

23.11.20 전자 서명

☰ 상태	Task
🕒 작성일시	@2023년 9월 11일 오후 8:56

Tasks

▼ 전자 서명 : 넓은 범위의 디지털 서명 방식

- 전자 서명의 개념
 - 서명자가 해당 전자문서에 서명하였음을 나타내기 위해 전자 문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보
 - 어떤 데이터가 정말 그 사람 것이 맞는지를 보장 해주는 것

▼ 전자 서명 장점

- **서명자 신원확인(User Authentication)** - 개인키의 소유자가 전자서명 행위자임을 증명 - 서명자 고유의 표식
- **위조 불가(Not forgeable)** - 합법적인 서명자 외에는 전자서명 생성 불가 증명
- **변경 불가(Unalterable)** - 서명한 문서의 내용과 서명의 변경 불가 증명
- **부인 불가(Non-Repudiation)** - 서명은 본인 이외에는 불가능함을 증명
- **재사용 불가(Not Reuseable)** - 다른 전자문서의 서명으로 사용 불가능함을 증명

▼ 전자 서명 방식

1. 주로 공개키 암호화 알고리즘을 사용하지만 해시함수와 대칭키 암호화도 종종 포함 된다.

▼ 공개키와 비밀키

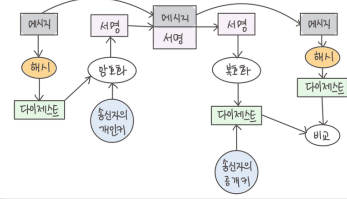
- 공개키 암호화 알고리즘 : 메시지의 무결성과 인증을 보장한다.
 - 해시 함수는 메시지의 무결성을 확인하고, 대칭키 암호화는 실제 메시지를 암호화하고 복호화하는 데 사용된다.
- 쉽게 이해하기 위해 공개키는 은행의 '**계좌번호**' 이고 , 비밀키는 그 계좌의 '**비밀번호**' 라고 생각 하면 된다.
- 공개키는 토큰을 전송하거나 수신할 때 사용
- 비밀키는 지갑과 지갑에 보유한 모든 자산에 대한 접근 권한을 가지고 있음

암호학 7 - 공개키와 비밀키를 이용한 전자서명 및 인증서

전자서명 ▶ 배경 종이 문서 사회에서 정보화 사회로의 진전으로 다양한 서비스 요구 데이터 무결성, 사용자 인증, 부인방지 서비스가 필수적 ▶ 목적 신뢰성 확보 (내용의 위·변조 및 신분 확

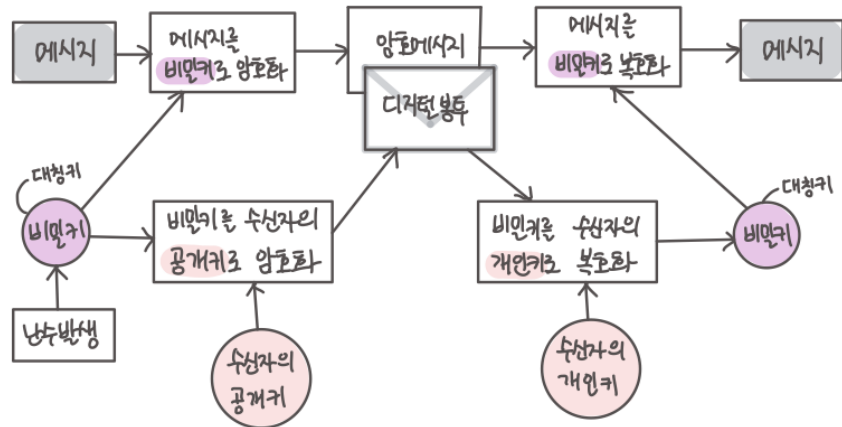
https://lemonandgrapefruit.tistory.com/163

<공개키를 이용한 전자서명>



전자서명의 이용 : 전자봉투 (원타임 비밀키)

