(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0117463
(43) 공개일자 2011년10월27일

(51) Int. Cl.
H04L 9/32 (2006.01) *H04L 9/14* (2006.01)
(21) 출원번호 10-2010-0036935
(22) 출원일자 2010년04월21일
심사청구일자 2010년04월21일

(71) 출원인
충남대학교산학협력단
대전 유성구 궁동 220 충남대학교
(72) 발명자
이광우
대전광역시 대덕구 법동 280-2 삼호아파트 3동102호
원동호
서울특별시 서초구 잠원동 한일17차아파트 334동 903호
김승주
서울특별시 송파구 문정동 150 올림픽훼밀리APT 234동 403호
(74) 대리인
특허법인정직과특허

전체 청구항 수 : 총 15 항

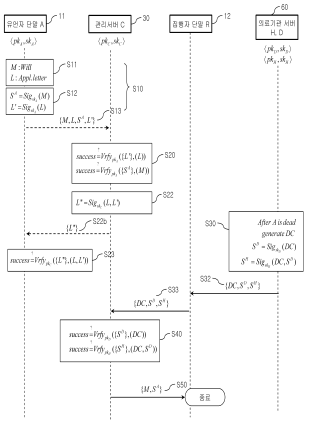
(54) 멀티미디어 형식의 유언장을 관리하는 인증서 기반 인터넷 전자유언장 관리 시스템 및 방법

(57) 요 약

자필, 음성, 또는 동영상 등 멀티미디어 형식으로 작성된 유언장을 인증기관에서 발급하는 인증서로 전자서명을 하여 부인방지 성질을 제공하는 인터넷 전자유언장 관리 시스템 및 방법에 관한 것으로서, (a) 유언자 단말은 유언자의 인증서로 신청서 및 유언장을 전자서명하여 관리서버로 전송하는 단계; (b) 관리서버는 전자서명된 신청서 및 유언장을 수신하여 신청서 및 유언장의 전자서명을 검증하고 저장하는 단계; (c) 관리서버는 유언자의 사망을 확인하는 단계; 및 (d) 유언자의 사망 확인후, 관리서버는 상기 유언집행자 단말로 전자서명된 유언장을 전송하는 단계를 포함하되, 상기 유언장은 멀티미디어 데이터를 포함하는 구성을 마련한다.

상기와 같은 인터넷 전자유언장 관리 시스템 및 방법에 의하여, 유언자가 유언내용을 자신이 원하는 어떤 형태로도 작성할 수 있고, 작성된 유언장의 내용이 부인될 수 없으면서 유언장의 내용이 유언자가 사망하기 전까지 알 수 없게 할 수 있다.

대 표 도 - 도3



특허청구의 범위

청구항 1

유언자 단말 및 유언집행자 단말과 네트워크로 연결된 유언장 관리서버에 의해, 인증기관에서 발급하는 인증서로 전자서명을 하여 유언장을 관리하는 인터넷 전자유언장 관리 방법에 있어서,

(a) 상기 유언자 단말은 유언자의 인증서로 신청서 및 유언장을 전자서명하여 상기 관리서버로 전송하는 단계;

(b) 상기 관리서버는 전자서명된 신청서 및 유언장을 수신하여 신청서 및 유언장의 전자서명을 검증하고 저장하는 단계;

(c) 상기 관리서버는 유언자의 사망을 확인하는 단계; 및

(d) 유언자의 사망 확인후, 상기 관리서버는 상기 유언집행자 단말로 전자서명된 유언장을 전송하는 단계를 포함하되,

상기 유언장은 멀티미디어 데이터를 포함하는 것을 특징으로 하는 인터넷 전자유언장 관리 방법.

청구항 2

유언자 단말 및 유언집행자 단말과 네트워크로 연결된 유언장 관리서버에 의해, 인증기관에서 발급하는 인증서로 전자서명을 하여 유언장을 관리하는 인터넷 전자유언장 관리 방법에 있어서,

(a) 상기 유언자 단말은 유언자의 인증서로 신청서 및 유언장을 전자서명하여 비밀키와 함께 상기 관리서버로 전송하되, 상기 유언장은 상기 비밀키로 암호화되는 단계;

(b) 상기 관리서버는 전자서명된 신청서 및 유언장과, 비밀키를 수신하여 신청서 및 유언장의 전자서명을 검증하고 저장하는 단계;

(c) 상기 관리서버는 유언자의 사망을 확인하는 단계; 및

(d) 유언자의 사망 확인후, 상기 관리서버는 상기 유언집행자 단말로 전자서명된 유언장 및 비밀키를 전송하는 단계를 포함하되,

상기 유언장은 멀티미디어 데이터를 포함하는 것을 특징으로 하는 인터넷 전자유언장 관리 방법.

청구항 3

제1항 또는 제2항에 있어서,

상기 멀티미디어 데이터는 음성 데이터, 동영상 데이터, 이미지 데이터 중 적어도 하나를 포함하는 것을 특징으로 하는 인터넷 전자유언장 관리 방법.

청구항 4

제2항에 있어서,

상기 (a)단계에서, 상기 유언자 단말은 상기 관리서버의 공개키로 비밀키를 암호화하고,

상기 (d)단계에서, 상기 관리서버는 암호화된 비밀키를 자신의 개인키로 복호화하여 전송하는 것을 특징으로 하는 인터넷 전자유언장 관리 방법.

청구항 5

제1항 또는 제2항에 있어서, 상기 방법은,

(b2) 상기 (b)단계이후, 상기 관리서버는 상기 신청서에 상기 신청서의 전자서명을 포함시켜 자신의 인증서로 2차 전자서명을 하고, 2차 전자서명을 상기 유언자 단말로 전송하는 단계; 및

(b3) 상기 유언자 단말은 상기 2차 전자서명을 검증하는 단계를 더 포함하는 것을 특징으로 하는 인터넷 전자유언장 관리 방법.

청구항 6

제1항 또는 제2항에 있어서,

상기 (c)단계에서, 상기 관리서버는 사망확인기관 서버로부터 전자서명된 사망확인서를 수신하고, 상기 사망확인서의 전자서명을 검증함으로써 유언자의 사망을 확인하는 것을 특징으로 하는 인터넷 전자유언장 관리 방법.

청구항 7

제6항에 있어서,

상기 (c)단계에서, 상기 전자서명된 사망확인서는 유언집행자 단말을 거쳐 전송되는 것을 특징으로 하는 인터넷 전자유언장 관리 방법.

청구항 8

제6항에 있어서,

상기 사망확인기관 서버가 의료기관 서버인 경우, 상기 전자서명된 사망확인서는 의사 및 병원의 인증서에 의해 전자서명된 유언자의 사망진단서인 것을 특징으로 하는 인터넷 전자유언장 관리 방법.

청구항 9

제8항에 있어서,

상기 전자서명된 유언자의 사망진단서는, 유언자의 사망진단서를 의사의 인증서에 의해 1차 전자서명하고 사망진단서에 1차 전자서명을 포함하여 의료기관의 인증서에 의해 2차 전자서명을 하여 생성되는 것을 특징으로 하는 인터넷 전자유언장 관리 방법.

청구항 10

제1항 또는 제2항에 있어서, 상기 방법은,

(b1) 상기 (b)단계이후, 상기 관리서버는 적어도 2명의 증인 단말에 전자서명된 신청서 및 유언장을 전송하는 단계;

(b2) 상기 증인 단말은 증인의 인증서로 신청서 및 유언장에 2차 전자서명을 하여 상기 관리서버로 송신하는 단계; 및

(b3) 상기 관리서버는 상기 증인단말로부터 증인의 인증서에 의한 2차 전자서명을 수신하여 검증하는 단계를 더 포함하는 것을 특징으로 하는 인터넷 전자유언장 관리 방법.

청구항 11

제10항에 있어서, 상기 방법은,

(b4) 상기 (b3)단계이후, 상기 관리서버는 신청서 및 유언장에 1차 전자서명 및 2차 전자서명을 포함시켜 자신의 인증서로 3차 전자서명을 하고, 2차 전자서명 및 3차 전자서명을 상기 유언자 단말로 전송하는 단계; 및

(b5) 상기 유언자 단말은 상기 3차 전자서명을 검증하는 것을 특징으로 하는 인터넷 전자유언장 관리 방법.

청구항 12

제1항 또는 제2항에 있어서, 상기 방법은,

(f) 상기 관리서버는 상기 유언자의 인증서 만료일 이전의 갱신기간이 도래하면, 타임스탬핑 기관(TSA)서버로부터 상기 신청서 및 유언장에 대한 타임스탬프 토큰을 획득하여, 상기 신청서 및 인증서에 추가하는 단계를 더 포함하되,

상기 (f)단계는 추가된 타임스탬프 토큰의 만료일 이전의 갱신기간이 도래하면, 타임스탬프 토큰을 재획득하는 것을 특징으로 하는 인터넷 전자유언장 관리 방법.

청구항 13

유언자 단말 및 유언집행자 단말과 네트워크로 연결되고, 인증기관에서 발급하는 인증서로 전자서명을 하여 유언장을 관리하는 인터넷 전자유언장 관리 시스템에 있어서,

상기 유언자 단말로부터 유언자의 인증서로 전자서명된 신청서 및 유언장을 수신하여 상기 신청서 및 유언장의 전자서명을 검증하고 저장하는 유언장 수신부;

유언자의 사망을 확인하는 사망확인 수신부; 및

유언자의 사망 확인후, 상기 유언집행자 단말로 전자서명된 유언장을 전송하는 유언장 전송부를 포함하고,

상기 유언장은 멀티미디어 데이터를 포함하는 것을 특징으로 하는 인터넷 전자유언장 관리 시스템.

청구항 14

유언자 단말 및 유언집행자 단말과 네트워크로 연결되고, 인증기관에서 발급하는 인증서로 전자서명을 하여 유언장을 관리하는 인터넷 전자유언장 관리 시스템에 있어서,

상기 유언자 단말로부터 유언자의 인증서로 전자서명된 신청서 및 유언장, 그리고 비밀키를 수신하여, 상기 신청서 및 유언장의 전자서명을 검증하고 저장하되, 상기 유언장은 상기 비밀키로 암호화되는 유언장 수신부;

유언자의 사망을 확인하는 사망확인 수신부; 및

유언자의 사망 확인후, 상기 유언집행자 단말로 유언장 및 비밀키를 전송하는 유언장 전송부를 포함하고,

상기 유언장은 멀티미디어 데이터를 포함하는 것을 특징으로 하는 인터넷 전자유언장 관리 시스템.

청구항 15

제13항 또는 제14항에 있어서,

상기 멀티미디어 데이터는 음성 데이터, 동영상 데이터, 이미지 데이터 중 적어도 하나를 포함하는 것을 특징으로 하는 인터넷 전자유언장 관리 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 자필, 음성, 또는 동영상 등 멀티미디어 형식으로 작성된 유언장을 인증기관에서 발급하는 인증서로 전자서명을 하여 부인방지 성질을 제공하는 인터넷 전자유언장 관리 시스템 및 방법에 관한 것이다.

[0002] 또한, 본 발명은 전자서명된 유언장에 사용된 인증서의 만료일 이전에 전자서명된 유언장에 대한 타임스탬프를 획득하여 장기 보관하는 인터넷 전자유언장 관리 시스템 및 방법에 관한 것이다.

배 경 기 술

[0003] 최근 들어, 자신이 죽을 경우를 대비하여 유언장을 미리 작성하는 것이 중요한 일이 되고 있다. 유언장은 유언자가 죽은 후에 유언자의 주변인들에게 메시지를 전달하는 유일한 방법이 된다. 만약 어떤 사람이 유언장을 작성하지 않고 죽었다면, 유언자의 가족들은 남겨진 재산의 분배 문제 등과 관련하여 분쟁이 발생할 수 있다.

