Cloud Security

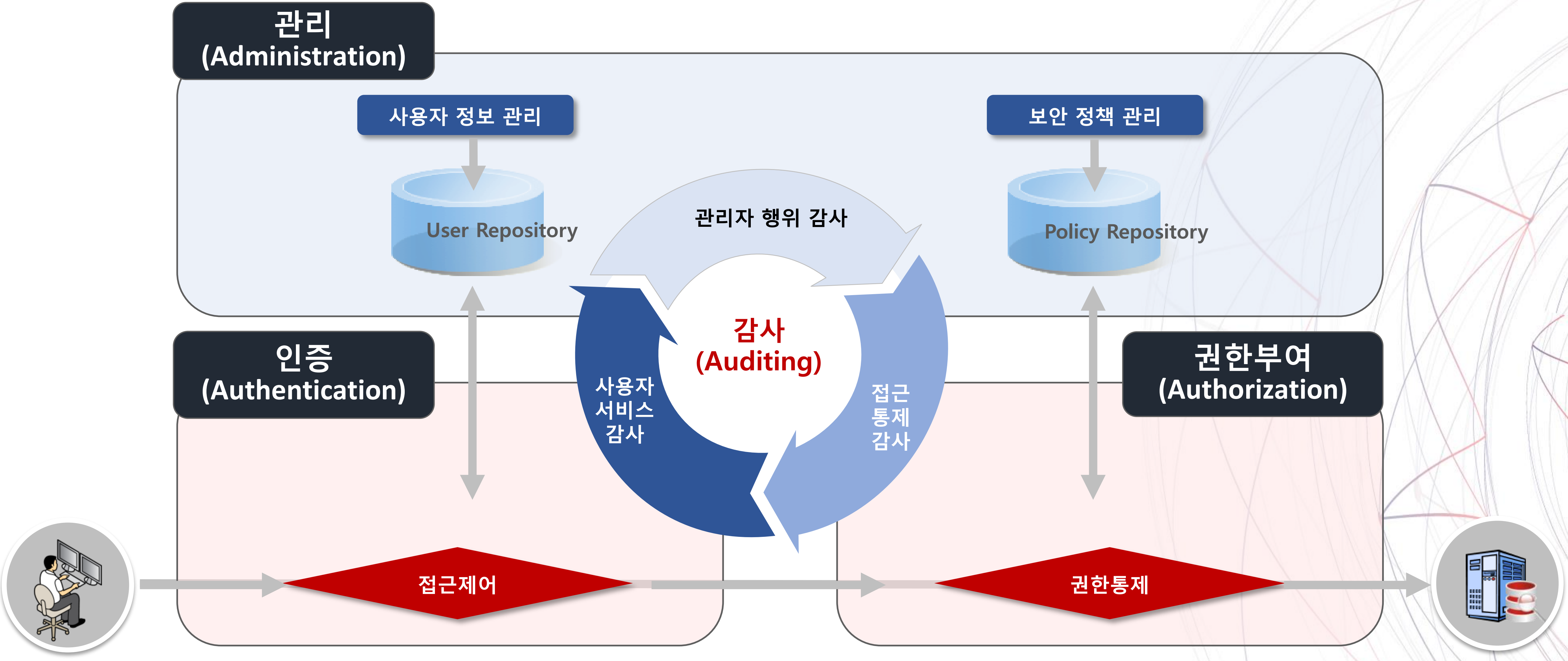
ByeongJae, Ryu
ORACLE

SAMSUNG SDS ORACLE

제5회 SAMSUNG ORACLE
Insight Forum
Breakthrough to the Next Stage

Contents

Security Overview



Security Governance

Governance Requirement

√ Compliance

1. 개인정보보호, 망법, 전자금융거래법
2. ISMS, ISO27001, 클라우드보안 인증
3. 고시, 내부 보안 지침 수용

√ Governance

4. 보안 전략 수립 및 연계 대응
5. 위험 관리
6. 정보/자산/등급 관리

√ Operation

7. 다양한 플랫폼 지원
8. 안정성
9. 업무 연속성(BCP) 체계 수립
10. 운영관리 비용 절감

√ Digital Transformation

11. Cloud Services
12. BYOA / BYOD
13. Cloud, Mobile, IoT, Big Data, AI

- 규제 준수
- 보안 전략
- 운영 관리
- 변화 대응
- 접근 통제
- 감사 체계
- 표준화

관리적 요건 | 기술적 요건

√ SSO/EAM/IM

1. SSO/EAM/IM
2. 비밀번호 관리 / Self Service
3. 보안 취약점 대응
4. 상황인식 기반 위험 통제
5. 모바일 / 네트웍 통제

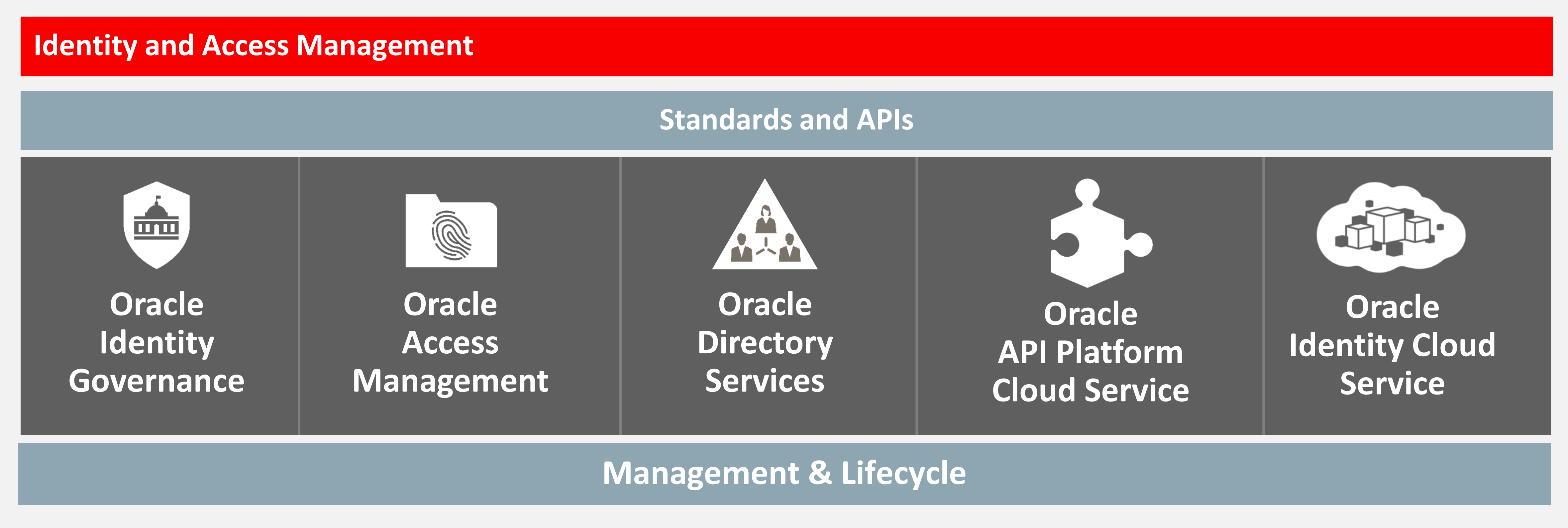
√ Audit

6. 관리자 행위 감사
7. 사용자 행위 및 서비스 감사
8. Certification & SoD(권한분리)
9. 지속적인 모니터링

√ Flexibility

10. MFA(Multi-factor authentication)
11. FIDO(생체인증)
12. Open & Standard, REST APIs
13. Work Flow

Identity HUB



IAM (Identity and Access Management)는 비용, 중단 시간 및 반복적인 작업을 줄이면서 기업이 보안과 생산성을 높이기 위해 올바른 사람에게 올바른 액세스를 제공 할 수있게 해주는 일련의 **비즈니스 프로세스, 정책 및 기술**입니다.

Digital Identity

IAM 1.0

IM + EAM + SSO

- 사용자 통합 저장소 구성 : AD 등
- IM : (De-)Provisioning, PWD 관리
- EAM : 중앙 집중식 권한 관리
- SSO : 단일 인증 체계 구성

중앙 집중식 계정/권한관리 체계 구축

- 일원화된 SSO, IM 프로세스

- Intranet 중심 구성

(De-)Provisioning, Audit Log, 인증 Token

IAM Governance

IAM + Governance + Compliance

- 계정/권한 Life Cycle 관리
- 지속적인 감사 및 모니터링 체계
- Certification, SoD
- 표준화된 통합 (SAML, SPML 등)
- System(OS, DB) + Apps 통합 관리

IAM Governance 체계 구축

- 보안 전략 체계 연계

- Compliance 대응 체계 수립

SAML, SPML, RBAC, XACML, Certification, SoD
MFA(FIDO), ISMS, ISO7001

Digital Identity

Enterprise + Mobile + Cloud

- Protect Access to Any Application from Any Device, Anywhere
- Identify and Audit Who Has Access to What, When, and How

Cloud Service 환경 전환

- Speed, Agility

- Mobile, Cloud 환경의 심층 보안

SAML, OpenID Connect, Oauth 2, SCIM++
클라우드 보안 인증, FedRAMP 등

Cloud Transformation Concerns

Preparation 79% 기업들이 클라우드의 적극적인 도입 검토
19%만이 보안 요구사항 준비

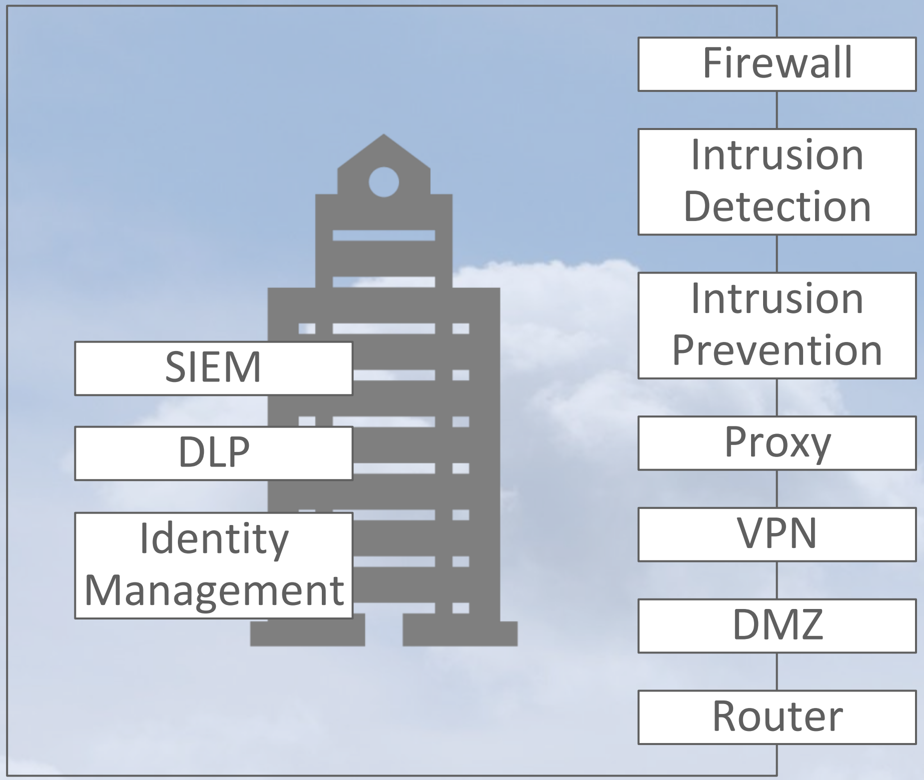
Workloads 71% 대기업은 2018까지 워크로드를 클라우드로 전환 (평균적으로 6개의 Cloud 도입)

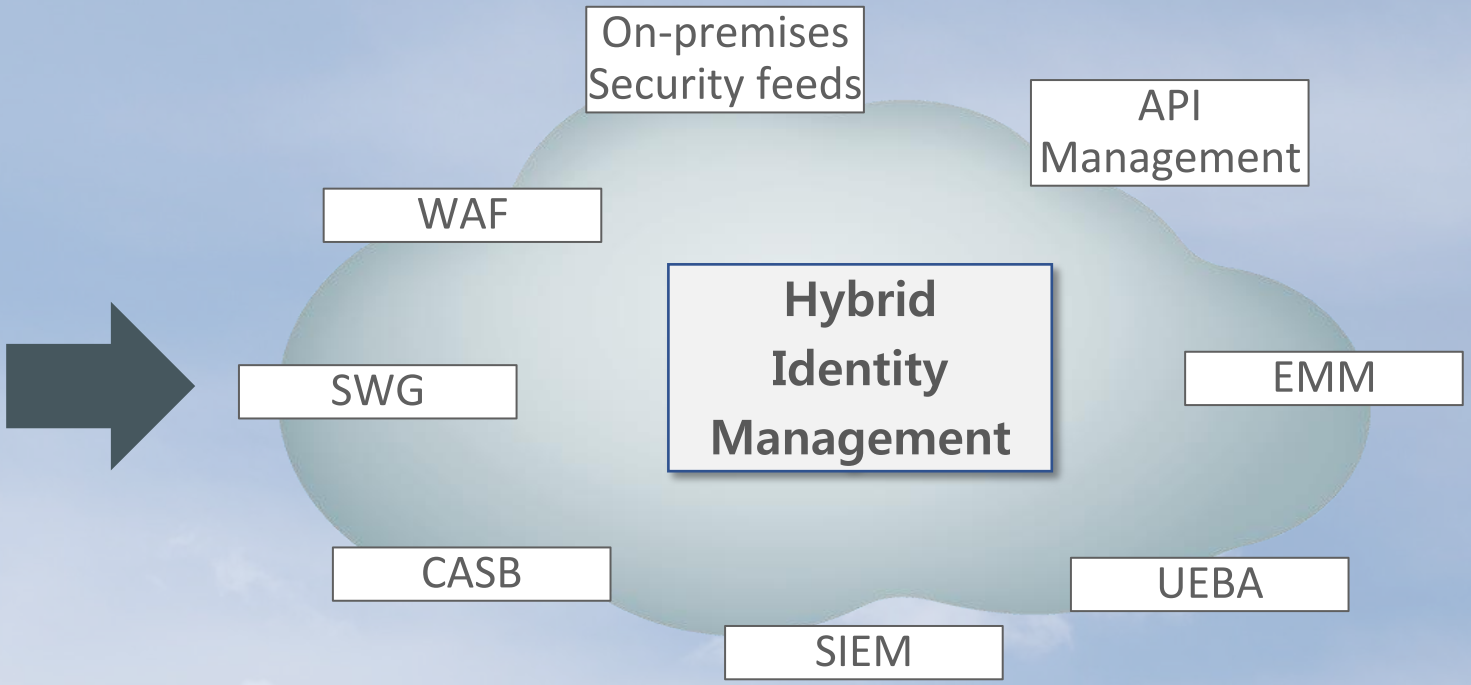
Perimeter 91% 대부분 조직에서 public cloud의 보안 걱정
14% 네트웍 보안 장비가 잘 보호할 것

