

2019년 6월 넷째주

해외 ICT 표준화 동향

목 차

본문

1. ETSI 오픈소스 표준 Rel6(Open Source MANO OSM Rel 6) 발표
2. CEN/CENELEC, 제 15차 연례회의에서 유럽표준의 청사진 논의
3. FIDO Alliance, 2개의 새로운 WG 신설 발표

※ 게시물 보기

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

TTA 한국정보통신기술협회
Telecommunications Technology Association

1. ETSI 오픈소스 표준 Rel 6 (Open Source MANO OSM Rel 6) 발표

ETSI OSM Release SIX enhances Edge support and lets your Network Service fly

보도날짜 19. 6. 20.
출 처 ETSI
사 이 트 https://www.etsi.org/newsroom/press-releases/1616-etsi-osm-release-six-enhances-edge-support-and-lets-your-network-service-fly

◆ 2019년 6월 20일, ETSI OSG(Open Source Group) OSM(Open Source MANO)은 OSM Rel 6를 발표함

* 2016년 2월 22일, ETSI는 세계 이동통신 산업전시회인 Mobile World Congress(MWC)에서 오픈소스그룹(OSG)인 Open Source MANO(OSM)의 신설을 발표함
* OSM은 오픈소스를 기반으로 하여 NFV(Network Function Virtualization, 네트워크 기능 가상화)[1] MANO(Management and Orchestration)의 구현을 위해 ETSI에서 지원하는 프로젝트이며 NFV-MANO는 NFV의 자원을 생성 및 관리, VNF(Virtualized network functions, 가상화 네트워크 기능) 관리 등을 수행함

◆ OSM Rel 6는 HetNet(heterogeneous networks, 이종 네트워크) 및 클라우드 기술 전반에 걸쳐 엔드-투-엔드 오케스트레이션(Orchestration)[2]을 제공 할 수 있는 새로운 기능을 제공

- Rel6는 네트워크 서비스 primitive의 확장된 기능과 서비스보증(SA, Service Assurance) 프레임워크의 확장으로 인해 복잡한 서비스 관리가 이전보다 수월해졌으며, OSM이 지원하는 기본 기술 범위를 더욱 넓혀줌

- FOG05 Edge Cloud, TAPI 기반 전송 네트워크, VMware의 vCloud Director 9.5 및 공용 클라우드를 위한 새로운 커넥터가 개발됨

1) NFV(Network Function Virtualization, 네트워크 기능 가상화) : 네트워크의 방화벽, 트래픽 부하 제어 관리, 라우터 등과 같은 하드웨어 장비의 기능과 처리 기능을 서버단에서 소프트웨어로 구현하는 기술. 네트워크 기능 가상화(NFV) 프레임워크는 크게 VNF(Virtualized network functions), NFVI(NFV infrastructure), NFV-MANO 아키텍처 프레임워크(NFV management and orchestration architectural framework)로 구성된다. VNF는 여러 응용 프로그램을 지원하는 네트워크 기능들의 집합이며, NFVI는 컴퓨터 프로세싱, 스토리지, 네트워킹 자원을 가상화하고 VNF 실행을 지원한다. [출처: TTA 정보통신용어사전]
2) 오케스트레이션(orchestration) : 일부 유용한 기능을 구현하기 위해 한 웹서비스가 다른 웹서비스를 호출하는 순서와 조건을 정의한다. [출처: TTA 정보통신용어사전]

- 지원을 개선하기 위해 추가적인 EPA(Enhanced Platform Awareness) 속성을 지원하고, 멀티 세그먼트 네트워크를 추가함으로서 이전 릴리스에서 이용 가능한 커넥터에 여러 가지 개선 사항이 추가됨

2. CEN/CENELEC, 제 15차 연례회의에서 유럽표준의 청사진 논의

AT THEIR ANNUAL MEETING, CEN AND CENELEC PRESENT THE WAY FORWARD FOR EUROPEAN STANDARDIZATION

보도날짜 19. 6. 14.
출 처 CEN
사 이 트 https://www.cencenelec.eu/News/Press_Releases/Pages/PR-2019-05.aspx

◆ 2019년 6월 5일부터 6일까지, CEN과 CENELEC은 루마니아 부쿠레슈티(Bucharest)에서 열린 제 15차 연례회의에서 유럽 표준의 지금까지의 성과를 평가하고 미래 나아가야 할 방향과 우선순위를 논의함