[0004] 따라서 만약 사후에 가족, 친지, 주변인들에게 남겨두는 재산이 있다면, 유언자가 그 재산들을 어떻게 분배되었으면 하는지를 유언장에 적어주는 것이 중요하다. 유언자가 원하는 바가 사후에도 제대로 반영되기 위해서는 가능한 효과적인 방법으로 문서화되는 것이 중요하다.

[0005] 일반적인 유언장은 유언자나 대리인에 의해서 종이 문서 형태로 작성되게 되는데, 이러한 방식은 대리인 수수료나 기타 부대 비용으로 인하여 값이 비싸고, 불편하다는 단점이 있다.

[0006] 이러한 문제점들을 해결하기 위해서 다양한 인터넷 기반 유언장 관련 서비스들이 등장하였다(참고문헌 1 내지 6 참조). 하지만 이러한 서비스들은 유언장 작성과 관련하여 매우 제한된 기능들만을 제공하고 있으며, 법적으로도 인정 받기가 어렵다.

[0007] [참고문헌 1] Electronic Time-Stamping, http://www.e-timestamping.com/ chi/about/app1/html

[0008] [참고문헌 2] Prepare Life Service, http://www.geocities.com/ preparelife/.

[0009] [참고문헌 3] RC Internet Law Center, http://www.rclaw.com.tw/.

[0010] [참고문헌 4] Your E Will, http://www.yourewill.com/added.html

[0011] [참고문헌 5] Hong Kong e-law service, http://www.hkelaw.com/.

[0012] [참고문헌 6] Taiwan Creative E-integrated services, http://egov.iii. org.tw/.

[0013] 또한, 인터넷 통신망을 이용하여 유언장을 작성하고 관리하는 기술이 제안되고 있으며, 그 일례가 [한국공개특허 10-2007-0108996, "인터넷 통신망을 이용한 유언장 작성시스템 및 그 방법"](이하 선행기술 1)에 제시되고 있다. 상기 선행기술 1은 인터넷 통신망을 통해 접속된 사용자가 유언장 작성에 필요한 정보를 제공받아 유언장을 작성하고, 작성된 유언장에 대하여 인증기관서버로부터 인증 절차를 수행하고, 작성된 유언장 및 인증된 유언장을 저장 관리고, 인터넷 통신망을 통해 열람 또는 전송하도록 하고, 유언자의 유고(有故)시 이에 대한 정보를 공공기관서버로부터 제공받는 기술을 제안하고 있다.

[0014] 그러나 상기 선행기술 1은 종이형태의 인증서를 이용하고 유언장에 대한 서명도 자필 등을 사용하므로, 단지 종래의 오프라인 상의 유언장 작성 및 관리방식을 단순히 전산화한 것에 지나지 않는다. 또한, 선행기술 1은 공증기관(인증기관서버)을 이용하므로 공증비용이 추가로 소요되는 등의 문제점을 가지고 있다.

[0015] Chien이 최근에 인터넷에의 유언장 작성 시스템으로 자필 전자유언장(holographic e-will system), 봉인 전자유언장 (sealed e-will system) 등 두 가지 종류의 유언서 작성 방식을 제안하고 있다. Chien은 그가 제안한 방식이 안전하고, 중화민국 시민법을 만족시킨다고 하였으나, 몇몇 문제점이 있다.

[0016] 도 1a에서 보는 바와 같이, Chien의 자필 전자유언장 방식은 시스템 설정 단계, 키등록 단계, 유언장 생성 단계, 사망진단서 발급 및 제출 단계, 및 유언장 공개 단계로 구성된다.

[0017] 시스템 설정 단계에서, 신뢰기관(TA 또는 법원)은 시스템 파라미터 $\{E, q, G_1, G_2, e, H_1, H_2, P, P_{TA}\}$를 설정한

다. G_1이 타원곡선 E 위에서의 군일 때 G_1과 G_2는 소수q 를 위수로 갖는 두 개의 군이며, P 를 G_1 의 생성자라고 할 때 함수 H1 은 사용자의 ID를 군 G_1의 한 점으로 대응시킨다. 암호학적 해쉬함수 H_2 를 H_2: $G_2 \rightarrow \{0,1\}^m$ 로 정의하고 e 는 Bilinear pairing 이라고 하자. 그러면 신뢰기관(TA)은 임의의 정수 s_{TA} 을 신뢰기관(TA)의 비밀키로 선택하고 시스템의 공개키 $P_{TA} = s_{TA} \cdot P$를 계산한다.

[0018] 등록단계에서, 시스템에 포함 된 각 구성요소들은 개인키 획들을 위해 신뢰기관(TA)에 등록해야 한다. 유언자 A의 공개키는 Q_A 다. 그리고 신뢰기관(TA), 의사(D), 병원(H) 모두 개인키 획득을 위해 신뢰기관(TA)에 등록해야 한다.

[0019] 유언장 생성 단계에서, 유언자 A는 신청서를 작성하고 작성 된 신청서를 신뢰기관(TA)으로 제출한다. 유언장이 작성되고, 날짜를 명시한 다음, 유언자 A는 유언장과 신청서에 서명을 한다. 마지막으로, 유언자 A는 유언장과 신청서를 TA에 제출하고 TA는 서명된 유언장과 신청서를 검증한다. 만약 서명에 대한 검증이 성공한다면 TA는 신청서에 서명을 하고, 공문서 (L")를 유언자에게 확인용으로 제공한다.

[0020] 친척에게 사망진단서(DC) 발급 및 제출 단계에서, 유언자가 사망한 후, 의사는 사망 원인을 진단하고, 전자사망진단서(DC)를 친척들(R)에게 발급한다. 사망진단서에는 의사의 전자서명(S^D) 과 병원의 전자서명(S^H)이 포함된다. 병원은 사망진단서(DC)와 S^D, S^H를 유언자(A)의 친척에게 전송한다. 친척은 병원으로부터 받은 전자사망진단서와 의사 및 병원의 서명 {DC, S^D, S^H}을 법원에 제출하고, 유언장의 공개를 요청한다.

[0021] 유언장 공개 단계에서, 신뢰기관(TA)은 전자사망진단서(DC)와 의사 및 병원의 서명{DC, S^D, S^H}을 검증한다. 검증 방법은 다음과 같다 : $IBSV_{QD}((S_D), (DC))$와 $IBSV_{QH}(\{S^H\}, (DC, S^D))$를 검증한다. $IBSV_{QD}((S^D), (DC))$는 전자사망진단서(DC)의 전자서명을 검증하는 것으로서 성공 또는 실패의 결과값을 반환한다.

[0022] 만약 전자사망진단서(DC)와 그에 대한 전자서명들이 제대로 검증된다면, 신뢰기관(TA)은 유언장(M)을 유언자의 친척에게 전송한다.

[0023] 또한, 도 1b에서 보는 바와 같이, Chien의 봉인 전자유언장 방식은 자필 전자유언장 방식에 비하여, 신뢰기관(TA)의 비밀키를 이용하여 유언장을 암호화한다. 이하에서, Chien의 자필 전자유언장 방식과 다른 부분만 설명한다.

[0024] 즉, 시스템 설정 단계에서, 신뢰기관(TA)은 시스템 파라미터를 설정하고, 임의의 정수 s_{TA} 를 TA의 비밀키로 선택하고 시스템의 공개키 $P_{TA} = s_{TA} \cdot P$를 계산한다.

[0025] 유언장 생성 단계에서, 유언자(A)는 신청서를 작성하고 유언자의 내용을 암호화하기 위해 대칭키(Symmetric key) k를 사용하여 암호화된 유언장(Sealed will)(C)을 얻는다. 대칭키(Symmetric key) k는 공개키 암호화 알고리즘을 이용하여 공개키(Q_{ADeath})로 암호화된다. 다음, 유언자(A)는 신청서(L)와 암호화된 유언장(C)을 전자서명한다. 그리고 유언자는 암호화된 유언장(C)과 암호화된 대칭키 ($Enc_{QADeath}$ (k)), 그리고 신청서(L)를 신뢰기관(TA)에 전송한다.

[0026] 또한, 법원은 유언자의 전자서명이 제대로 포함되었는지를 검증한 다음, 유언자를 제외한 유언자에 의해 지명된 둘 이상의 증인 (X, Y)에게 암호화된 유언장(C)과 신청서(L)를 전송하여 전자서명을 받고 적절하게 서명되었는지를 검증한다.

[0027] 마지막으로, 유언장을 공개하는 단계에서, 신뢰기관(TA)은 개인키 $S_{ADeath} = s_{TA} \cdot Q_{ADeath}$를 생성하고, 생성된 개인키를 암호화된 대칭키 (= $Enc_{QADeath}$ (k))를 계산하는데 사용한다. IBD 또는 IBE는 신원 기반(ID-based) 기반하여 복호화 또는 암호화하는 함수를 의미한다. 그리고 대칭키 k 는 봉인된 유언장(C)을 여는데 사용되며 평문 유언장과 서명 $M=(m||S^A)$ 은 유언자의 친척에게 전달된다.

[0028] 상기 Chien의 제안은 부인방지 특성이 부재하고 유언장 장기 서명 검증 방법이 부재하다는 문제점을 가지고 있

다.

[0029] 즉, Chien 등이 제안한 방식은 부인방지 속성을 만족하지 않는다. 유언장의 유효한 전자서명은 유언장이 실제 유언자에 의해서 생성되었음을 증명하며, 전송 중 유언이 변경되지 않았음을 증명한다. Chien 등이 제안한 방식에서 신뢰기관(TA)은 법원 등에 의해 수행된다고 가정되며, 제3의 신뢰 당사자(TTA, Trust Third Party)로 간주된다. 그러므로 신뢰기관(TA)은 사용자의 개인키(private key)를 알고 있다. 이러한 이유로 Chien 등이 제안한 방식에서 법원 등 신뢰기관(TA)은 유언자의 서명을 생성할 수 있게 된다.

[0030] 더군다나 어떤 국가에서도 Chien이 이용하는 ID 기반 전자 서명은 법적 효력을 가지지 않는다. 결과적으로 Chien 등이 제안한 방식은 전자서명법에 기반하여 법적 효력을 가지고 있지 않다.

[0031] 또한, Chien 등이 제안한 방식은 전자 서명에 대한 장기서명검증 방법을 제공하지 않는다. 이것은 만약 유언자가 죽은 후에 서명에 사용된 키의 유효기간의 초과하게 된다면, 유언자의 유언장의 유효성 검증이 어렵게 된다는 것을 의미한다.

[0032] 일반적으로 전자문서의 무결성은 전자서명에 의해서 보장된다. 하지만 전자서명의 검증은 인증서의 유효기간이 초과되었거나, 인증서가 폐기되었을 경우에는 불가능하게 된다.

발명의 내용

해결하려는 과제

[0033] 본 발명의 목적은 상술한 바와 같은 문제점을 해결하기 위한 것으로, 멀티미디어로 작성된 유언장을 인증기관에서 발급하는 인증서로 전자서명을 하여 부인방지 성질을 제공하는 인터넷 전자유언장 관리 시스템 및 방법을 제공하는 것이다.

[0034] 또, 본 발명의 목적은 전자서명된 유언장에 사용된 인증서의 만료일 이전에 전자서명된 유언장에 대한 타임스탬프를 획득하여 장기 보관하는 인터넷 전자유언장 관리 시스템 및 방법을 제공하는 것이다.

과제의 해결 수단

[0035] 상기 목적을 달성하기 위해 본 발명은 유언자 단말 및 유언집행자 단말과 네트워크로 연결된 유언장 관리서버에 의해, 인증기관에서 발급하는 인증서로 전자서명을 하여 유언장을 관리하는 인터넷 전자유언장 관리 방법에 관한 것으로서, (a) 상기 유언자 단말은 유언자의 인증서로 신청서 및 유언장을 전자서명하여 상기 관리서버로 전송하는 단계; (b) 상기 관리서버는 전자서명된 신청서 및 유언장을 수신하여 신청서 및 유언장의 전자서명을 검증하고 저장하는 단계; (c) 상기 관리서버는 유언자의 사망을 확인하는 단계; 및 (d) 유언자의 사망 확인후, 상기 관리서버는 상기 유언집행자 단말로 전자서명된 유언장을 전송하는 단계를 포함하는 것을 특징으로 한다.

