PKI 기반 보안 시스템

Public Key Infrastructure

2024-05-15

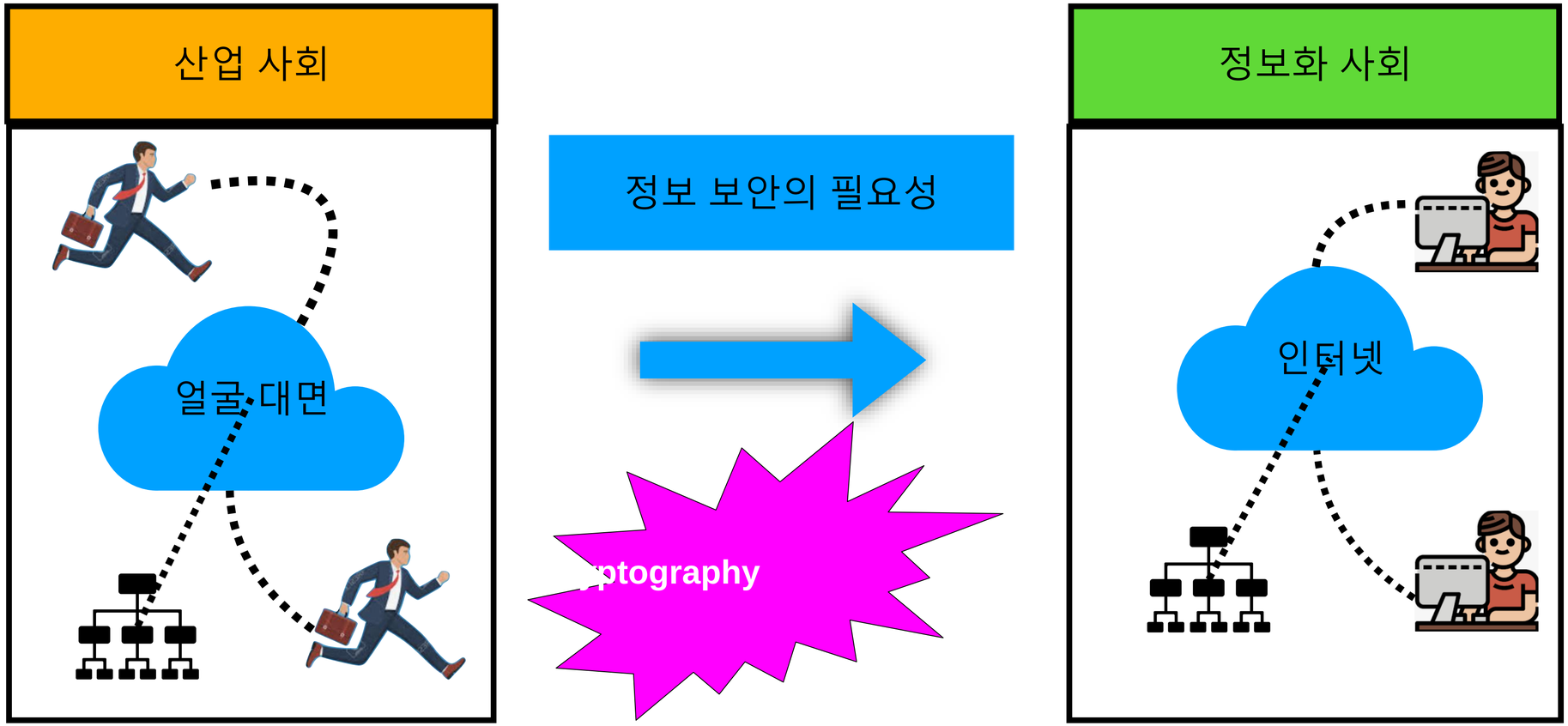
PKI 기반 보안 시스템

목차

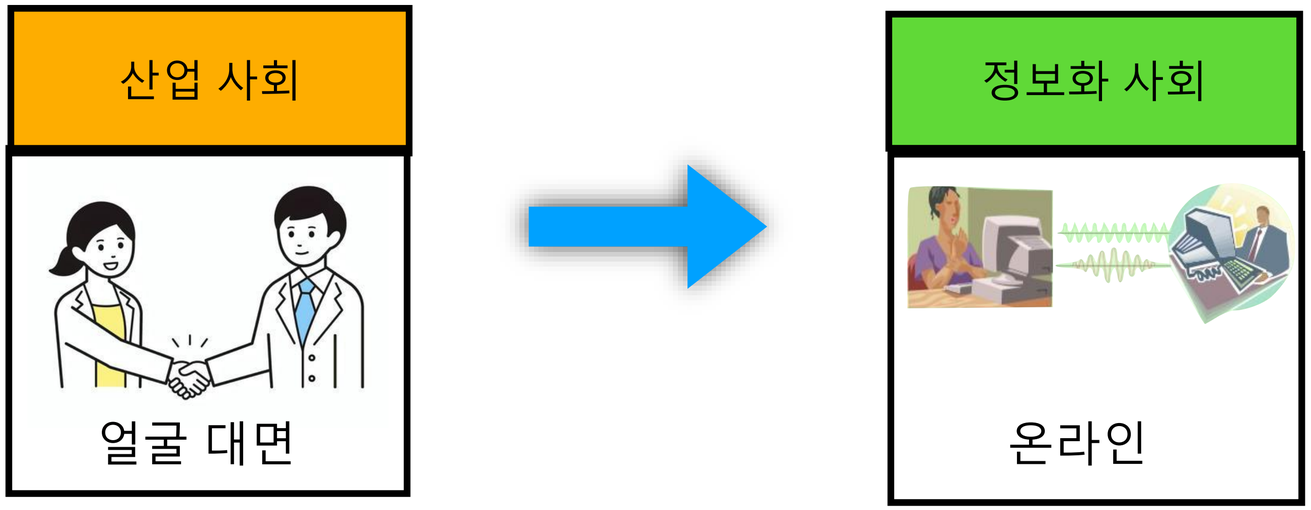
1. 교육의 개요

- 정보 보호를 위한 암호화 필요성 및 개념이해
- 인증서와 CRL 개념 이해
- PKI 구성 요소에 대한 이해
- PKI 시스템 서비스 및 관련 표준에 대한 이해

