전자문서의 무결성·진본성의 의미

❑ 진본성(Authenticity)

- 전자문서 원본의 본질적 특성을 재현하여 동일한 속성을 지니면서, 부당한 변경 또는 변조되지 않은 생성 당시 그대로 인 것.
- 진본 기록을 판단하는 기준으로 **생산된 연원, 무결성, 내적 완전성에 기반하여 판단**(ISO 15489)

❑ 무결성(Integrity)

- **망실 · 훼손 · 손상 · 변조 등에 의하여 기록이 변경되지 않고 완전한 상태를 유지하고 있음을 지칭**
- **전자기록 : 무결성 확보를 위해 어느 정도의 변형은 불가피 함으로, 그 기록이 담고 있는 의미가 변하지 않는 한, 완전하고 변조되지 않은 것으로 간주**
- **시스템측면에서 접근제어기능, 수정 기록(로고, 메타데이터 등)을 통해 무결성 보호(DRM관련 기술)**
- **종이기록 : 잉크 번짐, 모서리 멸실 등으로 무조건 무결성이 손상된 것으로 간주하지는 않음**

❑ 진본성과 무결성의 관계

- **진본성이 목표라면! 무결성을 보장하는 일은 진본성을 확보하기 위한 기본적 처리 과정**

무결성은 '보장'하는 것 < **진본성은 '입증'하는 것**

전자서명(Digital Signature)_1

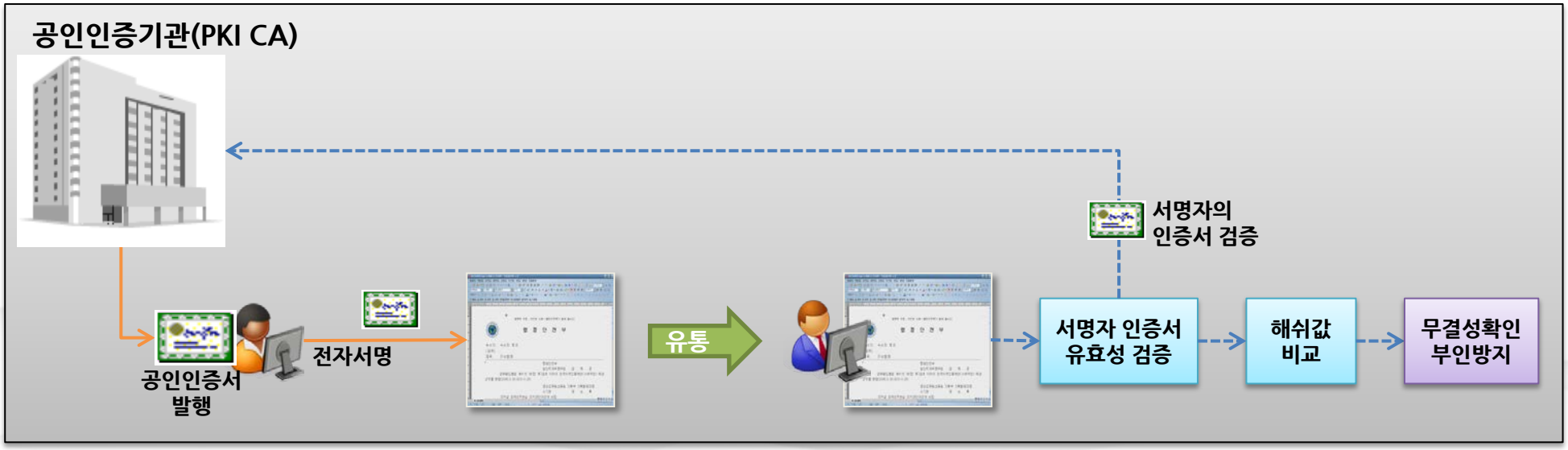
❑ 전자서명의 정의

- 법적 측면 : "전자서명"이라 함은 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.(전자서명법 제2조)
- 기술적 정의 : 전자문서의 해쉬값(HASH)에 서명자의 개인키로 암호화한 것

❑ 인증서 파일 구성

개인키 (전자서명생성정보)	공개키인증서 (전자서명검증정보)
	
