생체인증 솔루션 Nexsign 기능과 모바일 연계

SAMSUNG SAMSUNG SDS

Contents

왜 사용자 인증이 필요한가?

Who is he/she ?

- 불특정 다수
- 비 대면

왜 사용자 인증이 필요한가?

Offline

Online

사용자 인증 방법

1. What you knows
   지식
2. What you have
   소유
3. Something you are
   특성
4. Something you do
   행동

두 개 이상 방법 사용된 경우 보안성 보다 강화 됨 → 편이성은 감소
Multi-factor Authentication

인증 방법 - ① What you know

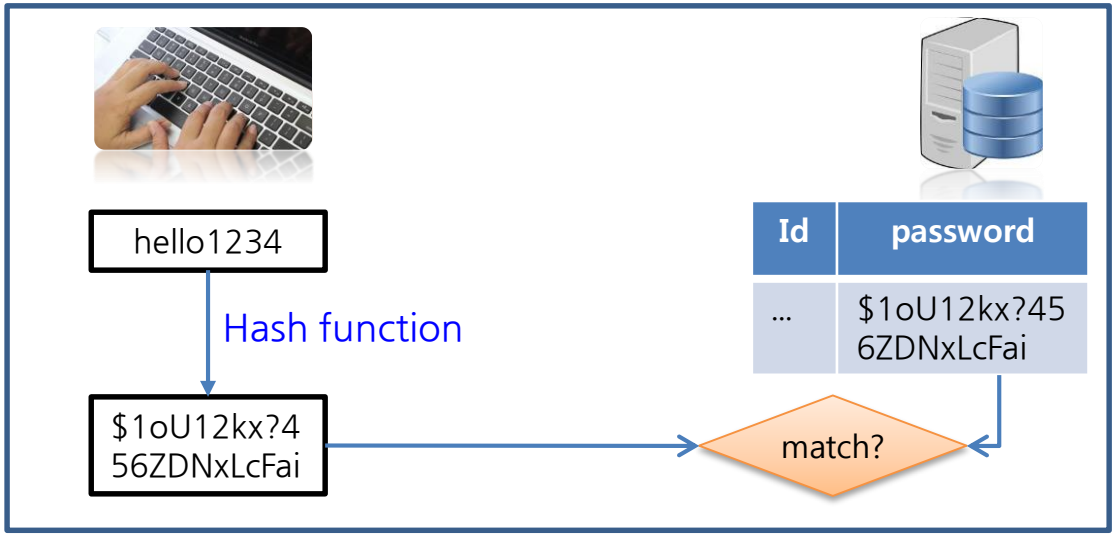
Password

PIN

(Personal Identification Number)

인증 방법 - ① What you know

- Password, PIN



Weakness

- ✓ easy to forget
- ✓ same password used
- ✓ need two hands
- ✓ brute-force attack

인증 방법 - ② What you have

교통카드

- 대칭키 기반

신용카드

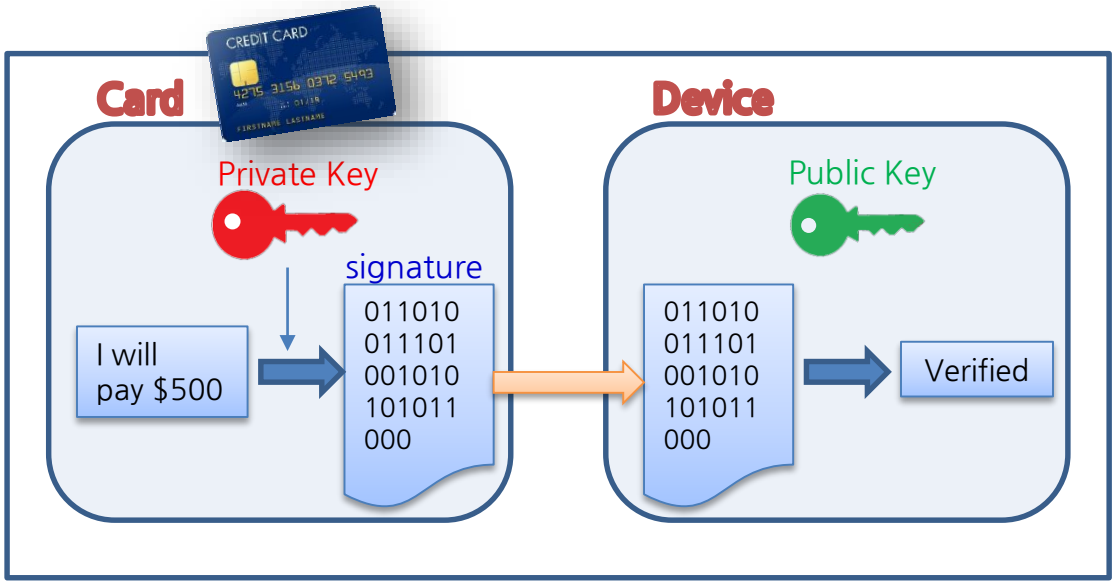
- 공개키 기반 : 비접촉식의 경우
  (PKI: Public Key Infracture)

