Cloud-Based Digital Signature

한국전자인증

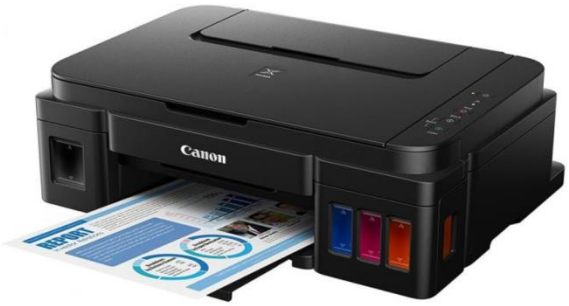
CloudSign

❖ Signature

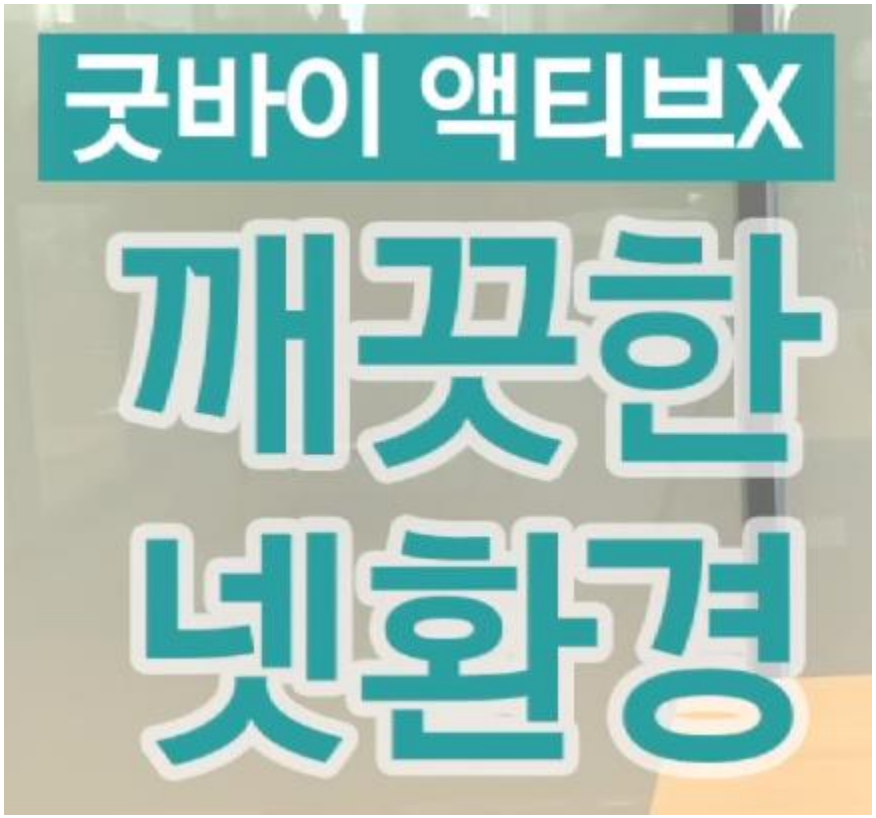
❖ 전자문서의 서명은?

Digital Document(Message)

서명을 위해



❖ Goodbye ActiveX



https://www.youtube.com/watch?v=ZtbJpsTF_04

❖ 전자서명법 개정 방향

- ✓ 공인인증 제도 폐지
- ✓ 전자서명 수단들의 공정한 경쟁
- ✓ 안전성 및 관리 체계를 위한 인증업무 평가제
- ✓ 법 개정 이후에도 공인인증서는 계속 사용

❖ 전자서명법 개정안 내용

	현행	개정
정의	공인전자서명 공인인증업무 공인인증기관	전자서명 전자서명인증업무 **전자서명인증사업자**
효력	법령, 공인전자서명, 당사자 약정서명	② 제1항 이외의 전자서명은 **전자적 형태라는 이유만으로 서명, 서명날인 또는 기명날인으로서의 법적 효력이 부인되지 아니한다**
운영기준	공인인증업무준칙 등	국제적으로 인정되는 기준 등을 고려한 전자서명인증업무 운영기준(이하 "운영기준"이라 한다)을 정하여 고시할 수 있다
평가	업무정지, 지정취소, 시정명령 조항을 두어 공인인증기관에 대한 엄격히 평가	전자서명인증사업자는 과학기술정보통신부장관이 정한 평가기관(이하 "평가기관"이라 한다)에 제4조의 운영기준을 준수하는지 여부에 대한 **평가를 신청할 수 있다**
활성화		**불가피하게 전자서명수단을 제한하여야 하는 경우에는** 법률, 대통령령, 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 감사원규칙으로 정한다

❖ 디지털 전자서명과 전자적 전자서명의 차이

Digital Signatures

- 암호화 기술을 기반으로 특정한 타입의 서명
- 서명자의 신원이 제3자에 의해 검증됨
- 서명이 암호연산과 연관되고 서명자와도 연관됨

Electronic Signatures

- 표준화되지 않음
- 서명자의 신원이 제3자에 의해 항상 검증되지 않음
- 서명이 이미지나 이니셜 등 일수도 있고 서명자와 반드시 연관 될 필요는 없음

❖ Why PKI?

