(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년09월01일
(11) 등록번호 10-2439782
(24) 등록일자 2022년08월30일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *H04W 4/00* (2018.01)
(52) CPC특허분류
H04L 63/0884 (2013.01)
H04W 4/80 (2018.02)
(21) 출원번호 10-2017-7003592
(22) 출원일자(국제) 2015년07월30일
심사청구일자 2020년07월28일
(85) 번역문제출일자 2017년02월08일
(65) 공개번호 10-2017-0041741
(43) 공개일자 2017년04월17일
(86) 국제출원번호 PCT/US2015/042786
(87) 국제공개번호 WO 2016/019089
국제공개일자 2016년02월04일
(30) 우선권주장
14/448,814 2014년07월31일 미국(US)
(56) 선행기술조사문헌
US20050223217 A1*
US20100299738 A1*
US20140189350 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
노크 노크 랩스, 인코포레이티드
미국 캘리포니아 산호세 잔커 로드 2890 스위트 203 (우: 95134)
(72) 발명자
바크다사리안, 다비트
미국 94303 캘리포니아 팔로 알토 스위트 105 겡 로드 2100
(74) 대리인
특허법인 남앤남

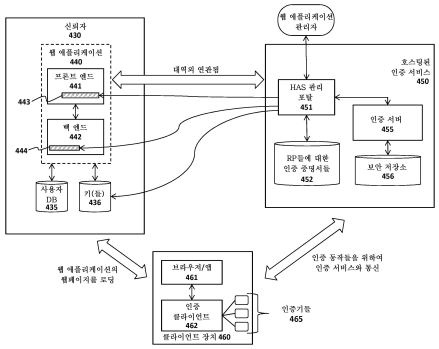
전체 청구항 수 : 총 20 항 심사관 : 홍기완

(54) 발명의 명칭 **호스팅된 인증 서비스를 구현하기 위한 시스템 및 방법**

(57) 요 약

호스팅된 인증 서비스를 위한 시스템, 장치, 방법, 및 기계 판독 가능 매체가 기재된다. 예를 들어, 시스템의 일 실시예는: 신뢰자들에 대한 인증 서비스를 제공하는 호스팅된 인증 서비스 - 호스팅된 인증 서비스는 신뢰자와 키를 공유함으로써 상기 신뢰자를 등록함 -; 및 상기 신뢰자에 의해 호스팅된 애플리케이션 내에 삽입되는 제1 프로그램 코드 컴포넌트 - 상기 제1 프로그램 코드 컴포넌트는 상기 애플리케이션에 액세스하는 클라이언트 장치로 하여금 인증 관련 기능들을 위하여 상기 호스팅된 인증 서비스로 재지향되도록 함 - 를 포함하고, 상기 호스팅된 인증 서비스는 상기 클라이언트 장치와 상기 호스팅된 인증 서비스 사이에서 일어나는 인증 관련 이벤트들을 명시하는 하나 이상의 표명을 상기 신뢰자에게 전송하고, 상기 신뢰자는 상기 키를 이용하여 상기 표명들을 확인한다.

대 표 도 - 도4



명 세 서

청구범위

청구항 1

시스템으로서,

신뢰자들에 대하여 인증 서비스들을 제공하기 위해 호스팅된 인증 서비스를 실행하는 하나 이상의 하드웨어 플랫폼 - 상기 호스팅된 인증 서비스 및 상기 신뢰자들은 별개의 것이고, 상기 호스팅된 인증 서비스는 신뢰자와 키를 공유함으로써 상기 신뢰자를 등록하며, 상기 호스팅된 인증 서비스는 관리 포탈을 포함하고, 신뢰자 관리자가 상기 신뢰자를 대신하여 인증 서비스들을 제공하도록 상기 관리 포탈을 통해 상기 호스팅된 인증 서비스를 구성함 -;

상기 신뢰자에 의해 호스팅된 애플리케이션에 삽입되는, 상기 호스팅된 인증 서비스에 의해 제공된 제1 프로그램 코드 컴포넌트 - 상기 제1 프로그램 코드 컴포넌트는 상기 애플리케이션에 액세스하는 클라이언트 장치로 하여금 사용자 인증 및 다른 인증 관련 기능들을 위해 상기 호스팅된 인증 서비스로 리다이렉팅되도록 하고, 상기 다른 인증 관련 기능들은 하나 이상의 새로운 인증자를 등록하는 것 및 사용자의 클라이언트 장치의 하나 이상의 인증자의 등록을 취소하는 것을 포함함 -; 및

상기 클라이언트 장치와 상기 호스팅된 인증 서비스 사이에서 일어나는 복수의 상이한 인증 관련 이벤트들에 기초하여, 상기 클라이언트 장치를 건너뛰고 상기 신뢰자로 바로 복수의 표명들(assertions)을 전송하는 상기 호스팅된 인증 서비스

를 포함하고,

상기 복수의 표명들 각각은 상기 클라이언트 장치와 상기 호스팅된 인증 서비스 사이에서 일어나는 하나의 상이한 인증 관련 이벤트를 명시하며, 상기 복수의 표명들의 각 표명은 적어도 하나의 표시를 포함하고, 제1 표명이 상기 사용자가 새로운 인증자를 등록했음을 표시하며, 제2 표명이 상기 사용자가 인증자의 등록을 취소했음을 표시하며, 제3 표명이 상기 사용자가 인증자를 이용하여 상기 인증 서비스를 인증했음을 표시하고, 상기 신뢰자는 상기 키를 사용하여 상기 복수의 표명들 각각을 확인하는(validating),

시스템.

청구항 2

제1항에 있어서, 상기 키는 대칭 표명 키를 포함하는, 시스템.

청구항 3

제2항에 있어서, 상기 호스팅된 인증 서비스는 상기 대칭 표명 키를 사용하여 상기 복수의 표명들 중 하나의 표명 내의 데이터에 대한 제1 서명을 생성하고,

상기 신뢰자는 상기 대칭 표명 키의 사본을 사용하여 상기 복수의 표명들 중 상기 하나의 표명 내의 데이터에 대한 제2 서명을 생성하고, 상기 제1 서명을 상기 제2 서명과 비교하여 상기 복수의 표명들 중 상기 하나의 표명을 확인하는,

시스템.

청구항 4

제1항에 있어서, 상기 제1 프로그램 코드 컴포넌트는 HTML(hypertext markup language) 코드를 포함하고, 상기 애플리케이션은 웹 애플리케이션을 포함하는, 시스템.

청구항 5

제1항에 있어서,

상기 신뢰자에 의해 호스팅된 상기 애플리케이션의 백 엔드 컴포넌트에 삽입된 제2 프로그램 코드 컴포넌트를

추가로 포함하고, 상기 제2 프로그램 코드 컴포넌트는 상기 키를 안전하게 저장하는, 시스템.

청구항 6

제5항에 있어서, 상기 애플리케이션은 상기 백 엔드 및 HTML 코드를 포함하는 프론트 엔드를 포함하는 웹 애플리케이션을 포함하는, 시스템.

청구항 7

삭제

청구항 8

제1항에 있어서, 상기 관리 포탈은 상기 애플리케이션의 프론트 엔드에 적용되는 프론트 엔드 코드 및 상기 애플리케이션의 백 엔드에 적용되는 백 엔드 코드를 생성하고, 상기 프론트 엔드 코드는 클라이언트 장치들을 상기 호스팅된 인증 서비스로 리다이렉팅하는데 이용가능하며, 상기 백 엔드 코드는 상기 키를 안전하게 저장하고 액세스하는데 이용가능한, 시스템.

청구항 9

삭제

청구항 10

제1항에 있어서, 상기 복수의 표명들 각각은 인증기 유형, 모델 또는 강도 중 적어도 하나에 대한 표시를 추가로 포함하는, 시스템.

