2020년
ICT국제표준 마에스트로
주요이슈 분석서

[ITU-T 정보보호 표준화]

한국정보통신기술협회

표준 마에스트로 주요이슈 분석서
(ITU-T 정보보호 표준화)

1 개요

1.1 Overall 기술 및 표준화 Trend

o ITU-T SG17 은 정보 및 정보 자산의 기밀성, 무결성, 가용성을 보장하기 위한 정보 보호 기술에 대한 국제표준을 개발하고 있는 표준화 그룹[1]이다.

o ITU-T SG17 표준화는 ICT 활용에 있어서 보안과 신뢰를 제공하기 위한 다양한 국제표준을 개발하고 있으며, 대표적인 분야가 5G 보안, 블록체인 보안, 양자정보통신 보안 기술 등이다. 현재 (2020년 11월) 진행중인 표준화의 세부 내용은 ITU-T SG17 work progrmme[2]를 살펴보기 바란다.

주요 이슈	표준화 그룹	표준 주도 국가/기관	표준 대응 업체/기관	대응 필요성/통찰
5G 보안	Q6/17 (통신서비스 보안)	중국/차이나모바일, 한국/순천향대,맥데이터, 일본/KDDI	3GPP, IETF, ETSI	- 5G 보안 가이드라인, 신뢰관계 프레임워크, 5G 엣지 컴퓨팅 보안 프레임워크, 고신뢰 저지연 수직 서비르를 위한 보안 요구사항 등은 5G 네트워크의 신뢰적 운영을 위해 필요함
블록체인 보안	Q14/17 (분산원장기술 보안)	중국/알리바바, 한국/순천향대, ETRI 등, 미국/Aetna	ISO TC 307	- 분산원장기술 용어정의, 분산원장기술 보안 위협, 보안 구조, DLT 시스템의 보안성 평가, DLT 기반 ID관리 등은 다양한 분산원장기술의 보안과 신뢰를 위해 필수적임
양자정보통신 보안	Q4/17 (사이버보안)	중국/CAS Quantum Network 등, 일본/NICT, 한국/SKT, KT 등	ETSI QKD WG, ISO/IEC JTC 1/SC 27	- 양자 내성 암호 알고리즘의 활용, 양자 키 분배 방식 네트워크 보안, 양자 난수 생성기는 양자정보통신을 위한 필수 불가결함

1) https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx
2) https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx

1.2 5G 보안 표준화 이슈 및 전망

ㅇ (기술개요)

5G 네트워크는 초고속, 초신뢰/초저지연, 초연결 특성을 갖는 융통성 있고 신리적인 새로운 이동통신망이다. 우리나라는 2019년 4월 세계 최초로 비독립형(NSA) 5G 통신망이 서비스를 시작하였고, 이후 미국, 영국 등이 상용 서비스를 시작하였다. 최근 중국도 5G 서비스를 시작하였다.

통신 사업자들은 5G 생태계 구축을 위해서 증강현실, 가상현실, OTT 등의 다양한 콘텐츠를 확대하고 있고, 로봇, 자율주행, 의료, 교통, 환경, 산업제어 산업 부문 등 다양한 산업 부문에서 기반 네트워크로 5G 네트워크의 활용이 기대되고 있다.

향후 5G 코어망까지 규격과 구현이 완비되고 코어망도 5G 시스템이 구축되면 독립형(SA) 5G 시스템이 운용될 것이며, 수년내로 5G 통신망은 국가 기간 통신망으로 운용될 것으로 보인다. 결국, 5G 통신 시스템이 활성화됨에 따라서 자율자동차, 스마트 팩토리 등 융합 서비스도 활성화될 것이고, 이로 인해 기존의 모바일 통신망 보안 위협과 상이한 새로운 보안위협이 지속적으로 등장할 것이다.

5G 보안은 5G 네트워크를 위한 보안과 5G 네트워크를 이용하는 다양한 산업 부문의 보안으로 구성된다. 따라서 다양한 공격 형태가 나타날 것이며, 공격자자 활용할 수 있는 공격 면적의 증가를 의미하게 된다. 이러한 다양한 위협에 대응할 수 있는 표준화된 보안통제의 개발과 적용이 필요하다.

ㅇ (기술 개발 현황)

글로벌 통신사 및 스마트폰 제조 업체는 5G 시범 서비스 및 단말기를 출시 중이다. Qualcomm 등은 2019년 2월, 바르셀로나에서 개최된 MWC 2019에서 5G 스마트폰을 비롯한 5G 제품 및 서비스 공개했다. 그 외 국외 주요 사업자 서비스 동향[3]은 다음과 같다.

