포스트코로나 시대 대응을 위한 개인정보보호 표준화 이슈

염흥열, PhD

순천향대학교 정보보호학과 교수
ITU-T SG17 국제의장

목차

뉴 노멀 시대
선도를 위한
ICT 표준의
역할

국제표준 개발 및 활용

- 개인정보 국제 표준 요구사항
  - 국가 규제를 만족하기 위한 요구사항
  - 위험 평가 결과로부터 요구사항
  - 기업 정책과 계약으로부터 요구사항
- 국제 표준 활용 단계
  - 인증 기준으로 활용
  - 개인정보처리자에 대한 신뢰도 증가
  - 국제 표준에 근거해 개인정보 처리자 운영 규칙 정의
  - 글로벌 차원의 서비스 상호 연동성 강화, 투명성 및 실용성 강화

★ 법 준수 입증 자료

ISO/IEC 29100 – 프라이버시 프레임워크 (2011)

GISC2020
Global ICT Standards Conference

뉴 노멀 시대
선도를 위한
ICT 표준의
역할

개인정보보호 원칙 (29100)

❑ 11대 프라이버시 원칙
- 동의 및 선택
- 목적 합법성 및 목적 명세
- 수집 제한
- 데이터 최소화
- 이용, 보유, 제공 제한
- 정확성 및 품질
- 공개, 투명성, 고지
- 정보주체 참여 및 접근
- 책임성
- 정보 보안
- 프라이버시 법 준수

★ 가명 정보와 익명 정보 정의

개인정보보호법 원칙 (2011년)

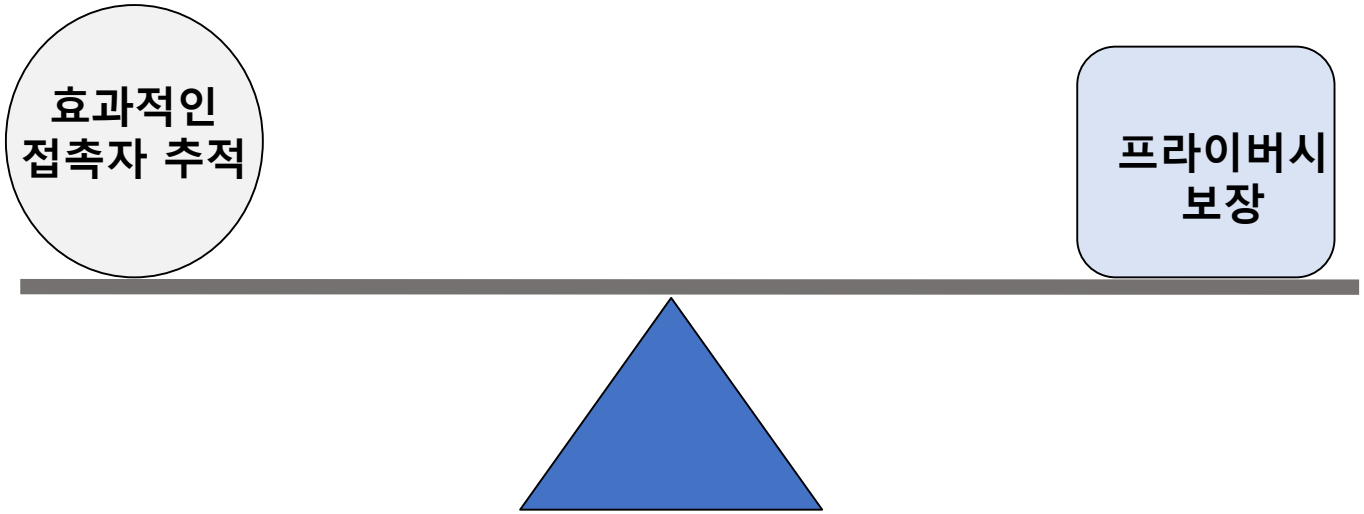
❑ 개인정보보호법 제3조 보호 원칙
- 처리 목적 명확
- 처리 최소화
- 목적 적법성
- 목적 외 용도 활용 금지
- 정확성, 완전성 및 최신성 보장
- 안전 관리
- 처리 공개, 정보주체 권리 보장
- 정보주체 사생활 침해 최소화
- 익명 처리
- 법 및 관계 법령 준수

★ 가명 정보 도입 및 활용 근거, 2020년

목차

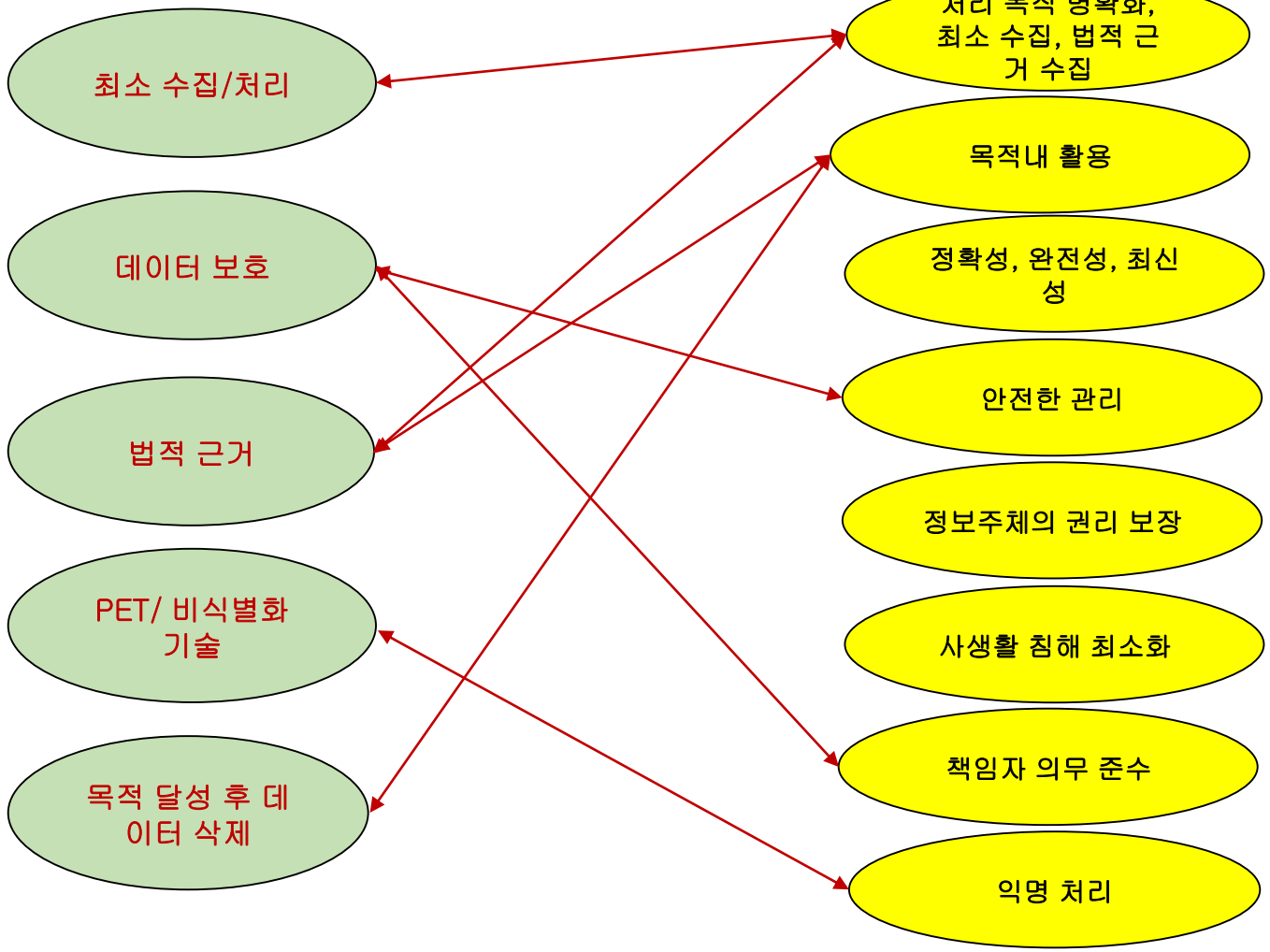
확진자 동선 추적과 프라이버시와 절충

- 검사·확진, 역학·추적, 격리·치료 (3T, test-trace-treat)
- 역학조사 – 추적은 감염병 확산 방지를 위한 유효한 수단
- 국내 접촉자 추적 관리 시스템
  - 역학조사 지원시스템, 자가 진단 앱, QR 코드 기반 전자출입명부
- 확진자 동선 추진의 효과성과 프라이버시 보호와의 균형점



