개인정보보호론

[11주차. 바이오인식정보]

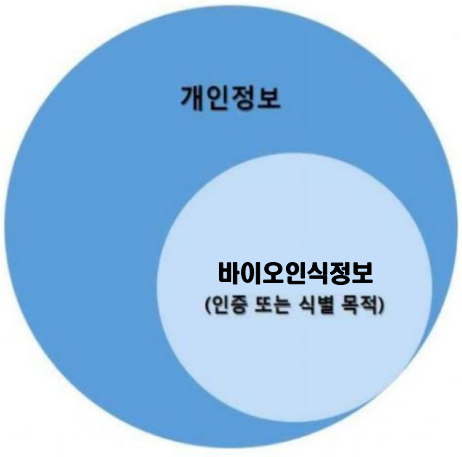
바이보정보

- 생체정보뿐만 아니라 유전정보, 건강 관련 정보를 포괄하는 개념

바이오인식정보 = 개인정보

- 지문, 홍채, 음성, 필적 등 개인의 신체적.행동적 특성에 관한 정보로서 개인을 인증 또는 식별하기 위하여 기술적으로 처리되는 개인 정보

신체적·행동적 특성에 관한 정보



구분	내용	적용 가능 범위
신체적 특징	개인이 유전적으로 타고나는 생리학적 정보	지문 인식, 홍채 인식, 손바닥정맥 인식, 손가락정맥 인식, 음성 인식, 안면 인식 등
행동적 특징	개인만의 독특한 행동습관에 기반한 패턴정보	키 스트로크 인식(타이핑 패턴), 서명 인식, 걸음걸이 인식 등

개인 인증 및 식별

- 인증(검증, verification, authentication) – 제시된 개인정보와 기존 정보, 둘 사이의 동일성의 비교를 통해 (같다/다르다)를 판단 ⇒ 정말 그 사람인가?

Verification(Authentication) 인증
- ID given => yes / no
- "Decision boundary" is the issue

- 식별(인식, recognition, identification) – 등록된 정보와 제시된 개인정보의 비교를 통해 등록된 정보가 있는지 확인 ⇒ 누구인가?

Recognition(Identification) 확인
- Who is the most likely in the DB?
- "Search" is the issue

- 인증은 기기에 입력된 바이오정보와 대조해 특정 개인을 확인하는 것
  - 지문·홍채·안면인식 등을 이용한 스마트폰 잠금 해제

- 식별은 데이터베이스에 저장된 다수 바이오정보와 대조해 여러 사람 중 특정인을 확인하는 것
  - 페이스북에 사진을 올리면, 안면인식을 통해 특정 개인을 태그 하는 서비스

인증(Authentication)

- 지식 기반 : 사용자가 알고 있는 것 (something you know)
  - Ex) PW, PIN
- 소유 기반 : 사용자가 소유하고 있는 것 (something you have)
  - Ex) 스마트카드, 토큰
- 존재 기반 : 사용자만의 고유한 특징 (something you are)
  - ex) 홍채, 지문

지식 기반 인증

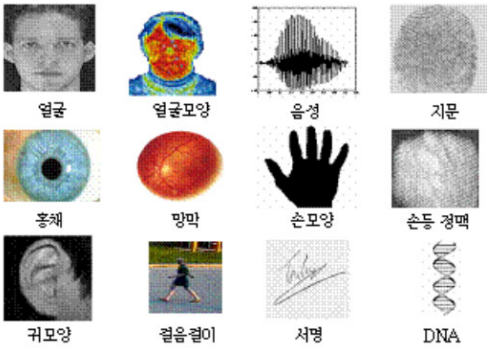
- 사용자가 알고 있는 것
  - 패스워드, 개인 식별 번호(PIN), 자물쇠 번호 등
- 단점
  - 사용자가 개인 정보를 잊어버리거나, 다른 사람이 인증에 사용 정보를 입수하여 시스템에 불법적으로 접근 가능
- 장점
  - 설치비용 적음

소유 기반 인증

- 사용자가 소유하고 있는 인증방법
  - 열쇠(카드 키), 티켓, 패스포트, 토큰, 스마트카드, 액세스 카드, 배지 등
- 사용자가 도구들을 잃어버려서 분실하거나 도난 될 경우 불법적인 시스템 접근에 악용될 수 있음

