공개키 기반구조란(지식정보사회의 핵심 기반 시설)

개요

인터넷의 등장, 그리고 이로 인해 비대면 거래가 활성화 되면서 안전개래의 중요성 대두!

예,쇼핑

1.인터넷 쇼핑 사이트를 어떻게 신뢰할 수 있는가

2. 주문한 고객이 정말 본인인지 어떻게 신뢰할 수 이는가, 주문 해 놓고 부인하면 어떻게 할 것인가

3. 거래내용의 비밀은 보장 되는가, 누군가 거래 내용을 도청할 수 있지 않는가

특히 BToB 거래에서 데이터들의 신뢰도는 매우 중요하다.

이러한 문제를 해결할 수 있는 대안 PIK(public key infrastructure)

pki기본구조

전자상거라, 정보유통의 안전성과, 신뢰성을 확보하기 위한 시스템,

상대방 신원확인, 비밀유지기능, 부인봉쇄 기능 제공

기술 : 공개키알고리즘, 전자서명 을 통해 위 기능 제공

즉, 암호화와 복호화키로 구성된 공개키를 이용해 송수신 데이터를 암호화하고, 디지털 인증서(전자서명)을 통해 사용자를 인증하는 시스템

공개키암호화나 전자서명이 안전하게 사용되기 위해서는 키의 생성과 인증, 그리고 분배와 안전한 관리를 위한 믿을 수 있는 체계가 필요한데 이것이 공개키 기반구조

공개키 암호화

주문서(주문자a) -> b의공개키로 암호화 -> 암호문 -> b의 개인키로 복호화 -> 주문서(판매자b)

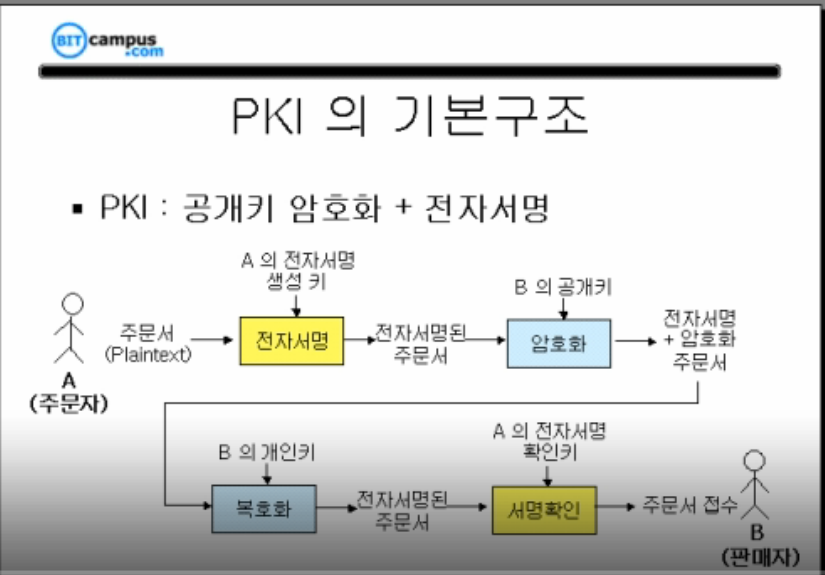
* 주문 내용의 비밀성 보장
* 주문 내용이 변조되지 않았음을 보장

전자서명 암호화

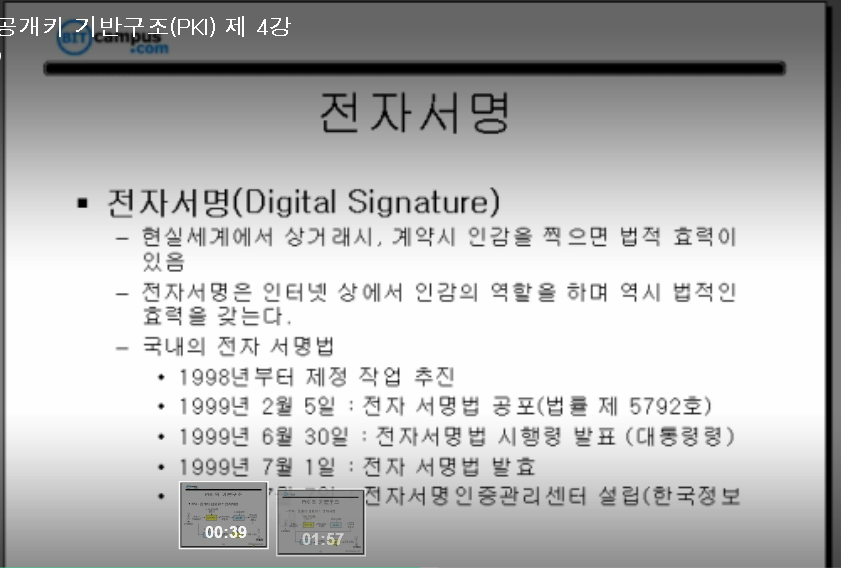
주문서(주문자a) -> a의 전자서명 생성키로 전자서명(개인키)-> 전자서명이 된 주문서 -> a의 전자서명 확인키(공개키)로 서명 확인 -> 주문서 접수(판매자 b)

