(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0076674
(43) 공개일자 2020년06월29일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 21/33* (2013.01)
G06Q 10/10 (2012.01) *G06Q 50/18* (2012.01)
H04L 12/58 (2006.01) *H04L 29/06* (2006.01)
H04W 12/06 (2009.01) *H04W 4/14* (2018.01)
(52) CPC특허분류
H04L 9/321 (2013.01)
G06F 21/33 (2013.01)
(21) 출원번호 10-2020-7010267
(22) 출원일자(국제) 2018년08월20일
심사청구일자 없음
(85) 번역문제출일자 2020년04월09일
(86) 국제출원번호 PCT/ES2018/070562
(87) 국제공개번호 WO 2019/058006
국제공개일자 2019년03월28일
(30) 우선권주장
17382631.4 2017년09월21일
유럽특허청(EPO)(EP)

(71) 출원인
예이다네트웍스 서비즈 텔레마틱스 에스.에이.
스페인 이-25003 예이다 2에이플란타 파르퀴 테트노로지코 아그로알리멘타리오 - 에디피시오 에이치 1
(72) 발명자
사페나 솔레 프란시스코
스페인 25003 예이다 2 에이플란타 파르퀴 테트노로지코 아그로알리멘타리오 에디피시오 에이치 1 예이다네트웍스 서비즈 텔레마틱스 에스.에이.
(74) 대리인
리앤목특허법인

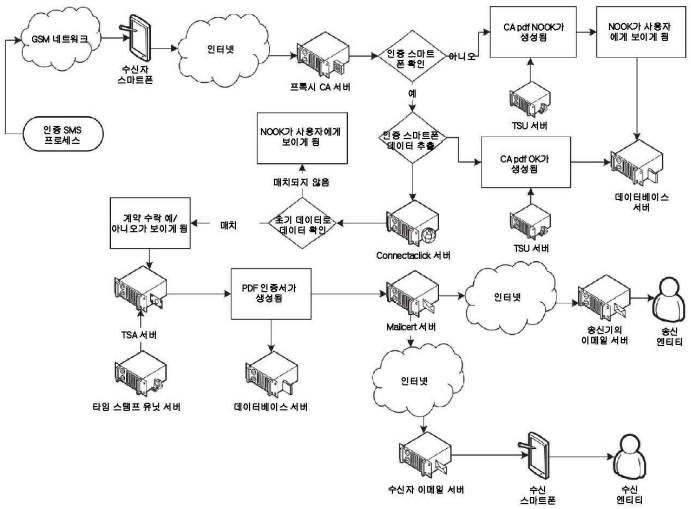
전체 청구항 수 : 총 4 항

(54) 발명의 명칭 **전자 신원확인 및 인증 서비스 (ＥＩＤＡＳ) 를 위한 전자 계약을 인증하는 플랫폼 및 방법**

(57) 요 약

본 발명의 목적은 통신 사업자 또는 전자 배달 제공자가 이메일로 계약을 하나 또는 다수의 수신자에게 송신하고, 계약의 내용을, 링크를 통해 수신자의 디지털 인증서 및 수신자의 신원을 확인하게 될 인증 기관(certification authority; CA)에 인증하며, 계약이 확인, 수락 또는 거부될 수 있는 계약 서버에 통신을 재송신하고 그리고 계약, 계약 엔티티, 계약 엔티티에 관한 CA에 의해 발행된 인증서 및 트랜잭션을 설명하는데 필요한 트랜잭션 데이터 모두가 있는 통신 사업자로서 트랜잭션의 증명을 생성할 수 있는 방법에 관한 것이다.

대 표 도



(52) CPC특허분류
G06Q 10/107 (2013.01)
G06Q 50/18 (2013.01)
H04L 51/34 (2013.01)
H04L 63/0823 (2013.01)
H04L 9/3247 (2013.01)
H04L 9/3268 (2013.01)
H04L 9/3297 (2013.01)
H04W 12/06 (2019.01)
H04W 4/14 (2013.01)

명 세 서

청구범위

청구항 1

전자 계약의 인증 플랫폼으로서, 통신 제공자에 연관되고 서로에 접속되는 이하의 것들 포함하는 것을 특징으로 하며,

상기 이하의 것들은,

- 전자 계약 이메일 시스템을 구현하는 계약 서버;
- 증거 수집 기능이 있는 이메일 관리 서버;
- 원본 이메일의 내용을 저장하기 위한 데이터베이스 서버;
- 타임 스탬프 서버;
- 계약 프로세스 중에 수집된 증거를 위한 서버;
- 수신자의 브라우저에 포함된 디지털 인증서를 사용하여 수신자의 신원을 확인하는 기능을 수행하는 확인 서버;
- 인증 메시지를 송신하는 기능을 수행하는 인증 메시지 서버; 및
- 문서 생성 서버에 의해 생성된 전자 계약 인증서를 저장하기 위한 생성 문서 서버;

를 포함하는, 전자 계약의 인증 플랫폼.