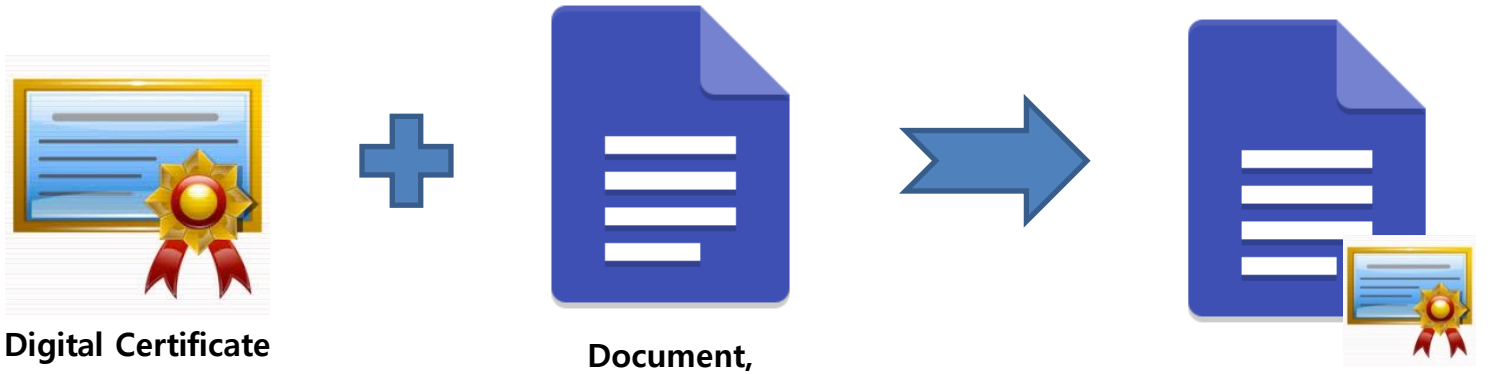
- ✓ PKI(Public Key Infrastructure) 기술은 보안의 핵심 기술 인정
- ✓ 대칭키의 문제점을 해결한 암호기술
- ✓ 공개키와 개인키가 한쌍을 이루어서 발급하고 개인키로 자신을 인증하는 방식
- ✓ 전세계적으로 더 확산 되어 가고 있는 기술
- ✓ 최근 UN RooT CA 구축. 인증서 + 지문카드 도입
- ✓ 유럽은 3단계 등급의 인증서를 정의하여 확산하려고 함
- ✓ 블록체인, FIDO, IoT 인증(OCF)도 PKI기술이 적용됨

❖ 디지털 전자서명은 무엇인가?

Digital Signature (Wikipedia 설명)

➢ 정의 : 네트워크에서 송신자의 신원을 증명하는 방법으로,
송신자가 자신의 개인키로 암호화한 메시지를
수신자가 송신자의 공개키로 해독하는 과정

➢ 3개의 알고리즘으로 구성
1. 공개 키 쌍을 생성하는 키 생성 알고리즘
2. 이용자의 개인 키를 사용하여 서명(전자서명)을 생성하는 알고리즘
3. 이용자의 공개 키를 사용하여 서명을 검증하는 알고리즘

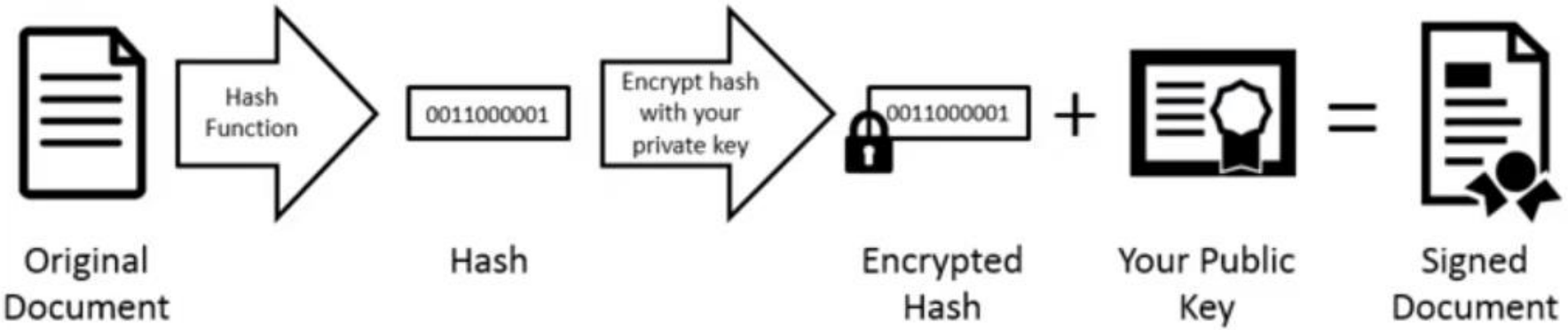


❖ 디지털 전자서명 얻을 수 있는 것은?

- ✓ **Integrity** : 무결성
- ✓ **Authentication** : 인증
- ✓ **Non-Repudiation** : 부인방지

