[RFID/USN] 표준과 시장의 괴리 - 수동형 RFID 보안기술

860-960 MHz 대역에서 동작하는 수동형 RFID 보안기술은 ISO/IEC JTC 1/SC 31/WG 7 (이하 WG7)에서 국제표준화를 담당하고 있다. 2009년 6월에 공식 출범하여 이번 2014년 10월 제 15차 미국 시애틀 회의까지 연 3~4차례의 대면회의를 개최하며 총 10건의 후보기술을 표준문서로 논의하고 있을 만큼 그 관심과 논쟁이 큰 상황이다.

UHF 수동형 RFID 보안기술 ISO/IEC 29167 표준문서 현황

WG7에서는 수동형 RFID 태그의 진위여부를 확인하는 태그 인증 프로토콜을 중심으로 다양한 보안기능을 제공할 수 있는 보안 프로토콜, 암호 알고리즘, 키 관리 기법 등을 정의하는 ISO/IEC 29167 시리즈 표준문서를 개발하고 있다. 각각의 표준문서에 따라 태그 인증, 리더 인증, 상호 인증, 데이터 암복호화 기능 등이 필수 또는 선택 구현사항으로 정의되어 있다. <표 1>은 경합 중인 10건의 RFID 보안기술 표준문서 현황을 정리한 것이다.

<표 1> WG7 표준문서 현황 (2014년 10월)

문서	제목	현단계	에디터
ISO/IEC 29167-10	Part 10: Crypto suite AES-128 security services for air interface communications	FDIS	Henk Dannenberg (네덜란드 NXP)
ISO/IEC 29167-11	Part 11: Crypto suite PRESENT-80 security services for air interface communications	IS (2014.7.22)	Peter Rombouts (벨기에 NXP)
ISO/IEC 29167-12	Part 12: Crypto suite ECC-DH security services for air interface communications	FDIS	Frantz Amtmann (오스트리아 NXP)
ISO/IEC 29167-13	Part 13: Air Interface for security services - Crypto suite Grain-128A	FDIS	Jim Springer (미국 EM)
ISO/IEC 29167-14	Part 14: Crypto suite AES OFB security services for air interface communications	DIS 투표 중	강유성 (한국 ETRI)
ISO/IEC 29167-15	Part 15: Air Interface for security services - Crypto suite XOR	2nd CD 투표 중	Hu Yanan (중국 IWCOMM)
ISO/IEC 29167-16	Part 16: Air Interface for security services crypto suite ECDSA-ECDH	DIS 투표 중	Du Zhiqiang (중국 IWCOMM)
ISO/IEC 29167-17	Part 17: Air Interface for security services crypto suite cryptoGPS	FDIS	Claude Tetelin (프랑스 Orange Telecom)
ISO/IEC 29167-19	Part 19: Air Interface for security services crypto suite RAMON	DIS 투표 예정	Klaus Finkenzeller (독일 G&D)
ISO/IEC 29167-20	Part 20: Crypto suite Algebraic Eraser security services for air interface communications	NP 투표 중	Louis Parks (미국 SecureRF)

* WD(Working Draft): 작업 초안

CD(Committee Draft): 위원회표준안

DIS(Draft International Standard): 국제표준안

FDIS(Final Draft International Standard): 최종 국제표준안

IS(International Standard): 국제표준

NP(New Proposal): 신규표준화과제

향후 전망과 국내 대응전략

UHF 수동형 RFID 에어 인터페이스 표준 및 시장의 주도세력은 임핀지(Impinj)와 NXP를 포함한 EPCglobal 멤버들이다. 그러나 EPCglobal 멤버들이 초기에 보안기술 개발과 표준화를 등한시하면서 수동형 RFID 보안기술은 한국이 기술개발 및 표준화에 적극성을 보였고 이어 중국과 프랑스가 관심을 가지고 적극적으로 참여하였다.

EPCglobal 멤버들은 보안기술에 대한 시장의 요구가 커짐을 깨닫고 뒤늦게 기술개발 및 표준화에 뛰어들면서 이미 진행되던 표준화 활동을 뒤엎고 자신들이 주도세력으로 나서고 싶어했다. 이러한 상황에서 기존의 보안기술 표준화 세력과 EPCglobal 세력이 팽팽하게 견제하면서 결국 총 10건의 RFID 보안기술 표준문서가 진행되게 되었다.

표준화 진행 상황이 혼전에 빠지다 보니 시장 역시 어느 표준을 따라야 할지 결정하지 못하고 각 기업들은 자체적인 기술개발과 표준화를 직접 수행하려는 움직임도 생겨났다. 즉 현재의 상황은 시장이 표준을 주도하지 못하고, 표준 또한 시장을 활성화시키지 못하는 악순환의 형태를 보이고 있다. 국제표준화 그룹에서 보기 드문 현상이긴 하지만 동일한 목적을 위해 너무 많은 표준문서가 등장하여 시장에 혼란을 야기시키는 상황임은 틀림없는 사실이다. 이를 극복하기 위해서 결국 각 후보기술에 대한 제품시연 및 호환성 검증 표준제정을 진행하기로 했으며, 이러한 과정을 통해 국제표준화 그룹은 각 표준의 특성을 잘 보여줌으로써 시장의 선택에 도움을 줄 예정이다.

후보기술이 너무 많은 관계로 결국은 서로 견제와 협력 속에 모든 후보기술들은 최종적으로 국제표준으로 채택될 가능성이 크다. 비록 시장과 표준의 괴리가 커져버린 좋지 못한 예를 보이고는 있지만 이를 극복하기 위한 일련의 노력을 펼치고 있으므로 서비스 제공업체와 제조업체 등 시장이 이러한 과정을 살펴보면서 최선의 선택을 할 것으로 예상된다.

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