바이오인증 발전과 정보보호 전략

금융결제원 차세대인증업무팀장 박정현

목차

1 인증의 개념과 바이오인증

인증의 개념과 인증방식

- **인증의 개념**
  - 실체의 신원이나 메시지 근원의 확인 (한국정보통신기술협회 정보통신용어사전)
  - **정보 혹은 사람 조직 디바이스 등의 속성이 올바른지의 확정 (위키피디아)**
  - 문서나 행위가 정당한 절차로 이루어졌다는 것의 증명 (국립국어원 표준국어대사전)

- **인증방식**
  - **인증서 방식**
  - **TA방식**
  - **공동이력인증 방식 : 블록체인**

※ 발표자 개인 의견

인증 서비스 분류 및 국제권고 기준

- **인증 서비스 분류**
  - 인증요소 기준 : 싱글팩터 / 멀티팩터
  - 인증대상 기준 : 객체인증 / 거래인증
  - 인증주체 기준 : 고객인증 / 서버인증
  - 인증채널 기준 : 싱글채널 / 멀티채널(멀티모달)

- **인증 국제권고 기준**
  - 바젤위원회 전자금융 위험관리 준칙 : **바이오인증** / PIN / 패스워드 / 스마트카드 / 인증서 등 제시

인증요소 기준 분류

구분	개념	종류
팩터1 (지식 기반)	고객만이 아는 정보	ID 및 PW / 사전등록 질의응답 / 신용카드·계좌 비번 또는 설정 이미지
팩터2 (소지 기반)	고객만이 가진 정보	인증서 / OTP / 디저털OTP / 폰 디바이스 ID 스마트카드 인증 ID
팩터3 (바이오정보 기반)	**고객만의 특징 정보**	**지문 / 홍채 / 손바닥정맥 / 손가락정맥 / 얼굴 / 음성 손바닥(융선)**

인증의 변화 동인

- 편의성(간편성)과 보안성(정확성 및 안전성) 딜레마
- **인증거래 성격 별 조화 지향 : 바이오인증**

인증 변화 동인의 핵심기술 : 바이오인증

- 2016년 초 바이오인증 본격화
- **FIDO(개인매체방식) 및 분산관리인증(금융서버방식) 보급**
- 금융결제원 바이오정보 분산관리센터 구축(2016.11월)

2 바이오인증서비스 소개

바이오인증서비스 소개

- **개인매체방식(스마트폰 중심)**
  - FIDO기술(국제규격) 중심 (기타 인증서 및 블록체인기반)
  - **국내 대다수 금융회사 제공(뱅킹, 주식거래, 보험계약, 지급결제)**
  - 금융결제원 바이오정보 분산관리센터 공동FIDO : 73개 금융회사 참가 (매년 거래량 7배 증가)
  - 지문, 손바닥(융선), 홍채, 얼굴, 음성 등 이용

- **금융서버방식(영업점, 대여금고, ATM, 디지털키오스크, 카드가맹점, 영업용테블릿 중심)**
  - **바이오정보 분산관리기술(금융표준) 중심**
  - 은행권 중심(증권사 및 카드사 도입 시작)
  - **보험권 계피상이(계약자와 피보험자가 다른) 전자계약 도입 예정(상법 개정)**
  - 금융결제원 바이오정보 분산관리센터 분산관리 : 40개 금융회사 참가 (매년 거래량 4배 증가)
  - 손바닥정맥, 지문, 홍채, 손가락정맥 등 이용

금융서버방식 바이오인증서비스 주요 사례



- **KB국민은행 : 키오스크·ATM·STM·영업점 적용 (국내 최초 인감·도장·통장이 필요 없는 바이오 예금출금 실시)**
- **신한은행 : 키오스크·ATM·스마트브랜치 적용 (국내 최초 바이오인증 실시)**
- 우리은행 : 키오스크 적용 (국내 최초 지문·홍채·손바닥정맥 3가지 인증기술 이용)
- 하나은행 : 현재 개발 진행 중
- 농협은행 : 금년 실시 추진 중
- 수협은행 : ATM·영업점 적용 (국내 최초 은행 모든 영업채널 적용 중)
- 대구은행 : 키오스크·ATM 적용 (국내 최초 CD공동망 연계)
- K뱅크 : ATM 적용 (국내 최초 GS편의점 연계)
- **롯데카드 : 신용카드 가맹점 적용 (국내 최초 바이오인증 신용카드 결제)**
- NH투자증권 : 영업점 적용 (국내 최초 증권사 바이오인증 실시)