파일명 : … .key	파일명 : … .cer
개인키, Password정보	발행자, 유효기간 소유자, 공개키정보, 발행자서명정보 등

❑ 전자서명 처리흐름



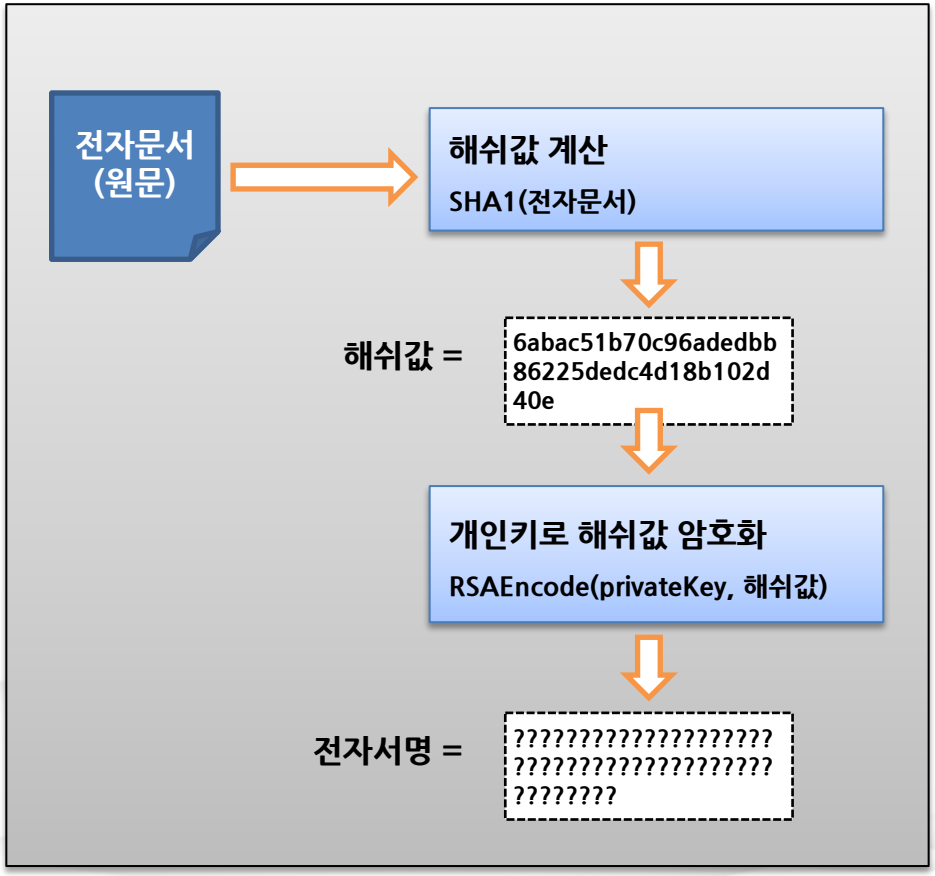
전자서명(Digital Signature)_2

❑ 전자서명 과정

전자문서

➔ 원문 해쉬(SHA)

➔ 개인키로 암호화(RSA)