Resources 66% 숙련된 사이버 보안인력 부족
95% 2020년까지 클라우드의 보안 실패는 대부분 사람의 실수

2016 Cloud Security Research Report, Crowd Research Partner

On-premise vs Cloud

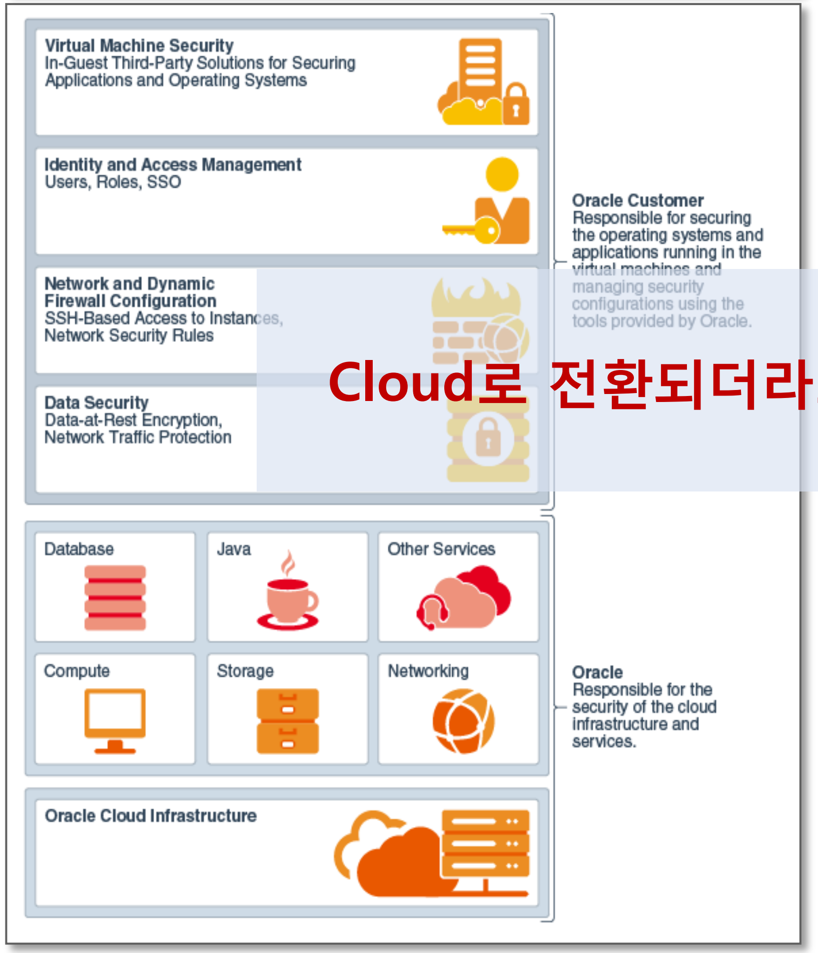


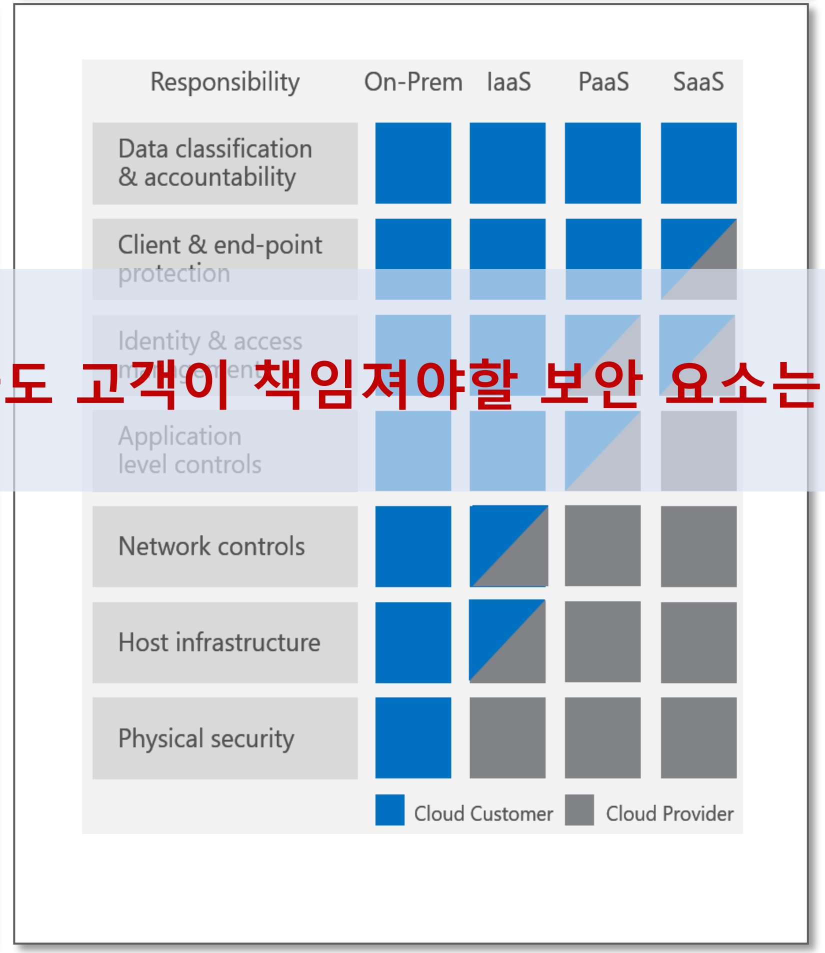


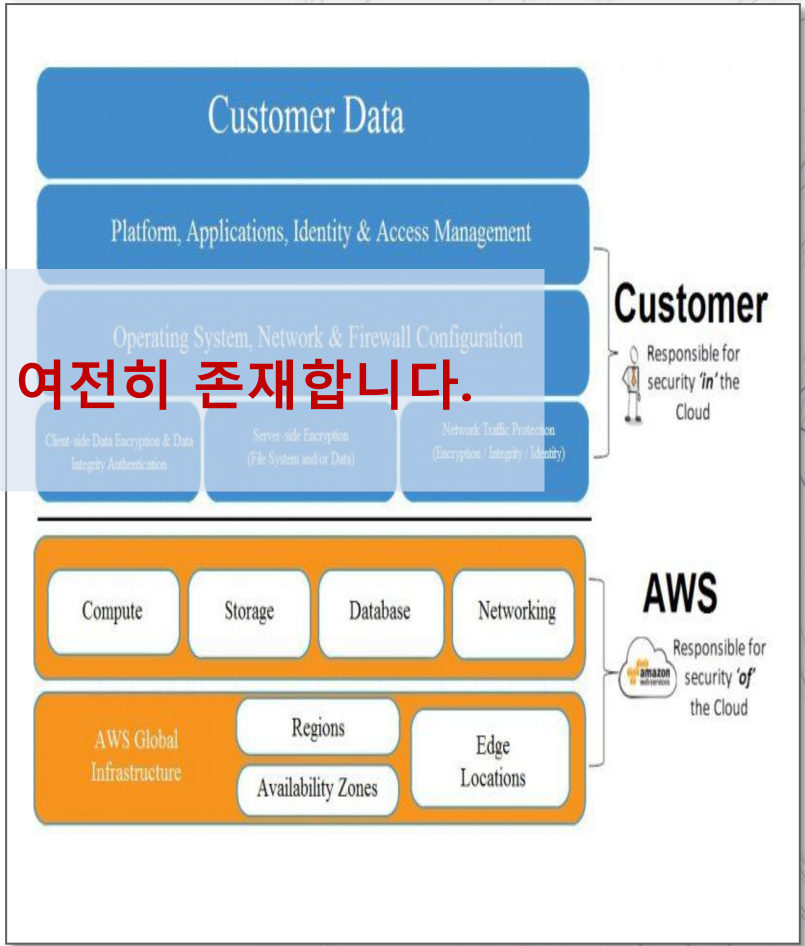
- **WAF** : Web Application Firewall
- **SWG** : Secure Web Gateway
- **CASB** : Cloud Access Security Broker
- **EMM** : Enterprise Mobility Management
- **UEBA** : User and Entity Behavior Analytics
- **SIEM** : Security information and event management

Responsibility for Cloud Security

Oracle	Azure	AWS

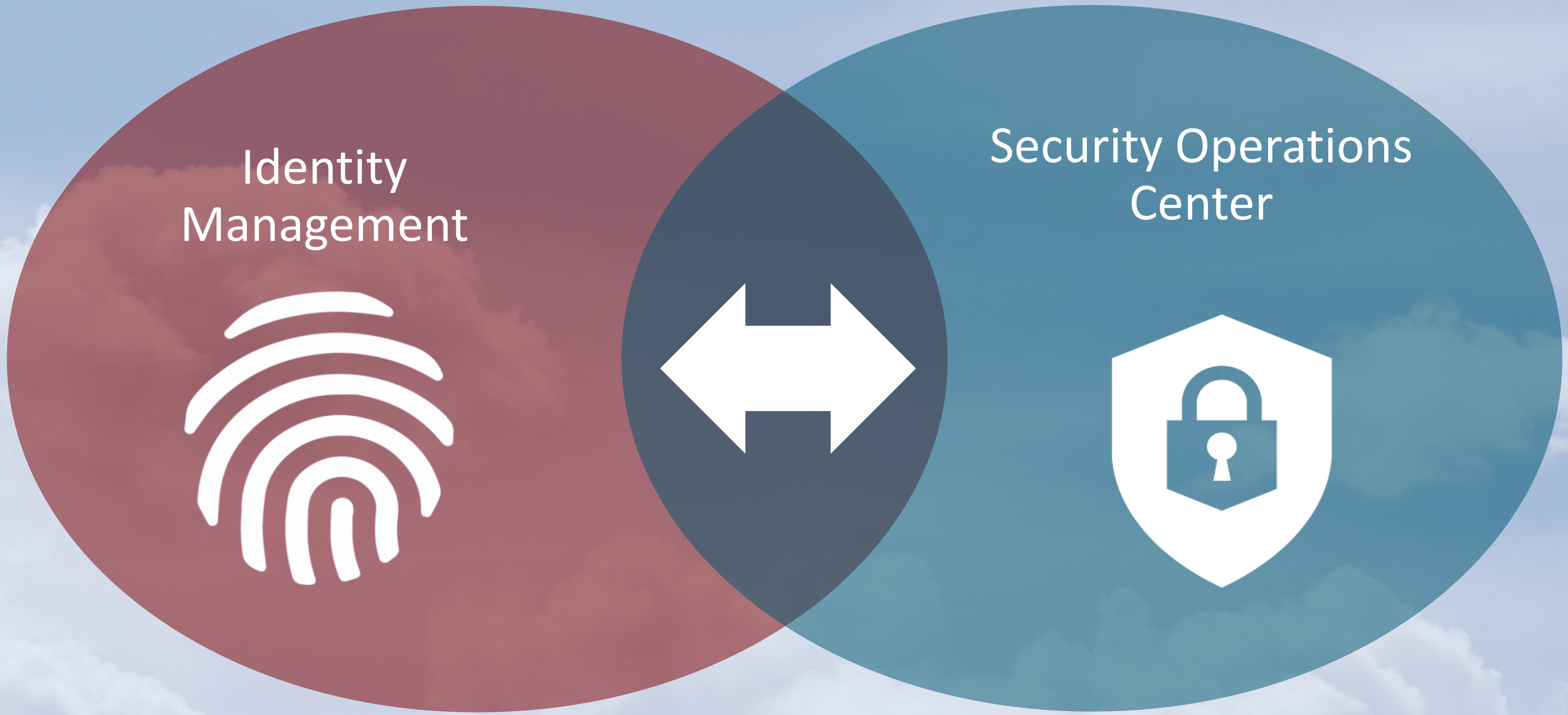






Cloud로 전환되더라도 고객이 책임져야할 보안 요소는 여전히 존재합니다.

Cloud Security Goal



Oracle Security Portfolio

IDCS
Identity Cloud Service

Hybrid 보안

SSO / 계정 관리

보안 포탈 서비스

CASB
Cloud Access Security

보안의 가시성 확보

위협 예방, 탐지, 분석

자동 사건 반응(대응)

Security Monitoring & Analytics

포괄적 보안 탐지

직관적인 시각화

SOC를 위한 차세대 서비스

API Platform Cloud Service

API 빌드 및 보호

손쉬운 배포 서비스

모니터링

Compliance Cloud Service

Compliance 준수

취약점 분석 및 지속적인 평가

Hybrid Data Security

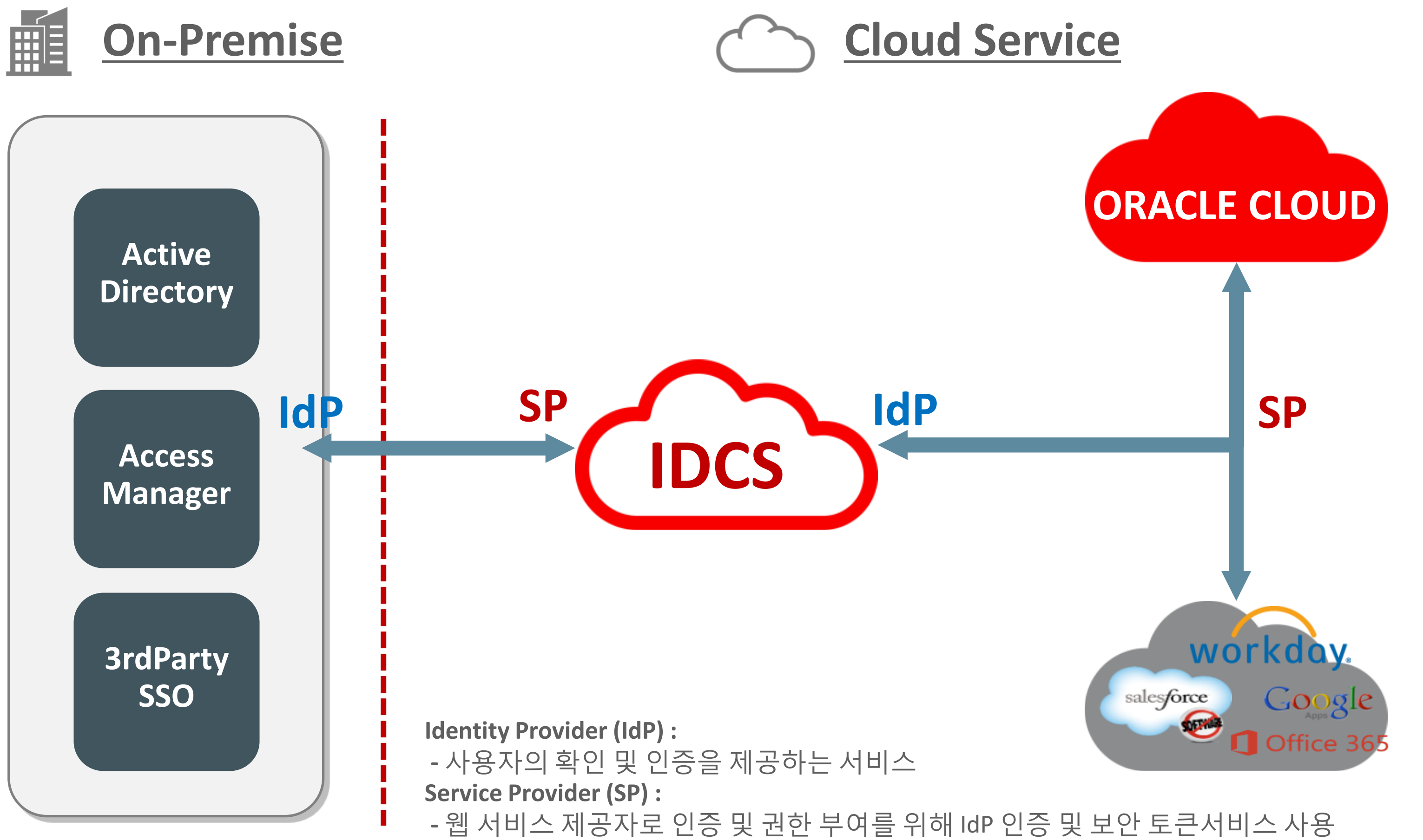
Hybrid 데이타 보호(on-Premise + Cloud)

Hybrid 감사 및 모니터링 관리

IDCS (Identity Cloud Service)

IDCS (Identity Cloud Service)

Identity Cloud Service



Identity Provider (IdP) :
- 사용자의 확인 및 인증을 제공하는 서비스

Service Provider (SP) :
- 웹 서비스 제공자로 인증 및 권한 부여를 위해 IdP 인증 및 보안 토큰서비스 사용

통합 계정 관리

On-Premise와 Cloud의 사용자 및 그룹 동기화를 통한 통합 계정관리

통합 인증 서비스

SSO, MFA(Multi Factor Authentication)

