

무인증서 공개키 시스템

정보보호이론 13장

2015.06.02

Contents

- ❖ **Introduction**
- ❖ **IBC(Identity-based Cryptography)**
 - ◆ HIBE(Hierarchical Identity-based encryption)
- ❖ **CLC(Certificateless Cryptography)**
- ❖ **Attribute-based Cryptography**
- ❖ **Conclusion**

Introduction

❖ PKI 인증서 관련 보안 사고

2014

- 악성코드에 의해 약 7천 개의 인증서가 해외로 유출됨

2011

- 이란 출신 해커에 의해 Comodo 인증기관(CA)의 거짓 인증서가 발급됨
- 네덜란드 최상위 인증기관인 DigNotar가 공격받아 Google 도메인에 대한 약 500개의 거짓 인증서가 부정 발급됨
- GloabalSign 인증기관이 공격받아 인증서 신규발급을 중지함
- 이란 원자력 시설을 파괴한 Stuxnet은 대만회사의 인증서를 위조하여 정식 소프트웨어로 위장함

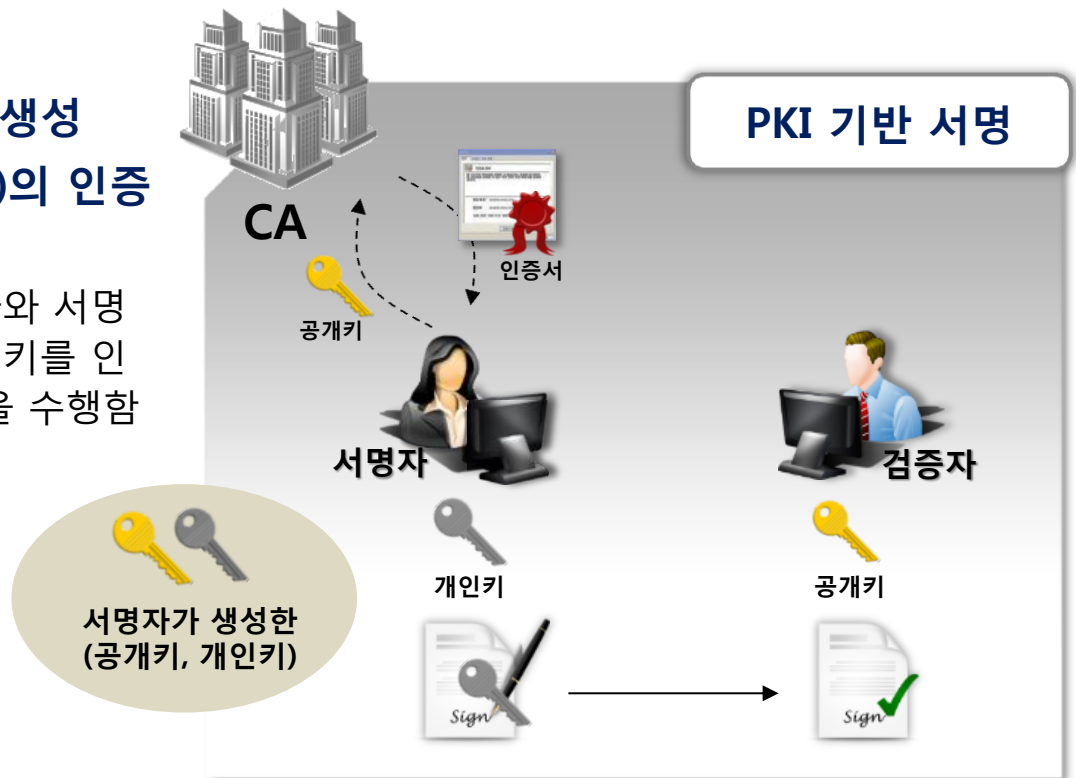


Introduction

❖ PKI(public key infrastructure)

- ◆ 공개키 기반 암호 시스템은 사용자가 생성하는 공개키/개인키 쌍을 이용하여 암호 및 서명을 수행
- ◆ 이때, 공개키는 난수로 구성되어 누구의 키인지 확인하기 어려움 → 신뢰기관 필요
 - ex) RSA 암호의 공개키 ($e, n=pq$)의 임의의 숫자로 구성됨

- ◆ 사용자가 공개키/개인키 쌍을 생성
- ◆ 공개키에 대하여 신뢰기관(CA)의 인증을 받아 인증서를 발급받음
 - 암호에서 암호화를 하는 사용자와 서명에서의 검증자는 상대방의 공개키를 인증서를 통해 검증한 뒤에 연산을 수행함

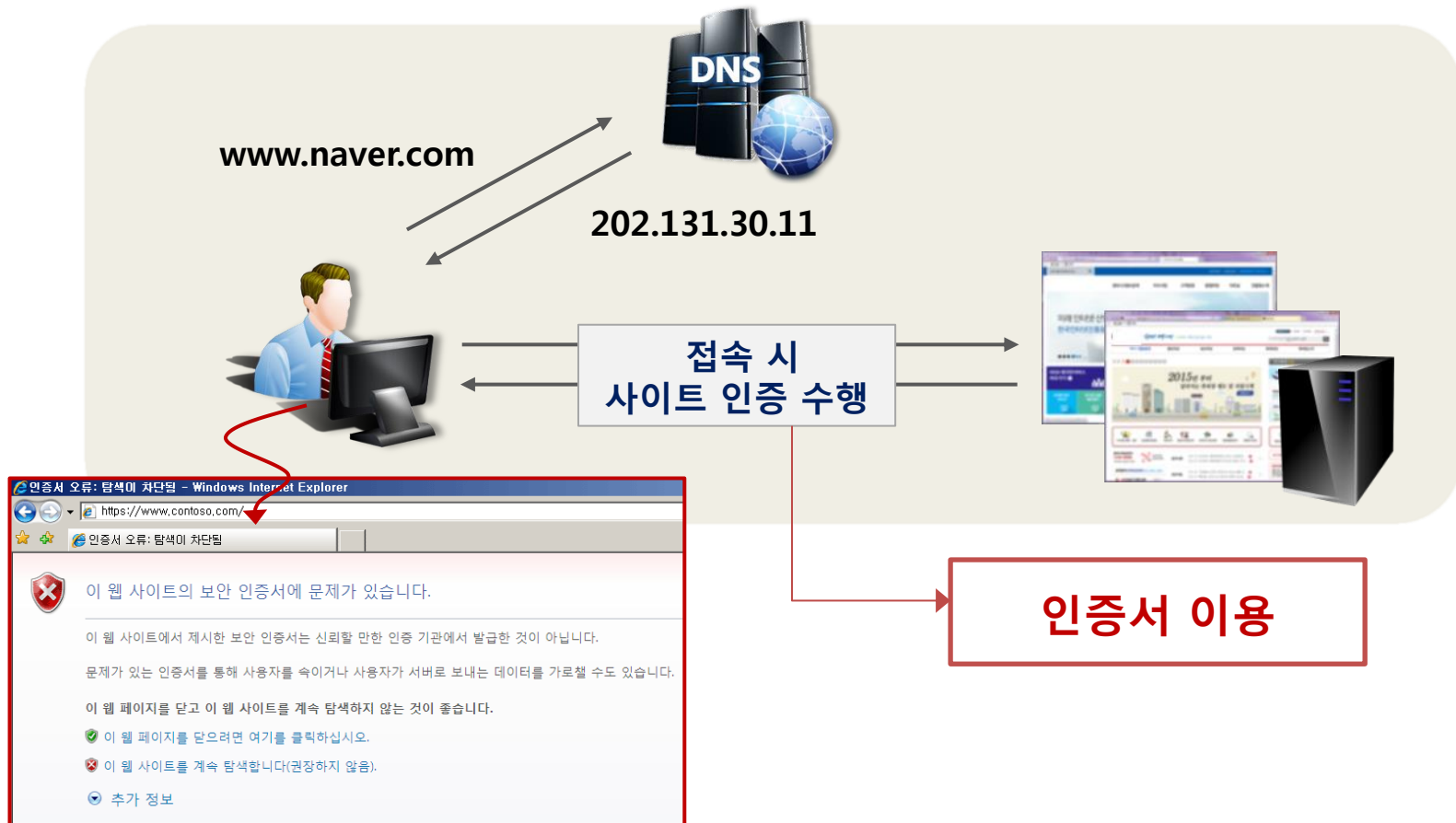


Introduction

❖ PKI Application

◆ PKI 기반 DNS(Domain Name System) 서버 인증

- 사용자가 사이트에 접속할 때, DNS 서버로부터 사이트의 IP 주소를 받아옴
- 이때, 사이트의 인증서를 이용하여 사이트 인증 수행

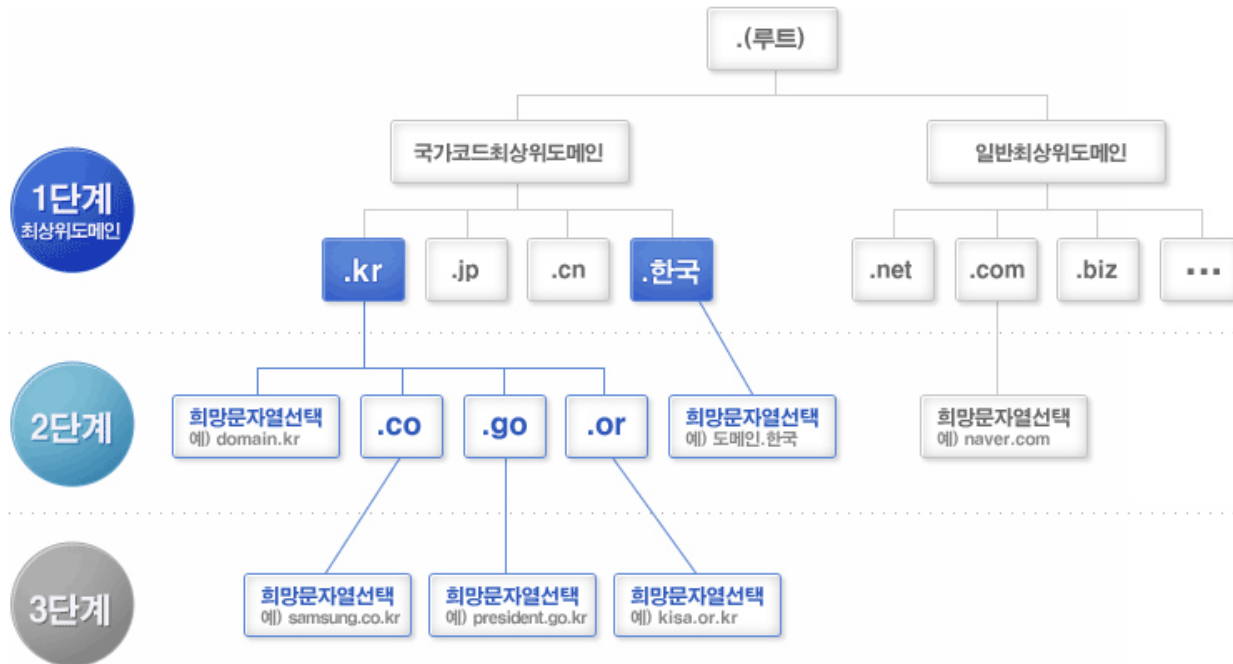


Introduction

❖ PKI Application

◆ DNS(Domain Name System)

- 도메인이나 호스트 이름을 숫자로 된 IP주소로 해석해주는 TCP/IP 네트워크 서비스
- 특정 컴퓨터(또는 네트워크로 연결된 임의의 장치)의 주소를 찾기 위해, 사람이 이해하기 쉬운 도메인 이름을 숫자로 된 식별 번호(IP 주소)로 변환
 - DNS는 .루트(root) 도메인 하에 계층적 트리 구조로 구성되어 있음
 - 루트 도메인 바로 아래 단계가 1단계 도메인 또는 최상위 도메인(TLD, Top Level Domain)
 - 최상위 도메인은 크게 두 가지로 분류: 국가 최상위 도메인(ccTLD), 일반 최상위 도메인(gTLD)



