Theme Article

시간제 차량 임대 사업과 NFC 활용

기술개발실 기술지원담당
이민구, 김동완, 손진수

1. 시간제 차량 임대 사업 현황

지난 2000년 미국 Boston에서 최초로 도로 주행을 시작한 Zipcar[1]는 2011년 4월 14일에 NASDAQ에 상장하여 상장 첫날의 주가가 공모가인 18USD에서 28USD로 56%이상 급등하는 대성공을 이루었다[2]. Zipcar는 적자를 면하지 못하던 사업자(2010년도 결산기준 14,100천USD 순손실)임에도 불구하고 주식 시장에서 성공적인 상장이 가능했던 이유는 투자자들이 시간제 차량 임대 사업의 미래를 매우 우호적으로 보았기 때문이다. 현재 Zipcar 이외에도 스코틀랜드의 CityCarClub, 호주의 GoGet, 독일의 Car2Go 등 세계적으로 많은 회사들이 시간제 차량 임대사업에 진출하고 있으며, 국내에서는 녹색희망 카쉐어링과 정부 차원의 전기차 쉐어링[3] 등이 추진되고 있다. 이러한 시간제 차량 임대 서비스는 이용 시간 기반의 렌트 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 있다. 따라서 렌터카 단기 이용 희망자들의 시간제 차량 임대에 대한 수요가 지속적으로 증가할 것으로 예측하고 있다. KT는 고유의 통신인프라와 더불어 최근에 인수한 렌터카와 신용카드사 및 단말제조사와의 제휴시 시간제 차량 임대 사업에 필요한 인프라 구축에 유리한 위치를 점할 수 있다. 따라서 이러한 산업간 인프라의 컨버전스 극대화를 위한 시간제 차량 임대사업의 진입을 적극적으로 고려할 필요가 있다.

시간제 차량 임대 사업을 보다 상세히 파악하기 위하여 가장 대표적인 사업자인 Zipcar의 사례를 살펴보자. Zipcar이용을 위해서는 먼저 서비스를 가입하고(초기 가입비 25USD와 연회비 50USD) 신용카드 정보 등의 서비스 이용료에 대한 결제 정보를 등록하여야 한다. 가입이 완료되면 Zipcar는 차량

[그림 1] Zipcard와 Reader

임대시 사용할 RFID가 장착된 zipcard를 사용자에게 발급한다. 사용자는 필요에 따라 사전에 차량을 예약하고, 해당 시각에 차량이 주차된 곳으로 찾아가 그림 1처럼 자신의 zipcard를 차량 앞유리에 장착된 RFID 리더기에 접근시킨다. 리더기는 카드 정보를 판독하여 차량에 설치된 "블랙박스(Black Box)"로 전달하고, 블랙박스는 중앙 서버로부터 무선 네트워크를 통하여 수신한 차량 예약 정보를 이용하여 차량 이용 허가 절차를 수행한다. 차량 이용 허가가 완료되면 차량의 문이 열리게 되며, 사용자는 예약한 시간까지 차량을 이용할 수 있게 되고, 이용 시간 만료시 차량을 반환지점에 반환하면, online을 통한 자동 정산이 이루어 진다. 차량 이용 중 주유는 차량 내부에 있는 gas card를 통하여 결제하며, 주유 금액 결제 시 사용자의 zipcard 멤버십 번호를 입력하도록 한다.