보안 포탈 서비스

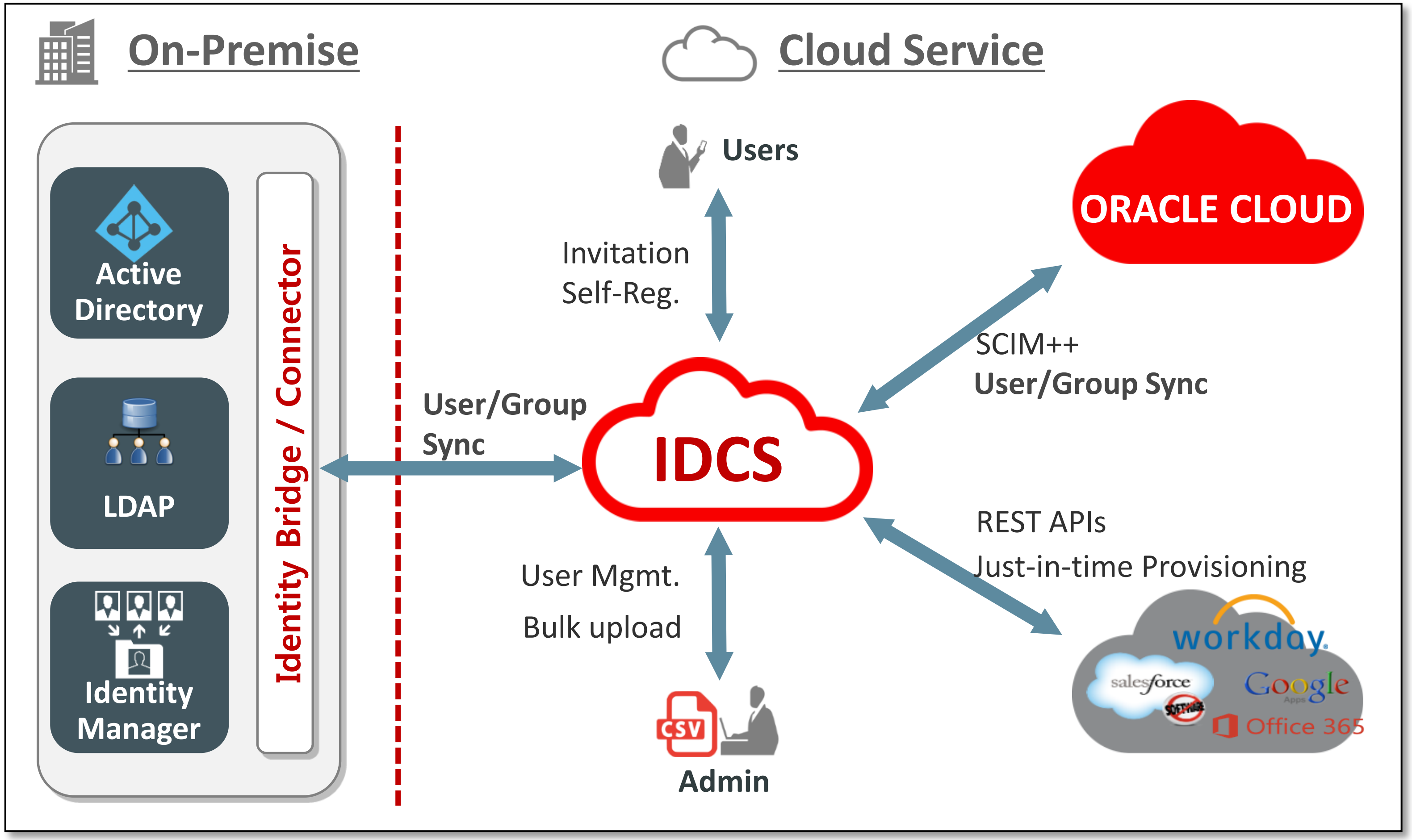
BYOA(Bring Your Own Application)

확장

Key Management, CASB, SIEM 연계를 통한 Digital Identity 확장

IDCS – 통합 계정 관리

Identity Cloud Service



통합계정관리

1. On-Premise 사용자 동기화

- Active Directory 자동 동기화
- LDAP User/Group 동기화
- Oracle Identity Governance Connector 연동

2. 사용자/그룹 통합관리

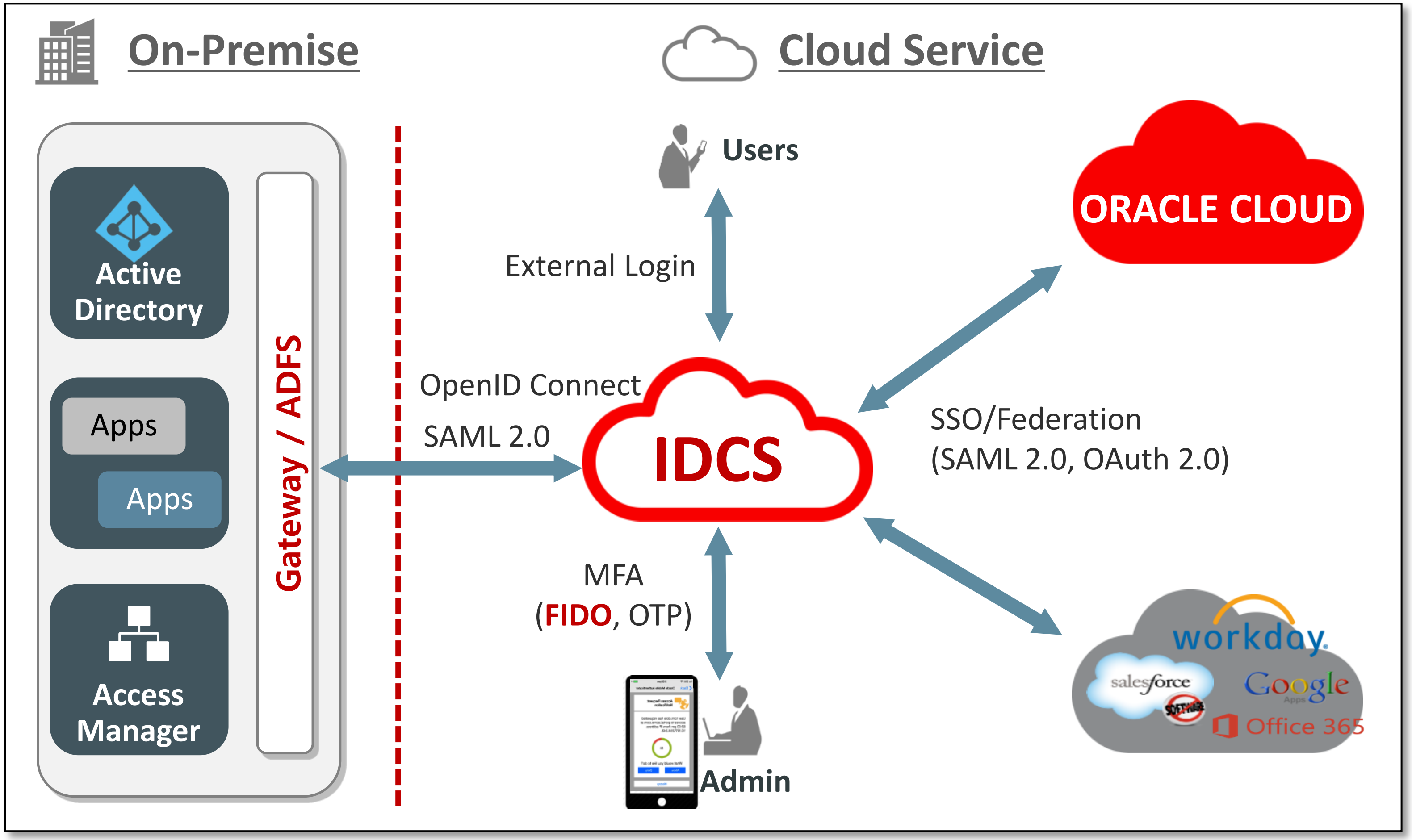
- 관리자에 의한 통합 관리
- 사용자 Self Service/Invitation

3. 클라우드 Provisioning

- Oracle Cloud Service Provisioning
- 3rd Party Cloud Service Provisioning

IDCS – 통합 인증 서비스(MFA/SSO)

Identity Cloud Service



통합인증관리

1. (Multi) Federation

- IDCS의 IdP역할을 통한 Federation
- 다양한 Cloud Service(SP) 에서 On-Premise (IdP)로의 다중 Federation 연계
- Multi IdP 연계
  (예: Region별 Multi AD에 대한 Federation)
- OIG와의 연계를 통한 확장

2. SSO

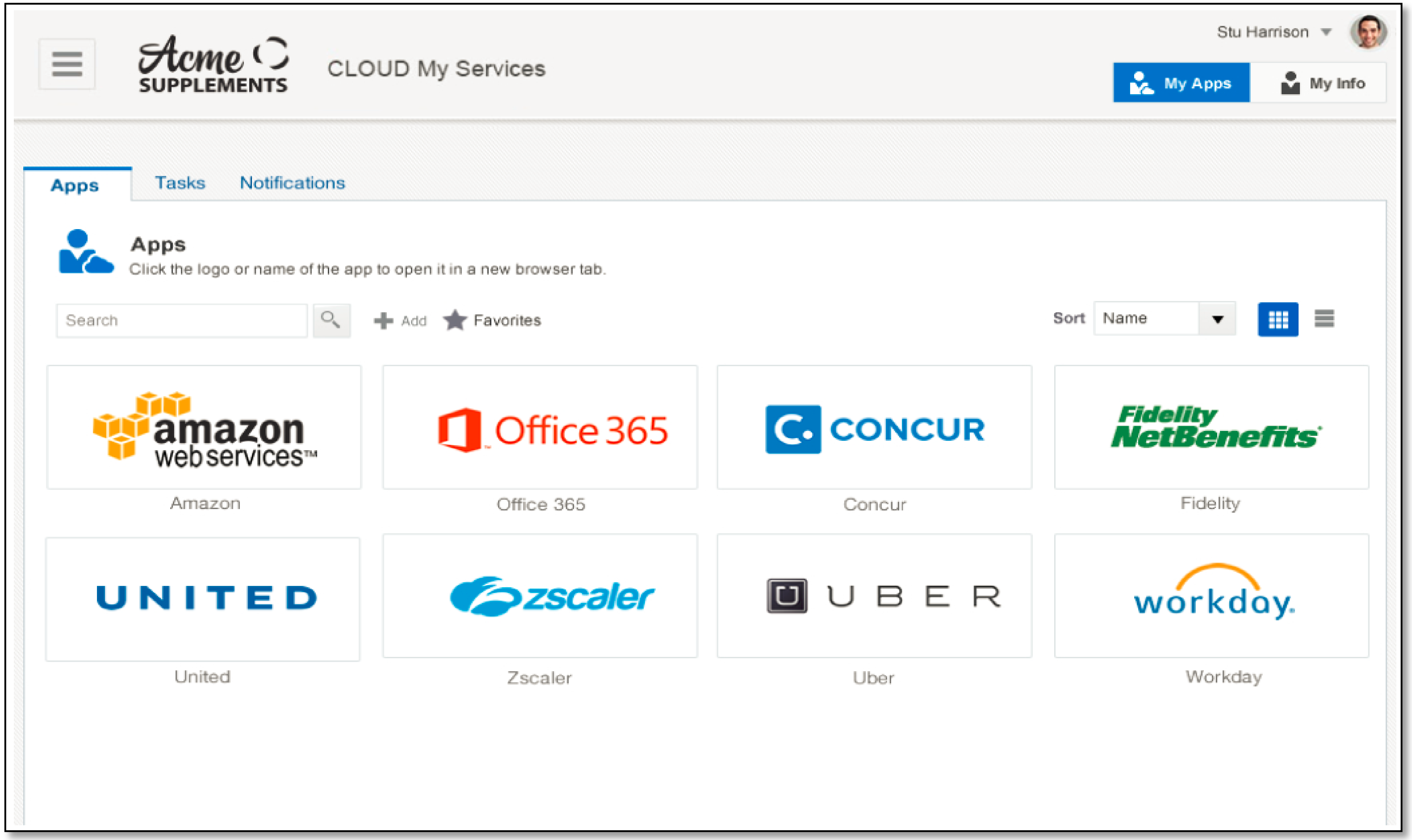
- 표준 기술을 통한 SSO 연계
- Authentication / Authorization

3. MFA

- SDS Nexsign(FIDO)를 통한 추가 인증
- 다양한 3rd Party 인증 연계

IDCS – BYOA(Bring Your Own Application)

Identity Cloud Service



보안 포탈 서비스

1. App Integration

- 어플리케이션 탬플릿을 이용한 신속한 통합
- 프로그램 App Catalog를 통한 직접 통합

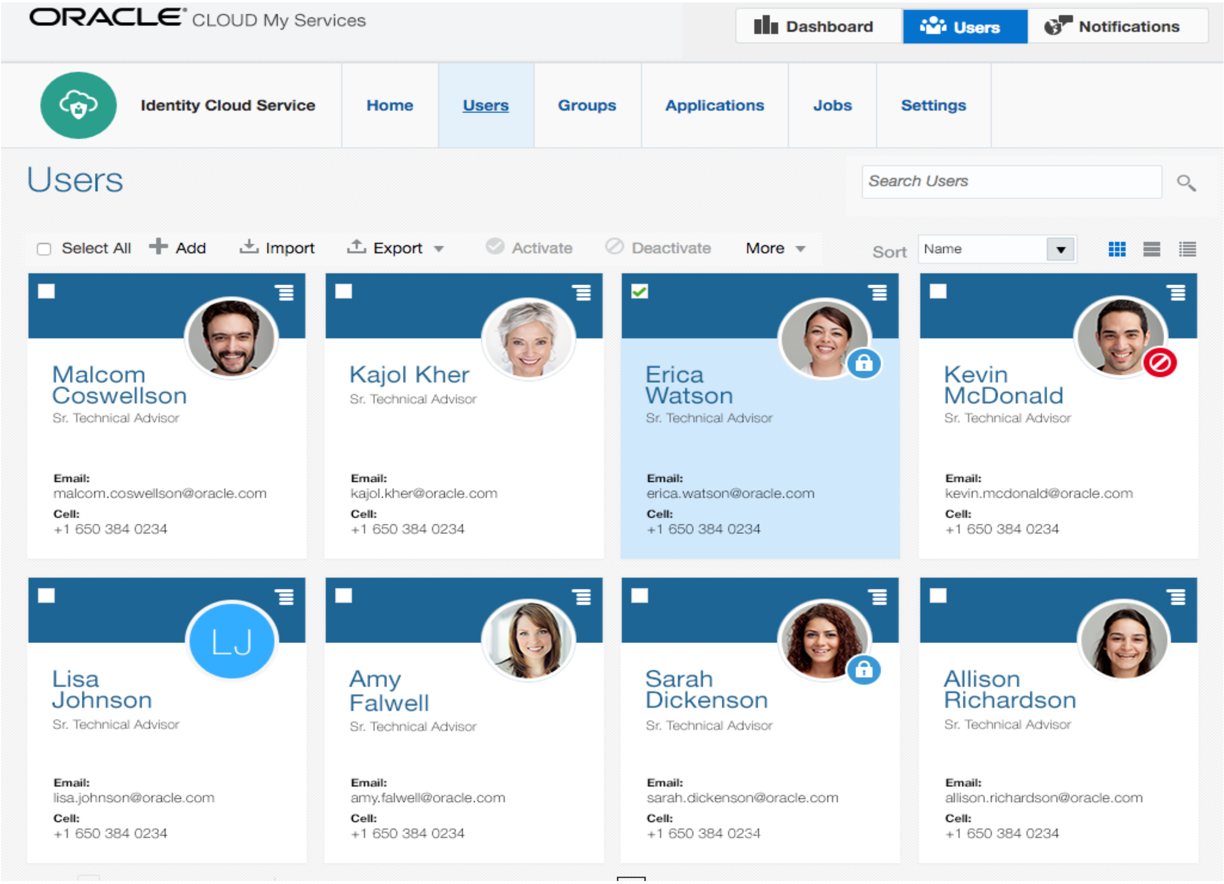
2. SSO 연계 표준

- SAML 2.0
- OpenID Connect or OAuth 2.0

3. 멀티 장치 플랫폼에서의 통합 사용자 환경 제공

IDCS – 확장

Identity Cloud Service



정책 관리 및 확장

1. 사용자, 그룹, 역할기반의 엑세스 정책

- 사용자의 신원 정보만으로 유연한 정책 설정
- 사용자 역할 및 그룹 구성원 자격을 통한 정책
- 컨텍스트 기반 접근제어 정책
- 실시간 속성을 이용한 상황별 접근제어
  : 위치, 장치 유형, 네트워크 등
- 외부 ID 공급자에 대한 접근정책 연계