3) ICT 표준화 로드맵 Ver 2020 – 차세대 보안

<국외 주요 사업자 서비스 동향>

사업자	주요 현황
AT&T	- 2019년 내로 모바일 5G 상용화 추진 - 2018년 12월, 12개의 미주 도시에서 모바일 라우터 기반 5G 서비스(FWA) 개시 - 2017년, 5G 테스트 개시 - 삼성전자, 노키아, 에릭슨을 5G 통신장비 공급 업체로 선정
NTT Docomo	- 2020년, 도쿄올림픽 개최 시 5G 서비스 개시 목표
Vodafone	- 2019년 7월, 영국 7개 도시에서 5G 서비스 개시 - 2018년 말, 맨체스터에서 5G 네트워크 시험 서비스 개시
BSI, TUV 등	- 다양한 인증심사기관, 컨설팅 업체 등이 ISMS 컨설팅 및 인증심사 서비스를 제공 중
TI	- 2017년 12월, 심전도·심박수들 동시에 측정하는 생체신호 센서용 MoC 상용화
Halipax, Royal Bank	- 2016년, 심전도·심박수 등 생체신호 인증기술을 이용한 금융고객 신원확인 서비스
Symantec	- 엔드포인트, 클라우드, 인프라 전반을 정교한 공격으로부터 방어할 수 있는 전략적인 통합 솔루션 제품 개발 - 2014년, 글로벌 보안업체들이 참여하는 위협 인텔리전스 정보 공유 플랫폼(CTA)에서 핵심 역할을 담당
Trend Micro	- 개인용 안티바이러스 백신에서부터 기업용 APT 대응 솔루션과 물리서버, 가상화서버, 클라우드 보안에 이르는 다양한 솔루션을 제공 - 보안위협을 분석하는 Deep Discovery, 가상화 보안 및 물리서버 보안을 제공하는 Deep Security와 클라우드 보안센터와의 연동을 통한 통합보안 솔루션을 개발
Facebook	- 2017년 1월, FIDO Alliance 보드멤버사로 활동 중이며, 전세계 20억 명이 넘는 사용자가 FIDO인증 솔루션을 지원하는 보안키를 사용해 로그인할 수 있도록 지원 중
KasperskyLab	- 악성코드 차단 기능과 함께 PC의 모든 파일 활동을 모니터링하고, 방대한 화이트리스트 DB를 활용한 애플리케이션 제어 기능을 통합하여 제로-데이 공격에 대응 - 각종 악성코드 차단뿐만 아니라, 클라우드 기반 방역, 애플리케이션 권한 제어, 특정 웹사이트에 대한 접근 제한, PC 취약점 체크 등의 보안 솔루션 제공
Microsoft	- 자사 윈도우 헬로에 대해서 FIDO2 인증을 획득함. 이로써 윈도우10 이상의 사용자는 FIDO2 인증지원이 가능
Google	- 구글 안드로이드가 FIDO2 인증을 획득해 FIDO2 프로토콜을 지원하는 웹사이트와 모바일 앱에서 패스워드 없이 로그인 가능. 사용자가 안드로이드 최신버전을 설치한 기기를 구매하거나 구글플레이 서비스 업그레이드를 통해 7.0이상 버전을 설치하면 FIDO 온라인 인증을 바로 사용 가능
Line	- 네이버 자회사인 일본의 라인(Line) 메신저 이용자들이 지문 또는 얼굴인식을 통한 인증으로 '패스워드 없는 로그인'이 가능. 메신저뿐만 아니라 그 계정을 연동하는 파트너, 타사 서비스에서도 온라인 간편인증 규격으로서 FIDO 표준기술을 활용

ㅇ (ITU-T SG17 Q6 표준화 현황)

ITU-T SG17에서는 5G 이동통신 환경을 고려하여 2018년부터 5G 보안 표준화를 적극적으로 추진하고 있다. 5G 보안을 위한 국제표준화는 ITU-T SG17의 연구과제 6(Q6/17)에서 수행되고 있다.

표준명	제목	에디터	표준 요약
X.1811 (X.5Gsec-q)	양자 내성 알고리즘을 5G 시스템에 적용하기 위한 보안 가이드라인	Feng Gao 등	이 권고는 양자 내성 알고리즘을 5G 시스템에 적용하기 위한 보안 가이드라인이다. 이 권고는 다음을 다룬다. - 5G 시스템의 보안 아키텍처 - 상용 양자 컴퓨터 가용시 5G 시스템에 대한 보안성 평가 - 5G 시스템에서 양자 안전 알고리즘의 활용
X.5Gsec-t	5G 에코시스템에서 신뢰관계에 기반한 보안 프레임워크	Jin Peng, 염흥열 등	이 권고는 신뢰 관계에 기반한 보안 프레임워크를 제시한다. 이 권고는 다음을 포함한다. - 5G 생태계의 이해 관계자 식별 - 그들 사이의 신뢰 관계 분석 - 각 이해 관계자에 대한 보안 책임성 명확화 - 이해 관계자 간의 보안 경계 정의 -5G 에코 시스템의 보안 프레임 워크 정의
X.5Gsec-ecs	5G 엣지 컴퓨팅 서비스를 위한 보안 프레임워크	Feng Gao 등	이 권고는 엣지 컴퓨팅 서비스의 잠재적 인 배치 계획 및 일반적인 애플리케이션 시나리오를 분석하고, 엣지 컴퓨팅 서비스에 특정한 보안 위협 및 요구 사항을 규정함으로써 운영자가 애플리케이션을 보호할 수있는 보안 프레임 워크를 구축한다.
X.5Gsec-guide	5G 통신 시스템을 위한 보안 가이드라인	염흥열, 김미연 등	이 권고는 5G 통신 시스템에 대한 보안 지침을 제공한다. 5G 통신 시스템의 보안과 관련된 구성 요소, 즉 사용자 장비, 액세스 네트워크, 핵심 네트워크, 서비스 및 인프라를 식별한다. 또한 에지 클라우드 컴퓨팅, 동적 네트워크 가상화 및 네트워크 슬라이싱과 같은 5G 통신 시스템의 고유한 네트워크 기능을 고려하여 일반 보안 Enabler에 대해 설명하고 각 구성 요소에 대한 위협 및 보안 기능을 제공한다.
X.5Gsec-netec	5G 에지 검퓨팅을 위한 네트워크 계층 보안 능력	Chen Zhang 등	5G EC는 5G 시대의 낮은 대기 시간 서비스 및 트래픽 오프로드 서비스에서 중요한 역할을 한다. 이 권고에서는 에지 클라우드 활용하는

			통신 사업자에게 네트워크 계층의 보안 요구사항과 보호조치를 제시한다.
X.5Gsec-ssl	5G 네트워크 슬라이스에서 보안 능력을 구분하기 위한 가이드라인	Zhiyuan Hu 등	이 권고의 목적은 네트워크 슬라이스 사용, 배포 및 관리의 보안을 안내 할 수 있는 5G 네트워크 슬라이스 보안 수준을 분류하기 위한 지침을 제공하는 것이다. 범위에는 5G 네트워크 슬라이스 보안 기능의 차별화, 5G 네트워크 슬라이스 보안 기능의 범주를 식별하기 위한 원칙 및 방법, 수직 산업의 5G 슬라이스에 대한 일반 보안 요구 사항에 대한 조사 및 조사가 포함된다.
X.5Gsec-vs	5G 사설망에서 초신뢰 저지연 통신을 지원하기 위한 수직 서비스를 위한 보안 요구사항	신성기, 염흥열 등	이 권고는 5G 비공개 네트워크에서 URLLC (Ultra Reliable and Low Latency Communication)를 지원하는 수직 서비스에 대한 보안 요구사항을 제시한다. 5G 비공개 네트워크에서 URLLC를 지원하는 수직 서비스를 제공 할 때 위협 및 위험 그리고 이를 해결하기 위한 보안 (모니터링) 요구 사항을 식별한다.

