(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0041729
(43) 공개일자 2017년04월17일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 63/0823 (2013.01)
H04L 63/166 (2013.01)
(21) 출원번호 10-2017-7003447
(22) 출원일자(국제) 2015년07월30일
심사청구일자 없음
(85) 번역문제출일자 2017년02월07일
(86) 국제출원번호 PCT/US2015/042827
(87) 국제공개번호 WO 2016/019106
국제공개일자 2016년02월04일
(30) 우선권주장
14/448,697 2014년07월31일 미국(US)

(71) 출원인
노크 노크 랩스, 인코포레이티드
미국 캘리포니아 팔로 알토 스위트 105 겡 로드 2100 (우: 94303)
(72) 발명자
블랑크, 윌리엄 제이.
미국 94303 캘리포니아 팔로 알토 스위트 105 겡 로드 2100
(74) 대리인
특허법인 남앤드남

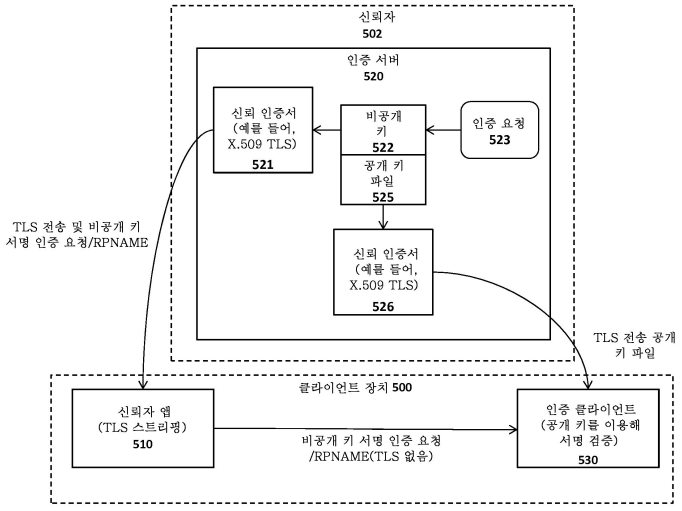
전체 청구항 수 : 총 24 항

(54) 발명의 명칭 **보안 전송 프로토콜을 사용하여 신뢰를 설정하기 위한 시스템 및 방법**

(57) 요 약

설명되는 시스템, 방법 및 기계 판독 가능 매체는 보안 통신 프로토콜을 사용하여, 인증기들을 갖는 클라이언트 장치로 지향되는 통신을 인증 서버에서 생성하고, 분산 공개 키 인프라스트럭처(PKI)로부터의 자체 서명 인증서의 키를 사용하여 제1 통신을 서명하고, 통신 인프라스트럭처를 사용하여 클라이언트 장치 상의 앱과 제1 채널을 설정하고, 서명을 갖는 제1 통신을 제1 채널을 통해 앱으로 전송하고, 신뢰 보안 통신 인프라스트럭처를 사용하여 클라이언트 장치 상의 인증 클라이언트와 제2 채널을 설정하고, 제2 채널을 통해 분산 PKI로부터 인증 클라이언트로 자체 서명 인증서의 제2 키를 전송하고, 앱으로부터 인증 클라이언트로 제1 통신을 제공하고, 인증 클라이언트가 제2 키를 사용하여 제1 키를 갖는 제1 인증 관련 통신에 대해 생성된 서명을 확인함으로써 신뢰를 설정하기 위한 것이다.

대 표 도 - 도5



(52) CPC특허분류
H04L 9/3263 (2013.01)

명 세 서

청구범위

청구항 1

신뢰자를 대신하여 인증 서버에서 제1 인증 관련 통신을 생성하는 단계 - 상기 제1 인증 관련 통신은 하나 이상의 인증기를 갖는 클라이언트 장치로 지향됨 -;

분산 공개 키 인프라스트럭처(PKI)로부터의 자체 서명 인증서의 제1 키를 사용하여 상기 제1 인증 관련 통신을 서명하는 단계;

신뢰 보안 통신 인프라스트럭처를 사용하여 상기 클라이언트 장치 상의 신뢰자 앱과 제1 보안 통신 채널을 설정하는 단계;

서명을 갖는 상기 제1 인증 관련 통신을 상기 제1 보안 통신 채널을 통해 상기 신뢰자 앱으로 전송하는 단계;

신뢰 보안 통신 인프라스트럭처를 사용하여 상기 클라이언트 장치 상의 인증 클라이언트와 제2 보안 통신 채널을 설정하는 단계;

상기 제2 통신 채널을 통해 상기 분산 PKI로부터 상기 인증 클라이언트로 상기 자체 서명 인증서의 제2 키를 전송하는 단계;

상기 신뢰자 앱으로부터 상기 인증 클라이언트로 상기 제1 인증 관련 통신을 제공하는 단계; 및

상기 인증 클라이언트가 상기 제2 키를 사용하여 상기 제1 키를 갖는 상기 제1 인증 관련 통신에 대해 생성된 상기 서명을 확인하는 단계

를 포함하는 방법.

청구항 2

제1항에 있어서, 상기 제1 키는 상기 분산 PKI의 비공개 키를 포함하고, 상기 제2 키는 대응하는 공개 키를 포함하는 방법.

청구항 3

제1항에 있어서, 상기 신뢰 보안 통신 인프라스트럭처는 상기 제1 및/또는 제2 보안 통신 채널을 위한 보안 전송 계층 보안(TLS) 접속을 설정하는 데 사용 가능한 신뢰 인증서를 포함하는 방법.

청구항 4

제3항에 있어서, 상기 신뢰 인증서는 X.509 인증서를 포함하는 방법.

청구항 5

제1항에 있어서,

상기 인증 클라이언트가 상기 제1 인증 관련 통신에 응답하여 제2 인증 관련 통신을 생성하는 단계를 추가로 포함하는 방법.

청구항 6

제5항에 있어서, 상기 제1 인증 관련 통신은 상기 신뢰자를 대신하여 동작되는 인증 서버에서 생성된 인증 요청을 포함하고, 상기 제2 인증 관련 통신은 상기 인증 클라이언트에 의해 생성된 인증 응답을 포함하는 방법.

청구항 7

제6항에 있어서, 상기 인증 요청은 랜덤 챌린지, 및 상기 클라이언트 장치 상의 인증기와 연관된 공개 키를 사용하여 상기 랜덤 챌린지에 대해 생성된 서명을 포함하는 방법.

청구항 8

제7항에 있어서, 상기 인증 클라이언트는 상기 서명을 확인하기 위해 상기 인증기와 연관된 비공개 키를 사용하는 방법.

청구항 9

제8항에 있어서, 상기 인증 클라이언트는 성공적인 사용자 인증에 응답하여 상기 클라이언트 장치 상의 상기 인증기들 중 하나 이상을 사용하여 상기 인증 응답을 생성하는 방법.

청구항 10

제9항에 있어서, 상기 클라이언트 장치 상의 상기 인증기들은 지문 인증기를 포함하는 방법.

청구항 11

제1항에 있어서, 상기 신뢰자 앱으로부터 상기 인증 클라이언트로 상기 제1 인증 관련 통신을 제공하는 단계는 상기 신뢰자 앱과 상기 인증 클라이언트 사이의 프로세스간 통신(IPC)을 구현하는 단계를 추가로 포함하는 방법.

청구항 12

제1항에 있어서, 상기 자체 서명 인증서의 상기 제2 키는 상기 제2 통신 채널을 통해 공개 키 파일로 전송되는 방법.

청구항 13

인증을 수행하기 위한 시스템으로서,

하나 이상의 인증기, 인증 클라이언트 및 신뢰자 앱을 갖는 클라이언트 장치; 및

신뢰자를 대신하여 동작되는 인증 서버를 포함하며, 상기 인증 서버는 상기 클라이언트 장치로 지향되는 제1 인증 관련 통신을 생성하고,

상기 인증 서버는 분산 PKI로부터의 자체 서명 인증서의 제1 키를 사용하여 상기 제1 인증 관련 통신을 서명하고,

상기 인증 서버는 신뢰 보안 통신 인프라스트럭처를 사용하여 상기 클라이언트 장치 상의 신뢰자 앱과 제1 보안 통신 채널을 설정하고,

상기 인증 서버는 서명을 갖는 상기 제1 인증 관련 통신을 상기 제1 보안 통신 채널을 통해 상기 신뢰자 앱으로 전송하고,

상기 인증 서버는 신뢰 보안 통신 인프라스트럭처를 사용하여 상기 클라이언트 장치 상의 인증 클라이언트와 제2 보안 통신 채널을 설정하고,

상기 인증 서버는 상기 자체 서명 인증서의 제2 키를 상기 제2 통신 채널을 통해 상기 분산 PKI로부터 상기 인증 클라이언트로 전송하고,

상기 신뢰자 앱은 상기 제1 인증 관련 통신을 상기 인증 클라이언트에 제공하고,

상기 인증 클라이언트는 상기 제2 키를 사용하여 상기 제1 키를 갖는 상기 제1 인증 관련 통신에 대해 생성된 상기 서명을 확인하는 시스템.

청구항 14

제13항에 있어서, 상기 제1 키는 상기 분산 PKI의 비공개 키를 포함하고, 상기 제2 키는 대응하는 공개 키를 포함하는 시스템.

청구항 15

제13항에 있어서, 상기 신뢰 보안 통신 인프라스트럭처는 상기 제1 및/또는 제2 보안 통신 채널을 위한 보안 전

송 계층 보안(TLS) 접속을 설정하는 데 사용 가능한 신뢰 인증서를 포함하는 시스템.

청구항 16

제15항에 있어서, 상기 신뢰 인증서는 X.509 인증서를 포함하는 시스템.

청구항 17

제13항에 있어서,

상기 인증 클라이언트에서 상기 제1 인증 관련 통신에 응답하여 제2 인증 관련 통신을 생성하는 것을 추가로 포함하는 시스템.

청구항 18

제17항에 있어서, 상기 제1 인증 관련 통신은 상기 신뢰자를 대신하여 동작되는 인증 서버에서 생성된 인증 요청을 포함하고, 상기 제2 인증 관련 통신은 상기 인증 클라이언트에 의해 생성된 인증 응답을 포함하는 시스템.

청구항 19

제18항에 있어서, 상기 인증 요청은 랜덤 챌린지, 및 상기 클라이언트 장치 상의 인증기와 연관된 공개 키를 사용하여 상기 랜덤 챌린지에 대해 생성된 서명을 포함하는 시스템.

청구항 20

제19항에 있어서, 상기 인증 클라이언트는 상기 서명을 확인하기 위해 상기 인증기와 연관된 비공개 키를 사용하는 시스템.

청구항 21

제20항에 있어서, 상기 인증 클라이언트는 성공적인 사용자 인증에 응답하여 상기 클라이언트 장치 상의 상기 인증기들 중 하나 이상을 사용하여 상기 인증 응답을 생성하는 시스템.

