제7장 전자서명

1. 전자서명 개요

우리는 많은 정보(메시지)가 인터넷과 같은 통신망을 통해 교환되는 정보사회에 살고 있다.

메시지 수신자는 다음 2가지 궁금증을 가진다.

- 제3자가 송신자를 가장하여 메시지를 보내지 않았을까?
- 전송 도중에 메시지 내용이 변경되지 않았을까?

2가지 궁금증을 확인할 수 있는 가장 효율적인 도구가 바로 **전자서명**이다.

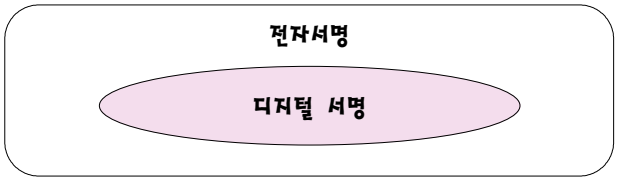
전자서명은 정보보호론에서 거의 모든 영역과 연관되어 있다.
개체 인증, 보안 알고리즘, 인터넷, 법규 등 관련되지 않은 것이 없을 정도이다.

통신은 얼굴을 모르는 수많은 사람과도 언제든지 대화가 가능한 공산이다.
과연 상대방을 얼마나 믿을 수 있을까? 대면하고 있어도 믿기 어려운 것이 많은데.....

전자서명은 대면하고 있지 않은 사람을 인증할 수 있는 기능이 있다.

◈ **전자서명 / 디지털 서명**

전자서명과 디지털 서명(digital signature)은 같은 용어인가?



• 모든 종류의 전자서명이 반드시 디지털 서명을 이용하는 형식은 아니다.
• 단지, 디지털 서명은 전자서명을 구현하기 위해 사용되는 하나의 방법론이다.
• 전자서명은 서명을 위한 모든 전자 데이터를 가리키는 상위어 개념이다.
• 현실적으로, 전자서명과 디지털 서명을 엄밀하게 구분하지 않고 사용되고 있을 뿐이다.

〈전자서명 요구조건〉

① **서명자 인증**(user authentication)
• 누구나 전자서명의 서명자를 **확인(검증)**할 수 있어야 한다.
• 전자서명은 검증하는 것이 쉬워야 한다.

② **위조 불가**(unforgeable)
• 서명자 이외의 타인의 서명을 위조하기 어려워야 한다.**(무결성)**
• 합법적 서명자만이 전자서명을 생성할 수 있어야 한다.

③ **부인 불가**(non-repudiation)
• 전자서명한 후에는 서명한 사실을 서명자는 부인할 수 없어야 한다.

④ **변경 불가**(unalterable)
• 전자서명된 문서의 내용은 변경될 수 없어야 한다.
• 전자서명생성키를 소유하지 않은 자는 서명한 문서의 내용을 변경할 수 없어야 한다.

⑤ **재사용 불가**(not reusable)
• 특정 문서의 전자서명을 다른 문서의 전자서명으로 사용할 수 없어야 한다.
• 전자서명과 문서의 관계는 반드시 "일-대-일"이어야 한다.**(유일성)**

◈ **전자서명이 제공하는 핵심 기능 - 3가지**

인증	서명은 신원이 올바른지 확인할 수 있다.
무결성	서명은 데이터 무결성을 확인할 수 있는 기능을 제공한다.
부인방지	서명의 고유성은 서명 소유자가 서명을 거부하지 못하도록 한다.

• 전자서명은 데이터 **기밀성**은 제공하지 않는다.
• 데이터 기밀성을 위해서는 **별도로 암호화**를 적용해야 한다.

기출문제 분석

1. 디지털 서명에 대한 설명으로 옳은 것을 〈보기〉에서 모두 고른 것은? [2018년 서울 9급]

------<보기>----------

ㄱ. 디지털 서명은 부인방지를 위해 사용할 수 있다.
ㄴ. 디지털 서명 생성에는 개인키를 사용하고 디지털 서명 검증에는 공개키를 사용한다.
ㄷ. 해시함수와 공개키 암호를 사용하여
생성된 디지털 서명은 기밀성, 인증, 무결성을 위해 사용할 수 있다.

---

① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ

♤ **디지털 서명**

ㄷ. 해시함수와 공개키 암호를 사용하여 생성된 디지털 서명은 기밀성, 인증, 무결성을 위해 사용할 수 있다.(×)
→ 디지털 서명은 기밀성을 제공하기 위한 것은 아니다.
→ 디지털 서명은 인증, 무결성, 부인방지를 제공한다.

