

More Safe, More Convenient way to authentication  
더 안전하고, 더 편리한 인증을 위한 보안 솔루션

# 스마트 인증 솔루션

## “Auth ME ”



## 1. 시장 환경

- 1.1 금융 인증 매체 현황
- 1.2 인터넷 서비스 인증 현황
- 1.3 시장 환경의 요구

### ※ 별첨

- 특허 출원 현황
- 시스템 지원 사양

## 2. 패키지 솔루션 소개

- 2.1 서비스 개요 및 목표
- 2.2 서비스 소개
- 2.3 서비스 기술 우수성
- 2.4 서비스 적용 방안
- 2.5 서비스 도입 분야
- 2.6 서비스 기대효과

## 3. 솔루션 도입 방안

- 3.1 세부 구축 방안
- 3.2 도입 기업의 기대효과



# 1. 시장 환경



- 해킹 취약점, 사용자 부주의, 높은 H/W 보급비용, 높은 O&M 비용 등의 단점
- **소프트웨어 보안상의 약점 내재, 근원적 대체수단 필요**

## 공인 인증서 인증

고정형 사용자 비밀번호 사용으로 인한 **비밀 번호 탈취 우려**

- . PC 악성코드 취약
- . 입력패턴 추출 위험



이슈 **1**

## 보안 카드 인증

보안카드를 복사, 촬영하여 **여러 곳에서 사용, 누출 위험**

- . 보안 카드 사본 유출
- . 보안카드 오남용



이슈 **2**

## 하드웨어OTP 인증

은행의 비용 증가, 사용자 부담으로 인한 **활성화 부진**

- . 은행 보급부담 한계
- . 고객 비용 부담저항
- . 보급 지연, 휴대불편



이슈 **3**

## 소프트웨어 인증

소프트웨어 OTP, SMS 인증 등의 방안시도, **활성화 지연**

- . 높은 운영유지비용
- SMS 비용(5억원/년↑)
- . 시간기반 OTP 취약점
- 승인번호 탈취 가능
- . USIM형 OTP 미 활성화
- 통신사-사업자간 이해관계

이슈 **4**



## 카드

### FACT FILE

- There are 2.8million fraudulent card transactions a year, costing the UK £610million
- More than three quarters of frauds involve internet, telephone or mail order shopping where there is no protection from pin codes
- More than seven per cent of card owners who shopped on the internet fell victim to fraud last year, compared to two per cent on the high street
- A quarter of those who fall victim to card fraudsters lose £200 or more
- Fraud by criminals getting into online bank accounts was put at £59.7million last year, a rise of 14 per cent on 2008

- 연간 280만건 사기성 카드거래
- 인터넷 쇼핑자의 7% 이상이 인터넷 사기의 피해자
- 카드도용 범죄 피해 금액이 연간 약 4천931억원 규모
- 비자 코드슈어 카드는 인터넷 등에서 결제하려면 카드 스크린에 1회용 암호가 나타나 이를 입력해야 결제가능

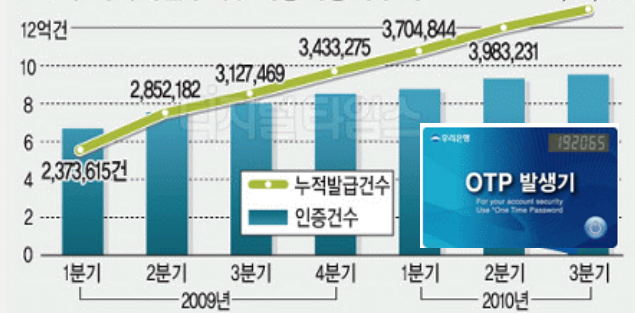


일반 신용카드와 크기와 재질은 똑같으나 OTP 출력이 가능한  
비자 코드슈어(CodeSure) 카드 유럽에서 론칭

## 은행

- 은행권(우리은행 등) Open-Banking 서비스의 핵심으로 OTP 솔루션 부각
- OTP 이용자 수 542만명(2011. 3분기)
- 은행권 OTP 무료발급 행사 등을 통해 이용자수 증가 예상
- 우리은행/농협 등은 카드형태의 OTP 장치를 발급함에 따라, 사용자의 휴대 불편 해소
- **스마트 폰 등에 모바일 OTP 탑재 시, 확장성과 휴대성 증대 예상**

OTP누적거래건수 및 이용자증가추이



인터넷 상거래 폭증에 따른 ISP 결제 시장의 비약적 성장에도 불구하고  
**결제 불편, 보안취약성 불안, 개인정보 유출 등 제반 문제 증가**

### 인터넷 결제 서비스 환경

- 스마트폰형 모바일 결제 솔루션 부재  
(종래 공인인증서 기반 모바일 결제 이용 상의 불편함 지속)
- 기존 온라인 안심클릭 방식의 경우, 사용자 입력 항목이 많아 **불편함 초래**
- 해킹 등을 통해 **온라인/모바일 신용카드 번호 유출 우려 등 상존**