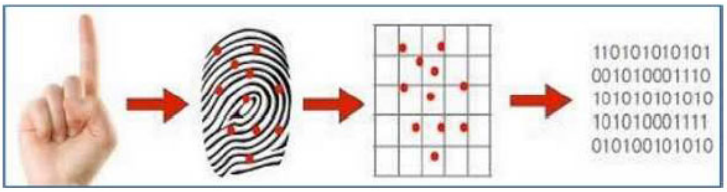
존재 기반 인증

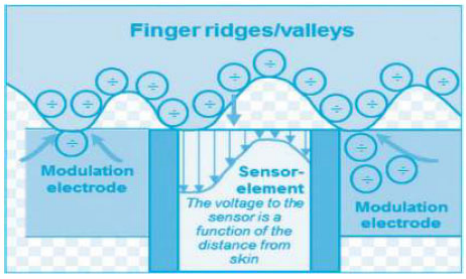
- 사용자만의 고유한 특징을 이용한 인증방법
  - 바이오인식 기술
- 유니크한 정보로 한번 노출되면 회복 불가



지문 인식(fingerprint recognition)

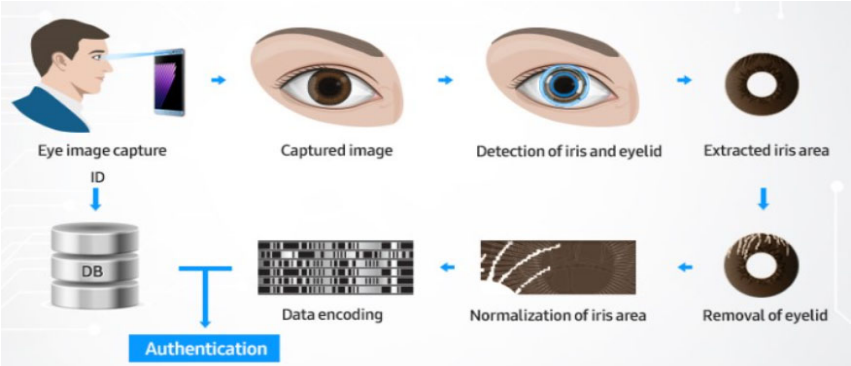
- 지문인식은 보통 지문 융기의 분기점, 끝점 등으로 구성되는 특징점의 위치와 속성을 추출, 저장, 비교하는 알고리즘을 채용
  - 지문인식은 인식방법에 따라 정전용량 방식, 광학 방식, 초음파 방식 등으로 구분





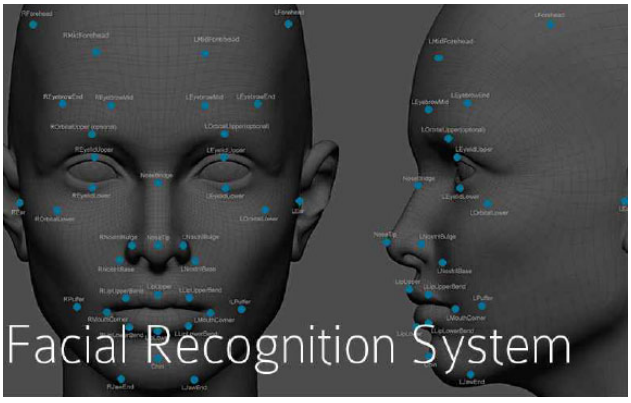
홍채 인식(Iris Recognition)

- 홍채인식은 안구 중앙의 검은 동공과 흰자위 사이에 있는 도넛 모양의 홍채를 이용한 인증 기술
  - 홍채인식 장치의 적외선 카메라가 홍채를 이미지화한 후, 홍채인식 알고리즘으로 사용자 고유의 홍채 코드를 생성, 등록 후 비교하는 방식



얼굴 인식

- 얼굴 인식은 각 개인 얼굴의 특징을 이용
  - 카메라를 통해 입력된 화상으로부터 각 개인마다 독특한 부위를 측정 단위로 추출하는 것으로, 독특한 부위가 어떠한 곳인지 결정하는데 이 기술의 정확도가 달려있음