Introduction

❖ PKI의 한계점



- 서비스 이용을 위해 설치하는 플러그인은 **보안 위협을 증가**시킴
- 주기적인 인증서 갱신작업은 사용자 **편의성을 저**해함
- CA는 인증서 폐기목록(CRL) 관리를 위해 **많은 비용을 소**모함

➔ **무인증서 기반 인증 기술이 필요함**

인증서 관리 및 검증 문제

인증기관 권한 문제

저성능 기기 적용 문제

Introduction

❖ PKI의 한계점



- 인증기관은 사용자의 공개키에 대한 인증서를 발급할 수 있는 **막강한 권한**을 가지고 있음
- 인증기관이 공격 당할 경우, 해커는 가짜 인증서를 발급하여 피싱(phishing) 공격에 활용할 수 있음

➔ **신뢰기관의 권한을 제한할 수 있어야 함**

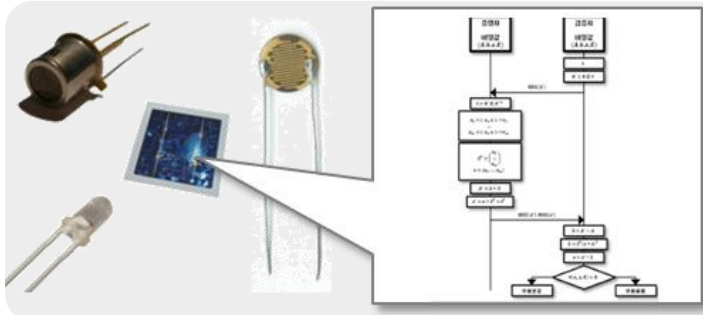
인증서 관리 및 검증 문제

인증기관 권한 문제

저성능 기기 적용 문제

Introduction

❖ PKI의 한계점



- 인증서 폐기 여부 검증과 같은 부가적인 연산은 저성능 기기가 수행하기에 부적합함
- 통신 연결이 간헐적인 극한 환경에서, 만료된 인증서를 적시에 갱신 하는 것이 불가능함

➔ 저성능 기기를 위한 인증기술 경량화가 필요함

인증서 관리 및 검증 문제

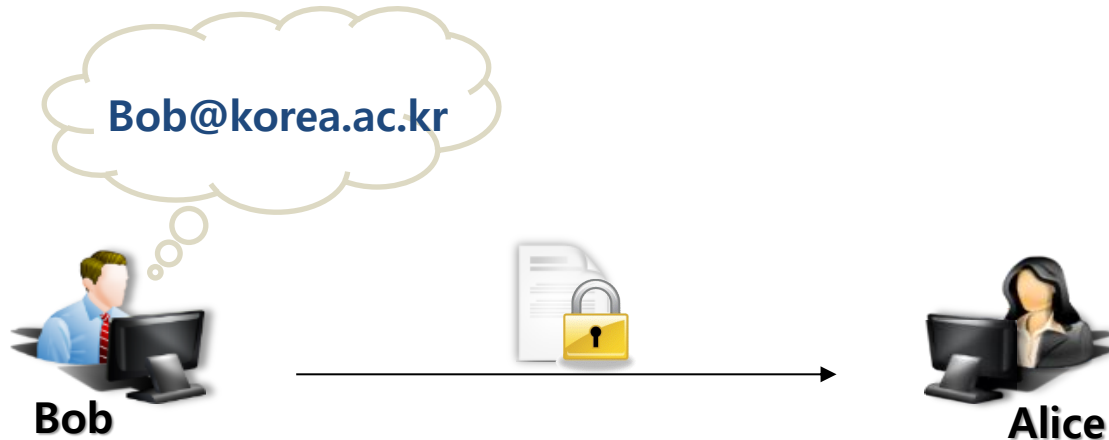
인증기관 권한 문제

저성능 기기 적용 문제

Introduction

❖ Alternative to PKI

- ◆ 시스템에 참여하는 개체는 이메일 주소, IP 번호, 기기 일련번호와 같이 일대일로 대응되는 고유한 식별자(ID)를 가지고 있음
- ◆ ID의 고유성에 의하여 별도의 인증서 없이 공개키(ID)와 개체 간 연관관계를 형성할 수 있음

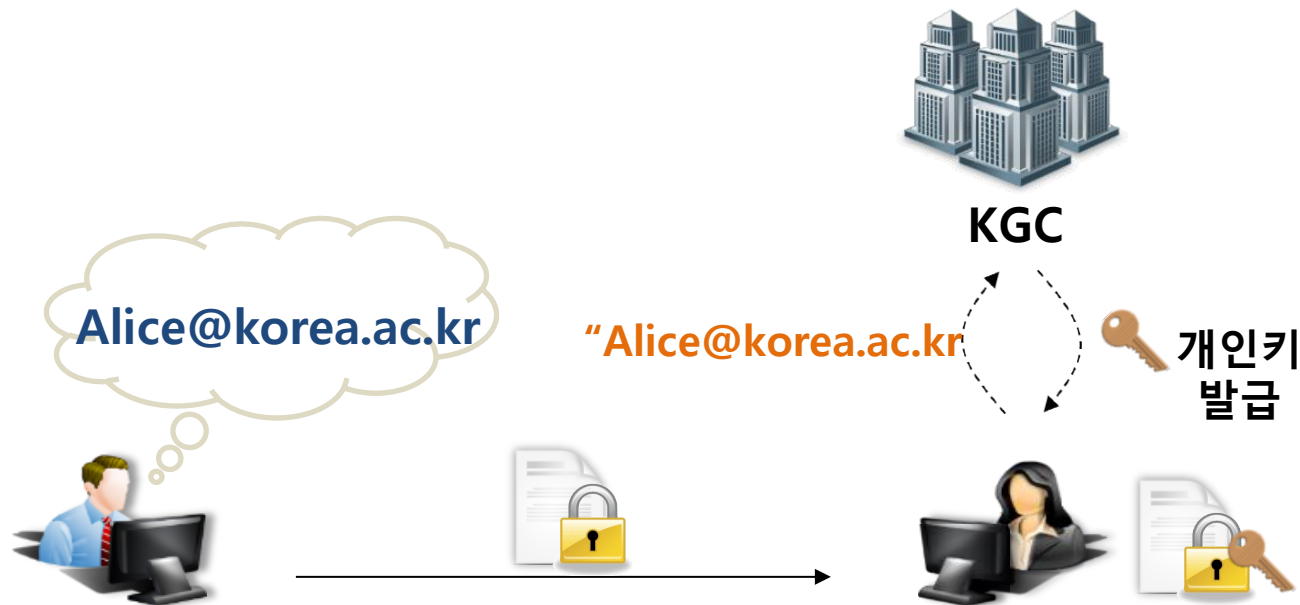


- ◆ **ID 기반 암호 시스템(Identity-based cryptography, IBC)**
 - 사용자의 식별할 수 있는 ID를 공개키로 사용함
- ◆ **CL 기반 암호 시스템(Certificateless cryptography, CLC)**
 - 사용자의 ID와 직접 생성한 난수를 함께 공개키로 사용함
- ◆ **속성 기반 암호 시스템(Attribute-based cryptography, ABC)**
 - 접근 정책 + 공개키 암호

IBE(Identity-based encryption)

❖ ID 기반 암호

- ◆ ID 기반 암호 또는 서명 시스템은 e-mail, 학번과 같이 누구나 식별할 수 있는 공개된 정보(ID)를 공개키(검증키)로 사용함



- ◆ PKI 기반 암호 시스템은 공개키가 난수 형태로 신뢰기관의 인증서가 필요하지만 ID 기반 암호 시스템은 식별이 가능한 ID를 공개키로 사용하기 때문에 **인증서가 필요하지 않음**
- ◆ 누구나 상대방의 ID를 알고 있는 소규모의 네트워크에 적용할 수 있음

IBE(Identity-based encryption)

❖ ID 기반 암호

◆ $Setup(1^\lambda) \rightarrow (PP, MSK)$

- 보안상수(security parameter)를 입력받아 공개 파라미터(public parameter) PP와 마스터키(master key) MSK를 출력하는 알고리즘. KGC에서 초기 셋업을 수행하기 위해 Setup 알고리즘을 사용함. PP는 모든 사용자에게 공개하고 MSK는 안전하게 저장함

◆ $KeyGen(PP, MSK, ID) \rightarrow sk$

- KGC에서 MSK를 이용하여 사용자 ID에 대한 개인키 sk를 생성하고 안전하게 전달함

◆ $Enc(PP, M, ID) \rightarrow C$

- 공개키 ID를 이용하여 메시지 M를 암호화

◆ $Dec(PP, C, sk) \rightarrow M$

- 개인키 sk를 이용하여 암호문 C를 M으로 복호화



IBE(Identity-based encryption)

❖ ID 기반 암호 대표 논문

◆ [BF01] Identity-Based Encryption from the Weil Pairing

◆ 곱선형 함수 (Bilinear map)

- $\mathbb{G}_1, \mathbb{G}_2$: 위수(order)를 소수 q 로 갖는 순환 군(group)
- 곱선형 함수 $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ 는 다음과 같은 성질을 만족함
 - 곱선형성(Bilinearity)
 - » $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$ and all $a, b \in \mathbb{Z}$
 - 비소실성(Non-degeneracy)
 - » The map does not send all pairs in $\mathbb{G}_1 \times \mathbb{G}_1$ to the identity in \mathbb{G}_2
 - 계산 가능성(Computability)
 - » 임의의 $P, Q \in \mathbb{G}_1$ 에 대해서 $e(P, Q)$ 를 계산하는 효율적인 알고리즘이 존재함
- $e(aP, Q) = e(P, Q)^a = e(P, aQ)$
- $e(aP, bQ) = e(P, Q)^{ab} = e(abP, Q)$

IBE(Identity-based encryption)

❖ ID 기반 암호 대표 논문

- ◆ [BF01] Identity-Based Encryption from the Weil Pairing

$$1^\lambda \rightarrow \text{Setup} \rightarrow PP = [e, H_1, H_2, P, P_{pub} = sP], \text{ **MSK** } = \text{ **s** }$$

$$MSK \rightarrow \text{KeyGen} \rightarrow sk = \text{ **s** } \cdot H_1(ID)$$

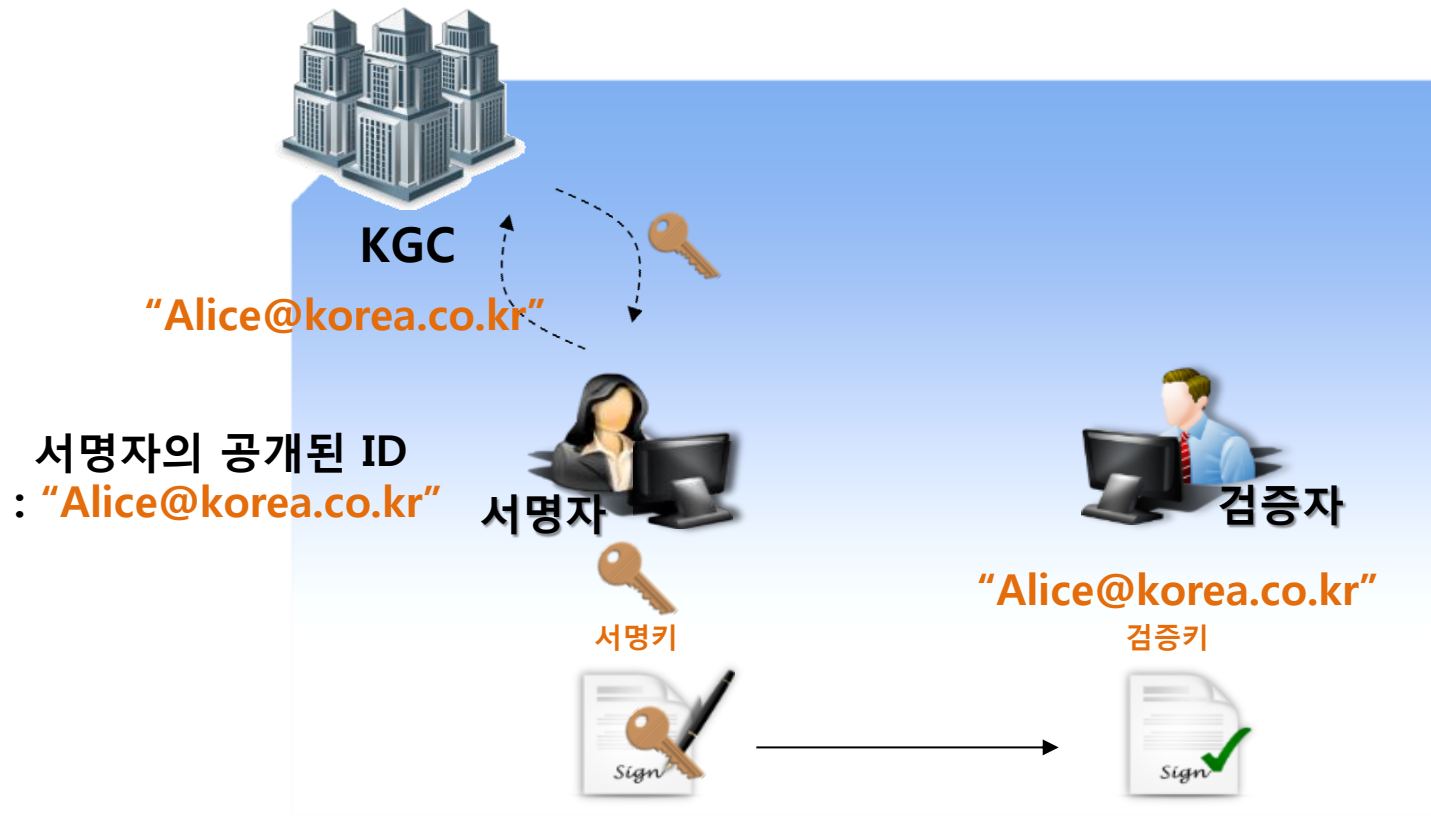
$$M, ID \rightarrow \text{Enc} \rightarrow C = [C_1, C_2] = \left[rP, M \oplus H_2\left(e\left(H_1(\text{ **ID** }), P_{pub}\right)^r\right) \right]$$