### 인터넷 인증 서비스 환경

- ID 기반 고정 패스워드 인증 방식으로 **개인 정보 유출 가능성**
- 온라인 게임 등 현금성 온라인 자산 피해 규모 증가
- 네이트 **개인 정보 유출 사고** 발생
- 리니지, 메이플 스토리 등 게임 사이트 개인 **아이템 유출 사고** 발생 등



“ 기존 결제/인증 방식으로 인한 **문제점 지속 발생 !!** ”

## 기존 인증 방식의 경제성, 보안성 이슈를 해결할 대체 인증 수단 필요

구분	하드웨어 OTP	모바일 OTP	고정 비밀번호/보안카드	SMS 인증
Key 생성	고정 키 방식으로 공장 출시 생성	OTP 서버 시간 기반 자동 생성	고정 키 방식으로 사용자 입력 시 자동 생성	없음
Serial Key 저장 방식	하드웨어 펌웨어 (사용자 복제 불가)	평문 저장 및 평문 전송으로 고의적 복사 가능	MD5 기반 알고리즘 적용이지만 고정 키이므로 복제 가능	없음
인증 방식	데이터베이스 저장 방식	데이터베이스 저장 방식	데이터베이스 저장 방식	인증 비밀번호 랜덤 생성 후 동적 입력
번호 추출방식	Time 방식(32Bit)	Time 방식(32bit)	해당사항 없음	랜덤 방식 (기본 알고리즘은 D5)
OTP 비밀번호	없음	없음	해당사항 없음	없음
이용기관	은행 고액 이체(분리매체 인증)	소액결제, 마일리지 결제, 기업 사내 임직원 인증 등	인터넷 서비스 인증 가입자 인증 등 대다수	ISP 결제 인증
보안성 심의	금융 인증 매체로 보안성 심의 대상 (공급자가 심의완료 후 공급)	금융 인증 매체가 아니므로 해당사항 없음	레코드 암호화 여부만 심의 대상임	금융 인증 매체가 아니므로 해당 사항 없음
장점	분리매체 인증(보안등급 높음) 분실 시 거래 노출 문제점 없음	모바일 단말/PC환경에서 쉽고 편리함	도입 비용 없음 가장 저렴하고 일반적인 인증 수단	비밀번호의 가변성을 통한 인증으로 탈취 위협 없음
단점	보관하기 어려움 (카드방식은 고가임)	보안성이 낮음 (기밀성/무결성/가용성 부족)	고정 비밀번호의 단점으로 쉽게 탈취 가능	건당 7~11원 비용발생 (연간 5억 이상)
특징	금융거래법 상 인증, 높은 보안등급 은행 거래 이체 시 활용도가 높음 구매비용 증가, 시장 활성화 저해 보관/이동성 불편으로 활성화 저해	쉽고 편리한 장점으로 활용도 높음 저가 솔루션으로 도입비용 절감	DB 암호화만 적용한 기술 보안성 수준이 가장 낮음 해킹, 탈취 위협이 가장 높은 특징	지속적인 비용 발생으로 인한 서비스 사업자의 부담 증가

편리성과 보안성의 모두 보장하는 스마트 폰 인증 솔루션으로 혁신,  
더 편리하면서도 더 안전한 **OTP 인증 서비스 제공**

#### 기존 인증 수단별 특징, 문제점

- **하드웨어 OTP - 구매부담 증가**
  - 기업 대상/개인별 이체 한도 기준 초과 고객대상 하드웨어 OTP 장려금 비용 증가하고 있음.
- **개인용 보안카드 - 보안/노출 위험 수위 증가**
  - PC에 보안카드 파일 생성 및 저장하는 사용자 증가
  - 개인 PC해킹에 따른 위험 노출
  - 항상 소지 해야 하는 불편함으로 개인 고객 편리성 결여
- **모바일 banking/결제 - 편리성 부족**
  - PIN인증, 보안카드/OTP 인증을 위해 별도 매체 소지 불편
  - VM뱅킹, 스마트 banking 이용자 불편함 증가
  - 서비스 편리성 부족으로 모바일 banking 사용저변 확대 지연
- **인터넷 서비스 - 보안/탈취 위험 수위 증가**
  - 고정 패스워드, PIN인증 등 다양한 인증 방식 도입
  - 각종 보안 사고 빈발, 위협 수위 심각
  - 개인정보 유출 사고가 지속적으로 발생

“새로운  
인증 수단”



#### 신 인증 매체 필요

- Two - Factor 인증 요건 해소
  - 법제, 수용환경 변화
  - 안정적인 인증 수단 필요
- 보안성 높은 인증 매체
  - 고정 패스워드 체계 고도화
- 편리한 인증 매체
  - 간편하고 저렴한 인증 수단
  - 사용자 편의성이 높은 인증 매체 필요





## 인증 매체의 근본적 환경변화

#### 저렴한 인증 기술

- 하드웨어 OTP를 대체할 수 있는 보안성 높은 인증 기술
- SMS 인증을 위한 연간 비용을 대체할 수 있는 인증 기술

#### 보안성 높은 인증 기술

- 탈취, 복제, 추적이 절대적으로 불가능한 인증 기술
- 무결성과 기밀성을 지원하는 인증 기술

#### 편리한 인증 기술

- 개인정보 유출 방지를 위한 개인 인증 기술
- 서비스 단계별 편리성을 지원하는 인증 기술
- 간편 인증을 통해서 보다 더 안정적으로 인증할 수 있는 기술