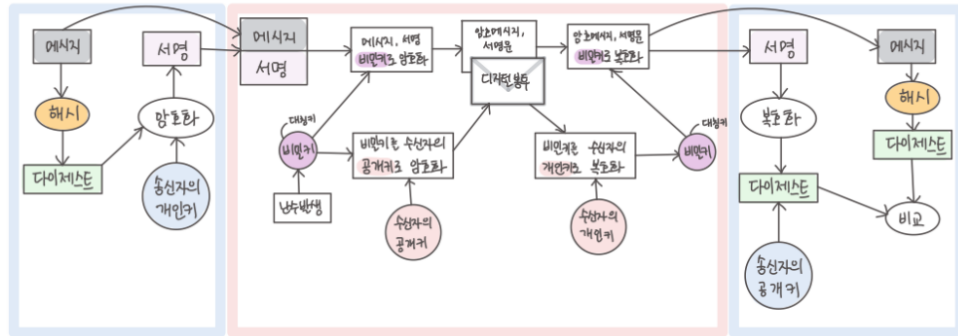
<전자서명의 이용 : 전자봉투 (원타임 비밀키)>



1. 송신자는 메시지와 암호화하기 위해 난수를 발생해 비밀키를 생성한다.
2. 메시지를 비밀키로 암호화해 암호메시지를 만든다.
3. 비밀키를 수신자의 공개키로 암호화한다.
4. 암호메시지와 공개키로 암호화한 비밀키를 디지털봉투에 담아 전송한다.
5. 수신자는 디지털 봉투에 있는 암호화된 비밀키를 수신자의 개인키로 복호화해 비밀키를 얻는다.
6. 암호화된 메시지를 비밀키로 복호화한다.

- ※ 사용할 때마다 난수를 발생시켜 비밀키로 정한다. 받는 사람의 공개키로 이 비밀키를 암호화한다.
- ※ 기밀성이 가능하지만 인증은 불가능하다.
- ※ 네트워크에서 빠르게 사용 가능하다.

< 공개키와 대칭키를 이용한 전자서명 >



공개키를 이용한 전자서명으로 사용자 인증이 가능하다.

대칭키를 이용한 전자서명으로 기밀성이 가능하다.

※ 인증과 기밀성이 가능하다.

2. 공인된 인증기관에서 발행한 디지털 인증서를 통해 전자 문서에 서명 (높은 수준의 보안 제공, 법적 인정)

▼ 디지털 서명

Acrobat Reader DC PDF 디지털 서명하는 방법 :: 디지털 싸인

오늘은 PDF 디지털 서명하는 방법에 대하여 알아보겠습니다. 디지털 서명은 한번 만들어 놓으면 2번째 작업할 때는 문서에 서명을 빠르고 간편하게 할 수 있으니 한번 만들어보시기를 바랍니다. 1. 갱신할 문서를 볼

<https://bomplays.com/110>

서명할 디지털 ID 구성

디지털 ID 구성

디지털 ID 유형 선택:

- ☐ 서명 작성 장치 사용 (컴퓨터에 연결된 스마트 카드 또는 토큰 구성)
- ☐ 파일에서 디지털 ID 사용 (도용될까? 기존 디지털 ID 가져오기)
- ☒ 새 디지털 ID 생성 (자제 서명된 디지털 ID 생성)

test1.pdf

- 네트워크에서 송신자의 신원을 증명하는 방법
- 송신자가 자신의 비밀키로 암호화한 메시지를 수신자가 송신자의 공용키로 해독하는 과정
- 공개 키 인증 구조(PKI) 기술을 통해 지원, 서명자는 신뢰하는 인증기관(CA)에서 발행한 인증서 기반의 디지털 ID를 받는다.
- 고급 인증이 필요한 거래에 적합
- TSP(Trust Service Provider)의 인증서 기반 디지털 ID를 사용하여 서명자 ID를 인증하고 암호화를 통해 문서에 각 서명을 연결하여 서명을 증명합니다.

▼ 장점


- 높은 신뢰성 및 규정 준수
- 간편한 인증
- 철저한 보안
- 고유한 인증방식

3. PDF파일이나 기타 문서에 직접 사인하는 방식 (문서의 인증과 무결성을 보장한다.)

▼ 전자 서명

PDF 문서 서명

Adobe Acrobat에서 다음 단계를 따라 서명 파일을 입력하거나, 끌어 오거나, 삽입하여 PDF 파일에 서명을 추가하십시오. Adobe Sign을 사용하여 다른 사람이 서명한 PDF를 가져옵니다.