$$C, sk \rightarrow \text{Dec} \rightarrow M = C_2 \oplus H_2\left(e(C_1, sk)\right)$$

IBS(Identity-based signature)

❖ ID 기반 서명

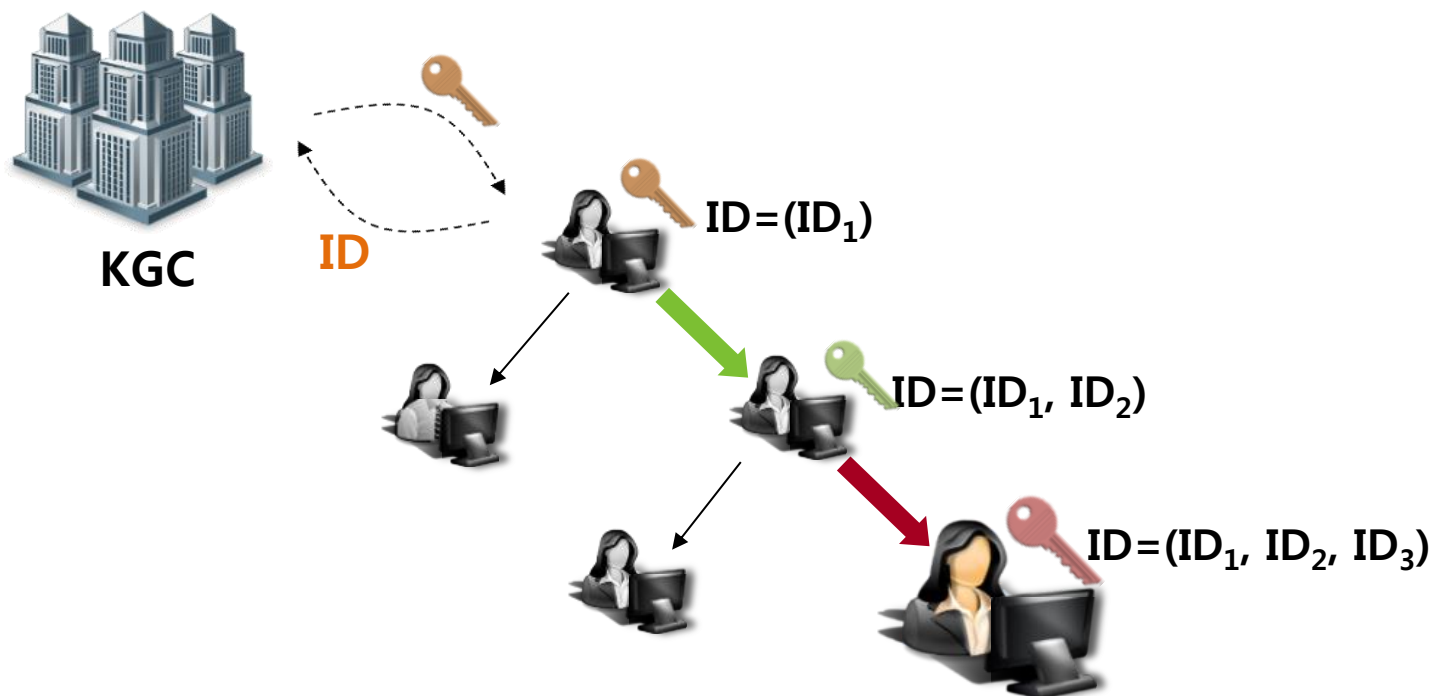
- ◆ 사용자의 식별할 수 있는 ID(email 주소, 학번 등)를 공개키로 사용함
 - 서명자는 키 생성기관(Key Generation Center, KGC)로부터 자신의 ID에 대응하는 개인 키(서명키)를 발급받아 문서에 서명함
 - 검증자는 서명자의 공개 ID를 사용하여 서명을 검증함



HIBE(Hierarchical Identity-based encryption)

❖ 계층적 ID 기반 암호

- ◆ 계층적 ID 기반 암호 시스템은 사용자 간의 계층 구조를 제공함
 - ID 간에 계층구조를 가지는 환경(ex. DNS)에 필요함
 - 모든 사용자가 KGC로부터 개인키를 발급받을 수 있으며, 추가적으로 상위 사용자가 자신의 개인키를 이용하여 하위 사용자에게 개인키를 발급해줄 수 있음
 - **ID 기반 암호의 한계점인 키 위탁문제와 키 폐기문제를 모두 안고 있음**

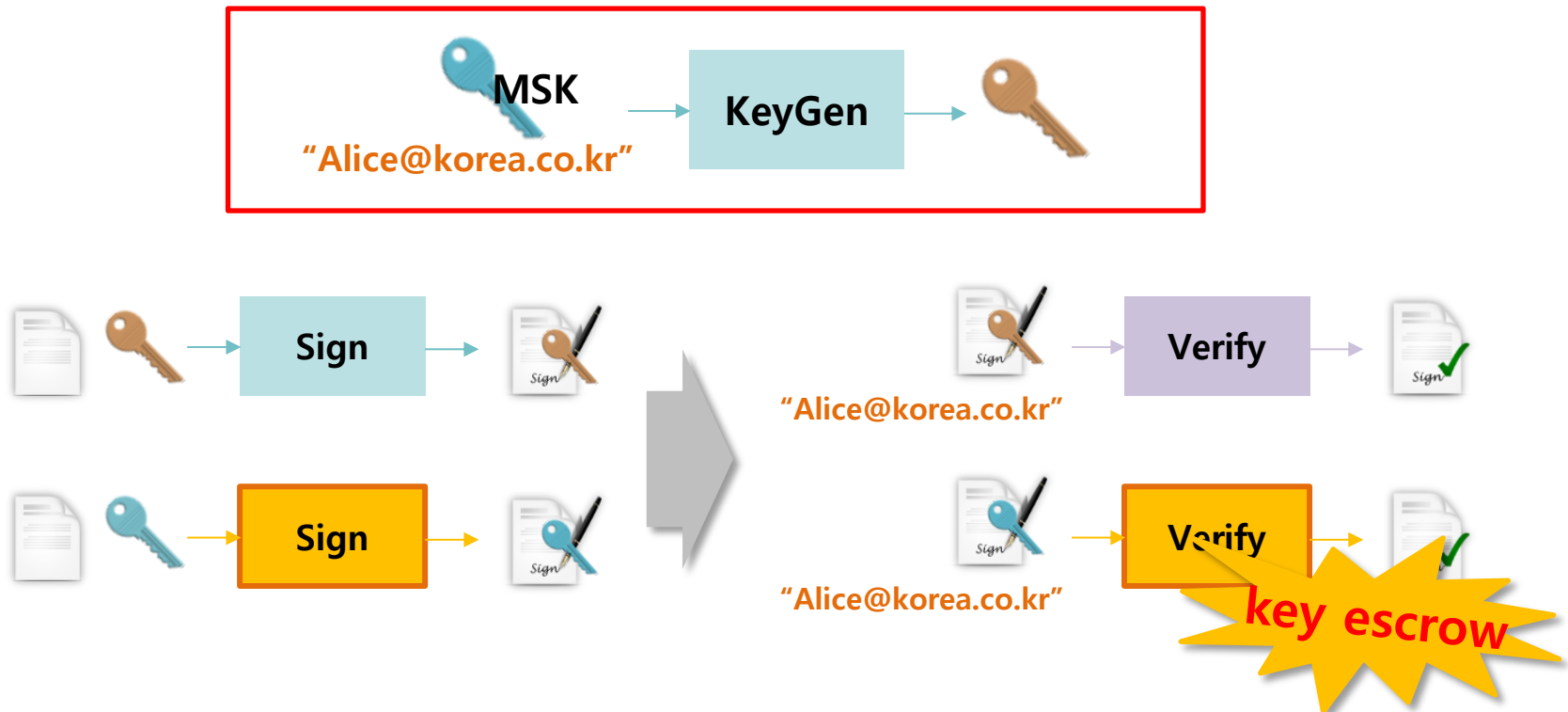


IBE(Identity-based encryption)

❖ ID 기반 암호 시스템의 한계점

◆ 키 위탁(escrow)문제가 발생

- MSK로부터 개인키(서명키)가 생성되기 때문에 KGC가 악의적으로 모든 사용자에게 대한 개인키(서명키)를 생성할 수 있음
- 또한 MSK 그 자체로도 복호화(서명생성)가 가능함

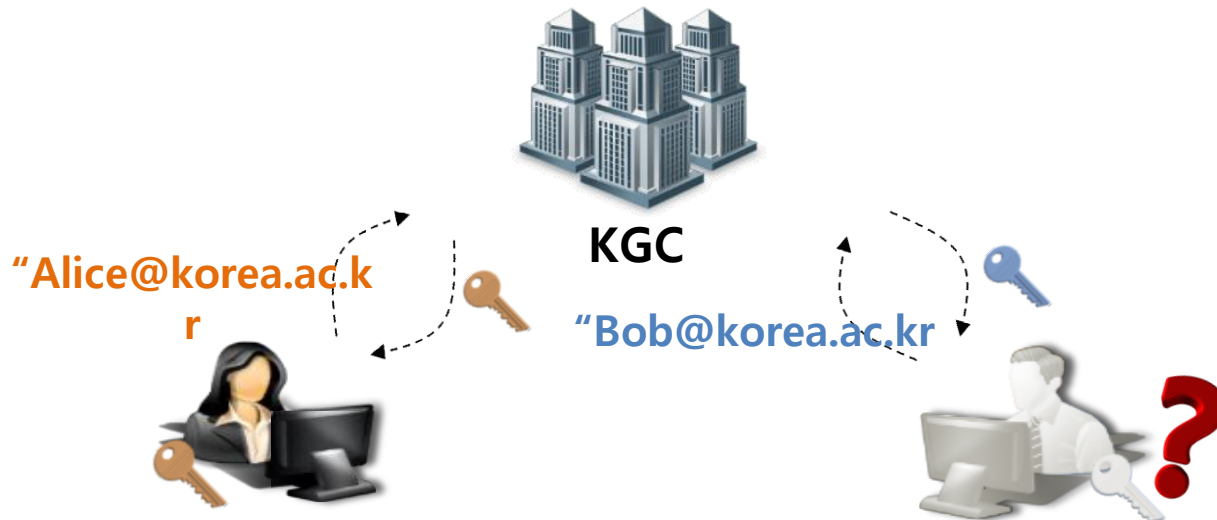


IBE(Identity-based encryption)

