(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년06월29일
(11) 등록번호 10-1863953
(24) 등록일자 2018년05월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06Q 20/38* (2012.01)
(52) CPC특허분류
H04L 9/3247 (2013.01)
G06Q 20/3825 (2013.01)
(21) 출원번호 10-2016-0075098
(22) 출원일자 2016년06월16일
심사청구일자 2016년06월16일
(65) 공개번호 10-2017-0141976
(43) 공개일자 2017년12월27일
(56) 선행기술조사문헌
KR100506700 B1*
KR101172871 B1*
KR1020130051636 A*
A. Menezes 외 2명, Handbook of Applied Cryptography, Chapter 12, CRC Press (1996)
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 티모넷
서울특별시 마포구 마포대로 86 , 6층 620호(도화동, 창강빌딩)
(72) 발명자
박진우
서울특별시 강남구 압구정로 151, 123동 601호 (압구정동, 현대아파트)
박경봉
경기도 수원시 장안구 장안로359번길 20, 205동 1504호 (이목동, 수원장안힐스테이트)
(뒷면에 계속)
(74) 대리인
리앤목특허법인

전체 청구항 수 : 총 11 항 심사관 : 양종필

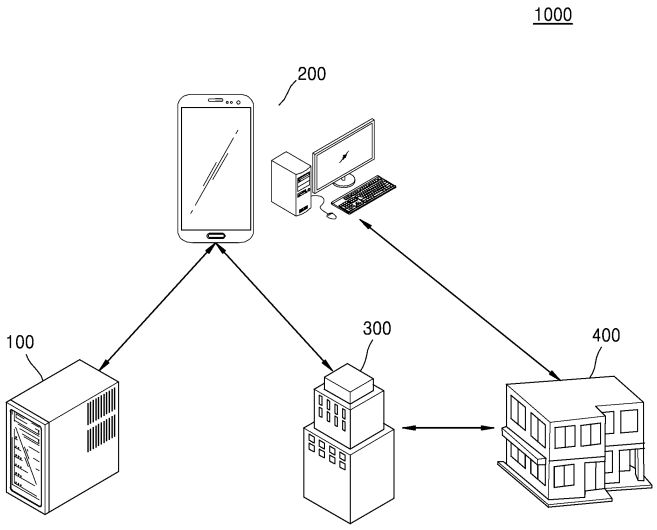
(54) 발명의 명칭 **전자 서명 서비스 시스템 및 방법**

(57) 요 약

전자 서명 서비스 시스템, 서버, 단말 및 방법이 제공된다.

개시된 실시예에 따르면, 전자 서명 서비스 서버가 사용자의 개인키를 등록할 수 있다. 전자 서명 서비스 서버는 사용자 단말로부터 서명 대상 데이터 및 서명 대상 데이터에 대한 전자 서명의 요청을 수신한다. 전자 서명 서비스 서버는 등록된 사용자의 개인키를 이용하여 전자 서명을 생성하고, 생성한 전자 서명을 사용자 단말에게 전송한다.

대 표 도 - 도1



(52) CPC특허분류
G06Q 20/3829 (2013.01)
G06Q 20/385 (2013.01)
H04L 9/3213 (2013.01)
H04L 9/3263 (2013.01)
(72) 발명자
김진근
서울특별시 양천구 신정로 293, 109동 704호 (신정동, 신트리1단지아파트)
이문혁
서울특별시 은평구 통일로68가길 18-2, 지층1호 (불광동)

명 세 서

청구범위

청구항 1

전자 서명 서비스 서버가 전자 서명 서비스를 제공하는 방법에 있어서,

사용자의 개인키를 상기 전자 서명 서비스 서버에 등록하는 단계;

사용자 단말에서 사용자가 입력하는 ID, 패스워드, PIN, 사용자의 생체 신호 중 적어도 하나를 포함하는 사용자 입력 정보에 의해 로컬 인증을 하는 단계;

상기 로컬 인증 후 상기 사용자 단말로부터 상기 사용자 단말을 인증하기 위해 기기 인증용 키 쌍에 포함된 기기 인증용 개인키에 의해 생성된 기기 인증 데이터를 수신하는 단계;

상기 전자 서명 서비스 서버의 프로세서가 상기 기기 인증 데이터를 검증하는 단계; 및

사용자 단말로부터 서명 대상 데이터 및 상기 서명 대상 데이터에 대한 전자 서명의 요청을 수신하는 단계;

상기 요청에 응답하여, 상기 사용자의 개인키를 이용하여 상기 서명 대상 데이터에 대한 상기 전자 서명을 생성하는 단계;

상기 전자서명을 상기 사용자 단말에게 전송하는 단계;를 포함하며,

상기 전자 서명 서비스 서버가 상기 사용자의 개인키를 이용하여 상기 전자 서명을 생성하는 전자 서명 생성 모듈을 포함하고,

상기 전자 서명 생성 모듈이 상기 프로세서와 분리된 하드 웨어 보안 모듈로 구성되고,

상기 전자 서명 생성 모듈을 제외한 다른 장치가 상기 개인키를 복제 및 확인할 수 없도록 상기 개인키를 상기 하드웨어 보안 모듈에 저장하며,

상기 사용자 단말에게 전송된 전자 서명은, 상기 서명 대상 데이터 및 상기 개인키에 대응되는 공개키와 함께, 상기 사용자 단말로부터 상기 전자 서명을 이용하는 이용 서버에게 제공되는 것인 전자 서명 서비스 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

제 1 항에 있어서,

상기 기기 인증 데이터를 검증하는 단계는,

상기 기기 인증 데이터를 상기 기기 인증용 키 쌍에 포함된 기기 인증용 공개키로 상기 기기 인증 데이터를 검증하는 전자서명 서비스 방법.

청구항 7

제 1 항에 있어서,

상기 기기 인증 데이터가 검증됨에 따라, 상기 전자 서명 서비스 서버와 상기 사용자 단말 간에 송수신되는 정보의 보안을 위해 상기 전자 서명 서비스 서버와 상기 사용자 단말 사이의 통신 보안 세션을 생성하는 단계;를 더 포함하는 전자 서명 서비스 방법.

청구항 8

제 7 항에 있어서,

상기 통신 보안 세션을 생성하는 단계는,

세션키 및 토큰을 생성하는 단계 및 상기 세션키 및 토큰을 기기 인증용 공개키로 암호화 하여 상기 사용자 단말에 전송하는 단계를 포함하는 전자 서명 서비스 방법.

청구항 9

제 8 항에 있어서,

상기 전자 서명의 요청을 수신하는 단계는, 상기 사용자 단말이 전송하는 토큰을 함께 수신하고,

상기 전자 서명을 생성하는 단계는, 상기 사용자 단말로부터 수신한 토큰과 전자 서명 서비스 서버가 생성한 토큰이 일치하는 지 확인하고, 상기 전자 서명을 생성하는 전자 서명 서비스 방법.

청구항 10

제 8 항에 있어서,

상기 통신 보안 세션을 생성하는 단계는,

상기 사용자 단말이 제1 난수로부터 상기 세션키를 이용하여 생성한 단말 인증 데이터를 상기 사용자 단말로부터 수신하고, 상기 단말 인증 데이터를 검증하는 단계 및

제2 난수로부터 상기 세션키를 이용하여 서버 인증 데이터를 생성하고 상기 서버 인증 데이터를 상기 사용자 단말에게 전송하여 검증하는 단계를 포함하는 전자 서명 서비스 방법.

청구항 11

제 8 항에 있어서,

상기 사용자 단말로부터 수신하는 상기 전자 서명의 요청 및 서명 대상 데이터는 상기 세션키를 이용하여 암호화 된 것으로,

상기 암호화 된 전자 서명의 요청 및 서명 대상 데이터를 상기 세션키를 이용하여 복호화 하는 단계;를 더 포함하는 전자 서명 서비스 방법.

청구항 12

전자 서명 서비스 서버가 전자 서명 서비스를 제공하는 방법에 있어서,

사용자 단말에서 사용자가 입력하는 ID, 패스워드, PIN, 사용자의 생체 신호 중 적어도 하나를 포함하는 사용자 입력 정보에 의해 로컬 인증을 하는 단계;

상기 사용자 단말로부터 기기 인증 데이터를 수신하는 단계;

상기 기기 인증 데이터를 검증하는 단계;

상기 기기 인증 데이터가 검증 됨에 따라 상기 사용자 단말로부터 상기 사용자의 전자 서명 생성을 위한 키 쌍 생성의 요청을 수신하는 단계;

상기 사용자의 전자 서명 생성을 위한 키 쌍을 생성하는 단계;

상기 키 쌍에 포함된 개인키를 저장부에 저장하는 단계; 및

상기 키 쌍에 포함된 공개키를 상기 사용자 단말에 전송하는 단계;를 포함하며,

상기 전자 서명 서비스 서버가 상기 전자 서명을 생성하는 전자 서명 생성 모듈을 포함하고, 상기 개인키는, 상기 전자 서명 생성 모듈이 서명 대상 데이터에 대한 전자 서명을 생성하는데 이용되고,

상기 기기 인증 데이터는 기기 인증용 키 쌍에 포함된 기기 인증용 개인키에 의해 생성되며,

상기 저장부는 상기 전자 서명 생성을 위한 키 쌍에 포함된 개인키를 저장하는 제1 저장 공간과, 인증서 데이터가 저장되는 제2 저장 공간을 포함하며, 상기 제1 저장 공간과 제2 저장 공간은 서로 다르며, 상기 제1 저장 공간 및 상기 전자 서명 생성 모듈이 하드웨어 보안 모듈을 구성하여 상기 전자 서명 생성 모듈만이 상기 개인키를 복제 및 확인할 수 있도록 구성된 전자 서명 서비스 방법.

청구항 13

삭제

청구항 14

삭제

청구항 15

제 12 항에 있어서,

상기 사용자 단말로부터 상기 키 쌍 생성의 확인을 위한 개인키 소유여부 검증정보 및 상기 개인키 소유여부 검증정보에 대한 전자 서명의 요청을 수신하는 단계;

상기 저장부에 저장된 상기 개인키를 이용하여 개인키 소유여부 검증정보에 대한 전자 서명을 생성하는 단계;

상기 개인키 소유여부 검증정보에 대한 전자 서명을 상기 사용자 단말에 전송하는 단계;를 포함하는 전자서명 서비스 방법.

청구항 16

삭제

청구항 17

사용자 단말에서 사용자가 입력하는 ID, 패스워드, PIN, 사용자의 생체 신호 중 적어도 하나를 포함하는 사용자 입력 정보에 의해 로컬 인증을 하는 사용자 단말과 통신하는 통신부;

사용자의 전자서명 생성을 위한 개인키를 저장하는 저장부;

상기 통신부가 상기 사용자 단말로부터 서명 대상 데이터 및 상기 서명 대상 데이터에 대한 전자 서명의 요청을 수신하면, 상기 개인키를 이용하여 상기 서명 대상 데이터에 대한 전자 서명을 생성하는 전자 서명 생성 모듈; 및

상기 사용자 단말로부터 획득된 단말 인증 데이터를 검증하고, 상기 사용자 단말에게 전송하는 서버 인증 데이터를 생성하는 프로세서;를 포함하며,

상기 통신부는 상기 전자 서명 생성 모듈이 생성한 상기 전자서명을 상기 사용자 단말로 전송하고,

상기 전자 서명 생성 모듈을 제외한 다른 장치가 상기 개인키를 복제 및 확인할 수 없도록 상기 개인키를 저장하고,

상기 저장부는 상기 개인키를 저장하는 제1 저장 공간과 인증서 데이터를 저장하는 제2 저장 공간을 포함하며, 상기 제1 저장 공간과 제2 저장 공간은 서로 분리되도록 구성되며,

상기 제1 저장 공간 및 상기 전자 서명 생성 모듈은 상기 프로세서와 분리된 하드웨어 보안 모듈을 구성하며,

상기 프로세서는 상기 사용자 단말로부터 획득한 기기 인증 데이터를 검증하며,

상기 기기 인증 데이터는 기기 인증용 키 쌍에 포함된 기기 인증용 개인키에 의해 생성된 것으로, 상기 프로세서는 상기 기기 인증용 키 쌍에 포함된 기기 인증용 공개키를 이용하여 상기 기기 인증 데이터를 검증하는 전자 서명 서비스 서버.

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

제 17 항에 있어서,

상기 프로세서는, 상기 기기 인증 데이터가 검증 됨에 따라, 상기 전자 서명 서비스 서버와 상기 사용자 단말 간에 송수신되는 정보의 보안을 위해 상기 전자 서명 서비스 서버와 상기 사용자 단말 사이의 통신 보안 세션을 생성하는 전자 서명 서비스 서버.

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

발명의 설명

기 술 분 야

[0001] 전자 서명 서비스를 제공하는 시스템, 서버, 단말 및 방법에 관한 것이다.

배 경 기 술

[0002] 공인 인증서는 공신력이 있는 공인인증기관에서 발급한 전자 서명 인증서로서, 우리나라의 경우 인터넷 뱅킹뿐만 아니라 온라인 증명서 발급, 전자상거래, 인터넷 주식거래 등 다양한 분야에서 필수적으로 사용되고 있다.

[0003] 기존의 PC 환경에서 공인 인증서 사용 형태를 살펴보면, 공인 인증서를 하드 디스크, 이동식 디스크, 휴대폰, 저장 토큰, 보안 토큰 등에 저장해 두고 있다가 인터넷 금융거래 등을 위해 공인인증이 필요한 경우 하드 디스크 등에 저장된 공인 인증서를 통해 전자 서명을 생성하고 이를 인증 서버가 검증함으로써 공인인증을 수행하는 방식이다.

[0004] 상술한 공인인증 방식에서는 사용자가 공인 인증서가 저장된 매체를 소지하고 다녀야 하는 불편함이 있다. 그리고, 사용자가 공인 인증서를 사용할 수 있는 매체 수를 늘리기 위해서는 공인 인증서를 여러 매체에 복사, 이동하는 작업을 수행해야 하는 번거로움이 있다. 또한, 다수 매체에 공인 인증서가 저장되어 있으면 매체의 분실 혹은 타인이 매체에 접근함으로써 공인 인증서의 유출 가능성이 높아지는 위험이 있다.

발명의 내용

해결하려는 과제

[0005] 일부 실시예는, 사용자의 개인키를 등록하고 등록된 사용자의 개인키를 이용하여 사용자 단말로부터 수신한 서명 대상 데이터에 대한 전자 서명을 생성하는 전자 서명 서비스 서버를 개시한다.

과제의 해결 수단

[0006] 일 측면에 따르면,

[0007] 전자 서명 서비스 서버가 전자 서명 서비스를 제공하는 방법에 있어서,

[0008] 사용자 단말로부터 서명 대상 데이터 및 상기 서명 대상 데이터에 대한 전자 서명의 요청을 수신하는 단계;

[0009] 상기 요청에 응답하여, 기 등록된 상기 사용자의 개인키를 이용하여 상기 서명 대상 데이터에 대한 상기 전자 서명을 생성하는 단계;

[0010] 상기 전자서명을 상기 사용자 단말에게 전송하는 단계;를 포함하며,

[0011] 상기 사용자 단말에게 전송된 전자 서명은, 상기 서명 대상 데이터 및 상기 개인키에 대응되는 공개키와 함께, 상기 사용자 단말로부터 상기 전자 서명을 이용하는 이용 서버에게 제공되는 것인 전자 서명 서비스 방법이 제공된다.

[0012] 상기 개인키를 등록하는 단계는, 상기 개인키를 이용하여 상기 전자 서명을 생성하는 전자 서명 생성 모듈을 제외한 다른 장치가 상기 개인키를 복제 및 확인할 수 없도록 상기 개인키를 저장할 수 있다.

[0013] 상기 사용자의 인증서 데이터는 상기 개인키와 함께 상기 전자 서명 서비스 서버에 등록되며,

[0014] 상기 사용자 단말에게 상기 사용자의 인증서 데이터를 전송하는 단계;를 더 포함할 수 있다.

[0015] 상기 전자 서명 서비스 방법은 상기 사용자 단말로부터 상기 사용자 단말을 인증하기 위한 기기 인증 데이터를 수신하는 단계; 및

[0016] 상기 기기 인증 데이터를 검증하는 단계;를 더 포함하며,

[0017] 상기 전자 서명을 생성하는 단계는, 상기 기기 인증 데이터가 검증 됨에 따라 상기 전자 서명을 생성할 수 있다.

[0018] 상기 기기 인증 데이터는 기기 인증용 키 쌍에 포함된 기기 인증용 개인키에 의해 생성된 것일 수 있다.