청구항 2

전자 계약의 인증 방법으로서,

상기 방법은, 통신 제공자가,

- 송신기의 일부인 송신 엔티티의 사용자를 통해 계약 서버에 액세스하는 것;
- 수신기인 수신 엔티티의 사용자의 데이터를 도입하는 것 - 상기 데이터는 수신자 이메일 주소 및 수신자 전화 번호 중 적어도 하나를 포함함 -;
- 수신자 전화 번호 또는 수신자 이메일 주소를 선택하는 것;
- 수신기에게, 인증 SMS 서버를 통한 SMS 또는 이메일 관리 서버를 통한 인증 이메일을 송신하는 것 - 인증 SMS 및 인증 이메일 양자 모두는 통신이 수행되게 하는 CA(certification authority) 서버의 프록시 서버에 링크하는 적어도 하나의 URL을 포함함 -;
- 상기 수신기의 일부를 통해 상기 URL에 액세스하고 바람직하게는 브라우저에 포함된 트랜잭션에 사용될 디지털 인증서를 선택하는 것;
- 디지털 인증서에 포함된 데이터를 확인하기 위해 CA의 프록시 서버를 통해 수신자의 일부에서 계약 서버에 액세스하는 것;
- 수신자에 의한 계약에 서명하는 것;
- 서명된 계약서 사본을 수신자에게 송신하는 것;

- 증거 생성 서버에 의한 증거를 생성하는 것;
- 증거 생성 서버를 통해, 모든 네트워크 데이터, 계약, CA의 프록시 서버에 의해 생성된 문서 및 사용된 작업의 트랜잭션 데이터를 지니는 트랜잭션 인증서를 생성하는 단계;
- 통신 제공자의 디지털 서명으로 트랜잭션 인증서에 서명하는 것;
- 일단 트랜잭션 인증서에 서명되면 타임 스탬프 서버를 통해 타임 스탬프를 트랜잭션 인증서에 적용하는 것; 및
- 트랜잭션의 서명 및 스탬프된 인증서의 사본 적어도 2통을 , 한 통은 송신 엔티티에 그리고 다른 한 통은 수신 엔티티에 대응하는 사용자에 의해 수집되도록 송신하는 것;

을 포함하는, 전자 계약의 인증 방법.

청구항 3

제2항에 있어서,

디지털 인증서 또는 그에 대한 액세스가 존재하지 않으며,

상기 전자 계약의 인증 방법은,

- 프로세스가 계속될 수 없다고 CA의 프록시 서버가 결정하는 것;
- 프록시 서버를 통해 비-준수 파일을 생성하는 것;
- 상기 비-준수 파일을 생성 문서 서버에 저장하는 것; 및
- 생성 문서 서버에서 상기 비-준수 파일을 타임 스탬핑하는 것;

을 포함하는 것을 특징으로 하는, 전자 계약의 인증 방법.

청구항 4

제2항 또는 제3항에 있어서,

상기 전자 계약의 인증 방법은,

초기에 도입된 데이터와의 비교를 통해 브라우저의 인증서에 포함된 데이터의 확인하는 것을 포함함을 특징으로 하는, 전자 계약의 인증 방법.

발명의 설명

기 술 분 야

[0001] 본 발명의 목적은 정보 및 통신 기술 분야에서 이루어진다.

[0002] 더 구체적으로는, 본원 명세서에 기재되어 있는 방법은 전자 문서의 중개 당사자, 송신, 수신 및 내용을 인증하기 위한 애플리케이션을 대상으로 한 것이다.

배 경 기 술

[0003] 디지털 인증 및 계약의 세계는 이미 몇 년 동안 발전해 왔지만, 인증 기관(certification authority; CA)들, 디지털 회사들, 전자 배달 제공자들, 인증 프로세스들, 인증 가능한 프로세스들 및 다른 방법들 간에는 디지털 인증 세계의 행위자들 간 일반적인 혼란이 있다. 또한, 디지털 서명된 문서들에는 상기 문서들에 서명한 사람에 관한 정보만이 포함되며 상기 문서들의 내용은 수정되지 않은 상태로 유지되지만, 다른 디지털 수단이 계약을 수락하여 계약에 디지털 방식으로 서명하는데 사용되는 경우에 상기 문서들에는 상기 문서들의 송신, 상기 문서들의 배달, 상기 문서들의 수락 또는 거부에 관한 정보가 포함되어 있지 않다.

[0004] 가장 일반적인 계약 방법은 인증서들, 서명들에 대해 단일 CA를 사용하여 모든 행위들을 채택 및 집결하고 단일 위치에서 이러한 행위들을 모두 수행하는 공고(notice)이었다. 그 자체로는 선험(a priori)이 가장 간단한 방법이지만, 필요한 인증서의 개수, 서명해야 할 위치들 그리고 채택 공고를 준비할 때 디지털 존재 또는 주기적인 액세스가 통지의 누락을 회피하는데 필요한 경우에 관련된 문제가 생긴다. 스페인 국가에서만, 전국적으로 운영하기를 원하면 액세스가 이루어지는 디지털 엔티티가 약 80,000개 있어야 한다.

