인증 기술의 변화와
IRUKEY · OTID 발전

코리아엑스퍼트 전략사업부

Yoo, In Ji

KoreaExpert

KoreaExpert

코리아 엑스퍼트는?

- ✓ 24년간 검증된 기술력과 노하우
- ✓ 550여 개 다수의 고객사
- ✓ Rule 기반 시스템
- ✓ Data Mining 분석 모델 개발
- ✓ **2015년 R&D 및 IRUKEY개발**
- ✓ **2017년 사용자 인증 사업 출범**

인증기술의 변화

KoreaExpert

[법제도 동향] 공인인증서 제도 폐지

공인인증서 사용 의무 폐지
(2015. 03)

보안카드 및 OTP 사용 의무 폐지
(2016.06)

보안카드·OTP 의무 사용 폐지

공인인증서 이어 일괄적 보안방식 없애
생체인증 등 다양한 핀테크 등장할 듯
보안 강화·금융서비스 확대 효과 기대

강은성 기자 esther@dt.co.kr | 입력: 2016-04-18 12:30

KoreaExpert

[법제도 동향] ISMS/PIMS 인증 통합 “ISMS-P”

기존 ISMS “정보보호 관리체계 인증제도“
인증기준 104개 항목

기존 PIMS “개인정보보호 관리체계 인증제도”
인증기준 86개 항목

ISMS-P
“정보보호 및 개인정보보호 관리체계 인증”
인증기준 102개 항목 통합

번호	항목	설명
신규 1.2.2	현황 및 흐름분석	관리체계 전 영역에 대한 정보보호 서비스 및 개인정보 처리 **현황을 분석하고 업무절차와 흐름을 파악**하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.
신규 2.3.1	외부자 현황 관리	**업무의 일부를 외부에 위탁하거나 외부의 시설 또는 서비스를 이용하는** 경우 그 현황을 식별하고 법적 요구사항 및 외부조직 서비스로부터 발생되는 **위험을 파악하여 적절한 보호 대책을 마련**하여야 한다.
신규 2.10.2	클라우드 보안	클라우드 서비스 이용 시 **서비스 유형에 따른 비인가 접근, 설정 오류 등에 따라 중요정보와 개인정보가 유출 및 노출되지 않도록 관리자 접근 및 보안설정** 등에 대한 보호 대책을 수립 이행하여야 한다.
신규 2.10.4	전자거래 및 핀테크 보안	전자거래 및 핀테크 서비스 제공 시 정보유출이나 데이터 조작 사기 등의 침해사고 예방을 위해 **인증 암호화 등의 보호대책을 수립**하고, **결제 시스템 등 외부시스템과 연계할 경우 안전성을 점검**하여야 한다.

[법제도 동향] 사용자 인증 보안성 강화 권고

주요 내용	설명
행정자치부 개인정보의 안정성 확보 조치 기준 해설서	• 제6조(접근통제) ② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. (인증수단 예시: 인증서, 보안토큰, 일회용 비밀번호 등)
금융위원회 전자금융감독규정	• 제17조(홈페이지 등 공개용 웹 서버 관리대책). 2. 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디, 비밀번호 이외의 추가인증수단을 적용할 것
교육부 학교생활기록부 기재 개선 방안	• 현재 공인인증서로 나이스에 로그인한 후 조회와 입력이 모두 가능하나, 향후에는 인증절차를 2단계로 설정할 계획 • 1차 인증은 개인공인인증서로 '조회'만 가능하고, 2차 인증은 ARS 또는 일회용번호로 인증 후 '조화와 입력'이 가능하도록 할 계획
공공기관 보안 감사 평가항목	• 업무시스템 보안, 전자우편 보안 등에 보안성을 강화한 사용자 인증 방식을 사용하는 것에 대한 항목

→ **외부 접속의 경우
안전한 접속수단 or 안전한 인증수단 적용**

→ **업무관련자 접속만 허용
ID, PW 이외의 추가인증 수단 적용**

→ **1차 (개인공인인증서) – '조회' 가능
2차 (ARS/일회용번호) – '조회+입력' 가능**

→ **보안성이 높은 사용자 인증 수단 사용
(생체인증, 일회용비밀번호 등)**

인증시장, 신기술이 많고, 서비스 유행에 민감하다.

서명패턴 인증

공인인증서

OTP

생체인식

멀티터치기반
비밀번호

키입력 패턴인증

일회용 ID

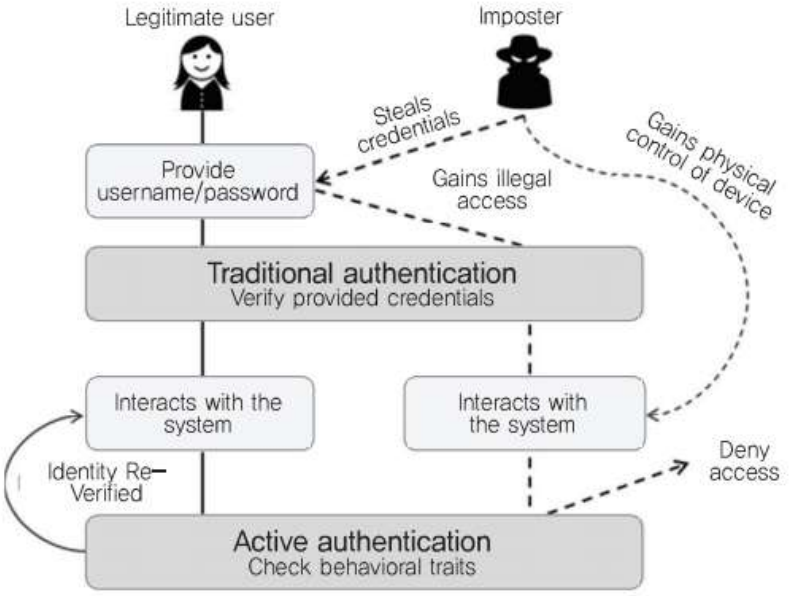
아이핀(i-PIN)