❖ ID 기반 암호 시스템의 한계점

◆ 키 폐기(revocation)문제가 발생

- 일정 시간이 지나 사용자가 탈퇴하는 경우, 발급된 키를 폐기해야 함
- 일반적인 ID 기반 암호 시스템에서 발급된 키 자체를 폐기할 수 없기 때문에 추가적인 시스템이 필요함



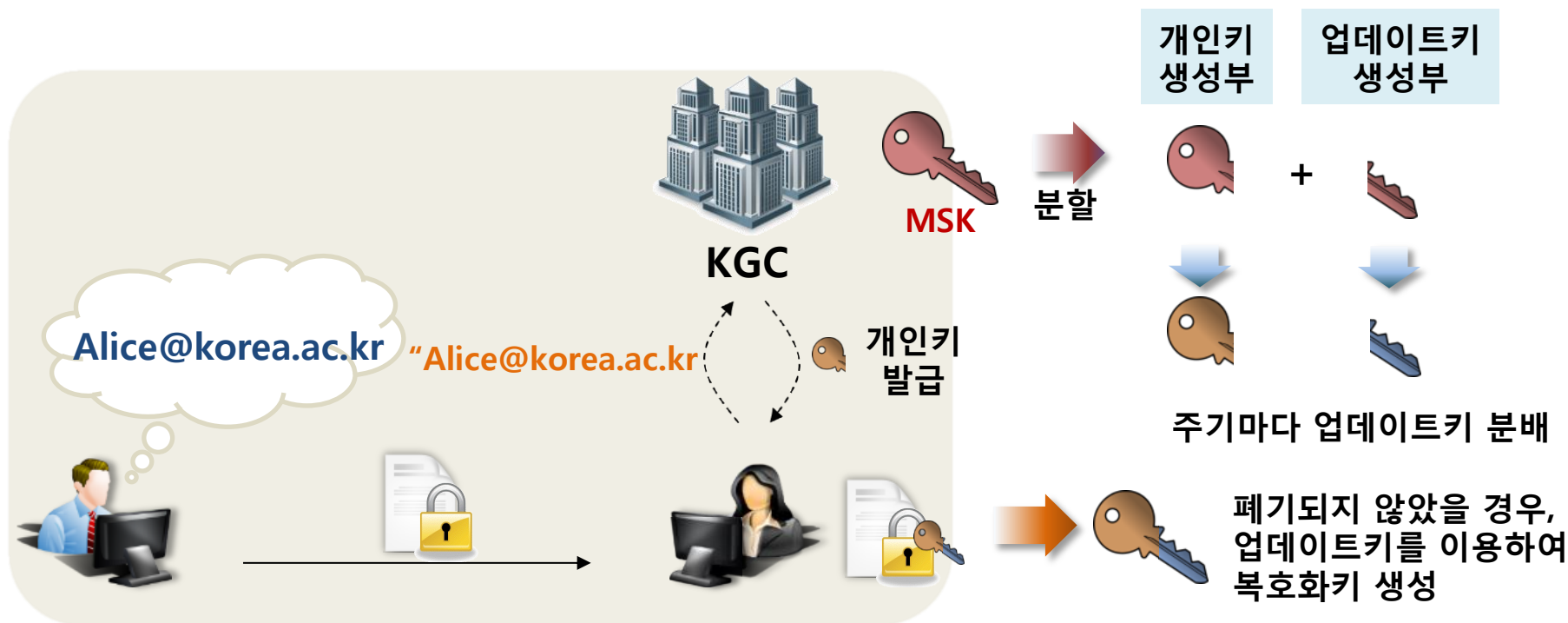
◆ 효율성 문제

- 일반적인 ID 암호 시스템은 연산 소모량이 큰 곱선형 함수를 사용하기 때문에 저전력 기기에서 수행하기 어려움

IBE(Identity-based encryption)

❖ 폐기 가능한 ID 기반 암호(Revocable IBE, RIBE)

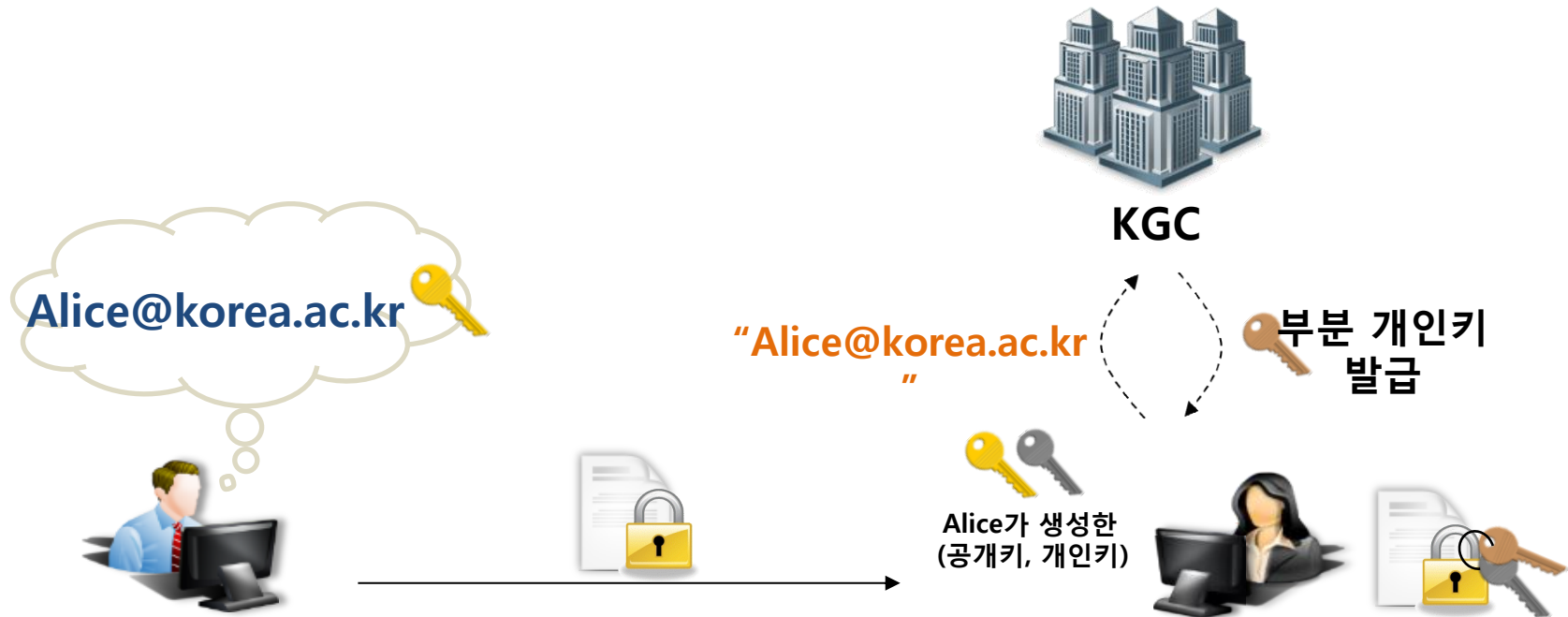
- ◆ 키 폐기 기능을 지원하는 기법들이 제안됨
- ◆ 매 주기마다 발급되는 업데이트 키를 이용함
 - 최초에 KGC로부터 발급된 개인키에 업데이트키를 결합하여 복호화키를 생성
 - MSK 분할 → 개인키 생성 + 갱신키 생성 → 새로운 복호화키
- ◆ 효율적인 RIBE 연구가 필요함



CL-PKE(Certificateless public key encryption)

❖ CL 기반 암호

- ◆ CL 기반 암호 또는 서명 시스템은 사용자의 ID와 직접 생성한 난수를 함께 공개키로 사용함



- ◆ PKI 기반 암호와 ID 기반 암호(IBC)의 장점을 결합하여 PKI의 인증서 문제와 ID 기반 암호의 키 위탁(Key escrow)문제를 해결함

CL-PKE(Certificateless public key encryption)

❖ CL 기반 암호

◆ $Setup(1^\lambda) \rightarrow (PP, MSK)$

◆ $Partial - Private - Key - Extract(PP, MSK, ID) \rightarrow Psk$

- KGC에서 MSK를 이용하여 사용자 ID에 대한 부분개인키 Psk를 생성하고 안전하게 전달

◆ $Set - Secret - Value(PP, ID) \rightarrow Ssk$

- 사용자가 자신의 ID로부터 비밀정보 Ssk를 생성함

◆ $Set - Private - Key(PP, Psk, Ssk) \rightarrow sk$

- 사용자가 부분개인키 Psk와 비밀정보 Ssk로부터 자신의 개인키 sk를 생성함

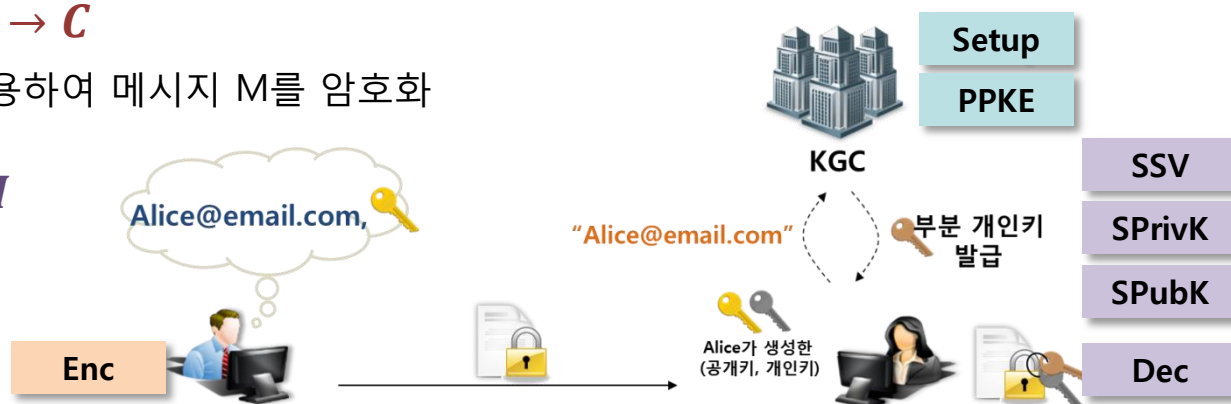
◆ $Set - Public - Key(PP, Ssk) \rightarrow pk$