[0036] 또한, 본 발명은 유언자 단말 및 유언집행자 단말과 네트워크로 연결된 유언장 관리서버에 의해, 인증기관에서 발급하는 인증서로 전자서명을 하여 유언장을 관리하는 인터넷 전자유언장 관리 방법에 관한 것으로서, (a) 상기 유언자 단말은 유언자의 인증서로 신청서 및 유언장을 전자서명하여 비밀키와 함께 상기 관리서버로 전송하되, 상기 유언장은 상기 비밀키로 암호화되는 단계; (b) 상기 관리서버는 전자서명된 신청서 및 유언장과, 비밀키를 수신하여 신청서 및 유언장의 전자서명을 검증하고 저장하는 단계; (c) 상기 관리서버는 유언자의 사망을 확인하는 단계; 및 (d) 유언자의 사망 확인후, 상기 관리서버는 상기 유언집행자 단말로 전자서명된 유언장 및 비밀키를 전송하는 단계를 포함하는 것을 특징으로 한다.

[0037] 또, 본 발명은 인터넷 전자유언장 관리 방법에 있어서, 상기 (a)단계에서, 상기 유언자 단말은 상기 관리서버의 공개키로 비밀키를 암호화하고, 상기 (d)단계에서, 상기 관리서버는 암호화된 비밀키를 자신의 개인키로 복호화하여 전송하는 것을 특징으로 한다.

[0038] 또, 본 발명은 인터넷 전자유언장 관리 방법에 있어서, 상기 방법은, (b2) 상기 (b)단계이후, 상기 관리서버는 상기 신청서에 상기 신청서의 전자서명을 포함시켜 자신의 인증서로 2차 전자서명을 하고, 2차 전자서명을 상기 유언자 단말로 전송하는 단계; 및 (b3) 상기 유언자 단말은 상기 2차 전자서명을 검증하는 단계를 더 포함하는 것을 특징으로 한다.

[0039] 또, 본 발명은 인터넷 전자유언장 관리 방법에 있어서, 상기 (c)단계에서, 상기 관리서버는 사망확인기관 서버로부터 전자서명된 사망확인서를 수신하고, 상기 사망확인서의 전자서명을 검증함으로써 유언자의 사망을 확인하는 것을 특징으로 한다.

[0040] 또, 본 발명은 인터넷 전자유언장 관리 방법에 있어서, 상기 (c)단계에서, 상기 전자서명된 사망확인서는 유언집행자 단말을 거쳐 전송되는 것을 특징으로 한다.

[0041] 또, 본 발명은 인터넷 전자유언장 관리 방법에 있어서, 상기 사망확인기관 서버가 의료기관 서버인 경우, 상기 전자서명된 사망확인서는 의사 및 병원의 인증서에 의해 전자서명된 유언자의 사망진단서인 것을 특징으로 한다.

[0042] 또, 본 발명은 인터넷 전자유언장 관리 방법에 있어서, 상기 전자서명된 유언자의 사망진단서는, 유언자의 사망진단서를 의사의 인증서에 의해 1차 전자서명하고 사망진단서에 1차 전자서명을 포함하여 의료기관의 인증서에 의해 2차 전자서명을 하여 생성되는 것을 특징으로 한다.

[0043] 또, 본 발명은 인터넷 전자유언장 관리 방법에 있어서, 상기 방법은, (b1) 상기 (b)단계이후, 상기 관리서버는 적어도 2명의 증인 단말에 전자서명된 신청서 및 유언장을 전송하는 단계; (b2) 상기 증인 단말은 증인의 인증서로 신청서 및 유언장에 2차 전자서명을 하여 상기 관리서버로 송신하는 단계; 및 (b3) 상기 관리서버는 상기 증인단말로부터 증인의 인증서에 의한 2차 전자서명을 수신하여 검증하는 단계를 더 포함하는 것을 특징으로 한다.

[0044] 또, 본 발명은 인터넷 전자유언장 관리 방법에 있어서, 상기 방법은, (b4) 상기 (b3)단계이후, 상기 관리서버는 신청서 및 유언장에 1차 전자서명 및 2차 전자서명을 포함시켜 자신의 인증서로 3차 전자서명을 하고, 2차 전자서명 및 3차 전자서명을 상기 유언자 단말로 전송하는 단계; 및 (b5) 상기 유언자 단말은 상기 3차 전자서명을 검증하는 것을 특징으로 한다.

[0045] 또, 본 발명은 인터넷 전자유언장 관리 방법에 있어서, 상기 방법은, (f) 상기 관리서버는 상기 유언자의 인증서 만료일 이전의 갱신기간이 도래하면, 타임스탬핑 기관(TSA)서버로부터 상기 신청서 및 유언장에 대한 타임스탬프 토큰을 획득하여, 상기 신청서 및 인증서에 추가하는 단계를 더 포함하되, 상기 (f)단계는 추가된 타임스탬프 토큰의 만료일 이전의 갱신기간이 도래하면, 타임스탬프 토큰을 재획득하는 것을 특징으로 한다.

[0046] 또한, 본 발명은 유언자 단말 및 유언집행자 단말과 네트워크로 연결되고, 인증기관에서 발급하는 인증서로 전자서명을 하여 유언장을 관리하는 인터넷 전자유언장 관리 시스템에 관한 것으로서, 상기 유언자 단말로부터 유언자의 인증서로 전자서명된 신청서 및 유언장을 수신하여 상기 신청서 및 유언장의 전자서명을 검증하고 저장하는 유언장 수신부; 유언자의 사망을 확인하는 사망확인 수신부; 및 유언자의 사망 확인후, 상기 유언집행자 단말로 전자서명된 유언장을 전송하는 유언장 전송부를 포함하는 것을 특징으로 한다.

[0047] 또한, 본 발명은 유언자 단말 및 유언집행자 단말과 네트워크로 연결되고, 인증기관에서 발급하는 인증서로 전자서명을 하여 유언장을 관리하는 인터넷 전자유언장 관리 시스템에 관한 것으로서, 상기 유언자 단말로부터 유언자의 인증서로 전자서명된 신청서 및 유언장, 그리고 비밀키를 수신하여, 상기 신청서 및 유언장의 전자서명을 검증하고 저장하되, 상기 유언장은 상기 비밀키로 암호화되는 유언장 수신부; 유언자의 사망을 확인하는 사망확인 수신부; 및 유언자의 사망 확인후, 상기 유언집행자 단말로 유언장 및 비밀키를 전송하는 유언장 전송부를 포함하는 것을 특징으로 한다.

[0048] 또, 본 발명은 인터넷 전자유언장 관리 시스템에 있어서, 상기 유언장 수신부는 시스템 자신의 공개키로 암호화된 비밀키를 수신하고, 상기 유언장 전송부는 암호화된 비밀키를 시스템 자신의 개인키로 복호화하여 전송하는 것을 특징으로 한다.

[0049] 또, 본 발명은 인터넷 전자유언장 관리 시스템에 있어서, 상기 유언장 수신부는, 전자서명이 검증되면, 신청서에 신청서의 전자서명을 포함시켜 시스템의 인증서로 2차 전자서명을 하고, 2차 전자서명을 상기 유언자 단말로 전송하되, 상기 2차 전자서명은 상기 유언자 단말에 의해 검증받는 것을 특징으로 한다.

[0050] 또, 본 발명은 인터넷 전자유언장 관리 시스템에 있어서, 상기 사망확인 수신부는 사망확인기관 서버로부터 전자서명된 사망확인서를 수신하고, 상기 사망확인서의 전자서명을 검증함으로써 유언자의 사망을 확인하는 것을 특징으로 한다.

[0051] 또, 본 발명은 인터넷 전자유언장 관리 시스템에 있어서, 상기 사망확인기관 서버가 의료기관 서버인 경우, 상기 전자서명된 사망확인서는 의사 및 병원의 인증서에 의해 전자서명된 유언자의 사망진단서인 것을 특징으로 한다.

[0052] 또, 본 발명은 인터넷 전자유언장 관리 시스템에 있어서, 상기 시스템은, 적어도 2명의 증인 단말에 전자서명된 신청서 및 유언장을 전송하고, 상기 증인 단말로부터 증인의 인증서에 의한 신청서 및 유언장의 2차 전자서명을 수신하고, 2차 전자서명을 검증하는 증인서명부를 더 포함하는 것을 특징으로 한다.

[0053] 또, 본 발명은 인터넷 전자유언장 관리 시스템에 있어서, 상기 시스템은, 상기 유언자의 인증서 만료일 이전의 갱신기간이 도래하면, 타임스탬핑 기관(TSA)서버로부터 상기 신청서 및 유언장에 대한 타임스탬프 토큰을 획득하여, 상기 신청서 및 인증서에 추가하는 장기검증부를 더 포함하되, 상기 장기검증부는 추가된 타임스탬프 토큰의 만료일 이전의 갱신기간이 도래하면, 타임스탬프 토큰을 재획득하는 것을 특징으로 한다.

발명의 효과

[0054] 상술한 바와 같이, 본 발명에 따른 인터넷 전자유언장 관리 시스템 및 방법에 의하면, 유언장은 유언자 인증서의 개인키로 전자서명이 되므로 유언자 자신만이 유효한 서명을 할 수 있기 때문에 유언장의 내용은 부인될 수 없는 효과가 얻어진다.

[0055] 또한, 본 발명에 따른 인터넷 전자유언장 관리 시스템 및 방법에 의하면, 유언장 관리기관이 유언장의 암호화를 위한 비밀키를 보유하고 인증기관(CA)이 유언장의 전자서명을 위한 인증서를 보유함으로써, 비밀키와 인증서(개인키)의 보관이 분리되어 유언장의 내용이 유언자가 사망하기 전까지 알 수 없게 되는 효과가 얻어진다.

[0056] 또한, 본 발명에 따른 인터넷 전자유언장 관리 시스템 및 방법에 의하면, 자필, 음성, 또는 동영상 등 멀티미디어 형식으로 작성된 유언장을 전자서명하여 관리함으로써, 유언자가 유언내용을 자신이 원하는 어떤 형태로도 작성할 수 있게 하는 효과가 얻어진다.

[0057] 또한, 본 발명에 따른 인터넷 전자유언장 관리 시스템 및 방법에 의하면, 전자서명된 유언장에 대하여 타임스탬프를 획득하여 장기 보관함으로써, 유언자가 사망한 후에 전자 서명을 장기간 검증할 수 있는 효과가 얻어진다.

도면의 간단한 설명

[0058] 도 1은 종래의 기술에 따른 인터넷 전자유언장 관리방법을 설명하는 흐름도이다.

도 2는 본 발명을 실시하기 위한 전체 시스템의 구성을 도시한 도면이다.

도 3은 본 발명의 제1 실시예에 따른 인터넷 전자유언장 관리방법을 설명하는 흐름도이다.

도 4는 본 발명의 제2 실시예에 따른 인터넷 전자유언장 관리방법을 설명하는 흐름도이다.

도 5는 도 3 또는 도 4의 표기에 대한 설명을 한 표이다.

도 6은 본 발명의 일실시예에 따른 인터넷 전자유언장 관리 시스템의 구성에 대한 블록도이다.

도 7은 본 발명에 따른 인터넷 전자유언자 관리 시스템 및 방법과 종래의 기술과의 효과를 비교한 대비표이다.

* 도면의 주요 부분에 대한 부호의 설명 *

11 : 유언자 단말	12 : 유언집행자 단말
13 : 증인 단말	20 : 네트워크
30 : 관리서버	31 : 유언장 수신부
32 : 사망확인 수신부	33 : 유언장 전송부
34 : 증인서명부	35 : 장기검증부
40 : 데이터베이스	41 : 유언장DB

42 : 비밀키DB

51 : 인증기관 서버　　52 : 타임스탬핑 서버

60 : 사망확인기관 서버

발명을 실시하기 위한 구체적인 내용

[0059] 이하, 본 발명의 실시를 위한 구체적인 내용을 도면에 따라서 설명한다.