간편결제
인증방식

휴대폰 인증

KoreaExpert

[인증기술 동향] 무자각 지속인증



출처: ETRI, 2018

무자각 지속인증

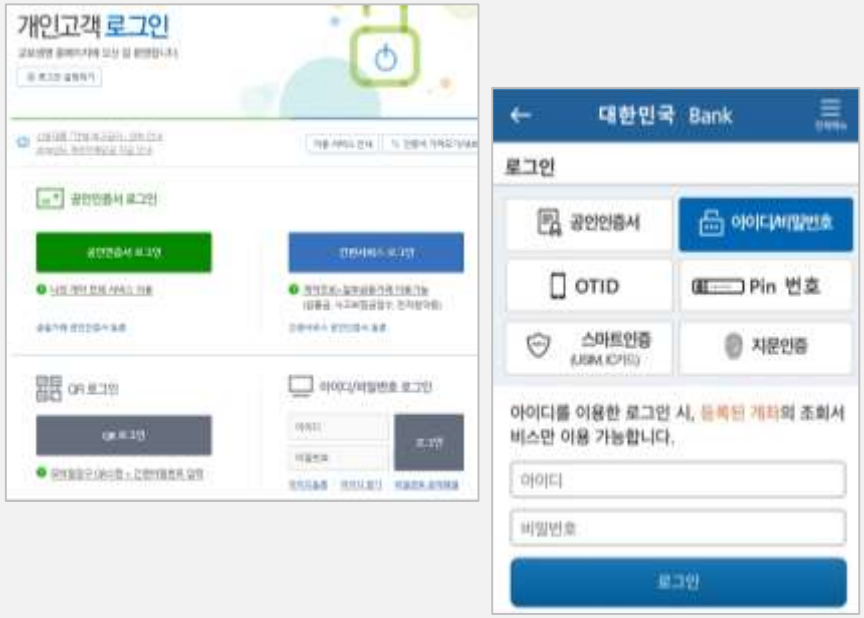
- ✓ 사용자는 인지하지 않아도 지속적 신원 검증이 이루어져 편리함
- ✓ 명시적 인증 절차를 통과하거나 인증 세션을 가로챈 해커일지라도 접근 차단이 가능

- → 행위 기반 인증 (음성,걸음걸이, 타이핑 패턴 등)
- → 사용자 디바이스 인증 (사용자 디바이스 내 앱 실행시 마다 인가된 사용자 기기인지 지속적으로 확인)

[인증서비스 동향] 사용자 선택형 인증

사용자 선택형 인증

- ✓ 획일화된 인증수단이 아닌 ID/PW, 공인인증서, 간편PIN, 생체인증 등 다양한 인증 수단을 제시
- ✓ 사용자가 원하는 수단을 선택하도록 함