- 사용자가 비밀정보 Ssk로부터 자신의 공개키 pk를 생성함

◆ $Enc(PP, M, ID, pk) \rightarrow C$

- 공개키 ID와 pk를 이용하여 메시지 M를 암호화

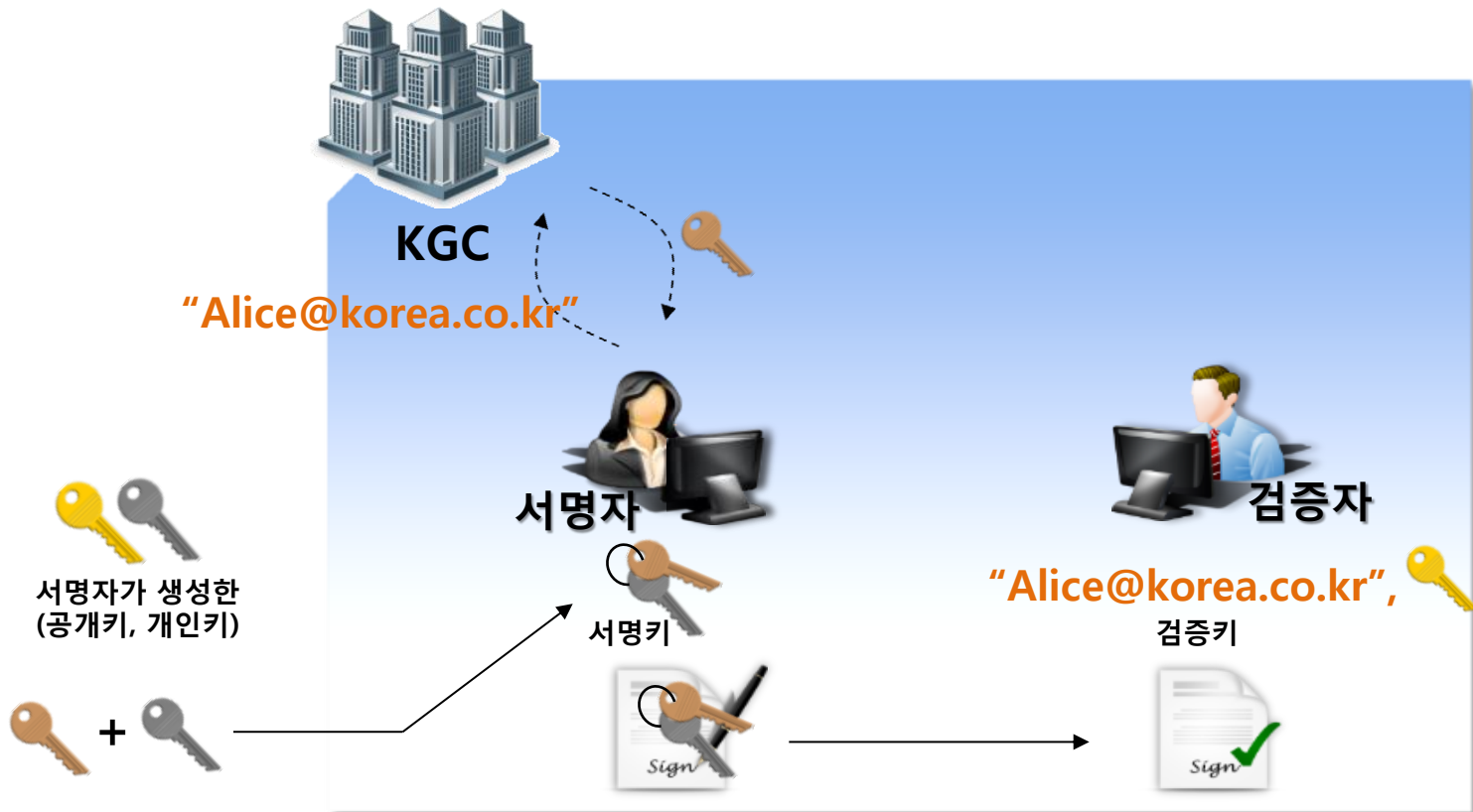
◆ $Dec(PP, C, sk) \rightarrow M$



CLS(Certificateless signature)

❖ CL 기반 서명

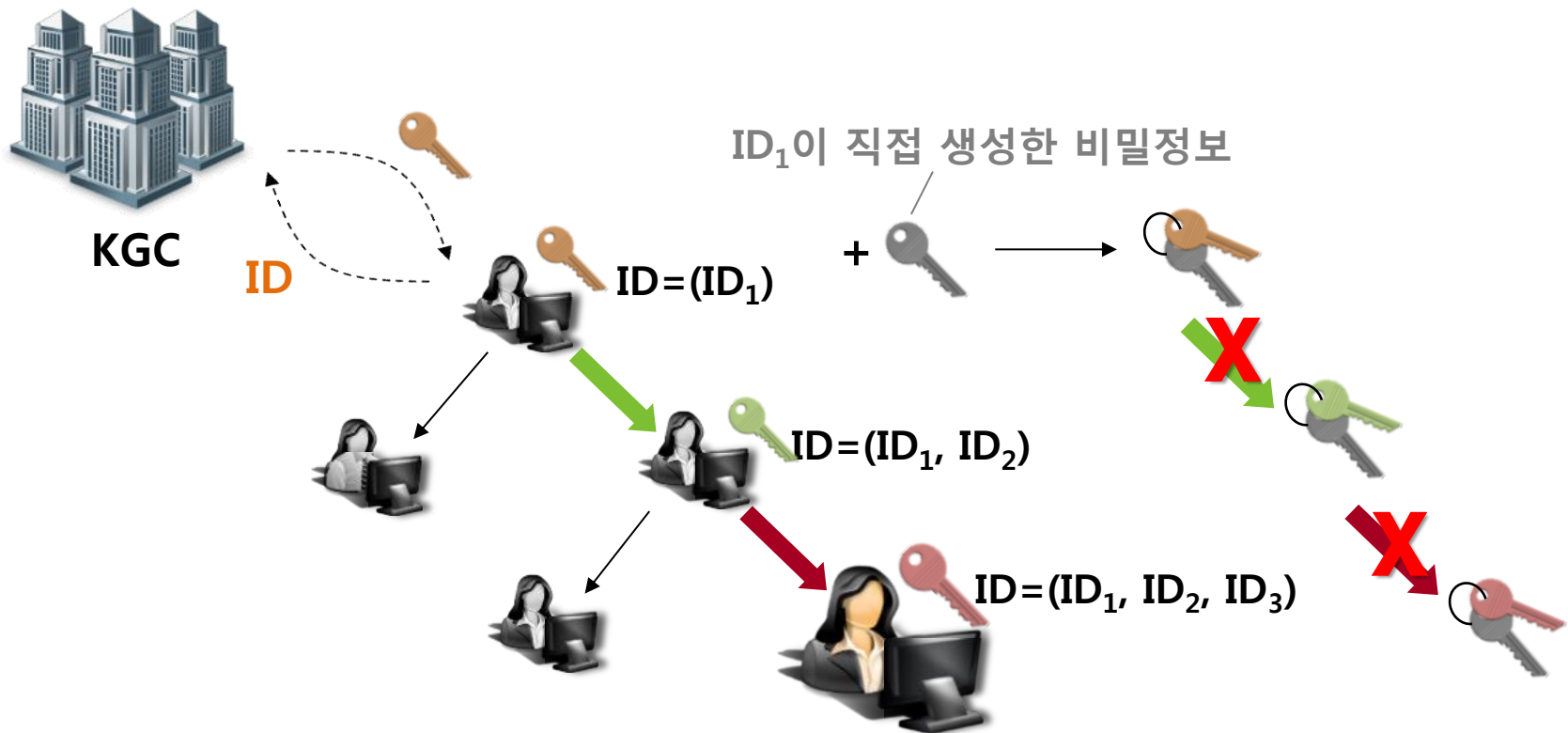
- ◆ 사용자의 ID와 직접 생성한 난수를 함께 공개키로 사용함
 - 서명자는 KGC로부터 자신의 ID에 대응하는 부분 개인키를 발급받고 자신이 직접 생성한 개인키와 결합하여 서명키를 생성한 뒤, 문서에 서명함
 - 검증자는 서명자의 공개 ID와 공개키를 사용하여 서명을 검증함



CL-PKE(Certificateless public key encryption)

❖ CL 기반 암호 시스템의 한계점

- ◆ CL 기반 암호 시스템은 ID 기반 암호 시스템과 달리 계층적 구조를 지원하지 않음



CL-PKE(Certificateless public key encryption)

❖ CL 기반 암호 시스템의 한계점

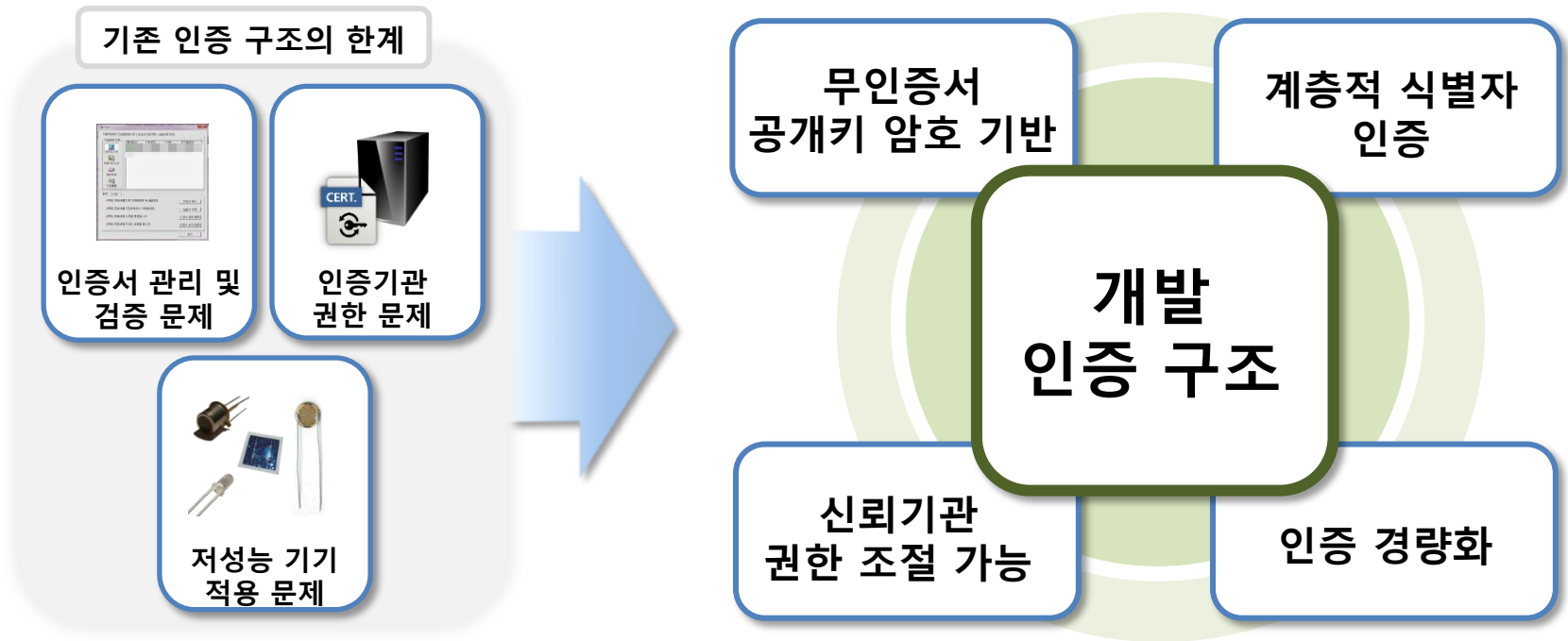
- ◆ ID 기반 암호 구조에 의존하는 CL 기반 암호는 ID 기반 암호에서 발생하는 문제점을 포함하고 있음(키 위탁문제 제외)
- ◆ **키 폐기문제**
 - 일정 시간이 지나 사용자가 탈퇴하는 경우 발급된 부분개인키를 폐기해야 함
 - 키 폐기가 가능한 ID 기반 암호 기법과 같이 CL에서도 키 폐기가 가능하도록 해야함
- ◆ **효율성 문제**
 - 저전력 기기도 지원할 수 있는 효율적인 기법이 필요함



CL-PKE(Certificateless public key encryption)

❖ 무인증서 기반의 공개키 인증기술의 설계 요구사항

- ◆ 무인증서 공개키 암호기반 : 고유 식별자(ID)를 이용한 인증
- ◆ 계층적 식별자 인증 : 트리 구조를 가지는 식별자에 대한 효율적인 인증
- ◆ 신뢰기관 권한 조절 : 사용자의 요구(demand)에 따라 개인키 생성 방식 결정
- ◆ 인증 경량화 : IoT 환경을 고려한 효율적인 ID 등록 및 인증 과정 경량화



CL-PKE(Certificateless public key encryption)

❖ 무인증서 기반 (계층적) 공개키 인증기술

◆ 마스터키 업데이트

- KGC가 손상된 경우, 모든 사용자의 개인키를 새롭게 셋팅하는 것이 아니라 마스터키를 업데이트함으로써 효율적인 키 관리가 가능해짐

◆ 키 위임 기능

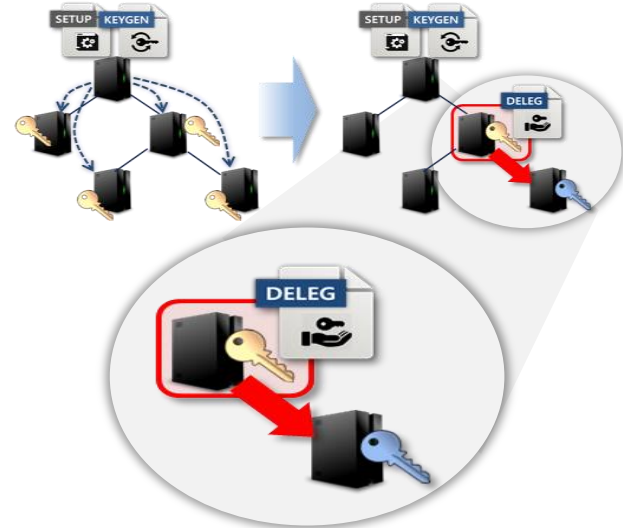
- 중간 노드가 하위 네트워크를 관리할 수 있게 됨

MSK update



키 발급기관(KGC)이 손상된 경우, 마스터 키(MSK)를 효율적으로 갱신하는 기능

Key Delegation



계층적 구조에서 상위 개체가 하위 개체에 개인키를 위임(delegation)하는 기능

CL-PKE(Certificateless public key encryption)