청구항 22

제21항에 있어서, 상기 클라이언트 장치 상의 상기 인증기들은 지문 인증기를 포함하는 시스템.

청구항 23

제13항에있어서, 상기 신뢰자 앱으로부터 상기 인증 클라이언트로 상기 제1 인증 관련 통신을 제공하는 것은 상기 신뢰자 앱과 상기 인증 클라이언트 사이의 프로세스간 통신(IPC)을 구현하는 것을 추가로 포함하는 시스템.

청구항 24

제13항에 있어서, 상기 자체 서명 인증서의 상기 제2 키는 상기 제2 통신 채널을 통해 공개 키 파일로 전송되는 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 데이터 처리 시스템의 분야에 관한 것이다. 더 구체적으로, 본 발명은 보안 전송 프로토콜을 사용하여 신뢰를 설정하기 위한 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 생체 측정 센서(biometric sensor)들을 이용하여 네트워크를 통해 보안 사용자 인증을 제공하기 위한 시스템들이 또한 설계되어 왔다. 그러한 시스템들에서는, 원격 서버에 대해 사용자를 인증하기 위해, 인증기에 의해 생성된 점수, 및/또는 다른 인증 데이터가 네트워크를 통해 전송될 수 있다. 예로서, 미국 특허 출원 제2011/0082801호("'801 출원")는 강한 인증(예를 들어, 신분 도용 및 피싱에 대한 보호), 보안 트랜잭션(예를 들어, 트랜잭션에 대한 "브라우저 내 멀웨어(malware in the browser)" 및 "중간자(man in the middle)" 공격에

대한 보호) 및 클라이언트 인증 토큰의 등재/관리(예를 들어, 지문 판독기, 얼굴 인식 장치, 스마트카드, 신뢰 플랫폼 모듈 등)를 제공하는 네트워크 상에서의 사용자 등록 및 인증을 위한 프레임워크를 설명한다.

[0003] 본 출원의 양수인은 '801 출원에서 설명된 인증 프레임워크에 대한 다양한 개량을 개발하였다. 이러한 개량들 중 일부는 본 양수인에게 양도된 다음과 같은 미국 특허 출원들("공계류 중인 출원들")의 세트에서 설명된다: 제13/730,761호, 인증 능력들을 결정하기 위한 조회 시스템 및 방법(Query System and Method to Determine Authentication Capabilities); 제13/730,776호, 다수의 인증 장치들로 효율적으로 등록, 기록, 및 인증하기 위한 시스템 및 방법(System and Method for Efficiently Enrolling, Registering, and Authenticating With Multiple Authentication Devices); 제13/730,780호, 인증 프레임워크 내에서 랜덤 챌린지들을 처리하기 위한 시스템 및 방법(System and Method for Processing Random Challenges Within an Authentication Framework); 제13/730,791호, 인증 프레임워크 내에서 프라이버시 클래스들을 구현하기 위한 시스템 및 방법(System and Method for Implementing Privacy Classes Within an Authentication Framework); 제13/730,795호, 인증 프레임워크 내에서 트랜잭션 시그널링을 구현하기 위한 시스템 및 방법(System and Method for Implementing Transaction Signaling Within an Authentication Framework); 및 제14/218,504호, 진보된 인증 기술들 및 응용들(Advanced Authentication Techniques and Applications)(이하, "'504 출원").

[0004] 간단히, 공계류 중인 출원들은 사용자가 클라이언트 장치 상의 생체 측정 장치들(예를 들어, 지문 센서들)과 같은 인증 장치들(또는 인증기들)에 등록하는 인증 기술들을 설명한다. 사용자가 생체 측정 장치에 등록할 때, (예를 들어, 손가락 스와이핑, 사진 스냅핑, 음성 기록 등에 의해) 생체 측정 참조 데이터가 캡처된다. 이어서, 사용자는 네트워크를 통해 하나 이상의 서버(예를 들어, 공계류 중인 출원들에서 설명된 바와 같은 보안 트랜잭션 서비스들을 갖춘 웹사이트 또는 다른 신뢰자(relying party))에 인증 장치들을 등록한 후에; 등록 프로세스 동안 교환된 데이터(예를 들어, 인증 장치들 내에 제공된 암호 키들)를 이용하여 그러한 서버들에서 인증받을 수 있다. 일단 인증되면, 사용자는 웹사이트 또는 다른 신뢰자와 하나 이상의 온라인 트랜잭션을 수행하는 것이 허가된다. 공계류 중인 출원들에서 설명된 프레임워크에서는, 사용자를 고유하게 식별하는 데 사용될 수 있는 지문 데이터 및 다른 데이터와 같은 민감한 정보를 사용자의 인증 장치 상에 국지적으로 유지하여 사용자의 프라이버시를 보호할 수 있다. '504 출원은, 단지 몇 가지 예로, 복합 인증기들을 설계하고, 인증 보증 레벨들을 지능적으로 생성하고, 비간섭적 사용자 검증을 이용하고, 인증 데이터를 새로운 인증 장치들로 전송하고, 인증 데이터를 클라이언트 리스크 데이터로 증대시키고, 인증 정책들을 적응적으로 적용하고, 신뢰 고리들을 생성하기 위한 기술들을 비롯한 다양한 추가 기술들을 설명한다.

도면의 간단한 설명

[0005] 아래의 도면들과 관련된 아래의 상세한 설명으로부터 본 발명의 더 양호한 이해가 얻어질 수 있으며, 도면들에서:

도 1a 및 도 1b는 보안 인증 시스템 아키텍처의 2개의 상이한 실시예를 나타낸다.

도 2는 키들이 어떻게 인증 장치들 내에 등록될 수 있는지를 보여주는 트랜잭션 도면이다.

도 3은 원격 인증을 보여주는 트랜잭션 도면을 나타낸다.

도 4는 신뢰자와의 인증이 어떻게 신뢰자 앱의 사용을 요구할 수 있는지를 나타낸다.

도 5는 보안 통신 프로토콜을 사용하여 신뢰를 설정함으로써 인증을 하기 위한 시스템의 일 실시예를 나타낸다.

도 6은 보안 통신 프로토콜을 이용하여 신뢰를 설정함으로써 인증하기 위한 방법의 일 실시예를 나타낸다.

도 7은 본 명세서에서 설명되는 클라이언트들 및/또는 서버들을 구현하기 위한 예시적인 데이터 처리 아키텍처를 나타낸다.

도 8은 본 발명에 설명되는 클라이언트들 및/또는 서버들을 구현하기 위한 다른 예시적인 데이터 처리 아키텍처를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0006] 아래에서는 진보된 인증 기술들 및 관련 응용들을 구현하기 위한 기기, 방법 및 기계 판독 가능 매체의 실시예들이 설명된다. 설명 전반에서, 설명의 목적으로, 본 발명의 완전한 이해를 제공하기 위해, 다수의 특정 상세가 설명된다. 그러나, 본 발명은 이러한 특정 상세 중 일부 없이도 실시될 수 있다는 것이 당업자에게 명백할

것이다. 다른 경우들에서, 본 발명의 기본 원리들을 불명확하게 하지 않기 위해 주지 구조들 및 장치들은 도시되지 않거나 블록도 형태로 도시된다.

[0007] 하기에 논의되는 본 발명의 실시예들은 생체 측정 양상 또는 PIN 엔트리와 같은 사용자 검증 능력을 갖는 인증 장치들을 포함한다. 이러한 장치들은 때때로 본 명세서에서 "토큰", "인증 장치" 또는 "인증기"로 지칭된다. 소정 실시예들이 얼굴 인식 하드웨어/소프트웨어(예를 들어, 사용자의 얼굴을 인식하고 사용자의 눈 움직임을 추적하기 위한 카메라 및 관련 소프트웨어)에 집중되지만, 일부 실시예들은 예를 들어 지문 센서, 음성 인식 하드웨어/소프트웨어(예를 들어, 사용자의 음성을 인식하기 위한 마이크 및 관련 소프트웨어) 및 광학 인식 능력(예를 들어, 사용자의 망막을 스캐닝하기 위한 광학 스캐너 및 관련 소프트웨어)을 비롯한 추가 생체 측정 장치들을 이용할 수 있다. 사용자 검증 능력은 PIN 엔트리와 같은 비생체 측정 양상도 포함할 수 있다. 인증기들은 암호 동작 및 키 저장을 위해 신뢰 플랫폼 모듈(TPM), 스마트카드 및 보안 요소와 같은 장치들을 이용할 수 있다.

[0008] 이동 생체 측정 구현에서, 생체 측정 장치는 신뢰자로부터 원격적일 수 있다. 본 명세서에서 사용되는 바와 같이, 용어 "원격"은 생체 측정 센서가 그것이 통신적으로 결합되는 컴퓨터의 보안 경계의 일부가 아니라는 것을 의미한다(예를 들어, 그것이 신뢰자 컴퓨터와 동일한 물리적 울타리 안에 넣어지지 않는다). 예로서, 생체 측정 장치는 네트워크(예를 들어, 인터넷, 무선 네트워크 링크 등)를 통해 또는 USB 포트와 같은 주변장치 입력을 통해 신뢰자에 결합될 수 있다. 이러한 조건들하에서는, 신뢰자가 장치가 신뢰자에 의해 허가된 장치(예를 들어, 허용 가능한 레벨의 인증 강도 및 무결성 보호를 제공하는 장치)인지 그리고/또는 해커가 생체 측정 장치를 손상시켰거나 심지어는 교체했는지를 알기 위한 방법이 존재하지 않을 수 있다. 생체 측정 장치의 신뢰성은 장치의 특정 구현에 의존한다.

[0009] 용어 "국지적"은 본 명세서에서 사용자가 ATM(automatic teller machine) 또는 POS(point of sale) 소매 체크아웃 위치와 같은 특정 위치에서 트랜잭션을 몸소 완료하고 있다는 사실을 지칭하는 데 사용된다. 그러나, 하기에 논의되는 바와 같이, 사용자를 인증하는 데 이용되는 인증 기술들은 원격 서버들 및/또는 다른 데이터 처리 장치들과의 네트워크를 통한 통신과 같은 비위치 컴포넌트들을 포함할 수 있다. 더욱이, 본 명세서에서는 (ATM 및 소매 위치와 같은) 특정 실시예들이 설명되지만, 본 발명의 기본 원리들은 트랜잭션이 최종 사용자에 의해 국지적으로 개시되는 임의의 시스템의 상황 안에서 구현될 수 있다는 점에 유의해야 한다.

[0010] 용어 "신뢰자"는 때때로 본 명세서에서 사용자 트랜잭션이 시도되는 엔티티(예를 들어, 사용자 트랜잭션을 수행하는 웹사이트 또는 온라인 서비스)뿐만 아니라, 본 명세서에서 설명되는 기본 인증 기술들을 수행할 수 있는 그러한 엔티티를 대신하여 구현되는 것으로 때때로 지칭되는 보안 트랜잭션 서버들도 지칭하는 데 사용된다. 보안 트랜잭션 서버들은 신뢰자에 의해 소유되고/되거나 그의 제어하에 있을 수 있거나, 사업 협정의 일부로서 신뢰자에게 보안 트랜잭션 서비스들을 제공하는 제삼자의 제어하에 있을 수 있다.