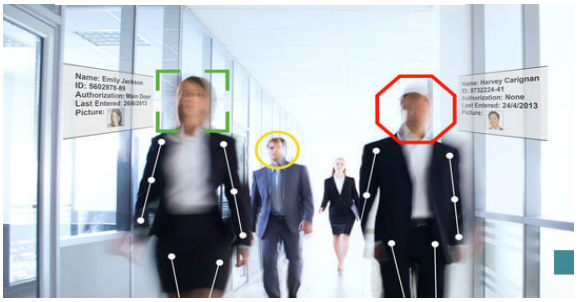


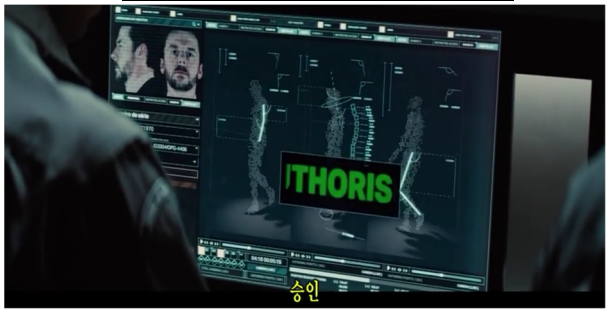
필체인식 (Signature)

- 필체인식 혹은 서명인식은 개인서명의 고유한 특징을 이용하여 인증하는 기술
  - 이미 작성된 서명을 인식하는 정적인 방법과 서명하는 과정을 동적으로 파악하는 방법으로 구분
    - ✓ 동적서명 인식은 새로운 서명 샘플과 원본 데이터 서명의 모양을 단순히 비교하는 방법이 아니라 원본 데이터와 샘플링된 데이터가 쓰여지는 방법을 비교하는 것으로 서명시간, 속도, 압력, 종이로부터 펜이 떨어진 횟수 등을 이용

Dynamic Biometrics

- 엄격한 인증(strong authentication) : 두가지 이상 병행





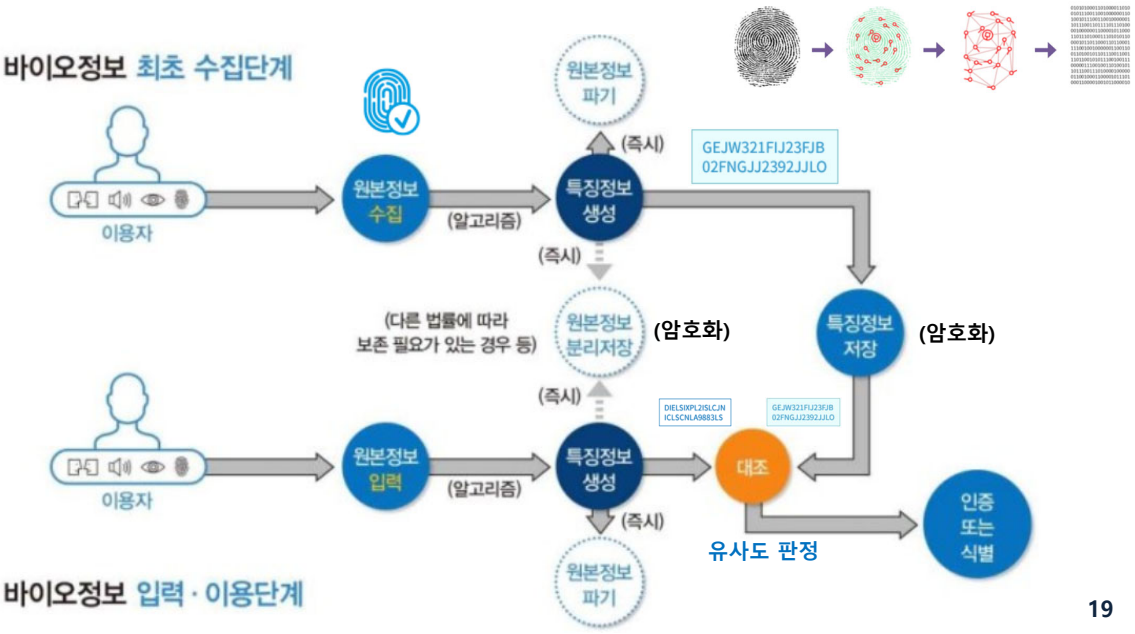
바이오인식정보 특성

- 보편성(Universaility) : 모든 사람에게 있는 특징이어야 한다
  - 그렇지 않다면 바이오인식을 처리하지 못하고 오류가 발생할 것이다.
- 고유성 (Uniqueness) : 서로 다른 개인을 식별할 수 있기 위해서는 사람마다 가지고 있는 정보가 달라야 한다
  - 즉, 그 개인에게 고유한 정보여야 한다
- 영구성(permanency) : 평생 변하지 않는 특성을 가지고 있어야 한다
  - 그렇지 않고 시간이 지나면서 혹은 어떤 영향으로 변화한다면 해당 개인을 더 이상 식별하거나 인증할 수 없게 될 것이다