산업 사회와 정보화 사회



전자 거래의 문제점

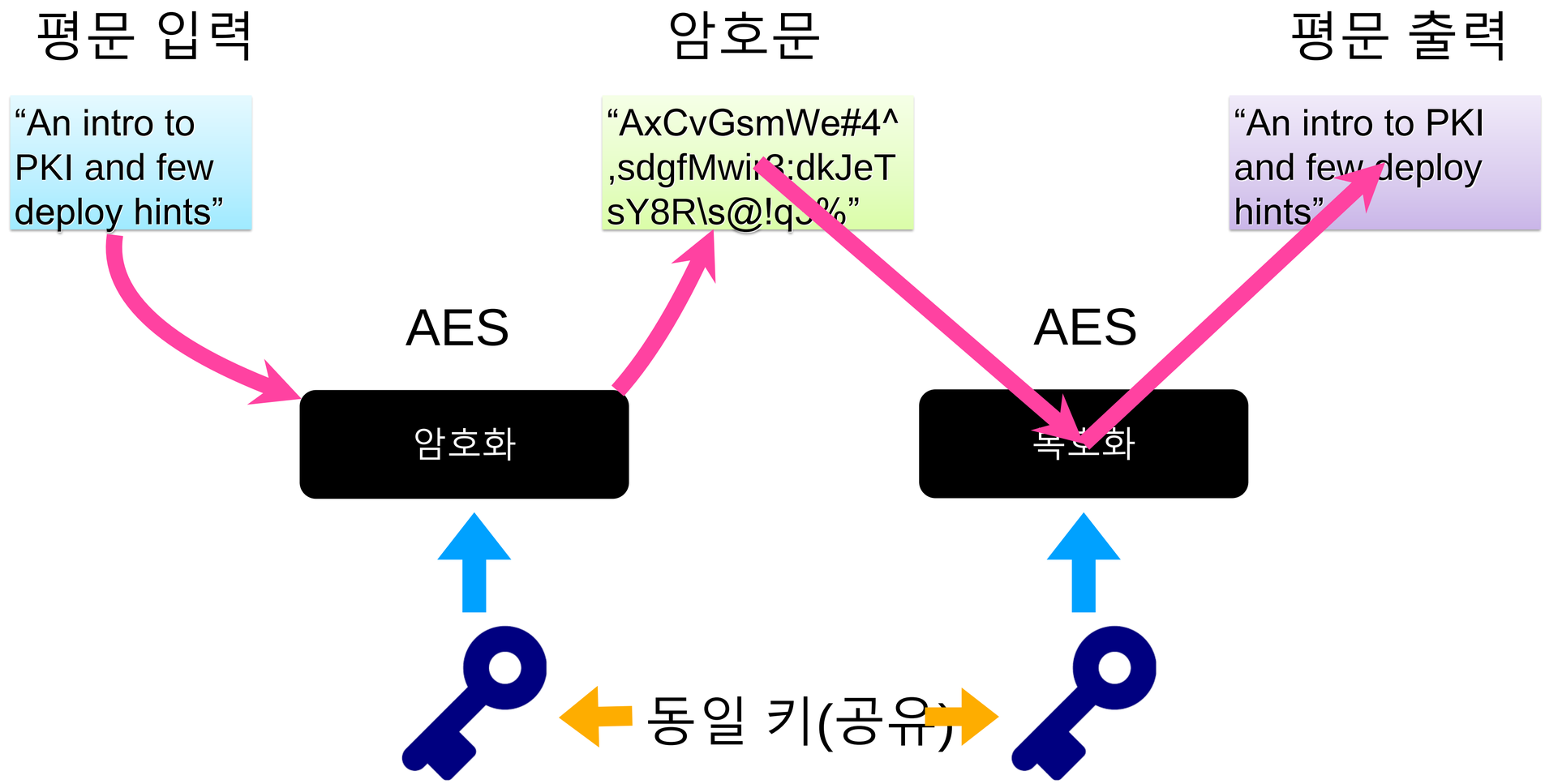


❖ 전자 거래 위험 요소
- 거래 정보 노출에 대한 위험성 → 기밀성 (Confidentiality) → Encryption
- 거래 정보 변경에 대한 위험성 → 무결성 (Integrity) → Digital Signature
- 정보 전송 사실에 대한 부인 위험 섬 → 부인 방지 (Non-Repudiation) → Digital Signature
- 발신자 신원 속임애 대한 위험 성 → 인증 (Authentication) → Digital Signature

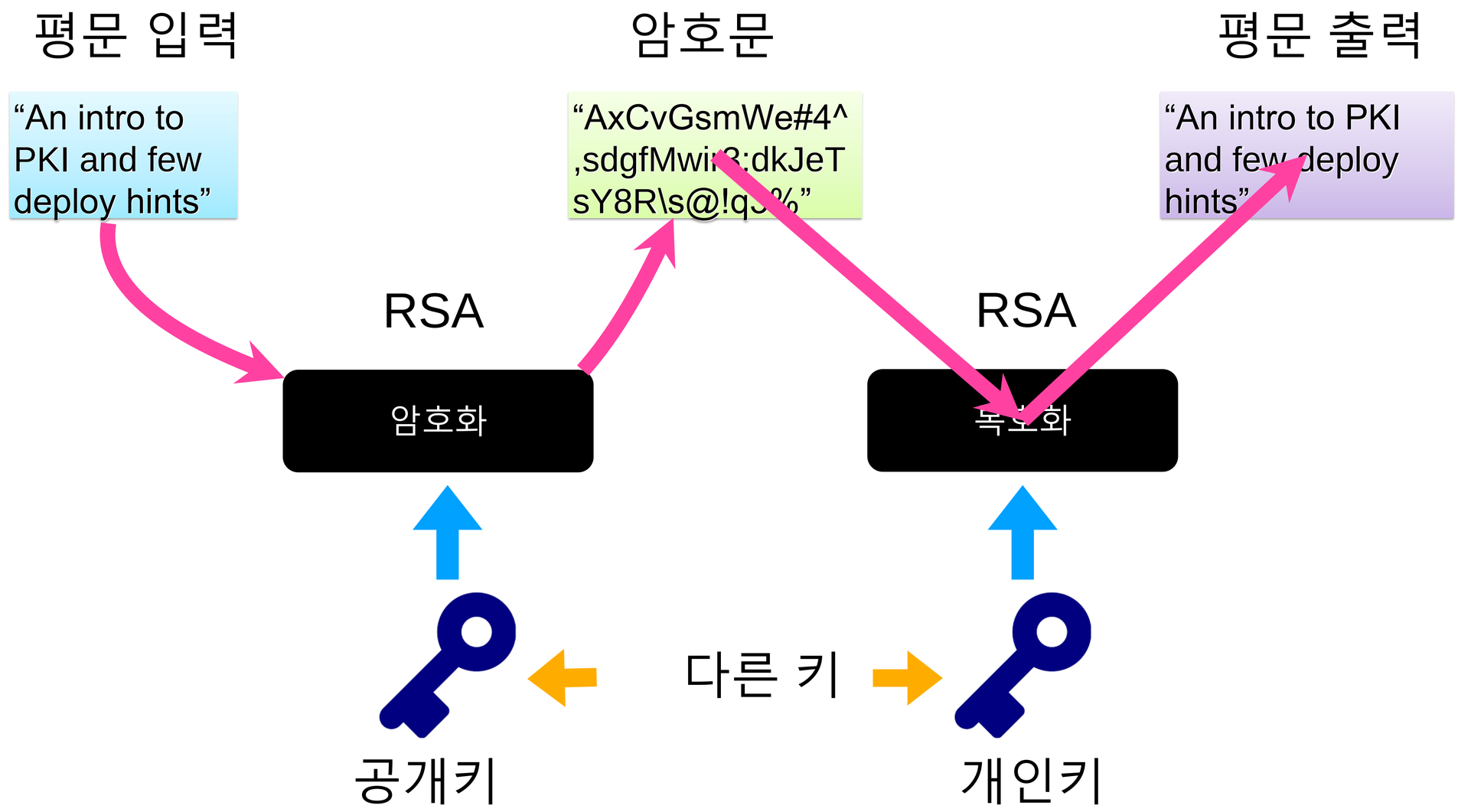
암호화 (Cryptography) 필요성

- 기밀성 (Confidentiality)
  - 모든 메세지를 가지고도 정보를 알 수 없어야 하는 것
- 무결성 (Integrity)
  - 메세지가 전송 되는 중에 변경 되지 않아야 하는 것
- 인증 (Authenticity)
  - 실제로 대화를 하는 대상이 해당 대상이 맞는지 검증 하는것
- 부인 방지 (Non-reputation)
  - 행위에 대한 부인을 할 수 없게 하는 것