청구항 11

신뢰자와 키를 공유함으로써 호스팅된 인증 서비스에 신뢰자를 등록하는 단계 - 상기 호스팅된 인증 서비스 및 상기 신뢰자는 별개의 것이고, 상기 호스팅된 인증 서비스는 관리 포탈을 포함하며, 신뢰자 관리자가 상기 신뢰자를 대신하여 인증 서비스들을 제공하도록 상기 관리 포탈을 통해 상기 호스팅된 인증 서비스를 구성함 -;

상기 호스팅된 인증 서비스에 의해 제공된 제1 프로그램 코드 컴포넌트를 상기 신뢰자에 의해 호스팅된 애플리케이션에 삽입하는 단계 - 상기 제1 프로그램 코드 컴포넌트는 상기 애플리케이션에 액세스하는 클라이언트 장치로 하여금 사용자 인증 및 다른 인증 관련 기능들을 위해 상기 호스팅된 인증 서비스로 리다이렉팅되도록 하고, 상기 다른 인증 관련 기능들은 하나 이상의 새로운 인증자를 등록하는 것 및 사용자 클라이언트 장치의 하나 이상의 인증자의 등록을 취소하는 것을 포함함 -; 및

상기 클라이언트 장치와 상기 호스팅된 인증 서비스 사이에서 일어나는 복수의 상이한 인증 관련 이벤트들에 기초하여, 상기 클라이언트 장치를 건너뛰고 상기 호스팅된 인증 서비스로부터 상기 신뢰자로 바로 복수의 표명들을 전송하는 단계

를 포함하고,

상기 복수의 표명들 각각은 상기 클라이언트 장치와 상기 호스팅된 인증 서비스 사이에서 일어나는 하나의 상이한 인증 관련 이벤트를 명시하며, 상기 복수의 표명들의 각 표명은 적어도 하나의 표시를 포함하고, 제1 표명이 상기 사용자가 새로운 인증자를 등록했음을 표시하며, 제2 표명이 상기 사용자가 인증자의 등록을 취소했음을 표시하며, 제3 표명이 상기 사용자가 인증자를 이용하여 상기 인증 서비스를 인증했음을 표시하고, 상기 신뢰자는 상기 키를 사용하여 상기 복수의 표명들 각각을 확인하는,

방법.

청구항 12

제11항에 있어서, 상기 키는 대칭 표명 키를 포함하는, 방법.

청구항 13

제12항에 있어서, 상기 호스팅된 인증 서비스는 상기 대칭 표명 키를 사용하여 상기 복수의 표명들 중 하나의

표명 내의 데이터에 대한 제1 서명을 생성하고,

상기 신뢰자는 상기 대칭 표명 키의 사본을 사용하여 상기 복수의 표명들 중 상기 하나의 표명 내의 데이터에 대한 제2 서명을 생성하고, 상기 제1 서명을 상기 제2 서명과 비교하여 상기 복수의 표명들 중 상기 하나의 표명을 확인하는,

방법.

청구항 14

제11항에 있어서, 상기 제1 프로그램 코드 컴포넌트는 HTML 코드를 포함하고, 상기 애플리케이션은 웹 애플리케이션을 포함하는, 방법.

청구항 15

제11항에 있어서,

상기 신뢰자에 의해 호스팅된 상기 애플리케이션의 백 엔드 컴포넌트에 삽입되는 제2 프로그램 코드 컴포넌트를 추가로 포함하고, 상기 제2 프로그램 코드 컴포넌트는 상기 키를 안전하게 저장하는, 방법.

청구항 16

제15항에 있어서, 상기 애플리케이션은 상기 백 엔드 및 HTML 코드를 포함하는 프론트 엔드를 포함하는 웹 애플리케이션을 포함하는, 방법.

청구항 17

삭제

청구항 18

제11항에 있어서, 상기 관리 포탈은 상기 애플리케이션의 프론트 엔드에 적용되는 프론트 엔드 코드 및 상기 애플리케이션의 백 엔드에 적용되는 백 엔드 코드를 생성하고, 상기 프론트 엔드 코드는 클라이언트 장치들을 상기 호스팅된 인증 서비스로 리다이렉팅하는데 이용가능하며, 상기 백 엔드 코드는 상기 키를 안전하게 저장하고 액세스하는데 이용가능한, 방법.

청구항 19

삭제

청구항 20

제11항에 있어서, 상기 복수의 표명들 각각은 인증기 유형, 모델 또는 강도 중 적어도 하나에 대한 표시를 추가로 포함하는, 방법.

청구항 21

프로그램 코드가 저장된 비일시적 기계 판독가능 매체로서,

상기 프로그램 코드는, 기계에 의해 실행될 때, 상기 기계로 하여금,

신뢰자와 키를 공유함으로써 호스팅된 인증 서비스에 신뢰자를 등록하고 – 상기 호스팅된 인증 서비스 및 상기 신뢰자는 별개의 것이고, 상기 호스팅된 인증 서비스는 관리 포탈을 포함하며, 신뢰자 관리자가 상기 신뢰자를 대신하여 인증 서비스들을 제공하도록 상기 관리 포탈을 통해 상기 호스팅된 인증 서비스를 구성함 –;

상기 호스팅된 인증 서비스에 의해 제공된 제1 프로그램 코드 컴포넌트를 상기 신뢰자에 의해 호스팅된 애플리케이션에 삽입하고 – 상기 제1 프로그램 코드 컴포넌트는 상기 애플리케이션에 액세스하는 클라이언트 장치로 하여금 사용자 인증 및 다른 인증 관련 기능들을 위해 상기 호스팅된 인증 서비스로 리다이렉팅되도록 하고, 상기 다른 인증 관련 기능들은 하나 이상의 새로운 인증자를 등록하는 것 및 사용자 클라이언트 장치의 하나 이상의 인증자의 등록을 취소하는 것을 포함함 –; 그리고

상기 클라이언트 장치와 상기 호스팅된 인증 서비스 사이에서 일어나는 복수의 상이한 인증 관련 이벤트들에 기초하여, 상기 클라이언트 장치를 건너뛰고 상기 호스팅된 인증 서비스로부터 상기 신뢰자로 바로 복수의 표명들을 전송하는

동작들을 수행하도록 하고,

상기 복수의 표명들 각각은 상기 클라이언트 장치와 상기 호스팅된 인증 서비스 사이에서 일어나는 하나의 상이한 인증 관련 이벤트를 명시하며, 상기 복수의 표명들의 각 표명은 적어도 하나의 표시를 포함하고, 제1 표명이 상기 사용자가 새로운 인증자를 등록했음을 표시하며, 제2 표명이 상기 사용자가 인증자의 등록을 취소했음을 표시하며, 제3 표명이 상기 사용자가 인증자를 이용하여 상기 인증 서비스를 인증했음을 표시하고, 상기 신뢰자는 상기 키를 사용하여 상기 복수의 표명들 각각을 확인하는,

비일시적 기계 판독가능 매체.

청구항 22

제21항에 있어서, 상기 키는 대칭 표명 키를 포함하는, 비일시적 기계 판독가능 매체.

청구항 23

제22항에 있어서, 상기 호스팅된 인증 서비스는 상기 대칭 표명 키를 사용하여 상기 복수의 표명들 중 하나의 표명 내의 데이터에 대한 제1 서명을 생성하고,

상기 신뢰자는 상기 대칭 표명 키의 사본을 사용하여 상기 복수의 표명들 중 상기 하나의 표명 내의 데이터에 대한 제2 서명을 생성하고, 상기 제1 서명을 상기 제2 서명과 비교하여 상기 복수의 표명들 중 상기 하나의 표명을 확인하는, 비일시적 기계 판독가능 매체.

청구항 24

제21항에 있어서, 상기 제1 프로그램 코드 컴포넌트는 HTML 코드를 포함하고, 상기 애플리케이션은 웹 애플리케이션을 포함하는, 비일시적 기계 판독가능 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 데이터 처리 시스템의 분야에 관한 것이다. 더 구체적으로, 본 발명은 호스팅된 인증 서비스를 구현하기 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(예로서, 신분 도용 및 피싱에 대한 보호), 보안 트랜잭션(예로서, 트랜잭션에 대한 "브라우저 내 멀웨어(malware in the browser)" 및 "중간자(man in the middle)" 공격에 대한 보호) 및 클라이언트 인증 토큰의 등재/관리(예로서, 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 출원들의 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 프레

임워크 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"). 이러한 출원들은 때때로 본 명세서에서 ("공계류 중인 출원들")로 지칭된다.

[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 장치에 등록할 때, (예를 들어, 손가락 스와이핑, 사진 스냅핑, 음성 기록 등에 의해) 생체 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 등록/프로비저닝한 후에; 등록 프로세스 동안 교환된 데이터(예를 들어, 인증 장치들 내에 프로비저닝된 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.