[0019] 상기 기기 인증 데이터를 검증하는 단계는,

[0020] 상기 기기 인증용 키 쌍에 포함된 기기 인증용 공개키로 상기 기기 인증 데이터를 검증할 수 있다.

[0021] 상기 기기 인증 데이터가 검증됨에 따라, 상기 전자 서명 서비스 서버와 상기 사용자 단말 간에 송수신되는 정보의 보안을 위해 상기 전자 서명 서비스 서버와 상기 사용자 단말 사이의 통신 보안 세션을 생성하는 단계;를 더 포함할 수 있다.

[0022] 상기 통신 보안 세션을 생성하는 단계는,

[0023] 세션키 및 토큰을 생성하는 단계 및 상기 세션키 및 토큰을 상기 기기 인증용 공개키로 암호화 하여 상기 사용자 단말에 전송하는 단계를 포함할 수 있다.

[0024] 상기 전자 서명의 요청을 수신하는 단계는, 상기 사용자 단말이 전송하는 토큰을 함께 수신하고,

[0025] 상기 전자 서명을 생성하는 단계는, 상기 사용자 단말로부터 수신한 토큰과 전자 서명 서비스 서버가 생성한 토큰이 일치하는 지 확인하고, 상기 토큰에 매칭되는 개인키를 이용하여 상기 전자 서명을 생성할 수 있다.

[0026] 상기 통신 보안 세션을 생성하는 단계는,

[0027] 상기 사용자 단말이 제1 난수로부터 상기 세션키를 이용하여 생성한 단말 인증 데이터를 상기 사용자 단말로부터 수신하고, 상기 단말 인증 데이터를 검증하는 단계 및

[0028] 제2 난수로부터 상기 세션키를 이용하여 서버 인증 데이터를 생성하고 상기 서버 인증 데이터를 상기 사용자 단

말에게 전송하는 단계를 포함할 수 있다.

[0029] 상기 사용자 단말로부터 수신하는 상기 전자 서명의 요청 및 서명 대상 데이터는 상기 세션키를 이용하여 암호화 된 것으로,

[0030] 상기 전자 서명 서비스 방법은, 상기 암호화 된 전자 서명의 요청 및 서명 대상 데이터를 상기 세션키를 이용하여 복호화 하는 단계;를 더 포함할 수 있다.

[0031] 다른 측면에 있어서,

[0032] 전자 서명 서비스 서버가 전자 서명 서비스를 제공하는 방법에 있어서,

[0033] 사용자 단말로부터 기기 인증 데이터를 수신하는 단계;

[0034] 상기 기기 인증 데이터를 검증하는 단계;

[0035] 상기 기기 인증 데이터가 검증 됨에 따라 상기 사용자 단말로부터 상기 사용자의 전자 서명 생성을 위한 키 쌍 생성의 요청을 수신하는 단계;

[0036] 상기 사용자의 전자 서명 생성을 위한 키 쌍을 생성하는 단계;

[0037] 상기 키 쌍에 포함된 개인키를 저장부에 저장하는 단계; 및

[0038] 상기 키 쌍에 포함된 공개키를 상기 사용자 단말에 전송하는 단계;를 포함하며,

[0039] 상기 개인키는, 전자 서명 서비스 서버의 전자 서명 생성 모듈이 상기 서명 대상 데이터에 대한 전자 서명을 생성하는데 이용되는 전자 서명 서비스 방법이 제공된다.

[0040] 상기 전자 서명 서비스 방법은, 상기 사용자 단말로부터 상기 사용자의 인증서 데이터를 수신하는 단계; 및

[0041] 상기 인증서 데이터를 상기 저장부에 저장하는 단계;를 더 포함할 수 있다.

[0042] 상기 인증서 데이터를 상기 저장부에 저장하는 단계는, 상기 인증서 데이터가 저장되는 저장 공간이 상기 개인키가 저장되는 저장 공간과 서로 달라지도록 상기 인증서 데이터를 저장할 수 있다.

[0043] 상기 전자 서명 서비스 방법은, 상기 사용자 단말로부터 상기 키 쌍 생성의 확인을 위한 개인키 소유여부 검증정보 및 상기 개인키 소유여부 검증정보에 대한 전자 서명의 요청을 수신하는 단계;

[0044] 상기 저장부에 저장된 상기 개인키를 이용하여 개인키 소유여부 검증정보에 대한 전자 서명을 생성하는 단계;

[0045] 상기 개인키 소유여부 검증정보에 대한 전자 서명을 상기 사용자 단말에 전송하는 단계;를 더 포함할 수 있다.

[0046] 다른 측면에 있어서,

[0047] 전자 서명 서비스 서버가 전자 서명 서비스를 제공하는 방법에 있어서,

[0048] 사용자 단말로부터 기기 인증 데이터를 수신하는 단계;

[0049] 상기 기기 인증 데이터를 검증하는 단계;

[0050] 상기 기기 인증 데이터가 검증 됨에 따라 상기 사용자 단말로부터 사용자의 전자 서명 생성을 위한 키 쌍 정보를 수신하는 단계;

[0051] 상기 키 쌍에 포함된 개인키는 저장부의 제1 저장 공간에 저장하고, 상기 키 쌍에 포함된 공개키는 저장부의 제2 저장 공간에 저장하는 단계;를 포함하며,

[0052] 상기 개인키는 상기 전자 서명을 생성하는 전자 서명 생성 모듈을 제외한 다른 장치가 복제 및 확인할 수 없도록 상기 제1 저장 공간에 저장되는 전자 서명 서비스 방법이 제공된다.

[0053] 다른 측면에 있어서,

[0054] 사용자 단말과 통신하는 통신부;

[0055] 사용자의 전자서명 생성을 위한 개인키를 저장하는 저장부;

[0056] 상기 통신부가 상기 사용자 단말로부터 서명 대상 데이터 및 상기 서명 대상 데이터에 대한 전자 서명의 요청을 수신하면, 상기 개인키를 이용하여 상기 서명 대상 데이터에 대한 전자 서명을 생성하는 전자 서명 생성 모듈;

을 포함하며,

[0057] 상기 통신부는 상기 전자 서명 생성 모듈이 생성한 상기 전자서명을 상기 사용자 단말로 전송하는 전자서명 서비스 서버가 제공된다.

[0058] 상기 저장부는 상기 전자 서명 생성 모듈을 제외한 다른 장치가 상기 개인키를 복제 및 확인할 수 없도록 상기 개인키를 저장할 수 있다.

[0059] 상기 저장부는 상기 개인키를 저장하는 제1 저장 공간을 포함하며,

[0060] 상기 제1 저장 공간 및 상기 전자 서명 생성 모듈은 하드웨어 보안 모듈(Hardware Security Module)을 구성할 수 있다.

[0061] 상기 통신부는 상기 사용자 단말로부터 상기 사용자의 인증서 데이터를 수신하고, 상기 저장부는 상기 인증서 데이터를 저장하는 제2 저장 공간을 포함하며, 상기 제1 및 제2 저장 공간은 서로 분리되도록 구성될 수 있다.

[0062] 상기 전자 서명 서비스 서버는 상기 사용자 단말로부터 획득된 단말 인증 데이터를 검증하고, 상기 사용자 단말에게 전송하는 서버 인증 데이터를 생성하는 프로세서;를 더 포함할 수 있다.

[0063] 상기 기기 인증 데이터는 기기 인증용 키 쌍에 포함된 기기 인증용 개인키에 의해 생성된 것으로,

[0064] 상기 프로세서는 상기 기기 인증용 키 쌍에 포함된 기기 인증용 공개키를 이용하여 상기 기기 인증 데이터를 검증할 수 있다.

[0065] 상기 프로세서는, 상기 기기 인증 데이터가 검증 됨에 따라, 상기 전자 서명 서비스 서버와 상기 사용자 단말 간에 송수신되는 정보의 보안을 위해 상기 전자 서명 서비스 서버와 상기 사용자 단말 사이의 통신 보안 세션을 생성할 수 있다.

[0066] 다른 측면에 있어서,

[0067] 사용자 단말이 전자 서명 서비스 서버로부터 전자 서명을 획득하는 방법에 있어서,

[0068] 상기 전자서명 서비스 서버에게 기기 인증 데이터를 제공하는 단계;

[0069] 상기 전자서명 서비스 서버에 의해 상기 기기 인증 데이터의 검증이 완료되면, 상기 전자서명 서비스 서버에게 서명 대상 데이터 및 상기 서명 대상 데이터에 대한 전자 서명의 요청을 전송하는 단계;

[0070] 상기 전자서명 서비스 서버에 등록된 상기 사용자의 개인키에 의해 생성된 전자 서명을 상기 전자 서명 서비스 서버로부터 수신하는 단계;

[0071] 상기 전자 서명을 이용하여 전자 서명문을 생성하는 단계; 및

[0072] 상기 전자서명문을 전자서명 전자 서명 이용 서버에 전송하는 단계;를 포함하는 전자 서명 획득 방법이 개시될 수 있다.

[0073] 상기 전자 서명 획득 방법은,

[0074] 사용자의 로컬 인증을 수행하는 단계;

[0075] 상기 로컬 인증이 완료되면,

[0076] 상기 기기 인증용 키 쌍에 포함된 기기 인증용 개인키를 이용하여, 상기 사용자 단말의 기기 인증을 위한 정보로부터 상기 기기 인증 데이터를 생성하는 단계;를 더 포함할 수 있다.

[0077] 상기 전자 서명 획득 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체가 제공된다.

발명의 효과

[0078] 실시예들에 따르면, 전자 서명 생성을 위한 개인키를 전자 서명 서비스 서버에서 등록 및 관리함으로써 사용자가 개인키가 저장된 매체를 소지하지 않아도 되는 효과가 발생한다. 또한, 개인키가 저장된 매체가 도용되는 것을 방지할 수 있다.

[0079] 또한, 전자 서명 서비스 서버(100)에 저장된 개인키를 전자 서명 생성 모듈 외에 다른 장치가 확인 및 복제하는

것을 차단함으로써, 사용자의 개인키에 대한 보안이 향상될 수 있다.

도면의 간단한 설명

[0080] 도 1은 예시적인 실시예에 따른 전자 서명 서비스 시스템(1000)을 나타낸 도면이다.

도 2는 도 1에서 나타낸 전자 서명 서비스 서버(100)를 대략적으로 나타낸 블록도이다.

도 3은 도 2에서 나타낸 저장부(130)의 저장 공간을 개념적으로 나타낸 블록도 이다.

도 4는 도 1에서 나타낸 사용자 사용자 단말(200)을 대략적으로 나타낸 블록도이다.

도 5는 도 1에서 나타낸 전자 서명 서비스 시스템에 의해 전자 서명 서비스가 제공되는 방법의 예시를 나타낸 흐름도이다.

도 6은 도 1에서 나타낸 전자 서명 서비스 시스템에 의해 전자 서명 서비스가 제공되는 방법의 다른 예시를 나타낸 흐름도이다.

도 7은 전자 서명 서비스 서버가 사용자 단말의 사용자를 인증하는 과정을 예시적으로 나타낸 흐름도이다.

도 8은 도 6에서 나타낸 전자 서명 서비스 방법에서 보안 통신 세션을 생성하는 단계가 추가된 예를 나타낸 흐름도이다.

도 9는 도 8에서 나타낸 보안 통신 세션 생성 단계가 수행되는 과정을 예시적으로 나타낸 흐름도이다.

도 10은 상기 보안 통신 세션을 이용하여 전자 서명 서비스 서버와 사용자 단말이 데이터를 송수신 하는 것을 나타낸 흐름도이다.

도 11a 및 도 11b는 도 1에서 나타낸 전자 서명 서비스 시스템에 의해 전자 서명 서비스가 제공되는 방법의 예시를 나타낸 흐름도이다.

도 12는 사용자 단말에 저장된 개인키 및 인증서 데이터를 전자 서명 서비스 서버에 이동시키는 과정을 예시적으로 나타낸 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0081] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 설명되는 실시 예들을 참조하면 명확해질 것이다. 그러나 본 발명은 아래에서 제시되는 실시 예들로 한정되는 것이 아니라, 서로 다른 다양한 형태로 구현될 수 있고, 본 발명의 사상 및 기술 범위에 포함되는 모든 변환, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 아래에 제시되는 실시 예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0082] 본 출원에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다. 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0083] 명세서 전체에서 전자 서명이란 전자 문서에 첨부되는 디지털 정보로서, 전자 서명을 생성한 사용자의 신원을 확인하고 사용자의 상기 전자 문서에 대한 승인을 나타낼 목적으로 사용되는 것을 의미한다.

[0084] 서명 대상 문서는 사용자의 전자 서명이 요구되는 전자 문서를 의미한다. 사용자는 상기 서명 대상 문서에 대해 전자 서명을 생성함으로써, 상기 서명 대상 문서에 대해 상기 사용자가 승인하였음을 인증할 수 있다. 서명 대상 문서는 전자 서명을 이용하는 이용 기관의 서버에 의해 작성될 수 있다. 상기 전자 서명 이용기관은 은행, 공공기관, 전자 상거래 서비스 운영기관, 주식 거래 기관 등일 수 있으며, 이에 제한되는 것은 아니다. 다른 예로, 서명 대상 문서는 서명의 권한이 있는 사용자 단말에 의해서도 작성될 수도 있다. 서명 대상 문서는 전자

문서로서, 온라인 증명서, 전자상거래 문서, 인터넷 주식 거래 문서 등을 포함할 수 있으며, 이에 제한되는 것은 아니다.

[0085] 서명 대상 데이터는 상기 서명 대상 문서로부터 도출된 데이터를 의미한다.

[0086] 예시적으로, 서명 대상 데이터는 소정의 알고리즘으로 서명 대상 문서의 원문 데이터를 가공한 데이터일 수 있다.

[0087] 예를 들어, 서명 대상 데이터는 서명 대상 문서의 원문 데이터를 해쉬 함수(Hash function)를 이용하여 가공한 데이터일 수 있다. 다른 예로, 서명 대상 데이터는 서명 대상 문서의 원문 데이터를 해쉬 함수 및 패딩(Padding) 알고리즘을 이용하여 가공한 데이터일 수 있다. 패딩이란 데이터의 크기가 목표하는 고정 길이보다 작은 경우 데이터 끝에 공백이나 의미가 없는 기호를 부가하여 데이터 크기를 조정하는 알고리즘을 의미한다.

[0088] 전술한 데이터 가공 알고리즘 들은 예시적인 것에 불과하며, 실시예가 이에 제한되는 것은 아니다. 또한, 서명 대상 데이터는 서명 대상 문서의 원문 데이터와 같을 수도 있다.

[0089] 인증서란 전자 서명이 사용자에 의해 생성되었음을 인증하기 위한 전자적 문서를 의미한다. 인증서는 전자 서명을 진행한 사용자 정보, 인증서의 용도, 인증서 유효기간, 인증서 만료일 및 인증서 발급기관에 대한 정보 중 적어도 하나를 포함할 수 있다.

[0090] 그리고, 인증서 데이터는 인증서로부터 도출된 데이터를 의미한다. 인증서 데이터는 인증서의 정보를 그대로 나타내는 데이터일 수 있다. 다른 예로, 인증서 데이터는 전자 서명 이용기관에 제출하기 위해 인증서를 적절한 포멧으로 변경한 데이터일 수도 있다.

[0091] 전자 서명문은 전자 서명을 이용하는 이용 기관에 제출되는 전자 문서를 의미한다. 전자 서명문에는 상기 전자 서명, 서명 대상 데이터, 인증서 데이터 및 전자 서명을 복호화 하기 위한 공개 키 데이터 등이 첨부되어 있을 수 있다. 전자 서명 이용 기관은 전자 서명문에 첨부된 공개 키 데이터로 상기 전자 서명을 검증함으로써, 전자 서명이 사용자에 의해 작성된 것인 지를 확인할 수 있다.

[0092] 이하, 본 발명에 따른 실시 예들을 첨부된 도면을 참조하여 상세히 설명하기로 하며, 첨부 도면을 참조하여 설명함에 있어, 동일하거나 대응하는 구성 요소는 동일한 도면번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

[0093] 도 1은 예시적인 실시예에 따른 전자 서명 서비스 시스템(1000)을 나타낸 도면이다.

[0094] 도 1을 참조하면, 실시예에 따른 전자 서명 서비스 시스템(1000)은 사용자 단말(200)과, 사용자의 전자 서명 생성을 위한 데이터를 저장하고 사용자에게 전자 서명 서비스를 제공하는 전자 서명 서비스 서버(100), 전자 서명을 이용하는 전자 서명 이용 서버(300) 및 전자 서명을 인증하는 인증 서버(400)를 포함할 수 있다.

