국방 인트라넷 전자서명 인증 시스템 구축 프레임워크

박춘석

cspark@eve.yonsei.ac.kr

2000. 10. 26

Coding & Information Theory Lab.

Department of Electrical and Electronic Engineering, Yonsei Univ.

Contents

- 도입(Introduction)
- 국방 인트라넷
- 공개키 기반구조
- mPKI(군 공개키 기반구조)
- mPKI 전자서명 인증시스템
- 결론 및 연구 방향

도입(Introduction)

❑전자서명 인증시스템의 필요성

- 범 국가적인 인증기반구조 구축 중
- 일부 기관 공개키 기반 전자서명 인증시스템 구축 완료 (예: 인터넷 뱅킹)
- 국방 인트라넷 전자거래 활용 미흡
- 내부자에 의한 정보유출 등 보안 위협
- 신뢰성있는 기관의 신원확인 및 인증
- 통신, 전산 장비 및 인력절감 효과
- 법적 분쟁시 증거자료

국방 인트라넷

❑국방 인트라넷 개념 및 특징

- 국방 전산 네트워크 기반
- 군 조직 내부 업무를 인터넷 환경에서 처리하도록 구성된 시스템
- 전군적 지역 구성
- 국방 통합 정보통신 망 운영 (C4I 및 MIS 지원)
- 노드 방식 통신 지원(스파이더 체계)

❑국방 인트라넷 구성체계('98)

- 국방 통합메뉴
- 전군 이름관리체계(DNS)
- 전자우편(E-mail) 체계
- 응용 체계

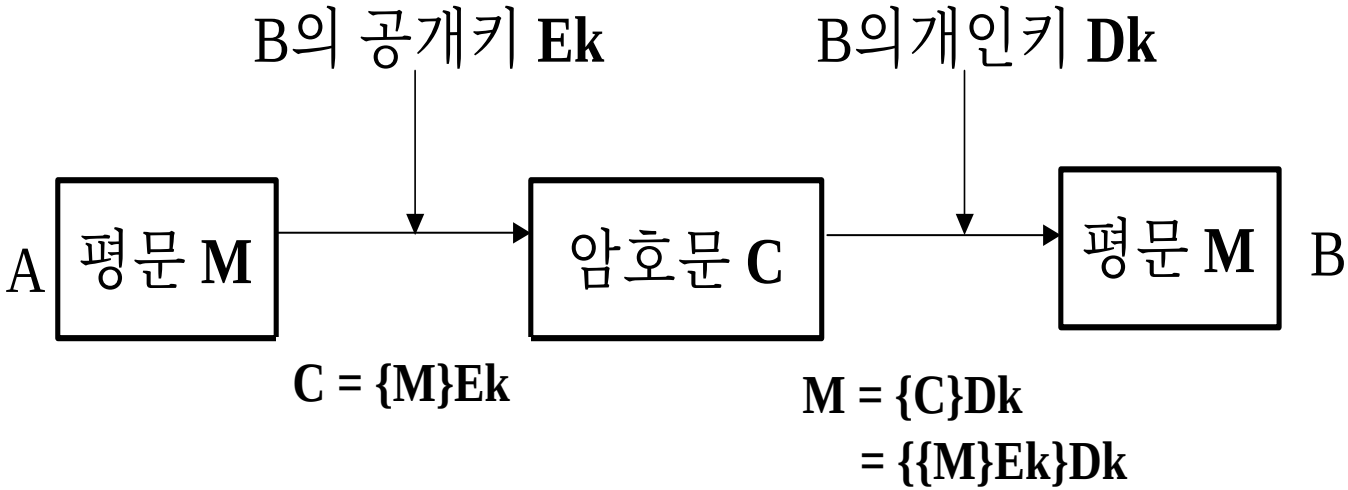
국방 인트라넷

- 국방 인트라넷 보안 요구사항
  - 예하 제대 업무통제/ 감사 용이
  - 사용자 인증 및 접근권한제어
  - 상호 인증(Cross-Authentication)
  - 기밀성 및 무결성 보장
  - 네트워크 침입탐지 및 차단