[0005] 앞서 언급한 문제점을 해결하여 프록시 CA에 구성된 임의의 디지털 인증서를 사용하고 그럼으로써 프로세스를 이메일과 SMS 양자 모두로 언제든지 개시할 수 있게 하여야 하고, 결과적으로는 프로세스에서 수행되는 단계들 모두를 기록하고 그럼으로써 계약 프로세스의 행위자들이 누구이며 언제 그리고 어떤 시점에서 계약 프로세스가 진행되었는지를 언제든지 시연할 수 있게 하여야 한다.

[0006] 전자 신뢰 서비스는,

[0007] • 전자 서명들, 전자 스탬프들 또는 전자 타임 스탬프들, 인증된 전자 배달 서비스들 및 이러한 서비스들에 관련된 인증서들의 생성, 확인 및 검증;

[0008] • 웹 사이트를 인증하기 위한 인증서들의 생성, 확인 및 검증;

[0009] • 이러한 서비스들에 관련된 서명들, 스탬프들 또는 전자 인증서들의 보존;

[0010] 으로 이루어진다.

[0011] 이러한 의미에서 전자 신원확인 및 인증 서비스(electronic identification and trust service; eIDAS) 프레임워크가 확립되어야 하며, eIDAS를 구현함으로써, 전자 거래를 위한 전자 신원확인 및 신뢰 서비스가 감독된다. eIDAS는 전자 서명들, 전자 거래들, 관련 기관들 및 그들의 포괄 프로세스들을 규제하여 사용자가 비즈니스 온라인 방식으로 그리고 전자 방식으로 공공 서비스와의 자금 이체 또는 거래를 수행할 수 있는 안전한 방법을 제공한다. 서명인 및 수취인 양자 모두는 높은 수준의 편의성 및 안전성을 접할 수 있다. 이메일, 팩스 서비스 또는 종이 문서들의 제시를 직접 채용하는 것과 같은 전통적인 방법에 의존하는 대신에, 이제는 예를 들어 "1 클릭(1 click)" 기술을 사용하여 국경 간 트랜잭션들이 수행될 수 있다.

[0012] 따라서 eIDAS의 구현으로, 트랜잭션이 종이 상에서 수행된 바와 같은 법적 엔티티(legal entity)와의 전자 트랜잭션을 전자 서명(electronic signature), 조건부 디지털 인증서(qualified digital certificate), 전자 스탬프(electronic stamp), 타임 마크(time mark) 및 인증 메커니즘에 대한 기타 테스트가 허용하는 표준이 확립된다.

발명의 내용

[0013] 본 발명의 제1 실시형태에서, 전자 계약의 인증을 위한 플랫폼이 있으며, 상기 플랫폼은 일련의 상호접속된 서비스들을 사용하는 통신 사업자에 의해 구현된다. 이리하여, 상기 플랫폼은 전자 계약 이메일 시스템을 구현하는 계약 서버, 증거 수집 기능을 지니는 이메일 관리 서버, 원본 이메일의 내용을 저장하는 데이터베이스 서버, 타임 스탬프 서버, 계약 프로세스 중에 수집된 증거를 생성하는 서버, 수신기의 브라우저에 포함된 디지털 인증서를 사용하여 수신자의 신원을 확인하는 기능을 수행하는 검증 서버, 메시지를 전송하는 기능을 수행하는 인증 메시지 서버 및 문서 생성 서버에 의해 생성된 전자 계약 인증서를 저장하려고 의도된 생성 문서를 위한 서버를 구현하도록 이루어진 구성을 지닐 수 있다.

[0014] 여기서 언급되어야 할 점은 상기 플랫폼이 전기 통신 사업자(또는 본원 명세서 전반에 걸친 통신 사업자)에 접속되고 바람직하게는 동일하게 구현되므로, 통신 사업자 외부의 네트워크 엔티티들에 대한 필요성 없이 인증 태스크들이 수행될 수 있다는 점이다.

[0015] 본 발명의 제2 실시형태에서, 본 발명의 목적은 통신 사업자 또는 전자 배달 제공자가 이메일로 계약을 하나 또는 다수의 수신자에게 송신하고, 계약의 내용을, 링크를 통해 수신자의 디지털 인증서 및 수신자의 신원을 확인하게 될 인증 기관(certification authority; CA)의 프록시 서버에 인증하며, 계약이 확인, 수락 또는 거부될 수 있는 계약 서버에 통신을 재송신하고 그리고 계약, 계약 엔티티, 계약 엔티티에 관한 CA에 의해 발행된 인증서 및 트랜잭션을 설명하는데 필요한 트랜잭션 데이터 모두가 있는 통신 사업자로서 트랜잭션의 증명을 생성할 수 있는 방법에 관한 것이다.