국내 감염병 추적 관리와 개인정보 보호 원칙

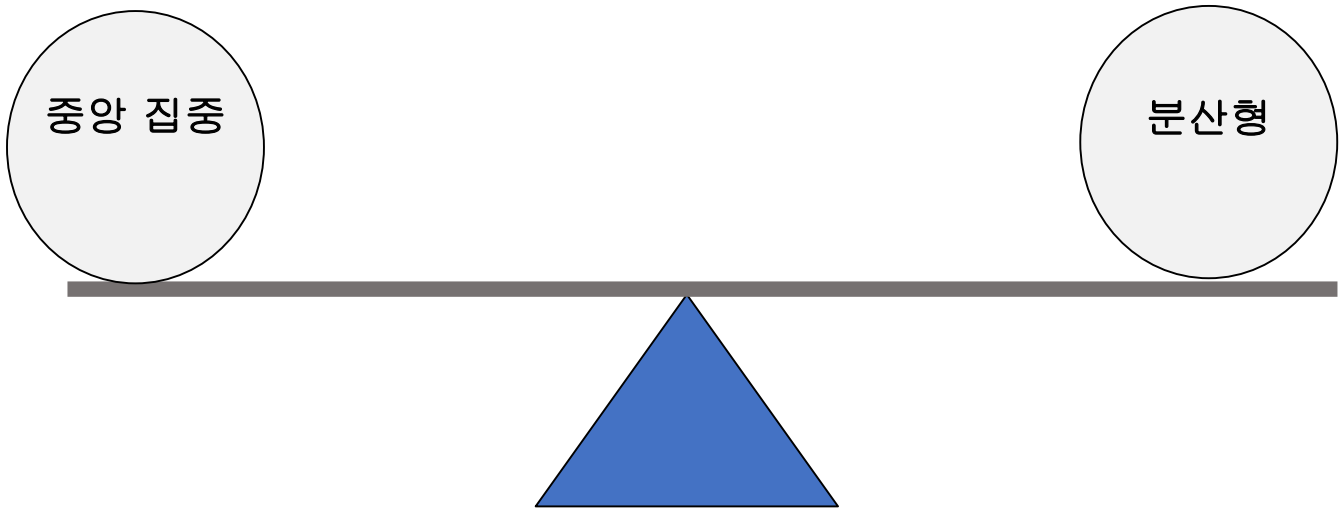
국내 감염병 관리 체계에서 중요하게 고려되어야 할 보호 원칙



국내 개인정보보호법 원칙

감염병 추적 관리 시스템 방식

- 추적 관리 체계 유형
  - 완전 중앙 집중
  - 브루투스 기반 중앙 집중
  - 브루투스 기반 분산 방식 – 구글, 애플 등



브루투스 기반 추적 관리 – 분산형, 집중형

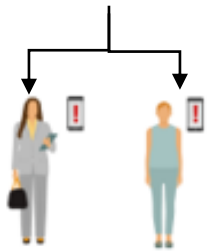
이용자 A와 이용자 B는 인접 시 "키코드"를 서로 교환.

코로나-19 감염.

이용자 A가 감염되면, 앱에서 자신의 상태를 감염으로 변경.

집중형

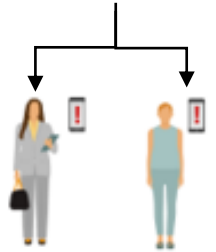
폰은 서버에 자신의 익명 ID와 다른 폰에서 수집된 "키코드"를 중앙 데이터베이스에 제공.



서버는 자신의 데이터베이스에서 수신된 "키코드"와 일치된 이용자 연락처 확인, 해당 이용자에게 경고 메시지 전달.

분산형

폰은 자신의 익명 ID만을 중앙 데이터베이스에 보냄. 서버는 익명 ID에 대응되는 "키코드" 값 저장.



폰은 서버 데이터베이스 다운로드 받아서, 자신의 폰의 키 코드와 비교해, 일치하면 경고 메시지를 이용자에게 전달.

분산형 브루투스 기반 추적 관리 – 구글, 애플 등

- 명시적 동의 기반
- 위치 정보 사용하지 않음
- 추적을 막기 위해 20분마다 랜덤 브루투스 ID 갱신
- 해당 폰에만 노출 통지
- 접촉 추적 용으로만 사용
- 필요치 않을 때 추적 관리 시스템 불능화

QR 코드 기반 전자출입명부 - 개요

특징

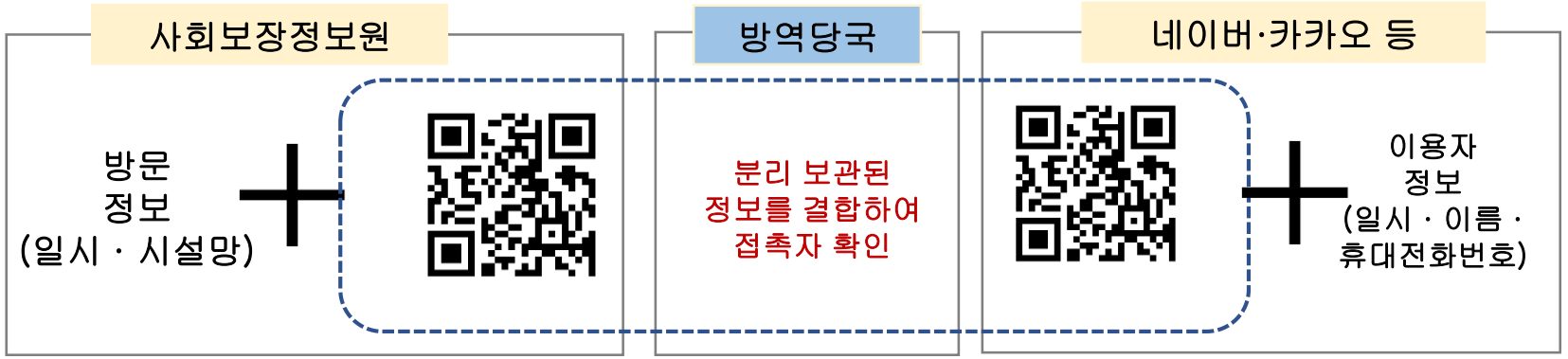
- 집단감염 우려가 큰 고위험시설에 대한 QR코드 기반의 전자출입명부 시스템 의무 도입
- 일반 다중이용시설에 대해서도 자율 도입
- 비밀 공유 기법 이용

의무 도입 고위험 다중 이용 시설

- 헌팅포차, 감성주점, 유흥주점(클럽·룸살롱 등), 단란주점, 콜라텍, 노래연습장
- 실내집단운동시설(줌바·태보·스피닝 등 격렬한 단체운동), 실내 스탠딩 공연장 (관객석 전부 또는 일부가 입석으로 운영되는 공연장)

