TTA-19078-SD

ICT 표준 활용·개발 맵 Ver.2020 | SW·AI/방송·콘텐츠/차세대보안 분야 – 지능정보, 클라우드컴퓨팅, 실감방송·미디어, 실감형콘텐츠, 정보·물리보안, 융합보안

http://www.tta.or.kr

실감방송·미디어

디지털 라디오

- 하이브리드 라디오 서비스 기술 (방향 | 전파작속실 | 표준특허전략 | ~'21) ETSI Broadcast DAB, RadioDNS WT
- 표인트 클라우드 부호화 기술 (방향 | 지속/확산공략 | 표준특허전략 | ~'21) JTC1 SC29 WG11
- JVET | ISO/IEC 23090-3, Coded Representation of Immersive Media Part5, Point Cloud Coding, ISO/IEC 23090-9, Part 9: Geometry-based point cloud compression
- 실감형 비디오 부호화 기술 (방향 | 지속/확산공략 | 표준특허전략 | ~'21) JVET, JTC1 SC29 WG11
- JTC1 SC29 | ISO/IEC 23090-5, Coded Representation of Immersive Media Part1, Versatile Video Coding
- JTC1 SC29 | ISO/IEC 23094-1, General Video Coding –Part 1: Essential Video Coding
- 실감형 비디오 부호화 기술 (방향 | 선도경쟁공략 | 표준특허전략 | ~'22) JTC1 SC29 WG11
- JTC1 SC29 | ISO/IEC 23090-4, Coded Representation of Immersive Media – Part 4: Immersive Media Metrics, ISO/IEC 23090-7, Part 7: Immersive Media Metadata
- 원안정해 이미지 부호화 기술 (방향 | 선도경쟁공략 | 표준특허전략 | ~'23) JTC1 SC29 WG1
- JTC1 SG29 | ISO/IEC 21794-1, Plenoptic image coding system (JPEG Pleno) Part1: Framework, ISO/IEC 21794-2, Part2: Light field coding
- 실감미디어 저장장치 기술 (방향 | 선도경쟁공략 | 표준특허전략 | ~'22) JTC1 SC29 WG11
- JTC1 SC29 | ISO/IEC 23090-2, Coded Representation of Immersive Media Part 2, Omni-directional Media Format, ISO/IEC 23090-10, Coded Representation of Immersive Media Part 10, Carriage of Point Cloud Date
- 네트워크 기반 미디어 처리 기술 (방향 | 지속/확산공략 | 표준특허전략 | ~'20) JTC1 SC29 WG11
- JTC1 SC29 | ISO/IEC 23090-8, Coded Representation of Immersive Media Part 8: Network Based Media Processing