contains **cryptographic keys** in the secure storage

인증 방법 - ② What you have

- **신용카드:** Secure Transaction using PKI

Public Key Infrastructure



Weakness

- ✓ 분실에 의한 오용
- ✓ 복제 가능성

인증 방법 - ③ Something you are / ④ do

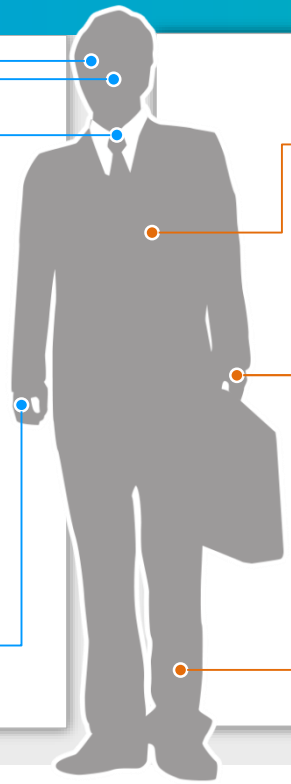
are (Physical Biometrics)

홍채
iris

얼굴
face

목소리
voice

지문
fingerprint



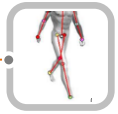
do (Behavioral Biometrics)

동작
gesture

서명
signature

키보딩 습관
typing pattern

걸음걸이
walking
pattern



사용자 인증 기술은, 최근 생체인증을 넘어 개인의 행동패턴을 추가로 검증하는 기술로 발전

물이 차오르는 집을 나오실 때,
지갑은 잘 챙기셨습니까?

➔ 생체인증 ATM 유용
Automated Teller Machine

구분	인식 수단
지식기반 (Wat you Know)	ID+PW, PIN
소유기반 (What you Have)	교통카드, 신용카드
특성기반 (Something you Are)	생체인증 (지문, 홍재, 망막, 손금, 얼굴,정맥, 목소리, 심장박동 등)
행동기반 (Something you Do)	말투, 걸음걸이, 서명, Key 스트로크, 마우스 움직임 등

Contents

생체인증 기술 개요

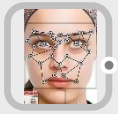
Nexsign을 이용한 바이오 인증 (2:25)

생체인증 기술 개요

생체인식(Biometrics)기반인증이란?

