(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년07월08일
(11) 등록번호 10-1634828
(24) 등록일자 2016년06월23일

(51) 국제특허분류(Int. Cl.)
G06F 21/35 (2013.01) *H04L 29/06* (2006.01)
H04L 29/08 (2006.01)
(21) 출원번호 10-2011-7005667
(22) 출원일자(국제) 2009년07월24일
심사청구일자 2014년06월24일
(85) 번역문제출일자 2011년03월10일
(65) 공개번호 10-2011-0057149
(43) 공개일자 2011년05월31일
(86) 국제출원번호 PCT/US2009/051628
(87) 국제공개번호 WO 2010/019370
국제공개일자 2010년02월18일
(30) 우선권주장
12/191,752 2008년08월14일 미국(US)
(56) 선행기술조사문헌
US05799086 A

(73) 특허권자
마이크로소프트 테크놀로지 라이센싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
가나패시, 나라야난
미국 98052-6399 워싱턴주 레드몬드 원 마이크로소프트 웨이 마이크로소프트 코포레이션 내
(74) 대리인
제일특허법인

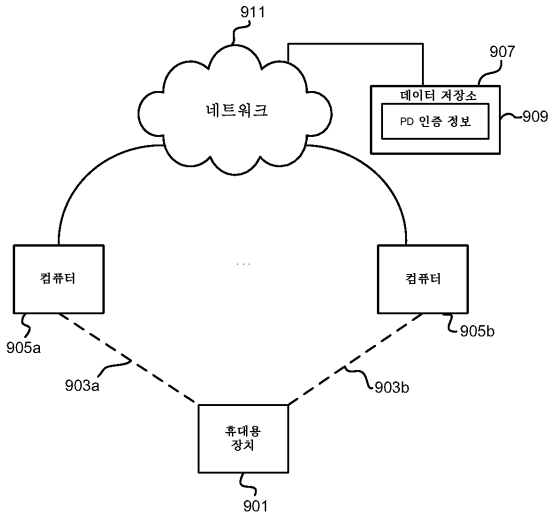
전체 청구항 수 : 총 20 항 심사관 : 박진아

(54) 발명의 명칭 **장치-스테이션 연결 프로토콜**

(57) 요 약

휴대용 장치가 복수의 컴퓨터와 자동으로 연결될 수 있게 해주는 기술이 설명되어 있다. 휴대용 장치와의 연결을 생성하기 전에, 휴대용 장치를 인증하고 신뢰할 수 있는 관계를 구축하기 위해 컴퓨터가 사용할 수 있는 정보가 생성되어, 복수의 컴퓨터에 의해 액세스가능하고 휴대용 장치의 사용자와 연관되어 있는 데이터 저장소에 저장된다. 컴퓨터가 아직 연결되지 않은 이러한 휴대용 장치를 검색할 때, 컴퓨터는 컴퓨터에 로그인된 사용자를 식별할 수 있고, 사용자를 식별해주는 정보를 사용하여, 휴대용 장치를 인증하고 자동 연결을 가능하게 해주기 위해 휴대용 장치에 의해 제공될 것으로 예상되는 장치 독립적인 인증 정보를 검색할 수 있다.

대 표 도 - 도2



명 세 서

청구범위

청구항 1

적어도 하나의 컴퓨터에 의해 실행될 때, 상기 적어도 하나의 컴퓨터에 대해 휴대용 장치를 인증하는 방법을 수행하는 복수의 명령어로 인코딩된 적어도 하나의 컴퓨터 판독가능 저장 매체로서,

상기 방법은,

(A) 상기 적어도 하나의 컴퓨터에 로그인된 사용자의 ID(identity)를 식별하는 단계,

(B) 상기 적어도 하나의 컴퓨터에서, 상기 휴대용 장치의 식별자 및 제1 보안화된 인증 정보를 포함하는 적어도 하나의 제1 통신을 상기 휴대용 장치로부터 수신하는 단계,

(C) 상기 적어도 하나의 컴퓨터에 의해, 상기 적어도 하나의 컴퓨터에 로그인된 사용자의 ID 및 상기 휴대용 장치의 식별자를 사용하여 적어도 하나의 제1 키 관련 자료(first keying material)를 검색하는 단계, 및

(D) 상기 적어도 하나의 제1 키 관련 자료를 사용하여 상기 제1 보안화된 인증 정보를 처리함으로써 상기 적어도 하나의 제1 통신이 상기 휴대용 장치를 인증하는지 여부를 판정하는 단계

를 포함하는 컴퓨터 판독가능 저장 매체.

청구항 2

제1항에 있어서,

상기 제1 보안화된 인증 정보는 디지털 서명을 포함하고, 상기 적어도 하나의 제1 키 관련 자료는 상기 휴대용 장치의 공개 키를 포함하며,

상기 적어도 하나의 제1 통신이 휴대용 장치를 인증하는지 여부를 판정하는 단계는 상기 휴대용 장치의 공개 키를 사용하여 상기 디지털 서명이 상기 휴대용 장치의 공개 키에 대응하는 비밀 키(secret key)를 사용하여 생성되었는지 여부를 검증하는 단계를 포함하는

컴퓨터 판독가능 저장 매체.

청구항 3

제1항에 있어서,

상기 사용자는 제1 사용자이고, 상기 휴대용 장치는 제1 휴대용 장치이며,

상기 적어도 하나의 제1 통신은 특정 사용자와 특정 휴대용 장치로 구성된 쌍을 식별해주는 적어도 하나의 식별자를 더 포함하고,

상기 적어도 하나의 제1 통신이 상기 휴대용 장치를 인증하는지 여부를 판정하는 단계는 상기 적어도 하나의 식별자가 상기 제1 사용자 및 상기 제1 휴대용 장치로 구성된 쌍을 일의적으로(uniquely) 식별해주는지 여부를 판정하는 단계를 포함하는

컴퓨터 판독가능 저장 매체.

청구항 4

제1항에 있어서,

상기 방법은,

상기 휴대용 장치가 상기 단계 (D)에서 인증된 것으로 판정되는 경우에, 상기 적어도 하나의 컴퓨터와 상기 휴대용 장치 간에 적어도 하나의 공유 키를 설정하는 단계, 및

상기 적어도 하나의 공유 키로부터 생성된 하나 이상의 키를 사용하여, 상기 적어도 하나의 컴퓨터와 상기 휴대

용 장치 간의 적어도 하나의 추가적인 통신을 암호화하는 단계

를 더 포함하는 컴퓨터 판독가능 저장 매체.

청구항 5

제4항에 있어서,

상기 적어도 하나의 공유 키는 상기 적어도 하나의 컴퓨터에 의해 액세스되어 상기 휴대용 장치에게 전송되는 제1 키와 상기 휴대용 장치에 의해 상기 적어도 하나의 컴퓨터에게 전송되는 제2 키를 결합하여 연산(computing)되는

컴퓨터 판독가능 저장 매체.

청구항 6

제1항에 있어서,

상기 방법은, 상기 제1 보안화된 인증 정보를 수신하는 단계 이전에, 상기 적어도 하나의 컴퓨터에 상기 로그인된 사용자를 식별해주는 적어도 하나의 이전의 통신을 상기 휴대용 장치에 송신하는 단계를 더 포함하는

컴퓨터 판독가능 저장 매체.

청구항 7

제1항에 있어서,

상기 방법은, 상기 휴대용 장치에 의해 처리될 제2 보안화된 인증 정보를 포함하는 적어도 하나의 제2 통신을 상기 적어도 하나의 컴퓨터로부터 상기 휴대용 장치에게 전송하여 상기 적어도 하나의 제2 통신이 상기 적어도 하나의 컴퓨터를 인증하는지 여부를 판정하는 단계 - 상기 보안화된 제2 인증 정보는 상기 휴대용 장치에 저장된 적어도 하나의 제2 키 관련 자료를 사용하여 상기 휴대용 장치에 의해 처리됨 - 를 더 포함하는

컴퓨터 판독가능 저장 매체.

청구항 8

제7항에 있어서,

상기 적어도 하나의 제2 통신은 상기 사용자와 상기 휴대용 장치로 구성된 쌍을 일의적으로 식별해주는 적어도 하나의 식별자를 더 포함하는

컴퓨터 판독가능 저장 매체.

청구항 9

휴대용 장치로서,

적어도 하나의 프로세서를 포함하되,

상기 프로세서는,

컴퓨터에 로그인된 사용자의 ID를 식별해주는 적어도 하나의 제1 통신을 상기 컴퓨터로부터 수신하고,

제1 키 관련 자료를 검색하며 - 상기 제1 키 관련 자료는 상기 컴퓨터에 액세스 가능하고 상기 사용자와 연관되어 있는 제2 키 관련 자료와 연관되어 있음 -,

상기 휴대용 장치의 식별자를 포함하는 적어도 하나의 제2 통신을 상기 컴퓨터에게 전송하도록 프로그램되고,

상기 적어도 하나의 제2 통신은 상기 제1 키 관련 자료에 의해 보안화되는 적어도 하나의 제1 정보(a first piece of information)를 더 포함하여, 상기 컴퓨터가 상기 제2 키 관련 자료를 사용하여 상기 제1 키 관련 자료에 의해 보안화되는 상기 적어도 하나의 제1 정보를 처리함으로써 상기 적어도 하나의 제2 통신이 상기 휴대용 장치를 인증하는지 여부를 판정할 수 있게 하는

휴대용 장치.

청구항 10

제9항에 있어서,

상기 적어도 하나의 프로세서는,

상기 사용자의 ID를 사용하여, 상기 사용자와 상기 휴대용 장치로 구성된 쌍을 일의적으로 식별해주는 적어도 하나의 식별자를 더 획득하고,

상기 적어도 하나의 식별자 및 상기 적어도 하나의 식별자를 사용하여 생성된 정보 중 적어도 하나를 상기 컴퓨터에게 전송하도록 더 프로그램되는

휴대용 장치.

청구항 11

제9항에 있어서,

상기 적어도 하나의 프로세서는,

상기 휴대용 장치에 저장된 제4 키 관련 자료와 연관되어 있는 제3 키 관련 자료에 의해 보안화되는 적어도 하나의 제2 정보(second piece of information)를 포함하는 적어도 하나의 제3 통신을 상기 컴퓨터로부터 수신하며,

상기 제4 키 관련 자료를 사용하여 상기 제3 키 관련 자료에 의해 보안화되는 상기 적어도 하나의 제2 정보를 처리함으로써, 상기 적어도 하나의 제3 통신이 상기 컴퓨터를 인증하는지 여부를 판정하도록 더 프로그램되는

휴대용 장치.

청구항 12

제11항에 있어서,

상기 사용자는 제1 사용자이고 상기 휴대용 장치는 제1 휴대용 장치이며,

상기 적어도 하나의 제3 통신은 특정 사용자와 특정 휴대용 장치로 구성된 쌍을 식별해주는 적어도 하나의 식별자를 더 포함하고,

상기 적어도 하나의 제3 통신이 상기 컴퓨터를 인증하는지 여부를 판정하는 단계는 상기 적어도 하나의 식별자가 상기 제1 사용자 및 상기 제1 휴대용 장치를 포함하는 쌍을 일의적으로 식별해주는지 여부를 판정하는 단계를 포함하는

휴대용 장치.

청구항 13

제9항에 있어서,

상기 제1 키 관련 자료는 상기 휴대용 장치의 비밀 키이고,

상기 적어도 하나의 프로세서는 상기 휴대용 장치의 비밀 키로 상기 적어도 하나의 제1 정보에 디지털 서명을 함으로써 상기 적어도 하나의 제1 정보를 보안화하도록 프로그램되며,

상기 제2 키 관련 자료는 상기 휴대용 장치의 공개 키인

휴대용 장치.

청구항 14

제11항에 있어서,

상기 적어도 하나의 프로세서는,

상기 적어도 하나의 제3 통신이 상기 컴퓨터를 인증하는 것으로 판정되는 경우에, 상기 컴퓨터와 상기 휴대용 장치 간에 공유되는 적어도 하나의 공유 키를 연산하고,

상기 적어도 하나의 공유 키로부터 생성되는 하나 이상의 키를 사용하여, 상기 컴퓨터에게 전송되는 적어도 하나의 추가적인 통신을 암호화하도록 더 프로그램되는

휴대용 장치.

청구항 15

제14항에 있어서,

상기 적어도 하나의 공유 키는, 상기 컴퓨터에 의해 상기 휴대용 장치에 전송되는 제1 키와 상기 휴대용 장치에 의해 액세스되어 상기 컴퓨터에 전송되는 제2 키를 결합함으로써 연산되는

휴대용 장치.

청구항 16

이전에 수동으로 쌍을 이룬 적이 없는 휴대용 장치와 컴퓨터를 상호 인증하는 방법으로서,

(A) 상기 컴퓨터를 통해, 상기 컴퓨터에 로그인된 사용자의 ID(identity)를 식별하는 단계,

(B) 상기 컴퓨터에 로그인된 사용자의 ID를 식별해주는 정보를 상기 컴퓨터에서 상기 휴대용 장치로 전송하는 단계,

(C) 상기 휴대용 장치에서, 제1 키 관련 자료를 검색하는 단계 - 상기 제1 키 관련 자료는 상기 컴퓨터에 액세스 가능하고 상기 사용자와 연관되어 있는 제2 키 관련 자료와 연관되어 있음 -,

(D) 상기 휴대용 장치의 ID를 식별해주는 정보를 포함하는 적어도 하나의 제1 통신을 상기 휴대용 장치에서 상기 컴퓨터로 전송하는 단계 - 상기 적어도 하나의 제1 통신은 상기 제1 키 관련 자료에 의해 보안화되는 적어도 하나의 제1 정보를 더 포함함 - ,

(E) 상기 컴퓨터에서, 상기 제2 키 관련 자료를 사용하여 상기 제1 키 관련 자료에 의해 보안화되는 적어도 하나의 정보를 처리함으로써 상기 적어도 하나의 제1 통신이 상기 휴대용 장치를 인증하는지 여부를 판정하는 단계,

(F) 상기 컴퓨터에서 상기 휴대용 장치의 ID를 사용하여 상기 컴퓨터에 독점되지 않는 데이터 저장소로부터 제3 키 관련 자료를 검색하는 단계 - 상기 제3 키 관련 자료는 상기 휴대용 장치에 저장되는 제4 키 관련 자료와 연관되어 있음 -,

(G) 상기 제3 키 관련 자료에 의해 보안화되는 적어도 하나의 제2 정보를 포함하는 적어도 하나의 제2 통신을 상기 컴퓨터에서 상기 휴대용 장치로 전송하는 단계, 및

(H) 상기 휴대용 장치에서, 상기 제4 키 관련 자료를 사용하여 상기 제3 키 관련 자료에 의해 보안화되는 적어도 하나의 제2 정보를 처리함으로써 상기 적어도 하나의 제2 통신이 상기 컴퓨터를 인증하는지 여부를 판정하는 단계

를 포함하는 방법.