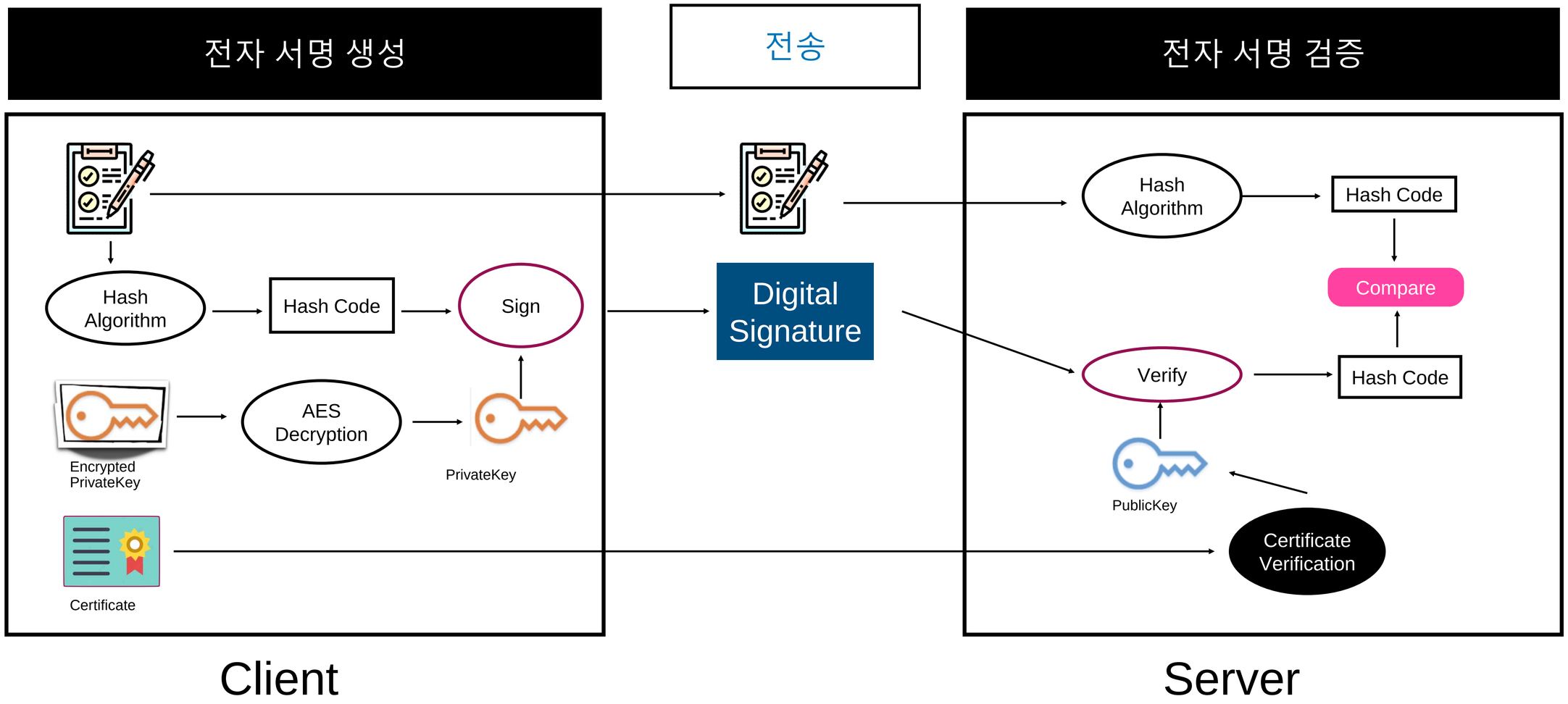
대칭키 암호 (Symmetric Encryption)



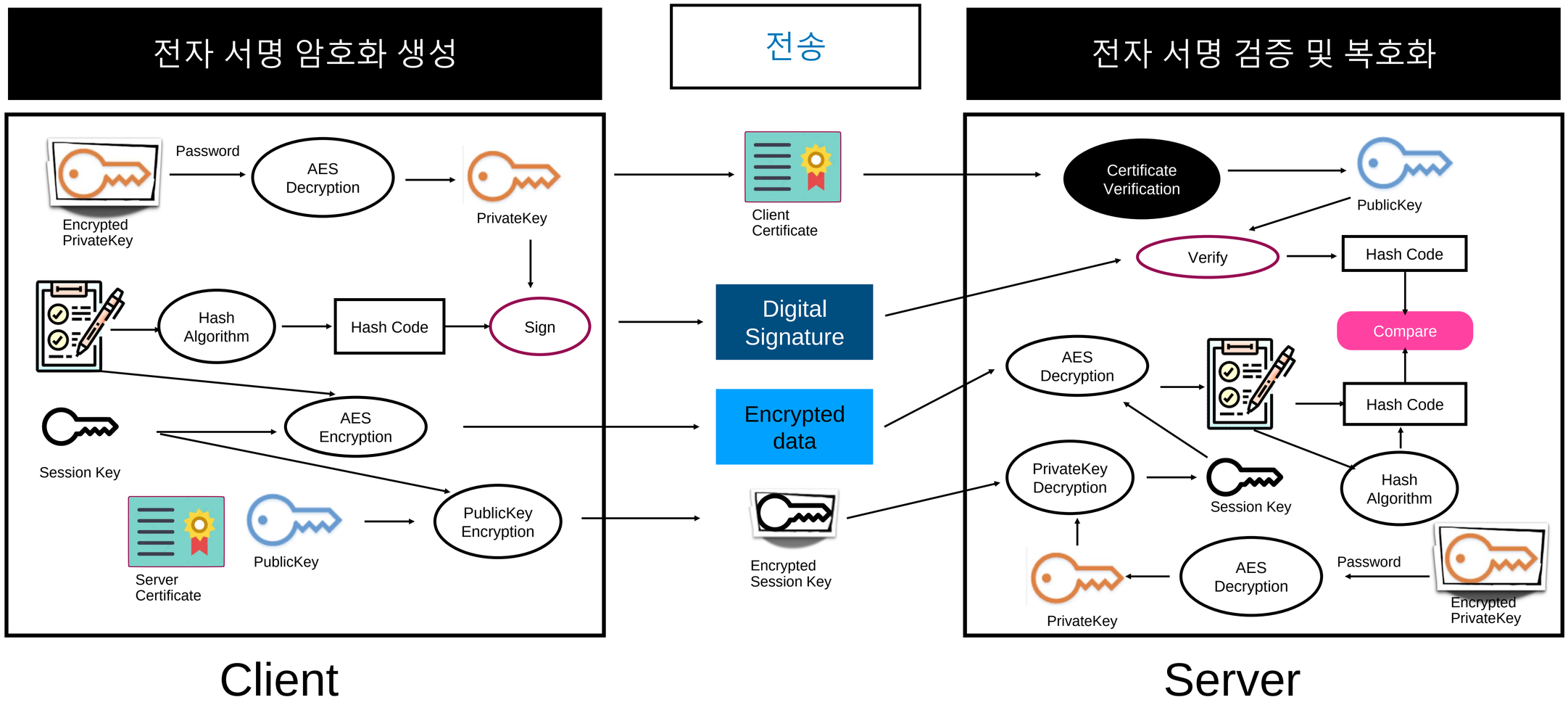
비 대칭키 암호(Asymmetric Encryption)