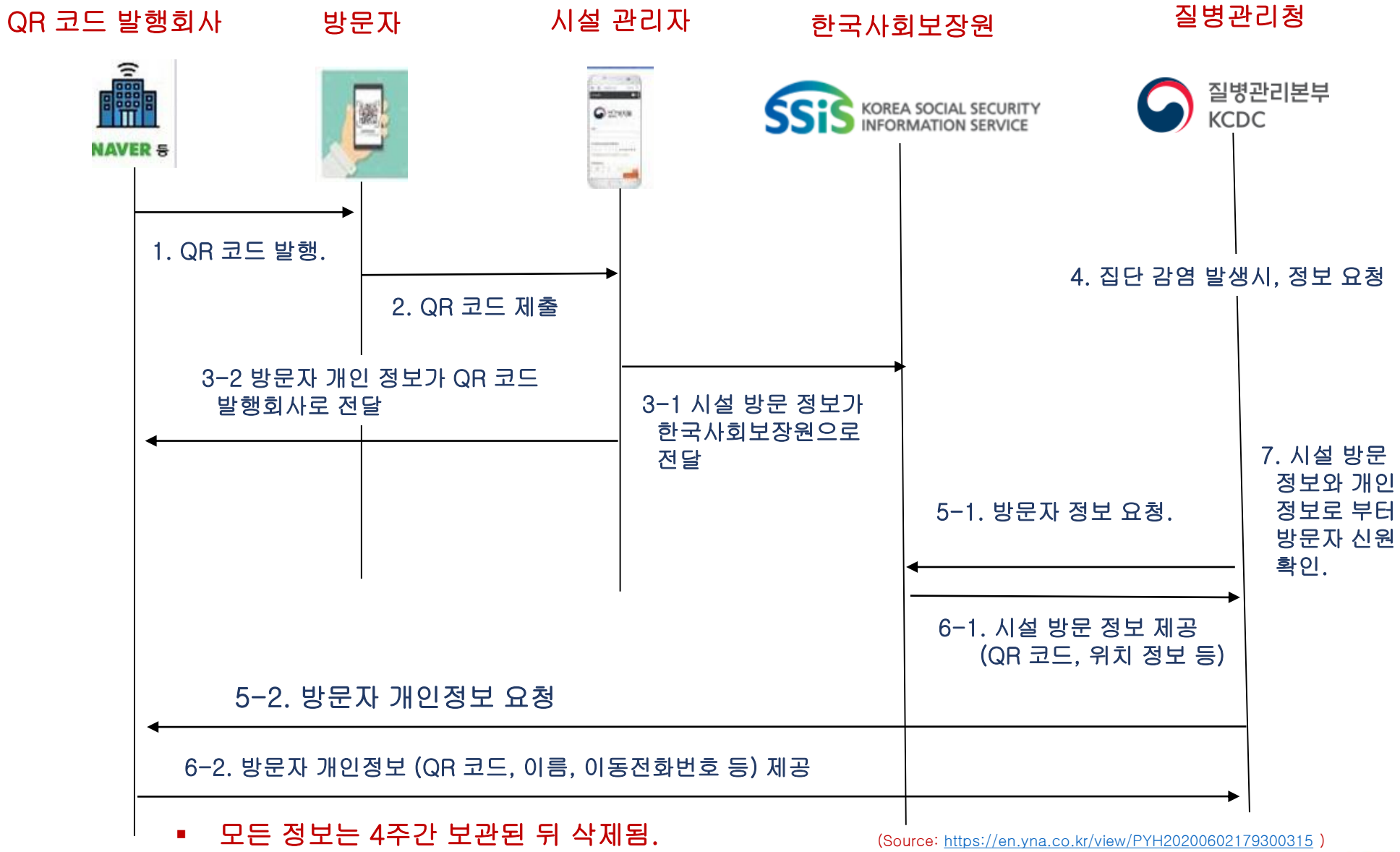
실적

- 3개월(2020.6.1 – 8.31) 간 약 23만개 업소가 앱 설치, 이용자는 7,215만 건 활용, 4주가 지나 자동 파기된 개인정보는 4,069만 건



뉴 노멀 시대
선도를 위한
ICT 표준의
역할

QR 코드기반 출입명부 동작 흐름도

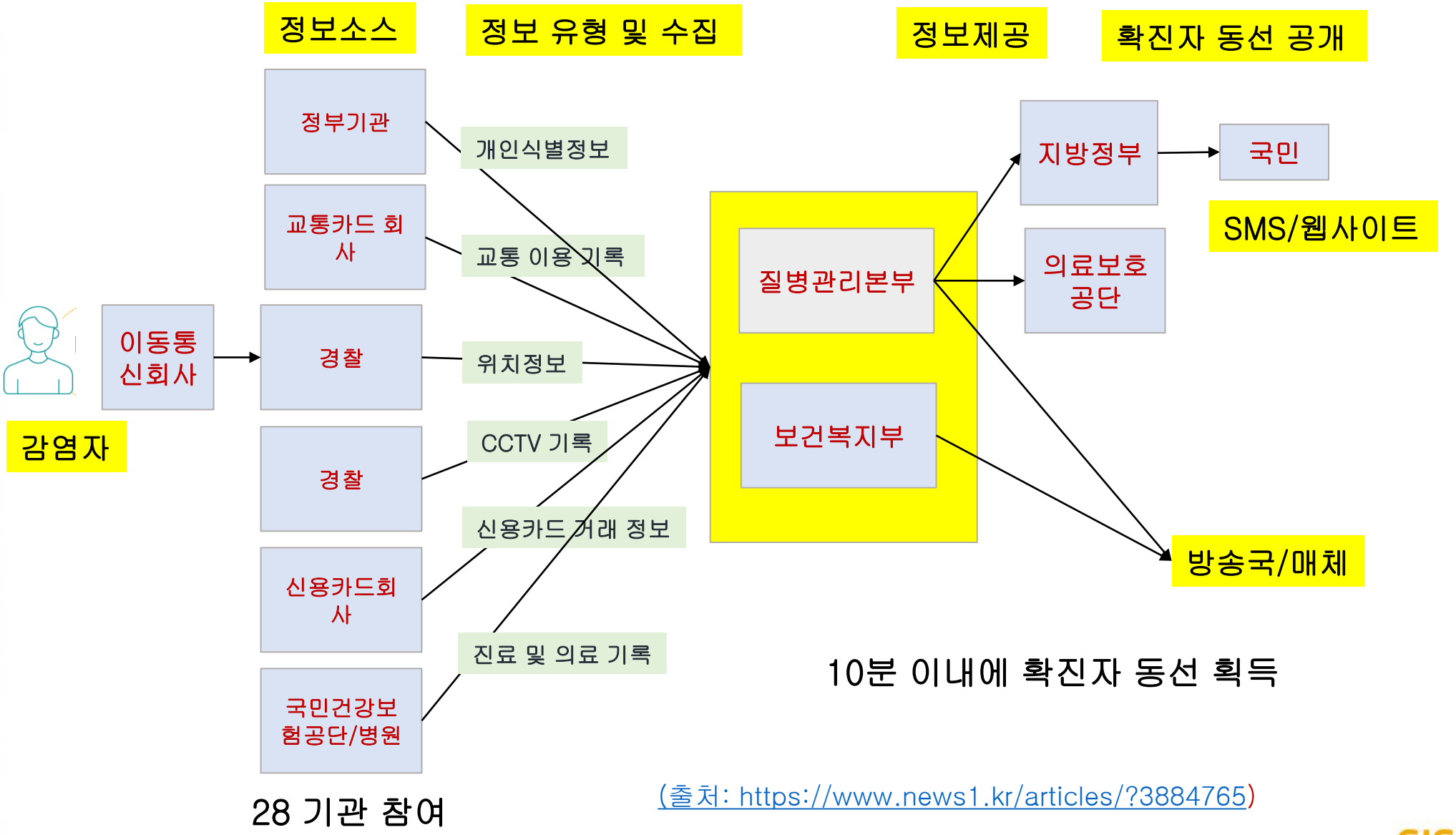


- 모든 정보는 4주간 보관된 뒤 삭제됨.

(Source: https://en.yna.co.kr/view/PYH20200602179300315)

