OTID
One Time Identity

금융 인증 혁신을 위한
OTID(일회용ID) 적용 전략

코리아엑스퍼트
전략사업팀 유인지

KoreaExpert

IRUKEY
Identity Random Unique KEY

회사소개

회사명	코리아엑스퍼트㈜		사업기간	21년 9개월 (1995년 3월 ~ 2016년 12월 현재)	
사업분야	**국내외 최초** One Time ID (사용자 인증 솔루션) 개발, 공급	**빅데이터 기반** Fraud and Detection, Credit, Underwriting 의사결정지원시스템 개발, 공급	**빅데이터 기반** 내부정보유출방지/ 신감사 시스템 개발, 공급	**미국 3대 분석 전문 기업** **FICO 사의** BRMS/통계솔루션 (MB, MDBT, IRE) 공급	**금융, 공공** 비즈니스 룰/통계 컨설팅 및 공공과제 수행
인증 및 특허	   ➢ 아이루키 관련 특허(유일 랜덤 코드 생성/일회성 비밀번호/가상계정)		 ➢ 아이루키 GS인증	 ➢ 사기방지시스템 GS인증	 ➢ 정보유출방지시스템 GS인증  ➢ ISO 9001 품질인증서

주요사업분야

- 금융 의사결정 업무에 대한 어플리케이션 PKG 개발, 공급 (보험청약/클레임, 대출심사, 사기탐지, 감사, 자금세탁방지 등 적용)

- 국내외 최초 사용자 인증 ID 솔루션 "아이루키" 개발, 공급 (일회용 비밀번호/랜덤코드생성/가상계정 부문 특허 출원)
- 빅데이터 기반 개인정보유출분석시스템 개발, 공급

- BRMS 솔루션 - 세계최고 비즈니스 지식처리 룰 엔진 (Blaze Advisor) 공급
- 통계 솔루션 - 데이터 마이닝 Tool (Model Builder, KeR)
- 연관관계분석 솔루션 IRE 등 공급
- 빅데이터 기반 통계 플랫폼 개발 /공급

- Fraud and Detection,Underwriting, 감사 업무 관련 시나리오 도출 컨설팅 전문 인력 보유
- 비즈니스 분야 시나리오/룰컨설팅
- 통계 기반의 예측 분석 모델링

주요제품

일회용 아이디 인증 솔루션 IRUKEY	개인정보 유출분석시스템 iArgos™	신감사시스템 NexS³-SAS	자금세탁방지 시스템 NexS³-AML
보험사기탐지 시스템 NexS³-FDS	보험청약심사 시스템 NexS³-EUS	여신전략운용 시스템 NexS³-CSS	여신감리 시스템 NexS³-CAS
BRMS 솔루션 Blaze Advisor	데이터 분석 솔루션 Model Builder, MBDT	연관관계 분석 솔루션 IRE	빅데이터 통계 솔루션 KeR

빅데이터 기반 NexS³-Framework Platform

보유 고객사

은행

우리은행
IBK 기업은행
KB 국민은행
하나은행
KDB산업은행
Standard Chartered
KEB 외환은행
pepper 저축은행
JT친애저축은행

보험

SAMSUNG 삼성생명
한화생명
KYOBO 교보생명
NH농협생명
신한생명
MG새마을금고
MetLife
Hyundai Life
산업은행계열 KDB생명
Prudential Financial
AIG
Heungkuk Life Insurance
Heungkuk Fire & Marine Insurance
동양생명
LIG 손해보험

캐피탈/카드

Hyundai Card
Hyundai Capital
Hyundai Commercial
아주캐피탈
효성캐피탈
하나캐피탈
DOOSAN 두산캐피탈
NH농협캐피탈
BCcard
신한카드

공공

기획재정부 MINISTRY OF STRATEGY AND FINANCE
건강보험심사평가원
ksure 한국무역보험공사
h·well 국민건강보험 National Health Insurance Service
EVERRICH 우체국예금보험
행정자치부
Your Best Credit Partner SGI서울보증
HF 한국주택금융공사
NIA 한국정보화진흥원
케이에프 KFPP 한국사학진흥재단

통신, 제조 및 기타

SK telecom
SK marketing & company
SK 이노베이션
LG전자
LG화학
LG U+
AMOREPACIFIC CORPORATION
HYUNDAI MOBIS
HYUNDAI
DOOSAN 두산인프라코어
GS 칼텍스
SERVEONE 주식회사 서브원
가톨릭대학교 THE CATHOLIC UNIVERSITY OF KOREA
한국외국어대학교

목차

금융 인증 환경

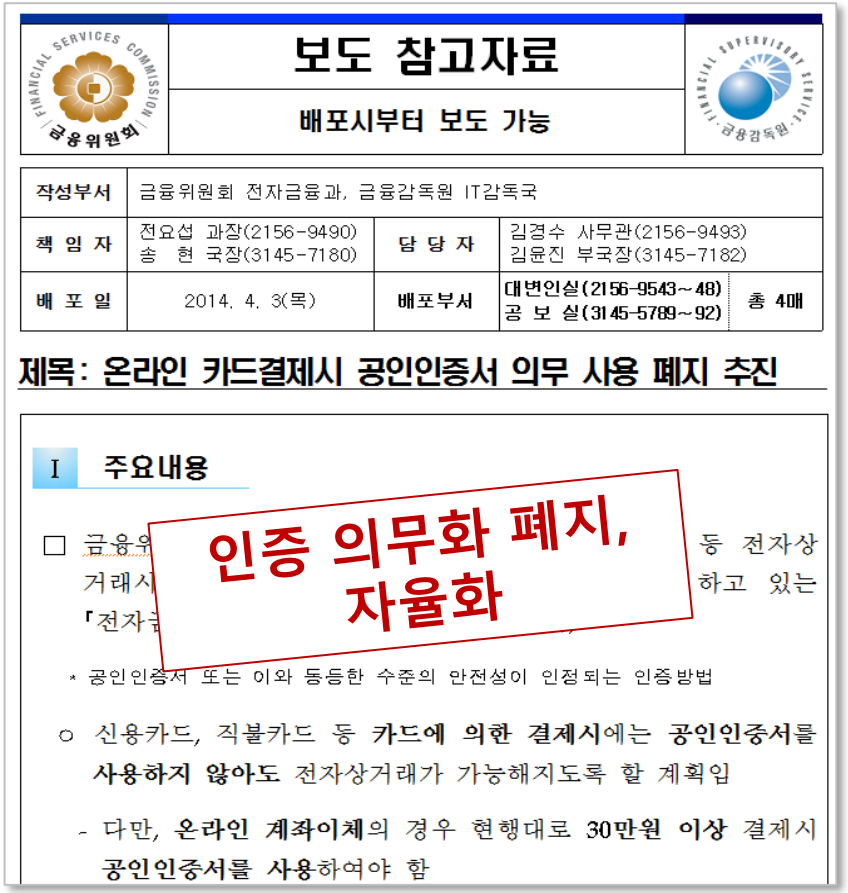
새로운 접근 - OTID

OTID 기술 융합 사례 및 업무

지금까지 금융권의 인증 환경에는 무슨 일이 ?