현재 ITU-T SG17의 5G 보안 표준화는 중국에서 적극적으로 추진 중이다. 중국은 2018년부터 적극적으로 5G 통신의 보안을 위한 권고안을 개발하도록 신규 작업항목을 제안하였다. 2018년 3월과 8월 회의를 통해서 5G 통신 시스템에 양자 내성 암호를 적용하기 위한 가이드라인(X.5Gsec-q), 5G 생태계에서 신뢰관계 기반의 보안 프레임워크(X.5Gsec-t) 등의 권고안이 신규 작업항목으로 채택되어 표준화가 진행 중이다. 이에 한국에서는 해당 권고안에 한국의 5G 통신 시스템 특성을 고려한 관련 위협에 대한 보안 대책이 적용될 수 있도록 지속적으로 기고서를 제출하거나 회의 중 의견을 내는 방법으로 대응하고 있다.

한국이 전세계 5G 서비스 시장을 선도하는 것에 발맞추어 보안 기술 표준화도 주도하기 위한 노력으로 한국은 2019년 1월 ITU-T SG17 회의에서 5G 통신 시스템의 전반적인 보안 요구사항을 개발하기 위한 신규 작업항목(X.5Gsec-guide)을 제안하였다. 5G 통신 시스템의 단위 기술에 대한 보안 가이드라인은 표준화되고 있으나 시스템 전반에 대한 보안 요구사항을 개발하는 표준화 작업항목이 없다는 점에 각국이 동의하였고, 해당 제안은 권고안(X.5Gsec-guide)으로 개발 중이다. 해당 권고안은 현재 3GPP에서 개발한 보안 규격과 ITU-T X.805 권고를 참고하여 개발할 예정이다.

5G 생태계를 위한 보안 프레임워크 권고안(X.5Gsec-t) 역시 5G 통신 시스템 전반에 대한 보안 요구사항과 보안 기능을 정의하는 표준이며, 향후 5G 시스템 보안에 중요한 역할을

하게 될 것으로 판단되어 한국의 보안기술을 적용하기 위해서 에디터쉽을 확보하였다.

2019년 두 차례의 회의에서 중국은 2018년부터 개발하던 권고안 외에 추가적으로 2건의 신규 작업항목을 제안하여 채택되었다. 이로 인해서 에지 컴퓨팅 서비스를 위한 보안 프레임워크(X.5Gsec-ecs), 5G 에지 컴퓨팅을 위한 네트워크 계층의 보안 능력(X.5Gsec-netec) 등의 표준이 추가적으로 개발되고 있다.

2020년 2차례 회의에서 중국은 5G 네트워크 슬라이스에서 보안 능력을 구분하기 위한 가이드라인 신규 표준을 제안해 채택했으며, 한국은 5G 사설망에서 초신뢰 저지연 통신을 지원하기 위한 수직 서비스를 위한 보안 요구사항 신규 표준을 제안해 채택했다.

ㅇ (해외 대응 현황)
ITU-T SG17에서 5G 보안에 관한 국제 표준화는 개발되는 국제표준 5개중 4개의 신규워크아이템 제안이 중국에 의해 이뤄졌고 반영되었다. 중국은 신뢰 관계 프레임워크, 양자 내성 암호 알고리즘의 5G 시스템에 활용, 에지 클라우드 보안, 에지클라우드 네트워크 계층 보안 등을 추진하고 있다. 일본은 최근 일본 NICT를 중심으로 5G 보안 국제표준화 추진을 위한 준비를 모색하고 있다. 미국, 영국 등은 국제 표준 개발 과정에 관찰하고 있다. 미국, 영국, 캐나다는 표준 개발과정에는 직접 참여하지 않고, 회의 현장에서 구두 의견 제시를 통해 국제 표준 개발과정에 관여하고 있다.

ㅇ (국내 대응 현황)
한국은 5G 시스템의 보안을 강화하기 위한 핵심 권고안인 5G 통신 시스템 보안 가이드라인(X.5Gsec-guide)과 5G 생태계에서 신뢰관계 기반의 보안 프레임워크(X.5Gsec-t) 등 2개의 권고안이 국제 표준으로 개발될 수 있도록 지속적으로 노력하고 있다. 한국의 현황과 입장을 반영한 기술적 내용을 담은 기고서를 지속적으로 제출하고, 국제회의에서 지속적으로 의견을 개진하여 한국의 주도로 5G 보안 국제표준이 개발될 수 있도록 할 것이다. 또한 수직 서비스를 위한 보안 요구사항은 5G 사설망에 적용할 수 있다. 더불어 해당 권고안이 원활히 개발되고 채택되도록 미국, 일본, 중국 등과 지속적인 협력도 추진할 예정이다.

ㅇ (국내 대응 필요성 및 전망)
현재 과기정통부의 주도로 신설된 '5G보안협의회'에서 논의되는 주요 표준화 추진 내용을 검토하여 향후 ITU-T SG17에서 국제 표준으로 개발될 수 있도록 노력할 예정이다. 이러한 노력을 통해서 한국이 국제사회에서 5G 보안기술의 주도국으로 도약할 수 있도록 하기 위한 기반을 다지고자 한다. 또한 2019년 9월 헝가리 부다페스트에서 열린 ITU CTO Summit에서 합의된 5G 보안에서 ITU 역할 강화를 위해 글로벌 5G 보안 표준화 조정활동을 위해 5G 보안에 대한 조인트 조정 회의의 제안도 고려할 필요가 있다. 또한 한국 실정을 반영한 신규워크아이템을 제안해 한국 5G 보안 기술을 반영할 필요가 있다.