[0016] 본 발명의 목적은 양단에서 강력한 신원확인을 사용하여 전자방식으로 수행되는 계약을 인증하는 방법을 제공하

며, 클라이언트의 신원확인은 상기 CA가 체크하게 되는 디지털 서명 인증서를 통해 이루어지고 제공자의 신원확인은 전자 트랜잭션의 증거 모두를 인증하는 전자 배달 제공자, 전기 통신 또는 통신 사업자에게 서비스를 계약함으로써 이루어진다.

[0017] 앞서 언급한 것에 의하면, 본 발명의 목적은 통신 제공자 또는 전자 통신 제공자라고도 할 수 있는 전기 통신 제공자 - 이는 항상 전자 배달 제공자임 - 또는 통신 사업자를 통해 전체 프로세스를 인증하는 계약 당사자의 브라우저에 삽입된 디지털 인증서를 사용하여 계약 당사자의 신원을 확인하기 위해 제3자 인증 기관의 프록시를 사용하는 특징을 지니는 전자 계약을 인증하는 방법이다. 마지막으로, 송신측 전자 통신 제공자의 클라이언트는 원본 이메일, 계약, 일자, 시간 및 이들의 트레이서빌리티(traceability), 고유 트랜잭션 번호 및 계약 당사자를 명백하게 식별하는 브라우저에 포함된 디지털 인증서에 포함된 식별 데이터를 지니는 CA 인증서를 포함하여 계약이 이루어졌거나 이루어지지 않은 인증서를 수신한다.

[0018] 본 발명의 방법은 계약 및 그의 내용을 인증하기 위해 사용될 수 있고 이메일 또는 SMS 메시지를 사용하여 구현될 수 있다.

[0019] 본 발명의 바람직한 실시 예에 따른, 본 발명의 특징을 더 잘 이해하기 위해 이루어진 설명을 보완하고 본 발명의 특징을 더 잘 이해하는데 도움을 주기 위해, 상기 설명에는 그의 일체 부분으로서 예시적이고 비-제한적인 일련의 도면들이 첨부된다.

도면의 간단한 설명

[0020] 도 1은 본 발명의 방법의 한 실시 예가 전자 계약에 관한 전자 트랜잭션을 목적으로 하여 표현된 흐름도 - 이러한 프로세스는 수신자 데이터 및 계약을 확인하기 위한 데이터를 도입하기 위해 송신 엔티티에 의해 개시됨 - 를 보여준다.

도 2는 본 발명의 방법의 한 실시 예가 전자 계약에 관한 전자 트랜잭션을 목적으로 하여 표현된 흐름도 - 이러한 프로세스는 인증 SMS 또는 SMS에 의해 개시됨 - 를 보여준다.

도 3은 본 발명의 방법의 한 실시 예가 전자 계약에 관한 전자 트랜잭션을 목적으로 하여 표현된 흐름도 - 이러한 프로세스는 인증 이메일 또는 이메일에 의해 개시됨 - 를 보여준다.

발명을 실시하기 위한 구체적인 내용

[0021] 본 발명의 전자 계약 목적을 위한 방법은 본 발명의 목적이며 수신 엔티티 및 송신 엔티티, (스마트폰 또는 수신기의 컴퓨터와 같은) 수신기 또는 수신 장치를 통한 수신 엔티티, 및 (컴퓨터 또는 송신기의 유사한 장치와 같은) 송신기 또는 송신 장치에 액세스 가능한 통신 제공자 및 서로에 상호접속된 일련의 서버들에 연관된 플랫폼에서 구현될 수 있고, 상기 서버들은,

[0022] - Connectaclick 서버라고 하는 계약 서버 - 무차별적인 방식으로 이메일, 웹 및 SMS를 사용하는 전자 계약 시스템과 같은 전자 계약 시스템을 구현하는 솔루션이므로 이렇게 불린다. 계약 서버는 통신 제공자와 밀접하게 접속되어 있거나 그의 일부이다 -;

[0023] - Mailcert라고 하는 이메일 관리 서버 - 이메일이 해당 이메일로부터의 증거 수집 - 여기서 증거는 특히 헤더, 본문 및 첨부물을 포함할 수 있음 - 을 통해 관리되는 것을 허용하는 서버 -;

[0024] - 헤더, 본문 및 첨부물, 송신에 상응하는 로그 부분 및 수신자 이메일 서버의 분석 정보를 포함하여 원본 이메일의 내용을 저장하는 Mailcert 데이터베이스 서버 - 이는 과거 데이터를 저장함 -;

[0025] - 타임 스탬프 서버 또는 타임 스탬프 유닛(time stamp unit; TSU), 인증 시스템에 의해 생성된 문서, 바람직하게는 PDF의 타임 스탬프를 위해 CA에 의해 현장에서 구현되는 타임 스탬프 시스템 - 이러한 서버는 바람직하게는 통신 사업자의 기반구조에 위치하지만, 특정 상황에서, 필요한 경우, 이는 제3자의 엔티티일 수 있고, 결과적으로는 통신 사업자의 기반구조 외부에 물리적으로 위치될 수 있음 -;

[0026] - TSA 서버라고 하는 증거 생성 서버 - 문서, 바람직하게는 계약 프로세스 동안 상기 증거의 컴파일로 인한 증거를 포함하는 PDF 포맷의 문서를 생성하는 서버 -;

[0027] - 수신자의 브라우저에 포함된 디지털 인증서를 사용하여 수신자의 신원을 확인하는 기능을 수행하는 서버인 CA 검증 프록시라고 하는 검증 서버;

[0028] - SMS를 통해 수행하기로 선택한 경우, 계약 송신기로부터 계약 수신자, 바람직하게는 SMS를 통해 GSM 네트워크로 인증 메시지를 송신하는 인증 메시지 서버;

[0029] - 대량의 생성된 전자 계약 인증서를 저장하는 기능을 수행하는 생성 문서 서버;

[0030] 일 수 있다.