홍채 iris 

동작 gesture 

얼굴 face 

서명 signature 

목소리 voice 

키보딩 습관 typing pattern 

지문 fingerprint 

걸음걸이 walking pattern 

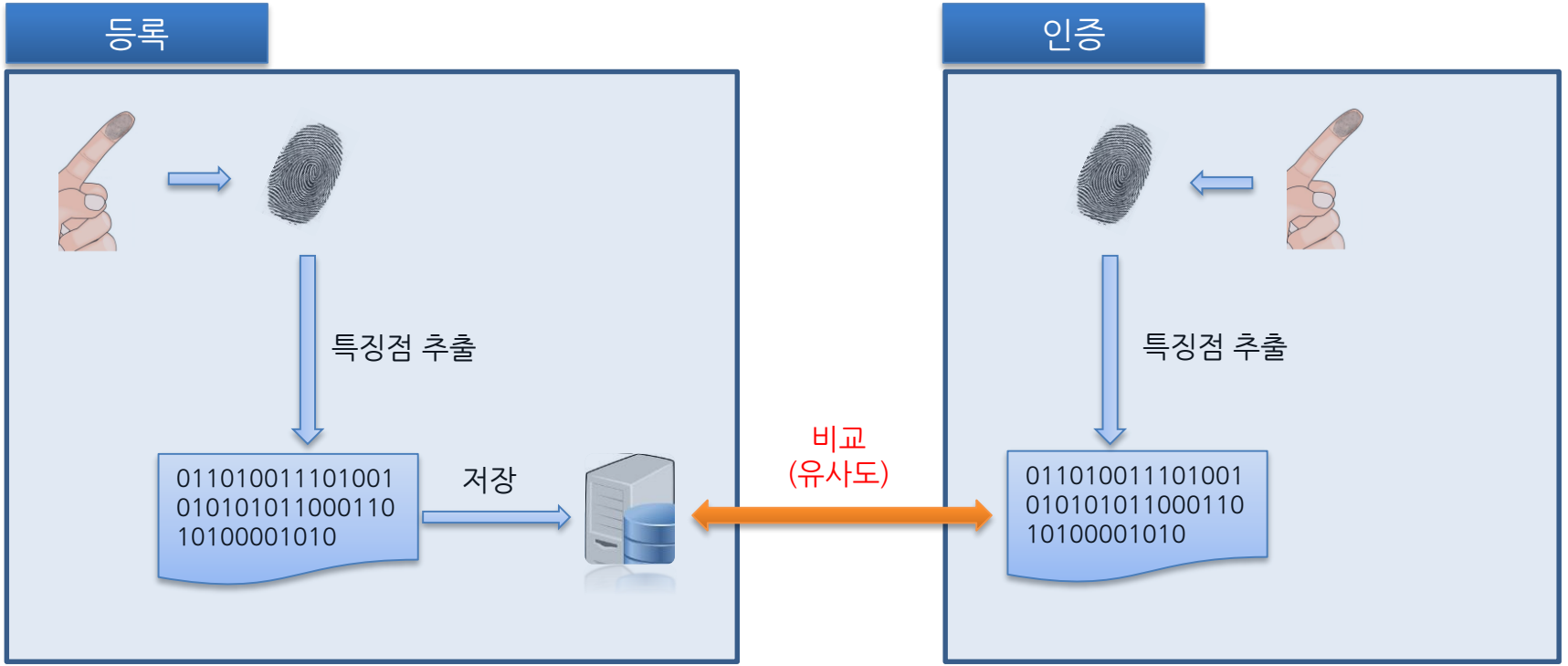
사용자가 가지고 있는
고유한 형태의 신체구조 또는
신체를 이용한 행동결과를 기반으로 인증