실감미디어 부호화

실감미디어 저장 및 처리기술

물입형 미디어 방송

UHDTV

실감형 콘텐츠

- 가능성평가 생태 측정 및 평가 표준 (방향 | 차세대공략 | 표준특허전략 | ~'23) JTC1 SC35 WG1/SC29 WG11, W3C
- TTA | TTAK.KO-10.1106, 이종 센서와 가능성평가 통합 방법, TTAK.KO-10.1107, 가능성평가 측정 평가를 위한 가능성 요구사항 JTC1 SC35 | ISO/IEC 30113-5, Gesture-based interface across devices and methods – Part 5: Gesture Interface Markup Language(GIML), ISO/IEC 30113-12, Part 12: Multi-point gesture for common system actions, ISO/IEC 30113-11, Part 11: Single-point gesture for common system actions, ISO/IEC 30113-13, Gesture-based interfaces across devices and methods – Part 13: Gesture-based interfaces across device.
- 아바타도 3차원기술 원천 및 디지털 정보 표준 (방향 | 선도경쟁공략 | 표준특허전략 | ~'22) GSA
- TTA | TTAK.KO-10.1028, 아바타도 개인 기기 디지털 정보 시스템 표준제조, TTAK.KO-10.0781, 아바타도 개인기기 인증 요구사항, TTAK.KO-10.0782, 아바타도 개인기기 운영관리 표준제조.
- VR 과금 시스템 표준 (추방 | 추격/협력공략 | 표준특허전략 | ~'21) EMV
- EMV | MV For U.S. Acquirers: Seven Guiding Principles for EMV Readiness
- 전자출판 콘텐츠 표준 기술 (선방 | 지속/확산공략 | 표준특허전략 | ~'23) JTC1 SC34, W3C
- TTA | TTAK.KO-10.1102, EPUB DRM 상호 운용 기술 명세서: 전자책 대출 프로토콜, TTAK.KO-10.0905~Part3, 독서 장애인을 위한 전자책 접근성 가이드라인: 개발 가이드, TTAK.KO-10.0399, 전자책 EPUB 3 표준 제작 파일 파싱을 위한 룰셋 규격, TTAK.KO-10.0902~Part1, 독서 장애인을 위한 전자책 접근성 가이드 – Part1: 개발 지침, TTAK.KO-10.0902~Part2, 독서 장애인을 위한 전자책 접근성 가이드 – Part2: 적용 기술
- RRA | KS X 6070-1, 전자책(EPUB) 3.0 개요, KS X 6070-2, 전자책(EPUB) 콘텐 3.0 KS X 6070-3, 전자책 EPUB 3 콘텐츠 제작 및 유통 지침, KS X 6070-4, 전자책(EPUB) 공개 오픈 웹 플랫폼 3.0 KS X 6070-5, 전자책(EPUB) 공개 오픈 웹 플랫폼 3.0 KS X 6080-2, 전자책(EPUB) 콘텐츠 문서 3.0 KS X 6080-3, 전자책(EPUB) 콘텐츠 문서 3.0 KS X 6080-4, 전자책(EPUB) 공개 콘텐츠 문서 3.0 KS X 6080-5, 전자책(EPUB) 미디어 오버레이 3.0 KS X 6080-6, 전자책(EPUB) 접근 애드온 서술자 1
- 디지털 가상현 요구사항 표준 (방향 | 지속/확산공략 | 표준특허전략 | ~'22) IEEE 2888
- IEEE | P2888.3, Sensor Interface for Cyber and Physical World
- 웹기반 콘텐츠 플랫폼 표준 (방향 | 선도경쟁공략 | 표준특허전략 | ~'21) W3C WoT WG, OCF
- TTA | 2019-P0149, 클라우드 환경상 – 데이터 스토리지 페이바이트 개요 및 기능 요구사항, TTAE.OT-10.0426, 클라우드 개방 API 연동 가이드라인
- AIM|CLOUD표준 | CCF.KO-1065/R1, 클라우드 개방 데이터 처리 서비스 요구사항 및 기능 구조, CCF.KO-1066/R1, 클라우드 개방 데이터 처리 서비스 개념, 범위 및 용어정리서.
- ITU-T SG13 | Y.cdf-reqts, Cloud computing-Functional architecture of data storage federation, Y.3505, Cloud computing—Overview and functional requirements for data storage federation

지능정보

로봇 지능지능 및 조작성능 표준

- 로봇 지능지능 및 조작성능 표준 (방향 | 차세대공략 | 표준특허전략) (~ '22) IEEE-ORA, ISO TC299
- TTA | TTAK.KO-10.1070-part1, 지능형 서비스 로봇 운용요구 – 제1부: 일반 사항, TTAK.KO-10.1070-part2, 지능형 서비스 로봇 운용요구 – 제2부: 지능 요구사항, TTAK.KO-10.1070-part3, 지능형 서비스 로봇 운용요구 – 제3부: 운영 요구사항
- 스마트로봇표준프레임 | KOROS 1129-1:2017, 지능형 서비스 로봇 운용요구 제1부 : 일반사항

사람과 로봇의 상호작용을 위한 인지지능 평가 표준

- 사람과 로봇의 상호작용시 로봇을 신뢰할 수 있는 로봇윤리 평가표준 (방향 | 선도경쟁공략 | 표준특허전략) (~ '23) JTC1 SC35, ISO TC299
- 사람과 로봇의 상호작용시 로봇을 신뢰할 수 있는 로봇윤리 평가표준 (방향 | 선도경쟁공략 | 표준특허전략) (~ '23) IEEE-SA
- IEEE-SA | P7000, Model Process for Addressing Ethical Concerns During System Design, P7001, Transparency of Autonomous Systems, P7002, Data Privacy Process, P7003, Algorithmic Bias Considerations, P7007, Ontological Standard for Ethically driven Robotics and Automation Systems, P7008, Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems, P7009, Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems, P7010, Wellbeing Metrics Standard for Ethical Artificial Intelligence and Autonomous Systems

