SSenStone

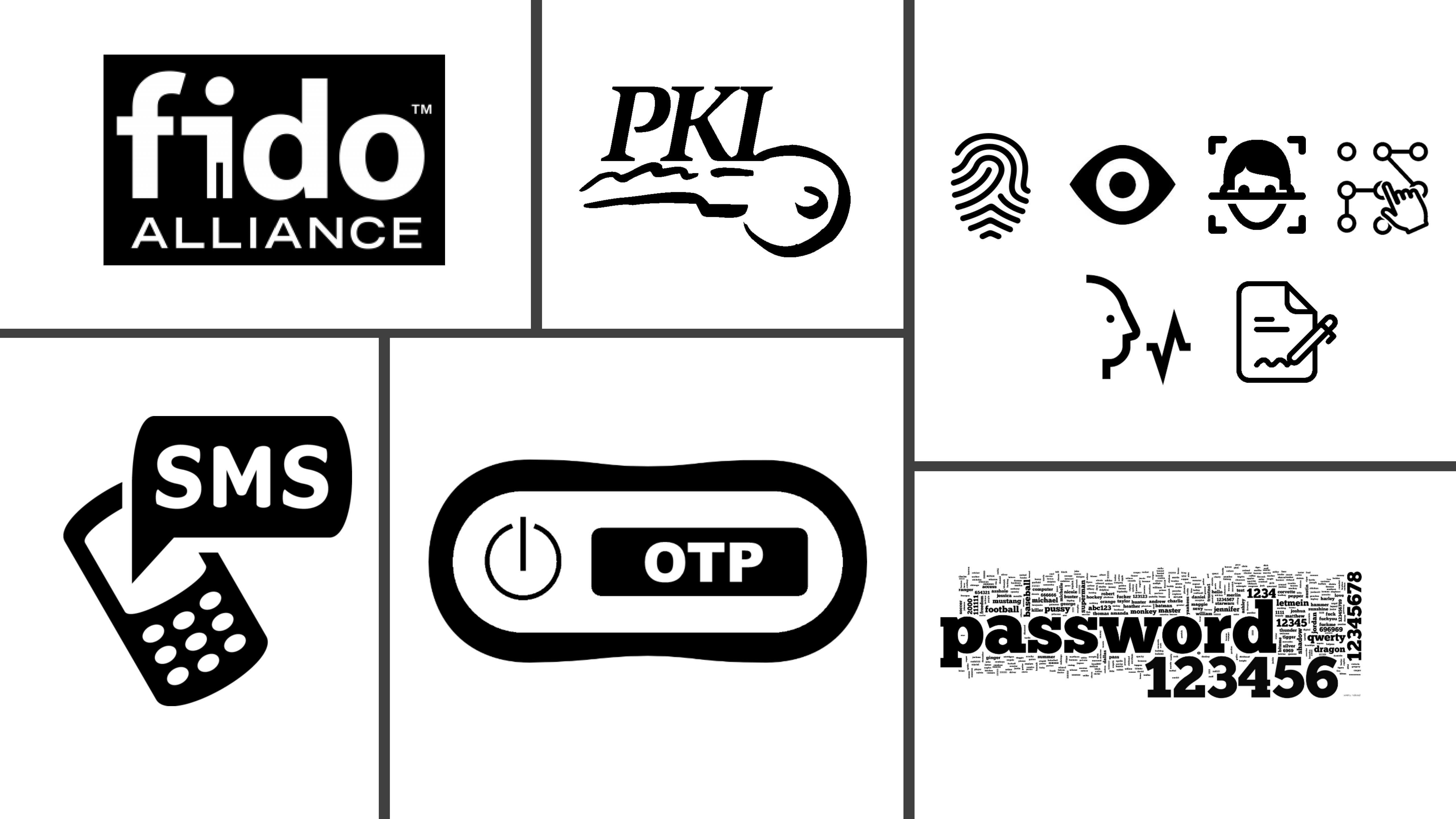
금융권을 위한

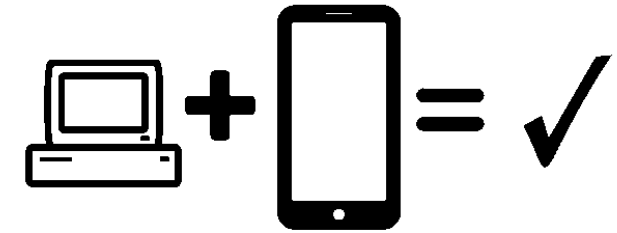
without ID/PW, Just One Time Code 인증 전략

(글로벌 첫 상용화 인증기술 중심으로)