Authentication, Integrity, Non reputation

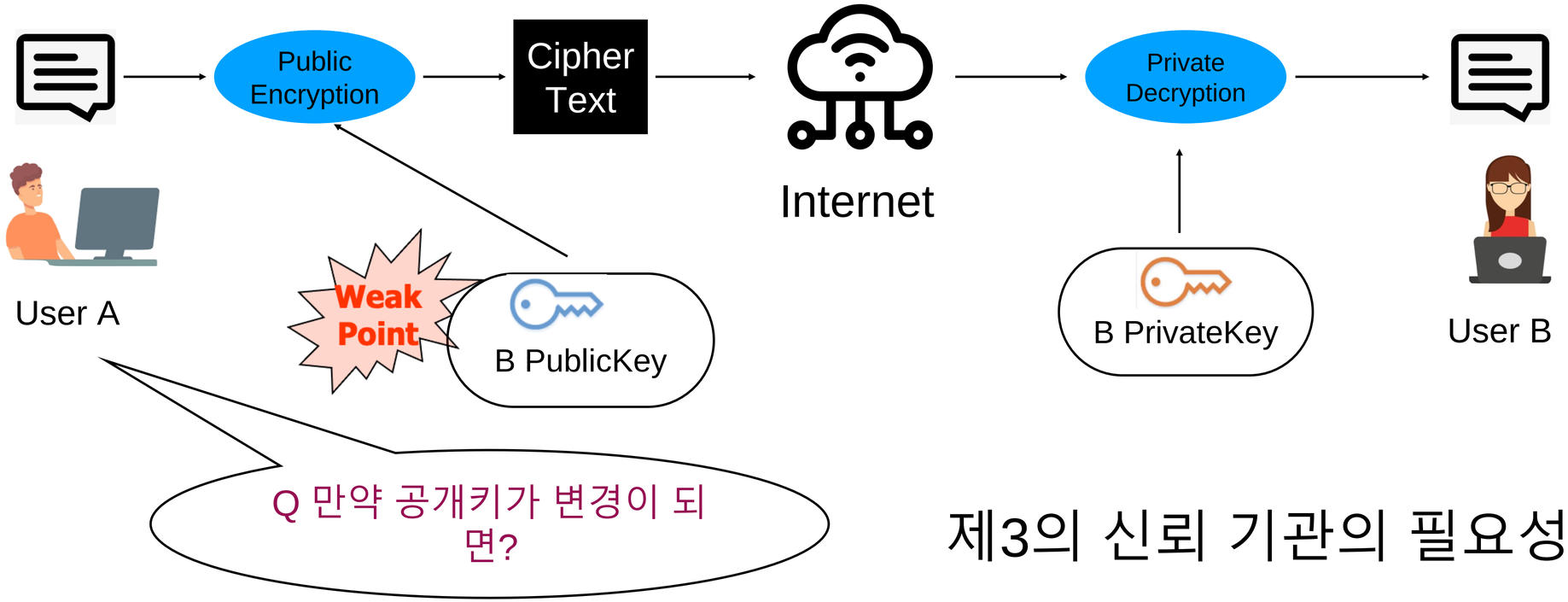


Authentication, Integrity, Non reputation,Confidentiality



인증서 필요성

PublicKey -> Certificate



제3의 신뢰 기관의 필요성

- CA (Certificate Authority)

인증서란 무엇인가?