1.3 블록체인 보안 표준화 이슈 및 전망

ㅇ (기술개요)

분산원장기술인 블록체인이 4차산업시대의 핵심 ICT 기술로 주목 받으면서 블록체인의 기반기술인 분산원장 기술에 대한 국제 표준화는 분산원장기술에 기반을 둔 다양한 응용과 분산원장기술의 신뢰적 운영을 위해 요구된다.

블록체인은 하나의 중앙 집중 데이터베이스에 정보를 저장 관리하는 것이 아니라 분산화된 여러 네트워크 노드에 하나의 정보를 블록형태로 암호학적 기법을 이용해 변경 불가능하도록 저장 및 관리하는 기술이다. 블록체인 기술은 디지털 서명 기술(암호 기술), 해시 기술, peer 간 통신 등의 여러 기술 요소로 구현된다. 블록체인 시스템에서 정보가 한번 블록에 저장되면 이후 변경이 어렵다는 특성으로 갖는다. 응용은 크게 모든 산업 부문에 적용될 수 있는 응용(분산 ID 등)과 특정 산업 부문에 적용될 수 있는 응용(공급자 체인 있 응용) 으로 구분된다.

블록체인을 포함한 분산원장기술에 대한 표준화는 ISO TC 307, ITU-T SG13, SG16, SG20, IEEE 등 여러 표준화 기구에서 추진되고 있다.

ㅇ Q14/17 표준화 현황

ITU-T SG17에서는 2017년 8월 한국의 제안으로 분산원장기술 보안 표준화를 위한 신규 연구과제(Q14/17)을 신설하였으며, 한국에서 코라포처를 확보하여 표준 개발을 주도하고 있다.

표준명	제목	에디터	요약
X.1400 (X.dlt-td)	분산 원장 기술에 대한 용어 및 정의	염흥열, 김지혜	이 문서는 분산원장기술에 대한 용어 및 정의를 제공한다. 용어 정의는 용어의 기본 특성을 제공하며, 적절한 경우 추가 명확성을 제공하기 위해 메모가 포함된다. 분산 원장 기술 관련 표준의 기초이며 분산 원장 기술의 보안 측면에 대한 표준에 대한 이해와 일관성을 높이는 것이 목표이다.
X.1401 (X.sct-dlt)	분산원장 기술의 보안 위협	Ke Wang, 염흥열 등	이 권고는 DLT 개발, 운영 또는 사용에 대한 보안 분석을 제공하고 DLT 기반 플랫폼 또는 서비스 시스템에 대한 보안 분석을 제공한다. 또한 DLT 자체가 달성한 보안 기능을 연구하고 DLT에 대한 보안 위협을 나열한다.

X.1402 (X.sra-dlt)	분산원장기술을 위한 보안 프레임 워크	Xiaoyuan Bai, Tatiana 등	이 권고는 DLT 응용 프로그램 공급자 및 서비스 공급자에게 지침을 제공하여 보안 위험을 줄이고 DLT를 기반으로하는 응용 프로그램 및 서비스의 보안을 향상 시키며 DLT를 최대한 활용하여 더 나은 응용 프로그램 및 서비스를 제공한다.
X.1403 (X.dlt-sec)	ID 관리에 분산원장기술 데이터를 사용하기 위한 보안 고려사항	Abbie Barbir	이 권고는 ID 관리에서 DLT 데이터를 사용하기 위한 통신 관련 개인정보 및 보안 고려사항을 제공한다.
X.das-mgt	분산원장기술을 기반으로 하는 데이터 액세스 및 공유 관리 시스템을위한 보안 프레임워크	염흥열, 김미연 등	이 권고는 분산원장기술 (DLT)을 기반으로 하는 데이터 액세스 및 공유 관리 시스템을 위한 보안 프레임워크를 제공한다. DLT 기반의 데이터 액세스 및 공유 관리 시스템에 대한 참조 모델을 설명한다. DLT 기반의 데이터 액세스 및 공유 관리 시스템에 대한 엔티티 및 해당 역할을 식별한다. 또한 데이터 액세스 및 공유 관리 시스템에 대한 보안 위협을 식별한다. 또한 이러한 보안 위협을 해결하는 보안 요구사항을 설명한다.
X.gscdlt	분산원장 기술에 대한 보안 관리 통제	오경희, 박근덕 등	이 문서는 분산원장시스템 관리, 보안 정책, DLT 플랫폼, DLT 관리자, 스마트 계약, 합의 메커니즘, DLT 오라클, DLT 상호 운용성 등을 포함하는 분산원장기술 특정 보안 통제에 대한 지침을 제공한다. 구현 지침은 각각 DLT 서비스 제공자와 DLT 서비스 고객에게 제공 될 수 있다.
X.sa-dlt	분산 원장 기술에 대한 보안 보증	염흥열, 김미연 등	이 권고는 분산원장기술 (DLT)의 보안 보증 수준에 대한 지침을 제공한다. 데이터 무결성, 기밀성, 통신 보안 및 자격 증명 관리 측면에서 DLT 보안 보증 프레임 워크를 정의한다. 특히, 데이터 무결성을 지원하는 작업 증명과 기밀성을 지원하는 암호화에 대한 보안 보증에 중점을 둔다. DLT의 3 가지 수준의 보안 보증 (LoSA)을 정의한다. 또한 위 보안 측면에만 관련된 보안 위협을 완화하r기 위한 통제에 대한 지침을 제공한다.