[0060] 또한, 본 발명을 설명하는데 있어서 동일 부분은 동일 부호를 붙이고, 그 반복 설명은 생략한다.

[0061] 먼저, 본 발명을 실시하기 위한 전체 시스템의 구성의 일례에 대하여 도 2를 참조하여 설명한다.

[0062] 도 2에서 보는 바와 같이, 본 발명을 실시하기 위한 전체 시스템은 유언자 단말(11), 유언집행자 단말(12), 사망확인기관 서버(60), 유언장관리 서버(30), 인증기관 서버(51)로 구성된다. 또, 증인 단말(13), 타임스탬핑 기관서버(52)를 더 포함하여 구성될 수 있다. 상기 서버 또는 단말들은 모두 네트워크(20)로 연결된다.

[0063] 유언자 단말(11), 유언집행자 단말(12), 또는 증인 단말(13)은 유언자 또는 유언집행자가 이용하는 PC, 노트북, 넷북, PDA, 모바일 등의 통상의 컴퓨팅 단말기이다. 유언자, 유언집행자, 또는 증인은 상기 단말을 이용하여 유언장을 작성하거나, 수신하거나, 증언하는 등의 유언장 관련 작업을 수행한다. 이하에서 유언자, 유언집행자, 또는 증인의 도면부호를 상기 단말의 도면부호와 동일하게 사용한다. 즉, 유언자(11)가 어떤 작업을 수행한다는 것은 유언자 단말(11)을 통해 처리한다는 것을 의미한다.

[0064] 한편, 유언집행자(12)는 유언자의 상속인, 친척, 대리인 등 유언을 집행할 수 있는 사람들을 모두 포함한다.

[0065] 증인(13)은 유언장이 유언자(11)에 의해 작성되었음에 대한 증거를 제공하기 위해 유언자(11)에 의해서 임명된다. 영유아(Infants), 금치산자(interdicted persons), 상속인(heirs), 상속인의 배우자(the heirs' spouses), 상속인의 직계친척(heirs'lineal relatives by blood) 등은 증인이 될 수 없다.

[0066] 사망확인기관 서버(60), 유언장관리 서버(30), 인증기관 서버(51), 또는 타임스탬핑 서버(52)는 통상의 서버로서 네트워크(20)에 연결되고, 네트워크(20)를 통해 접속하는 단말들에 대하여 서비스를 제공하는 어플리케이션 서버이다. 상기 서버들은 웹 상에서 서비스를 제공하는 웹서버 또는 웹어플리케이션 서버도 해당된다.

[0067] 상기 서버는 각각 사망확인기관, 유언장관리기관, 인증기관, 타임스탬핑 기관 등에 의해 운영되고 상기 기관들의 서비스를 제공한다. 이하에서 상기 기관의 도면부호를 상기 서버의 도면부호와 동일하게 사용하고, 상기 기관이 제공하는 서비스에 관한 기재는 곧 상기 서버를 통해 제공되는 것을 의미한다.

[0068] 사망확인기관(60)은 유언자의 사망을 확인해주는 의료기관, 관공서 등의 기관들이다. 일반적으로 사람이 사망하는 경우에는 의료기관이 사망자에 대한 사망진단서를 발급하여 사망자의 사망을 확인해준다. 그러나 실종에 의한 사망선고나 재난 등에 의해 시신을 찾지 못하는 경우에는 관계기관이 사망을 확인시켜준다.

[0069] 사망확인기관(60)이 의료기관인 경우, 의료기관은 사망자에 대한 (전자)사망증명서를 가족 또는 친척에게 발급할 책임이 있다. 전자사망증명서는 이름, 성별, 생년월일, 혈액형, 사망일, 사망원인, 사망자에 대한 기타 정보를 포함하는 증명서이다. 이 전자문서는 의사(doctors (D))와 병원(hospital(H))에 의해서 서명 되어진다.

[0070] 인증기관(51)은 공개키 인증서 또는 인증서를 발급하는 통상의 인증기관(Certificate Authority)이다. 이 인증서는 해당 공개키가 특정 개인이나 단체, 서버에 속해 있음을 증명한다. 인증기관의 의무는 인증서에 대한 정보를 사용자에게 확인시켜 주는 것이다.

[0071] 인증기관(51)에 의한 인증서는 PKI(Public Key Infrastructure) 기반에 의해 수행된다. 즉, 해당 인증서를 발급한 인증기관(6)으로부터 OCSP(Online Certificate Status Protocol: 온라인 인증서 상태 프로토콜), CRL(Certificate Revocation List: 인증서 폐지목록) 또는 ARL(Authority Revocation List: 인증기관의 인증서 폐지목록) 등의 인증서 상태확인정보를 전송받아 그 유효성이 검증된다.

[0072] 타임스탬핑 기관(TSA, Time Stamping Authority)(52)은 전자문서에 대한 타임스탬프 토큰을 생성한다. 이 타임스탬프 토큰은 해당 전자문서의 해쉬값과 시간소스를 포함하며, TSA의 인증서 서명이 첨부된다. 결국 전자문서의 유효성 검증 가능기간은 TSA의 인증서 유효기간만큼 늘어날 수 있게 된다. 이 유효기간은 TSA의 인증서 만료 전에 새로운 타임스탬프 토큰을 추가 생성함으로써 갱신될 수 있다. IETF(Internet Engineering Task Force)

RFC3126은 이와 같이 전자문서의 유효성 검증 가능기간을 적절하게 연장시키는 방법을 제시하고 있다.

[0073] 유언장 관리서버(30)는 법원 등 유언장을 관리하는 기관의 서버로서, 작성된 유언장을 보관하거나 열람시켜주는 등의 유언장 관리 서비스를 제공한다.

[0074] 다음으로, 본 발명의 제1 실시예에 따른 인터넷 전자유언장 관리 방법을 도 3을 참조하여 설명한다. 도 3은 본 발명의 제1 실시예에 따른 인터넷 전자유언장 관리 방법을 설명하는 흐름도이고, 도 3에 표시된 표기법은 도 5와 같다.

[0075] 도 3에서 보는 바와 같이, 본 발명의 제1 실시예에 따른 인터넷 전자유언장 관리 방법은 등록 단계, 유언장 생성 단계, 사망진단서 발급 및 제출 단계, 및 유언장 공개 단계로 구성된다.

[0076] ① 등록단계(Registration phase)

[0077] 향상된 전자 유언장 시스템은 전자서명을 사용한다. 각 시스템 구성요소들(A, C, H, D)은 공개키(public key) pk_i와 개인키(private key) sk_i를 생성하고, 인증서를 발급 받는다. 예를 들어, 유언자는 CA에 등록을 하고, 인증서 $Cert_A$ 를 발급받는다. 이때 인증서에는 공개키(public key)가 포함되어 있다.

[0078] 관리서버(C), 의사(D), 그리고 병원(H)은 인증기관(CA)로부터 인증서를 요청하고, 인증서에 공개키(public key)를 포함하여 받는다. 따라서 각각의 프로토콜 참여자들은 인증서를 가지게 된다. 개인키(private key)의 경우에는 Personal Identification Number (PIN)에 의해 보호된다고 가정한다.

[0079] ② 유언장 생성 단계(Creating a living will)

[0080] 유언자 단말은 유언자의 인증서로 신청서 및 유언장을 전자서명하여 상기 관리서버로 전송한다(S10).

[0081] 유언자(A)(또는 유언자 단말 11)는 유언장 (M)과 신청서(L)를 작성한다(S11). 유언장이 작성되고, 날짜를 명시한 다음, 유언자 A는 유언장(M)과 신청서(L)에 전자서명을 한다(S12). 마지막으로, 유언자(A)는 유언장과 신청서를 관리서버(C)에 전송한다(S13).

[0082] 유언장(M)은 전자문서로 작성되거나, 멀티미디어 데이터로 작성된다. 멀티미디어 데이터 자체가 유언장(M)이 될 수도 있다. 또는 유언장(M)은 전자문서로 작성되고 상기 전자문서에 멀티미디어 데이터를 첨부할 수 있다. 멀티미디어 데이터는 음성 데이터, 동영상 데이터, 이미지 데이터 등을 포함한다.

[0083] 음성 데이터는 유언자가 자신의 유언 내용을 음성으로 녹음한 데이터이다. 음성 데이터는 마이크 등 음성녹음장치를 통해 녹음되어 파일 형태로 저장된다. 동영상 데이터는 유언자가 자신의 유언 내용을 음성으로 말하거나 행동을 취하는 것을 영상으로 녹화한 데이터이다. 동영상 데이터는 캠코더, 카메라 또는 웹카메라 등 영상녹화장치를 통해 녹화되어 파일 형태로 저장된다. 이미지 데이터는 유언자가 자신의 유언 내용을 자필로 필기 용지에 쓴 것, 또는 자신의 유언 내용에 유언자의 자필 사인이나 지장, 인감 등 날인한 것 등을 이미지로 변환한 데이터이다. 이미지 데이터는 카메라, 스캐너 등 이미지 장치를 통해 이미지 파일로 저장된다.

[0084] 상기 멀티미디어는 음성 데이터, 동영상 데이터, 이미지 데이터 중 하나로 작성되거나 2개 이상으로 작성될 수 있다. 따라서 유언장(M)은 전자문서, 음성 데이터, 동영상 데이터, 이미지 데이터 중 하나로 작성되거나 2개 이상으로 작성될 수 있다.

[0085] 유언장(M)은 상기 전자문서 또는 데이터로 구성된 전체 데이터를 하나의 디지털 데이터 또는 디지털 문서로 간주된다. 유언장(M)은 하나의 전자문서로서 전자서명되고 관리된다. 이하에서 유언장(M)을 하나의 문서 또는 전자문서로도 기재하더라도, 유언장의 데이터 형식이 전자문서로 한정된 것이 아니다.

[0086] 상기와 같이, 유언자는 자신이 편리한 방식으로 어느 형태라도 선택하여 유언을 할 수 있다. 특히, 대부분의 유언자는 나이가 많거나 몸이 불편한 경우가 많기 때문에, 전자문서 방식 보다 음성, 동영상, 자필 유언을 더 선호한다.

[0087] 관리서버(30)는 전자서명된 신청서 및 유언장을 수신하여 신청서 및 유언장의 전자서명을 검증하고 저장한다(S20).

[0088] 즉, 관리서버(C)는 전자서명된 유언장(M)과 전자서명된 신청서(L)를 검증한다(S20). 만약 서명에 대한 검증이 성공한다면, 관리서버(C)는 신청서(L)에 전자서명을 하고, 공문서(L")를 유언자에게 확인용으로 제공한다(S22).

다시 말하면, 관리서버는 신청서에 상기 신청서의 전자서명을 포함시켜 자신의 인증서로 2차 전자서명을 하고, 2차 전자서명을 상기 유언자 단말로 전송한다.

[0089] 유언자 단말은 상기 2차 전자서명을 검증한다(S23).

[0090] ③ 친척에게 사망진단서(DC)발급

[0091] 사망확인기관 서버(60)는 사망확인서를 전자서명하여 관리서버(30)로 전송한다. 이때, 전자서명된 사망확인서는 유언집행자 단말(12)을 거쳐 전송될 수 있다. 사망확인기관 서버가 병원 등 의료기관 서버인 경우, 전자서명된 사망확인서는 의사 및 병원의 인증서에 의해 전자서명된 유언자의 사망진단서이다.

[0092] 즉, 유언자가 사망한 후, 의사는 사망 원인을 진단하고, 전자사망진단서(DC)를 친척들(R)에게 발급한다(S30). 사망진단서에는 의사의 전자서명(S^D)과 병원의 전자서명 (S^H)이 포함된다. 병원은 사망진단서(DC)와 S^D, S^H를 유언자(A)의 친척에게 전송한다(S32).