인간과 로봇의 원만한 조화를 위한 표준 개발

- 인간과 로봇의 원만한 조화를 위한 표준 개발 (방향 | 지속/확산공략 | 표준특허전략) (~ '23) JTC1 SC35, ISO TC299
- TTA | 2017-596, 인공지능 서비스의 성능 평가 항목 및 절차
- 스마트로봇표준프레임 | KOROS 1141:2019, 로봇의 정확 · 정확 성능 측정의 최장 및 평가 방법
- KATS | KS B ISO/TS10066, 로봇 및 로봇 장치 – 협동로봇
- ISO TC299 | ISO/CD 18646-3, Robotics – Performance criteria and related test methods for service robots – Part 3: Manipulation
- IEEE-SA | IEEE P7008, Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems

지능 생성/재구성을 위한 오픈인 상호운용성 표준

- 지능 생성/재구성을 위한 오픈인 상호운용성 표준 (방향 | 선도경쟁공략 | 표준특허전략) (~ '22) ISO TC299
- TTA | TTAK.KO-10.0600/R1, 개인정 상호 소프트웨어 플랫폼-제1부: 원칙 및 시스템구조, TTAK.KO-10.0420/R1, 개인정 상호 소프트웨어 플랫폼-제2부: 표준인터, TTAK.KO-10.0808, 개인정 상호 소프트웨어 플랫폼 평가, TTAK.KO-10.0992, 개인정 상호 소프트웨어 플랫폼-제3부: 장치 추상화를 위한 공통 로봇 인터페이스
- 스마트로봇표준프레임 | KOROS 1106-1:2015, 서비스 로봇을 기계적 전기적 모듈화 제부 : 일반사항, KOROS 1067-6, 개인정 상호 소프트웨어 플랫폼 – 제3부 장치 추상화를 위한 공통 로봇 인터페이스
- ISO TC299 | ISO 22166-1, Modularity for service robots – Part1: General requirements

인공지능

빅데이터

지능정보 응용

지능정보 플랫폼

지능정보 보안

정보·물리보안

IT서비스 보안성 평가기준

- IT서비스 보안성 평가기준 (방향 | 전략작속실 | 표준특허전략) (~ '20) JTC1 SC27 WG3, CCRA, CCUF
- TTA | TTAK.KO-12.0356, 클라우드 컴퓨팅 환경에서 개인정보보호 지침
- RRA | KS X ISO/IEC 27009, 정보기술-보안기술-ISO/IEC 27001의 분야별 적용 – 요구사항, KS X ISO/IEC 27011, 정보기술-보안기술-ISO/IEC 27002에 기초한 통신조직을 위한 정보보호관리, KS X ISO/IEC 27003, 정보기술-보안기술-정보보호관리시스템 이행지침
- IT서비스보안사무국 | KECS-PP-0933-2019, 국가용 네트워크 장치를 위한 보호프로파일 V1.0, KECS-PP-0905-2018, 국가용 데이터베이스 접근제어 보호프로파일 V1.0, KECS-PP-0904-2018, 국가용 스마트폰 부팅단계 보호프로파일 V1.0, KECS-PP-0822-2017, 국가용 웹방화벽 보호프로파일 V1.0, KECS-PP-0821-2017, 국가용 보안토큰 보호프로파일 V1.0, KECS-PP-0820-2017, 국가용 데이터베이스 접근제 보호프로파일 V1.0, KECS-PP-0819-2017, 국가용 유선랜인증시스템 보호프로파일 V1.0, KECS-PP-0803-2017, 국가용 침입방지시스템 보호프로파일 V1.0, KECS-PP-0804-2017, 국가용 호스트 침입방지시스템 보호프로파일 V1.0
- JTC1 SC27 | ISO/IEC 15408-1, Evaluation criteria for IT security: Part1: Introduction and general model(Amendment), ISO/IEC 15408-2, Part2: Security functional components(Amendment), ISO/IEC 15408-3, Part3: Security assurance components(Amendment), ISO/IEC 15408-4, Part 4: Framework for the specification of evaluation methods and activities(Amendment), ISO/IEC 15408-5, Part 5: Pre-defined packages of security requirements(Amendment), ISO/IEC 18045, Methodology for IT security evaluation(Amendment), TR 22216, Introductory guidance on Evaluation for IT security(Amendment), ISO/IEC 19896-1, Competence requirements for information security testers and evaluators, ISO/IEC 19896-3, Part 3: Knowledge, skills and effectiveness requirements for CC evaluator, ISO/IEC 15446, Guide for the production of Protection Profiles and Security Targets(Amendment)
- CCRA | Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 5, Common Methodology for Information Technology Security Evaluation, Version 3.1, revision 5, collaborative Protection Profile for Network Devices v2.0