X.srip-dlt	분산원장기술을 기반으로 하는 지적 재산 관리를 위한 보안 요구사항	Yunwei Zhao 황정연, 기주희 등	이 권고는 디지털 컨텐츠를 배포, 제어 및 추적하는 지적 재산 관리을 제공한다. 이 권고는 DLT 기반 솔루션에서 관련 위협 및 보안 요구사항을 규정한다.
X.ss-dlt	분산원장 기술을 기반으로 한 보안 서비스	Yue Chen 등	이 권고는 DLT 기반 보안 제품 / 서비스를 제공하는 방법, DLT 및 그 사용 사례를 기반으로 실현 될 수 있는 보안 서비스의 예에 대한 권장 사항을 제공한다.
X.stov	분산원장 기술을 사용한 온라인 투표에 대한 보안 위협	박근덕, 염흥열 등	이 권고는 통신 / ICT 인프라에 기반한 DLT를 사용하여 온라인 투표에 대한 보안 위협을 식별한다. 이 권고는 DLT를 사용한 온라인 투표 모델의 예를 제안하고 모델을 근거로 온라인 투표 프로세스의 보안 위협에 중점을 둔다.
X.str-dlt	분산 원장 기술을 기반으로 한 디지털 지불 서비스에 대한 보안 위협 및 요구 사항	김창오, 오경희 등	이 권고는 지불 서비스 사용 사례와 용어를 명확히 한다. 이용 사례 분석을 기반으로 하여 기반 서비스 모델이 설명되고 보안 위협과 문제가 분석된다. 보안 요구사항은 위협과 문제에 대비하여 제공된다.
X.tf-spd-dlt	분산원장기술을 기반으로 한 안전한 소프트웨어 프로그램 배포 메커니즘을 위한 기술 프레임워크	Feng Gao 등	이 권고는 분산원장기술을 기반으로 안전한 소프트웨어 프로그램 배포 메커니즘을 위한 기술 프레임워크을 제시한다.
TR.qs-dlt	양자 안전 DLT 시스템 지침	Ke Wang, 염흥열 등	본 기술보고서는 양자 내성 DLT 시스템을 위한 지침을 제공한다.
X.sa-dsm	DLT 상의 데이터 공유 관리의 보안 구조	Feng Gao 등	이 권고는 분산원장기술을 기반으로 데이터 공유 관리의 보안 아키텍처를 규정한다. 아키텍처를 기반으로 DLT 기반의 데이터 공유 관리 절차와 기능 엔티티 간의 인터페이스를 규정한다.

해당 연구과제에서는 2017년부터 한국, 중국 등의 적극적인 참여로 다양한 국제 표준을 개발 중이다. 현재 SG17에서 개발 중인 분산원장기술 보안 관련 개발 중인 국제표준은 총 12개에 달하며, 그 중 6건의 표준이 한국의 주도로 개발 중에 있다.

한국이 에디터쉽을 확보하여 주도하여 개발하고 있는 권고안은 분산원장기술 용어 정의(X.1400(X.td-dlt)), 분산원장기술의 보안 보증 등급(X.sa-dlt), 분산원장기술을 이용한 데이터 접근 보안(X.das-mgt), 분산원장기술에 대한 보안 통제사항(X.1401(X.sc-dlt)), 분산원장기술을 이용한 전자지불시스템의 보안 위협(X.str-dlt), 분산원장기술을 이용한 전자 투표 시스템 보안(X.stov) 등이 있다. 그 외 5개의 권고안은 중국의 주도로 개발 중이며, 1건은 미국의 주도로 개발 중이다.

2019년 SG17에서는 분산원장기술 보안에 대한 첫 번째 권고안으로 분산원장기술의 보안위협(X.1401)을 채택(AAP)하였다. 해당 권고안은 분산원장기술을 이용한 프레임워크를 개발·구축·운영하는 과정에서 보안위협을 고려할 수 있도록 분산원장기술의 프로토콜·네트워크·데이터 등에 대한 보안위협을 명세하였다. 해당 권고안은 2017년 중국의 제안으로 표준화를 시작하게 되었으나, 진행 과정에서 한국이 지속적으로 기고서를 제출하며 에디터쉽을 확보하여 공동으로 권고안을 개발하였다. 한국은 중국 및 미국과 지속적으로 협의하여 한국의 기고서 내용이 반영된 권고가 개발되도록 하였다.

2019년 8월 회의에서 한국은 분산원장기술 용어 정의를 개발하기 위한 신규 작업항목을 제안하였다. 동 작업항목은 ITU-T FG-DLT의 산출물 중 하나인 용어 정의(FG-DLT D1.1)를 ITU-T 권고안으로 개발하고자 하는 것이다. 신규 작업항목이 분산원장기술 보안 표준화에 있어 중요한 문서임에 대해 중국, 영국, 캐나다 등 대부분의 국가가 동의하였으나, 현재 FG-DLT 산출물이 아직 TSAG에서 SG17에 배정하지 않아서 우선은 이 문서는 기술문서(TR.td-dlt)로 개발을 시작한 후 TSAG 이 이 산출물을 SG17로 전달하면 권고로 변경하기로 하였다. 참고로 지난 9월 TSAG 회의에서 해당 산출물은 SG17 에 배정되었다. 2020년에는 분산원장기술 용어정의 (X.1400)가 채택되었다.

2019년 8월 회의에서 한국은 분산원장기술에 대한 보안 통제 지침을 국제표준으로 개발하기 위해 신규 작업항목을 제안하였으며, 동 회의에서 신규 작업항목(X.1401(X.sc-dlt))으로 채택되었다. 해당 권고안은 미국, 영국, 일본 등 주요국이 필요성을 인정하고 중국, 인도 등도 개발을 지지하였다. 다만 영국과 일본이 ITU-T X.1051 및 ISO/IEC 27002 표준과 연계하여 개발하도록 요구하였으며, 한국은 X.sc-dlt 권고안은 ISO/IEC 27002 표준에서 다루지 않으나 분산원장기술에 반드시 반영되어야 하는 보안 통제 지침에 집중하여 개발하는 것이 목표임을 주장하여 설득하여 신규 작업항목으로 채택되게 하였다.