청구항 17

제16항에 있어서,

상기 제1 키 관련 자료는 상기 휴대용 장치의 비밀 키이고,

상기 적어도 하나의 제1 정보는 상기 휴대용 장치의 상기 비밀 키로 상기 적어도 하나의 제1 정보에 디지털 서명을 함으로써 보안화되며,

상기 제2 키 관련 정보는 상기 휴대용 장치의 공개 키인

방법.

청구항 18

제16항에 있어서,

상기 사용자는 제1 사용자이고 상기 휴대용 장치는 제1 휴대용 장치이며,

상기 적어도 하나의 제1 통신은 특정 사용자와 특정 휴대용 장치로 구성된 쌍을 식별해주는 적어도 하나의 식별자를 더 포함하고,

상기 적어도 하나의 제1 통신이 상기 휴대용 장치를 인증하는지 여부를 판정하는 단계는 상기 적어도 하나의 식별자가 상기 제1 사용자 및 상기 제1 휴대용 장치로 구성된 쌍을 일의적으로(uniquely) 식별해주는지 여부를 판정하는 단계를 포함하는

방법.

청구항 19

제16항에 있어서,

상기 제3 키 관련 자료는 상기 사용자의 비밀 키이고,

상기 적어도 하나의 제2 정보는 상기 사용자의 상기 비밀 키로 상기 적어도 하나의 제2 정보에 디지털 서명을 함으로써 보안화되며,

상기 제2 키 관련 정보는 상기 사용자의 공개 키인

방법.

청구항 20

제16항에 있어서,

상기 사용자는 제1 사용자이고 상기 휴대용 장치는 제1 휴대용 장치이며,

상기 적어도 하나의 제2 통신은 특정 사용자와 특정 휴대용 장치로 구성된 쌍을 식별해주는 적어도 하나의 식별자를 더 포함하고,

상기 적어도 하나의 제2 통신이 상기 컴퓨터를 인증하는지 여부를 판정하는 단계는 상기 적어도 하나의 식별자가 상기 제1 사용자 및 상기 제1 휴대용 장치로 구성된 쌍을 일의적으로(uniquely) 식별해주는지 여부를 판정함으로써 상기 컴퓨터에 로그인된 사용자가 상기 제1 사용자인지 여부를 판정하는 단계를 포함하는

방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 휴대용 전자 장치를 하나 이상의 컴퓨팅 장치와 안전하게 연결(associating 또는 pairing)하는 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 점점 더, 사용자는 많은 여러 유형의 휴대용 전자 장치[예를 들어, 무선 헤드폰, 디지털 카메라, PDA(personal digital assistant), 휴대폰, 마우스 등]를 자신의 컴퓨터를 사용하여 동작시킨다. 많은 휴대용 전자 장치가 블루투스(Bluetooth), 초광대역(UWB, ultra-wide band), 무선 USB(Universal Serial Bus) 및 근거리 통신(NFC, Near Field Communication)과 같은 단거리 무선 기술을 지원한다.

[0003] 단거리 무선 기술 및 유선 연결은 서로 아주 근접하여 위치하는 장치들 간의 통신만을 허용한다. 물리적 근접성이라는 이러한 제한으로 인해, 보안 위협이 다소 완화된다. 즉, 공격측 장치가 대상 컴퓨팅 장치에 물리적으로 연결되어야 하거나, 그의 전송 범위 내에서, 통신을 가로채기하고 및/또는 삽입할 수 있어야 한다. 그럼에도 불구하고, 컴퓨팅 장치가 신뢰할 수 있는 인증된 장치에만 연결되어 통신하도록 보장하기 위하여, 보안 기능이 통상적으로 이용된다.

[0004] 종래에는, 휴대용 장치가 컴퓨팅 장치와 연결되기 전에, 휴대용 장치가 신뢰할 수 있다는 것을 보장하는 프로세스가 수행된다. 일례로, 무선 기술을 지원하는 컴퓨팅 장치는, 동일한 기술을 지원하고 통신 범위 내에 있는 다른 장치들의 목록을 얻기 위해, 검색 프로토콜을 수행할 수 있다. 이어서, 컴퓨팅 장치는, 자동으로 또는 사

용자의 요청 시에, 검색된 장치 중 하나와 통신 세션을 시작할 수 있다. 2개의 장치 간에 신뢰를 구축하기 위하여, 통상적으로 장치 중 하나 또는 둘다와 상호작용하도록 사용자에게 요청한다. 일례로, 각각의 장치는 숫자 값을 디스플레이 할 수 있으며, 사용자가 양쪽 장치들을 제어하고 있고 따라서 휴대용 장치가 신뢰할 수 있는 것이라는 것을 확인하기 위하여, 2개의 디스플레이된 숫자 값이 일치하는 경우, 장치 중 하나 또는 둘다에 "예"를 입력하도록 사용자에게 요청한다. 사용자가 수동으로 동의하는 동작(affirmative manual action)을 필요로 하기 때문에, 이러한 사용자-보조 인증 프로세스를 일반적으로 "수동 연결(manual pairing)"이라고 말한다.

[0005] 종래의 수동 연결 프로세스의 일부로서, 사용자가 신뢰할 수 있는 장치 간의 연결이라는 것을 확인하면, 향후의 장치 간의 연결이 사용자 동작 없이 장치들에 의해 자동으로 수행될 수 있도록 이후의 통신에서 사용하기 위하여, 장치는 보안 정보(예를 들어, 암호화 키 관련 자료)를 저장한다. 따라서, 향후에 동일한 2개의 장치가 서로를 검색하는 경우, 수동 연결 절차를 한번 더 수행할 필요 없이, 장치들이 서로를 신뢰할 수 있는 것으로 인식할 수 있게 해주기 위해, 저장된 보안 정보가 검색되고 교환될 수 있다.

발명의 내용

[0006] <발명의 요약>

[0007] 본 발명의 측면들은 휴대용 장치(예를 들어, 휴대폰, MP3 플레이어, 무선 헤드셋과 같은 무선 장치)를 2개 이상의 서로 다른 컴퓨터에 자동으로 연결하는 향상된 기술에 관한 것이다. 종래의 기술을 사용하면, 휴대용 장치는, 차후의 자동 연결을 용이하게 해주기 위해, 컴퓨터와 수동으로 연결되어 컴퓨터와 신뢰할 수 있는 관계를 구축해야만 했으며, 사용자가 컴퓨터와 함께 휴대용 장치를 사용하고자 하는 그 각각의 컴퓨터에 대해 개별적으로 수동 연결 프로세스가 수행되어야만 했다. 예를 들어, 새로운 무선 헤드셋을 구입하여 이를 업무용 컴퓨터 및 가정용 컴퓨터 둘다와 함께 사용하고자 하는 사용자가 종래에는, 무선 헤드셋과 신뢰할 수 있는 관계를 구축하기 위하여, 이들 컴퓨터 각각과의 수동 연결 프로세스를 거칠 필요가 있다. 수동 연결 프로세스의 일부로서, 장치들이 서로를 인증하여 자동 연결을 형성할 수 있게 해주기 위해 향후에 사용될 수 있는 인증 정보가 컴퓨터와 휴대용 장치(예를 들어, 무선 헤드셋) 간에 교환된다. 따라서, 장치가 컴퓨터와 한번 수동 연결된 후에, 장치들이 향후에 통신 범위 내에 들어올 때, 장치들은 서로를 인증하여 신뢰할 수 있는 관계를 구축하고 자동으로 통신을 설정할 수 있다.

[0008] 종래 기술의 단점은 휴대용 장치가 함께 사용될 모든 컴퓨터와 개별적으로 수동 연결 동작을 해야만 한다는 것이며, 이는 사용자, 특히 다수의 컴퓨터와 함께 수많은 휴대용 장치를 이용하는 사용자에게 번거로울 수 있다. 본 발명의 일 실시예에 따르면, 다수의 수동 연결 동작을 수행할 필요성이 극복된다. 이것은 임의의 몇가지 방식으로 달성될 수 있다. 한 측면에서, 제1 컴퓨터와의 수동 연결 동작 동안에, 휴대용 장치와 휴대용 장치에 수동 연결되는 컴퓨터의 사용자 간에 인증 정보가 설정된다. 이어서, 인증 정보는 임의의 수의 컴퓨터에 의해 전역적으로 액세스가능한 데이터 저장소에 저장된다. 따라서, 인증 정보가 설정된 후에, 사용자가 임의의 새로운 컴퓨터(휴대용 장치와 이전에 수동으로 연결된 적이 없는 컴퓨터를 포함함)와 함께 휴대용 장치를 사용하고자 할 때, 그 컴퓨터는, 컴퓨터에 로그인된 사용자의 ID(identity)에 기초하여, 전역적으로 액세스가능한 저장소로부터 인증 정보를 검색할 수 있으며, 새로운 컴퓨터와 휴대용 장치가 수동으로 연결될 필요 없이 자동으로 서로를 인증하고 연결을 설정할 수 있게 해주기 위해 그 인증 정보를 사용할 수 있다. 이것이 유리한 이유는, 사용자가 컴퓨터와 함께 휴대용 장치를 사용하고자 할 때 그 모든 컴퓨터와의 차후의 수동 연결 동작을 거칠 필요없이, 사용자가 단지 휴대용 장치를 하나의 컴퓨터와 수동으로 연결하고, 그 후에 휴대용 장치가 사용자가 로그인하는 임의의 컴퓨터와 자동으로 연결될 수 있게 해주기 때문이다.

[0009] 대안의 측면에서, 휴대용 장치가 임의의 특정 컴퓨터와 수동으로 연결될 필요 없이, 인증 정보가 설정되고 전역적으로 액세스가능한 저장소에서 제공될 수 있다.

[0010] 본 발명의 다른 실시예는, 사용자가 로그인되어 있는 어떤 컴퓨터에서도 인증 정보가 이용될 수 있도록, 특정 컴퓨터 자체가 아니라 컴퓨터의 사용자와 관련되어 있는 인증 정보를 사용하여 컴퓨터에 대해 휴대용 장치를 인증하는 프로토콜에 관한 것이다.

도면의 간단한 설명

[0011] 첨부 도면들은 축척대로 그려져 있지 않다. 도면들에서, 여러 도면들에 나타내어져 있는 각각의 동일한 또는 거의 동일한 구성요소는 유사한 참조 번호로 표시되어 있다. 명확함을 위해, 모든 도면들에서 구성요소들 모두

에 참조 번호가 표시되어 있는 것은 아니다.

도 1은 본 발명의 일 실시예에 따른, 모바일 장치와 단일 컴퓨터와의 수동 연결 동작 및 그후의 추가 컴퓨터와의 자동 연결을 나타낸 도면.

도 2는 본 발명의 일 실시예에 따른, 하나 이상의 컴퓨터가 휴대용 장치를 자동으로 인증하고 연결하기 위한 정보를 포함하는 전역적으로 액세스가능한 데이터 저장소를 포함하는 컴퓨터 시스템을 나타낸 도면.

도 3은 본 발명의 일 실시예에 따른, 휴대용 장치를 컴퓨터와 자동으로 연결하기 위해 인증 정보를 생성하고 사용하는 예시적인 프로세스의 플로우차트.

도 4는 본 발명의 일 실시예에 따른, 휴대용 장치에 대한 인증 정보를 생성하고 복수의 컴퓨터가 액세스할 수 있는 방식으로 인증 정보를 저장하는 프로세스를 나타낸 도면.

도 5는 본 발명의 일 실시예에 따른, 휴대용 장치를 인증하기 위하여 컴퓨터에 로그인한 사용자를 식별하고 사용자와 연관된 인증 정보를 검색함으로써 휴대용 장치를 컴퓨터와 자동으로 연결하는 프로세스를 나타낸 도면.

도 6은 인증된 장치 연결을 수행하는 종래의 프로세스를 나타낸 도면.

도 7은 본 발명의 일 실시예에 따른, 인증 정보를 생성하기 위해 컴퓨터와 휴대용 장치를 수동으로 연결하는 프로세스를 나타낸 도면.

도 8은 본 발명의 일 실시예에 따른, 복수의 사용자와 휴대용 장치에 대한 인증 정보를 포함하는 데이터 저장소의 예시적 구현을 나타낸 도면.

도 9는 컴퓨터 사용자의 ID에 기초하여 컴퓨터에 대해 휴대용 장치를 인증하기 위한 정보를 포함하는 휴대용 장치 상의 데이터 저장소의 예시적 구현을 나타낸 도면.

도 10은 본 발명의 일 실시예에 따른, 휴대용 장치와 컴퓨터를 인증하기 위해 프로파일을 가져오는 프로세스를 나타낸 도면.

도 11은 본 발명의 일 실시예에 따른, 컴퓨터와 휴대용 장치를 상호 인증하고 이들 간의 자동 연결을 가능하게 해주기 위해, 컴퓨터와 휴대용 장치 간에 통신하는 프로토콜의 일례를 나타낸 도면.