- 법/규제 변화
- 수단의 전환
- 서비스 주체 변화
- 기술 보안성/안정성

금융 관련 보도 및 트랜드



보도 참고자료

배포시부터 보도 가능

작성부서	금융위원회 전자금융과, 금융감독원 IT감독국			
책 임 자	전요섭 과장(2156-9490) 송 현 국장(3145-7180)	담 당 자	김경수 사무관(2156-9493) 김윤진 부국장(3145-7182)	
배 포 일	2014. 4. 3(목)	배포부서	대변인실(2156-9543~48) 공 보 실(3145-5789~92)	총 4매

제목: 온라인 카드결제시 공인인증서 의무 사용 폐지 추진

Ⅰ 주요내용

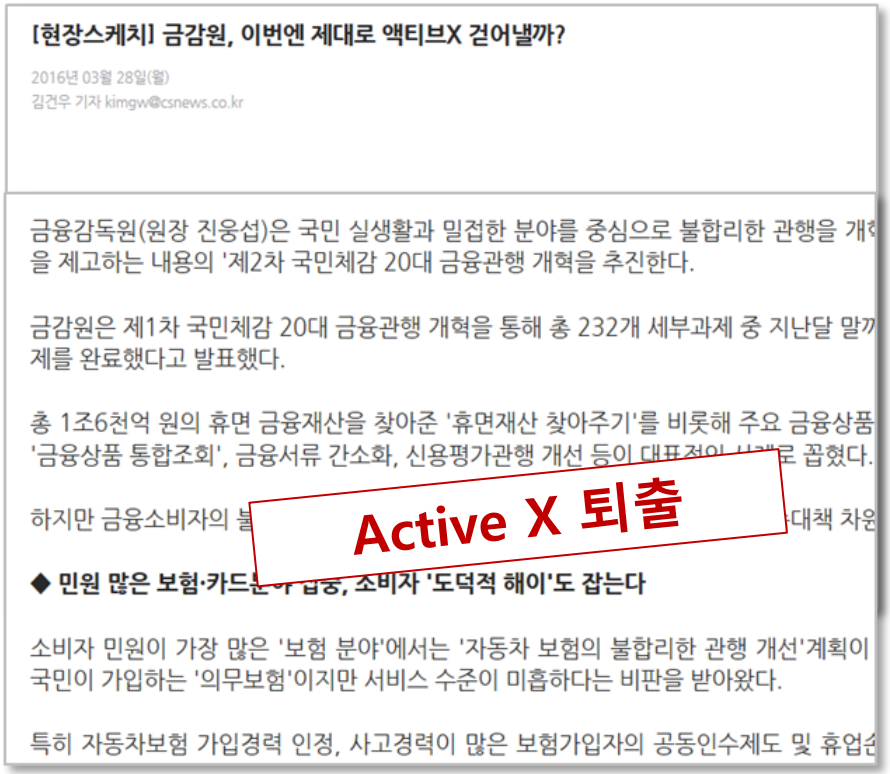
인증 의무화 폐지, 자율화

□ 금융위 … 등 전자상거래시 … 하고 있는 「전자금…

* 공인인증서 또는 이와 동등한 수준의 안전성이 인정되는 인증방법

○ 신용카드, 직불카드 등 **카드에 의한 결제시**에는 **공인인증서**를 **사용하지 않아도** 전자상거래가 가능해지도록 할 계획임

- 다만, **온라인 계좌이체**의 경우 현행대로 **30만원 이상** 결제시 **공인인증서**를 **사용**하여야 함



[현장스케치] 금감원, 이번엔 제대로 액티브X 걷어낼까?

2016년 03월 28일(월)
김건우 기자 kimgw@csnews.co.kr

금융감독원(원장 진웅섭)은 국민 실생활과 밀접한 분야를 중심으로 불합리한 관행을 개… 을 제고하는 내용의 '제2차 국민체감 20대 금융관행 개혁을 추진한다.

금감원은 제1차 국민체감 20대 금융관행 개혁을 통해 총 232개 세부과제 중 지난달 말까… 제를 완료했다고 발표했다.

총 1조6천억 원의 휴면 금융재산을 찾아준 '휴면재산 찾아주기'를 비롯해 주요 금융상품… '금융상품 통합조회', 금융서류 간소화, 신용평가관행 개선 등이 대표적인 …로 꼽혔다.

Active X 퇴출

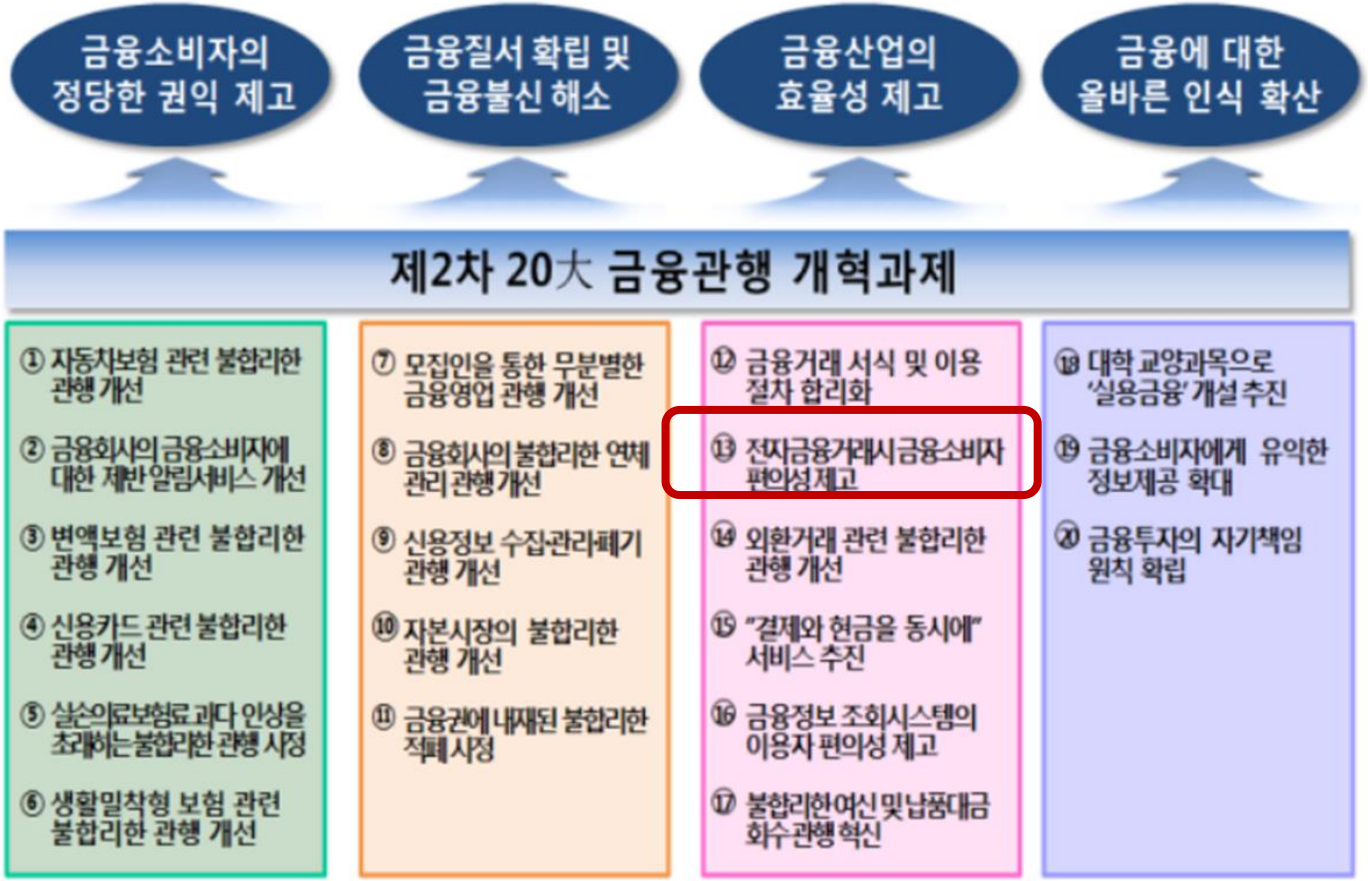
하지만 금융소비자의 불… …대책 차원…

◆ **민원 많은 보험·카드분야 집중, 소비자 '도덕적 해이'도 잡는다**

소비자 민원이 가장 많은 '보험 분야'에서는 '자동차 보험의 불합리한 관행 개선'계획이… 국민이 가입하는 '의무보험'이지만 서비스 수준이 미흡하다는 비판을 받아왔다.