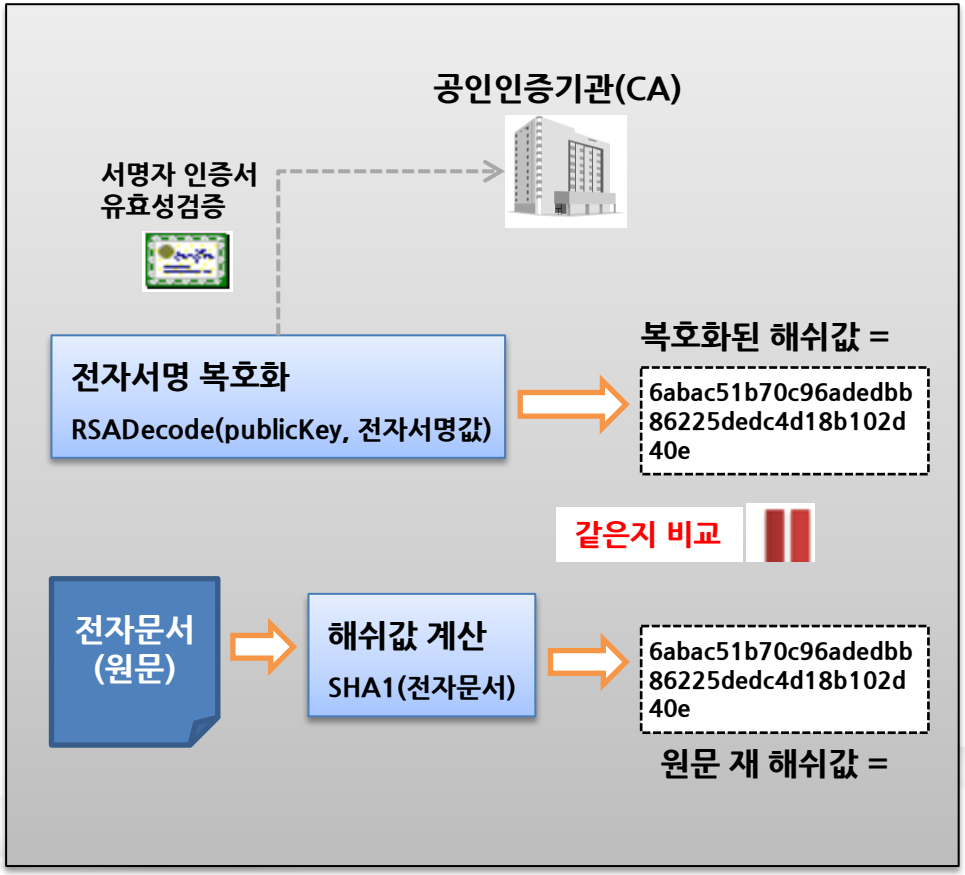


❑ 전자서명 검증과정

서명자인증서유효성체크

➔ 서명값 복호화

➔ 원본 재 해쉬 ➔ 해쉬값 상호 비교



전자서명(Digital Signature)_3

❑ 전자서명의 효과

- 무결성 : 원문을 조금이라도 조작하게 되면, 해쉬함수의 효과로 인해 해쉬값이 완전히 다르게 나옴
- 부인방지, 본인확인 : 개인키(서명자 본인만 소유)로 암호화 하고, 공개키로 복호화하는 비대칭 암호화 방식
- 기밀성 : 암호화, 복호화 기술 사용

❑ 진본성·무결성 관점에서의 기술특징

- 전자서명은 무결성은 보장되지만, 서명자 본인의 개인키로 암호화 함으로, 진본성을 입증 하기에는 서명자의 신뢰도에 따라 다소 한계가 있음

