하는 것은 매우 어려운 일이므로 이를 극복하기 위하여 확장 가능한 인증 규약(Extensible Authentication Protocol - EAP)[28]을 도입하였다.

EAP 규약은 EAP-Request, EAP-Response, EAP-Success, EAP-Failure 등의 주요 메시지로 구성되어 있다. 인증자는 EAP메시지 내부의 정보를 파악하지 않아도 메시지 유형만 구분하여 처리하도록 되어 있어 매우 단순하게 구현될 수 있다. EAP-Response와 EAP-Request는 요청자와 인증 서버 사이의 인증 절차를 위한 메시지이고, EAP-Success와 EAP-Failure는 인증 서버에서 인증자로 인증 결과를 통보하는 메시지이다. EAP 규약은 인증자에서 인증 메시지를 직접 처리하는 것이 아니라 인증 서버로의 단순 중계만 수행하여 인증 절차가 요청자와 인증 서버 사이에 이뤄지도록 하는 규약이므로 인증자는 인증 규약에 대한 개발이 없이도 EAP 규약만 지원하면 다양한 인증 규약으로의 확장을 지원할 수 있어 NFC 인증의 요구사항 ⑦을 만족시킨다. 또한 인증자는 요청자와 인증서버간 인증 규약을 파악할 필요 없이 EAP-Request와 EAP-Response를 전달하는 것으로 인증이 가능하여 인증에 필요한 주요 정보를 파악하지 못하도록 인증 절차의 구성이 가능하므로, 인증자를 해킹 하더라도 요청자의 주요 정보 확보가 불가능하여 NFC 인증의 요구 사항 ①을 만족시킨다.

EAP 기반 인증 규약은 각 응용의 보안 요구사항에 따라 ID와 비밀번호를 이용하는 EAP-MD5[28]에서부터 공유비밀키를 활용하는 EAP-AKA[29], 인증서를 활용하는 EAP-TLS[30]등의 다양한 인증 방법이 존재한다. 다양한 인증 방식 중 EAP-MD5 등의 일부 규약은 상호 인증 기능이 없어 서버 인증이 불가능하므로 NFC 인증의 요구사항 ③을 만족시킬 수 없으나, EAP-AKA, EAP-TLS, EAP-TTLS[31], EAP-PSK[32] 등의 방식은 요청자에서 자신의 인증을 위한 정보를 인증 서버로 제공하기 이전에 인증 정보를 요청하는 인증 서버를 사전에 인증하는 상호 인증 기능을 제공하여 NFC 인증의 요구사항 ③을 만족시킬 수 있다. 표 2는 상호 인증이 가능한 대표적인 EAP 인증 규약의 비교표이다.

표 2. EAP 인증 규약의 특징 비교
Tab. 2. Comparisons of EAP protocols

규약	서버 인증	사전 공격 방어	세션 키	자격 증명	인증서
EAP-AKA	가능	가능	가능	공유 비밀 키	불필요
EAP-TLS	가능	가능	가능	인증서	서버/단말
EAP-TTLS	가능	가능	가능	내부 인증방식 의존	서버
EAP-PSK	가능	가능	가능	공유 비밀 키	불필요

3. 안전한 NFC 인증 방법 - NFC 능동형 신용카드

2절에서는 네트워크 접속 인증 체계의 특징을 확인하고, 해당 체계가 NFC 기반의 인증을 제공하기 위한 요구 사항에 만족시킨다는 것을 살펴 보았다. 그러나 네트워크 접속인증 체계에 사용되는 규약들

표 1. RADIUS와 Diameter의 비교
Tab. 1. Comparisons between RADIUS and Diameter protocols

분야	RADIUS	Diameter
데이터 크기 제한	속성 길이가(attribute length)가 1바이트로 속성값(attribute data)로 보낼 수 있는 메시지의 크기가 255바이트로 제한	속성 길이를 3바이트로 확장하여 해결
제어 흐름	UDP를 기반으로 흐름 제어 및 충돌 회피 기능 부족	TCP를 사용하여 흐름 제어 및 충돌 회피 기능 제공
분실 패킷 처리	RADIUS 클라이언트에서만 분실 패킷의 재전송 가능	중간 노드들에서의 분실 패킷의 재전송 지원
장애 탐지	장애 발생 노드의 탐지가 불가하여 장애 극복이 효율적으로 지원되지 못함	Hop-by-Hop 장애 탐지를 지원하여 보다 향상된 장애 극복 기능 제공
서버의 메시지 생성	클라이언트-서버 모델을 사용하여 서버에서 필요한 메시지 생성 불가	동등계층간 통신 모델을 사용함으로써 서버에서도 메시지를 생성 가능
세션 제어	서버 메시지 생성이 불가능하여 세션 제어 어려움	서버에서 세션 단절, 재인증 등 요청 가능
보안	Hop-by-Hop 보안만 지원하며, 속성-값 쌍(attribute-value pair)에 대한 보안이 취약함	IPSec/TLS등을 이용하여 단대단 보안을 지원하여 속성-값 쌍에 대한 보안 제공
회사별 명령어	미지원	지원

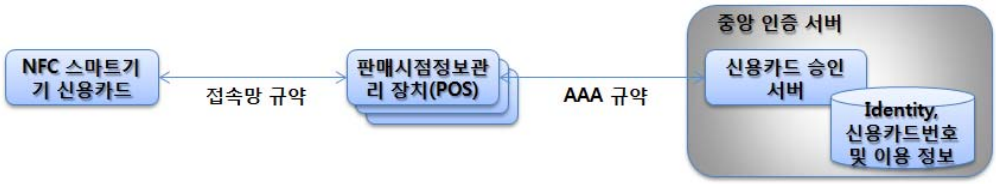

그림 5. NFC기반 안전한 능동형 신용카드 결제 응용의 구성도
Fig. 5. Structure of secure payment process of NFC active credit card

은 다양한 NFC를 이용한 인증에 활용하기 위해 몇 몇 추가 기능이 필요하다. 그러므로 이번 절에서는 네트워크 접속 인증 규약을 안전한 NFC 기반의 인증에 적용하는 방법을 살펴본다.