악성코드 분석 정보 공유 포맷

- 악성코드 분석 정보 공유 포맷 (방향 | 차세대공략 | 표준특허전략) (~ '23) JTC1 SC27, IEEE MMDEF, JTC1 SC27
- TTA | TTAE.IT-X.1546, 악성코드 식별 목록 및 속성
- ITU-T SG17 | X.1546, Malware attribute enumeration and characterization
- IEEE MMDEF | MMDEF-B v1.0, Malware Metadata Exchange Format Bibliography

정보보호 관리체계

- 정보보호 관리체계 (방향 | 차세대공략 | 표준특허전략) (~ '21) ISO TC307, JTC1 SC27, ITU-T SG17
- TTA | TTAK.KO-12.0344, 효과적인 정보보호 거버넌스를 위한 금융보안 조직체계 지침, 디지털 변환 정보보호 요구사항 – 표준과 규제간의 비교기술보고서
- RRA | KS X ISO/IEC 27009, 정보기술-보안기술-ISO/IEC 27001의 분야별 적용 – 요구사항, KS X ISO/IEC 27011, 정보기술-보안기술-ISO/IEC 27002에 기초한 통신조직을 위한 정보보호관리, KS X ISO/IEC 27003, 정보기술-보안기술-정보보호관리시스템 이행지침
- JTC1 SC27 | ISO/IEC 27000, 정보기술-보안기술-ISO/IEC 27001 및 ISO/IEC 27002에 기초한 통신조직을 위한 정보보호관리, KS X ISO/IEC 27001, 정보기술-보안기술-ISO/IEC 27002에 기초한 통신조직을 위한 정보보호관리, KS X ISO/IEC 27002, 정보기술-보안기술-정보보호 실무 규칙, ISO/IEC 27003, 정보기술-보안기술-정보보호관리시스템 이행지침, ISO/IEC 27004, 정보기술-보안기술-정보보호 측정, ISO/IEC 27005, 정보기술-보안기술-정보보호 위험관리, ISO/IEC 27006, 정보보호관리시스템 인증기관 요구사항, ISO/IEC 27007, 정보기술-보안기술-정보보호관리시스템 감사 지침, ISO/IEC 27008, 정보기술-보안기술-정보보호 통제 실행 지침, ISO/IEC 27010, 통신기술 보안 및 프라이버시 가이드라인, ISO/IEC 27011, 정보기술-보안기술-ISO/IEC 27002에 기초한 통신조직 사용자 지침, ISO/IEC 27013, 정보기술-보안기술-ISO/IEC 20000-1과 ISO/IEC 27001의 통합 구현 지침, ISO/IEC 27014, 정보기술-보안기술-정보보호 거버넌스, ISO/IEC 27015, 정보기술-보안기술-통신 분야 정보보호 가이드라인, ISO/IEC 27016, 정보기술-보안기술-정보보호 경제 관점, ISO/IEC 27017, 정보기술-보안기술-ISO/IEC 27002에 기초한 클라우드 서비스 정보보호 실무 규칙, ISO/IEC 27018, 정보기술-보안기술-공개 클라우드 컴퓨팅 환경에서 개인정보 처리를 위한 실무 규칙, ISO/IEC 27019, 정보기술-보안기술-에너지 유틸리티 산업 정보보호 실무 규칙, ISO/IEC 27021, 정보기술-보안기술-정보보호 전문가 역량 요구사항, ISO/IEC 27031, 정보기술-보안기술-사업 연속성 정보통신 기술 준비 가이드라인, ISO/IEC 27032, 정보기술-보안기술-사이버 보안 가이드라인, ISO/IEC 27033-1, 정보기술-보안기술-네트워크 보안 – 제1부: 개요 및 개념, ISO/IEC 27033-2, 정보기술-보안기술-네트워크 보안 – 제2부: 네트워크 보안 설계 및 구현 지침, ISO/IEC 