



2020년 6월 셋째주

해외 ICT 표준화 동향

목차

20.05.05 EU, ICT 표준화 롤링플랜 2020 발표

금주 표준화 동향에서는 EU(유럽연합)에서 발표한
"ICT 표준화 롤링플랜 2020" 중 우선순위 분야인
5G, 클라우드, 사이버보안, 빅데이터, IoT에 대한 요약 정보를 제공합니다

※ 게시물 보기

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

EU, ICT 표준화 롤링플랜 2020

(Rolling Plan for ICT Standardisation 2020)

<https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2020>

- EC(유럽연합 집행위원회)는 지난 5월 5일 'ICT 표준화 롤링플랜 2020'을 발표. 롤링플랜을 통해 매년 ICT 주요 분야에 대한 유럽연합의 정책과 글로벌 표준화 동향을 분석하여 활동 방향을 제시하고 있음
- 본 롤링플랜에서는 핵심요소(Key enabler) 및 보안, 사회적 과제, 유럽 단일시장을 위한 혁신, 지속가능한 성장 등 4가지 주제를 바탕으로, 총 165개의 활동 아이টে를 제시함
- 특히, 핵심요소 주제로 ICT 표준화 우선순위 5개 분야를 매년 포함하고 있음. 유럽연합은 '16년 디지털 단일시장을 위해 ICT 표준화가 가장 시급한 5대 분야로 5G, 클라우드, 사이버보안, 빅데이터, IoT를 꼽은 바 있음¹⁾.

※ 본 문서에서는 위 우선순위 5개 분야에 대한 정책과 활동 아이টে를 위주로 정리함

1. 5G

■ 정책 목표

- 2015년부터 시작한 유럽 디지털 단일시장(DSM) 전략과 2016년 7월 “유럽의 기가비트 사회를 위한 연결성” 통신문을 통해 5G와 같은 대용량 네트워크는 향후 글로벌 경쟁력의 핵심 자산으로 정의한 바 있음
- 3GPP Release 15 규격으로 5G 표준화의 1단계가 완료되었고, 3GPP Release 16를 통해 2단계 표준화가 진행 중이며, 2020년 3월까지 완료될 것으로 예상됨. EC는 해당 목표 달성을 위해 2013년 말 5G 민관 협력체(5G-PPP)를 출범시킴(*Release 16은 COVID-19 영향으로 일정 조정이 있음)
- 5G는 비(非)ICT 산업 부문에도 디지털 비즈니스 모델을 통해 융합의 새로운 물결을 만들 것으로 예측됨. 이러한 맥락에서 유럽연합은 5G를 산업계의 디지털화 및 DSM 전략의 광범위한 목표 달성을 위한 핵심 인프라로 인식하고 있음
- 5G 네트워크의 다양한 이점과 함께 공공 및 내부 보안 영역과 관련된 많은 과제와 우려 또한 존재함. “보호하는 유럽”의 맥락에서 EC는 5G 네트워크를 전략적 자산으로 식별함에 따라 높은 사이버보안 표준²⁾과 합법적인 조사 기능³⁾을 요구하고 있으며, 이러한 목표 달성을 위해 공공 및 내부 보안 분야에서 법 집행기관 및 기타 관련 기관의 요구는 진행 중인 5G 표준화 활동을 고려하여 조정된 접근이 이뤄져야 함

1) Communication on ICT Standardisation Priorities for the Digital Single Market (COM (2016) 176 final).

2) Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks

3) 8268/19 11 April 2019, Position paper on 5G, Europol

■ EC의 전망과 현황

- 3GPP의 5G 표준 첫 단계는 향상된 모바일 광대역 통신에 초점을 맞추는 동시에 초고신뢰(ultra-reliability) 및 저지연(low latency)을 지원함. 두 번째 단계는 산업용 애플리케이션과 관련된 유스케이스 또는 법적 감청(lawful interception)과 같은 횡단적 요구 유스케이스에 대한 표준을 제공해야 함. 이러한 부분에서 오픈 이노베이션을 촉진하는 표준의 가용성과 스타트업의 기회도 중요할 것으로 예상됨
- EC는 회원국 및 산업계에 다음과 같은 목표 달성을 요구해 왔음
 - 2019년 말까지 미래 발전 역량을 유지하며 5G 글로벌 표준의 가용성을 목표로 하는 표준화 접근법
 - 글로벌 표준화 기구내에서 무선 접속 및 핵심망 분야를 함께 다루며 혁신적인 유스케이스를 포괄하고 개방형 혁신을 촉진하는 총체적 표준화 접근법
 - 늦어도 2017년까지 산업 간 파트너십을 구축하여, 부분적으로 국제 협력 파트너십을 활용한 시기적절한 표준 제정을 지원하며, 특히 산업의 디지털화를 지향
- 5G 개발에 따른 우려사항도 파악된 바 있음. 특히 범죄를 탐지하고 조사하기 위한 법 집행 기관의 적절한 기능을 보장하기 위해 법적 감청에 대한 만일의 사태에 대비할 필요가 있음. 이를 위해 법 집행기관이 5G 통신망에서도 합법적인 법적 감청을 요청할 수 있도록 적절한 기술적 수단을 마련하는 것이 무엇보다 중요함. 이와 관련하여, 지금까지 적절한 표준화 활동으로 이점을 얻을 수 있는 4가지 주요 도전 과제가 확인되었으며 아래와 같음
 - 새롭게 강화된 5G 보안 기능에서도 IMSI(SIM에 저장된 가입자 고유번호) 식별 가능
 - 5G의 단편화 및 가상화에서도 감청된 통신의 전체 복사본을 활용 가능
 - 감청된 통신의 클리어 복사본 활용 가능(5G 기본 암호화만 고려하고 있으며 OTTs 암호화는 고려대상이 아님)
 - 법적 감청 시스템의 기밀성 보장. 물리적으로 분리되어 있으면서도 5G 네트워크에서 논리적 구성요소가 될 수 있다는 점을 고려