2. 확장

- Key Management, CASB, SIEM 연계를 통한 Digital Identity 확장

Identity Cloud Service

Hybrid

On-Premise + Cloud

- OIG, AD와의 계정동기화
- Governance Cloud 확장
- Federation 인증/인가
- 감사, SoD 확장 연계

Standard

Open & Standard based

- Application 신속한 통합
- 100% 표준 기반
- SAML, OAuth, OpenID, SCIM
- REST APIs 확장성

Secure

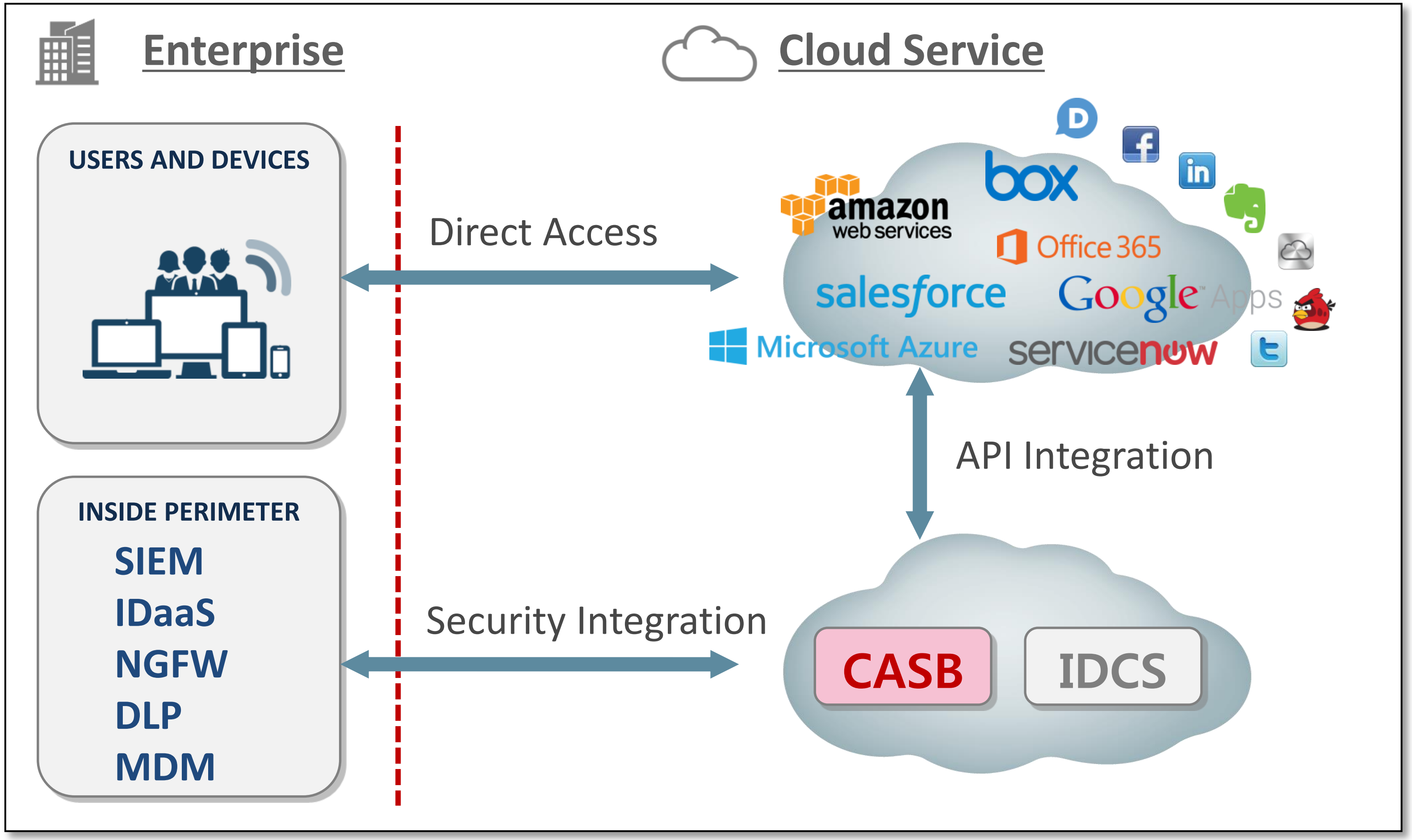
Secure Defense-in-Depth

- Public Cloud 기반 심층보안
- 상황인식 기반 보안 확대
- 기존 Infra 보안 연계

CASB (Cloud Access Security Broker)

CASB 필요성

Cloud Access Security Broker



Visibility

누가 어떤 Apps에 접근하고 있는가?
누가 승인되지 않은 Apps에 접근하고 있는가?
관리되지 않는 사용자는 무엇을 하고 있는가?

Compliance

개발운영 작업은 규정을 준수하는가?
접근키는 규정을 준수하는가?
과도한 특권 사용자가 있는가?

Data Security

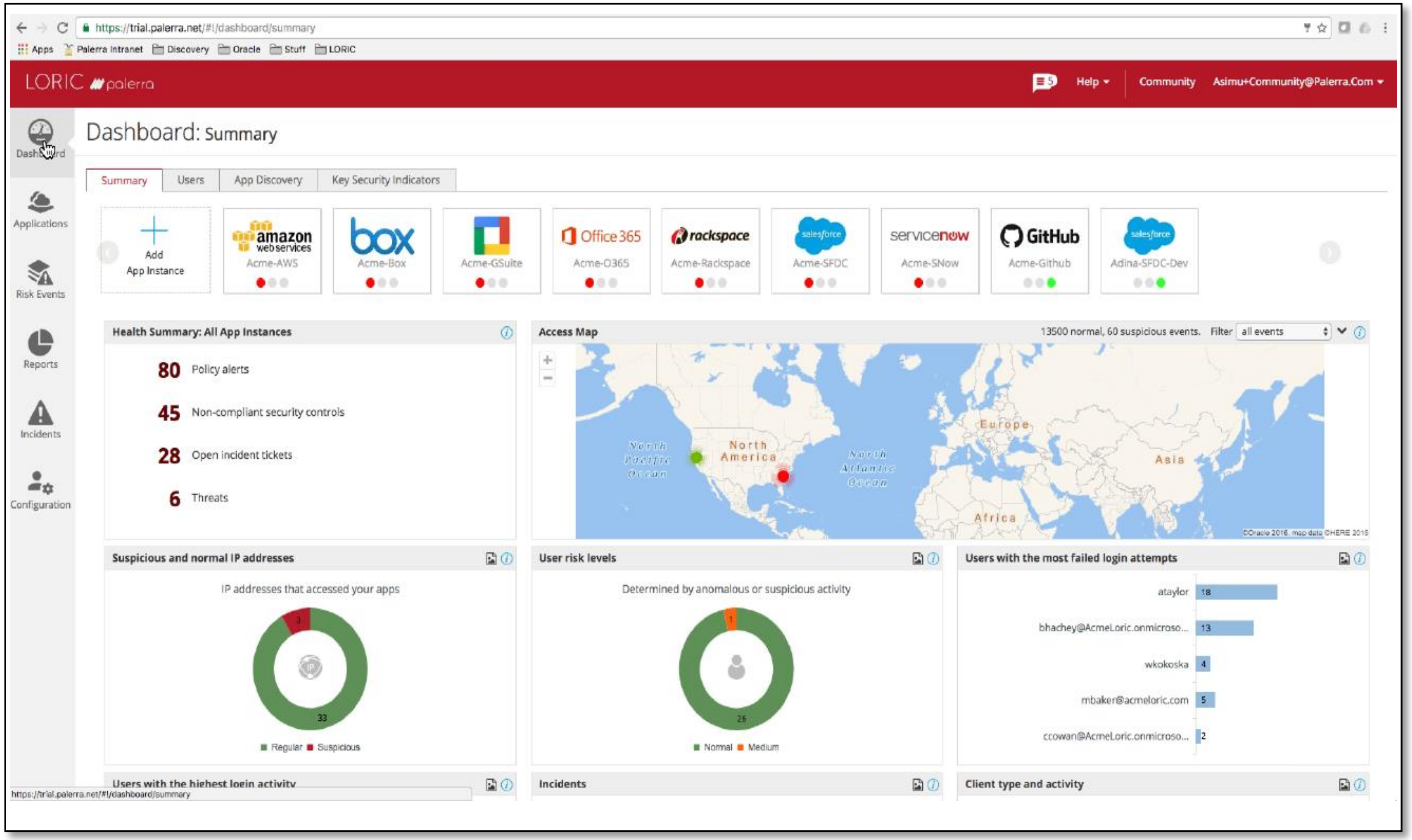
누가 데이타를 공개하고 있는가?
보안 책임을 이행하고 있는가?
어떠한 보안 취약점이 있는가?

Threat Protection

시스템 상에 위험한 사용자는 누구인가?
빨리 위험한 사용자를 차단할 수 있는가?
빨리 위험한 Apps을 차단할수 있는가?

CASB 역할

Cloud Access Security Broker



Discover

클라우드 서비스의 **보안 위협에 대한 지속적인 탐지**

Secure

users, data, content, applications, settings, infrastructure의 **자동화된 제어**

Monitor

위협 및 컴플라이언스 위험을 식별하는 사용자 활동 및 보안 구성의 **지속적인 모니터링**

Respond

IDCS등 기존 솔루션과의 통합 및 사고관리의 **재조정 자동화**

Cloud Security Goal

One-Stop SOC Dashboard

Security Monitoring & Analytics Cloud Service

Content Security	User Security	Configuration
CASB Cloud Service	Identity Cloud Service	Configuration & Compliance Cloud Service

Security Posture

Applications, data and user activity analytics, threat intelligence, and compliance

Automated Incident Response & Remediation (Orchestration Cloud Service)

Register for a Security Assessment Today

- GDPR Best Practices
- Cloud Security
- Security Program Review
- Customer/External Identities
- Employee Identities
- Partner/Contractors
- Bespoke Single Sign-On
- Web Single Sign-on
- **Authentication**
  - **Multi-Factor**
  - **Adaptive**
  - **Passwordless**
- Privileged Account Management
- Access Certification
- API Security & Management
- Automated Provisioning

Next

Biometric Security on IAM

Nexsign with Oracle IAM

박희진
삼성SDS

SAMSUNG SDS ORACLE

제5회 SAMSUNG ORACLE Insight Forum

Breakthrough to the Next Stage

Contents

왜 사용자 인증이 필요한가?

Offline

Online

왜 사용자 인증이 필요한가?

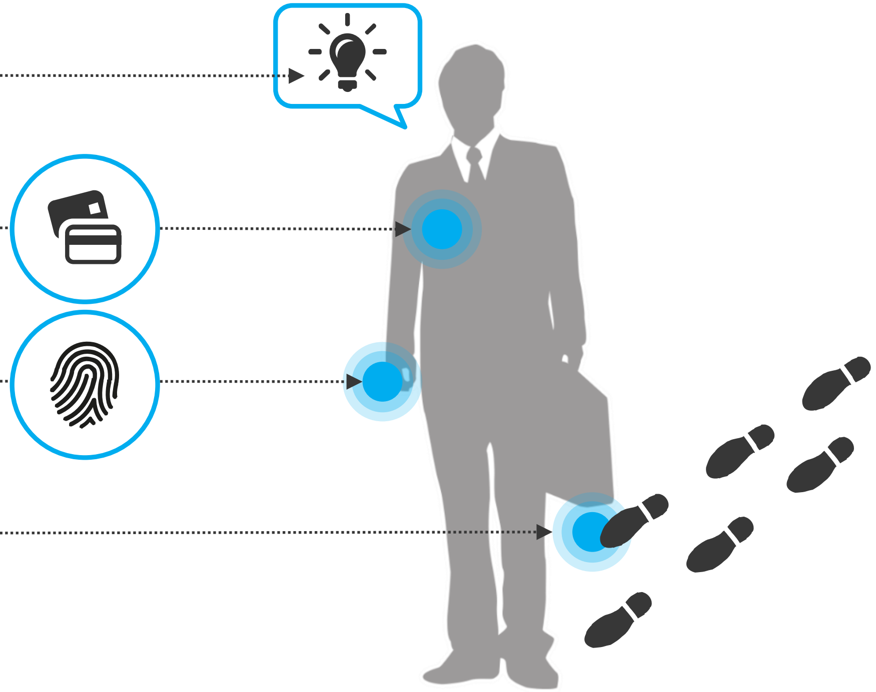
Who is he / she ?

불특정 다수

비 대면

사용자 인증 방법

1. Something you **know** 지식
2. Something you **have** 소유
3. Something you **are** 특성
4. Something you **do** 행동



두 개 이상 방법 사용된 경우 **보안성 보다 강화** 됨 ▸▸▸ **편이성**은 감소

* Multi-factor Authentication

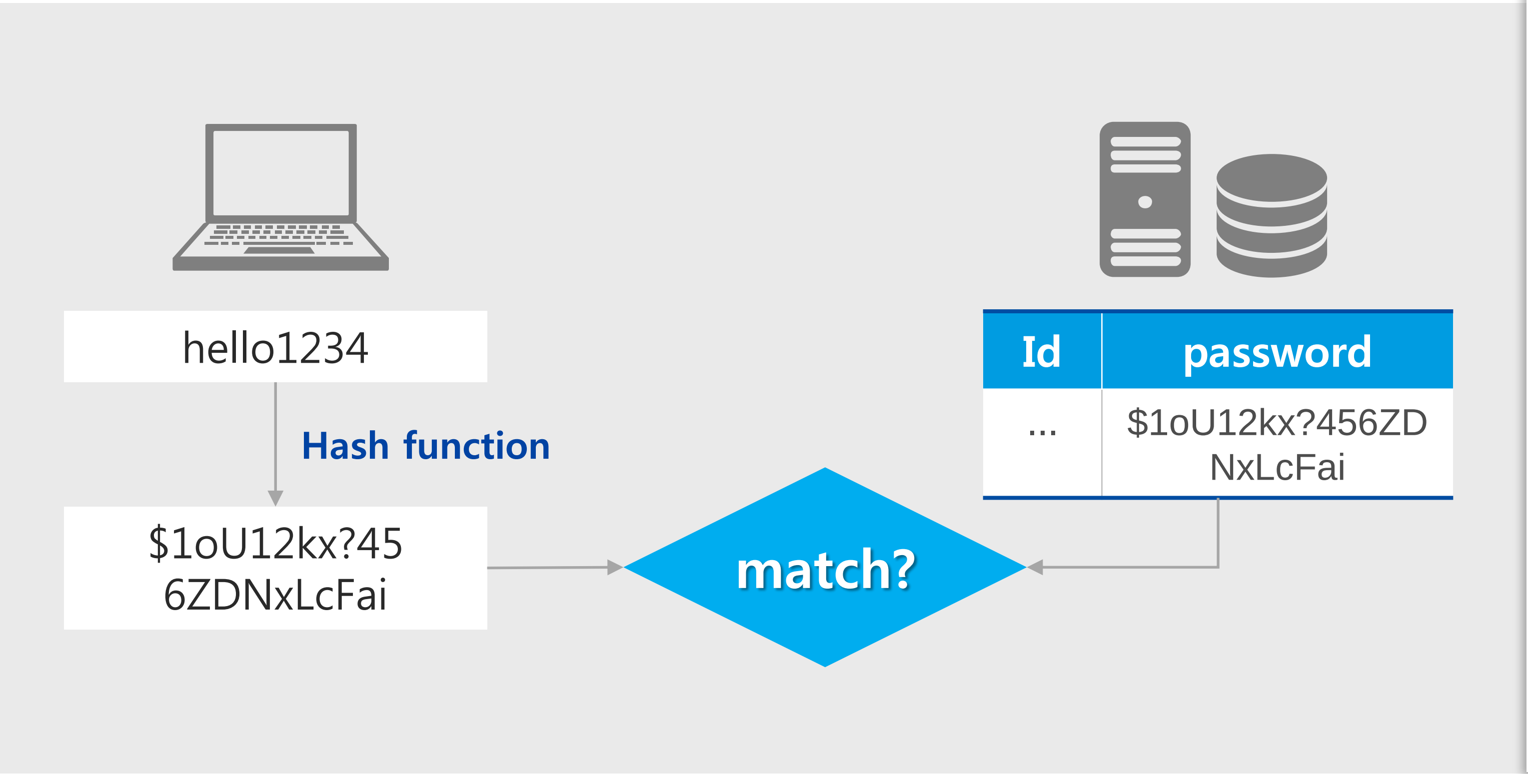
인증 방법 ❶ What you know

Password

PIN(Personal Identification Number)