[0011] 용어 "서버"는 본 명세서에서 클라이언트로부터 네트워크를 통해 요청들을 수신하고, 그에 응답하여 하나 이상의 동작을 수행하고, 전형적으로 동작들의 결과들을 포함하는 응답을 클라이언트로 전송하는 하드웨어 플랫폼 상에서(또는 다수의 하드웨어 플랫폼에 걸쳐) 실행되는 소프트웨어를 지칭하는 데 사용된다. 서버는 클라이언트 요청들에 응답하여 네트워크 "서비스"를 클라이언트들로 제공하거나, 제공하는 것을 돕는다. 중요하게, 서버는 단일 컴퓨터(예를 들어, 서버 소프트웨어를 실행하기 위한 단일 하드웨어 장치)로 한정되지 않으며, 사실상 다수의 하드웨어 플랫폼에 걸쳐, 잠재적으로는 다수의 지리학적 위치에 분산될 수 있다.

[0012] 예시적인 시스템 아키텍처 및 트랜잭션

[0013] 도 1a 및 도 1b는 인증 장치들을 등록하고 사용자를 인증하기 위한 클라이언트측 및 서버측 컴포넌트들을 포함하는 시스템 아키텍처의 2개의 실시예를 나타낸다. 도 1a에 도시된 실시예는 웹사이트와 통신하기 위해 웹 브라우저 플러그인 기반 아키텍처를 이용하는 반면, 도 1b에 도시된 실시예는 웹 브라우저를 필요로 하지 않는다. 사용자를 인증 장치들에 등록하고, 인증 장치들을 보안 서버에 등록하고, 사용자를 검증하는 것과 같은, 본 명세서에서 설명되는 다양한 기술들은 이러한 시스템 아키텍처들 중 어느 것에서도 구현될 수 있다. 따라서, 도 1a에 도시된 아키텍처는 후술하는 실시예들 중 여러 실시예의 동작을 설명하는 데 사용되지만, 동일한 기본 원리들은 (예를 들어, 서버(130)와 클라이언트 상의 보안 트랜잭션 서비스(101) 간의 통신을 위한 매개물로서의 브라우저 플러그인(105)을 제거함으로써) 도 1b에 도시된 시스템 상에서 쉽게 구현될 수 있다.

[0014] 먼저, 도 1a를 참조하면, 도시된 실시예는 최종 사용자를 등록 및 검증하기 위한 (때때로 당업계에서 인증 "토큰" 또는 "인증기"로 지칭되는) 하나 이상의 인증 장치들(110 내지 112)을 구비한 클라이언트(100)를 포함한다.

전술한 바와 같이, 인증 장치들(110 내지 112)은 지문 센서, 음성 인식 하드웨어/소프트웨어(예를 들어, 사용자의 음성을 인식하기 위한 마이크 및 관련 소프트웨어), 얼굴 인식 하드웨어/소프트웨어(예를 들어, 사용자의 얼굴을 인식하기 위한 카메라 및 관련 소프트웨어) 및 광학 인식 능력(예를 들어, 사용자의 망막을 스캐닝하기 위한 광학 스캐너 및 관련 소프트웨어)과 같은 생체 측정 장치, 및 PIN 검증과 같은 비생체 측정 양상들에 대한 지원을 포함할 수 있다. 인증 장치들은 암호 동작들 및 키 저장을 위해 신뢰 플랫폼 모듈(TPM), 스마트카드 또는 보안 요소를 이용할 수 있다.

[0015] 인증 장치들(110 내지 112)은 보안 트랜잭션 서비스(101)에 의해 노출되는 인터페이스(102)(예를 들어, 애플리케이션 프로그래밍 인터페이스 또는 API)를 통해 클라이언트에 통신적으로 결합된다. 보안 트랜잭션 서비스(101)는 네트워크를 통해 하나 이상의 보안 트랜잭션 서버(132, 133)와 통신하기 위한 그리고 웹 브라우저(104)의 상황 내에서 실행되는 보안 트랜잭션 플러그인(105)과 인터페이스하기 위한 보안 애플리케이션이다. 도시된 바와 같이, 인터페이스(102)는 장치 식별 코드, 사용자 식별 코드, 인증 장치에 의해 보호되는 사용자 등록 데이터(예를 들어, 스캐닝된 지문 또는 다른 생체 측정 데이터), 및 본 명세서에서 설명되는 보안 인증 기술들을 수행하는 데 사용되는 인증 장치에 의해 봉인된 키들과 같은, 인증 장치들(110 내지 112) 각각과 관련된 정보를 저장하는 클라이언트(100) 상의 보안 저장 장치(120)에 대한 보안 액세스도 제공할 수 있다. 예를 들어, 하기에 상세히 논의되는 바와 같이, 고유 키가 인증 장치들 각각 내에 저장되고, 인터넷과 같은 네트워크를 통해 서버들(130)에 통신할 때 사용될 수 있다.

[0016] 하기에 논의되는 바와 같이, 웹사이트들(131) 또는 다른 서버들과의 HTTP 또는 HTTPS 트랜잭션들과 같은 소정 타입의 네트워크 트랜잭션들이 보안 트랜잭션 플러그인(105)에 의해 지원된다. 일 실시예에서, 보안 트랜잭션 플러그인은 보안 기업 또는 웹 목적지(130)(아래에서 때때로 간단히 "서버(130)"로 지칭됨) 내의 웹 서버(131)에 의해 웹페이지의 HTML 코드 내에 삽입된 특정 HTML 태그들에 응답하여 개시된다. 그러한 태그의 검출에 응답하여, 보안 트랜잭션 플러그인(105)은 처리를 위해 트랜잭션들을 보안 트랜잭션 서비스(101)로 전송할 수 있다. 게다가, (예를 들어, 보안 키 교환과 같은) 소정 타입의 트랜잭션들을 위해, 보안 트랜잭션 서비스(101)는 구내(즉, 웹사이트와 같은 곳에 배치된) 트랜잭션 서버(132)와의 또는 구외 트랜잭션 서버(133)와의 직접 통신 채널을 개설할 수 있다.

[0017] 보안 트랜잭션 서버들(132, 133)은 후술하는 보안 인증 트랜잭션들을 지원하는 데 필요한 사용자 데이터, 인증 장치 데이터, 키들 및 다른 보안 정보를 저장하기 위한 보안 트랜잭션 데이터베이스(120)에 결합된다. 그러나, 본 발명의 기본 원리들은 도 1a에 도시된 보안 기업 또는 웹 목적지(130) 내의 논리 컴포넌트들의 분리를 필요로 하지 않는다는 점에 유의해야 한다. 예를 들어, 웹사이트(131) 및 보안 트랜잭션 서버들(132, 133)은 단일 물리 서버 또는 개별 물리 서버들 내에 구현될 수 있다. 더욱이, 웹사이트(131) 및 트랜잭션 서버들(132, 133)은 후술하는 기능들을 수행하기 위해 하나 이상의 서버 상에서 실행되는 통합 소프트웨어 모듈 내에 구현될 수 있다.

[0018] 전술한 바와 같이, 본 발명의 기본 원리들은 도 1a에 도시된 브라우저 기반 아키텍처로 한정되지 않는다. 도 1b는 독립 애플리케이션(154)이 보안 트랜잭션 서비스(101)에 의해 제공되는 기능을 이용하여 네트워크를 통해 사용자를 인증하는 대안 구현을 나타낸다. 일 실시예에서, 애플리케이션(154)은 아래에서 상세히 설명되는 사용자/클라이언트 인증 기술들을 수행하기 위해 보안 트랜잭션 서버들(132, 133)에 의존하는 하나 이상의 네트워크 서비스(151)와의 통신 세션들을 설정하도록 설계된다.

[0019] 도 1a 및 도 1b에 도시된 실시예들 중 어느 하나에서, 보안 트랜잭션 서버들(132, 133)은 키들을 생성할 수 있고, 이어서 이 키들은 보안 트랜잭션 서비스(101)로 안전하게 전송되고, 보안 저장소(120) 내에 인증 장치들 내로 저장된다. 게다가, 보안 트랜잭션 서버들(132, 133)은 서버 측의 보안 트랜잭션 데이터베이스(120)를 관리한다.

[0020] 인증 장치들을 원격으로 등록하고 신뢰자와 인증하는 것과 연관된 소정 기본 원리들이 도 2 내지 도 5와 관련하여 설명될 것이며, 이어서 보안 통신 프로토콜들을 사용하여 신뢰를 설정하기 위한 본 발명의 실시예들의 상세한 설명이 이어질 것이다.

[0021] 도 2는 (도 1a 및 도 1b의 클라이언트(100) 상의 장치들(110 내지 112)과 같은) 클라이언트 상의 인증 장치들을 등록하기 위한 일련의 트랜잭션들을 나타낸다. 단순화를 위해, 보안 트랜잭션 서비스(101) 및 인터페이스(102)는 인증 클라이언트(201)로서 함께 조합되고, 보안 트랜잭션 서버들(132, 133)을 포함하는 보안 기업 또는 웹 목적지(130)는 신뢰자(202)로서 표현된다.

[0022] 인증기(예를 들어, 지문 인증기, 음성 인증기 등)의 등록 동안, 인증기와 연관된 키는 인증 클라이언트(201)와 신뢰자(202) 사이에서 공유된다. 도 1a 및 도 1b를 다시 참조하면, 키는 클라이언트(100)의 보안 저장소(120) 및 보안 트랜잭션 서버들(132, 133)에 의해 사용되는 보안 트랜잭션 데이터베이스(120) 내에 저장될 수 있다. 일 실시예에서, 키는 보안 트랜잭션 서버들(132, 133) 중 하나에 의해 생성되는 대칭 키이다. 그러나, 하기에 논의되는 다른 실시예에서는, 비대칭 키들이 사용된다. 이 실시예에서, 공개/비공개 키 쌍은 보안 트랜잭션 서버들(132, 133)에 의해 생성될 수 있다. 이어서, 공개 키는 보안 트랜잭션 서버들(132, 133)에 의해 저장될 수 있으며, 관련 비공개 키는 클라이언트 상의 보안 저장소(120) 내에 저장될 수 있다. 대안 실시예에서, 키(들)는 클라이언트(100) 상에서 (예를 들어, 보안 트랜잭션 서버들(132, 133)보다는 인증 장치 또는 인증 장치 인터페이스에 의해) 생성될 수 있다. 본 발명의 기본 원리들은 임의의 특정 타입의 키들 또는 키들을 생성하는 방식으로 한정되지 않는다.