❖ 무인증서 기반 계층적 인증기술

◆ 신뢰기관의 권한 조절

- ID 기반 암호에서는 KGC의 권한이 여전히 막강함
- CL 기반 암호에서는 사용자가 직접 선택한 값을 함께 키로 사용하기 때문에 KGC의 권한을 최소화할 수 있음

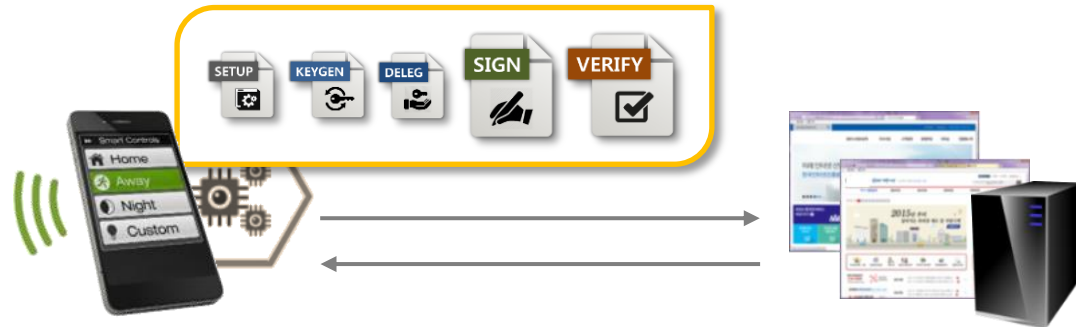
- 사용자의 요구(demand)에 따라 개인키 생성 방식을 결정할 수 있도록 구성
- ID 기반 암호와 CL 기반 암호의 **호환성**을 제공



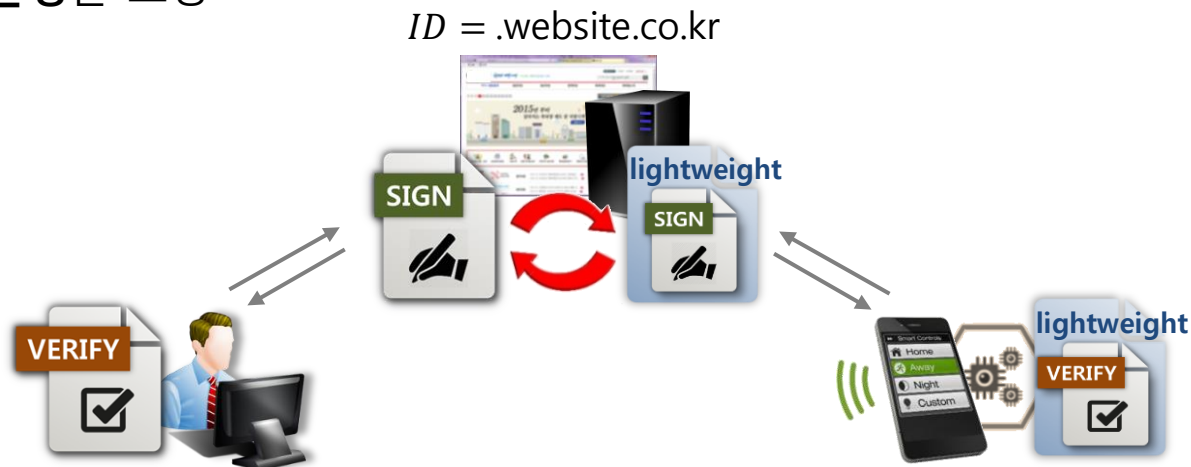
CL-PKE(Certificateless public key encryption)

❖ 인증기술의 경량화

- ◆ IoT 기기를 지원할 수 있도록 IoT 기기가 수행하는 요소 기술의 경량화



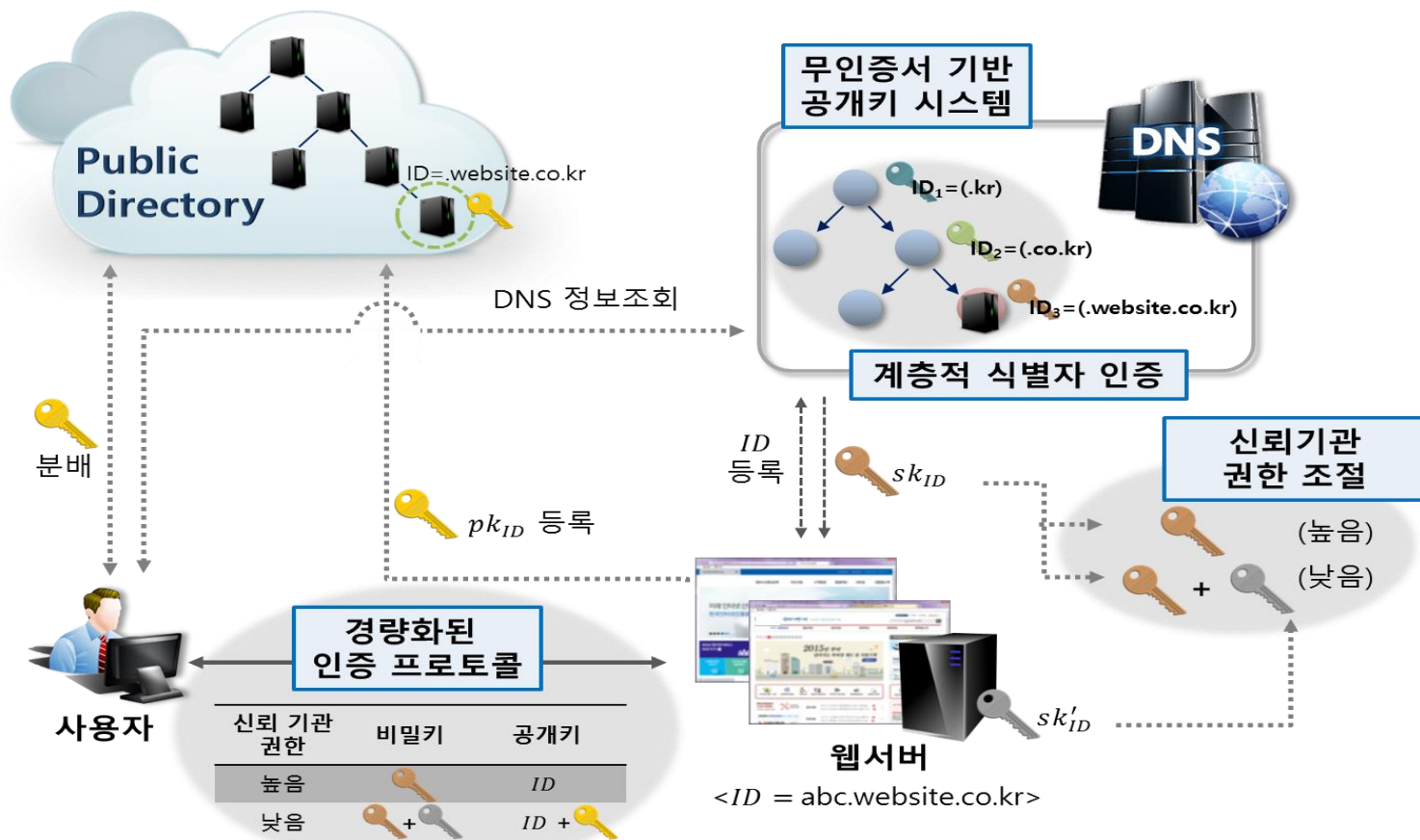
- ◆ 일반 인증 모듈과 경량화된 모듈이 웹서버 접속 개체에 따라 선택적으로 사용될 수 있도록 호환성을 보장



CL-PKE(Certificateless public key encryption)

❖ (Hierarchical) Certificateless public-key authentication

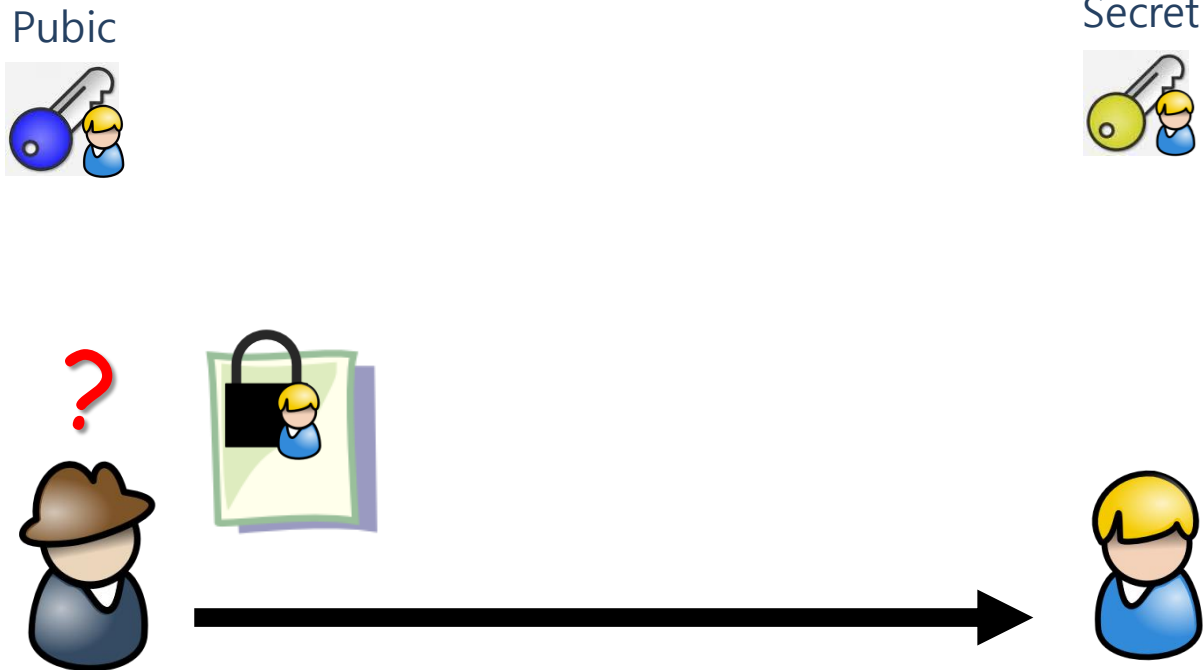
- ◆ PKI 문제를 해결할 수 있고, IoT 기기도 지원하는 무인증서(certificateless) 공개키 암호 기술 기반의 계층적 식별자를 가진 인터넷 개체 인증 구조 개발이 필요함



AB-PKE(Attribute-based public key encryption)

