[RFID/USN] 860-960 MHz 대역 RFID 보안기술 표준화 전투의 본격화

860-960 MHz 대역의 UHF 수동형 RFID 기술의 새로운 도전 과제로 떠오른 보안기술 표준화를 위한 치열한 논쟁이 본격화되고 있으며, 그 중심에는 ISO/IEC JTC 1/SC 31/WG 7 (이하 WG7)이 자리잡고 있다.

2009년 6월에 호주 시드니에서 공식 승인된 WG7은 기존의 보안 요구사항 정의 수준을 넘어 기술적 해결책을 표준화하기 위한 목표를 가지고 있다. 제 1차 회의는 2009년 8월에 영국 런던에서 개최되었고 주요 결정 사항으로는 ISO/IEC 18000 시리즈에 대응되도록 주파수 대역 별 보안기술 표준화를 추진하기로 한 것이었다. 제 2차 회의는 2010년 3월에 우리나라 제주에서 개최되었으며 미국 Impinj, 미국 Revere Security, 네덜란드 NXP 및 한국 ETRI에서 제시한 주요 후보 기술들이 소개되었다.

최근 2010년 5월 25일에 중국 베이징에서 개최된 제 3차 WG7 회의는 주요 후보 기술로 압축된 미국 Impinj, 네덜란드 NXP, 한국 ETRI 멤버들의 논쟁이 주를 이루었다.

ISO/IEC 29167 시리즈와 ISO/IEC 18000 시리즈 관계

RFID 보안 서비스와 파일 관리를 위한 에어 인터페이스 표준은 오스트리아의 신규작업화 (NWIP: New Work Item Proposal) 제안 직후 2008년 7월 11일부터 2008년 10월 8일까지 약 3개월의 NWIP 국가투표 후에 통과되어 ISO/IEC 29167 문서번호를 부여 받고 표준화가 시작되었다. 표준화 범위는 사용자 메모리에 대한 파일 관리, 사용자 메모리에 대한 보안 접근 방법, 그리고 비인가 읽기에 대한 UII(Unique Item Identifier) 보호 기술로 명시되어 있다. 또한 호환되는 에어 인터페이스는 ISO/IEC 18000 시리즈로 한정시키고 있다. 즉, ISO/IEC 18000 시리즈가 정의된 형태에 따라 각 주파수 대역별로 구분하여 각 주파수 특성과 변복조 방식에 최적화된 보안 기술을 정의하고자 하였다.

현재는 다음과 같이 29167-1, 3, 6 파트에 대해 에디터를 선정하고 표준화를 추진 중이며, 29167-2, 4, 7 파트에 대해서는 표준화를 책임질 수 있는 멤버가 의사표현을 할 경우 신규 작업화가 진행될 것으로 예상된다.

- ISO/IEC 29167 Part 1: Air Interface for security and file management for RFID architecture (공동에디터: 오스트리아 CISC의 Josef Preishuber-Pflügl, 네덜란드 NXP의 Henk Dannenberg)
- ISO/IEC 29167 Part 3: Air Interface for security and file management for RFID at 13.56 MHz (공동에디터: 오스트리아 CISC의 Josef Preishuber-Pflügl, 네덜란드 NXP의 Henk Dannenberg)
- ISO/IEC 29167 Part 6: Air Interface for security and file management for RFID at 860 - 960 MHz (공동에디터: 오스트리아 CISC의 Josef Preishuber-Pflügl, 한국 ETRI의 강유

성)

ISO/IEC 29167-6 UHF 대역 RFID 보안기술 표준화 논쟁

ISO/IEC 29167-6에서는 ISO/IEC 18000-6 Type C에 호환되는 수동형 RFID 보안기술 표준화를 추진하고 있다. 한국 ETRI에서는 보안 프로토콜, 암복호화 방법, 명령/응답 메시지 포맷, 보안 파라미터 정의 및 보안 태그 상태 다이어그램을 제시한 상황이다. 네덜란드 NXP는 자신들이 보유한 스마트카드 보안 솔루션을 수동형 RFID 태그에도 적용하려는 움직임을 보이고 있으며, 미국 Impinj는 18000-6 Type C 표준의 태그 상태 다이어그램을 그대로 유지하면서 보안 기능을 추가하려는 움직임을 보이고 있다. 제안된 주요 기술을 분석하면 아래 표와 같다.

	한국 ETRI	네덜란드 NXP	미국 Impinj
주요 특징	-18000-6 Type C 호환 고려한 경량 구현 검증 모델 -UII 인식 과정에서 미리 보안 파라미터 전달로 효율성 향상 -키 관리 고려 -인증 프로토콜, 데이터보호프로토콜 별도제시 -AES-OFB like mode 사용	-수동형 RFID 목표로 하기 보다는 RFID 보안 프레임워크 중심의 제안 -AES-CBC mode 사용 -ECC 알고리즘 사용 -구현 검증 사례 공개된 것 없음	-태그 state diagram 기반의 설명 -UII 인식 이후에 보안 프로토콜 수행하기로 함 -명령/응답 순서만 설명될 뿐 구체적 동작과 알고리즘 활용 설명이 없음 -파일 관리 고려
지원 기능	-인증 -데이터보호 -Untraceability	-인증 -데이터보호 -Untraceability	-인증 -데이터보호 -Untraceability
기타 사항	-29167-6 공동에디터 보유 -수동형 RFID 보안기술에 집중	-비접촉식 IC 카드인 MIFARE 제조업체 -IC 카드 보안기술 관련 주요기술/특허 보유업체임	-18000-6 Type C 에디터 소속 업체임 -18000-6 Type C 주요기술/특허 보유업체임
장점	-18000-6 Type C 호환성 -경량 구현 검증 완료	-검증된 IC 카드 적용 기술의 활용 -다양한 확장성 고려	-분석 불가 (자료 미흡) -18000-6 Type C 호환성 가능할 것으로 예상
단점	-AES 알고리즘 의존 -알고리즘/프로토콜 확장성 미흡	-18000-6 Type C 적용 가능성 여부 의심 -경량 구현이 어려움	-분석 불가 (자료 미흡)

향후 전망과 국내 대응전략

ISO/IEC 29167-6 표준화에서는 제안된 주요 기술 중 한국 ETRI 기술과 미국 Impinj 기술이 경합을 벌일 것으로 예상된다. 물론, 어느 하나의 일방적인 승리가 아니라 함께 공존하며 사용자가 해당 모드를 선택하는 방식으로 결론이 날 수도 있다. 따라서, 가급적이면 한국에서 제안된 기술의 장점과 우수성을 널리 인식시켜 보다 지배적인 위치의 기술로 자리잡을 수 있도록 노력해야 할 것으로 판단된다.

강유성 (한국전자통신연구원 지식정보보안연구부 선임연구원, youskang@etri.re.kr)