[0005] '504 출원은, 단지 몇 가지 예로, 복합 인증기들을 설계하고, 인증 보증 레벨들을 지능적으로 생성하고, 비간섭적(non-intrusive) 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

[0006] 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 호스팅된 인증 서비스를 구현하기 위한 시스템의 일 실시예를 나타낸다.

도 5는 신뢰자를 호스팅된 인증 서비스에 등록하기 위한 방법의 일 실시예를 나타낸다.

도 6은 호스팅된 인증 서비스를 이용하기 위한 방법의 일 실시예를 나타낸다.

도 7은 서버들 및/또는 클라이언트들을 위해 사용되는 컴퓨터 아키텍처의 일 실시예를 나타낸다.

도 8은 서버들 및/또는 클라이언트들을 위해 사용되는 컴퓨터 아키텍처의 일 실시예를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0007] 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 구체적인 상세 사항들이 설명된다. 그러나, 본 발명은 이러한 구체적인 상세 사항들 중 일부가 없이도 실시될 수 있다는 것이 통상의 기술자에게 명백할 것이다. 다른 경우들에서, 본 발명의 기본 원리들을 불명확하게 하지 않기 위해 주지 구조들 및 장치들은 도시되지 않거나 블록도 형태로 도시된다.

[0008] 하기에 논의되는 본 발명의 실시예들은 생체 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 장치들을 이용할 수 있다. 사용자 검증 능력은 PIN 엔트리와 같은 비생체 양상도 포함할 수 있다. 인증기들은 암호 동작 및 키 저장을 위해 신뢰 플랫폼 모듈(TPM), 스마트카드 및 보안 요소와 같은 장치들을 이용할 수 있다.

[0009] 이동 생체 구현에서, 생체 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 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 장치를 손상시켰거나 심지어는 교체했는지를 알기 위한 방법이 존재하지 않을 수 있다. 생체 장치의 신뢰성은 장치의 특정 구현에 의존한다.

[0010] 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.

[0011] 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.

[0012] 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.

[0013] 예시적인 시스템 아키텍처 및 트랜잭션

[0014] 도 1a 및 도 1b는 인증 장치들을 등록하고(또한 때때로 "프로비저닝"으로 지칭됨) 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.

[0015] 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 장치, 및 PIN 검증과 같은 비생체 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.

[0016] 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 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.

[0017] 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 유형의 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.

[0018] 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.

[0019] 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 구현예를 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.

[0020] 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.

[0021] 원격으로 인증 장치들을 등록하고 신뢰자를 인증하는 것과 연관된 특정 기본 원리들이 도 2 또는 도 3에 대하여 기술되고, 이어서 보안 통신 프로토콜을 이용하여 신뢰를 구축하기 위한 발명의 실시예들의 상세한 설명이 기재될 것이다.

[0022] 도 2는 클라이언트 상의 인증 장치들(예컨대 도 1a 및 도 1b의 클라이언트(100) 상의 디바이스들(110 내지 112))을 등록하기(때때로 인증 장치들을 "프로비저닝"하는 것으로 지칭됨) 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.

[0023] 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. 대안적인 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.

[0024] 보안 키 프로비저닝 프로토콜은 일 실시예에서 보안 통신 채널을 통해 클라이언트와 키를 공유하는 데

채용된다. 키 프로비저닝 프로토콜의 일례는 동적 대칭 키 프로비저닝 프로토콜(DSKPP)(예를 들어, RFC(Request for Comments) 6063 참조)이다. 그러나, 본 발명의 기본 원리들은 임의의 특정 키 프로비저닝 프로토콜로 한정되지 않는다. 하나의 특정 실시예에서, 클라이언트는 공개/비공개 키 쌍을 생성하여 공개 키를 서버로 전송하며, 이는 증명 키로 증명될 수 있다.

[0025] 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 이용하여 신뢰자(202)와 통신한다. 보안 접속을 개시하기 위하여, 인증 클라이언트(201)는 랜덤 챌린지를 다시 신뢰자(202)에 제공할 수 있다(잠재적으로는 랜덤 챌린지에 대해 생성된 서명과 함께). 게다가, 인증 클라이언트(201)는 (예를 들어, 프로비저닝되는 인증 장치(들)의 타입을 고유하게 식별하는 인증 증명 ID(AAID)를 이용하여) 프로비저닝될 등록될 사용자의 아이덴티티(예를 들어, 사용자 ID 또는 다른 코드) 및 인증 장치(들)의 아이덴티티를 전송할 수 있다.

[0026] 신뢰자는 사용자 이름 또는 ID 코드(예를 들어, 사용자 계정 데이터베이스)를 이용하여 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 대해 보안 트랜잭션 데이터베이스(예를 들어, 도 1a 및 도 1b의 데이터베이스(120)) 내의 새로운 엔트리를 생성한다. 일 실시예에서, 신뢰자는 그것이 인증을 허용하는 인증 장치들의 데이터베이스를 유지한다. 그것은 프로비저닝되는 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.

[0027] 일 실시예에서, 신뢰자(202)는 프로비저닝되는 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 내로 키를 프로비저닝한다(그것을 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.

[0028] 도 3은 프로비저닝된 인증 장치들을 이용한 사용자 인증을 위한 일련의 트랜잭션들을 나타낸다. 장치 등록이 완료되면(도 2에 설명된 바와 같이), 신뢰자(202)는 유효한 인증 응답으로서 클라이언트 상의 국지적 인증 장치에 의해 생성된 인증 응답(때때로 "토큰"으로 지칭됨)을 허용할 것이다.

[0029] 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). 신뢰자는 또한 인증을 위해 인증 클라이언트(201)에 의해 사용될 인증기를 식별할 수 있다. 전술한 바와 같이, 신뢰자는 클라이언트 상에서 이용가능한 각각의 인증 장치를 프로비저닝할 수 있고 각각의 프로비저닝된 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.

[0030] 인증 요청의 수신에 응답하여, 사용자는 (예를 들어, 웹 페이지 또는 인증 애플리케이션/앱의 GUI 의 형태로) 인증을 요청하는 그래픽 사용자 인터페이스(GUI)를 제시받을 수 있다. 이어서 사용자는 인증을 수행한다(예를 들어, 지문 판독기 상에서 손가락을 스와이핑하는 등). 이에 응답하여, 인증 클라이언트(201)는 인증기와 연관된 비공개 키를 이용해 랜덤 챌린지에 대한 서명을 포함하는 인증 응답을 생성한다. 그것은 또한 인증 응답 내에 사용자 ID 코드와 같은 다른 관련 데이터를 포함할 수 있다.

[0031] 인증 응답을 수신하면, 신뢰자는 (예를 들어, 인증기와 연관된 공개 키를 사용하여) 랜덤 챌린지에 대한 서명을

확인하고 사용자의 신원을 확인할 수 있다. 일단 인증이 완료되면, 도시된 바와 같이, 신뢰자와의 보안 트랜잭션에 들어가도록 허용된다.

[0032] 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.

[0033] 호스팅된 인증 서비스를 구현하기 위한 시스템 및 방법

[0034] 본 발명의 일 실시예는 다수의 신뢰자들에 병렬로 완전 인증 서버 기능을 제공하지만, 신뢰자 개발자에 의한 최소한의 통합 노력을 요구하는 호스팅된 인증 서비스를 포함한다.

[0035] 통상적인 인증 서버 구현예들은 신뢰자의 네트워크 기반구조 내에 활용된다. 이는 중요한 보안 자산이 자신들만의 기반구조 외부로 반출되지 않도록 하는 정책을 갖는 큰 조직을 위한 공통 활용 옵션이다. 그러나 인증 서버를 기존의 기반구조에 통합시키는 것은 쉬운 업무가 아니며 상당한 투자를 필요로 할 수 있다.

[0036] 일부 신뢰자들은 그러한 투자를 포기하고 대신에 동일한 인증 서버 능력을 제공하면서 통합의 복잡함을 숨기는 호스팅된 인증 서비스와의 통합을 선호할 수 있다. 그러나, 호스팅된 인증 서비스들이 수용되기에 충분한 보안 메커니즘들이 준비되어야 한다.

