[RFID/USN] 10개 후보기술의 경합, 수동형 RFID 보안기술 유력 후보는?

860-960 MHz 대역의 UHF 수동형 RFID 태그와 리더에 적용될 보안기술은 ISO/IEC JTC 1/SC 31/WG 7 (이하 WG7)에서 국제표준화를 담당하고 있다. 2009년 6월에 공식 출범하여 2009년 8월 런던 미팅을 시작으로 이번 2013년 4월 제 12차 미국 콜로라도스프링스 미팅까지 연 3~4차례의 대면회의를 개최하며 그 관심과 논쟁이 증폭되고 있다.

애초에 합의점을 찾지 못한 채 2013년 4월 현재 WG7에 총 10건의 후보기술이 신규제안서로 선정되어 경합을 벌이고 있는 상황이다. 뿐만 아니라 1~2건의 후보기술이 신규제안서를 제출하려고 준비 중에 있다. 이미 WG7은 표준화 그룹 차원에서의 의견 일치를 통한 단일 표준문서 작성을 포기했으며 대동소이한 후보기술들이 표준화 절차에 따라 표준문서로 작성되고 있는 상황이다.

UHF 수동형 RFID 보안기술 ISO/IEC 29167 시리즈 추진 현황

WG7에서는 수동형 RFID 에어 인터페이스를 준용하면서 보안기능을 제공할 수 있는 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 경합 중인 10건의 RFID 보안기술 표준문서 현황을 정리한 것이다.

<표 1> WG7 표준문서 현황 (2013년 4월)

문서	제목	현단계	에디터
ISO/IEC 29167-10	Part 10: Air Interface for security services crypto suite AES128	2nd CD 투표 예정	Henk Dannenberg (네덜란드 NXP)
ISO/IEC 29167-11	Part 11: Air Interface for security services crypto suite PRESENT-80	DIS 투표 예정	Peter Rombouts (벨기에 NXP)
ISO/IEC 29167-12	Part 12: Air Interface for security services crypto suite ECC-DH	2nd 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	CD 투표 예정	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	2nd CD 투표 예정	Du Zhiqiang (중국 IWCOMM)
ISO/IEC 29167-17	Part 17: Air Interface for security services crypto suite cryptoGPS	2nd CD 투표 예정	Loic Ferreira (프랑스 Orange Telecom)

ISO/IEC 29167-18	Part 18: Air Interface for security services crypto suite HB2	WD	Daniel Engels (미국 Revere Security)
ISO/IEC 29167-19	Part 19: Air Interface for security services crypto suite RAMON	WD	Klaus Finkenzeller (독일 G&D)

향후 전망과 국내 대응전략

이번 회의 분위기를 요약하면, 한국의 가장 강력한 경쟁자로 생각한 NXP의 기술 3건뿐만 아니라 미국 Revere Security의 HB2와 독일의 RAMON 기술이 신규표준으로 표준화가 시작되면서 강력한 경쟁상대가 더 많아졌다는 것이다. HB2 에디터는 MIT의 AutoID Lab 초기 멤버로서 보안 및 RFID 전문가이고, RAMON은 RFID Handbook 저자인 독일의 Klaus Finkenzeller가 제시한 기술이기 때문에 향후 큰 관심을 받을 것으로 예상된다. 현재 총 10개 후보기술은 NXP 3건, 중국 2건, 미국 2건, 한국 1건, 프랑스 1건 및 독일 1건이다. 각각의 특징을 요약하면 다음과 같다.

- NXP 3건: 태그 인증만을 지원함. NXP가 대량 생산이 가능한 제조업체라는 장점이 있음.
- 중국 2건: 1건은 보안 취약점을 노출되었으며, 다른 1건은 능동형 RFID 대상기술임.
- 미국 2건: Grain 128A, HB2 모두 태그 인증, 상호 인증 등을 지원하는 우수한 기술적 특징을 가짐.
- 한국 1건: 미국의 Grain 128A, HB2 등과 유사한 보안 기능을 제공하며, 현재도 우수한 보안 성능 및 구현 가능성을 인정받으면서 동시에 강력한 견제도 받고 있음.
- 프랑스 1건: 경량 공개키 알고리즘을 사용하고 있지만, 큰 관심을 받고 있지는 않음.
- 독일 1건: 공개된 기술적 정보가 미흡하여 구체적 분석이 어려운 상황임.

후보기술이 너무 많은 관계로 결국은 서로 견제와 협력 속에 모든 후보기술들은 최종적으로 국제표준으로 채택될 가능성이 크다. 따라서 어느 기술이 실제 시장에서 활용될 것인지는 결국 서비스 제공업체와 제조업체 등 시장의 결정에 맡겨질 것으로 예상된다.

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