모바일 RFID 보안기술 표준화 동향 및 표준화 추진 전략

Standardization Trend and Strategy of Mobile RFID Security Technology

강유성 (Y.S. Kang) RFID/USN보안연구팀 선임연구원
최두호 (D.H. Choi) RFID/USN보안연구팀 팀장
김호원 (H.W. Kim) 부산대학교 조교수

목 차

* 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행되었음.[2005-S-088-04, 안전한 RFID/USN을 위한 정보보호 기술]

모바일 RFID 환경이란 휴대전화가 RFID 리더를 가지고 있어서 사용자가 자신의 휴대전화를 통해 RFID 태그가 부착된 제품의 정보를 손쉽게 얻을 수 있는 환경을 의미한다. 모바일 환경에서 사용되는 RFID 기술은 고정형 RFID 리더를 사용하는 환경과는 다른 사용자 요구사항 및 보안 요구사항이 존재한다. 모바일 RFID 기술에 특화된 국제표준화 논의가 2007년 상반기부터 본격적으로 논의되고 있다. 따라서 모바일 RFID 보안기술은 모바일 RFID 전체 프레임워크와 호환성을 유지하면서 모바일 환경의 요구사항을 만족하는 방향으로 표준화가 진행되어야 한다. 본 고에서는 모바일 RFID 기술의 표준화 동향을 살펴보고, 모바일 환경을 고려한 모바일 RFID 보안 프레임워크 및 인증, 키 관리, 데이터 보호, 프라이버시 보호 등의 모바일 RFID 보안 서비스를 설명한다. 그리고 이러한 보안 서비스를 제공하기 위해 필요한 표준화 대상을 제안하고, 표준화 대상에 대한 기술 개발과 지적재산권 확보 및 이를 연계한 국제표준화 추진 전략을 설명하며 결론을 맺는다.

I. 서론

최초 RFID 기술의 태동은 제품 식별자의 자동인식에서 시작되었으며, 기업의 물류 시스템 혁신 및 재고관리 등 B2B 서비스의 효율성과 신뢰성을 높이고자 RFID 기술을 적용시키려는 노력이 진행되어 왔다. 즉, RFID 태그가 부착된 다수의 제품에 대해 하나의 RFID 리더가 제품 식별자를 얻고자 하는 기능 중심으로 기술 발전을 추구해 왔다. 따라서 그 동안의 RFID 기술 표준화도 이러한 추세에 맞게 물리계층 규격에서는 전송량은 적더라도 비교적 간단하게 구현할 수 있는 ASK 또는 PSK와 같은 변조 방식을 채택했으며, 충돌 방지 기법에서는 태그들의 응답 충돌을 최소화하여 태그 식별자를 얻기 위한 알로하 프로토콜(ALOHA protocol) 또는 바이너리 트리 프로토콜(binary tree protocol) 등을 채택하였다[1]. 이러한 RFID 기술은 보다 짧은 시간에 이동중인 사물에 부착된 RFID 태그를 정확하고 신뢰성 있게 판독하는 것이 매우 중요한 성능 판단의 척도였다.

그러나 모바일 RFID 서비스는 위와 같은 기존의 RFID 태그 식별자 인식과는 다른 서비스 환경을 갖고 있다. 모바일 RFID 기술은 이동통신망에 RFID 기술을 접목한 것으로 사용자가 자신이 휴대한 휴대전화로 제품에 부착된 RFID 태그의 식별자를 읽고, 이 식별자를 이동통신망을 통해 네트워크로 전달하여 제품에 대한 정보를 얻거나 활용하는 기술로 정의할 수 있다[2]. 제품에 RFID 태그를 부착하고 개인 사용자에게 제품의 정보를 제공하는 것은 기업의 역할이며, 제품 구입 및 제품 정보 획득은 개인 사용자의 역할이므로 모바일 RFID 기술은 B2C 서비스를 획기적으로 향상시킬 수 있는 기술적 대안으로 주목 받고 있다.

모바일 RFID 서비스 환경에서 기능적으로 가장 중요한 것은 개인 사용자가 RFID 태그가 부착된 제품의 정보를 정확하고 신뢰성 있게 얻는 것이며, 보안 측면에서 가장 중요한 것은 제품 정보의 안전한 제공 및 개인 프라이버시 보호이다. 따라서 기술 표준화에 있어서도 다수의 사용자들이 개별 제품에 부착된 RFID 태그의 식별자를 안정적으로 읽을 수 있는 표준이 필요하며, 또한 개별 제품이 특정 사용자의 소유가 되었을 때 해당 제품에 대한 접근 제어, 데이터 보호 및 해당 사용자의 개인 프라이버시 보호 등이 보장되는 기술 표준이 제정되어야 한다.

본 고에서는 모바일 RFID 서비스 제공시 반드시 해결되어야 하는 모바일 RFID 보안 기술에 대한 국제 표준화 전략에 초점을 맞추며, 이를 위하여 다음과 같은 순서로 구성된다. 제 II장에서는 기본적인 모바일 RFID 시스템 구성을 위한 국내외의 표준화 현황을 간략하게 정리하고, 제 III장에서 모바일 RFID 서비스를 안전하게 제공하기 위한 보안 요구사항을 정리한다. 이렇게 정리된 보안 요구사항을 만족하는 향상된 모바일 RFID 보안 서비스 및 표준화 대상에 대하여 제 IV장에서 상세히 설명하며, 제 V장에서 국제 표준화 전략을 수립한다. 끝으로 제 VI장에서 모바일 RFID 보안 기술의 국제 표준화의 기대효과를 정리하며 본 고의 결론을 맺는다.