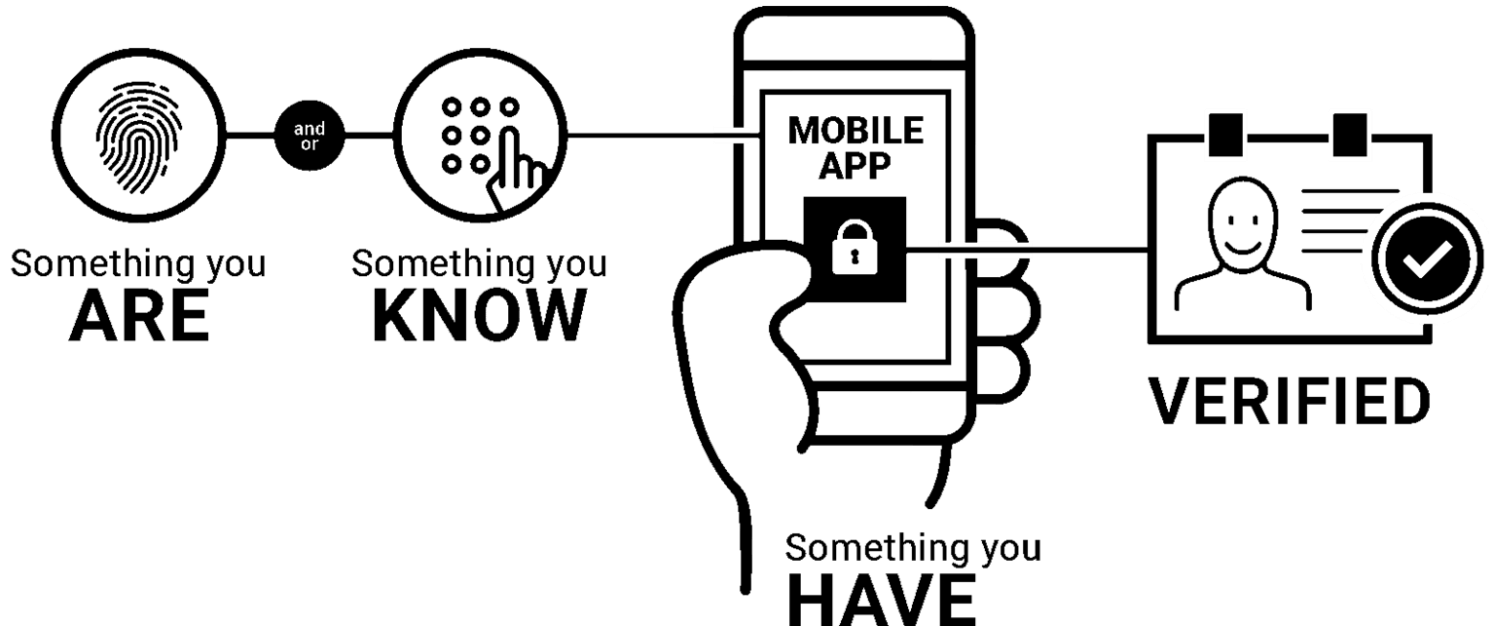
2018. 12

㈜센스톤


fido™
ALLIANCE
PKI
SMS
OTP
password
123456
12345678
qwerty
1234
12345
letmein
dragon