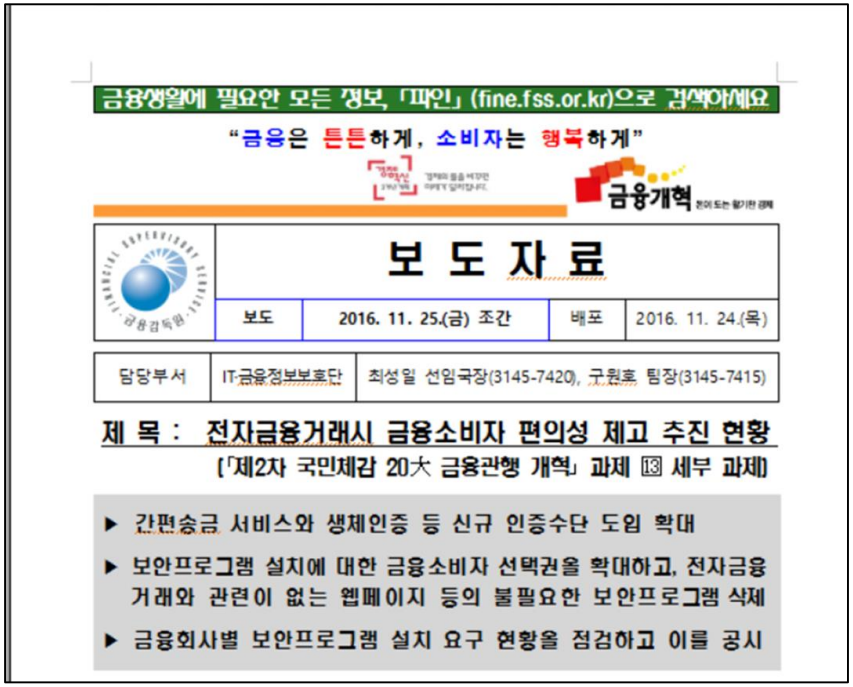
특히 자동차보험 가입경력 인정, 사고경력이 많은 보험가입자의 공동인수제도 및 휴업…

2016. 3월 금융의 선진화와 국민신뢰 제고를 위한 「제2차 국민체감 20大 금융관행개혁」추진계획



참고 : 금융감독원 「제2차 국민체감 20大 금융관행 개혁」추진 계획

➔ 고객의 편의성 향상과 인증 수단의 다양화..



금융생활에 필요한 모든 정보, 「파인」 (fine.fss.or.kr)으로 검색하세요

"금융은 튼튼하게, 소비자는 행복하게"

금융개혁

보 도 자 료

보도	2016. 11. 25.(금) 조간	배포	2016. 11. 24.(목)

담당부서	IT금융정보보호단	최성일 선임국장(3145-7420), 구원호 팀장(3145-7415)

제 목 : 전자금융거래시 금융소비자 편의성 제고 추진 현황
(「제2차 국민체감 20大 금융관행 개혁」 과제 ⑬ 세부 과제)

- 간편송금 서비스와 생체인증 등 신규 인증수단 도입 확대
- 보안프로그램 설치에 대한 금융소비자 선택권을 확대하고, 전자금융 거래와 관련이 없는 웹페이지 등의 불필요한 보안프로그램 삭제
- 금융회사별 보안프로그램 설치 요구 현황을 점검하고 이를 공시

발췌 http://www.fss.or.kr

1. 전자금융 거래 시 다양한 인증수단 활성화

2. 보안프로그램 강제설치 대상 최소화

3. 보안프로그램 설치 선택권 부여

- 금융소비자가 보안프로그램의 설치 여부를 선택할 수 있도록 개선

모바일: 현재와 미래 트랜드에 빠질 수 없는 수단

"2016년 9월 기준 페이스북 한달에 한번 이상 접속하는 사용자는 ?"

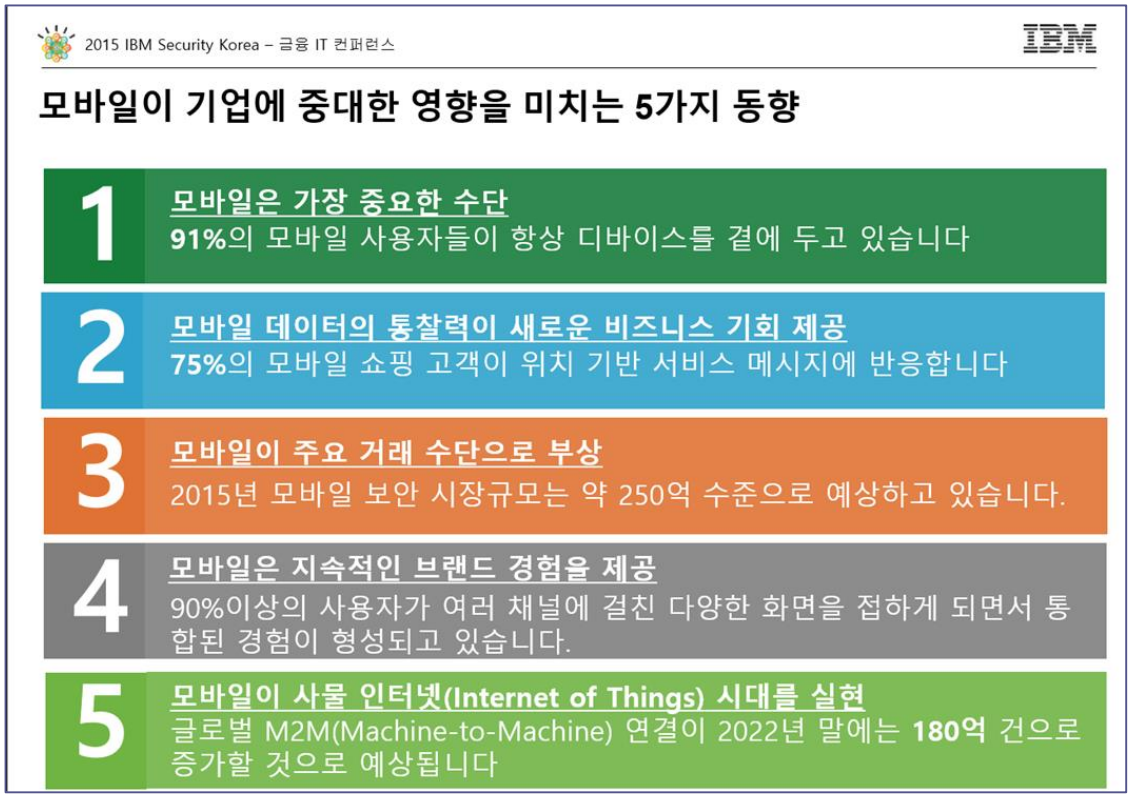
17억 9천만 명

"이 중 한국 접속자는? "

모바일사용자 96% 이상

1천 700 만명

➔ 모바일 수단을 고려하고 있는 기업들



2015 금융 IT 컨퍼런스 IBM Security Korea

모바일은

금융, 교육, 관광, 여행, 주거, 의료, 게임, 영화까지 다양한 산업에 적용되며 일상으로 파고 들고 있다.

모바일과 관련한 사업들이 부상하고 있다. VR, AI..

인간의 곁으로 다가온 기술

- **사용자에게 부담을 주지 않는 방법이 무엇이 있나요?**
- **새로운 프로세스를 만들지 않고 절차에 반영할 수 있나요?**

'2016년 신기술 하이프 사이클 보고서'와 '10대 전략 기술 동향 보고서'

- 순수 몰입 경험
- 증강 인간(augmented human)
- 사물인터넷(Internet of Things, IoT) 플랫폼 등

➔ **인간과 기계의 상호작용이 미래 기술의 지향점**
➔ **기술 중심이 아닌 인간 중심의 기술로 변화**

➔ 인간 중심으로 패러다임으로 혁신하라.