● 용 어 해 설 ●

RFID: 무선인식 또는 전파식별로 번역되며, 원격에서 신속하고 정확하게 사물의 식별을 가능하게 하는 기술

모바일 RFID: 개인의 휴대전화에 RFID 리더 기능을 추가하여 RFID 서비스를 개인별로 특화시킬 수 있는 기술

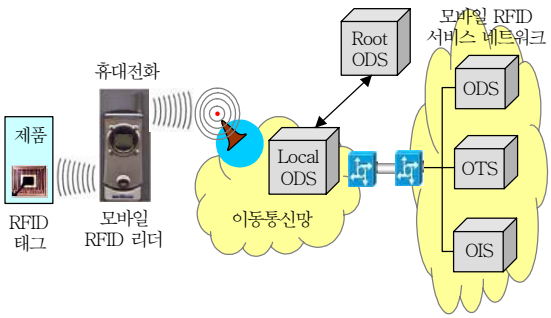
II. 모바일 RFID 기술 표준화 동향

본 고에서는 모바일 RFID 기술을 900MHz 기반의 RFID 주파수 대역을 사용하는 기술로 한정한다. 이는 NFC 포럼이 개발하는 13.56MHz 기반의 RFID 기술과 구분하기 위함이다. NFC 포럼은 RFID 리더와 태그가 모두 결합된 RFID 장치를 만들어 이를 휴대전화에 장착하는 구조를 생각하였고, RFID 리더를 이용하는 응용 모델로서 영화 포스터에 부착된 RFID 태그를 읽어 정보 서비스를 이용하는 응용 그리고 RFID 태그를 이용하는 응용 모델로서 태그를

출입통제용 신분증으로 이용하는 응용을 고려하였다[3]. 따라서 RFID 리더가 태그를 읽어 정보 서비스를 받는다는 기능이 유사하기 때문에 NFC 기술과 모바일 RFID 기술이 동일하다는 오해가 생길 수 있으므로 이를 구분할 필요가 있다. 즉, 본 고에서 언급하는 모바일 RFID 서비스는 RFID 태그와 리더 사이의 무선 통신이 900MHz 주파수 대역을 사용하는 ISO/IEC 18000-6 타입 C 무선 통신 규격을 준수하는 서비스로 한정한다.

1. 모바일 RFID 기술 개요

모바일 RFID 서비스는 우리나라에서 이동통신 인프라를 바탕으로 휴대전화를 이용하여 사물과 사람 사이의 직접적 정보소통 관계를 제공하기 위하여 시작된 융합 서비스이다. (그림 1)은 모바일 RFID 시스템 개념도이다. (그림 1)의 모바일 RFID 서비스 네트워크에 존재하는 ODS 서버는 RFID 태그 식별자와 관련된 제품정보가 있는 OIS 서버의 위치를 알려주는 역할을 하며, OTS 서버는 개인 사용자에게 제품의 유통 정보 또는 OIS 서버의 이력을 제공하는 역할을 하며, OIS 서버는 RFID 태그 식별자와 관련된 제품의 주요 정보를 저장하고 관리하는 역할을 한다. 이러한 서버들과 휴대전화와의 통신은 이동통신망을 통해 수행된다. (그림 1)의 구성요소에 맞춰 모바일 RFID 서비스 제공을 설명하면 다음과 같다. 휴대전화를 소유한 개인 사용자가 휴대전화에 장착된 RFID 리더로 제품에 부착된 RFID 태그로부터 식별자를 읽는다. 휴대전화는 이동통신망을 통해 태그 식별자를 로컬 ODS 서버로 전달하여 태그 식별자와 관련된 제품정보를 가진 OIS 서버의 위치를 파악한다. 휴대전화는 OIS 서버로부터 제품정보를 얻어 사용자에게 보여준다.



(그림 1) 모바일 RFID 시스템

2. 국내 표준화 동향

모바일 RFID 기술 표준화를 위한 국내 활동은 모바일 RFID 포럼을 중심으로 매우 활발하게 전개되고 있다[4]. 2005년 2월 창립총회를 개최하며 출범한 모바일 RFID 포럼은 창립 1년이 채 안된 2005년 12월에 자체 제정한 포럼 표준을 TTA 표준으로 제안하여 '모바일 RFID 응용 데이터 형식' 등 7건의 단체표준과 '모바일 RFID 서비스 메시지 전송 프로토콜' 등 9건의 기술보고서를 승인받았다[5]. 또한 2006년에는 '모바일 RFID 리더 제어 프로토콜' 등 15건의 포럼 표준을 TTA 표준으로 제안하여 승인받기도 하였다.

모바일 RFID 기술과 관련된 TTA 단체표준 중에는 보안 기술 표준으로서 2건의 단체표준과 1건의 기술보고서가 포함되어 있다. TTAS.KO-06.0120 문서번호의 '모바일 RFID 서비스 보안 요구사항'과 TTAS.KO-06.0146 문서번호의 '모바일 RFID 프라이버시 보호 프레임워크'는 TTA 단체표준으로 채택되어 있으며[6],[7], TTAR-06.0014 문서번호의 '모바일 RFID 프라이버시 보호 가이드라인'은 기술보고서로 채택되어 있다[8]. 이미 국내 TTA 표준으로 제정되어 있는 모바일 RFID 기술 규격들은 국제 표준화 추진 시에 참조될 수 있으며, 국제 표준화 논의에서 기술 주도권을 행사하는 든든한 버팀목이 되고 있다. 본 고에서 고려하는 모바일 RFID 보안 기술의 국제 표준화 추진 역시 TTA의 모바일 RFID 보안 기술 표준의 내용을 포함시켜 추진할 예정이며, 이미 일부 내용은 ITU-T 표준화 회의를 통해 국제 표준화가 추진중이다.