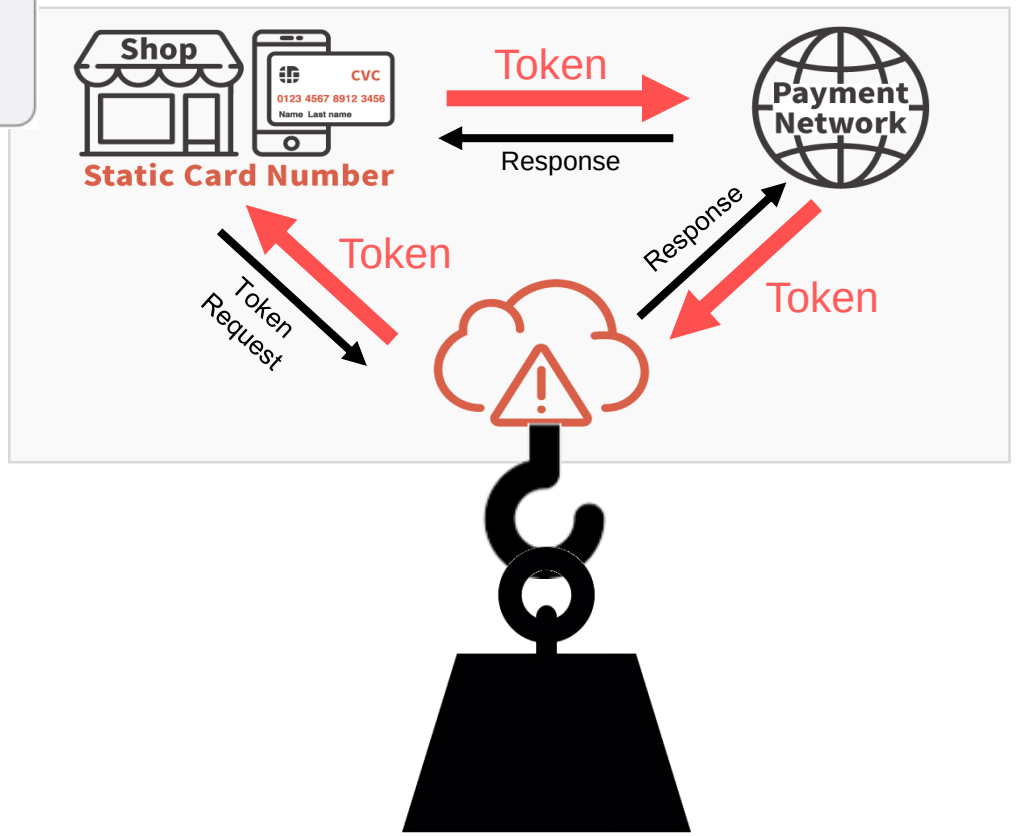


Multi Factor Authentication



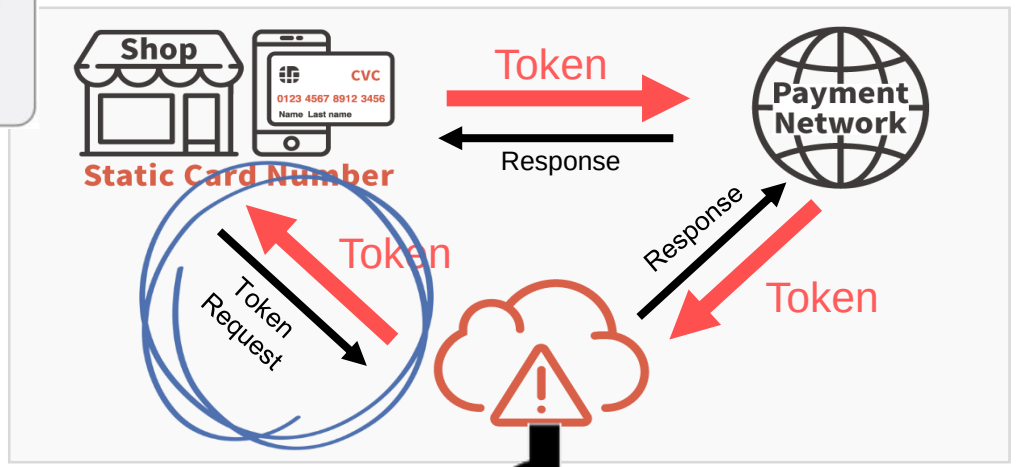
인증
Authentication

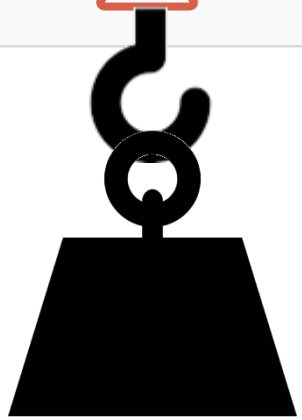
동적
Dynamic

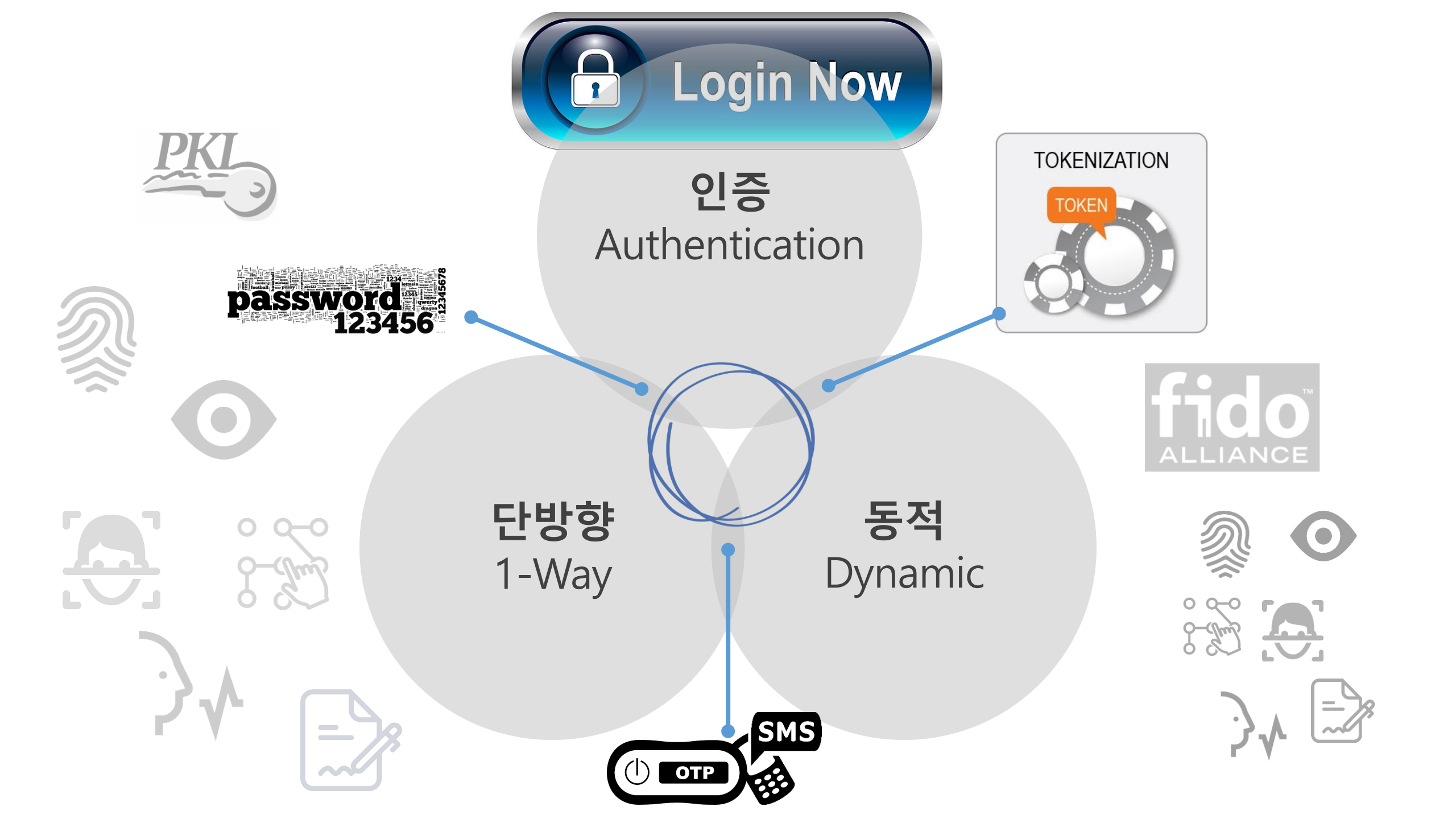


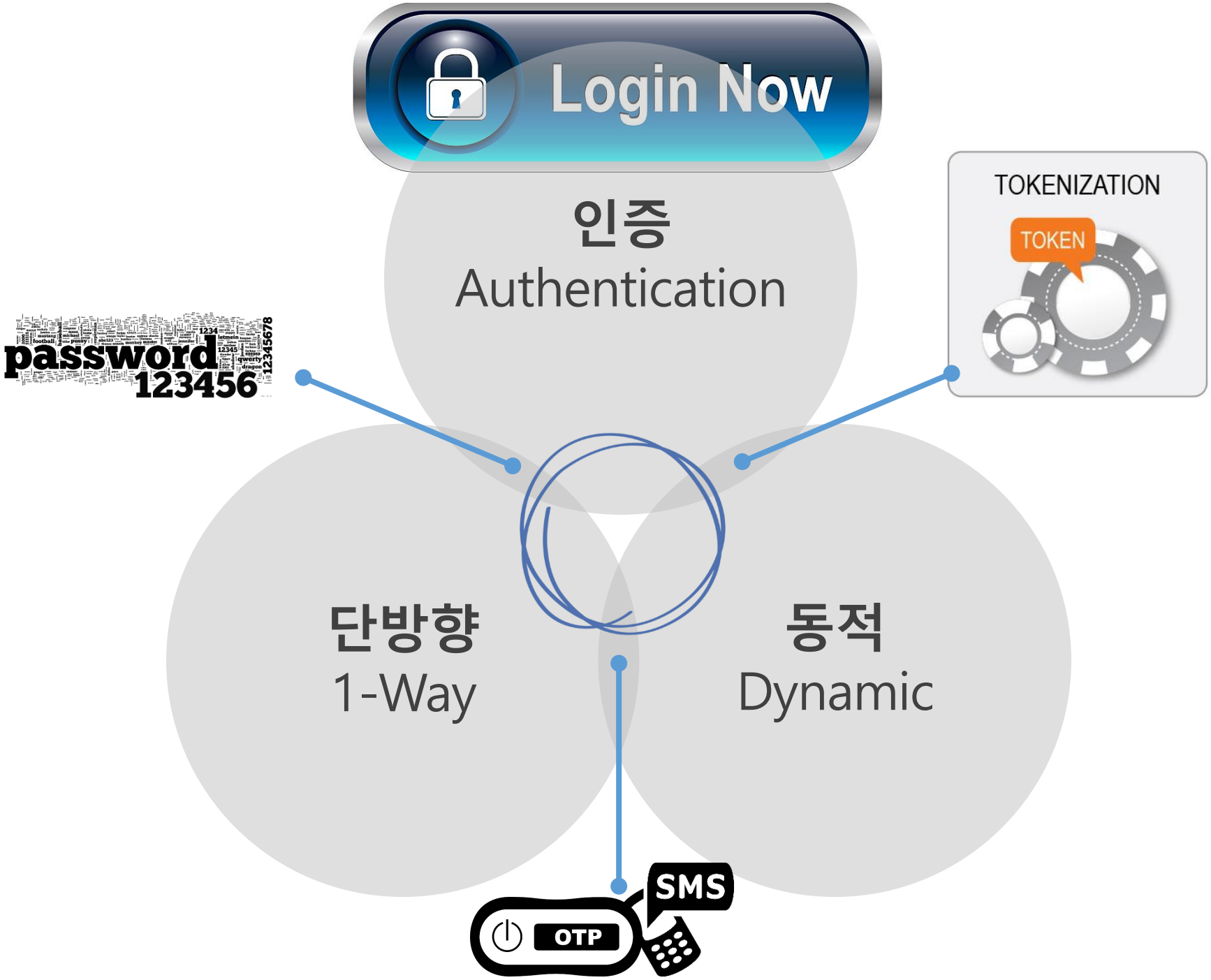
인증
Authentication

동적
Dynamic



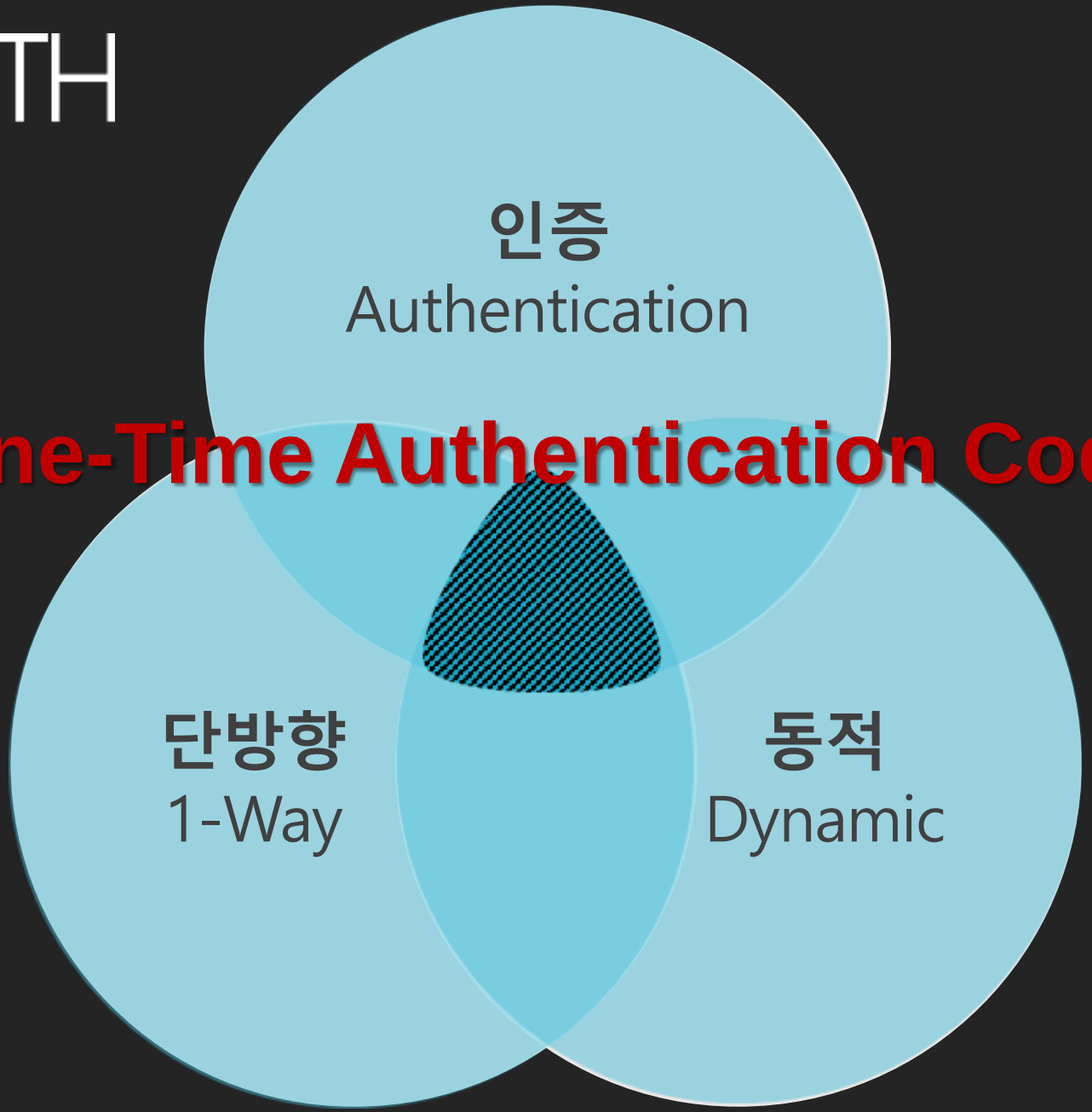



Login Now
PKI
password