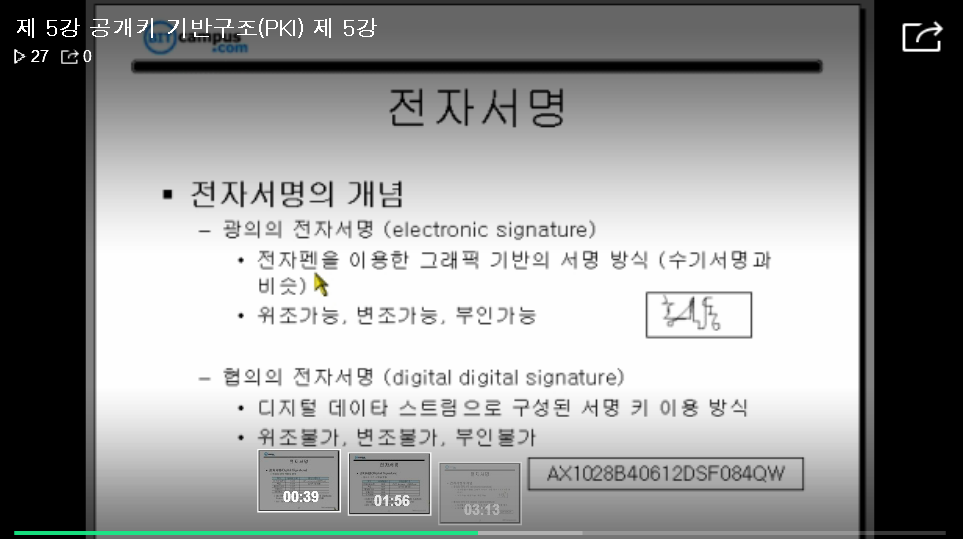
* 주문서가 a가 보내는 것임을 증명
* A는 주문서를 보내지 않았다고 부인할 수 없다.