변화에 대한 사례 1)

UI → UX

변화에 대한 사례 2)

MP3

디지털카메라

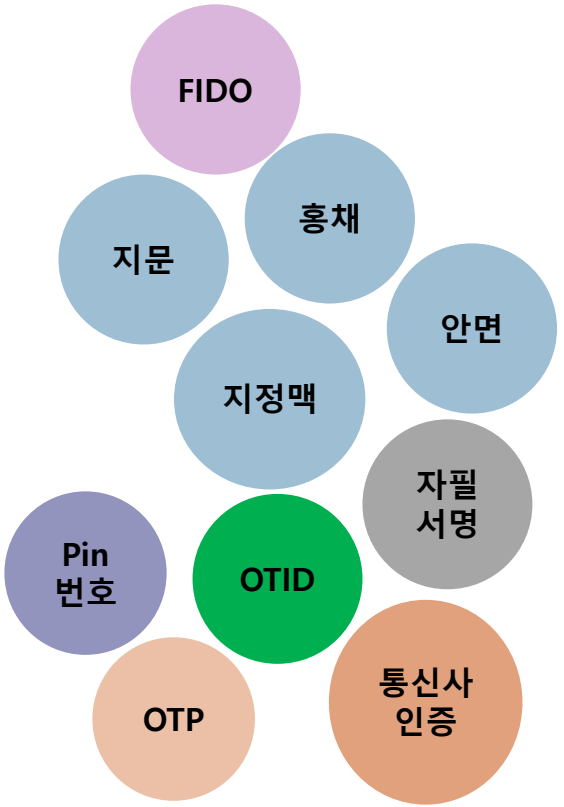
핸드폰

→ 스마트폰

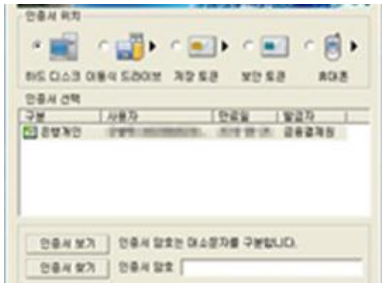
➔보안성 보장은 당연히 기본

- 금보원/금융위/금감원/국정원 등 인증을 받은 솔루션입니까?
- 금융 기관 레퍼런스는 어디입니까?
- 보안성점검 및 모의해킹을 통한 이행점검을 받으셨나요?
- 인증으로 인한 장애 및 사고 시 누가 책임을 지나요?
- 기술 알고리즘으로 증명할 수 있나요?

현재 대두되고 있는 인증기술

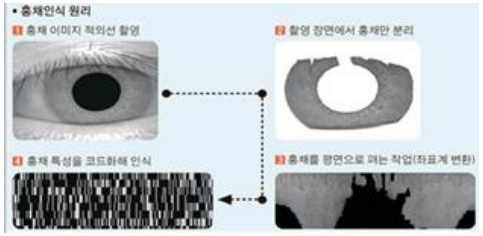


인증 사고의 위험 요소



➔인증하는 요소의 위험 요소

’고정된 ID , 고유한 생체 정보,
고정된 파일 및 코드 등’



목차

금융 인증 환경

새로운 접근 - OTID

OTID 기술 융합 사례 및 업무

사용자 인증 문제의 근본적인 원인

'나'를 제일 처음 인증하는 단계인 '고정된 Code' 로 인해 끊임없는 사용자 인증 문제 발생

ID 로 사용하는 전제조건은?

아이디, ID 란?

사용자가 컴퓨터 시스템이나 통신망에 들어갈 때 입력하게 되어 있는
자기의 고유 이름. 문자·숫자·기호 등의 배열로 이루어진 코드

ID 로 사용하기 위한 조건은?

?

'나'를 제일 처음 인증하는 단계인 '고정된 ID' 로 인해 끊임없는 사용자 인증 문제 발생

OTID

One Time Identity(일회용 ID)

IRUKEY

Identity, Random, Unique Key
나에게만 유일한 OTID로 편리하고 안전하게
사용자를 인증하는 신개념 간편 인증 솔루션

" 사용자 인증, 간편인증, 추가인증
하나로 해결하는 신개념 간편 인증 솔루션"

➔ ID, P/W의 암기/분실, 유출/해킹, 인증비용발생 문제 해결 가능!

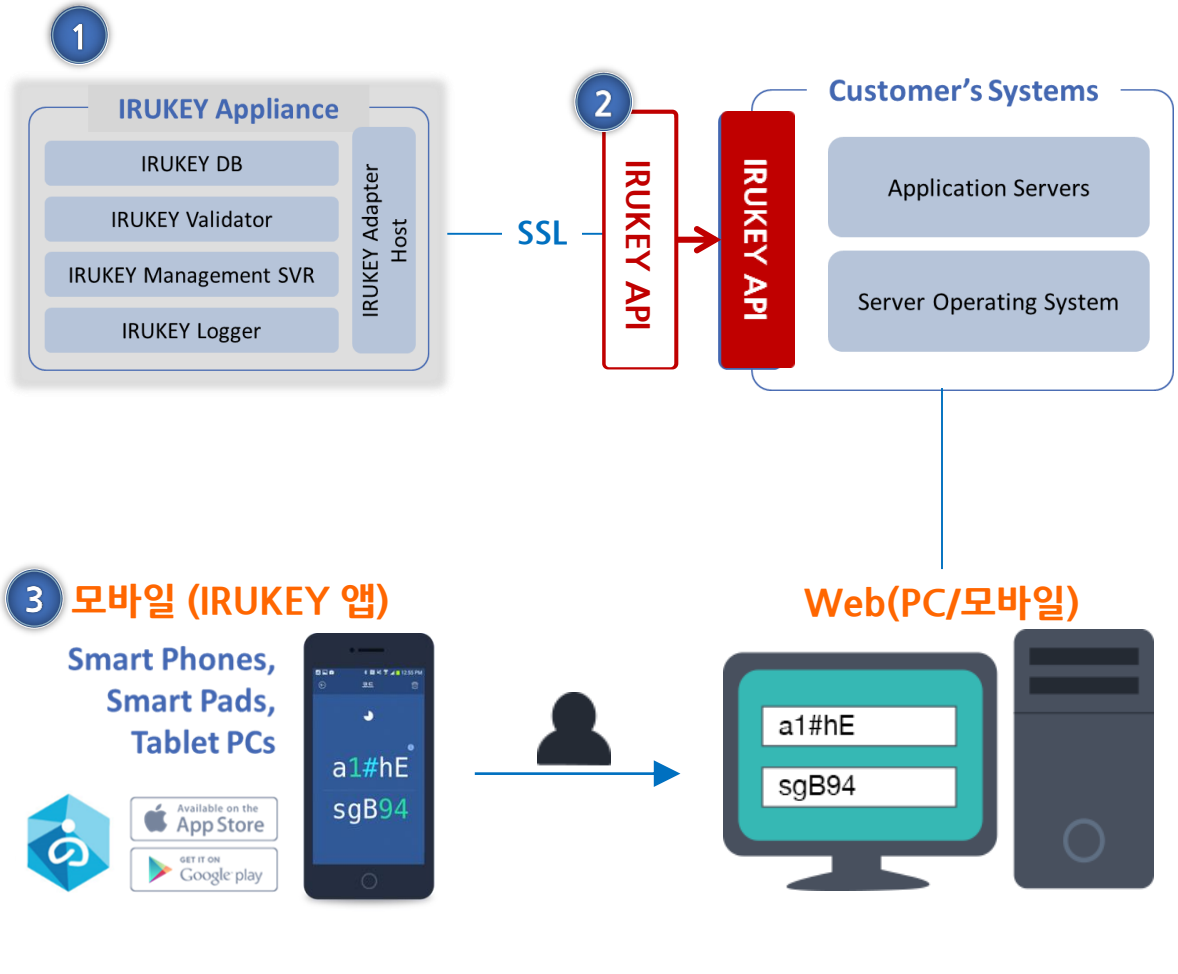
사용자에게 부담을 주지 않는 인증 코드

인증기술 OTID (IRUKEY) 기술 도입 시 검토 사항

편의성 | 경제성 | 보안성 | 호환성

- 보안성이 높은가?
- 사용자를 구분하는가? (사용자별 중복되지 않는다)
- Single Factor , Multi Factor 모두 만족하는가?
- 유출되도 의미가 없는 코드인가? 일회성 코드인가?
- 패턴을 유추할 수 없는 무작위 성 코드인가?
  (문자의 조합 및 자리 수 조정 가능)
- 통신하지 않는 인증하는 방식으로 유출 및 해킹에도 안전
- 생체인증에 의해 실행 될 수 있는가?