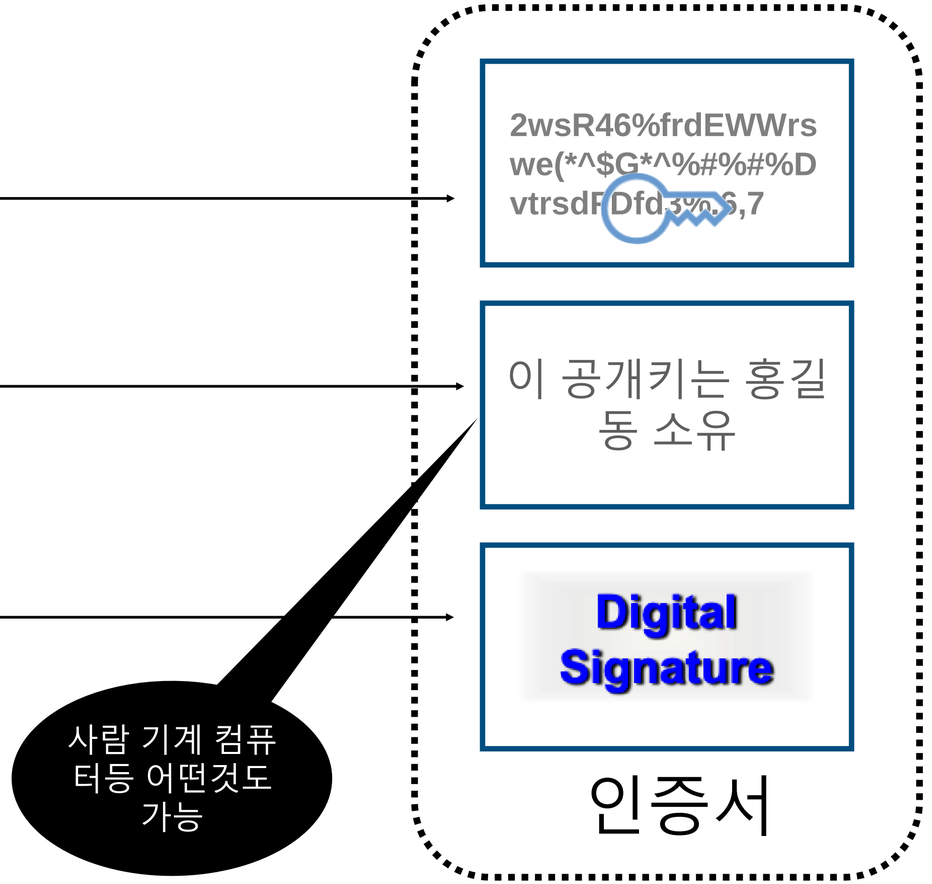
인증서 정보 내용

공개키

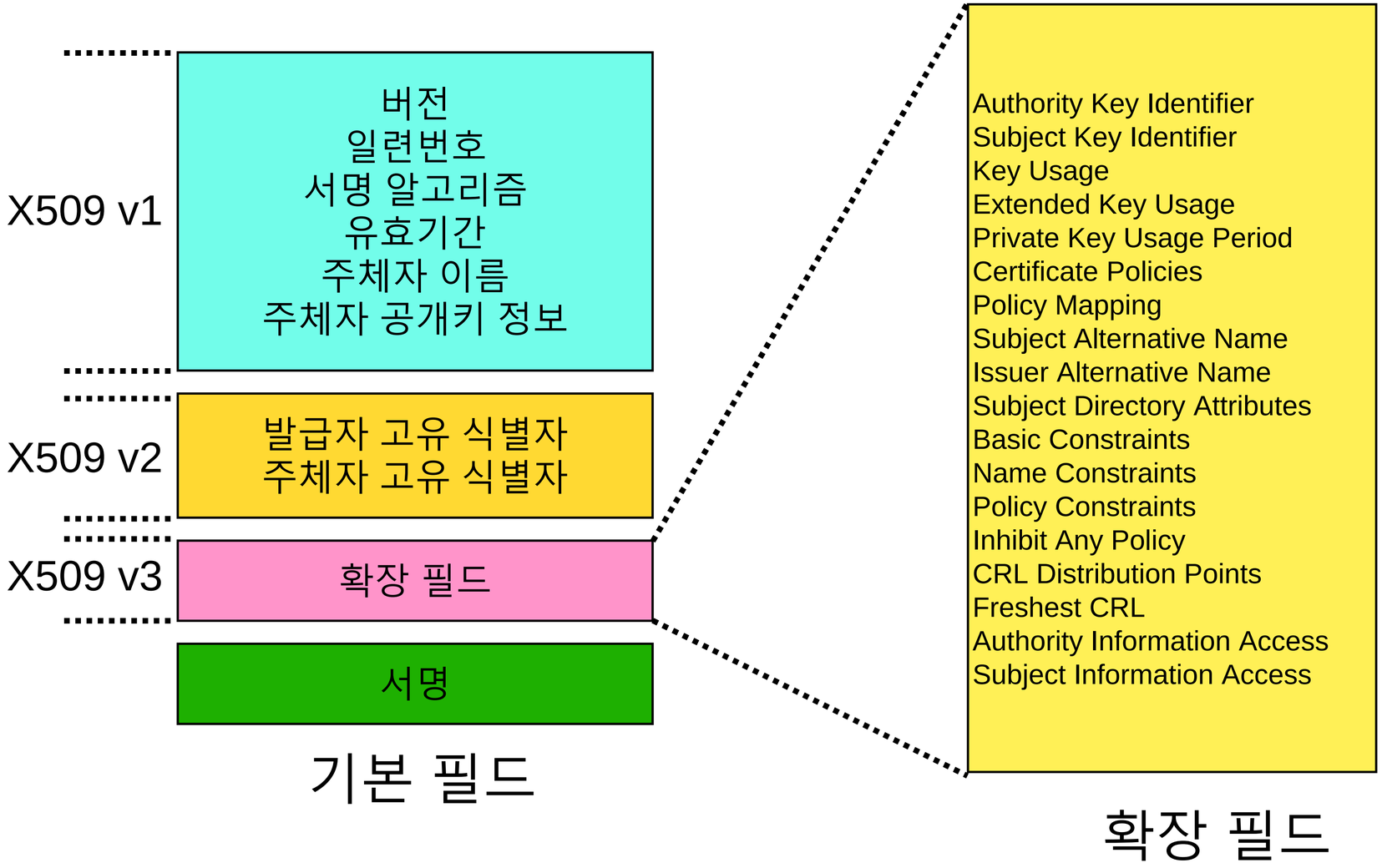
공개키를 가지는 인증서 관련 정보

신뢰된 기관의 서명

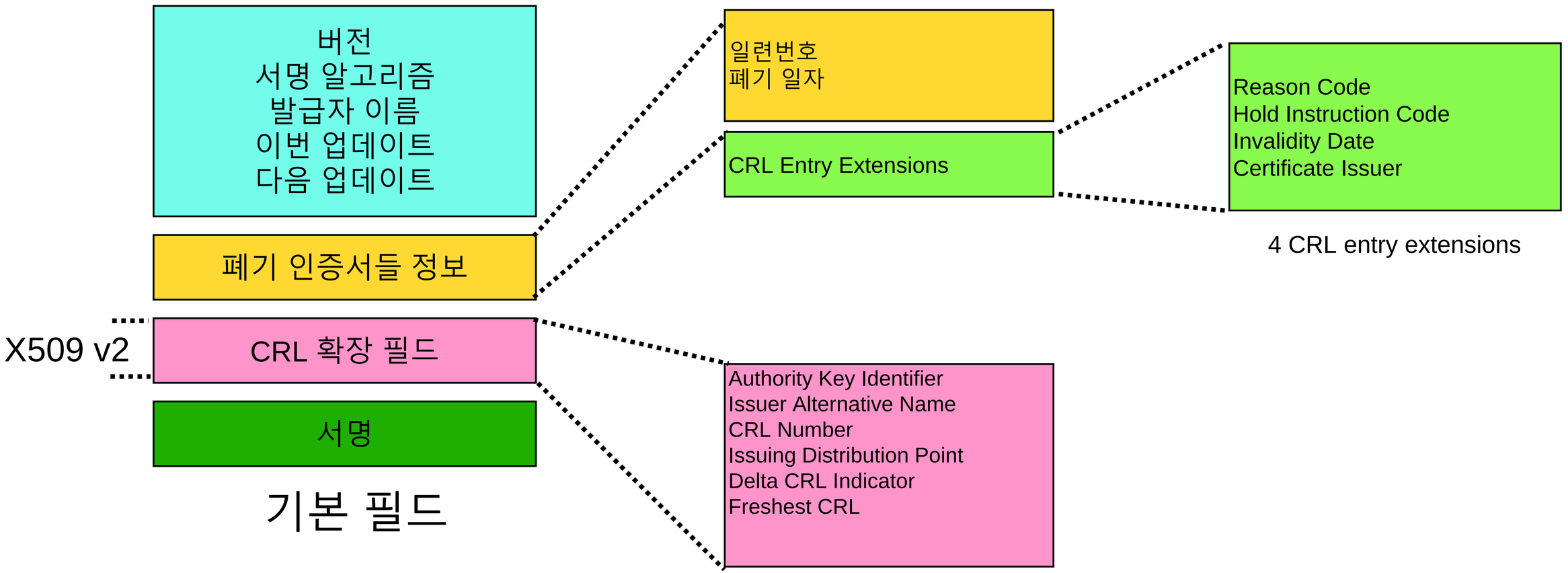
CA 기관



X.509 인증서 프로파일

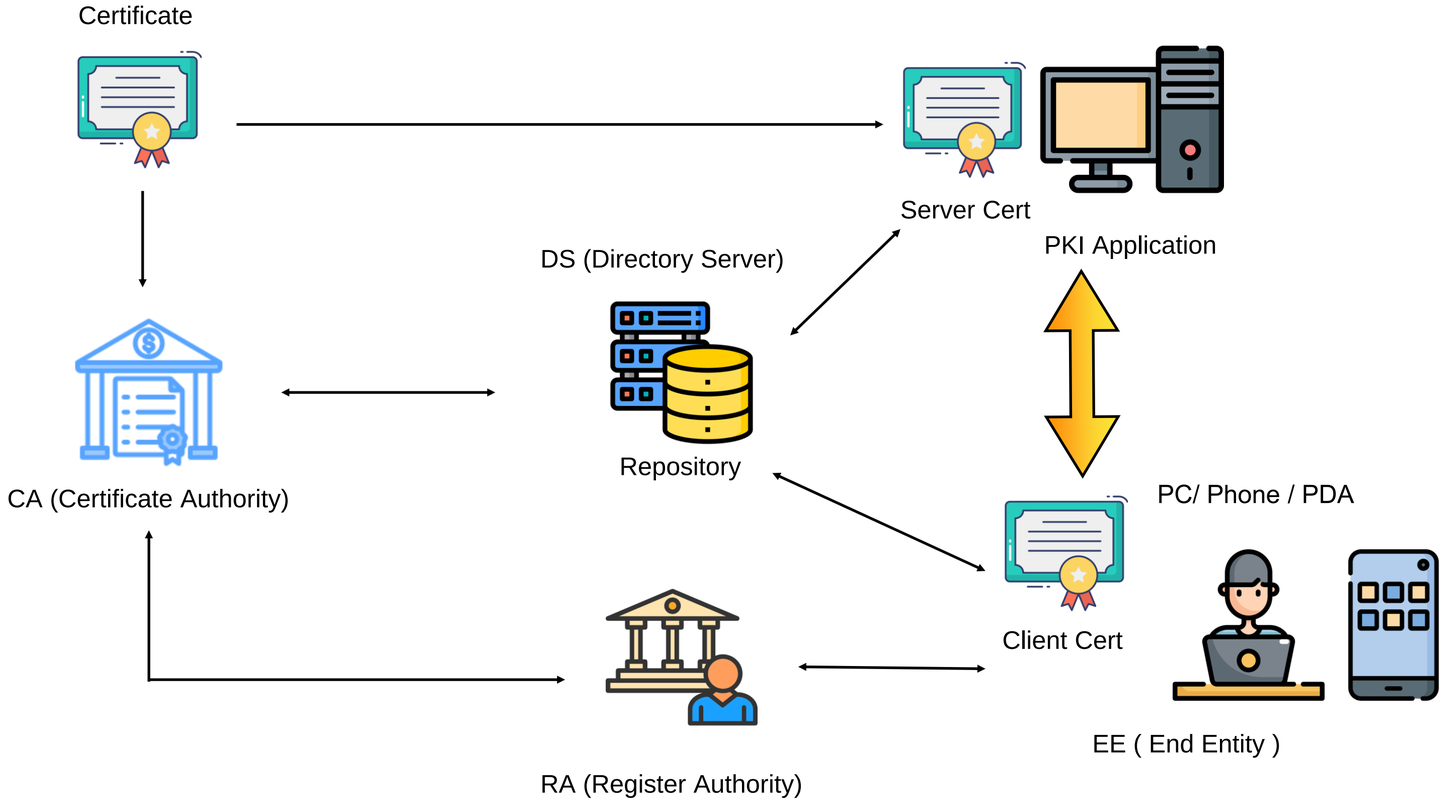


X.509 CRL 프로파일

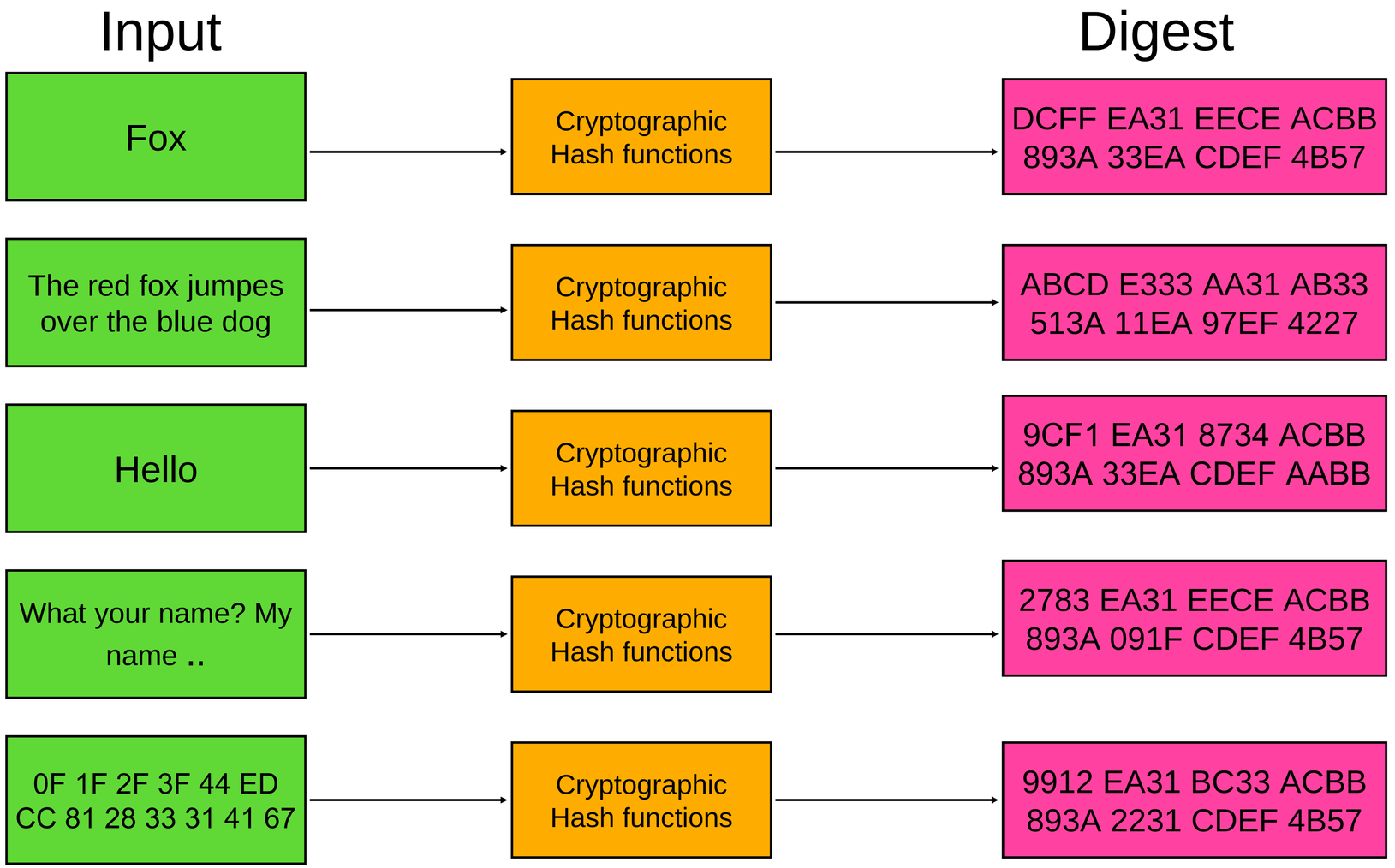


Public Key Infrastructure