[0037] 도 4에 나타난 바와 같이, 본 발명의 일 실시예는 위에서 언급한 인증 능력을 제공하기 위하여 네트워크(예를 들어, 인터넷)를 통해 신뢰자(430)에 통신적으로 결합된 온라인 시스템으로서 구현된 호스팅된 인증 서비스(HAS)(450)를 포함한다. 도시된 바와 같이, HAS 기반 아키텍처는 3개의 컴포넌트를 포함한다: 신뢰자(RP) 웹 애플리케이션(440); 호스팅된 인증 서비스(450); 및 인증기(들)(465), 인증 클라이언트(462), 및 브라우저 또는 애플리케이션(461)으로 구성된 클라이언트 장치(460).

[0038] 일 실시예에서, RP 웹 애플리케이션(440)은 웹 기반 온라인 서비스, 예컨대, 금융 기관 웹사이트, 소셜 네트워크 웹사이트, 웹 기반 이메일 서비스, 웹 기반 엔터테인먼트 포탈 등이다. 그것은 웹 애플리케이션(440) 및 로그인 시스템에 의해 제공되는 서비스에 가입한 사용자(435)의 데이터베이스를 갖는다. RP 웹 애플리케이션(440)은 통상적으로 프론트 엔드 컴포넌트(441) 및 백 엔드 컴포넌트(442)로 설계된다. 프론트 엔드 컴포넌트(441)는 사용자 요청에 응답하여 동적으로 웹 페이지를 생성하기 위하여 HTML(Hypertext Markup Language) 코드 또는 기타 웹 기반 코드로 구현된 웹 서버일 수 있다. 백 엔드 컴포넌트(442)는 통상적으로 하나 이상의 데이터베이스(435)에 액세스하고, 프론트 엔드 컴포넌트(441)에 의해 생성되는 웹 페이지에 사용되는 기본 데이터를 검색 및/또는 생성하기 위한 비지니스 로직(business logic)을 포함한다. 예를 들어, 신뢰자가 금융 기관인 경우, 백 엔드 코드(442)는 사용자 요청에 응답하여 계정 데이터를 포함하는 데이터베이스(435)에 액세스할 수 있다. 이어서 백 엔드 컴포넌트(442)는 계정 데이터를 이용하여 계산을 수행하고/하거나 단순히 계정 데이터를 프론트 엔드 컴포넌트(441)를 제공할 수 있고, 이는 이후에 계정 데이터 또는 웹 페이지 내의 계정 데이터를 이용하여 수행되는 계산을 포함할 것이다. 기본 데이터가 사용자에게 표시되는 방식은 통상적으로 프론트 엔드 컴포넌트(441)에 의해 정의된다.

[0039] 일 실시예에서, 호스팅된 인증 서비스(450)는 신뢰자들(430)을 대신하여 활용되는 인증 서버(455)를 갖는 온라인 서비스이다. 이전에 논의된 바와 같이, 인증 클라이언트(462)를 갖춘 클라이언트 장치(460)는 그것의 인증기(465)를 인증 서버(455)에 등록할 수 있다(예를 들어, 도 2 참조). 이어서 인증기들(465)과 연관된 키 및 기타 증명서는 인증 서버(455)에 의해 보안 저장소(456)에 저장될 수 있다(그리고 도 3에 예시된 바와 같이 검색되어 최종 사용자를 인증함). 일 실시예에서, 도 4에 예시된, 호스팅된 인증 서비스(450)는 또한 다수의 RP 웹 애플리케이션들(440)에 대한 등록된 인증 증명서들(인증 등록)을 저장하기 위한 데이터베이스(452)를 유지한다.

[0040] 언급한 바와 같이, 클라이언트 장치(460)는 인증 클라이언트(462)를 구비하고 인증기(465)에 액세스하는 랩톱, 태블릿, 전화기, 또는 임의의 기타 데이터 처리 장치일 수 있다. 클라이언트 장치는 또한 신뢰자들(430)에 의해 제공되는 서비스들에 액세스하는(예를 들어, 신뢰자 웹사이트 또는 다른 형태의 온라인 서비스에 액세스하는) 브라우저 또는 애플리케이션(461)을 포함한다.

[0041] 도 4는 RP 웹 애플리케이션(440)은 호스팅된 인증 서비스(아래에 논의됨)와 대역외 연관성을 갖고, RP 웹 애플리케이션의 웹 페이지는 호스팅된 인증 서비스(450)와의 통신을 관리하는 일 실시예를 나타낸다. 도 4에 나타난 호스팅된 인증 아키텍처는 RP 웹 애플리케이션 개발자들에게 많은 이익을 제공한다. 특히, 사용자들은 임의의 기타 인증 기반 웹 애플리케이션을 이용하는 것과 동일한 사용자 경험을 갖는다. 또한, 신뢰자들은 인증 증명서들을 내부적으로 유지할 필요없이, 웹 애플리케이션(440)의 백 엔드(442) 및 프론트 엔드(441) 상에 작은

통합 노력만이 요구된다(아래에 논의되는 바와 같음).

[0042] 일 실시예에서, 통합 프로세스는 RP 웹 애플리케이션(440)을 호스팅된 인증 서비스(450)에 등록함으로써 개시된다. 웹 애플리케이션 관리자(예를 들어, 신뢰자의 정보 기술 스태프의 구성원)는 호스팅된 인증 서비스 관리 포탈(451)을 통해 액세스할 수 있고, 필요한 상세 사항들(예를 들어, 아래에 논의되는 바와 같이 웹 애플리케이션(440)에 관련된 정보)을 제공함으로써 계정을 생성할 수 있다. 일 실시예에서, 신뢰자 관리자는 관리 포탈(451)에 액세스하기 위하여 미리 인증 증명서들(예를 들어, PIN 또는 패스워드와 같은 비밀 코드)이 제공된다. 그러면 관리자는 증명서들을 이용하여 관리 포탈(451)에 로그인 할 수 있다. 일 실시예에서, 관리 포탈(451)은 관리자의 브라우저를 통해 액세스가능한 웹 기반 포탈이다. 그러나, 본 발명의 기본 원리는 관리 포탈(451)에 액세스하는 임의의 특정 방식에 한정되지 않는다.

[0043] 웹 애플리케이션 관리자는 관리 포탈(451)에 필요한 로그인 증명서들 및 기타 적절한 정보, 예컨대, 웹 애플리케이션의 프론트 엔드 프로그램 코드 및 백 엔드 프로그램 코드에 액세스하는 데 필요한 네트워크 어드레스(들)를 제공할 수 있다. 일 실시예에서, 웹 애플리케이션 관리자로부터 웹 애플리케이션(440)을 호스팅된 인증 서비스(450)에 등록하기 위한 요청에 응답하여, 관리 포탈(451)은 웹 애플리케이션(440)의 프론트 엔드(441)(예를 들어, 웹 애플리케이션의 웹페이지)에 포함되는 HTML 코드(443)를 생성한다. HTML 코드(443)는 pure Javascript, HTML 아이프레임에서 또는 웹 애플리케이션(440)과 호환되는 임의의 기타 프로그래밍 언어를 이용하여 구현될 수 있다. 일 실시예에서, HTML 코드는 웹 애플리케이션(440) 프로그램 코드(예를 들어, 프론트 엔드 코드(441))와 직접 통신할 것이다.

[0044] 일 실시예에서, 호스팅된 인증 서비스 포탈(451)은 또한 웹 애플리케이션의 백 엔드(442)에 포함되는 백 엔드 코드(444)를 생성한다. 관리 포탈(451)에 의해 생성되는 HTML 코드(443) 및 백 엔드 코드(444)는 도 4의 웹 애플리케이션(440)의 활성화 경우에 적용되는 것으로 도시된다. 그러나, 일 실시예에서, 새로운 코드(443 및 444)의 설치는 웹 애플리케이션의 실행 이전에 수행될 수 있다(예를 들어, 대용량 저장 장치에 저장된 애플리케이션 바이너리 및 라이브러리에 적용됨).