공개키 기반 전자서명 인증서비스

공개키 기반구조

❑공개키 암호기술



❑공개키 기반구조

- 인증서 관리체계
- 인증서 기반의 공개키 사용이 용이하도록 관리하는 인증기관들 간의 유기적인 결합체

공개키 기반구조

❑PKI 구성 객체

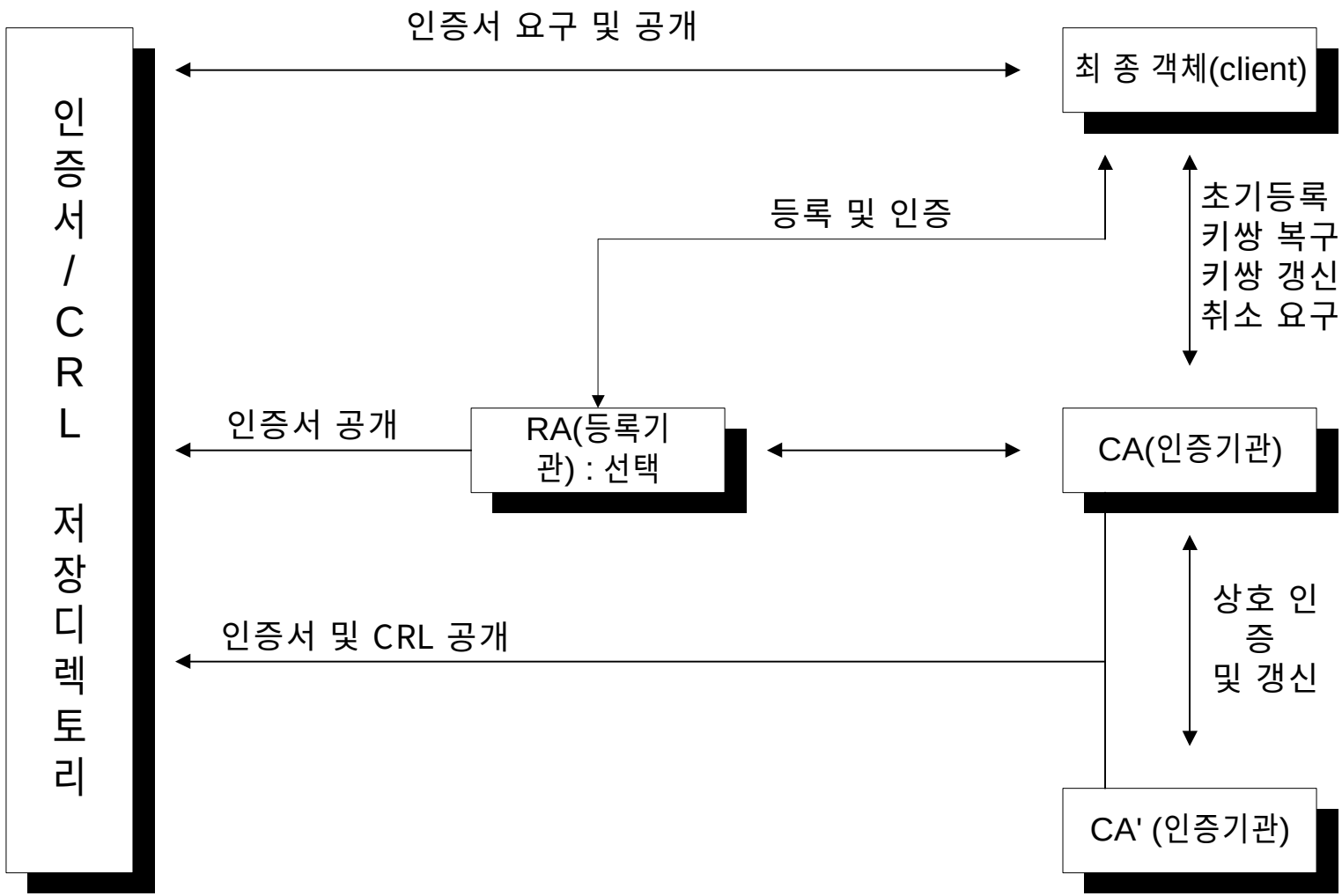
- 인증기관(CA)
  - 정책승인기관(PAA:Policy Approving Authority))
  - 정책인증기관(PCA:Policy Certification Authority))
  - 인증기관(CA:Certification Authority)
- 등록기관(RA:Registration Authority)
- 디렉토리 서버(Directory Server)
- 최종 객체(Client)