뛰어난 사용편의성

강력한 보안성

보편성 | 유일성 | 지속성

생체인증 이용 절차



생체인증 성능 지표

생체인증은 확률적 비교 사용

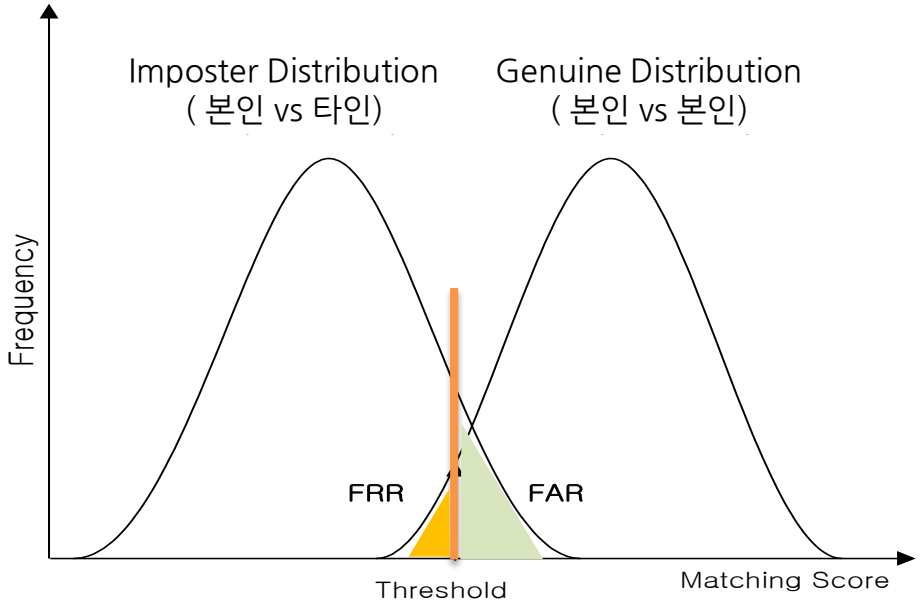
생체인증 방법별 FAR, FRR

타인 수락율 FAR : False Acceptance Rate

타인을 자신으로 인식하는 에러율

본인 거부율 FRR : False Rejection Rate

자기 자신이 거부되는 에러율

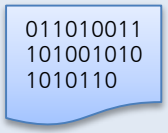


생체인증 구분 서버 매칭 vs. 단말 매칭

서버 매칭

서버에 보관된 생체정보와 비교

1)지문 취득



2)정보전송

3)인증수행

- 서버에 보관된 생체정보와 비교
- 개인정보보호 이슈

단말 매칭

단말에 보관되어 있는 생체정보와 비교

1)지문 취득
2)인증 수행

3)결과 전송

- 단말內 생체정보 보관 문제
- 인증결과 위/변조 위험

Contents

FIDO 개요

"새로운 인증 표준 탄생"

Fast IDentity Online(FIDO)은,

'14년 12월 v1.0이 릴리즈된 국제 표준으로
UAF와 U2F 방식으로 나뉘어 집니다.

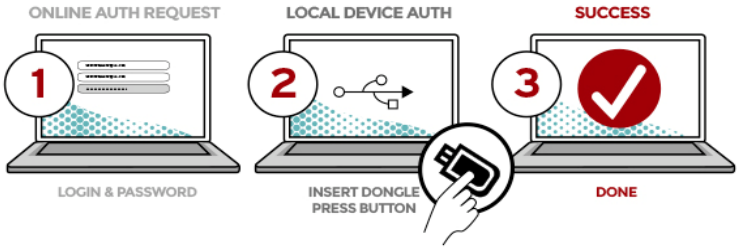
UAF (Universal Authentication Framework)

PASSWORDLESS EXPERIENCE

단말에 탑재된 생체인식 기능 이용한 온라인 인증 방식

U2F (Universal 2nd Factor)