NFC를 활용한 능동형 인증의 다양한 응용 중 우선 신용카드 승인 처리를 위한 방법을 살펴보자. 능동형 신용카드 응용은 그림 5처럼 스마트기기에 있는 NFC 능동형 신용카드, 신용카드 결제를 수행하는 NFC 판매시점정보관리 장치, 그리고 실제 중앙의 승인을 처리해주는 신용카드 승인 서버로 구성된다. NFC 판매시점정보관리 장치는 네트워크에 연결이 가능하면 지역적으로 분산되어 설치가 가능하며, 신용카드 승인 서버는 안전한 신용카드 회사 혹은 결제 대행업체 등의 전산실에 설치되는 중앙 서버로 안전한 운용이 가능한 시스템이다. 실제 신용카드 승인에는 다양한 정보를 활용하지만 본 논문에서는 논의를 단순화하기 위하여 요청 금액, 통화종류, 가맹점 정보, 할부 개월 등의 정보만을 이용하여 승인 처리하는 것으로 가정한다. 또한 승인 요청, 조회, 승인 취소 등 다양한 트랜잭션 유형이 존재하나, 승인과 승인 취소에 대한 구현 방법만 살펴보고, 카드 승인 취소를 위해 필요한 정보는 승인 번호만 사용하는 것으로 가정한다. 또한 신용카드 번호는 중앙 서버에서 가지고 있으며, NFC 능동형 신용카드의 신분(identity)과 1:1로 매핑 되는 값으로 가정하여 혹시 모를 NFC 능동형 신용카드의 해킹에도 신용카드 번호가 노출되지 않도록 한다. 만약 한 NFC 스마트기기에 복수의 신용카드를 사용할 수 있다면, 각 신용카드 별로 별도의 신분과 자격(credential)을 가지고 있는 것으로 가정한다.

신용카드 승인 요청과 신용카드 승인 취소를 위한 규약은 EAP나 RADIUS/Diameter 규약에 정의되어 있지 않으므로 새로 정의가 필요하다. 신규 EAP 메시지 유형 등의 확장도 가능할 수 있으나, 신규 메시지를 정의하면 신용카드 승인 서버와 NFC 능동형 신용카드 간 통신에 추가적인 메시지가 필요하므로, 기존 EAP 메시지에 필요한 정보를 포함(piggyback)시켜 통신하는 방법을 사용한다. 이를 위하여 EAP 인증에 반드시 필요한 NFC 판매시점정보관리 장치에서 NFC 능동형 신용카드에 신분 정보를 질의하는 EAP-Request(Identity) 메시지에 요청타입|승인번호|금액|통화|할부|가맹점 정보를 포함시켜 보낼 수 있도록 확장하고, NFC 능동형 신용카드가 NFC 판매시점정보관리 장치에 신분 정보를 응답하는 EAP-Response(Identity) 메시지에도 요청타입|승인번호|금액|통화|할부|가맹점 정보를 포함시킬 수 있도록 확장한다. 또한 NFC 판매시점정보관리 장치는 신용카드 승인 절차를 파악할 수 없으므로, 최종적으로 신용 승인 여부를 신용카드 승인 서버로부터 받기 위하여 인증의 성공과 실패를 알려주는 EAP-Success 및 EAP-Failure 메시지에 각각 필요한 정보를 포함시키도록 확장한다. 표 3은 신용카드 승인 처리를 위한 EAP 메시지의 수정 사항을 나타낸다.

그림 6은 표 3의 내용으로 확장된 EAP 메시지를 활용한 EAP-AKA 기반의 신용카드 승인 트랜잭션 처리 절차를 나타낸다. EAP-AKA 이외에 EAP-TLS나, EAP-TTLS 등 다양한 인증 규약의 활

표 3. 신용카드 승인 절차를 위한 EAP 메시지의 확장
Tab. 3. Extensions of EAP messages for credit approvement

Code	Type	Type Data
0x01 Request	1 Identity	요청타입|승인번호|금액|통화|할부|가맹점 정보를 포함
0x02 Response	1 Identity	요청타입|승인번호|금액|통화|할부|가맹점 정보를 포함
0x03 Success		요청타입|승인번호|금액|통화|할부|가맹점 정보를 포함
0x04 Failure		요청타입|실패사유코드|실패사유 정보를 포함

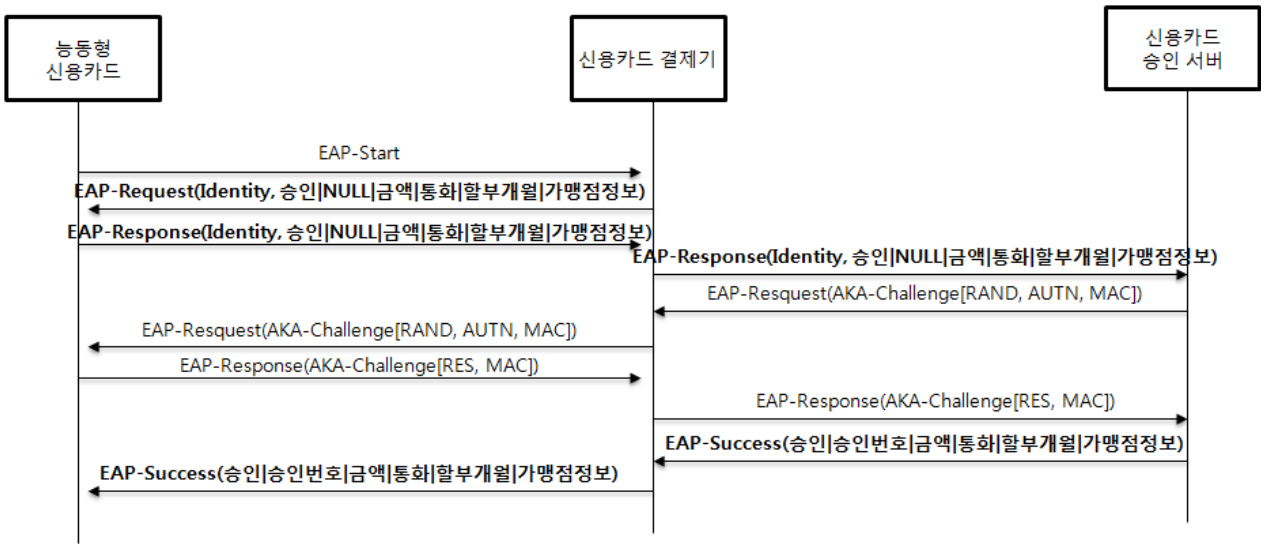

그림 6. EAP-AKA 기반의 정상 신용카드 승인 절차
Fig. 6. Credit approval processes of active authentication based on EAP-AKA

용이 가능하나, 본 논문에서는 NFC 신용카드가 설치되어 있는 스마트기기의 대다수가 WCDMA 혹은 LTE 등의 통신망 접속을 위하여 USIM 카드를 가지고 있으므로, 해당 USIM을 활용하여 구축이 가능한 EAP-AKA를 이용하는 절차를 보여준다. EAP-AKA는 공유비밀키를 기반으로 서버와 단말을 상호 인증하여 NFC 능동형 신용카드는 USIM카드의 신분과 공유 비밀키 값을 사용할 수 있으며, 이미 통신 네트워크에서 검증된 안전한 인증 방식으로 다양한 인증 응용에 적합한 방법이다. EAP-AKA 이외에도 USIM에 애플릿 추가 설치하여 EAP-TLS나 EAP-TTLS 등의 인증 방식을 활용할 수 있으며, EAP-AKA 인증방식을 사용한다 하더라도 서로 다른 신분 정보 및 공유비밀키를 활용할 수도 있다.