[0045] 일 실시예에서, 호스팅된 인증 서비스 포탈(451)은 또한 암호 키(예를 들어, 대칭 키 또는 증명서)를 생성하는데, 이는 본 명세서에서 호스팅된 인증 서비스 "표명 키"로 지칭되며, 이후 웹 애플리케이션의 백엔드 기반구조에서 보안 저장소(436)에 저장된다. 일 실시예에서, 이후에 키(436)는 백 엔드(442)에 의해 호스팅된 인증 서비스(450) 표명들(아래에 논의되는 바와 같음)을 확인하는 데 사용된다. 호스팅된 인증 서비스 코드(443 및 444)를 웹 애플리케이션에 통합하고 키(들)(436)을 제공한 이후에, 통합은 완료된다.

[0046] 통합 프로세스가 완료되면, 웹 애플리케이션 사용자들은 클라이언트측 인증기들(465)을 이용하여 신뢰자(430)로 인증하기 시작할 수 있다. 일 실시예에서, 호스팅된 인증 서비스(450)에 의해 제공된 HTML 코드(443)는 인증 관련 통신을 포함하는 사용자 인증 경험을 관리할 것이다. 일 실시예에서, 일단 사용자의 브라우저(461)에 다운로드되면, HTML 코드(443)는 직접 인증 클라이언트(462)와 통신하여 인증 클라이언트(462)를 호스팅된 인증 서비스(450) 상의 인증 서버(455)로 인도할 것이다. 일 실시예에서, HTML 코드(443)는 플러그인(예를 들어, 도 1a에 도시된 보안 트랜잭션 플러그인(101))과 통신하는데, 이는 클라이언트 장치의 브라우저(461) 상에 설치되어 호스팅된 인증 서비스(450) 및 인증 클라이언트(462)와의 보안 통신을 가능하게 한다.

[0047] 일 실시예에서, 이어서 호스팅된 인증 서비스(450) 상의 인증 서버(455)는 인증 요청을 생성하고 다른 인증 관련 메시지들을 인증 클라이언트와 교환할 것이다(예를 들어, 도 2 및 도 3 및 관련 텍스트 참조). 인증 관련 동작들이 완료되면(예를 들어, 등록, 사용자 인증, 등록취소 등) 호스팅된 인증 서비스(450)는 호스팅된 인증 서비스 표명 키(436)를 이용하여 암호 표명을 통해 웹 애플리케이션(440)에 통지할 것이다. 예를 들어, 인증 서버(455)는 웹 애플리케이션(440)에 전송되는 각각의 표명에 대하여 표명 키(436)를 이용하여 서명을 생성할 수 있다. 그러면 웹 애플리케이션(440)에서 실행되고 있는 백 엔드 코드(444)는 자신만의 키(436) 사본을 이용하여 서명을 확인함으로써 표명들을 검증할 수 있다. 유사하게, 백 엔드 코드(444)는 웹 애플리케이션(440)으로부터 호스팅된 인증 서비스(450)로 전송되는 임의의 통신에 대하여 키(436)를 이용하여 서명을 생성할 수 있고, 이는 그것의 키 사본을 이용하여 통신을 확인할 수 있다.

[0048] 일 실시예에서, 호스팅된 인증 서비스(450)로부터 전송된 표명들은 인증기들(465)의 프로비저닝/등록 및 인증기들(465)을 통해 수행된 인증들에 관련된 임의의 정보를 포함할 수 있다. 예를 들어, 표명들은 인증 장치의 등록과 같은 활동 및 보안 강도(예를 들어, 사용자(X)가 인증기를 보안 강도(Y)로 등록했음); 특정 인증기 또는 인증기 유형을 이용하는 사용자에 의한 성공적인 인증(예를 들어, 사용자(X)가 방금 인증기로 보안 강도(Y)로 인증했음); 및 인증기의 등록취소(예를 들어, 사용자(X)가 인증기(Y)를 등록취소했음)와 같은 인증 장치에 관련

된 적절한 정보에 관하여 웹 애플리케이션(440)에 통지할 수 있다.

[0049] 표명은 SAML(Security Assertion Markup Language), OAuth, OpenID 또는 임의의 기타 유사한 기술을 이용하여 구현될 수 있다. 일부 호스팅된 인증 서비스 아키텍처에서, 표명들은 호스팅된 인증 서비스 서버(455)로부터 직접 웹 애플리케이션(440) 서버로 진행할 수 있다(예를 들어, 클라이언트 장치(460)를 건너뜀). 대안적인 구현예에서, 표명은 (예를 들어, 브라우저(461)에 전송된 Javascript가 이어서 웹 애플리케이션(440) 상으로 표명들을 전달하는 것과 같이) 클라이언트 장치(460)를 통해 전송될 수 있다.

[0050] 도 5는 본 발명의 일 실시예에 따라 호스팅된 인증 서비스에 신뢰자를 등록하기 위한 방법을 나타내고, 도 6은 호스팅된 인증 서비스를 이용하여 인증 장치의 등록 및 등록취소 및 사용자 인증과 같은 동작들을 수행하기 위한 방법을 나타낸다. 방법들은 도 4에 도시된 아키텍처의 맥락 내에서 구현될 수 있지만, 임의의 특정 시스템 아키텍처로 한정되지 않는다.

[0051] 501에서, 신뢰자 관리자는 호스팅된 인증 서비스의 관리 포탈에 (예를 들어, 제공된 증명서들을 이용하여) 로그인하고 새로운 신뢰자 계정을 생성하는 데 필요한 데이터를 제공한다. 이는 네트워크를 통해 신뢰자 웹 애플리케이션(들)을 식별하는 데 필요한 네트워킹 데이터 및 잠재적으로 웹 애플리케이션(특히, 웹 애플리케이션의 프론트 엔드 프로그램 코드 및 백 엔드 프로그램 코드)에 액세스 하기 위한 인증 증명서들(예를 들어, 사용자 이름/패스워드)을 포함할 수 있다.

[0052] 502에서, 웹 애플리케이션 관리자로부터 호스팅된 인증 서비스에 웹 애플리케이션을 등록하기 위한 요청에 응답하여, 관리 포탈은 웹 애플리케이션의 프론트 엔드(예를 들어, 웹 애플리케이션의 웹페이지)에 포함되는 프론트 엔드 코드(예를 들어, HTML 코드) 및 웹 애플리케이션의 백 엔드에 포함되는 백 엔드 코드를 생성한다. 또한, 502에서, 호스팅된 인증 서비스 포탈은 암호 표명 키(예를 들어, 대칭 키 또는 증명서)를 생성한다.

[0053] 503에서, 프론트 엔드 코드, 백 엔드 코드, 및 표명 키가 신뢰자에게 전송된다. 504에서, 신뢰자는 프론트 엔드 코드 및 백 엔드 코드를 그것의 플랫폼 내에 통합하고 표명 키를 안전하게 저장한다. 언급한 바와 같이, 일 실시예에서, 표명 키는 후속적으로 호스팅된 인증 서비스 표명들을 확인하는 데 사용된다.

[0054] 이제 도 6을 참조하면, 601에서 하나 이상의 인증 장치를 갖춘 클라이언트 장치는 신뢰자의 웹사이트에 접속하고 프론트 엔드 코드를 포함하는 웹 페이지를 다운로드한다. 일부 경우들에서 웹페이지는 (프론트 엔드 코드 자체가 아닌) 프론트 엔드 코드에 의해 동적으로 생성된 코드를 포함할 수 있다. 본 명세서에 사용되는 바와 같이, "프론트 엔드 코드"는 프론트 엔드 코드 자체 및 클라이언트 장치 상에서의 사용을 위해 프론트 엔드 코드에 의해 동적으로 생성된 코드 둘 모두를 지칭한다.

[0055] 602에서, 프론트 엔드 코드는 클라이언트 장치 상의 인증 클라이언트 및 호스팅된 인증 서비스(또는, 더 정확하게는, 호스팅된 인증 서비스의 인증 서버)와의 통신을 구축한다. 603에서, 새로운 인증기 등록, 사용자 인증 수행, 및/또는 인증기 등록취소와 같은 하나 이상의 트랜잭션이 수행된다.

[0056] 604에서, 호스팅된 인증 서비스는 표명 키를 이용하여 트랜잭션들과 관련된 암호 표명들을 생성한다. 예를 들어, 암호 표명은 새로운 등록된 인증기, 등록취소된 인증기, 인증기의 정확성/정밀성(예를 들어, 인증기 강도)과 같은 인증기에 관련된 정보, 및 인증기를 이용한 사용자 인증을 나타낼 수 있다. 언급한 바와 같이, 암호 표명들은 표명 키를 이용하여 서명될 수 있다.