SECOND FACTOR EXPERIENCE



패스워드 인증 강화 위해 별도의 인증 추가하는 방식

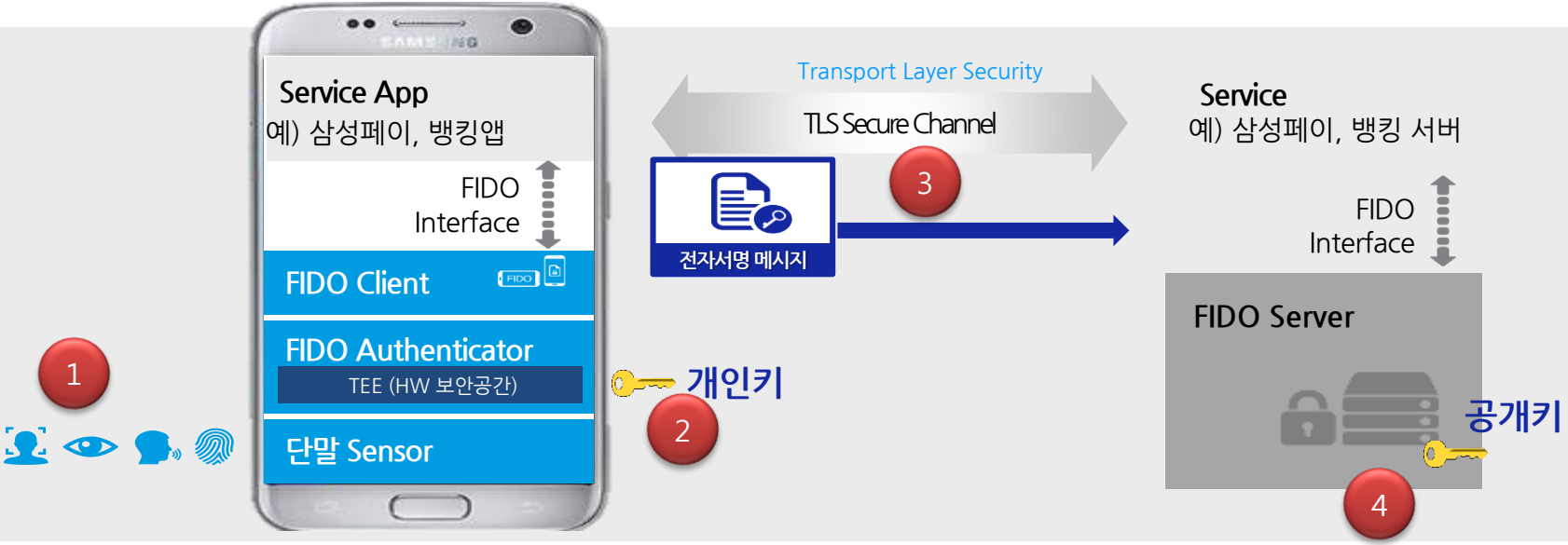
FIDO 개요

① 디바이스에 전달되는 사용자 생체정보와 디바이스내 보관된 생체정보 매칭

② 매칭되면 디바이스내 보관되어 있던, 개인키 이용 서명

③ 서명정보가 TLS 보안채널 통해 서버에 전달

④ FIDO서버에 보관되어 있는 사용자 공개키로, 보내진 서명정보 검증



FIDO 특장점

"개인정보 이슈 없이 생체인증 사용 가능"