■ 활동 아이템

- 활동 아이템 1 : 글로벌 산업 표준. EU의 리더십을 바탕으로 주요 5G 기술(무선 접속망, 핵심망)과 네트워크 아키텍처에 대한 글로벌 산업 표준의 출현을 촉진하며, 이는 EU와 핵심적 국제표준화기구(3GPP, ITU, ETSI NFV)에서의 5G 민간협력 결과 활용을 통함
- 활동 아이템 2 : High-level 이벤트. 5G 표준이 수직적 산업의 혁신적인 유스케이스와 호환함을 보장. 특히 분야별 니즈를 가진 산업계의 광범위한 참여와 타 산업 분야의 표준 개발 기구와 긴밀한 협력을 통해 5G 표준화기구에서 이뤄짐
- 활동 아이템 3 : 법적 감청 관련 표준. 법적 감청 메커니즘을 가능하게 하는 적절한 규정을 보장하는 표준 개발을 촉진. 이는 5G 네트워크의 맥락을 가지며, 5G 표준화 관련 위원회(ETSI TC LI, 3GPP SA3-LI 등)에 법 집행권자 참여를 독려 및 조율하고 유럽의 접근방식을 홍보

2. 클라우드 컴퓨팅

■ 정책 목표

- 클라우드 컴퓨팅을 위한 일관된 프레임워크와 기준은 구축은 디지털 어젠다의 핵심 우선순위 중 하나였음. 디지털 단일시장 전략에서 클라우드 컴퓨팅의 중요성을 확인하고 있으며, 디지털 기술, 혁신 향상, 디지털 단일시장, 콘텐츠 접근성 구현에 있어 패러다임 전환을 주도하고 있음

■ EC의 전망과 현황

- 클라우드 컴퓨팅의 핵심 역할은 “유럽 클라우드 이니셔티브”와 “유럽 데이터 경제 구축 이니셔티브”를 통해 제시되었음. 클라우드 컴퓨팅 분야는 빠르게 발전하고 있으며, 이러한 발전으로 인해 2013년 95억 유로의 유럽 클라우드 시장이 2020년에는 448억 유로로 성장할 수 있을 것으로 추산되며, 이는 2013년 시장 규모의 거의 5배에 달하는 규모임. 2018년 말 발표된 Eurostat 데이터를 통해 현재 기업 클라우드 컴퓨팅 사용에 관한 EU의 상태를 파악할 수 있으며, 주요 결과는 아래와 같음⁴⁾
 - EU 기업의 26%가 2018년 이메일 시스템을 호스팅하고 파일을 전자형태로 저장하는 데에 클라우드 컴퓨팅을 사용함
 - 이러한 기업의 55%는 재무 및 회계 소프트웨어 애플리케이션, CRM(고객 관계 관리) 또는 컴퓨팅 성능을 비즈니스 애플리케이션을 실행하는 데 사용하는 것과 관련된 고급 클라우드 서비스를 사용함
 - 2018년에는 사설클라우드서버(11%)보다 공용클라우드서버(18%)를 더 많이 사용함 (전용 인프라를 사용하는 기업이 다수)
 - 2014년에 비해 특히 대기업에서 클라우드 컴퓨팅 사용이 증가함 (+21%p)
- 클라우드 컴퓨팅 시장의 발전과 클라우드 서비스의 효율적인 제공은 특히 규모의 경제를 구축할 수 있는 능력에 달려 있음. 디지털 단일시장은 클라우드 컴퓨팅의 유럽의 잠재력을 최대한 발휘하는데 필요한 규모로 만들 것임
- 데이터보호에 대한 제29조 작업반(Article 29 data protection working party)에서는 2012년 “클라우드 컴퓨팅에 관한 견해”를 발표함. 위 문서에서는 클라우드 컴퓨팅 서비스의 광범위한 구현이 유발할 수 있는 데이터보호 위험, 개인 데이터 통제 결여, 처리된 방법, 위치, 사용자에 대한 불충분한 정보 등을 간략히 설명하고 있음
- ICT 표준화 우선순위에 대한 통신문에서는 몇가지 조치를 제안하고 있음. 조치 중에는 2012/2013에 시작된 클라우드 표준 조정의 후속조치가 있으며, 이는 EC에서 이해관계자들을 조율하기 위해 필요한 표준에 관한 상세맵(보안, 상호 운용성, 데이터 이동 및 변경 가능성 등)을 ETSI에 요청한 것임
- C-SIG(Cloud Select Industry Group, 클라우드선택산업그룹)은 클라우드 컴퓨팅 이슈에 큰 관심을 가지고 유럽 클라우드 시장에서 활발하게 활동하고 있는 모든 기관, 그룹 및 개인에게 개방되어 있음. “유럽에서 클라우드 컴퓨팅의 잠재력을 펼치다 (2012)” 통신문은 C-SIG가 지원해야 할 핵심 조치를 제시함