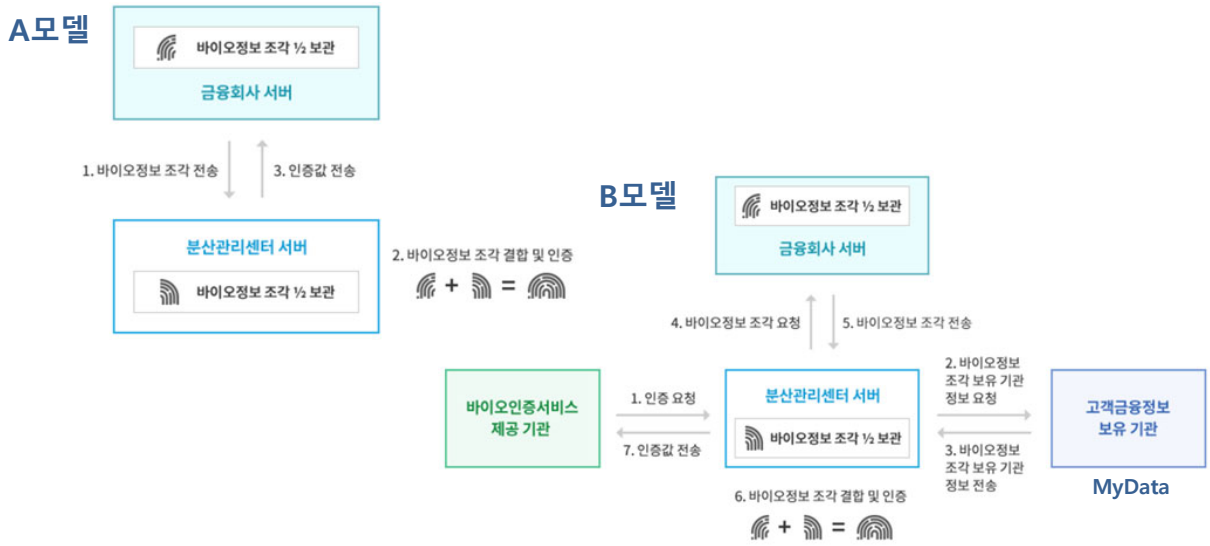
바이오인식정보 시스템 4단계

- 1. 획득 : 바이보 특성을 디지털 형태로 변환
- 2. 특징추출 : 사람마다 고유하면서 변별력이 높은 특징점 추출
- 3. 비교 : 등록된 특징과 입력된 특징을 신속 정확하게 비교
- 4. 유사도 판정 : 비교된 두 특징들이 동일인의 특성인가를 판단

바이오인식정보 시스템



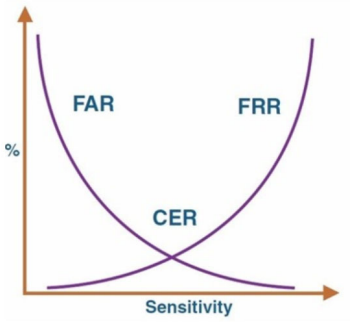
원본정보 분리 저장



유사도 판정 : 바이오인식정보 정확성 평가 지표

- **FRR(False Rejection Rate) 오거부율**
  - 오거부율은 바이오인식 시스템의 에러로 개인을 식별하지 못하는 등 인식을 거부할 확률
- **FAR(False Acceptance Rate) 오인식률**
  - 오 인식률은 타인의 바이오인식 정보를 특정인의 것으로 잘못 인식할 수 있는 확률

➢ **CER(Crossover Error Rate) / EER(Equal Error Rate)**
  - ➢ FRR과 FAR이 일치하는 지점으로 수치가 낮을수록 정확
  - ✓ 사용자 편의성이 높아지는 경우 FRR은 낮아지고 FAR이 높아진다
  - ✓ 보안성을 강화할 경우에는 FAR은 낮아지고 FRR이 높아진다



FIDO (Fast IDentity Online)