123456
인증
Authentication
TOKENIZATION
TOKEN
fido
ALLIANCE
단방향
1-Way
동적
Dynamic
SMS
OTP


Login Now
인증
Authentication
password
123456
TOKENIZATION
TOKEN
단방향
1-Way
동적
Dynamic
OTP
SMS

StoneAUTH

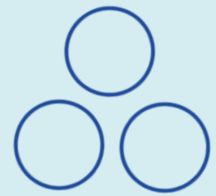
VOTC



One-Time Authentication Code

OTP와 기술 비교

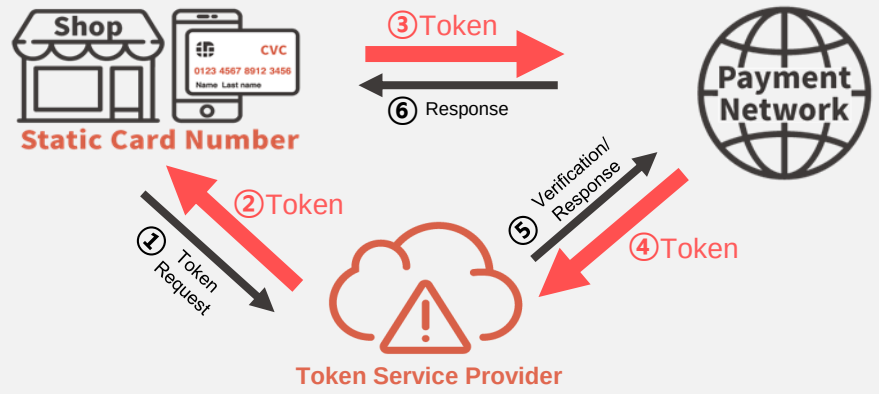