4) https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

- EC는 또한 클라우드 컴퓨팅 분야에서 국제적 협력을 도모하고 있음. 일본, 브라질, 한국과 정책 및 공동 연구 이니셔티브가 시행되었으며 미국과 시행 중임
- EC는 CloudWatch2 프로젝트에 자금을 지원하고 있음. 해당 프로젝트는 상호운용성 및 보안 표준 현황에 대한 보고서를 발표하였고, 클라우드 서비스 목록을 작성하여 EU 클라우드 서비스 및 공급자를 매핑함
- 인증과 관련하여, 사용자가 자신의 데이터가 어디에 위치하던 서비스 제공자가 누구인지에 관계없이 자신의 데이터가 안전함을 확인하고 알 수 있는 방법에 대해, EC는 클라우드 컴퓨팅 인증 체계 연구(SMART 2016/0029)에 착수하였고 2017년 10월 공개 의견수렴을 종료함
- EC는 또한 소비자를 위한 공정한 시장을 촉진하기 위해 클라우드 제공자 전환 연구(SMART 2016/0032)에 착수하여 제공자 전환 시 법적, 경제적, 기술적 문제에 대한 자료를 수집한 바 있음
- 2018년 4월 EC는 2개의 DSM 클라우드 이해관계자 그룹을 출범함⁵⁾. 클라우드 인증 계획에 대한 DSM 작업그룹은 클라우드 보안에 관한 EU 인증 계획을 검토할 것이며, 국가 사이버보안 기관, 클라우드 서비스 제공업체, 클라우드 서비스 고객 및 감사(audit) 기관으로 구성됨
- 유럽보안인증프레임워크(EU-SEC)는 클라우드 서비스에 대한 IT의 외부화(externalisation) 확대에 인한 보안, 개인정보보호, 투명성 문제를 다룸. EU-SEC는 기존 인증 및 보증 체계가 공존할 수 있는 인증 프레임워크를 구축할 것임. EU-SEC는 Horizon 2020으로부터 자금 지원을 받으며 결과물을 웹사이트에 게시하고 있음(www.sec-cert.eu)
- 두 번째 DSM 작업그룹인 SWIPO(working group on cloud switching/porting data)는 데이터 이동 및 클라우드 전환을 촉진하기 위해 자체 규제 행동 코드를 정의함. 이러한 이동성 코드는 2018년 말 완료된 규정 제6조의 비(非)개인 데이터의 이동을 지원하고자 함이며, SWIPO의 목표는 '벤더 종속(vendor lock-in)'을 줄이는 것으로, 전문적인 사용자가 공급업체를 바꾸거나 데이터를 자신의 IT 시스템으로 포팅하길 원하는 경우, 적용되는 프로세스, 기술 요구사항, 기간 체계, 요금이 명확하다면 공급업체를 전환하기가 용이할 것임
- EC의 JRC(Joint Research Centre, 공동연구센터)는 2019년 말 오픈소스 소프트웨어와 표준 설정의 관계에 대한 연구를 발표한 바 있음.⁶⁾ 본 연구의 목적은 표준화 프로세스와 오픈소스(OSS) 프로세스 간의 상호작용에 대한 가능한 공통점과 장벽, 특히 표준화에서 OSS와 FRAND(Fair, Reasonable, and Non-Discriminatory) 라이선스 간의 상호작용을 식별하는 데 있음

■ 활동 아이템

- 활동 아이템 1 : 클라우드 서비스의 상호운용성, 데이터보호 및 이식성(portability)을 더욱 향상시키고 각 개발 활동을 지속 또는 개시하기 위한 ICT 표준 및 오픈소스

5) <https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security>

6) <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/relationship-between-open-source-software-and-standard-setting>