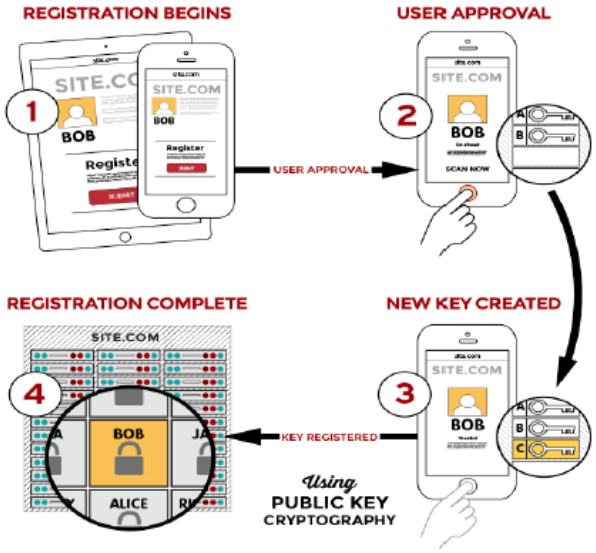
- **FIDO 인증 : 온라인 환경에서 사용자의 신원을 편리하고 안전하게 인증하기 위한 기술 표준으로, 주로 사용자 개인의 고유한 바이오정보를 이용하는 인증 기술**
  - 아이디와 비밀번호 조합 대신 지문, 홍채, 얼굴 인식, 목소리, 정맥 등을 활용한 새로운 인증 시스템을 의미

구분	서버저장 방식	FIDO 방식
방식	• 개인 생체정보를 **서버에 저장** • 바이오 인식 단말에서 추출한 정보와 비교	• 개인 생체정보를 **단말기에 저장** • 전자서명 방식으로 단말기에서 인증 과정 진행
사례	• 신한은행 디지털 키오스크 • 기업은행 홍채인증 ATM	• 우리은행, 신한은행, KEB하나은행 등 주요 은행 모바일뱅킹

1. 사용자가 서버에 로그인 요청시 서버는 사용자에게 챌린지 값과 인증 토큰을 전송하여 인증 요청합니다.

2. 사용자는 등록된 지문으로 개인키가 저장된 단말 내 보안 영역을 열고, 개인키를 꺼내어 챌린지값에 전자서명 후 그 결과값을 서버에 전달합니다.

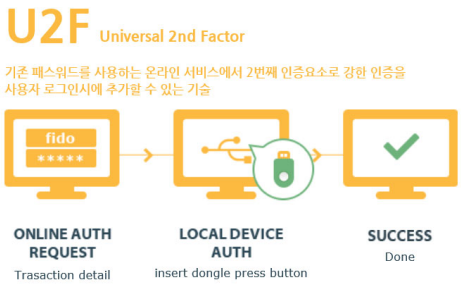
3. 서버는 사용자가 보낸 결과값을 공개키로 검증하여 인증 승인합니다.



FIDO 방식 : UAF & U2F

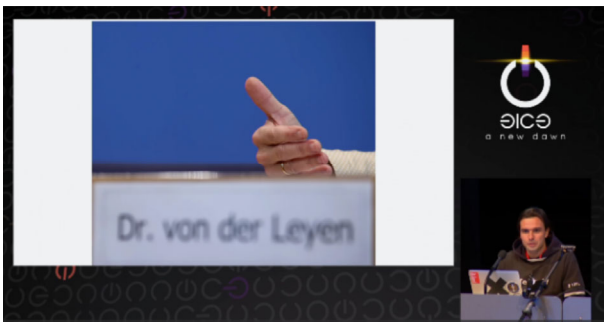
- **UAF(Universal Authentication Framework)**
  - 사용자의 단말기에서 제공하는 인증방법을 온라인 서비스와 연동하여 인증하는 기술로 패스워드 없이(passwordless) 바이오정보만으로 인증을 완료하는 것
- **UAF 방식은 스마트폰과 같은 모바일 환경에 적합**
  - 모바일 기기에는 지문 인식 모듈, 홍채 인식 카메라, 마이크 등이 탑재돼 바이오 정보를 인식하기 위한 기반이 마련되어 있기 때문

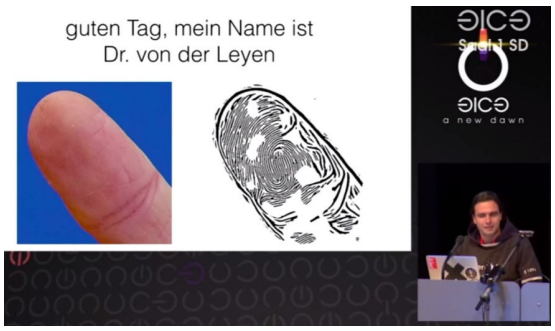
- **U2F(Universal 2nd Factor)**
  - 기존 패스워드를 사용하는 지식기반 인증에서 USB, NFC 보안키, 바이오인증 등의 두 번째 인증요소를 추가 하는 것
- **기존 PC 기반 온라인 서비스에 적합**
  - PC 기반 온라인의 경우 ID/패스워드 기반의 개인 인증 시스템이 주로 사용되어 바이오인증 방식으로의 갑작스런 전환은 사용자의 편의성을 저해할 우려가 있으며, 바이오인증 시스템 구축을 위한 전환비용 등의 문제 역시 존재