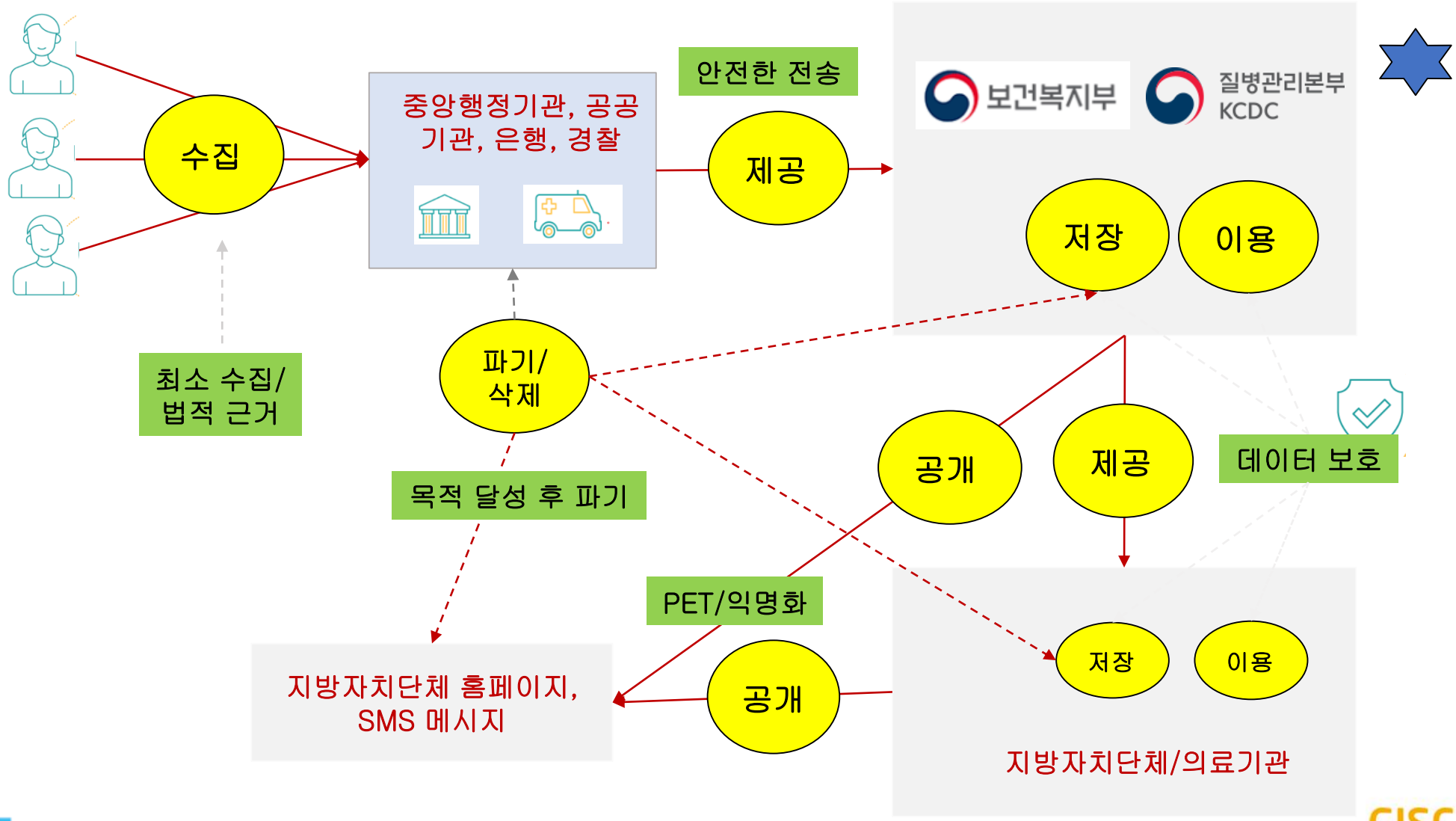
뉴 노멀 시대
선도를 위한
ICT 표준의
역할

코로나19 역학조사 시스템 – 소스, 유형, 수집, 공개



(출처: https://www.news1.kr/articles/?3884765)

국내 감염병 추적 지원 시스템 – 프라이버시 보호 대책



소결론

- 보건 안전을 확보하면서 프라이버시를 고려해야 K 방역 감염병 접촉자 추적 관리체계가 글로벌 표준이 될 수 있음
  - 목적: 감염병 추적 용
  - 관리: 기술적 및 관리적 보호조치, QR 코드 기반 전자출입명부 – 비밀 분산 기법 적용
  - 최소 수집의 원칙: 수기 출입명부의 경우, 이름, 전화번호만 수집
  - 이용, 제공 제한: 제공 기관의 제한
  - 파기: 목적 달성 후 반드시 파기
- 팬데믹 상황에서 중앙집중 방식과 분산 방식 중 어느 방식이 좋은 지 ?
- 새로운 놈 (표준)의 적용이 필요
- 기존 프라이버시 국제 표준에 근거한 국내 감염병 추적 관리 관행 개선
- 감염병 예방 법에 개인정보보호 가이드라인에 대한 항목 제정 필요
  - 공개/저장 개인정보의 이용 목적 달성 후 삭제
  - 관리되는 개인정보의 기술적/조직적 보호조치 달성
  - PET 기술을 활용한 기술적 대안도 고려해야 함

목차

- 시작하면서
- 감염병 추적 관리 체계와 개인정보 보호
- 분산 신원확인과 온라인 인증
- 개인정보보호 국제표준화 기구 및 현황

뉴 노멀 시대
선도를 위한
ICT 표준의
역할

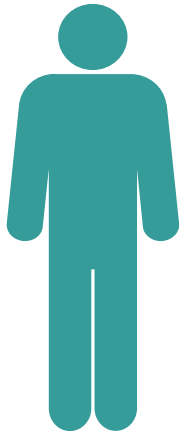
디지털 신원(identity)

신원 확인 (identity verification)

(실세상)

사이버 공간

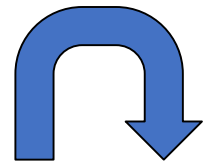
발행



신분증

신원 증명 (identity proofing)

간접 신원 증명



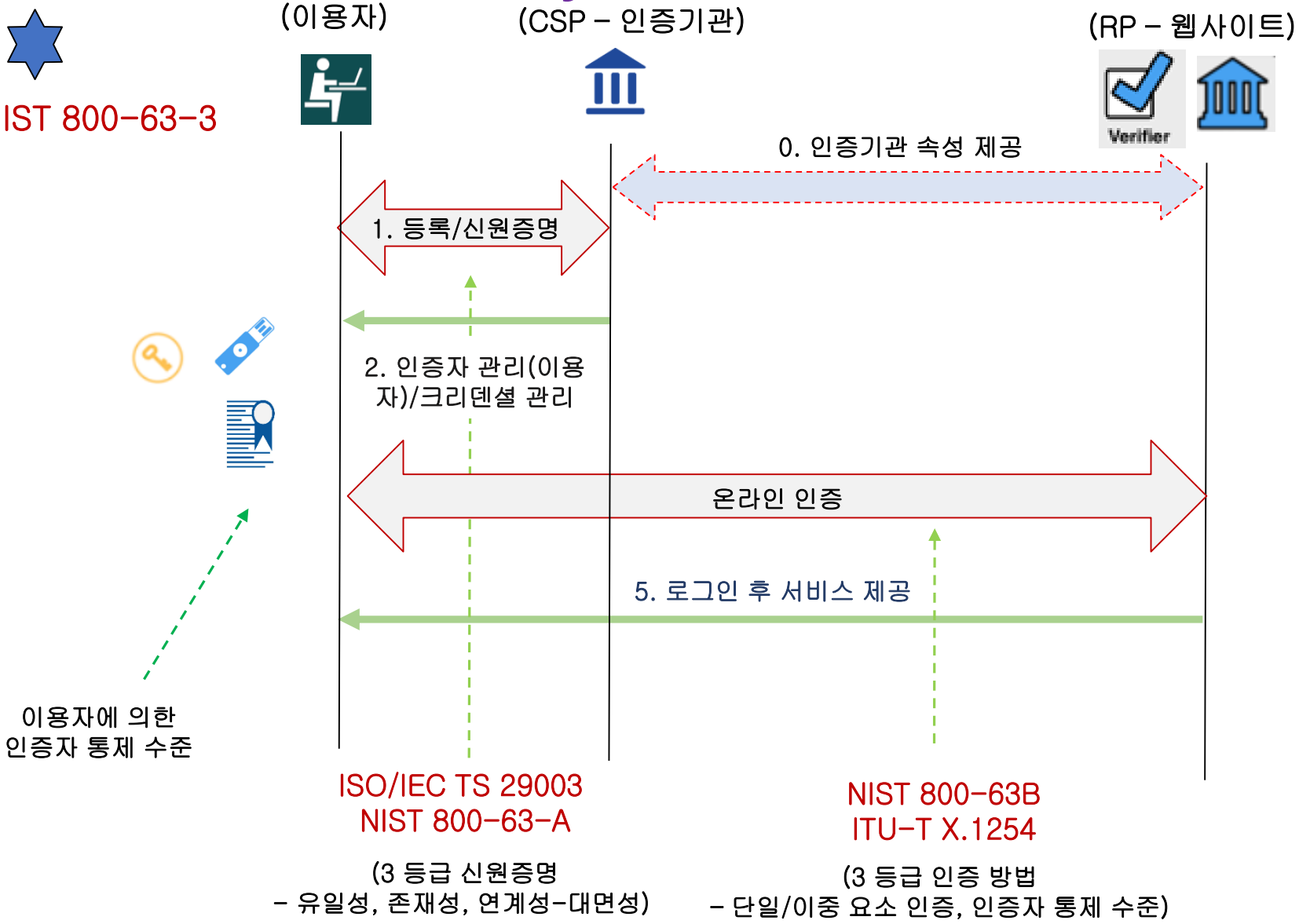
인증
(authentication)