사용자는 신용카드 결제를 위하여 NFC 능동형 신용카드가 설치된 NFC 스마트기기를 NFC 판매시점정보관리 장치로 접근시킨다. NFC 판매시점정보관리 장치와 NFC 스마트기기간 무선 채널이 생성되면 NFC 능동형 신용카드는 NFC 판매시점정보관리 장치에 EAP-Start 메시지를 전달하여 신용카드 승인 절차의 시작을 요청한다. 신용카드 결제기는 해당 메시지를 받아 확장된 EAP-Request(Identity) 메시지에 신용 승인에 필요한 처리 유형(승인요청), 승인번호(승인 요청이므로 NULL), 금액, 통화, 할부 개월, 가맹점 정보를 포함하여 NFC 능동형 신용카드에 전달한다. 해당 메시지를 받은 NFC 능동형 신용카드는 신용 승인 절차의 처리 이전에 승인 요청 정보를 사용자에게 NFC 신용카드가 설치된 NFC 스마트기기의 화면에 표시하여 사용자에게 신용카드 결제기에서 요청한 금액에 대한 결제의 동의를 요청하는 의미로 결제비밀번호(신용카드 비밀번호와는 다른)의 입력을 요청한다. 결제비밀번호는 NFC 스마트기기에서 NFC 능동형 신용카드와 자체 확인을 수행하고, 해당 결과에 따라 NFC 스마트기기는 EAP-Response(Identity) 메시지에 결제 금액, 통화, 할부개월, 가맹점 정보 등 수신 받은 결제 요청 정보를 포함시켜 NFC 판매시점정보관리 장치에 보낸다. 이 시점에서의 신분 정보 및 결제 요청 정보는 아직 비보안 무선 채널로 연동되어 외부에서 도청이 가능할 수 있으나, 신분 정보 및 결제 요청 정보만으로는 재생 공격 등이 불가능하다. 그러나 이러한 신분 정보의 노출 문제를 해소하기 위하여 EAP-AKA에는 가명(pseudonym) 기법을 제공하고 있으므로, 필요시 해당 기법을 적용할 수도 있다. 확장된 EAP-Response(Identity)를 수신한 NFC 판매시점정보관리 장치는 EAP-Response 메시지를 RADIUS나 Diameter를 통하여 신용카드 승인 서버로 전달한다. EAP-Response(Identity)를 받은 신용카드 승인 서버는 수신한 신분 정보의 유효성을 검증하고, 유효한 신분 정보인 경우 공유비밀키를 이용하여 AKA 알고리즘을 수행하여 RAND(난수)와 AUTN(네트워크 인증 토큰)을 생성한다. 신용카드 승인 서버는 무결성 검증을 위한 MAC(메시지 인증 코드)를 포함한 EAP-Request(AKA-Challenge[RAND, AUTN, MAC])의 시도(challenge) 메시지

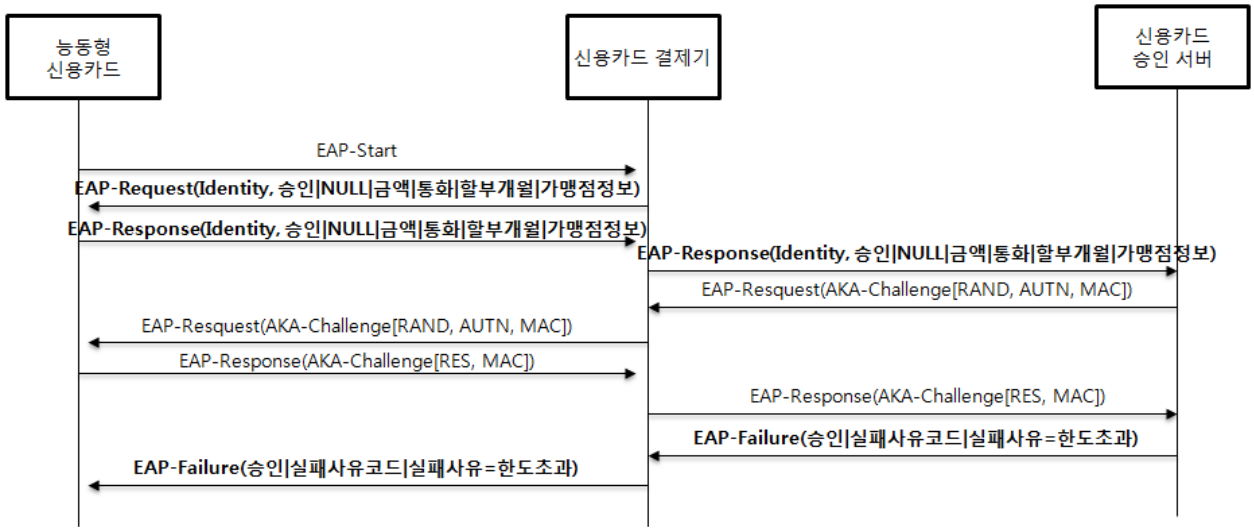

그림 7. EAP-AKA 기반의 신용카드 승인 절차의 실패 예제 - 한도 초과
Fig 7. Credit approval processes of active authentication based on EAP-AKA when approval is rejected by the server due to excess of credit limit