[0023] 보안 키 프로비저닝 프로토콜은 일 실시예에서 보안 통신 채널을 통해 클라이언트와 키를 공유하는 데 이용된다. 키 프로비저닝 프로토콜의 일례는 DSKPP(Dynamic Symmetric Key Provisioning Protocol)이다(예를 들어, RFC(Request for Comments) 6063 참조). 그러나, 본 발명의 기본 원리들은 임의의 특정 키 제공 프로토콜로 한정되지 않는다. 하나의 특정 실시예에서, 클라이언트는 공개/비공개 키 쌍을 생성하여 공개 키를 서버로 전송하며, 이는 증명 키로 증명될 수 있다.

[0024] 도 2에 도시된 구체적인 상세들로 돌아가서, 등록 프로세스를 개시하기 위하여, 신뢰자(202)는 장치 등록 동안 인증 클라이언트(201)에 의해 제시되어야 하는 랜덤 생성 챌린지(예를 들어, 암호 논스)를 생성한다. 랜덤 챌린지는 제한된 기간 동안 유효할 수 있다. 이에 응답하여, 인증 클라이언트(201)는 신뢰자(202)와의 대역외 보안 접속(예를 들어, 대역외 트랜잭션)을 개시하고, 키 프로비저닝 프로토콜(예를 들어, 전술한 DSKPP 프로토콜)을 사용하여 신뢰자(202)와 통신한다. 보안 접속을 개시하기 위하여, 인증 클라이언트(201)는 랜덤 챌린지를 (잠재적으로는 랜덤 챌린지에 대해 생성된 서명과 함께) 다시 신뢰자(202)에게 제공할 수 있다. 게다가, 인증 클라이언트(201)는 (예를 들어, 등록 중인 인증 장치(들)의 타입을 고유하게 식별하는 인증 증명 ID(AAID)를 이용하여) 등록될 사용자의 아이덴티티(예를 들어, 사용자 ID 또는 다른 코드) 및 인증 장치(들)의 아이덴티티를 전송할 수 있다.

[0025] 신뢰자는 (예를 들어, 사용자 계정 데이터베이스 내의) 사용자 이름 또는 ID 코드를 이용해 사용자를 찾고, (예를 들어, 서명을 사용하거나, 단순히 랜덤 챌린지를 전송된 것과 비교함으로써) 랜덤 챌린지를 확인하고, 하나가 전송되었으면(예를 들어, AAID) 인증 장치의 인증 코드를 확인하고, 사용자 및 인증 장치(들)에 대한 보안 트랜잭션 데이터베이스(예를 들어, 도 1a 및 도 1b의 데이터베이스(120)) 내의 새로운 엔트리를 생성한다. 일 실시예에서, 신뢰자는 그것이 인증에 허용하는 인증 장치들의 데이터베이스를 유지한다. 그것은 등록 중인 인증 장치(들)가 인증에 허용 가능한지 여부를 결정하기 위해 AAID(또는 다른 인증 장치(들) 코드)로 이 데이터베이스에 문의할 수 있다. 만약 그러한 경우, 그것은 등록 프로세스를 계속할 것이다.

[0026] 일 실시예에서, 신뢰자(202)는 등록 중인 각각의 인증 장치에 대한 인증 키를 생성한다. 그것은 키를 보안 데이터베이스에 기록하고, 키 프로비저닝 프로토콜을 사용하여 키를 인증 클라이언트(201)로 다시 전송한다. 일단 완료되면, 인증 장치와 신뢰자(202)는 대칭 키가 사용된 경우에는 동일 키를, 또는 비대칭 키들이 사용된 경우에는 상이한 키들을 공유한다. 예를 들어, 비대칭 키들이 사용된 경우, 신뢰자(202)는 공개 키를 저장하고 비공개 키를 인증 클라이언트(201)에 제공할 수 있다. 신뢰자(202)로부터 비공개 키를 수신하면, 인증 클라이언트(201)는 인증 장치 내에 키를 프로비저닝한다(그것을 인증 인증 장치와 연관된 보안 저장소 내에 저장함). 이어서 그것은 (후술하는 바와 같이) 사용자의 인증 동안 키를 사용할 수 있다. 대안 실시예에서, 키(들)는 인증 클라이언트(201)에 의해 생성되고, 키 프로비저닝 프로토콜은 키(들)를 신뢰자(202)에 제공하는 데 사용된다. 어느 경우이든, 프로비저닝이 완료되면, 인증 클라이언트(201) 및 신뢰자(202)는 각각 키를 갖고, 인증 클라이언트(201)는 신뢰자에게 완료를 통지한다.

[0027] 도 3은 등록된 인증 장치들과 관련된 사용자 인증을 위한 일련의 트랜잭션들을 나타낸다. 장치 등록이 완료되면(도 2에 설명된 바와 같이), 신뢰자(201)는 유효 인증 응답으로서 클라이언트 상의 국지적 인증 장치에 의해 생성된 인증 응답(때때로 "토큰"으로 지칭됨)을 허용할 것이다.

[0028] 도 3에 도시된 구체적인 상세들로 돌아가서, 사용자가 인증을 필요로 하는 신뢰자(202)와의 트랜잭션을 개시하는 것(예를 들어, 신뢰자의 웹사이트로부터 지불을 개시하는 것, 개인 사용자 계정 데이터에 액세스하는 것 등)에 응답하여, 신뢰자(202)는 랜덤 챌린지(예를 들어, 암호 논스)를 포함하는 인증 요청을 생성한다. 일 실시예에서, 랜덤 챌린지는 그와 연관된 시간 제한을 갖는다(예를 들어, 그것은 특정된 기간 동안 유효하다). 신

뢰자는 또한 인증을 위해 인증 클라이언트(201)에 의해 사용될 인증기를 식별할 수 있다. 전술한 바와 같이, 신뢰자는 클라이언트 상에서 이용가능한 각각의 인증 장치를 등록할 수 있고 각각의 등록된 인증기에 대한 공개 키를 저장한다. 따라서, 그것은 인증기의 공개 키를 사용할 수 있거나, 또는 인증기 ID(예를 들어, AAID)를 사용하여 사용될 인증기를 식별할 수 있다. 대안적으로, 그것은 사용자가 선택할 수 있는 인증 옵션들의 목록을 클라이언트에 제공할 수 있다.

[0029] 인증 요청의 수신에 응답하여, 사용자는 (예를 들어, 웹 페이지 또는 인증 애플리케이션/앱의 GUI 의 형태로) 인증을 요청하는 그래픽 사용자 인터페이스(GUI)를 제공받을 수 있다. 이어서 사용자는 인증을 수행한다(예를 들어, 지문 판독기 상의 손가락 스와이핑 등). 이에 응답하여, 인증 클라이언트(201)는 인증기와 연관된 비공개 키를 사용해 랜덤 챌린지에 대한 서명을 포함하는 인증 응답을 생성한다. 그것은 또한 인증 응답 내에 사용자 ID 코드와 같은 다른 관련 데이터를 포함할 수 있다.

[0030] 인증 응답을 수신하면, 신뢰자는 (예를 들어, 인증기와 연관된 공개 키를 사용하여) 랜덤 챌린지에 대한 서명을 확인하고 사용자의 아이덴티티를 확인할 수 있다. 일단 인증이 완료되면, 도시된 바와 같이 사용자는 신뢰자와의 보안 트랜잭션에 들어가도록 허용된다.

[0031] 전송 계층 보안(Transport Layer Security; TLS) 또는 보안 소켓 계층(Secure Sockets Layer; SSL)과 같은 보안 통신 프로토콜이, 도 2 및 도 3에 도시된 트랜잭션들 중 임의의 것 또는 전부에 대해 신뢰자(201)와 인증 클라이언트(202) 사이의 보안 접속을 설정하는 데 사용될 수 있다.

[0032] 보안 전송 프로토콜을 사용하여 신뢰를 설정하기 위한 시스템 및 방법

[0033] 전술된 바와 같이, 원격 인증을 사용하는 소정의 구현예들에서, 신뢰자와 인증 클라이언트 사이에서 안전하게 데이터를 교환하도록 TLS 또는 SSL과 같은 보안 통신 프로토콜이 사용될 수 있다. 간단히, TLS와 SSL은 보통 비보안 통신 채널(예를 들어, 인터넷)을 통해 보안 통신을 제공하는 암호화 프로토콜들이다. 이들은 대칭 키를 교환하기 위해 비대칭 암호화를 구현하는 X.509 인증서를 사용한다. 이 대칭 키는 이어서 통신 세션 동안 사용되어 당사자 사이의 데이터 채널을 암호화한다. 본 상세 설명의 나머지 부분은 TLS의 사용에 중점을 두지만, 본 발명의 기본 원리는 SSL과 같은 다른 암호화 프로토콜을 사용하여 구현 될 수 있다.

[0034] 일 실시예에서, TLS는 신뢰자와 인증 클라이언트 사이의 통신 채널을 보안하고 송신자의 아이덴티티를 확인하기 위해 사용된다. 즉, X.509 인증서에 의해 지원되는 비대칭 암호화를 사용함으로써, 일 당사자(예를 들어, 인증 클라이언트)가 상대방(예를 들어, 신뢰자)의 아이덴티티를 확인할 수 있는 능력을 가질 수 있고, 그 역도 또한 같다. 상대방의 아이덴티티는 예를 들어 신뢰자(예를 들어, "RPNAME")를 식별하거나 인증 클라이언트, 또는 신뢰자(예를 들어, "AppID")와의 통신 채널을 설정하는 데 사용되는 클라이언트 상의 특정 애플리케이션을 식별하는 코드 또는 이름으로 구현될 수 있다. (위에서 제공된 예시들처럼) 인증 클라이언트와 신뢰자 사이에 직접 채널이 존재하는 경우, 데이터가 일반적으로 인터넷을 통해 전송되고 TLS가 항상 사용 가능하기 때문에 TLS 사용은 이러한 용도에 적합하다.

[0035] 그러나 iOS™, Android™ 및 NFC(Near Field Communication) 트랜잭션과 같은 소정 컴퓨팅 장치 플랫폼에서는 이러한 TLS 전제가 적용되지 않는다. 도 4에 일반적으로 도시된 바와 같이, 이들 플랫폼 상에서, 신뢰자 앱(410)과 같은 제삼자 코드는 신뢰자(402)와 인증 클라이언트(401) 사이의 모든 통신을 관리할 것으로 기대된다. 따라서, 신뢰자 앱(410)은 본질적으로 신뢰자(402)와 인증 클라이언트(401) 사이의 중간자와 같이 작용한다. 또한, 인증 클라이언트(401)는 신뢰자 앱(410)에 의해 설정된 TLS 접속의 유효성에 관한 어떠한 정보도 갖지 않는다. 인증 클라이언트(401)는 이러한 결정을 내리고 IPC 메커니즘들을 사용하여 인증 요청을 핸드오프하기 위해 제삼자 코드에 의존해야 한다(도시된 바와 같음). 이러한 IPC 메커니즘들은 송신 앱의 식별 코드(예를 들어, '번들 ID')에 대한 액세스를 가질 수 있지만, 번들 ID를 사용하여 송신자/수신자(예를 들어, RPNAME, AppID)의 아이덴티티의 진위를 확인하는 것은 운영체제, 및 신뢰자 앱을 배포한 앱 스토어에 의해 구현된 검증 프로세스의 보호에 과도하게 의존한다.