❑PKI 관리 대상

- 인증서(Certificate)
- 상호 인증서 쌍(Cross-Certification Pair)
- 인증서 취소목록(Certification Revocation List)

공개키 기반구조

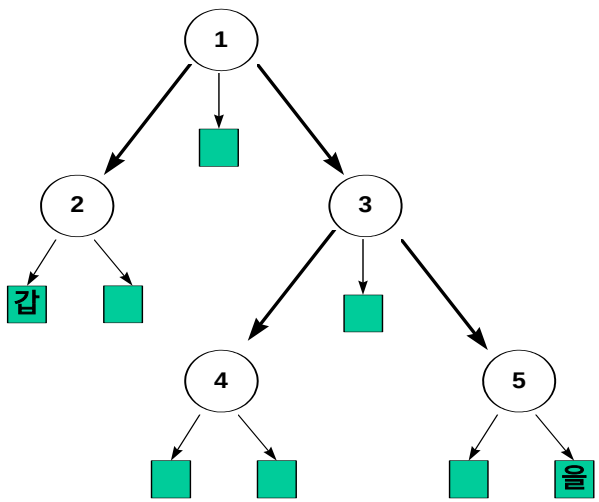
❑구성 객체 및 요소간 유기적 관계



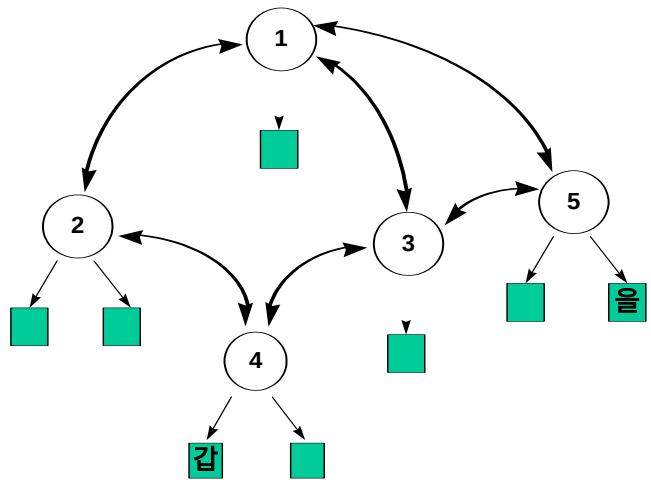
공개키 기반구조

❑PKI 토폴로지(topology)

- 계층적 인증구조: 계층적 CA간 수직적 상하 인증
- 네트워크적 인증구조: 독립적 인접 CA간 상호 인증



[계층적 구조]



[네트워크적 구조]