101011010101010

## 2. 패키지 솔루션 소개



신 인증 솔루션을 통한 **인증의 편리성, 경제성, 보안성 보장**

## 스마트폰 사용자를 위한 신 개념 인증 서비스 제공

1. 1인, 1스마트폰, 1인증 어플리케이션 멀티 인증 매체 등록 서비스 제공
2. 개인 사용자 기밀성 보장 : 1인, 1스마트폰, 1어플리케이션만 사용 가능
3. 데이터 무결성 보장 : 단말에 인증 번호 생성 안됨, 네트워크 Seed Value에 의한 가변 승인 번호 생성



1. 네트워크 Seed Value 승인 번호 서비스
2. QR 코드 인증 승인 번호 서비스
3. 보안카드 인증 승인 번호 서비스

**도입 고객의 3가지 다중 인증 선택 지원**

인증 시 개인정보를 노출하지 않고 스마트폰 인증 어플리케이션을 사용함으로써,  
**사용자 편리성 확보와 함께 높은 보안성을 제공**

### 1 사전/앱 등록

#### ① 사전 등록

사용자는 도입 고객의 Auth Me 서버로부터 사전 등록 시행  
(등록 정보 : 사용자 ID 자동 생성, 단말 고유 정보 등록)

#### ② 사용자 인증 어플리케이션 자동 다운로드

#### ③ 인증 어플리케이션 첫 실행 시에 1회성 승인 번호 입력

#### ④ 1인 = 1 단말 = 1 어플리케이션 정상 등록

### 2 인증 대상 등록

#### “멀티 인증 대상 등록”

결제 카드  
등록 후 사용

인증 ID  
등록 후 사용

결제 계좌  
등록 후 사용

### 3 인증 진행

#### ● 인증 A.

단말에서 인증 번호 요청 -> 사용자 ID, 어플ID, 네트워크 ID, 단말 ID 자동 인증 후 인증 번호 수령

#### ● 인증 B.

단말에서 인증 번호 요청 -> QR코드 추출 및 인증, 사용자 ID, 어플ID, 네트워크 ID, 단말 ID 자동 인증 후 인증 번호 수령

#### ● 인증 C.

단말에서 인증 번호 요청 -> 보안카드 번호 입력, QR코드 추출 및 인증, 사용자 ID, 어플ID, 네트워크 ID, 단말 ID 자동 인증 후 인증 번호 수령

### 1 스마트폰 사용자의 무결성 등록 후 사용

- 스마트 폰 USIM 정보, 단말 Serial 정보, 전화번호 등록



### 2 인증 번호의 무결성, 기밀성 보장

- 인증 어플리케이션에서 네트워크, 위치, 단말 고유 ID 자동추출을 통한 1회성 고유의 네트워크 Seed 값 생성
- 단말에 승인 번호 생성 또는 저장이 없으므로 무결성, 기밀성 보장



### 3 탈취, 복제 위험 방지

- 1인 스마트폰 단말 등록 후 사용정책으로 인한 복제 불가능
- 네트워크 기반 Seed Value 생성을 통한 승인번호 탈취, 복제 불가능
- 생성 알고리즘의 복잡성
  - . MD5 알고리즘+네트워크 Key 암호화 알고리즘 + 일반 Hash 알고리즘
  - . 복합 알고리즘으로 패턴 추출 불가능



사용자 인증 번호, 개인정보는 도입 고객사 외  
통신망(쇼핑몰/PG포함)상에서 **절대 유출 불가**

### 1단계 - 사용자 서비스 등록 단계

- 1) 사용자 인증 사전 등록 시, 단말기 고유 정보와 사용자를 1:1로 인증하여 고유의 인증ID를 자동 생성 및 등록
- 2) 어플리케이션 다운로드 후 1회성 사용 승인 번호 인증 후 사용자의 기밀성 보장
- 3) 사용자 인증 대상을 선택(카드정보, 계좌정보, 인증 ID정보)하여 등록한 후 기간계와 연동 완료 후 사용

### 2단계 - 승인/인증 요청 단계

- 1) 인증/결제 승인 서비스에서 “Auth ME 인증” 선택 시, 인증 요청 인증 주체(도입 고객)시스템에 전송
  - 2) 사전 등록된 스마트폰에 서버에서 생성된 1회성 네트워크 Seed Value 가 일정 시간 동안 출력
  - 3) 인증/승인 화면에서 스마트폰에 출력된 인증 번호 입력 후 인증, 승인 요청
- \* QR코드, 보안카드 인증 대상은 상기 절차에 추가적으로 QR코드 자동 인식, 보안카드 번호 입력 절차필요

### 3단계 - 승인/인증 처리 단계

- 1) 도입 고객사 서비스 시스템에서 Auth ME 관리 서버와 연동하여 사용자 ID 조회 후 승인/인증 번호 인증 후 사용자 ID에 대응하는 인증 대상 확인(승인 카드번호, 인증 ID 등)
- 2) 사용자 인증 대상의 무결성, 기밀성을 확인 후 승인/ 인증 여부 응답 처리