를 NFC 판매시점정보관리 장치에 전송한다. EAP-Request(AKA-Challenge[RAND, AUTN, MAC]) 메시지를 수신한 NFC 판매시점정보관리 장치는 수신 메시지를 NFC 능동형 신용카드로 전달하며, 해당 메시지를 수신한 NFC 능동형 신용카드는 공유 비밀키를 이용하여 AKA 알고리즘을 수행하여 AUTN을 검증하여 합법적인 신용카드 승인 서버인지 검증하고, MAC 검증을 통하여 위/변조 되지 않은 정상 메시지인지 검증한다. NFC 능동형 신용카드에서 서버 인증이 완료되면 AKA 알고리즘에 의해 서버에서 보낸 시도에 대한 응답으로 RES을 생성하고 무결성 검증을 위한 MAC을 포함하여 EAP-Response(AKA-Challenge[RES, MAC])의 메시지를 NFC 판매시점정보관리 장치에 전송한다. NFC 판매시점정보관리 장치는 수신한 EAP-Response (AKA-Challenge[RES, MAC])를 신용카드 승인 서버로 전달하며, 신용카드 승인 서버는 수신한 EAP-Response(AKA-Challenge[RES, MAC]) 메시지의 RES를 확인하여 NFC 능동형 신용카드가 정상적인 공유 비밀키를 가지고 있는지 검증하고, MAC을 검증하여 위변조 되지 않은 메시지인지 검증한다. NFC 능동형 신용카드의 인증에 성공한다면 신용카드 승인 서버는 신용카드 결제를 위한 권한 검증을 수행하고, 해당 결과에 따라 실제 승인 처리를 수행하여 승인 번호를 발행하고, EAP-Success 메시지에 승인 번호, 금액, 통화, 할부 개월 등의 정보를 추가하여 NFC 판매시점정보관리 장치에 전송한다. EAP-Success 메시지를 수신한 NFC 판매시점정보관리 장치는 EAP-Success 메시지로 정상 승인되었음을 판단하게 되고, 해당 메시지를 다시 NFC 능동형 신용카드로 전달하며. NFC 능동형 신용카드는 해당 메시지를 받아 정상 승인되었음을 판단하게 되고, 승인 번호를 파악할 수 있게 된다.

그림 7은 신용카드 승인 절차에 있어 한도 초과의 사유로 인증에 실패하는 절차를 보여준다. 신용카드 한도 초과등에 대한 검증은 기본적으로 개인정보에 포함되므로 인증이 완료 된 이후에 권한 검증 절차에서 수행되어야 한다. 그러므로 모든 절차는 그림 6과 동일하나, NFC 능동형 신용카드에서 생성한 EAP-Response(AKA-Challenge[RES, MAC])를 받은 이후 신용카드 승인 서버가 NFC 능동형 신용카드에 대한 인증을 완료하면, 신용 한도액 등의 권한 검증을 수행하며, 권한 검증에서 한도 초과 등의 이슈가 발생되는 경우 EAP-Success가 아닌 EAP-Failure 메시지를 생성하여 권한 검증 실패 및 사유 등을 NFC 판매시점정보관리 장치로 전달한다. 그러므로 NFC 판매시점정보관리 장치는 EAP-Failure 메시지를 받아 승인 실패를 파악하게 되고, 다른 방법의 결제를 사용자에게 요청할 수 있게 된다.

그림 8은 신용카드 승인 취소의 흐름도를 나타낸다. EAP-Request 메시지를 통하여 결제기는 해당 신용카드의 승인 번호를 기반으로 NFC 능동형 신용카드에 승인 취소 요청을 보내면, NFC 능동형 신용카드는 승인번호와 승인 취소 메시지 타입을 통하여 신용카드 승인 서버에 승인 취소를 요청한다. 신용카드 승인 서버에서는 승인 취소를 요청할

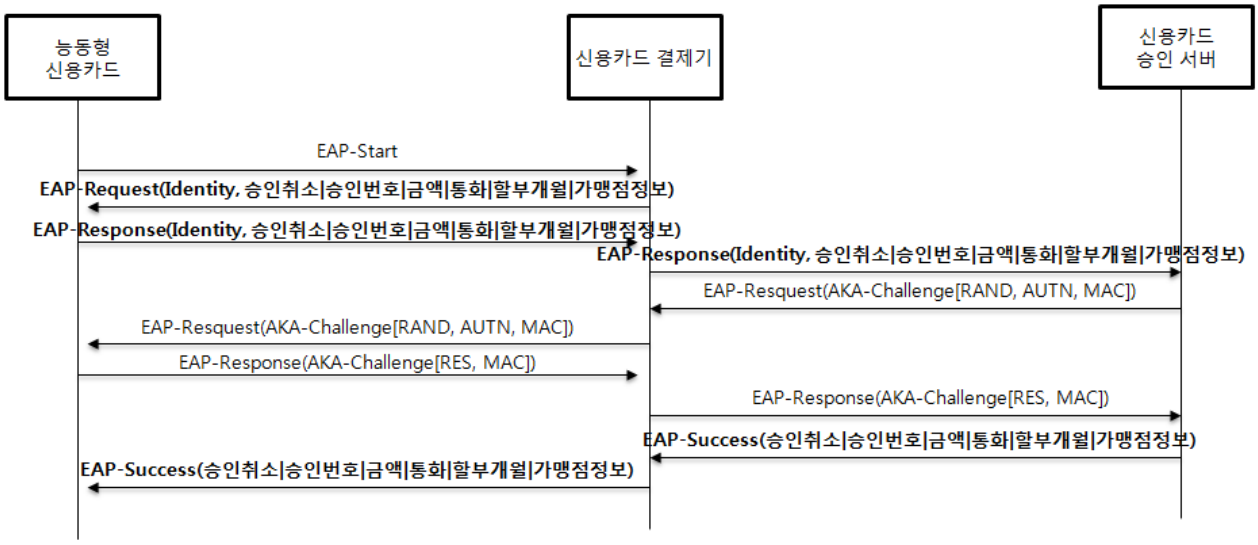

그림 8. EAP-AKA 기반의 신용카드 승인 취소 절차
Fig. 8. Cancelation process of credit approval based on EAP-AKA

수 있는 카드의 소유 여부를 파악하기 위한 인증 절차를 승인과 마찬가지로 수행하고, 인증이 완료되면 해당 승인 요청에 대한 취소 처리를 수행하고, NFC 판매시점정보관리 장치에 EAP-Success 메시지로 성공을 알려준다. 물론 승인 취소 처리에 대한 실패사유 발생시 EAP-Failure 메시지를 통하여 신용카드 결제기에 통보할 수 있다.

그림 9는 신용카드 승인 처리 중 NFC 능동형 신용카드가 제공한 신분 정보를 신용카드 승인 서버에서 검증 실패하는 경우의 흐름도를 나타낸다. 신용카드 승인 서버는 자신에게 등록되지 않은 신분 정보에 대한 승인 요청이 들어오면 즉시 EAP-Failure 메시지를 발행시켜 신용카드 승인이 불가능함을 통보한다. 반대로 그림 10은 신용카드 승인 서버의 인증에 실패하여 추가 정보 제공을 거부하는 절차를 나타낸다. 앞서 논의한대로 NFC 판매시점정보관리 장치 등의 해킹을 통한 중간자 공격에 대비하기 위하여 반드시 서버 인증이 필요하며, EAP-AKA는 공유비밀키를 활용하여 서버 인증을 수행한다.. NFC 능동형 신용카드는 신용카드 승인 서버에서 보내온 EAP-Request(AKA-Challenge[RAND, AUTN, MAC]) 메시지를 검증하는 도중 메시지의 AUTN 값에 오류가 있거나, MAC이 변경되어 메시지 무결성 등이 만족되지 않는 경우 신용카드 승인 서버의 검증에 실패하게 되고, 신뢰할 수 없는 서버로의 정보 제공을 차단하기 위하여 EAP-Response 메시지에AKA-Authentication-Reject를 담아 NFC 판매시점정보관리 장치로 전송한다.

