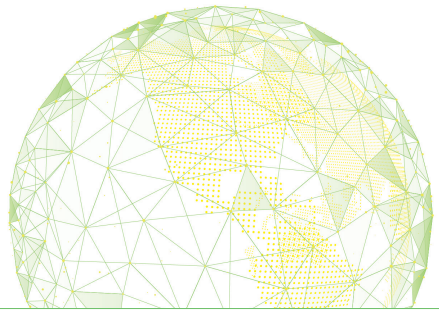
# 해외 표준화기구 동향

TTA 표준화본부 표준기획단



## 1. 지역 및 국가별 표준화기구 동향

### 1.1 유럽

#### 1.1.1 ETSI, ETSI TS 103 457 사이버 보안 규격 발표[1]

2019년 2월 7일, ETSI 사이버 기술위원회(TC CYBER)는 'ETSI TS 103 457(CYBER; Trusted Cross-Domain Interface: Interface to offload sensitive functions to a trusted domain)' 사이버 보안 규격을 발표하였다.

* ETSI TS 103 457은 직접적인 통제 하에 있지 않은 클라우드를 사용하면서 고객 데이터를 보호하고 안전한 스토리지와 관련된 문제를 해결하고 있다.

데이터를 보호할 때 가상 네트워크 또는 클라우드에 보관된 경우 스토리지 솔루션을 제어하지 못하는 어려움이 있으나 TS 103 457은 신뢰할 수 있는 '안전한 볼트(secure vault)'와 볼트에 저장된 민감한 데이터가 있는 클라우드 사이의 인터페이스를 표준화하여 이 문제를 해결한다.

ETSI TS 103 457 규격은 다양한 유스케이스를 제공하고 있다. 이 인터페이스는 새로운 네트워크 기능 가상화(NFV, Network Function Virtualization) 기술과 함께 사용되어 사용자를 안전하게 인증하며, 이 인터페이스를 사용하여 개인적인 데이터를 검색하여 보호한다. 이 규격의 로깅(logging) 기능을 통해 데이터 유출을 쉽게 감지하여 악의적인 활동을 방지하며 기업이 '볼트(Vault)' 또는 클라우드 제공자를 변경하거나 이전과 동일한 기능을 수행할 수 있도록 새로운 상호 운용 가능한 인터페이스를 제안한다.

### 1.2 미국

#### 1.2.1 TIA, IoT 커뮤니티, 사물인터넷과 스마트빌딩 개발 가속화 합의 발표[2]

2019년 1월 17일, TIA(Telecommunications Industry Association, 미국통신산업협회)와 IoT Community는 IoT(Internet of Things, 사

* TTA는 해외 표준화기구의 최신 동향을 조사하여 주간/월간으로 '해외 ICT 표준화 동향 정보'를 제공하고 있습니다. 본 원고는 2019년 1월 말부터 2019년 3월 초까지 게재한 정보를 요약 정리하였습니다.

물인터넷)의 디지털 전환과 스마트빌딩 개발을 가속화하기로 합의했다고 발표하였다.

* IoT Community는 영국에 본사를 두고 있는 비상장 기업으로 22,000명이 넘는 고위 비즈니스 리더 및 IoT 전문가로 구성된 CXO 커뮤니티이다. 2016년에 설립된 이 공동체는 상업 환경에서의 IoT 채택 및 적용에 중점을 두고 기술 적용에 대한 이해와 기여를 모색하며 다양한 장벽, 기술 및 운영 문제 등을 극복하는 데 초점을 두고 있다.

두 기구는 스마트빌딩, 제조, 커넥티드 차량(Connected Vehicels), 지능형교통(Intelligent Transportation), 건강관리 등에 관한 이니셔티브 협력을 위해 MoU(Memorandum of Understanding, 양해각서)를 체결하였다. 향후, TIA와 IoT Community는 상업, 기술 및 표준화 통찰력을 공유하고 기술 협력, 정보 및 전문 지식 교환 기회를 모색하여 IoT 개발을 가속화하는 솔루션을 개발할 예정이다.

TIA와 IoT Community는 스마트빌딩, IoT 및 기타 관심 분야와 관련된 기술을 공유하고 토론·탐구하기 위해 함께 노력할 것이라고 밝혔다. 또한, 이러한 목표에 따라 관련된 IoT 및 이니셔티브의 교육 내용을 개발하고 공유할 것이며, 건물에서 사용하는 IoT 역할에 대해 교육하고, 관련 행사를 협력하며 연구 및 전문 지식을 공유할 것이라고 강조하였다.