타임스탬프 (Time Stamp)_1

❑ 타임스탬프의 정의

- 신뢰할 수 있는 제3자(TTP, Trusted Third Party)에 의해, 전자문서가 특정 시점(타임스탬프 발급시점)에 존재하고 있었고, 이후 전자문서의 무변경성을 보장

❑ 국제표준

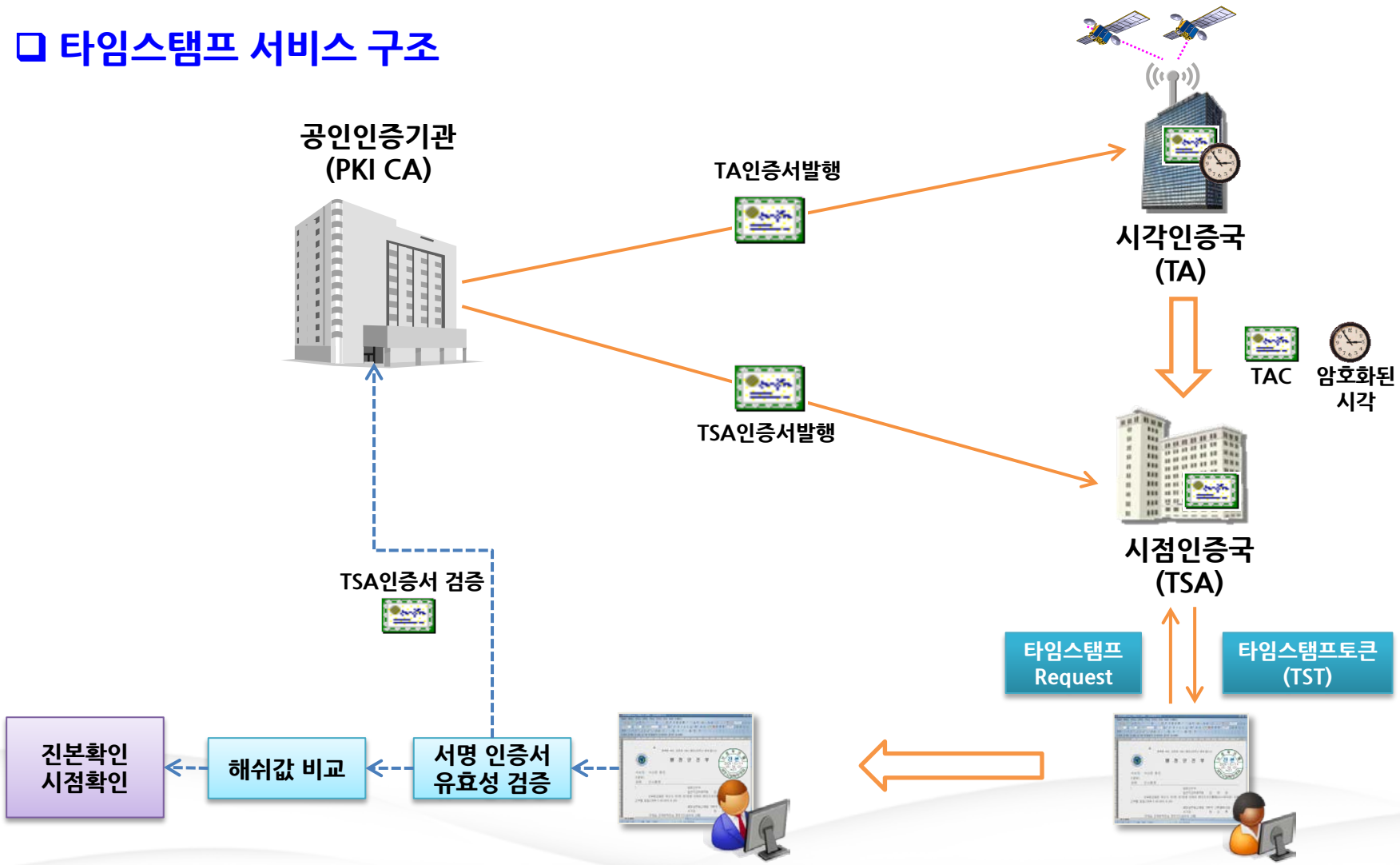
- ISO/IEC 18014 Information Technology - Security Techniques - Time Stamping Services
- RFC 3161 Internet X.509 Public Key Infrastructure Time Stamp Protocol