[0031] 본 발명의 제2 실시형태의 전자 계약 목적의 인증 방법은 도 2에서 보인 바와 같은 SMS 메시지 또는 도 3에서 보인 바와 같은 이메일, 다시 말하면 인증 SMS 또는 인증 이메일(이하 인증 이메일)을 사용하여 서로 구별되는 2가지 가능한 실시 예를 지닌다.

[0032] 이리하여, 본 발명의 제2 실시형태의 방법은 인증 전자 계약의 생성이 수행되게 하고, 송신 엔티티는 컴퓨터와 같은 전자 송신 장치에 의해 송신기로서 식별되는 인터넷과 같은 데이터 네트워크에 대한 액세스 수단을 통해 계약 서버(Connectaclick 서버)에 액세스한다.

[0033] 일단 사용자가 인증되면, 확인되어야 할 클라이언트의 데이터, 사용자가 수행하고자 하는 전자 계약(이하 계약) 및 이러한 문서 전반에 걸쳐 수신기 또는 수신자라고 하는 수신기의 전화번호 또는 이메일 주소가 소개된다. 하나 또는 다른 유형의 메시지를 선택하면 다음과 같이 따라야 할 단계가 결정된다.

[0034] - 전화번호가 도입되면, 인증 SMS 서버를 통해 SMS가 송신되고 인증 SMS로 프로세스가 개시된다.

[0035] - 이메일이 도입되면, 인증 이메일이 Mailcert 서버를 통해 송신되고 인증 이메일을 통해 송신되고 인증 이메일로 프로세스가 개시된다.

[0036] 인증 SMS를 사용하는 프로세스는 수신자의 수신 전자 장치가 스마트폰과 같은 액세스 능력 및 데이터 통신을 지니는 메시지를 수신할 때 개시되고, 상기 메시지는 CA 서버의 프록시 서버에 링크되는 URL(인터넷 주소)을 포함하고 이를 통해 나머지 서버들과의 모든 통신이 수행된다.

[0037] 인증 SMS를 사용하는 프로세스는 수신자의 일부에서 상기 URL에 대한 액세스를 계속하고 이 경우에 CA의 프록시 서버가 트랜잭션에 사용되도록 수신 장치의 브라우저에서 가능한 내용으로부터 디지털 인증서를 요청한다.

[0038] 디지털 인증서가 없거나 유효하지 않거나 동일하게 액세스할 수 없는 경우에, CA의 프록시 서버는 프로세스를 완료하고 프로세스를 계속할 수 없음을 표시하여 "CA pdf NOOK"이라 하는 비-준수 파일을 생성하고 이는 생성 PDF 서버상에 저장될 PDF 형식인 것이 바람직하며; 선택적으로는, TSU 서버로부터의 타임 스탬프가 상기 비-준수 파일(CA pdf NOOK)에 추가될 수 있다. 인증서가 있는 경우 후속 확인을 위해 인증서를 포함하는 일련의 데이터가 추출되어 해당 데이터를 사용하여 "CA pdf OK"이라는 준수 파일을 생성하고 비준수 파일에서 발생하는 경우 선택적으로 TSU의 타임 스탬프를 추가한 다음에, 생성 PDF 서버에 저장한다.

[0039] 이러한 방식으로, 상기 브라우저의 인증서에 포함 된 데이터가 처음으로 도입된 데이터와 매치(match)되면, 서명해야 할 계약이 보이게 된다. 수신자가 계약을 수락하지 않는 경우(예를 들어, 서명 거부), 수신자가 수락하지 않은 것으로 보이게 되고 프로세스가 완료되는 반면에 계약을 수락하면 수신자의 이메일 주소가 수신자용 사본을 송신하도록 요청되고 수신자와의 세션이 마무리된다.

[0040] 일단 수신자와의 세션이 마무리되면, 증거 생성 서버인 TSA 서버는 인터넷을 통한 데이터 전송에 관한 모든 데이터, 계약 자체 및 그의 내용, 프록시 CA의 생성 PDF 및 사용된 작업의 임의 트랜잭션 데이터를 컴파일링하는 수단을 통해 트랜잭션 인증서를 생성한다. 일단 생성되면, 결과적으로 생성된 인증서는 타임 스탬프 서버(TSU 서버)를 통해 통신 제공자의 디지털 서명 및 타임 스탬프로 서명된다.