인증 방법 1 What you know

- Password, PIN



Weakness

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

인증 방법 ❷ What you have

대칭키 vs. 비대칭 키

교통 카드

- 대칭키 기반

신용 카드

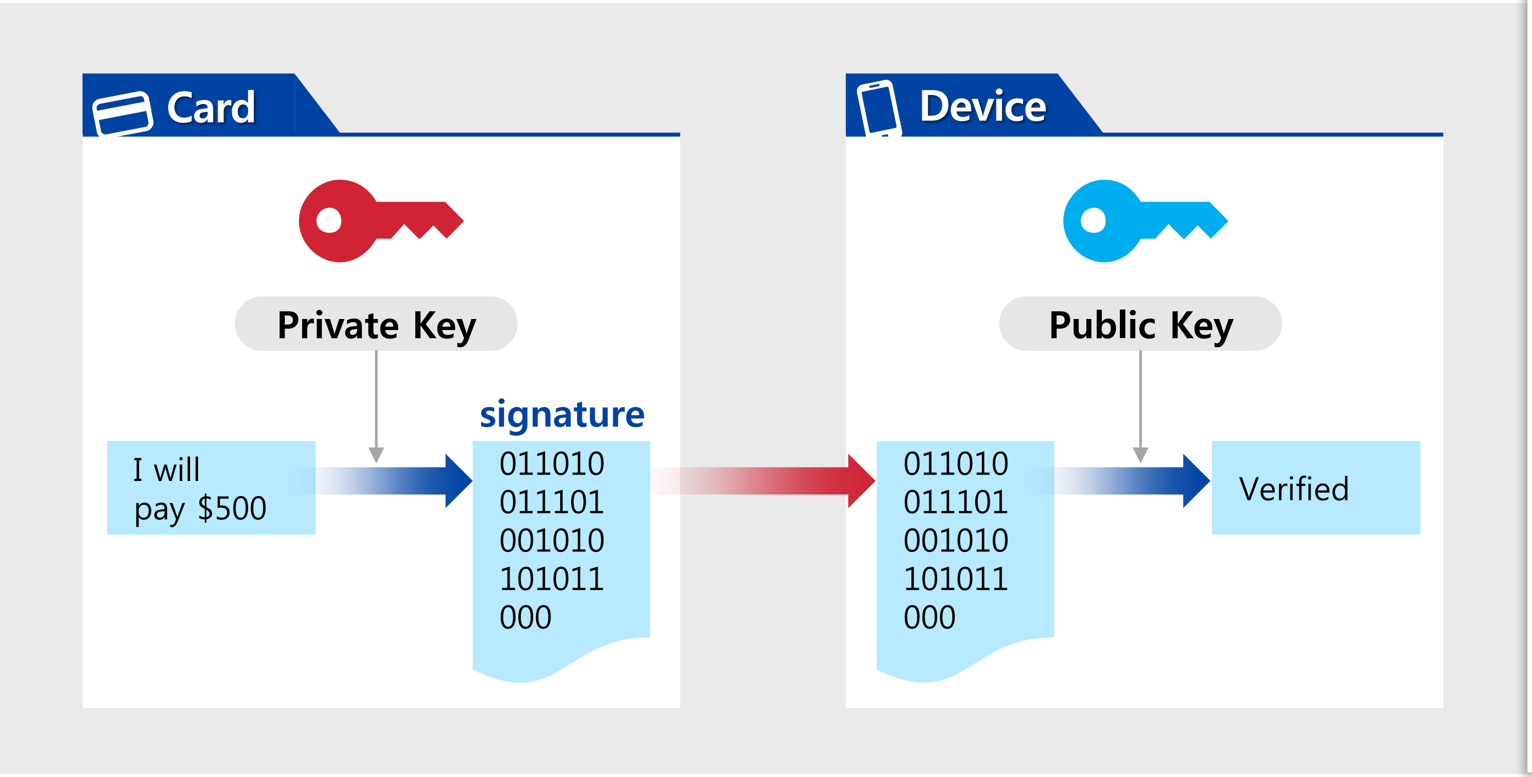
- **공개키 기반 :** 비접촉식의 경우(PKI: Public Key Infracture)

▸▸▸ contains cryptographic keys in the secure storage

인증 방법 ❷ What you have

- **신용카드 :** Secure Transaction using PKI

* Public Key Infrastructure



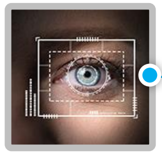
Weakness

- 분실에 의한 오용
- 복제 가능성

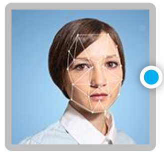
인증 방법 3 Something you are / 4 do

are (Physical Biometrics)

홍채
iris

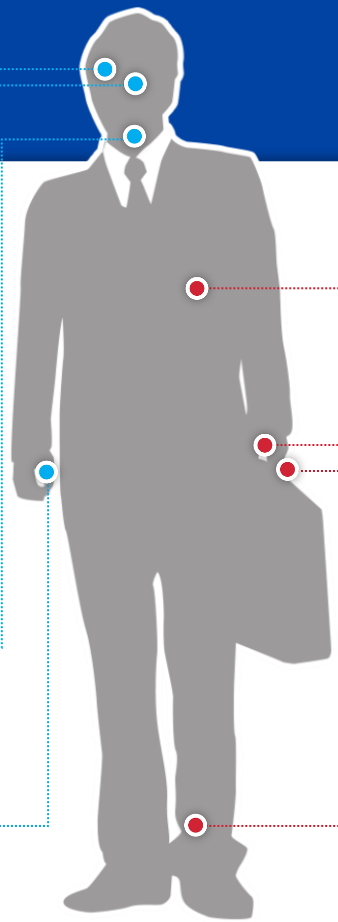


얼굴
face



목소리
voice

지문
fingerprint



do (Behavioral Biometrics)

동작
gesture

서명
signature

키보딩 습관
typing pattern

걸음걸이
walking pattern

생체인증 기술 개요

생체인식(Biometrics)기반인증이란?

홍채
iris

얼굴
face

목소리
voice

지문
fingerprint

동작
gesture

서명
signature

키보딩 습관
typing pattern

걸음걸이
walking pattern

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

뛰어난 사용편의성 …… **강력한 보안성**

보편성 **유일성** **지속성**

사용자 인증 어디까지 진화할 것인가

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-stroke, 마우스 움직임 등

Contents

SDS 생체 인증 솔루션: Nexsign

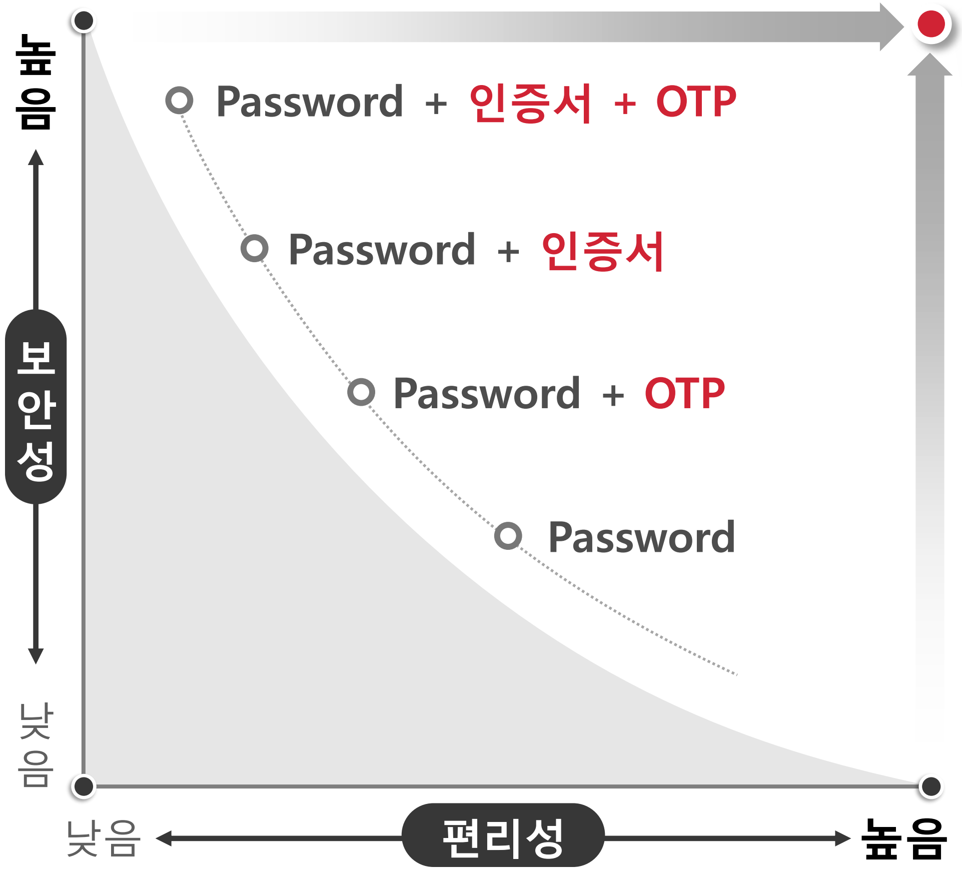
" Samsung SDS
Nexsign "

(**Nex**t generation + **Sign**ature)

※ 적용예시 : 삼성페이

지문, 얼굴, 음성 등을 이용한 **생체**인증과,
PKI(공개키 암호화) 인증이 결합된 **복합 인증**으로,
편리하면서도 보안이 강화된 혁신적인 **모바일 보안 솔루션**

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
- 생체정보, 암호화 키는 외부로 누출되지 않고, 단말 내 보안공간에 안전하게 보관
- 해킹 방지를 위한 서버↔스마트폰까지 보안채널 지원

핵심기술

* Public Key Infrastructure

- 공개키 암호화 방식(PKI)의 인증체계기반 서버 인증
- 스마트폰 보안공간 (TEE, Secure Element 等) 활용 해킹 방지

* Trusted Execution Environment

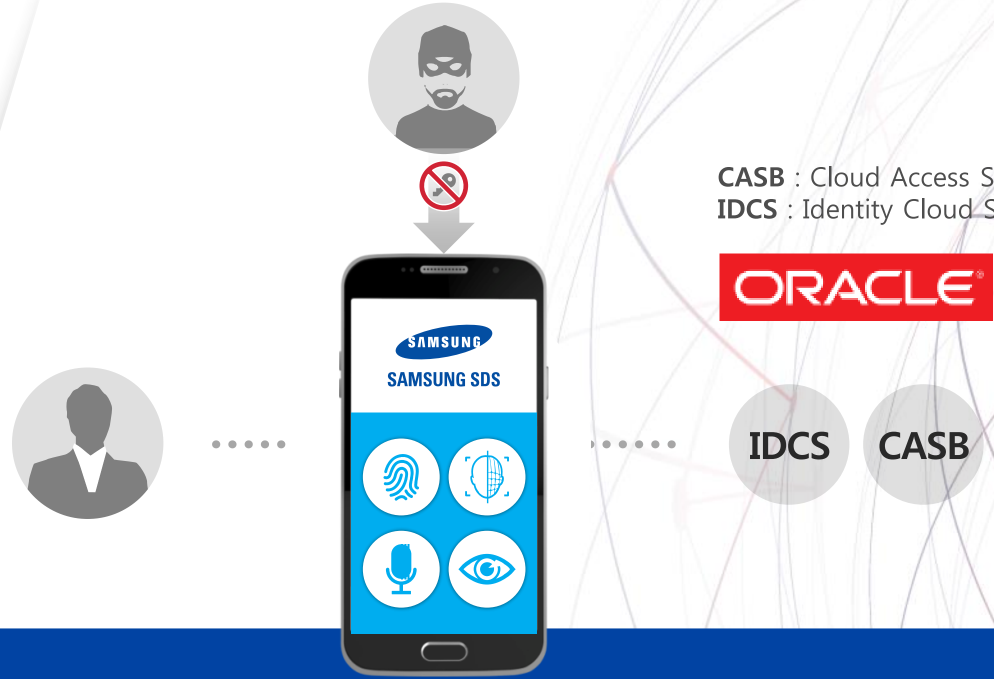
Nexsign 활용 분야

Contents

통합 Offering

SAMSUNG SAMSUNG SDS & ORACLE

Scalable · Secure · Simple · Fast

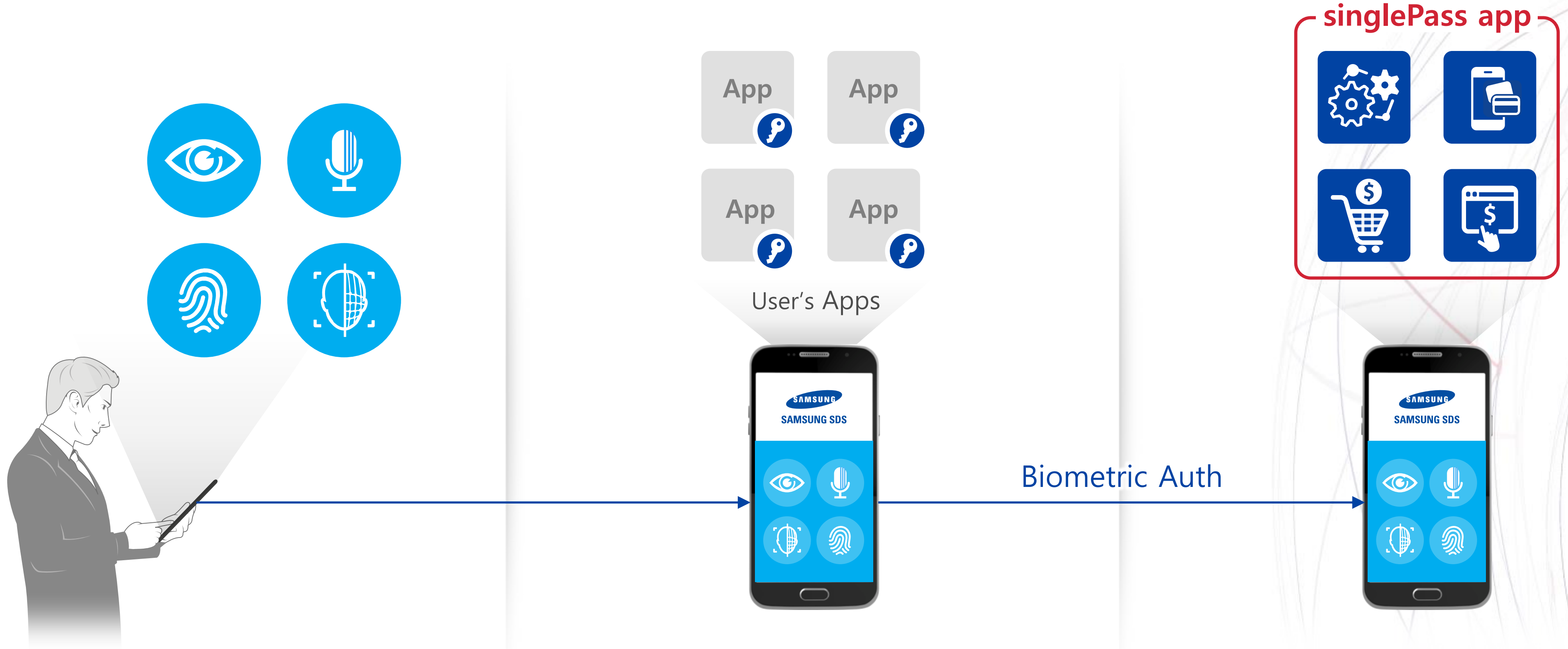


CASB : Cloud Access Security Brokers
IDCS : Identity Cloud Service

Front-End Authentication with multi-modality **BY SAMSUNG**

Back-End Authentication with adaptive access **BY ORACLE**

Nexsing기반 Single Sign On



1 Nexsign 로그인
(생체인증 기반)

2 Identity Federation Registration
(Oracle Access Portal)

3 Password-less Nexsign을
통한 통합 앱 접근

Customer Value

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

Time for Password Crack

Brute Force Calculator

Password Length	6
Keys per second	Raw SHA-256 - (2600K k/s)
Charset [len:62]	mixalpha-numeric
	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
	Get Time

To brute force the entire keyspace it will take about

6 hours 10 minutes 4 seconds

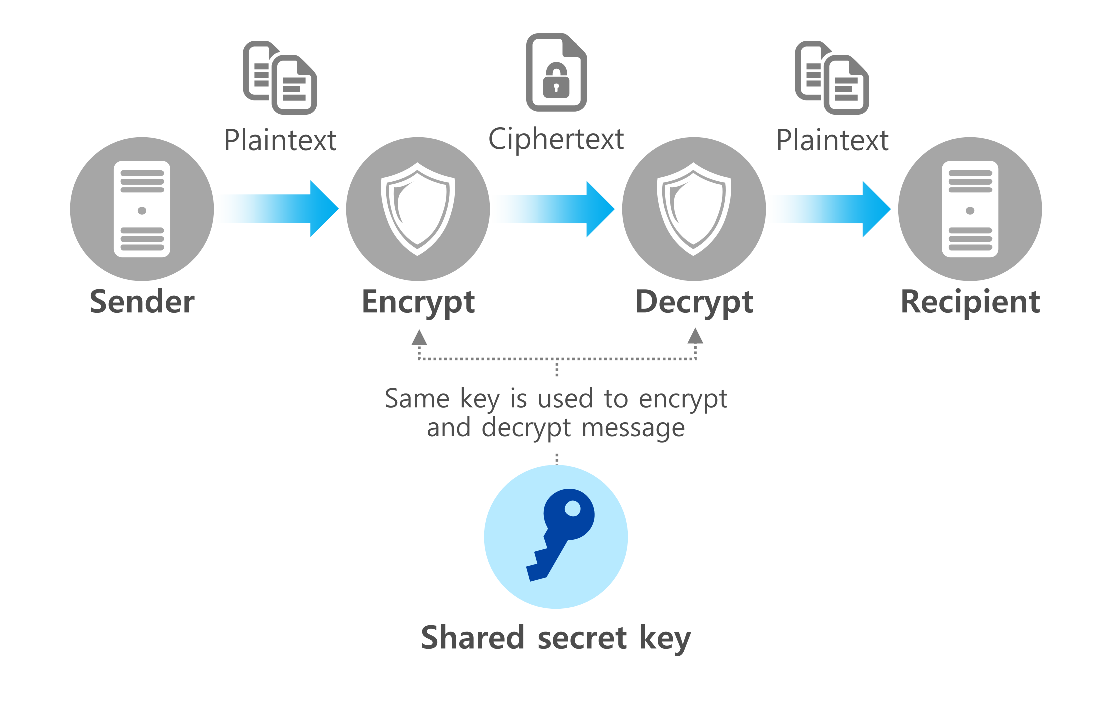
(57731386986 password combinations)