❖ Concept

◆ 공개키 암호



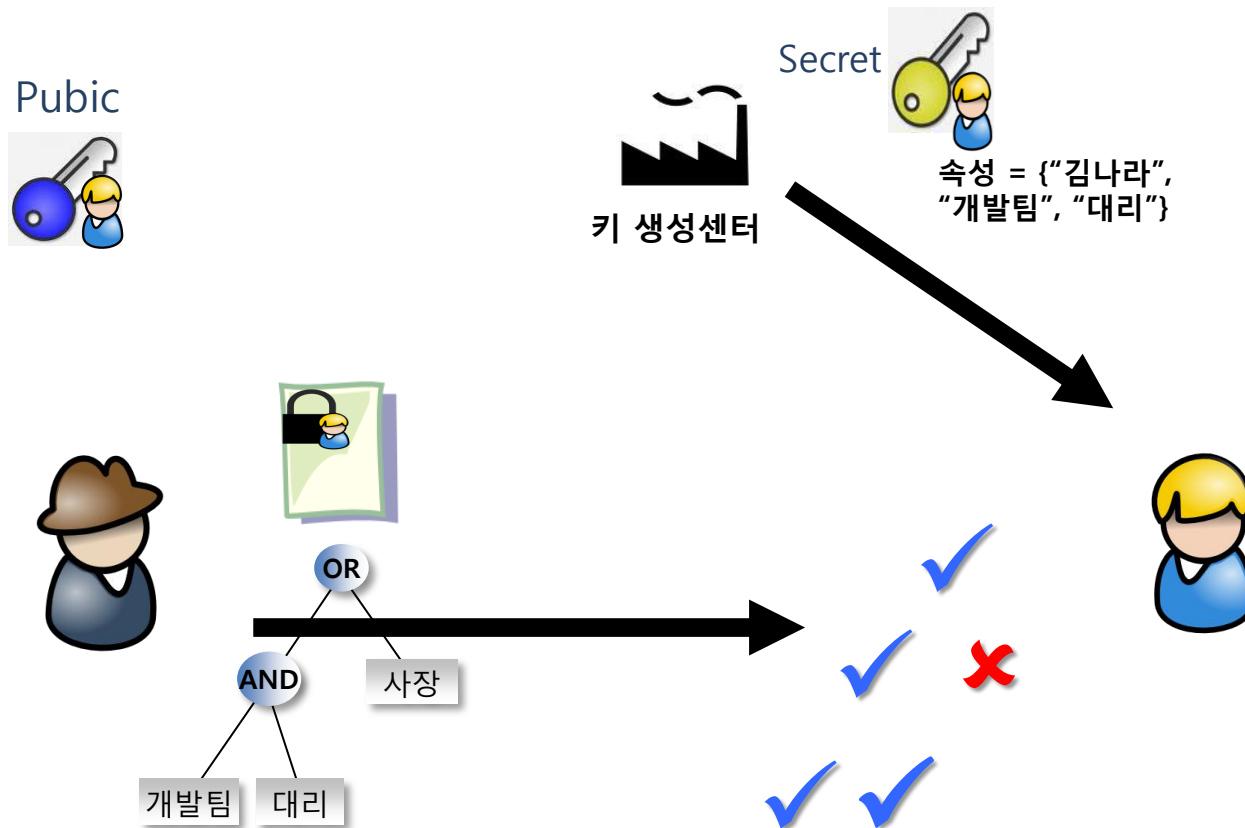
문제점 : 정책과 암호의 분리

Who should see this? → Need Descriptive One

AB-PKE(Attribute-based public key encryption)

❖ Concept

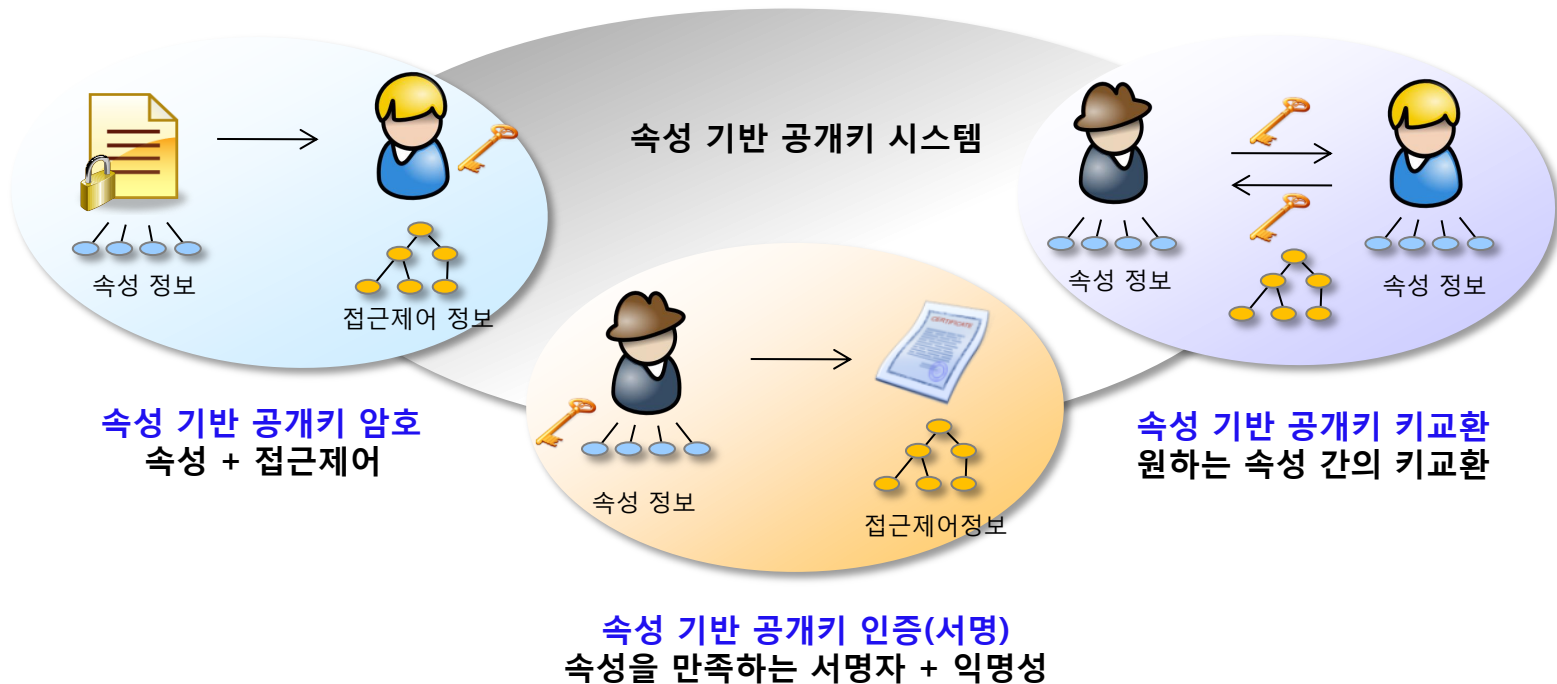
- ◆ 속성기반 암호(ABE: Attribute-Based Encryption)



AB-PKE(Attribute-based public key encryption)

❖ Concept

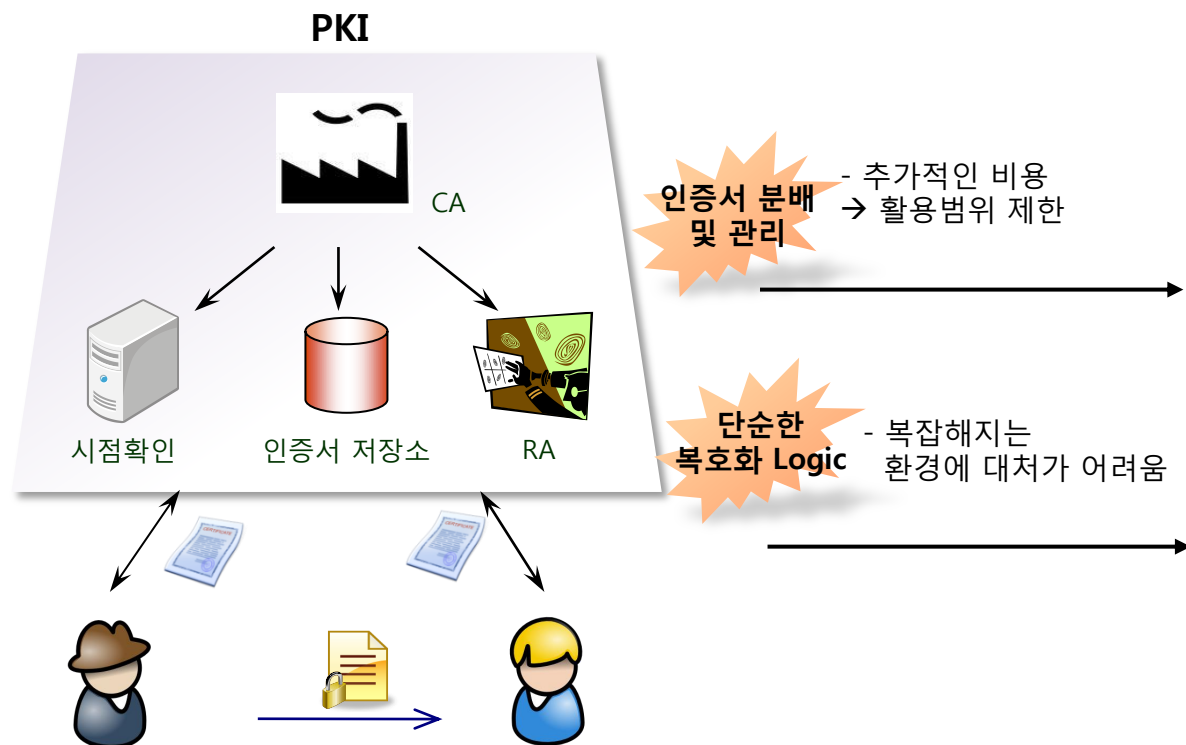
- ◆ 공개키 시스템 + 접근 제어



AB-PKE(Attribute-based public key encryption)

❖ Concept

◆ 속성기반 PKC vs. PKC



속성 기반 PKC

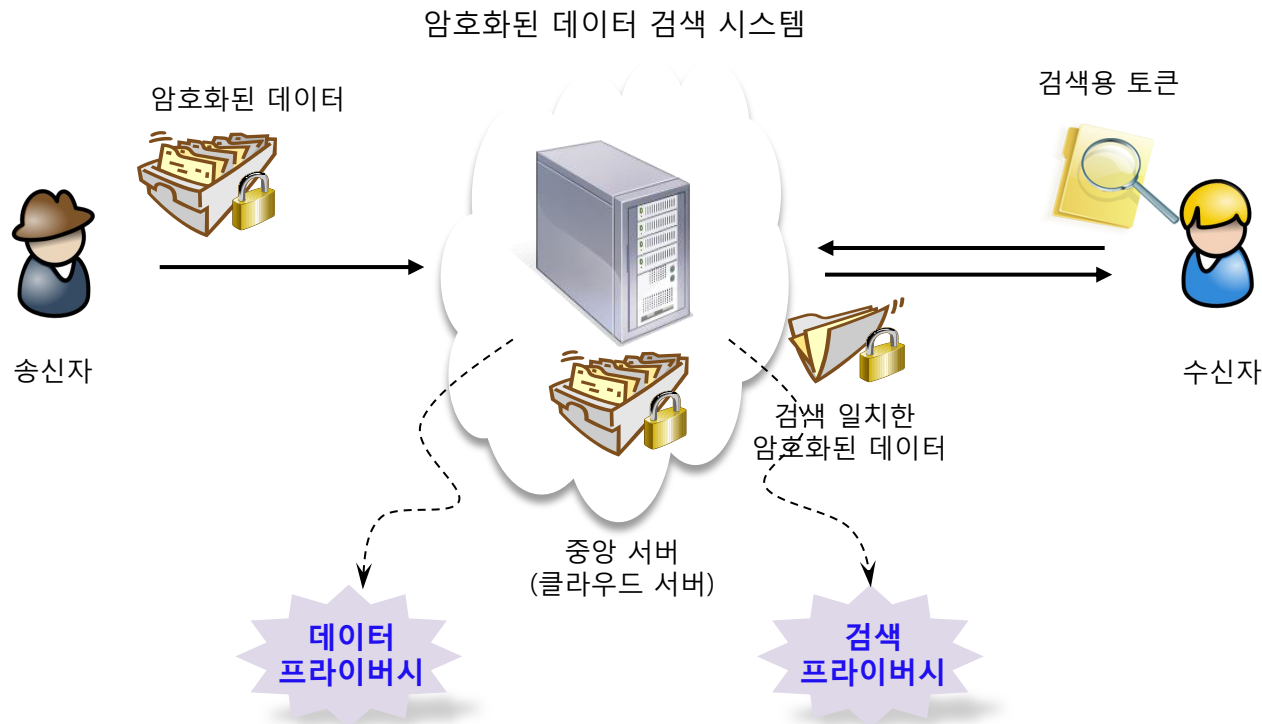
- 임의 스트링이 공개키를 대체
- 랜덤한 공개키 불필요함

- 접근제어 정보를 이용한 유연한 복호화 Logic
- 다양한 환경에 적용이 가능함

AB-PKE(Attribute-based public key encryption)