Fast IDentity Online(FIDO)은,

생체정보를 사용자 단말에 저장하고,
FIDO서버에는 저장하지 않아 개인정보 이슈 없음

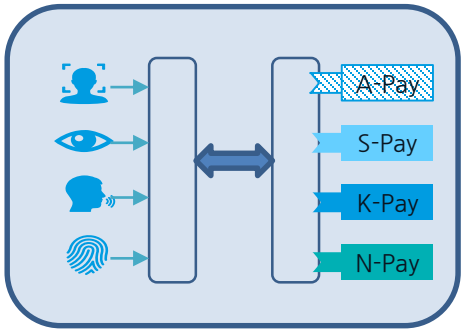
Convenient

- 패스워드 기억 주필요
- 인증소요시간 단축

Secure

- Multi-Factor 인증: 생체 + PKI
- 생체정보 노출 없음

Extensible



- 생체인증 수단 선택 가능
- FIDO지원 모든 단말 호환

Remained issues for FIDO

✓ 보안성 보장

FIDO Certification은 FIDO표준 준수만 검증하고 보안적합성은 검증하지 않음

✓ 단말 내 생체정보와 개인키의 안전한 보관

Private-Key

✓ 생체인증이 불가한 경우에 대한 대안

Contents

Samsung SDS

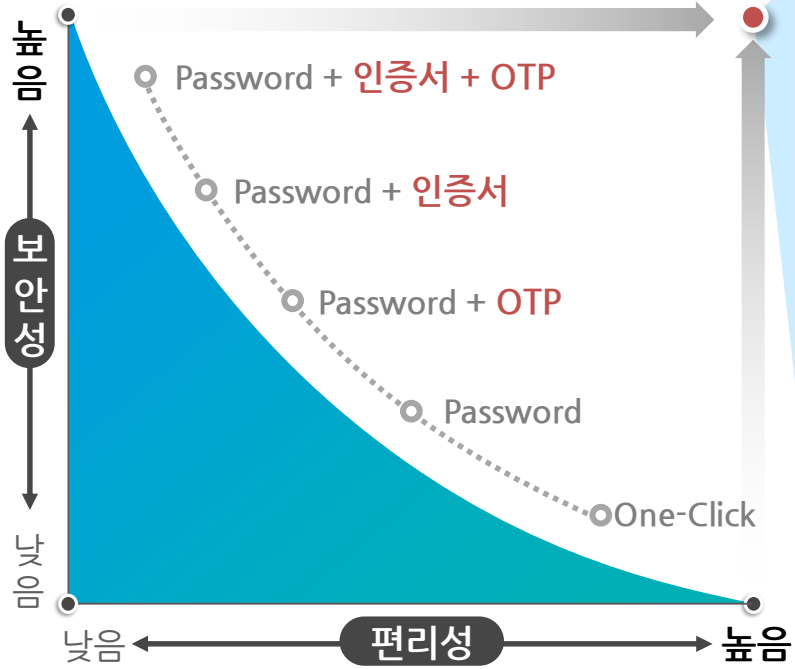
Nexsign

(Next generation + Signature)

※ 적용예시 : 삼성페이

- FIDO 제품군 '세계유일' CC(Common Criteria) 인증 획득
  - ➔ 보안적합성 보장
  - CC인증: IT제품의 보안성을 평가하기 위한 국제기준(ISO 표준)
- 단말 내 Secure Storage(SW, HW) 구현/사용
  - ➔ 생체정보 및 암호화 키에 대한 저장 보안성 확보
- 생체인증(지문, 얼굴, 음성, 홍채) 및 타 인증수단(PIN, PW) 지원
  - ➔ 인증수단 다양성 확보(생체인증 불가 시 대응 가능)

Nexsign 솔루션 개요



Samsung SDS

Nexsign

편리성

- 다양한 생체 정보를 활용한 Passwordless 인증 수단 제공

지문 안면 음성 홍채

보안성

- 요구되는 보안 수준에 따른 다양한 인증 정책 수립 지원
- 해킹 방지를 위한 서버↔스마트폰까지 안전한 인증 환경 구축
- 스마트폰에서 안전한 문서 보안 열람 기능 제공

핵심 기술

- 공개키 암호화 방식(PKI)의 인증체계기반 서버 인증
  * Public Key Infrastructure
- 스마트폰 보안공간 (TEE, Secure Element 等) 활용 해킹 방지
  * Trusted Execution Environment