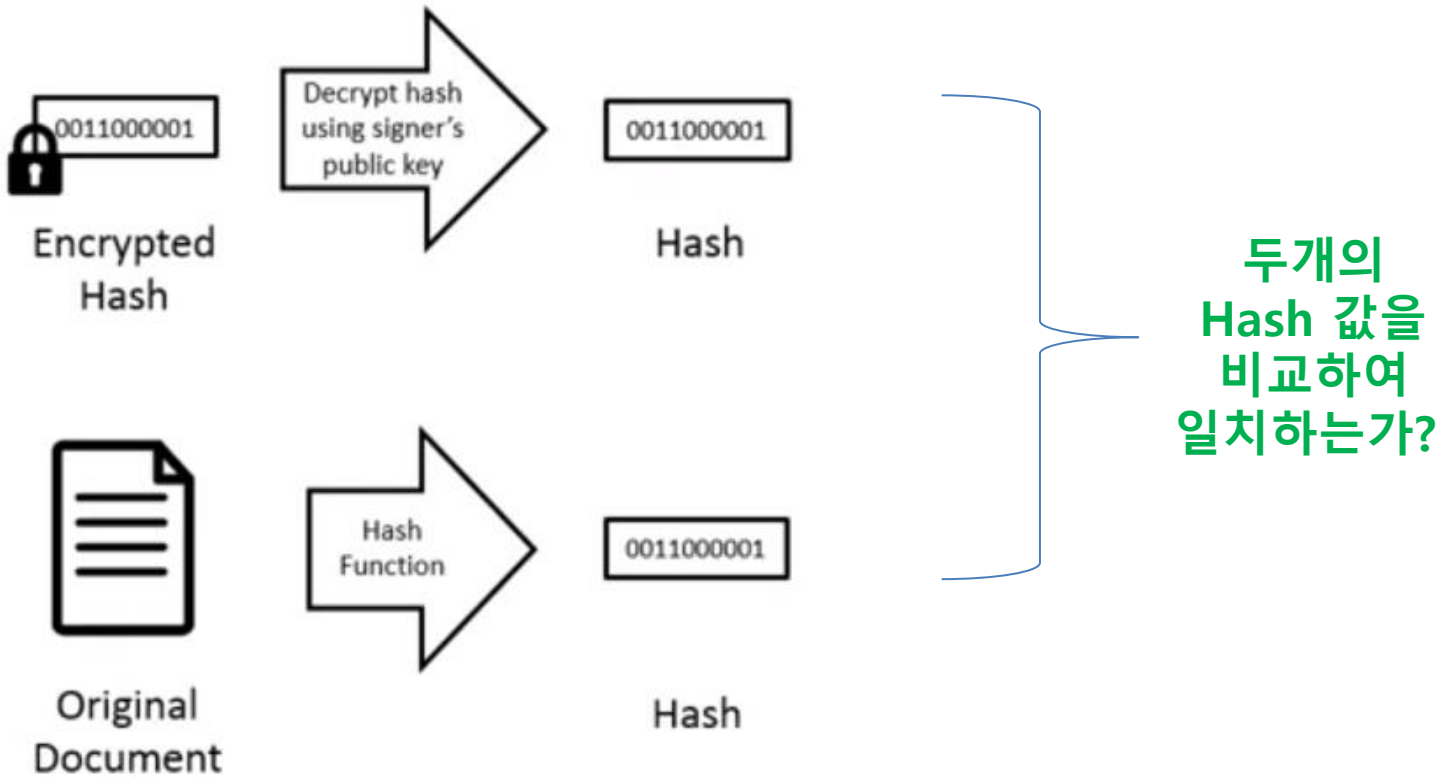
❖ 디지털 전자서명 절차

1. 디지털 전자서명 적용



❖ 디지털 전자서명 절차

2. 디지털 전자서명 검증



❖ 디지털 전자서명으로 얻은것

✓ Hash Check ➔ Integrity(무결성)

✓ Public Key ➔ Authentication(인증)

✓ Asymmetric encryption
➔ Non-Repudiation(부인방지)