기술의 요구사항을 파악. 사용 가능한 오픈소스 기술과 여러 클라우드의 상호운용성, 데이터보호 및 관리에 대한 이들의 역할을 고려해야 함

- 활동 아이템 2 : 클라우드 서비스의 상호운용성, 데이터보호, 이동성 및 멀티 클라우드 관리를 더욱 개선하는데 필요한 ICT 표준 사용 촉진
- 활동 아이템 3 : 클라우드 영역에서 표준화와 오픈소스간의 연동을 더욱 강화하고 오픈소스 및 표준화의 긴밀한 협력을 위한 양자간 조치를 수립하고 지원
- 활동 아이템 4 : SLAs(서비스수준계약)과 CoC(클라우드행동강령)의 사용에 대한 국제 표준을 촉진
- 활동 아이템 5 : 유럽표준화기구(ESO)는 최종 사용자(특히 SME(중소기업) 및 공공부문)를 위한 클라우드 표준 및 가이드라인 매핑을 국제 표준개발기구(SDO), 클라우드 공급자 및 최종 사용자와 협력하여 업데이트해야 함. 이러한 조치는 클라우드 표준 조정 단계 1과 2에서 수행하는 표준 매핑을 업데이트하는 등 개발된 자료에 적용될 수도 있음
- 활동 아이템 6 : ISO/IEC JTC 1 참조 클라우드 아키텍처의 사용을 장려하고 일반적인 클라우드 아키텍처 구성요소를 정의. 사용가능한 표준을 일반 클라우드 아키텍처 구성 블록에 매핑하여 각 빌딩 블록에 대한 개인 정보 보호, 보안 및 테스트 표준을 정의할 수 있음. 이를 통해 클라우드 인프라 설계 및 구현을 위한 오픈소스의 주요 역할을 고려하여 개방형 클라우드 플랫폼 및 아키텍처에 사용할 수 있는 표준을 결정하는데 기여할 수 있음

3. 공공 부문 정보, 개방형 데이터 및 빅데이터

■ 정책 목표

- 데이터 양이 지속적으로 증가하고(이른바 '빅데이터'), 개방형 데이터의 양이 증가함에 따라, 이러한 데이터의 가치를 활용하는 부분에서 상호운용성의 중요성이 더욱 부각되고 있음
- 정형 데이터와 비정형 데이터를 포함한 모든 유형의 데이터, 지리공간 데이터, 통계 데이터, 기상 데이터, 공공 부문 정보(PSI) 및 연구 데이터 등 다양한 데이터에 기반한 혁신을 육성한다는 전체적인 목표와 광범위한 데이터 통합, 데이터 교환 및 상호운용성을 실현하기 위해 서로 다른 레벨(메타데이터 집합, 데이터 표현 형식 및 개방형 데이터의 라이선싱 조건 등)에서의 표준화는 필수적임

■ EC의 전망과 현황

- 전반적으로 다양한 부문과 수직 시장에 걸쳐 일관성있고 상호운용가능한 방식으로 서로 다른 소스에서 데이터를 수집하고 처리하기 위한 표준 및 공유 형식과 프로토콜의 적용이 요구됨. 일례로 R&D⁷⁾ 프로젝트, 유럽 개방형 데이터 포털⁷⁾, 유럽 데이터 포털이 있음⁸⁾
- EC의 연구에서 기업과 시민들이 공공 부문 정보를 찾고 재사용하는데 어려움을 겪고

7) <https://data.europa.eu/euodp>

8) <https://data.europa.eu/europeandataportal>

있다는 것을 보여준 바 있음. "개방형 데이터에 대한 통신문"에서는 "기계가 읽을 수 있는 형식의 정보가용성과 공통적으로 합의된 메타데이터의 얇은 계층을 통해 데이터의 상호참조와 상호운용성을 용이하게 하여 재사용의 가치를 상당히 향상시킬 수 있다"고 언급함⁹⁾