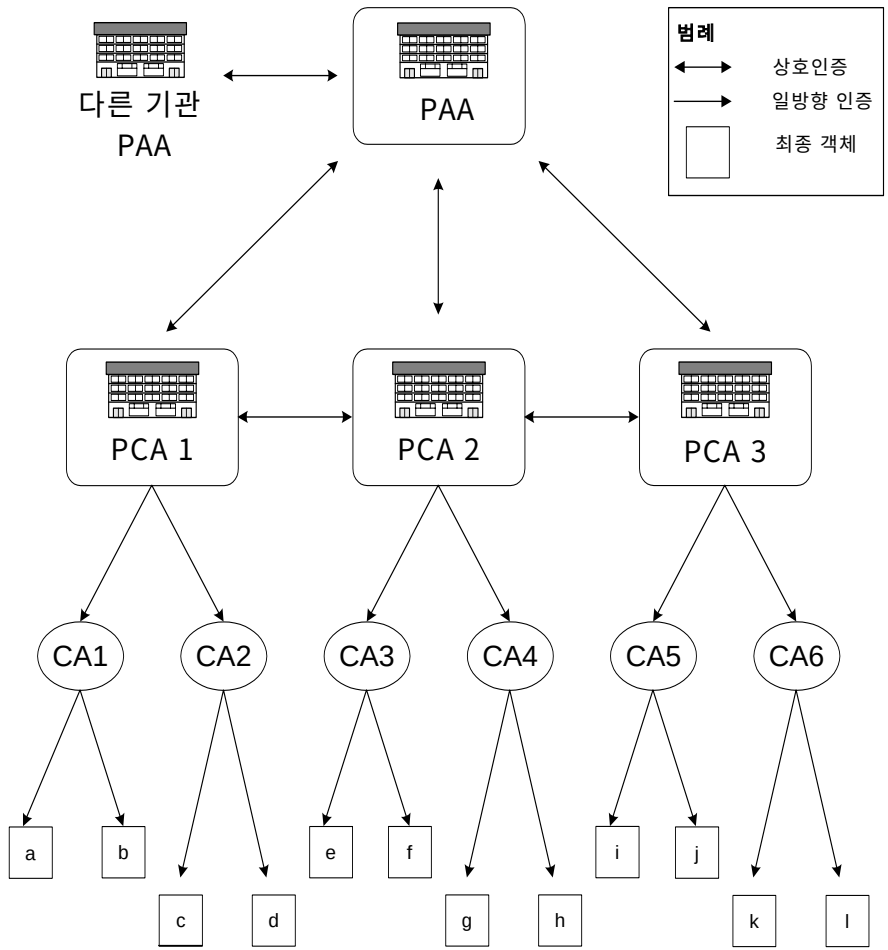
mPKI 전자서명 인증시스템 구축

❑시스템 구축시 고려사항

- PKI 형태 선정 및 PKI 보안 요구사항
- 보안 알고리듬(해쉬 알고리듬, 전자서명 알고리듬 등)
- 디렉토리 서비스(DAP/LDAP)
- 인증 실무 준칙(CPS)
- 사용자측 PKI 응용 소프트 웨어
- 전자서명 인증서비스 절차
- 시스템 구성 및 운영 원칙

mPKI(military PKI)

핵심 업무 유형	PKI 인증 구조
전자우편 교환	네트워크적 구조
전자결재 문서 하달 및 보고	계층적 구조
무기체계 개발 및 군수지원 업무(MIS)	네트워크적 구조
국방 응용체계 정보 공동 활용	네트워크적 구조
정보 수집 및 분석	네트워크적 구조
군사 작전간 지휘 통제 통신(C4I)	네트워크적 + 계층적 구조
교육훈련 및 훈련 자원 관리	계층적 구조
군 관련 민원 행정 서비스	계층적 구조



mPKI(military PKI)

❑mPKI 형태의 특성

- 다수의 인증기관 구성
- 업무유형별 인증경로 상이
- 계층적 구조 + 네트워크적 구조
- 상급인증기관(PAA/ PCA)간 상호인증체계 구축
- 모든 클라이언트 최상위CA의 공개키 인지