- OTP(One-Time Password)는 ID/PASSWORD 취약점을 보완하기 위해 사용자 소유형 (서버와 통신되지 않는)기기에서 발생한 동적 코드로 인증을 강화합니다.
- **하지만, OTP코드는 사용자 식별이 불가능하여 ID/PASSWORD 인증과 같은 1차 인증 결과를 기반으로 단순 2차 인증용으로 사용이 제한**되어 있습니다.

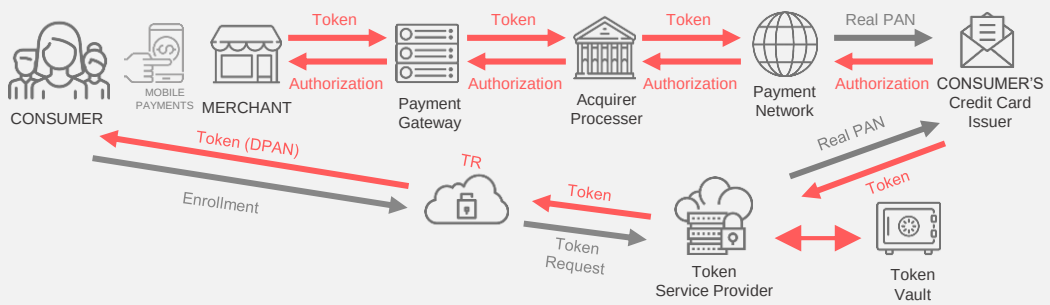
OTP	StoneAUTH One-Time Authentication Code
무작위 번호로 주민증 소지자가 누구인지 **본인 식별이 불가능** 	무작위 번호로 주민증 소지자가 누구인지 **정확한 본인 식별 가능** 
무작위 번호가 다른 사람과 **중복 가능성 존재** 	무작위 번호가 다른 사람과 **중복 가능성 0%** 