3 바이오인증서비스 정보보호기술

바이오인증서비스 정보보호 구간

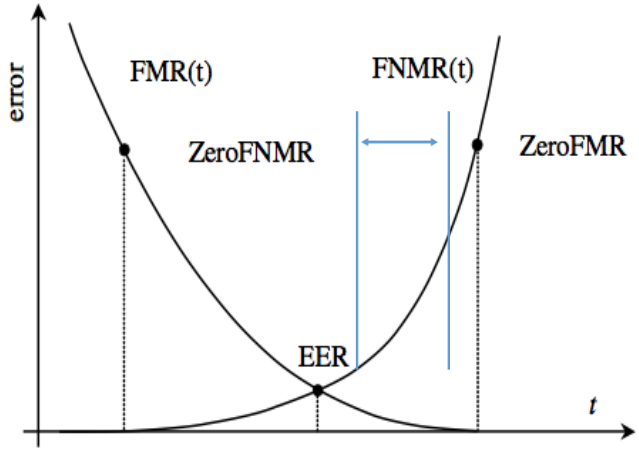
- 바이오정보 입력부 : 채널에서 바이오정보 취득 구간
- 바이오정보 추출부 : 바이오정보에서 특징정보 추출 (등록템플릿 변환부) 구간
- 바이오정보 전송부 : 채널에서 서버까지 특징정보(등록템플릿) 전송 구간
- **바이오정보 저장부 : 특징정보(등록템플릿) 및 개인정보 저장 구간**
- 바이오정보 인증부 : 저장부의 특징정보(등록템플릿)와 입력된 특징정보(인식템플릿) 간 매칭 및 인증 구간

위조 및 변조(재사용) 방지 기술

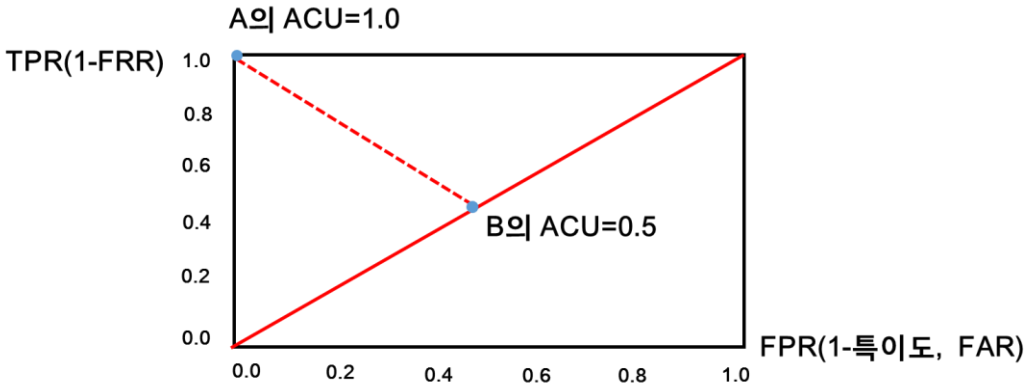
- Live Detection
- Water Mark
- Time Stamp
- Hashing
- Cyclic redundancy check code
- Template Log Management
- Security Attacker List Management
- Multi Modal
- Attempt Management(ISO 19092 : Max 3)
- Threshold Management
- EER·AUC Management

바이오인증 인증정확도 관리

· **EER은 금융회사의 경우 EER 우측에 Threshold 위치**
· FMR/FNMR(알고리즘), FAR/FRR(센서), PFAR/PFRR(시스템), GFAR/GFRR(등록실패율 반영) 이용
· KISA 기준 : EER(0.01)
· 금융결제원 기준(ISO/IEC 19795 기준 보정) : GFAR(0.01/0.003/0.001), GFRR(0.02/0.15/0.01)



· **AUC는 민감도 및 특이도 이용**
· AUC값이 1에 가까울수록 성능 우수
· 금융결제원 기준 : AUC값 0.95 이상



해킹(유출방지) 및 오남용 방지 기술

- Encryption
- HSM
- Non-Identification
- Cancelable Biometrics
  - Noninvertible Geometric Transforms
  - Random Projections
  - Random Convolution Filter
  - BioConvolving
  - Bloom Filters
  - BioHashing
  - Random Permutations
  - Salting Methods
- Management of segregated biometric information **(분산관리 : 오남용 방지 가능)**