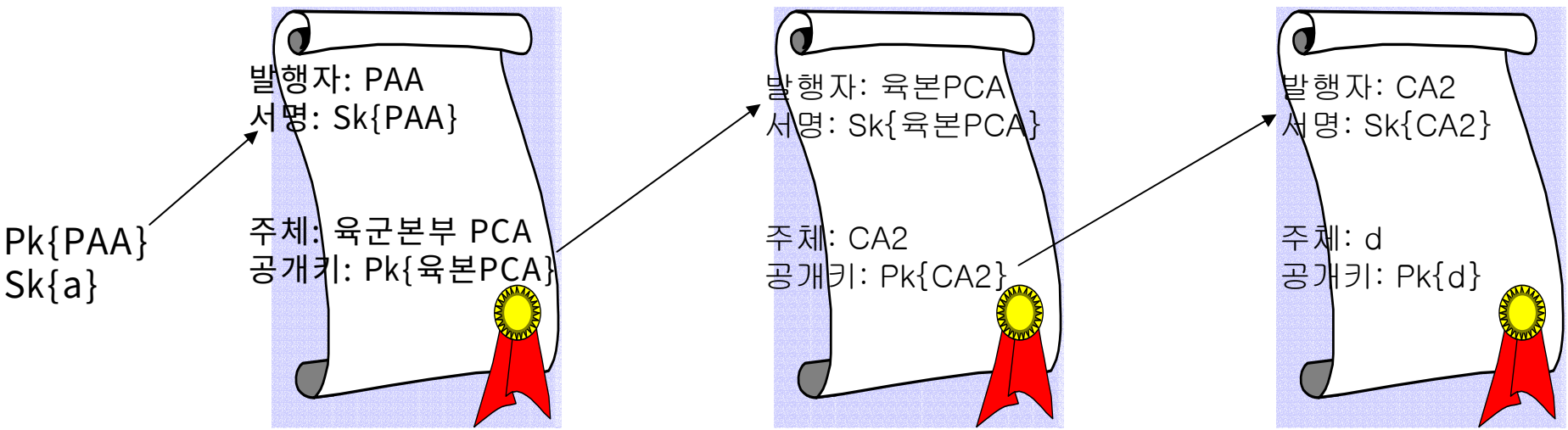
❑인증기관 수행제대(방안)

- PAA : 국방부
- PCA : 육해공군 본부 및 1,2,3군 사령부
- CA : 군단급 이상제대

mPKI(military PKI)

❑mPKI 인증서 검증과정

– 육본PCA내 CA1의 최종객체 a가 육본PCA내 CA2의 최종객체 d의 인증서를 검증하고자 할때



mPKI 전자서명 인증시스템

❑전자서명 인증시스템 개요

- mPKI 인증 기관 내부 시스템
- 전자서명 인증관리 체계의 안전 및 신뢰성 확보
- 전자서명 인증제도 및 전자문서 이용 활성화

❑구축 기본 원칙

- 국방 인트라넷 및 mPKI 특성 고려
- 업무별 다단계 복합 접근 통제
- 네트워크 침입차단 및 침입 탐지 체계 구축
- 중요 시스템 오프라인(off-line) 방식 구축
- 핵심 인증시스템 이중화 운영