[0036] NFC의 경우 전송 메커니즘에 수반되는 번들 ID와 같은 식별 코드가 없으므로 상황이 더욱 악화된다. NFC는 일반 MIME(Multipurpose Internet Mail Extensions) 핸들러에 의해 핸들링된다. 인증 클라이언트(401)는 주장 중인 식별 코드(예를 들어, RPNAME)는 무엇이든 정확하며 인증 요청이 유효한 소스로부터 오고 있다고 가정해야 한다.

[0037] 보다 구체적으로, iOS 장치에서, 인증 클라이언트 (401)와 통신 중인 앱(410)은 다중 요소 인증 클라이언트의 AppDelegate 코드에서 openURL() 호출의 sourceApplication 파라미터를 사용하여 결정된다: -

(BOOL)application:(UIApplication *)application openURL:(NSURL *)url sourceApplication:(NSString *)sourceApplication annotation:(id)annotation.

[0038] 본 예에서 sourceApplication은 호출하고 있는 앱의 번들 ID를 포함한다. 번들 ID는 Apple™ 데이터베이스의 앱을 식별하는, 호출하고 있는 앱의 피-리스트(plist) 매니페스트(manifest) 내의 고유한 문자열이다. 번들 ID는 회사의 기본 URL을 역순 표기로 사용하여 부분적으로 작성하는 것이 권장된다(예를 들어, com.paypal.app). 따라서 Apple은 이 문자열을 검증하여 앱이 다른 응용 프로그램을 스푸핑(spoof)하지는 않는지 확인할 것으로 전제된다.

[0039] Android 장치의 경우 처리 중인 다중 요소 인증 프로세스로 현재의 트랜잭션을 전송했던 신뢰자 프로세스에 할당된 Linux uid를 리턴하기 위해 getCallingUid()가 시스템 Binder에서 먼저 호출되는데. 예를 들면 다음과 같다:

[0040] int callerUId = Binder.getCallingUid();;

[0041] 앱은 이어서 해당 사용자 ID와 연관된 패키지들을 시스템 PackageManager로부터 검색한다. 패키지들은 신뢰자의 기본 URL을 구성 요소로 사용하여 명명되되 역순 표기로 한다(예를 들어, "com.fido.android.sample.app.paypal"). 예를 들어:

[0042] String packageNames[] = mPackageManager.getPackagesForUid(callerUId);;

[0043] NFC의 경우, 상대방 식별자(예를 들어, RPNAME 또는 AppID)에 매핑될 수 있는 신뢰할 수 있는 정보가 없다. Android에서 NFC를 사용하면, 요청은 MIME 핸들러를 통해 도착하며 발신자는 식별 가능하지 않다. 따라서 요청에 포함된 임의의 식별자는 유효하거나 유효하지 않을 수 있다.

[0044] 본 발명의 일 실시예는 신뢰 인증서를 사용하여 인증 요청 및 발신지 식별자에 서명함으로써 이러한 제한을 해결한다. 모바일 장치의 루트 인증서 저장소에 대해 확인될 수 있는 웹 서버로부터의 SSL X.509 인증서는 일 실시예에서 채용되는 하나의 옵션이다. 그러나 신뢰자의 인증 서버는 해당 키에 대한 액세스를 갖지 않을 수 있다. 인증 서버를 위해 새로운 X.509 인증서를 특정하게 생성하는 것도 다른 옵션이지만 이는 또 다른 X.509 인증서를 관리하기 위한 추가 오버헤드를 의미한다.

[0045] 이러한 문제점을 피하기 위해, 도 5에 도시된 본 발명의 일 실시예는 분산 공개 키 인프라스트럭처(PKI)로부터의 자체 서명 인증서를 사용하여 신뢰자(502)의 인증 서버(520)로부터의 인증 요청들 및 대응하는 발신자 식별자(예를 들어, "RPNAME "식별자)를 서명한다. 특히 일 실시예에서, 자체 서명 인증서는 비공개 키(522), 및 인증 서버(520) 상의 공개 키 파일(525)에 저장된 하나 이상의 공개 키로 구성된다. X.509 인증서와 달리 이러한 자체 서명 인증서들은 루트 신뢰 인증서에 그들을 접속시키는 체인이 없기 때문에 자체적으로 신뢰될 수 없다.

[0046] 일 실시예에서, 신뢰를 설정하기 위해, 웹 서버상의 공개 키 파일(525)에 저장된 공개 키는 (예를 들어, TLS 접속을 여는 데 사용되는 기존의 X.509 신뢰 인증서들과 같은) 신뢰 인증서(526)를 사용하여 설정된 보안 통신 채널을 통해 클라이언트 장치(500)(예를 들어, 모바일 스마트 폰) 상의 인증 클라이언트(530)에 전송된다. TLS를 사용하면 공개 키 파일(525)의 취약한 자체 서명 공개 키가 올바른 소유자로부터 얻어지는 것이 보장되는데, 왜냐하면 이들을 인터넷을 통해 웹 서버로부터 전송하기 위해 사용되는 신뢰 인증서/키(526)가 루트 인증서 저장소에 대해 검증될 수 있기 때문이다(X.509 또는 다른 공지의 표준이 사용되는 경우임). 파일(526) 내의 이들 자체 서명 공개 키는 암시적으로 신뢰되고, 발신지 식별자(예를 들어, RPNAME)를 포함하는 인증 요청(523)을 검증하는데 사용될 수 있다.

[0047] 인증 요청(523)은 도 3과 관련하여 전술된 것과 동일한 방식 및 동일한 환경에서 인증 서버(520)에 의해 생성될 수 있다. 예를 들어, 인증 서버(520)는 랜덤 챌린지를 생성하고, 사용될 클라이언트측 인증기를 식별할 수 있다(예를 들어, 인증기에 대해 등록된 공개 키를 이용함). 랜덤 챌린지 및 인증기 ID 정보는 인증 요청(523) 내로 패키징될 수 있다.

[0048] 또한, 일 실시예에서, 인증 요청(523)은 분산 PKI의 비공개 키(522)를 사용하여 서명된다. 언급한 바와 같이, 일 실시예에서, 비공개 키(522)는 파일(525)의 공개 키에 대응한다. 예를 들어, 비공개 키(522)에 의해 생성된 임의의 서명은 공개 키들 중 하나를 사용하여 확인될 수 있다.

[0049] 다시 한번, 신뢰를 설정하기 위해, 인증 서버 (520) 상의 비공개 키(522)를 사용하여 서명된 인증 요청(523)은 (예를 들어, TLS 접속을 여는 데 사용되는 기존의 X.509 신뢰 인증서들과 같은) 신뢰 인증서(521)를 사용하여 설정된 보안 통신 채널을 통해 클라이언트 장치(500) 상의 신뢰자 앱(510)에 전송된다. 일 실시예에서, 신뢰

인증서(521)는 인증 클라이언트(530)와 TLS 채널을 설정하는 데 사용되는 신뢰 인증서(526)와 동일하다. 비공개 키 서명 인증 요청(523)은 이어서 TLS 채널을 사용하여 발신지 식별자(예를 들어, 신뢰자를 식별하는 RPNAME)와 함께 신뢰자 앱(510)에 전송된다.

[0050] 일 실시예에서, 신뢰자 앱(510)은 기본 비공개 키 서명 인증 요청을 추출(즉, TLS 데이터를 스트리핑)하고 이를 클라이언트 장치(500) 상의 인증 클라이언트(530)에 제공한다. 신뢰자 앱(510)은 공지된 프로세스간 통신(IPC) 메커니즘을 사용하여 인증 클라이언트(530)와 통신할 수 있다. 그러나 본 발명의 기본 원리는 클라이언트 장치(500)에 관한 정보를 교환하기 위한 임의의 특정 통신 메커니즘에 제한되지 않는다.

[0051] 인증 클라이언트(530)는 비공개 키 서명 인증 요청(523)을 수신하면 공개 키 파일로부터의 공개 키를 사용하여 서명을 확인한다. 서명이 유효하면 이어서 위에 설명된 바와 같이 인증 응답을 생성한다. 예를 들어, 사용자에 의한 성공적인 인증에 응답하여, 인증 클라이언트(530)는 인증기의 비공개 키를 사용하여 인증 요청(523)에 포함된 랜덤 챌린지에 대한 서명을 생성하고, 결과적인 인증 응답을 (예를 들어, 직접적으로 또는 신뢰자 앱(510)을 통해) 인증 서버(520)에 전송할 수 있다. 인증 서버(520)가 대응하는 공개 인증 키를 사용하여 서명을 검증한 경우, 사용자는 신뢰자(502)에 대해 인증되고 원하는 트랜잭션을 완료하는 것이 허용된다.

[0052] 본 명세서에서 설명된 기술을 사용하여, 인증 요청(523)들 및 발신지 식별자(예를 들어, RPNAME)들은 중앙집중식 SSL X.509 키에 의해 암호학적으로 검증되되, 분산 PKI가 제공하는 유연성 및 관리 오버헤드의 최소치를 유지한다. 이러한 인증서들이 포함된 파일이 소정 웹 서버에 있다는 사실을 사용하여 자체 서명 인증서의 유효성을 암시적으로 신뢰하는 것은 몇 가지 위험을 갖는다. 웹 서버 상에서 이 파일을 수정할 능력을 가진 사람은 누구나 공개 키를 변경할 수 있다. 그러나 파일에 대한 액세스가 X.509 인증서를 관리하는 기능만큼 신중하게 보호된다면, 두 솔루션에서 제공하는 신뢰도는 서로 비슷할 것이다.

[0053] 본 발명의 일 실시예에 따른 방법이 도 6에 도시되어 있다. 방법은 도 5에 도시된 아키텍처를 사용하여 구현될 수 있지만, 임의의 특정 아키텍처로 제한되지는 않는다.

[0054] 601에서, 신뢰자를 대신하여 인증 서버에서 제1 인증 관련 통신이 생성된다. 일 실시예에서, 제1 인증 관련 통신은 (예를 들어, 랜덤 챌린지, 인증기 ID 등을 포함하는) 위에 언급된 인증 요청(523)을 포함한다.

[0055] 602에서, 분산 공개 키 인프라스트럭처(PKI)로부터의 자체 서명 인증서의 제1 키를 사용하여 제1 인증 관련 통신이 서명된다. 일 실시예에서, 제1 키는 위에 논의된 비공개 키(522)를 포함한다.