OTID 시스템 구성



1 IRUKEY 서버

- 보안성 강화 및 최적화(해킹 대비 등) 일체형 Appliance Server로 제공
- 단일 Appliance에 모든 사용자등록, Random ID발생, 인증 구성요소 등을 포함

2 IRUKEY API

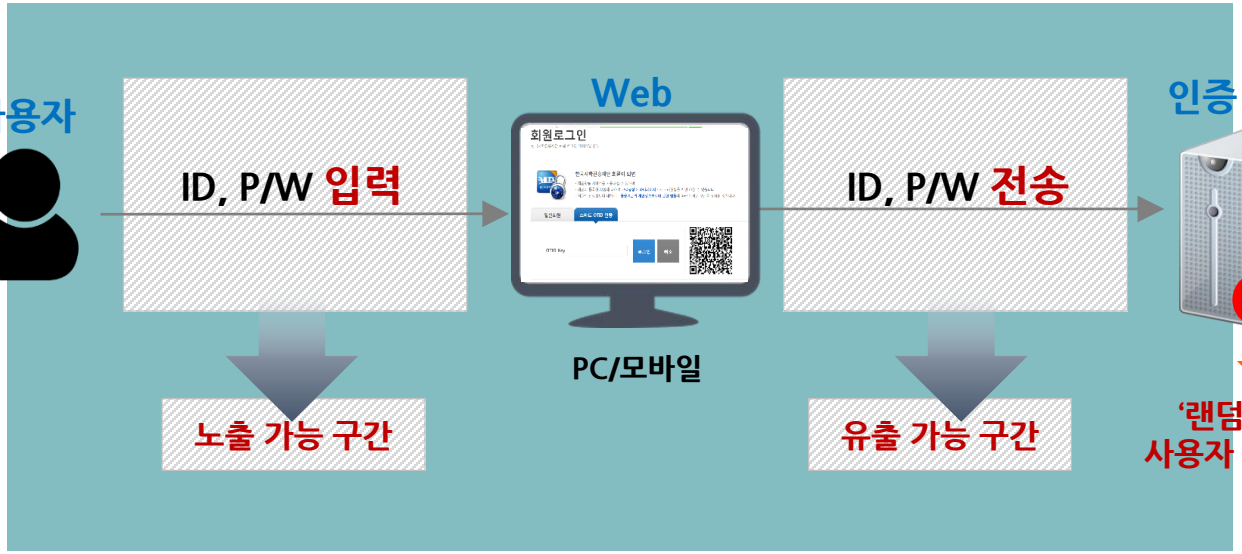
- 제안사가 제공하는 IRUKEY API는 TLS v1.2 로 암호화 통신을 수행함

3 IRUKEY App.

- IRUKEY App.에서 자동생성 되는 일회용 랜덤ID로 사용자에게 인증 서비스 제공
- Android, iOS 제약없이 App Store, Google Play 등을 통해 다운로드 후 설치 가능

새로운 기술 도입으로 인한 내부시스템 수정 영향도?

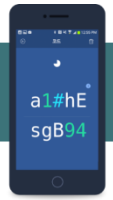
〈 기존 ID 사용 시 **노출** 및 **유출**될 수 있는 구간 〉



ID	P/W	…
Admin	1234	
Gdhong	2345	
Irukey	1234	….
….		

기존 내부 계정 체계

〈 사용 되는 코드〉



OTID - 랜덤 코드 → 기존 ID/PW유지

기존의 ID/PW 체계를 내부적으로 바꾸지 않고 내부 시스템 수정을 최소화합니다.

목차

금융 인증 환경

새로운 접근 - OTID

OTID 기술 융합 사례 및 업무

지금까지의 인증 단계 및 종류

- ID 는 사용자를 구분합니다
- P/W 는 ID 가 셋팅해놓은 정보일 뿐입니다.
- 2factor 인증으로 다양한 수단 및 기술이 발생하고 있습니다.

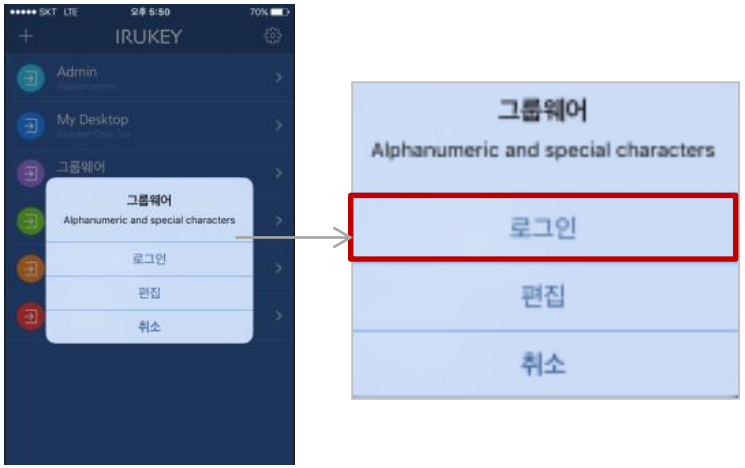
OTID 로 인증을 대체 / 융합할 수 있습니다.

다양한 방식의 사용 방법

보고 입력

스캔

모바일 자동 로그인



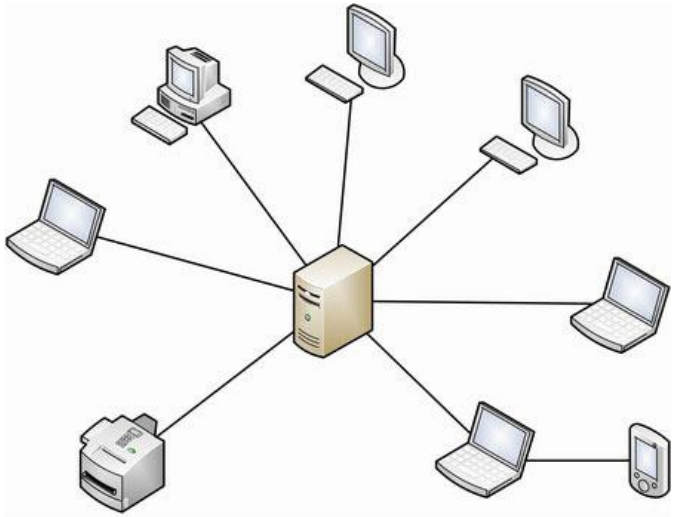
스마트폰 태핑 / 지문 인식

중요 시스템에는

ID 보호 코드를 통과해야만,

ID/PW 를 입력할 수 있다?

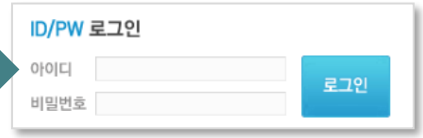
OTID 기술 적용 및 검토 사례 : ID 보호



AS-IS

EASY

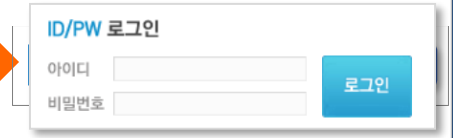
Brute force attack



To-Be

ID Protector

?