도 12는 본 발명의 측면들이 구현될 수 있는 예시적인 컴퓨터를 개략적으로 나타낸 도면.

발명을 실시하기 위한 구체적인 내용

[0012] 이상에서 논의된 바와 같이, 종래의 장치 연결 프로토콜은 처음에 2개의 장치 간의 신뢰를 구축하기 위해 사용자의 수동 개입에 의존한다. 이전의 수동 연결 절차 동안에 설정되거나 교환된 인증 정보(예를 들어, 암호화 키 관련 자료)는 이어서 이전에 연결된 적이 있는 2개의 장치가 사용자 개입없이 자동으로 연결될 수 있게 해주기 위해 나중에 사용될 수 있다. 그러나, 이전에 연결된 적이 없는 임의의 2개의 장치에 대해 필요한 보안 정보의 교환을 설정하기 위해 수동 연결 절차가 적어도 한번 수행되어야 한다.

[0013] 출원인은 어떤 사용자가 동일한 하나 이상의 휴대용 장치(들)(예를 들어, 헤드폰, MP3 플레이어, 휴대폰 등)를 연결하고자 할 수 있는 2개 이상의 서로 다른 컴퓨팅 장치(예를 들어, 하나는 집에 있고, 다른 하나는 직장에 있음)를 이용한다는 것을 알고 있다. 출원인은 또한 수동 연결 프로세스가 장치 사용자에게 시간이 많이 걸리고 번거로울 수 있으며, 휴대용 장치를 다수의 컴퓨팅 장치에 연결하기 위해 이 프로세스가 동일한 휴대용 장치에 대해 여러번 반복되어야 하는 경우에 특히 그렇다는 것을 알고 있다.

[0014] 따라서, 도 1에서 개념적으로 도시된 본 발명의 일 실시예에 따르면, 사용자는 (예를 들어, 221에서) 휴대용 장치[예를 들어, 휴대폰(210)]를 컴퓨터[예를 들어, 가정용 데스크톱(220)]와 수동으로 한번 연결할 수 있으며, 휴대용 장치가 나중에 동일한 사용자에 의해 사용되는 다른 컴퓨터와[예를 들어, 231로 도시된 바와 같이 랩톱(230)과, 또는 241로 도시된 바와 같이 사무실 데스크톱(240)과] 자동으로 연결될 수 있다. 본 명세서에서 사용되는 바와 같이, 휴대용 장치가 자동으로 연결된다는 말은, 컴퓨터에 대해 휴대용 장치를 인증하거나 휴대용 장치에 대해 컴퓨터를 인증하고 이들 간의 연결을 용이하게 해주기 위하여, 휴대용 장치와 컴퓨터의 사용자가 어떠한 조치도 취할 필요가 없음을 나타낸다.

[0015] 휴대용 장치와 이 휴대용 장치에 이전에 수동으로 연결된 적이 없는 컴퓨터 간의 자동 연결을 가능하게 해주는 것에 관련된 본 발명의 측면은, 임의의 특정의 구현 기술로 제한되지 않기 때문에, 임의의 적합한 방식으로 구

현될 수 있다. 본 발명의 예시적인 일 실시예에 따르면, 2개 이상의 컴퓨터와 연결될 수 있는 휴대용 장치에서 사용하기 위한 기술이 이용된다. 휴대용 장치를 인증하는 인증 정보가 생성되고, 인증 정보를 휴대용 장치의 사용자와 연관시키는 방식으로, 인증 정보가 2개 이상의 컴퓨터에 의해 액세스가능한 데이터 저장소에 저장된다. 인증 정보가 생성되고 휴대용 장치와 이전에 연결된 적이 없는 컴퓨터가 액세스가능한 데이터 저장소에 저장되면, 그 컴퓨터는, 수동 연결 동작을 필요로 하지 않고, 인증 정보에 액세스하고 이를 이용하여 휴대용 장치를 자동으로 인증할 수 있다. 이것은 임의의 적당한 방식으로 달성될 수 있다.

[0016] 예를 들어, 본 발명의 다른 실시예에 따르면, 컴퓨팅 장치가 그와 연결된 적이 없는 적어도 하나의 휴대용 장치를 발견하면, 컴퓨팅 장치는 컴퓨팅 장치에 로그인된 사용자를 식별하고, 로그인된 사용자를 식별해주는 정보를 사용하여 휴대용 장치에 대한 인증 정보를 검색하며, 검색된 인증 정보를 사용하여 휴대용 장치를 인증하고 휴대용 장치를 컴퓨팅 장치와 자동으로 연결할 수 있다.

[0017] 이상의 내용으로부터 잘 알 것인 바와 같이, 출원인은 휴대용 장치를 다수의 컴퓨팅 장치와 연결하는 종래의 기술들의 단점이, 휴대용 장치와 컴퓨팅 장치 간에 인증 정보가 교환될 때, 자동 연결을 가능하게 해주기 위해 향후에 휴대용 장치를 인증하는 데 사용될 수 있는 정보가 종래에는 그 컴퓨팅 장치가 로컬로만 액세스가능한 방식으로 컴퓨팅 장치에 의해 저장된다는 것임을 알았다. 본 발명의 일 실시예에 따르면, 휴대용 장치에 대한 인증 정보는 하나 이상의 컴퓨팅 장치, 심지어 인증 정보를 설정하기 위해 휴대용 장치와 통신하는 데 사용되지 않는 컴퓨팅 장치가 보다 전역적으로 액세스할 수 있는 방식으로 저장된다. 그 결과, 휴대용 장치가 이러한 컴퓨팅 장치에 의해 처음으로 검색될 때, 컴퓨팅 장치가 이전에 휴대용 장치와 수동으로 연결된 적이 없더라도, 컴퓨팅 장치는 데이터 저장소에 액세스하고, 인증 정보를 검색하며, 인증 정보를 사용하여 휴대용 장치를 인증하고 자동으로 연결할 수 있다. 이것이 도 2에 개념적으로 도시되어 있으며, 여기서 휴대용 장치(901)는, 점선(903a 및 903b)으로 나타낸 바와 같이 서로 다른 때에, 2개 이상의 컴퓨터(905a 및 905b)와 연결될 수 있다. 휴대용 장치(901)를 인증하는 데 사용될 수 있는 인증 정보(909)는 2개 이상의 컴퓨터(905a 및 905b)가 액세스할 수 있는 데이터 저장소(907)에 저장된다. 따라서, 인증 정보를 설정하기 위해, 휴대용 장치(901)와 이전에 수동으로 연결된 적이 없는 컴퓨터를 포함하여 컴퓨터(905a 및 905b) 중 하나에 의해 휴대용 장치(901)가 검색될 때, 컴퓨터(905a 및 905b)는 데이터 저장소(907)에 액세스하여 인증 정보(909)를 검색할 수 있으며, 인증 정보를 사용하여 휴대용 장치(901)를 인증하고 컴퓨터와 자동으로 연결할 수 있다.

[0018] 도 2에 도시된 구성에서, 데이터 저장소(907)는 각각의 컴퓨터(905a 및 905b)가 네트워크(911)를 통하여 액세스가능한 것으로 나타내어져 있다. 본 발명의 일 실시예에 따르면, 네트워크(911)는 임의의 적합한 네트워크(예를 들어, 인터넷)일 수 있으며, 데이터 저장소(907)는 컴퓨터(905a 및 905b) 중 어느 것과도 구별되는 컴퓨팅 장치(예를 들어, 데이터베이스 서버 또는 기타 유형의 컴퓨팅 장치)와 연결될 수 있다. 그러나, 본 명세서에 기술된 본 발명의 측면들이 이 점에서 제한되지 않는다는 것을 잘 알 것이다. 예를 들어, 데이터 저장소(907)는 컴퓨터(905a 및 905b) 중 하나에 제공되거나 그와 연결될 수 있으며, USB 플래시 키 또는 임의의 다른 적합한 통신 매체를 통해 컴퓨터(905a 및 905b)에 의해 액세스될 수 있다.

[0019] 이하에서 논의되는 본 발명의 일 실시예에 따르면, 인증 정보(909)는 휴대용 장치(901)를 컴퓨터(905a 및 905b) 중 하나와 수동으로 연결하는 것을 통해 발생되고, 이어서 수동 연결을 수행하는 컴퓨터 또는 다른 컴퓨터 상의 데이터 저장소일 수 있는 데이터 저장소(907)에 저장된다. 그러나, 인증 정보가 임의의 적합한 방식으로 발생되고 데이터 저장소(907)에 저장될 수 있기 때문에, 본 명세서에서 기술된 본 발명의 측면들이 이 점에서 제한되지 않는다는 것을 잘 알 것이다. 예를 들어, 본 발명의 다른 대안의 실시예에서, 인증 정보(예를 들어, 키 관련 자료)가 수동 연결 동작을 수행하지 않고 생성될 수 있다. 그 후에, 자동 연결 동안 휴대용 장치에 의해 사용되는 키 관련 자료의 부분(들)은 임의의 적합한 방식으로 휴대용 장치 상에 직접 저장될 수 있으며, 하나 이상의 컴퓨터에 의해 사용되는 키 관련 자료의 부분(들)은 전역적으로 액세스가능한 저장소에 저장될 수 있다.

[0020] 이상의 내용으로부터 잘 알 것인 바와 같이, 본 발명의 일 실시예는 휴대용 장치를 컴퓨터와 연결하는 도 3에서 도시된 유형의 프로세스에 관한 것이다. 먼저, 동작(1001)에서, 휴대용 장치를 인증하는 데 사용될 수 있는 인증 정보[예를 들어, 인증 정보(909)]를 생성하기 위하여, 휴대용 장치는 제1 컴퓨터[예를 들어, 도 2의 컴퓨터(905a)]에 수동으로 연결된다. 인증 정보가 다른 대안으로서 이상에서 언급한 바와 같은 다른 방식으로 설정될 수 있다는 것을 잘 알 것이다. 동작(1003)에서, 인증 정보는 다른 컴퓨터[예를 들어, 컴퓨터(905b)]가 액세스할 수 있는 데이터 저장소[예를 들어, 데이터 저장소(907)]에 저장되며, 휴대용 장치(901)의 사용자와 연관된다. 이 점에서, 본 발명의 일 실시예에 따르면, 인증 정보는 그 정보를 휴대용 장치의 사용자와 연관시키는 방식으로 데이터 저장소에 저장되고, 그에 따라 휴대용 장치를 검색하는 컴퓨터는 컴퓨터의 사용자를 식별하고 그 정보를 사용하여 어떤 인증 정보를 데이터 저장소로부터 검색해야 하는지를 식별할 수 있다. 이 점에

서, 본 발명의 몇몇 실시예에 따르면, 데이터 저장소[예를 들어, 데이터 저장소(907)]는 임의의 수의 휴대용 장치 및/또는 임의의 수의 하나 이상의 사용자에 대한 인증 정보를 포함할 수 있고, 그에 따라 다수의 사용자의 장치에 대한 정보가 저장될 때, 휴대용 장치를 검색하는 컴퓨터의 사용자의 ID가 그 사용자의 장치에 적절한 인증 정보를 식별하는 데 사용될 수 있다. 그러나, 임의의 적합한 기술이 이용될 수 있기 때문에, 모든 실시예들이 휴대용 장치를 인증하는 데 어떤 인증 정보를 사용할지를 식별하기 위하여 사용자를 식별해주는 정보를 사용하는 것으로 제한되는 것은 아님을 잘 알 것이다.

[0021] 동작(1005)에서, 인증 정보 생성을 위해 휴대용 장치와 수동으로 연결되었던 컴퓨터 이외의 컴퓨터[예를 들어, 컴퓨터(905b)와 같은 제2 컴퓨터]는 데이터 저장소에 액세스하여 인증 정보[예를 들어, 인증 정보(909)]를 검색할 수 있다. 이 동작은 그 컴퓨터가 휴대용 장치를 검색한 것에 응답하여 또는 임의의 다른 적합한 때에 수행될 수 있다.

[0022] 마지막으로, 동작(1007)에서, 컴퓨터는 검색된 인증 정보[예를 들어, 인증 정보(909)]를 사용하여 휴대용 장치(901)를 인증하고, 휴대용 장치가 성공적으로 인증되었을 때, 휴대용 장치를 컴퓨터(예를 들어, 905b)와 자동으로 연결할 수 있다. 이러한 방식으로, 휴대용 장치는, 컴퓨터[예를 들어, 컴퓨터(905b)]와 수동으로 연결된 적이 없는 상태에서, 그 컴퓨터와 자동으로 연결될 수 있다.

[0023] 이상의 내용으로부터 잘 알 것인 바와 같이, 도 3에 예시된 프로세스는, 인증 정보가 [예를 들어, 인증 정보를 얻기 위해 수동 연결 동작을 수행한 컴퓨터에 의해 로컬로만 사용되는 것과는 달리, 다른 컴퓨터가 액세스가능한 데이터 저장소에] 저장되는 방식 및 (예를 들어, 수동 연결 동작을 수행하기 보다는 데이터 저장소로부터 인증 정보를 획득함으로써) 컴퓨터와 이전에 연결된 적이 없는 휴대용 장치를 컴퓨터가 처음으로 검색할 때 컴퓨터에 의해 수행되는 프로세스 둘다에서, 휴대용 장치를 하나 이상의 컴퓨터에 연결하는 종래의 기술과 다르다.

[0024] 이 점에서, 도 4는 휴대용 장치에 대한 인증 정보를 이전에 휴대용 장치와 연결된 적이 없는 하나 이상의 컴퓨터가 이용할 수 있게 해주는 것을 포함하는 본 발명의 일 실시예에 따른 프로세스를 나타낸 것이다. 동작(1101)에서, 휴대용 장치를 인증하는 데 사용될 수 있는 인증 정보가 생성된다. 이상에서 논의된 바와 같이, 본 명세서에 기술된 본 발명의 측면들이 인증 정보를 생성하는 임의의 특정 기술로 제한되지 않기 때문에, 인증 정보는 휴대용 장치를 컴퓨터와 수동으로 연결함으로써 또는 임의의 다른 적합한 방식으로 생성될 수 있다.