❖ 디지털 전자서명의 장점

Digital Signatures | Electronic Signatures

Advantage

문서가 인증 되었고 출처가 확실하다

서명자를 신뢰할 수 있는 기관(인증기관)에 의해 확인되었다

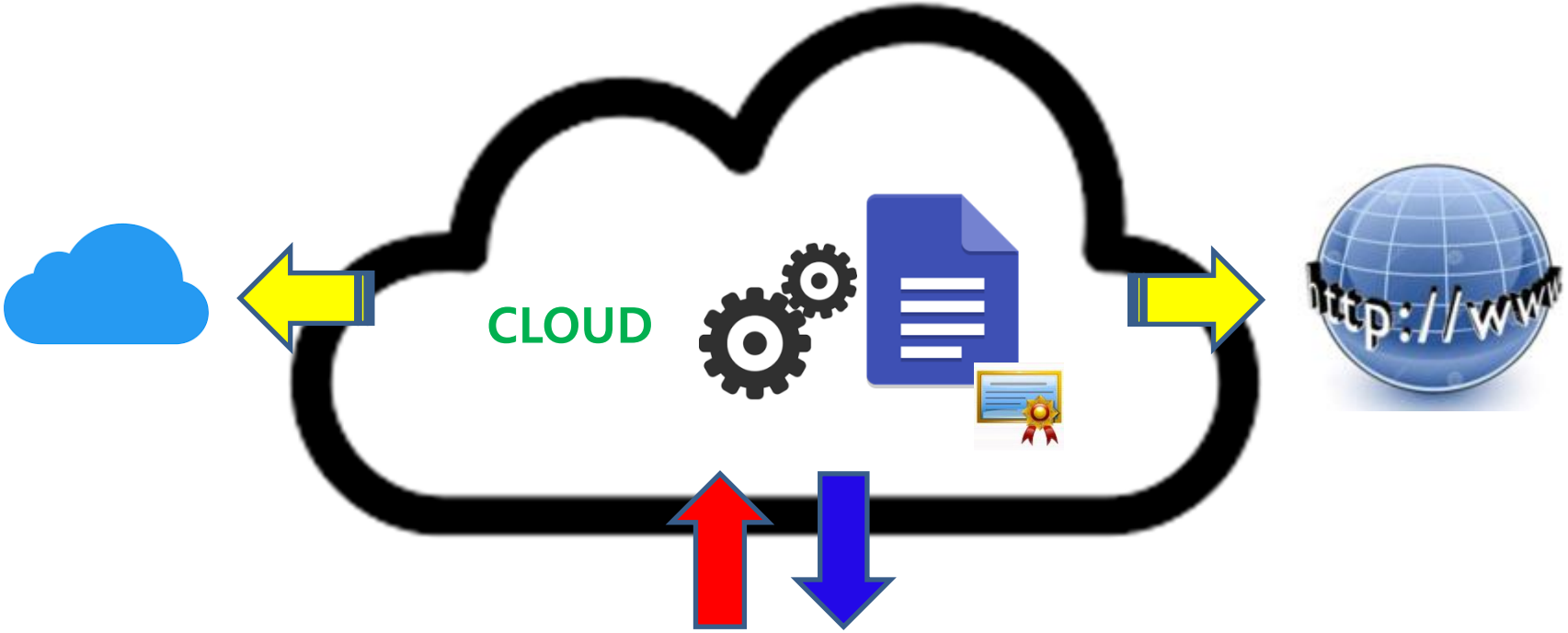
자신의 서명을 부인할 수 없다

문서에 무단 변조 방지 장치를 제공한다

❖ 현재 사용중인 디지털인증서

인증서 종류	목적		이용회사
공인인증서	범용		모든 기관
	특수 목적용	은행용, 증권용, 전자세금계산용	해당 업무 이용기관
		홍채용	삼성패스
자체인증서 (사설인증서)	Managed PKI (Symantec)		포스코, LG생활건강, 기업은행
	협력사 또는 유관기관 업무		티몬, IITP, 저작권위원회
	학생학부모서비스		NEIS
	내부 직원용		S사
	은행간편인증(든든인증)		KB국민은행
	앱 인증		카카오뱅크, 토스
	송금, 페이		카카오페이
	Blockchain ID		뱅크사인

❖ Cloud-Based Digital Signature



Digital Document(Message)

No ActiveX

No 프로그램 설치

❖ 클라우드기반의 전자서명 장점

- ✕ 하드웨어 투자나 유지비용이 필요 없음
- ✕ 전자서명 개발 작업이 필요 없음
- ✕ 암호화 및 서명의 전문 지식이 필요 없음

- ○ 장소나 시간에 관계없이 전자서명 가능
- ○ 클라우드에 직접 인증서 발급 가능
- ○ 최고 수준의 물리적 보안 저장소인 HSM에 인증서 저장

❖ Global 기업의 클라우드 전자서명 서비스

- **Adobe사 클라우드 기반 디지털 서명 발표 (2017. 2)**

Sign on the go.
Sign documents using web browsers and mobile devices, in addition to desktop.

No downloads.
No need to download the document before signing.

Simple certificate ownership.
Certificates are managed in the cloud by the trusted service provider of your choice.

Easy deployment for signers and companies.
An alternative to smart cards, USB tokens, driver installations, or dedicated software.

- **GlobalSign Digital Signing Service 발표 (2017. 6)**

Cloud-based Digital Signing Service

GlobalSign's cloud-based Digital Signing Service makes digital signatures accessible to organizations through document workflow providers, creating a true end-to-end solution and lowering barriers such as cost, hardware requirements, maintenance, and internal expertise.

Bringing together all the cryptographic components necessary to offer the most feature rich and collaborative digital signature service, it is also the most secure — with no database of private keys to compromise and no documents are ever stored, even in hashed forms.

- Build trusted digital signatures into existing document workflow solutions
- Sign with individual or department-level identity
- Outsource cryptography and PKI to a trusted third party CA
- All crypto components included – signing, certificate issuance, timestamping, etc.
- Meet regulatory compliance around e-signatures
- Easy integration via API or SDK and high throughput scale to meet signature demand

Signing Certificates Stored on HSM

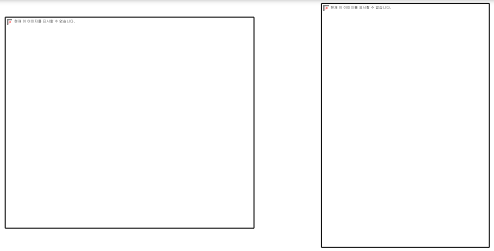
Organizations who want to integrate with an internally developed or off-the-shelf automated document application, can use an HSM deployment. Internal PKI expertise is required to configure the integration between the HSM and document workflow.

The signing credential, issued by GlobalSign, is issued to organization- or department-level identities (e.g., Accounting, Finance) and is stored and protected on a FIPS-compliant hardware security module (HSM).

- Build digital signatures into existing document workflows and automate the signing process
- Sign with organization- or department-level identity
- Support higher volume signature needs
- Meet digital signature compliance regulations
- Timestamp documents to support time-sensitive transactions, audit trails, and non-repudiation

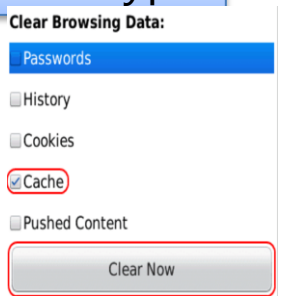
❖ 국내 전자서명의 이슈

설치 프로그램 전자서명 Type



브라우저 전자서명 Type

www.aaa.com www.bbb.com



스마트폰 전자서명 APP

❖ 국내 클라우드 전자서명 서비스

한국전자인증

이니텍

위즈베라

티모넷

❖ 이니텍 - INIPASS

❖ 이니텍 - INIPASS

1. 노 플러그인(No-Plugin)

➡ **Non-Active X, No Plugin 공인인증서 사용으로, 사용자의 불편함을 감소하고 정부에서 권장하는 형태의 공인인증서 사용환경을 제공함**

- 정부의 No-PlugIn 정책에 따른 가입자 S/W 지원

2. 안전한 저장

➡ **발급한 공인인증서를 스마트폰 내 트러스트존(TrustZone)과 클라우드 HSM에 보관해 해킹으로부터 공인인증서가 유출되는 것을 차단함**