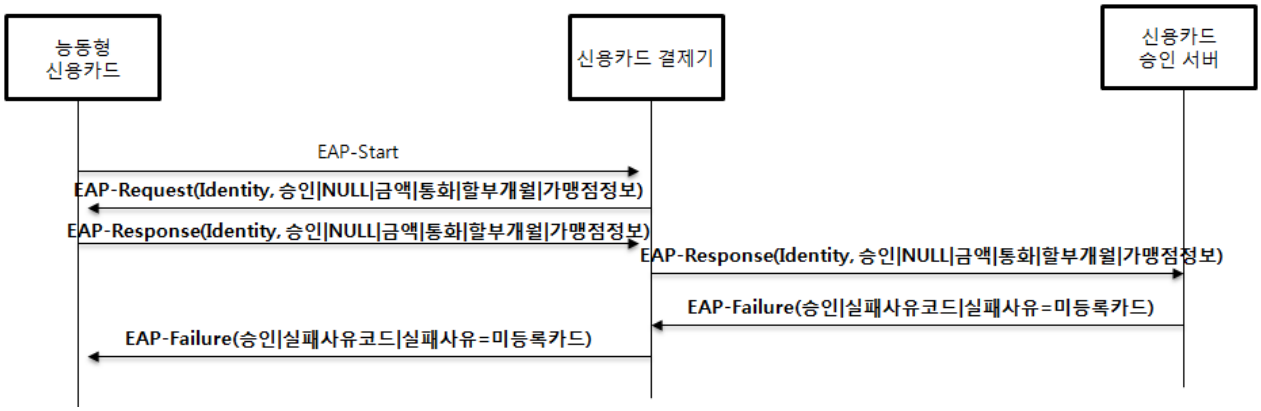

그림 9. EAP-AKA 기반 신용카드 승인 처리 실패 - 미등록 신분 정보
Fig. 9. Authentication failure case of credit approval by authentication server due to un-registered identity based on EAP-AKAv

승인 처리 중 NFC 능동형 신용카드에서 신용카드 해당 메시지를 받은 NFC 판매시점정보관리 장치는

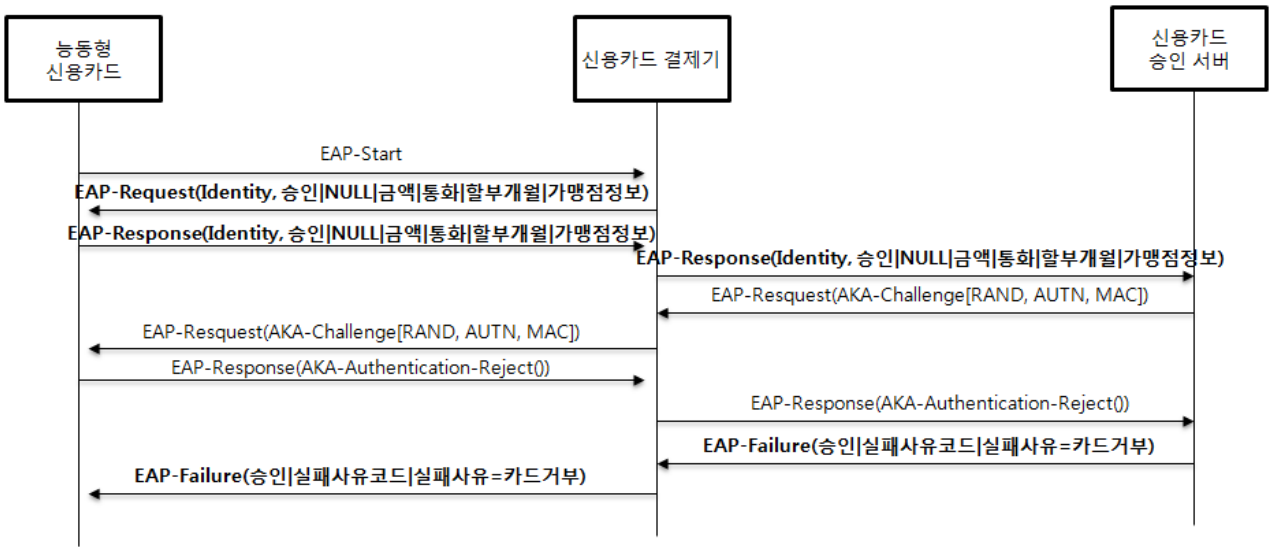

그림 10. EAP-AKA 기반 신용카드 승인 처리 중 NFC 신용카드에서 신용카드 승인 서버의 인증 거부 흐름도
Fig. 10. Reject processes of credit apporval when server authentication was failed at the NFC credit card

신용카드 승인 서버로 전달하게 되고, 승인 서버에서는 EAP-Failure 메시지를 전달하여 신용카드 결제기가 인증에 실패했음을 파악하게 한다. 그러므로 EAP-AKA 인증 방식을 활용한 신용카드 승인 처리는 MAC을 통하여 중간자 공격의 메시지 변조를 차단할 수 있으며, NFC 판매시점정보관리 장치는 인증에 필요한 공유 비밀키와 관련된 어떤 정보도 확보할 수 없어도 EAP-Success와 EAP-Failure만으로 처리 결과를 파악할 수 있게 하여 높은 보안성을 유지할 수 있다.

3.4. 안전한 NFC 인증 방법 - NFC 능동형 스마트 키

3절에서는 NFC 기반의 능동형 신용카드에 적용 방법을 살펴보았다. 그러나 신용카드의 예에서는 1절에서 살펴본 안전한 인증 지원을 위한 요구 사항의 ⑤인 세션 기반의 인증 제어 항목이 불필요한 응용이다. 즉, 신용카드 승인 절차 및 그와 유사한 출입 통제등의 응용 분야는 세션을 지속 유지하면서 서비스를 제공하는 형태가 아닌, 결제가 필요한 시점에만 인증을 수행하는 응용이다. 그러므로 이번 절에서는 세션 유지가 필요한 임대 사업에 NFC 능동형 인증 방법을 적용하여 세션 관리의 적용 방법을 살펴보자. 차량 임대 사업의 새로운 모델인 시간제 렌터카란 이용시간 기반의 임대 비용과 유류비를 포함한 제반 비용을 주행 거리에 따라 부과하는 형태로 기존 렌터카의 일 단위 임대의 고비용 부담을 해소하고 차량 보험 및 유류비 정산 등의 복잡한 절차를 생략하여 이용자가 보다 편리하게 서비스를 이용할 수 있게 하는 사업 모델[18]이다. 차량 임대의 특성에 따라, 차량을 임대하여 사용하기 시작하면 사용을 종료할 때까지 차량 이용 기간 동안의 세션이 유지되어야 하며, 해당 세션에 대한 차량 이용 정보가 AAA 규약을 기반으로 중앙 서버로 전달되어야 한다. 이러한 세션이 유지되는 동안 예약 시간 초과나, 차량의 도난 등의 이벤트가 발생될 수 있으며, 이러한 이벤트에 대한 대응을 위해 세션 기반 처리가 가능해야 한다.