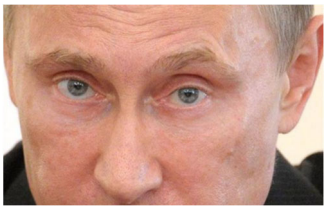
바이오인식정보 해킹

- **Chaos Computer Club(CCC) hacker**

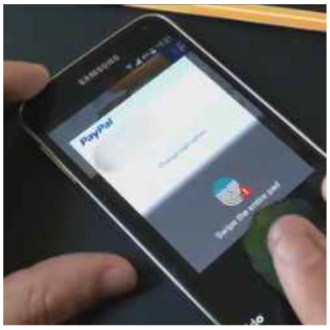




- 독일의 해커단체 CCC는 구글검색을 통해 러시아 대통령 푸틴의 고해상도 사진을 출력하여 홍채 복제(Print attack)*
  - 위조지문은 별도 제작이 필요하나, 홍채는 사진 출력만으로 복제 가능

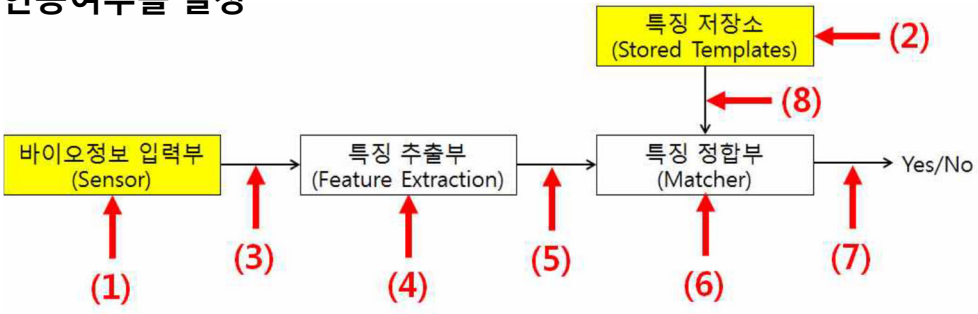


- 독일의 시큐리티리서치랩스는 목재용 접착제에 사용자 지문을 복제하여 지문인식 잠금장치 해제
  - 위조지문을 이용해 갤럭시와 연동된 페이팔(PayPal) 결제도 가능



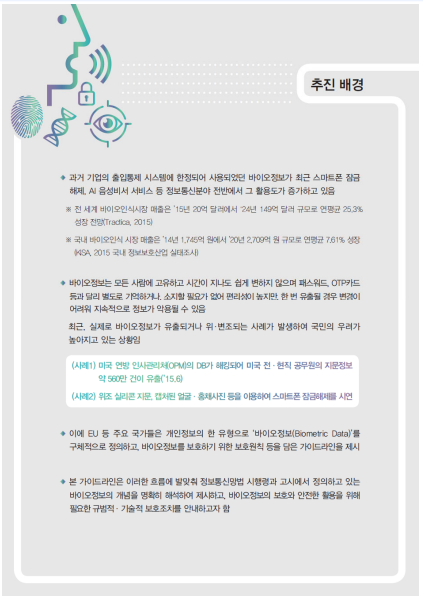
바이오인식정보 인증시스템의 보안상 취약점

- 바이오인식정보 인증시스템은 크게 4개의 모듈로 구분됨
  - 바이오정보 입력부 : 센서를 통해 바이오정보를 취득
  - 특징 추출부 : 취득된 바이오정보로 부터 특징정보를 추출
  - 특징 저장소 : 특징정보 및 개인정보 등을 저장하는 저장소
  - 특징 정합부 : 저장된 특징정보와 새로 입력된 특징정보를 비교하여 인증여부를 결정