[0025] 동작(1103)에서, 인증 정보는, 하나의 컴퓨터만 액세스가능한 로컬화된 방식으로 저장되는 것과는 달리, 임의의 적합한 기술(그 일례들이 본 명세서에 기술되어 있음)을 사용하여 복수의 컴퓨터가 액세스가능하게 해주는 방식으로 저장된다. 본 발명의 일 실시예에 따르면, 이상에서 논의된 바와 같이 검색을 용이하게 해주기 위하여 인증 정보를 휴대용 장치의 사용자와 연관시키는 방식으로 인증 정보가 저장된다.

[0026] 도 5는 본 발명의 일 실시예에 따른, 컴퓨터를 휴대용 장치와 자동으로 연결하기 위하여 컴퓨터가 수행할 수 있는 프로세스를 나타낸 것이다. 도 5의 프로세스는 컴퓨터가 휴대용 장치를 검색한 것에 응답하여 또는 임의의 다른 적합한 이벤트에 응답하여 시작될 수 있다. 동작(1201)에서, 프로세스는 컴퓨터에 로그인된 사용자를 식별한다. 그 후에, 동작(1203)에서, 프로세스는, 휴대용 장치와 연관되고 또한 동작(1201)에서 컴퓨터에 로그인된 것으로 식별되는 사용자와 연관되어 있는 인증 정보를, 데이터 저장소로부터 검색한다. 이것은 임의의 적합한 방식(그 일례들이 본 명세서에서 논의됨)으로 수행될 수 있다. 동작(1205)에서, 컴퓨터는 인증 정보를 사용하여, 휴대용 장치[예를 들어, 휴대용 장치(901)]가 그 자신을 신뢰할 수 있는 장치로서 성공적으로 인증할 수 있는지 여부를 결정한다. 이것은 임의의 적합한 방식(그 일례들이 이하에 기술됨)으로 수행될 수 있다. 동작(1205)에서 휴대용 장치가 그 자신을 신뢰할 수 있는 장치로서 인증할 수 없다고 결정되면, 프로세스는 종료되고 휴대용 장치는 컴퓨터와 연결되지 않는다. 다른 대안으로서, 동작(1205)에서 휴대용 장치가 그 자신을 신뢰할 수 있는 장치로서 인증할 수 있다고 결정되면, 프로세스는 수동 연결 동작이 수행될 필요가 없도록 휴대용 장치가 컴퓨터와 자동으로 연결되는 동작(1207)으로 진행된다.

[0027] 이상에서 논의된 바와 같이, 다수의 컴퓨터가 액세스가능한 데이터 저장소에 저장될 수 있는 인증 정보(예를 들어, 도 2의 909)는 임의의 적합한 형태를 가질 수 있다. 예를 들어, 인증 정보는, 공개적으로 액세스될 수 없고(본 명세서에서 편의상 "비밀"이라고 함) 인증 정보를 사용하여 휴대용 장치를 인증하는 컴퓨터가 인증 정보와 연관된 신뢰할 수 있는 휴대용 장치만이 제공할 수 있다고 예상하는 몇몇 정보를 포함할 수 있다.

[0028] 다른 대안으로서, 본 발명의 다른 실시예에 따르면, 인증 정보는 하나 이상의 보안 프로토콜에 따라 휴대용 장치와 통신하기 위하여 키 관련 자료(들)를 검색하는 컴퓨터에 의해 사용될 수 있는 하나 이상의 키 관련 자료를 포함할 수 있다. 예를 들어, 비제한적인 일 실시예에서, 키 관련 자료(들)의 일부는 통신에 수반되는 디지털

서명을 확인하고, 그로써 통신이 실제로 신뢰할 수 있는 휴대용 장치에 의해 전송되었다는 것을 확인하기 위해 컴퓨터에 의해 사용될 수 있는데, 그 이유는 인증 정보와 연관된 신뢰할 수 있는 휴대용 장치만이 유효한 디지털 서명과 함께 그러한 통신을 송신할 수 있었을 것이기 때문이다. 다른 일례에서, 키 관련 자료(들)의 일부는 휴대용 장치에 의해 암호화된 통신을 복호화하기 위하여 컴퓨터에 의해 사용될 수 있다.

[0029] 본 명세서에서, "키 관련 자료"라는 어구는 통신을 보호할 목적으로, 예를 들어, 메시지의 비밀 및 무결성을 유지하고 및/또는 메시지 소스를 인증하기 위해, 사용될 수 있는 임의의 정보를 말하는 데 사용된다. 키 관련 자료의 일례는 공개-개인 키 쌍(비대칭 키 암호화 및 전자 서명에서 사용됨), 비밀 키(대칭 키 암호화에서 사용됨), 논스(nonce)(즉, 한번 사용되고 버려지는 랜덤한 값), 및 체크섬(checksum)/해시(hash)[통상적으로 암호화 해시 함수에 의해 생성되어 무결성 확인 및/또는 확정(commitment) 등의 다른 목적으로 사용됨]를 포함한다. 이들은 본 명세서에 기술된 일부 실시예에 따라 사용되는 인증 정보를 설정하기 위해 사용될 수 있는 키 관련 자료들의 일례에 불과하다. 그에 부가하여, 본 명세서에 기술된 본 발명의 측면들이 임의의 특정 유형의 키 관련 자료 또는 기타 인증 정보를 이용하는 것으로 제한되지 않기 때문에, 데이터 저장소에 저장된 인증 정보가 임의의 적합한 방식으로 휴대용 장치를 인증하기 위해 컴퓨터가 데이터 저장소에 액세스할 수 있게 해주는 어떤 정보라도 구현할 수 있다는 것을 잘 알 것이다.

[0030] 본 발명의 일 실시예에 따르면, 자동 연결을 허용하기 전에 컴퓨터에 대해 휴대용 장치를 인증할 뿐만 아니라, 이와 유사하게 휴대용 장치가 컴퓨터를 그와 자동으로 연결될 수 있게 해주기 전에 휴대용 장치에 대해 컴퓨터 및/또는 그 사용자를 인증하기 위해 단계들이 취해진다. 따라서, 이하에서 기술될 본 발명의 일부 실시예는, 컴퓨터와 휴대용 장치 간의 자동 연결을 가능하게 해주기 전에 컴퓨터에 대해 휴대용 장치를 인증하는 것에 부가하여, 휴대용 장치에 대해 컴퓨터 및/또는 그 사용자를 인증하는 기술을 구현한다. 그러나, 본 명세서에 설명된 기술들이 자동 연결을 가능하게 해주기 위해 컴퓨터에 대해 단지 휴대용 장치를 인증하는 데 이용될 수 있기 때문에, 본 발명의 모든 측면들이 이 점에서 제한되지 않는다는 것을 잘 알 것이다.

[0031] 종래의 자동 장치 연결 기술들은 각각의 컴퓨터가 자신과 자동으로 연결될 수 있는 각각의 휴대용 장치에 대해 개별적인 키 관련 자료 집합(수동 연결 동안 발생됨)을 저장하도록 요구한다. 마찬가지로, 휴대용 장치는 종래에는 장치와 자동으로 연결될 수 있는 각각의 컴퓨터에 대해 개별적인 키 관련 자료 집합(역시 수동 연결 동안 발생됨)을 저장해야 한다. 이러한 이유는, 기존의 장치 연결 기술에서, 2개의 장치를 수동으로 연결한 결과로 발생되는 키 관련 자료들이 장치에 고유하고 장치들과 관련되어 있기 때문이다.

[0032] 종래의 연결 기술의 일례로서, 도 6은 단순화된 버전의 블루투스 간편 연결 프로토콜(Bluetooth Simple Pairing protocol)을 나타낸 것이다. 먼저, 동작(310)에서, 2개의 블루투스-지원(Bluetooth-enabled) 장치가 서로를 검색하고, 동작(320)에서, 보안되지 않은 통신 채널을 설정한다. 그 다음에, 동작(330)에서, 2개의 참여 장치가 자신의 공개 키를 교환한다. 동작(340)에서, 참여 장치의 교환된 공개 키 및/또는 블루투스 주소에 기초하여, 확인 값(confirmation value)이 계산되며, 동작(350)에서, 연결을 관리하는 링크 키(link key)가 참여 장치의 블루투스 주소를 사용하여 계산되며, 동작(360)에서, 링크 키가 암호화된 통신에 참여하기 위해 사용된다.

[0033] 이상의 내용으로부터 잘 알 것인 바와 같이, 블루투스 간편 연결을 사용하여 설정된 키 관련 자료는 참여 장치의 블루투스 주소에 관련된다. 그 결과, 두 쌍이 공통으로 한 장치를 가지고 및/또는 키 관련 자료가 한 장치에서 다른 장치로 전송될 수 있더라도, 한 쌍의 장치 간에 설정된 키 관련 자료는 통상적으로 다른 쌍의 장치들을 연결하는 데 재사용되지 않는다. 일례로, 휴대용 장치와 제1 블루투스 주소를 가지는 제1 컴퓨터에 대해 설정된 키 관련 자료가 제2 컴퓨터와 휴대용 장치를 연결하기 위해 사용된 경우, 휴대용 장치는 제2 컴퓨터와의 연결을 거절할 수 있는데, 그 이유는 키 관련 자료가 제1 블루투스 주소와 관련되어 있고 제2 컴퓨터가 다른 블루투스 주소를 가진다는 것을 휴대용 장치가 알 수 있기 때문이다. 따라서, 본 발명의 일 실시예에 따르면, 장치 독립적인 암호화 키 관련 자료가 이용되며, 그에 따라 그 암호화 키 관련 자료가 장치 연결을 목적으로 서로 다른 컴퓨터에 의해 쉽고 안전하게 공유될 수 있다.

[0034] 일 실시예에서, 장치 독립적인 키 관련 자료는, 수동 연결 절차를 통해 또는 다른 방식으로, 휴대용 장치와 임의의 특정 컴퓨터 간이 아니라 휴대용 장치와 그 사용자 간에 생성된다. 따라서, 종래의 장치 연결 프로토콜을 사용하여 형성된 키 관련 자료와는 달리, 키 관련 자료가 임의의 특정 컴퓨터에 관련되지 않으며, 따라서 휴대용 장치를 임의의 컴퓨터 또는 컴퓨터 그룹과 연결하는 데 사용될 수 있다. 본 발명의 일 실시예에 따르면, 장치-독립적인 키 관련 자료를 사용하여 휴대용 장치를 컴퓨터와 연결하는 연결 프로토콜이 이용된다. 그러나, 본 명세서에 기술된 키 관련 자료, 연결 프로토콜 및 기타 기술은 이 점에서 제한되지 아니하며, 휴대용 장치와 종래에 컴퓨터라고 했던 장치(예를 들어, 랩톱 또는 개인용 컴퓨터)간 뿐만 아니라 임의의 유형의 임의의 2개의

장치 간을 포함하는 임의의 유형의 임의의 2개 이상의 장치 간의 연결을 수행하는 데 사용될 수 있다. 그에 부가하여, 컴퓨터 또는 컴퓨팅 장치(본 명세서에서 서로 바꾸어 사용될 수 있음)라는 것이, 본 명세서에서, 종래에는 컴퓨터라고 할 수 없던 장치들을 포함하여 프로그램된 프로세서를 가지는 임의의 장치를 말하는 데 사용된다는 것을 잘 알 것이다. 그에 부가하여, 본 명세서에 설명된 기술은 장치 그룹들 사이에 연결을 수행하는 데 사용될 수 있다. 일례로, 본 명세서에 설명된 기술은, 제1 키 관련 자료 집합을 공유하는 장치 그룹이 제2 키 관련 자료 집합을 공유하는 다른 장치 그룹과 연결될 수 있게 해주는 브로드캐스트 또는 멀티캐스트 시나리오에서 사용될 수 있다.

[0035] 일 실시예에 따라 사용되는 장치 독립적인 키 관련 자료는 휴대용 장치를 연결하기 위해 어떤 컴퓨터라도 이용할 수 있게 되어 있을 수 있다. 이것은 임의의 적당한 방식으로 달성될 수 있다. 예를 들어, 키 관련 자료는 휴대용 장치와 연결되는 제1 컴퓨터에 저장될 수 있고, 나중에 사용자의 요청 시에 또는 제2 컴퓨터로부터의 자동 요청에 응답하여 제2 컴퓨터로 전달될 수 있다. 다른 대안으로서, 제1 컴퓨터는 전역적으로 액세스가능한 저장소에 키 관련 자료를 저장할 수 있으며, 그에 따라 제2 컴퓨터는 그로부터 키 관련 자료를 검색할 수 있다. 전역적으로 액세스가능한 저장소는 제1 컴퓨터에 또는 별도의 컴퓨터에 있을 수 있고 및/또는 웹 인터페이스, 네트워크 파일 시스템 인터페이스 또는 임의의 다른 적합한 인터페이스와 같은 임의의 적합한 인터페이스를 사용하여 검색될 수 있다.

[0036] 이하에서 기술될 본 발명의 일 실시예에 따르면, 휴대용 장치를 연결하기 위해 다수의 컴퓨터에 의해 사용되는 장치 독립적인 키 관련 자료는 사용자와 휴대용 장치 둘다에 대한 고유 식별자(ID)를 사용하여 발생된다. 이들 ID를 이용하여 키 관련 자료를 발생하는 본 발명의 측면들이 이 점에서 제한되지 않기 때문에, 이들 고유 식별자는 임의의 적합한 방식으로 설정될 수 있다. 예를 들어, 고유 사용자 ID는 사용자의 전자 메일 주소이거나, Microsoft Corporation으로부터 이용가능한 Windows Live ID와 같이 고유 식별자를 제공하는 서비스 또는 임의의 다른 서비스를 통해 제공되는 고유 식별자일 수 있거나, 임의의 다른 적합한 방식으로 제공될 수 있다. 이와 유사하게, 휴대용 장치는 GUID(Globally Unique Identifier)과 같은 임의의 적합한 기술 또는 임의의 다른 적합한 기술을 사용하는 고유 식별자를 통해 식별될 수 있다.