### 1.2.2 TIA, 에지 데이터 센터의 표준 개발을 위한 태스크그룹 신설 발표[3]

2019년 2월 7일, TIA(Telecommunications Industry Association, 미국통신산업협회)는 에지 데이터 센터(Edge Data Center)의 산업표준 개발을 위한 태스크그룹(TG, Task Group) 신설을 발표하였다. TR-42.1 구내 통신 인프라구조 소위원회(Premises Telecommunications Infrastructure Subcommittee) 산하의 태스크그룹 신설을 통해 TIA는 5G 기술 도입을 가속화할 것으로 기대된다. 에지 데이터 센터는 빠르고 신뢰할 수 있는 정보를 제공하기 위해 사용자가 요구하는 영역에 정보를 제공하며 사이버 보안, 물리적 보안, 위치, 연결성 및 복원력과 같은 문제를 해결하는 표준 및 프로그램을 개발할 계획을 밝혔다. 이번에 신설된 에지 데이터 센터의 태스크그룹은 통신 인프라 구조에 대한 참조 아키텍처, 지침, 모범 사례 및 산업 표준을 제공할 계획이다.

### 1.2.3 NIST, 스마트제조를 위한 보안과 추적을 제공하는 블록체인[4]

2019년 2월, NIST(National Institute of Standards and Technology, 미국국립표준기술연구소)는 스마트제조를 위한 보안과 추적성을 제공하는 블록체인 기술에 대한 보고서를 발표하였고 스마트제조 시스템에 있어서 블록체인을 이용한 디지털 스레드(Digital Thread) 프로젝트를 소개하였다.

이 보고서에 따르면 블록체인을 이용한 보안 시스템은 제조 데이터의 변조 방지 전송 기능을 제공할 뿐만 아니라 생산 과정에서 사용자에게 추적 가능한 정보를 제공하여 블록체인을 통해 디지털 제조 네트워크의 신뢰성을 높일 수 있다고 언급하였다. 또한, 스마트제조 네트워크에 블록체인을 적용하는 데 필요한 컴퓨터 모델링 시스템인 UML(Unified Modeling Language, 통합 모델링 언어)에 대해 자세히 설명하고 있다. 디지털화된 과정을 통해 생산된 제품은 각 수명주기 단계마다 데이터를 생성하기 때문에 제품 수명주기 동안 지속적으로 생성된 데이터

의 원활한 흐름이 중요해진다. 따라서 이 기간 동안 블록체인을 통해 안전하게 정보를 보호하며 전달하도록 도와주는 것을 디지털 스레드(Digital Thread)라고 한다. 디지털 스레드는 설계에서 제조에 이르기까지 정보가 컴퓨터에서 컴퓨터로, 기계에서 기계로 전달될 때 제품의 설계 및 제조 정보를 오류 없이 작성, 교환 및 처리할 수 있는 방법을 파악하여 제공한다. 사용자는 데이터를 주고받는 사람, 데이터를 교환하는 사람, 교환이 이루어지는 시기, 교환되는 대상 및 방법 등 각 단계에서 인증된 블록을 이용하게 된다. NIST는 스마트제조를 위한 블록체인 사용을 촉진하고 홍보하기 위해 노력하고 있다.

#### 1.2.4 NIST, PQC(포스트-양자암호) 26개 후보 알고리즘 공개[5]

2019년 1월 30일, NIST(National Institute of Standards and Technology, 미국국립표준기술연구소)는 양자컴퓨팅 환경에서 안전한 암호 알고리즘으로 정보를 보호할 수 있는 일련의 표준을 만들기 위한 프로젝트의 일환으로 26개의 후보 PQC(Post-Quantum Cryptography, 포스트-양자암호) 알고리즘을 발표하였다.

* 양자컴퓨팅을 실행할 수 있는 양자컴퓨터를 이용할 수 있더라도 그 암호의 안전성이 본질적으로 쉽게 해독되지 않는 암호를 '포스트-양자암호'라 한다.

2017년 11월 NIST에 제출된 82건의 알고리즘 후보를 검토하는 첫 번째 단계에서 69건이 최소 수용기준과 요구사항을 모두 충족하였고, 이중 PQC 후보 알고리즘으로 2019년 1월에 26개가 선정되었다. 포스트-양자암호 중 공개키 암호 후보로 언급되는 것은 Lattice-based cryptography(격자기반암호), Code-based cryptograph(코드기반암호), Multivariate cryptography(다변수암호) 등이 있다.