(1) 위조지문, 고해상도 사진 등 위조된 바이오 정보를 센서에 입력하여 인증을 우회
(2) 저장소에 침투하여 기 저장된 특징정보를 조작, 삭제, 유출
(3) 불법 취득한 바이오 정보를 재생(replay)하여 인증
(4) 위조된 특징정보를 임의로 생성
(5) 정상적인 특징정보를 임의의 위조된 특징정보로 대체
(6) 특징 정합부에서 인증 결과값을 임의로 변경
(7) 최종 인증결과를 조작
(8) 저장소에서 정합부로 전송되는 특징정보를 절취 또는 타인의 정보로 대체

바이오정보 보호 가이드라인



적용범위

바이오정보는 지문, 홍채, 음성, 필적 등 개인의 신체적 행동적 특성에 관한 정보로서 개인을 인증 또는 식별하기 위하여 기술적으로 처리되는 개인정보를 말한다.

-지문

-홍채

-음성

-필적

대상 사업자

이용자의 바이오정보를 직접 처리하는 정보통신서비스 제공자를 포함하여 바이오정보의 안전한 이용환경 조성에 관여하고 있는 제조사 등*(이하 '사업자')을 포함

-바이오정보를 전송받는 사업자

-스마트폰 등 기기 제조사

-바이오정보 접근관리 OS 사업자

-바이오정보가 활용되는 앱 개발자

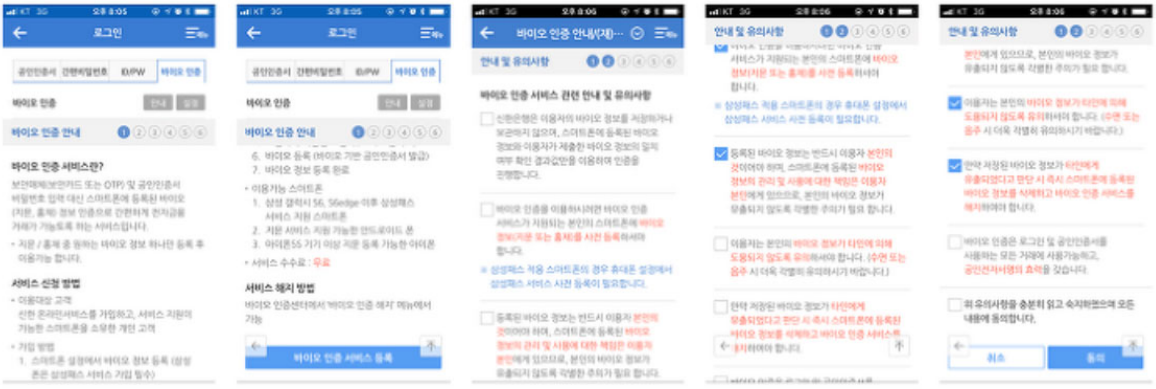
바이오정보 보호 6원칙

- **비례성 원칙**
  - 바이오정보를 활용함에 따라 수반되는 위험이 사업 상 바이오정보의 필요성 및 예상되는 편익에 비해 과도하지 않은지 등을 검토 후, 수집·이용 여부를 판단하여야 한다

원칙	세부 원칙	원칙 설명
① 비례성 원칙	- 위험성 검토	- 바이오 정보 사용 시 위험과 편익 검토
	- 위험성 최소화	- 위험 최소화 바이오 정보 사용

- **수집.이용 제한의 원칙**
  - 바이오정보의 수집·이용 목적, 항목, 보유기간을 이용자에게 명확히 알리고 동의 받아야 한다.
  - 인증·식별 목적에 필요한 최소한의 바이오정보를 수집·이용해야 한다.

원칙	세부 원칙	원칙 설명
② 수집/이용 제한 원칙	- 수집/이용 정보 명시 및 동의	- 바이오정보 동의필요 - 목적, 항목, 보유기간
	- 특징 생성 후 파기 원칙	- 원본정보 즉시 파기 - 민감정보 추출방지



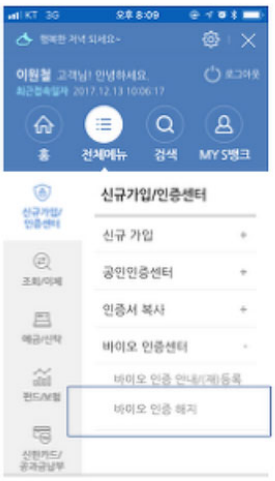
신한은행: 신한S뱅크

- **목적 제한의 원칙**
  - **바이오정보는 이용자에게 동의 받은 인증 또는 식별 이외의 목적으로 무단으로 활용되어서는 아니 된다.**

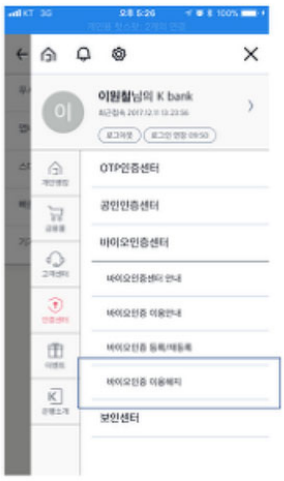
원칙	세부 원칙	원칙 설명
③ 목적 제한 원칙	- 동의받은 내용 외 활용금지	- 이용자의 동의 외 무단 활용 금지