2. 시간제 차량 임대 사업을 위한 기술적 이슈

시간제 차량 임대사업을 위해서는 차량 제어 기능, 정산 기능 및 차량 관리 기능이 필수적으로 요구 되며, 고객의 편의성 제고를 위한 스마트폰 연계 기능 등이 필요할 수 있다. 차량 제어 기능은 기본적으로 ① 현재 사용자가 이용하고자 하는 차량이 사용자 본인에게 예약된 올바른 차량인가? ② 현재 차량의 이용 시각이 사용자에게 허용된 시간에 포함되는가? ③ 현재 차량을 이용하고자 하는 사람이 적합한 사람인가? 등의 질문을 통해 차량의 접근 제어를 수행하여야 하며, 해당 조건이 모두 만족되는 경우 차량의 시동장치, 잠금 장치 등을 제어하여 차량을 이용할 수 있도록 해 주는 기능을 의미한다(Authentication&Authorization). 정산 기능은 차량의 사용에 따른 비용 정산을 위한 기능으로 ①차량의 이용 시간, ②차량의 주행 거리, ③주유 금액 및 주유 용량 등의 정보를 확보하여 정산을 수행하는 서버로 전달하는 기능을 의미한다(Accounting). 마지막으로 차량 관리 기능은 ①차량의 위치, ②차량의 잔여 유류량, 속도, 주행거리 등의 실시간 상태, ③현재 차량 사용자 등에 대한 정보를 실시간으로 시스템에서 확보할 수 있도록 하여, 차량 도난, 고장 및 범죄에 이용에 대응한 적절한 조치가 가능하도록 하는 기능을 의미한다(Profile&Context). 스마트폰 연계 기능은 고객 소유의 스마트폰을 통해 주변의 이용 가능한 차량의 상태 조회 및 예약 등 기본적인 애플리케이션을 제공할 수 있다. 이러한 기능들은 적법한 사용자에 한해 네트워크 접속을

허용하고, 트래픽 사용량+ 정보를 수집하여 이용료를 부과하고, 접속 단말 및 사용자와 관련된 세션정보를 실시간으로 관리하는 네트워크 접속 제어 및 인증 체계(AAA)[4]와 유사한 속성을 내포한다.

시간제 차량임대에서 이러한 기능들은 일반적으로 중앙서버, 이용자 식별용 전자카드 및 이들과의 정보 연동을 통해 차량을 제어하는 OBU(On Board Unit)등을 통해 구현된다. 특히 OBU는 차량의 시동 장치와 잠금 장치 등을 제어하여 허가된 사용자만이 차량을 이용할 수 있도록 통제하고, 사용자가 불법적으로 차량 내부로 진입하더라도 차량의 시동장치를 제어하여 허가되지 않은 차량의 사용이 불가능하도록 한다. 또한 OBU는 차량 내부에서 생성되는 여러 정보들을 수집하여 중앙 서버로 전송한다.

일반적으로 이용자 카드와 OBU간의 사용자 식별은 RFID를 이용하고 있으나, RFID의 단방향 통신에 따른 제약으로 차량임대 사업에 활용하기에 충분한 기능을 제공하지 못하고 있다. 대표적인 사례로 차량의 OBU는 차문을 여는 시점의 사용자는 파악할 수 있으나, 주행 중의 사용자 변경은 파악이 어려운 문제가 있다. 또한 이용자 운행 중 주유시, 해당 금액의 사후 정산에 필요한 정보를 확보할 수 있어야 하지만, RFID만으로는 정산을 위한 인프라 구축이 어렵다. 더욱이 스마트폰 이외에 별도의 RFID 카드를 항상 소지하여야 하며, 스마트폰 기반의 차량임대 사업자 APP(예약, 정산 등)을 이용하는 경우 스마트폰 자체가 인증 정보를 가지고 있지 않으므로, 이용자 카드와 별도의 인증수단(ID/PW 등)을 통하여 인증을 수행해야 한다. 그러므로 RFID를 이용한 Zipcar에서는 스마트폰을 이용한 서비스를 제공한다고 하더라도 예약 및 차량 경적음 발생 등 단편적인 서비스에 불과할 수 밖에 없다.