Nexsign 활용 분야

온라인 쇼핑몰

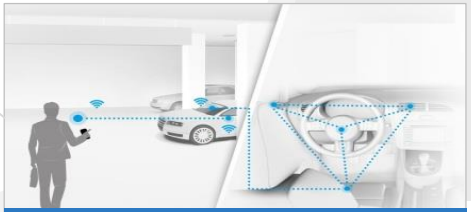
데모

모바일 뱅킹/금융 상품가입

증권 MTS

동영상

사내 시스템



Smart Car

- SSO
- Mouse log-in

01. Passwordless 기반 고객 편의성 제고

- 복잡한 결제 과정으로 인한 구매 포기 고객의 이탈 방지
- 간편하고 안전한 인증으로 고객 만족도 증대 및 기업 이미지 제고

02. 모바일 중심 기업 경쟁력 강화

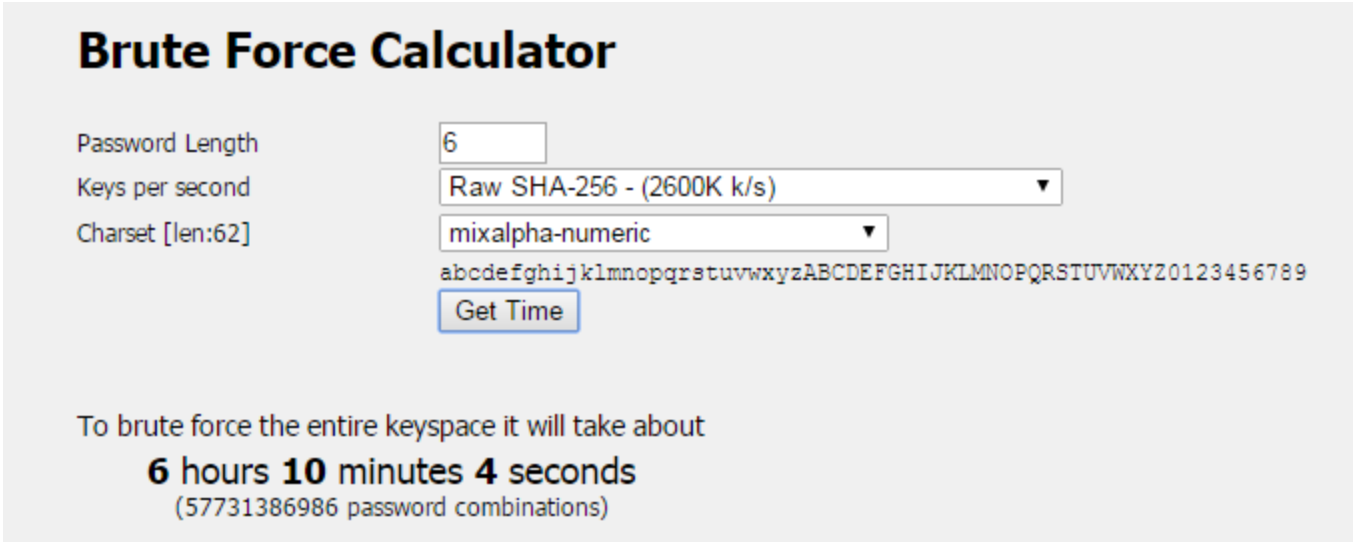
- 안전하고 편리한 모바일 중심의 업무 환경 구축 지원
- 모바일기반 현장완결型 서비스 제공으로 업무 생산성 및 고객 만족도 제고