[0095] 전자 서명 이용 서버(300)는 전자 서명을 이용하는 기관에 의해 운영되는 서버를 의미한다. 전자 서명 이용 서버(300)는 은행 서버, 공공 기관에 의해 운영되는 서버, 전자 상거래 서비스를 제공하는 서버 등을 포함할 수 있으며, 이에 제한되는 것은 아니다. 전자 서명 이용 서버(300)는 사용자의 인증이 필요한 전자 문서, 즉 서명 대상 문서를 발행할 수 있다. 전자 서명 이용 서버(300)는 상기 서명 대상 문서로부터 도출된 서명 대상 데이터를 사용자 단말(200)에 전송할 수 있다. 상기 서명 대상 데이터는 서명 대상 문서의 원문 데이터를 그대로 포함할 수도 있고, 서명 대상 문서의 원문 데이터를 후술하는 암호화에 적절하도록 가공한 데이터를 포함할 수도 있다. 전자 서명 이용 서버(300)는 상기 서명 대상 데이터에 대한 전자 서명을 사용자 단말(200)에게 요청할 수 있다.

[0096] 인증 서버(400)는 전자 서명의 검증을 위한 인증서를 발행하고 관리하는 공인 인증 기관에 의해 운영되는 서버를 의미한다. 상기 공인 인증 기관의 예로는 금융결제원, 한국정보인증, 한국증권전산, 한국전자인증, 한국전산원,한국무역정보통신 등이 있다.

[0097] 사용자 단말(200)은 전자 서명의 권한을 가진 사용자가 사용하는 장치를 의미한다. 사용자 단말은 스마트 폰, 태블릿 PC, 랩톱 등을 포함할 수 있으나 이에 제한되는 것은 아니다. 사용자 단말(200)은 전자 서명 이용 서버(300) 및 전자 서명 서비스 서버(100)와 통신할 수 있는 통신 수단을 포함할 수 있다. 사용자 단말(200)은 전자 서명 이용 서버(300)로부터 서명 대상 데이터 및 서명 대상 데이터에 대한 전자 서명의 요청을 수신할 수 있다.

[0098] 사용자 단말(200)은 전자 서명을 직접 생성하지 않고, 전자 서명 서비스 서버(100)에게 전자 서명을 생성해 줄 것을 요청할 수 있다. 필요한 경우, 사용자 단말(200)은 상기 서명 대상 데이터를 전자 서명이 용이한 포멧으로

가공한 후, 가공된 서명 대상 데이터에 대한 전자 서명의 요청을 전자 서명 서비스 서버(100)에게 전송할 수 있다.

[0099] 사용자 단말(200)은 전자 서명 서비스 서버(100)로부터 전자 서명을 수신하면, 전자 서명을 이용하여 전자 서명문을 생성할 수 있다. 전자 서명문은 전자 서명 이용 서버(300) 또는 인증 서버(400)에서 검증이 가능한 포멧으로 작성될 수 있다. 사용자 단말(200)은 생성한 전자 서명문을 전자 서명 이용 서버(300)에 전송할 수 있다.

[0100] 전자 서명 서비스 서버(100)에는 사용자의 전자 서명 생성을 위한 정보가 등록되어 있을 수 있다. 예를 들어, 전자 서명 서비스 서버(100)에는 전자 서명 생성을 위한 키 쌍 가운데 개인키가 등록되어 있을 수 있다. 전자 서명 서비스 서버(100)는 미리 등록된 사용자의 개인키를 이용하여 전자 서명을 생성할 수 있다. 전자 서명 서비스 서버(100)는 생성한 사용자의 전자 서명을 사용자 단말(200)에 전송할 수 있다.

[0101] 도 2는 도 1에서 나타낸 전자 서명 서비스 서버(100)를 대략적으로 나타낸 블록도이다.

[0102] 도 2를 참조하면, 실시예에 따른 전자 서명 서비스 서버(100)는 사용자 단말(200)과 통신하는 통신부(110)와, 사용자의 전자서명 생성을 위한 개인키를 저장하는 저장부(130) 및 통신부(110)가 사용자 단말(200)로부터 서명 대상 데이터 및 상기 서명 대상 데이터에 대한 전자 서명의 요청을 수신하면, 상기 개인키를 이용하여 상기 서명 대상 데이터에 대한 전자 서명을 생성하는 전자 서명 생성 모듈(140)을 포함할 수 있다. 또한, 전자 서명 서비스 서버(100)는 통신부(110)가 사용자 단말(200)로부터 수신한 기기 인증 데이터를 검증하는 프로세서(120)를 더 포함할 수 있다. 프로세서(120)는 통신부(110)가 송수신 하는 데이터를 암호화 및 복호화 하는 연산 작업을 수행할 수도 있다.

[0103] 통신부(110)는 사용자 단말(200)과 정보 및 데이터를 주고 받을 수 있다. 통신부(110)는 데이터의 전송 및 수신의 역할을 수행하는 하드웨어 자원을 포함할 수 있다.

[0104] 통신부(110)는 소정의 통신망을 통해 사용자 단말(200)과 연결될 수 있다. 상기 소정의 통신망은, 전자 서명 서비스 서버(100)의 통신부(110)와 사용자 단말(200)을 연결하는 역할을 수행하는 매개체로써, 사용자 단말(200)이 전자 서명 서비스 서버(100)에 접속한 후 데이터를 송수신할 수 있도록 접속 경로를 제공하는 경로 등을 포함할 수 있다. 상기 통신망은 유선 네트워크 또는 무선 네트워크일 수 있다. 유선 네트워크는 LANs(Local Area Networks), WANs(Wide Area Networks), MANs(Metropolitan Area Networks), ISDNs(Integrated Service Digital Networks)등을 포함할 수 있고, 무선 네트워크는 무선 LANs, CDMA, 블루투스, 위성 통신 등을 포함할 수 있으나 실시예가 이에 제한되는 것은 아니다.

[0105] 저장부(130)에는 사용자의 전자 서명 생성을 위해 전자 서명 서비스 서버(100)에 등록된 정보가 저장되어 있을 수 있다. 예를 들어, 저장부(130)에는 사용자의 전자 서명 생성을 위한 개인키가 저장되어 있을 수 있다. 또한, 저장부(130)에는 사용자의 인증서 데이터가 함께 저장되어 있을 수 있다.

[0106] 저장부(130)는 전자 서명 생성 모듈(140)을 제외한 다른 장치가 사용자의 개인키를 복제 및 확인할 수 없도록 할 수 있다. 반면, 저장부(130)에 저장된 인증서 데이터는 사용자 단말(200)의 요청에 의해 통신부(110)를 통해 사용자 단말(200)로 전송될 수 있다. 따라서, 저장부(130)는 인증서 데이터와 개인키를 서로 다른 저장 공간에 저장할 수 있다.

[0107] 도 3은 도 2에서 나타낸 저장부(130)의 저장 공간을 개념적으로 나타낸 블록도 이다.

[0108] 도 3을 참조하면, 저장부(130)는 제1 저장 공간(132)과 제2 저장 공간(134)을 포함할 수 있다. 제1 저장 공간(132)과 제2 저장 공간(134)은 하드웨어 적으로 분리되어 있을 수도 있고, 분리되지 않을 수도 있다. 예시적으로 제1 저장 공간(132)에는 사용자의 개인키가 저장되어 있을 수 있다. 또한, 제2 저장 공간(134)에는 인증서 데이터, 사용자 식별 정보 등이 포함되어 있을 수 있다. 프로세서(120)는 제2 저장 공간(134)에 저장된 데이터 및 정보 중 적어도 일부를 이용할 수 있다. 또한, 제2 저장 공간(134)에 저장된 인증서 데이터 등은 통신부(110)를 통해 외부로 전송될 수 있다.

[0109] 제1 저장 공간(132)에 저장된 정보는 전자 서명 서비스 서버(100)의 외부에서 확인 및 복제가 불가능 하도록 구성될 수 있다. 제1 저장 공간(132)에 저장된 개인키는 전자 서명 생성 모듈(140)만이 확인 및 이용할 수 있도록 구성될 수 있다. 예를 들어, 제1 저장 공간(132)과 전자 서명 생성 모듈 (140)은 함께 하드웨어 보안 모듈(Hardware Security Module; HSM)(150)을 구성할 수 있다. 제1 저장 공간(132)과 전자 서명 생성 모듈(140)이 하드웨어 보안 모듈 (150)을 구성함으로써, 제1 저장 공간(132)에 저장된 개인키는 공개되지 않고 안전하게 관리될 수 있다.

[0110] 전자 서명 생성 모듈(140)은 저장부(130)의 제1 저장 공간(132)에 저장된 개인키를 이용하여 통신부(110)가 수신한 서명 대상 데이터를 암호화할 수 있다. 전자 서명 생성 모듈(140)은 상기 암호화에 필요한 연산 과정을 수행할 수 있다. 전자 서명 생성 모듈(140)은 서명 대상 데이터를 암호화 함으로써 전자 서명을 생성할 수 있다. 전자 서명 생성 모듈(140)이 생성한 전자 서명을 통신부(110)에 전달하면, 통신부(110)는 상기 전자 서명을 사용자 단말(200)에게 전송할 수 있다.

[0111] 다시 도 2를 참조하면, 프로세서(120)는 사용자 단말(200)로부터 획득한 기기 인증 데이터를 검증할 수 있다. 상기 기기 인증 데이터는 상기 사용자 단말(200)의 기기 인증을 위한 정보로부터 생성된 데이터일 수 있다. 또한, 상기 기기 인증을 위한 정보는 사용자 단말(200)의 기기에 부여된 고유 식별번호, 기기 정보, 사용자가 전자 서명 서비스에 가입할 때 사용자 단말(200)에 부여된 ID 등을 포함할 수 있다. 그리고, 기기 인증 데이터는 상기 기기 인증을 위한 정보의 전부 또는 일부를 변조함으로써 획득된 데이터일 수 있다.

[0112] 프로세서(120)는 사용자 단말(200)로부터 획득한 기기 인증 데이터를 검증함으로써 사용자가 전자 서명을 획득할 권한이 있는 지를 판단할 수 있다. 프로세서(120)는 저장부(130)의 제2 저장 공간(134)에 저장된 정보를 이용하여 상기 사용자 단말(200)로부터 획득한 기기 인증 데이터를 검증할 수 있다. 프로세서(120)는 통신부(110)가 사용자 단말(200)로부터 획득한 기기 인증 데이터로부터 사용자가 전자 서명을 생성할 권한이 있는 지를 판단할 수 있다.

[0113] 프로세서(120)는 기기 인증 데이터에 대한 검증을 완료하면, 전자 서명 생성 모듈(140)에게 사용자가 사용할 권한이 있는 개인키를 이용하여 서명 대상 데이터에 대한 전자서명 생성을 요청할 수 있다. 프로세서(120)는 사용자 인증 절차에 필요한 연산과정을 수행할 수 있는 하드웨어 자원을 포함할 수 있다.

[0114] 도 4는 도 1에서 나타낸 사용자 사용자 단말(200)을 대략적으로 나타낸 블록도이다.

[0115] 도 4를 참조하면, 예시적인 실시예에 따른 사용자 단말(200)은 통신부(210)와, 사용자의 입력 정보를 획득하는 입력부(230), 및 프로세서(240)를 포함할 수 있다.

[0116] 통신부(210)는 전자 서명 서비스 서버(100), 전자 서명 이용 서버(300) 및 인증 서버(400)와 데이터 및 정보를 송수신할 수 있다. 통신부(210)는 전자 서명 서비스 서버(100)에게 전자 서명의 요청을 전송할 수 있다. 통신부(210)는 전자 서명 서비스 서버(100)로부터 전자 서명을 수신하고, 상기 전자 서명을 이용하여 생성된 전자 서명문을 전자 서명 이용 서버(300)에 전송할 수 있다.

[0117] 입력부(230)는 사용자의 입력정보를 획득할 수 있다. 프로세서(240)는 입력부(230)가 획득한 사용자 입력 정보에 기초하여 통신부(210)가 전송하는 데이터를 생성할 수 있다. 입력부(230)의 입력 방식은 버튼 입력방식 또는 터치 스크린 방식일 수 있다. 버튼 입력방식의 경우, 입력부(230)는 소정의 버튼 입력장치를 포함할 수 있다. 터치 스크린 방식의 경우, 입력부(230)는 터치 스크린 기능을 지원하는 디스플레이를 포함할 수 있다. 프로세서(240)는 입력부(230)에게 UI(User Interface) 정보를 제공할 수 있다. 상술한 예는 예시적인 것에 불과하며 실시예가 이에 제한되는 것은 아니다. 예를 들어, 입력부(230)는 음성 인식이나 기타 다른 방법으로 사용자의 입력을 입력 받을 수 도 있다.

[0118] 프로세서(240)는 전자 서명 서비스 서버(100)에 의해 배포된 소정의 애플리케이션을 탑재하고 있을 수 있다. 프로세서(240)는 입력부(230)에 대한 UI 정보를 제공하고, 통신부(210)가 전송하는 데이터를 생성할 수 있다. 프로세서(240)는 전자 서명문 생성에 필요한 연산 기능을 수행할 수 있다. 또한, 프로세서(240)는 전자 서명 서비스 서버(100)와의 통신 보안을 위해 필요한 연산 기능을 수행할 수 있다.

[0119] 실시예에 따른 사용자 단말(200)은 로컬 인증부(220)를 더 포함할 수 있다. 도 4에서는 로컬 인증부(220)는 프로세서(240)를 별도 구성으로 나타냈지만 이 것이 양 구성이 하드웨어 적으로 분리되어 있다는 것을 의미하는 것은 아니다. 예를 들어, 로컬 인증부(220)와 프로세서(240)는 적어도 일부의 하드웨어 자원을 공유하거나 공유하지 않을 수도 있다.

[0120] 로컬 인증부(220)는 사용자의 로컬 인증 프로세스를 수행할 수 있다. 로컬 인증부(220)는 입력부(230)에서 획득한 사용자 입력 정보에 기초하여 로컬 인증을 수행할 수 있다. 여기서, 로컬 인증이란 사용자 단말(200)이 외부와 데이터를 주고 받지 않으면서 수행되는 사용자 인증 절차를 의미한다. 로컬 인증 방식에 대해서는 후술하는 설명 부분에서 보다 상세히 설명한다.

[0121] 도 5는 도 1에서 나타낸 전자 서명 서비스 시스템(1000)에 의해 전자 서명 서비스가 제공되는 방법의 예시를 나타낸 흐름도이다.

[0122] 도 5를 참조하면, 전자 서명 서비스 서버는 미리 등록된 사용자의 개인키를 이용하여 서명 대상 데이터에 대한 전자 서명을 생성할 수 있다.

[0123] 1105 단계에서, 전자 서명 서비스 서버(100)는 사용자의 전자 서명을 생성하기 위한 개인키를 저장부(130)에 등록할 수 있다. 전자 서명 서비스 서버(100)는 사용자 단말(200)의 요청에 의해 키 쌍을 생성한 후 상기 키 쌍에 포함된 개인키를 저장부(130)에 저장할 수 있다. 예를 들어, 전자 서명 서비스 서버(100)는 상기 키 쌍에 포함된 개인키는 도 3에서 나타낸 제1 저장 공간(132)에 저장하고, 공개키는 제2 저장 공간(134)에 저장할 수 있다.

[0124] 다른 예로, 전자 서명 서비스 서버(100)는 사용자 단말(200)로부터 기 생성된 개인키를 전달 받을 수도 있다. 이 경우, 전자 서명 서비스 서버(100)가 사용자 단말(200)로부터 수신하는 개인키는 암호화 되어 있을 수 있다. 사용자의 개인키를 등록하는 1105 단계에 대해서는 후술하는 설명 부분에서 보다 상세히 설명한다.

[0125] 1110 단계에서 사용자 단말(200)은 전자 서명 이용 서버(300)로부터 전자 서명의 요청을 수신할 수 있다. 상기 전자 서명의 요청은 전자 서명 이용 서버(300)에서 확인하고자 하는 서명 대상 데이터에 대해 전자 서명을 생성해줄 것을 요청하는 것을 의미한다. 서명 대상 데이터는 전자 서명 이용 서버(300)에서 생성될 수 있다. 이 경우, 전자 서명 이용 서버(300)는 전자 서명 요청과 함께 서명 대상 데이터를 함께 사용자 단말(200)에 전송할 수 있다.