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

별첨

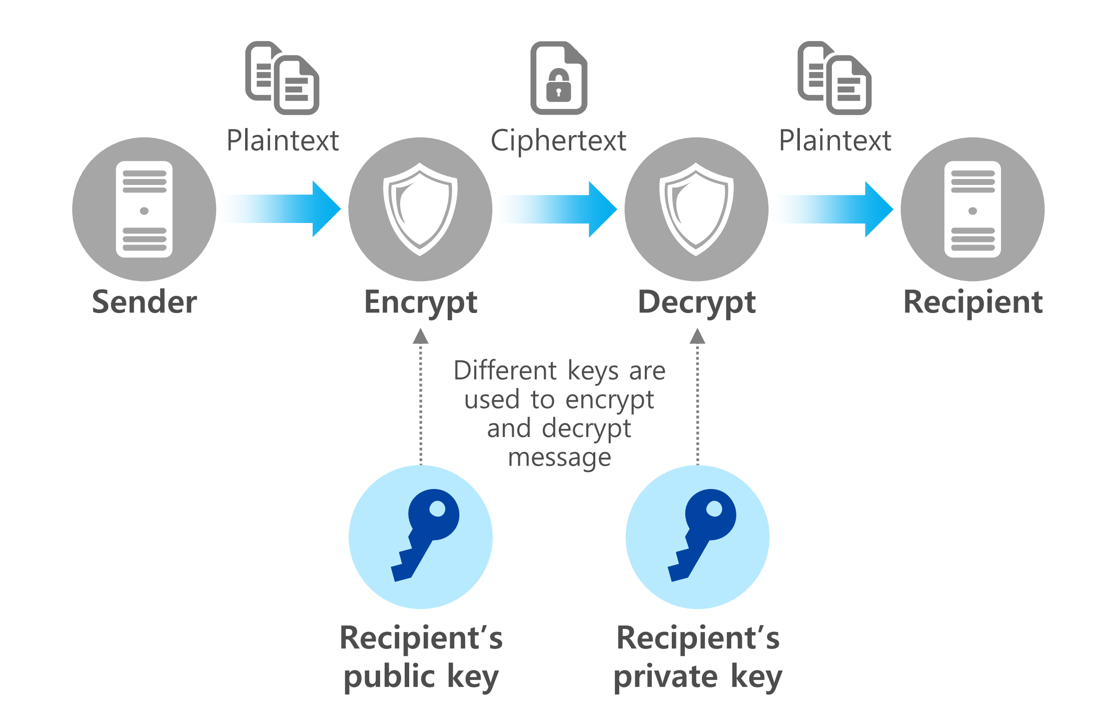
대칭 키 vs. 비대칭 키

대칭 키



- ☑ 치환, 전치
- ☑ DES, AES (SEED, ARIA)
- ☑ 사용 : 암호화/복호화

비 대칭 키



- ☑ 수학
- ☑ RSA, ECC
- ☑ 사용 : 서명/검증

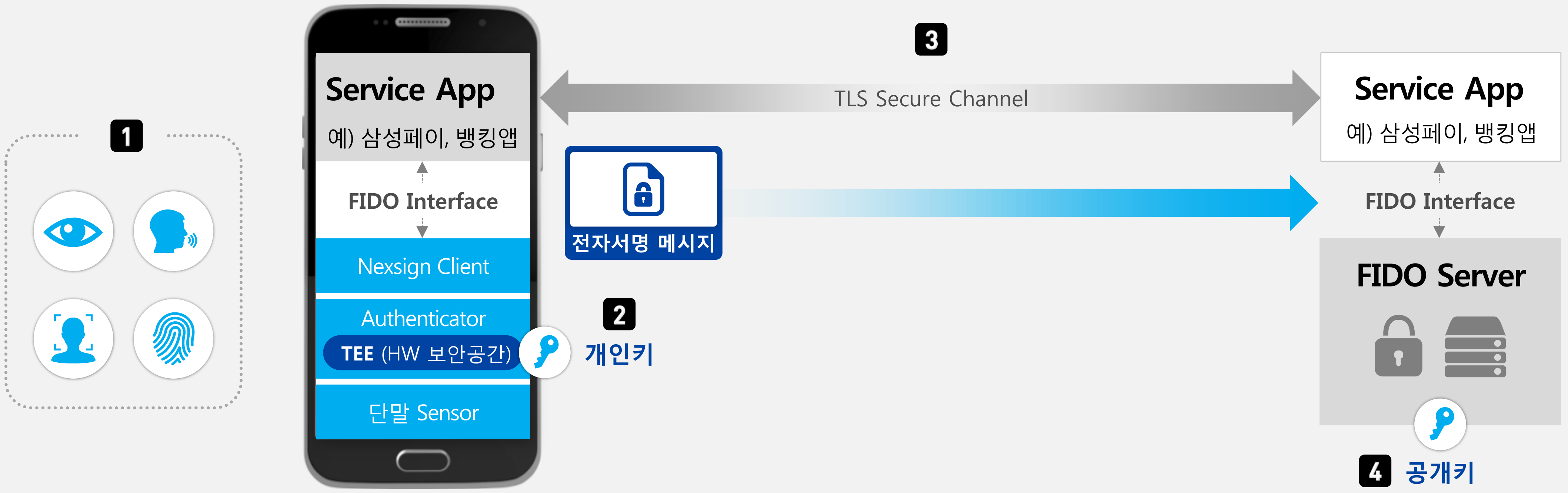
Nexsign 동작 상세

1 디바이스에 전달되는 사용자 **생체정보**와 디바이스내 보관된 생체정보 매칭

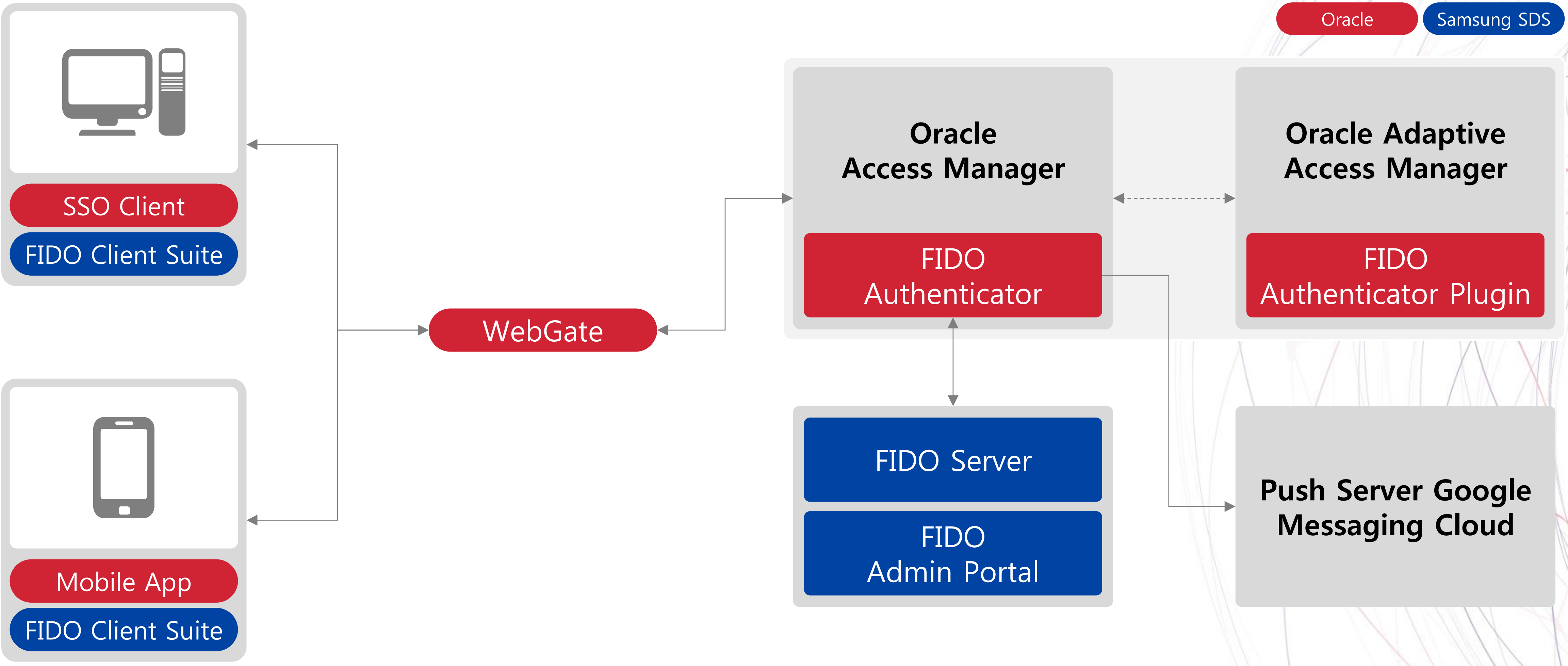
2 매칭되면 디바이스내 보관되어 있던, **개인키** 이용 서명

3 서명정보가 **TLS** 보안채널 통해 서버에 전달

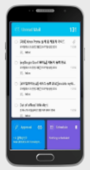
4 FIDO서버에 보관되어 있는 사용자 **공개키**로, 보내진 서명정보 검증



SSO : Concept Diagram



Nexsign differentiation

국내·외 기술력 입증	FIDO Alliance의 국제 표준 규격 및 최고 수준의 **국제 보안 인증 획득(CC인증)** 국내·외 권위 있는 **IT 상 수상**	'17. 2月 **Glomo Award- Best Mobile Security 수상** '15.10月 **K-ICT 대상 수상** '15. 9月 **세계 최초 CC* 획득** *Common Criteria '15. 5月 **국내 최초 FIDO Certified™ 획득** 
시장 검증 완료	대규모 금융 서비스 대상 **생체인증 적용** 기업/정부의 높은 **보안 레벨 충족**	 삼성페이 ('15.8月)  K-Bank ('17.4月)  Knox Portal Mobile ('15.7月)
삼성전 Device + SDS 솔루션 결합 시너지	HW보안+SW보안 결합으로 최고 수준의 **모바일 보안 환경 제공**	 Galaxy S7  Galaxy Note5 + Knox Workspace: SDS Secure Doc. / SDS EMM / SDS Nexsign ※ 적용 사례: 싱가포르 국방부 산하 과학 기술국('16.9月)

End of Document

Nexsign with Oracle IAM

박희진
삼성SDS

SAMSUNG SDS ORACLE

제5회 SAMSUNG ORACLE
Insight Forum
Breakthrough to the Next Stage

Contents

왜 사용자 인증이 필요한가?

Offline

Online

왜 사용자 인증이 필요한가?

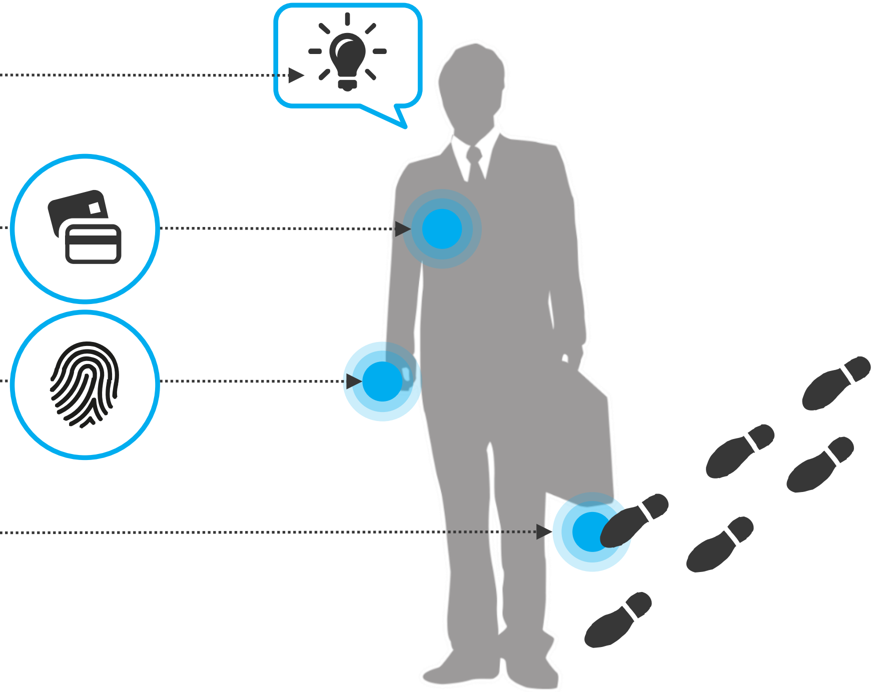
Who is he/she ?

불특정 다수

비 대면

사용자 인증 방법

1. Something you **know** 지식
2. Something 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

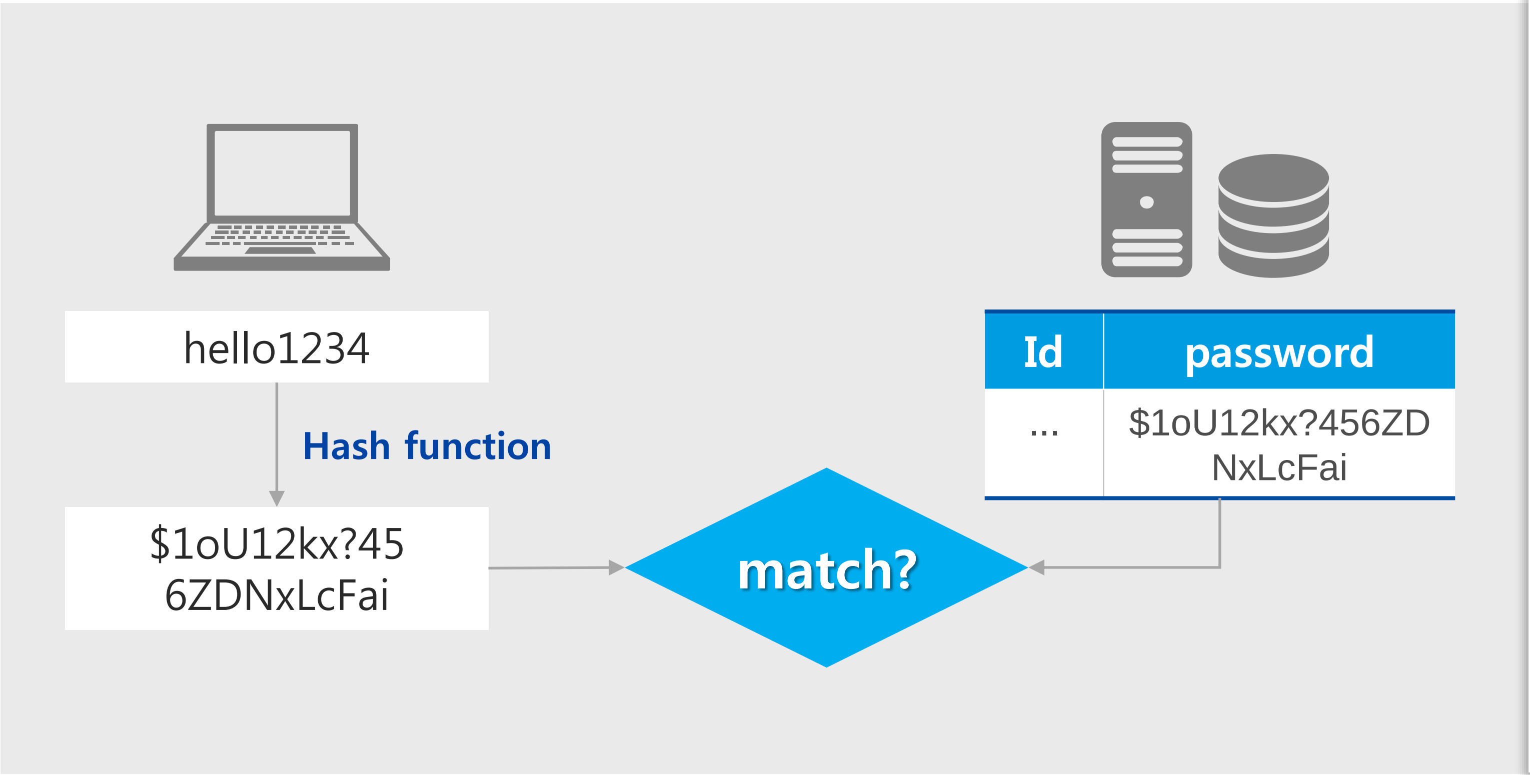
인증 방법 1 What you know

Password

PIN(Personal Identification Number)