❑ 전자서명과의 비교

구 분	전자서명	타임스탬프
원문처리방식	원문 hash 후 개인키로 서명(암호화)	좌동
서명자	본인	신뢰할 수 있는 제3자(TTP) - TSA
시각정보	없거나 서명 당시 컴퓨터 시각	신뢰할 수 있는 표준시
효과	무결성, 본인(서명자)확인, 부인방지	진본성, 무결성, 시점확인

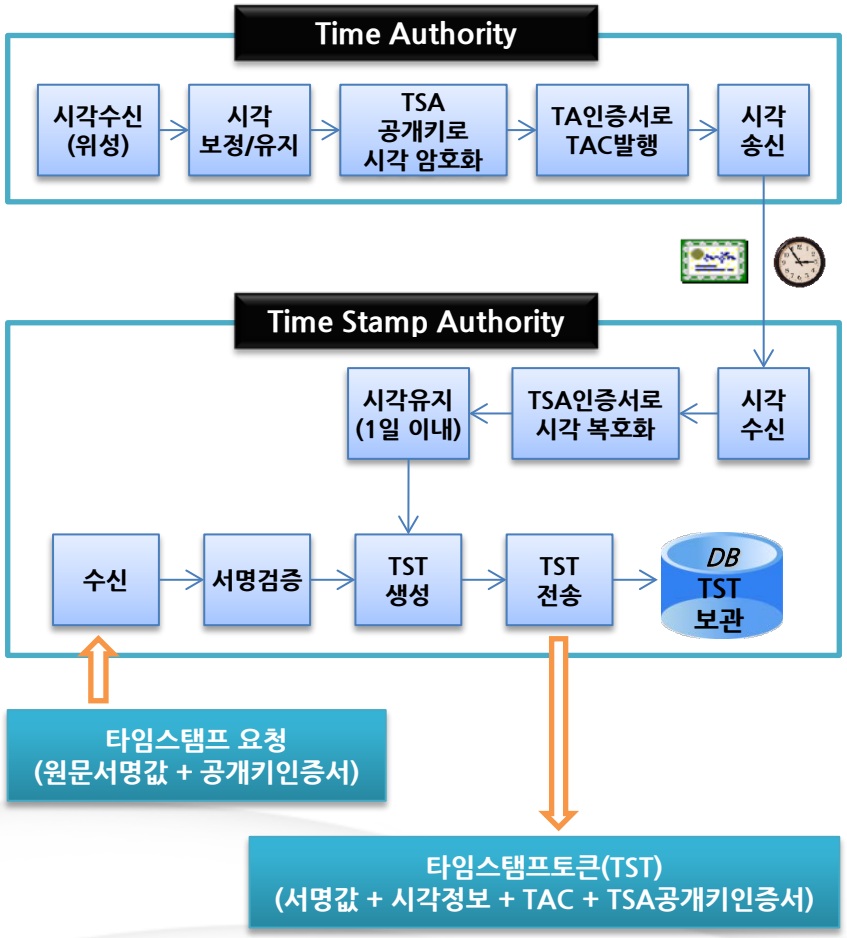
타임스탬프 (Time Stamp)_2

❑ 타임스탬프 서비스 구조

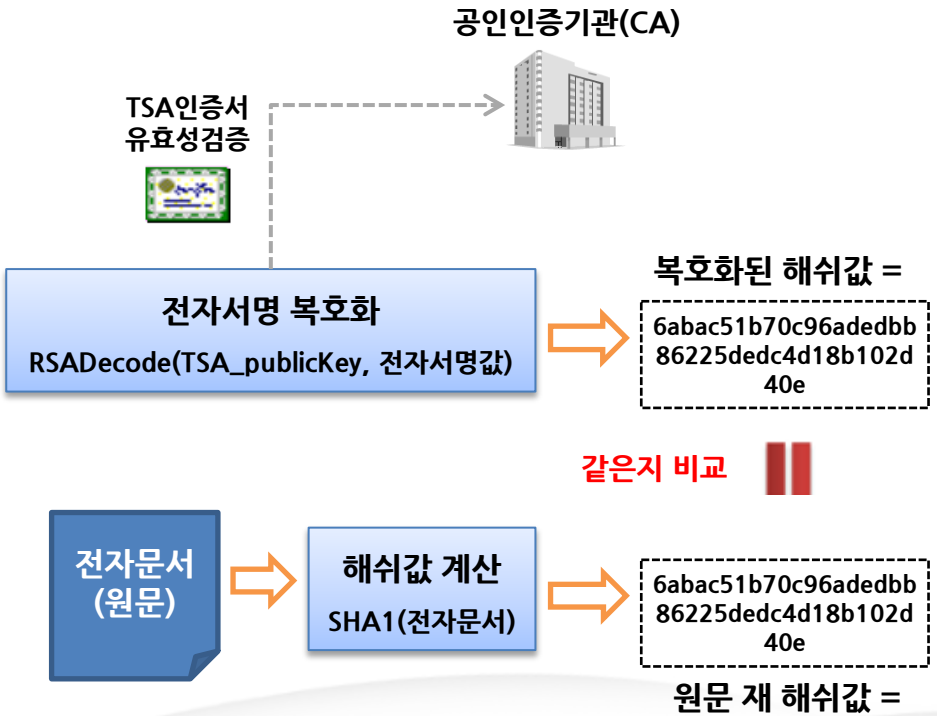


타임스탬프 (Time Stamp)_3

❑ 타임스탬프 발급과정

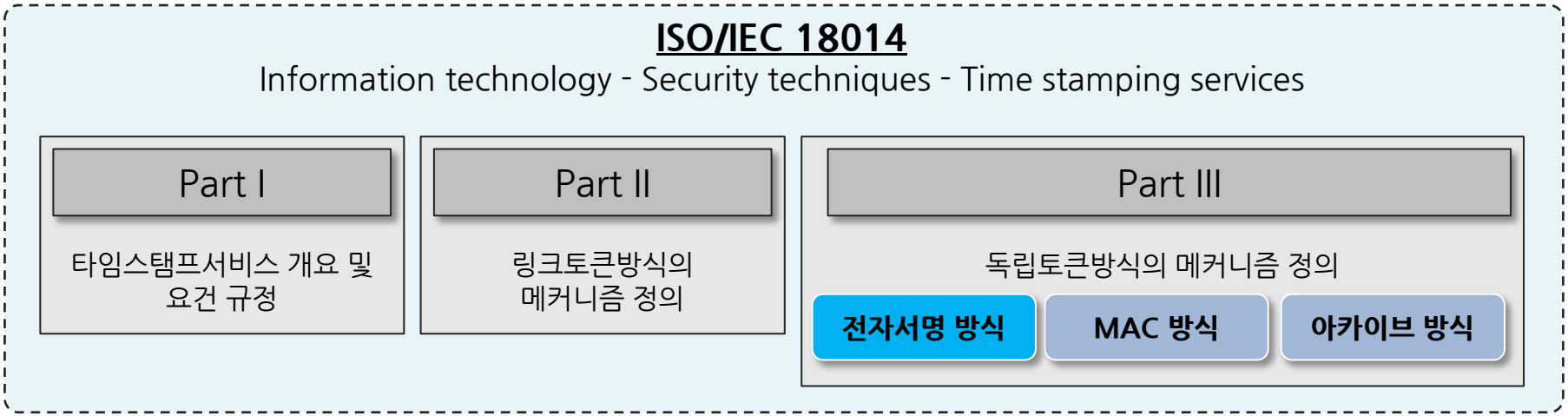


❑ 타임스탬프 검증과정



타임스탬프 (Time Stamp)_4

❑ 타임스탬프 서비스 분류



❑ 타임스탬프토큰 관리방법 분류

- Embedded 방식 : 원문파일 내에 포함하여 저장하는 방식으로 포함 이후 원래의 파일형식(포맷)은 유지됨
- Attached 방식 : 원문파일에 이어서 덧붙이는 방식으로 원문파일의 형식(포맷)은 변경됨
- Separated 방식 : 원문파일과 독립적으로 별개의 파일로 저장하는 방식
- DB Meta data 방식 : 원문파일과 별도로 DB에 저장하는 방식

전자서명과 타임스탬프 비교(1)

구분		전자서명	타임스탬프
원문처리방식		원문 hash 후 개인키로 서명(암호화)	좌동
서명자		본인	신뢰할 수 있는 제3자(TTP) - TSA
시각정보		없거나 서명 당시 컴퓨터 시각	신뢰할 수 있는 표준시
유효기간		1일(최소) ~ 1년(최대)	9년(최소) ~ 10년(최대)
효과		무결성, 본인(서명자)확인, 부인방지	진본성, 무결성, 시점확인
법적근거		전자서명법	전자서명법, 전자정부법, 전자거래기본법
전자계약 적용 시 장단점	인증서 소지	인증서를 소지해야 함 (모바일 단말기에)	인증서 소지 불필요