27033-3, 정보기술-보안기술-네트워크 보안 – 제3부: 네트워크 보안 위협, 방법 및 요구사항, ISO/IEC 27033-4, 정보기술-보안기술-네트워크 보안 – 제4부: 게이트웨이 간 통신 보안 보호, ISO/IEC 27033-5, 정보기술-보안기술-네트워크 보안 – 제5부: 가상 사설망 보안 지침, ISO/IEC 27034-1, 정보기술-보안기술-응용 프로그램 보안 – 제1부: 개요 및 개념, ISO/IEC 27034-2, 정보기술-보안기술-응용 프로그램 보안 – 제2부: 조직 규범, ISO/IEC 27034-3, 정보기술-보안기술-응용 프로그램 보안 – 제3부: 응용 보안 관리 프로세스, ISO/IEC 27034-5, 정보기술-보안기술-응용 프로그램 보안 – 제5부: 보안 검증 및 검토 프로토콜, ISO/IEC 27034-5-1, 정보기술-보안기술-응용 프로그램 보안 – 제5-1부: 보안 검증 데이터 형식, ISO/IEC 27035-1, 정보기술-보안기술-정보보호 사고 관리 – 제1부: 원칙 및 절차, ISO/IEC 27035-2, 정보기술-보안기술-정보보호 사고 관리 – 제2부: 사고 대응 준비 지침, ISO/IEC 27037, 정보기술-보안기술-디지털 증거 식별, 수집, 획득 및 보존 지침, ISO/IEC 27038, 정보기술-보안기술-디지털 문서 수정 명세, ISO/IEC 27039, 정보기술-보안기술-침입 탐지 및 방지 시스템(IDPS) 선택, 배치 및 운영 지침, ISO/IEC 27040, 정보기술-보안기술-저장 보안, ISO/IEC 27041, 정보기술-보안기술-사건 조사 및 증거 수집 방법 보증 지침, ISO/IEC 27042, 정보기술-보안기술-디지털 증거 분석 및 해석 지침, ISO/IEC 27043, 정보기술-보안기술-사건 조사 원칙 및 절차, ISO/IEC 27050-1, 전자 증거 개시 – 제1부: 개요 및 개념, ISO/IEC 27050-3, 전자 증거 개시 – 제3부: 전자 증거 개시 프로세스 지침, ISO/IEC 27050-4, 전자 증거 개시 – 제4부: 정보 보호 및 보안, ISO/IEC 27550, 개인정보 보호 공학 지침, ISO/IEC 29100, 정보기술-보안기술-개인정보 보호 프레임워크, ISO/IEC 29101, 정보기술-보안기술-개인정보 보호 아키텍처 프레임워크, ISO/IEC 29134, 정보기술-보안기술-개인정보 영향 평가 – 지침, ISO/IEC 29146, 정보기술-보안기술-접근 관리 프레임워크, ISO/IEC 29151, 정보기술-보안기술-개인정보 보호 운영 규범, ISO/IEC 29190, 정보기술-보안기술-개인정보 보호 능력 모델, ISO/IEC 29191, 정보기술-보안기술-부분 익명 및 부분 기밀성 요구사항, ISO/IEC 29184, 정보기술-보안기술-온라인 개인정보 보호 고지 및 동의, ISO/IEC 29187-1, 정보기술-보안기술-위치 기반 서비스 개인정보 보호 프레임워크 – 제1부: 일반 사항, ISO/IEC 29192-2, 정보기술-보안기술-경량 암호화 – 제2부: 블록 암호, ISO/IEC 29192-3, 정보기술-보안기술-경량 암호화 – 제3부: 스트림 암호, ISO/IEC 29192-4, 정보기술-보안기술-경량 암호화 – 제4부: 결정론적 암호화, ISO/IEC 29192-5, 정보기술-보안기술-경량 암호화 – 제5부: 블록 암호 AIRA, 제4부: 블록 암호 LEA, 제5부: 블록 암호 LEA, 제6부: 블록 암호 SEED, ISO/IEC 29192-6, 정보기술-보안기술-경량 암호화 – 제6부: 블록 암호 HIGHT, KS X 3262, 해시 함수 LSH