또한, 한국은 분산원장기술에 대한 보안기술의 표준화 로드맵을 개발하여, 웹사이트에 개

시하고 있다. 해당 로드맵은 ITU-T SG17, ISO TC 307, IEEE 등 표준화기구에서 진행되고 있는 분산원장기술 표준화 활동을 소개하고 있다.

ㅇ (해외 대응 현황)
중국은 X.1401(X.sct-dlt) (DLT 위협) 등을 2017년 8월 회의에 신규워크아이템으로 제안하고 반영했으며 2019년 8월 회의에서 사전 채택되었다. 2019년 11월 ITU-T 최초로 블록체인 분야 국제표준으로 채택되었다. 이외에 중국은 DLT 기반의 지재권 시스템에 대한 신규워크아이템을 제안해 반영하였다. 미국 Aetna는 분산 ID 권고를 신규워크아이템으로 제안해 반영했고, 2020년에 분산 ID(X.1403)를 위한 국제표준으로 채택되었다.

영국은 데이터 공유 및 접근 국제표준(X.1404(X.sa-dlt)) 개발시 프라이버시 우려가 발생하지 않도록 회의에서 구두 의견을 반영하고 있다. 미국과 일본은 전반적으로 국제 표준 개발 과정을 관찰하고 있다. 2020년에는 보안 보증 (X.1404)가 채택되었다.

ㅇ (국내 대응 현황)
한국은 2020년 3월 회의에서 분산원장기술을 이용한 전자지불시스템의 보안 위협(X.str-dlt), 분산원장기술을 이용한 전자 투표 시스템 보안(X.stov) 등의 권고안이 사전채택(AAP)될 수 있도록 추진할 예정이다. 더불어 2020년 9월 회의에서는 분산원장기술 용어 정의(TR.td-dlt), 분산원장기술 보안 보증 등급(X.sa-dlt) 등의 권고안이 사전채택(AAP)될 수 있도록 추진할 것이다. 이를 위해서 각 권고안의 최종안을 다듬어 국제회의에 기고서를 제출할 예정이며, 제출된 기고서가 최종안으로 채택될 수 있게 일본, 미국, 영국 등과 적극적으로 협력할 예정이다.

2019년 8월 회의에서 한국이 제안하여 신규로 개발을 시작하게 된 분산원장기술 보안 통제 지침 권고안(X.sc-dlt)을 지속적으로 개발하기 위해서 한국의 현황을 반영한 기고서를 지속적으로 제출하고, 미국, 중국, 일본, 인도, 아이보리코스트 등과 적극적으로 협력할 계획이다.

한국은 현재 개발하고 있는 분산원장기술에 대한 보안기술의 표준화 로드맵을 지속적으로 업데이트하여 ITU-T 부속서(Supplement)로 개발할 수 있도록 할 예정이다.

ㅇ (국내 대응 필요성 및 전망)
블록체인 보안은 4차 산업혁명시대에서 매우 중요한 신규 기술이며, 다양한 응용 분야를 갖고 있다. 블록체인 시스템에서 보안 및 프라이버시는 필수 기능이다. 현재 과학기술정보통신부 블록체인 연구개발 연구전략을 고려하고 다양한 시범 사업의 추진을 고려하면 한국 주도의 국제 표준화는 계속되어야 한다.

1.4 양자정보통신 보안 보안 표준화 이슈 및 전망

ㅇ (기술개요)

최근 IBM, 구글 등의 양자컴퓨터 상용화 기술 수준 등을 고려할 때 머지않은 미래에 실용 가능한 수준의 양자컴퓨터가 도입될 것으로 보인다. 양자컴퓨터의 실용화는 기존의 신뢰성의 근간이었던 공개키 암호 체계의 안전성에 큰 영향을 준다.

이산대수문제와 소인수분해 문제로 알려진 기존에 풀기 어려운 것으로 다루어지던 다양한 문제를 짧은 시간에 해결함으로써 기존에 안전한 것으로 알려져 사용되고 있던 공개키 기반 암호 알고리즘이 쉽게 해독될 수 있다. 이에 양자컴퓨팅 환경에 내성을 가지는 새로운 공개키 암호 알고리즘을 표준으로 개발하고자 하는 움직임이 미국과 유럽에서 진행되고 있다. 특히 NIST에서는 현재 다양한 후보에 대해서 검토하며 공개키 암호화 및 키교환 알고리즘, 전자서명 알고리즘 등의 표준화를 진행 중이다.

ㅇ Q4/17 표준화 현황

ITU-T SG17 Q4에서도 인큐베이션 과정으로 다가오는 양자컴퓨팅 환경에서 나타나는 새로운 보안 위협에 대응하기 위해서 2018년부터 양자암호통신 기술에 대한 표준화를 추진해 왔다.

표준명	제목	에디터	요약
TR.sec-qkd	통신 네트워크의 양자 키 분배를 보안 프레임워크에 대한 기술 보고서	Matthieu Legré, 심동희	이 기술 보고서는 양자 키 분배의 보안 프레임워크를 제공한다. 통신 네트워크에서 QKD의 보안 기능을 위한 일반 아키텍처인 QKD 네트워크 소개, QKD 시스템과 다른 엔티티 간의 통신을 위한 위협 및 보안 기능에 대해 설명힌다.
X.1702 (X.qrng-a)	양자 잡음 난수 생성기 구조	Matthieu Legré, 심동희 등	이 권고는 양자 엔트로피 소스의 일반적 아키텍처, 잡음 소스의 엔트로피를 추정하는 일반 방법, 난수 추출기를 규정하기 위한 일반 방법을 제시한다.
X.1710 (X.sec-QKDN-ov)	양자 키 분배 네트워크 보안 요구사항 – 개요	Hao Qin, Jiajun Ma	이 권고는 보안 위협을 식별하고 신뢰할 수 있는 노드의 보안 요구사항과 요구사항을 충족하는 일부 구현