◆ 2019년 6월 6일은 CEN과 CENELEC 회원국들은 각각 따로 만나 구체적인 조직적, 절차적 요소를 논의한 뒤 공동 이익에 관한 문제를 논의하기 위한 공동 세션을 개최하였으며, 공동 세션에서 CEN과 CENELEC 담당자는 유럽 표준화와 관련된 주요 전략, 정책 및 기술적 문제에 대해 보고함

◆ CEN과 CENELEC 총회는 미래 발전을 위한 다음의 몇 가지 중요한 조치와 결정을 승인함

- 유럽 위원회와의 협력 강화를 위한 노력의 일환으로, 일치된 표준 개발 과정의 성과에 대한 적절한 모니터링을 위해 공동 KPI가 제안됨

- 국제적인 맥락에서 유럽 시스템의 강점을 고려하기 위해 'Strategy beyond 2020'에 대한 논의를 계속하기로 결정하였고, 2019년 7월 17부터 18일까지 'Strategy beyond 2020' 특별 워크숍 개최 예정임

- CEN과 CENELEC의 디지털 전환 전략(Digital Transformation Strategy)의 일부인 IT 프로젝트와 시범사업 등의 포괄적이고 효율적인 관리를 위해 새로운 DITSAG (Strategic Advisory Group on Digital and Information Technology, 디지털 정보기술의 전략자문그룹)를 설립

- CEN과 CENELEC은 ETSI와의 협력을 더욱 강화하고자하는 목표를 확인함

◆ 사이버보안과 표준화에 대한 심도 깊은 논의도 진행되었음

- 사이버 보안 인증 프레임워크에서, CEN과 CENELEC은 사이버 보안이 비즈니스, 정책결정자에게 도움이 되는 사이버보안과 표준화에 대한 논의와 과제를 심층적으로 분석하였으며, 안전하고, 접근 가능하고, 신뢰할 수 있는 새로운 기술을 만들기 위해 표준화가 기여할 수 있는 몇 가지 방법을 제안함

- 사이버 보안과 관련하여 EU는 2018년 말에 ICT 제품, 시스템 및 서비스에 대한 유럽의 공통 사이버 보안 인증 프레임워크를 구축하여 사이버 공격에 효과적으로 대응할 수 있는 능력을 확보하는 것을 목표로 자체적인 '사이버 보안법[3]'을 제안한바 있음

3) https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en 참고

3. FIDO Alliance, 2개의 새로운 WG 신설 발표

FIDO Alliance Announces New Identity Verification and IoT Initiatives to Expand the Reach and Impact of FIDO Authentication

보도날짜 19. 6. 26
출 처 FIDO Alliance
사 이 트 https://fidoalliance.org/fido-alliance-announces-id-and-iot-initiatives/

◆ 2019년 6월 26일, FIDO Alliance는 IoT(Internet Of Things, 사물인터넷)와 본인인증에 관한 표준 기술 규격 및 시험인증 프로그램 개발 준비를 위한 두 개의 워킹그룹의 신설을 발표함

◆ 두 개의 워킹그룹은 다음과 같음 : 'IoT TWG(IoT 기술 워킹 그룹, IoT Technical Working Group)'과 'IDWG(본인 인증 및 바인딩 워킹그룹, Identity Verification and Binding Working Group)'

- IoT TWG는 2020년 약 200억개 이상의 사물이 연결될 것으로 예측되는 사물인터넷 시장에 종합적인 인증 프레임워크를 제공하여 부족한 사물인터넷 보안 표준 그리고 이들이 운영되는 네트워크와 프로세스 상에서 야기될 수 있는 대규모 해킹공격에 대한 우려를 해결하고자 함

- IDWG는 원격 신원 확인 기준을 정의하고 시험인증 프로그램과 교육 자료를 개발해 FIDO 인증장치를 분실하거나 도난당한 경우 계정 복구 프로세스가 사용자 계정의 무결성을 유지 역할을 할 예정임

◆ Fido Alliance는 신규로 신설된 두 개의 WG을 통하여 해당 분야의 가이드라인과 시험인증 기준을 세워 본인 증명 강화를 통해 계정 복구 프로세스를 개선하고자 함

- 또한, IoT 환경에서 비밀번호 사용을 제거하기 위해 온보딩(Onboarding)을 자동화 하고자 하는 목표를 두고 있음