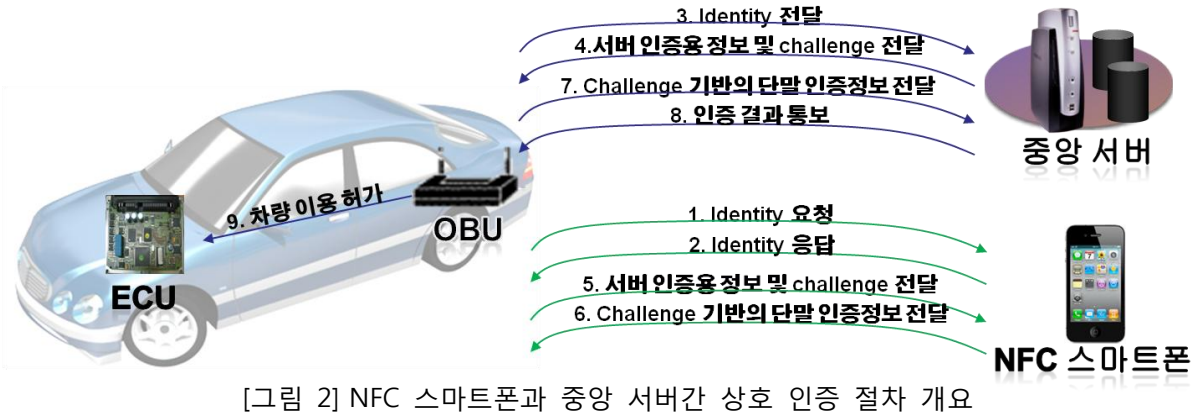
3. NFC 스마트폰을 이용한 시간제 차량 임대 사업

RFID의 단방향 통신이라는 한계를 극복한 새로운 통신 기술로 NFC가 등장하여 최근 각광받고 있다. NFC는 RFID의 기본적인 기능은 물론 양방향 통신을 제공하여 스마트폰과 RFID를 하나로 융합시킨 BM이 가능하게 한다. 즉 NFC 스마트폰으로 차량 이용자를 인증하게 되면, 차량과 스마트폰이 NFC 채널로 직접 통신하여 차량의 잠금 장치를 해제하거나, 경적음 발생 등 기본적인 제어가 가능하며, 스마트폰에서 직접 차량을 시동시키고, 정지시키는 등의 제어가 가능하다. 더욱이 수동형인 RFID와 달리 스마트폰을 활용하면 PIN번호 설정 등을 통한 추가적 보안성 확보가 가능하며, NFC의 핵심 응용 분야인 전자 지갑과의

연계가 가능하다. 그러나 NFC를 RFID와 유사하게 TAG 형태로만 활용한다면 RFID의 취약점을 답습하여 악의적 사용자에 의한 해킹 시도에 취약할 수 있다.

기본적으로 NFC는 무선 통신이므로 SSL 등 별도의 무선구간 보안을 확보하지 않는 경우 도청에 취약[5]하며, 악의적 NFC 리더장치를 활용한 relay 공격 등 다양한 공격 유형을 통한 NFC 카드 정보가 노출[6]될 수 있다. 이러한 위험이 발생되는 주요 원인은 OBU(NFC 리더 장치)가 사용자의 NFC 인증정보를 직접 읽고 중앙서버로부터 해당 가입자 정보를 제공받아 인증을 수행하기 때문이며, 이 과정에서 이용자 정보가 노출될 수 있다. 따라서 보다 안전한 임대 차량 및 가입자 관리를 위해 OBU가 직접 인증하는 것이 아니라, NFC 스마트폰과 중앙 서버간 OBU를 통한 상호 인증으로 OBU는 스마트폰의 이용자 정보를 중앙 서버로 투명하게 전달하고, 서버에서 인증 결과 정보만을 수신토록 하여야 한다.