NIST PQC 표준화 과정 단계가 완료되고 나면 선정된 PQC 후보 알고리즘은 NIST에서 양자공격에 취약한 것으로 간주되는 세 개의 표준(FIPS 186-4, NIST SP 800-56A 및 NIST SP 800-56B)을 보완하거나 대체할 것이라고 언급하였다. PQC 표준화는 AES나 SHA-3 표준화와 같이 하나의 표준 알고리즘이 아닌 여러 개의 알고리즘을 제정하는 방향으로 진행될 것으로 예상된다. 26개의 후보 알고리즘을 검토하는 이번 단계에서는 광범위한 시스템 전반에서 이 알고리즘이 외부 공격에 대응하는 성능을 평가하는 데 더욱 중점을 둘 예정이며, 대형컴퓨터와 스마트폰뿐만 아니라 프로세서 기능이 제한적인 장치에서도 이 알고리즘이 어떻게 작동하는지 검토할 예정이다.

### 1.3 중국

#### 1.3.1 중국, 단체표준관리규정 최종버전 발표[6]

2019년 1월 29일, SAC(Standardization Administration of China, 중국국가표준화 관리위원회)와 MCA(Ministry of Civil Affairs, 민정부)는 단체표준관리규정(Management Regulations for Association Standards)의 최종 버전을 공동으로 발표하였다.

새로운 단체표준관리규정은 중국의 개정된 중국표준화법을 시행하고, 중국 표준화 개혁을 심화시키는 토대로 마련되었다. 최신 규정은 5장(chapter)으로 구성되어 단체 표준의 수립, 구현과 감독을 수월하게 하는 새롭고 간소화된 프로세스를 수립하였다. 특히, 첫째 협회 표

준 개발의 우선 목표를 신기술, 신사업, 신규 비즈니스 유형과 모델을 포함하기 위한 새로운 시장 니즈를 충족시키는 표준이 개발되어야 함을 제안하였고 둘째, 협회가 공개한 플랫폼을 통해 표준 정보를 공개하고 투명하게 만들어져야 함을 권장하고 있다. 또한, 규정 6조는 국무원(State Council)에 협회 표준에 대한 자체 공개와 감독 메커니즘 시행을 요구하고 있으며, 표준화 연구소가 표준 개발, 인력 양성 및 기술자문과 관련된 전문 서비스를 수행하도록 지시하였다.

## 2. 사실표준화 기구 동향

### 2.1 DMTF, PMCI 보안을 위한 새로운 아키텍처 공유[7]

2018년 12월 17일, DMTF(Distributed Management Task Force, 분산관리작업단체)의 PMCI(Platform Management Components Intercommunication, 플랫폼관리요소 상호통신) 보안TF(Task Force)는 'PMCI 표준 및 프로토콜을 위한 보안(Security Proposal for PMCI Standards and Protocols)'을 발표하였다. 이 새로운 아키텍처는 차세대 보안 규격에 대한 세부 정보를 담고 있다.

PMCI 표준 및 프로토콜에 대한 추가 보안 규격은 업계 전반의 구성 요소 인증 및 무결성 개체를 지원하는 목표를 두고 있으며 다른 표준화 기구가 참조 가능하도록 설계되었다.

PMCI의 새로운 아키텍처에는 모든 인증 명령에 대해 DMTF의 MCTP(Message Transport Format, 메시지 전송 포맷) 메시지 유형 5를 사용하는 규격의 기본 원칙에 대한 자세한 내용이 설명되어 있으며, 미래의 보안 전송을 위해 MCTP 메시지 유형 6을 적절하게 사용하고 있다.

- USB Type-C 형식 활용
- 완료 코드 필드 없음, 요청/응답 코드를 사용하여 오류 전달
- 바이트를 최적화하지 않도록 함
- USB Body를 적절하게 참조하고 적절한 곳까지 확장

PMCI 보안 TF팀은 MCTP 외에도 NC-SI(Network Controller-Sideband Interface) 및 PLDM(Platform Level Data Mode) 규격을 개발 중이며, 관리 서브시스템 구성요소 간의 향상된 통신을 위한 포괄적인 공통 아키텍처를 제공한다.

### 2.2 OGC, NGFR(차세대 긴급 구조원)에 대한 정보 요청서 발표[8]

2019년 1월 15일, OGC(Open Geospatial Consortium, 개방형 공개정보 컨소시엄)는 DHS S&T(Department of Homeland Security Science and Technology Directorate, 미국 국토 안보부 과학 기술부서)가 개발한 NGFR(Next Generation First Responder, 차세대 긴급 구조원)에 대한 상용제품의 실현 가능성에 관한 정보 요청서를 발행하였다.