			예를 제공한다.
X.1714 (X.cf-QKDN)	양자 키 분배 네트워크에서 생성된 키에 대한 암호학적 기능의 사용	MMatthieu Legré, 심동희	이 권고는 QKD 시스템을 승인할 수 있도록 QKD에 대한 사양을 기존 암호화 표준에 추가하는 것을 목표로 한다. 이 권고는 QKD 시스템에서 생성 및 배포된 키를 기존 표준에 따라 승인 할 수 있도록하는 데 중점을 둔다.
X.sec-QKDN-km	양자 키 분배 네트워크 보안 요구사항 – 키 관리	Matthieu Legré, 심동희 등	이 권고는 QKD 시스템을 검증할 수 있도록 QKD 규격을 기존 암호화 표준에 추가하는 것이다. 이 권고는 QKD 시스템에서 생성 및 분배된 키를 기존 표준에 따라 승인 할 수 있도록 하는 데 중점을 둔다.
X.sec_QKDN_intrq	QKDN과 보안 네트워크 구조의 통합을 위한 보안 요구사항	Kaoru Kenyoshi,	QKDN (Quantum Key Distribution Network)을 위하여, 이 권고는 QKDN을 다양한 사용자 네트워크 (예 : 스토리지, 클라우드, 센서, 콘텐츠 등)와 통합하기 위한 보안 요구사항을 규정한다.
X.sec-QKDN-tn	QKDN 신뢰 노드의 보안 요구사항과 설계	Jiajun Ma 등	이 권고의 목적은 QKD 네트워크의 신뢰할 수 있는 노드에 대한 보안 요구사항에 대한 지침을 한다. 이 권고는 보안 위협을 식별하고 신뢰할 수 있는 노드의 보안 요구사항과 요구 사항을 충족하기위한 일부 구현 예를 제공한다.

2018년 한국의 제안으로 양자암호통신 기술에 대한 신규 작업항목 2건이 채택되었으며, 중국의 적극적인 관심으로 양자암호통신 분야의 표준화가 현재 SG17에서 주요한 표준화 주제 중 하나로 다루어지고 있다. 2018년 채택된 작업항목은 양자 잡음 난수생성기 구조(X.1702(X.qrng-a))와 통신망에서 양자키 분배를 위한 보안 프레임워크 기술문서(TR.sec-QKD) 등이다. 2020년 X.1702 는 국제표준으로 채택되었고, 기술문서(TR.sec-QKD)도 채택되었다.

2020년에 일본은 QKDN과 보안 네트워크 구조의 통합을 위한 보안 요구사항 신규표준(X.sec_QKDN_intrq)을 제안해 채택했다.

ㅇ (해외 대응 현황)
미국, 영국, 중국, 튀니지아, 말레이시아 등의 양자암호통신 표준화에 대한 관심을 표명하였다. 한국은 2019년 3월 회의에서 양자암호통신 보안 연구과제를 SG17에 신설할 것을 제안하였다. 현재 SG17에서 SK텔레콤이 양자암호통신 분야에서 적극적으로 활동하고 있어 신설될 경우 한국이 해당 연구과제의 리더쉽을 확보함으로써 ITU-T 내 양자암호통신 보안 표준화를 주도할 수 있을 것으로 생각되었다. 하지만 캐나다, 영국 등에서 연구과제 신설 시기가 적절하지 않음을 들어 연구과제 신설을 반대하였다. 결국 2019년 9월 회의에서도 해당 연구과제의 신설 여부는 합의를 이루지 못했고, 다음 회기에서 별도의 연구과제로 개설할지에 대해서는 현재 지속적으로 논의 중에 있다.

ㅇ (국내 대응 현황)
한국은 2019년 1월과 8월 회의에서 양자 잡음 난수생성기 구조 권고안(X.qrng-a)을 개발하기 위한 기고서를 지속적으로 제출하였고, 해당 권고안은 2019년 8월 회의에서 ITU-T X.1702 권고로 사전채택(AAP)되었으며, 2019년 11월 ITU-T X.1702는 최종 승인되었다. X.1702 권고가 사전 채택되도록 한국은 중국, 일본, 스위스, 캐나다, 이집트 등과 협의를 통해 지지를 확보하였고, 캐나다, 영국 등의 제안에 대해 적극적으로 대응하여 내용을 보정하였다. 이를 통해서 한국, 중국, 캐나다, 스위스, 영국 등 대부분의 국가가 X.1702 권고의 승인을 지지하였다.

2019년 1월 회의에서 SKT는 통신망에서 양자키 분배 네트워크의 보안 요구사항을 정의하기 위한 신규 작업항목을 제안하였고, 해당 제안은 중국의 적극적인 지지와 캐나다, 영국 등의 동의를 통해서 신규 작업항목으로 채택되었다. 양자키 분배 네트워크에 포함되는 내용이 방대하므로 내용을 구분하여 개요(X.sec-QKDN-ov), 키관리(X.sec-QKDN-km), 신뢰노드(X.sec-QKDN-tn), 생성된 키의 암호화 기능 사용 방법(X.cf-QKDN) 등의 네 개의 권고안으로 개발하기로 합의되었다. 현재 개요와 키관리, 생성된 키의 암호화 기능 사용 방법 등에 대한 부분은 한국에서 에디터쉽을 확보하고 있으며, 신뢰 노드 부분도 적극적으로 개발에 참여하고 있다.

현재 ITU-T의 각 SG는 내년에 개최되는 WTSA-20을 대비하여 다음 회기(2021 ~ 2024) 동안의 연구반 구성에 대해 논의 중이다. SG17에서도 CG를 구성하여 지속적으로 전화회의를 통해 논의를 지속하고 있다. 해당 논의에서 한국은 양자암호통신 표준화가 지속적으로 SG17의 주요 연구과제가 될 수 있도록 지속적으로 제안할 것이며, 이를 통해서 양자암호통신 보안 표준화에 대한 한국의 입지를 공고히 하고자 한다.