[0056] 603에서, 기존의 신뢰 통신 인프라스트럭처를 사용하여 클라이언트 장치 상의 신뢰자 앱과 제1 보안 채널이 설정된다. 일 실시예에서, 기존의 신뢰 통신 인프라스트럭처를 사용하는 것은 신뢰 X.509 인증서를 사용하여 신뢰자와 보안 전송 계층 보안(TLS) 채널을 설정하는 것을 포함한다.

[0057] 604에서, 제1 보안 통신 채널을 통해 신뢰자 앱에 제1 인증 관련 통신이 전송된다. 언급된 바와 같이, 일 실시예에서, 발신지 식별자(예를 들어, RPNAME)가 통신과 함께 제공된다.

[0058] 605에서, 기존의 신뢰 통신 인프라스트럭처를 사용하여 제2 보안 통신 채널이 클라이언트 장치 상의 인증 클라이언트와 설정된다. 언급된 바와 같이, 일 실시예에서, 기존의 신뢰 통신 인프라스트럭처를 사용하는 것은 신뢰 X.509 인증서를 사용하여 신뢰자와 보안 TLS 채널을 설정하는 것을 포함한다.

[0059] 606에서, 분산 PKI로부터의 자체 서명 인증서의 제2 키가 제2 보안 통신 채널을 통해 인증 클라이언트로 전송된다. 일 실시예에서, 제2 키는 분산 PKI로부터의 자체 서명 인증서와 연관된 공개 키를 포함한다. (위에서 논의된 바와 같이) 하나 이상의 추가 키들이 공개 키 파일(526)을 통해 또한 제공될 수 있다.

[0060] 607에서, 서명을 갖는 제1 인증 관련 통신이 신뢰자 앱으로부터 인증 클라이언트로 제공된다. 일 실시예에서, 이는 클라이언트 장치 상의 기존의 프로세스간 통신(IPC) 메커니즘을 준수하여 수행된다.

[0061] 608에서, 인증 클라이언트는 제2 키를 사용하여 제1 키를 이용해 생성된 서명을 확인한다. 검증이 성공적이면, 인증 클라이언트는 제1 인증 관련 통신에 응답하여 제2 인증 관련 통신을 생성한다. 예를 들어, 전술된 바와 같이, 제1 인증 관련 통신이 인증 요청을 포함하는 경우, 제2 인증 관련 통신은 인증 응답을 포함할 수 있다. 응답을 생성하기 위해, 인증 클라이언트는 먼저 사용자로 하여금 클라이언트 장치 상에서 인증을 수행도록 요구할 수 있다(예를 들어, 손가락을 스와이핑하고, 음성을 녹음하고, 코드를 입력하는 등). 인증이 성공적인 경우, 인증 클라이언트는 인증 요청과 함께 제공된 랜덤 챌린지와 같은 다른 검증 가능한 정보와 함께 성공적인 인증의 표시를 전송할 수 있다. 인증 서버가 제2 인증 관련 통신을 수신한 경우, 사용자는 신뢰자에 대해 인증

될 수 있고 신뢰자와의 거래를 개시하도록 허용될 수 있다.

[0062] 예시적인 데이터 처리 장치

[0063] 도 11은 본 발명의 일부 실시예들에서 사용될 수 있는 예시적인 클라이언트들 및 서버들을 나타내는 블록도이다. 도 11은 컴퓨터 시스템의 다양한 컴포넌트들을 도시하지만, 이것은 컴포넌트들을 상호접속하는 임의의 특정 아키텍처 또는 방식을 나타내는 것을 의도하지 않는다는 것을 이해해야 하는데, 이는 그러한 상세들이 본 발명과 밀접한 관련이 없기 때문이다. 더 적은 컴포넌트들 또는 더 많은 컴포넌트들을 갖는 다른 컴퓨터 시스템들도 본 발명과 관련하여 사용될 수 있다는 것을 알 것이다.

[0064] 도 7에 도시된 바와 같이, 데이터 처리 시스템의 형태인 컴퓨터 시스템(700)은 처리 시스템(720), 전원(725), 메모리(730) 및 비휘발성 메모리(740)(예를 들어, 하드 드라이브, 플래시 메모리, 상변화 메모리(PCM) 등)와 결합되는 버스(들)(750)를 포함한다. 버스(들)(750)는 당업계에 주지된 바와 같은 다양한 브리지, 제어기 및/또는 어댑터를 통해 서로 접속될 수 있다. 처리 시스템(720)은 메모리(730) 및/또는 비휘발성 메모리(740)로부터 명령어(들)를 회수하고, 명령어들을 실행하여 전술한 바와 같은 동작들을 수행할 수 있다. 버스(750)는 위의 컴포넌트들을 함께 상호접속하고, 또한 그러한 컴포넌트들을 옵션인 독(dock)(760), 디스플레이 제어기 및 디스플레이 장치(770), 입출력 장치들(780)(예를 들어, 네트워크 인터페이스 카드(NIC), 커서 제어(예를 들어, 마우스, 터치스크린, 터치패드 등), 키보드 등) 및 옵션인 무선 송수신기(들)(790)(예를 들어, 블루투스, 와이파이, 적외선 등)에 상호접속한다.

[0065] 도 8은 본 발명의 일부 실시예들에서 사용될 수 있는 예시적인 데이터 처리 시스템을 나타내는 블록도이다. 예를 들어, 데이터 처리 시스템(800)은 핸드헬드 컴퓨터, 개인 휴대 단말기(PDA), 이동 전화, 휴대용 게이밍 시스템, 휴대용 미디어 플레이어, 이동 전화, 미디어 플레이어 및/또는 게이밍 시스템을 포함할 수 있는 태블릿 또는 핸드헬드 컴퓨팅 장치일 수 있다. 다른 예로서, 데이터 처리 시스템(800)은 네트워크 컴퓨터, 또는 다른 장치 내의 내장된 처리 장치일 수 있다.

[0066] 본 발명의 일 실시예에 따르면, 데이터 처리 시스템(800)의 예시적인 아키텍처는 전술한 이동 장치들을 위해 사용될 수 있다. 데이터 처리 시스템(800)은 하나 이상의 마이크로프로세서 및/또는 집적 회로 상의 시스템을 포함할 수 있는 처리 시스템(820)을 포함한다. 처리 시스템(820)은 메모리(810), (하나 이상의 배터리를 포함하는) 전원(825), 오디오 입출력(840), 디스플레이 제어기 및 디스플레이 장치(860), 옵션인 입출력(850), 입력 장치(들)(870) 및 무선 송수신기(들)(830)와 결합된다. 도 8에 도시되지 않은 추가 컴포넌트들도 본 발명의 소정 실시예들에서 데이터 처리 시스템(800)의 일부일 수 있으며, 본 발명의 소정 실시예들에서는 도 8에 도시된 것보다 적은 컴포넌트들이 사용될 수 있다는 것을 알 것이다. 게다가, 도 8에 도시되지 않은 하나 이상의 버스가 당업계에 주지된 바와 같은 다양한 컴포넌트들을 상호접속하는 데 사용될 수 있는 것을 알 것이다.

[0067] 메모리(810)는 데이터 처리 시스템(800)에 의한 실행을 위해 데이터 및/또는 프로그램들을 저장할 수 있다. 오디오 입출력(840)은 마이크 및/또는 스피커를 포함하여, 예를 들어 스피커 및 마이크를 통해 음악을 재생하고/하거나 전화 기능을 제공할 수 있다. 디스플레이 제어기 및 디스플레이 장치(860)는 그래픽 사용자 인터페이스(GUI)를 포함할 수 있다. 무선(예를 들어, RF) 송수신기들(830)(예를 들어, 와이파이 송수신기, 적외선 송수신기, 블루투스 송수신기, 무선 셀룰러 전화 송수신기 등)은 다른 데이터 처리 시스템들과 통신하는 데 사용될 수 있다. 하나 이상의 입력 장치(870)는 사용자가 시스템에 입력을 제공하는 것을 가능하게 한다. 이러한 입력 장치들은 키패드, 키보드, 터치 패널, 멀티 터치 패널 등일 수 있다. 옵션인 다른 입출력(850)은 독에 대한 커넥터일 수 있다.

[0068] 본 발명의 실시예들은 전술한 바와 같은 다양한 단계들을 포함할 수 있다. 단계들은 범용 또는 특수 목적 프로세서가 소정 단계들을 수행하게 하는 기계 실행 가능 명령어들로 구현될 수 있다. 대안적으로, 이러한 단계들은 단계들을 수행하기 위한 하드와이어드 로직을 포함하는 특정 하드웨어 컴포넌트들에 의해, 또는 프로그래밍된 컴퓨터 컴포넌트들과 맞춤형 하드웨어 컴포넌트들의 임의의 조합에 의해 수행될 수 있다.

[0069] 본 발명의 요소들은 또한 기계 실행 가능 프로그램 코드를 저장하기 위한 기계 판독 가능 매체로서 제공될 수 있다. 기계 판독 가능 매체는 플로피 디스켓, 광 디스크, CD-ROM 및 광자기 디스크, ROM, RAM, EPROM, EEPROM, 자기 또는 광학 카드, 또는 전자 프로그램 코드를 저장하기에 적합한 다른 타입의 매체/기계 판독 가능 매체를 포함할 수 있지만 이에 한정되지 않는다.

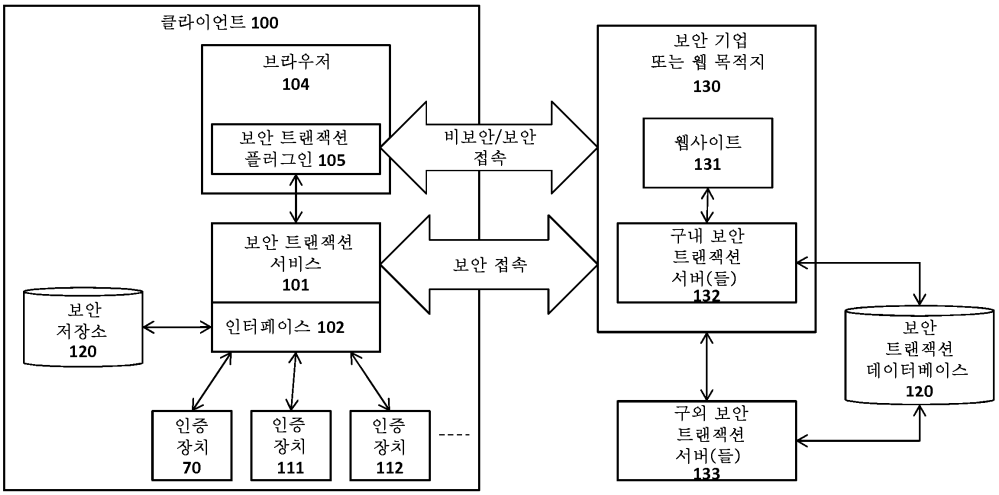
[0070] 위의 설명 전반에서는, 설명의 목적으로, 본 발명의 완전한 이해를 제공하기 위해 다수의 특정 상세가 설명되었다. 그러나, 본 발명은 이러한 특정 상세들 중 일부 없이도 실시될 수 있다는 것이 당업자에게 명백할 것이다.