[0037] 도 7을 참조하면, 본 발명의 일 실시예에 따른 장치 독립적인 키 관련 자료를 설정하기 위하여 휴대용 장치와 컴퓨터를 수동으로 연결하는 프로세스가 메시지 차트의 형태로 도시되어 있다. 도 7에서 예시된 프로세스는 휴대용 장치(410)와 컴퓨터(420)가 서로를 검색하고 임의의 적합한 방법으로 통신 채널(예를 들어, 보안되지 않은 채널)을 설정한 후에 시작할 수 있다. 블루투스의 경우에, 예를 들어, 휴대용 장치(410)는 검색 가능 모드에 있었을 수 있으며, 컴퓨터(420)는 스캔을 수행하여 휴대용 장치(410)를 검색했을 수 있고 휴대용 장치(410)와 통신을 시작했을 수 있다. 통신의 기본 방법에 따라, 도 7에 예시된 통신의 교환이 검색 및 통신 설정 동안에 또는 2개의 참여 장치들 간의 임의의 적합한 통신 단계 동안에 수행될 수 있는데, 그 이유는 본 발명이 이 점에서 제한되지 않기 때문이다.

[0038] 동작(430)에서, 컴퓨터(420)는 사용자의 ID(ID_{user}), 사용자의 공개 키(PK_{user}), 및 사용자와 휴대용 장치(410) 간의 연결을 위해 발생된 랜덤한 값($R_{user,dev}$)을 포함하는 제1 정보 컬렉션을 휴대용 장치(410)로 송신한다. 랜덤한 값($R_{user,\ dev}$)은 사용자와 휴대용 장치(410) 간의 연결을 일의적으로 식별해주는 비밀 정보이다. 이하에서 논의되는 바와 같이, 일 실시예에 따르면, $R_{user,dev}$는 자동 연결을 설정하기 위해 장치가 부적절하게 자신을 표현하려고 하는 재생 공격(replay attack)에 대한 보안을 제공하기 위해 사용될 수 있다.

[0039] 그러나, 일부 실시예에서 생략될 수 있기 때문에(예를 들어, 그러한 공격의 위험이 최소한이라고 생각되는 경우), 장치 독립적인 키 관련 자료를 발생하는 프로토콜과 관련된 본 발명의 측면이 그러한 공격으로부터 보호하기 위해 $R_{user,dev}$와 같은 부가의 비밀 정보를 이용하는 것으로 제한되지 않는다는 것을 잘 알 것이다. 그에 부가하여, 일 실시예에서 비밀 정보가 난수로서 제공되고 있지만, 난수로 제한되지 않기 때문에, 비밀 정보를 설정하는 데 어떤 기술이라도 이용될 수 있다는 것을 잘 알 것이다.

[0040] 일 실시예에서, 난수를 휴대용 장치로 전송하는 것을 보호하는 기술이 이용된다. 이것은 임의의 적당한 방식으로 행해질 수 있다. 예를 들어, 다른 장치가 도청하는 것을 실제로 불가능하게 만들 정도로 작은 전송 범위를 갖는 NFC와 같은 근접 무선 기술 또는 USB 장치를 통해 전송이 행해질 수 있다.

[0041] 동작(440)에서, 휴대용 장치(410)는 휴대용 장치(410)의 ID(ID_{dev}) 및 휴대용 장치(410)의 공개 키(PK_{dev})를 포함하는 제2 정보 컬렉션을 컴퓨터(420)로 송신한다.

[0042] 본 명세서에 기술된 기술들이 동작(430 및 440) 동안에 교환되는 정보의 정확한 조합 또는 도 7에 도시된 통신의 횟수 및 순서로 제한되지 않는다는 것을 잘 알 것이다. 예를 들어, 일 실시예에서, 보안을 강화하기 위하여, 공개 키는 휴대용 장치(410)와 컴퓨터(420) 둘다가 신뢰하는 인증 기관에 의해 서명된 인증서에 넣어 휴대용 장치(410)와 컴퓨터(420) 간에 송신될 수 있지만, 꼭 이럴 필요는 없다. 게다가, 동작(430 및 440)을 다수의 통신으로 분해하는 것 및 통신을 임의의 적합한 순서로 인터리빙하는 것을 비롯한 임의의 적합한 방식으로 정보가 교환될 수 있다.

[0043] 동작(450)에서, 휴대용 장치(410)는 컴퓨터(420)에 의해 제공되는 정보 또는 그로부터 파생되는 정보의 적어도 일부를 그의 디스플레이 상에 디스플레이하며, 이와 유사하게, 컴퓨터(420)는, 사용자가 통신하는 장치가 올바른 장치임을 확인하고 그에 따라 통신이 신뢰할 수 있음을 확증할 수 있게 해주기 위해, 휴대용 장치(410)로부터 수신된 정보 또는 그로부터 도출된 정보의 적어도 일부를 그의 디스플레이 상에 디스플레이한다. 디스플레이되는 정보는 사용자가 신뢰할 수 있는 관계를 설정하기 위하여 다른 장치에 의해 제공된 것으로 확인할 수 있는 정보이다. 이것은 임의의 적합한 방식(그 일례들이 이하에 기술됨)으로 수행될 수 있다. 예를 들어, 일 실시예에서, 휴대용 장치(410)는 ID_{user}를 디스플레이할 수 있고 컴퓨터(420)는 ID_{dev}를 디스플레이할 수 있으며, 이와 유사하게, 사용자는 각각의 장치에서 상대방 장치로 전송되는 ID를 볼 수 있었을 수 있으며[예를 들어, 사용자는 휴대용 장치(410) 상에서 ID_{dev} 를 볼 수 있고 컴퓨터(420)로부터 ID_{user}를 볼 수 있었을 수 있음], 그에 따라 각각의 장치가 다른 장치로부터 전송된 식별자를 적절하게 디스플레이하는지를 사용자가 확인할 수 있다.

[0044] 일부 장치[예를 들어, 휴대용 장치(410)]는 사용자에게 그 정보를 시각화하고 확인할 기회를 주기 위해 정보를 디스플레이할 수 있는 디스플레이 또는 사용자 인터페이스를 가지고 있지 않을 수 있다. 본 발명의 일 실시예에 따르면, 이러한 장치의 경우, 그 휴대용 장치 상에 정보를 디스플레이하는 단계가 생략될 수 있다. 그 단계를 생략하는 것은 휴대용 장치가 원하는 컴퓨터(예를 들어, 420)와 정보를 교환하는 것을 사용자가 확인하지 못하게 할 수 있다. 그러나, 사용자가 그로 인한 보안의 저하를 받아들일 의사가 있는 경우, 그 단계가 완전히 생략될 수 있다. 다른 대안으로서, 이러한 상황에서, 휴대용 장치와 컴퓨터 간에 정보를 교환하는 데 사용되는 통신 매체는 2개의 신뢰할 수 있는 장치가 통신 중이라는 것을 확증해주는 것일 수 있다. 예를 들어, 통신은 유선 연결을 통해, USB 플래시 장치와 같은 휴대용 통신 매체를 통해, 또는 매우 적은 전송 범위를 가지며 제3 컴퓨팅 장치가 통신을 가로채기하고 및/또는 삽입할 가능성을 없애주는 NFC와 같은 통신 기술을 사용하여 수행될 수 있다.

[0045] 동작(460)에서, 사용자는, 휴대용 장치(410) 및 컴퓨터(420) 중 하나 또는 둘다와 상호작용함으로써, 신뢰할 수 있는 장치 간에 연결 및 정보 교환이 있었다는 것을 확인한다. 예를 들어, 동작(450)에서 디스플레이된 ID가 올바른 경우, 사용자는 휴대용 장치(410) 및 컴퓨터(420)의 사용자 인터페이스를 동작시켜 이것을 표시할 수 있다. 그렇게 표시된 경우, 컴퓨터(420) 및 휴대용 장치(410)는 이하에서 기술되는 방식으로 계속할 것이다. 다른 대안으로서, 정보가 신뢰할 수 있는 장치 간에 교환되었다는 것을 사용자가 나타내지 않은 경우, 프로세스는 종료되고 연결 정보는 저장되지 않을 것이다.

[0046] 컴퓨터(420) 및 휴대용 장치(410)에 디스플레이될 것으로 예상되는 정보가 임의의 적합한 방식으로 사용자에게 통지될 수 있다는 것을 잘 알 것이다. 예를 들어, 신뢰할 수 있는 관계를 확인하기 위하여 다른 장치 상에서 보게 될 것으로 예상되는 정보를 사용자가 알 수 있도록, 각각의 장치[예를 들어, 휴대용 장치(410) 및 컴퓨터(420)]는 그 자신의 ID 또는 기타 정보를 사용자에게 디스플레이할 수 있는 사용자 인터페이스를 제공할 수 있다. 예를 들어, 이상에서 언급한 바와 같이, 컴퓨터(420)가 올바른 휴대용 장치(410)와 연결되어 있다는 것을 확인하기 위하여, 어떤 정보가 컴퓨터(420)에 의해 디스플레이될 것으로 예상되는지를 사용자가 알 수 있도록, 휴대용 장치는 그 자신의 사용자 인터페이스 상에서 자신의 ID를 사용자에게 디스플레이할 수 있다. 그러나, 이것은 일례에 불과한데, 그 이유는 연결 장치 중 하나 또는 둘다에 표시될 것으로 예상되는 정보가 사용자에게 임의의 적합한 방식으로 통지될 수 있기 때문이다.

[0047] 이상에서 논의된 바와 같이, 사용자가 휴대용 장치(410) 및 컴퓨터(420) 중 하나 또는 둘다와 상호작용함으로써 관계가 신뢰할 수 있다는 것을 확인할 때, 휴대용 장치(410) 및 컴퓨터(420)는 단계(430 및 440)에서 수신된 정보 및/또는 그로부터 도출된 정보의 적어도 일부를 저장한다. 예를 들어, 휴대용 장치(410)는 휴대용 장치에서 이용가능한 임의의 내부 저장소(예를 들어, 메모리)에 <ID_{user}, PK_{user}, $R_{user,dev}$> 프로파일을 저장할 수 있는 반면에, 컴퓨터(420)는 전역적으로 액세스가능한 저장소의 사용자와 연관된 위치에 <ID_{dev}, PK_{dev}, $R_{user,dev}$> 프로파일을 저장할 수 있다. 본 명세서에 설명된 기술들이 임의의 특정 정보가 교환되는 것으로 제한되지 않기 때문에,

부가의 및/또는 대안의 정보가 획득되어 이들 프로파일에 저장될 수 있다. 다른 적당한 유형의 정보도 역시 이용될 수 있다. 도 7에서 생성된 프로파일이 하나 이상의 컴퓨터[컴퓨터(420) 이외의 컴퓨터를 포함함]에 대해 휴대용 장치를 인증하고 자동 연결을 용이하게 해주기 위해 사용될 수 있는 방식의 예시적 일례에 대해 이하에서 기술한다.

[0048] 도 8은 도 7에 예시된 프로토콜 및 정보를 사용하여 복수의 사용자들(사용자 1 내지 사용자 N)에 대해 설정된 장치 프로파일을 저장하는 전역적으로 액세스가능한 데이터 저장소(801)의 예시적 구성을 나타낸 것이다. 이상에서 언급한 바와 같이, 이러한 프로파일은 단지 예시적인 것이며, 따라서 전역적으로 액세스가능한 데이터 저장소가 다른 유형의 정보를 저장하기 위해 다른 방식으로 구성될 수 있다. 도 8에 예시된 일 실시예에서, 각각의 사용자가 다수의 장치들과 연관될 수 있다. 예를 들어, 사용자 1과 연관되어 있는 저장된 정보는 3개의 항목(805a 내지 805c)을 포함하며, 그 각각은 사용자 1과 연관된 서로 다른 장치에 대응한다. 예를 들어, 항목(805a 내지 805c)이 모두 동일한 사용자에게 속하는 휴대폰, MP3 플레이어 및 무선 헤드폰 세트에 대응할 수 있지만, 이들이 단지 일례에 불과한데, 그 이유는 사용자와 연관된 휴대용 장치(들)이 임의의 적합한 휴대용 장치(들)일 수 있기 때문이다.

[0049] 동일한 휴대용 장치가 다수의 사용자에 의해 공유될 수 있음을 잘 알 것이다. 따라서, 도 8에 예시된 본 발명의 일 실시예에 따르면, 동일한 장치가 데이터 저장소(801) 내의 다수의 사용자들과 연관될 수 있다. 이것이, 예를 들어, 식별자 ID_{dev1}로 식별되는 장치가 항목(805a)에 의해 사용자 1과 연관되어 있고, 또한 항목(807a)에 의해 사용자 2와 연관되어 있는 것으로 나타내어져 있다.

[0050] 도 8에서 알 수 있는 바와 같이, 일 실시예에 따르면, 사용자와 휴대용 장치 간의 연결을 식별해주는 값이 서로 다르기 때문에(예를 들어, $R_{user1,dev1}$ 및 $R_{user2,dev1}$), 항목(805a과 807a)이 동일하지 않다.