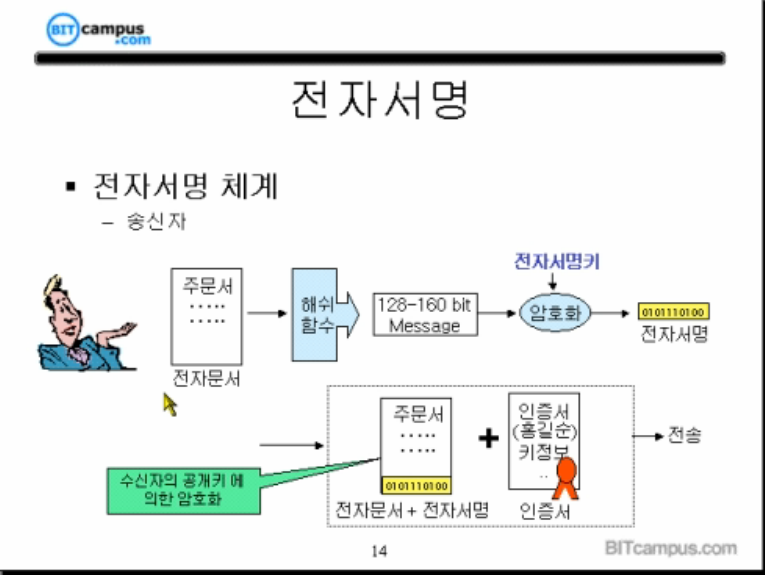
실제 PKI구조

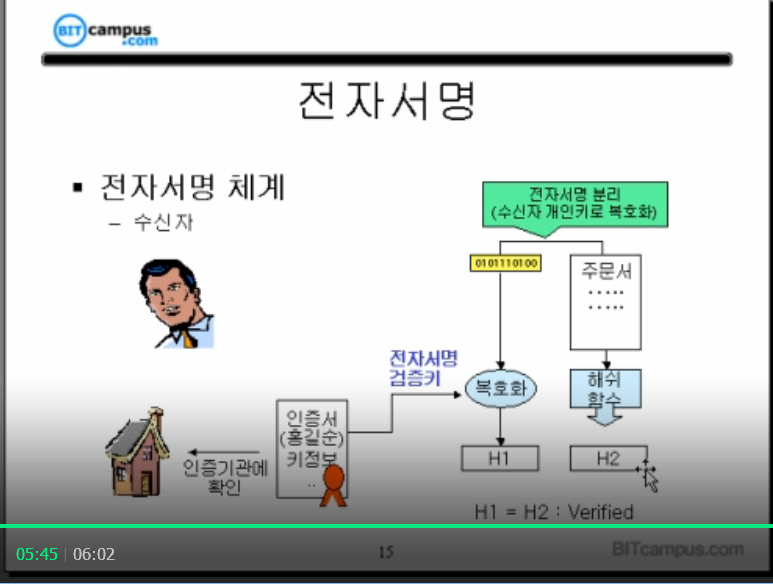


전자서명

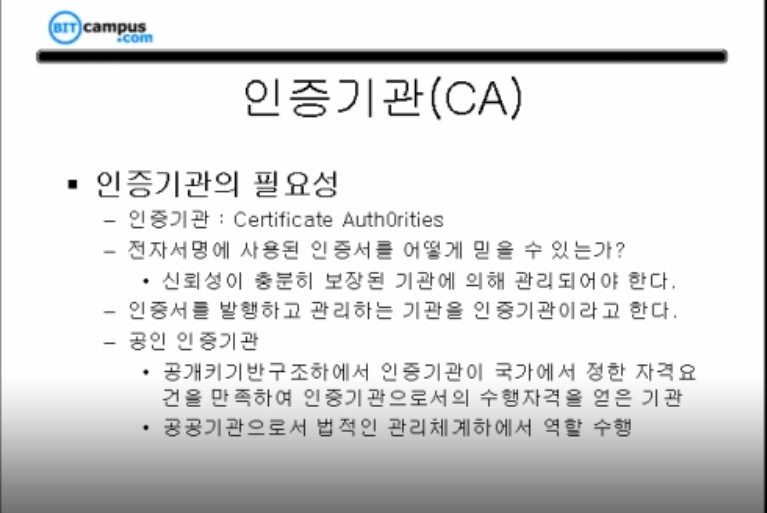


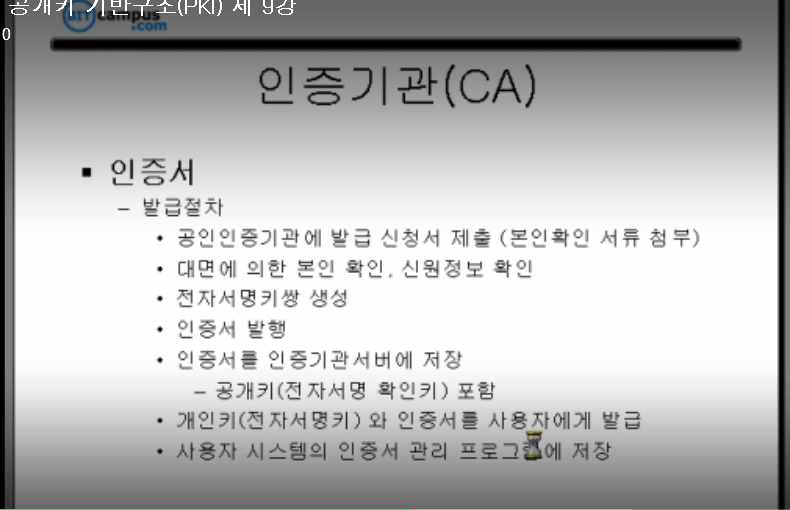