이를 위한 NFC 스마트폰과 중앙 서버간 OBU를 통한 상호인증 절차를 그림 2에서 상세히 살펴본다. 우선 NFC 스마트폰이 차량에 근접하면 OBU와 NFC 스마트폰은 NFC 장치간 통신 채널을 설정한다. NFC 통신이 설정되면 OBU는 NFC 스마트폰에 identity를 요청하는 메시지를 전송(1)한다. NFC 스마트폰은 OBU의 요청에 자신의 identity를 응답(2)하고, OBU는 수신한 identity를 중앙 서버로 전달(3)한다. 중앙 서버는 수신한 identity가 정상적인 사용자인지 검증하고, NFC 스마트폰에서 서버를 검증하기 위한 정보와, NFC 스마트폰을 인증하는데 필요한 challenge 정보를 OBU로 응답(4)한다. OBU는 해당 정보를 NFC 스마트폰에 전달(5)하고, NFC 스마트폰은 서버 검증 정보를 기반으로 서버를 인증한다. NFC 스마트폰에서 서버 인증을 완료하면, 중앙 서버로부터 수신한 challenge와 자신의 인증키로 인증 정보를 생성하여 OBU로 송신(6)한다. OBU는 수신한 인증 정보를 중앙 서버로 전달(7)하고, 중앙 서버는 수신한 인증 정보의 적합성을 판단(Authentication)하여 적합한 경우 해당 사용자가 이용하고자 하는 차량 정보 및 예약 시간 등의 추가 검증(Authorization)하여 인증 완료를 OBU로 응답(8)한다. OBU는 중앙 서버로부터 정상적인 인증 완료 응답을 받은 경우 해당 사용자가 적절한 사용자로 판단하고 차량의 이용을 허가(9)하여 차량의 ECU에 통보한다. 더불어 OBU는 NFC 스마트폰과 무선 구간 암호화를 수행하여 보안무선

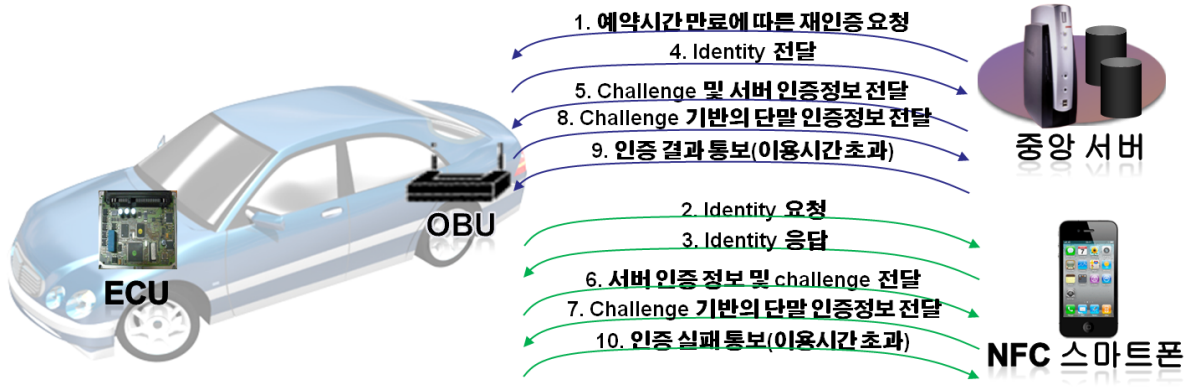


[그림 2] NFC 스마트폰과 중앙 서버간 상호 인증 절차 개요

채널을 확보하여 NFC 스마트폰에서 차량의 정보를 조회하거나 엔진 시동 및 정지 등의 제어를 수행할 수 있게 한다. 추가로 OBU에서 수신한 인증 완료 메시지에는 중앙 서버로부터 해당 사용자의 예약 시간 등의 추가 정보가 포함되어 있어 OBU는 기 인증된 사용자의 예약 시간이 완료되면 추가적인 차량 이용이 불가능하도록 차단하는 등의 역할을 수행해야 한다.