3. 국제 표준화 동향: ITU-T 동향

우리나라는 모바일 RFID 포럼과 TTA에서의 표

준화를 바탕으로 표준의 국제화와 시장 확대를 도모하고 있는데, 그 노력의 일환으로 ETRI를 중심으로 한 한국 대표단은 ITU-T 표준화 회의에서 모바일 RFID 기술의 비전을 설명하고 표준화 필요성을 주장하면서 표준화를 위한 작업 공간 확보를 시도하였다. 그 결과 ITU-T의 표준화 추진 전략을 수립하는 작업반을 만들어 의장과 보고서 작성자 지위를 확보하게 되었고, 또한 ITU-T SG13, SG17[1]에서 표준 권고안 작성에 대한 승인도 얻게 되었다. 이렇듯 ITU-T에서의 모바일 RFID 표준화 작업은 우리나라에서 주도권을 쥐고 있는 상황이며, 휴대전화에서의 B2C 서비스에 관심을 가지고 있는 일부 국가에서 적극적으로 참여하고 있다. 2006년 7월의 ITU-T TSAG(표준화 자문 그룹) 회의에서는 RFID 표준화를 위한 공식적인 협력 그룹으로서 JCA 그룹이 만들어졌으며, 모바일 RFID 기술은 JCA 활동을 통해 지속적으로 표준화 활동이 견인될 예정이다.

모바일 RFID 기술 중 ITU-T 산하의 표준화 그룹에서 표준화 대상으로 삼는 기술적 영역은 태그-리더 사이의 무선 통신 영역을 제외한 모바일 RFID 네트워크 영역 및 응용 서비스 영역이다. 현재 작성중인 표준 권고안에는 'NGN에서의 모바일 RFID의 서비스 요구사항', 'RFID 응용을 위한 OID 할당 및 관리', 'RFID 서비스에 대한 프라이버시 보호 지침', 'RFID 서비스를 위한 X.500 디렉토리 서비스 확장', 'RFID 프라이버시 관리 프레임워크' 등이 있다.

4. 국제 표준화 동향: ISO/IEC JTC1 동향

ISO/IEC JTC1 산하의 표준화 그룹에서는 태그-리더 사이의 무선 통신과 관련된 핵심 기술을 주요 표준화 대상으로 삼고 있다. 900MHz 수동형 RFID 통신 규격을 정의하고 있는 ISO/IEC 18000-6 표준도 ISO/IEC JTC1 산하의 SC31 WG4 SG3에서 작성한 문서이다.

ISO/IEC JTC1 산하 표준화 그룹에서 모바일 RFID 표준화 논의가 본격적으로 시작된 것은 2007년 1월 ISO/IEC JTC1 SC31 WG4 SG3[2] 시드니 회의에서 ETRI 연구진이 모바일 RFID 기술 소개 및 리더 칩이 내장된 휴대폰을 공개하면서 본격화 되었다. 이후 2007년 3월 워싱턴 WG4 정기 회의에서 모바일 RFID 서비스를 포함한 시연 동영상과 리더 칩을 내장한 휴대폰을 다시 보여주며 모바일 RFID 표준화 추진을 제안하였다. 그러나 WG4 의장과 일부 유럽 국가에서 NFC의 경쟁상대로 인식한 탓에 비우호적인 태도를 보였고, 신규 제안서 제출 분위기가 조성되지 못한 채 모바일 RFID ad-hoc 그룹을 결성하여 2007년 6월 남아프리카공화국 프리토리아 SC31 정기회의 전까지 좀 더 논의해 보자는 것으로 마무리되었다.

SC31 WG4 산하에 결성된 모바일 RFID ad-hoc 그룹은 3차례의 텔레컨퍼런스를 통해 논의한 결과 최종적으로 2개 안을 제시하였다. 첫번째 안은, WG4 산하에 SG6를 결성하여 모바일 RFID 관련 내용만을 표준화하는 것이고 두번째 안은, SC31 산하에 "Mobile item identification and management"를 표준화하는 WG6를 별도로 만들고 WG6 산하에 4개의 SG를 결성하여 모바일 RFID, 모바일 ORM, USN 등을 아우르는 표준화를 진행하자는 방안이다. 그러나 남아프리카공화국 프리토리아 회의에서는 신규 그룹의 생성에 대해서는 어떠한 결정도 내리지 못하였고, 차기 SC31 정기 회의까지 SC31 산하에 "Mobile item identification and management in support of consumer applications"라는 이름의 ad-hoc 그룹을 결성하여 신규 표준화 그룹 생성에 관한 타당성을 논의한다는 것으로 결론을 내었다. 비록 WG4 SG3에서는 상위 그룹인 WG4로 넘기고, WG4에서는 다시 SC31로 책임을 전가시키는 양상이 되었지만, 사실상의 모바일 RFID 표준화

1) ITU-T 표준화 그룹 구조는 ITU-T 산하에 SG(Study Group)이 있으며, 각 SG 산하에 WP(Working Party)가 존재하고 그 산하에 Question 그룹이 존재함. 예) ITU-T SG17 WP2 Q.9

2) ISO/IEC JTC1 표준화 그룹 구조는 ISO/IEC JTC1 산하에 SC(Sub Committee)가 존재하고, SC 산하에 WG(Working Group)이 있음. 규모가 큰 WG인 경우에 그 산하에 SG(Sub Group)이 존재하기도 함. 예) ISO/IEC JTC1 SC31 WG4 SG3

로드맵은 ad-hoc 그룹에서 도출할 수 있고, ad-hoc 그룹의 간사를 한국대표단의 일원인 ETRI에서 맡아 첫번째 ad-hoc 그룹 회의를 2007년 10월에 한국에서 개최하기로 결정하였기 때문에 한국이 모바일 RFID 국제 표준화에 있어서 명실상부한 주도권을 쥘 수 있게 되었다[9].

Ⅲ. 모바일 RFID 보안 요구사항

미국 NIST에서 2007년 4월에 발간한 "Guidelines for Securing Radio Frequency Identification Systems"에 따르면[10] RF 신호의 암호화, RFID 사용자에 대한 인증, RFID 태그의 재활용 또는 파괴 기술 등을 권고하고 있으므로 이를 해결하기 위해서는 표준화된 경량의 RFID 암호 기술, RFID 보안/인증 프로토콜, RFID 키 관리 기술 등이 필요하다. 또한 TTA 단체표준인 TTAS.KO-06.0111 문서번호의 'RFID 프라이버시 보호 가이드라인'과 TTAR-06.0014 문서번호의 '모바일 RFID 프라이버시 보호 가이드라인'에 따르면[8],[11] RFID 태그로부터 개인정보를 얻을 수 있는 경우에 개인 정보의 암호화, 개인 위치 정보의 보호 및 개인 프라이버시 침해가 없어야 함을 명시하고 있어서 RFID 사용자의 프라이버시 보호를 위한 킬 태그 기법, 리코딩 기법, 프로파일 기반 프라이버시 보호기법 등의 표준화가 요구되고 있다.