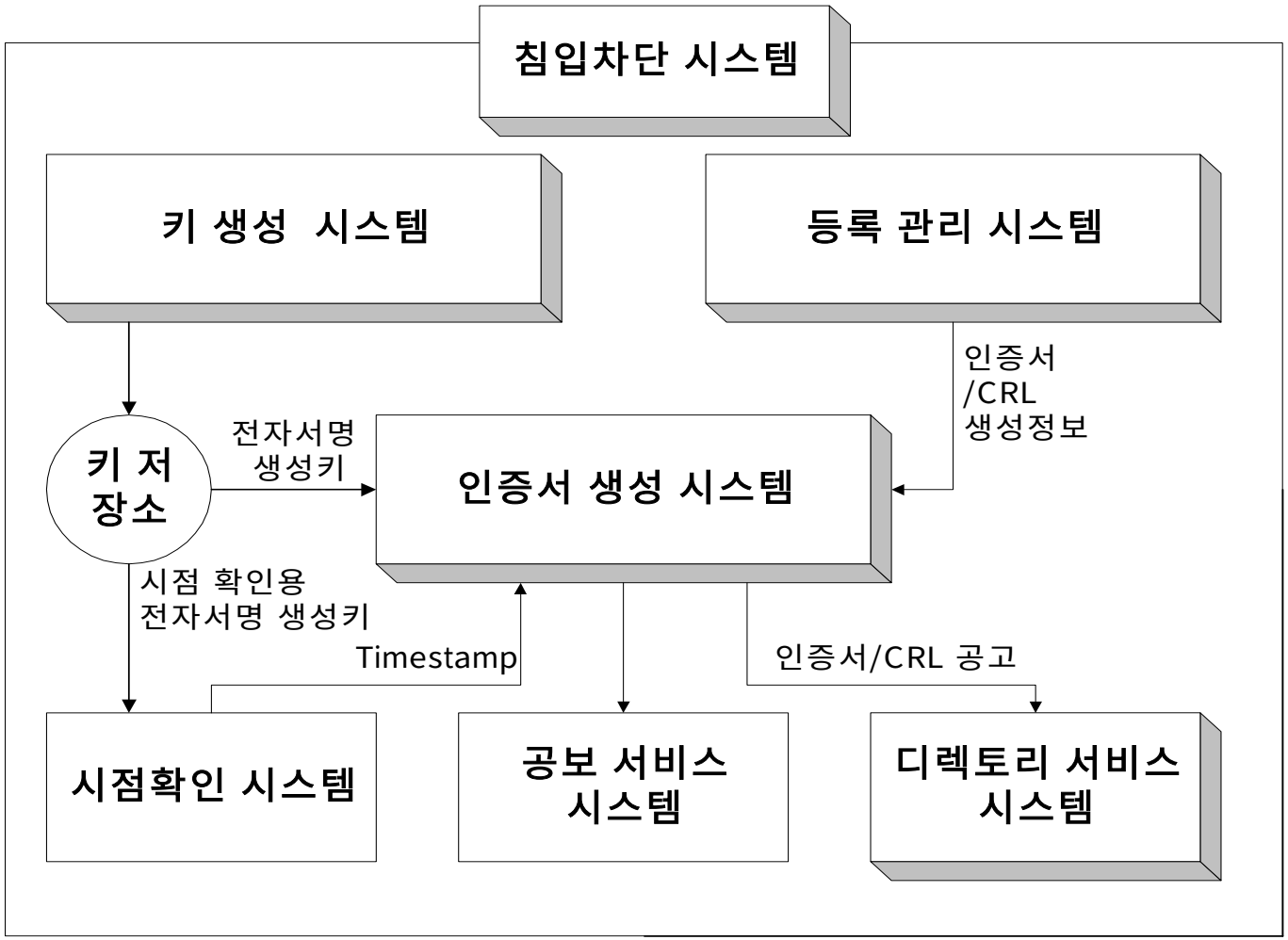
mPKI 전자서명 인증시스템

❑시스템 구성 및 역할

- **침입차단 시스템** : 국방 인트라넷 접근 통제 및 보안(이중 구성)
- **키 생성 시스템** : 중앙 집중식 키 생성(이중 구성)
- **인증서 생성 및 관리 시스템** : 자가 및 하위 인증기관 인증서 생성 및 관리(이중 구성)
- **디렉토리 시스템** : 인증 정보 저장 및 공고(이중 구성)
- **등록 관리 시스템** : 가입자 및 인증서 관리(이중구성)
- **시점 확인 시스템** : Timestamp 및 표준 시각 보정
- **공보 서비스시스템** : 인증기관 및 인증서 상태 정보 제공