전 세계 최초로 네트워크 기반 Seed Value 알고리즘 개발 적용  
**해킹, 탈취 위협 불가능 알고리즘 개발**

#### Integrated Application

- Access Data Monitoring
- GUI Library
- I/O Library
- Seed Data Management
- User Data Management
- Application Version Mgmt

#### Auth ME Library

- GUI Library
- Data I/O Library
- Data Management
- Security Library

#### Serial Registration

- 사용자 암호 설정
- 사용자 고유 관리
- ESN/UICC ID/MDN
- 사용자 인증 프로세스

#### Seed Creator

- Seed Key Parser
- Memory Management
- Seed Data Manager
- Message/API/Data Hooking Mgmt

#### Auth ME I/O

- Data I/O
- Traffic Flag Process
- Traffic Analysis

#### Security

- Data Encryption
- Data Decryption
- Message Parser
- Verification

#### Data Management

- Local Data Monitoring
- Data Access Management
- Buffer Cache Management

#### Auth ME Server

S/N Management



Seed Value Creator

Authentication

Registration

Serial Number

Seed Value

- 
**인증 코드 인덱스 정보의 암호화 및 입력단계에서의 입력자를 통한 유출 방지**  
 → 기존 Off-Line OTP 대비, 인증코드 인덱스 정보 보안성 강화  
 → 스마트 폰 프로그램의 해킹을 통한 인증코드 인덱스 정보 보안 강화
- 
**하드웨어 변경 감지 및 어플리케이션 위.변조 시 기존 정보 초기화를 통한 보안성 강화**  
 → 스마트 폰 변경에 대비하여 기존 정보 초기화  
 → 악의적, 고의적 해킹을 방지하기 위한 알고리즘으로 보안성 강화 (기존 정보 초기화 및 신규 발급 유도)
- 
**네트워크 정보 기반의 오차범위 내의 이동 거리 추출 알고리즘 적용**  
 → 패턴 추출 탈취 및 기밀성, 무결성 보안 강화  
 → 단말 해킹 위협과 승인번호 탈취 위협 해소

단 계	과 정	보안 강화 방안	비 고
발급단계	인덱스 정보 암호화 (단말 고유정보, 어플리케이션, 사용자 정보 일치 등록)	암호화 모듈/ 네트워크 Seed	보안 향상
통신단계	전반적인 공통 단계로 SSL 보안 통신 방식	보안 통신(보안모듈)	기존과 동일
사용단계	자체 네트워크 Seed 추출 알고리즘 단말/사용자 변경 추출 알고리즘	보안 이중화	보안 향상
감시단계	온라인 환경에서의 환경적 보안을 강화	위치정보/위치시간 알고리즘	보안 향상



“ 보안강화를 목적으로 한 상기 내용의  
**전 방위 보강 특허 출원 완료** ”



Single Application 구조와 도입 고객의 서비스 Application에 활용될 Library 구조로 이원화 구현

#### 구동환경

- 3G/WIFI/Wibro 등 모든 네트워크 환경에 적합한 Standard Local Application 구동
- 웹 서비스와 연동하기 위한 API 기반 연동 인터페이스 제공
- 서비스 화면에서 QR코드 자동 생성 제공 및 QR 자동 인식 기능 제공

#### Application 구조

- Seed Value를 생성/저장하지 않고 Auth Me 전용 Dummy Terminal 구조
- 1회성 Seed Value를 인증하는 Dummy Process 구조

#### 지원 스마트 폰



iOS(iPhone)

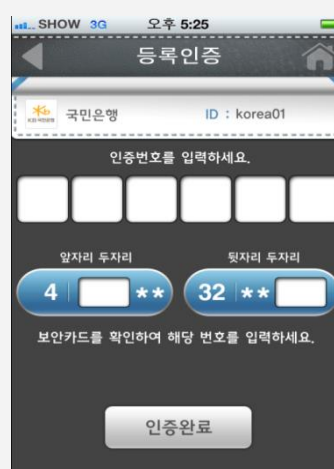
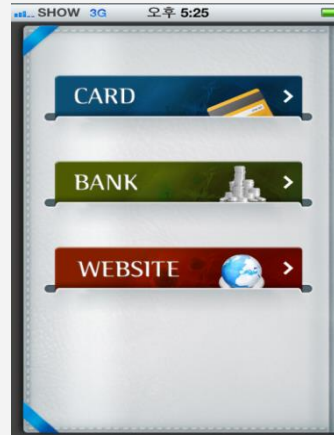


