



# 해외 ICT 표준화 동향

2017. 02

1<sup>st</sup> week

# TTA

## 목차

- |             |   |
|-------------|---|
| <b>본문</b>   | <b>1. Z-Wave 연합, Z-Wave 인증 보안기준(S2) 개정</b>  |
| <b>기타소식</b> | <ul style="list-style-type: none"> <li>- IEEE-SA · AIOTI · oneM2M · W3C, 시멘틱 상호운용성 백서 작업 협력</li> <li>- AMA · DHX · HIMSS · AHA, 모바일 건강 앱 평가 가이드라인 위한 연합 결성</li> </ul> |

\* 게시물 보기

TTA 홈페이지 > 자료마당 > TTA 간행물 > 표준화 이슈 및 해외 동향

# 1. Z-Wave 연합, Z-Wave 인증 보안기준(S2) 개정

(Z-Wave Alliance Announces New Security Requirements for All Z-Wave Certified IoT Devices)

---

보도날짜 2016.11.17.

출 처 Market wired

사 이 트 <http://www.marketwired.com/press-release/z-wave-alliance-announces-new-security-requirements-all-z-wave-certified-iot-devices-2176741.htm>

- 2016년 11월 17일, Z-Wave 연합<sup>1)</sup> 기존 상호운용성 인증 절차의 보안기준(S2) 개정
  - Z-Wave는 무선 홈 제어 기술과 관련하여 ITU 국제표준(G.9959)의 IoT 보안에 대한 상호호환성에 대한 인증으로, 전세계에서 약 1,500개 넘는 상호호환성 제품이 인증을 득하였음
  - Z-Wave은 2017년 4월 2일부터 Z-Wave 인증을 받은 모든 제품에 대해 개정된 '시큐리티 2(S2) 프레임워크'를 의무 적용하기로 결정함
- 지난 몇 년간 Z-Wave 연합은 전세계 모든 가정기기에 IoT 확장을 위하여, 가정과 관련한 장치의 보안을 세계적 수준으로 끌어올리기 위해 노력해왔음
  - 2016년 인텔 시큐리티 조사에 따르면 소비자의 3명 중 2명은 커넥티드 기기의 사이버보안에 대해 걱정하였음
- Z-Wave의 S2 프레임워크는 사이버보안 해킹 전문가와 함께 개발한 것으로 Z-Wave 장치에 새로운 수준의 침투불가 능력을 향상시킨 것임
  - S2는 가정기기 장치와 클라우드 기능에서의 허브 또는 게이트웨이의 커뮤니케이션을 보호함으로써 네트워크에 그대로 접근해 있으면서도 해킹에 대한 피해를 줄일 수 있을 것임
  - S2 프레임워크는 스마트홈기기와 컨트롤러(controllers), 게이트웨이 및 허브에 가장 최신 보안기술을 제공할 것임
  - 또한, 장치에서 자체적으로 QR 코드나 pin 코드를 사용함으로써 네트워크에 고유한 인증을 부여받게 될 것임

---

1) Z-Wave 연합(Z-Wave Alliance): 2005년 1월에 설립된 Z-Wave 표준에 기반한 무선 가전제어 제품 제조사들의 컨소시엄임. 회원사에는 ADT, FAKRO, Ingersoll Rand Nexia Intelligence, Jasco Products, LG 유플러스, Nortek Security & Control, SmartThings and Sigma Designs 등이 있음.

- 보편적으로 사용되는 디피-헬만 타원 곡선(ECDH, Elliptic Curve Diffie-Hellman) 방식<sup>1)</sup>을 사용한 안전한 키 교환 방식을 통하여 '중간자 공격(man in the middle)'이나 무차별 공격(brute force) 등과 같은 일반적 해킹 방식을 무력화할 것임
- Z-Wave는 클라우드 통신을 강화하여 안전한 TLS 1.1 터널을 통해 모든 Z/IP(Z-Wave over IP) 트래픽을 터널링함으로써 취약성을 제거함
- Z-Wave는 기술인증 프로그램은 2005년 Z-Wave 기기를 테스트하고 인증할 목적으로 도입되었으며, 유럽, 미국, 아시아에서 제 3자 테스트 시설에서 작업이 이루어짐
- 커맨드 클래스(command classes), 타이머(timer), 기기 타입을 정확히 구현하는지에 대해 S2 보안 솔루션들이 잘 시행되는지 확인할 것임



---

1) 디피-헬만 타원 곡선(ECDH, Elliptic Curve Diffie-Hellman): 각 타원 곡선 공개-개인 키(key) 페어(pair)가 비보안 채널을 통해 공유된 비밀들을 마련하기 위한 익명의 키 동의 프로토콜임. 공유된 비밀은 직접 하나의 키로 사용되거나 대칭된 키 암호를 사용하여 연속(후속) 통신을 암호화하는데 사용될 수 있는 다른 키를 파생시킬 수 있음 (출처: 위키백과)

## 기타 소식

### IEEE-SA · AIOTI · oneM2M · W3C, 시멘틱 상호운용성 백서 작업 협력

- ▶ 출처 : [http://standards.ieee.org/news/2016/semantic\\_interoperability.html](http://standards.ieee.org/news/2016/semantic_interoperability.html) (2016.12.20)
- 2016년 12월 20일, IEEE-SA, AIOTI, oneM2M, W3C, 시멘틱 상호운용성에 대한 백서 발간<sup>1)</sup> 작업에 협력하기로 함
  - 본 백서에서는 IoT 분야의 시멘틱 상호운용성의 중요성을 강조하며 각 기관 및 이해관계자와의 협업을 통해 IoT 분야의 공통된 로드맵을 개발할 것임

### AMA · DHX · HIMSS · AHA, 모바일 건강 앱 평가 가이드라인 위한 연합 결성

- ▶ 출처 : <https://www.ama-assn.org/alliance-forms-develop-guidelines-evaluation-mhealth-apps>(2016.12.12)
- 2016년 12월 12일, 모바일 건강 앱의 평가를 위한 가이드라인 마련을 위하여 미국건강협회(AHA), 미국의학협회(AMA), DHX 그룹, 건강관리와 정보관리시스템연합(HIMSS)이 협력하기로 함

1)백서 요약:

[https://www.researchgate.net/publication/307122744\\_Semantic\\_Interoperability\\_for\\_the\\_Web\\_of\\_Things?channel=doi&linkId=57c1df6008aeda1ec38cf5f5&showFulltext=true](https://www.researchgate.net/publication/307122744_Semantic_Interoperability_for_the_Web_of_Things?channel=doi&linkId=57c1df6008aeda1ec38cf5f5&showFulltext=true)