디지털 서명 인증관리센터의 인증서버 구현

인천대학교 정보통신공학과
송 영 부
(unipico@linux.inchon.ac.kr)

목 차

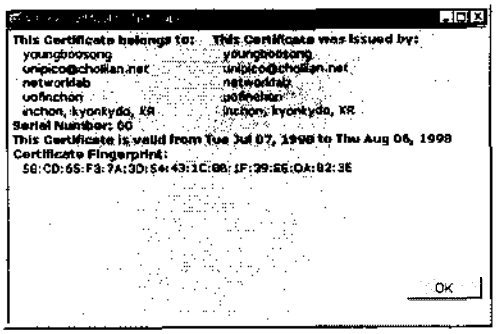
- 서론
- 전자인증서
  - X.509 v3 인증서
  - X.509 v2 CRL
- 인증서버 설계 및 구현
  - 인증시스템, 디렉토리시스템
  - 구현환경
  - 인증서버의 안전성 검증
- 결론 및 향후과제

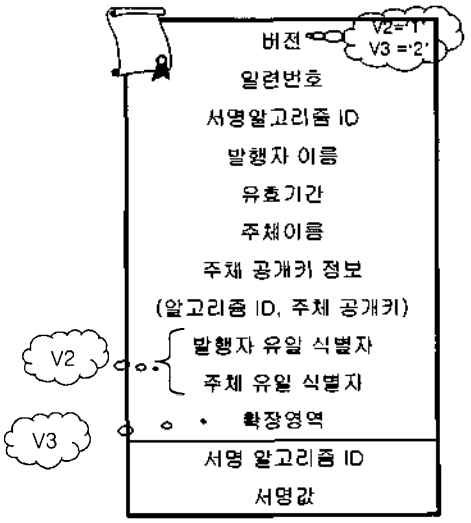
서론

- 디지털 콘텐츠(Digital Contents)란?
  - 컴퓨터상에서 Digital(0 또는 1)로 존재하는 무형의 데이터 (예, 멀티미디어, 영상, MP3, S/W)
- 디지털 콘텐츠 보호의 필요성
  - 불법복제 파일의 유통방지
  - 디지털 저작권 보호, 지적재산권 보호
  - 사용자 인증, 기밀성, 무결성
- 암호학적 방법
  - 공개키기반구조(PKI), 인증구조(X.509)
  - 전자서명기법

전자인증서

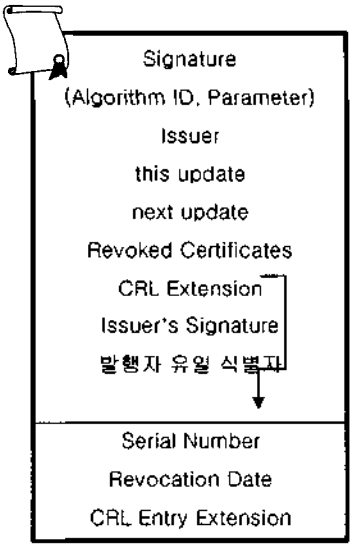
- X.509 v3인증서





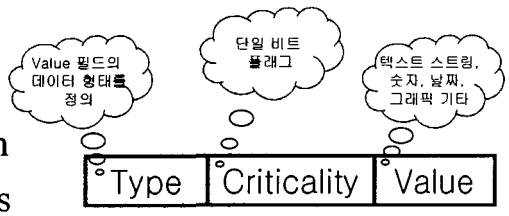
전자인증서

- X.509 v2 CRL
  - Extension
    - Authority key ID
    - CRL Number
    - Issure Distribution point(critical)
    - Delta CRL indicator(critical)
  - CRL Entry Extension
    - Reasion Code(noncritical)
    - Hold Instruction Code(noncritical)
    - Invalidity Code(noncritical)



전자인증서 확장구조

- 확장필드 이름(ID)
- Critical여부 구분 필드
- 확장내용
  - Key & Policy Information
  - Subject & Issue Attributes
  - Certificate Path Constraints
  - Basic CRL Extensions
  - CRL Distribution point and data CRL



인증서버 설계 및 구현

■ 인증시스템 구성도

인증 시스템

■ CA 서버 기능

- 사용자의 서명용/암호용 인증서 등록/취소/갱신
- 사용자 등급에 따른 전자인증서 On/Off Line 발급
- 발급한 인증서 및 CRL을 디렉토리에 등록
- 인증정책 공지

디렉토리 시스템

- LDAP 서버 기능
  - LDAP 프로토콜을 이용한 X.500 디렉토리 접근
  - 전자인증서 및 CRL 배포
  - Referral 정보를 이용한 분산환경
- Web Gateway
  - LDAP의 디렉토리 정보를 HTML문서 형태로 변환

시스템 구현 환경

- 인증 시스템 및 디렉토리 시스템
  - Pentium II 400MHz
  - Windows NT 4.0 + OptionPack 4
- 사용자
  - 486/Pentium PC
  - Windows 95/98/NT

인증서버의 안전성 검증

- El-Gamal 서명 기법
  - 서명 확인/전환 무결성 검증
- 유효하지 않은 인증서에 대한 처리 검증
- 디렉토리 서버와 인증서버 간의 세션 접속시간 최소화
- 웹서버에 SSL 설치 운영

결론 및 향후과제

- 결론
  - PKI의 X.509 전자인증서를 인증서버(CA)에 적용
  - 인증기관의 관리기능 설계 및 구현
  - PKI의 구현에 관련된 요구사항과 기능 분석
  - X.509 인증서를 이용한 디지털 콘텐츠 정보 보호
  - 사용자 인증 및 기밀성, 무결성 효과
- 향후과제
  - CA간 상호인증 분야 확대
  - 멀티미디어/영상 데이터에 대한 사용자 인증 적용