Android

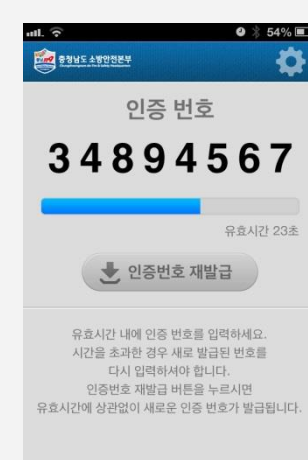
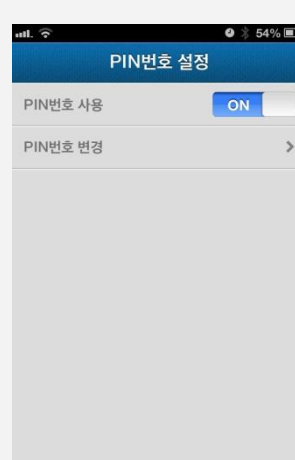
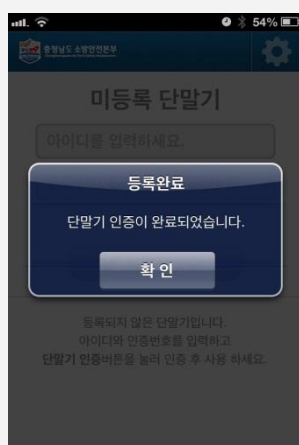
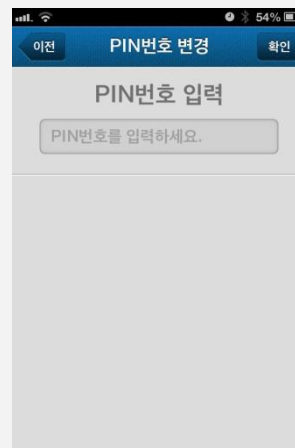
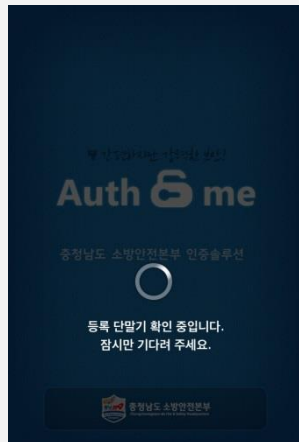
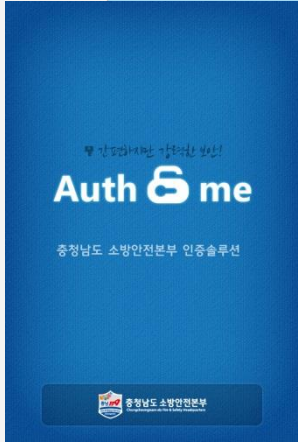


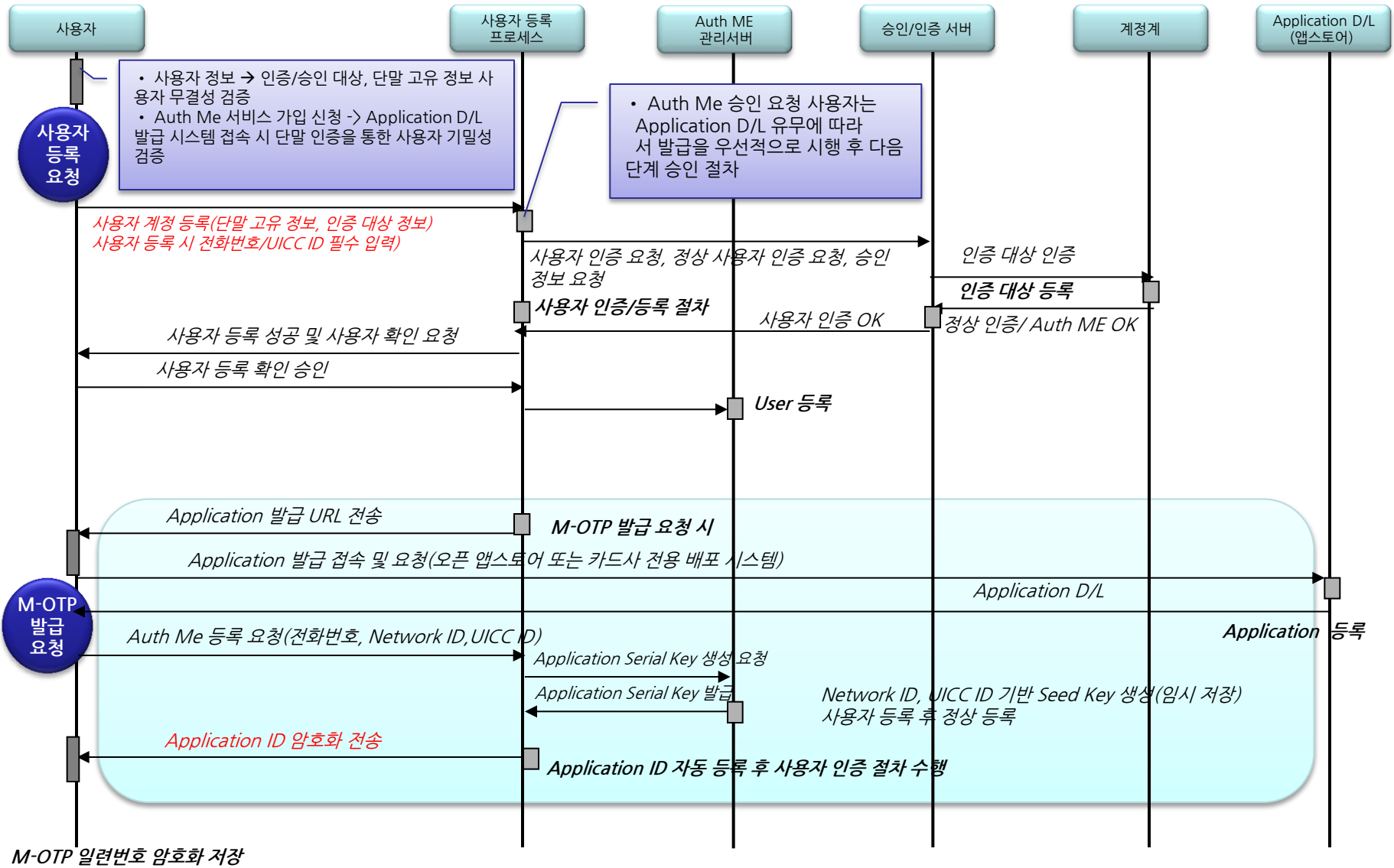
\* 향후 출시되는 모든 스마트폰 OS 를 지원할 예정입니다.