차량의 예약 시간은 이용 중 변경이 가능하므로 OBU는 인증시 받은 예약 시간이 완료되는 경우 일방적 접속 차단이 아닌 재인증을 수행하여 중앙 서버로부터 현행화된 예약 정보를 다시 요청해야 한다. 그림 3은 예약 시간이 완료되는 경우 재인증을 수행한 결과, 인증 정보는 맞더라도 예약시간이 초과하여 권한 부여에 실패하는 경우를 나타낸다. 예약시간 만료 등의 이벤트가 발생되면 중앙서버는 OBU로 재인증을 요청(1)하고, OBU는 재인증 요청에 따라 통상적인 재 인증 절차를 따른다. 재인증 절차를 통해 중앙 서버에서 NFC 스마트폰을 인증한 이후 권한 검증을 수행하며, 권한 검증 결과 이용시간 초과 사유로 차량 이용이 불가능함을 OBU에 통보(9)하면, OBU는 차량의 이용이 불가능하도록 조치하고, NFC 스마트폰에 해당 사유를 통보한다. 이러한 재 인증 절차는 이용시간 만료 이외에도, 차량의 도난 등이 발생하는 경우 서버에서 OBU를 제어하기 위한 방법으로 사용이 가능하며, 만약 차량 이용 중 재인증 절차를 수행한 결과 인증 실패인 경우 OBU는 ECU를 제어하여 차량의 정상 운행이 어렵도록 제어하여야 한다. 차량의 엔진 정지등은 사고 발생의 위험등이 있으므로, 차량의 경적음을 울리거나, 비상등 점멸, 최대속도 제한등 다양한 방법을 도입해야 한다. 또한 차량의 현재 위치등에 대한 정보도 OBU가 중앙 서버로 보내 사후 조치가 가능하도록 해야 한다.

정상적인 인증을 완료하고 사용자가 차량을 이용하는 동안 OBU는 차량의 상태 정보를 생성하여 중앙 서버로 송신(Accounting)한다. 차량 이용 정보에는 현재



[그림 3] 예약 시간 만료시 재인증 절차

위치, 주행 거리, 이동 시간, 현재 속도, 연비, 유류 소모량 등의 관리 및 정산에 필요한 정보일 수 있으며, 개인 프라이버시의 침해를 막기 위해 현재 위치 등의 정보는 필요에 따라 생략할 수 있어야 한다. 중앙 서버는 OBU에서 수신한 과금 메시지를 이용하여 주행거리, 사용 시간 등의 정산을 위한 정보를 관리하며, 차량 이용이 종료되면 사용량을 기반으로 사용자에게 청구한다. 더욱이 과금 정보는 단순 차량 이용 대금 청구 외, 차량의 이용 패턴, 분실 및 도난 차량의 위치 추적 등의 차량의 관리 기능(Profile and Context)에 사용되어 차량 이용에 대한 다양한 정보 확보가 가능할 수 있어야 한다.

지금까지 살펴본 차량 임대 서비스 제공을 위한 인프라는 일반적엔 네트워크 접속에 대한 제어를 수행하는 AAA와 유사하다. 즉, NFC 스마트폰은 네트워크 접속을 위해 중앙 서버와의 안전한 인증 방식으로 상호인증을 수행한 후 서비스를 사용하며, OBU는 Network Access Server(NAS)와 유사하게 단말과 서버간 인증을 중계하고, 서버로부터의 인증 결과에 따라 단말의 서비스 이용을 제어하는 역할을 수행하며, 중앙 서버는 접속 인증 시스템에서 수행하는 인증(Authentication), 권한제어(Authorization) 및 과금(Accounting) 처리와 유사하게 NFC 스마트폰을 인증하고, 차량 이용량에 따른 과금 정보를 생성하는 역할을 한다. 그러므로 NFC를 활용한 시간제 차량 임대사업은 네트워크 접속인증에서 사용하는 네트워크 접속 제어 및 인증 체계(AAA)에 사용하는 다양한 기술을 활용할 수 있다. NAS와 인증서버간 통신은 RADIUS[7] 혹은 Diameter[8] 프로토콜을 사용이 가능하며, 접속 단말과 인증서버간 인증은 EAP-AKA[9], EAP-SIM[10], EAP-TLS[11] 등 상호인증 기능을 제공하는 다양한 인증

프로토콜의 사용이 가능하나 NFC 스마트폰은 USIM카드 기반 접속인증기능을 수행하므로 유사한 EAP-AKA나 EAP-SIM 인증 방식이 적합하다. 이러한 기술들은 이미 KT의 다양한 유무선 네트워크(인터넷, Wi-Fi 및 와이브로 등) 접속 인증 및 과금에 활용하고 있으며, KT에 내재화 되어 있어 큰 비용 없이 구현이 가능한 방식으로 네트워크 사업자에게 매우 유리하다.