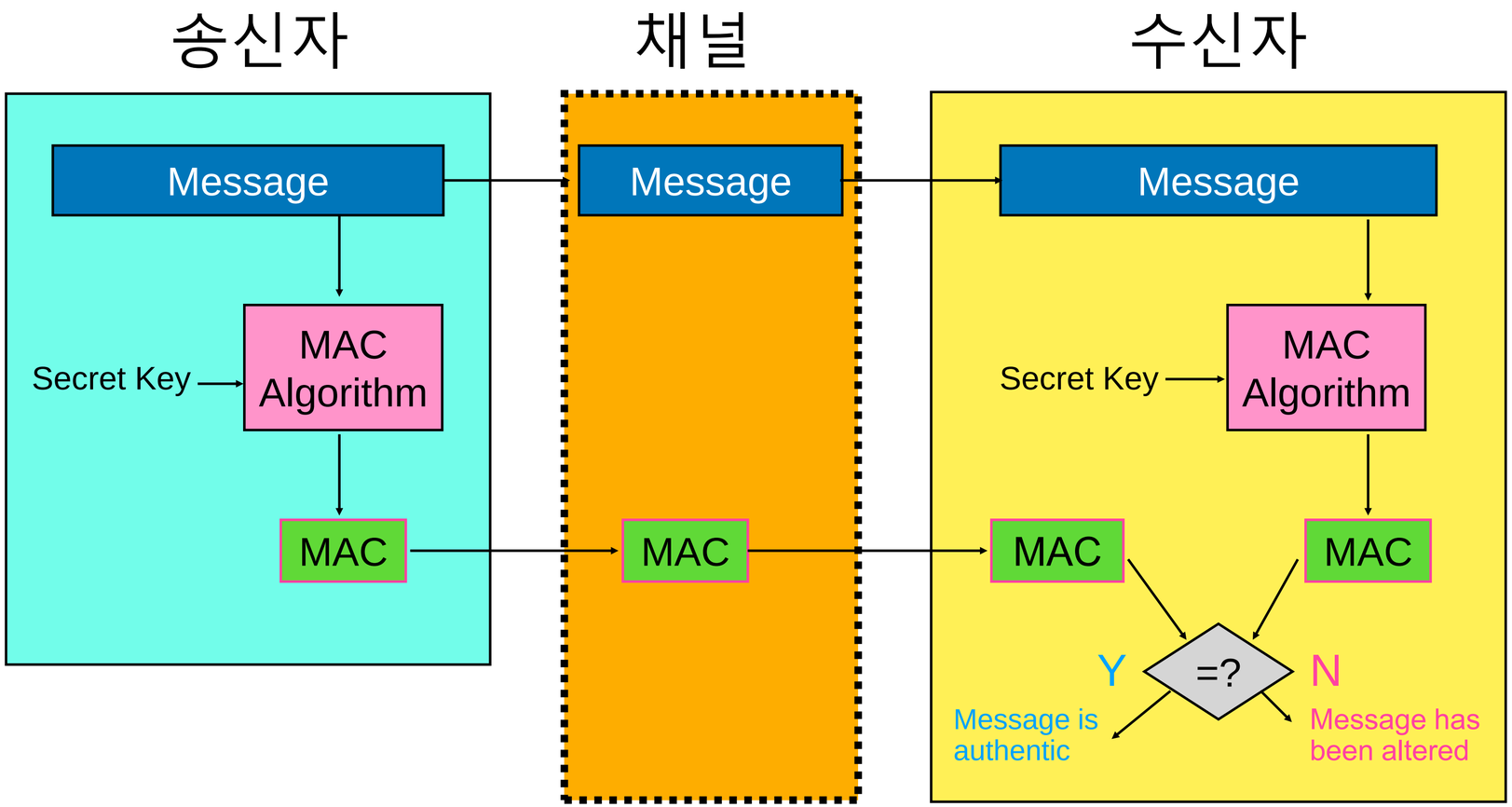
♣ 공개키 기반 구조(PKI) 는 디지탈 세계에서 사람이나 장치에 대한 인증을 위한 기술이며 공개 키 암호화를 기반으로 정보를 교환하는 안전한 방법을 만드는 시스템이다.



Hash function



MAC (Message Authentication Code)



PKI 구성 요소

❖ CA (Certificate Authority)

- 다른 CA, 사용자 또는 RA 인증서 발급 및 배포
- RA 또는 사용자로 부터 폐기 요청 처리
- 인증서 또는 CRL 을 DS 에 배포

❖ RA (Register Authority)