상점/은행

e-ID (모바일 공무원증 등)

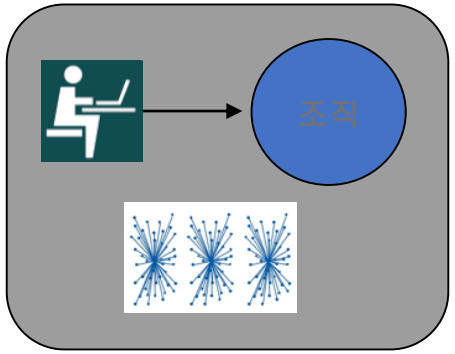
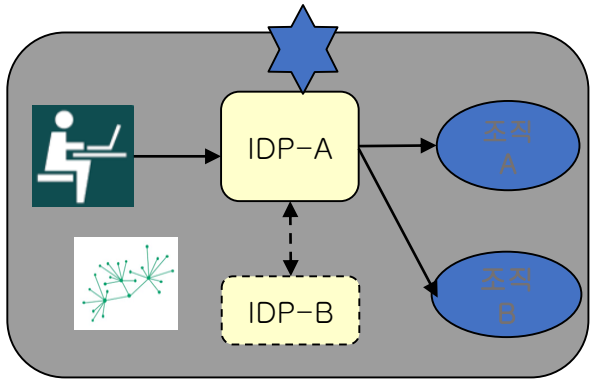
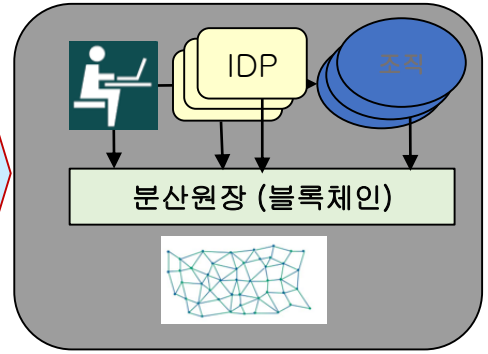
뉴 노멀 시대
선도를 위한
ICT 표준의
역할

디지털 신원(identity) 절차 - NIST 800-63-3



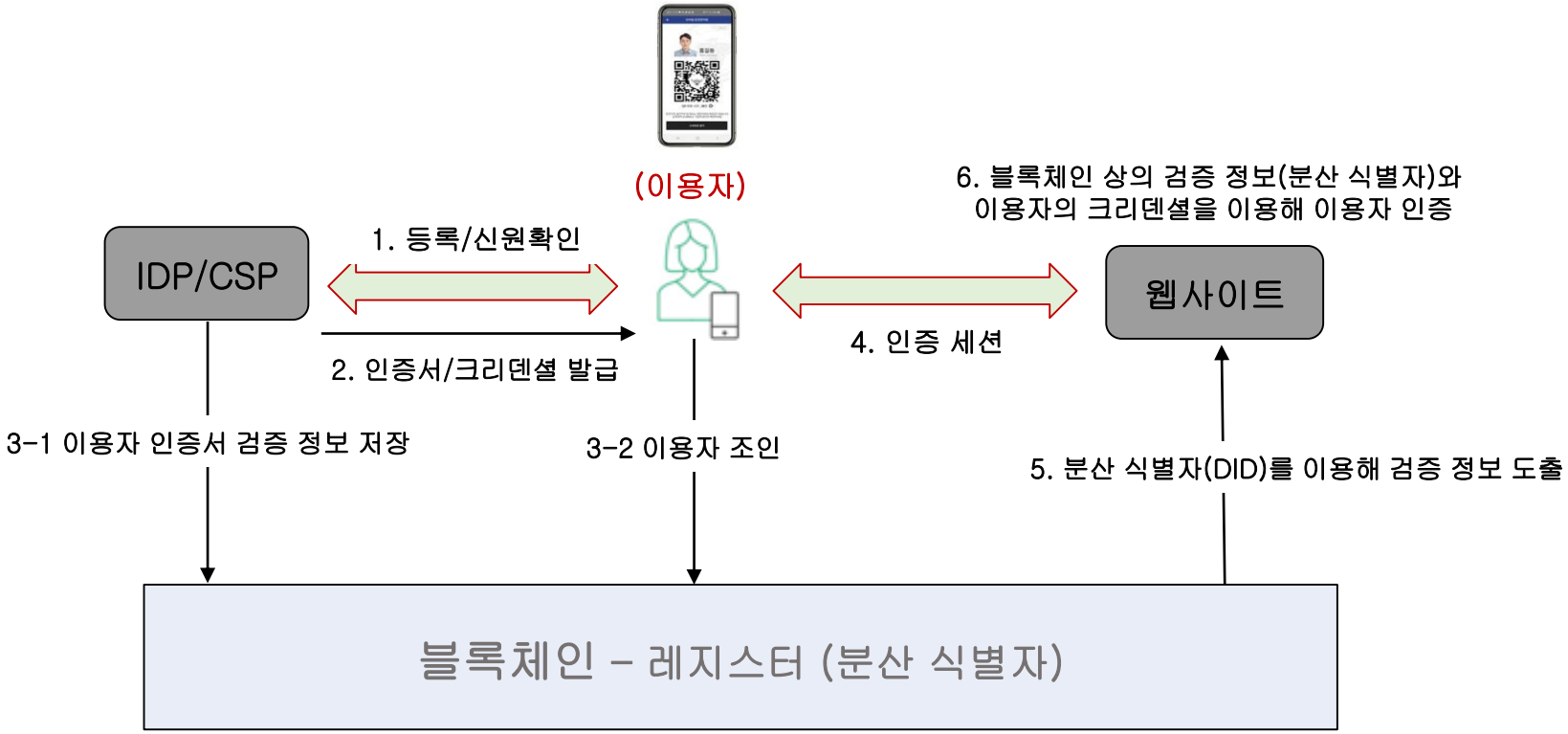
뉴 노멀 시대
선도를 위한
ICT 표준의
역할

디지털 신원 관리 모델

	(중앙집중 ID 모델-제1세대)	(연계 ID 모델-제2세대)	(분산 ID 모델-제3세대)
모델			
요소 기술	▪ ID/PW, 다중 요소 인증 ▪ 싱글사인온 ▪ TLS	▪ OpenID ▪ OASIS SAML (ITU-T X.1141)	▪ 분산원장기술 ▪ 암호기술
특징	▪ 기업마다 각각 신원정보 관리 체계 유지 ▪ 기업이 이용자 데이터 통제 ▪ 이용자의 크리덴셜 데이터가 공격의 하니팟	▪ IdP 가 로그인 크리덴셜을 관리 ▪ 여러 조직간의 IDP를 통한 로그인 연계 ▪ IDP 크리덴셜이 공격의 허니팟	▪ 이용자 지갑 (wallet) 에서 자신의 신원 정보 관리 ▪ 자기 통제 분산 데이터로 인해 데이터 노출 우려 감소
국내 예	▪ ID 연계 없는 대학이나 기업의 ID 관리	▪ 아이핀 (As Is)	▪ 분산 ID 얼라이언스 (To Be)

뉴 노멀 시대
선도를 위한
ICT 표준의
역할

분산 신원확인(DID)