[0051] 본 발명의 일 실시예에 따르면, 특정 사용자와 특정 장치 간의 연결을 식별해주는 고유 값의 사용은 신뢰할 수 없는 사용자에 의한 잠재적인 재생 공격으로부터 보호하기 위해 사용될 수 있다. 이 점에서, 본 명세서에 설명된 기술들이 다수의 사용자에 의해 공유될 수 있는 컴퓨터 및 다른 장치에서 이용될 수 있다는 것을 잘 알 것이다. 따라서, 본 발명의 일 실시예에 따르면, 사용자와 휴대용 장치 간의 연결을 식별해주는 고유 값의 사용은 신뢰할 수 없는 사용자에 의해 주도되는 재생 공격을 막기 위하여 이용될 수 있다. 이러한 공격은 어느 한 형태 또는 여러 형태를 취할 수 있다. 예를 들어, 이상의 내용으로부터 잘 알 것인 바와 같이, 컴퓨터와 특정 휴대용 장치(이 일례에서, 장치 1이라고 함) 간에 인증 정보를 교환하는 프로세스에서, 장치 1은 컴퓨터에 로그인된 사용자의 ID를 인증하기 위하여 컴퓨터가 송신하는 정보(예를 들어, 사용자와 연관된 키에 의해 서명된 ID_{user})를 수신할 것이다. 따라서, 그 정보는 휴대용 장치(예를 들어, 이 일례에서 장치 1)에 저장될 수 있다. 다른 사용자가 휴대용 장치(예를 들어, 장치 1)를 제어하고 있는 경우, 사용자가 그 휴대용 장치로 하여금 컴퓨터로부터 수신된 정보를 재생하게 할 수 있는 위험이 있으며, 그에 따라 실제로는 휴대용 장치가 다른 사용자(예를 들어, 사용자 2)의 제어 하에 있을 때, 휴대용 장치는 기본적으로 자신이 제1 사용자(예를 들어, 사용자 1)가 로그인한 컴퓨터라고 스푸핑(spoofing)할 수 있고, 사용자 1로서 다른 장치(예를 들어, 장치 2)와 자동 연결하려고 할 수 있다.

[0052] 휴대용 장치를 인증하기 위해 정보의 교환에 참여하는 컴퓨터는 휴대용 장치가 그 자신을 인증하기 위해 사용하는 정보(예를 들어, 휴대용 장치의 키로 서명된 휴대용 장치에 대한 고유 식별자)를 수신할 것이고 이러한 정보가 컴퓨터에 저장되고, 사용자 1 이외의 사용자(예를 들어, 사용자 2)가 로그인되어 있는 다른 컴퓨터 또는 다른 유형의 장치와 연결을 형성하려고 할 때, 휴대용 장치의 ID를 스푸핑하기 위해 컴퓨터에 의해 재생될 가능성이 있을 수 있다는 유사한 위험이 존재한다는 것을 잘 알 것이다. 예를 들어, 컴퓨터와 장치 1 간에 인증 정보를 교환하는 프로세스에서, 컴퓨터는 장치 1이 자신을 인증하기 위해 송신하는 정보(예를 들어, dev1와 연관된 키로 서명된 ID_{dev})를 수신할 것이다. 이어서, 그 정보가 컴퓨터에 저장될 수 있다. 적대 관계에 있는 엔터티가 그 컴퓨터를 제어하고 있는 경우, 적대 관계에 있는 엔터티가 그 컴퓨터로 하여금 장치 1로부터 수신된 정보를 재생하게 할 수 있으며, 그에 따라 컴퓨터가 장치 1인 것으로 기본적으로 스푸핑을 할 수 있고 장치 1로서 다른 사용자(예를 들어, 사용자 2)와 자동으로 연결하려고 할 수 있는 위험이 있다.

[0053] 본 발명의 일 실시예에 따르면, 특정 사용자와 특정 장치 간의 연결을 일의적으로 식별해주는 값을 장치들 간에 교환되는 인증 정보에 포함시키는 것은 이상에서 논의된 유형의 재생 공격을 막는다. 예를 들어, 장치가 특정 사용자가 로그인되어 있다고 알려진 컴퓨터로부터 수신된 통신을 적절히 인증하기 위해, 장치는 그 자신(즉, 특정 장치)과 사용자 간의 연결을 식별해주는 특정한 고유 값을 확실히 수신하는지를 확인할 것이다. 따라서, 컴

퓨터로부터 인증 정보를 수신하는 장치가 컴퓨터에 로그인된 사용자의 ID를 인증하는 데 필요로 하는 모든 정보를 가지고 있는 반면, 임의의 다른 장치가 사용자를 인증하기 위해 필요로 하는 정보는 수신하지 않는데, 그 이유는 각각의 장치가 그 자신과 사용자 간의 연결과 관련된 그 자신의 고유 값을 가지기 때문이다. 따라서, 사용자로부터 인증 정보를 수신하는 장치(예를 들어, 이상의 일례에서 장치 1)는 다른 장치(예를 들어, 이상의 일례에서 장치 2)와 연결하기 위해 사용자가 로그인되어 있는 컴퓨터의 ID를 성공적으로 스푸핑할 수 없는데, 그 이유는 이러한 재생 공격을 시도하는 장치가 다른 장치(예를 들어, 장치 2)가 사용자의 ID를 인증하기 위해 수신할 것이라고 예상되는 특정한 값을 소유하지 않기 때문이다.

[0054] 이와 유사하게, 특정 사용자와 특정 장치 간의 연결을 특정하여 식별해주는 값을 사용하는 것은, 로그인된 사용자와 연관될 임의의 장치(예를 들어, 장치 1)로부터 인증 정보를 수신한 컴퓨터가 그 장치의 ID를 스푸핑하여 다른 사용자가 로그인되어 있는 다른 컴퓨터 또는 다른 장치와 연결을 형성하려고 시도하는 것을 막기 위해 이용될 수 있다. 예를 들어, 컴퓨터가 컴퓨터에 로그인되어 있는 사용자와 연관된 것으로 알려진 휴대용 장치로부터 수신된 통신을 적절히 인증하기 위해, 컴퓨터는 휴대용 장치와 컴퓨터에 로그인된 사용자 간의 연결을 식별해주는 특정한 고유 값을 확실히 수신하는지를 확인할 것이다. 따라서, 제1 사용자와 연결할 휴대용 장치로부터 인증 정보를 수신하는 컴퓨터는 제1 사용자에 대해 휴대용 장치의 ID를 인증하기 위해 필요한 모든 정보를 가지는 반면, 휴대용 장치를 인증하기 위해 제2 사용자에게 주어질 필요가 있는 정보는 수신하지 않는데, 그 이유는 각각의 사용자가 각각의 사용자와 휴대용 장치 간의 연결에 관련된 고유 값을 갖기 때문이다. 따라서, 제1 사용자(예를 들어, 이상의 일례에서 사용자 1)와 연결할 휴대용 장치(예를 들어, 이상의 일례에서 장치 1)로부터 인증 정보를 수신하는 컴퓨터는, 다른 사용자(예를 들어, 이상의 일례에서 사용자 2)가 로그인되어 있는 다른 컴퓨터와 연결하기 위해 장치 1의 ID를 성공적으로 스푸핑할 수 없는데, 그 이유는 그러한 재생 공격을 시도하는 컴퓨터가 휴대용 장치의 ID를 인증하기 위해 다른 사용자(예를 들어, 사용자 2)가 수신할 것이라고 예상되는 특정 값을 소유하지 않기 때문이다.

[0055] 일 실시예에서, 연결을 일의적으로 식별해주는 값은 하나 이상의 안전하고 변조 방지 위치에 저장된다. 다른 대안으로서, 값이 암호화된 형태로 저장될 수 있는 반면, 복호화 키는 하나 이상의 안전하고 변조 방지 위치에 저장된다.

[0056] 게다가, 이상에서 기술한 프로파일 대신에 또는 그에 부가하여, 다른 유형의 정보가 전역적으로 액세스가능한 저장소에 저장될 수 있다는 것을 잘 알 것이다. 예를 들어, 도 11에 도시된 프로토콜에서 사용되는 사용자의 공개 및 비밀 키는 전역적으로 액세스가능한 저장소에 저장될 수 있다. 그러나, 사용자가 다른 저장소 위치로부터, 예를 들어, 사용자가 로그인되어 있는 컴퓨터의 로컬 저장소 위치에서 공개 및 비밀 키를 검색할 수 있기 때문에, 꼭 이럴 필요는 없다.

[0057] 도 9는 휴대용 장치의 사용자에 대해 설정된 복수의 프로파일(903a 내지 903b)을 포함하는 휴대용 장치의 메모리의 예시적 구성을 예시한 것이다. 도 9에 단지 2개의 프로파일(903a 및 903b)만이 도시되어 있지만, 임의의 적합한 수의 프로파일이 저장될 수 있다는 것을 잘 알 것이다. 동일한 개인이 시스템에 의해 (예를 들어, 다른 사용자 ID에 의해) 서로 다른 사용자로 인식될 수 있도록, 각각의 프로파일이 휴대용 장치의 서로 다른 사용자에 대응될 수 있거나, 사용자가 서로 다른 상황에서 사용하기 위한 다수의 프로파일을 정의할 수 있다. 예시적인 시나리오에서, 사용자는 ID_{user1}을 사용하여 하나 이상의 가정용 컴퓨터에 로그인할 수 있고, ID_{user2}를 사용하여 하나 이상의 업무용 컴퓨터에 로그인할 수 있다. 휴대용 장치에 2개의 프로파일(하나는 ID_{user1}에 대한 것이고 다른 하나는 ID_{user2}에 대한 것임)을 저장하는 것에 의해, 휴대용 장치는 사용자의 ID 중 어느 하나를 사용하여 사용자가 로그인되어 있는 임의의 컴퓨터에 자동으로 연결할 수 있다. 본 발명이 휴대용 장치와 동시에 연결될 수 있는 사용자의 수에 대해 제한되지 않는다는 것을 잘 알 것이다. 일부 실시예에서, 휴대용 장치는 한 번에 단 한명의 사용자와의 연결을 허용할 수 있는 반면, 다른 실시예에서, 휴대용 장치는 한 번에 2명 이상의 사용자와의 연결을 허용할 수 있다(예를 들어, 휴대용 장치와 동시에 연결할 수 있는 사용자 수에 관한 상한을 가질 수 있다).

[0058] 다시 말하지만, 도 9에 도시된 프로파일 대신에 또는 그에 부가하여, 다른 유형의 정보가 휴대용 장치의 메모리에 저장될 수 있음을 잘 알 것이다. 예를 들어, 도 11에 도시된 프로토콜에서 사용되는 휴대용 장치의 공개 및 비밀 키가 저장될 수 있다.

[0059] 프로파일이 설정되고 휴대용 장치 및 전역적으로 액세스가능한 데이터 저장소(본 명세서에서 사용된 바와 같이, 데이터 저장소가 전역적으로 액세스가능하다는 것은 데이터 저장소가 단일 컴퓨터에 관련되지 않고 2개 이상의

서로 다른 컴퓨터에 의해 액세스될 수 있다는 것을 의미함)에 저장되면, 그 안에 들어 있는 정보는 휴대용 장치와 컴퓨터를 상호 인증하고 임의의 적합한 기술(그 일례가 이하에서 논의됨)을 사용하여 자동 연결을 용이하게 해주는 데 사용될 수 있다. 그러나, 프로파일 정보(또는 이상에서 논의된 바와 같이 인증을 위해 사용될 수 있는 임의의 다른 유형의 비밀 또는 키 관련 자료)가 도 7의 수동 연결 프로세스를 사용하는 것 이외의 방식으로 형성될 수 있음을 잘 알 것이다. 예를 들어, 이상에서 논의된 바와 같이, 본 발명의 일 실시예에 따르면, 비밀 정보는 휴대용 장치와 임의의 컴퓨터 간에 수동 연결 동작을 거치지 않고 설정될 수 있다. 도 8 및 도 9와 관련하여 이상에서 논의된 특정 프로파일에서 사용하기 위한 이 유형의 예시적 프로세스가 도 10에 도시되어 있다. 그러나, 수동 연결 없이 키 관련 자료의 형성을 가능하게 해주는 본 발명의 측면이 도 8 및 도 9에 도시된 프로파일에 포함된 특정한 유형의 키 관련 자료에 대해 사용하는 것으로 제한되지 않음을 잘 알 것이다.

[0060] 도 10의 프로세스에서, 동작(710)에서 사용자와 휴대용 장치에 대해 공개-개인 키 쌍 및 랜덤한 값을 포함하는 키 관련 자료가 획득된다. 공개-개인 키 쌍 및 난수가 동작(710)에서 새로 생성될 수 있거나, 기존의 공개-개인 키 및 난수 값이 검색될 수 있다. 임의의 적합한 컴퓨팅 장치(들)가 키 관련 자료를 획득하기 위해 사용될 수 있는데, 그 이유는 본 발명이 이 점에서 제한되지 않기 때문이다.

[0061] 동작(720)에서, 휴대용 장치에 저장될 키 관련 자료의 부분(들)이 임의의 적합한 방식으로 (예를 들어, 키 관련 자료를 가지고 있고, 키 관련 자료를 유선 또는 무선 연결을 거쳐, 키 관련 정보 등을 다운로드하기 위하여 휴대용 장치에 연결될 수 있는 휴대용 컴퓨터-판독가능 매체를 통하여, 휴대용 장치로 전달하는 컴퓨터로부터) 휴대용 장치로 전송된다. 저장된 정보는 휴대용 장치가 그 자신을 인증하기 위하여 컴퓨터에 제공하는 정보(예를 들어, ID_{dev}, PK_{dev} 및 $R_{user,dev}$), 장치와 자동으로 연결할 수 있는 컴퓨터에게 전송되는 공개 키와 함께 공개-개인 키 쌍을 형성하는 장치에 대한 개인 키(예를 들어, SK_{dev}), 그리고, 휴대용 장치의 각각의 사용자에 대해, 휴대용 장치가 컴퓨터 또는 그 사용자를 인증할 수 있게 해주기 위해 컴퓨터로부터 휴대용 장치로 전송될 것으로 예상되는 정보(예를 들어, ID_{user}, PK_{user}, $R_{user,dev}$)를 포함할 수 있다.

[0062] 동작(730)에서, 휴대용 장치를 인증하고 자동 연결을 가능하게 해주기 위해 컴퓨터에 의해 사용되는 정보는 전역적으로 액세스가능한 데이터 저장소에 저장되며 (예를 들어, 도 8에서 도시된 바와 같이) 사용자와 연관된다. 따라서, 도 8에 도시된 일 실시예에서, 사용자와 연결된 각각의 장치에 대한 장치 프로파일 <ID_{dev}, PK_{dev}, $R_{user,dev}$>이 저장된다.