정보보호 응용

정보보호 기반 기술

- 정보보호 기반 기술 (추방 | 선도경쟁공략 | 표준특허전략) (~ '22) JTC1 SC27, IETF
- TTA | 2016-1893, 파티 인증 표준제품 – 제2부: 파티 인증 프로토콜들, TTAK.KO-12.0334, 해시함수 개발 지침 함수, TTAK.KO-12.0333, 해시 기반 키 유도 함수, TTAK.KO-12.0332, HMAC 기반 공통목적 난수생성기, TTAK.KO-12.0331, 해시 함수 기반 공통목적 난수생성기, TTAK.KO-12.0330, 해시 함수 기반 의사난수 함수, TTAK.KO-12.0329, 단위 키 분배, TTAK.KO-12.0328-Part1, 파티 인증 프로토콜 – 제1부: 일반 모델, TTAK.KO-12.0308, 802.1D 기반 상호운용 이종인 인증 및 키 협의 프로토콜, TTAK.KO-12.0271, 키워드 블록 인증 모드
- RRA | 세션, 블록 암호 및 스트림 암호 – 제2부: 블록 암호 LEA, 제3부: 블록 암호 ARIA, 제4부: 블록 암호 LEA, 제5부: 블록 암호 HIGHT, KS X 3262, 해시 함수 LSH
- JTC1 SC27 | ISO/IEC 9797-2, Message authentication codes(MACs)-Part 2(MD): Mechanisms using a dedicated hash-function, ISO/IEC 18033-3, Encryption algorithm-Part 3(DX): Block ciphers, ISO/IEC 29192-6, Lightweight cryptography – Part 6(DX): Message authentication codes(MACs), ISO/IEC 29192-7, Part 7(RTS): Broadcast authentication protocol, ISO/IEC 29192-2, Part 2(FDIS): Block ciphers, ISO/IEC 11770-4, Amendment 1(DAmd): Unilateral-authenticated key-agreement with identity-based cryptosystems(ECIKAS-IBC), ISO/IEC 18033-6, Encryption algorithms – Part 6: Homomorphic encryption, ISO/IEC 10118-3, Hash-functions – Part 3: Dedicated hash-functions, ISO/IEC 11770-4, Key management–Part 4: Mechanisms based on weak secrets
- IETF | RFC 8554, Leighton-Micali hash-based signatures, RFC 8349, ChaCha20 and Poly1305 for IETF protocols, RFC 8391, XMSS:eXtended Merkle Signature Scheme, RFC 8236, J-PAKE: Password-authenticated key exchange by juggling, RFC 8235, Schnorr non-interactive zero-knowledge proof, RFC 8133, The security-updated standards for password-authenticated key exchange(SESPAKE) Protocol, RFC 8032, Edwards-curve digital signature algorithm(EdDSA)