DHS S&T는 개발, 설계, 테스트 및 통합을 지원하기 위해 상업적으로 개발된 기술을 수행할 수 있는 '플러그 앤 플레이' 표준 기반 환경을 요약한 NGFR 통합 핸드북을 만들었으며 NGFR Apex 프로그램은 구조원(responder)의 요구사항을 처리할 수 있는 상호 운용 가능한 기술 개발을 장려하는 것을 목표로 하고 있다. NGFR Apex 프로그램은 비상 대응, 구조원의 안전 및 상황 인식 개선을 위해 최신 및 신기술을 통합

함으로써 개방형 표준을 사용하여 향상된 데이터 분석 및 경보를 구조원과 연결하여 안전한 보호와 인식을 높이는 아키텍처를 개발하였다.

### 2.3 FIDO Alliance, '2019 강력인증 현황보고서' 발표[9]

2019년 1월 22일, FIDO Alliance는 Javelin Research에서 연구한 '2019 강력인증 현황보고서(The State of Strong Authentication 2019)'를 발표하였다. 30페이지 분량의 이 보고서에는 온라인 피싱 공격 방지를 위한 계정보호와 데이터 및 시스템 접근을 안전하게 보장하는 강화된 인증 역할에 대해 설명하고 있다.

이번 보고서에는 강력인증이 2017년부터 급속히 증가했으며, EU와 미국 캘리포니아 주에서 실시한 데이터보호규정과 PSD2(Payment Service Directive2, 지불서비스 지침)의 도입으로 강력인증 채택에 대한 규제가 강화되고 있음을 시사하고 있으며 표준 기반의 강화된 인증 솔루션을 채택하고 FIDO 인증과 같은 암호화된 보안 방식을 사용하면 점점 정교해지는 피싱을 따라 잡는 데 드는 비용을 줄일 수 있다고 강조하고 있다. 실제 이번 보고서에는 Google, Tradelink 및 Visa의 사례 연구가 포함되어 있으며 FIDO 인증을 활용하여 데이터를 보다 강력하게 보호하는 사례를 설명하고 있다. FIDO Alliance의 브렛 맥도웰(Brett McDowell) 전무이사는 이번 연구가 FIDO Alliance 및 W3C의 업계 표준을 준수하는 새로운 암호 기반 인증에 대한 인식을 높이는 결과를 가져올 것으로 기대한다고 밝혔다.

### [참고문헌]


[1] https://www.etsi.org/newsroom/press-releases/1545-2019-02-etsi-releases-cybersecurity-specification-to-secure-sensitive-functions-in-a-virtualized-environment

[2] https://www.tiaonline.org/press-release/tia-and-iot-community-announcepartnership-to-accelerate-smart-buildings-and-the-internet-of-things/

[3] https://www.tiaonline.org/press-release/tia-launches-task-group-to-develop-industry-standards-for-edge-data-centers/

[4] https://www.nist.gov/news-events/news/2019/02/nist-blockchain-provides-security-traceability-smart-manufacturing

[5] https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals

[6] https://www.ansi.org/news_publ-cations/news_story?menuid=7&articleid=131d08ec-3cb8-47e8-b1fe-f62e2634d2b2

[7] https://www.dmtf.org/content/dmtf-shares-new-architecture-pmci-security

[8] http://www.opengeospatial.org/pressroom/pressreleases/2932

[9] https://fidoalliance.org/new-report-shows-data-breaches-phishing-and-regulations-driving-rapid-adoption-of-strong-authentication/


### [주요 용어 풀이]

- DMTF(Distributed Management Task Force, 분산관리 작업단체): ICT 시스템 자원 관리 분야의 표준화를 진행하는 산업 표준 단체. 미국의 인텔, IBM, DEC, 휴렛 팩커드, 마이크로소프트 등 8개사가 1992년에 결성하여 Desktop Management Task Force(DMTF)라 부르다가 가상화 기술이 실용되면서 이를 수용하기 위한 조직으로 변모되면서 명칭도 Distributed Management Task Force(DMTF)로 변경하고 다수의 관련업체가 참여하는 단체로 발전하였다.
- 네트워크 기능 가상화(NFV, Network Functions Virtualization): 네트워크의 방화벽, 트래픽 부하 제어 관리, 라우터 등과 같은 하드웨어 장비의 기능과 처리 기능을 서버단에서 소프트웨어로 구현하는 기술이다.