[0093] 다시 말하면, 전자서명된 유언자의 사망진단서는, 유언자의 사망진단서를 의사의 인증서에 의해 1차 전자서명하고 사망진단서에 1차 전자서명을 포함하여 의료기관(또는 병원)의 인증서에 의해 2차 전자서명을 하여 생성된다.

[0094] 친척(또는 유언집행자)은 병원으로부터 받은 전자사망진단서와 의사 및 병원의 서명 $\{DC,S^D,S^H\}$을 관리서버에 제출한다(S33).

[0095] 친척은 전자사망진단서 제출과 함께 유언장의 공개를 요청할 수 있다.

[0096] ④ 관리서버의 전자사망진단서(DC) 인증

[0097] 관리서버(C)는 전자사망진단서와 의사 및 병원의 서명 $\{DC,S^D,S^H\}$을 검증한다(S40). 검증 방법은 다음과 같다.

[0098] $Vrfy_{pkD}$ ($\{S^D\}$,DC)) and $Vrfy_{pkH}$ ($\{S^H\}$,(DC,S^D))).

[0099] 만약 전자사망진단서(DC)와 그에 대한 전자서명들이 제대로 검증된다면, 다음 단계를 수행한다.

[0100] ⑤ 관리서버가 유언장 공개

[0101] 관리서버는 유언장(M)과 유언장에 대한 유언자의 전자서명(SA)을 유언자의 친척에게 전송한다(S50).

[0102]

[0103] 다음으로, 본 발명의 제2 실시예에 따른 인터넷 전자유언장 관리 방법을 도 4를 참조하여 설명한다. 도 4는 본 발명의 제2 실시예에 따른 인터넷 전자유언장 관리 방법을 설명하는 흐름도이고, 도 4에 표시된 표기법은 도 5와 같다.

[0104] ① 등록단계(Registration phase)

[0105] 앞에서 설명한 제1 실시예와 동일하다.

[0106] ② 유언장 생성 단계(Creating a living will)

[0107] 유언자 단말(11)은 유언자의 인증서로 신청서 및 유언장을 전자서명하여 비밀키와 함께 상기 관리서버(30)로 전송하되, 상기 유언장은 상기 비밀키로 암호화된다.

[0108] 즉, 유언자(A)는 신청서(L)를 작성하고, 유언장의 내용을 암호화하기 위해 대칭키(symmetric key) k를 사용하여 암호화한 후 암호화된 유언장(sealed will) (C)을 얻는다. 대칭키(The symmetric key) k는 공개키 암호화 알고리즘을 이용하여 관리서버의 공개키 (pk_C)로 암호화된다.

[0109] 유언장(M)은 전자문서로 작성되거나, 멀티미디어 데이터로 작성된다. 멀티미디어 데이터 자체가 유언장(M)이 될 수도 있다. 또는 유언장(M)은 전자문서로 작성되고 상기 전자문서에 멀티미디어 데이터를 첨부할 수 있다. 멀티미디어 데이터는 음성 데이터, 동영상 데이터, 이미지 데이터 등을 포함한다.

[0110] 음성 데이터는 유언자가 자신의 유언 내용을 음성으로 녹음한 데이터이다. 음성 데이터는 마이크 등 음성녹음장치를 통해 녹음되어 파일 형태로 저장된다. 동영상 데이터는 유언자가 자신의 유언 내용을 음성으로 말하거나 행동을 취하는 것을 영상으로 녹화한 데이터이다. 동영상 데이터는 캠코더, 카메라 또는 웹카메라 등 영상녹화

장치를 통해 녹화되어 파일 형태로 저장된다. 이미지 데이터는 유언자가 자신의 유언 내용을 자필로 필기 용지에 쓴 것, 또는 자신의 유언 내용에 유언자의 자필 사인이나 지장, 인감 등 날인한 것 등을 이미지로 변환한 데이터이다.

[0111] 이미지 데이터는 카메라, 스캐너 등 이미지 장치를 통해 이미지 파일로 저장된다.

[0112] 상기 멀티미디어는 음성 데이터, 동영상 데이터, 이미지 데이터 중 하나로 작성되거나 2개 이상으로 작성될 수 있다. 따라서 유언장(M)은 전자문서, 음성 데이터, 동영상 데이터, 이미지 데이터 중 하나로 작성되거나 2개 이상으로 작성될 수 있다.

[0113] 유언장(M)은 상기 전자문서 또는 데이터로 구성된 전체 데이터를 하나의 디지털 데이터 또는 디지털 문서로 간주된다. 유언장(M)은 하나의 전자문서로서 전자서명되고 관리된다. 이하에서 유언장(M)을 하나의 문서 또는 전자문서로도 기재하더라도, 유언장의 데이터 형식이 전자문서로 한정된 것이 아니다.

[0114] 다음, 유언자(A)는 신청서(L)와 암호화된 유언장(C)을 전자서명한다. 유언자는 암호화된 유언장(C)과 암호화된 대칭키 (Enc_{pkC} (k)),그리고 신청서(L)를 관리서버(C)에 전송한다(S12).

[0115] 관리서버는 유언자의 전자서명이 제대로 포함되었는지를 검증한다(S21b).

[0116] 그 다음, 유언자를 제외한 유언자에 의해 지명된 둘 이상의 증인 (X,Y)에게 암호화된 유언장(C)과 신청서(L)를 전송하여 전자서명을 받아야 한다. 관리서버는 증인으로부터 암호화된 유언장(C)과 신청서(L)를 받으면(S23b), 유언자(A)에 의해 작성된 유언장(C)과 신청서(L)에 2명의 증인 (X,Y)으로부터 적절하게 서명되었는지를 검증한다(S25b).

[0117] 즉, 관리서버(30)는 적어도 2명의 증인 단말(13)에 전자서명된 신청서 및 유언장을 전송하고(S22b), 증인 단말(13)은 증인의 인증서로 신청서 및 유언장에 2차 전자서명을 하여(S23b) 상기 관리서버로 송신한다(S24b). 그리고 관리서버(30)는 증인단말(13)로부터 증인의 인증서에 의한 2차 전자서명을 수신하여 검증한다(S25b).

[0118] 그리고 관리서버는 신청서 및 유언장에 1차 전자서명 및 2차 전자서명을 포함시켜 자신의 인증서로 3차 전자서명을 하고, 2차 전자서명 및 3차 전자서명을 상기 유언자 단말로 전송한다(S27b). 그리고 유언자 단말(11)은 상기 3차 전자서명을 검증한다(S28b).

[0119] ③ 친척에게 사망진단서(DC)발급

[0120] 유언자가 사망한 후, 의사는 사망 원인을 진단하고, 전자사망진단서(DC)를 친척들(R)에게 발급한다. 사망진단서에는 의사의 전자서명 (S^D)과 병원의 전자서명 (S^H)이 포함된다(S30). 병원은 사망진단서(DC)와 S^D, S^H를 유언자(A)의 친척에게 전송한다(S32).

[0121] 친척은 병원으로부터 받은 전자사망진단서와 의사 및 병원의 서명 {DC,S^D,S^H}을 관리서버에 제출하고(S33), 유언장의 공개를 요청한다.

[0122] ④ 관리서버의 전자사망진단서(DC) 인증

[0123] 관리서버(C)는 전자사망진단서와 의사 및 병원의 서명 {DC,S^D,S^H}을 검증한다(S40). 검증 방법은 다음과 같다 :

[0124] $Vrfy_{pkD}$ ({S^D},DC)) and $Vrfy_{pkH}$ ({S^H},(DC,S^D))).

[0125] 만약 전자사망진단서(DC)와 그에 대한 전자서명들이 제대로 검증된다면, 다음 단계를 수행한다.

[0126] ⑤ 관리서버가 유언장 공개 : 관리서버는 암호화된 대칭키 k를 복호화하기 개인키(private key) sk_C 를 사용한다(S51). 암호화된 유언장(C)을 k를 이용하여 복호화한 다음 유언장 내용(m)과 전자서명 위해서 유언장(M)과 유언장 내용에 대한 유언자의 전자서명(S^A), 그리고 관리서버의 공개키(pk_C)를 유언자의 친척에게 전송한다(S50).

[0127] 다음으로, 본 발명의 일실시예 따른 인터넷 전자유언장 관리 시스템의 구성을 도 6을 참조하여 설명한다.

[0128] 본 발명의 일실시예 따른 인터넷 전자유언장 관리 시스템은 유언자 단말(11), 유언집행자 단말(12), 및 사망확인기관(60)과 네트워크(20)로 연결된 유언장 관리서버(30)를 의미한다.

[0129] 도 6에서 보는 바와 같이, 일실시예 따른 인터넷 전자유언장 관리 시스템은 유언장 수신부(31), 사망확인 수신부(32), 및 유언장 전송부(33)로 구성된다. 추가적으로, 증인서명부(34), 장기검증부(35)를 더 포함하여 구성될 수 있다.

[0130] 제1 실시예로서, 유언장 수신부(31)는 유언자 단말(11)로부터 유언자의 인증서로 전자서명된 신청서 및 유언장을 수신하여 상기 신청서 및 유언장의 전자서명을 검증하고 저장한다.

[0131] 제2 실시예로서, 유언장 수신부(31)는 유언자 단말(11)로부터 유언자의 인증서로 전자서명된 신청서 및 유언장, 그리고 비밀키를 수신하여, 상기 신청서 및 유언장의 전자서명을 검증하고 저장하되, 상기 유언장은 상기 비밀키로 암호화된다. 특히, 유언장 수신부(31)는 시스템 자신의 공개키로 암호화된 비밀키를 수신한다.

[0132] 한편, 유언장 수신부(31)는 전자서명이 검증되면, 신청서에 신청서의 전자서명을 포함시켜 시스템의 인증서로 2차 전자서명을 하고, 2차 전자서명을 상기 유언자 단말로 전송하되, 상기 2차 전자서명은 상기 유언자 단말(11)에 의해 검증받는다.

[0133] 사망확인 수신부(32)는 사망확인기관 서버(60)로부터 전자서명된 사망확인서를 수신하여 상기 사망확인서의 전자서명을 검증한다.

[0134] 한편, 사망확인기관 서버(60)가 의료기관 서버인 경우, 상기 전자서명된 사망확인서는 의사 및 병원의 인증서에 의해 전자서명된 유언자의 사망진단서이다.

[0135] 유언장 전송부(33)는 사망확인서를 수신한 후 유언집행자 단말(12)로부터 유언장 열람 신청을 수신하면, 전자서명된 유언장을 전송한다.

[0136] 제2 실시예로서, 유언장 전송부(33)는 비밀키를 더 포함하여 전송한다. 특히, 유언장 전송부(33)는 암호화된 비밀키를 시스템 자신의 개인키로 복호화하여 전송한다.

[0137] 증인서명부(34)는 적어도 2명의 증인 단말(13)에 전자서명된 신청서 및 유언장을 전송하고, 상기 증인 단말(13)로부터 증인의 인증서에 의한 신청서 및 유언장의 2차 전자서명을 수신하고, 2차 전자서명을 검증한다.

[0138] 장기검증부(31)는 유언자의 인증서 만료일 이전의 갱신기간이 도래하면, 타임스탬핑 기관(TSA)서버(52)로부터 상기 신청서 및 유언장에 대한 타임스탬프 토큰을 획득하여, 상기 신청서 및 인증서에 추가한다. 또한, 장기검증부(31)는 추가된 타임스탬프 토큰의 만료일 이전의 갱신기간이 도래하면, 타임스탬프 토큰을 재획득한다.

[0139] 상기 인터넷 전자유언장 관리 시스템 중 생략된 부분은 앞서 설명한 인터넷 전자유언장 관리 방법의 설명을 참조한다.

[0140] 다음으로, 본 발명의 일실시예에 따른 유언장의 전자서명에 대한 장기서명 검증에 대하여 구체적으로 설명한다.