물론 모바일 RFID 응용 서비스에 따라 보안 요구사항이 거의 필요 없는 서비스도 있을 수 있다. 예를 들면 영화 포스터에 부착된 RFID 태그는 정보 제공자의 오프라인 하이퍼텍스트 역할을 수행하는 것으로서 개인 사용자가 얻고자 하는 영화 정보는 누구에게나 동일하게 제공되는 정보이므로 별도의 보안 조치를 요구하지 않는다. 그러나 RFID 태그가 부착된 제품을 개인 사용자가 구매한 경우, 구매 이후에는 RFID 태그 식별자를 비롯한 RFID 태그 연결 정보는 오직 구매 당사자의 소유이므로 이를 보장해야 할 보안 기술이 요구된다. 즉, 현재의 모바일 RFID 서비스는 RFID 리더가 장착된 휴대전화로 누구나 태그에 대한 접근이 가능하고, 태그 정보가 불법적으로 수집될 수 있으며 추적이 가능하므로 모바일 RFID 환경에 최적화된 경량의 보안 및 프라이버시 보호 기술이 필요하다.

본 고에서는 체계화된 분석을 위하여 (그림 1)의 구성요소에 기반하여 데이터 전송이 이뤄지는 각 구간별 보안 요구사항을 정리하며, 주로 참고문헌[6]의 내용을 참조하였다.

1. 태그와 리더 구간 보안 요구사항

강화된 보안 기능을 위해서는 태그와 리더간 인증 기능이 필요하며, 태그 식별자 및 태그의 사용자 메모리 영역을 보호하기 위한 접근 제어, 데이터 기밀성, 무결성이 보장되어야 한다. 태그의 접근 제어나 기능 정지를 위한 패스워드 사용시 안전한 패스워드 전송 및 관리 기능을 제공해야 하며 리더는 패스워드를 안전하게 보관해야 한다. 그 밖에도 태그의 사용자 메모리 영역에 저장된 정보에 대한 부인방지 기능이 필요하며, 위장 리더 또는 위장 태그로부터 유입되는 대량의 메시지를 차단할 수 있는 서비스 거부 공격 방어 기능이 요구된다.

2. 리더와 ODS 서버 구간 보안 요구사항

리더 인증을 요구하는 ODS 서버의 경우, 모바일 RFID 리더에는 인증을 위한 정보와 인증 절차를 수행하는 기능이 포함되어 있어야 한다. ODS 서버는 리더의 질의에 대한 응답 후 개인 사용자 프라이버시 보호를 위해 리더의 질의 내용을 별도로 수집하지 않아야 한다. 로컬 ODS 서버와 루트 ODS 서버 간에는 접근 통제를 위한 상호 인증이 제공되어야 하며, 기밀성 및 무결성 보장을 위해 보안 통신이 필요하다.

3. 리더와 OIS/OTS 서버 구간 보안 요구사항

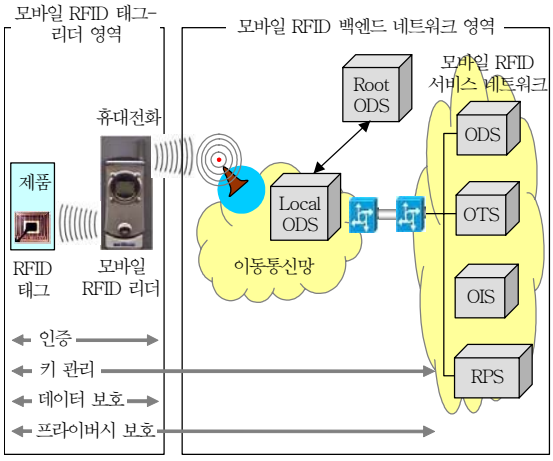
OIS/OTS 서버 접근시 인증이 필요한 경우에는

모바일 RFID 리더에 인증 정보와 인증 절차 수행 기능이 포함되어야 하며 리더와 OIS/OTS 서버 사이의 상호 인증 기능이 제공되어야 한다. 개인 정보나 결재 정보 및 태그 관리를 위한 패스워드 등과 같은 보안이 필요한 정보가 전달되는 경우에는 리더와 OIS/OTS 서버 구간에는 기밀성, 무결성, 부인 방지 기능이 제공되어야 한다.

Ⅳ. 향상된 모바일 RFID 보안 서비스 및 표준화 대상

1. 모바일 RFID 보안 프레임워크

제 Ⅲ장에서 분석한 모바일 RFID 보안 요구사항을 충족시키기 위해서는 (그림 1)의 모바일 RFID 시스템을 (그림 2)와 같이 RPS 서버를 포함시킨 형태의 향상된 모바일 RFID 보안 프레임워크로 확장해야 한다[7]. RPS 서버의 활용은 각 태그 또는 각 사용자마다 정의된 프라이버시 보호 수준별 접근 정책을 지정하고, 이에 따른 서비스 접근 제어를 가능하게 한다. 본 고에서는 (그림 2)의 보안 프레임워크에서 제공 가능한 향상된 모바일 RFID 보안 서비스를 설명하며, 각각의 보안 서비스 제공을 위한 기술적 해결책이 표준화 대상이 되어야 함을 강조할 것이다. 그리고 본 고에서는 안전한 모바일 RFID 서비스를 제공하기 위해서 RFID 태그의 한정된 자원 제약사항을 고려하여 새로이 표준화가 추진되어야 할 대상에 관심을 두며, 기존의 네트워크 보안 기술로 대체할 수 있는 백엔드 네트워크 영역은 안전한 통신이 가능하다고 가정한다.