[0041] 결과적으로 생성된 인증서는 일단 스탬프 처리되면된 이메일을 송신하는 기능을 수행하는 Mailcert 서버에 송신되고, 이미 서명한 계약의 인증서 사본 2통과 생성된 모든 증거를 한 통은 송신 엔터티에 그리고 다른 한 통은 수신 엔터티에 송신하고 이들은 대응하는 사용자들에 의해 수집되도록 대응하는 이메일 서버들에 의해 수신된다.

[0042] 상기 방법이 인증 메일 또는 인증 이메일을 사용하는 일부 실시 예들에서, 상기 방법은 유사하고 수신자의 착신 이메일 서버가 초기에 송신된 인증 이메일을 수신할 때 개시되며, 이 경우에 상기 인증 이메일은 서명해야 할 계약을 포함할 수 있지만, 이는 나머지 서버들과의 모든 통신이 수행되게 하는 CA의 프록시 서버를 가리키는 URL(인터넷 주소)을 포함한다. 인증 이메일을 사용하는 프로세스는 수신자인 수신기가 자신의 스마트폰 또는 컴퓨터를 통해 이메일에 액세스하고 상기 이메일에 포함된 URL에 액세스할 때 계속되고 여기서 CA 프록시 서버는 스마트폰 또는 컴퓨터의 브라우저에 포함된 디지털 인증서가 트랜잭션에 사용되고 있는 지를 수신자에게

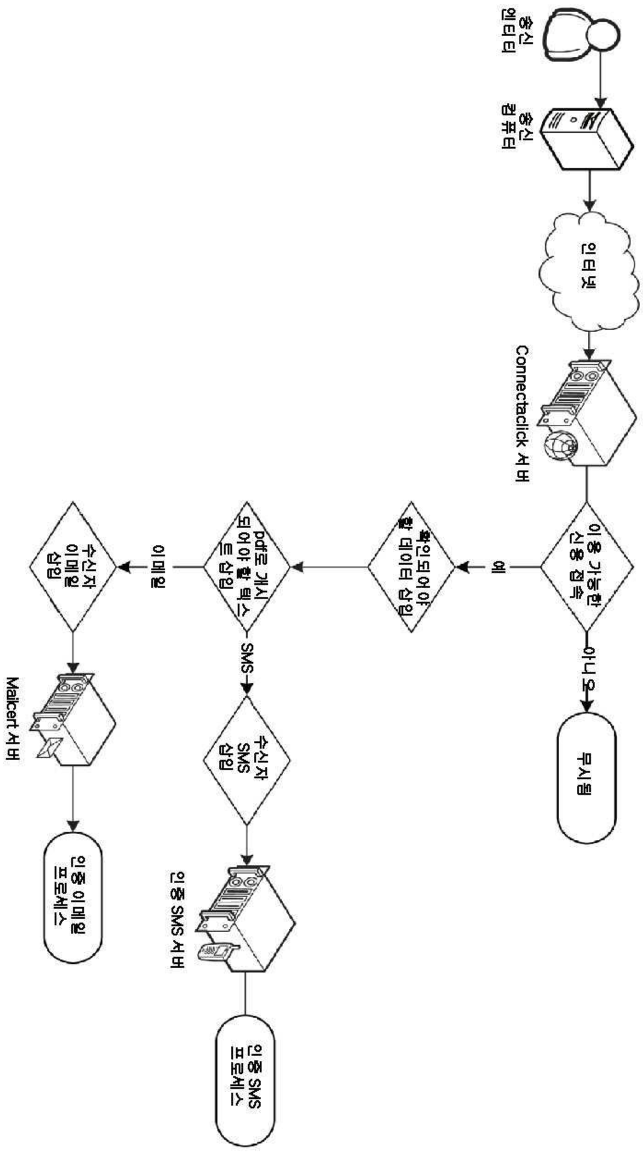
묻는다. 그들을 지니지 않거나 그들에 액세스할 수 없는 경우에, 프록시 CA 서버는 프로세스가 계속될 수 없음을 보여주고 타임 스탬프(TSU)가 추가될 수 있는 생성 문서 서버상에 저장되는 PDF 포맷의 CA pdf NOOK 파일을 생성한다. 상기 브라우저에 상기 인증서가 있는 경우, 후속 확인을 위해 포함하는 데이터가 추출되어 상기 데이터와 함께 CA pdf OK 파일이 생성되고 TSU 서버의 타임 스탬프가 추가되어 생성 PDF 서버에 저장된다. 사용자가 프록시 CA를 통해 Connectaclick 서버에 액세스하면 프로세스가 계속되며 여기서 브라우저의 인증서에 포함된 데이터가 처음으로 도입된 데이터와 매치되는지 확인되고 서명해야 할 계약이 보이게 된다. 수신자가 수락하지 않는 경우에, 그들이 수락하지 않은 것으로 보이게 되고 마무리된다. 계약을 수락하는 경우, 사본을 송신하도록 이메일이 요청되고 수신자와의 세션이 마무리된다.