- **통제권 보장의 원칙**
  - 이용자가 바이오정보를 수정하거나 삭제할 수 있도록 다양한 통제 수단을 제공해야 한다.
  - 이용자가 바이오정보의 제공을 원하지 않거나 신체적 장애 등으로 제공할 수 없는 경우를 대비하여 가능한 대안을 마련하는 것이 바람직하다.

원칙	세부 원칙	원칙 설명
④ 통제권 보장 원칙	- 통제수단 제공	- 수정/삭제 가능수단 - 기기 통제권 행사
	- 대안 마련	- 미동의, 제공불가 시 다른 정보 활용



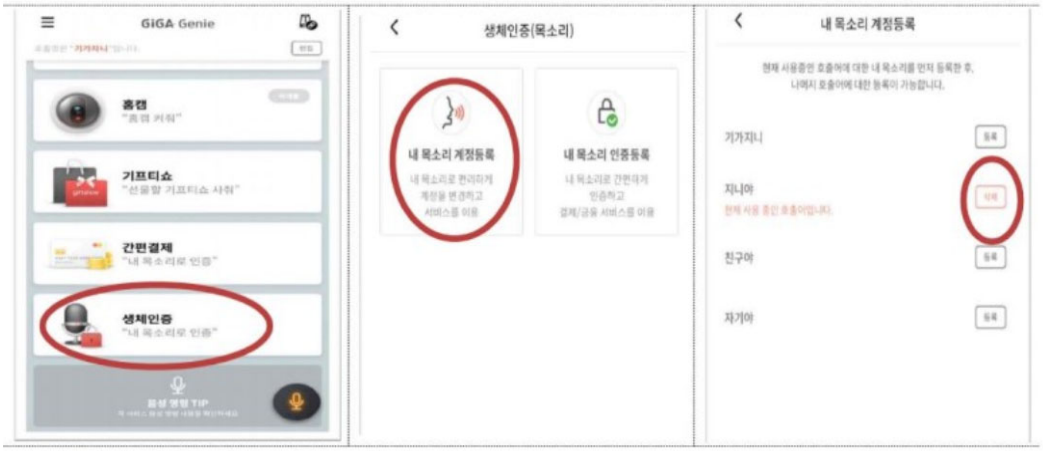
신한은행: 신한S뱅크



K뱅크: K뱅크

- **투명성 원칙**
  - **바이오정보 보호에 관한 사항을 이용자에게 적극적으로 안내해야 한다.**
  - **바이오정보 서비스와 관련된 이용자의 문의 및 침해 민원 등을 처리하기 위한 피해구제 기능을 마련·운영해야 한다.**

원칙	세부 원칙	원칙 설명
⑤ 투명성 원칙	- 관련내용 적극 안내	- 바이오정보 종류 - 보호조치, 행사방법
	- 이용자 문의 민원 기능	- 통제권행사 피해신고 - 처리부서, 연락처



▲ 아이폰 바이오정보 관리 방법

▲ AI 스피커 바이오정보 관리 방법

- **바이오정보 보호 중심설계 및 운영 원칙**
  - **바이오정보를 활용한 서비스의 개발·설계 단계부터 이용자의 바이오정보 보호를 고려하도록 권고한다.**
  - **대량의 바이오정보를 서버로 전송하여 처리하는 경우, 사전에 이용자의 프라이버시에 미칠 영향 및 개인정보 위험 요인 등을 조사·분석·평가하는 절차를 마련하는 것이 바람직하다.**

원칙	세부 원칙	원칙 설명
⑥ 바이오정보 보호중심 설계 및 운영원칙	- 설계단계부터 정보보호 고려	- default값 보호 설정 - 특징정보 암호화
	- 프라이버시고려 - 위험요인 조사	- PIA 개인정보영향평가 - 위험분석, 개선도출