지금까지 논의한 차량 임대사업의 인증 인프라의 구축 방안을 표 1에 간략히 정리하였다. RFID는 Zipcar와 유사하게 RFID로 인증을 수행하는 경우, NFC는 NFC를 스마트폰에 탑재하여 인증하는 경우, NFC+상호인증은 NFC의 인증 구조를 중앙 서버와 단말간 상호 인증을 제공하는 경우를 나타낸다.

[표 1] RFID, NFC 및 상호인증 기반의 NFC 인증의 비교

구분	RFID	NFC	NFC+상호인증
보안성(카드 정보 노출 가능성)	취약	보통(Relay공격에 취약)	우수(상호인증)
스마트폰 연계성	취약	우수(양방향 지원)	우수(양방향 지원)
세션키 기반 무선 보안 채널 생성	취약	취약	우수(인증시 세션키 생성)
서버에서 재인증 요청(분실 대처 등)	취약	취약	우수(재인증 요청 가능)
전자결제 연계성	취약	우수(NFC 전자지갑 연계)	우수(NFC 전자지갑 연계)

3. 결론

최근 Zipcar의 성공적인 사업 진행에 따라 시간제 차량 임대사업은 많은 관심을 받고 있다. 시간제 차량 임대 사업은 고객의 비용 편리성뿐만 아니라 친환경 차량 이용이 가능하도록 하므로 범 정부차원의 추진도 이뤄지고 있다. KT는 고유의 통신인프라에 최근 인수한 렌터카, 신용카드사 및 단말제조사와의 제휴를 통해 시간제 차량 임대 사업에 필요한 인프라 구축에 경쟁사보다 유리한 위치를 점할 수 있다. 따라서 이러한 산업간 인프라의 컨버전스 극대화를 위한 시간제 차량 임대사업의 진입을 적극적으로 고려할 필요가 있다. 본 고에서는 시간제 차량 임대사업의 추진에 있어 해결해야 할 다양한 기술적 이슈를 살펴보고, 기존 RFID를 활용한 시간제 차량 임대사업의 제약점을 살펴보았다. RFID의 단방향 통신이 가진 문제의 해결 방안으로 NFC 스마트폰을 이용한 인프라 구축 방법을 살펴보았으나 NFC의 도입만으로는 안전한 서비스 제공을 위한 보안 이슈를 모두 해결할 수 없음을 보였다. 따라서 본 고에서는 서버와 단말간 상호 인증을 사용해서 해결할 수 있는 방법을 살펴 보았으며, KT에 이미 내재화 되어 있는 네트워크 기술들을 이용하여 손쉽게 구현 가능함을 보였다.

<참 고 문 헌>

[1] http://zipcar.com

[2] 이태훈, "[Best Practice] 美 신개념 렌터카업체 `집카`", 한국경제신문, 2011년 4월

[3] 이상순, "'전기차 셰어링' 하반기 도입 등 전기차 대중화 시동", YTN, 2011년 4월

[4] Nakhjiri and Nakhjiri, "AAA and Nework Security for Mobile Access," Wiley, 2005.

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

[6] Gerhard P. Hancke, "A practical relay attack on ISO/IEC 14443 proximity cards", February 2005.

[7] RADIUS, RFC 2865, http://www.ietf.org/rfc/rfc2865.txt

[8] Diameter Base Protocol, RFC 3588, http://www.ietf.org/rfc/rfc3588.txt

[9] EAP-AKA, RFC 4187, http://www.ietf.org/rfc/rfc4187.txt

[10] EAP-SIM, RFC 4186, http://www.ietf.org/rfc/rfc4186.txt

[11] EAP-TLS, RFC 5216, http://www.ietf.org/rfc/rfc5216.txt