정답 : ①

2. 전자서명(digital signature)은 내가 받은 메시지를 어떤 사람이 만들었는지를 확인하는 인증을 말한다. 다음 중 전자서명의 특징이 아닌 것은? [2015년 서울 9급]

① 서명자 인증 : 서명자 이외의 타인이 서명을 위조하기 어려워야 한다.
② 위조 불가 : 서명자 이외의 타인의 서명을 위조하기 어려워야 한다.
③ 부인 불가 : 서명자는 서명 사실을 부인할 수 없어야 한다.
④ 재사용 가능 : 기존의 서명을 추후에 다른 문서에도 재사용할 수 있어야 한다.

♤ **전자서명 요구조건**

• **재사용 불가** : 특정 문서의 전자서명을 다른 문서의 전자서명으로 사용할 수 없어야 한다.
→ 현실에서 사용되는 인감과 전자서명은 적용 방식이 다르다.
→ 하나의 인감은 여러 곳에 사용한다.
• 항목 ①과 ②는 다른 특징인데 설명이 같다.(출제자 실수??)

정답 : ④

3. 부인방지 서비스를 제공하기 위한 전자서명에 대한 설명으로 옳지 않은 것은? [2021년 국가 9급]

① 서명할 문서에 의존하는 비트 패턴이어야 한다.
② 다른 문서에 사용된 서명을 재사용하는 것이 불가능해야 한다.
③ 전송자(서명자)와 수신자(검증자)가 공유한 비밀정보를 이용하여 서명하여야 한다.
④ 서명한 문서의 내용을 임의로 변조하는 것이 불가능해야 한다.

♤ **전자서명**

- 전송자(서명자)와 수신자(검증자)가 **공유한 비밀정보**를 이용하여 서명하여야 한다.**(×)**
  → 서명은 **송신자**의 **개인키**를 이용하여 서명한다.
- 서명할 문서에 의존하는 비트 패턴이어야 한다. - 재사용 불가를 의미

◈ **전자서명이 제공하는 핵심 기능 - 3가지**

인증	서명은 신원이 올바른지 확인할 수 있다.
무결성	서명은 데이터 무결성을 확인할 수 있는 기능을 제공한다.
부인방지	서명의 고유성은 서명 소유자가 서명을 거부하지 못하도록 한다.

- 전자서명은 데이터 **기밀성**은 제공하지 않는다.
- 데이터 기밀성을 위해서는 **별도로 암호화**를 적용해야 한다.

정답 : ③

4. 전자서명(digital signature) 보안 메커니즘이 제공하는 보안 서비스가 아닌 것은? [2020년 지방 9급]

① 근원 인증
② 메시지 기밀성
③ 메시지 무결성
④ 부인방지

♤ **전자서명이 제공하는 핵심 기능 – 3가지**

- 인증 : 서명은 신원이 올바른지 확인할 수 있다.
- 부인방지 : 서명의 고유성은 서명 소유자가 서명을 거부하지 못하도록 한다.
- 데이터 무결성 : 서명은 데이터 무결성을 확인할 수 있는 기능을 제공한다.

정답 : ②

5. 전자서명의 활용 사례로 적합하지 않은 것은? [2020년 국회 9급]

① 인증서 로그인을 통해 사용자의 신원을 증명한다.
② 다운로드하는 소프트웨어의 위변조 여부를 확인한다.
③ 이메일 내용이 중간 메일서버에 노출되지 않도록 한다.
④ 웹브라우저로 통신하는 서버의 사이트가 유효한지 검증한다.
⑤ 폐기된 인증서들을 모아서 인증서 폐기 목록(CRL)을 발행한다.

♤ **전자서명이 제공하는 핵심 기능 - 3가지**

인증	서명은 신원이 올바른지 확인할 수 있다.
무결성	서명은 데이터 무결성을 확인할 수 있는 기능을 제공한다.
부인방지	서명의 고유성은 서명 소유자가 서명을 거부하지 못하도록 한다.

• 전자서명은 데이터 기밀성은 제공하지 않는다.(데이터 기밀성을 위해서는 별도로 **암호화 적용**)
• 이메일 내용이 중간 메일서버에 노출되지 않도록 한다. ← **기밀성 유지 (암호화)**

정답 : ③