(그림 2) 모바일 RFID 보안 프레임워크

2. 인증

모바일 RFID 서비스에서의 인증은 모바일 RFID 리더에 대한 장치 인증과 서비스 사용자 인증으로 구분할 수 있다.

장치 인증은 휴대전화에 장착되어 있는 RFID 리더 장치에 대한 인증을 의미하며 모바일 RFID 서비스가 이종망(이동통신망-RFID 응용 서비스망)간의 연동 서비스를 기반으로 하고 있으므로 장치 인증이 제공되어야 할 필요성이 증대하였다. 모바일 RFID 리더는 휴대전화에 내장되므로 이동통신망 접속시 제공되는 휴대전화 장치 인증으로 대체될 수 있으며, 특별히 리더 장치 인증이 필요한 경우를 대비하여 별도의 장치 인증 규격이 표준화 대상이 될 수 있다. 특별한 요구가 있는 응용 환경에서는 태그도 인증 대상이 될 수 있으며, 이러한 경우에는 태그 측에 구현되어야 할 인증 정보 및 인증 절차가 표준화되어 있어야 한다.

사용자 인증은 모바일 RFID 서비스 사용자에 대한 인증을 의미하며, 일반적으로는 모바일 RFID 리더가 OIS 서버에 접속하여 모바일 서비스 콘텐츠를 제공받기 위해 사용자 인증 과정이 수행되어야 한다. 모바일 RFID 응용 서비스가 개인 프라이버시 보호를 위해 RPS 서버와 연동되는 경우에는 모바일 RFID 리더가 사용자 인증 과정을 거친 후에만 RPS 시스템에 접속하도록 기술 표준을 정의할 수도 있다. 이때 OIS 서버와 RPS 서버는 사용자 편의를 위해 싱글 사인 온 인증 기능을 지원할 수도 있다. 로컬 ODS 접근 제어가 필요한 모바일 RFID 응용 서비스의 경우에 이에 대한 인증도 리더를 통해 수행될 수 있어야 한다. 또한 리더는 모바일 RFID 서비

스 네트워크를 OIS 서버나 RPS 서버에 인증할 수 있으며, 이러한 인증 절차도 표준화 대상이 된다.

3. 키 관리

제품에 부착된 RFID 태그의 기능을 정지하거나 태그의 메모리 영역에 대한 접근 제어를 위해 패스워드를 사용해야 하는 모바일 RFID 응용 서비스의 경우, 이러한 패스워드를 안전하게 전달, 관리할 수 있는 키 관리 메커니즘이 표준화되어야 한다. 주로 이러한 키 관리는 모바일 RFID 서비스 네트워크에 위치한 별도의 키 관리 서버에서 제공되는 보안 서비스로서 일반적인 키 관리 메커니즘 측면에서 살펴보면, 키 관리 서버가 모바일 RFID 리더에게 안전하게 패스워드를 전달해 준다. 만일 보안성 강화를 위해 계층적 키 관리 기법이 필요한 경우에는 키 관리 서버는 리더에게 마스터 키를 전달하고, 리더와 태그는 마스터 키를 이용하여 별도의 세션 키를 설립해야 한다. 이런 환경에서는 RFID 태그의 연산능력을 고려한 경량의 키 설립 프로토콜이 표준화 대상이 된다.

4. 데이터 보호

모바일 RFID 서비스에서 보호해야 할 정보는 기본적으로 다음과 같은 세 종류의 데이터이다. 첫째, 모바일 RFID 리더와 태그와의 통신을 통해 전달되는 태그 식별자 정보와 사용자 메모리 영역 정보 및 태그 기능 정지나 사용자 메모리 접근을 위한 패스워드 정보, 둘째, ODS 서버를 통한 태그 식별자 해석 과정을 통해 전달되는 URI 정보, 그리고 셋째, OIS 서버와의 통신을 통한 모바일 응용 서비스 콘텐츠 정보이다. 위의 둘째, 셋째 정보는 백엔드 네트워크에서 주고받는 정보이므로 기존의 네트워크 보안 기술로 안전성을 확보한다고 가정할 때, 본 고에서 표준화 대상으로 삼아 보호 기술을 적용할 정보는 리더와 태그 사이에서 주고받는 정보이다.

중요 정보에 대한 데이터 보호 서비스는 기밀성 유지, 무결성 보장, 부인 방지 등의 기능을 포함하는 개념이다. 기밀성 유지 측면에서 볼 때, 태그와 모바일 리더 사이의 무선 통신 구간에서 전달되는 태그 식별자 정보와 사용자 메모리 정보는 모바일 RFID 서비스에서 사용하는 수동형 RFID 태그의 자원의 한계로 인하여 기밀성을 보장하는 데 기본적인 한계를 안고 있으나 태그가 부착되어 있는 제품을 개인 사용자가 소유하게 되는 경우, 데이터의 기밀성 유지는 반드시 해결되어야 한다. 무결성 보장 측면에서 보면, 개인 사용자가 소유한 제품에 부착된 RFID 태그에 대해서는 현재 제공되고 있는 CRC 방식 이외의 추가적인 암호학적 무결성 제공 방법이 구현되어야 한다. 그리고 부인 방지 기능은 RFID 태그의 사용자 메모리 영역에 어떤 정보가 담길 때 허가 받은 기관이 기록했음을 보장하기 위해 필요한 기능이다.

모바일 RFID 보안 프레임워크에서 위와 같은 데이터 보호 서비스를 제공하기 위해서는 낮은 연산능력과 적은 메모리 사용에 적합한 경량의 암호 알고리듬과 보안 프로토콜의 표준화가 선행되어야 한다.