NFC 능동형 스마트키는 시간제 차량 임대 사업을 제공하기 위하여 필수적인 기능으로, 사용자는 자신의 스마트기기를 활용하여 필요한 위치에 주차되어 있는 임대 가능 차량을 검색하여 예약하게 된다. 사용자가 예약 절차를 마치게 되면 차량 임대 사업자는 차량에 대한 총괄적 제어를 수행하는 차량 이용 승인/제어 시스템에 해당 사용자가 차량 이용 예약 정보를 관리하게 된다. 차량에는 차량 이용 승인/제어 시스템에서 제어를 받아 실제 차량을 제어하는 차량 제어 유닛이 설치되어 있으며, 사용자가 예약한 차량으로 접근하여 차량의 문을 열고자 하면 사용자의 NFC 스마트기기를 스마트키로 동작시켜, 차량에 설치된 차량 제어 유닛에 자신이 적합한 차량 이용자임을 확인할 수 있도록 하여, 차량 제어 유닛에서 차량의 문 개폐 및 시동 제어를 수행하도록 한다. 또한 차량 제어 유닛은 차량의 이용 정보(주행 거리, 주행 시간 등)를 차량 이용 승인/제어 시스템에 전달하여 차량에 대한 이용 금액 정산

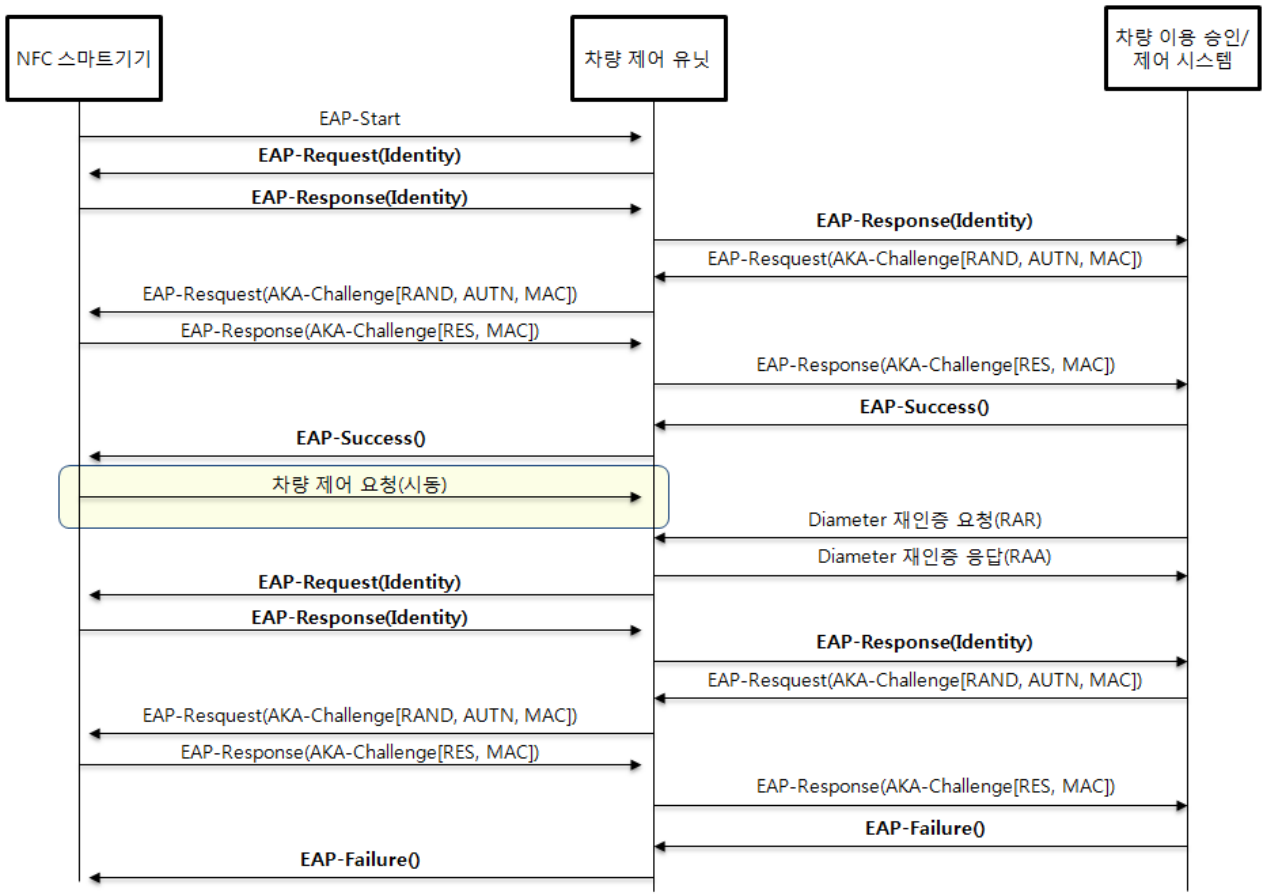

그림 11. EAP-AKA 기반 세션 제어가 가능한 차량 임대 사업의 인증 흐름도
Fig. 11. Authentication processes of Car sharing business using EAP-AKA

등이 가능하도록 해야 한다.

그림 11은 차량 임대 사업을 위한 NFC 능동형 스마트키의 인증 절차를 나타낸다. 사용자가 차량에 접근하면 NFC 능동형 스마트키는 EAP-Start 메시지를 차량 제어 유닛에 전송하여 인증 절차의 시작을 요청하며, 차량 제어 유닛은 중앙의 승인/제어 시스템과의 연동을 통하여 일반적인 EAP-AKA 인증 규약에 따라 인증을 수행한다. 신용카드 승인과 달리 NFC 능동형 스마트키는 별도의 EAP 메시지 확장 등이 불필요하며, 인증 및 권한 제어가 완료되면 바로 서비스 이용이 가능하게 된다. 도 11의 EAP-AKA 인증 결과에 따라 차량 제어 유닛은 EAP-Success 혹은 EAP-Failure의 메시지를 받게 되고, 해당 메시지에 따라 차량 이용을 허가 혹은 차단할 수 있다. EAP-AKA 인증 방식은 인증 절차 도중 무선 구간의 보안 확보를 위한 세션 단위의 공유 비밀키의 생성이 가능하므로 EAP-Success 메시지 이후 NFC 스마트기기와 차량 제어 유닛간에는 보안 채널 확보가 가능할 수 있으며, 이 보안 채널을 통하여 스마트기기와 차량 제어 유닛간 통신이 안전하게 지원이 가능하다.