Token인증(양방향)과 기술 비교

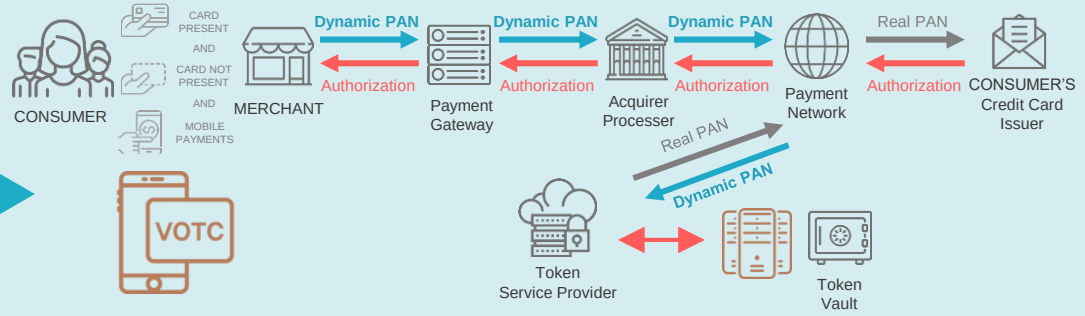
- 사용자와 서버 간의 정해진 규칙에 의해 생성되는 인증 동적 값(Key)를 통해 접근 등 권한 부여합니다.
- Token 인증 서비스는 **서버와 통신 연결된 상태 또는 장치에만 구동되는 한계**로 카드형(Card) 매체 또는 생성기(Generator) 형태에서는 구현 불가능 합니다.

Token(양방향)





OTAC



Current Authentication method : ID/PW

ID, Password 방식의 한계, OTAC 의 필요성

- ID, PASSWORD 는 사용자 측에서 전달한 식별 값(Key)으로 인증하는 방식이며 **고정된 식별 값으로 유출/노출에 취약**합니다.
- 주기적인 비밀번호 변경, 어려운 비밀번호 생성, 서비스 별 다른 비밀번호 설정 등으로 한계를 극복하고 있습니다.

비밀번호 관리 규정

매월 교체

비밀번호 생성 규칙

영문/숫자/특수문자

비밀번호 단계별 관리

CMOS/OS/파일/화면

잦은 비밀번호 변경

복잡한 변경 규칙

너무 많은 비밀번호

비즈니스 모델 예시

Applications

Business model #1 : OTAC로 사용자 인증을 더 안전하고 간편하게

- OTAC(One-Time Authentication Code)는 OTP(One-Time Password)와 달리 사용자가 매번 중복없이 변경/생성되는 랜덤코드만 전달하여도 사용자를 정확하게 식별할 수 있는 기술입니다.
- 이제 로그인을 위해 ID/PW, OTP 등 복잡한 절차없이 랜덤코드 하나만으로 안전하고 간편하게 로그인하는 환경을 제공합니다.

랜덤코드로 안전하고 간편한 로그인 방식

[활용1] 랜덤코드 로그인(폐쇄망 적용)

STEP 1

랜덤코드 생성

STEP 2

로그인 화면 > 랜덤코드 입력

※ 내부망/폐쇄망 적용 가능

STEP 3

로그인 완료

[활용2] 랜덤코드 – 2차인증(2FA)

STEP 1

랜덤코드 생성

STEP 2

랜덤코드 입력

STEP 3

다양한 2FA 적용 /
PUSH 장치 관리

*Option

STEP 4

로그인 완료

OTP 방식과 기술 비교

기 술 명		OTAC (One-Time Authentication Codes)	OTP (One-Time Password)
기술 원리		다차원 구조에서 추적 매칭 방식 (Tracking Matching in Multi-Dimensional Structure)	1차원 구조에서 비교 매칭 방식 (Comparative matching in 1-dimensional structure)
보안 강도	실시간 생성 번호(Realtime)	O	O
	매번 변경되는 번호(Random)	O	O
	그룹 내 다른 대상과 비중복성(Unique)	O	X
식별 강도	1단계 식별 (코드만으로 대상 식별)	O	X
	2단계 식별 (사전 식별 선행 후 식별 강도 보강)	O	O
시스템 구성	클라이언트 모듈	O	O
	서버 모듈	O	O
트랜젝션	클라이언트 단	클라이언트 코드생성	클라이언트 코드생성
	서버 단	클라이언트 코드수신 클라이언트 코드 추적 비교	클라이언트 코드수신 서버 코드 생성 클라이언트 코드 / 서버 코드 비교
단독 인증 용도 사용성		O	X
비고		기존 OTP의 사용분야를 포함하며, 더 확장된 사용성 확보	

Business model #2 : OTAC 기술로 Dynamic PAN 실현

- 네트워크와 연결되지 않는 디지털 카드의 **카드번호가 끊임없이 바뀝니다.**
- 매번 변경되는 **VOTC 동적 카드번호 만으로 실제 카드 사용자를 식별**할 수 있습니다.
- VOTC 동적 카드번호는 다른 사용자들과 **중복 가능성 0 %입니다.**
- VOTC 동적 카드번호는 **현재 카드번호 표준 체계에 따라 변경되어 현재 결제 인프라에** 즉시 적용됩니다.
- **VOTC 동적 카드번호를 기존 소유자 번호로 변환하는 단계는 모든 단계 가능합니다.**