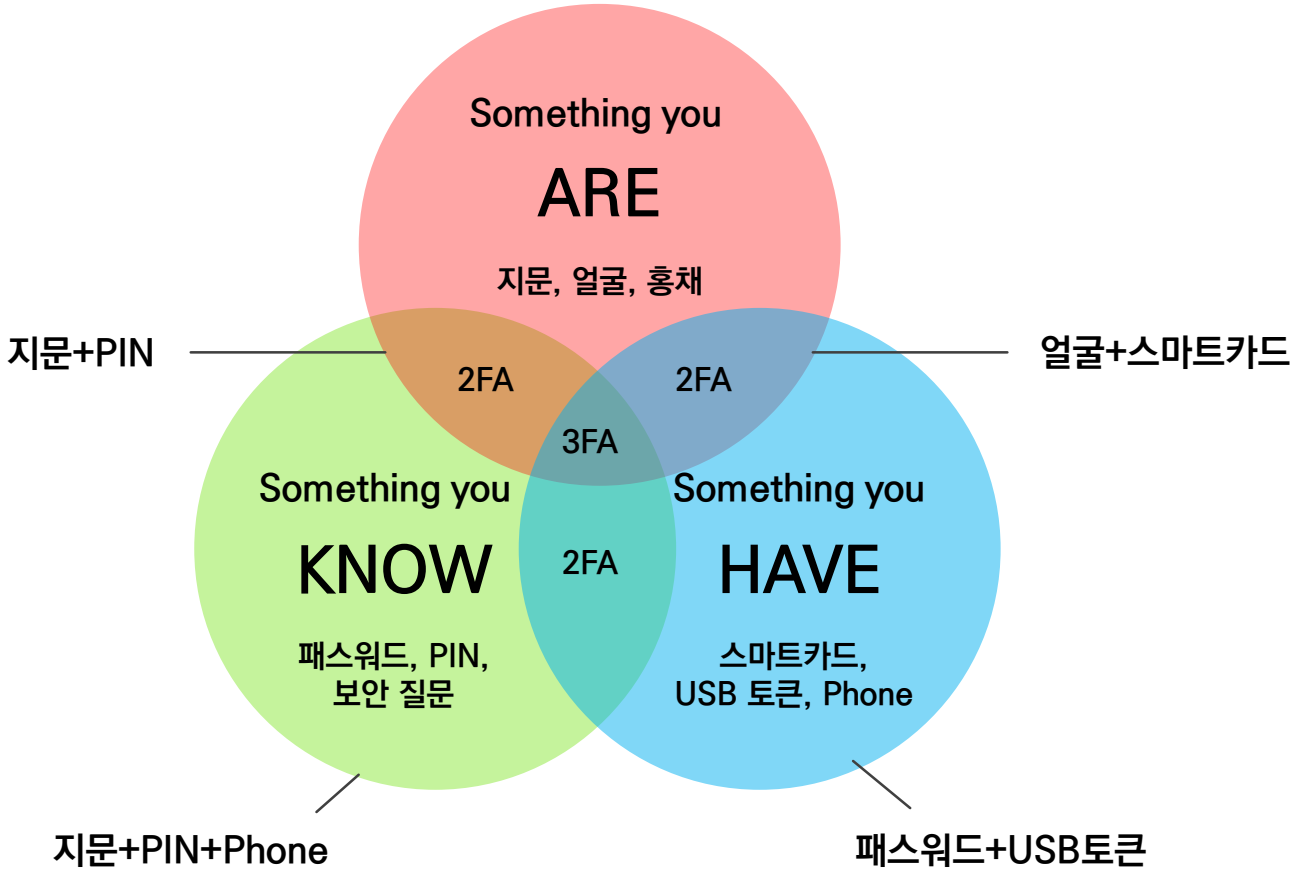


회원 가입 없는 간편 인증

- ✓ 별도의 회원가입 없이 서비스를 이용할 수 있도록 함
- ✓ 비회원 로그인, SNS를 활용한 로그인 등의 방식을 제공

KoreaExpert

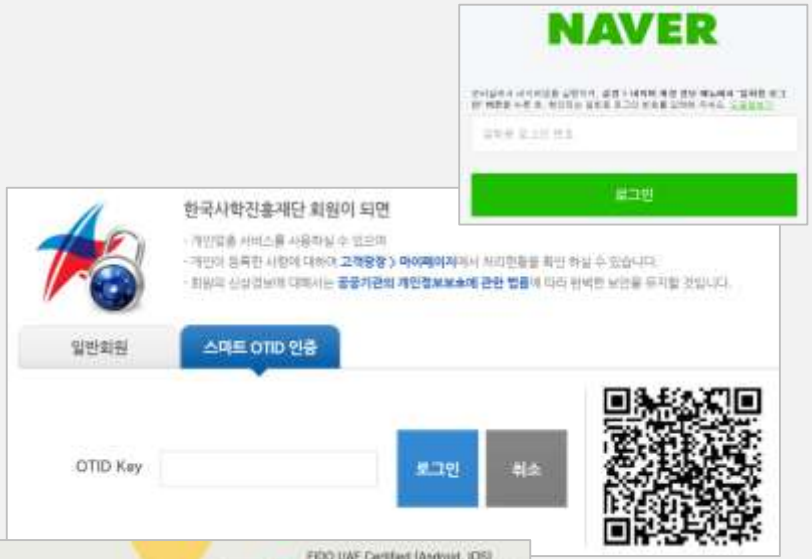
[인증서비스 동향] MFA, Multi Factor Authentication



KoreaExpert

[인증서비스 동향] Password-less 인증

Password-less 추세 확산



[Summary]

법·제도 동향
- 공인인증서 의무화 폐지
- 전자서명법 개정
- ISMS-P 인증 통합
- 국제 표준 ISO/IEC 29115
- 추가인증, MFA 의무, 권고 강화

인증기술 동향
- 최신기술 기반의 인증수단 다양화
- 블록체인 신원 인증
- 무자각 지속 인증

서비스 동향
- 사용자 선택형의 다양한 인증수단 제시
- 다중요소 인증(MFA)
- Password-less 인증

일회용ID기반 인증 솔루션 'IRUKEY(아이루키)'는?

- ☑ 인증관련 최신 법, 제도 및 표준에 부합
- ☑ 사설인증 역할 / 추가인증(2팩터 인증) 역할 가능
- ☑ 최신 기술 기반의 사용자 편의성 위주의 인증수단 역할
- ☑ 사용자 선택형 인증 중 하나의 수단으로, MFA / 무자각 지속인증 / Password-less 인증에 부합