5. 프라이버시 보호

모바일 RFID 서비스는 최종 사용자를 대상으로 한 B2C 서비스이기 때문에 필연적으로 개인 프라이버시 침해 문제가 발생할 수 있으며, 이에 대한 해결책을 표준화하여야 한다. 모바일 RFID의 개인 프라이버시 문제는 위치 프라이버시 문제(location privacy), 휴대전화 소유자 프라이버시 문제(consumer privacy), 그리고 정보 프라이버시 문제(information privacy)로 구분할 수 있다.

위치 프라이버시 문제는 태그 부착 물품을 지니고 있는 개인에 대해 태그 식별자를 개인의 식별자로 사용하여 개인의 위치를 추적하여 발생하는 프라이버시 문제이다. 위치 프라이버시 보호를 위해서는 개인 식별자로 사용될 수 있는 태그 식별자에 대한 접근 제어를 통해 해결할 수 있다. 위치 프라이버시를 보호할 수 있는 방안으로는 태그 식별자 접근에 대한 인증 기법을 통한 방안과 태그 식별자 특성을

제거하는 기법을 통한 방안이 있다. 따라서 위치 프라이버시 보호가 필요한 모바일 RFID 응용 서비스에서는 태그 소유자의 위치 프라이버시 정책에 따라 추가로 위치 프라이버시를 보호할 수 있는 기능을 제공할 수 있도록 해당 기술의 표준화가 필요하다.

휴대전화 소유자 프라이버시 측면에서 보면, 모바일 RFID 리더가 장착된 휴대전화를 소유한 개인 사용자가 공개된 RFID 태그를 읽는 경우 휴대전화 소유자의 프라이버시 침해 위협에 대한 보호도 보장되어야 한다. 즉 공개된 태그를 읽는 순간, 태그를 읽는 리더가 탑재된 휴대전화의 개인 정보는 이동통신 사업자의 망을 통하여 OIS 사업자로 전달될 수 있다. 다시 말해, RFID 태그를 읽는 사용자 정보와 위치 정보뿐만 아니라 주로 어떠한 정보를 수집하는지, 얼마나 자주 이용하는지 등의 개인별 취향이 해당 사업자에게 노출될 수 있다. 이러한 정보들은 태그가 부착된 제품을 구매하는 것과 관계없이 모바일 RFID 리더 기능을 가진 휴대전화에서 태그를 읽는 순간 즉각 발생되는 개인 프라이버시 문제이다. 따라서 모바일 RFID 서비스 사업자는 개인 프라이버시 침해가 되는 정보를 수집하여야 하는 경우, 사용자가 정한 정책 또는 사용자가 동의한 정책에 따라 수집하여야 하며 이를 기술적으로 뒷받침할 수 있는 표준 규격이 논의되어야 한다.

정보 프라이버시 보호 문제는 일반적으로 일상생활에서 생성되는 개인 데이터의 이용, 전달 및 처리에 관한 정보 통제권의 문제이다. 그러나 모바일 RFID 서비스에 대한 정보 프라이버시 문제는 RFID 네트워크 인프라 내에 위치하고 있는 태그 부착 제품의 정보 자체가 물품 소유자를 식별하고 소유자의 특성을 알아낼 수 있는 개인 데이터의 일부가 될 수 있다는 문제에서 출발한다. 따라서 태그 부착 제품을 사용자가 소유한 이후에도 계속적인 서비스가 필요한 경우에는, 정보 프라이버시 보호 기능을 제공해야 하며 이를 지원할 수 있는 프레임워크 제안 및 기술 표준화가 필요하다. (그림 2)의 RPS 서버는 정보 프라이버시 보호 기능을 제공할 수 있는 좋은 예이다. RPS 서버를 활용하여 개인 사용자는 자신의 개인 프라이버시 보호 수준을 정할 수 있으며, 프라이버시 보호 정책을 수정할 수 있다. RPS 서버는 이러한 개인 사용자별 프라이버시 보호 정책을 OIS 서버에게 전달하여 OIS 서버로부터 제공되는 태그 연결 콘텐츠가 사용자가 정한 프라이버시 보호 정책을 반영할 수 있도록 할 수 있다.

Ⅴ. 모바일 RFID 보안기술 표준화 전략

RFID 기술 개발에 있어 국내외적으로 산업체에서의 연구뿐만 아니라 표준화 논의에서도 최소의 규격으로 사물 및 환경에 대한 정보를 실시간으로 획득하려는 노력이 진행되어 왔다. 이러한 노력의 결과라 할 수 있는 ISO/IEC 18000-6 타입 C 태그는 자체적인 전원을 갖고 있지 않은 수동형 RFID 태그로서 낮은 연산 능력과 적은 정보 저장 능력으로 구현되고 있다. 이러한 제약 조건으로 인하여 기본적인 통신 기능 이외에 데이터 보호 및 개인 프라이버시 예방을 위한 보안 기능이 취약한 상황이다. 모바일 RFID 기술 표준화 대상 중 무선 통신 규격은 ISO/IEC 18000-6 타입 C 규격을 모바일 환경에 맞게 수정하는 방향으로 진행될 예정이다. 따라서 모바일 RFID 보안 기술의 국제 표준화 추진을 위해서는 ISO/IEC 18000-6 타입 C 규격의 보안 특징을 살펴볼 필요가 있다.

ISO/IEC 18000-6 타입 C 태그는 보안 기능으로서 태그 메모리 접근 제어 패스워드와 태그 기능 정지 패스워드를 사용할 수 있도록 표준을 정하였으나, 연산 능력의 제약 때문에 보안 강도가 강한 알고리듬의 사용이 불가능하여 단순히 랜덤 수와 패스워드의 XOR 연산만을 수행하도록 정의하였다. 이 때 랜덤 수 자체가 무선 구간에서 평문으로 노출되는 값이기 때문에 불법적인 도청자는 단순한 RFID 통신의 도청만으로 패스워드를 알아낼 수 있는 취약점이 존재한다. 이러한 패스워드 노출의 약점과 더불어 RFID 태그 소유자의 위치 추적과 태그 식별자 노

출의 개인 프라이버시 침해의 위험성도 널리 알려진 약점이다. 이러한 약점을 극복하기 위하여 상당부분 진행된 기술 개발 사례들도 있는데, 대표적인 기술로는 정책 기반의 접근 제어, RFID 태그의 안테나를 절단하여 통신 거리를 최소화함으로써 도청 취약성을 약화시키는 기술 등이 있다[12]. 따라서 모바일 RFID 보안 기술의 표준화 전략을 수립하는 데 있어 가장 먼저 할 일은 현재 개발된 기술도 고려하면서 널리 알려진 보안 취약점을 극복하고 보안성을 강화하는 방향으로 모바일 RFID 보안 기술 표준화를 추진하는 것이다.