[0057] 605에서, 암호 표명들은 신뢰자에 전송되고, 606에서, 표명 키를 이용하여 표명을 확인할 수 있다. 예를 들어, 백 엔드 코드는 표명 키를 검색하고, 그것만의 서명을 생성하고, 생성된 서명을 호스팅된 인증 서비스로부터 전송된 서명과 비교할 수 있다. 서명들이 매칭되는 경우, 표명이 확인되고 표명에 기초하여 사용자는 트랜잭션을 수행하도록 허용될 수 있다. 예를 들어, 사용자가 호스팅된 인증 서비스에 성공적으로 인증했음을 표명이 나타내는 경우, 신뢰자는 인증을 수용하고 사용자가 트랜잭션(예를 들어, 금융 트랜잭션, 사적 데이터에 대한 액세스 등)을 완료하도록 허락할 수 있다.

[0058] 일 실시예에서, 호스팅된 인증 서비스는, 예를 들어, SAML(Security Assertion Markup Language), JSON(JavaScript Objection Notation) 웹 서명, OAuth, 또는 호스팅된 인증 서비스 표명들을 신뢰자에게 전달하기 위한 유사한 기술을 포함하는 다양한 상이한 프로토콜/언어들을 이용하여 구현될 수 있다. 또한, 호스팅된 인증 서비스 시스템은 신뢰자의 웹페이지에 내장된 프론트 엔드 및 백 엔드 코드를 위하여 아이프레임들을 사용할 수 있다(예를 들어, 호스팅된 인증 서비스 표명들에 관한 신뢰자의 웹사이트에 전달함). 그러나, 본 발명의 기본 원리는 임의의 특정 프로토콜 및/또는 프로그래밍 언어에 제한되지 않는다는 것에 유의하여야 한다.

[0059] 본 명세서에 기재된 발명의 실시예들은 기존의 연합 아이덴티티 서버 및 아이덴티티 제공자들에게 바람직할 수 있는데, 그 이유는 최종 사용자의 프라이버시가 더 보호되기 때문이다. 신뢰자는 스스로 사용자와 관련된 정보를 가질 수 있고, 이 정보는 본 명세서에서 기재된 호스팅된 인증을 구현하기 위하여 인증 호스팅 서비스(또는 임의의 기타 신뢰자들)와 공유될 필요가 없다. 이는 신뢰자들이 상이한 신뢰자들에 걸쳐 사용자들을 추적할 수 있도록 하는 기존의 아이덴티티 제공자들 및 연합 서버와 대조적이다.

[0060] 예시적인 데이터 처리 장치

[0061] 도 7은 본 발명의 일부 실시예들에서 사용될 수 있는 예시적인 클라이언트들 및 서버들을 나타내는 블록도이다. 도 7은 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.

[0062] 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.

[0063] 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.

[0064] 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.

[0065] 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.

[0066] 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.

[0067] 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,

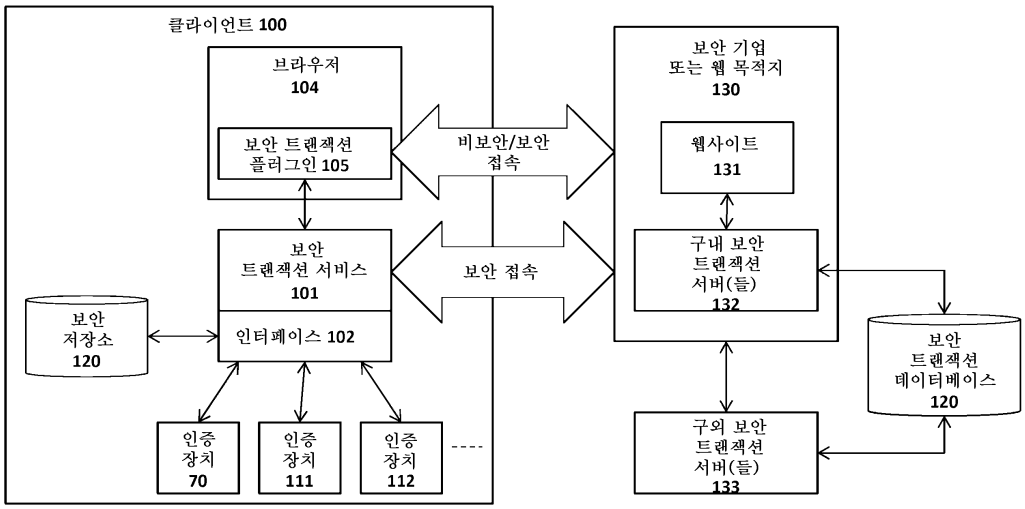
EEPROM, 자기 또는 광학 카드, 또는 전자 프로그램 코드를 저장하기에 적합한 다른 유형의 매체/기계 판독 가능 매체를 포함할 수 있지만 이에 한정되지 않는다.

[0068] 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.

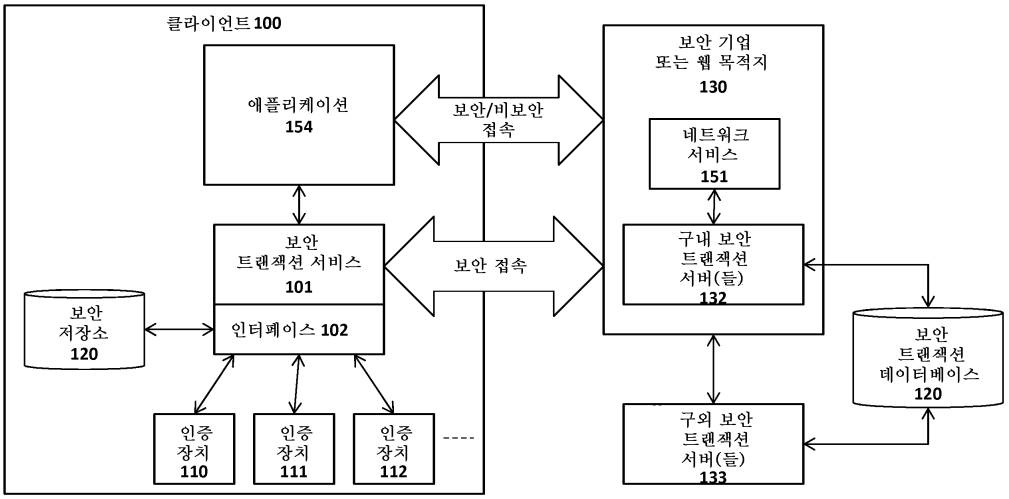
[0069] 본 발명의 실시예들은 전술한 바와 같은 다양한 단계들을 포함할 수 있다. 단계들은 범용 또는 특수 목적 프로세서가 소정 단계들을 수행하게 하는 기계 실행 가능 명령어들로 구현될 수 있다. 대안적으로, 이러한 단계들은 단계들을 수행하기 위한 하드와이어드 로직을 포함하는 특정 하드웨어 컴포넌트들에 의해, 또는 프로그래밍된 컴퓨터 컴포넌트들과 맞춤형 하드웨어 컴포넌트들의 임의의 조합에 의해 수행될 수 있다.