- 유럽의 개방형 데이터 포털의 개방형 데이터를 참조하기 위한 공통 표준은 유용할 것임. 공통 표준의 후보로는 유럽의 데이터 포털용 애플리케이션 프로파일(DCAT)과 FIWARE 오픈스택 기반 규격과 개방형 표준 API가 있으며,¹⁰⁾ FIWARE 솔루션은 현재 CEF(Connecting Europe Facility) "Context Broker" 빌딩 블록에 통합됨. 한편 CEF는 "Context Broker"를 ETSI NGSI-LD 규격(ETSI GS 009 V1.3.1 NGSI-LD API)에 사용하도록 개정하기로 합의했으며, FIWARE Foundation은 API를 개선하여 개방형 데이터 교환을 위한 ETSI 표준으로 발전시키고 있음
 - DCAT 애플리케이션 프로파일은 공공 부문 데이터 카탈로그 및 데이터셋을 설명하고 유럽 전역의 데이터 포털에서 사용할 규격을 홍보하기 위해 ISA2 프로그램, 간행물 사무소(PO) 및 CNECT에서 공통 프로젝트로 개발됨. 공통 애플리케이션 프로파일에 합의하고 회원국 간에 이를 홍보하는 것은 데이터 카탈로그 간의 상호 운용성과 회원국 간의 데이터 교환을 실질적으로 개선하는 것임. DCAT-AP은 Connecting European Facility 인프라의 일부인 유럽 데이터 포털 뿐만 아니라 많은 EU 회원국의 개방형 데이터 포털 등에서 사용되는 규격임. 지리공간 데이터(GeoDCAT-AP) 및 통계 데이터(StatDCAT-AP)에 대한 확장을 포함한 DCAT-AP 관련 작업도 핵심 표준에 대한 추가 작업의 필요성을 부각시키고 있음
 - 기존 관련 표준을 여러 빅데이터 영역에 매핑하는 것 또한 도움이 될 것임. 데이터 표준을 개발하기 위해 충분히 관련 활동을 하는 유럽의 산업 클러스터를 파악하는 것이 유용할 것이며, 특히 공개 데이터의 경우, PSI 지침의 현재 및 제안된 개정안에서 권장된 바와 같이 데이터 검증 및 라이선싱(기계 판독 가능 라이선스의 잠재성 등)의 주제를 다루어야 함
 - PSI 지침은 반드시 디지털 형식으로 사용가능하며 전자적으로 처리된 표준 라이선스의 사용을 권장함(8조 2항). 또한, 본 지침에서는 온라인에서 사용할 수 있는 공개 라이선스의 사용을 권장하고 있으며, 이는 결국 EU 전체에서 일반적인 관행으로 자리잡게 될 것임을 나타냄(Recital 26). 회원국들이 개정된 조항을 변경하도록 돕기 위해, EC는 PSI의 재사용을 위한 표준 공개 라이선스의 사용 권장 지침을 채택함
 - 2018년 4월 25일, EC는 '데이터 패키지'를 채택하여 정부 데이터와 공적 자금 연구 결과를 포함한 공공 보유 또는 공공 자금 지원 데이터, 기업 간(B2B) 및 기업과 정부 간(B2G) 환경에서의 데이터 공유를 촉진하기 위한 일련의 조치를 시행하였고, 기업이 데이터 중심 혁신의 잠재력을 활용하거나 인공지능을 활용한 솔루션을 개발할 수 있도록 도와주는 데이터의 가용성은 필수적임을 강조함. 데이터 패키지의 주요 요소는 다음과 같음
1. 개방형 데이터 및 공공 부문 정보 재사용에 관한 지침 채택(개정된 지침 2013/37/EU에 의해 재구성된 지침 2003/98/EC)
 - 공개 데이터 및 공공 부문 정보의 재사용에 관한 유럽 의회 및 2019년 6월 20일

9) http://ec.europa.eu/information_society/policy/psi/docs/pdfs/report/final_version_study_psi.docx

10) https://ec.europa.eu/isa2/solutions/dcat-application-profile-data-portals-europe_en & <https://www.fiware.org>

EC의 새로운 지침 2019/1024가 채택되어 2019년 6월 26일 발표되었으며, 2021년 7월 17일 이전에 국가 법률로 전환될 것으로 예상됨¹¹⁾

- 개방형 데이터 지침 제14조는 EC가 불임문서에 명시한 6가지 주제 범주에 속하는 특정 고부가가치 데이터셋의 목록을 작성하고 공공 부문 기관 및 공공 업무에서 보유하는 시행령을 채택할 수 있도록 함. 지침에서는 데이터셋의 재사용을 보다 효율적으로 하기 위해 데이터셋을 기계판독가능한 버전으로 API를 통해 무료로 제공할 수 있어야 하며 특정 경우에 대용량 다운로드 또한 가능해야 한다고 하고 있음. 또한 구현 법률에서는 고부가가치 데이터셋의 발행 및 재사용을 위한 준비사항을 명시할 수 있으며, 개방형 표준 라이선스와 호환되어야 함. 여기에는 재사용에 적용되는 용어, 데이터 및 메타데이터 형식, 배포를 위한 기술 준비 등이 포함될 수 있음. 영향 평가 연구, 이해관계자 상담 및 공청회 등 고부가가치 데이터셋의 정의에 관한 작업은 2020년 실시될 예정이며, 고부가가치 데이터셋에 대한 이행 규정은 2021년 상반기에 채택될 것으로 예상됨

2. 과학 정보에 대한 접근 및 보존 권고(2012) 검토

- 연구 데이터 개방 및 연구원 데이터 공유를 위한 인센티브 제도 조성에 관한 지침 개발로 전반적인 정책을 업데이트하고 강화
- European Open Science Cloud와 일관성을 보장

3. 민간 부문 데이터 공유에 대한 지침 개발

- EC는 공정한 데이터 공유 관행에 대한 원칙을 제시하고 B2B 및 B2G 데이터 공유의 법적, 비즈니스적, 기술적 측면에 대한 지침을 포함하는 기업 혹은 공공기관에 데이터를 제공하고자 하는 기업에 대한 지침을 제안