차량을 이용하는 동안 세션은 지속 유지되며, 특정 이벤트가 승인/제어 시스템에서 발생하는 경우 승인/제어시스템은 차량 제어 유닛에 재인증을 요청할 수 있다. 재인증은 이용시간 만료, NFC 스마트기기 분실 등의 사유가 발생하여 차량 제어유닛이 새로운 정책을 받아들일 필요가 있을 때 수행된다. 렌터카에 새로운 정책 적용이 필요한 경우 승인/제어시스템은 차량 제어 유닛으로 RAR(Re-Authentication Request)의 Diameter 메시지를 보내면, 차량 제어 유닛은 RAA(Re-Authentication Answer)의 Diameter로 응답을 보낸 후, NFC 능동형 스마트키에 재인증을 요청하는 EAP-Request(Identity) 메시지를 보낸다. EAP-Request(Identity) 메시지를 받은 NFC 능동형 스마트키는 정상적인 AKA 인증 절차를 수행하게 되며, 승인/제어 시스템에서 인증 완료 후 권한 검증을 다시 수행하게 된다. 이 경우 만약 새로 인증한 NFC 능동형 스마트키에 분실 신고가 접

수된 경우 추가적인 차량의 이용이 불가능하도록 EAP-Failure 메시지를 차량 제어 유닛에 전송하게 된다. 차량 제어 유닛은 수신한 EAP-Failure 메시지를 기반으로 차량의 제어 정책을 변경하여 분실된 NFC 능동형 스마트키 사용에 따른 차량 이용 제한을 수행하게 된다.

Ⅳ. 결 론

NFC의 응용 분야가 넓게 확장됨에 따라 많은 수의 스마트기기들이 NFC를 채택하고 있으며 지속 확장되면서 NFC 스마트기기 하나를 소유하면 결제, 인증, 차량 이용 등 많은 부분의 서비스를 이용할 수 있을 것으로 기대되고 있다. 이러한 기대에 부응하기 위해서는 응용 시스템의 개발뿐만 아니라, 서비스의 제공여부를 판단하기 위한 NFC 기반 안전한 인증 절차가 필요하다. 각 응용에 따라 인증의 보안 요구사항에 차이가 발생할 수 있지만, 본 논문에서는 NFC를 기반으로 한 안전한 인증 방식을 제공하기 위하여 필요한 다양한 요구사항을 분석하였으며, 해당 요구사항을 만족시키기 위한 NFC의 능동 모드 동작을 활용한 능동형 인증 방법을 제시하였다. 제시한 인증 방법은 현재 다양한 유무선 접속망에서 사용되고 있는 네트워크 접속 및 인증 체계를 활용하여, 이미 많은 서비스에서 그 안전성이 입증된 인증 절차를 활용할 수 있음을 보였다. 본 논문에서 예로 든 EAP-AKA는 WCDMA 기반 스마트기기의 인증에 사용하고 있는 방법으로 그 안전성은 충분히 입증되었고, 이미 대다수의 단말에 이미 배포되어 있는 기능이므로 실제 응용 시스템의 구축이 쉽게 가능할 수 있음을 보였다. 또한 EAP 인증 절차를 활용하면 분산된 다수의 인증자는 보안의 추가 확보를 위한 새로운 새로운 인증 방식의 도입에도 별다른 수정 없이 지원이 가능함을 보였으며, 각 응용에 따른 보안 요구사항에 따라 신용카드 승인 절차에는 EAP-TLS를 활용하고, 시간제 차량 임대사업에는 EAP-AKA를 활용하는 등 다양한 형태로 확장이 가능함을 보였다.

본 연구 결과를 통하여 NFC 기반 안전한 능동형 인증 방법을 제시하였으나, 아직 추가적으로 연구를 수행해야 할 부분이 남아 있다. 우선 신용카드 결제 응용에서 PIN 관련 내용은 단말에 저장되어 있다고 가정하고, PIN을 단말에 입력하는 형태로 규약을 설계하였으나, PIN 번호는 매우 중요한 번호로 단말에 저장시키는 것 보다 중앙 서버에 저장되어 있는 것이 적합하다. 그러므로 신용카드 인증에 있어 PIN 번호를 중앙 서버를 통해 인증 받을 수 있는 EAP 규약의 확장이 필요하다. 그러나 PIN을 중앙 서버에서 인증받기 위하여 추가적인 인증 메시지의 수를 증가시키지 않는 방법을 찾아야 한다. 또한 본 논문에서 이용한 EAP-AKA 등의 방식을 사용하지 않는 경우에 신용카드 결제 응용에 필요한 인증의 주요 정보인 신분 정보와 공유 비밀키, 인증서 등의 정보를 OTA(Over-The-Air) 형태로 안전하게 배포하는 방법이 필요하다. 만약 하나의 신분 정보로 모든 응용에 공통으로 사용한다면 USIM 카드 내의 신분 정보를 활용하는 것으로 해소될 수 있으나, 다수의 신용카드를 하나의 능동형 NFC 신용카드로 제공하는 등 복수의 신분 정보를 요구하는 응용을 위해서는 별도의 신분 정보 및 자격 정보의 배포 절차의 확보가 필요하며, EAP-TLS 등 다른 인증 규약을 사용하는 경우 인증에 필요한 정보의 안전한 배포 절차가 반드시 요구된다.