신원증명 - ISO/IEC TS 29003/NIST 800-63

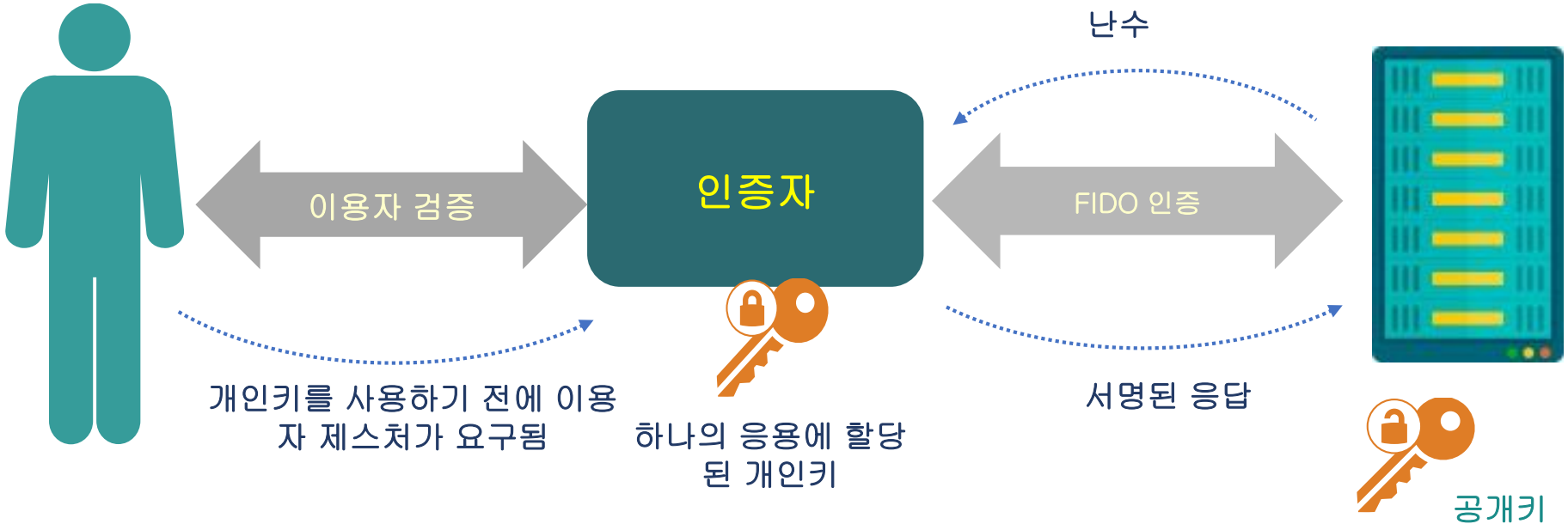
- 등급 분류 기준
  - 유일 (unique)
  - 존재 (existence)
  - 결합 (binding)

- 보증 등급
  - 등급 1
    - (29003) 신원 유일성, 존재성 전제, 주체가 신원에 결합되다고 가정
    - (800-63-3) 실세상 신원과 연결하는 요구사항 없음
  - 등급 2
    - (29003) 신원 유일성, 약한 존재성 수립, 정보주체가 신원과 어느정도 결합됨
    - (800-63-3) 실제 존재, 원격 또는 대면
  - 등급 3
    - (29003) 신원 유일성, 강한 신원 존재성 수립, 정보주체가 신원과 강하게 결합됨
    - (800-63-3) 대면, 식별 속성 검증

FIDO 인증 - 높은 보증 수준의 강한 인증

- 높은 수준의 인증 =
  - 이중 인증 요소 시용 
  - 적어도 하나의 공개키 암호 이용 
  - 피싱, 중간자 공격 / 다른 타깃 공격에 취약하지 않음

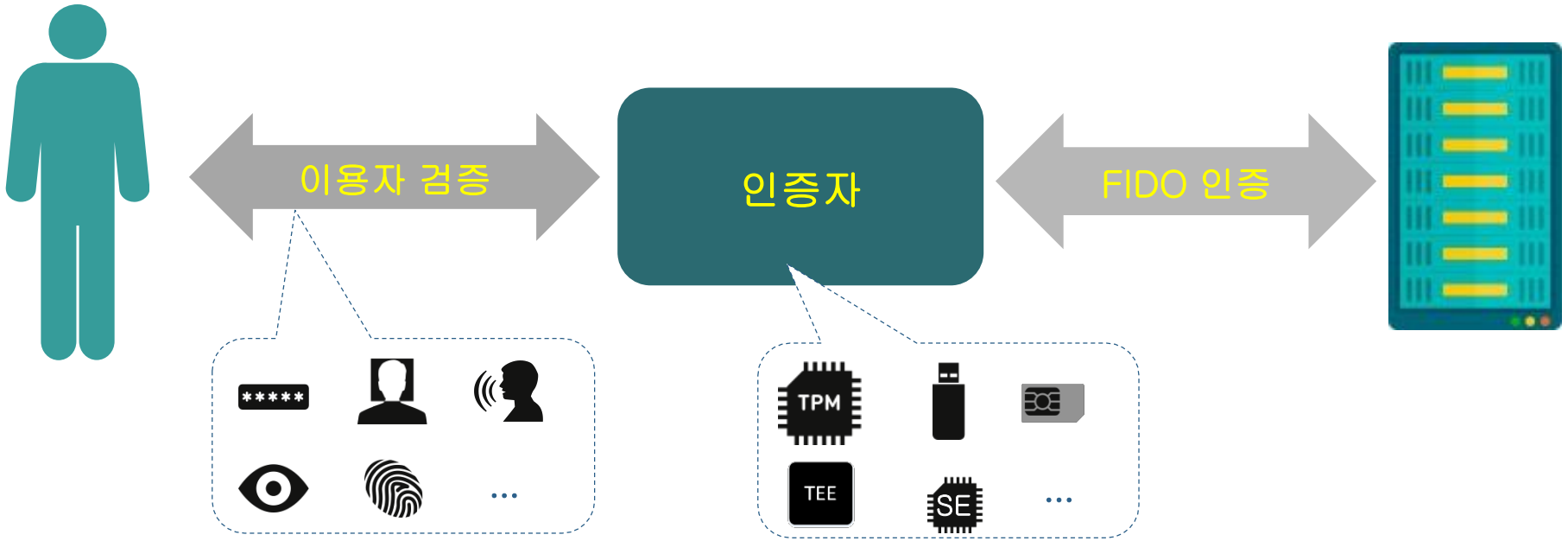
FIDO 인증 원리 – 구성요소



가정

- 공개키 암호 체계 기반
- 개인키를 안전한 영역에 보관 관리
- 생체 인증 이용 가능
- 개인키는 사용자 단말에 보관
- 공개 정보만이 서버에 저장