- FIDO 인증 등을 통해 본인확인이 된 경우에만 해당 키에 접근 가능

3. 갱신 후 재등록 無

➡ **OAuth 인증을 통해 얻은 사용자 식별자는 인증서가 갱신되어도 변하지 않아 재등록 없이 사용 가능함**

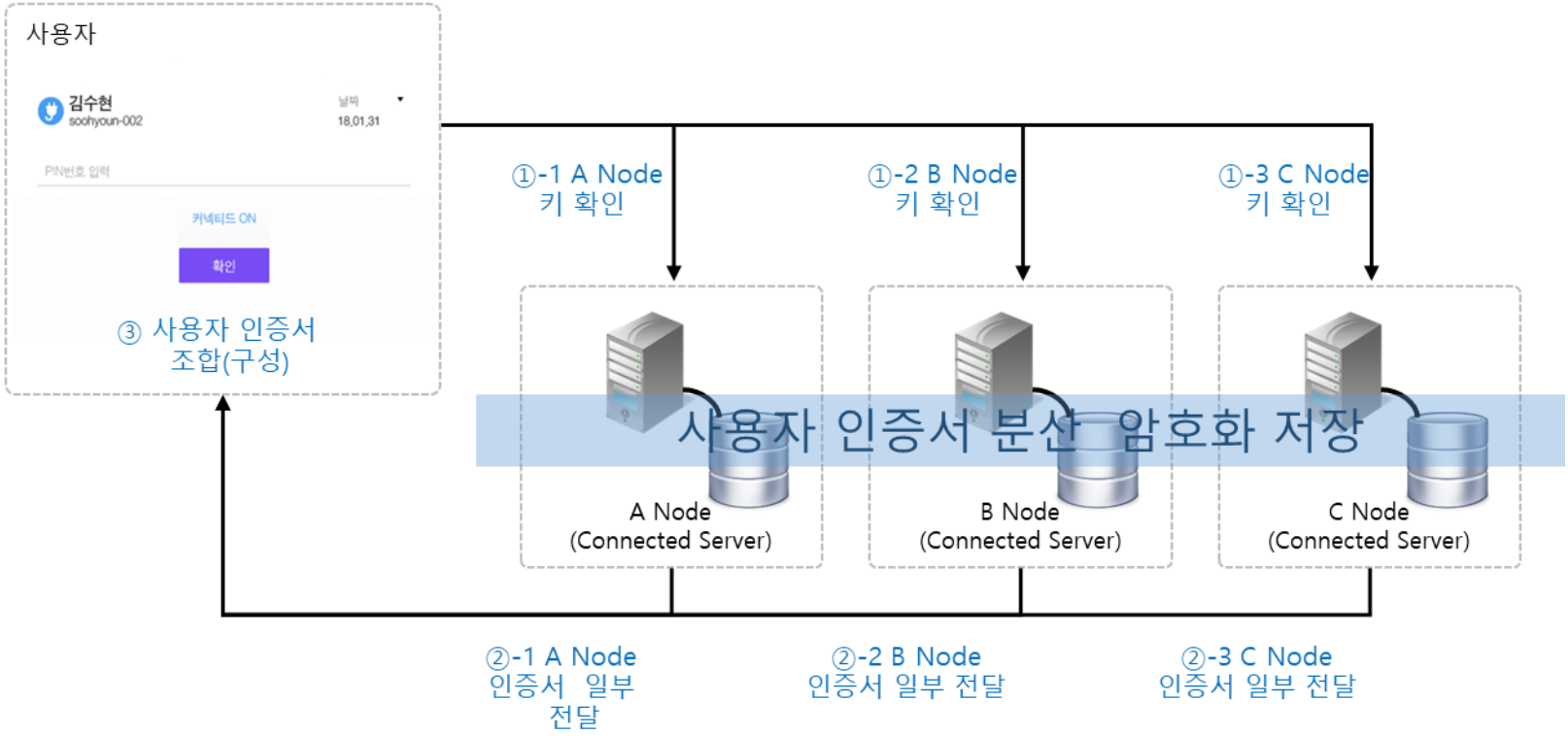
- 3년 유효기간으로 갱신의 불편함 최소화
- 갱신 후에도 재등록 없이 공인인증서 로그인 가능

4. 간편 발급

➡ **이용자가 어떤 통신사를 쓰던, 전국 250개 KT직영점(M&S)을 통해 신분증과 스마트폰만 있으면 그 자리에서 바로 발급 가능**

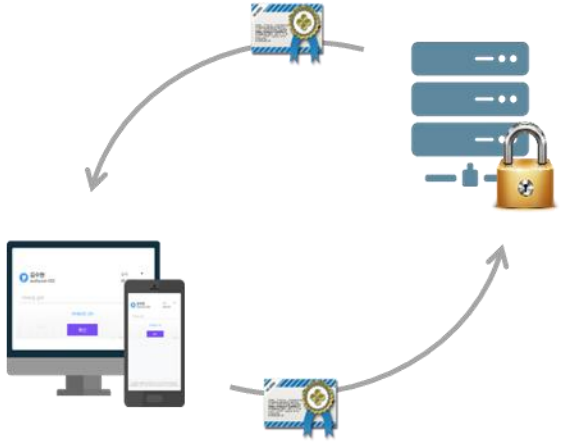
- 등록기관의 다양화를 통한 이용자 접근성, 편의성 향상

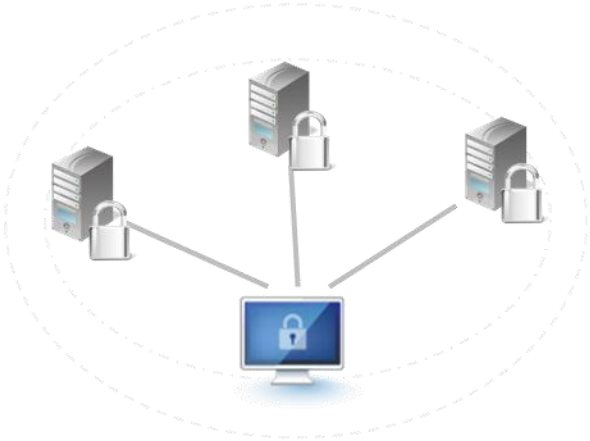
- 구성
  - WizIn-connected 서버에 분산 처리 보관
  - 분산 서버에 접근할 수 있는 별도의 키를 사용자 WebCrypto 영역에 보관



언제 어디서나 간편하게!!

- 인증서 휴대 없이 언제 어디서나 인증서 사용 가능
- 설치 없이 휴대전화 번호 연동으로 간편 사용
- 디바이스 및 브라우저에 영향 받지 않는 범용성 제공





더 강력해진 보안으로 신뢰성 확보!!