[0063] 동작들(710, 720 및 730)이 임의의 논리적으로 일관된 순서로 수행될 수 있고 각각이 다수의 동작으로 분해될 수 있으며 그 동작들이 임의의 논리적으로 일관된 순서로 인터리빙되거나 수행될 수 있음을 잘 알 것이다. 그에 부가하여, 이상에서 언급한 바와 같이, 서로 다른 키 관련 정보를 사용하는 본 발명의 다른 실시예들이 이용될 수 있기 때문에, 도 8에 예시된 특정한 키 관련 정보는 단지 예시적인 것이다.

[0064] 도 11은, 본 발명의 일 실시예에 따른, 이전에 수동으로 연결된 적이 없는 컴퓨터와 휴대용 장치가 자동 연결을 용이하게 해주는 신뢰할 수 있는 관계를 설정하기 위하여 서로를 인증할 수 있는 예시적인 프로토콜을 예시하고 있다. 상세하게는, 도 11의 프로토콜을 성공적으로 실행하면, 휴대용 장치(810)는 휴대용 장치(820)가 실제로 자처하는 장치(즉, 식별자 ID_{dev}로 식별되는 장치)라는 것을 컴퓨터(820)에게 증명한 것이 되고, 컴퓨터(820)는 ID_{dev}로 식별된 장치에 대한 연결이 ID_{user}로 식별된 사용자에 의해 수락된 것으로 확인한 것이 된다. 그에 부가하여, 컴퓨터(820)는 ID_{user}로 식별된 사용자에 의해 컴퓨터(820)가 사용되고 있음을 휴대용 장치에게 증명한 것이 되고, 휴대용 장치(810)는 ID_{user}로 식별된 사용자가 휴대용 장치(810)가 자동 연결을 수락하는 사용자들 중에 있음을 확인한 것이 된다.

[0065] 도 7에 예시된 프로세스에서와 같이, 도 11의 프로토콜은 휴대용 장치(810) 및 컴퓨터(820)가 서로를 검색하고 임의의 적합한 방식으로 통신 채널을 설정한 후에 실행될 수 있다. 그러나, 도 11에 예시된 실시예가 이 점에서 제한되지 않기 때문에, 도 11에 예시된 통신이, 검색 및 통신 설정 동안 또는 휴대용 장치(810)와 컴퓨터(820) 간의 임의의 적합한 통신 단계 동안에, 수행될 수 있다는 것을 잘 알 것이다.

[0066] 도 11은 휴대용 장치(810) 및 컴퓨터(820)가 도 8과 도 9에 예시된 유형의 이전에 설정된 프로파일을 이용하여 서로를 인증하기 위해 사용할 수 있는 예시적 프로토콜을 나타낸 것이다. 컴퓨터에 대해 휴대용 장치를 인증하고 및/또는 휴대용 장치에 대해 컴퓨터를 인증하기 위해 임의의 적합한 유형의 프로파일이 사용될 수 있기 때문에, 본 발명이 컴퓨터와 휴대용 장치 간의 상호 인증을 가능하게 해주기 위해 도 8과 도 9에 예시된 유형의 프

로파일들에서 사용되는 것으로 제한되지 않음을 잘 알 것이다. 게다가, 도 11의 프로토콜은 휴대용 장치(810) 및 컴퓨터(820) 간에 공유키(shared key)를 설정하게 한다. 이 공유키는, 직접 또는 간접적으로, 휴대용 장치(810)와 컴퓨터(820) 간의 통신을 암호화하고 복호화하기 위한 대칭 암호화 키를 획득하는 데 사용될 수 있다. 그러나, 본 발명은, 신뢰할 수 있는 관계가 설정된 경우, 안전한 통신을 가능하게 하기 위해 임의의 특정 유형의 키 관련 자료를 설정하는 것 또는, 신뢰할 수 있는 관계가 설정된 경우, 통신을 보호하지 않는 시스템에서 사용하는 것으로 제한되지 않는다.

[0067] 동작(830)에서, 컴퓨터(820)는 [예를 들어, 컴퓨터(820)에 로그인된 사용자의 ID에 기초하여] 휴대용 장치(810)와 연결될 사용자의 ID를 휴대용 장치(810)에게 통지한다. 동작(840)에서, 휴대용 장치(810)는 동작(830)에서 수신된 사용자를 식별해주는 정보(예를 들어, ID_{user})를 사용하여, 휴대용 장치가 그 사용자에 대해 저장하는 프로파일(도시된 일례에서 PK_{user} 및 $R_{user,dev}$를 포함함)을 (예를 들어, 자신의 메모리로부터) 검색한다. ID_{user}와 연관된 프로파일을 찾을 수 없는 경우(이는 휴대용 장치가 현재 ID_{user}로 식별되는 사용자와의 연결을 수락하지 않는다는 것을 나타냄), 휴대용 장치(810)는, 예를 들어, 프로토콜을 종료함으로써, 연결을 거절할 수 있다. 다른 대안으로서, 휴대용 장치는 수동 연결 절차를 시작할 수 있다(도시되지 않음). 사용자에 대한 프로파일을 찾을 수 있는 경우, 프로파일로부터 정보가 검색되고, 그에 따라 그 정보가 휴대용 장치(810)의 비밀 키(SK_{dev})와 함께 사용되어, 동작(850) 동안 컴퓨터(820)에게 다시 비밀을 제공하여 이하에서 논의되는 바와 같이 휴대용 장치(810)를 인증할 수 있다. 그에 부가하여, 도 11에 예시된 일 실시예에서, 검색된 정보는 휴대용 장치(810)가 이와 유사하게 이하에서 논의되는 방식으로 컴퓨터(820)를 인증할 수 있게 해주는 정보를 포함한다.

[0068] 예시된 실시예에서, 동작(840) 동안 휴대용 장치(810)의 비밀 키(SK_{dev})가 검색된다. 그러나, 본 발명은 비밀 키(SK_{dev})가 검색되는 때에 대해 제한되지 않는다. 예를 들어, 비밀 키(SK_{dev})는 컴퓨터(820)로부터 ID_{user}를 수신하기 전에 검색될 수 있다. 이와 유사하게, 예시된 실시예에서 동작(840) 동안 새로운 키(K_{dev})(그 용도에 대해서는 이하에서 논의함)가 발생되지만, 이 키가 동작(840)보다 앞서 발생될 수도 있는데, 그 이유는 본 발명이 이 점에서 제한되지 않기 때문이다.

[0069] 동작(850)에서, 휴대용 장치(810)는 제1 서명[도 11에 $sign_{SKdev}(ID_{dev})$로 표시됨]을 얻기 위해 SK_{dev}를 사용하여 ID_{dev}에 전자적으로 서명하며, 제1 서명, $R_{user,dev}$, ID_{dev}, 및 K_{dev}를 포함하는 제1 메시지를 구성한다. 이어서, 제1 메시지는 PK_{user}를 사용하여 암호화되고 컴퓨터(820)에게 송신된다. SK_{user}(즉, PK_{user}에 대응하는 비밀 키)를 소유한 엔터티만이 제1 메시지의 내용에 액세스할 수 있도록 암호화가 수행된다. 이것은 전송 범위 내의 임의의 다른 컴퓨터가 제1 서명을 비롯한 제1 메시지의 내용을 포착하는 것을 방지한다. 제3자가 나중에 제1 서명을 사용하여 휴대용 장치(820)로 "가장"할 수 있기 때문에, 제3자가 제1 서명을 포착하는 것을 방지하는 것이 바람직할 수 있다.

[0070] 동작(860)에서, 컴퓨터(820)는 새로운 키(K_{user})(그 용도에 대해서는 이하에서 논의함)를 생성하고 SK_{user}를 검색한다. 다시 말하지만, 이들 2개의 동작은 어떤 순서로든 수행될 수 있고, 동작(860)보다 앞서 수행될 수 있는데, 그 이유는 본 발명이 이 점에서 제한되지 않기 때문이다. 컴퓨터(820)는 SK_{user}를 사용하여 암호화된 제1 메시지를 복호화한다. 사용자가 실제로 제1 메시지의 의도된 수신자인 경우[즉, 휴대용 장치(820)가 ID_{user}로 식별된 사용자와 연결될 것으로 예상하고, 휴대용 장치(810)가 PK_{user}를 사용하여 제1 메시지를 암호화함으로써 SK_{user}를 소유한 장치만이 그 메시지를 복호화할 수 있음], 복호화가 성공하고 컴퓨터(820)는 제1 메시지로부터 ID_{dev}를 추출할 수 있다. 다른 대안으로서, ID_{dev}는 어떤 다른 수단에 의해, 예를 들어, 휴대용 장치(810)와 컴퓨터(820) 간의 이전의 정보 교환을 통해 획득될 수 있다. ID_{dev}를 사용하여, 컴퓨터(820)는 ID_{user}로 식별되는 사용자와 연결된 위치에 있는 전역적으로 액세스가능한 저장소로부터 <ID_{dev}, PK_{dev}, $R_{user,dev}$> 프로파일을 검색할 수 있으며, 그에 따라 휴대용 장치(820)가 실제로 자처하는 장치(즉, 식별자 ID_{dev}로 식별되는 장치)이고 ID_{dev}로 식별되는 장치와의 연결이 ID_{user}로 식별되는 사용자에 의해 수락되어 있는지를 확인하기 위해 검색된 프로파일에 포함된 정보가 사용될 수 있다.

[0071] 일 실시예에서, 컴퓨터(820)는 ID_{user}로 식별되는 사용자에 대해 설정된 장치 프로파일에 액세스하기 위하여 전역적으로 액세스가능한 저장소에 대해 인증을 받아야 할지도 모른다. 예를 들어, 컴퓨터(820)는 ID_{user}로 식별되는

사용자가 컴퓨터(820)에 로그인할 때 컴퓨터(820)가 자동으로 얻을 수 있는 특정 사용자 자격증명을 전역적으로 액세스가능한 저장소에 제시할 필요가 있을 수 있다. 다른 대안으로서, ID_{user}로 식별되는 사용자는 로그인한 후의 어떤 시점에서 요구된 자격증명을 제공할 수 있다.

[0072] ID_{dev} 및 ID_{user}와 연관된 프로파일을 전역적으로 액세스가능한 저장소에서 찾을 수 없는 경우[ID_{user}로 식별되는 사용자가 현재 휴대용 장치(810)와의 자동 연결을 수락하지 않는다는 것을 나타냄), 컴퓨터(820)는, 예를 들어, 프로토콜을 종료함으로써, 연결을 거절할 수 있다. 다른 대안으로서, 컴퓨터(820)는 수동 연결 절차를 시작할 수 있다(도시되지 않음).

[0073] 장치 프로파일 <ID_{dev}, PK_{dev}, $R_{user,dev}$>을 전역적으로 액세스가능한 저장소에서 찾을 수 있는 경우, 컴퓨터(820)는 프로파일을 검색하고 그로부터 PK_{dev}를 추출한다. 이어서, 제1 메시지로부터 제1 서명을 추출하고, PK_{dev}를 사용하여 제1 서명을 확인한다. 제1 서명을 발생하는 데 사용되는 서명 알고리즘은, 서명이 공개 키에 대응하는 비밀 키를 사용하여 발생된 경우에만, 공개 키를 사용하여 서명이 유효한지를 확인하도록 되어 있다. 예시된 실시예에서, SK_{dev}를 소유한 엔터티만이 PK_{dev}로 유효한지가 확인되는 서명을 발생할 수 있다. 이러한 방식으로, 휴대용 장치(810)는 휴대용 장치(820)가 실제로 자처하는 장치(즉, 식별자 ID_{dev}로 식별되는 장치)임을 컴퓨터(820)에게 증명한다.

[0074] 이상에서 논의된 바와 같이 재생 공격을 막기 위하여, 컴퓨터(820)는 또한 메시지로 수신된 랜덤한 값이 전역적으로 액세스가능한 저장소로부터 검색된 $R_{user,dev}$ 값과 동일한지를 확인한다.

[0075] 따라서, 제1 서명이 유효하고 $R_{user,dev}$ 값이 올바른 경우, 컴퓨터(820)는 휴대용 장치(810)를 신뢰하고 계속하여 이하에서 논의되는 이유로 $K_{dev}+K_{user}$로서 공유 키를 계산한다. 그렇지 않은 경우, 컴퓨터(820)는, 예를 들어, 프로토콜을 종료함으로써, 연결을 거절할 수 있다. 게다가, 제1 서명이 유효한 경우, 컴퓨터(820)는 SK_{user}를 이용하여 ID_{user}에 전자적으로 서명하여 제2 서명을 발생하며, 제2 서명[도 11에서 $sign_{SKuser}(ID_{user})$로 표시됨], $R_{user,dev}$, ID_{user}, 및 K_{user}를 포함하는 제2 메시지를 구성할 수 있다. 이어서, 동작(870)에서, 제2 메시지는 PK_{dev}를 사용하여 암호화되고 휴대용 장치(810)에게 송신된다. 다시 말하지만, SK_{dev}를 소유한 엔터티만이 제2 메시지의 내용에 액세스할 수 있도록 암호화가 수행된다. 그렇지 않은 경우, 전송 범위 내의 어떤 컴퓨터라도 제2 서명을 비롯한 제2 메시지의 내용을 포착할 수 있다. 제3자가 나중에 제2 서명을 사용하여 ID_{user}로 식별되는 사용자로 "가장"할 수 있기 때문에, 제3자가 제2 서명을 포착하는 것을 방지하는 것이 바람직할 수 있다.