도면

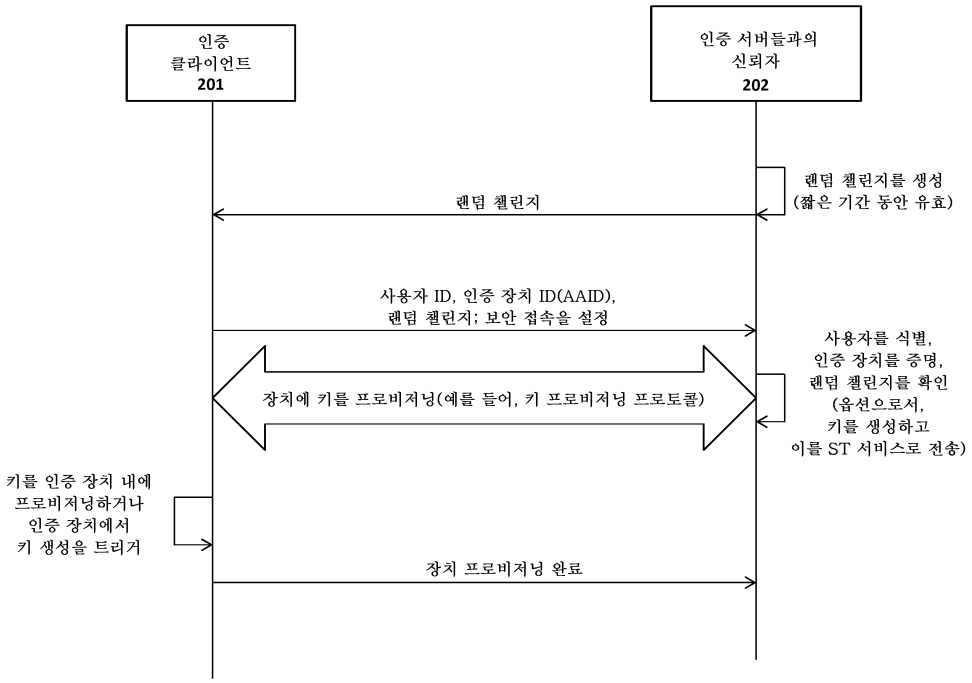
도면1a



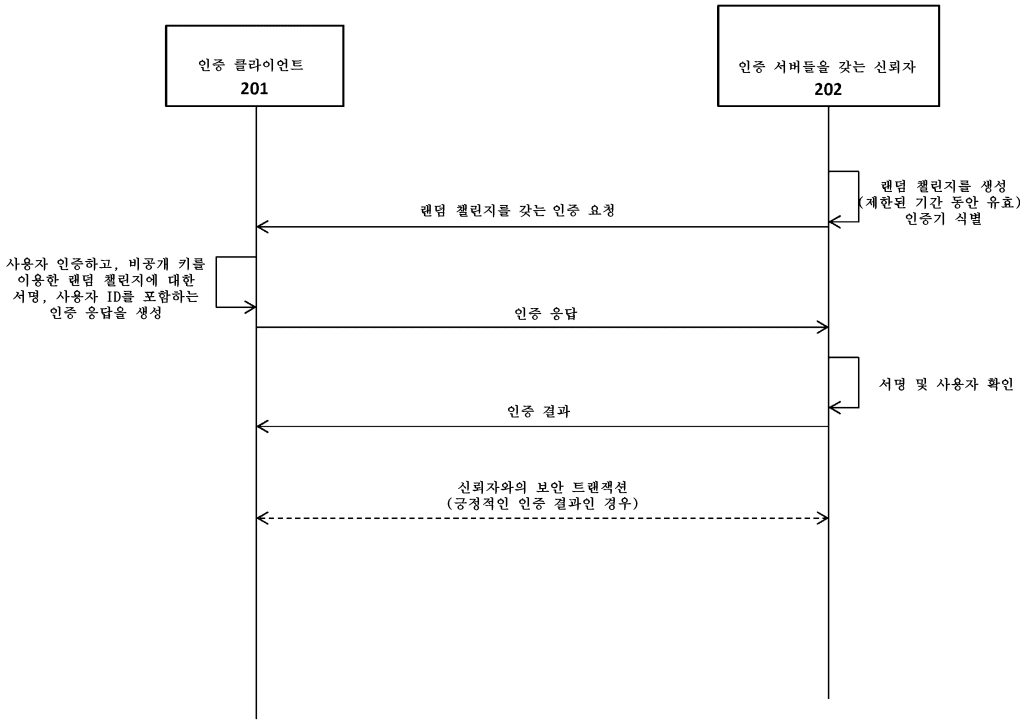
도면1b



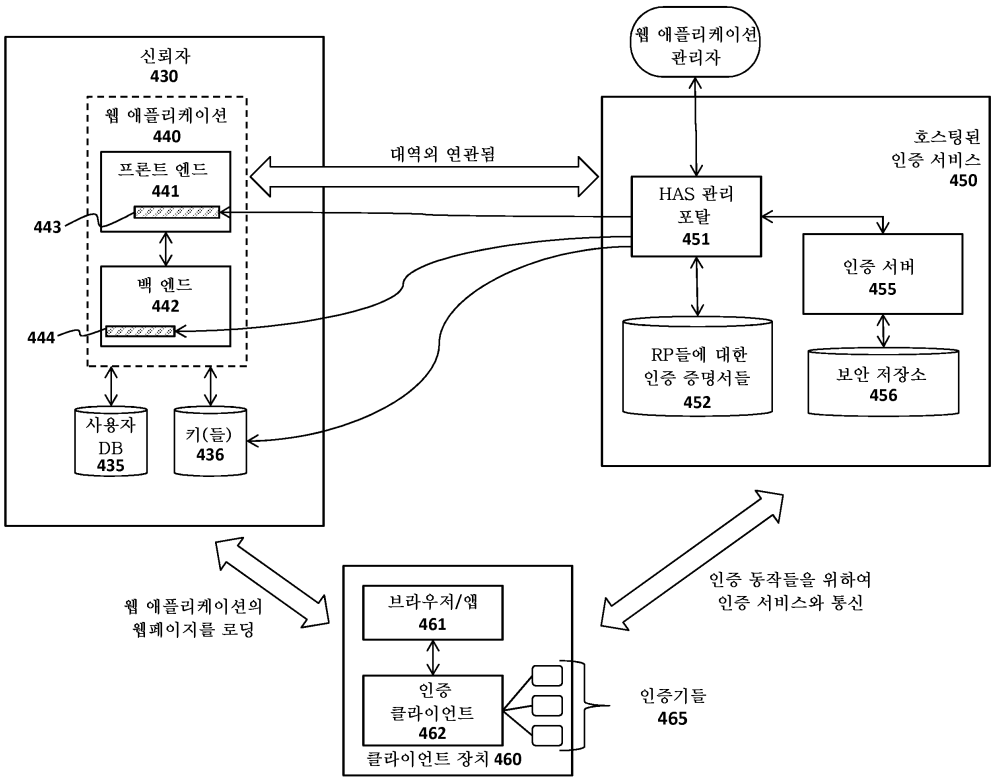
도면2


인증
클라이언트
201
인증 서버들과의
신뢰자
202
랜덤 챌린지를 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 프로비저닝(예를 들어, 키 프로비저닝 프로토콜)
키를 인증 장치 내에
프로비저닝하거나
인증 장치에서
키 생성을 트리거
장치 프로비저닝 완료

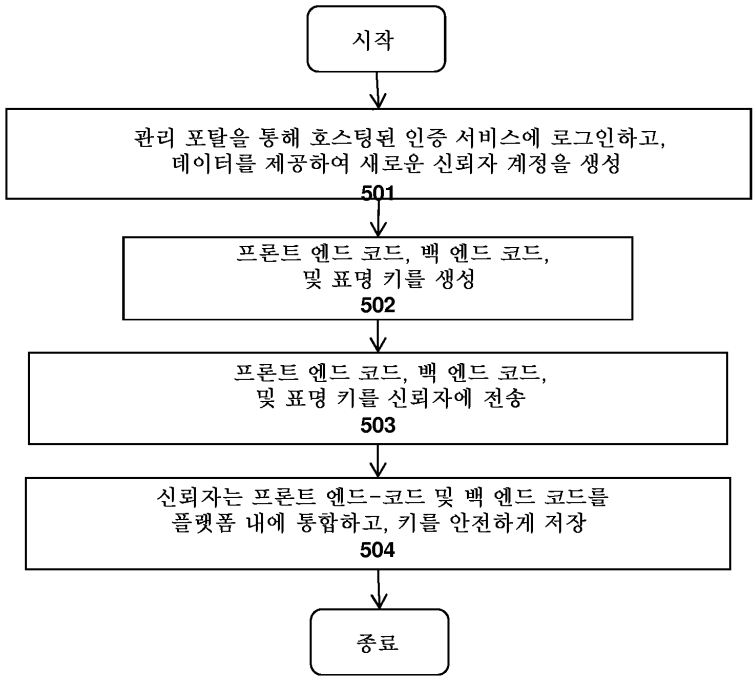
도면3


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)