인증 방법 1 What you know

- Password, PIN



Id	password
…	$1oU12kx?456ZD NxLcFai

Weakness

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

인증 방법 ❷ What you have

대칭키 vs. 비대칭 키

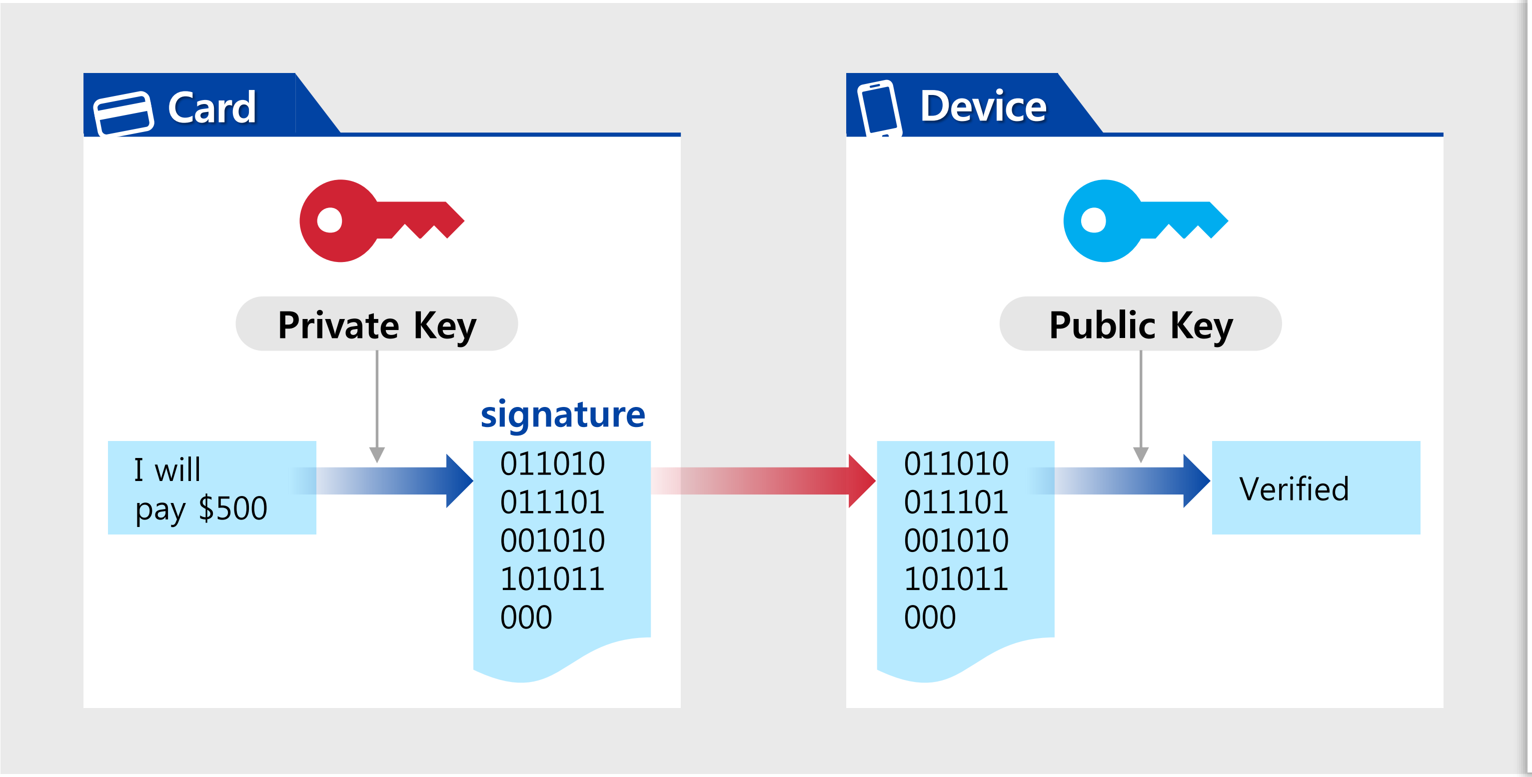
교통 카드	신용 카드
대칭키 기반	**공개키 기반 :** 비접촉식의 경우(PKI: Public Key Infracture)

▸▸▸ contains **cryptographic keys** in the secure storage

인증 방법 ❷ What you have

- **신용카드 :** Secure Transaction using PKI

* Public Key Infrastructure



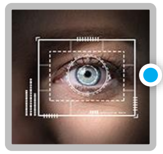
Weakness

- 분실에 의한 오용
- 복제 가능성

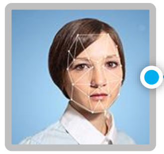
인증 방법 3 Something you are / 4 do

are (Physical Biometrics)

홍채
iris

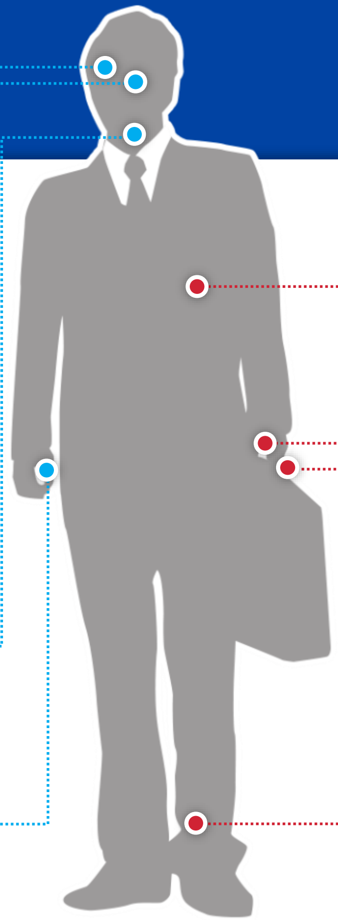


얼굴
face



목소리
voice

지문
fingerprint



do (Behavioral Biometrics)

동작
gesture

서명
signature

키보딩 습관
typing pattern

걸음걸이
walking pattern

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**

사용자 인증 어디까지 진화할 것인가

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 (Something you Know)	ID+PW, PIN
소유기반 (Something you Have)	교통카드, 신용카드
특성기반 (Something you Are)	생체인증 (지문, 홍채, 망막, 손금, 얼굴, 정맥, 목소리, 심장박동 등)
행동기반 (Something you Do)	말투, 걸음걸이, 서명, Key-stroke, 마우스 움직임 등

Contents

SDS 생체 인증 솔루션: Nexsign

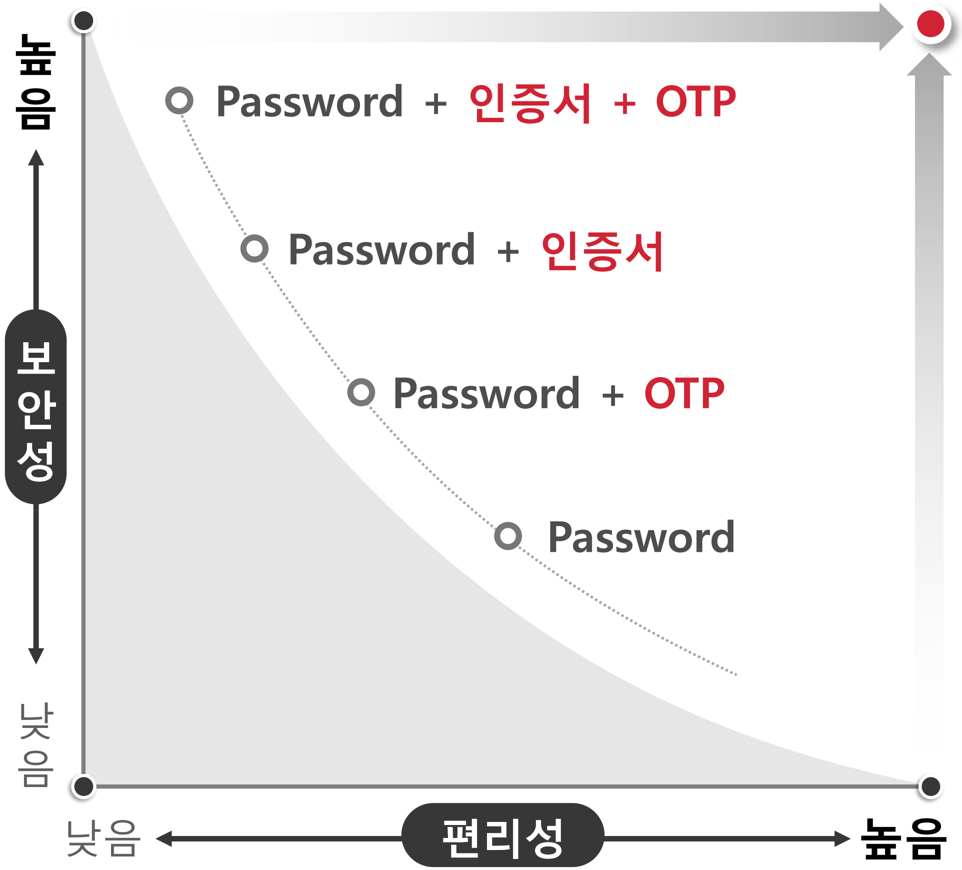
“ Samsung SDS
Nexsign ”

(**Nex**t generation + **Sign**ature)

※ 적용예시 : 삼성페이

지문, 얼굴, 음성 등을 이용한 **생체**인증과,
PKI(공개키 암호화) 인증이 결합된 **복합 인증**으로,
편리하면서도 보안이 강화된 혁신적인 **모바일 보안 솔루션**

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
- 생체정보, 암호화 키는 외부로 누출되지 않고, 단말 내 보안공간에 안전하게 보관
- 해킹 방지를 위한 서버↔스마트폰까지 보안채널 지원

핵심기술

- 공개키 암호화 방식(PKI)의 인증체계기반 서버 인증
- 스마트폰 보안공간 (TEE, Secure Element 等) 활용 해킹 방지

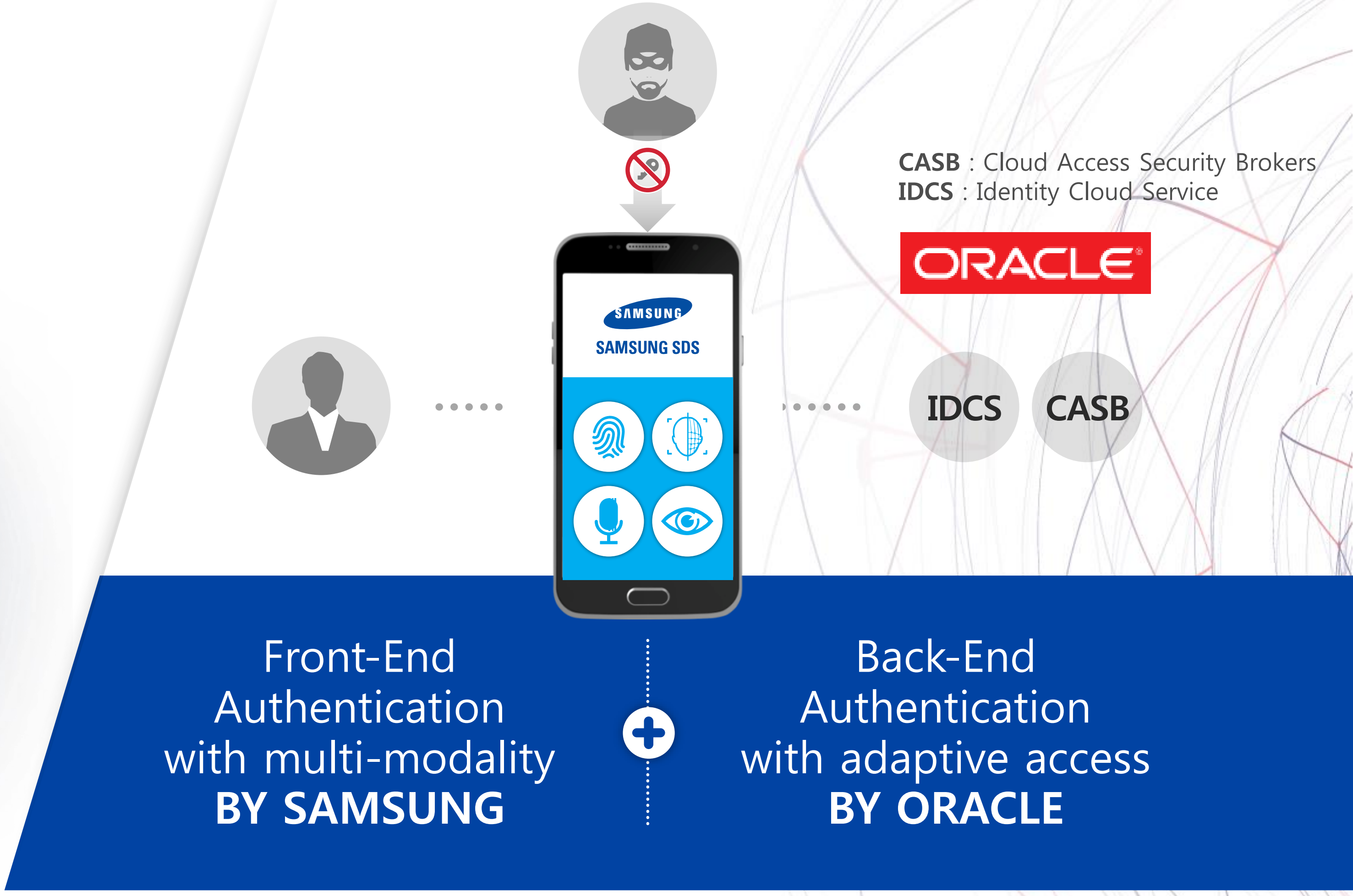
* Public Key Infrastructure
* Trusted Execution Environment

Nexsign 활용 분야

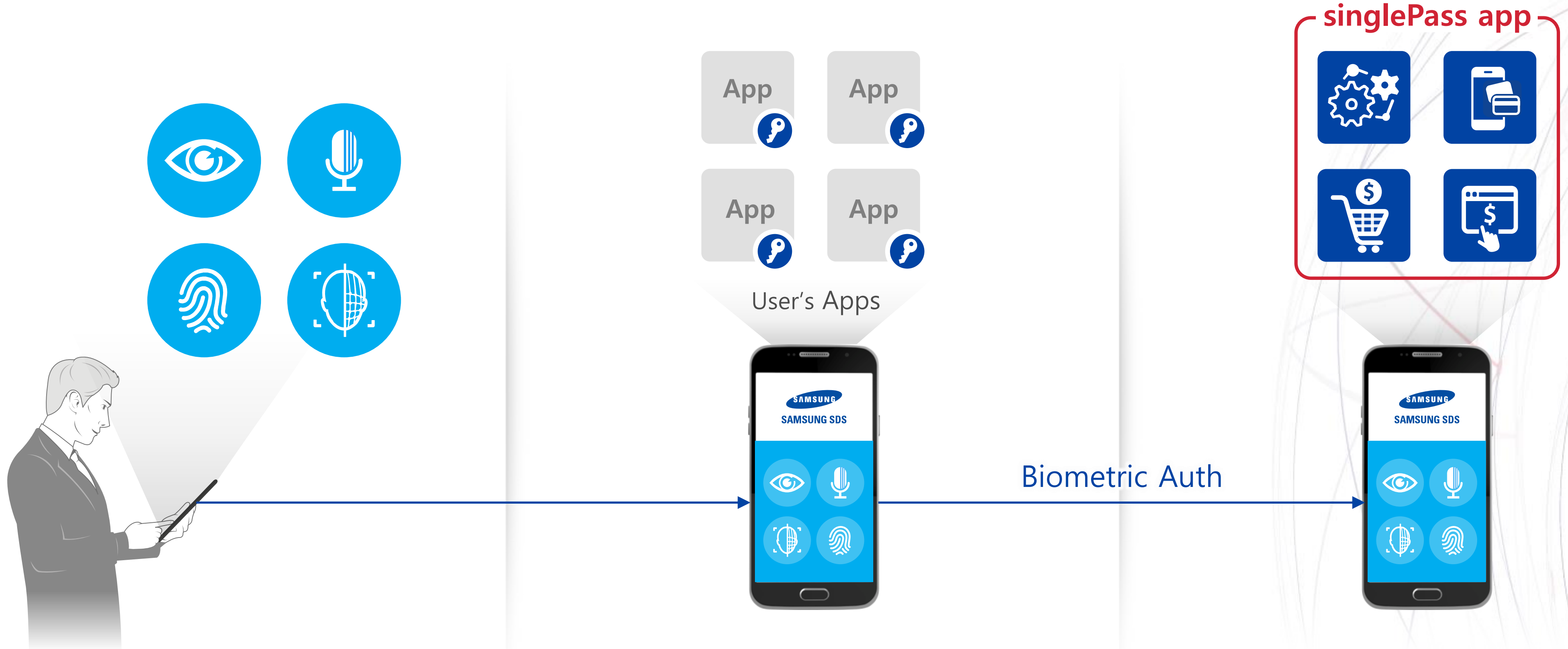
Contents

통합 Offering


SAMSUNG
SAMSUNG SDS
&
ORACLE
Scalable
Secure
Simple
Fast


SAMSUNG
SAMSUNG SDS
CASB : Cloud Access Security Brokers
IDCS : Identity Cloud Service
ORACLE
IDCS
CASB
Front-End Authentication with multi-modality BY SAMSUNG
Back-End Authentication with adaptive access BY ORACLE