❖ Concept

- ◆ 사회적 현안 및 잠재적 이슈 관련된 연구 분야 II
 - 암호화 데이터의 검색 : 서버에 암호문 정보를 노출하지 않고 암호문 검색
 - 익명성을 제공하는 속성 기반 암호를 이용하여 암호화 데이터 검색



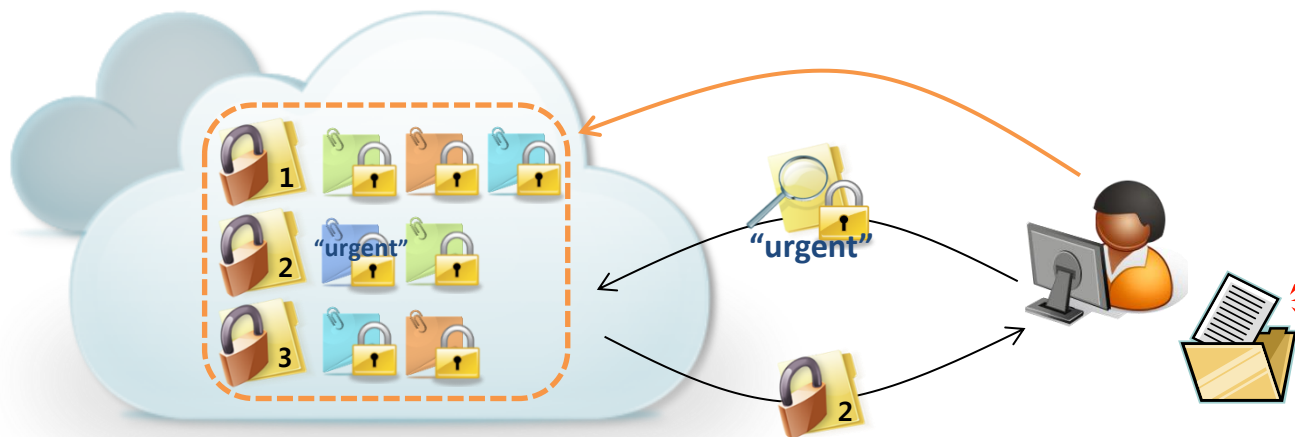
Cloud is growing →
Data must be encrypted

암호화된 검색-Introduction

❖ Background

- ◆ To store sensitive data in a secure way on an untrusted server, the data has to be encrypted
- ◆ How to search on encrypted data on the server side, without decrypting the data

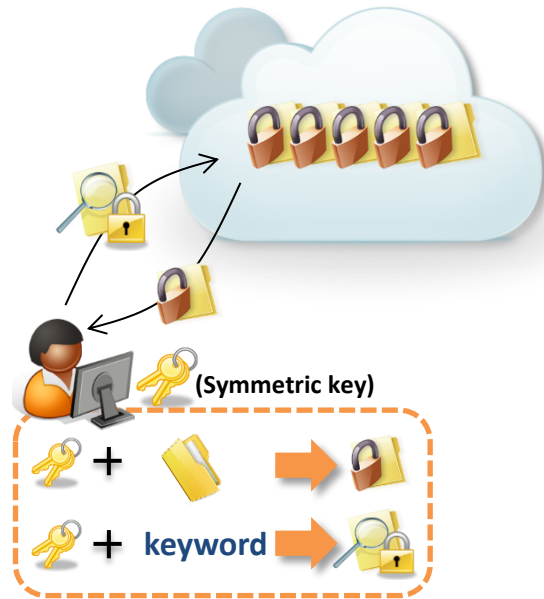
❖ General model of Searchable Encryption scheme



❖ Major applications : cloud storage service, e-mail

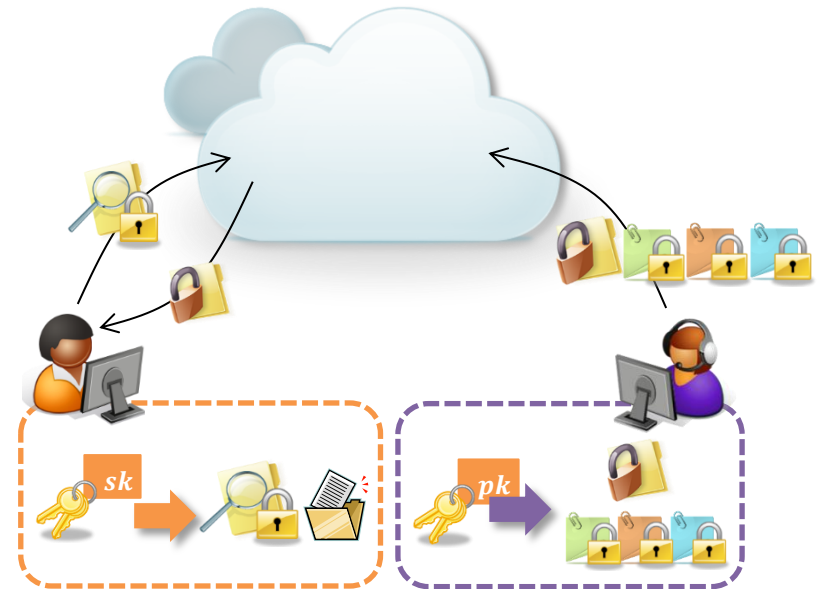
암호화된 검색- Symmetric vs. Asymmetric

❖ Symmetric SE



- Only the private key holder can create searchable ciphertexts & trapdoors
- Some SE schemes allow other users to search his data using secret key distribution

▶ Asymmetric SE



- Anyone who has the public key can create searchable ciphertexts
- Only the private key holder can perform search & decryption

암호화된 검색- Single user vs. Multiple users

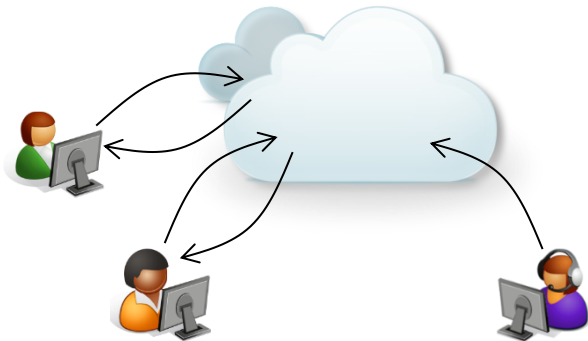
❖ S/S

- ◆ Single writer / Single reader
- ◆ Private cloud storage service



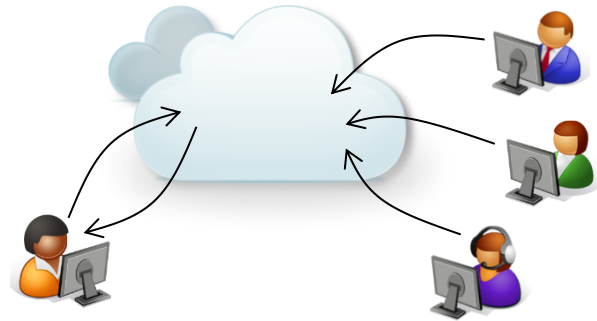
▶ S/M

- Single writer / Multiple readers



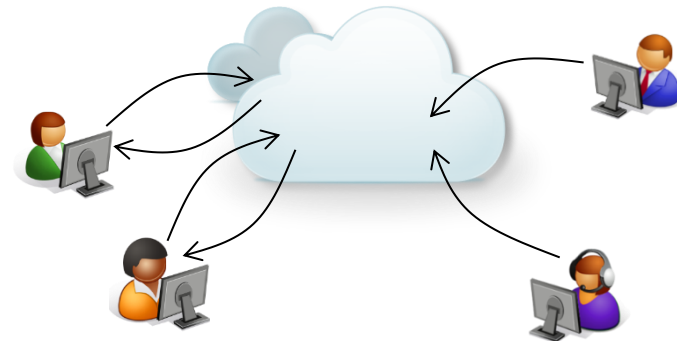
▶ M/S

- Multiple writers / Single reader
- PEKS (e-mail service)



▶ M/M

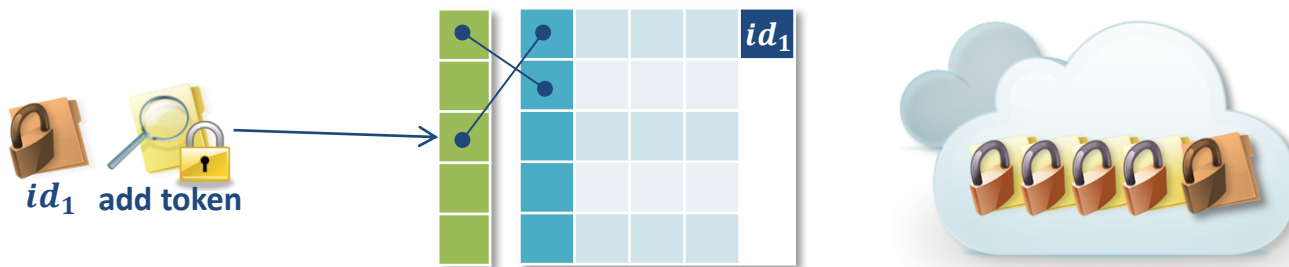
- Multiple writers / Multiple readers




암호화된 검색- Others

❖ Dynamic

- ◆ In the index-based symmetric searchable encryption(SSE)
- ◆ Dynamic SSE allows the **addition** and **removal** of files
- ◆ Both of these operations are handled using "**tokens**"



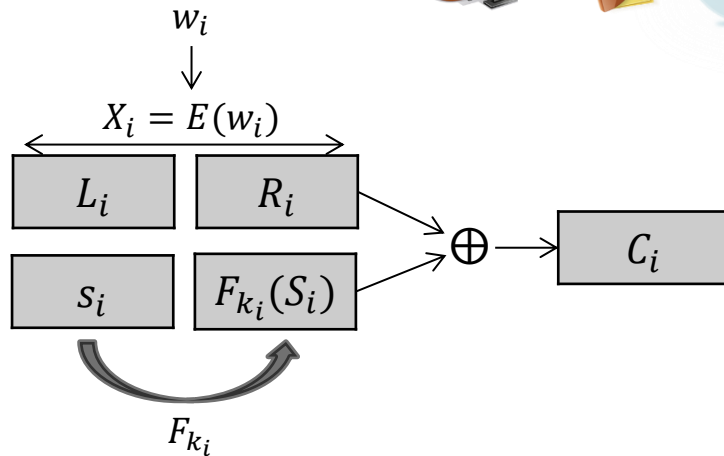
❖ Complex queries

Conjunctive keyword search	"patient \wedge urgent \wedge female"
Fuzzy/similarity search	"su <u>c</u> cess" \longrightarrow  (containing "su <u>cc</u> cess")
Range queries	"80 < value < 100"
Subset queries	"sender $\in S$ "

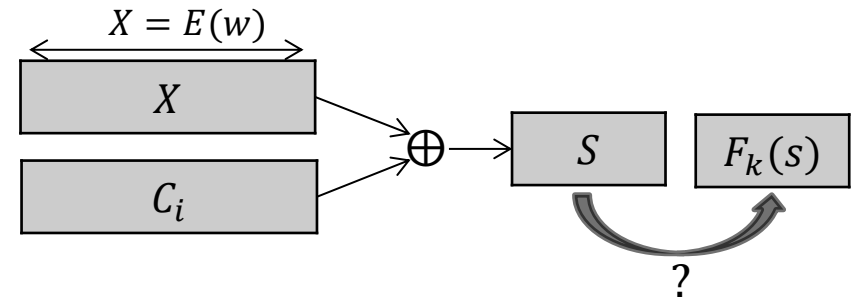
암호화된 검색- S/S – Concept

❖ Song et al. (2000)

- ◆ First practical scheme for searching in encrypted data
- ◆ Use a special two-layered encryption construct
- ◆ Encrypt each word separately and then embed a hash value inside the ciphertext



(a) Encryption



(b) Sequential search