[0126] 예를 들어, 전자 서명 이용 서버(300)는 온라인 증명서, 전자상거래 문서, 인터넷 주식 거래 문서 등을 서명 대상 문서로 생성할 수 있다. 그리고, 전자 서명 이용 서버(300)는 상기 서명 대상 문서로부터 도출된 서명 대상 데이터를 사용자 단말(200)에게 전송할 수 있다. 전자 서명 이용 서버(300)가 전송하는 서명 대상 데이터는 서명 대상 문서의 원본 데이터 그대로이거나 서명 대상 문서의 원본 데이터를 가공한 것일 수도 있다.

[0127] 다른 예로, 서명 대상 데이터는 사용자 단말(200)에서 생성될 수도 있다. 즉, 사용자 단말(200)이 전자 서명의 대상이 되는 서명 대상 문서를 직접 생성할 수도 있다. 이 경우, 전자 서명 이용 서버(300)는 사용자 단말(200)에게 사용자 단말(200)이 생성한 서명 대상 데이터 및 전자 서명을 전자 서명 이용 서버(300)에게 전송해 줄 것을 요청할 수 있다.

[0128] 1120 단계에서, 사용자 단말(200)은 서명 대상 데이터를 가공할 수 있다. 예를 들어, 사용자 단말(200)은 해쉬(hash) 함수를 이용하여 서명 대상 데이터를 인코딩(encoding) 함으로써 서명 대상 데이터를 가공할 수 있다. 해쉬 함수 값의 데이터는 일정한 크기를 가지므로, 상기 해쉬 함수를 이용한 인코딩 과정을 통해 서명 대상 데이터의 크기가 변경될 수 있다. 사용자 단말(200)은 서명 대상 데이터를 가공하여 서명 대상 데이터의 크기를 변경함으로써 후술하는 전자 서명 생성이 용이하도록 할 수 있다.

[0129] 사용자 단말(200)은 서명 대상 데이터를 가공하는 과정에서 패딩 과정을 더 수행할 수 있다. 사용자 단말(200)은 패딩을 통해 서명 대상 데이터의 크기를 조절할 수 있다. 상기 패딩 절차는 해쉬 함수를 이용한 인코딩에 의해 가공된 데이터의 크기가 후술하는 전자 서명 생성을 위해 요구되는 데이터의 크기보다 작을 경우 수행될 수 있다. 사용자 단말(200)은 가공된 서명 대상 데이터를 전자 서명 서비스 서버(100)에 전송할 수 있다.

[0130] 도 5에서는 서명 대상 데이터를 가공하는 1120 단계가 사용자 단말(200)에서 수행되는 것을 예시적으로 나타냈지만, 실시예가 이에 제한되는 것은 아니다. 다른 실시예에 따르면, 1120 단계는 전자 서명 서비스 서버(100) 또는 전자 서명 이용 서버(300)에서 수행될 수도 있다.

[0131] 전자 서명 이용 서버(300)가 서명 대상 문서를 생성하는 경우, 전자 서명 이용 서버(300)에서 서명 대상 문서의 데이터에 대해 전술한 인코딩 및 패딩 절차를 수행할 수도 있다. 다른 예로, 전자 서명 서비스 서버(100)가 사용자 단말(200)로부터 서명 대상 데이터의 크기가 전자 서명 생성에 적절한 크기가 아닌 경우, 전자 서명 서비스 서버(100)가 서명 대상 데이터를 가공한 후, 가공된 데이터에 대해 전자 서명을 생성할 수도 있다.

[0132] 1124 단계에서, 사용자 단말(200)은 서명 대상 데이터 및 전자 서명 요청을 전자 서명 서비스 서버(100)에게 전송할 수 있다. 상기 전자 서명 요청은 사용자의 개인키를 이용하여 서명 대상 데이터에 대한 전자 서명을 생성해줄 것을 요청하는 것을 의미한다. 1124 단계에서 전송되는 서명 대상 데이터는 서명 대상 문서의 원본 데이터이거나 서명 대상 문서의 원본 데이터를 상기 인코딩 및 패딩을 통해 가공한 데이터일 수 있다.

[0133] 1126 단계에서, 전자 서명 서비스 서버(100)는 서명 대상 데이터 및 사용자의 개인키를 이용하여 전자 서명을 생성할 수 있다. 통신부(110)는 사용자 단말(200)로부터 수신한 서명 대상 데이터를 전자 서명 생성 모듈(140)에 전달할 수 있다. 전자 서명 생성 모듈(140)는 제1 저장 공간(132)에 저장된 개인키를 이용하여 서명 대상 데이터를 암호화 할 수 있다. 전자 서명 생성 모듈(140)는 RSA, Rabin 및 ECDSA(Elliptic Curve DSA) 알고리즘

중 적어도 하나를 이용하여 서명 대상 데이터를 암호화 할 수 있다. 상술한 알고리즘들은 예시적인 것에 불과하며 실시예가 이에 제한되는 것은 아니다.

[0134] 전자 서명 생성 모듈(140)은 서명 대상 데이터를 개인키를 이용하여 전자 서명을 생성할 수 있다. 전자 서명 생성 모듈 (140)에서 생성된 전자 서명은 통신부(110)로 전달될 수 있다. 하지만, 저장부(130)의 제1 저장 공간(132)에 등록된 개인키는 도 3의 하드웨어 보안 모듈(150) 외부로 전송되지 않을 수 있다. 따라서, 전자 서명 서비스 서버(100)가 전자 서명 서비스를 제공하는 동안, 사용자의 개인키는 외부에 공개되지 않을 수 있다.

[0135] 1128 단계에서, 통신부(110)는 전자 서명 생성 모듈 (140)에서 생성된 전자 서명 및 제2 저장 공간(134)에 저장된 사용자의 인증서 데이터를 사용자 단말(200)에게 전송할 수 있다. 인증서 데이터는 전자 서명을 진행한 사용자 정보, 인증서 용도, 인증서 유효기간, 인증서 만료일, 인증서 발급기관 등에 관한 정보를 포함할 수 있다. 또한, 인증서 데이터는 상기 전자 서명을 검증 하기 위한 공개키를 포함할 수 있다. 또한, 인증서 데이터에는 인증서 데이터의 위조, 변조 여부를 판단하기 위해 제공되는 추가 서명이 첨부되어 있을 수 있다. 상기 추가 서명은 인증 서버(400)에서만 검증이 가능하도록 구성되어 있을 수 있다.

[0136] 1130 단계에서, 사용자 단말(200)의 프로세서(240)는 전자 서명 서비스 서버(100)로부터 수신한 전자 서명 및 인증서 데이터를 이용하여 전자 서명문을 생성할 수 있다. 전자 서명문에는 서명 대상 데이터, 서명 대상 데이터에 대한 전자 서명 및 상기 전자 서명을 인증하는 인증서 데이터가 첨부될 수 있다. 사용자 단말(200)은 소정의 프로토콜(Protocol)을 이용하여 전자 서명문을 생성할 수 있다.

[0137] 1132 단계에서, 사용자 단말(200)의 통신부(210)는 프로세서(240)에서 생성된 전자 서명문을 전자 서명 이용 서버(300)에 전송할 수 있다.

[0138] 1134 단계에서 전자 서명 이용 서버(300)는 전자 서명문에 첨부된 인증서 데이터를 검증해줄 것을 인증 서버(400)에게 요청할 수 있다.

[0139] 1136 단계에서, 인증 서버(400)는 인증서 데이터를 검증할 수 있다. 인증 서버(400)는 인증서 데이터에 첨부된 추가 서명을 검증 해봄으로써 인증서 데이터의 위조, 변조 여부를 검증할 수 있다.

[0140] 1138 단계에서, 인증 서버(400)는 인증서 데이터에 대한 검증 결과를 전자 서명 이용 서버(300)에 전송할 수 있다.

[0141] 1140 단계에서, 인증서 데이터의 검증이 완료된 경우, 전자 서명 이용 서버(300)는 사용자 단말(200)로부터 수신한 전자 서명문을 검증할 수 있다. 전자 서명 이용 서버(300)는 전자 서명문에 첨부된 공개키를 이용하여 전자 서명문에 첨부된 전자 서명을 검증 할 수 있다. 전자 서명 이용 서버(300)는 전자 서명을 복호화 한 결과 데이터와 전자 서명문에 첨부된 서명 대상 데이터를 비교함으로써 전자 서명문을 검증할 수 있다.

[0142] 도 5에서 나타낸 실시예에 따르면, 전자 서명 서비스 서버(100)가 사용자의 개인키를 등록하고 관리하기 때문에 사용자 단말(200)에서 상기 개인키를 관리하지 않아도 된다. 따라서, 사용자가 개인키가 저장된 매체를 직접 소지하지 않아도 되는 효과가 발생한다. 또한, 사용자가 전자 서명을 위한 개인키를 여러 매체에 이동 또는 복사해야 하는 번거로움이 사라지는 효과가 발생한다.

[0143] 실시예에 따르면, 개인키가 전자 서명 서비스 서버(100)에 저장되므로, 사용자가 개인키가 저장된 매체를 잃어버림에 따라 사용자의 전자 서명이 도용 당하는 것을 방지하는 효과가 발생할 수 있다. 그리고, 전자 서명 서비스 서버(100)의 제1 저장 공간(132)과 전자 서명 생성 모듈(140)로 하드웨어 보안 모듈(150)을 구성함으로써, 사용자의 개인키를 타인이 복제 또는 확인하는 것을 방지할 수 있다.

[0144] 실시예에 따르면, 전자 서명 서비스 시스템(1000)에 의해 전자 서명 서비스가 수행되는 방법은 전자 서명 서비스 서버(100)가 사용자 단말(200)의 사용자를 인증하는 과정을 더 포함할 수 있다.

[0145] 도 6은 도 1에서 나타낸 전자 서명 서비스 시스템(1000)에 의해 전자 서명 서비스가 제공되는 방법의 다른 예시를 나타낸 흐름도이다.

[0146] 도 6의 실시예를 설명함에 있어서, 도 5와 중복되는 내용은 생략하기로 한다. 도 6을 참조하면, 전자 서명 서비스 서버(100)가 사용자 단말(200)의 사용자를 인증할 수 있다. 전자 서명 서비스 서버(100)의 프로세서(120)는 사용자 단말(200)로부터 획득한 기기 인증 데이터를 검증하는 과정을 수행할 수 있다. 프로세서(120)는 기기 인증 데이터의 검증이 완료되면, 전자 서명 생성 모듈(140)에게 사용자가 이용 권한이 있는 개인키를 이용하여 전자 서명을 생성할 것을 요청할 수 있다.

[0147] 1210 단계에서, 전자 서명 서비스 서버(100)는 사용자 단말(200)로부터 기기 인증 데이터를 획득할 수 있다. 기기 인증 데이터는 상술한 기기 인증을 위한 정보로부터 도출될 수 있다. 사용자 단말(200)이 기기 인증 데이터를 생성하는 과정에 대해서는 후술하는 설명에서 보다 상세히 기술한다.

[0148] 1212 단계에서, 전자 서명 서비스 서버(100)의 통신부(110)는 사용자 단말(200)로부터 기기 인증 데이터를 수신할 수 있다. 프로세서(120)는 통신부(110)가 수신한 기기 인증 데이터를 검증할 할 수 있다. 프로세서(120)는 사용자가 저장부(130)에 저장된 개인키를 사용할 수 있는 권한이 있는 지 여부를 판단할 수 있다. 또한, 저장부(130)에 복수 개의 개인키가 저장된 경우, 프로세서(120)는 사용자가 사용할 수 있는 개인키가 어느 것인지를 결정할 수 있다. 전자 서명 서비스 서버(100)가 기기 인증 데이터를 검증하는 과정에 대해서는 후술하는 설명에서 보다 상세히 기술한다.

[0149] 1214 단계에서, 전자 서명 서비스 서버(100)는 기기 인증 데이터를 검증한 결과를 사용자 단말(200)에게 전송할 수 있다. 프로세서(120)에서 기기 인증 데이터에 대한 검증이 실패한 경우, 통신부(110)는 사용자 인증이 실패하였다는 메시지를 사용자 단말(200)에게 전송할 수 있다. 프로세서(120)에서 기기 인증 데이터에 대한 검증을 완료한 경우, 통신부(110)는 사용자 인증이 완료되었다는 메시지를 사용자 단말(200)에 전송할 수 있다.

[0150] 기기 인증 데이터에 대한 검증이 완료되면, 통신부(110)는 사용자가 사용할 수 있는 인증서 목록 정보를 사용자 단말(200)에 전송할 수 있다. 만약, 사용자가 사용할 수 있는 인증서의 개수가 복수 개인 경우, 사용자 단말(200)은 사용자로부터 인증서의 선택 정보를 입력 받을 수 있다. 그리고, 사용자 단말(200)은 전자 서명 서비스 서버(100)에게 인증서의 선택 정보를 전송할 수 있다.

[0151] 이하에서는 기기 인증 데이터로부터 사용자를 인증하는 절차를 예시적으로 설명한다.

[0152] 도 7은 전자 서명 서비스 서버(100)가 사용자 단말(200)의 사용자를 인증하는 과정을 예시적으로 나타낸 흐름도이다.

[0153] 도 7을 참조하면, 사용자 단말(200)은 로컬 인증 절차를 수행할 수 있다. 사용자 단말(200)은 로컬 인증 절차가 완료되면, 기기 인증을 위한 정보로부터 기기 인증 데이터를 생성하고, 상기 기기 인증 데이터를 전자 서명 서비스 서버(100)에게 전송할 수 있다. 전자 서명 서비스 서버(100)는 기기 인증 데이터를 검증함으로써 사용자를 인증할 수 있다.

[0154] 상기 기기 인증을 위한 정보는 사용자 단말(200)의 기기에 부여된 고유 식별번호, 기기 정보, 사용자가 전자 서명 서비스에 가입할 때 사용자 단말(200)에 부여된 ID 등을 포함할 수 있다. 그리고, 기기 인증 데이터는 상기 기기 인증을 위한 정보의 전부 또는 일부를 변조함으로써 획득된 데이터일 수 있다.

[0155] 1510 단계에서, 사용자 단말(200)은 로컬 인증 절차를 수행할 수 있다. 로컬 인증은 사용자 단말(200) 내부에서 진행되는 것으로 사용자 단말(200)은 자체적으로 사용자가 입력하는 사용자 인증 정보를 검증할 수 있다. 사용자 단말(200)의 입력부(230)는 사용자로부터 사용자 인증 정보를 입력 받을 수 있다. 입력부(230)는 사용자 ID, 사용자의 생체 정보, 패스워드 등을 상기 사용자 인증 정보로 입력 받을 수 있다. 입력부(230)가 사용자의 생체 정보를 입력 받는 경우, 입력부(230)는 사용자의 생체 신호를 감지하는 센서를 포함할 수 있다.

[0156] 로컬 인증부(220)는 입력부(230)가 입력 받은 사용자 인증 정보로부터 사용자를 인증할 수 있다. 로컬 인증부(220)는 로컬 인증 과정에서 상기 사용자 인증 정보가 외부로 유출되지 않도록 관리할 수 있다. 로컬 인증부(220)의 로컬 인증 과정은 후술하는 설명에서 상세히 기술한다.

[0157] 1530 단계에서, 프로세서(240)는 기기 인증용 키 쌍을 이용하여 기기 인증 데이터를 생성할 수 있다. 기기 인증용 키 쌍은 암호화를 위한 기기 인증용 개인키와 기기 인증용 개인키로 암호화 된 데이터를 복호화 하기 위한 기기 인증용 공개키를 포함할 수 있다. 기기 인증용 키 쌍은 기기 인증을 위한 정보로부터 기기 인증 데이터를 생성하는데 이용되는 것으로 전자 서명 생성을 위한 키 쌍과는 서로 다른 것일 수 있다. 기기 인증용 키 쌍은 사용자 단말(200)에 의해 생성된 것이거나 전자 서명 서비스 서버(100)가 사용자 단말(200)에게 제공한 것일 수 있다.

[0158] 프로세서(240)는 기기 인증용 키 쌍에 포함된 기기 인증용 개인키를 이용하여 기기 인증 데이터를 생성할 수 있다. 사용자 단말(200)은 상기 기기 인증용 개인키를 이용하여 기기 인증을 위한 정보의 전부 또는 일부를 암호화 함으로써 기기 인증 데이터를 생성할 수 있다. 프로세서(240)는 RSA, Rabin 및 ECDSA(Elliptic Curve DSA) 알고리즘 중 적어도 하나를 이용하여 기기 인증을 위한 정보의 적어도 일부를 암호화 할 수 있다. 상술한 알고리즘들은 예시적인 것에 불과하며 실시예가 이에 제한되는 것은 아니다.