참 고 문 헌

[1] NFC Forum, "What is NFC?", http://www.nfc-forum.org/aboutnfc/

[2] Zigbee Alliance, "Understanding ZigBee", http://www.zigbee.org/About/UnderstandingZigBee.aspx

[3] Bluetooth Special Interest Group, "Bluetooth Basics", http://www.bluetooth.com/Pages/Basics.aspx

[4] 이유지, "KT텔레캅, NFC 적용한 출입통제시스템 개발", 디지털 데일리, 2011년 5월 24일, http://www.kttelecop.co.kr/jsp/board/board.jsp?sa=ci&bid=8&pg=2&no=5181

[5] Darren Murphy, "Charge Anywhere update turns Nexus S into full-on mobile payment terminal", Engadget, 2011년 3월 25일, http://www.engadget.com/2011/03/25/charge-anywhere-update-turns-nexus-s-into-full-on-mobile-payment/

[6] ISO/IEC 14443, Identification cards-Contractless integrated circuit cards-Proximity cards, ISO, Geneva, Switzerland, 2008

[7] Ernst Haselsteiner and Klemens Breitfuß, "Security in near field communication (NFC)," Philips Semiconductors Workshop on RFID Security(RFIDSec 06), July 2006

[8] ECMA International, "NFC-SEC NFCIP-1 Security Services and Protocol, Cryptography Standard using ECDH and AES", Ecma/TC47/2008/089, http://www.ecma-international.org/activities/Communications/tc47-2008-089.pdf

[9] Joan Daemen and Vincent Rijmen, "The Design of Rijndael: AES-The Advanced Encryption Standard." Springer, 2002. ISBN 3-540-42580-2

[10] Pablo Holman, "How to hack RFID-enabled Credit Cards for $8", BoingBoingTV, http://www.youtube.com/watch?v=vmajlKJlT3U

[11] NXP Semiconductor, MIFARE Classic - a pioneer and front runner in contactless smart card ICs, http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/mifare_classic/

[12] Gerhard P. Hancke, "A practical relay attack on ISO/IEC 14443 proximity cards", Project Report, 2005년 1월

[13] Dan Balaban, "Tansport for London to Discard Mifare classic", NFC times, Jan. 21, 2010, http://www.nfctimes.com/news/transport-london-discard-mifare-classic-seeks-desfire-sims

[14] 길민권, "해킹 시연 'RFID 적용 탄약고 · 물류센터 등 해킹에 무방비'," 보안뉴스, 2007년 5월 22일, http://www.boannews.com/media/view.asp?idx=6226&kind=2

[15] T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels, and T. O'Hare. "Vulnerabilities in first-generation RFID-enabled credit cards". In Proceedings of Eleventh International Conference on Financial Cryptography and Data Security, Lecture Notes in Computer Science, Vol. 4886, pages 2--14, Lowlands, Scarborough, Trinidad/Tobago, Feb. 2007.

[16] Thomas Ricker, "Duch RFID e-passport cracked-US next?" Engadget, 2006년 2월 23일, http://www.engadget.com/2006/02/03/dutch-rfide-passport-cracked-us-next/

[17] 양진비, "전자여권, 10분이면 감쪽같이 '해킹'", 프레시안, 2008년 9월 29일, http://www.pressian.com/article/article.asp?articlenum=60080929141547&Section=

[18] Hsu-Chen Cheng, Wen-Wei Liao, Tian-Yow Chi and Siao-Yun Wei, "A secure and practical key management mechanism for NFC read-write mode", The 13th International Conference on Advanced Communication Technology(ICACT), Feb. 13-16, 2011, Seoul, Korea, 2011

[19] Sandeep Tamrakar, Jan-Erik Ekberg and N. Asokan, "Identity Verification Schemes for Public Transport Ticketing with NFC Pohones", Proceedings of the sixth ACM workshop on Scalable trusted computing, OCT. 17-21, Chicago, USA, 2011

[20] Wei-Dar Chen, Mayes, K.E, Yuan-Hung Lien and Jung-Hui Chiu, "NFC Mobile Payment with Citizen Digital Certificate", The 2nd International Conference on Next Generation Information Technology (ICNIT), Jun. 21-23, Gyeongju, Korea, 2011

[21] Wei-Dar Chen, Mayes, K.E, Yuan-Hung Lien and Jung-Hui Chiu, "NFC Mobile Transactions and Authentication based on GSM Network", The 2nd International Workshop on Near Field Communication, Apr. 20-20, Monaco, 2010

[22] Wei-Dar Chen, Mayes, K.E, Yuan-Hung Lien and Jung-Hui Chiu, "Using 3G Network Components to Enable NFC Mobile Transactions and Authentication", 2010 IEEE International Conference on Progress Informatics and Computing (PIC), Dec. 10-12, Sanghai, China, 2010

[23] 이민구, 김동완, 손진수, "시간제 차량 임대 사업과 NFC 활용", R&D Horizon, Vol. 25, No. 2, Jun. 2011

[24] Nakhjiri and Nakhjiri, AAA and Network Security for Mobile Access, Wiley, 2005

[25] Carl Rigney, Allan C. Rubens, William Allen Simpson and Steve Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, http://ietf.org/rfc/rfc2865.txt

[26] Pat R. Calhoun, John Loughney, Jari Arkko, Erik Guttman and Glen Zorn, "Diameter Base Protocol", RFC 3588,

http://ietf.org/rfc/rfc3588.txt
[27] Brian Lloyd and William Allen Simpson, "PPP Authentication Protocols", RFC 1334, http://ietf.org/rfc/rfc1334.txt
[28] Bernard Aboba, Larry J. Blunk, John R. Vollbrecht, James Carlon and Henrik Levkowetz, "Extensible Authentication Protocol(EAP)", RFC 3748, http://ietf.org/rfc/rfc3748.txt
[29] Jari Arkko and Henry Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, http://ietf.org/rfc/rfc4187.txt
[30] Bernard Aboba and Dan Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, http://ietf.org/rfc/rfc2716.txt
[31] Paul Funk and Simon Blake-Wilson, "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)", RFC 5281, http://ietf.org/rfc/rfc5281.txt
[32] Florent Bersani and Hannes Tschofenig, "The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method", RFC 4764, http://ietf.org/rfc/rfc4764.txt

이 민 구 (Min-Gu Lee) 정회원

2000년 2월 한양대학교 전자,전자통신,전파 공학과 졸업
2002년 2월 포항공과대학교 전자전기공학과 석사
2007년 2월 포항공과대학교 전자컴퓨터공학과 박사
2007년 1월~현재 KT 종합기술원 연구원
<관심분야> 유무선 네트워크, 인증, 보안, NFC, 분산처리, 병렬처리 등

김 동 완 (Dong-Wan Kim) 정회원

1991년 2월 홍익대학교 전산학과 졸업
2003년 2월 홍익대학교 전산학과 석사
1993년 3월~현재 KT 종합기술원 연구원
<관심분야> 유무선 결합서비스, 인증, NFC 등

손 진 수 (Jin-Soo Sohn) 정회원

1982년 2월 성균관대학교 전자공학과 졸업
1983년~1985년 전자통신연구원 연구원
1984년 2월 성균관대학교 전자공학과(석사)
1985년~현재 KT 종합기술원 상무
<관심분야> 유무선 네트워크, 네트워크 응용서비스, 스마트그린서비스 등