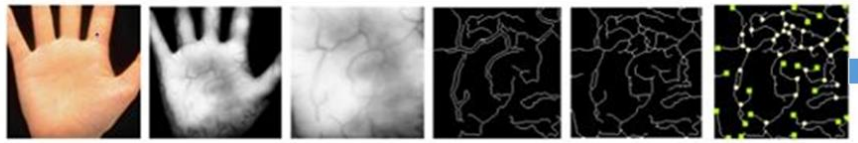
바이오정보 분산관리 정보보호 체계

- 실명(비대면) 확인
- Multi Modal
- Live Detection
- Security Attacker List Management
- Attempt Management
- Threshold Management
- EER·AUC Management (성능평가시스템 운영)

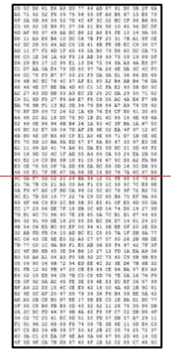
- Encryption : Triple
- HSM
- Non-Identification : Double
- 재사용 방지
- 위변조 방지
- 힐클라이밍 대응
- 분산관리

1. 바이오영상 추출

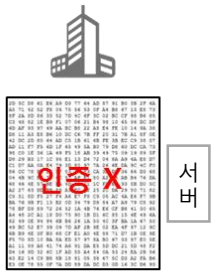
2. 특징정보 추출



3. 템플릿 변환

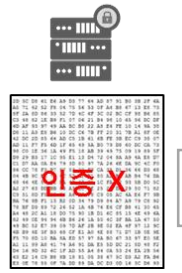


4. 템플릿 분할



5. 분산 저장

KFTC



- 분산적합성 시험
- 바이오인증 성능시험

유로 바이오정보 보호의견서 주요 내용

- 원본정보가 아닌 특징정보(템플릿)의 사용
- 중앙집중형보다 분산관리형 권장
- 갱신과 파기 보장
- 암호화 저장
- 속임수 보장
- 목적달성 후 자동 삭제
- 식별정보 분리

4 바이오인증 발전과 정보보호 전략

바이오인증 발전전략

- **금융회사 간 바이오인증 연계 및 호환 강화**
  - 금융회사 간 호환인증(2016. 12.) : 바이오정보 분산관리센터 제공
  - CD공동망 연계(2017.11.) : 계좌조회 및 타행 출금 실시 (계좌이체 추가 예정)
  - 나이스 점외CD망 연계(2017.11.)
  - 금융회사 및 기타 공공기관 연계 확대 중

- O2O(Online to Offline) 바이오인증서비스 제공
  - 한번 등록된 바이오정보를 온·오프라인 이용

- **바이오인증 서명기능 추가**
  - 개인매체방식 : 기존 제공 (FIDO PKI방식)
  - 금융서버방식 : 신규 제공 (금년 보험사 전자청약 적용 예정 : 바이오정보를 서명키로 HMAC방식)

- 바이오정보 등록 편의성 강화

- 바이오인증기술 다변화

- 바이오인증 이용범위 다각화 (금융 외 분야)