	인증서 갱신	인증서가 만료되면, 계약체결이 불가능함으로 만료 전 재발급 필요	인증기관(TSA)의 인증서 갱신 필요
	인증서 관리주체	개인별 관리 (인증서 발급/소지/갱신/모바일 탑재 등)	인증기관(TSA)
	진본인증	제3자 진본인증 안됨 (개인 인증서로 서명함으로)	제3자 진본 인증 가능 (공인인증기관의 인증서로 서명함으로)
	유효기간	인증서 유효기관 만료직전 서명한 문서는 서명직후 실효될 수 있음	최소 9년 이상의 유효기간 보장

전자서명과 타임스탬프 비교(2)

❖ **정보의 안전한 이용은 전자서명의 본인확인 기능과 타임스탬프의 진본성 및 시점확인 기능을 병행해서 사용하면 가장 효과 적이고 확실함**

구 분	전자서명(Digital Signature)		타임스탬프(Time Stamp)	
목 적	 본인증명	 진본성 확인 **(본인 인증)**	 진본성 확인 **(3자 공증)**	 시점확인
적용 기술	• 개인키에 대한 비밀번호 확인으로 본인인증 • 공개키인증서에 있는 유효기간 등의 확인으로 유효성 인증	• 전자문서를 해쉬함 • 해쉬값에 개인 비밀키를 이용 암호화	• 전자문서를 해쉬함 • 해쉬값에 대한 TSA로 부터 시점확인 요청 • TSA서버 비밀키 이용하여 해쉬값 암호화 • TSA로 부터 수신한 TST에서 해쉬값 추출	• TSA로 부터 수신한 TST에서 시각 정보 추출
특징 장점	• 인터넷 상에서 대면 없이 본인확인을 할 수 있는 가장 확실한 방법 • 유일한 개인키와 발급시 본인확인하는 공개키 인증서 이용(PKI)	본인이 직접 서명 [진 본 성] **신뢰하는 제3자 서명** 재서명 가능 [신 뢰 성] **새로운 서명추가** 조작가능(PC/서버) [시각정보] **신뢰하는 제3자 시각** 불명확 [서명시점] **명확** **불가능** [원본증명] 가능 1년 [유효기간] **10년** **조직, 인력 증가 [원본증명 비용] 시스템으로 대체**		• 신뢰할 수 있는 기관에 시각 관리 및 서비스로 표준시 제공 • 신뢰할 수 있는 시각서비스로 존재증명 가능 • 전자문서의 시점확인 가능