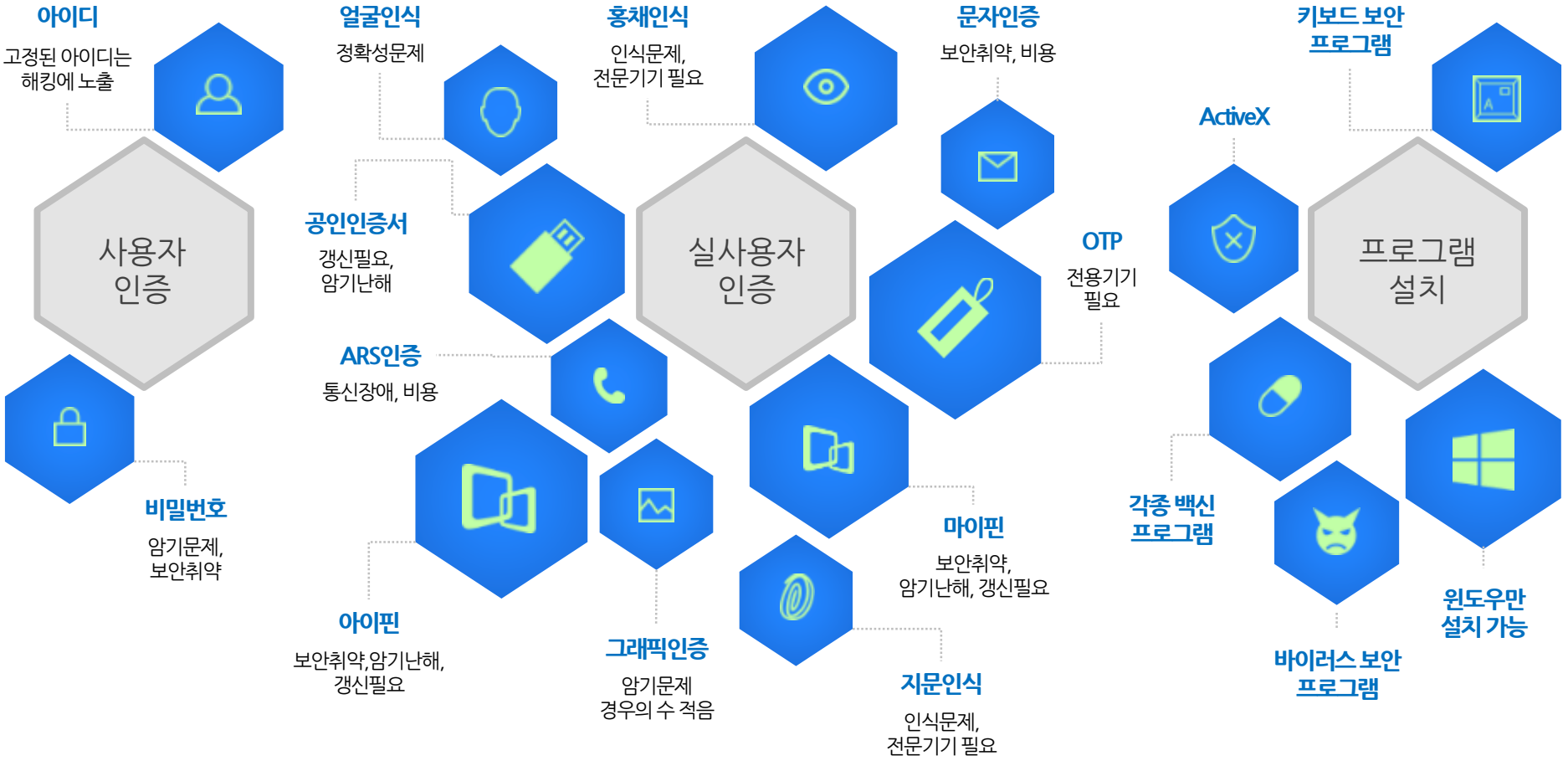
ID/PW 통합한 OTID
IRUKEY 소개

OTID
One Time Identity

IRUKEY
Identity Random Unique KEY

KoreaExpert

사용자 인증의 근본적인 문제 : 고정된 ID



KoreaExpert

IRUKEY 개요

OTID
(One Time ID)

사용자를 구분하는 일회용 랜덤 코드

- 1회성 사용
- 랜덤
- 유일성 (사용자구분)
- 자체발생 (통신하지 않음)
- 다형성 (용도/방식 다양)