■ 활동 아이템

- 활동 아이템 1 : DCAT-AP 표준화 프로세스 지원을 위한 CEN 협력 요구. DCAT-AP는 유럽 내 데이터 포털의 특정 애플리케이션 요구를 충족하기 위한 메타데이터 기록에 대한 규격이 포함되어 있으며, EuroVoc¹²⁾의 재사용 및 기존 메타데이터 어휘(SDMX, INSPIRE 메타데이터, 더블린 코어 등)와의 매핑을 기반으로 다른 애플리케이션과의 의미적 상호 운용성을 제공함. DCAT-AP와 그 확장은 다양한 분야의 전문가 그룹에 의해 개발되었으며, 국제 표준화 조직의 전문가들이 개방형 데이터 포털 오너와 함께 참여하여 규격의 상호운용성 확인하고 해당 표준화를 지원한 바 있음. 이러한 매핑은 Geo/DCAT-AP(지리공간 데이터 집합)을 포괄하는 DCAT-AP 확장을 이미 제공한 이력이 있음. 해당 규격은 INSPIRE 지침 구현을 위해 작업중인 JRC 팀의 협력 하에 개발되었음. 그 외 Stat/DCAT-AP_ftnref2라는 통계 데이터 집합 확장 또한 2016년 발표된 바 있으며 EUROSTAT과 PO에서 개발에 참여함
- 활동 아이템 2 : 표준화 촉진. 개방형 데이터 인프라, 특히 2015-2020 CEF 프로그램에 따라 디지털 서비스 인프라의 일부로 구축되는 유럽 데이터 포털을 통해 표준화를 촉진
- 활동 아이템 3 : 다양한 표준화 활동 지원. Horizon 2020, R&D&I 활동 등 특히 ISA2

11) <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561993244509&uri=CELEX:32019L1024>

12) <http://eurovoc.europa.eu/drupal>

프로그램에서 개발된 DCAT-AP 규격과 FIWARE NGSI-LD 및 FIWARE CKAN 등과 같은 미래 인터넷 민간 협력하에 개발된 사양에 대한 표준화의 국제화를 지원. 또한 ISA2 프로그램에 의해 구현된 핵심 공공 서비스 애플리케이션 프로파일 뿐만 아니라 Core Vocabularies를 사용하여 표준화를 개선

- 활동 아이템 4 : 유럽 데이터 커뮤니티의 통합. H2020 Big Data Value 민관 파트너십을 포함한 유럽 데이터 커뮤니티를 통합하고, 기존의 국제적인 접근 방식 특히 ISO/IEC JTC 1 SC 42의 작업을 고려하여 빅데이터 참조 아키텍처에 대한 누락된 표준 및 설계 옵션을 파악
- 활동 아이템 5 : CEN을 W3C와 관련된 그룹과 협력하도록 촉진. DCAT-AP를 표준화하기 위해 호환되지 않는 변경과 표준의 사용 조건에 대해 W3C의 관련 그룹과 조율하는 것을 권장
- 활동 아이템 6 : EC는 공공 조달시 참조되어야 하는 국가간 서비스 제공을 위한 기술 규격을 개발하는 EU 지원 파일럿과 프로젝트(ISA², CEF/DEP 파일럿, eDelivery의 eSens)에서 표준화를 어떻게 다룰지 고려하기 위해 SDO와 교류

4. IoT(사물인터넷)

■ 정책 목표

- IoT는 디지털 단일시장의 핵심 우선순위 영역임. IoT는 산업 가공 기계와 산업적으로 처리되는 품목(사이버-물리적 시스템), 가정용 장비, 웨어러블 전자제품, 자동차, 센서 등 더 많은 물체를 인터넷에 연결하는 이머징 기술임. 연결 기기의 수는 2020년까지 200억대를 넘어설 것으로 예상됨. IoT는 많은 산업 분야의 혁신 가능성 외에도 기후 변화, 자원 및 에너지 효율, 노화 등 많은 사회적 과제를 해결하는 데 도움을 줄 수 있는 잠재력을 가지고 있음
- 다수의 독점적 또는 반 폐쇄적 솔루션이 특정 문제 해결을 위해 등장해 오면서, 서로 다른 아키텍처와 프로토콜을 바탕으로 상호운용이 불가능한 개념을 이끌고 있음. 결과적으로, 진정한 IoT 애플리케이션의 구현, 즉 연결 가능한 "사물"에 대한 정보를 유연하게 취합한 확장은 "Intranets of things 또는 goods"으로 제한되어 왔음
- 이머징 IoT 경제에서 자발적 글로벌 표준은 기술 도입을 가속화하고 경쟁을 촉진하며 비용효율적으로 신기술 도입을 가능하게 함. 표준화는 글로벌 규모로 서로 다른 기술 솔루션 간의 상호운용성, 호환성, 신뢰성, 보안 및 효율성을 촉진하여 산업 혁신을 촉진하고 기술 진화에 대한 보다 명확성을 제공함. 가치사슬을 이루는 서로 다른 기업이 운영하는 IoT 네트워크 간의 상호운용성은 유럽 정책 목표 달성의 기회를 제공할 것임 - 더 나은 순환 경제¹³⁾를 위한 자원 효율성, 투명성과 추적성을 통한 지속가능성과 책임있는 공급망 등
- 산업계는 글로벌 IoT 생태계 기회와 과제를 해결하기 위한 기술 표준과 솔루션을 개발하는 최적의 위치에 있음. 글로벌 IoT 생태계 전반에서 상호운용 가능하고 확장 가능한 보안 솔루션이 요구됨. 이러한 맥락에서 2016년 제안서를 받은 유럽의 대형 파일럿(LSP)은 사용자와 공공의 수용성(acceptability)과 채택을 테스트 및 개선하고