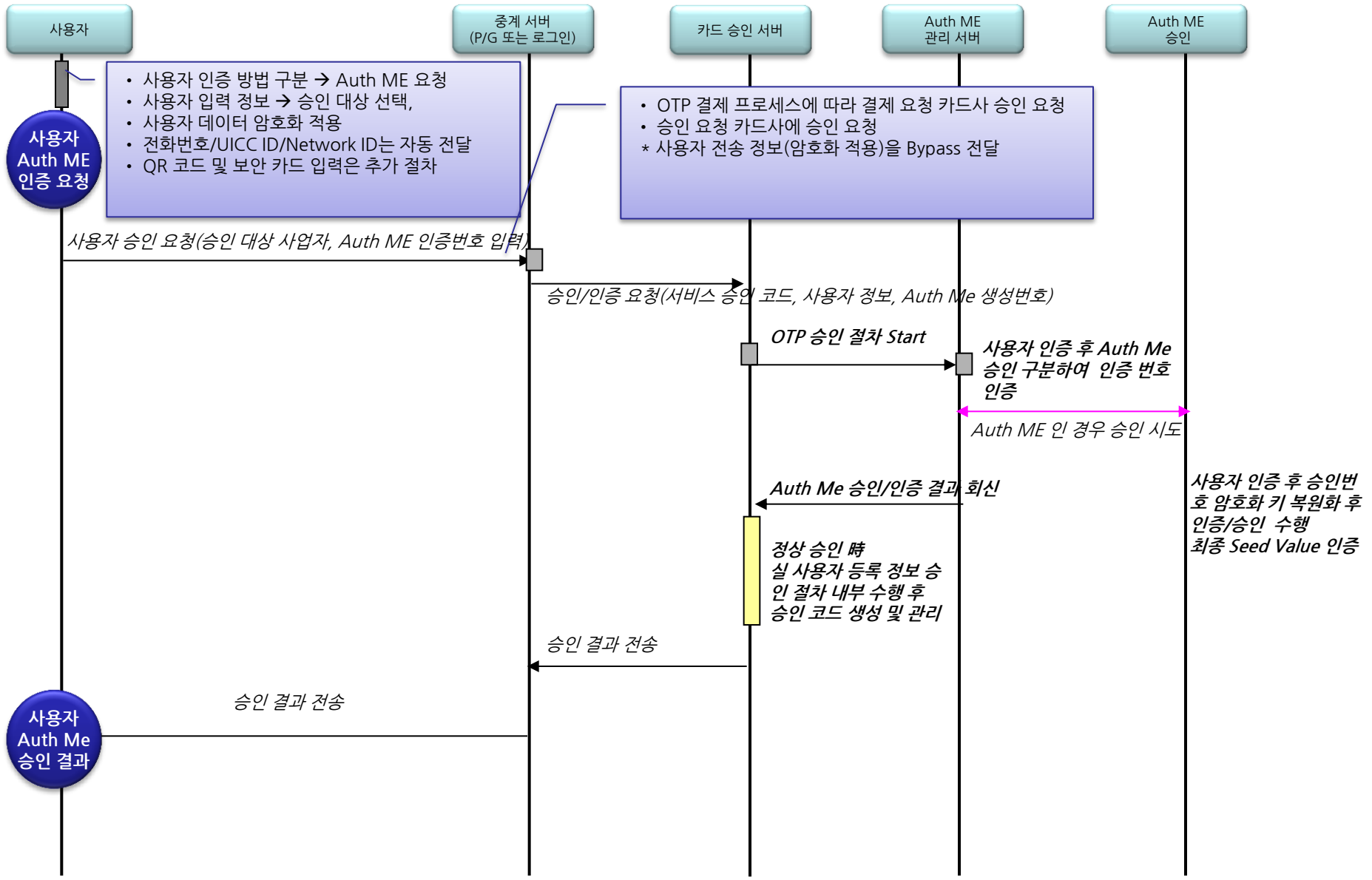
## 미 예시



## 실 적용 화면







금융, 인터넷 상거래, 인터넷 서비스 등 인증/승인을 위한 **모든 패스워드 대체 가능**

인증  
분야

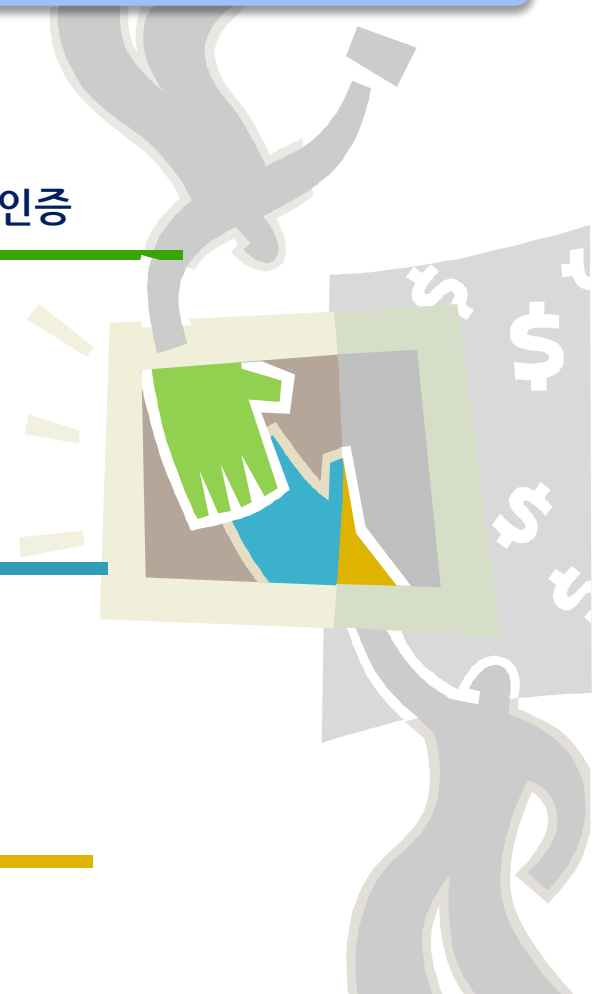
포탈 사용자 인증, 게임 서비스 사용자 인증,  
기업 내부 업무 포탈 로그인 인증, 전자결재 인증

결제  
분야

ISP 인터넷 결제 승인, P/G 결제 대행사 승인,  
쇼핑몰 SSO 인증 등

뱅킹  
분야

공인 인증서 QR코드 인증, 이체 시  
보안카드 + QR코드 인증 도입



스마트 폰 앱 형태의 편리하고 안전한 OTP 서비스를 **다양한 인증 서비스로** 제공

1

편리한 승인 서비스를 통한  
안정적 결제 환경 구축

2

안정적인 로그인 인증을 통한  
서비스 이용자 만족도 향상

3

뱅킹 인증의 보안성 향상  
(공인인증서, 이체보안카드 인증)

4

경제적이고 높은 보안 기술  
도입을 통한 서비스 품질 향상



5