모바일로 자체 생성된

일회용 랜덤코드로 사용자 인증

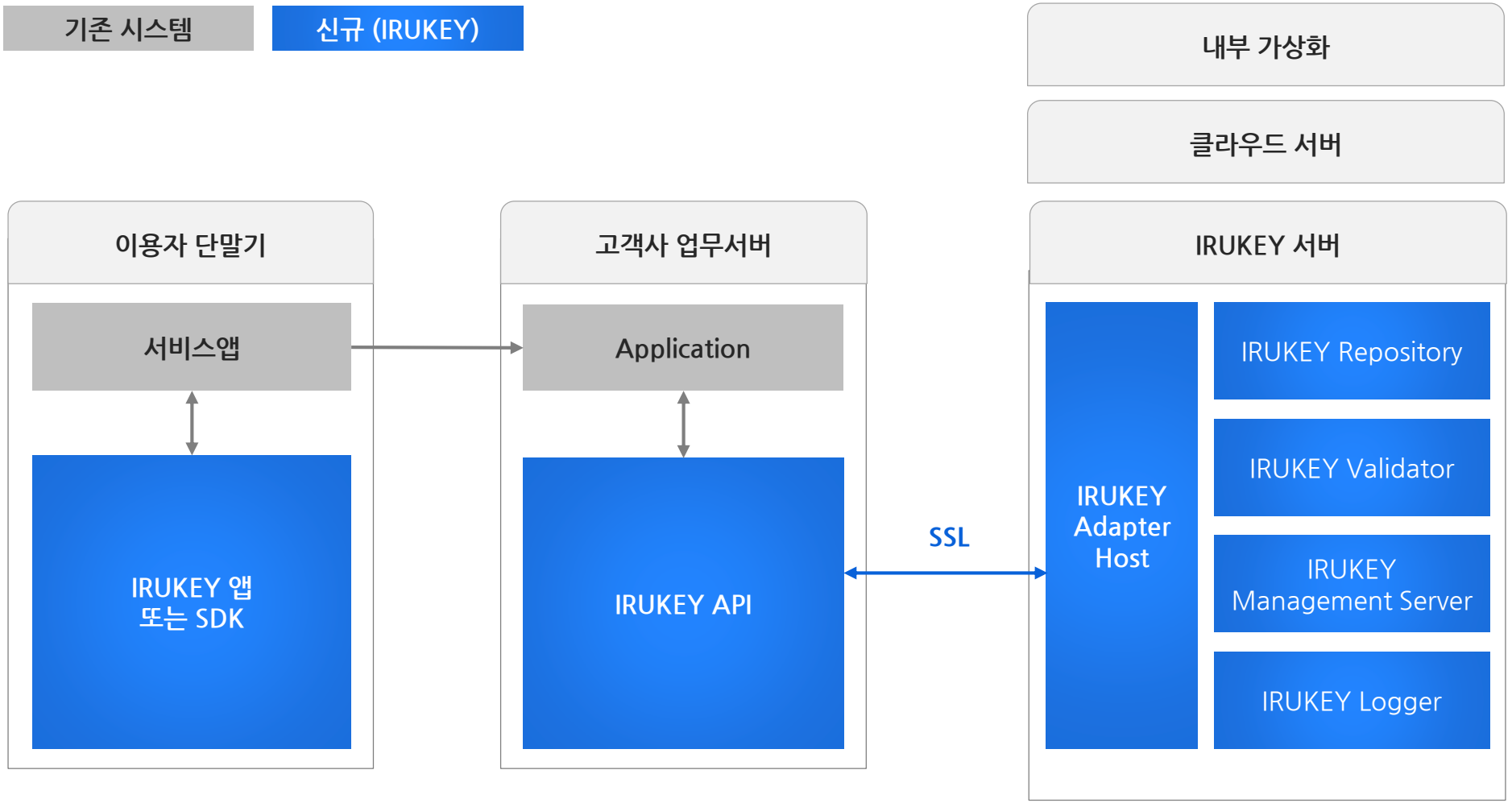
ID 뿐만 아니라

다양한 인증방식 대체

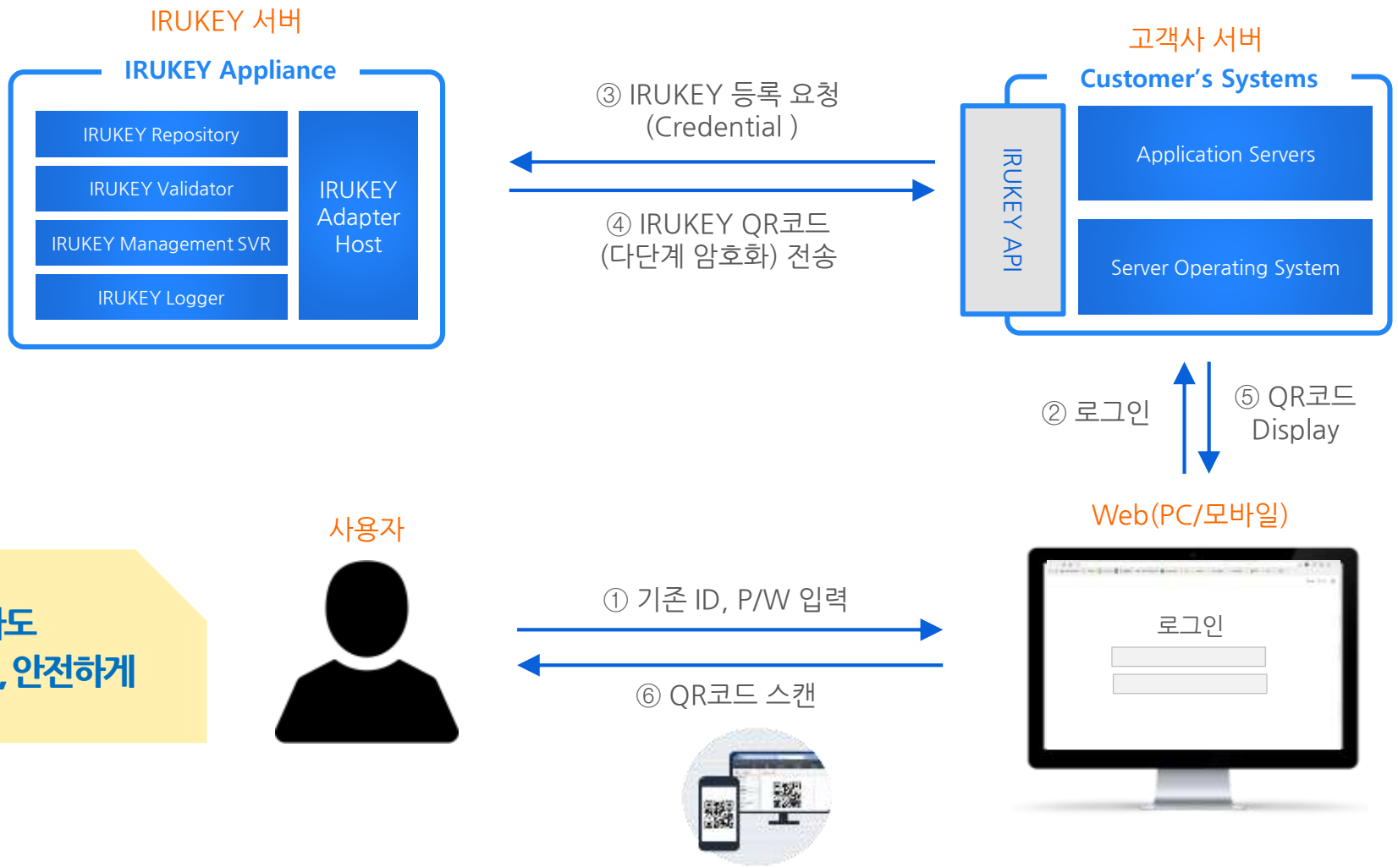
OTP | ID,P/W | 인증서 | ARS | SMS | PIN인증 | ID Protector