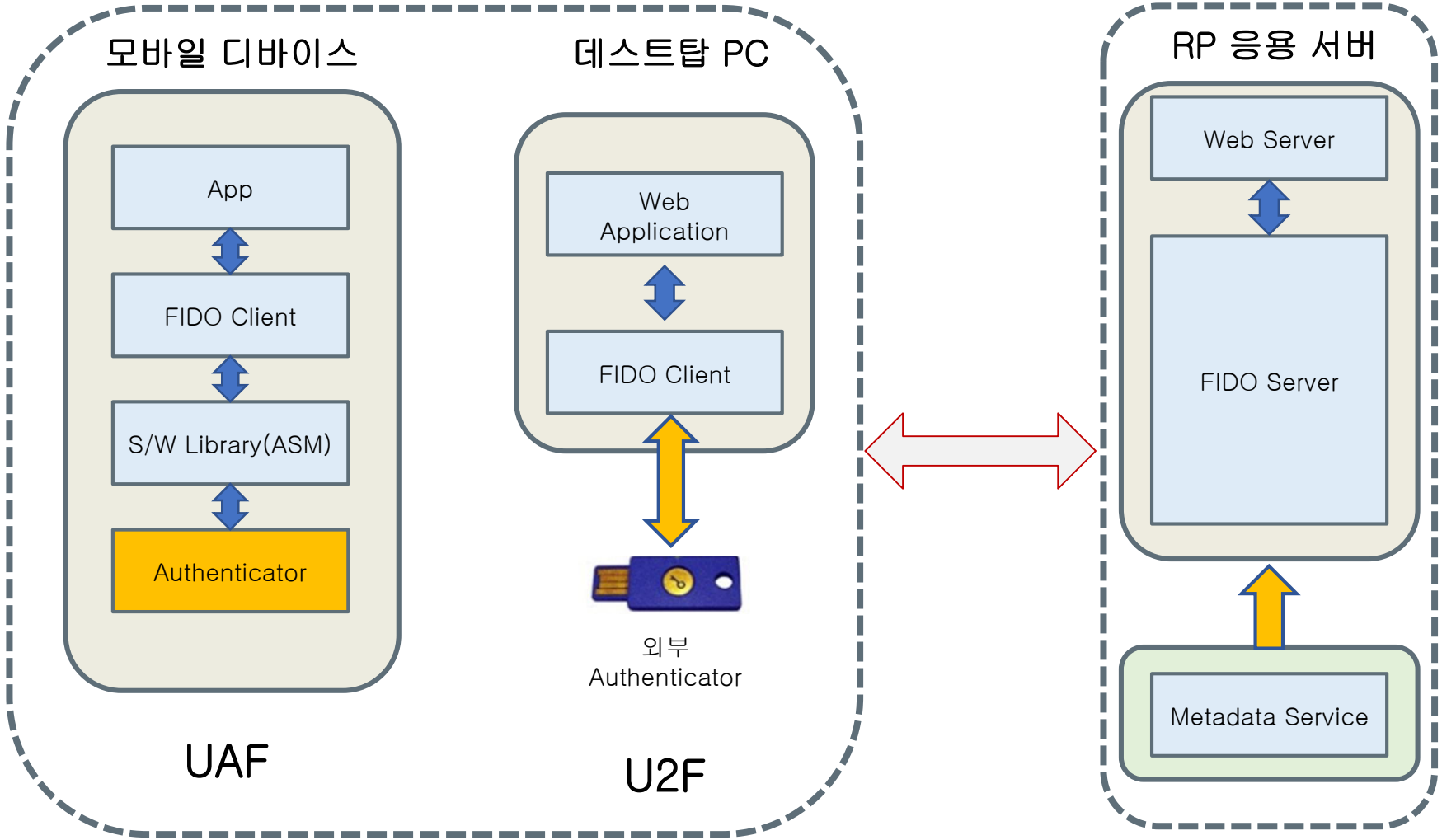
FIDO 인증 원리 – 세부 요소 기술



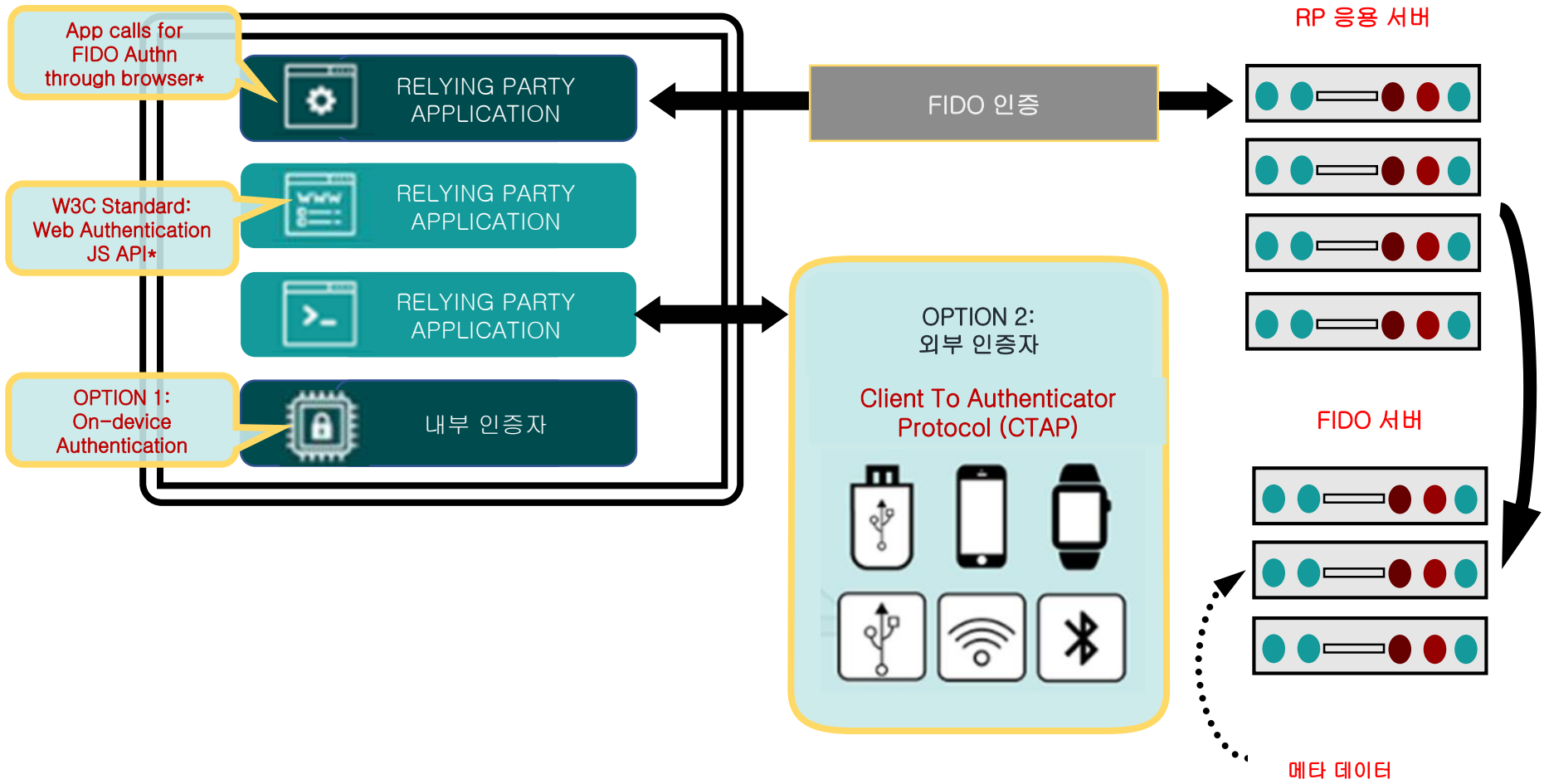
FIDO 인증 원리 - 등록


Signed Attestation Object
AUTHENTICATOR
AUTHENTICATOR
Private
attestation key
FIDO 등록
메타 데이터
Verify using trust anchor inc
luded in Metadata
Understand Authenticator
security characteristic by
looking into Metadata from
mds.fidoalliance.org