13) https://ec.europa.eu/environment/circular-economy/index_en.htm

공급업체에게는 새로운 EU 시장기회를 조성함으로써 IoT 솔루션 구축을 지원하고 있음

- LSP는 실제 IoT 솔루션을 실생활 환경에 구축할 수 있는 기회를 제공하고 있으며, 공급자는 비즈니스 기회를 테스트할 수 있도록 추진되어야 함. 이 개념은 계속 확대되어 수직적 부분까지 확대. 주요 과제를 중심으로 활동들을 통합하는 교차 프로그램을 위해 '유럽 산업과 서비스의 디지털화 및 변환'의 맥락으로 확대
- 2018년과 2019년의 제안서 요청(calls for proposals)을 통해 더 많은 LSP가 착수될 것이며, 제조, 보건 및 관리, 농업, 연결 및 자율 주행의 디지털 변환을 두드러지게 다룰 것임, 아울러 공간 데이터와 관련 플랫폼의 통합을 포함할 것임

■ EC의 전망과 현황

- 지난 몇 년간의 주요 성과 중 하나는 IoT 표준화에 관련된 모든 이해관계자 간의 협력이 점진적으로 구축되었고, 전략적 IoT 표준화 문제에 대한 높은 수준의 구성이 성공적인 도구로 입증되어 현재 여러 분야에서 공통적으로 사용되고 있다는 것임
- ETSI TC Smart M2M에서는 유망한 비즈니스 모델 및 사용 사례를 고려하여, IoT 및 갭 분석 표준 매핑을 하였고, ETSI TS 103 375 및 TS 103 376 문서로 발표하였음
- IoT 표준은 시스템 및 기기 통합의 상업적 역량을 발휘하는 비즈니스 모델의 출현을 뒷받침하고 있음. 표준 선택 뿐만 아니라, 기업이 공유할 수 있는 구현 참조 모델을 파악하는 것도 중요함. 이 방식은 미래인터넷 PPP(FI-PPP)에서 시작하여, 현재는 다른 산업 기관에서 채택되고 있음. 예를 들어, 사물인터넷혁신연합(AIOTI), 빅데이터가치협회(BDVA), Open & Agile Smart Cities(OASC) 등이 있음. AIOTI는 상위구조 참조 모델을 관리하고 있으며, 우선순위 주제로 새로운 결과를 통합하고 있음
- ISO/IEC JTC 1/SC 41(사물인터넷 및 관련기술), oneM2M, ITU SG 20 등 기존의 글로벌 이니셔티브 간 IoT 표준화에 대한 입장을 맞추는 필요가 있으며, 공통 주제에 대한 협력과 유럽의 결과를 전세계적인 활동으로 채택하기로 한 합의는 매우 고무적인 결과물임
- 의미론적 상호운용성, 보안성, 개인정보보호, 5G/IoT 상호작용 등이 가장 높은 우선순위를 차지하고 있음
- IoT의 수직적 산업이 확대됨에 따라 주요 과제는 파트너십(PPPs 및 기타 연합)에 걸쳐 협업을 끌어내고, 모든 표준화 노력이 수렴되도록 공통 목표를 향한 협력을 지속하고 심화시킴으로써 영역 전체에 걸쳐 모범 사례의 보급과 도입을 보장하는 것임. 이를 위한 구체적인 첫 단계로 DEI(유럽 산업의 디지털화) 이해관계자 거버넌스와 MSP(European Multi-Stakeholder Platform on ICT Standardisation) 사이의 공동 작업 그룹을 출범하여 플랫폼 구축과 파일럿 활동의 조정, 표준화 동기화 및 가속화에 기여해왔음

■ 활동 아이템

- 활동 아이템 1 : SDO는 산업자동화에 필요한 초고신뢰 초저지연(URLL) 기술 등 IoT가 요구하는 무선기술의 격차 분석을 통해 지속적인 격차 분석을 보완
- 활동 아이템 2 : SDO는 진보된 데이터 상호운용성을 위해 의미 표준(semantic standards) 영역에서 지속적인 작업을 수행

- 활동 아이템 3 : SDO는 IoT 제품, 시스템, 애플리케이션 및 프로세스의 준수(compliance)에 사용할 수 있는 표준을 제공
- 활동 아이템 4 : ISO 270xx 및 GDPR 규정에 근거한 조직의 현재 준수 프레임워크와 일치하는 제품의 사이버보안 준수를 위한 유럽 표준을 개발. 가급적 이러한 표준은 NIS directive(네트워크 및 정보보안 지침)에 명시된 요건에 부합하여 사용될 수 있음
- 활동 아이템 5 : ISO/IEC JTC 1 SC41에서 개발된 IoT용 국제 레퍼런스 아키텍처의 개발과 도입을 촉진
- 활동 아이템 6 : SDO는 유럽 사이버 보안법 또는 부문별 법률에 따라 IoT 소비자 제품의 안전 및 사이버보안에 관한 표준을 개발하고 격차를 평가
- 활동 아이템 7 : SDO는 수직 산업으로의 확장과 추가를 고려