KoreaExpert

IRUKEY 시스템 구성



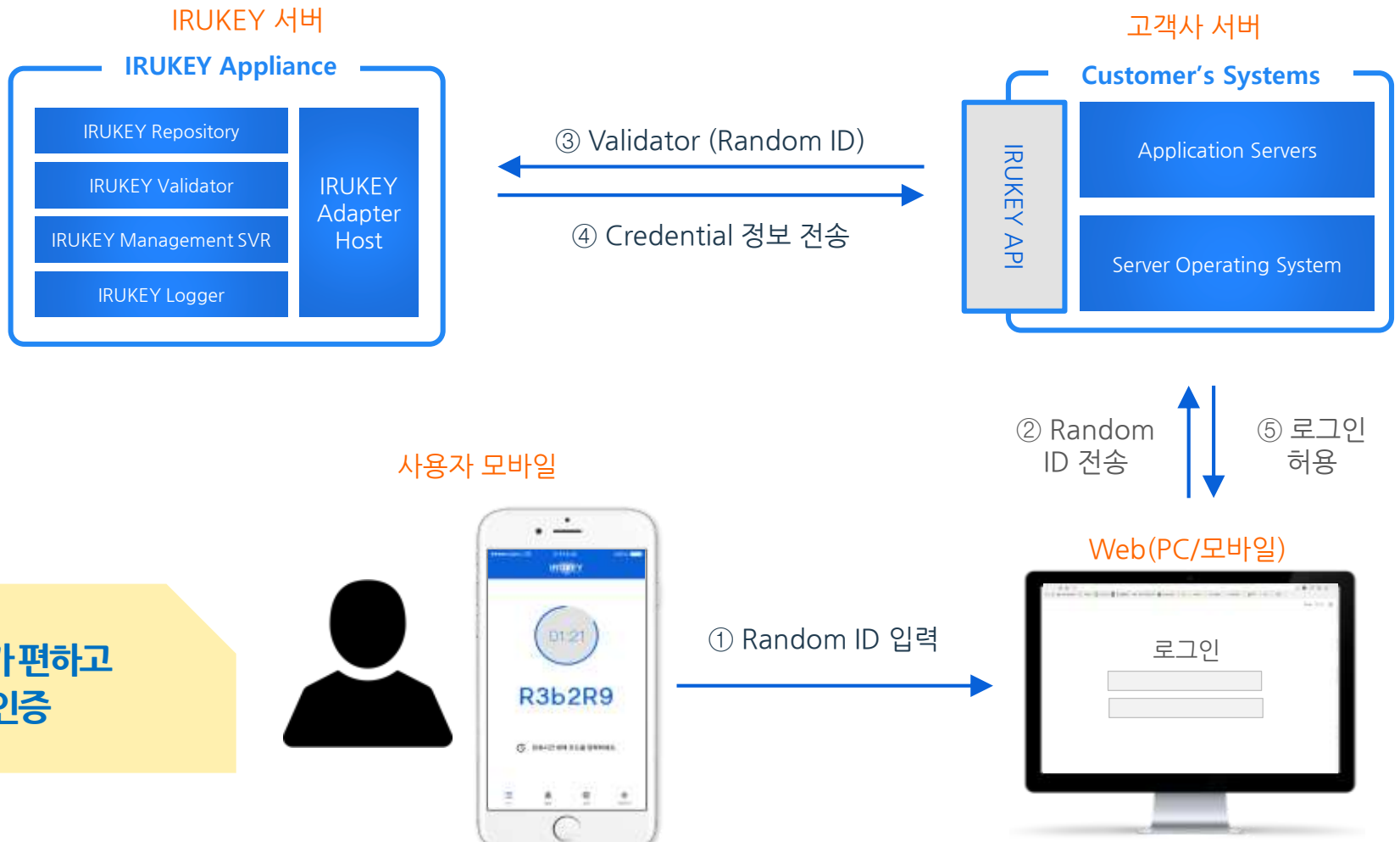
IRUKEY 서비스 절차 – 등록



등록 절차도
편리하고, 안전하게

KoreaExpert

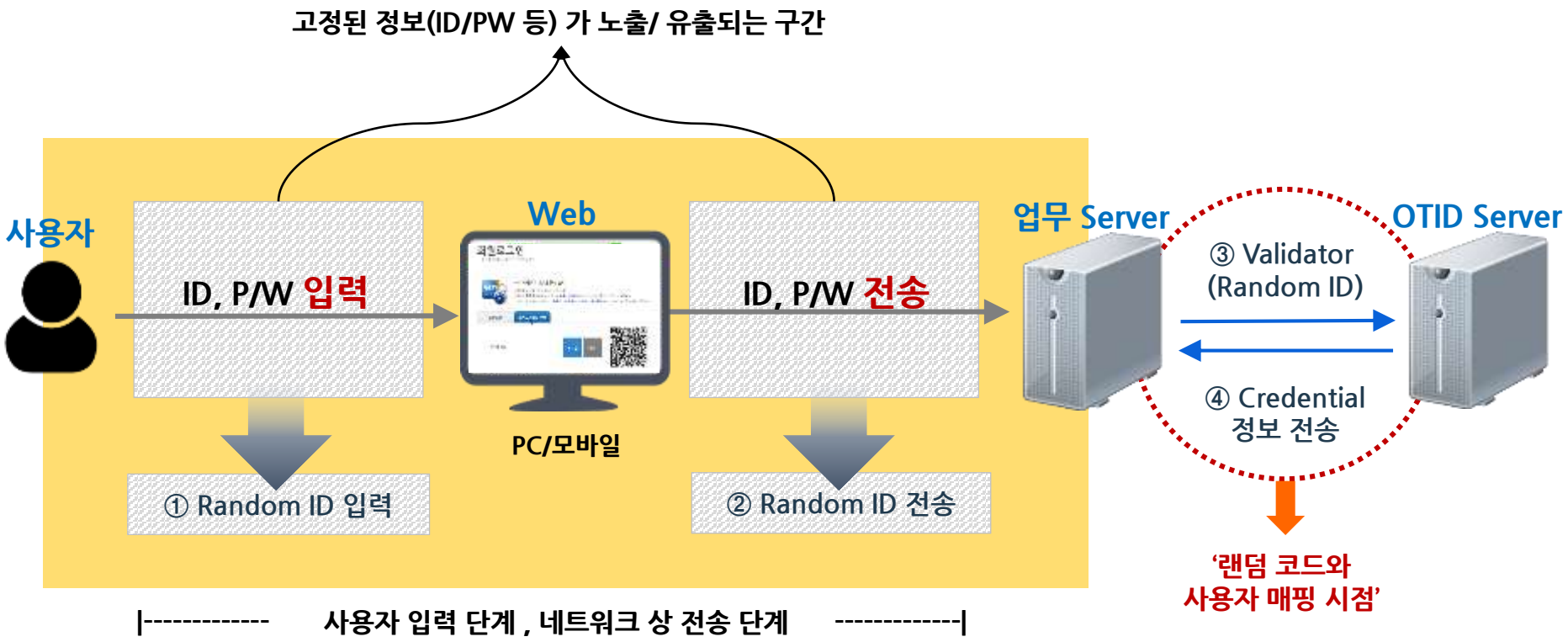
IRUKEY 서비스 절차 – 인증



사용자가 편하고 안전한 인증

KoreaExpert

IRUKEY 등록 / 인증 프로세스



OTID - 랜덤 코드 사용

