

# 전자입찰 시스템 보안

한국전자통신연구원 전자상거래연구부  
정승욱

2000. 8.29

## 목 차

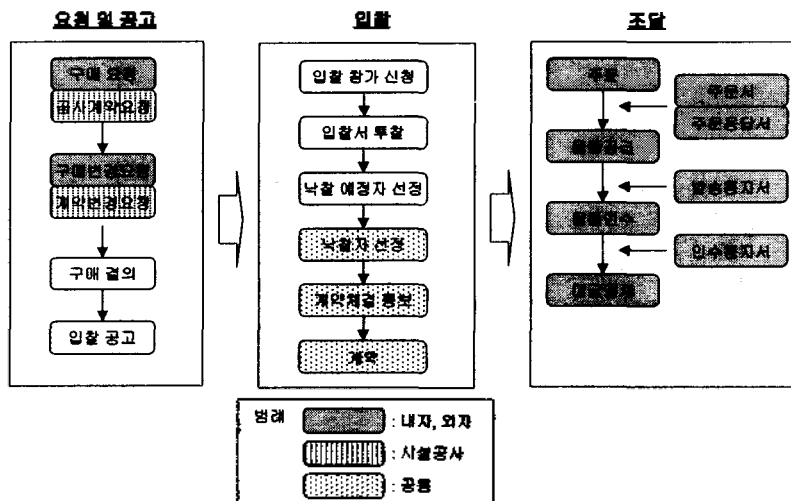


1. 개요
2. 전자입찰 프로세스
3. 전자입찰 시스템 구성도
4. 전자입찰 시스템 보안
5. 결론

# 1. 개요

- ▣ 정의
  - ◆ 전자 입찰 시스템 : 전자적으로 안전한 문서 교환을 통해 입찰 프로세스를 진행할 수 있는 시스템
- ▣ 필요성
  - ◆ 효율적인 업무처리, 경제적인 비용절감효과
  - ◆ 웹상에서 이뤄지는 정보교환의 안전성을 위하여 암호화와 전자서명이 적용된 전자입찰 시스템 요구
- ▣ 특징
  - ◆ 입찰 프로세스
    - 내자, 외자, 시설통사
    - 관리자 : 입찰 기관
    - 사용자 : 수요 기관, 공급 기관
- ▣ 적용분야
  - ◆ 기업이나 공공기관의 물품구매 구매입찰에 활용