FIDO 표준 – UAF / U2F



FIDO2.0 표준 – UAF / CTAP / U2F



뉴 노멀 시대
선도를 위한
ICT 표준의
역할

전자서명/인증 - 국제 표준화 그룹

소결론

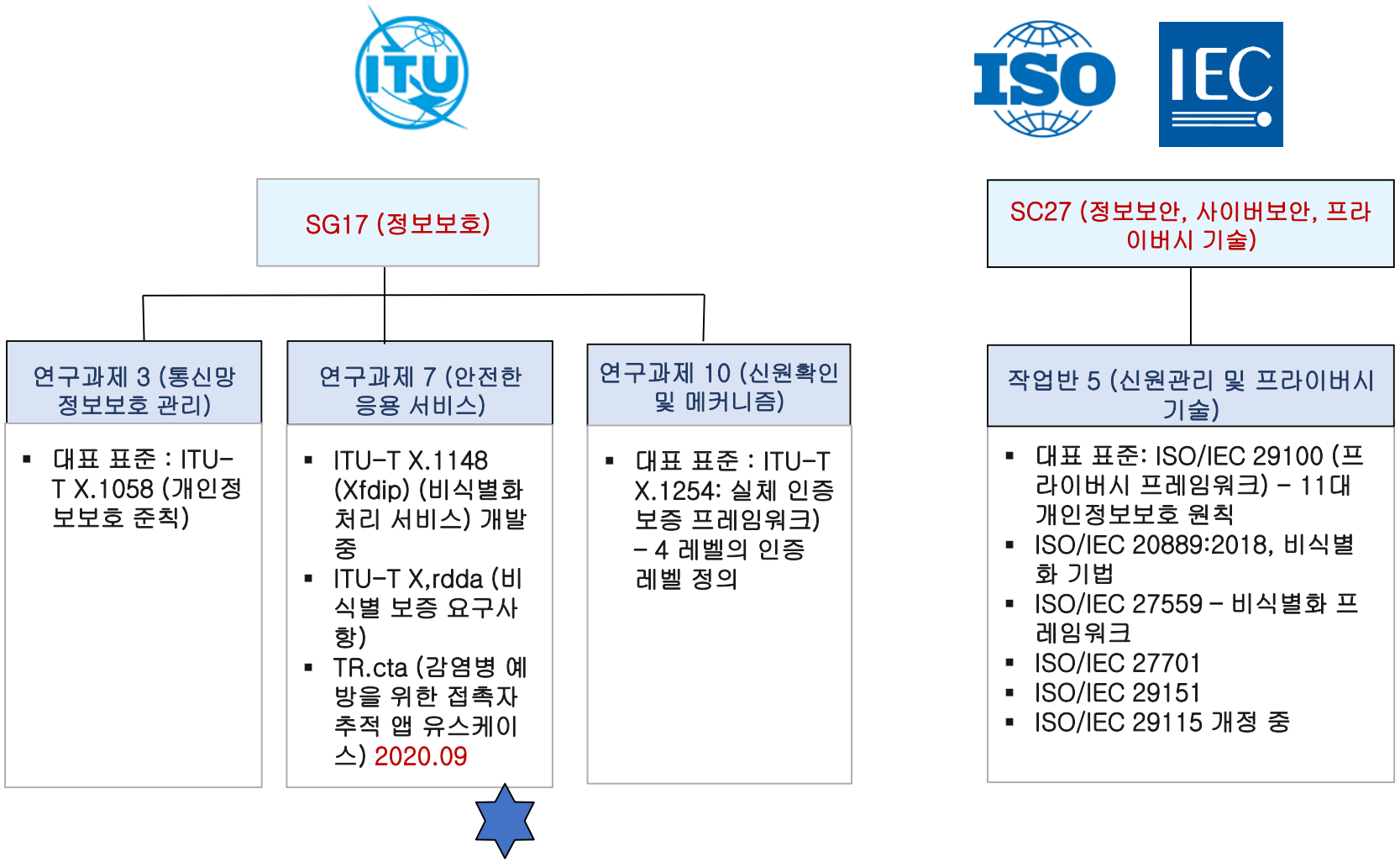
- 안전한 온라인 신원 확인을 위해서는 안전한 인증 방식의 채택이 매우 중요함
- 국제 표준에 근거한 온라인 인증 체계 구축
- 등록/신원 증명, 크리덴셜 관리, 인증/서명 과정에서 안전성 확보
  - 안전 영역 (모바일) / 하드웨어 기반 크리덴셜 관리(PC)로 전환
- 편리하면서도 안전한 인증 및 전자 서명 체계 유지
- 글로벌 인증 및 전자서명 사업자와 경쟁체제 대비

목차

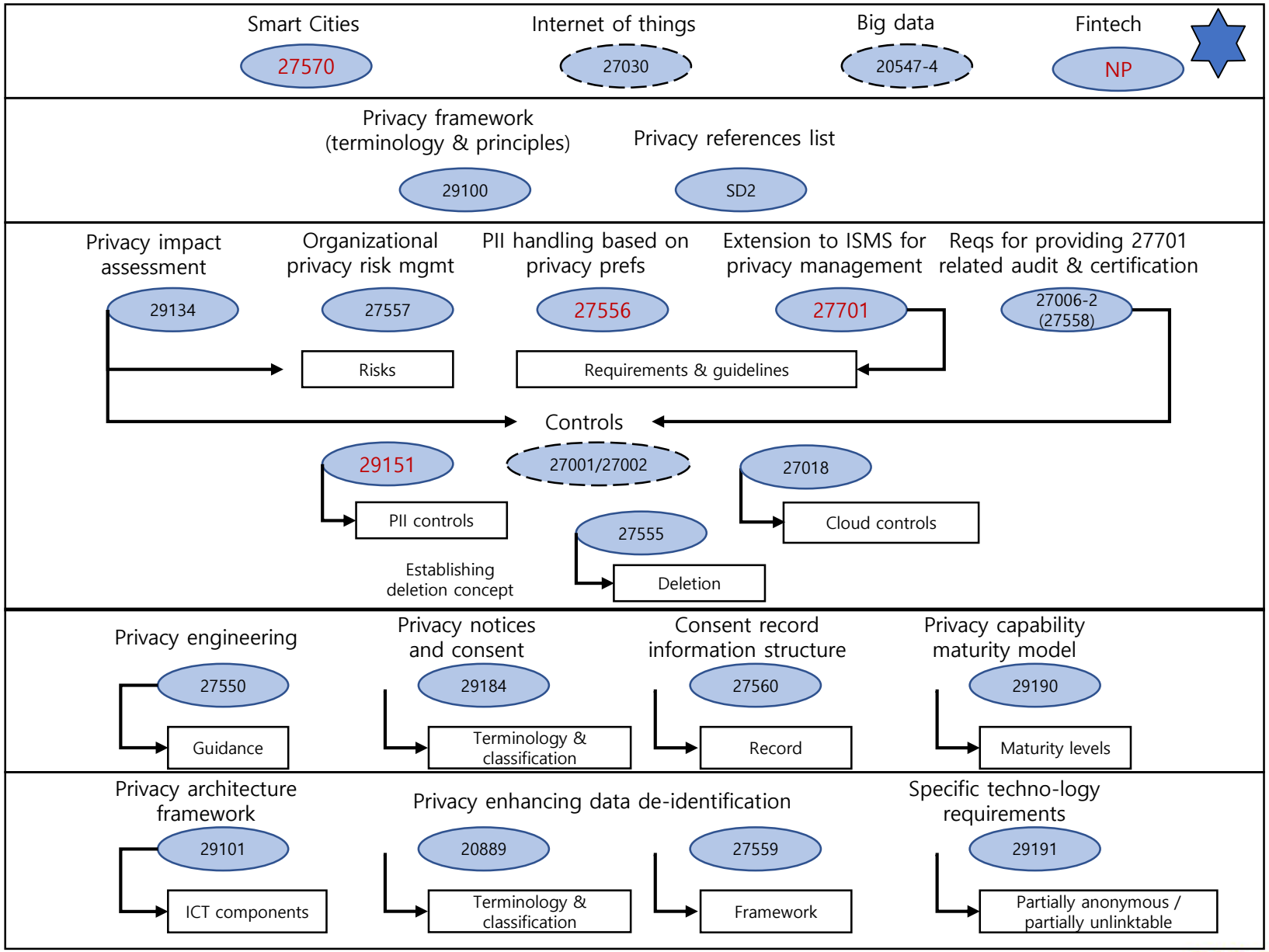
- 시작하면서
- 감염병 추적 관리 체계와 개인정보 보호
- 분산 신원확인과 온라인 인증
- 개인정보보호 국제표준화 기구 및 현황

뉴 노멀 시대
선도를 위한
ICT 표준의
역할

개인정보 보호 표준화 그룹 및 주요 표준



SC 27/WG 5 국제표준 현황



뉴 노멀 시대
선도를 위한
ICT 표준의
역할

개인정보보호 주요 이슈와 국제 표준

글로벌 개인정보보호 법제도

- 한국 개인정보보호법 개정(2020.02.04)
- EU GDPR 유럽의회 공표(2016.04), 시행(2018.05.25)
- 일본 개인정보보호법 개정 (2015.09)
- EU eIDAS (electronic identification and trusted service)

주요 이슈

프라이버시 체계 인증

- 한국 ISMS-P 인증 (개인정보보호법 32조2)
- EU GDPR 인증 메커니즘 (제43조)
- 클라우드 사업자 ISMS 인증

비식별 처리

- 한국 개인정보보호법 개정 – 가명처리 개념 도입 (2020.02.04)
- EU GDPR – 가명화 기법 (2016.04)
- 일본 개인정보보호법 – 가명익명정보 (2015.09)
- 미국 NIST - 비식별화

개인정보 영향평가

- 한국 개인정보 영향평가 – 제33조
- EU GDPR – 고 위험 개인정보처리자 의무화

온라인 본인 확인

- 한국 정보통신망법 / 전자서명법
- EU eIDAS – 유럽 인터넷 단일 시장을 위한 본인 식별 및 서명

개인정보 보호 지원하기 위한 국제 표준화

- ISO/IEC 27701
- ITU-T X.1058 | ISO/IEC 29151
- ISO/IEC 27018

- ISO/IEC 20889
- ITU-T X.1148
- ITU-T X.rdda
- ISO/IEC 2WD 27559

- ISO/IEC 29134

- ITU-T X.1254
- ISO/IEC 29115
- ITU-T X.509

감사합니다.