[0043] 일단 수신자와의 세션이 마무리되면, 증거 생성 서버는 모든 인터넷 데이터, 계약, 프록시 CA의 생성된 PDF 및 사용된 작업의 임의 트랜잭션 데이터를 사용하여 트랜잭션 인증서를 준비한다. 완료되면, 결과적으로 생성된 인증서는 통신 제공자의 디지털 서명 및 타임 스탬프 서버(TSU 서버)를 통한 타임 스탬프로 서명된다. 생성된 인증서는 이메일을 송신하는 기능을 수행하는 Mailcert 서버에 송신되고, 서명된 계약의 인증서 사본과 생성된 모든 증거 사본 2통은, 한 통이 송신 엔티티에 그리고 다른 한 통이 수신 엔티티에 송신되게 하고 이들은 대응하는 사용자들에 의해 수집되도록 대응하는 이메일 서버에 의해 수신된다.

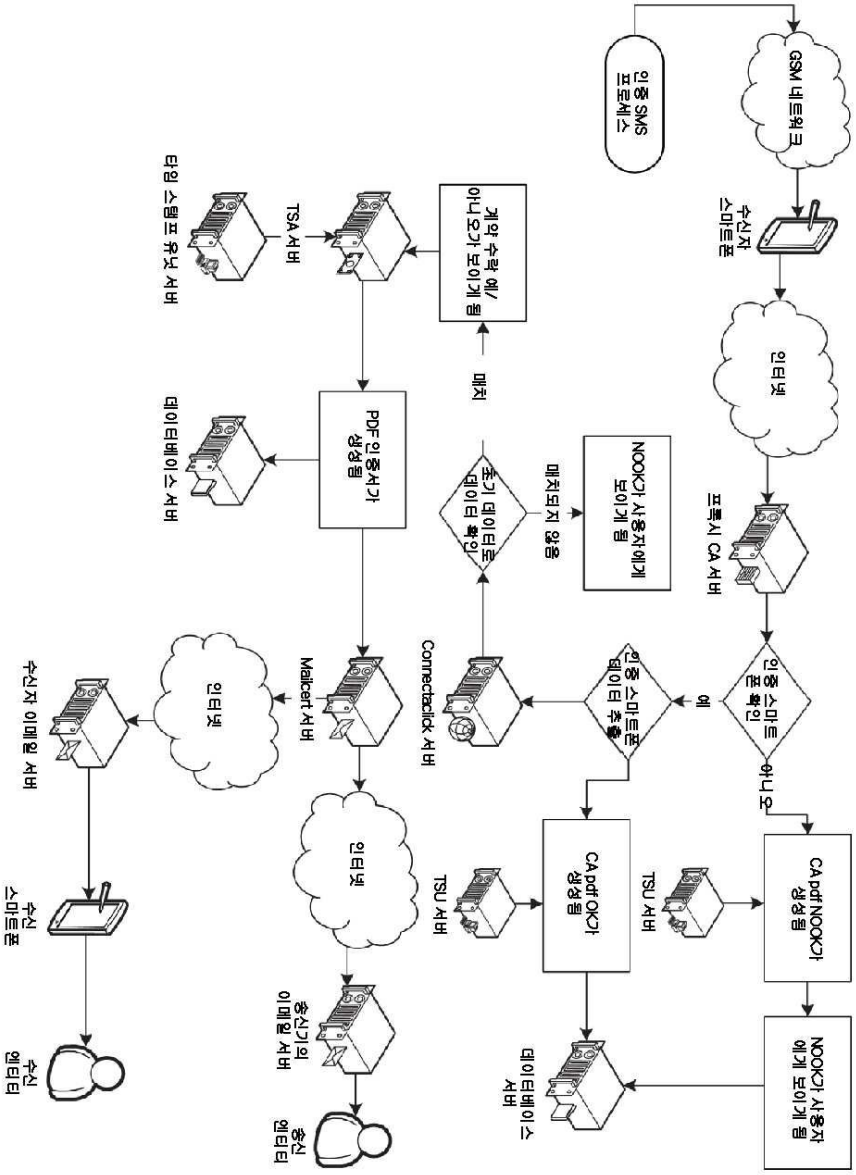
[0044] 위에서 언급한 내용에 의하면, 본 발명의 방법 목적은 상이한 CA 또는 인증 엔티티로부터 올 수 있는 사용된 디지털 증거 및 인증서의 이점을 제공하며, 가능한 대안 실시 예에서, 프록시 CA 서버의 제공자 및 계약의 모든 증거를 궁극적으로 패키징하여 계약의 전체 프로세스의 인증서를 생성하는 기능을 수행하는 제3 전자 배달 제공자인 제2 CA가 사용될 수 있다.