[0159] 기기 인증용 키 쌍은 기기 인증 데이터를 생성할 때 마다 새롭게 갱신될 수 있다. 하지만, 실시예가 이에 제한되는 것은 아니다. 예를 들어, 기기 인증용 키 쌍은 소정의 횟수만큼 반복 사용된 후, 폐기될 수도 있다.

[0160] 1540 단계에서, 사용자 단말(200)의 통신부(210)는 기기 인증용 키 쌍에 포함된 기기 인증용 공개키 및 기기 인증 데이터를 전자 서명 서비스 서버(100)에 전송할 수 있다.

[0161] 1550 단계에서, 전자 서명 서비스 서버(100)의 통신부(110)는 사용자 단말(200)로부터 기기 인증용 공개키 및 기기 인증 데이터를 수신할 수 있다. 그리고, 전자 서명 서비스 서버(100)의 프로세서(120)는 상기 기기 인증용 공개키를 이용하여 기기 인증 데이터를 검증할 수 있다. 예시적으로, 프로세서(120)는 기기 인증용 공개키를 이용하여 기기 인증 데이터를 복호화 함으로써 기기 인증 데이터를 검증할 수 있다. 프로세서(120)는 기기 인증 데이터를 검증함으로써 사용자가 전자 서명의 생성 권한이 있는 지 여부를 판단할 수 있다.

[0162] 도 7에서 나타낸 바와 같이, 사용자 단말(200)에서 수행되는 로컬 인증 및 사용자 단말(200)과 전자 서명 서비스 서버(100) 사이에서 이루어지는 원격 인증이 병행하여 이루어 짐으로써, 사용자 인증에 대한 보안이 강화될 수 있다. 또한, 사용자 단말(200)이 기기 인증을 위한 정보를 기기 인증 데이터로 변조하여 전자 서명 서비스 서버(100)에 전송함으로써, 상기 기기 인증을 위한 정보가 외부 장치에 의해 탈취되는 것을 방지할 수 있다.

[0163] 1510 단계에서 나타낸 로컬 인증 과정은 다양한 방식으로 이루어질 수 있다. 예를 들어, 사용자 단말(200)의 로컬 인증부(220)는 캡챠를 생성할 수 있다. 캡챠는 컴퓨터가 구별하기 어려운 왜곡된 문자 또는 숫자 이미지를 포함할 수 있다. 또한, 캡챠는 문자 또는 숫자를 읽어주는 음성에 잡음을 섞은 음성 파일을 포함할 수도 있다. 그리고, 사용자 단말(200)은 상기 캡챠를 이용하여 사용자 인증이 기계가 아닌 사람에 의해 이루어지는 것임을 확인할 수 있다.

[0164] 또한, 사용자 단말(200)의 입력부는 사용자 인증을 위한 사용자의 입력 정보를 획득할 수 있다. 상기 사용자 입력 정보는 사용자가 입력하는 ID, 패스워드, PIN, 사용자의 생체 신호 등을 포함할 수 있다. 로컬 인증부(220)는 입력부가 입력 받은 상기 사용자 입력 정보를 검증함으로써 로컬 인증을 수행할 수 있다. 로컬 인증이 완료되면, 원격 인증 절차가 진행될 수 있다.

[0165] 다시 도 6을 참조하면, 1210, 1212 및 1214 단계에서 사용자 인증이 완료되고 나면, 사용자 단말(200)과 전자 서명 서비스 서버(100)는 전자 서명 서비스와 관련된 데이터 및 정보를 서로 송수신할 수 있다. 1224, 1228 단계 등에서 전자 서명 서비스 서버(100)와 사용자 단말(200) 사이에서 송수신 되는 데이터 및 정보는 전자 서명의 도용 방지 및 사용자의 프라이버시 보호를 위해 외부에 공개되는 것을 방지할 필요가 있다.

[0166] 도 8은 도 6에서 나타낸 전자 서명 서비스 방법에서 보안 통신 세션을 생성하는 단계(1220)가 추가된 예를 나타낸 흐름도이다. 도 8의 실시예를 설명 함에 있어서, 도 6과 중복되는 내용은 생략하기로 한다.

[0167] 도 8을 참조하면, 전자 서명 서비스 시스템(1000)의 전자 서명 서비스 방법은 보안 통신 세션을 생성하는 단계(1220)를 포함할 수 있다.

[0168] 1120 단계에서, 전자 서명 서비스 서버(100)의 프로세서(120)는 사용자 단말(200) 사이에 송수신 되는 데이터 및 정보를 암호화 하기 위한 세션키 및 토큰을 생성할 수 있다. 세션키는 상기 보안 통신 세션에서 송수신 되는 데이터 및 정보를 암호화하기 위한 키를 의미한다. 또한, 토큰은 상기 보안 통신 세션에서 데이터 및 정보를 수신하고 전송할 수 있는 권한을 나타내는 메시지의 일종이다.

[0169] 전자 서명 서비스 서버(100)의 프로세서(120)는 상기 세션키 및 토큰을 생성하고 상기 세션키 및 토큰을 사용자 단말(200)과 공유함으로써 보안 통신 세션을 생성할 수 있다. 보안 통신 세션이 생성되면, 전자 서명 서비스 서버(100)와 사용자 단말(200)은 각각 송신하는 정보 및 데이터에 상기 토큰을 함께 첨부함으로써, 상기 보안 통신 세션을 이용할 권한이 있음을 인증할 수 있다. 또한, 전자 서명 서비스 서버(100)는 사용자 단말(200)로부터 수신한 토큰을 검증함으로써 사용자가 전자 서명을 생성할 권한이 있는지 여부를 판단할 수 있다. 또한, 전자 서명 생성 모듈(140)은 저장부(130)에 저장된 개인키들 가운데 상기 토큰에 대응하는 개인키가 무엇인 지를 결정하고, 상기 토큰에 대응하는 개인키를 이용하여 사용자의 전자 서명을 생성할 수 있다.

[0170] 상기 보안 통신 세션을 통해 전자 서명 서비스 서버(100)와 사용자 단말(200) 사이에서 송수신 되는 정보 및 데이터는 상기 세션키에 의해 암호화 될 수 있다. 예를 들어, 1224 단계에서 사용자 단말(200)은 서명 대상 데이터 및 전자 서명 요청을 상기 세션키로 암호화 하여 전자 서명 서비스 서버(100)에 전송할 수 있다. 그리고, 전자 서명 서비스 서버(100)의 프로세서(120)는 상기 세션키를 이용하여 상기 암호화 된 전자 서명 요청 및 서명 대상 데이터를 복호화 할 수 있다.

[0171] 마찬가지로, 1228 단계에서 전자 서명 서비스 서버(100)의 프로세서(120)는 사용자의 전자 서명 및 인증서 데이터를 상기 세션키로 암호화 하여 사용자 단말(200)에 전송할 수 있다. 그리고, 사용자 단말(200)의 프로세서(240)는 상기 세션키를 이용하여 상기 암호화 된 전자 서명 및 인증서 데이터를 복호화 할 수 있다.

[0172] 도 8을 참조하여 설명한 실시예에 따르면, 1220 단계에서 생성된 세션키를 이용하여 전자 서명 서비스 서버(100)와 사용자 단말(200) 사이에서 송수신되는 데이터 및 정보를 암호화 할 수 있다. 전자 서명 서비스 서버(100)와 사용자 단말(200) 사이에서 송수신되는 데이터 및 정보를 암호화 함으로써 사용자의 전자 서명이 탈취되는 것을 방지할 수 있다. 또한, 사용자의 전자 서명 서비스 이용 정보가 외부로 유출되는 것을 방지할 수 있다.

[0173] 도 9는 도 8에서 나타낸 보안 통신 세션 생성 단계(1220)가 수행되는 과정을 예시적으로 나타낸 흐름도이다.

[0174] 1610 단계에서, 전자 서명 서비스 서버(100)의 프로세서(120)는 세션키 및 토큰을 생성할 수 있다.

[0175] 1612 단계에서, 프로세서(120)는 세션키 및 토큰을 암호화 할 수 있다. 세션키 및 토큰은 다양한 방법으로 암호화 될 수 있다. 예를 들어, 프로세서(120)는 도 7에서 나타낸 1540 단계에서 획득한 기기 인증용 공개키를 이용하여 상기 세션키 및 토큰을 암호화 할 수 있다. 프로세서(120)는 RSA, Rabin 및 ECDSA(Elliptic Curve DSA) 알고리즘 중 적어도 하나를 이용하여 상기 세션키 및 토큰을 암호화 할 수 있다.

[0176] 1614 단계에서, 전자 서명 서비스 서버(100)는 통신부(110)를 통해 암호화 된 세션키 및 토큰 데이터를 사용자 단말(200)에 전송할 수 있다.

[0177] 1620 단계에서, 사용자 단말(200)의 프로세서(240)는 암호화 된 세션키 및 토큰 데이터를 복호화 할 수 있다. 예를 들어, 프로세서(240)는 도 7에서 나타낸 1520 단계에서 생성된 기기 인증용 개인키를 이용하여 상기 암호화 된 세션키 및 토큰 데이터를 복호화 할 수 있다.

[0178] 1622 단계에서, 사용자 단말(200)의 프로세서(240)는 제1 난수를 생성할 수 있다. 상기 제1 난수는 사용자 단말(200)에 의해 랜덤으로 생성되는 숫자 배열을 의미한다.

[0179] 1624 단계에서, 사용자 단말(200)의 프로세서(240)는 세션키를 이용하여 제1 난수로부터 유도하여 단말 인증 데이터를 생성할 수 있다. 예시적으로, 프로세서(240)는 세션키를 이용하여 제1 난수를 암호화 함으로써 단말 인증 데이터를 생성할 수 있다. 상기 단말 인증 데이터는 제1 난수의 암호화 결과의 전부 또는 일부를 포함할 수 있다.

[0180] 1626 단계에서, 사용자 단말(200)은 통신부(210)를 통해 제1 난수 및 제1 난수로부터 생성된 단말 인증 데이터를 전자 서명 서비스 서버(100)에게 전송할 수 있다.

[0181] 1630 단계에서, 전자 서명 서비스 서버(100)의 프로세서(120)는 세션키를 이용하여 단말 인증 데이터를 검증 할 수 있다. 프로세서(120)는 1624 단계와 동일한 과정을 통하여 제1 난수로부터 세션키를 이용하여 생성한 데이터와 사용자 단말(200)로부터 수신한 단말 인증 데이터를 비교함으로써, 단말 인증 데이터를 검증할 수 있다. 프로세서(120)는 단말 인증 데이터를 검증함으로써, 사용자 단말(200)이 세션키 및 토큰을 획득했다는 것을 확인할 수 있다.

[0182] 1632 단계에서, 전자 서명 서비스 서버(100)의 프로세서(120)는 단말 인증 데이터의 검증이 완료되면, 제2 난수를 생성할 수 있다.

[0183] 1634 단계에서, 전자 서명 서비스 서버(100) 프로세서(120)는 세션키를 이용하여 제2 난수로부터 유도하여 서버 인증 데이터를 생성할 수 있다. 예시적으로, 프로세서(120)는 세션키를 이용하여 제2 난수를 암호화 함으로써 서버 인증 데이터를 생성할 수 있다. 상기 서버 인증 데이터는 제2 난수의 암호화 결과의 전부 또는 일부를 포함할 수 있다.

[0184] 1636 단계에서, 전자 서명 서비스 서버(100)는 통신부(110)를 통해 제2 난수 및 서버 인증 데이터를 사용자 단말(200)에게 전송할 수 있다.

[0185] 1640 단계에서, 사용자 단말(200)의 프로세서(240)는 세션키를 이용하여 서버 인증 데이터를 검증할 수 있다. 프로세서(240)는 1634 단계와 동일한 과정을 통하여 생성된 데이터와 전자 서명 서비스 서버(100)로부터 수신한 서버 인증 데이터를 비교함으로써, 상기 서버 인증 데이터를 검증할 수 있다. 프로세서(240)는 서버 인증 데이터를 검증함으로써, 세션키 및 토큰이 전자 서명 서비스 서버(100)에 의해 생성되었다는 것을 확인할 수 있다.

[0186] 상술한 단말 인증 데이터 및 서버 인증 데이터에 대한 검증이 완료되면, 전자 서명 서비스 서버(100)와 사용자 단말(200) 사이에 보안 통신 세션이 생성될 수 있다. 전자 서명 서비스 서버(100)와 사용자 단말(200)은 상기 세션키를 이용하여 송수신 데이터를 암호화 할 수 있다. 전자 서명 서비스 서버(100)와 사용자 단말(200) 사이의 송수신 데이터가 암호화 됨에 따라 전자 서명 서비스의 보안이 향상될 수 있다.

[0187] 도 9에서는 서버 인증 데이터 및 단말 인증 데이터가 제1 및 제2 난수로부터 생성되는 것을 예시적으로 나타냈지만 실시예가 이에 제한되는 것은 아니다. 예를 들어, 단말 인증 데이터는 사용자 단말(200)에 저장된 다른 인증 정보로부터 생성될 수 있다. 또한, 서버 인증 데이터는 전자 서명 서비스 서버(100)에 저장된 다른 인증 정보로부터 생성될 수도 있다.

[0188] 도 10은 상기 보안 통신 세션을 이용하여 전자 서명 서비스 서버(100)와 사용자 단말(200)이 데이터를 송수신하는 것을 나타낸 흐름도이다.

[0189] 1712 단계에서, 사용자 단말(200)의 프로세서(240)는 전자 서명 서비스 서버(100)에게 전송하고자 하는 단말 송신 데이터를 생성할 수 있다. 상기 단말 송신 데이터는 사용자 단말(200)로부터 전자 서명 서비스 서버(100)로 송신되는 데이터를 의미한다. 예를 들어, 단말 송신 데이터는 전자 서명의 요청, 서명 대상 데이터 등을 포함할 수 있다.

[0190] 1714 단계에서, 사용자 단말(200) 의 프로세서(240)는 세션키를 이용하여 상기 단말 송신 데이터를 암호화 할 수 있다.

[0191] 1716 단계에서, 사용자 단말(200)은 통신부(210)를 통해 암호화 된 단말 송신 데이터를 전송할 수 있다.

[0192] 1720 단계에서, 전자 서명 서비스 서버(100)의 프로세서(120)는 통신부(110)가 수신한 상기 암호화 된 단말 송신 데이터를 복호화 할 수 있다. 프로세서(120)는 세션키를 이용하여 상기 암호화 된 단말 송신 데이터를 복호화 할 수 있다.

[0193] 1722 단계에서, 상기 단말 송신 데이터가 소정의 서비스를 요청하는 서비스 요청을 포함하는 경우, 전자 서명 서비스 서버(100)는 상기 요청을 처리할 수 있다. 예를 들어, 단말 송신 데이터에 전자 서명 생성의 요청이 포함된 경우, 전자 서명 서비스 서버(100)는 사용자의 전자 서명 생성을 진행할 수 있다.

[0194] 1724 단계에서, 전자 서명 서비스 서버(100)의 프로세서(120)는 사용자 단말(200)에게 전송하고자 하는 서버 송신 데이터를 생성할 수 있다. 상기 서버 송신 데이터는 전자 서명 서비스 서버(100)로부터 사용자 단말(200)로 송신되는 데이터를 의미한다. 예를 들어, 서버 송신 데이터는 전자 서명, 인증서 데이터 등을 포함할 수 있다.

[0195] 1726 단계에서, 전자 서명 서비스 서버(100)의 프로세서(120)는 세션키를 이용하여 상기 서버 송신 데이터를 암호화 할 수 있다.

[0196] 1730 단계에서, 전자 서명 서비스 서버(100)는 통신부(110)를 통해 암호화 된 서버 송신 데이터를 전송할 수 있다.

[0197] 1732 단계에서, 사용자 단말(200)의 프로세서(240)는 통신부(210)가 수신한 상기 암호화 된 서버 송신 데이터를 복호화 할 수 있다. 프로세서(240)는 세션키를 이용하여 상기 암호화 된 서버 송신 데이터를 복호화 할 수 있다.

[0198] 이상에서 예시적으로, 전자 서명 서비스 서버(100)가 미리 등록된 사용자의 개인키를 이용하여 전자 서명을 생성하고, 생성한 전자 서명을 사용자 단말(200)에게 제공하는 것에 관해 설명하였다.

[0199] 이하에서는 전자 서명 서비스 서버에 사용자의 개인키를 등록하는 과정에 대해서 설명한다.