ID 관리 기술

- ID 관리 기술 (방향 | 선도경쟁공략 | 표준특허전략) (~ '24) ITU-T SG17, ISO TC307, W3C
- TTA | 2019-P0168, 분산형 식별자(Decentralized Identifiers (DIDs)), 2019-P0165, 검증가능한 크레덴셜 데이터 모델 1.0(Verifiable Credentials Data Model 1.0)
- 표준개발기술표준프레임 | 2019-P0168, 분산형 식별자(Decentralized Identifiers (DIDs)), W3C | W3C Candidate Recommendation, Verifiable Credentials Data Model 1.0–Expressing verifiable information on the Web, W3C Draft Report, Decentralized Identifiers(DIDs) v0.13–Data Model and Syntaxes
- ITU-T SG17 | X.sct-ctl, Security threats of distributed ledger technology(ledger technologies, X.dlt-sec, Security considerations for using distributed ledger technology data in identity management
- ISO TC307 | ISO/DTR 23244, Blockchain and distributed ledger technologies–Privacy and personally identifiable information protection considerations, ISO/NP DTR 23245, Blockchain and distributed ledger technologies–Security risks, threats and vulnerabilities, ISO/NP TR 23246, Blockchain and distributed ledger technologies–Overview of identity management using blockchain and distributed ledger technologies

PKI 기반 기술

- PKI 기반 기술 (방향 | 선도경쟁공략 | 표준특허전략) (~ '22) IEEE 802, CAMP, ETSI, 3GPP
- TTA | TTAK.KO-12.0342, 클라우드 커넥트 지침 보안 요구사항, TTAK.KO-06.0441, 양자 키분배망을 위한 차량 통신 규격
- 사물인터넷융합표준 | 2017-0023, 사단 인증형 차량용 내부 네트워크 보안 요구사항, 2017-0090, 클라우드 커넥트 지침의 보안 요구사항
- IEEE | IEEE 1609.2-2016, Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages
- U.S. DOT/NHTSA | Conformance test specifications for Wireless Access in Vehicular Environments(WAVE)-802.11, Test Suite Structure and Test Purposes
- European Commission | Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems(C-ITS)

FIDO 및 공용기술

- FIDO 및 공용기술 (방향 | 선도경쟁공략 | 표준특허전략) (~ '22) FIDO Alliance
- FIDO Alliance | FIDO2, UAF 1.1(Universal Authentication Framework), U2F 1.2(Universal 2nd Factor)

생체인증기반 발화하이오 인증기술

- 생체인증기반 발화하이오 인증기술 (방향 | 선도경쟁공략 | 표준특허전략) (~ '22) ISO TC215, ITU-T SG17, ABC
- TTA | 2018-2251, 생체신호를 이용한 웰니스케어 응용서비스 기술보고서, TTAK.KO-12.0324, 개인건강을 생체신호 정보보호 지침, TTAK.KO-12.0325, 생체신호 인증 요구사항 상호 시험 지침, TTAK.KO-12.0323, 개인건강을 상전도 및 상용량체형 특징점 데이터 교환 표준
- ITU-T SG17 | X.1094, Telebiometric authentication using bio-signals

차세대보안 기반 기술

무인항공시스템 보안

사물인터넷 보안

핀테크 보안

자율자동차 보안

스마트헬스 보안

스마트공장 보안

블록체인기반 IoT 보안표준개발프레임워크

- 블록체인기반 IoT 보안표준개발프레임워크 (방향 | 차세대공략 | 표준특허전략) (~ '22) ITU-T SG20, oneM2M SDS, IEEE-SA, FIDO Alliance
- ITU-T SG20 | Q3/20 IoT-ef–dt, OID-based Resolution framework for translation of distributed ledger assigned IoT resources, Q4/20 TSC-ldm, Framework of blockchain-based self-organization networking in IoT based environment
- IEEE P2418 | P2418, the Frame work of Blockchain Use in IoT

스마트공장 기기 상호 보안인증기술, 스마트공장 정보보호 인증기술

- 스마트공장 기기 상호 보안인증기술, 스마트공장 정보보호 인증기술 (방향 | 전략작속실 | 표준특허전략) (~ '22) IEC TC65 WG10, ISA 99, JTC1 SC27
- TTA | TTAK.KO-12.0307-part1, 산업제어시스템 보안요구사항-제1부: 개념 및 정의, TTAK.KO-12.0307-part2, 산업제어시스템 보안요구사항-제2부: 전반적인 계획, TTAK.KO-12.0307-part3, 산업제어시스템 보안요구사항-제3부: 시스템 보안 요구사항 및 보안 수준, TTAK.KO-12.0307-part4, 산업제어시스템 보안요구사항-제4부: 운영 개발
- IEC TC65 | IEC 62443-1, General Series, IEC 62443-2, Policy & Procedure Series, IEC 62443-3, System Series, IEC 62443-4, Component Series