- 사용자 확인 및 사용자 정보 등록
- CA 에게 인증서 발급 요청
- DS로 부터 인증서 및 CRL 검색
- 인증서 폐기 요청

❖ DS (Directory Server)

- 인증서 및 CRL 저장 및 배포
- LDAP (Lightweight Directory Access Protocol) 지원

❖ EE (End Entity)

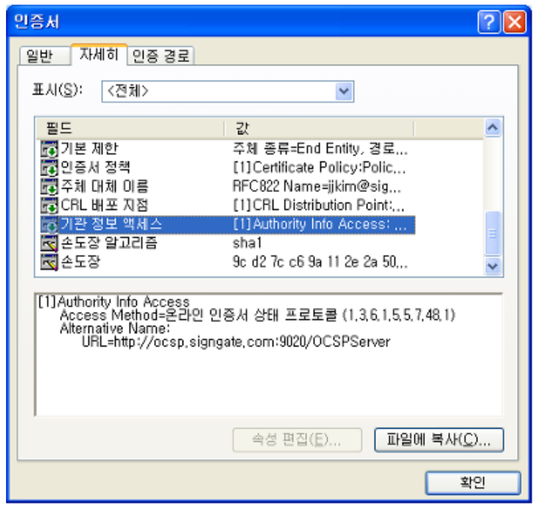
- CA 로 부터 발급한 인증서의 대상자
- 전자 서명 생성 및 검증 하기

Online Certificate Status Protocol (OCSP)