*** ID 보호 이슈?**

중요업무 시스템 또는 SSO 접근 시

➔ 보안 취약성을 어떻게 해결할 것인가?

업무 시스템 접근 시

복잡한 접근을 간소화 하되

보안성을 강화 할 수 있다?

OTID 기술 적용 및 검토 사례 : 인증 단계 간소화

업무 시스템 접속 시 ID,PW,공인 인증서로 로그인 하는 형태

AS-IS

ID → PW → 공인인증서

TO-BE

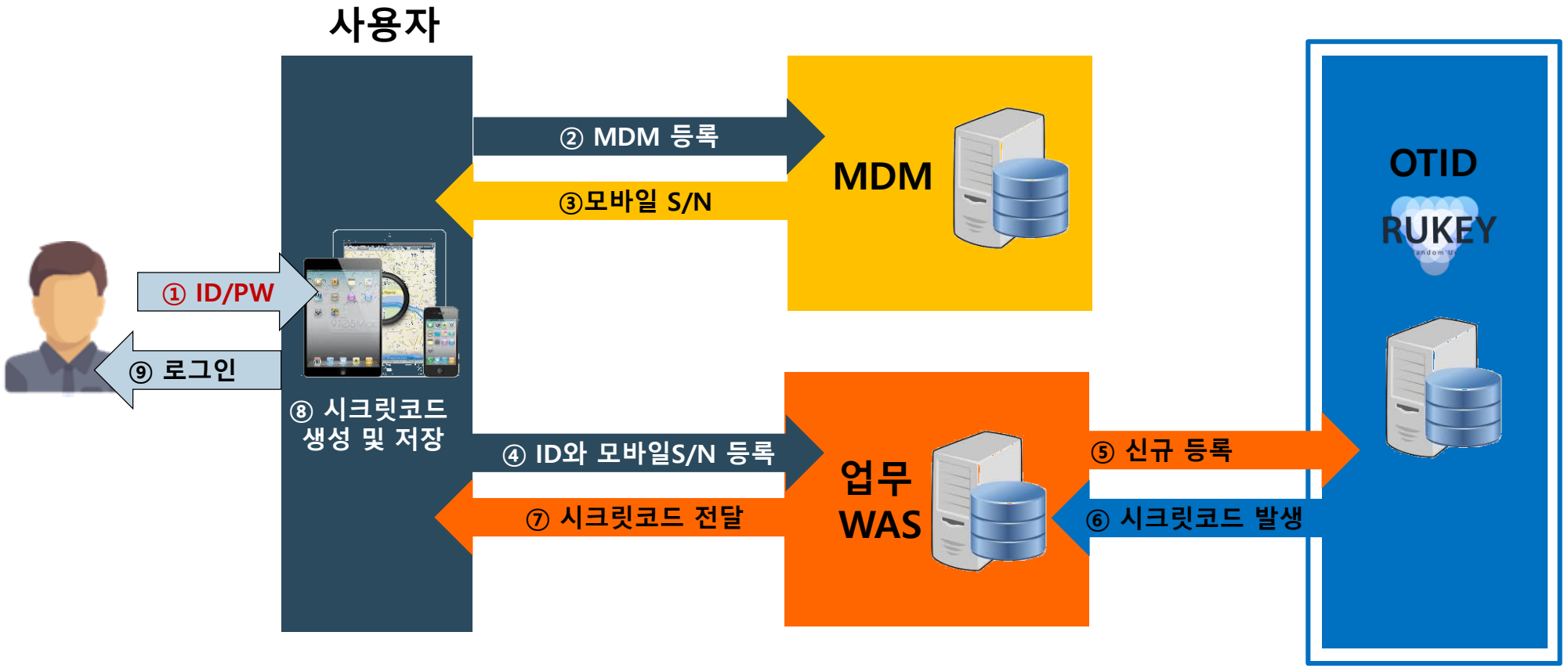
ID → PW → 공인인증서

➔ 사용자는 ID/PW만 입력 , 시스템 상으로는 **Multi Factor 만족**

➔ 사용자에게는 **단계 간소화, 보안성 향상**

OTID 기술 적용 및 검토 사례 : 인증 단계 간소화

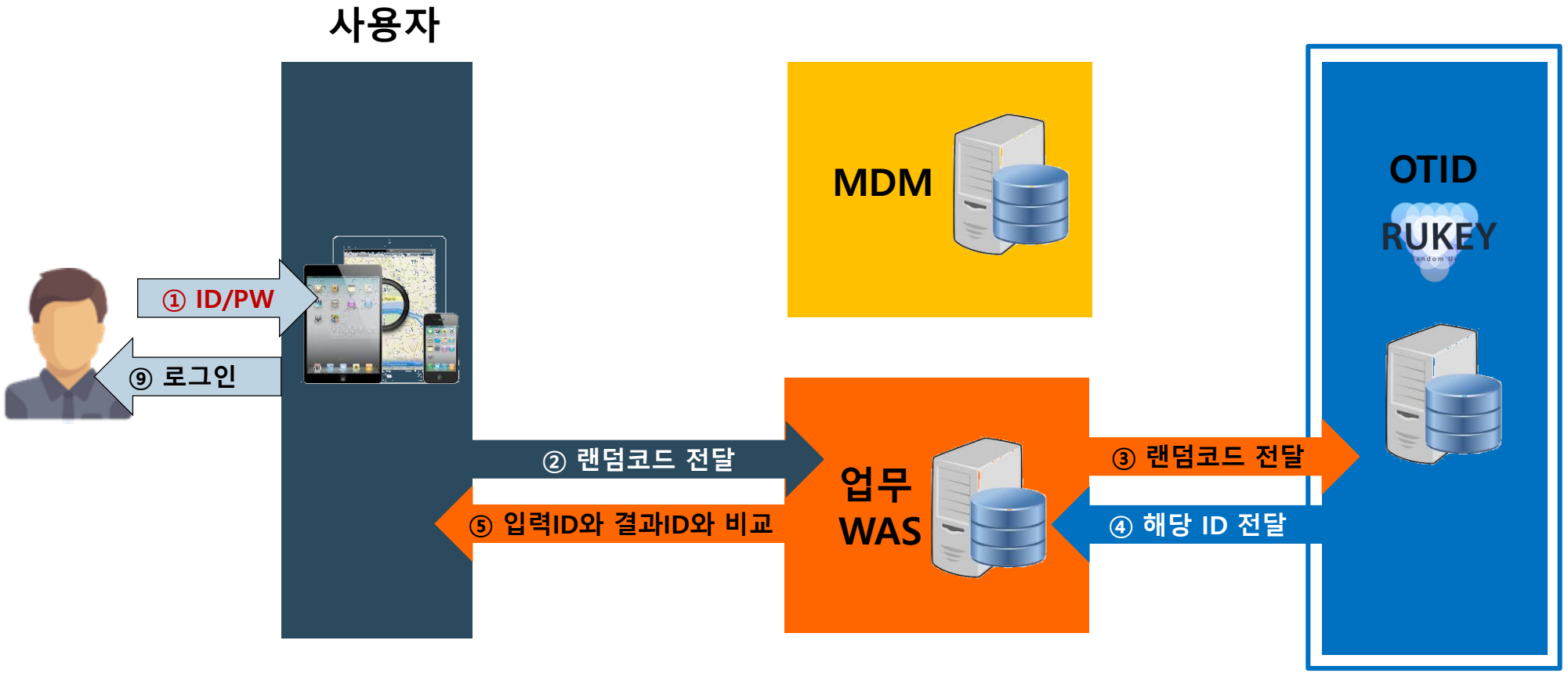
Device 를 통한 인증 시 등록 절차



* Mobile device management

OTID 기술 적용 및 검토 사례 : 인증 단계 간소화

입력은 ID/PW 만, 실제 인증은 OTID 로 추가 인증 효과
기존 공인인증을 통한 2차 인증단계 간소화, 보안 강화

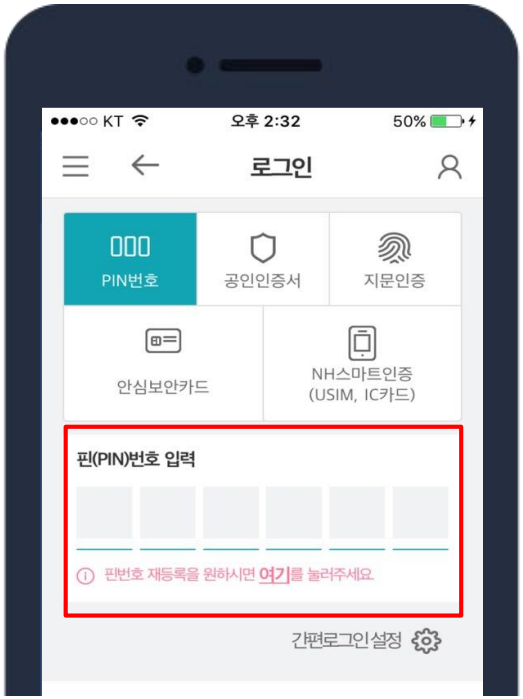


기존의 간편한 인증방식은 유지하면서

보안성은 강화한다?

현재 사용하고 있는 PIN번호 및 숫자 비밀번호 이용 상황

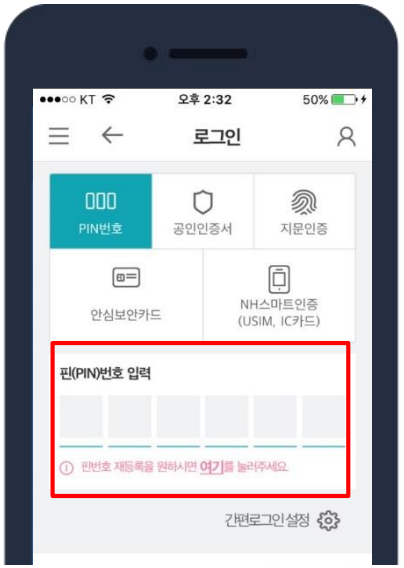
1 인터넷뱅킹 등 이용 시 설정 PIN



2 계좌 비밀번호 4자리

현재 사용하고 있는 PIN번호 및 숫자 비밀번호의 장·단점

1 인터넷뱅킹 등 이용 시 설정 PIN



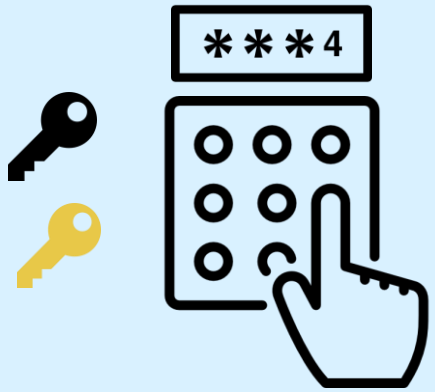
2 계좌 비밀번호 4자리

장점
- 암기하기 쉬움
- 간편한 인증

단점
- 짧은 키 길이
- 고정되어있는 키
- 유추할 수 있는 정보

현재 사용하고 있는 PIN번호 및 숫자 비밀번호의 단점 해결방안

해결방안 ▶ 사용자 측면의 사용법 변화 없이 편의성은 유지하고 보안성은 높인다.