모바일 RFID 보안 취약점을 극복하려는 기존의 노력은 악의적인 공격자의 도청이나 불법적인 정보 수집 등 어느 특정한 공격에 대해서는 효과를 얻는 데 큰 도움이 될 수 있다. 디지털 통신 장치인 태그와 리더에 대한 보안 취약성과 디지털 통신 시스템으로서 모바일 RFID 시스템에서의 보안 취약성을 해결하려는 보안성 강화 노력을 해왔으며, 이러한 노력은 국제 표준화 추진에 있어서도 1차적인 추진 방향이기도 하다.

그러나 기존의 전통적인 공격과는 달리 새롭게 등장한 다양하고 복합적인 공격과 위협이 모바일 RFID 기술에 큰 도전이 되고 있다. 최근에는 디지털 가상공간에서의 위협뿐만 아니라 RFID 태그 자체에 대한 물리적인 공격 위협으로 확대되고 있는 상황이다. 이러한 물리적인 공격은 RFID 해킹으로 규정할 수 있으며, 그 대표적인 예로는 복제(cloning), 재전송 공격(replay attack), 부채널 분석(side-channel analysis)이 있다. 복제 공격은 RFID 태그의 하드웨어 특성을 파악한 후 동일한 하드웨어를 사용하여 물리적으로 동일한 RFID 태그를 복제하거나 또는 RFID 태그의 메모리 정보를 모두 해킹한 후에 동일한 정보를 가진 쌍둥이 RFID 태그를 만들어서 모바일 RFID 시스템을 교란시키는 공격이다. 재전송 공격은 공격자가 RFID 태그의 동작 절차와 응답 데이터 등을 알아낸 후에 모바일 RFID 리더의 요청이 있을 시 공격자도 응답 데이터를 전송하여 모바일 RFID 리더를 혼란시키는 공격이다. 물론 그 반대의 경우도 가능하여 공격자의 악의적인 리더가 RFID 태그들을 공격할 수도 있다. 이러한 복제 및 재전송 공격에서 공격자가 RFID 태그 정보를 획득할 때 사용되는 공격 기법에는 알려진 통신 프로토콜을 이용하는 단순 도청, 하드웨어 특성 파악을 이용하는 하드웨어 복제 및 RFID 태그에서의 연산 과정에서 누설되는 누설 전력 또는 전자기파를 이용하는 부채널 분석이 있다.

따라서 모바일 RFID 보안 기술의 표준화 전략을 수립하는 데 있어 가장 중점을 둬야 할 부분은 기존의 모바일 RFID 시스템 취약성과 최근의 RFID 해킹 공격을 동시에 극복하는 방향으로 표준화 대책을 강구하며, 동시에 국내외적으로 영향력을 행사할 수 있는 지적재산권을 확보하는 것이다. 다양하고 복합적인 공격과 위협을 해결하기 위하여 초경량 보안 프로토콜의 표준화, 응용 환경에 최적화된 암호 알고리듬의 표준화 그리고 PUF 기술을 이용한 하드웨어 복제 방지 기법의 표준화와 같이 크게 3가지 기술 표준화로 접근할 계획이다.

첫째, 초경량 보안 프로토콜의 표준화는 모바일 RFID 응용별로 특화된 형태로 설계될 수 있으며 인증, 키 관리, 접근 제어, 도청 방지, 서비스 거부 공격 방지 등을 지원하기 위한 표준화 추진 전략이다.

둘째, 응용 환경에 최적화된 암호 알고리듬의 표준화는 자원 제약이 심한 모바일 RFID 시스템에서 암호 알고리듬을 구동시키기 위하여 각 응용 환경을 고려하여 암호 알고리듬을 선택하려는 표준화 추진 전략이다.

셋째, PUF(물리적 복제 방지) 기술을 이용한 복제 방지 기법도 모바일 RFID 보안 기술의 표준화 추진 대상이 될 것이다. PUF 기술은 대부분의 디지털 장치의 복제 방지에 사용되어지는 기술로써 디지털 로직의 하드웨어 구현시 각 공정의 특성, 선로 지연(wire delay), 게이트 지연(gate delay) 등이 생산품에 미치는 영향을 이용하여 복제 여부를 알아내는 기술이다. 또한 누설 전력 및 누설 전자기파를 탐지하는 부채널 분석 공격을 방어하기 위한 방어 회로 또는 방어 소자에 대한 권고안 등도 모바일 RFID

보안 기술의 국제 표준화 추진시 고려해야 할 사항이다.

위와 같은 기술적 분석에 따라 표준화 추진 전략을 수립하는 것은 안전한 모바일 RFID 시스템을 구축하기 위한 기술적 토대를 마련하는 가장 중요한 작업이다. 현재까지는 기존의 모바일 RFID 취약성과 최근의 RFID 해킹을 동시에 극복하는 기술 개발이나 표준화 활동은 미비한 상태이므로 이 부분에 대해서 보다 발빠르게 지적재산권을 확보하고 기술 개발을 통해 검증하여 이를 바탕으로 국제 표준화를 추진하면 큰 성과가 있을 것으로 판단된다.