## 2.1 입찰 프로세스 전체 흐름도



## 2.2 입찰 프로세스 관련 사용자 정의

### ▣ 수요기관

- 물품을 구매하거나 공사계약을 원하는 기관

### ▣ 입찰기관

- 구매요청을 접수하고 입찰과 계약을 수행하는 기관

### ▣ 계약당사자

- 입찰에 참가하여 낙찰된 후 조달 요청된 물품의 납품 담당자

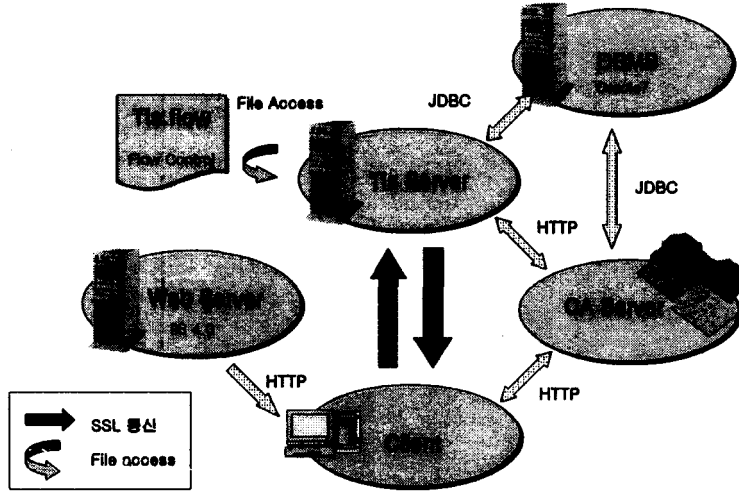
### ▣ 공급기관

- 입찰공고를 확인하고 입찰에 참가하고자 하는 업체

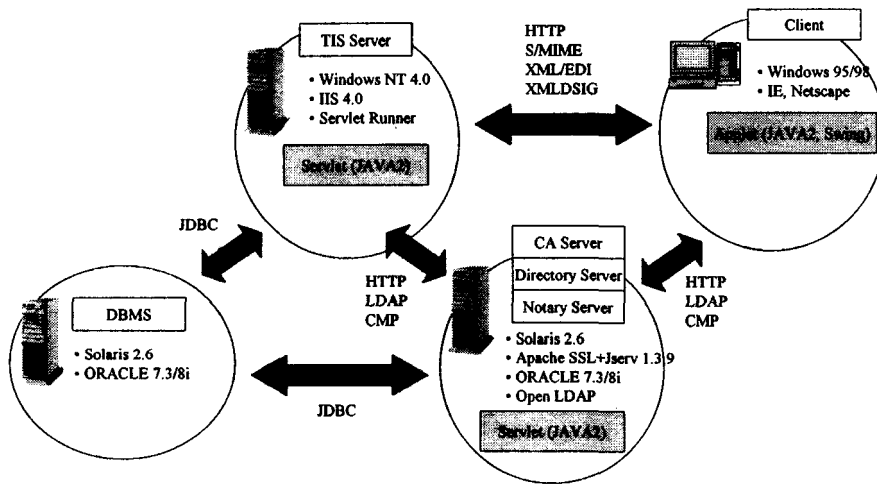
## 2.2 입찰 프로세스 기능 분석

구분	관련 프로세스	관련 기관
요청 및 공고	구매요청/공사계약요청, 구매변경요청/계약변경요청 규격사전공개, 규격검토/계약방법 및 기술검토협의 구매결의, 입찰공고	수요기관 ↔ 입찰수행기관
입찰	입찰참가신청, 낙찰예정자선정, 낙찰자선정 계약체결통보, 계약	공급기관 ↔ 입찰수행기관
조달	주문, 주문종단, 물품공급, 발송통지, 물품인수, 인수통지 대금결제	공급기관 ↔ 수요기관

### 3.1 전체 시스템 아키텍처



### 3.2 시스템 구현 환경



## 4.1 보안 요구 사항

### ☐ 인증(Authentication)

- ◆ PKI 기반의 X.509 인증서로 사용자, 서버 인증

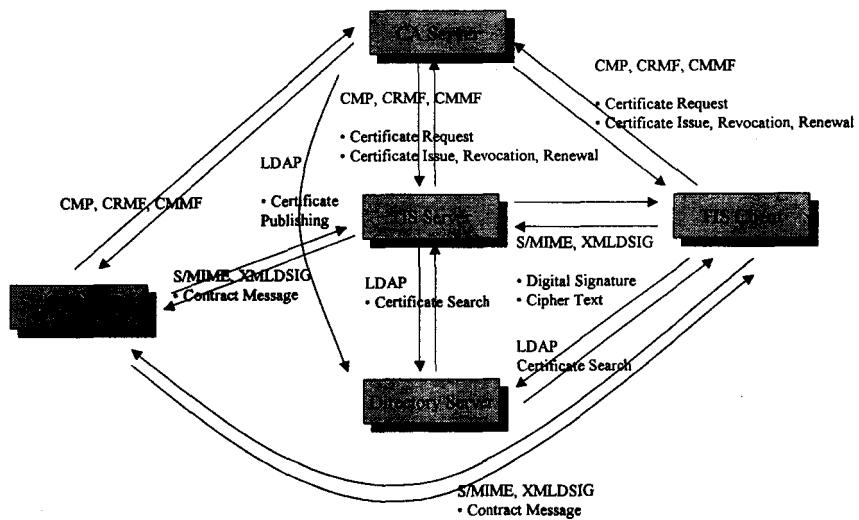
### ☐ 접근제어(Access Control)

- ◆ 인증된 사용자에개만 접근 권한 부여

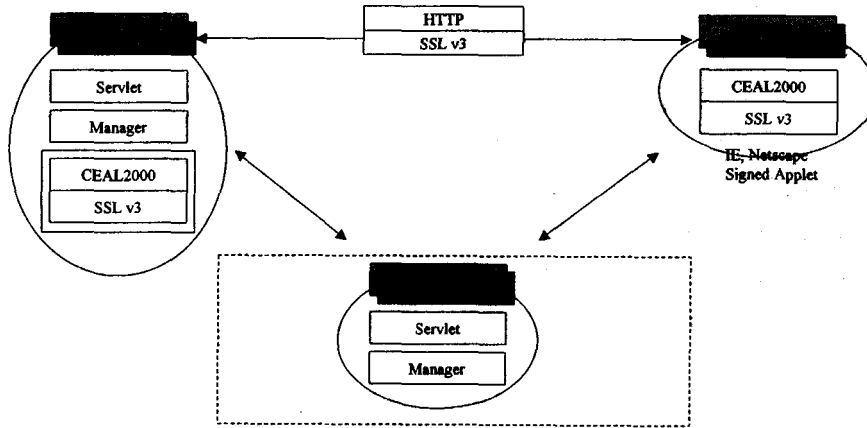
### ☐ 암호화, 전자서명(Crypto, Signature)