예를 들어, 본 명세서에서 설명되는 기능 모듈들 및 방법들은 소프트웨어, 하드웨어 또는 이들의 임의 조합으로서 구현될 수 있다는 것을 당업자가 손쉽게 알 수 있을 것이다. 더욱이, 본 명세서에서는 본 발명의 일부 실시예들이 이동 컴퓨팅 환경의 상황 내에서 설명되지만, 본 발명의 기본 원리들은 이동 컴퓨팅 구현으로 한정되지 않는다. 예를 들어 데스크탑 또는 워크스테이션 컴퓨터들을 비롯한 사실상 임의의 타입의 클라이언트 또는 피어 데이터 처리 장치들이 일부 실시예들에서 사용될 수 있다. 따라서, 본 발명의 범주 및 사상은 아래의 청구범위의 관점에서 판단되어야 한다.

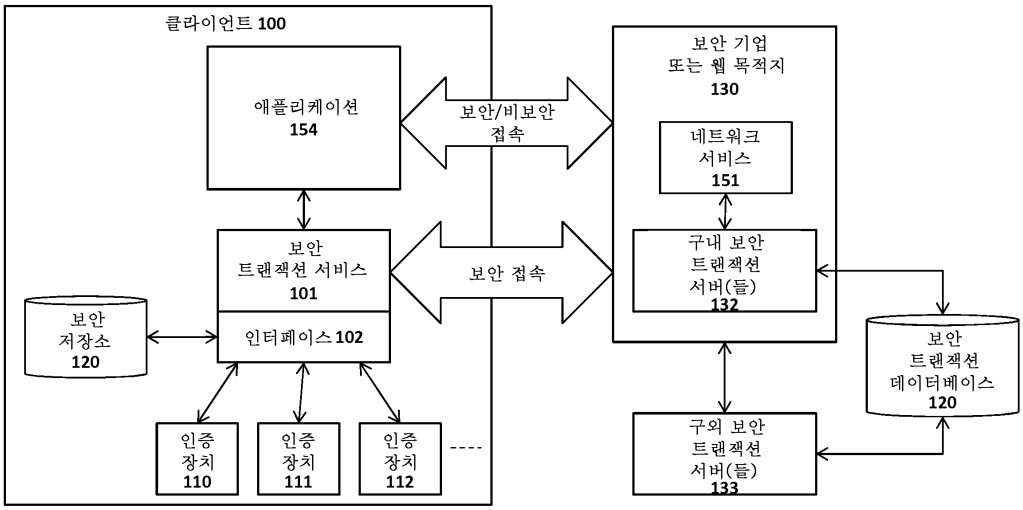
[0071] 본 발명의 실시예들은 전술한 바와 같은 다양한 단계들을 포함할 수 있다. 단계들은 범용 또는 특수 목적 프로세서가 소정 단계들을 수행하게 하는 기계 실행 가능 명령어들로 구현될 수 있다. 대안적으로, 이러한 단계들은 단계들을 수행하기 위한 하드와이어드 로직을 포함하는 특정 하드웨어 컴포넌트들에 의해, 또는 프로그래밍된 컴퓨터 컴포넌트들과 맞춤형 하드웨어 컴포넌트들의 임의의 조합에 의해 수행될 수 있다.

도면

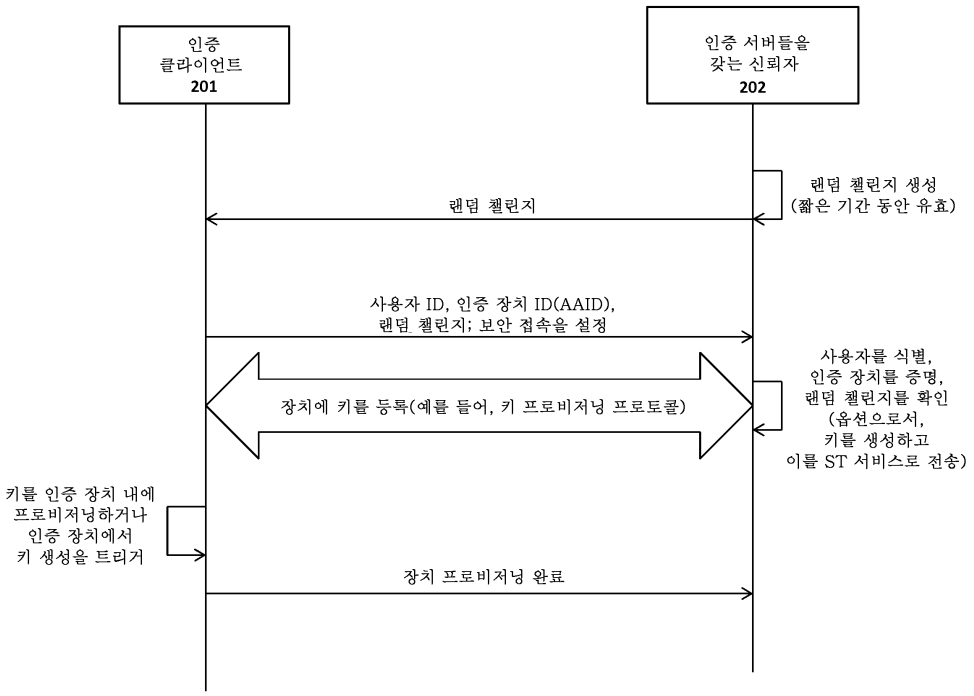
도면1a



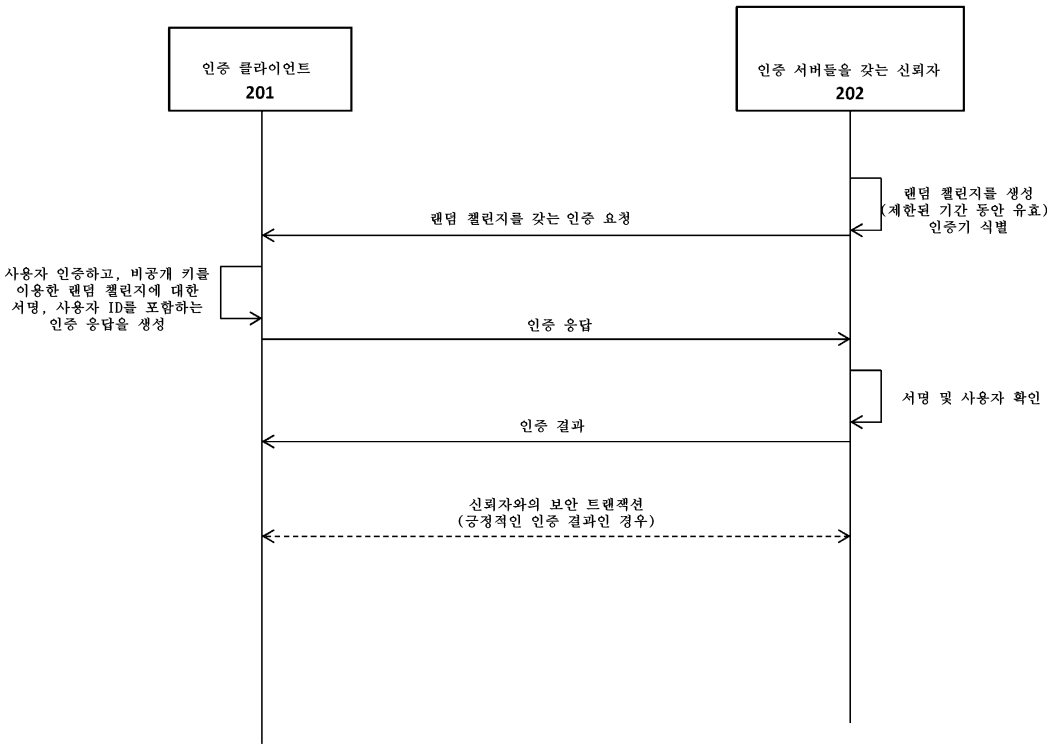
도면1b



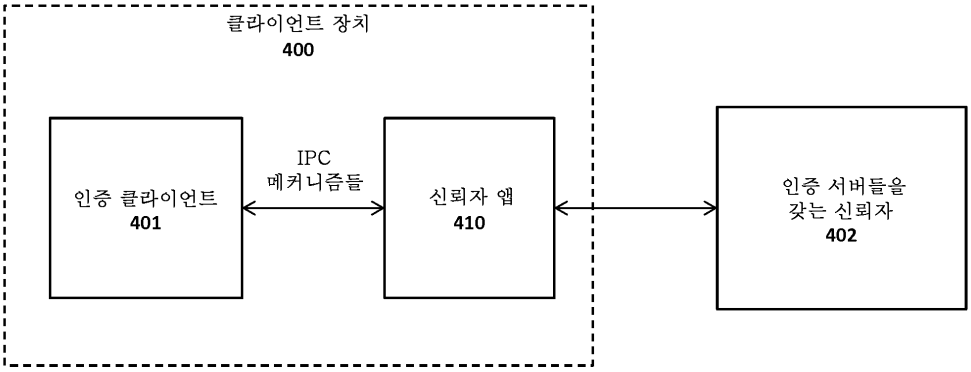
도면2


인증
클라이언트
201
인증 서버들을
갖는 신뢰자
202
랜덤 챌린지 생성
(짧은 기간 동안 유효)
랜덤 챌린지
사용자 ID, 인증 장치 ID(AAID),
랜덤 챌린지; 보안 접속을 설정
사용자를 식별,
인증 장치를 증명,
랜덤 챌린지를 확인
(옵션으로서,
키를 생성하고
이를 ST 서비스로 전송)
장치에 키를 등록(예를 들어, 키 프로비저닝 프로토콜)
키를 인증 장치 내에
프로비저닝하거나
인증 장치에서
키 생성을 트리거
장치 프로비저닝 완료