이와 더불어 국제 표준화 그룹에서의 활동 방향에 대한 전략을 수립하는 것도 중요하다. ETRI에서 그 동안 단일 아이템으로써 RFID 보안 기술만을 국제 표준화하고자 노력했을 때, 이미 핵심적인 RFID 통신 기술을 표준화했던 기존 세력들의 반대에 부딪히는 경우가 많았으나 이번 모바일 RFID 보안 기술의 표준화는 전체적인 모바일 RFID 시스템 표준화 과정에서 일부분으로 포함되어 동시에 진행될 예정이므로 훨씬 표준화 추진이 원활할 것으로 보인다. 또한 그 동안 ETRI에서는 이미 ITU-T 및 ISO/IEC JTC1의 RFID 관련 표준화 회의에서 수 차례의 RFID 보안 기술 발표를 통해 RFID 보안 기술 논의에 기여하면서 다수의 RFID 표준 위원들에게 우리나라가 RFID 보안 기술에 대한 전문가적 지식과 관심을 가지고 있음을 강조해 왔고, 모바일 RFID 논의를 위한 ad-hoc 그룹에도 적극적으로 참여해 왔으므로 향후 모바일 RFID 보안 기술 표준화 추진에서도 매우 유리할 것으로 전망된다.

Ⅵ. 결론

최근의 RFID 보안 대책의 경향은 단편적인 기술 개발보다는 다양한 환경을 고려한 융합 보안 기술 개발 및 보안 인프라 구축에 초점이 맞춰지고 있다. 결국 사회가 고도화되고 개인의 행복추구와 프라이버시 보호에 대한 요구가 높아질수록 이를 보장하면서 동시에 국가의 전체 질서와 공공의 이익을 유지할 수 있는 법적, 제도적, 기술적 지원이 유기적으로 결합되어야 하는데, 모바일 RFID 기술도 이러한 기본적인 사회법칙과 그 궤를 함께할 것으로 판단된다.

따라서 모바일 RFID 응용별로 요구되는 법적, 제도적 환경에 맞게 모바일 RFID 보안 기술 개발, 표준화 추진 및 보안 인프라 구축이 이루어져야 하며 유비쿼터스 사회로 가는 과정을 염두에 두고 향후 다른 기술과의 협력을 통한 융합서비스 제공시 안전한 유비쿼터스 환경을 지원할 수 있는 방향으로 발전해 나가야 할 것이다.

본 고에서는 B2C 서비스를 지향하는 모바일 RFID 서비스 환경을 고려하여 기존의 보안 취약점과 최근의 RFID 해킹을 모두 극복하는 방향으로 표준화 추진이 진행되어야 함을 강조하였다. 또한 모바일 RFID 보안 프레임워크를 제안하였고, 표준화 대상에 있어서는 향상된 보안성 제공을 위해서 인증, 키 관리, 데이터 보호 및 프라이버시 보호 서비스를 지원하는 주요 기술들이 표준화 대상이 되어야 함을 주장하였다.

결론적으로 향후 모바일 RFID 보안 기술의 국제 표준화 과정에서 초경량 보안 프로토콜, 응용 환경에 최적화된 암호 알고리듬, 물리적 복제 방지 기술 등과 같은 미래 지향적인 보안 핵심 기술 및 개인 사용자 프라이버시 보호를 위한 새로운 프레임워크의 제안을 통해 모바일 RFID 보안 기술의 국제 표준화 추진시 기술적 우위를 선점할 수 있을 것으로 기대되며, 꾸준하고 성실한 국제 표준화 회의 참석과 기여가 진행되어 왔으므로 ITU-T와 ISO/IEC JTC1 양측 모두에서 의미 있는 표준을 만들어 낼 수 있을 것으로 기대된다.

약 어 정 리

ASK	Amplitude Shift Keying
B2B	Business-to-Business
B2C	Business-to-Customer
CRC	Cyclic Redundancy Check
JCA	Joint Coordination Activity
NFC	Near Field Communication

NIST National Institute of Standards and Technology
ODS Object Directory Service
OID Object Identifier
OIS Object Information Service
ORM Optical Readable Media
OTS Object Traceability Service
PSK Phase Shift Keying
PUF Physically Unclonable Function
RPS RFID user Privacy management Service
URI Uniform Resource Identifier
USN Ubiquitous Sensor Network

참 고 문 헌

[1] ISO/IEC 18000-6, Information Technology - Radio Frequency Identification(RFID) for Item Management - Part 6: Parameters for air interface communications at 860MHz to 960MHz, 2004. 8. 15.
[2] 장병준, 이윤덕, "모바일 RFID 기술 동향 및 주요 이슈," IITA, 주간기술동향, 통권 1206호, 2005, pp.26-35.
[3] 김형준, "모바일+RFID," TTA 저널, 통권 108호, 2006, pp.46-53.
[4] 모바일 RFID 포럼, http://www.mrf.or.kr
[5] 한국정보통신기술협회(TTA), http://www.tta.or.kr
[6] TTAS.KO-06.0120, 모바일 RFID 서비스 보안 요구사항, 한국정보통신기술협회(TTA), 2006.
[7] TTAS.KO-06.0146, 모바일 RFID 프라이버시 보호 프레임워크, 한국정보통신기술협회(TTA), 2006.
[8] TTAR-06.0014, 모바일 RFID 프라이버시 보호 가이드라인, 한국정보통신기술협회(TTA), 2006.
[9] 강유성, "모바일 RFID 보안기술 국제 표준화 현황," *IT Standard Weekly*, 제 2007-34호, 한국정보통신기술협회(TTA), 2007.
[10] Tom Karygiannis, Bernard Eydt, Greg Barber, and Lynn Bunn, "Ted Phillips, Guidelines for Security Radio Frequency Identification(RFID) Systems," NIST Special Publication 800-98, 2007.
[11] TTAS.KO-06.0111, RFID 프라이버시 보호 가이드라인, 한국정보통신기술협회(TTA), 2006.
[12] Paul A. Moskowitz, Andris Lauris, and Stephen S. Morris, "Privacy-Enhancing Radio Frequency Identification Tag: Implementation of the Clipped Tag," *IBM White Paper*, 2006.