- ◆ 암호화 : SEED, RSA, HAS-160
- ◆ S/MIME을 이용하여 전자서명, 사용자 인증

## 4.2 보안 시스템 구성



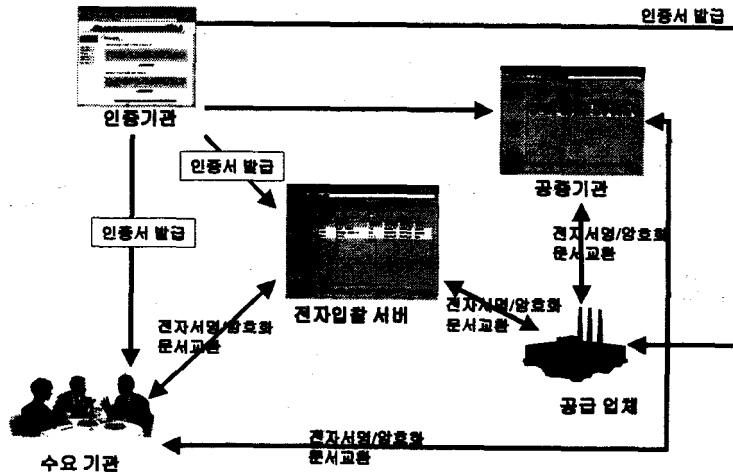
### 4.3 보안 설계 모듈



### 4.4 입찰 시스템 보안

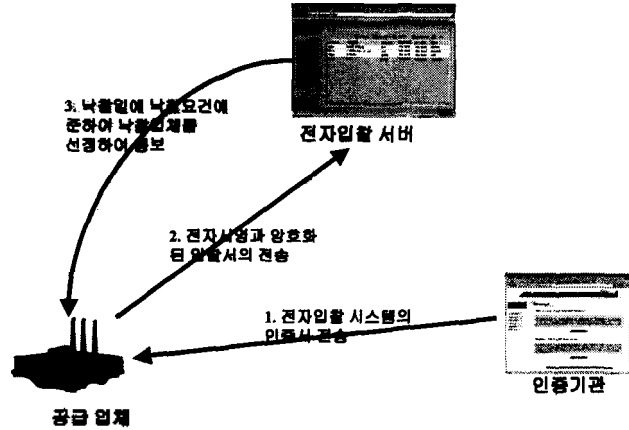


- 무결성과 부인봉쇄가 요구되는 문서의 전자 서명
- 기밀성이 요구되는 문서의 암호화



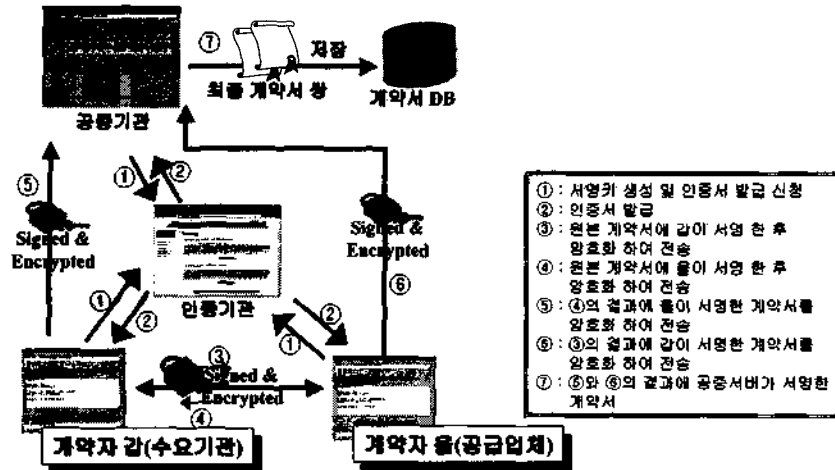
### 4.5 입찰서(입찰가격) 제출과정에서의 보안

- 공급업체는 입찰가가 적힌 입찰서를 작성하여 전자서명과 암호화를 하여 전자입찰 시스템으로 전송
- 전자 입찰 시스템의 관리자는 낙찰업체 입찰서를 복호화하여 낙찰업체를 선정



### 4.6 계약서 교환 과정에서의 보안

- 공공기관은 계약자간 교환하는 계약서의 유효성을 검증
- 최종 계약서 형은 전자서명/암호화 하여 XML/EDI문서로 DB에 보관



## 5. 결론

### ▣ 전자 입찰

- ◆ 기업간 전자상거래를 위한 개방형 시스템
- ◆ 보안이 필수적

### ▣ 보안

- ◆ 인증
- ◆ 접근 제어
- ◆ 암호화
- ◆ 전자서명