- 인증서는 Connected 서버에 분산 처리 보관
- Connected 서버에 접근할 수 있는 Key 별도 발급
- Connected에 저장된 인증서는 사용 시에 사용자에게 전달
- **현행 전자서명법 제2조 3 에 부합**
  - **전자서명생성정보가 가입자에게 유일하게 속할 것**
  - **서명 당시 가입자가 전자서명생성정보를 지배관리하고 있을 것**

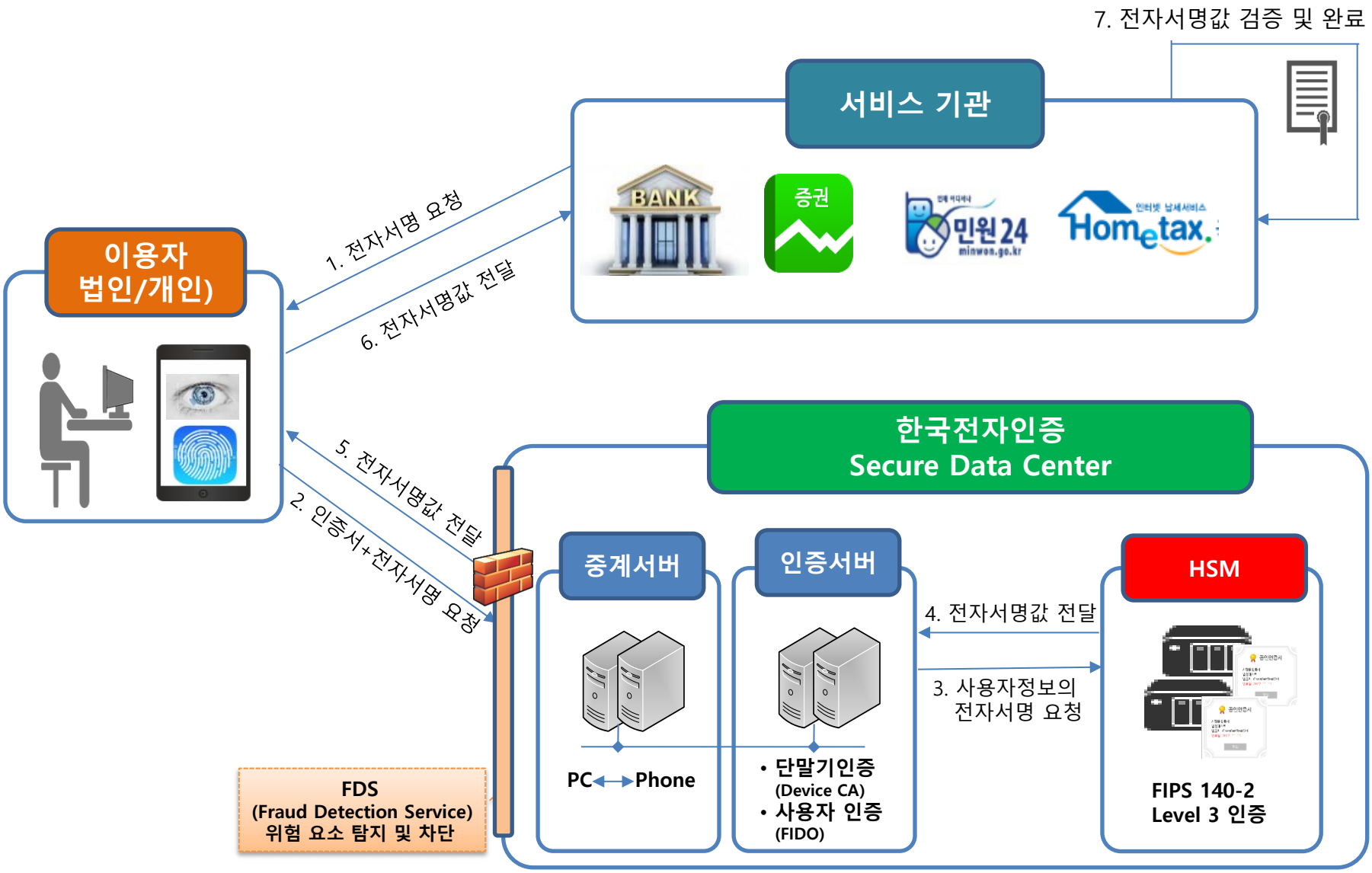
❖ 한국전자인증 – 클라우드사인

✓ 국내 최초 클라우드 전자서명 서비스 – 2017년 11월 Open

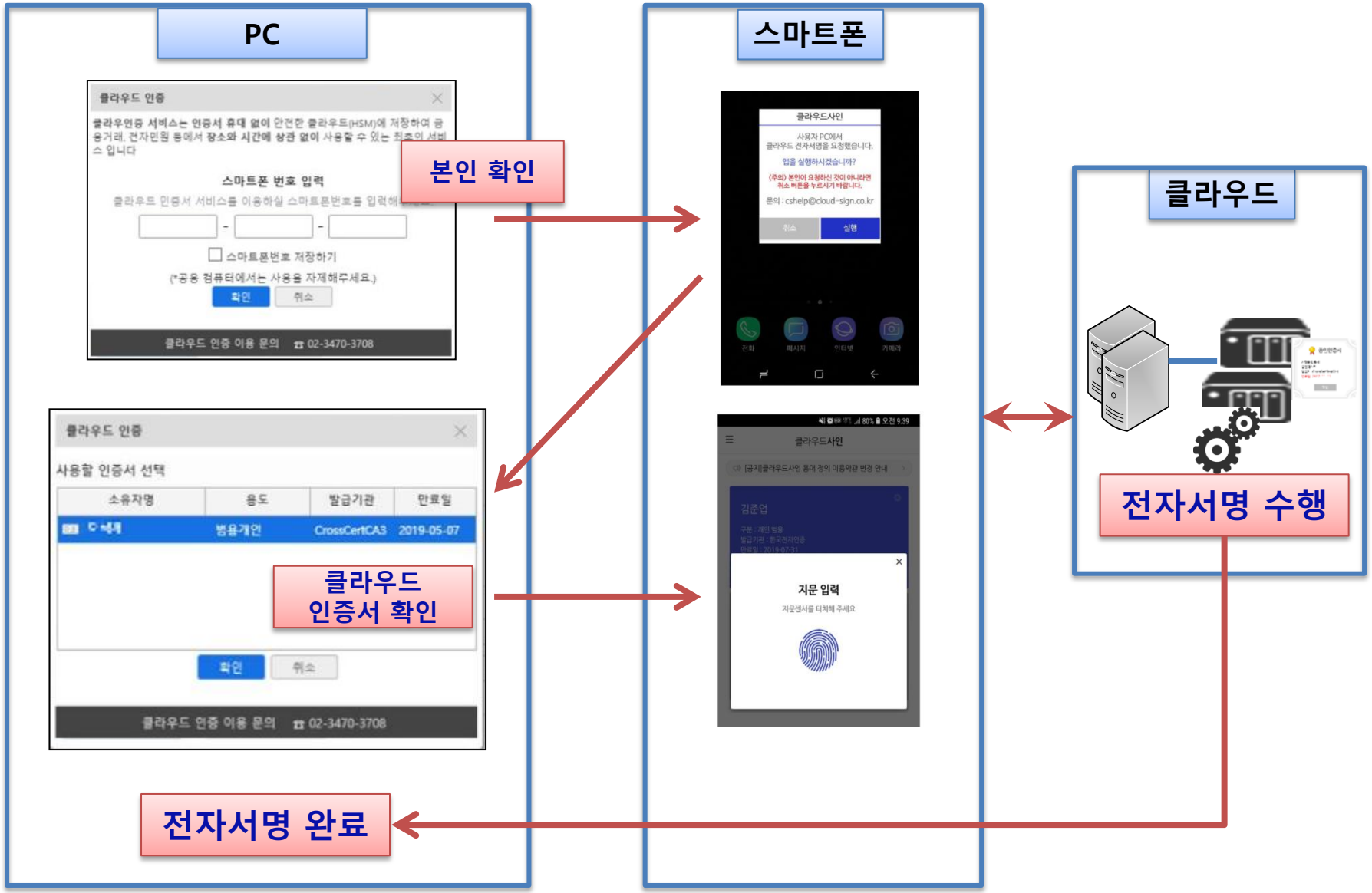
CloudSign

구분	기존 전자서명 서비스	클라우드사인
편리성	프로그램 설치	무설치
	비밀번호 입력	지문, 간편비밀번호
	저장매체 소지	클라우드 이용
안전성	인증서 유출	HSM 보관 (Hardware Security Module)
비용	고비용	무료(개인 인증서)