높은 보안 인증매체 도입을  
통한 금융 보안 사고 방지

6

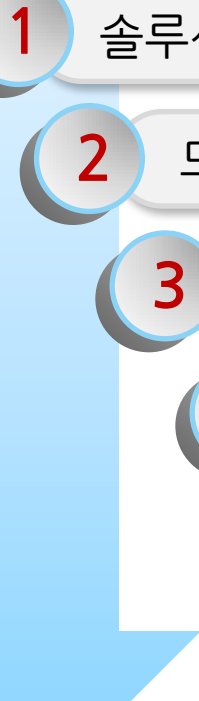
스마트 폰 기반 인증/승인 선도  
기업으로서 이미지 제고

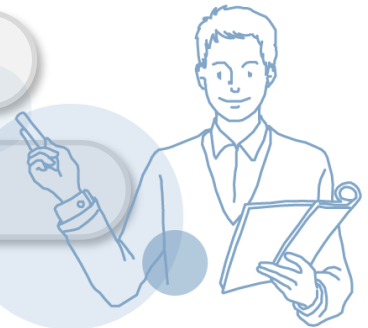
### 3. 솔루션 도입 방안





Auth Me 관리 서버 설치 후 **4주 이내 상용화 지원!**

- 
- 1 솔루션 도입 계약 체결
  - 2 도입 기능 정의 (인증/승인 대상 정의)
  - 3 Auth ME 관리 서버 패키지 설치
  - 4 기간계, 연동대상 시스템 선정 및 개발
  - 5 서비스 검증
  - 6 서비스 상용화



### 도입 효율성 향상

- 내부 전자결재 서비스 활용
- 업무 포탈 로그인 활용
- 계열사 통합 도입을 통한 저비용 고효율



### 신 개념의 인증 인프라 환경 구축

- 보안카드와 QR코드 인증 도입을 통한 신 개념의 Two-Factor 인증 체계 도입
- 비밀번호 탈취 위협과 이체 보안성 강화
- 개인정보 유출 방지 인프라 구축을 통한 서비스 만족도 향상