[0141] 본 발명에 따른 인터넷 전자유언장 관리 시스템 및 방법의 안전성은 전자적으로 작성된 유언장 및 신청서에 작성된 전자서명의 안전성에 기반한다. 일반적으로 전자 문서의 무결성은 전자서명에 의해서 보장된다. 하지만, 장기간의 시간이 지난 후 전자서명의 신뢰성은 절대적으로 보장되기 어렵다. 오랜 시간이 지난 후에, 해쉬 알고리즘이나 공개키 알고리즘은 취약해질 수 있으며, 인증서가 유효하지 않을 수 있다. 이러한 문제를 해결하기 위해서는 전자서명에 대한 장기서명검증방법이 요구된다.

[0142] 이러한 전자서명에 대하여 장기서명검증이 가능하도록 하기 위해서는 전자적으로 서명된 데이터가 인증서가 유효하지 않게 되기 전에 이미 존재하였음을 증명하는 것이 필수적이다. 이것은 타임스탬프에 의해 증명될 수 있다. 하지만, 타임스탬프 또한 전자서명과 같이 동일한 문제를 가지고 있다. 이러한 문제를 해결하기 위해, 타임스탬프는 기존 타임스탬프가 유효성을 잃기 전에, 새로운 타임스탬프를 얻어야 하는데, 이때 기존 원본 데이터와 그에 대한 타임스탬프를 포함하여 다시 갱신되어야 한다.

[0143] 즉, 관리서버(30)는 상기 유언자의 인증서 만료일 이전의 갱신기간이 도래하면, 타임스탬핑 기관(TSA)서버(52)로부터 상기 신청서 및 유언장에 대한 타임스탬프 토큰을 획득하여, 상기 신청서 및 인증서에 추가한다. 그리

고 추가된 타임스탬프 토큰의 만료일 이전의 갱신기간이 도래하면, 타임스탬프 토큰을 재획득한다.

[0144] 본 발명에 따른 인터넷 전자유언장 관리 시스템 및 방법의 효과를 도 7을 참조하여 보다 구체적으로 부연한다.

[0145] 본 발명에 따른 인터넷 전자유언장 관리 시스템 및 방법은 부인방지(Non-repudiation), 사전공개의 방지(Prevention of Pre-reveal), 장기서명검증(Long-term validation)의 측면에서 다음과 같은 효과가 있다.

[0146] 부인방지 보안 요구사항을 만족하기 위해서, 유언장의 내용은 부인될 수 없어야 한다. 인터넷 전자유언장 관리 시스템 및 방법에서, 유언장은 실제 유언자에 의해서만 생성 및 수정될 수 있어야 한다. 기존 Chien등이 제안한 방식의 경우에, TA가 유언자의 개인키(private key)를 쉽게 계산할 수 있거나, 알 수 있었다. 따라서, TA는 유언자와 증인의 전자서명을 생성할 수 있었다. 이것은 TA가 유언장을 위조할 수 있음을 의미한다. 그러나 본 발명은 단지 유언자만의 자신의 개인키를 가지고 있기 때문에, 유언자 자신만이 유효한 서명을 생성할 수 있다. 또한 어떤 누구도 유언자가 사망한 후, 유언장의 내용을 수정할 수 없다. 뿐만 아니라, 공개적으로 가능한 파라미터를 통하여 유언장의 전자서명을 검증할 수 있다. 따라서 본 발명은 부인방지 속성을 만족한다.

[0147] 봉인 전자 유언장 시스템에서 유언장 사전공개 방지 요구사항에 따라서, 유언자가 사망하고, 병원이 사망증명서를 발급하기 전까지는 유언장의 내용이 다른 사람에게 알려지면 안 된다. ID 기반 암호시스템을 사용하는 Chien 등이 제안하는 방식에서는 TA가 관리서버의 개인키(private key)를 알고 있다. 따라서 TA는 암호화된 유언장을 복호화할 수 있다. 결과적으로, Chien 등이 제안한 방식은 사전 공개 방지 속성을 제공하지 않는다. 하지만, 본 발명에 따른 방식은 공개키 기반 구조(PKI)에 기반하고 있으므로, CA와 관리서버가 분리되어 있다. 이것은 다시 말하면, 관리서버를 제외한 어떤 누구도 암호화된 유언장을 복호화할 수 없으므로, 유언자가 사망하기 전까지는 유언장의 내용을 알 수 없음을 의미한다. 따라서 본 발명은 사전 공개 방지 속성을 만족한다.

[0148] 오랜 시간이 흐르면, 해시(Hash) 알고리즘과 공개키 알고리즘은 취약해 질 수 있으며, 인증서는 유효하지 않게 될 수 있다. 그러므로 전자 유언장 시스템은 유언자가 사망한 후에 전자 서명을 장기간 검증할 수 있는 방법을 필요로 한다. 본 발명에서는 유언장에 대한 전자서명 장기 검증 방안을 제시하였다. 따라서 본 발명은 장기서명 검증 요구사항을 만족한다.

[0149]

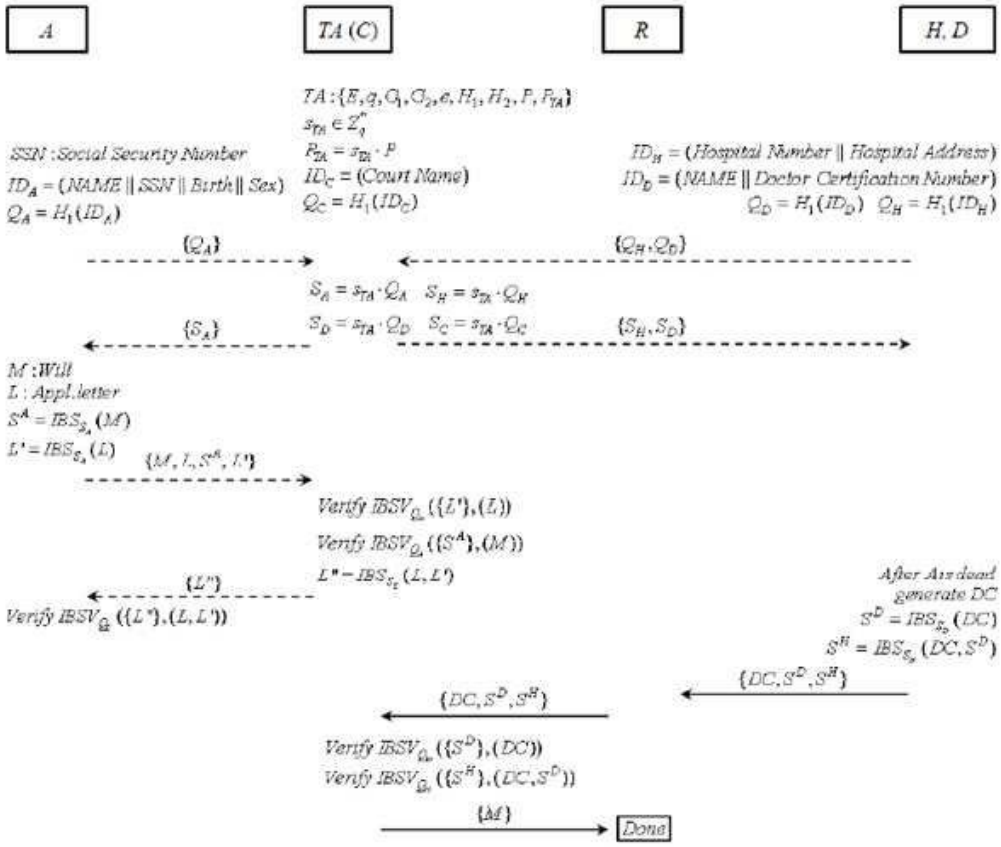
[0150] 이상, 본 발명자에 의해서 이루어진 발명을 상기 실시 예에 따라 구체적으로 설명하였지만, 본 발명은 상기 실시 예에 한정되는 것은 아니고, 그 요지를 이탈하지 않는 범위에서 여러 가지로 변경 가능한 것은 물론이다.

산업상 이용가능성

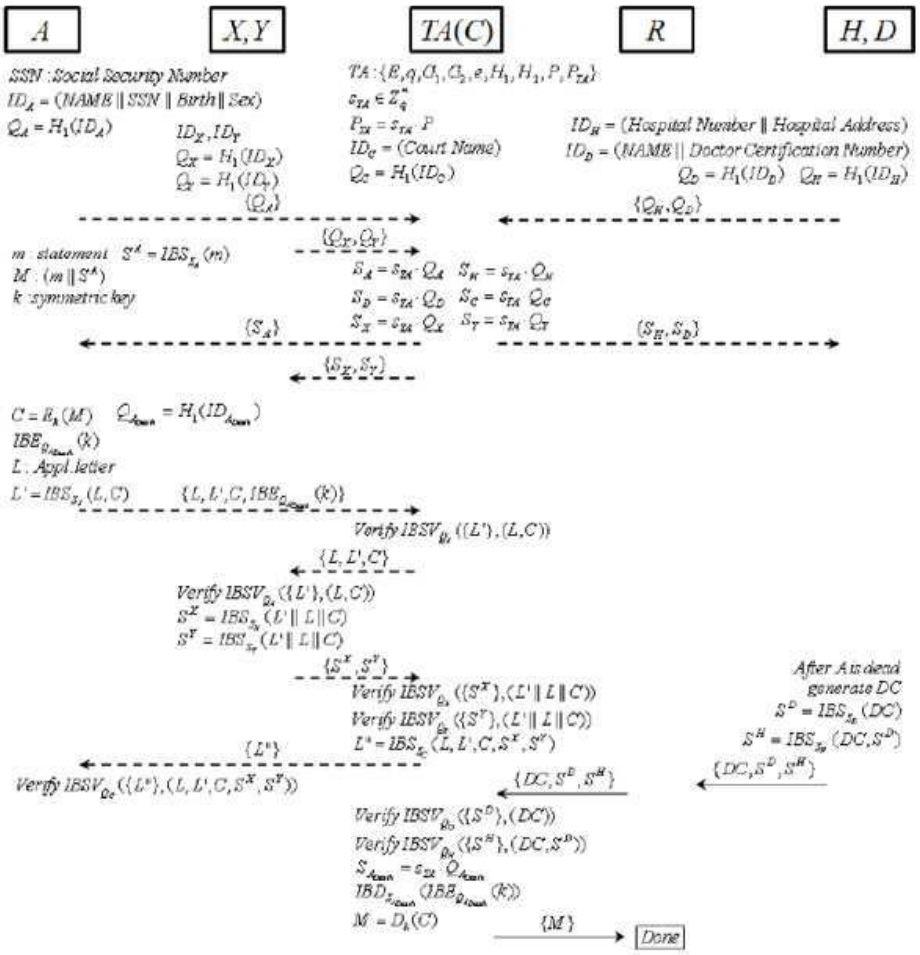
[0151] 본 발명은 멀티미디어로 작성된 유언장을 인증기관에서 발급하는 인증서로 전자서명을 하여 부인방지 성질을 제공하는 인터넷 전자유언장 관리 시스템 및 방법을 개발하는 데 적용이 가능하다. 특히, 본 발명은 전자서명된 유언장에 사용된 인증서의 만료일 이전에 전자서명된 유언장에 대한 타임스탬프를 획득하여 장기 보관하는 인터넷 전자유언장 관리 시스템을 개발하는 데 유용하다.