❖ 한국전자인증 - 클라우드사인



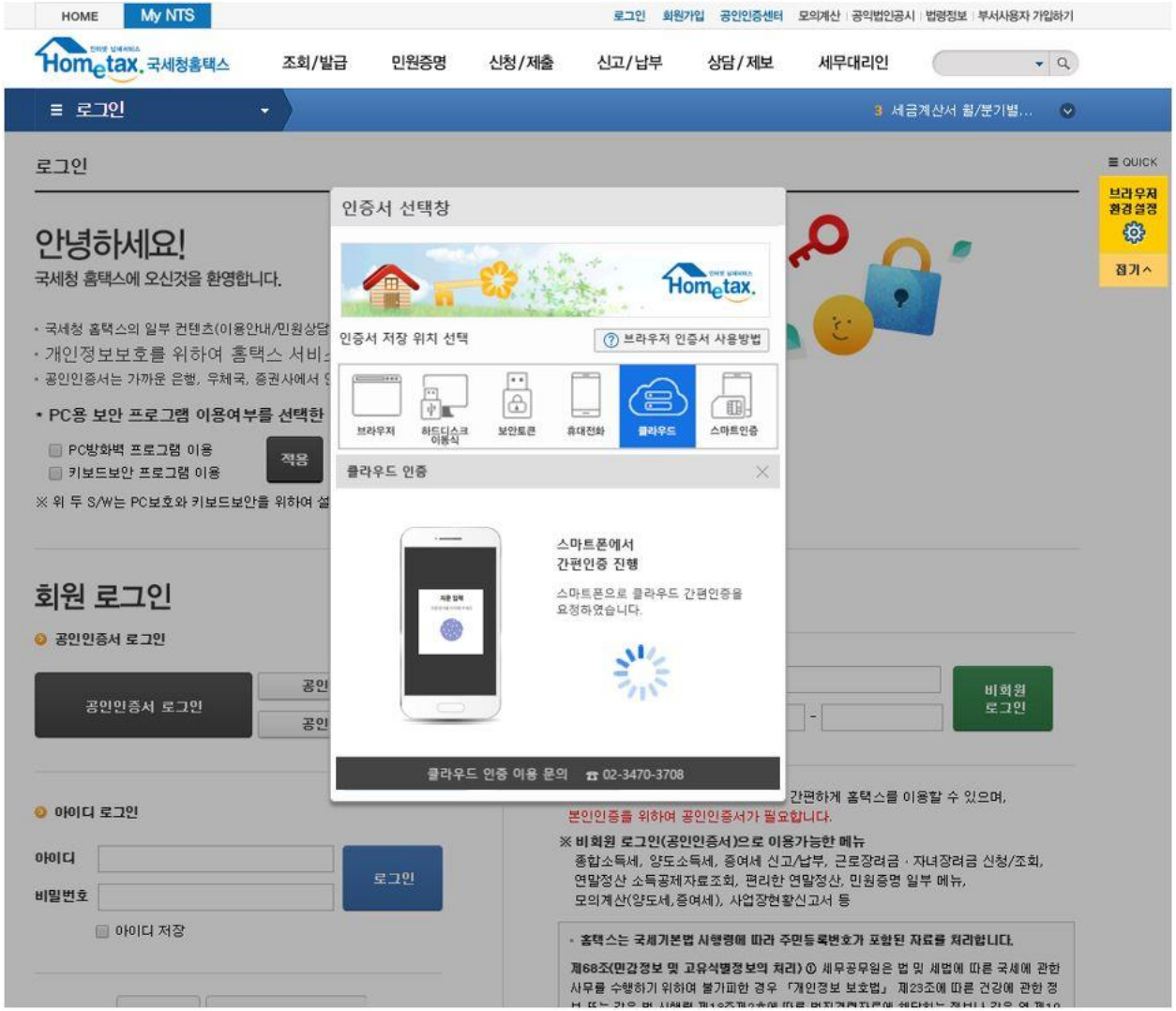
❖ 무설치의 클라우드사인



❖ 한국전자인증 - 클라우드사인 특장점

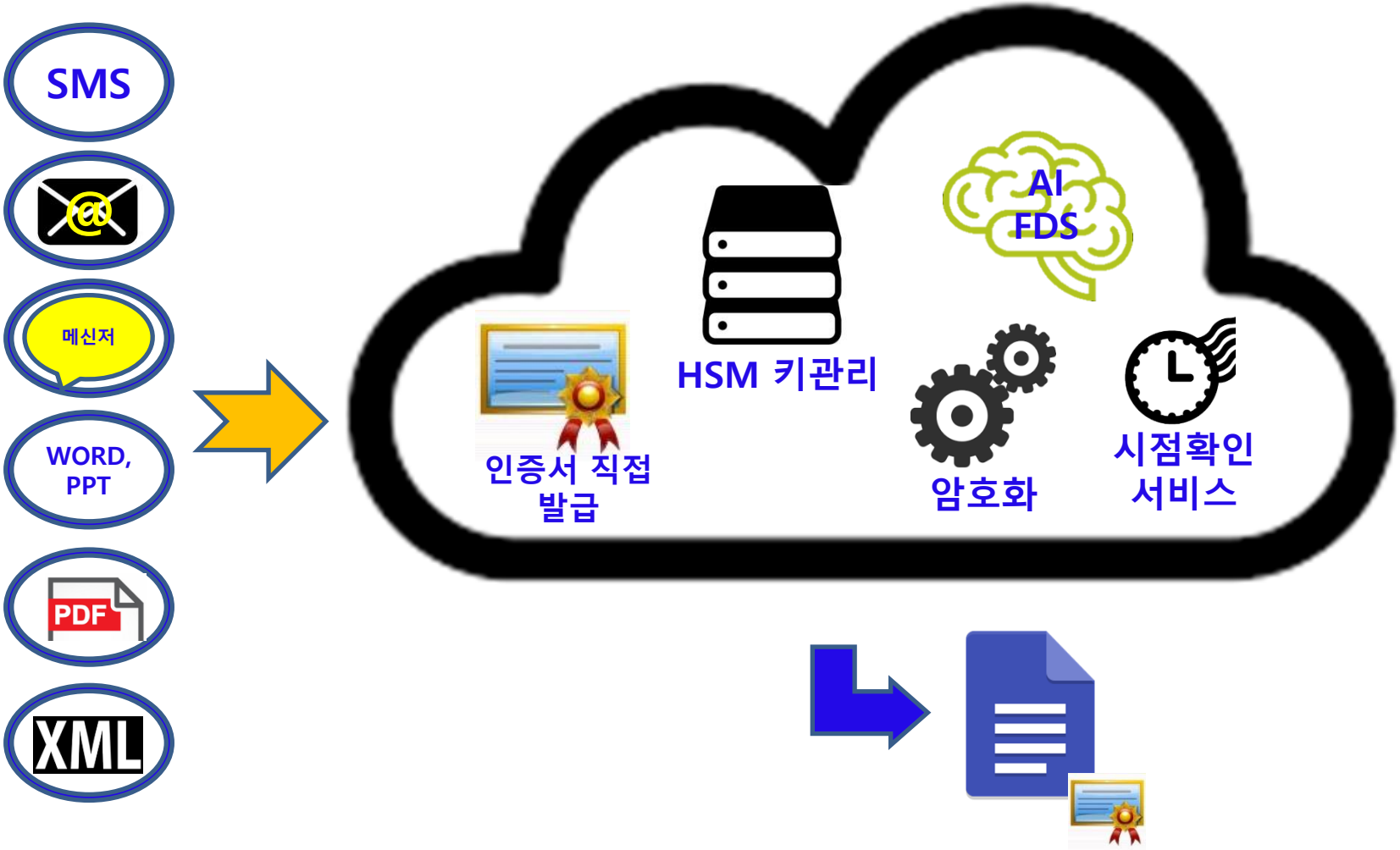
- **공인전자서명, 사설전자서명 모두 이용 가능**
- **ActiveX, EXE 프로그램 설치 없는 100% 무설치 환경 제공**
- **장소, 시간의 제한 없이 인가된 기기로 안전하고 편리하게 접근 사용**
- **기존의 인증모듈과도 호환성을 확보**하여 모든 사이트 이용가능
- FIPS140-2 Level 3 보안매체(HSM)에 보관하여 **외부 유출 문제 해결**
- **소유자의 통제성 강화 - 지문인증, 디바이스인증, 사용기기 제어(On/Off 설정)**
- **매년 갱신 불편 해소 - 유효기간 3년형 인증서 발급**

❖ 한국전자인증 - 클라우드사인 홈택스 데모 영상



❖ 클라우드기반의 전자서명 향후

Cloud-based Digital Signature



❖ Q & A

Google Play App Store

한국전자인증 안군식 본부장, ksahn@crosscert.com