 <https://helpx.adobe.com/kr/acrobat/using/signing-pdfs.html>

test2.pdf

- 서명자가 해당 전자문서에 서명하였음을 나타내기 위해 전자 문서에 첨부 되거나 논리적으로 결합된 전자적 형태의 정보
- 전자 문서나 양식에 대한 동의 또는 승인을 받는 합법적인 방법

▼ 장점

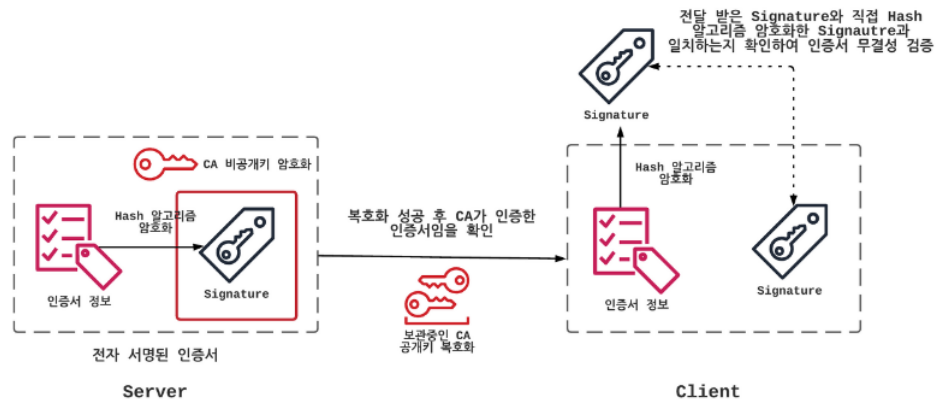
- 탁월한 비용 대비 효과
- 법적 구속력
- 탁월한 효율성 (업무시간 절감)

4. 전자 서명과 디지털 서명의 차이점

- “전자 서명”은 동의서 또는 기록물의 승인을 나타내는 모든 전자 프로세스
- “디지털 서명”은 특정 유형의 전자 서명인 인증서 기반의 디지털 서명

▼ 디지털 서명 인증서 도식화

1. 인증서 전달 과정



- ① 전자 서명된 인증서(인증서 정보를 Hash 알고리즘으로 암호화 후 CA 비공개키로 암호화한 Signature를 포함)하여 Server -> Client로 보낸다.
- ② Client는 전자 서명된 인증서를 받고 브라우저에서 보관중인 CA List의 공개키로 복호화하여 해당 인증서가 CA로부터 받은 인증서임을 신뢰한다.
- ③ Client는 전달 받은 인증서를 Hash 알고리즘으로 암호화한 Signature와 Server로부터 전달 받은 Signature를 비교하여 인증서의 무결성을 검증한다.

1. 어떤 사람 A가 자신의 비밀키를 사용하여 원본 데이터의 해시값을 암호화(서명) 한다.
2. 그 후에 믿을 수 있는 기관 B에 A의 공개키를 배포한다.
3. 그러면 믿을 수 있는 기관 B는 자신의 비밀키로 A의 공개키를 서명하고, A의 주체 정보와 B의 공개키 등을 담아 인증서를 만들어 배포한다.
4. 그리고 A는 이 인증서와 함께 원본 데이터와 원본 데이터의 해시값을 서명한 데이터를 합쳐 배포한다.(이를 “코드사인”이라고 한다.)

• 전자서명의 효력

제 3조

- ① 전자서명은 전자적 형태라는 이유만으로 서명, 서명날인 또는 기명날인으로서의 효력이 부인되지 아니한다.
- ② 법령의 규정 또는 당사자 간의 약정에 따라 서명, 서명날인 또는 기명날인의 방식으로 전자서명을 선택한 경우 그 전자 서명은 서명, 서명 날인 또는 기명 날인으로서의 효력을 가진다.