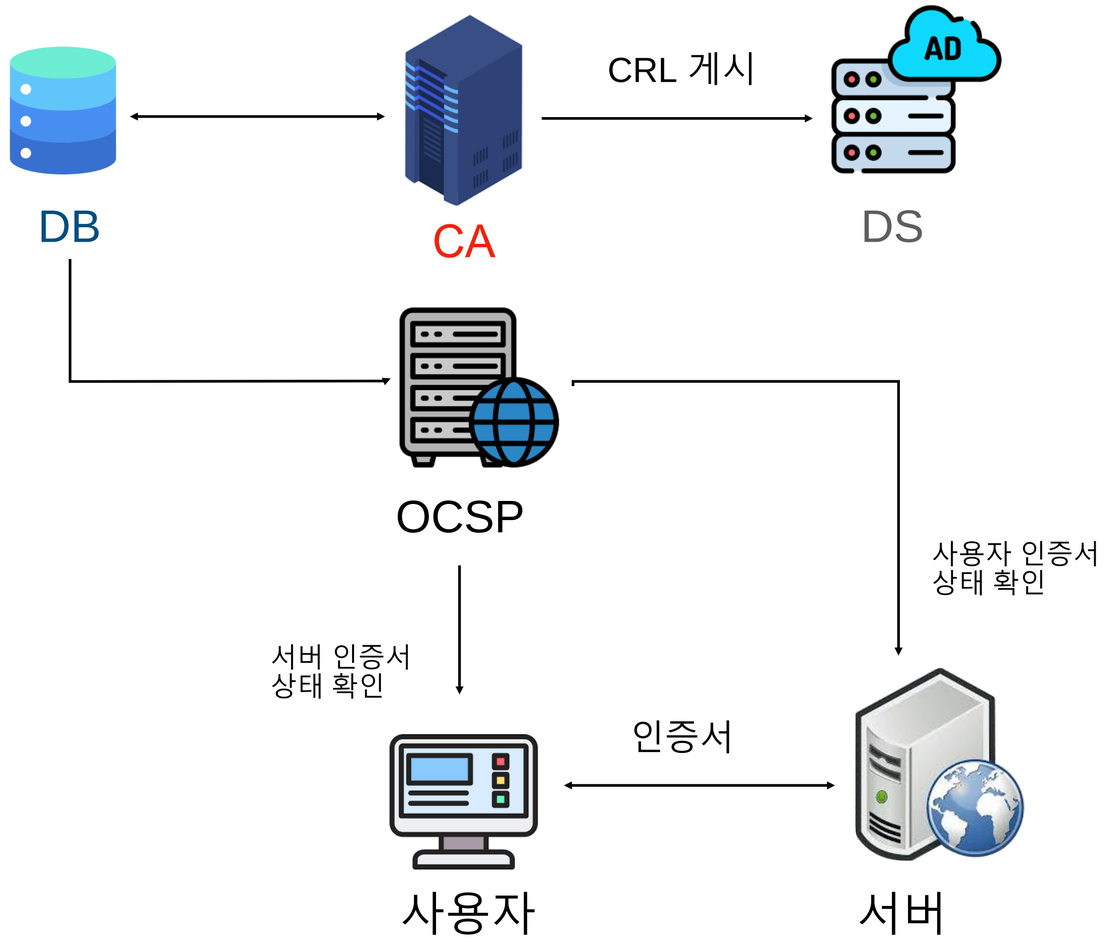
❖ CRL 문제점

1. 실시간이 아님
2. CRL은 점점 커짐
3. 네트워크 트래픽 증가

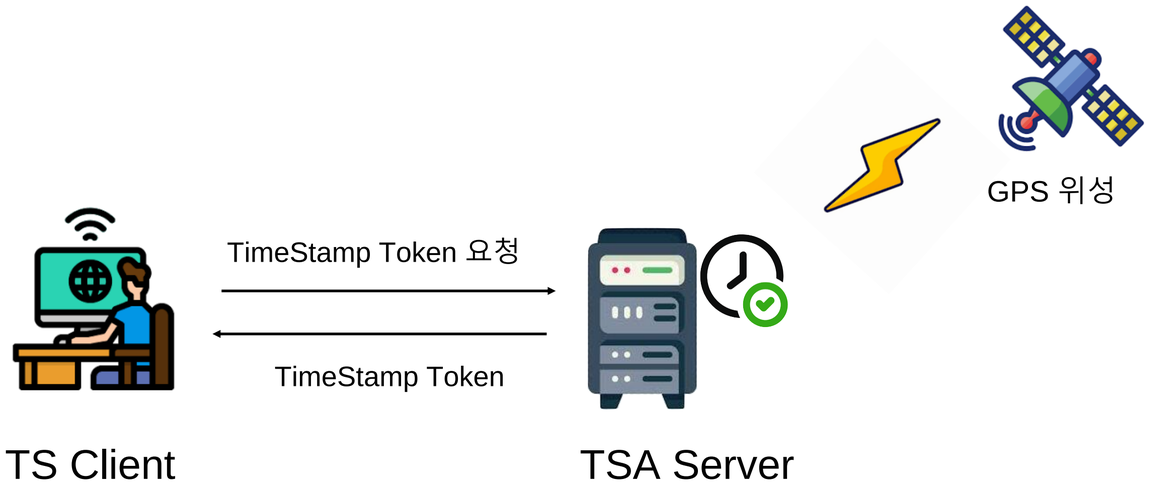
❖ OCSP 정보 확인



Authority Access Information



TimeStamp Protocol (TSP)



❖ TimeStamp Authority

TSA의 역할은 특정 시간 이전에 데이터가 존재 했음 을 나타내는 증거를 확립하기 위해 데이터에 타임 스탬프를 찍는 것

1. 해당 인증서가 폐기 시간 전 전자서명 검증을 하기 위한것
2. 전자거래의 시간이 중요한 경우 신뢰된 시간과 순서를 기록 하기 위한것
3. TSP 는 TSA 와 통신을 위한 프로토콜이다

PKCS Standard

PKCS	제목	설명
PKCS#1	RSA Cryptography Standard	RSA 암호화 설명
PKCS#2	Withdrawn	PKCS#1 로 병합 됨
PKCS#3	Diffie Hellman Key Agreement Standard	DH 키 합의 표준 설명
PKCS#4	Withdrawn	PKCS#1 으로 병합 됨
PKCS#5	Password-based Encryption Standard	패스워드 기반 암호화 표준 (PBKDF)
PKCS#6	Extended-Certificate Syntax Standard	X.509 v1 인증서 확장 표준 설명 (V3에서 사용 안함)
PKCS#7	Cryptography Message Syntax Standard	메세지 암/복호화 및 서명 검증에 관한 표준
PKCS#8	Private-Key Information Syntax Standard	개인키 암호화 복호화 표준
PKCS#9	Selected Attribute Types	PKCS#6 #7 #8 #10 속성 타입 정의 표준
PKCS#10	Certification Request Standard	인증서 서명 요청서 표준 문서
PKCS#11	Cryptographic Token Interface	Cryptoki 라이브러리 API 정의 문서
PKCS#12	Personal Information Exchange Syntax Standard	PFX 파일인 인증서, 체인 및 개인키 내보내기 파일 포맷
PKCS#13	Elliptic-curve cryptography Standard	ECC 알고리즘 표준 문서
PKCS#14	Pseudo-random Number Generation	랜덤값 생성 표준 문서 (현재는 사용 하지 않음)
PKCS#15	Cryptographic Token Information Format Standard	토큰 장치의 데이타 포맷에 대한 표준 문서

RFC standard

RFC	제목	설명
RFC 3280 RFC5280	Certificate and Certificate Revocation List (CRL) Profile	인증서 및 CRL 프로파일 설명
RFC 6960 RFC 2560	Online Certificate Status Protocol - OCSP	실시간 인증서 온라인 검증 프로토콜
RFC 3161	Time-Stamp Protocol (TSP)	타임스탬프 프로토콜
RFC 2510 RFC 4210	Certificate Management Protocols	인증서 발급 프로토콜
RFC 2511 RFC 4211	X.509 Certificate Request Message Format	인증서 요청 메세지 포맷
RFC 8894	Simple Certificate Enrolment Protocol	심플 인증서 발급 프로토콜
RFC 8555	Automatic Certificate Management Environment (ACME)	자동 인증서 관리 환경