- ✓ PIN 번호 4자리/6자리 입력 방식 같음
- ✓ 인증 절차 같음
- ✓ 간편 인증 유지

어떻게

기존의 간편한 인증방식은 유지하면서

보안성은 강화하지?

OTID 기술 적용 및 검토 사례 : 핀패드

현재 사용하고 있는 PIN번호 및 숫자 비밀번호 OTID적용 시 효과

사용자 측면

- 실제 사용법 및 절차 변화 X
- 간편한 입력과 인증이 가능
- 안심하고 인증 가능

보안성 강화

신뢰도 형성

기업 측면

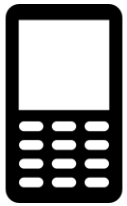
- 핀넘버 혹은 짧은 숫자 비밀번호의 유출 사고 방지
- 기존의 인증 수단 및 절차 변화 X
- 고객의 신뢰 확보
- 보안성 강화

ID 를 공유하지 않고

계정계에서 ID를 발급하지 않고,

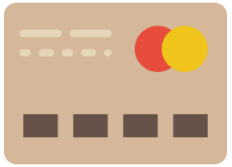
업무 처리가 가능할까?

계정 공유 가 이루어 지고 있는 산업 군의 특성 - 대리점 보유



텔레콤

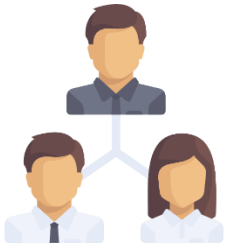
보험



카드/캐피탈

유통

대리점에서 아이디를 공유하며 사용하고 있다.

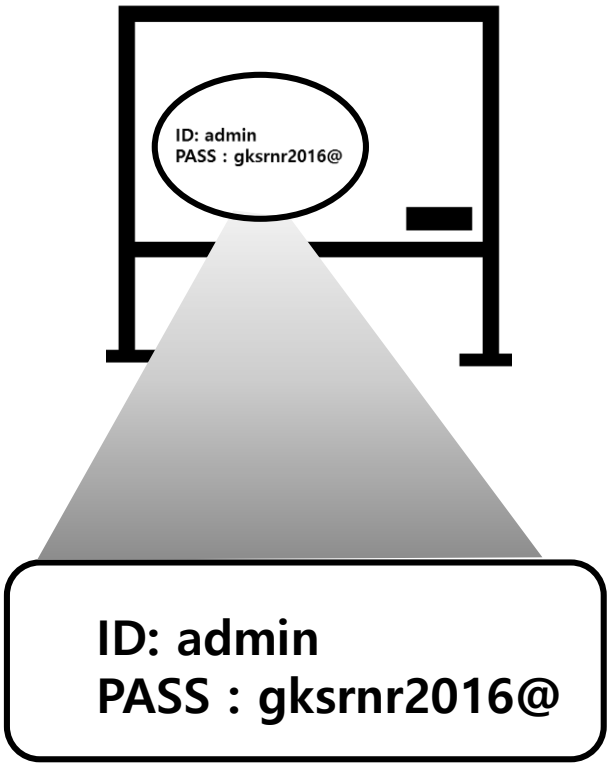


구성원 : 대리점 주, 계약직, 아르바이트생 등등.

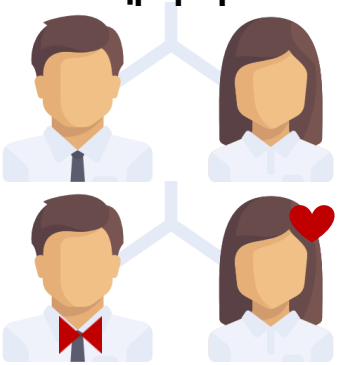
OTID 기술 적용 및 검토 사례 : 가상계정

지금도 대리점/지점에서는 많이 이루어지고 있는 현상입니다.

대리점 주



계약직



ID: admin
PASS : gksrnr2016@

Log in

OTID 기술 적용 및 검토 사례 : 가상계정

가장 명확한 방법 !!!

1)ID/PW 공유하지 않는다.

2)대리점 주가 모든 것을 다한다.

3)Legacy(본사)에서 ID 를 생성해준다.

현실로는 불가능하다.

그렇다면 해결하기 위한 전제 조건?

공유한 ID가 다른 사람에게 전달이 되면 안된다.

대리점 주가 권한을 모두 가지고 있어야 한다.