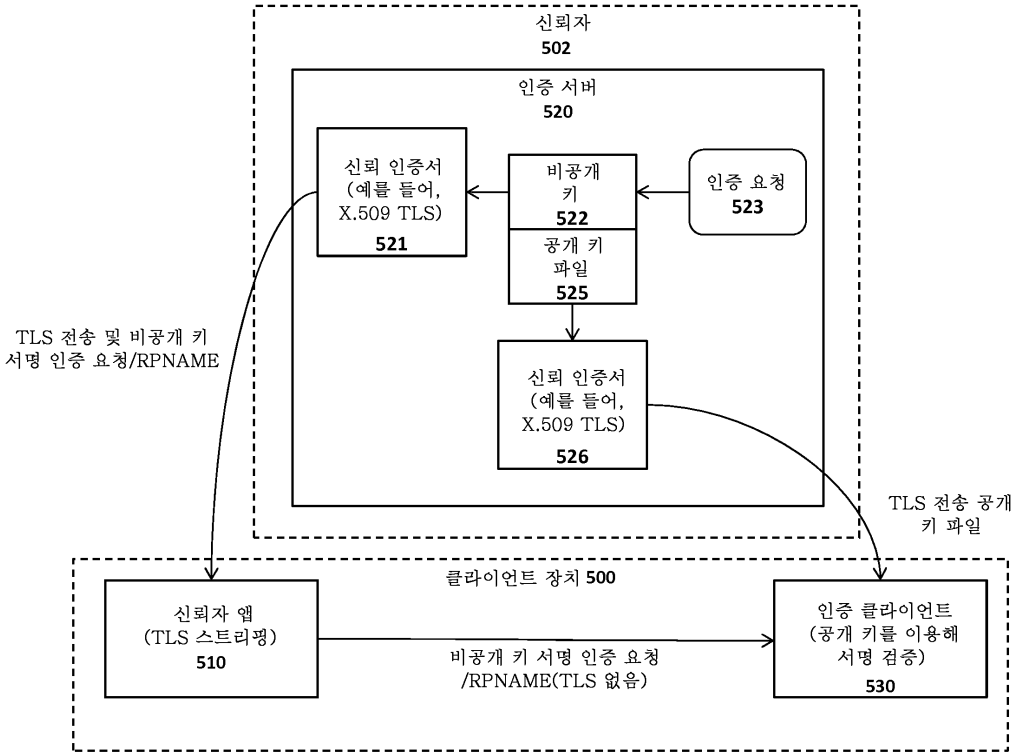
도면3


인증 클라이언트
201
인증 서버들을 갖는 신뢰자
202
랜덤 챌린지를 생성
(제한된 기간 동안 유효)
인증기 식별
랜덤 챌린지를 갖는 인증 요청
사용자 인증하고, 비공개 키를
이용한 랜덤 챌린지에 대한
서명, 사용자 ID를 포함하는
인증 응답을 생성
인증 응답
서명 및 사용자 확인
인증 결과
신뢰자와의 보안 트랜잭션
(긍정적인 인증 결과인 경우)

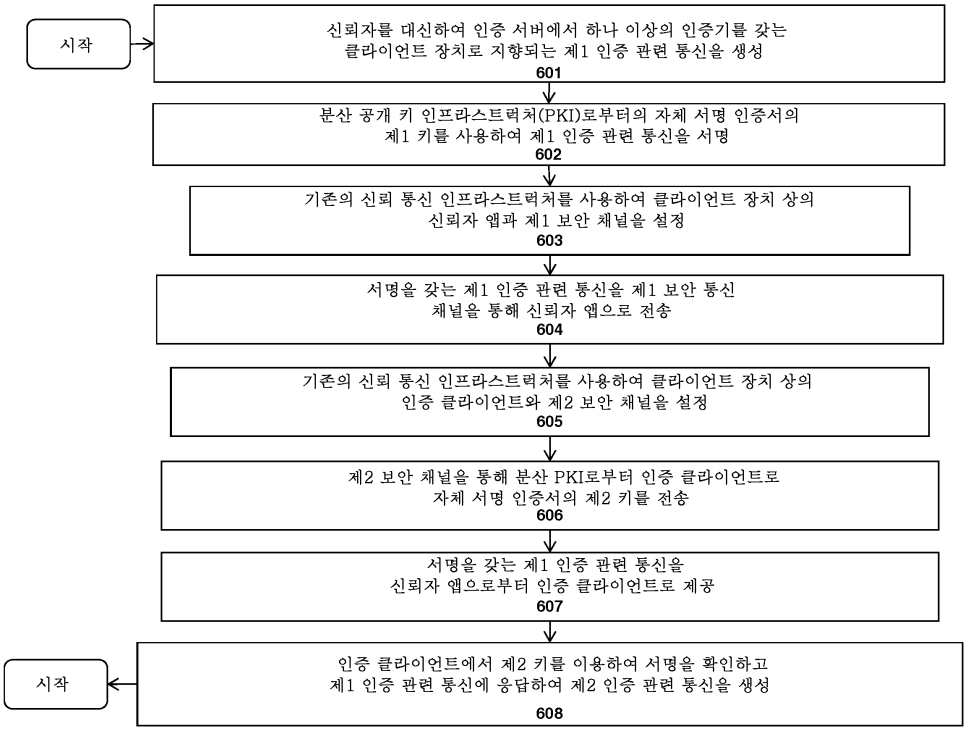
도면4


클라이언트 장치
400
인증 클라이언트
401
IPC
메커니즘들
신뢰자 앱
410
인증 서버들을
갖는 신뢰자
402

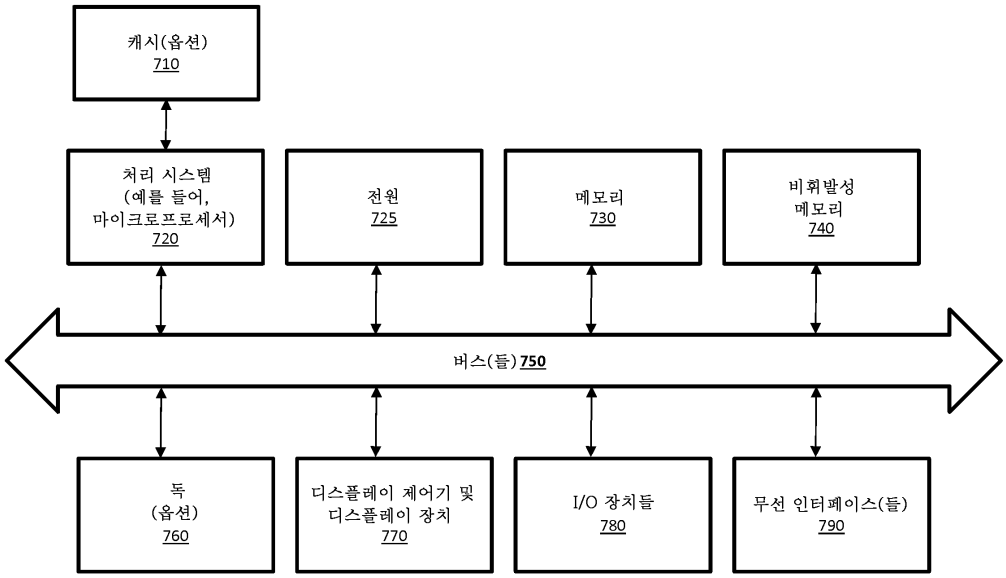
도면5


신뢰자
502
인증 서버
520
신뢰 인증서
(예를 들어,
X.509 TLS)
521
비공개
키
522
인증 요청
523
공개 키
파일
525
신뢰 인증서
(예를 들어,
X.509 TLS)
526
TLS 전송 및 비공개 키
서명 인증 요청/RPNAME
TLS 전송 공개
키 파일
클라이언트 장치 500
신뢰자 앱
(TLS 스트리핑)
510
비공개 키 서명 인증 요청
/RPNAME(TLS 없음)
인증 클라이언트
(공개 키를 이용해
서명 검증)
530

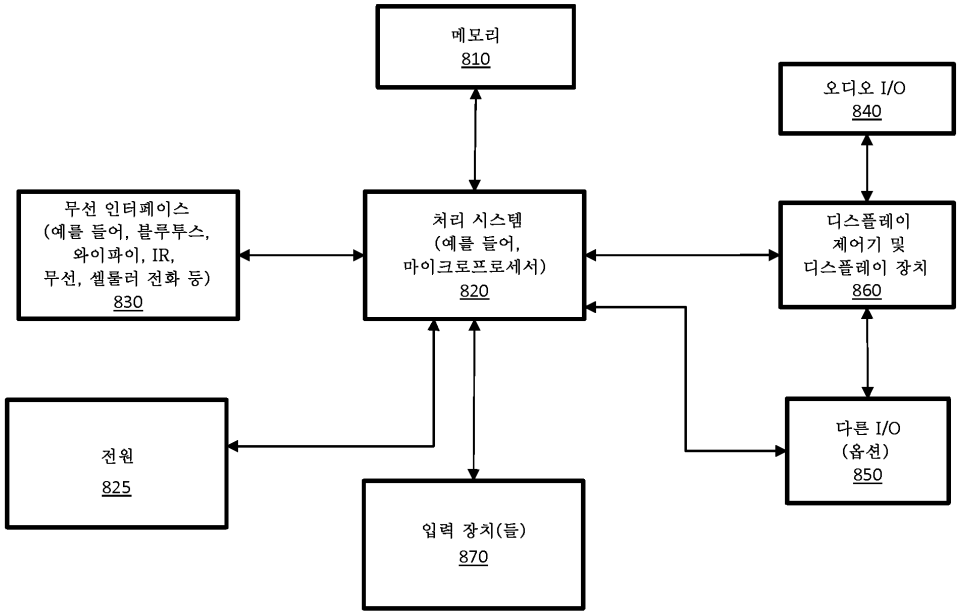
도면6


시작
신뢰자를 대신하여 인증 서버에서 하나 이상의 인증기를 갖는 클라이언트 장치로 지향되는 제1 인증 관련 통신을 생성
601
분산 공개 키 인프라스트럭처(PKI)로부터의 자체 서명 인증서의 제1 키를 사용하여 제1 인증 관련 통신을 서명
602
기존의 신뢰 통신 인프라스트럭처를 사용하여 클라이언트 장치 상의 신뢰자 앱과 제1 보안 채널을 설정
603
서명을 갖는 제1 인증 관련 통신을 제1 보안 통신 채널을 통해 신뢰자 앱으로 전송
604
기존의 신뢰 통신 인프라스트럭처를 사용하여 클라이언트 장치 상의 인증 클라이언트와 제2 보안 채널을 설정
605
제2 보안 채널을 통해 분산 PKI로부터 인증 클라이언트로 자체 서명 인증서의 제2 키를 전송
606
서명을 갖는 제1 인증 관련 통신을 신뢰자 앱으로부터 인증 클라이언트로 제공
607
시작
인증 클라이언트에서 제2 키를 이용하여 서명을 확인하고 제1 인증 관련 통신에 응답하여 제2 인증 관련 통신을 생성
608

도면7


캐시(옵션)
710
처리 시스템
(예를 들어,
마이크로프로세서)
720
전원
725
메모리
730
비휘발성
메모리
740
버스(들) 750
독
(옵션)
760
디스플레이 제어기 및
디스플레이 장치
770
I/O 장치들
780
무선 인터페이스(들)
790

도면8


메모리
810
오디오 I/O
840
무선 인터페이스
(예를 들어, 블루투스,
와이파이, IR,
무선, 셀룰러 전화 등)
830
처리 시스템
(예를 들어,
마이크로프로세서)
820
디스플레이
제어기 및
디스플레이 장치
860
전원
825
다른 I/O
(옵션)
850
입력 장치(들)
870