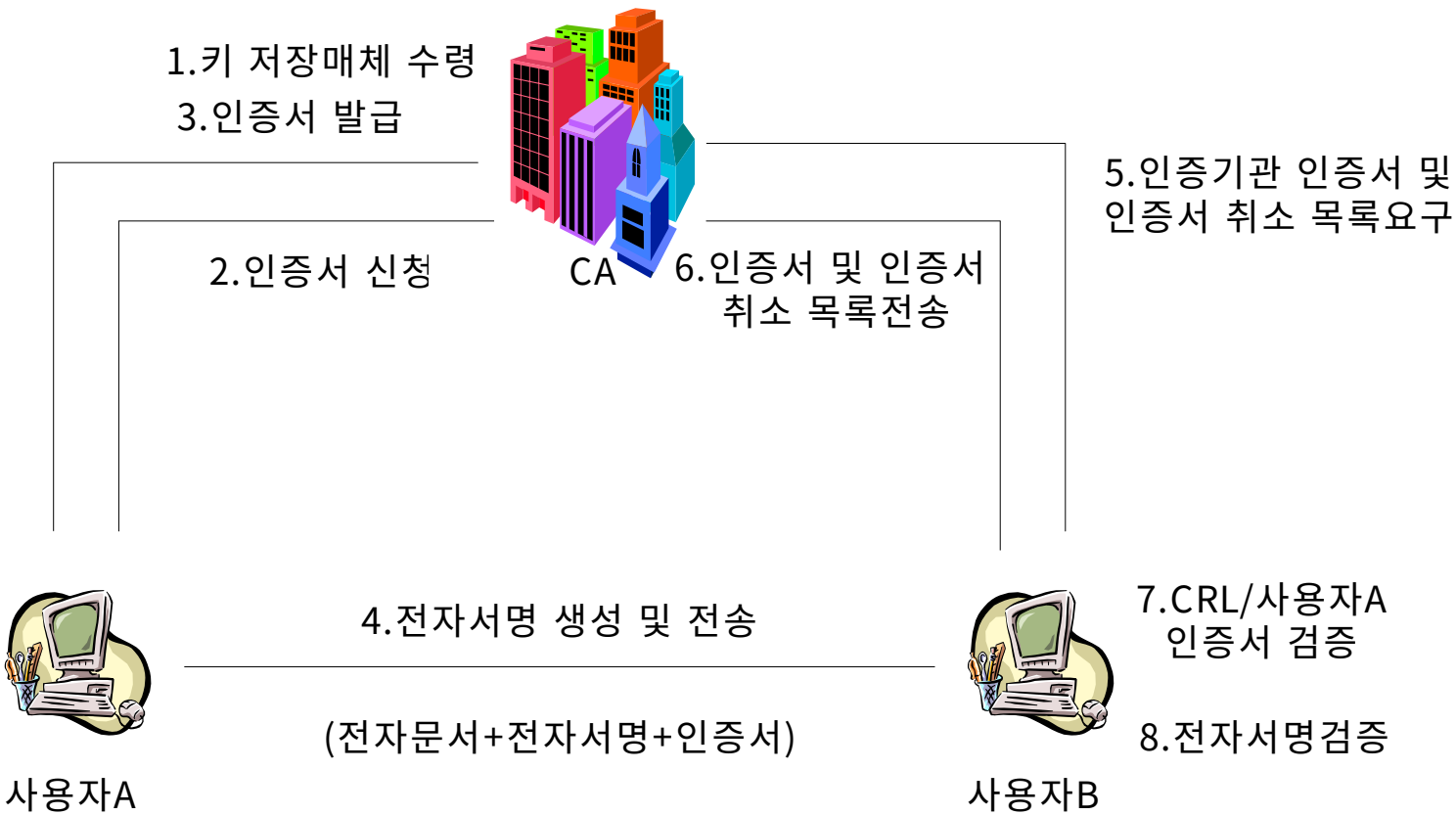
mPKI 전자서명 인증시스템

❑시스템 구성도



mPKI 전자서명 인증시스템

❑mPKI 기반 전자서명 인증서비스 절차



결론 및 연구 방향

❑Contribution

- 군내 공개키 기반 전자서명 인증관리 체계 구축
- 안전한 전자결재 시스템
- 효율적인 전자 문서 송 • 수신 체계
- 국방 정보 문화 흐름 변경

❑향후 연구 방향

- 취약한 키 생성 및 분배 관리 시스템 강화
- 최단거리 인증경로 탐색 알고리듬
- CRL과 실시간 취소 검증 방법 병행
- 인증서 사용 권한 제어