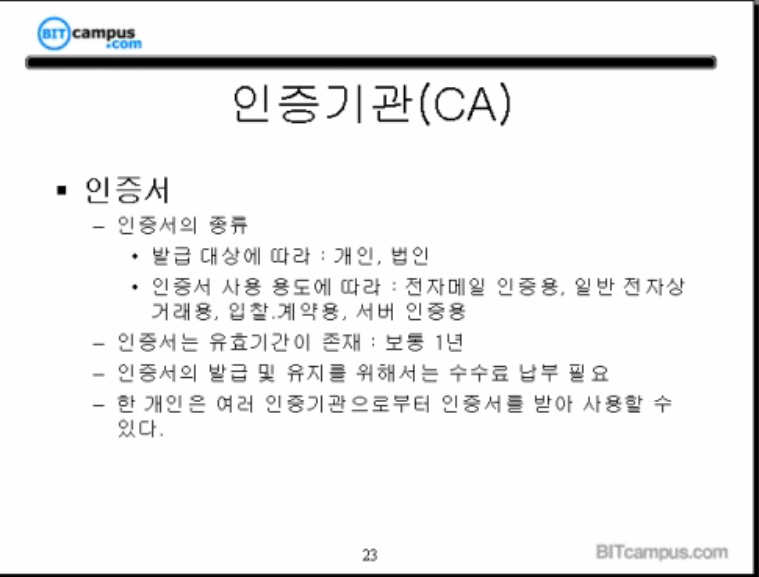


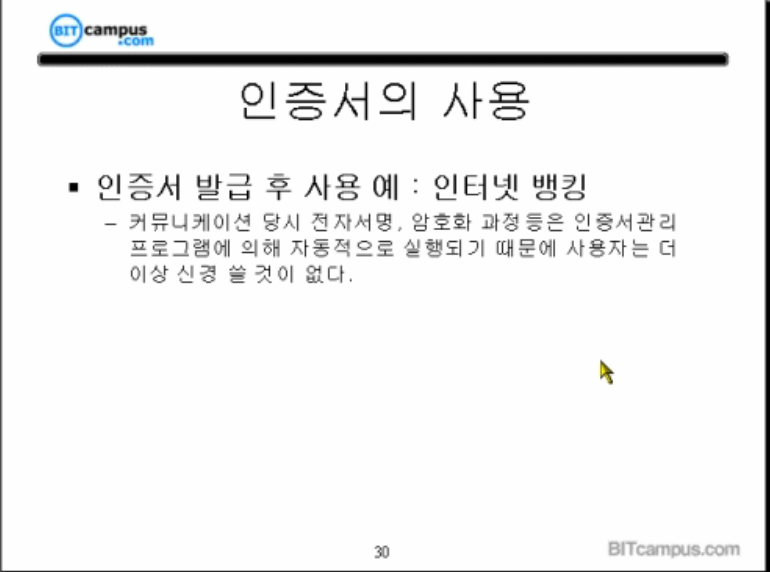


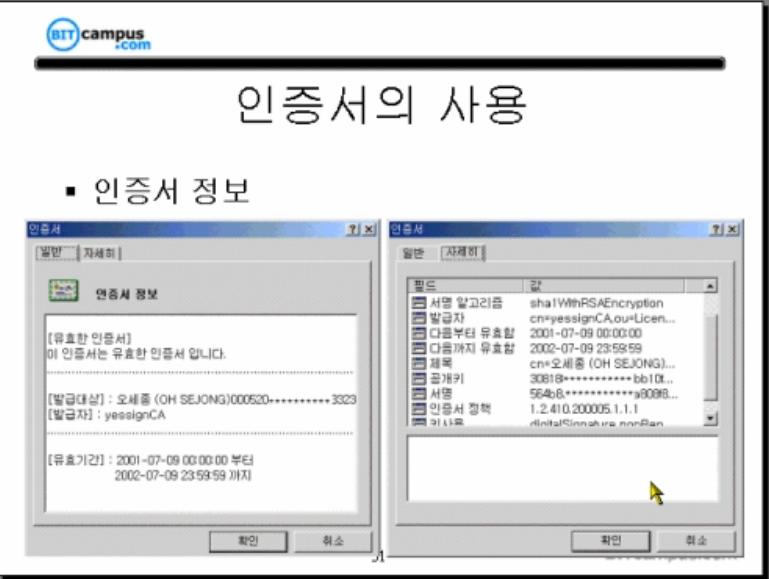
인증기관(cA, certificate authorities)











인증서의 사용