업무 수행자가 누구인지 구분해야 한다. Why ?

Legacy(본사)에도 계정 발급의 부담을 최소화해야 한다.

OTID 기술 적용 및 검토 사례 : 가상계정

대리점 주

➔ 대리점 주는 ID 공유 없이 역할 부여

- 사용자 이름 : 김루키
- ID : Admin

계약직

➔ 부여 받은 사용자의 구분 하에 ID 공유되지 않은 나만의 코드로 업무 처리 진행

- 4월 1일 오전 9시 00분 접속자
- 4월 1일 오전 11시 10분 접속자
- 4월 1일 오후 9시 25분 접속자

하나의 인증 솔루션으로

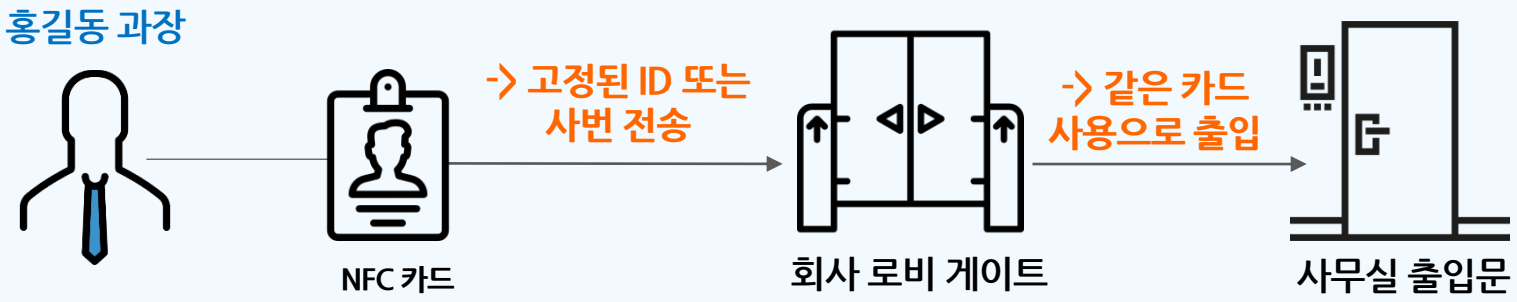
온·오프라인을 연결하고

간편하지만 안전하게 할 수 있을까?

현재 기업의 온라인, 오프라인 인증 절차 상황

1 오프라인 인증

- 출입통제 시 : NFC카드 형태의 사원증 / 방문증을 사용
  - ▶ 고정된 ID / 사번을 전송하여 사용자 인증



2 온라인 인증

- 시스템 로그인 : ID/PW, OTP, 공인인증서 등 다양한 수단을 사용
  - ▶ 고정된 ID / 사번을 전송하여 사용자 인증
  - ▶ 복잡하고 귀찮은 절차

OTID 기술 적용 및 검토 사례 : O2O 연계

현재 기업의 온라인, 오프라인 상황의 문제점 해결방안

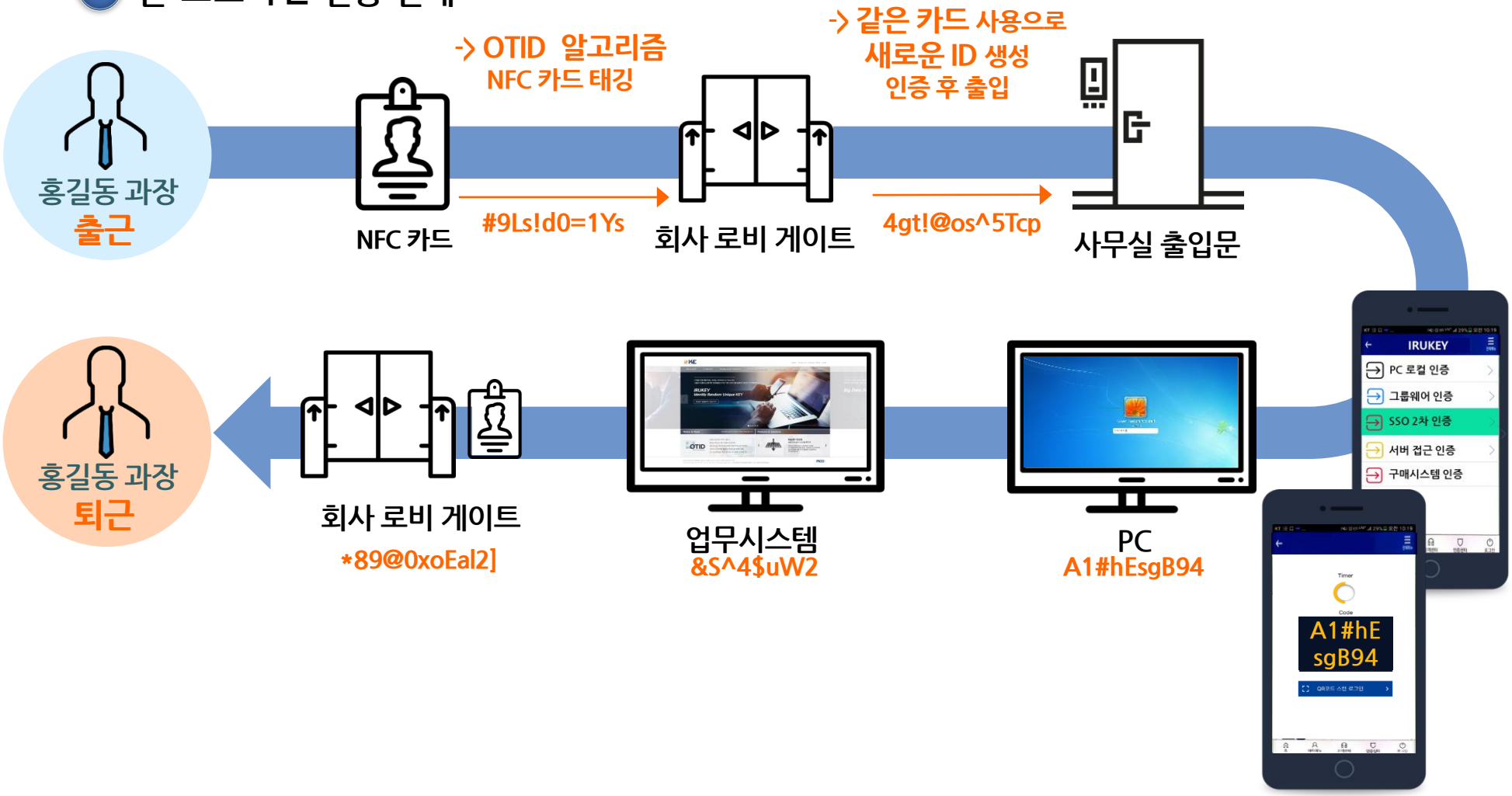
하나의 인증 솔루션으로

온·오프라인을 연결하고

간편하지만 안전하게 할 수 있을까?

현재 기업의 온라인, 오프라인 상황의 OTID 적용 시 모습

1 온·오프라인 인증 연계



다형성을 지닌 인증 기술과 정책의 조합으로 고객을 위한 서비스가 만들어 집니다.

1. 어떤 기술을 적용하느냐가 아니라, 어떤 서비스를 제공하느냐 입니다.
2. 기술의 안정성 검토는 기본이고, 내부의 보안 기준과 정책의 조합입니다.
3. 상식이란 틀을 벗어난 인식의 변화만으로 혁신이 될 수 있습니다.
4. 기술 하나로 모든 것을 해결해주지는 않습니다.
   융합으로 고객에게 신뢰를 더 할 수 있습니다.

Thank You

유 인 지 | Yoo, In Ji | Korea Expert Inc

전략사업팀 | 팀장
Strategic Business TM | Manager
M. 010-3379-083 | **E.**@ijyoo@kei.co.kr