[0200] 도 11a 및 도 11b은 도 1에서 나타낸 전자 서명 서비스 시스템(1000)에 의해 전자 서명 서비스가 제공되는 방법의 예시를 나타낸 흐름도이다. 도 11a 및 도 11b를 참조하면, 사용자가 발급 또는 갱신한 인증서에 대응하는 키 쌍의 적어도 일부가 전자 서명 서비스 서버(100)에 등록될 수 있다.

[0201] 2110, 2112, 2114 단계에서 사용자 인증이 이루어질 수 있다. 사용자 인증 과정은 도 6 내지 도 8을 참조하여 설명한 실시예들에 따라 이루어질 수 있다.

[0202] 2120 단계에서, 사용자 단말(200)은 전자 서명 서비스 서버(100)에게 사용자의 전자 서명 생성을 위한 키 쌍의 생성을 요청할 수 있다.

[0203] 2122 단계에서, 전자 서명 서비스 서버(100)의 프로세서(120)는 사용자 단말(200)의 요청에 응답하여 키 쌍을 생성할 수 있다. 전자 서명 서비스 서버(100)는 상기 키 쌍에 포함된 개인키를 등록할 수 있다. 전자 서명 서비스 서버(100)는 상기 개인키를 저장부(130)의 제1 저장 공간(132)에 저장함으로써, 상기 개인키를 등록할 수 있다. 개인키는 전자 서명 서비스 서버(100) 외부로 공개되지 않을 수 있다. 상기 키 쌍에 포함된 공개키는 저장부(130)의 제2 저장 공간(134)에 저장될 수 있다. 다른 예로, 상기 공개키는 저장부(130)에 저장되지 않고, 사용자 단말(200)에게 전송될 수도 있다.

[0204] 2124 단계에서, 전자 서명 서비스 서버(100)는 통신부(110)를 통해 사용자 단말(200)에게 키 쌍의 생성 결과를 전송할 수 있다.

[0205] 2126 단계에서, 사용자 단말(200)은 전자 서명 서비스 서버(100)에게 공개키를 전송해 줄 것을 요청할 수 있다.

[0206] 2128 단계에서, 전자 서명 서비스 서버(100)는 통신부(110)를 통해 키 쌍에 포함된 공개키를 사용자 단말(200)에게 전송할 수 있다.

[0207] 2130 단계에서, 사용자 단말(200)은 통신부(210)를 통해 개인키 소유여부 검증정보 및 개인키 소유여부 검증정보에 대한 전자 서명의 요청을 전자 서명 서비스 서버(100)에게 전송할 수 있다. 상기 개인키 소유여부 검증정보는 사용자의 정당한 개인키 소유여부를 검증하기 위한 목적으로 생성된 데이터로서 인증 서버(400)에서 요구하는 프로토콜에 따라 다르게 생성될 수 있다

[0208] 2132 단계에서, 전자 서명 서비스 서버(100)의 전자 서명 생성 모듈(140)은 2122 단계에서 생성되어 등록된 사용자의 개인키를 이용하여 개인키 소유여부 검증정보에 대한 전자 서명을 생성할 수 있다. 예를 들어, 전자 서명 생성 모듈(140)은 상기 사용자의 개인키를 이용하여 개인키 소유여부 검증정보의 전부 또는 일부에 대한 전자 서명을 생성할 수 있다.

[0209] 2134 단계에서, 전자 서명 서비스 서버(100)는 전자 서명 생성 모듈(140)이 생성한 개인키 소유여부 검증정보에 대한 전자 서명을 통신부(110)를 통해 사용자 단말(200)에게 전송할 수 있다.

[0210] 2140 단계에서, 사용자 단말(200)의 프로세서(240)는 상기 키 쌍에 대응하는 인증서 데이터를 생성해줄 것을 요청하는 전문을 생성할 수 있다. 상기 인증서 데이터를 생성해줄 것을 요청하는 전문은 인증 서버(400)에서 요구하는 프로토콜에 따라 생성될 수 있다.

[0211] 2142 단계에서, 사용자 단말(200)은 통신부(210)를 통해 상기 인증서 데이터를 생성해줄 것을 요청하는 전문을 공인 인증 기관이 운영하는 인증 서버(400)에 전송할 수 있다. 또한, 사용자 단말(200)은 전자 서명 서비스 서버(100)로부터 획득한 개인키 소유여부 검증정보에 대한 전자 서명을 인증 서버(400)에 전송할 수 있다.

[0212] 2144 단계에서, 인증 서버(400)는 사용자 단말(200)로부터 수신한 개인키 소유여부 검증정보에 대한 전자 서명을 검증할 수 있다. 예를 들어, 인증 서버(400)는 공개키를 이용하여 상기 개인키 소유여부 검증정보에 대한 전자 서명을 검증할 수 있다. 인증 서버(400)는 개인키 소유여부 검증정보에 대한 전자 서명이 검증되면, 사용자가 개인키를 이용하여 전자 서명을 생성할 권한을 획득한 것으로 판단할 수 있다.

[0213] 2144 단계에서, 그리고, 인증 서버(400)는 사용자 단말(200)로부터 수신한 인증서 데이터 생성 요청 전문에 응답하여 사용자의 인증서 데이터를 생성할 수 있다.

[0214] 2146 단계에서, 인증 서버(400)는 사용자 단말(200)에게 인증서 데이터를 전송할 수 있다. 사용자 단말(200)은 인증 서버(400)로부터 수신한 인증서 데이터를 사용자 단말(200)의 메모리에 보관할 수도 있고, 보관하지 않을 수도 있다.

[0215] 2148 단계에서, 사용자 단말(200)은 통신부(210)를 통해 상기 인증서 데이터를 전자 서명 서비스 서버(100)에 전송할 수 있다.

[0216] 2150 단계에서, 전자 서명 서비스 서버(100)는 사용자 단말(200)로부터 수신한 인증서 데이터를 등록할 수 있다. 예시적으로, 전자 서명 서비스 서버(100)는 인증서 데이터를 저장부(130)의 제2 저장 공간(134)에 저장함으로써 인증서 데이터를 등록할 수 있다. 제2 저장 공간(134)에 저장된 인증서 데이터는 프로세서(120)가 이용할 수 있으며, 통신부(110)를 통해 사용자 단말(200)에게 전송될 수도 있다.

[0217] 도 11에서는 신규로 생성되는 키 쌍이 전자 서명 서비스 서버(100)에 등록되는 것을 예시적으로 나타냈지만 실시예가 이에 제한되는 것은 아니다. 예를 들어, 사용자는 사용자 단말(200)에 미리 저장된 개인키 및 인증서 데이터를 전자 서명 서비스 서버(100)에 이동시킴으로써, 전자 서명 서비스 서버(100)에 개인키 및 인증서 데이터

를 등록할 수 있다.

[0218] 도 12는 사용자 단말(200)에 저장된 개인키 및 인증서 데이터를 전자 서명 서비스 서버(100)에 이동시키는 과정을 예시적으로 나타낸 흐름도이다.

[0219] 2310, 2312, 2314 단계에서 사용자 인증이 이루어질 수 있다. 사용자 인증 과정은 도 6 내지 도 8을 참조하여 설명한 실시예들에 따라 이루어질 수 있다.

[0220] 2320 단계에서, 사용자 단말(200)의 프로세서(240)은 사용자 단말(200)에 저장된 개인키를 암호화 할 수 있다. 프로세서(240)는 도 10에서 나타낸 1610 단계에서 생성된 세션키를 이용하여 사용자 단말(200)에 저장된 개인키를 암호화 할 수 있다.

[0221] 2322 단계에서, 사용자 단말(200)은 통신부(210)를 통해 암호화 된 개인키를 전자 서명 서비스 서버(100)에게 전송할 수 있다.

[0222] 2324 단계에서, 전자 서명 서비스 서버(100)의 프로세서(120)는 도 10에서 나타낸 1610 단계에서 생성된 세션키를 이용하여 암호화 된 개인키를 복호화 할 수 있다. 또한, 전자 서명 서비스 서버(100)는 복호화 연산에 의해 획득된 개인키를 저장부(130)에 저장할 수 있다. 예시적으로, 전자 서명 서비스 서버(100)는 개인키를 제1 저장 공간(132)에 저장할 수 있다.

[0223] 2330 단계에서, 사용자 단말(200)의 프로세서(240)는 사용자 단말(200)에 저장된 인증서 데이터를 암호화 할 수 있다. 프로세서(240)는 도 10에서 나타낸 1610 단계에서 생성된 세션키를 이용하여 사용자 단말(200)에 저장된 인증서 데이터를 암호화 할 수 있다.

[0224] 2332 단계에서, 사용자 단말(200)은 통신부(210)를 통해 암호화 된 인증서 데이터와 암호화 된 공개키를 전자 서명 서비스 서버(100)에게 전송할 수 있다.

[0225] 2334 단계에서, 전자 서명 서비스 서버(100)의 프로세서(120)는 도 10에서 나타낸 1610 단계에서 생성된 세션키를 이용하여 암호화 된 개인키를 복호화 할 수 있다. 또한, 전자 서명 서비스 서버(100)는 복호화 연산에 의해 획득된 인증서 데이터 및 공개키를 저장부(130)에 저장할 수 있다. 예시적으로, 전자 서명 서비스 서버(100)는 인증서 데이터 및 공개키를 제2 저장 공간(134)에 저장할 수 있다.

[0226] 이상에서 도 1 내지 도 12를 참조하여 실시예들에 따른 전자 서명 서비스 시스템, 서버, 단말 및 방법에 관하여 설명하였다.

[0227] 상술한 실시예들에 따르면, 전자 서명 생성을 위한 개인키를 전자 서명 서비스 서버에서 등록 및 관리함으로써 사용자가 개인키가 저장된 매체를 소지하지 않아도 되는 효과가 발생한다. 또한, 개인키가 저장된 매체가 도용되는 것을 방지할 수 있다.

[0228] 또한, 전자 서명 서비스 서버(100)에 저장된 개인키를 전자 서명 생성 모듈 외에 다른 장치가 확인 및 복제하는 것을 차단함으로써, 사용자의 개인키에 대한 보안이 향상될 수 있다.

[0229] 한편, 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성 가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다. 또한, 상술한 본 발명의 실시예에서 사용된 데이터의 구조는 컴퓨터로 읽을 수 있는 기록매체에 여러 수단을 통하여 기록될 수 있다. 상기 컴퓨터로 읽을 수 있는 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드 디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등)와 같은 저장매체를 포함한다.

