[RFID/USN] UHF 수동형 RFID 보안기술 표준전쟁의 승자는 누가 될 것인가?

860-960 MHz 대역의 UHF 수동형 RFID 태그와 리더에 적용될 보안기술은 ISO/IEC JTC 1/SC 31/WG 7 (이하 WG7)에서 국제표준화가 활발하게 진행 중이다. 2009년 6월에 공식 출범하여 2009년 8월 런던 미팅을 시작으로 이번 2012년 10월 제11차 네덜란드 Groenlo 미팅까지 연 3~4차례의 대면회의를 개최하며 그 관심과 논쟁이 커져가고 있다.

이러한 관심을 반영하듯 2012년 12월 현재 WG7에 총 8건의 후보기술이 신규제안서로 선정되어 경합을 벌이고 있는 상황이다. 뿐만 아니라 이미 선정된 위의 8건 후보기술과 별도로 2건의 후보기술이 신규제안서로 제출되어 각 국가별 투표가 진행 중이다. 이렇듯 총 10건의 후보기술들이 난립하게 된 이유는 초기 주도권 싸움에서 유일한 승자가 나오지 못한 채 각 참여기업들이 독자적으로 신규제안서를 제출하였고, 이러한 상황에서 자신들의 제안이 거절당할까 두려워서 서로 강력한 견제 없이 서로서로 밀어주는 분위기가 형성되었기 때문이다.

UHF 수동형 RFID 보안기술 ISO/IEC 29167 시리즈 추진 현황

WG7에서는 UHF 수동형 RFID 에어 인터페이스 규격인 ISO/IEC 18000 시리즈에 정의된 Command/Response 포맷을 활용하는 구체적인 보안 프로토콜, 암호 알고리즘, 키 관리 기법 등을 정의하는 ISO/IEC 29167 시리즈 표준문서를 개발하고 있다(예를 들면, ISO/IEC 29176-14 표준문서에서 AES-OFB(Advanced Encryption Standard-Output FeedBack)를 사용하여 인증, 데이터 보호 등의 보안 서비스를 제공하는 보안기술을 정의하고 있음). <표 1>은 WG7의 표준문서 현황을 정리한 것이다.

<표 1> WG7 표준문서 현황 (2012년 12월 현재)

문서	제목	현단계	에디터
ISO/IEC 29167-10	Part 10: Air Interface for security services crypto suite AES128	CD 투표 예정	Henk Dannenberg (네덜란드 NXP)
ISO/IEC 29167-11	Part 11: Air Interface for security services crypto suite PRESENT-80	CD 투표 예정	Peter Rombouts (벨기에 NXP)
ISO/IEC 29167-12	Part 12: Air Interface for security services crypto suite ECC-DH	CD 투표 예정	Frantz Amtmann (오스트리아 NXP)
ISO/IEC 29167-13	Part 13: Air Interface for security services crypto suite Grain-128A	WD	Jim Springer (미국 EM)

ISO/IEC 29167-14	Part 14: Air Interface for security services crypto suite AES OFB	WD	강유성 (한국 ETRI)
ISO/IEC 29167-15	Part 15: Air Interface for security services crypto suite XOR	WD	Hu Yanan (중국 IWCOMM)
ISO/IEC 29167-16	Part 16: Air Interface for security services crypto suite ECDSA-ECDH	CD 투표 예정	Du Zhiqiang (중국 IWCOMM)
ISO/IEC 29167-17	Part 17: Air Interface for security services crypto suite CryptoGPS	CD 투표 예정	Loic Ferreira (프랑스 Orange Telecom)
ISO/IEC 29167-xx	Part xx: Air Interface for security services crypto suite HB2	NP 투표 중	Daniel Engels (미국 Revere Security)
ISO/IEC 29167-xx	Part xx: Air Interface for security services crypto suite RAMON	NP 투표 중	미국

향후 전망과 국내 대응전략

차기 WG7 회의는 2013년 4월 8일~9일에 미국 콜로라도 스프링스에서 개최되며, 위의 표에 언급된 10건의 후보기술들에 대한 각 국가 및 각 에디터의 견제와 협력 등이 가속화될 전망이다. 초기부터 가장 활발하게 RFID 보안기술 표준화에 앞장섰던 곳은 네덜란드 NXP와 한국 ETRI였으며, 현재도 가장 우수한 성능 및 구현가능성을 인정받으면서 동시에 강력한 견제도 받고 있는 상황이다. 국내 기술인 ISO/IEC 29167-14는 UHF 수동형 RFID 태그에서 구현 가능한 경량의 AES 암호모듈을 탑재하여 태그 인증, 리더 인증, 상호 인증 그리고 데이터 암복호화 기능 및 간단한 키 관리 기능을 제공할 수 있다. 그러나 NXP에서 제출한 3건의 표준문서가 모두 태그 인증만을 정의하고 있다. 즉, 그 동안 NXP에서는 암호 알고리즘과 동작 모드를 기존의 스마트 카드가 수용할 만한 수준의 기술을 언급했었는데 결국은 UHF 수동형 RFID 태그에 그대로 적용하지 못한 채 단순히 태그에서 최소 수준의 연산만을 수행하여 태그를 인증하는 태그 인증만을 표준화 추진하고 있다. 이러한 기술적 사항은 한국 표준안이 NXP 표준안보다 훨씬 활용 가치가 높다는 것으로 해석될 수 있다.

따라서 국내 TTA와 RFID/USN융합포럼 등에서 논의하였던 경험을 되살려 한국 표준안의 기능적 우수성과 구현 가능성을 강조하면서 UHF 수동형 RFID 보안기술의 국제표준화에서 지적재산권이 확보된 국내기술의 국제표준 반영을 위해 더욱 더 노력하면 좋은 결실이 있을 것으로 기대된다.

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