보안 관리 운영 서버

5G 보안

사이버 위협 대응

보안관리/보안평가

인증기술

암호기술

물리보안

융합보안

자율형 지능보안시스템 구현 방법 표준

- 자율형 지능보안시스템 구현 방법 표준 (방향 | 선도경쟁공략 | 표준특허전략) (~ '22) ITU-T SG16/SG17, SAE Electric Committee, ISO TC22 SC3/SC32
- TTA | TTAE.IT-X.1373, ITS 통신 대역이스를 위한 인증한 소프트웨어 업데이트 프로세스.
- ITU-T SG17 | X.itscec-4, Methodologies for intrusion detection system on in-vehicle systems, X.mdcv, security-related misbehaviour detection mechanism based on big data analytics for connected vehicles, X.itssec-3, Security requirements for vehicle gateway devices, X.1373, Secure software update capability for intelligent transportation system communication devices
- SAE | SAE J2945/5, Service Specific Permissions and Security Guidelines for Connected Vehicle Applications
- ISO TC22 | ISO/SAE AWI 21434, Road Vehicles–Cybersecurity engineering
- ISO TC204 | ISO/AWI TS 21177, ITS–Secure vehicle interface–ITS-station security services for secure session establishment and authentication, ISO/AWI TS 21184, ITS Secure vehicle interface–Data dictionary of vehicle-based information for C-ITS applications, ISO/AWI TS 21185, ITS Secure vehicle interface–Communication profiles for secure connection between an ITS–station and a vehicle

V2X 통신 보안인증 표준 보안 가이드라인

- V2X 통신 보안인증 표준 보안 가이드라인 (방향 | 선도경쟁공략 | 표준특허전략) (~ '20) ITU-T SG17, SAE DSRC Committee, ISO TC204 WG16
- TTA | TTAK.KO-12.0318, 자율차 군집 주행 서비스를 위한 자율 등록 절차, TTAE.IT-X.1373, ITS 통신 대역이스를 위한 인증한 소프트웨어 업데이트 프로세스
- IEEE | IEEE Std 1609.2–2016, Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages
- ITU-T SG17 | X.itssec-5, Security guidelines for vehicular edge computing, X.ecrd, security requirements for categorized data in V2X communication, X.stcv, security threats in connected vehicles, X.itssec-2, Security guidelines for V2X communication systems, X.1373, Secure software update capability for intelligent transportation system communication devices
- SAE | SAE J3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
- ISO TC22 SC32 WG11 | ISO/SAE AWI 21434, Road Vehicles–Cybersecurity engineering

범례

온라인 배포판

- TTA홈페이지(http://www.tta.or.kr)
- 자료마당
- TTA간행물
- ICT표준 활용/개발 맵

표준화 및 표준특허 전략

- 표준화 특성
- 선행: 선 표준화 후 기술개발/상용화 | 병행: 표준화/기술개발 동시 추진 | 후행: 선 기술개발/상용화 후 표준화
- 표준화 전략
- 차세대 공략 | 선도경쟁 공략 | 지속/확산 공략
- 국내 내부 / 국내 외부
- 신규 표준화 선점 가능 분야 | 국제표준 선도가능 분야 | 후속/개정 표준 및 시장확산 필요 분야
- 추격/협력 공략 | 전략적 수용
- 다각화 협력 필요 분야 | 국제표준 수용/적용 분야
- 기획 | 국제 표준화 단계 | 채택
- 표준화 전략
- 표준개발 | 표준 및 R&D 초기 전략 | 표준 및 R&D 중후기 전략
- 기초연구 | 과제승인 | 개발 | 검토 | 표준채택
- 기초연구 | 실험 | 시작품 | 제품화 | 사업화
- 연구개발 | 출처 : KSTA

* 본 자료는 정부(과학기술정보통신부) 정보통신방송표준개발지원 사업의 일환으로 수행된 과제(No. 2017-0-00059, ICT표준화 체계분석 및 전략연구) 연구결과로 발간된 자료입니다.

TTA 한국정보통신기술협회 Telecommunications Technology Association