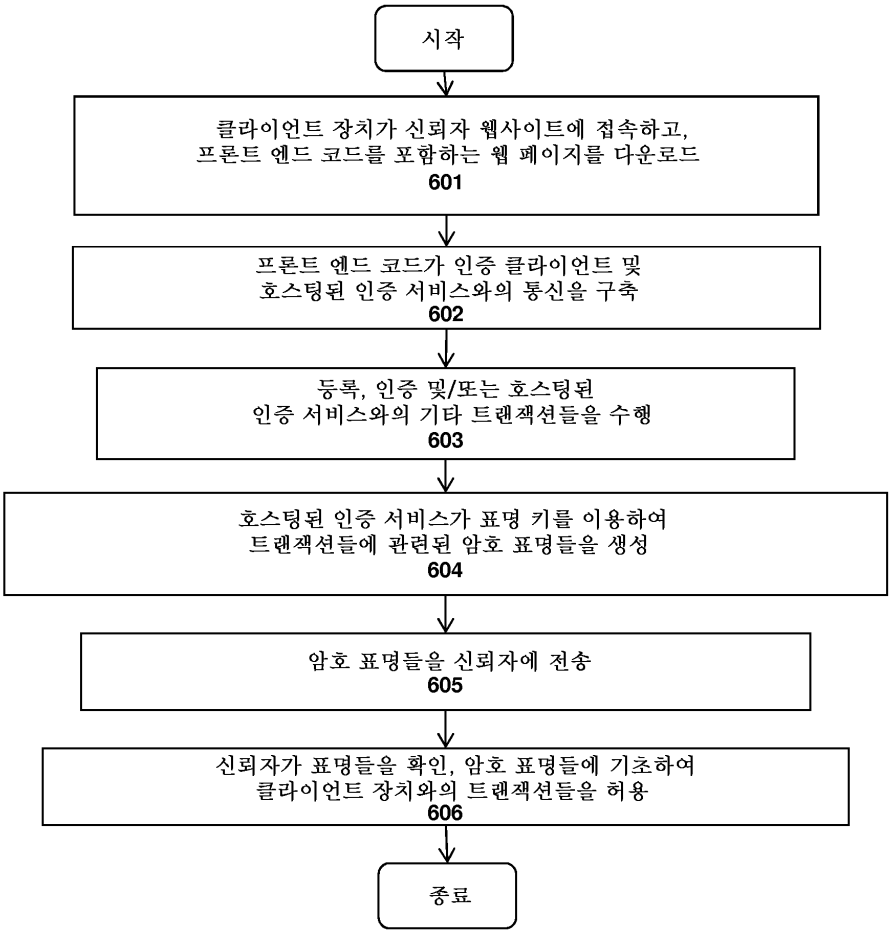
도면4


웹 애플리케이션
관리자
신뢰자
430
웹 애플리케이션
440
프론트 엔드
441
443
백 엔드
442
444
사용자
DB
435
키(들)
436
대역외 연관됨
호스팅된
인증 서비스
450
HAS 관리
포탈
451
인증 서버
455
RP들에 대한
인증 증명서들
452
보안 저장소
456
웹 애플리케이션의
웹페이지를 로딩
인증 동작들을 위하여
인증 서비스와 통신
브라우저/앱
461
인증
클라이언트
462
클라이언트 장치 460
인증기들
465

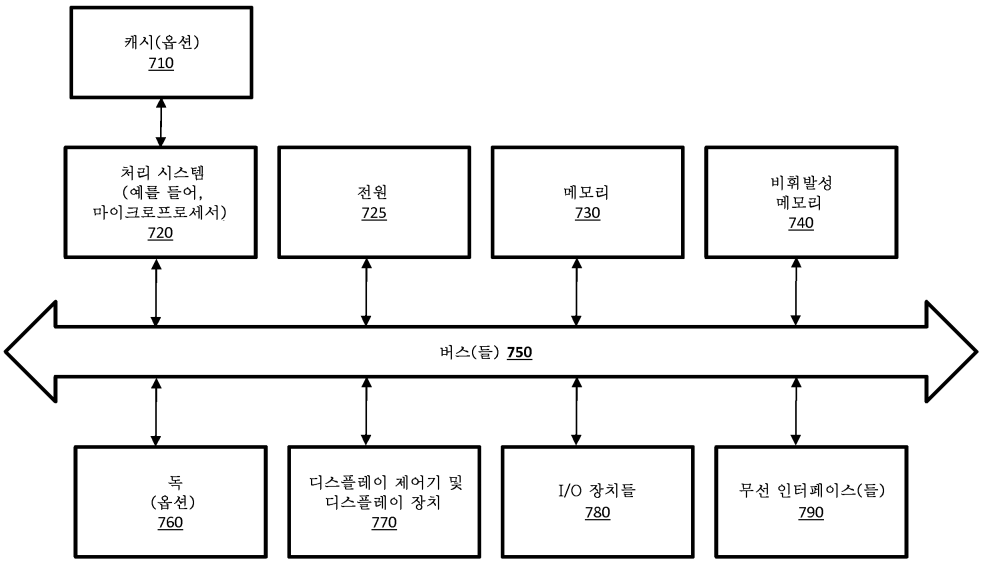
도면5


시작
관리 포탈을 통해 호스팅된 인증 서비스에 로그인하고,
데이터를 제공하여 새로운 신뢰자 계정을 생성
501
프론트 엔드 코드, 백 엔드 코드,
및 표명 키를 생성
502
프론트 엔드 코드, 백 엔드 코드,
및 표명 키를 신뢰자에 전송
503
신뢰자는 프론트 엔드-코드 및 백 엔드 코드를
플랫폼 내에 통합하고, 키를 안전하게 저장
504
종료

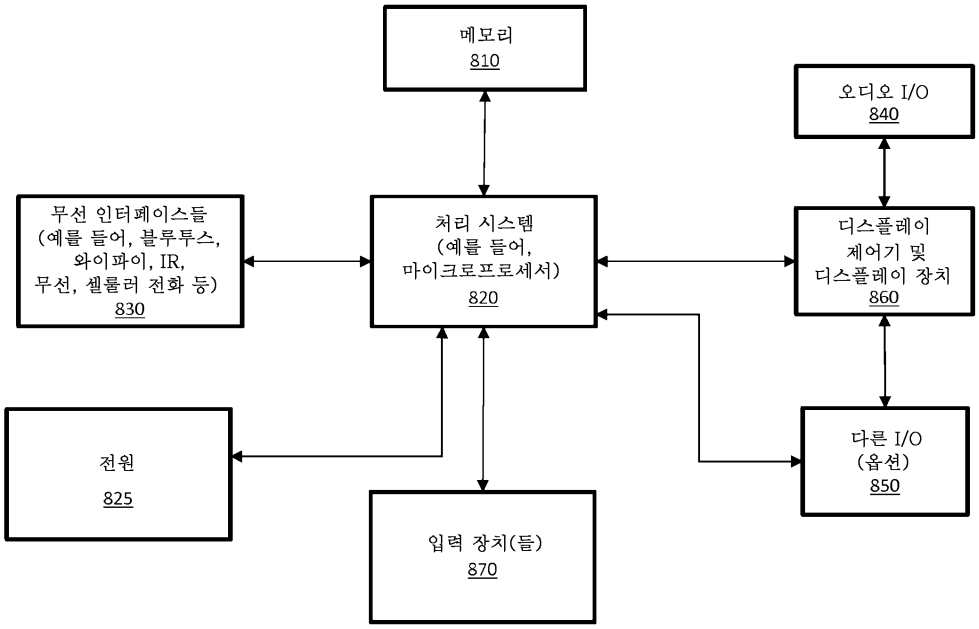
도면6


시작
클라이언트 장치가 신뢰자 웹사이트에 접속하고,
프론트 엔드 코드를 포함하는 웹 페이지를 다운로드
601
프론트 엔드 코드가 인증 클라이언트 및
호스팅된 인증 서비스와의 통신을 구축
602
등록, 인증 및/또는 호스팅된
인증 서비스와의 기타 트랜잭션들을 수행
603
호스팅된 인증 서비스가 표명 키를 이용하여
트랜잭션들에 관련된 암호 표명들을 생성
604
암호 표명들을 신뢰자에 전송
605
신뢰자가 표명들을 확인, 암호 표명들에 기초하여
클라이언트 장치와의 트랜잭션들을 허용
606
종료

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 인터페이스들
(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