5. 사이버보안/네트워크 및 정보 보안

■ 정책 목표

- 유럽 네트워크 및 정보 시스템의 높은 수준의 보안에 대한 조치에 관련된 지침인 NIS Directive는 ICT 보안 표준의 개발 및 도입을 촉진하기 위한 조치를 제공함
- EU사이버보안법(규정 EU 2019/881)은 유럽 사이버보안인증 프레임워크를 수립하여, EU의 사이버보안 수준을 높이고, 유럽 사이버보안인증제도에 대한 EU 차원의 통일된 접근방식이 가능하도록 하여 내부시장 기능을 개선하고자 함. 유럽 사이버보안인증 프레임워크는 유럽 사이버보안인증제도를 확립하고, 이러한 체계에 따라 ICT 제품, ICT 서비스, ICT 프로세스가 보안 요구사항을 준수하는지 평가하여 입증하는 메커니즘을 제공합니다. 요구사항은 저장, 전송, 가공된 데이터 또는 기능 또는 제품주기 동안 해당 제품, 서비스, 프로세스가 제공하거나 액세스 할 수 있는 서비스의 가용성, 신뢰성, 무결성, 기밀성을 보호하기 위함
- 5G 네트워크의 사이버 보안에 관한 2019년 3월 26일 EC의 권고 (EU) 2019/534는 5G 네트워크 사이버보안을 보장하기 위한 EU 접근 방식을 지원하는 일련의 조치를 제시함

■ EC의 전망과 현황

- 필수 서비스 운영자에 대한 보안 및 통지 요건의 경우, 네트워크 및 정보 보안과 관련된 다수의 참조 표준 및/또는 규격을 설정하여, 관련되는 경우, EU 전역에 걸쳐 표준화 관행을 일관성 있게 채택할 수 있도록 하는 기반이 될 것임
- 디지털 단일 시장 전략 목표에 부합하는 디지털 서비스 공급자를 위한 보안 및 알림 요구사항은 NIS 지침에 따라 EU내 어디에서나 유사한 규칙을 통해 일련의 통일된 요구 사항 구축을 목표로 함
- 특히 모든 조직이 사이버보안을 위한 표준과 프레임워크의 필요성을 인식하는 것이 중요. 일반적으로 ICT 제품, 서비스 또는 프로세스의 설계 및 개발에 참여하는 조직, 제조업체 또는 공급업체는 사이버공격 발생을 미연에 예상하여 그 영향을 최소화하기 위해 설계와

개발의 초기 단계에서 적절한 조치를 시행하여 제품, 서비스 및 프로세스의 보안을 가능한 최대로 설계하는 것을 권장함 ('security-by-design')

■ 활동 아이템

- 활동 아이템 1 : SDO는 중요한 인프라 보호를 위한 표준을 개발하여 NIS Directive에 명시된 요구사항을 지원하고 이에 대응
- 활동 아이템 2 : SDO는 유럽 사이버보안인증 프레임워크를 지원하는 데 필요한 기존 표준을 평가하여 모든 인증 활동의 핵심을 제공하기 위해 표준을 사용할 수 있도록 도모. 특히, SDO는 ICT 제품이나 서비스의 설계, 개발, 제공, 유지보수와 관련된 절차에서 보안과 관련된 것뿐만 아니라, ICT 제품이나 서비스의 보안 속성에 대한 규격과 평가 관련 표준에 대한 작업을 권장
- 활동 아이템 3 : SDO는 개인용 컴퓨터의 악성소프트웨어 이슈를 조사. ENISA(유럽 트윙크정보보안기구)는 다수의 개인용 컴퓨터에 (금융) 트랜잭션을 모니터링할 수 있는 악성소프트웨어가 포함되어 있다고 발표. eBusiness와 e-Transactions에 대한 의존도가 점점 더 높아지고 있기 때문에, 유럽 이니셔티브는 이러한 주제를 조사해야 함
- 활동 아이템 4 : SDO는 제약 조건이 높은 장치 및 프로토콜 상호작용(저대역폭/초단시간 세션지속시간(50ms)) 저처리 기능 네트워크에 대한 보안 프로토콜 요구사항을 조사
- 활동 아이템 5 : SDO는 NIS Directive에서 디지털 서비스 공급자에 대한 보안 및 사고 통보 요구 사항에 대한 표준의 가용성을 조사
- 활동 아이템 6 : SDO는 특히 SME(중소기업)에 해당되는 ISO/IEC 270xx 시리즈(특정 활동 영역을 포함한 정보 보안 관리 시스템)의 "지침" 버전을 개발하기 위해 ISO/IEC 27003에 제시된 기존 지침을 확장하여 ISO/IEC JTC1 SC27 WG1과 협업을 추진. 이 지침은 ISO/IEC 270xx와 100% 호환되어야 하며 부족한 리소스 및 역량 시나리오를 포함하여 SME가 이를 실질적으로 적용할 수 있도록 지원
- 활동 아이템 7 : SDO는 유럽 사이버보안법을 준수하는 인증 제도를 지원하기 위해 소비자 제품의 사이버보안에 대한 표준을 개발하고 격차를 평가