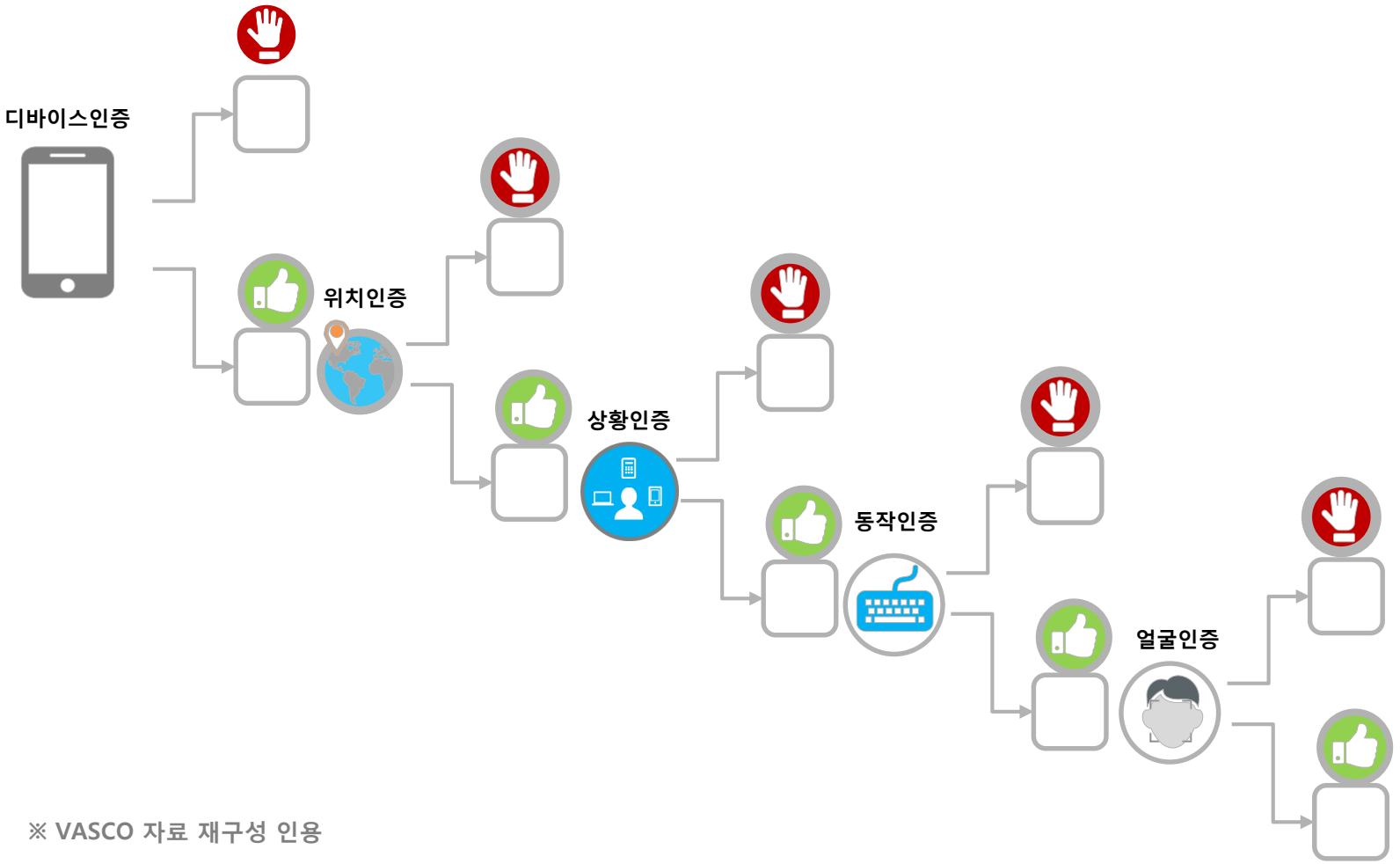
- **인공지능기술과 결합한 무자각인증 제공**

바이오인증 중심 무자각인증 체계

· 공급자가 소비자를 알아서 인증하는 공급자 능동적 인증인 무자각인증 공급

· 인증요소 : 인증기간/인증시간/인증시도횟수/인증실패횟수/인증매체 종류/인증위치/인증방법 ··· 인증성향

(예시) 디바이스 → 인증위치 → 인증상황 → 인증동작 → 바이오인증



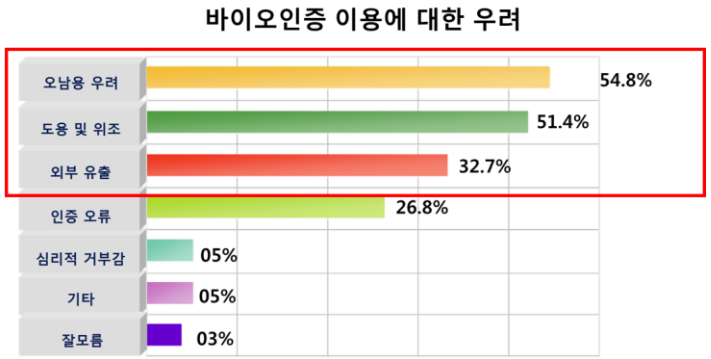
※ VASCO 자료 재구성 인용

바이오인증 정보보호 전략

- 바이오인증 Live Detection 기능 강화 및 모니터링 실시

- 금융회사 바이오인증시스템 운영평가체계 가동
  - 성능평가 체계 : 알고리즘평가 / 시나리오평가 / 운영평가
  - GFAR/GFRR 평가 필요
  - 금융결제원 운영평가체계(평가DB 기준, 테스트 요소, 평가방법 및 평가기준) 기 수립(시범실시 방침)

- 바이오정보 분산관리체계 보급 확대
  - 등록 바이오정보 오남용 방지를 위한 기관 간 분산 필요



(자료출처) : 바이오정보 수집 이용 실태조사(국가인권위, 2016.11.)

- **바이오인증의 고객 자기주권화 방안 마련**
  - 금융회사 내 등록 바이오정보의 일괄 조회 및 삭제
  - 금융회사 등록 바이오정보의 이용 내역 관리

감사합니다.