[0230] 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

[0231] 1000 : 전자 서명 서비스 시스템

100 : 전자 서명 서비스 서버

110 : 통신부

120 : 프로세서

130 : 저장부

132, 134 : 제1, 제2 저장 공간

140 : 전자 서명 생성 모듈

200 : 사용자 단말

210 : 통신부

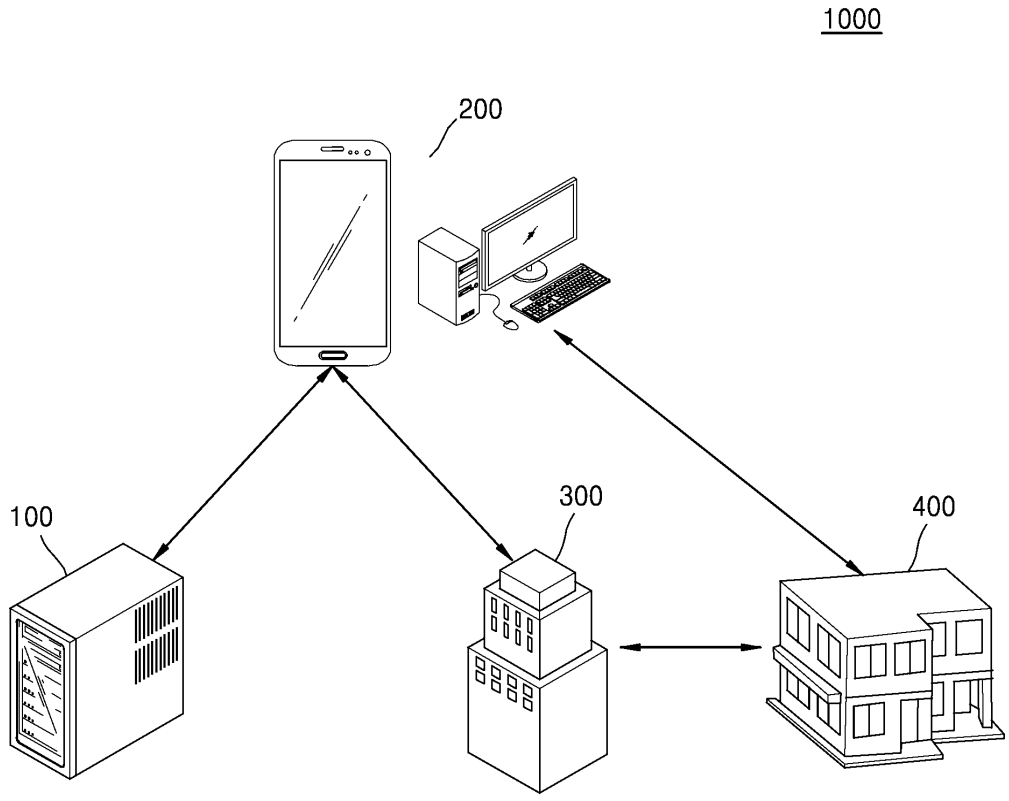
220 : 로컬 인증부

230 : 입력부

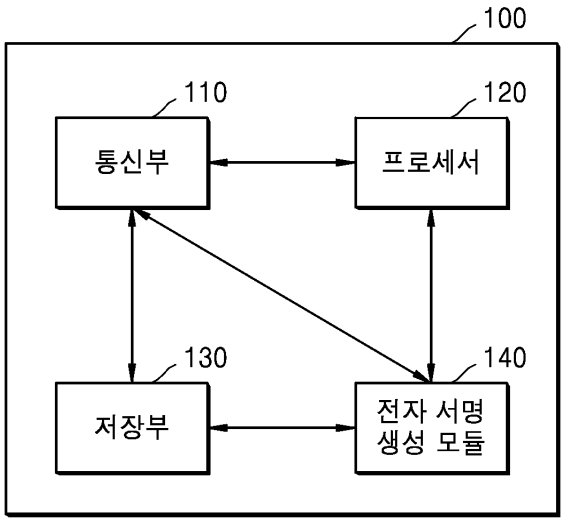
240 : 프로세서

도면

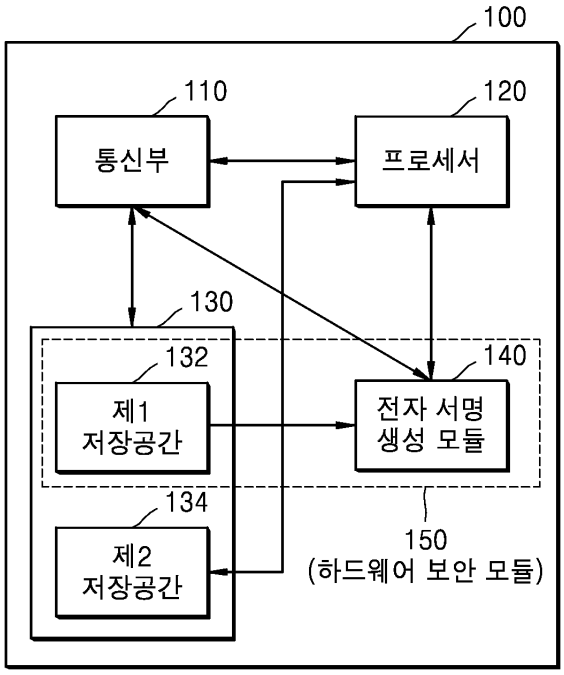
도면1



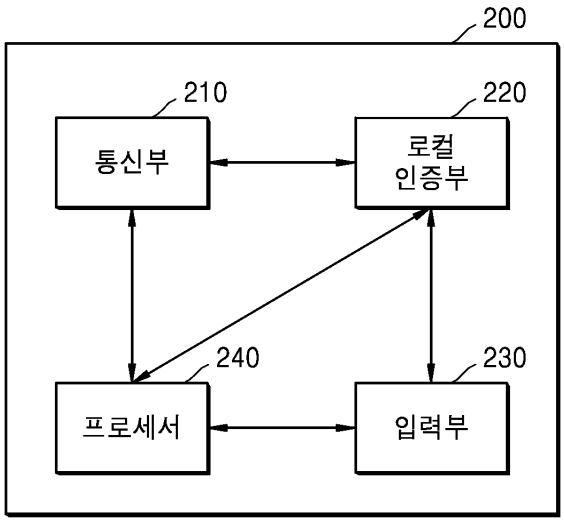
도면2


100
110
120
통신부
프로세서
130
140
저장부
전자 서명
생성 모듈

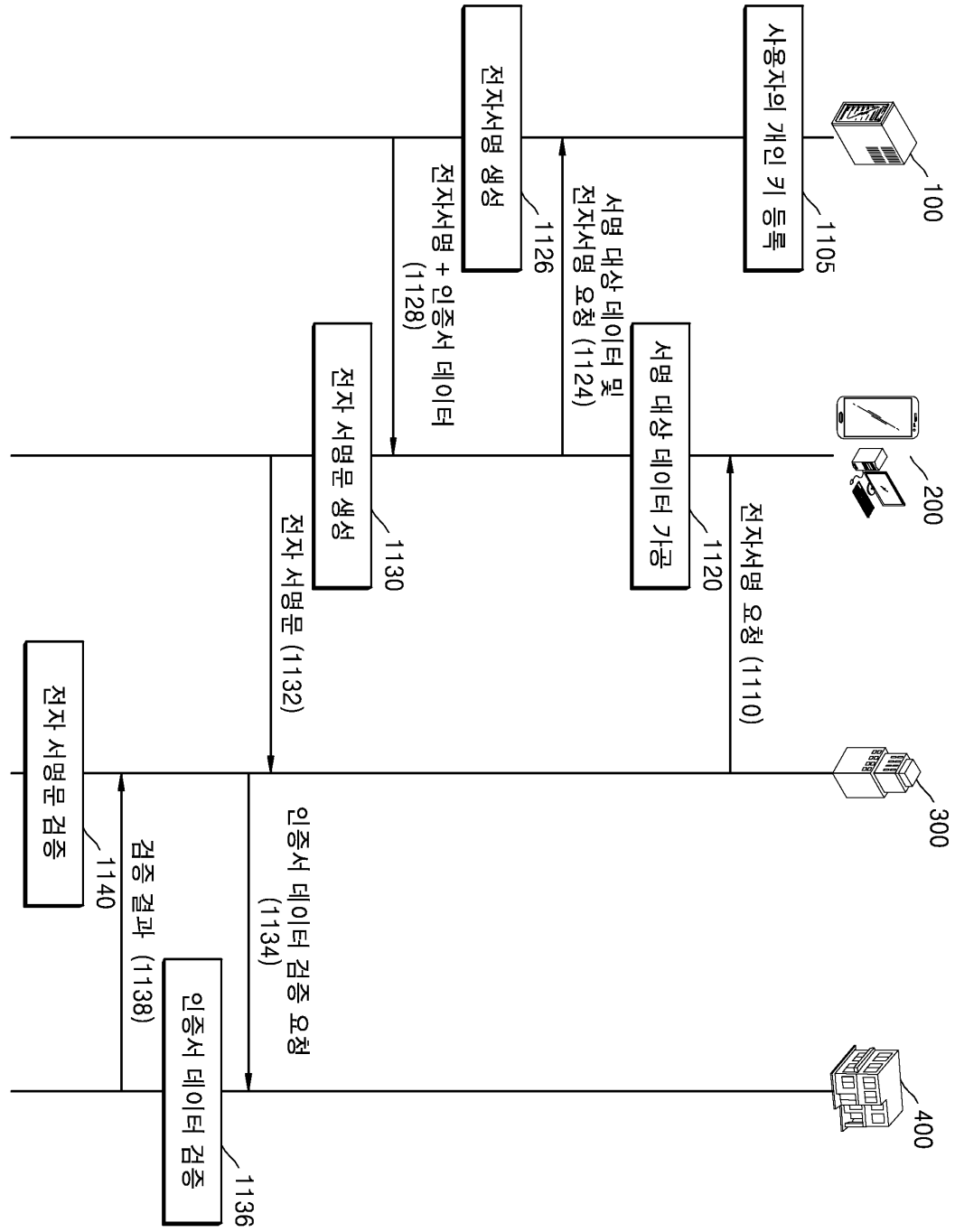
도면3


100
110
120
통신부
프로세서
130
132
140
제1
저장공간
전자 서명
생성 모듈
134
150
제2
저장공간
(하드웨어 보안 모듈)

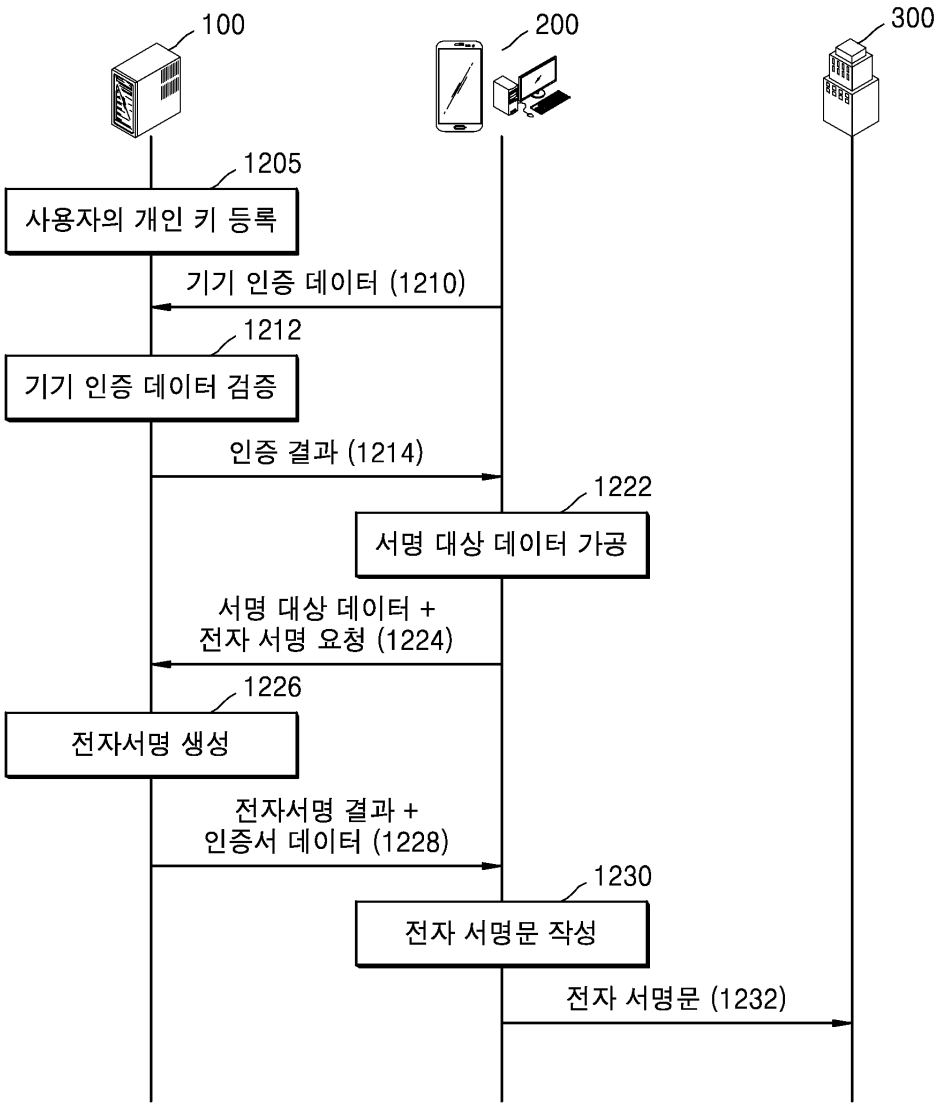
도면4



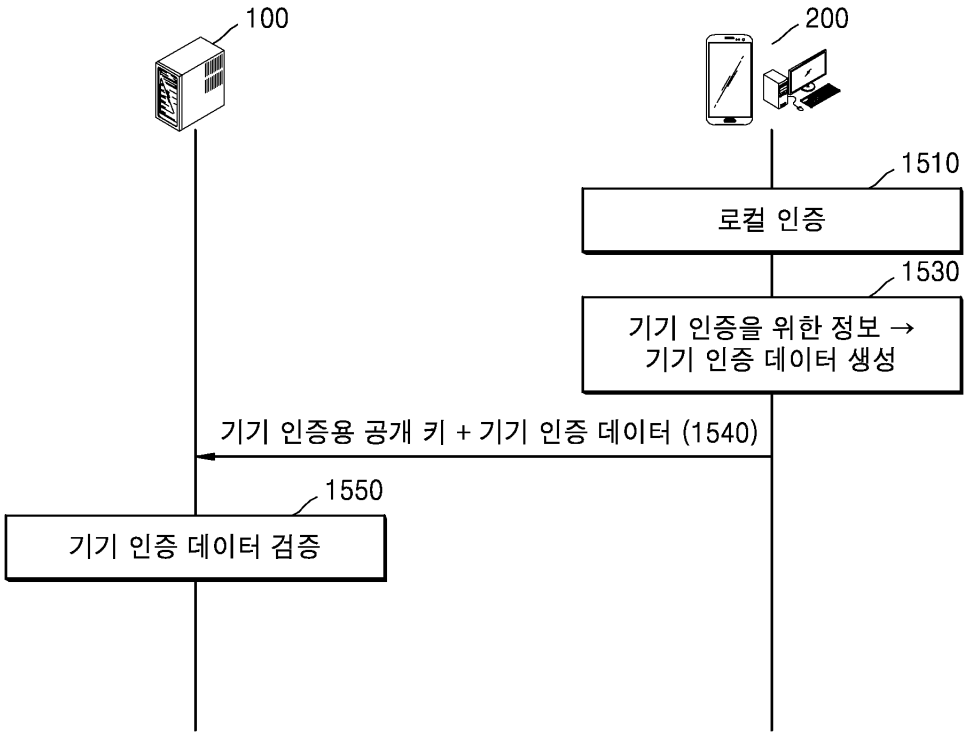
도면5


사용자의 개인 키 등록
1105
100
전자서명 생성
1126
서명 대상 데이터 및
전자서명 요청 (1124)
전자서명 + 인증서 데이터
(1128)
서명 대상 데이터 가공
1120
전자서명 요청 (1110)
200
전자 서명문 생성
1130
전자 서명문 (1132)
300
전자 서명문 검증
1140
검증 결과 (1138)
인증서 데이터 검증 요청
(1134)
인증서 데이터 검증
1136
400

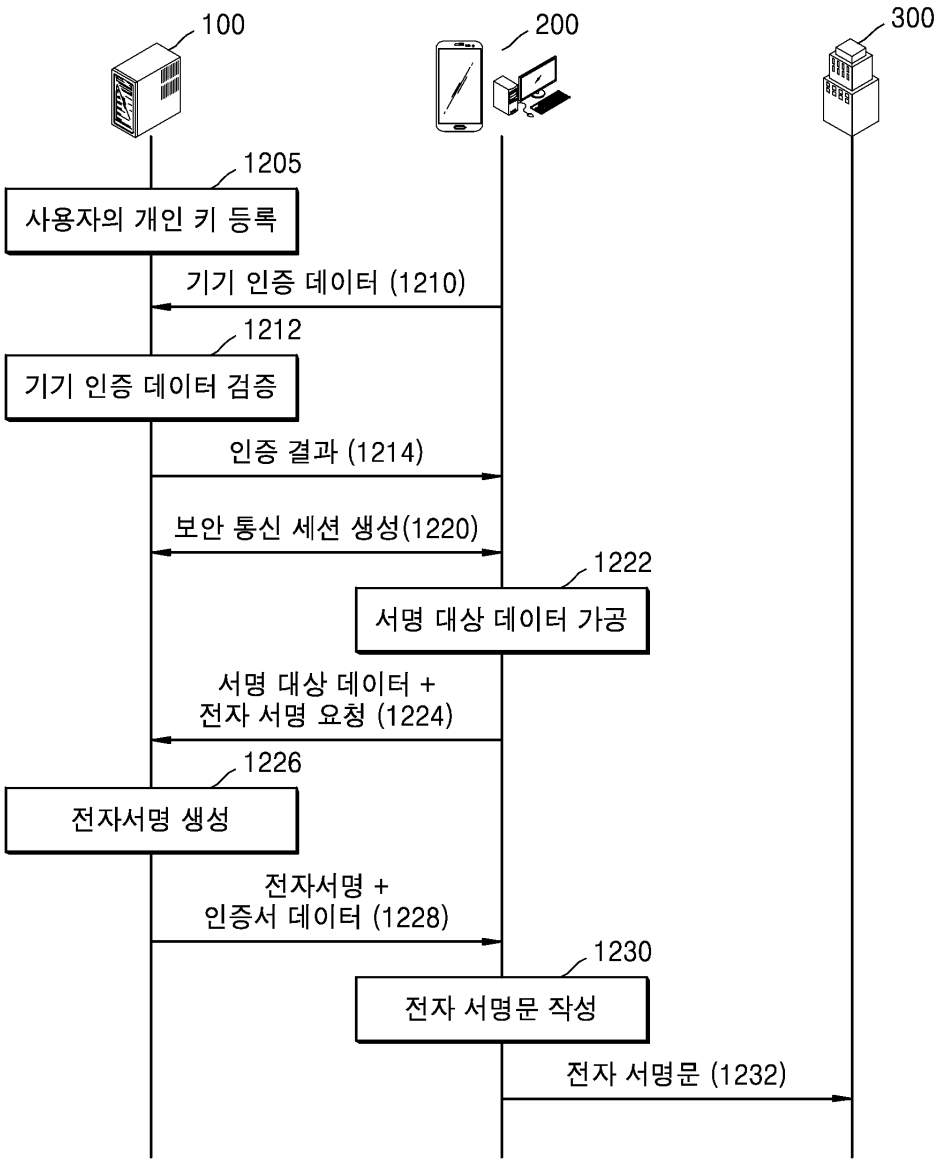
도면6


100
200
300
1205
사용자의 개인 키 등록
기기 인증 데이터 (1210)
1212
기기 인증 데이터 검증
인증 결과 (1214)
1222
서명 대상 데이터 가공
서명 대상 데이터 +
전자 서명 요청 (1224)
1226
전자서명 생성
전자서명 결과 +
인증서 데이터 (1228)
1230
전자 서명문 작성
전자 서명문 (1232)

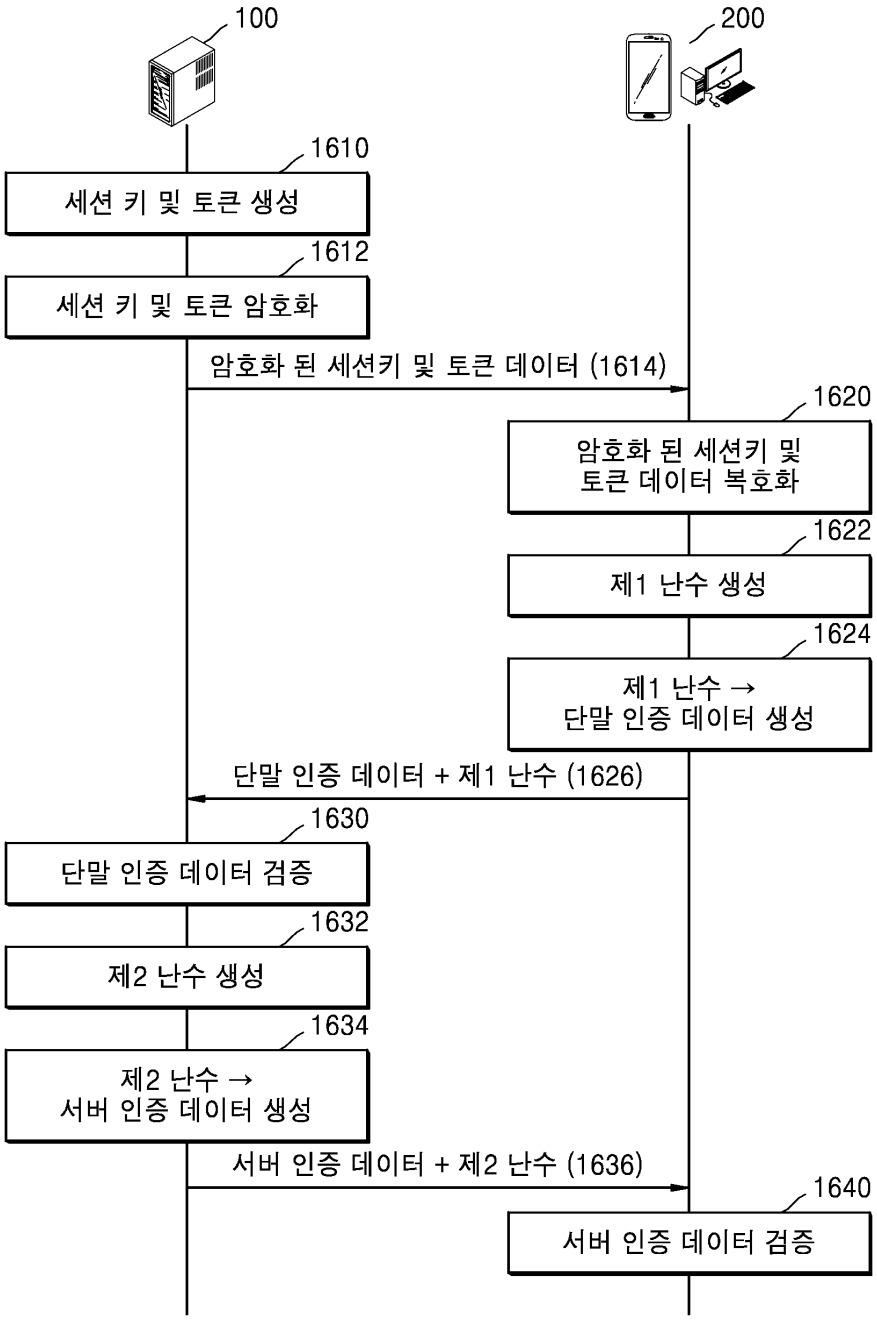
도면7


100
200
1510
로컬 인증
1530
기기 인증을 위한 정보 →
기기 인증 데이터 생성
기기 인증용 공개 키 + 기기 인증 데이터 (1540)
1550
기기 인증 데이터 검증