- 네트워크 기반 알고리즘을 통해 추출된 신개념의 인증 프로세스 도입
- 고정형 인증 체계를 탈피한 보안사고 방지 인프라 구축



- 신 개념의 편리한 인증 서비스 제공을 통한 서비스 품질 향상
- 서비스 환경 선진화를 통한 고객 만족도 향상



### 보안 인증 인프라 구축을 통한 보안사고 방지

### 선도적 보안 서비스 기업 이미지 상승

# 별첨



# 특허 출원 현황

	적용 분야	적용 모델	건수
1	은행/증권사 (Banking/Payment)	<ul style="list-style-type: none"> <li>- 금융계좌와 매핑된 무선OTP를 이용한 banking 관련 모델(14건)</li> <li>- 서비스 제공자와 매핑된 무선OTP를 이용한 banking 관련 모델(5건)</li> <li>- 동적 씨드로 생성된 무선OTP를 이용한 banking 관련 모델(8건)</li> <li>- 사용자 매체 인증을 통해 생성된 무선OTP를 이용한 banking 관련 모델(8건)</li> <li>- 씨드 교환으로 생성된 무선OTP를 이용한 banking 관련 모델(5건)</li> <li>- 생체정보를 이용하여 생성된 무선OTP를 이용한 banking 관련 모델(7건)</li> <li>- 방법, 시스템, 장치, 서버, 스마트폰 관련 특허로 구성</li> </ul>	47건
2	카드사 (온/오프라인 Payment)	<ul style="list-style-type: none"> <li>- 카드와 매핑된 무선OTP를 이용한 온/오프라인 결제 모델(13건)</li> <li>- 무선OTP를 이용하는 (일회용)카드번호 생성 관련 모델(5건)</li> <li>- 무선OTP를 이용한 일회용 카드 제공 관련 모델(4건)</li> <li>- 씨드 교환으로 생성된 무선OTP를 이용한 카드 결제 관련 모델(6건)</li> <li>- 서비스 제공자와 매핑된 무선OTP를 이용한 카드 결제 관련 모델(5건)</li> <li>- 동적 씨드로 생성된 무선OTP를 이용한 카드 결제 관련 모델(7건)</li> <li>- 방법, 시스템, 장치, 서버, 스마트폰 관련 특허로 구성</li> </ul>	40건
3	게임/포탈 (웹서비스 인증/로그인)	<ul style="list-style-type: none"> <li>- 하나 이상의 매체를 이용한 인증용 무선OTP 생성 관련 모델(7건)</li> <li>- 네트워크와 연동하는 인증용 무선OTP 생성 관련 모델(10건)</li> <li>- 사용자 매체 인증을 이용한 인증용 무선OTP 생성 관련 모델(15건)</li> <li>- 생체정보를 이용한 인증용 무선OTP 생성 관련 모델(13건)</li> <li>- 스마트폰 인식 변수를 이용한 인증용 무선OTP 생성 관련 모델(8건)</li> <li>- 방법, 시스템, 장치, 서버, 스마트폰 관련 특허로 구성</li> </ul>	62건
4	소액결제	<ul style="list-style-type: none"> <li>- 온/오프라인 소액결제 관련 모델(6건)</li> <li>- 방법, 시스템, 장치, 서버, 스마트폰 관련 특허로 구성</li> </ul>	6건
<b>무선OTP/일회용보안코드 관련 특허 출원 총 155건</b>			

- ※ 인증/로그인 관련 모델은, 은행/증권사 banking 모델, 카드사 페이먼트 모델 및 소액결제 모델에도 적용 가능한 모델
- ※ 분야별로 분류하였으나, 대부분의 모델이 상호 유기적으로 연결되어 시너지를 낼 수 있도록 구성
- ※ 무선 OTP 모델을 이용하는 다양한 분야에 대한 지속적인 관련 특허 개발 중

# 시스템 사양 및 지원 단말

## 1 시스템 사양

Auth ME* Application Server		Auth ME* Database Server	
Operating System	OS 독립 ( RHEL 권장 )	DBMS	MySQL권장 (MS-SQL, Oracle 지원가능)
CPU	Above Xeon*2ea	운영체제	RHEL권장(지원 DBMS에 따른 OS)
RAM(Memory)	Above 6Gbytes	CPU / RAM	Above Xeon*2ea / Above 6Gbytes
비고(공통)	① NAS 부재 시 Application Server의 저장장치 사용 / ② 시스템 이중화 시 SAN Storage & Switch 필요		

## 2 지원 단말


 iOS			 Android			 Windows		
iPhone	지원	-	Galaxy	지원	-			
iPad	지원	-	Galaxy Tab	지원	-			
			Others	지원	-			
비고	iOS 5.1 이상 지원		비고	Above OS 2.3 이상 지원		비고	단말 출시 시	

## Project Experience - Smart Authentication



은행, 통신, 현장업무 등 스마트 폰 보안 인증 수단으로 도입 사용중인 검증된 인증 솔루션입니다.

**충남소방본부 현장정보지원시스템 등의 Reference 보유**

Client	서비스	구축완료	비고
 <p>충청남도</p>	<p>현장정보지원시스템 사용자 인증</p>	<p>2012. 12</p>	<p>Android ICS, Tablet</p>