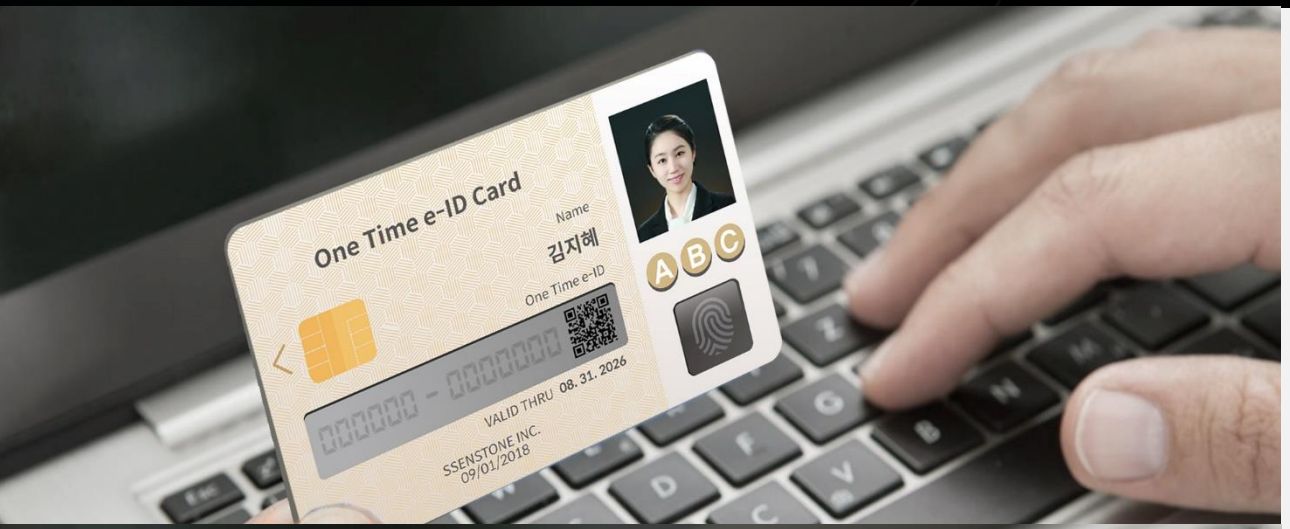
Business model #3 : OTAC 기술로 현 Ai Speaker Authentication 문제 해결

- Ai스피커의 보급으로 해킹, 사생활 침해, 온라인 상품 주문 오류 등 또 다른 위협과 불편함이 발생되고 있습니다.
- 사용자는 언제 어디서나 매번 변경되는 1회성 코드(OTAC)를 Ai 스피커에 불러주는 것만으로도 사용자 식별이 가능해져 IoT기기 페어링부터 쇼핑, 결제까지 안전한 인증을 기반으로 Ai 스피커 기술과 생태계 확장이 가능합니다.

VR(Voice Recognition)

▶▶▶ Shopping & Payment ?

차세대 주민등록 체계의 핵심 기술, 무작위 고유식별 인증코드 기술



비통신 환경

무작위 생성

타인과 중복성 0%

기존 번호 자릿수 유지

- **식별번호를 매번 무작위로 변경하며 발행하는 기술**
  - 비통신 매체(카드)에서도 절대 중복되거나 겹치지 않는 무작위 식별번호 발행
  - 식별번호 전달만으로 본인 확인 가능
  - 해킹/유출, 노출에 전혀 문제없는 차세대 주민번호(식별번호) 발행 기술

- **용도에 따라 식별번호 선택적 노출**
  - 사용자가 직접 자신의 식별번호 노출 범위를 선택
  - 용도별(공공, 금융 등) 및 신분확인 등급에 따라 식별번호 선택 사용

    ※ 식별번호 구성 : 생년월일, 성별, 임의번호 등

- **단순 신분 확인용 외 다양한 IT분야 활용**
  - 최신 IT기술 적용으로 전자/ 모바일 주민증 활용 분야 확대(블록체인, 클라우드 등)
  - 실시간 디지털 정보 연계 (가명정보, 빅데이터 활용)

OTAC 기술 산학연 연구용역

- 건국대학교와 『무작위 고유식별 인증코드 기술의 확장성 설계 실증연구』를 통해 주민등록번호체계 개편의 핵심 기술인 OTAC(One-Time Authentication code)에 대한 기술 검증 및 확정성 검토
- 전자주민번호, 온라인 접근제어 및 본인 확인 대체번호 등 다양한 활용성에 대한 연구 진행

[대학저널 최진 기자] 건국대학교(총장 민상기)는 지난 9일 교내 신공학관에서 (주)센스톤(공동대표 유창훈, 이준호)과 '무작위 고유식별 인증코드 기술'의 확장성 연구를 위한 산학협력 협약식을 체결했다. 협약식은 건국대 클라우드인공지능연구센터(김두현 센터장) 주관으로 진행됐다.

이번 협약을 통해 두 기관은 센스톤의 차세대 인증 기술 OTAC(One-Time Authentication Codes)의 확장성 설계 및 실증 연구를 협력한다. 또한 OTAC 인증 기술의 ▲본인식별 대체번호 공동 연구개발 ▲디지털 모바일ID 설계 및 신뢰성 검증 ▲클라우드 기반 인증 체계를 위한 상호 협력 ▲국가사업 공동 추진 및 연구과제 발굴 등을 추진할 예정이다.

센스톤은 핀테크 인증 보안 분야의 스타트업으로 생체 인증 국제표준인 FIDO(Fast Identity Online) 사용자 간편인증 솔루션, 'StonePASS(스톤패스)'를 출시해 국내 인증 시장에 진출했다.