'한번 사용하고 버려지는 소유기반의 사용자 정보'

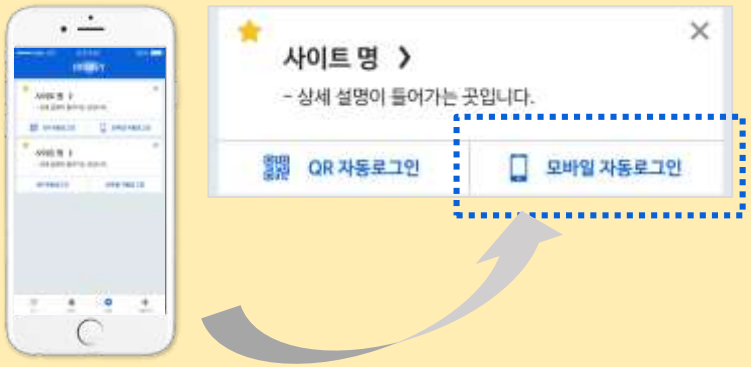
IRUKEY 주요기능 – 다양한 인증방식 제공

랜덤 코드 입력

❖ 보고 입력 또는 듣고 입력하는 방식
(랜덤코드 음성지원 가능)

간편 스캔

모바일 자동 로그인



PIN 입력

유효시간이 지나면
랜덤하게 바뀌는 ID 테이블

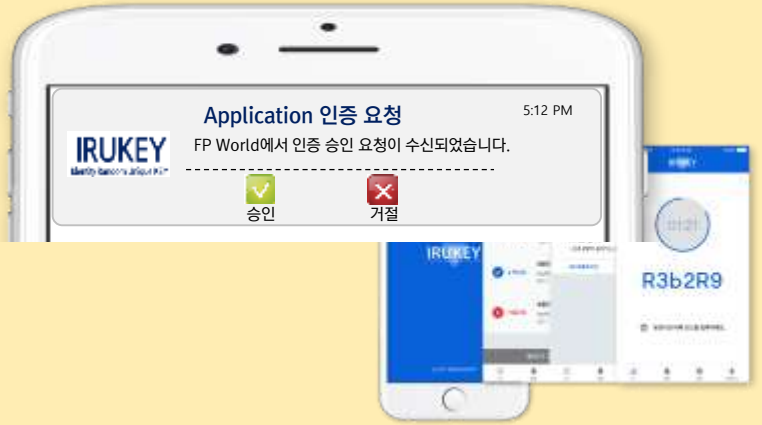
[사용자 입력 키패드(셔플링)]