ㅇ (국내 대응 필요성 및 전망)

양자정보통신 보안 기술은 산업적 파급효과가 매우 크다. 따라서 국내 이동통신사업자를 중심으로 국제표준화를 추진이 필요하다.

또한, 현재 개발 중인 양자키 분배 네트워크에 대한 권고안 및 기술문서가 2020년 중으로 개발이 완료될 수 있도록 지속적으로 기고서를 제출할 필요성이 있다. 물론 해당 제안이 권고안에 반영될 수 있도록 미국, 영국, 캐나다 등의 의견에 적극적으로 대응할 것이며, 이를 위해서 권고안 개발에 적극 참여하고 있는 중국, IDQ(스위스), 허드슨 연구소(미국) 등과 지속적으로 협력할 예정이다. 이를 통해서 현재 개발 중인 X.1714(X.cf-QKDN), X.1710(X.sec-QKDN-ov), X.sec-QKDN-km 등의 권고가 2020년에 최종 승인 될 수 있도록 노력할 필요가 있다.

2 국제표준화 영향력 확대 방향 및 전략

2.1 국제표준화에서 한국의 취약점

ㅇ 블록체인 보안 분야의 국내 산업체의 참여가 미흡함
- 블록체인 보안 분야의 표준화를 국내 대학, 연구소 중심으로 대응되고 있음, 따라서 과학기술부의 블록체인 시점 사업에 참여하고 있는 산업체의 참여가 필요함
- 블록체인 기반의 분산 ID 시스템은 다양한 산업 부문에 이용될 수 있는 가능성이 매우 크고 산업적 파급효과가 크므로 국내 산업체의 참여가 필요함

ㅇ 5 G 보안 분야의 국제표준화 그룹간의 조정과 국내 산업체 참여가 미흡함
- 5G 보안 국제표준화는 3GPP, ITU-T, IEEE 등에서 분산 추진되고 있어서 표준화 그룹간의 표준 개발과 활용을 위한 조정 활동이 필요함
- 현재 5G 보안 분야 역시 대학 중심으로 대응되고 있음, 따라서 한국 이동통신사를 비롯한 산업체의 참여가 필요함

2.2 취약점 개선을 위한 전략(접근방법 등)

ㅇ 블록체인 보안 분야와 5G 보안 분야 국제표준화에 산업체 참여를 위한 동인 부여 필요
- 추진되고 있는 표준화 현황을 알리고, 개발되는 국제표준의 의견 제시 및 신규 워크아이템의 제안을 위한 산업체의 관심을 유도할 필요 있음
- 마에스트로 사업에서 추진되고 있는 멘토링 제도를 활용해 중소 중견 기업의 국제 표준화 개발 과정의 참여를 유도할 필요가 있음

ㅇ 5G 보안 분야 국제 표준화 그룹간의 조정활동 추진 필요
- ITU-T SG17에 '조인트조정활동(JCA, joint coordination activity)'를 신설해 한국 주도의 국제표준화 그룹간의 조정활동을 추진할 필요가 있음
- 이를 위해 과기부 산하에 신설된 '5G 보안협의회' '표준분과' 활동과 연계해 추진할 필요 있음

2.3 우리나라이 리더쉽 확대 방안

ㅇ (ITU-T SG17 의장단 현황)[4)]

4) http://www.itu.int/net4/ITU-T/lists/loqr.aspx?Group=17&Period=16

개발기구	의장단 현황	이름/소속	특이사항
ITU-T SG17	Q14/17 (DLT 보안)	코라포처 오경희 대표(TCA 서비스)	블록체인 보안 국제표준 개발
	Q4/17 (사이버 보안)	라포처 김종현 박사(ETRI), 부라포처 심동희 팀장(SKT)	양자정보통신 보안 국제표준 개발
	Q6.17 (통신망 보안)	코라포처 백종현 팀장 (KISA)	5G 보안 국제표준 갸발
	Q2/17 (보안 구조)	코라포처 오흥룡 박사(TTA)	SDN, NFV 보안 표준 개발중

ㅇ (ITU-T SG17 한국의 기고 현황)

- (5G 보안) 지난 2019년 8월 회의에 한국은 X.5Gsec-guide(보안 가이드라인), X.5Gsec-t (신뢰관계 프레임워크), X.5Gsec-q (양자내성 알고리즘 활용)에 대해 국가 기고서를 제출해 반영한 실적이 있음.
- (블록체인 보안, 양자정보통신 보안) 한국 주도로 개발중인 국제표준에 대한 국가기고서를 지속적으로 제출해 반영하고 있음

ㅇ (국제표준화 진출 및 확대 필요성 및 전망)

- 우리나라는 관련 연구과제의 라포처를 확보하고 있음
- 따라서 향후에는 새로 개발될 국제표준의 에디터쉽을 학보할 필요가 있음

ㅇ (국제표준화 진출 및 확대 전략)

- 5G 보안 및 블록체인 보안의 경우, 마에스트로 사업의 멘토링 제도를 활용해 산업체 인사와 신규 워크아이템을 제안하고 반영한 후 그 국제표준의 에디터십을 확보케 하는 전략이 필요함

3. 시사점 및 결언

ㅇ (시사점)
- 4차 산업혁명 시대에서 블록체인, 5G, 양자정보통신 보안은 핵심 요소기술임
- 산업적 파급효과가 매우 클 것으로 예측됨
- 보안과 프라이버시가 내재화된 국제표준화 활동은 지속적으로 추진될 필요 있음

ㅇ (정책적 방향 제시)
- 과학기술정보통신부 '5G 보안 협의회'와 블록체인 시범 사업의 결과를 국제표준으로 개발할 필요가 있음

ㅇ (결언)
- 블록체인 보안, 5G 보안 분야의 국제 표준화에 대한 정부의 지원과 관심이 필요함