산학협력 연구책임자 도경화 교수는 "최근 IoT, 클라우드, 블록체인 등 새로운 ICT 환경에서 접근통제와 사용자 인증에 대한 새로운 기술의 연구는 매우 중요하다"며 "특히 센스톤의 기술이 랜덤 식별번호 생성을 기본으로 하고 있어 인증과 개인정보보호를 한번에 잡을 수 있다. 다양한 확장성 연구가 기대된다"고 말했다.

최진 기자 cj@dhnews.co.kr

센스톤 & 건국대학교 : StoneAUTH 기술 확장 설계 연구

1. 본인식별 대체번호 공동 연구 개발

2. 디지털 모바일ID 설계 및 신뢰성 검증
3. 클라우드 기반의 인증 체계를 위한 상호 협력
4. 국가사업 공동 추진 및 연구과제 발굴

Business model #5 : OTAC 기술로 Dynamic Digital Command Code

- IoT 기기 간 고정된 디지털 명령어(Key)로 원격 송/수신 하는 방식에서 매번 변경되는 디지털 명령어로 변경하여 송.수신 함으로 해킹, 중간자 공격 등을 차단할 수 있는 기술입니다.

SSenStone

회사소개

History

SSenStone Inc.

2015

11월 ㈜센스톤 설립

12월 기업부설연구소(KOITA)설립

2-Way Dynamic Key Matching Algorithm 개발완료

StonePASS(차세대 사용자인증 솔루션) 출시

2016

2월 기술보증기금 투자 유치(투자 옵션부 보증)

벤처기업 인증(기술 보증기금)

3월 롯데 L-Camp 1기

Spark Labs 7기

4월 금융보안원 보안컨설팅 완료

경기창조경제혁신센터 K-Champ Lab 3기

5월 KEB하나금융 1Q Lab 3기

8월 한화 드림플러스63 1기

9월 FIDO 얼라이언스 국제공인인증 획득(iOS, Android)

11월 KEB하나은행, 한화그룹, 신용보증기금 투자 유치

12월 ICT 유망기업 K-Global 300 선정

전자정부 경진대회 수상

2017

1월 일본 핀테크 FIBC 2017 한국대표 선정

2월 GS인증 1등급 획득

미래부 후원 SW 경쟁력 대상, 우수상 수상

일본 iSiD 금융권 기준 보안 컨설팅 진행

3월 일본, 싱가폴, 미국 특허 등록 결정

4월 충남창조센터 '해외 사업화 프로그램(GEP 5기 베트남)' 선정

6월 인천창조경제혁신센터 K-Champ 유니콘 기업육성 프로그램 선정

8월 Dynamic One-Time Authentication Code 개발완료

VOTC(Virtual One-Time Codes) 특허 출원(3건/5개국)

11월 K-Global 스타트업 공모전(일반부문) 우수상 수상

K-Global 시큐리티 스타트업 대상 수상

2018

2월 Money20/20 Asia 글로벌 보안 스타트업 TOP 5 선정

5월 StonePASS 블록체인 인증 플랫폼 사업 진출

6월 VOTC(Virtual One-Time Codes) 특허 추가 출원(8건/5개국)

Money20/20 Europe) 스타트업 아카데미 선정

시리즈A 투자 유치(소틱인베스트먼트, 지온인베스트먼트)

1등급 GOOD Software

fido ALLIANCE

fido CERTIFIED UAF

SSenStone

SSenStone : References

공공

행정안전부 · 문화체육관광부 · 헌법재판소 Constitutional Court of Korea · h·well 국민건강보험 National Health Insurance Corporation · 생명보험협회 Korea Life Insurance Association

교육

한국폴리텍대학 · 국립 한밭대학교 · 덕성여자대학교 DUKSUNG WOMEN'S UNIVERSITY

금융

한화손해보험 · IBK 연금보험 · SBI 저축은행 · 푸른저축은행 · DB저축은행 · lifeplanet 교보라이프플래닛생명 · NICE

유통 및 서비스

LOTTE Members · 한화S&C · 한국가상화폐거래소(주) KOVEX · bithumb

INVESTORS

SparkLabs · LOTTE Accelerator · KDIT 신용보증기금 · Hanwha · KEB Hana Bank · STIC INVESTMENTS · GEON Investment

문화체육관광부
대한민국 공직자 대상 '**공직자통합메일**' 사용자 인증시스템 도입

헌법재판소
국내 최초 공공기관, 전자재판 시스템의 **선택형 인증** 적용

국민건강보험공단
'원격연구 시스템' 서비스 **2차인증(2FA)** 적용

국립 한밭대학교
국립대 최초로 교내 IT시스템 '통합인증시스템' 도입

한화손해보험
'간편인증 시스템'의 **내부 사용자 보안 인증**시스템 도입 (안면인증 포함)

생명보험협회
'**보험설계사 시스템**' 서비스로 지문, 보안PIN을 적용한 **2차인증(2FA)** 시스템 구축

롯데멤버스
국내 최다 사용자(3,000만 이상) 대상 **L-Point, L-Pay 선택형 통합인증** 선정

한화 S&C
블록체인 기반의 **그룹사 통합인증** 시스템 적용 (OTAC 포함)

각종 기술 인증 및 심의 통과
FIDO 국제표준 인증, 기술특허 등록, 금융보안원 보안컨설팅 완료, 개별 금융사 보안 심의통과, 모의해킹 검증 완료

fido CERTIFIED UAF · 1등급 GOOD Software

Active Discussions for Global

G+D Mobile Security

Black Tree

ENTREPRENEURS ARE GREAT
BRITAIN & NORTHERN IRELAND

RBS The Royal Bank of Scotland

NatWest

mastercard

HQ in UK

TOPPAN

First Data

Developer Approval Process

SSenStone

Q n A


감사합니다.
SSenStone