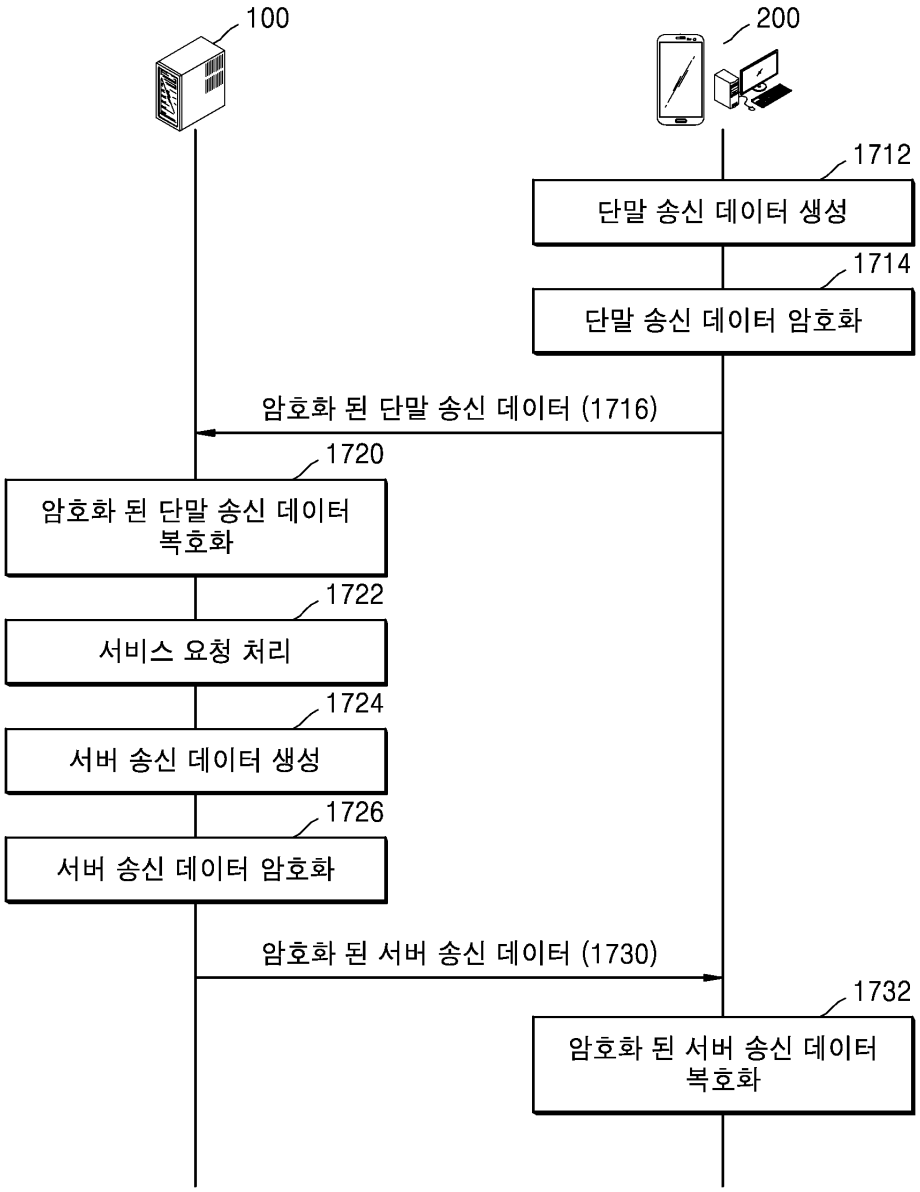
도면8


100
200
300
1205
사용자의 개인 키 등록
기기 인증 데이터 (1210)
1212
기기 인증 데이터 검증
인증 결과 (1214)
보안 통신 세션 생성(1220)
1222
서명 대상 데이터 가공
서명 대상 데이터 +
전자 서명 요청 (1224)
1226
전자서명 생성
전자서명 +
인증서 데이터 (1228)
1230
전자 서명문 작성
전자 서명문 (1232)

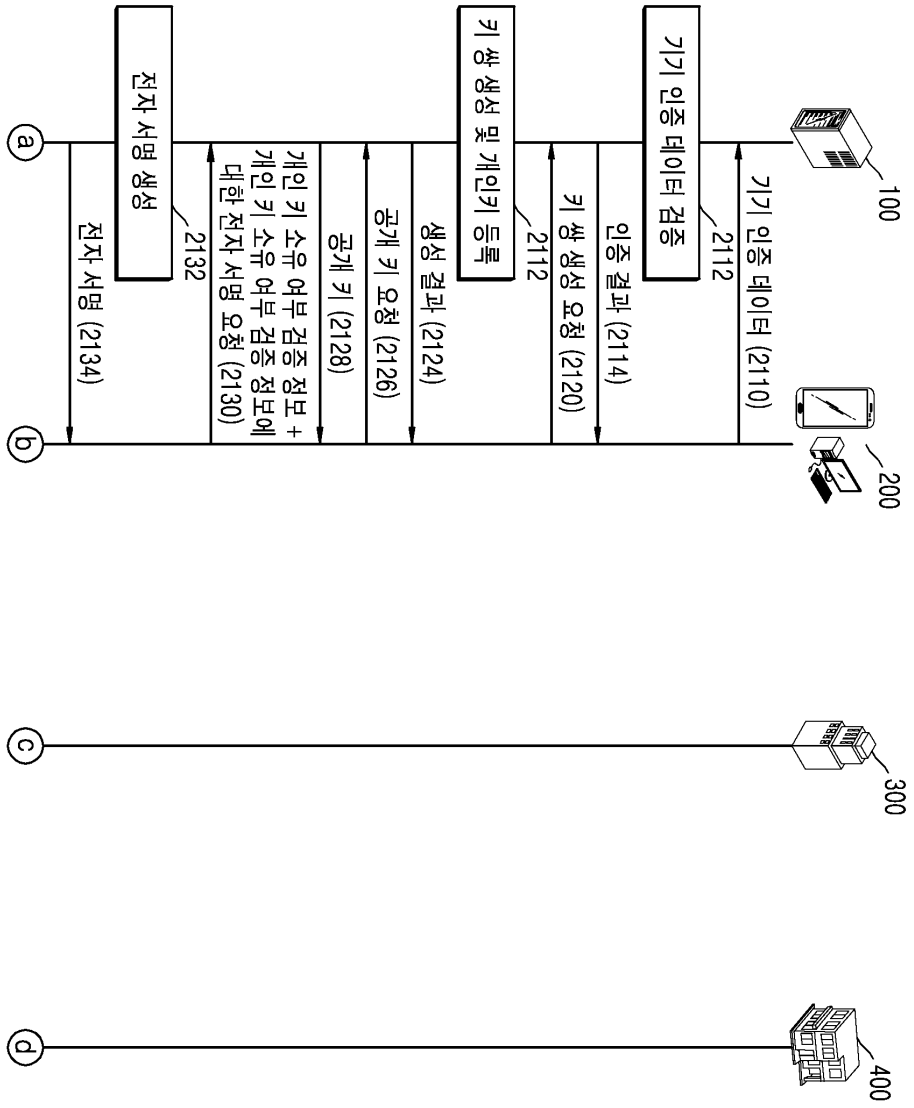
도면9


100
200
1610
세션 키 및 토큰 생성
1612
세션 키 및 토큰 암호화
암호화 된 세션키 및 토큰 데이터 (1614)
1620
암호화 된 세션키 및
토큰 데이터 복호화
1622
제1 난수 생성
1624
제1 난수 →
단말 인증 데이터 생성
단말 인증 데이터 + 제1 난수 (1626)
1630
단말 인증 데이터 검증
1632
제2 난수 생성
1634
제2 난수 →
서버 인증 데이터 생성
서버 인증 데이터 + 제2 난수 (1636)
1640
서버 인증 데이터 검증

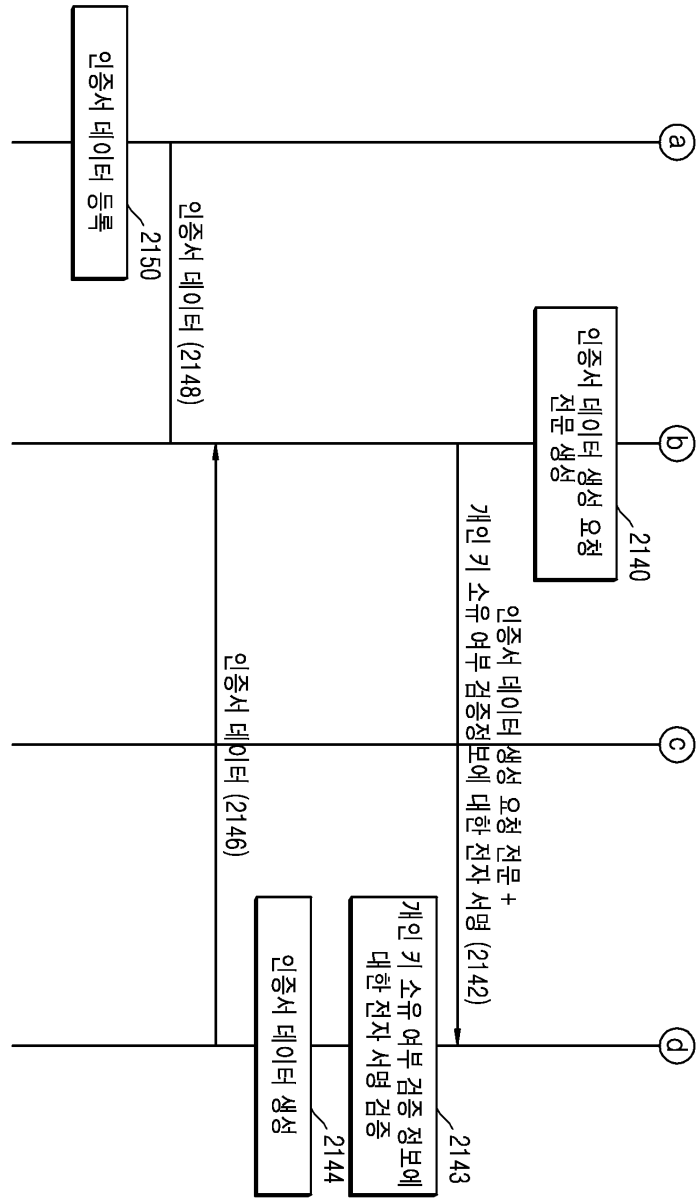
도면10


100
200
1712
단말 송신 데이터 생성
1714
단말 송신 데이터 암호화
암호화 된 단말 송신 데이터 (1716)
1720
암호화 된 단말 송신 데이터 복호화
1722
서비스 요청 처리
1724
서버 송신 데이터 생성
1726
서버 송신 데이터 암호화
암호화 된 서버 송신 데이터 (1730)
1732
암호화 된 서버 송신 데이터 복호화

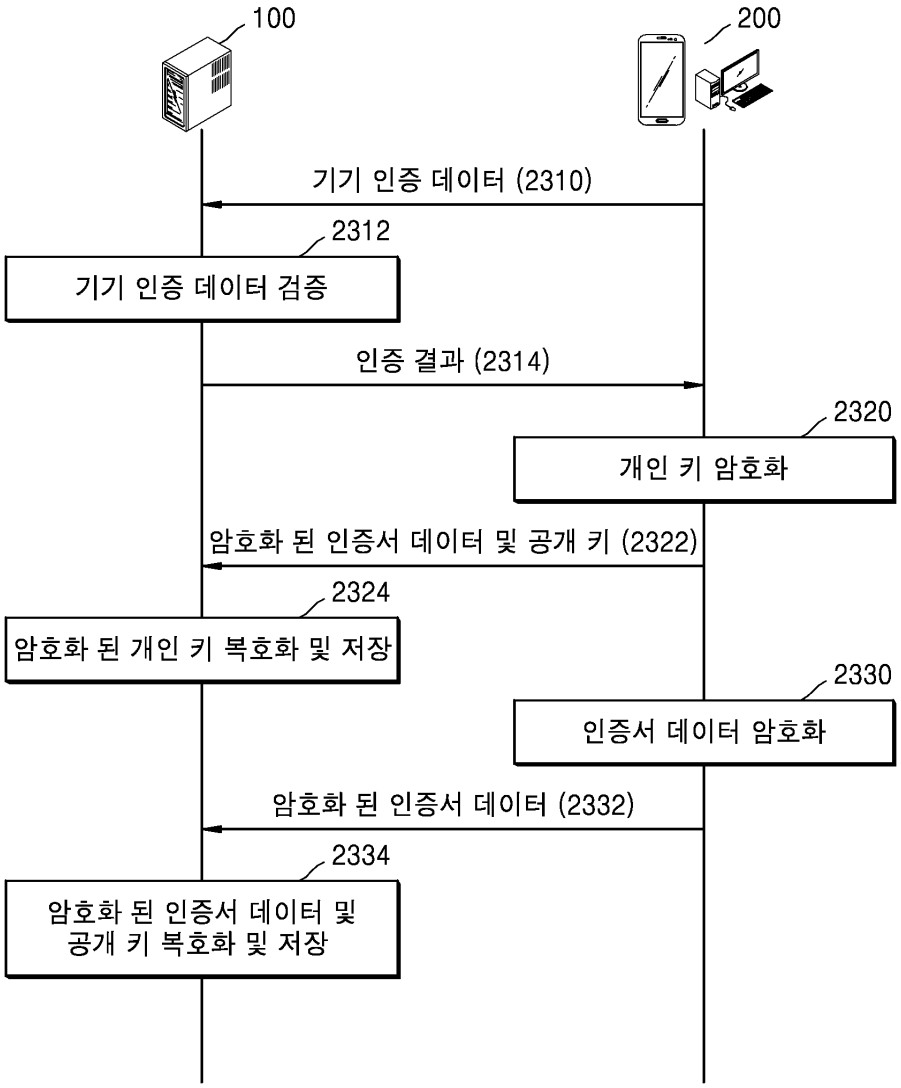
도면11a


a
b
c
d
100
200
300
400
기기 인증 데이터 (2110)
기기 인증 데이터 검증
2112
인증 결과 (2114)
키 쌍 생성 요청 (2120)
키 쌍 생성 및 개인키 등록
2112
생성 결과 (2124)
공개 키 요청 (2126)
공개 키 (2128)
개인 키 소유 여부 검증 정보 + 개인 키 소유 여부 검증 정보에 대한 전자 서명 요청 (2130)
전자 서명 생성
2132
전자 서명 (2134)

도면11b


인증서 데이터 등록
2150
인증서 데이터 (2148)
인증서 데이터 생성 요청
전문 생성
2140
인증서 데이터 생성 요청 전문 +
개인 키 소유 여부 검증정보에 대한 전자 서명 (2142)
인증서 데이터 (2146)
개인 키 소유 여부 검증 정보에
대한 전자 서명 검증
2143
인증서 데이터 생성
2144
ⓐ
ⓑ
ⓒ
ⓓ

도면12



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제17항

【변경전】

상기 인증서 데이터를 저장하는 제2 저장 공간을 포함하며

【변경후】

인증서 데이터를 저장하는 제2 저장 공간을 포함하며