도면

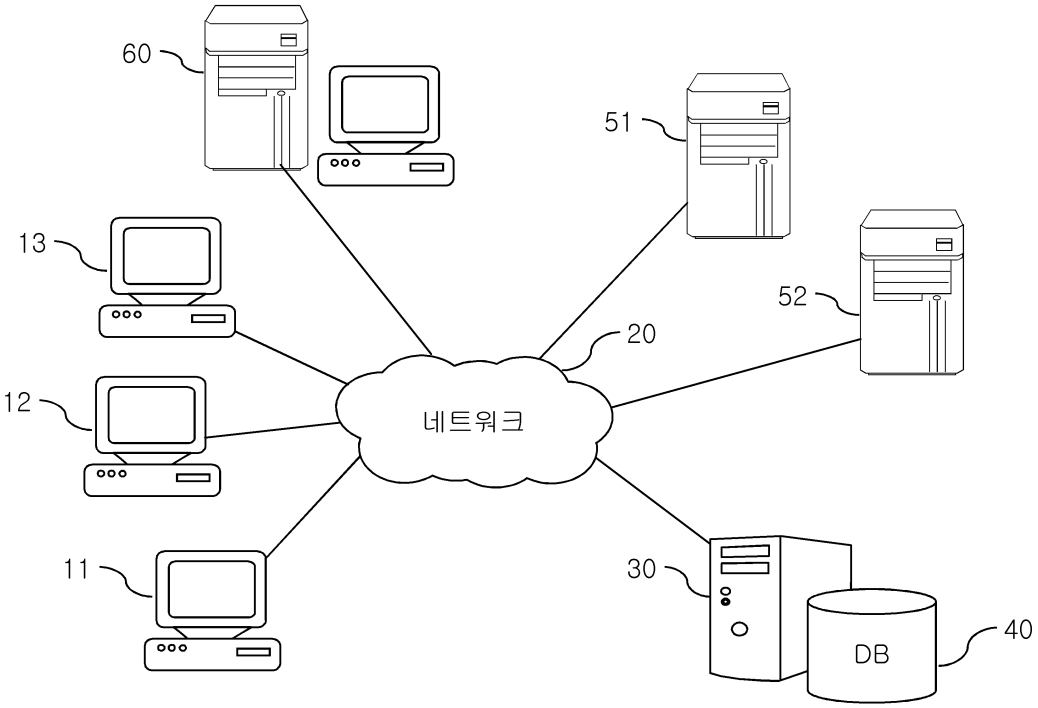
도면1a


A
TA (C)
R
H, D
TA : {E, q, G1, G2, e, H1, H2, P, PTA}
sTA ∈ Z*q
PTA = sTA · P
IDC = (Court Name)
QC = H1(IDC)
SSN : Social Security Number
IDA = (NAME || SSN || Birth || Sex)
QA = H1(IDA)
IDH = (Hospital Number || Hospital Address)
IDD = (NAME || Doctor Certification Number)
QD = H1(IDD) QH = H1(IDH)
{QA}
{QH, QD}
SA = sTA · QA SH = sTA · QH
SD = sTA · QD SC = sTA · QC
{SA}
{SH, SD}
M : Will
L : Appl.letter
SA = IBSSA (M)
L' = IBSSA (L)
{M, L, SA, L'}
Verify IBSVQA ({L'}, (L))
Verify IBSVQA ({SA}, (M))
L" = IBSSC (L, L')
{L"}
Verify IBSVQA ({L"}, (L, L'))
After Assisted
generate DC
SD = IBSSD (DC)
SH = IBSSH (DC, SD)
{DC, SD, SH}
{DC, SD, SH}
Verify IBSVQA ({SD}, (DC))
Verify IBSVQA ({SH}, (DC, SD))
{M}
Done

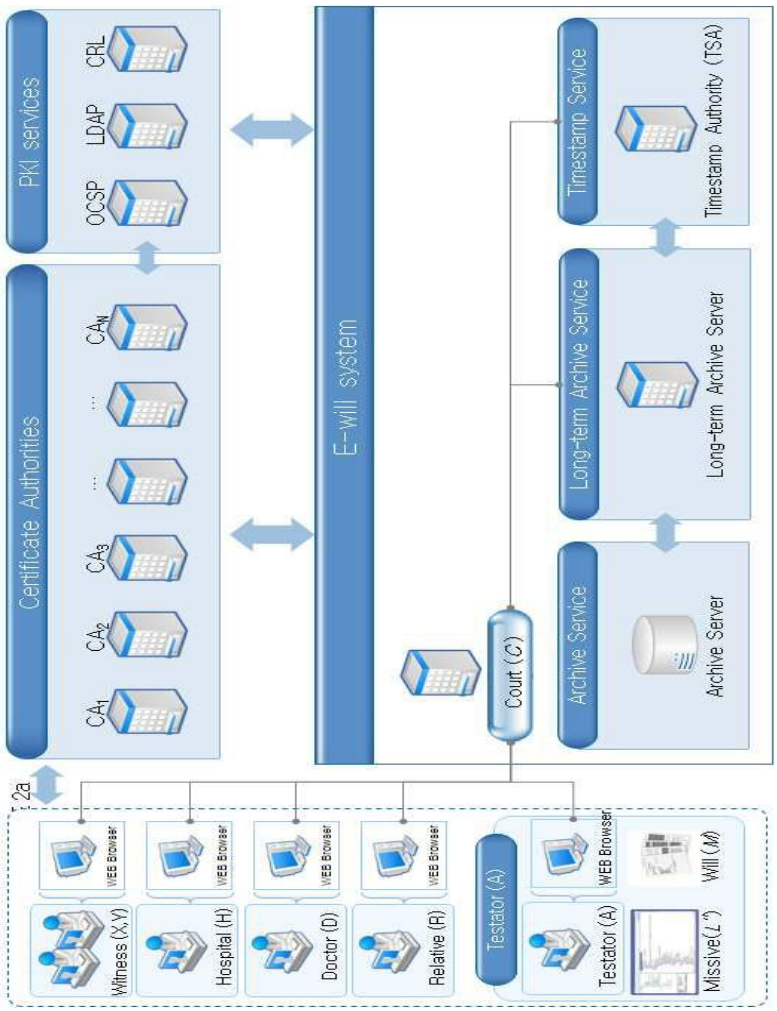
도면1b


A
X,Y
TA(C)
R
H,D
SSN : Social Security Number
$ID_A = (NAME \| SSN \| Birth \| Sex)$
$Q_A = H_1(ID_A)$
ID_X, ID_Y
$Q_X = H_1(ID_X)$
$Q_Y = H_1(ID_Y)$
$\{Q_A\}$
$TA : \{E, q, G_1, G_2, e, H_1, H_2, P, P_{TA}\}$
$s_{TA} \in Z_q^*$
$P_{TA} = s_{TA} \cdot P$
$ID_C = (Court\ Name)$
$Q_C = H_1(ID_C)$
$ID_H = (Hospital\ Number \| Hospital\ Address)$
$ID_D = (NAME \| Doctor\ Certification\ Number)$
$Q_D = H_1(ID_D)$ $Q_H = H_1(ID_H)$
$\{Q_H, Q_D\}$
$\{Q_X, Q_Y\}$
m : statement $S^A = IBS_{S_A}(m)$
M : $(m \| S^A)$
k : symmetric key
$S_A = s_{TA} \cdot Q_A$ $S_H = s_{TA} \cdot Q_H$
$S_D = s_{TA} \cdot Q_D$ $S_C = s_{TA} \cdot Q_C$
$S_X = s_{TA} \cdot Q_X$ $S_Y = s_{TA} \cdot Q_Y$
$\{S_A\}$
$\{S_H, S_D\}$
$\{S_X, S_Y\}$
$C = E_k(M)$ $Q_{A_{com}} = H_1(ID_{A_{com}})$
$IBE_{Q_{A_{com}}}(k)$
L : Appl.letter
$L' = IBS_{S_A}(L, C)$
$\{L, L', C, IBE_{Q_{A_{com}}}(k)\}$
$Verify\ IBSV_{Q_A}(\{L'\}, (L, C))$
$\{L, L', C\}$
$Verify\ IBSV_{Q_A}(\{L'\}, (L, C))$
$S^X = IBS_{S_X}(L' \| L \| C)$
$S^Y = IBS_{S_Y}(L' \| L \| C)$
$\{S^X, S^Y\}$
$Verify\ IBSV_{Q_X}(\{S^X\}, (L' \| L \| C))$
$Verify\ IBSV_{Q_Y}(\{S^Y\}, (L' \| L \| C))$
$L^* = IBS_{S_C}(L, L', C, S^X, S^Y)$
$\{L^*\}$
$Verify\ IBSV_{Q_C}(\{L^*\}, (L, L', C, S^X, S^Y))$
After A is dead generate DC
$S^D = IBS_{S_D}(DC)$
$S^H = IBS_{S_H}(DC, S^D)$
$\{DC, S^D, S^H\}$
$\{DC, S^D, S^H\}$
$Verify\ IBSV_{Q_D}(\{S^D\}, (DC))$
$Verify\ IBSV_{Q_H}(\{S^H\}, (DC, S^D))$
$S_{A_{com}} = s_{TA} \cdot Q_{A_{com}}$
$IBD_{S_{A_{com}}}(IBE_{Q_{A_{com}}}(k))$
$M = D_k(C)$
$\{M\}$
Done