KoreaExpert

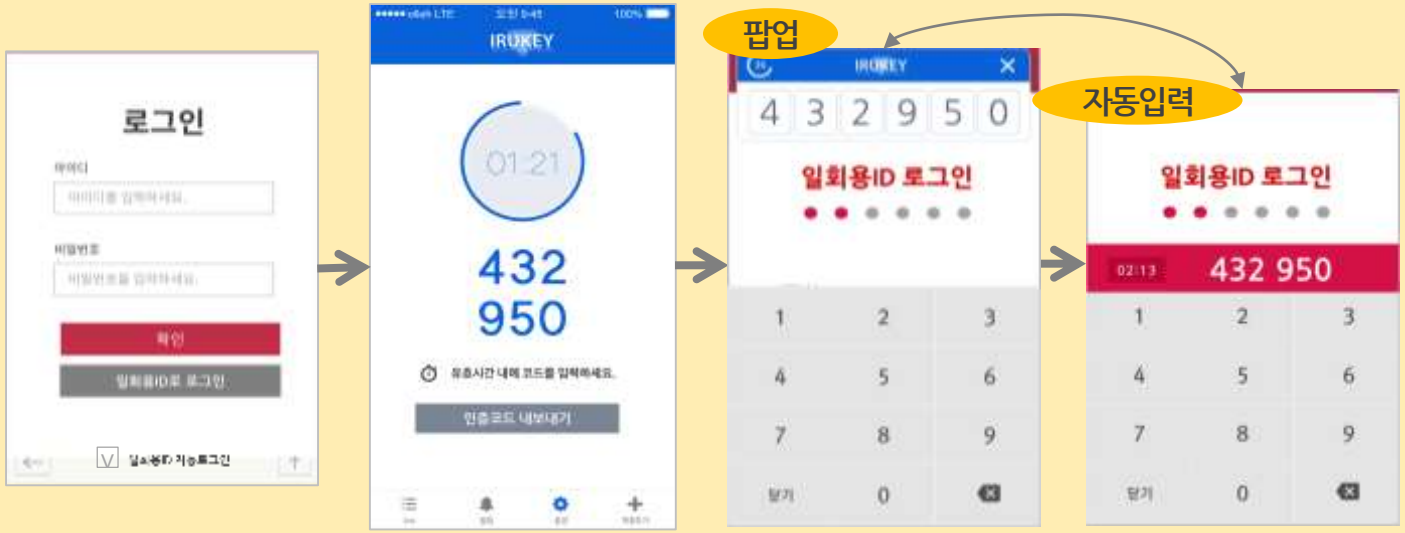
IRUKEY 주요기능 – 다양한 인증방식 제공

Push 알람

❖ 보고 입력 또는 듣고 입력하는 방식
(랜덤코드 음성지원 가능)



팝업 창& 자동입력



KoreaExpert

IRUKEY 주요기능 –서비스 연동 및 코드 설정 기능

다양한 서비스 연동 가능

다양한 구성의 랜덤코드 설정 가능

숫자

숫자 + 소문자

숫자 + 대/소문자 + 특수문자

KoreaExpert

IRUKEY 핵심기술

1 사용자 별 중복 없이 랜덤한 코드를 부여하는 IRUKEY 핵심 기술

랜덤코드 생성 기술

82개 문자로 수많은 경우 수로 + 동일 시점에 중복 없이 생성

"사용자 인증을 위한 ID 본연의 역할"

- 충돌 없음 → 유일성 보장
- 변경 패턴을 유추할 수 없는 일회성의 랜덤 ID로 제공
  → 사용자 식별을 위한 ID로써 역할 가능
- 82개의 영문 대소문자/숫자/특수문자로 다양한 코드의 조합 가능
- 6자리 랜덤ID 구성 시, 82^6 → 약 3천억(304,006,671,424개) ID 생성

2 랜덤 ID가 특정 사용자임을 확인하기 위한 Mapping 기술

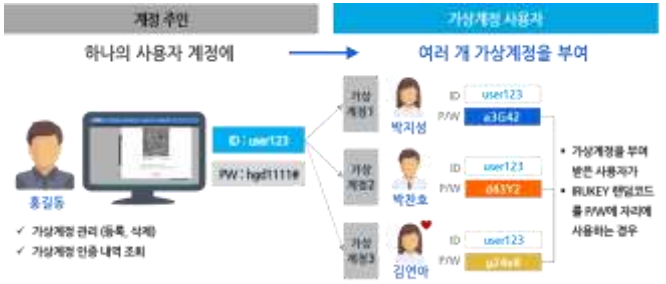
사용자 맵핑 기술

- IRUKEY만의 사용자 Mapping 기술은, 랜덤ID로 로그인을 시도한 사람이 특정 사용자임을 확인해주는 특허기술 기반의 차별화된 기능을 제공

3 하나의 계정에 여러ID를 부여하여 인증할 수 있는 기술

가상계정 사용자 인증

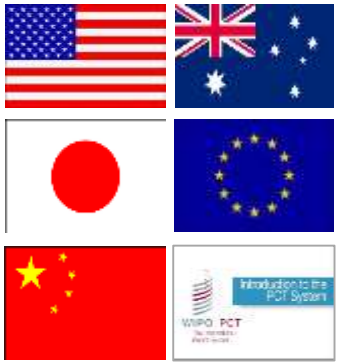
- Legacy 수정없이(추가 계정 발급 없이)하나의 계정에 여러ID를 부여할 수 있는 기술
- 계정의 실 소유자가 계정을 공유하고자 하는 사용자에게 가상계정을 부여하여 사용, 관리할 수 있도록 함



KoreaExpert

IRUKEY 특허 / 인증

특허등록



특허협력조약- 국제특허

GS인증 1등급

보안컨설팅

금융보안원

앱 취약성 점검

KISA 한국인터넷진흥원

모의해킹

TIGER TEAM

KoreaExpert

아이루키 적용가능 분야

금융기관 | 공공기관 | 그룹사 | 제조 | 교육 | 의료 | 게임/상품권 | ...

대외 서비스(대국민)

- ☑ **홈페이지 구축/개편**
- ☑ **모바일 웹/앱 구축/개편**
- ☑ **간편인증 시스템 구축/개편**
  - **– 인터넷/모바일뱅킹, 보험사 사이버창구 등**
  - **– 홈쇼핑 간편인증**
  - **– 대학 이러닝 2차인증**
  - **– 병원 모바일 환자카드, 의료통합정보시스템**

대내 시스템 (임직원/협력사)

- ☑ SSO, 그룹웨어, 이메일, 파일서버, 문서중앙화 등
- ☑ **보안솔루션 연동** (VPN, VDI, 서버/ DB접근제어, NAC)
- ☑ 업무지원 시스템 (Ex. 보험 설계사 영업지원시스템)
- ☑ 기타 시스템 관리자 인증
- ☑ 디바이스 인증
- ☑ 계정공유가 불가피한 경우 (보험사 GA법인 대리점 (대리점주–내근직), 통신사 대리점(대리점주–직원), 대학교(교수/조교), 병원(의사–인턴), 법인인증서 사용 시 (임직원간)

IRUKEY Case Study

OTID
One Time Identity

IRUKEY
Identity Random Unique KEY

★부득이하게 자료 배포가 안되는 점 양해 바랍니다.

KoreaExpert

감사합니다

OTID
One Time Identity

IRUKEY
Identity Random Unique KEY

KoreaExpert