03. 서비스 보안 강화 Cost Saving

- 보안위협을 사전에 차단하여 금융보안사고 발생 비용 예방
- 사용자 실수로 인한 결제 건 부인방지로 기업손실 감소


Q&A

[별첨]Time for Password Crack

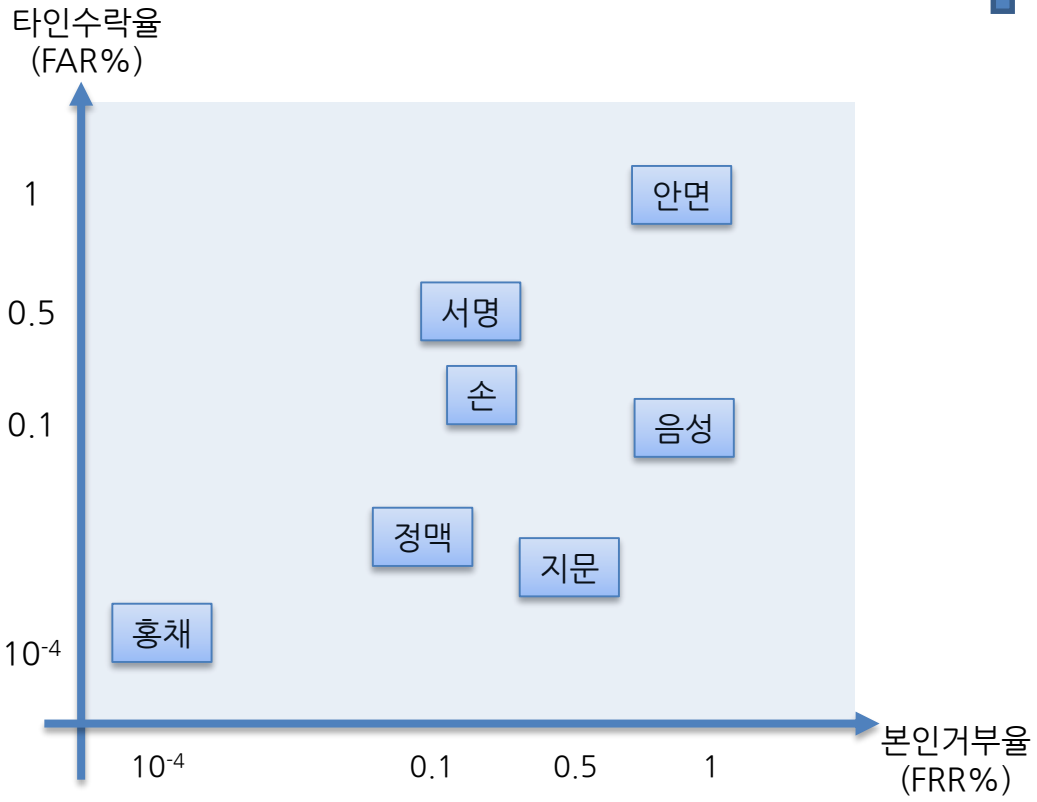


Reference: http://calc.opensecurityresearch.com/

[별첨]생체인증 수단별 정밀도

수단	본인거부율 (FRR%)	타인수락율 (FAR%)
지문	0.5	10^{-2}
홍채	10^{-4}	10^{-4}
서명	0.2	0.6
안면	1.0	1.0
음성	1.0	10^{-1}
손	0.2	0.2
정맥	10^{-1}	10^{-3}

출처: [논문]다중 생체인식 기반의 인증기술과 과제-조병철, 박종만



[별첨]Nexsign CC Certified

Secure Storage 확보를 통해 생체정보 및 개인키를 안전하게 보관하여 최고수준의 보안환경 제공

검증된 보안 솔루션, Samsung SDS Nexsign

- FIDO Alliance 공식 인증된 UAF 제품군 보유
- **FIDO 제품군 '세계유일' CC(Common Criteria) 인증 획득**
- **삼성페이, Kpay, K뱅크, 대구은행, 삼성카드** 등 대규모 레퍼런스로 보안성, 안전성 입증
- 국내외 권위있는 IT 상 수상
  - ✓ **K-ICT 대상, 기술선도 부문 「대통령상」 수상 ('15.10)**
  - ✓ **MWC Glomo Award-Best Mobile Security 수상 ('17.2)**

공통평가기준(Common Criteria)이란?

- IT제품의 보안성을 평가하기 위한 국제기준(ISO 표준)
- 민간업체에서 개발한 정보보호제품 내의 보안기능에 대한 안전성을 국가에서 인증하는 제도

FIDO Certified™ , CC 인증, 국내외 IT 수상 및 대규모 레퍼런스로 솔루션 호환성, 보안성, 안전성 입증

Secure Storage 적용을 통한 보안수준 상향

- **생체정보 및 개인키를 Secure Storage에 저장하고 Secure Storage 내에서 암복호화, 서명, 공개키쌍 생성 수행**
- TEE(Trusted Exdcution Environment): TrustZone H/W 기반의 독립된 보안환경 제공
- WBC(White Box Crytography): 암호키가 암복호 알고리즘 내부에 암호기술로 숨겨져 있어 암호키 해석을 어렵게 하는 암호 기술

[별첨]Nexsign 다양한 인증 수단

Multi-Modal 및 Multi-Factor 등 다양한 인증수단을 활용하여 간편하고 범용적인 사용자 인증절차 제공

Multi-Modal/Multi-Factor Authentication 제공

- Multi-Modal 지원 : 지문, 얼굴, 음성 등 다양한 생체정보를 활용, FIDO Protocol 기반 사용자 인증 지원
  - 간편하고 보안성 높은 Nexsign 솔루션 제공
- Multi-Factor 지원 : 기존 ID/PW, PIN 등 기존에 사용하던 인증방식을 활용하여 FIDO 인증 제공
  - 다수의 사용자에게 Nexsign 인증 제공 가능

편의성

보안성