도면

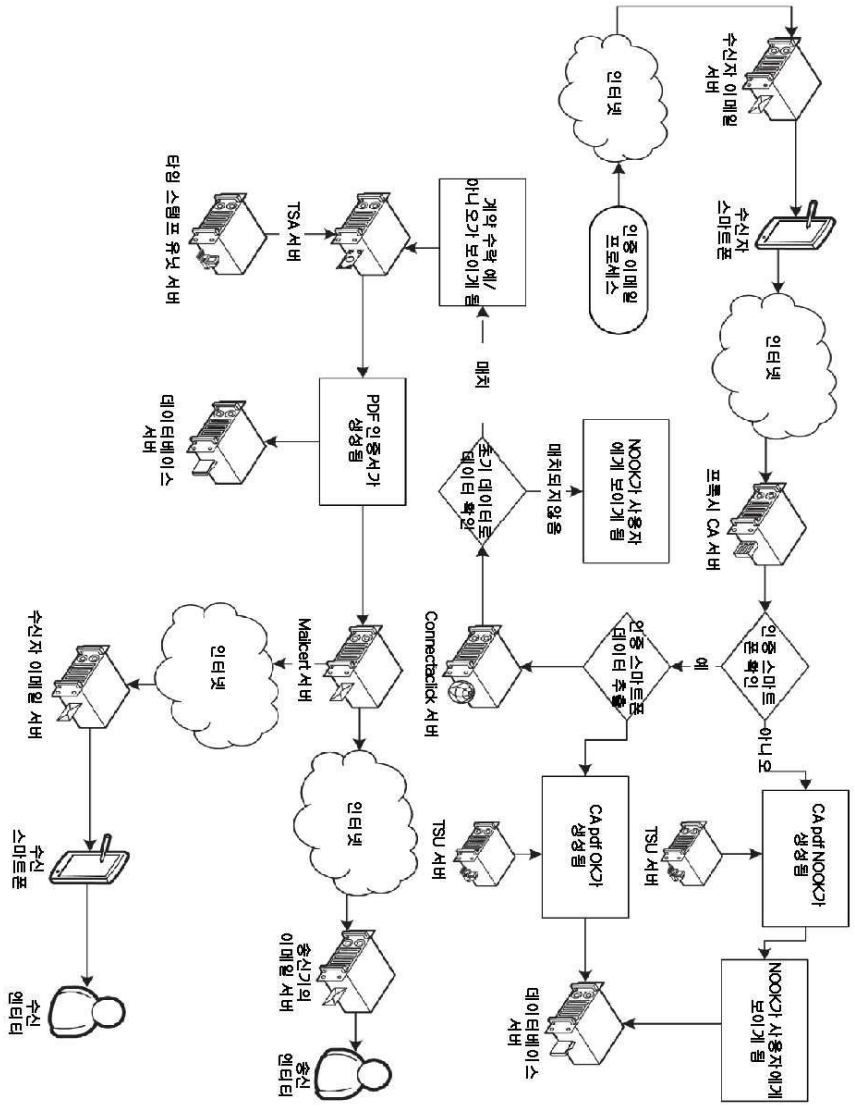
도면1


송신 엔티티
송신 컴퓨터
인터넷
Connectaclick 서버
이용 가능한 신용 접속
예
아니오
무시됨
확인되어야 할 데이터 삽입
pdf로 게시되어야 할 텍스트 삽입
이메일
SMS
수신자 이메일 삽입
수신자 SMS 삽입
Mailcert 서버
인증 SMS 서버
인증 이메일 프로세스
인증 SMS 프로세스

도면2


GSM 네트워크
인증 SMS 프로세스
수신자 스마트폰
인터넷
프록시 CA 서버
인증 스마트폰 확인
아니오
CA pdf NOOK가 생성툴
NOOK가 사용자에게 보이게 툴
데이터베이스 서버
에
인증 스마트폰 데이터 추출
CA pdf OK가 생성툴
TSU 서버
TSU 서버
Connectaclick 서버
초기 데이터로 확인
메치되지 않음
NOOK가 사용자에게 보이게 툴
메치
계약 수락 예/아니오가 보이게 툴
TSA 서버
타임 스탬프 유닛 서버
PDF 인증서가 생성툴
데이터베이스 서버
Mailcert 서버
인터넷
인터넷
수신자 이메일 서버
수신 스마트폰
수신 엔티티
송신기의 이메일 서버
송신 엔티티

도면3


수신자 이메일 서버
인터넷
인증 이메일 프로세스
수신자 스마트폰
인터넷
프톨시 CA 서버
인증 스마트폰
아니오
예
인증 스마트폰 데이터 추출
CA pdf NOOK가 생성될
CA pdf OK가 생성될
TSU 서버
TSU 서버
NOOK가 사용자에게 보이게 될
데이터베이스 서버
NOOK가 사용자에게 보이게 될
초기 데이터로 데이터 확인
매치되지 않음
Connectaclick 서버
PDF 인증서가 생성될
데이터베이스 서버
매치
계약 수락에/ 아니오가 보이게 될
TSA 서버
타임 스탬프 유닛 서버
Mailcert 서버
인터넷
수신자 이메일 서버
수신 스마트폰
수신 엔티티
인터넷
송신기의 이메일 서버
송신 엔티티