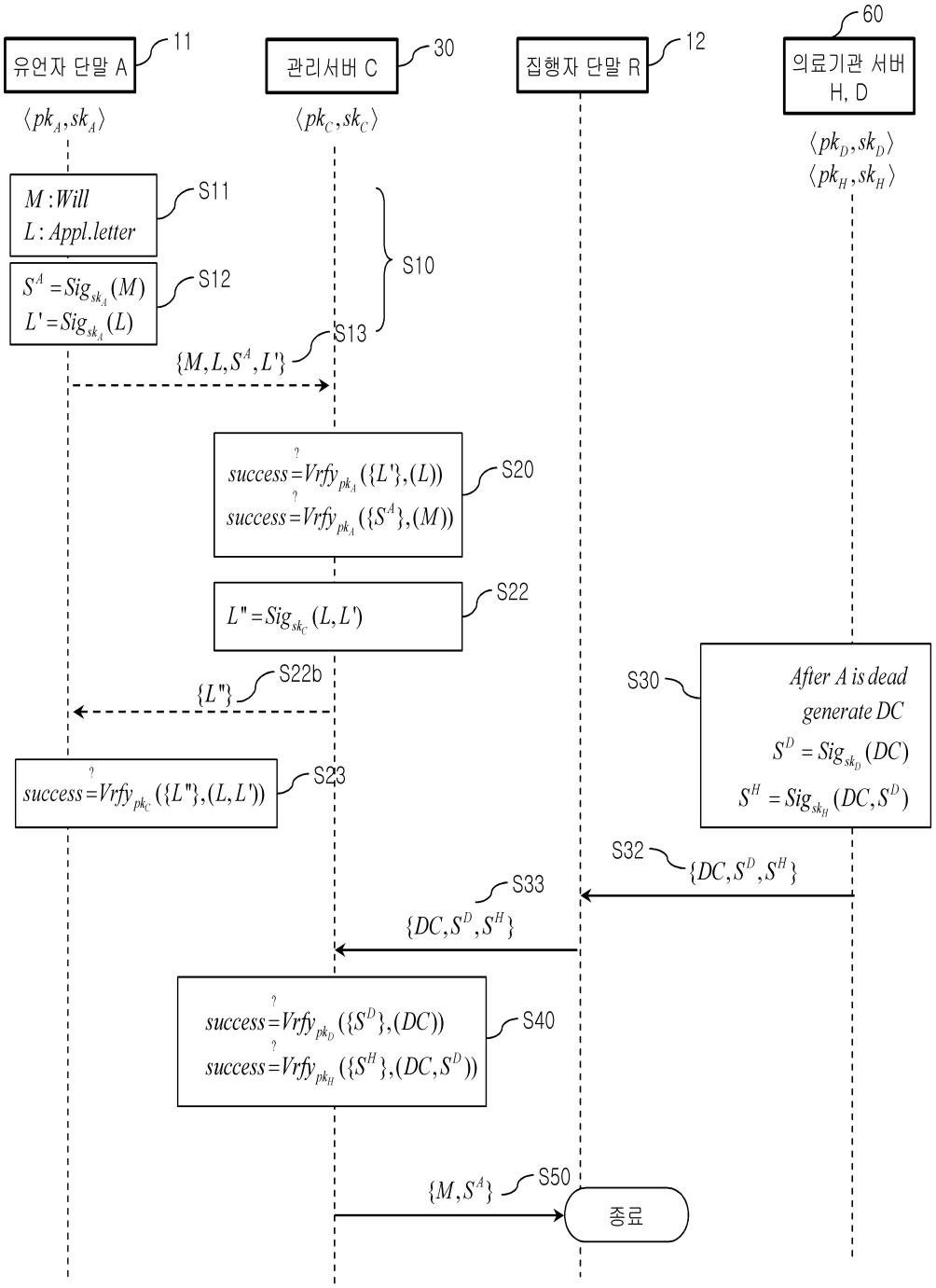
도면2a



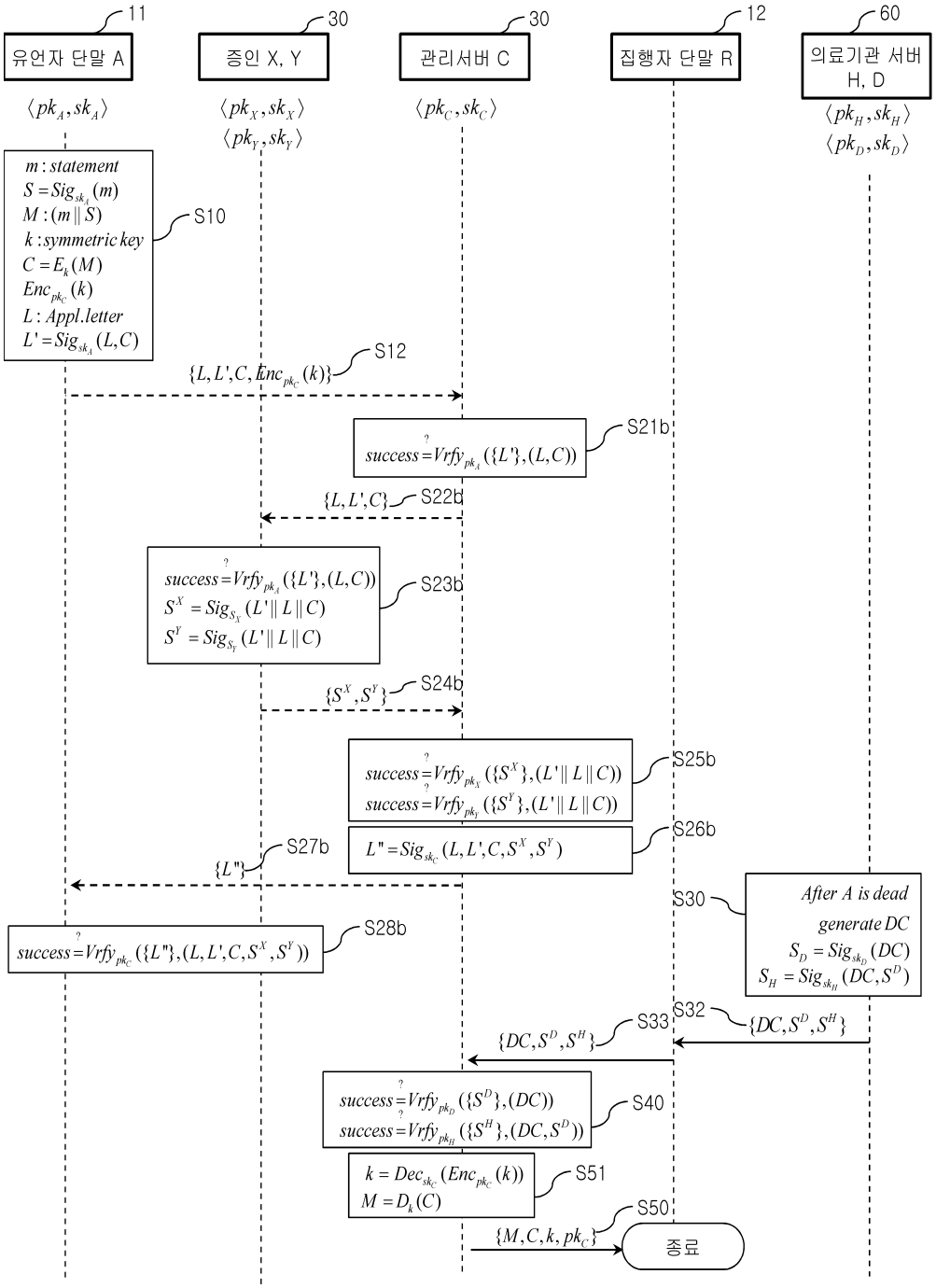
도면2b


PKI services
CRL
LDAP
OCSP
Certificate Authorities
CA1
CA2
CA3
...
CAN
E-will system
Timestamp Service
Timestamp Authority (TSA)
Long-term Archive Service
Long-term Archive Server
Archive Service
Archive Server
Court (C)
2a
WEB Browser
Witness (X,Y)
Hospital (H)
Doctor (D)
Relative (R)
Testator (A)
Testator (A)
Will (W)
Missive(L'')

도면3


유언자 단말 A
11
관리서버 C
30
집행자 단말 R
12
의료기관 서버
H, D
60
$\langle pk_A, sk_A \rangle$
$\langle pk_C, sk_C \rangle$
$\langle pk_D, sk_D \rangle$
$\langle pk_H, sk_H \rangle$
$M : Will$
$L : Appl.letter$
S11
$S^A = Sig_{sk_A}(M)$
$L' = Sig_{sk_A}(L)$
S12
S10
S13
$\{M, L, S^A, L'\}$
$success \overset{?}{=} Vrfy_{pk_A}(\{L'\}, (L))$
$success \overset{?}{=} Vrfy_{pk_A}(\{S^A\}, (M))$
S20
$L'' = Sig_{sk_C}(L, L')$
S22
$\{L''\}$
S22b
S30
After A is dead
generate DC
$S^D = Sig_{sk_D}(DC)$
$S^H = Sig_{sk_H}(DC, S^D)$
$success \overset{?}{=} Vrfy_{pk_C}(\{L''\}, (L, L'))$
S23
S32
$\{DC, S^D, S^H\}$
S33
$\{DC, S^D, S^H\}$
$success \overset{?}{=} Vrfy_{pk_D}(\{S^D\}, (DC))$
$success \overset{?}{=} Vrfy_{pk_H}(\{S^H\}, (DC, S^D))$
S40
$\{M, S^A\}$
S50
종료

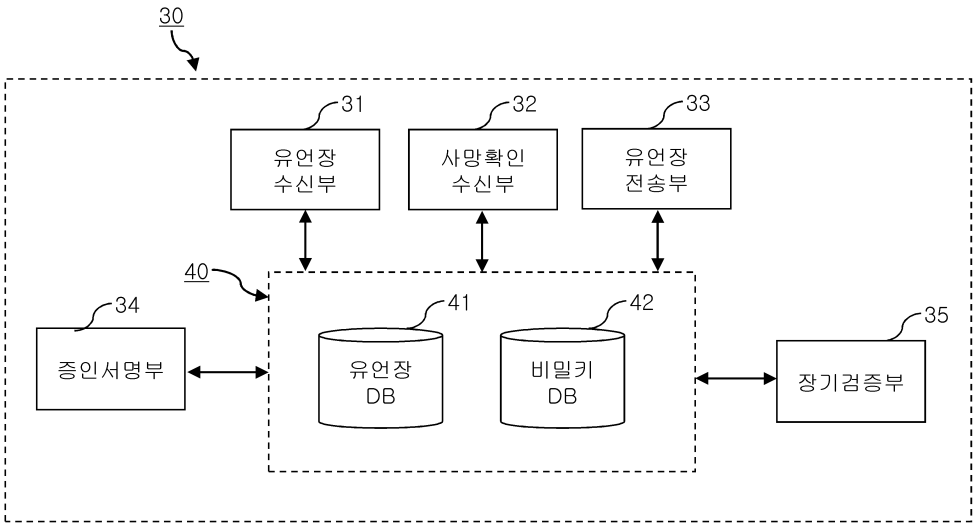
도면4


11
유언자 단말 A
30
증인 X, Y
30
관리서버 C
12
집행자 단말 R
60
의료기관 서버 H, D
$\langle pk_A, sk_A \rangle$
$\langle pk_X, sk_X \rangle$
$\langle pk_Y, sk_Y \rangle$
$\langle pk_C, sk_C \rangle$
$\langle pk_H, sk_H \rangle$
$\langle pk_D, sk_D \rangle$
$m : statement$
$S = Sig_{sk_A}(m)$
$M : (m \| S)$
$k : symmetric\ key$
$C = E_k(M)$
$Enc_{pk_C}(k)$
$L : Appl.letter$
$L' = Sig_{sk_A}(L, C)$
S10
$\{L, L', C, Enc_{pk_C}(k)\}$
S12
$success \stackrel{?}{=} Vrfy_{pk_A}(\{L'\}, (L, C))$
S21b
$\{L, L', C\}$
S22b
$success \stackrel{?}{=} Vrfy_{pk_A}(\{L'\}, (L, C))$
$S^X = Sig_{S_X}(L' \| L \| C)$
$S^Y = Sig_{S_Y}(L' \| L \| C)$
S23b
$\{S^X, S^Y\}$
S24b
$success \stackrel{?}{=} Vrfy_{pk_X}(\{S^X\}, (L' \| L \| C))$
$success \stackrel{?}{=} Vrfy_{pk_Y}(\{S^Y\}, (L' \| L \| C))$
S25b
$L'' = Sig_{sk_C}(L, L', C, S^X, S^Y)$
S26b
$\{L''\}$
S27b
$success \stackrel{?}{=} Vrfy_{pk_C}(\{L''\}, (L, L', C, S^X, S^Y))$
S28b
S30
$After\ A\ is\ dead$
$generate\ DC$
$S_D = Sig_{sk_D}(DC)$
$S_H = Sig_{sk_H}(DC, S^D)$
$\{DC, S^D, S^H\}$
S32
$\{DC, S^D, S^H\}$
S33
$success \stackrel{?}{=} Vrfy_{pk_D}(\{S^D\}, (DC))$
$success \stackrel{?}{=} Vrfy_{pk_H}(\{S^H\}, (DC, S^D))$
S40
$k = Dec_{sk_C}(Enc_{pk_C}(k))$
$M = D_k(C)$
S51
$\{M, C, k, pk_C\}$
S50
종료

도면5

표기	설명
$Cert_X$	X의 인증서
$C \leftarrow Enc_{pki}(M)$	공개키 pki에 의한 메시지 M의 공개키 암호화
$\{M \text{ or } \perp\} \leftarrow Dec_{ski}(C)$	i의 개인키를 사용하여 암호화된 메시지 C를 공개키 복호화
$S^i \leftarrow Sig_{ski}(M)$	서명자의 개인키 ski로 메시지 M을 공개키 서명
$Vrfy_{pki}(S^i, M)$	서명을 공개키 pki로 검증하여 성공 또는 실패 값을 반환
$E_k(M)$ / $D_k(C)$	대칭키 k 하에 메시지 M 또는 C의 대칭적으로 암호화/복화화
pk_A	A주체의 공개키
sk_A	A주체의 개인키
L”	유언장과 신청서의 접수를 유언자에게 확인시켜주기 위해 관리서버가 발급하는 공문서
S^A /S^D / S^H	A주체, 의사, 병원의 전자서명
<---	암호화 채널에 의한 데이터 전송
←	공개 채널에 의한 데이터 전송

도면6



도면7

안정성 요구	종래기술의 일반 방식	종래기술의 봉인 방식	본 발명의 제1 실시예	본 발명의 제2 실시예
부인방지	X	X	O	O
사전공개의 방지	N/A	X	N/A	O
장기서명검증	X	X	O	O
대만 시민법의 준수	O	O	O	O
전자서명법의 준수	X	X	O	O

※ X: 불만족
※ O: 만족