Nexsing기반 Single Sign On



1 Nexsign 로그인
(생체인증 기반)

2 Identity Federation Registration
(Oracle Access Portal)

3 Password-less Nexsign을
통한 통합 앱 접근

Customer Value

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

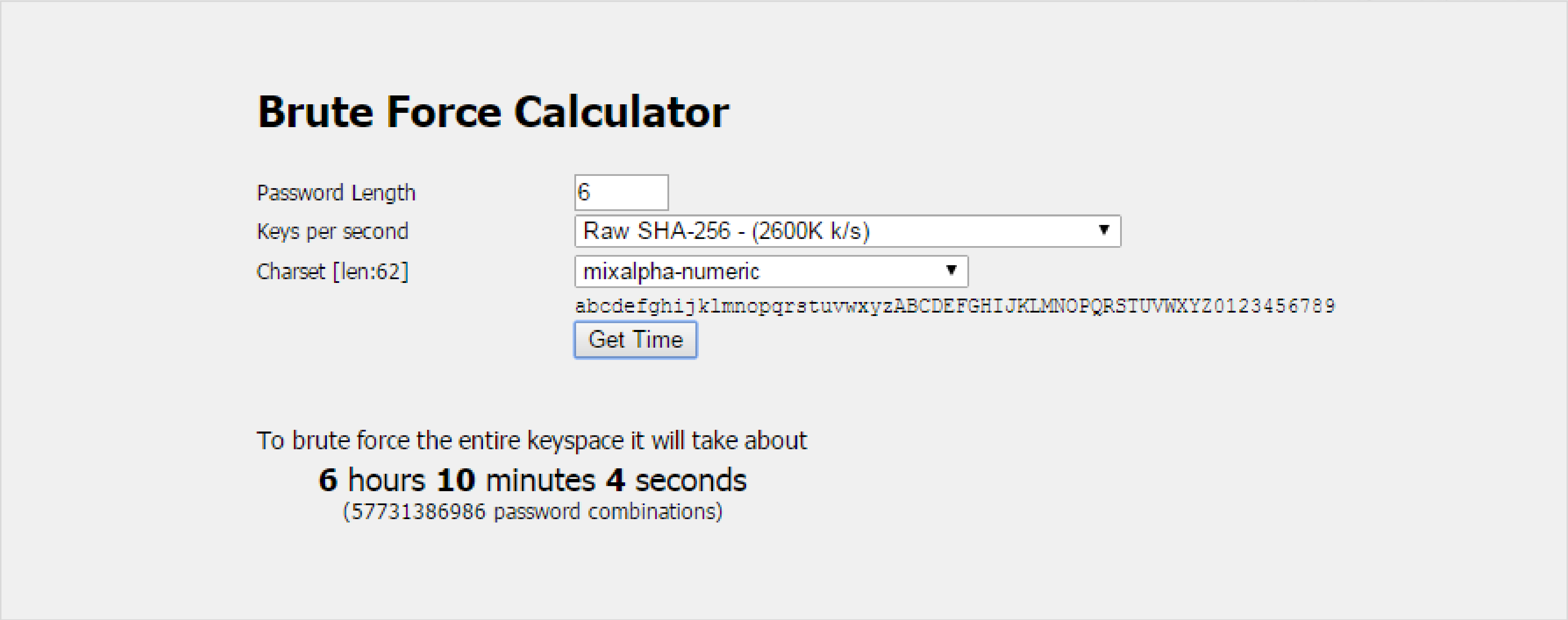
- 안전하고 편리한 모바일 중심의 업무 환경 구축 지원
- 모바일기반 현장완결型 서비스 제공으로 업무 생산성 및 고객 만족도 제고

03 서비스 보안 강화 Cost Saving

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

별첨

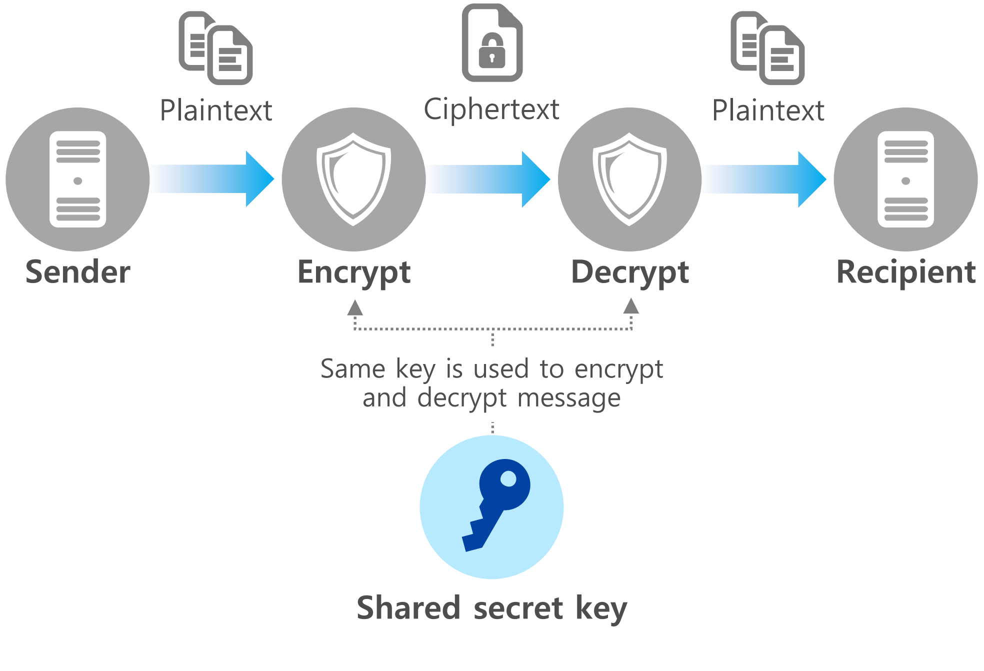
Time for Password Crack



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

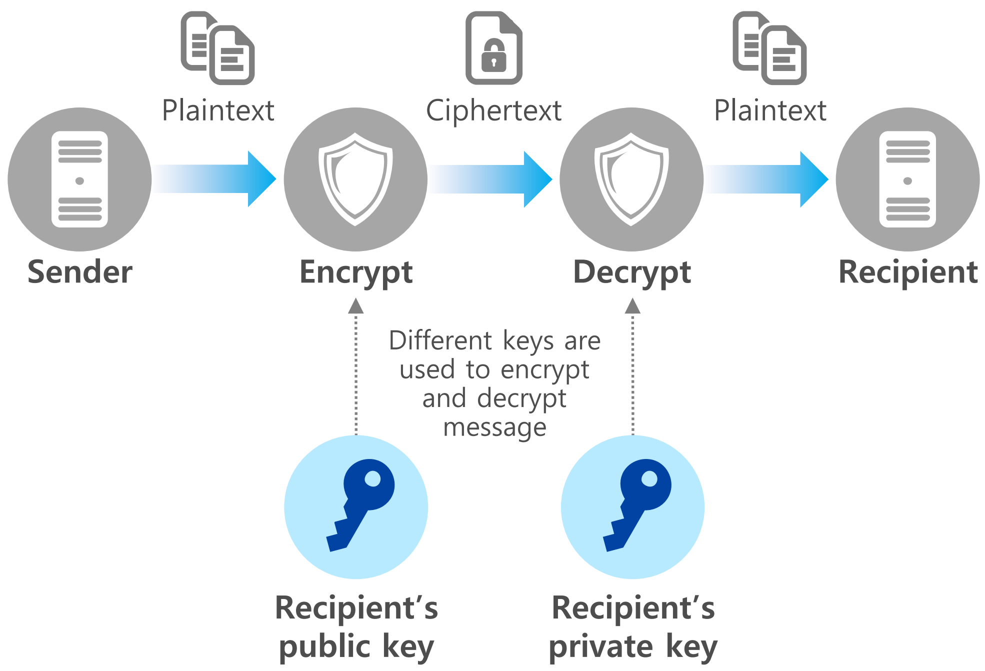
대칭 키 vs. 비대칭 키

대칭 키



- ☑ 치환, 전치
- ☑ DES, AES (SEED, ARIA)
- ☑ 사용 : 암호화/복호화

비 대칭 키



- ☑ 수학
- ☑ RSA, ECC
- ☑ 사용 : 서명/검증

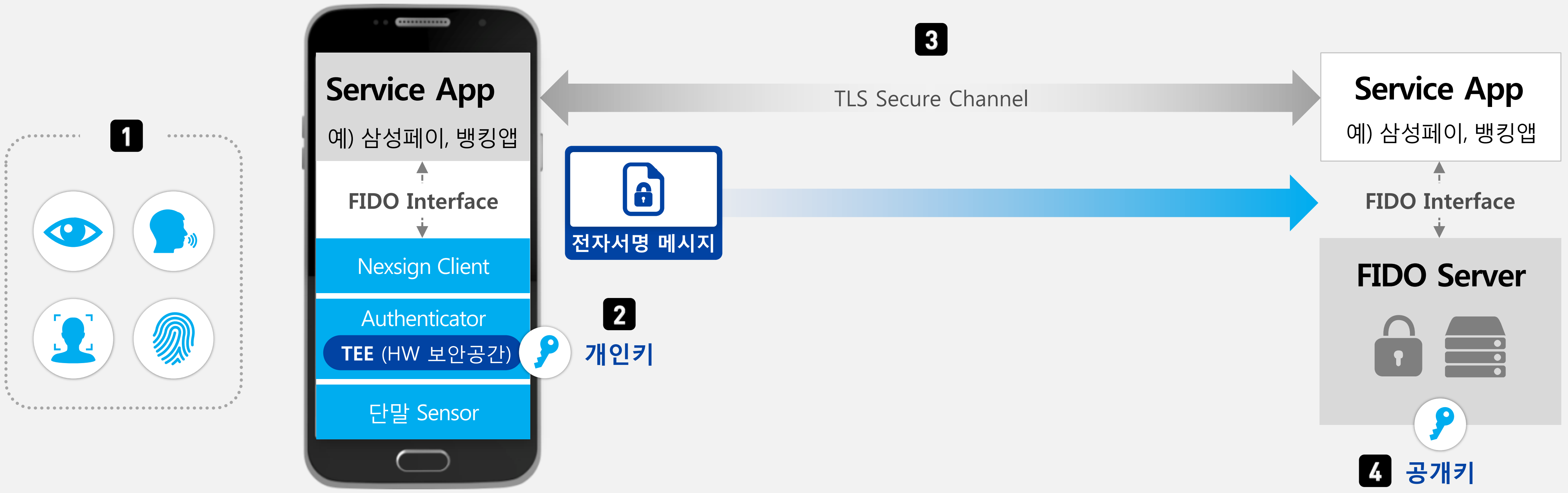
Nexsign 동작 상세

1 디바이스에 전달되는 사용자 **생체정보**와 디바이스내 보관된 생체정보 매칭

2 매칭되면 디바이스내 보관되어 있던, **개인키** 이용 서명

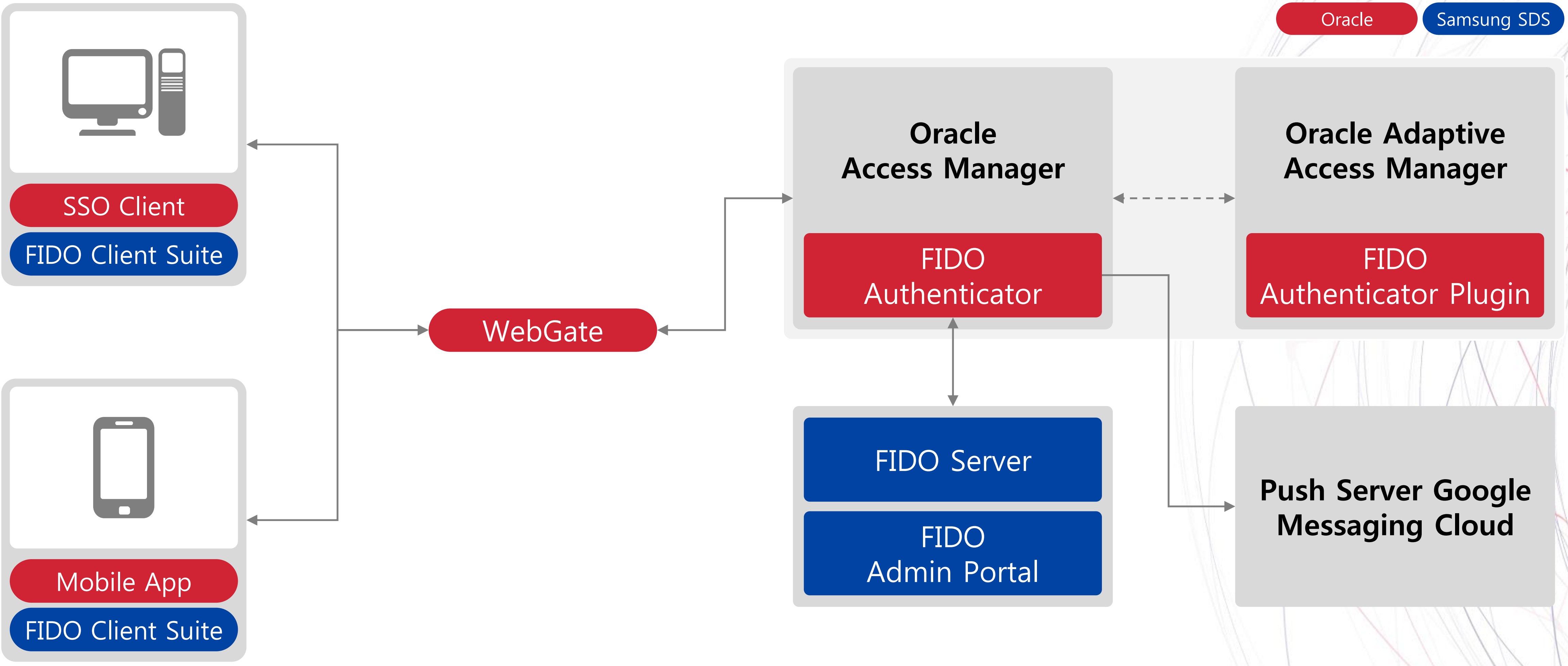
3 서명정보가 **TLS** 보안채널 통해 서버에 전달

4 FIDO서버에 보관되어 있는 사용자 **공개키**로, 보내진 서명정보 검증

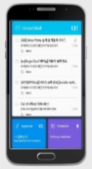


별첨

SSO : Concept Diagram



Nexsign differentiation

국내·외 기술력 입증	FIDO Alliance의 국제 표준 규격 및 최고 수준의 **국제 보안 인증 획득(CC인증)** 국내·외 권위 있는 **IT 상 수상**	'17. 2月 Glomo Award- Best Mobile Security 수상 '15.10月 K-ICT 대상 수상 '15. 9月 세계 최초 CC* 획득 *Common Criteria '15. 5月 국내 최초 FIDO Certified™ 획득 
시장 검증 완료	대규모 금융 서비스 대상 **생체인증 적용** 기업/정부의 높은 **보안 레벨 충족**	 삼성페이 ('15.8月)  K-Bank ('17.4月)  Knox Portal Mobile ('15.7月)
삼성전 Device + SDS 솔루션 결합 시너지	HW보안+SW보안 결합으로 최고 수준의 **모바일 보안 환경 제공**	 Galaxy S7  Galaxy Note5 + Knox Workspace: SDS Secure Doc. / SDS EMM / SDS Nexsign ※ 적용 사례: 싱가포르 국방부 산하 과학 기술국('16.9月)

End of Document