[0076] 동작(880)에서, 휴대용 장치(810)는 SK_{dev}를 사용하여 암호화된 제2 메시지를 복호화한다. 이어서, 휴대용 장치(810)는 제2 메시지로부터 제2 서명을 추출하고, PK_{user}를 이용하여 제2 서명을 확인한다. 휴대용 장치(810)는 또한 메시지로 수신된 랜덤한 값이 자신의 메모리로부터 검색된 $R_{user,dev}$ 값과 동일한지를 확인한다. 제2 서명이 유효하고 $R_{user,dev}$ 값이 올바른 경우, 휴대용 장치(810)는 ID_{user}로 식별되는 사용자에 의해 인증될 컴퓨터(820)를 신뢰하는데, 그 이유는 SK_{user}를 소유한 엔터티만이 PK_{user}를 사용하여 확인될 때 유효한 서명을 발생했을 수 있고 올바른 $R_{user,dev}$ 값을 획득했을 수 있기 때문이다. 그렇지 않은 경우, 휴대용 장치는, 예를 들어, 프로토콜을 종료함으로써, 연결을 거절할 수 있다.

[0077] 이상의 내용으로부터 잘 알 것인 바와 같이, 도 11의 프로토콜은 그로써 휴대용 장치(810)와 컴퓨터(820)가, 수동으로 연결된 적이 없었더라도, 서로를 상호 인증하여 신뢰할 수 있는 관계를 구축할 수 있게 해준다. 그 후에, 2개의 장치는 임의의 원하는 방식으로 신뢰할 수 있는 통신에 참여할 수 있는데, 그 이유는 본 명세서에 기술된 본 발명의 측면들이 이 점에서 제한되지 않기 때문이다. 도 11에 예시된 일 실시예에 따르면, 새로운 키(K_{dev}와 K_{user})가 이상에서 논의된 바와 같이 생성되었다. 일 실시예에 따르면, 제2 서명 및 $R_{user,dev}$ 값이 유효할 때, 휴대용 장치(810)는 $K_{dev}+K_{user}$로서 공유 키를 계산한다. 이 시점에서, 컴퓨터(820)와 휴대용 장치(810) 둘 다는 공유 키인 $K_{dev}+K_{user}$를 올바르게 계산하였으며, 이 공유 키는 또한 휴대용 장치(810)와 컴퓨터(820) 간의 통신 채널을 보호하기 위한 암호화 키를 도출하는 데 사용될 수 있다. 그러나, 본 명세서에 기술된 본 발명의 측면들이 이 점에서 제한되지 않고, 컴퓨터(820)와 휴대용 장치(810) 간의 통신이 임의의 적합한 방식으로 보호되거나 보호되지 않을 수 있기 때문에, 본 명세서에 기술된 본 발명의 측면들이 이러한 방식으로 공유 키를 발

생하는 것으로 제한되지 않는다는 것을 잘 알 것이다.

[0078] 도 11에 예시된 프로토콜이 사용자의 개입없이 휴대용 장치(810) 및 컴퓨터(820)에 의해 자동으로 수행될 수 있다는 것을 잘 알 것이다. 예를 들어, 컴퓨터(820)는, 휴대용 장치(810)를 검색하고 휴대용 장치(810)와의 통신 채널을 설정할 시에, 자동으로 동작(830)을 수행할 수 있다. 컴퓨터(820)가 전역적으로 액세스가능한 저장소로부터 장치 프로파일을 검색하는 데 사용되는 자격증명에 액세스할 수만 있다면, 동작(860)도 역시 자동으로 수행될 수 있다.

[0079] 게다가, 동작들(830 내지 880)은, 다수의 동작들로 분해하는 것 및 임의의 적합한 순서로 다수의 동작들을 인터리빙하는 것을 비롯하여, 임의의 적합한 순서로 수행될 수 있다.

[0080] 이상에서 논의된 바와 같이, 본 명세서에 기술된 본 발명의 측면들은 이상에서 기술된 임의의 동작들을 수행하도록 프로그램될 수 있는 프로세서를 가진 임의의 컴퓨터 또는 장치들에서 사용될 수 있다. 도 12는 본 발명의 측면들이 구현될 수 있는 예시적인 컴퓨터(1300)를 개략적으로 나타낸 것이다. 컴퓨터(1300)는 프로세서 또는 처리 장치(1301)와 휘발성 및 비휘발성 메모리 둘다를 포함할 수 있는 메모리(1302)를 포함한다. 컴퓨터(1300)는 또한, 시스템 메모리(1302)에 부가하여, 저장 장치[예를 들어, 이동식 저장 장치(1304) 및 비이동식 저장 장치(1305)]를 포함한다. 메모리(1302)는 본 명세서에 기술된 임의의 기능을 수행하도록 처리 장치(1301)를 프로그램하는 하나 이상의 명령어를 저장할 수 있다. 상기한 바와 같이, 본 명세서에서 컴퓨터라고 하는 것은, 랙 탑재 컴퓨터, 데스크톱 컴퓨터, 랩톱 컴퓨터, 태블릿 컴퓨터, 또는 프로그램된 프로세서를 포함하는, 일반적으로 컴퓨터라고 간주되지 않을 수 있는 임의의 수많은 장치들(예를 들어, PDA, MP3 플레이어, 휴대폰, 무선 헤드폰 등)을 비롯하여, 프로그램된 프로세서를 가지는 임의의 장치를 포함할 수 있다.

[0081] 또한, 컴퓨터는 도 13에 도시된 장치(1306, 1307) 등의 하나 이상의 입력 및 출력 장치를 가질 수 있다. 이들 장치는, 그 중에서도 특히, 사용자 인터페이스를 제공하는 데 사용될 수 있다. 사용자 인터페이스를 제공하는 데 사용될 수 있는 출력 장치들의 일례로는 출력의 시각적 표현을 위한 프린터 또는 디스플레이 화면 및 출력의 청각적 표현을 위한 스피커 또는 기타 사운드 발생 장치가 있다. 사용자 인터페이스용으로 사용될 수 있는 입력 장치들의 일례로는 키보드 및 포인팅 장치[마우스, 터치 패드, 및 디지타이징 태블릿(digitizing tablet) 등]가 있다. 다른 일례로서, 컴퓨터는 음성 인식을 통해 또는 기타 가청 포맷으로 입력 정보를 수신할 수 있다.

[0082] 본 발명의 상기한 실시예들은 수많은 방법들 중 어떤 방법으로도 구현될 수 있다. 예를 들어, 이들 실시예는 하드웨어, 소프트웨어 또는 이들의 조합을 사용하여 구현될 수 있다. 소프트웨어로 구현될 때, 소프트웨어 코드는, 단일 컴퓨터에 제공되어 있든 다수의 컴퓨터들 간에 분산되어 있든 간에, 임의의 적당한 프로세서 또는 일군의 프로세서들에서 실행될 수 있다.

[0083] 또한, 본 명세서에 개략적으로 설명된 다양한 방법들 또는 프로세스들이 각종의 운영 체제 또는 플랫폼 중 임의의 것을 이용하는 하나 이상의 프로세서에서 실행가능한 소프트웨어로서 코딩될 수 있다는 것을 잘 알 것이다. 그에 부가하여, 이러한 소프트웨어는 다수의 적당한 프로그래밍 언어 및/또는 프로그래밍 또는 스크립팅 도구 중 임의의 것을 사용하여 작성될 수 있고, 또한 프레임워크 또는 가상 컴퓨터에서 실행되는 실행가능 기계어 코드 또는 중간 코드(intermediate code)로서 컴파일될 수 있다.

[0084] 이 점에서, 본 명세서에 기술된 본 발명의 어떤 측면들은, 하나 이상의 프로세서 상에서 실행될 때, 상기한 본 발명의 다양한 실시예를 구현하는 방법을 수행하는 하나 이상의 프로그램으로 인코딩된 컴퓨터 판독가능 매체(또는 다수의 컴퓨터 판독가능 매체)[예를 들어, 컴퓨터 메모리, 하나 이상의 플로피 디스크, 컴팩트 디스크, 광 디스크, 자기 테이프, 플래시 메모리, FPGA(Field Programmable Gate Array) 또는 기타 반도체 장치 내의 회로 구성, 기타 유형의(tangible) 컴퓨터 저장 매체]로서 구현될 수 있다. 컴퓨터-판독가능 매체 또는 매체들은 그에 저장된 프로그램 또는 프로그램들이 상기한 바와 같은 본 발명의 다양한 측면을 구현하기 위해 하나 이상의 서로 다른 컴퓨터 또는 기타 프로세서에 로드될 수 있도록 전송가능한 것(transportable)일 수 있다.

[0085] "프로그램" 또는 "소프트웨어"라는 용어는, 본 명세서에서 일반적인 의미로, 상기한 바와 같은 본 발명의 다양한 측면을 구현하도록 컴퓨터 또는 프로세서를 프로그램하는 데 이용될 수 있는 임의의 종류의 컴퓨터 코드 또는 일련의 컴퓨터-실행가능 명령어를 지칭하는 데 사용되며, 임의의 컴퓨터 프로그램 마이크로코드, 기타를 포함할 수 있다. 그에 부가하여, 실행될 때 본 발명의 방법을 수행하는 하나 이상의 컴퓨터 프로그램이 단일의 컴퓨터 또는 프로세서 상에 존재할 필요가 없고 본 발명의 다양한 측면을 구현하기 위해 다수의 서로 다른 컴퓨터 또는 프로세서 간에 분산되어 있을 수 있다는 것을 잘 알 것이다.

[0086] 컴퓨터-실행가능 명령어는 하나 이상의 컴퓨터 또는 기타 장치에 의해 실행되는 프로그램 모듈과 같은 다수의 형태로 되어 있을 수 있다. 프로그램 모듈은 특정의 작업을 수행하거나 특정의 추상 데이터 유형을 구현하는 루틴, 프로그램, 개체, 구성요소, 데이터 구조, 기타 등등을 포함할 수 있다. 프로그램 모듈의 기능이 다양한 실시예에서 원하는 바에 따라 결합되거나 분산되어 있을 수 있다.

[0087] 또한, 데이터 구조가 컴퓨터-판독가능 매체에 임의의 적당한 형태로 저장될 수 있다. 설명의 간단함을 위해, 데이터 구조가 데이터 구조 내에서의 위치를 통해 관련되어 있는 필드를 갖는 것으로 도시되어 있을 수 있다. 이러한 관계는 마찬가지로 필드들 간의 관계를 전달하는 컴퓨터-판독가능 매체에서의 위치를 가지는 필드에 대한 저장소를 할당함으로써 달성될 수 있다. 그렇지만, 데이터 요소들 간의 관계를 설정하는 포인터, 태그 또는 기타 메카니즘을 사용하는 것을 비롯하여, 데이터 구조의 필드들 내의 정보 사이의 관계를 설정하는 데 임의의 적당한 메카니즘이 사용될 수 있다.

[0088] 본 발명의 다양한 측면이, 이상에서 구체적으로 설명하지 않은 것을 비롯하여, 단독으로, 결합하여 또는 임의의 적당한 배열 또는 조합으로 사용될 수 있다. 예를 들어, 일 실시예에 기술된 측면이 다른 실시예에 기술된 측면과 임의의 방식으로 결합될 수 있다.

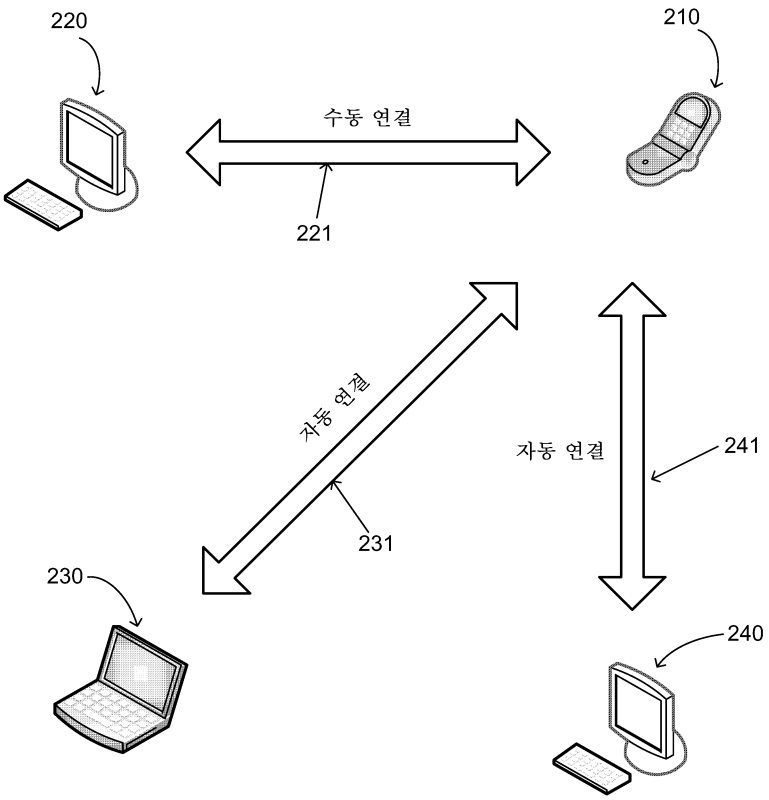
[0089] 청구 범위에서 청구항 구성요소를 수식하기 위해 "제1", "제2", "제3", 기타 등등의 서수 용어를 사용하는 것은 그 자체로 한 청구항 구성요소의 다른 구성요소에 대한 우선권, 우선순위 또는 순서, 또는 방법의 동작이 수행되는 시간적 순서를 의미하지 않으며, 단지 어떤 이름을 갖는 한 청구항 구성요소를 동일한 이름을 갖는(그렇지만, 서수 용어를 사용함) 다른 구성요소와 구분하여 청구항 구성요소들을 구별하기 위한 표시로서 사용된다.

[0090] 또한, 본 명세서에서 사용되는 어구 및 전문 용어가 설명을 위한 것이며, 제한하는 것으로 보아서는 안된다. 본 명세서에서 "포함하는", "구비하는", 또는 "갖는", "내포하는", "수반하는" 및 이들의 변형을 사용하는 것은 그 이후에 열거되는 항목 및 그의 등가물은 물론 부가의 항목을 포괄하기 위한 것이다.

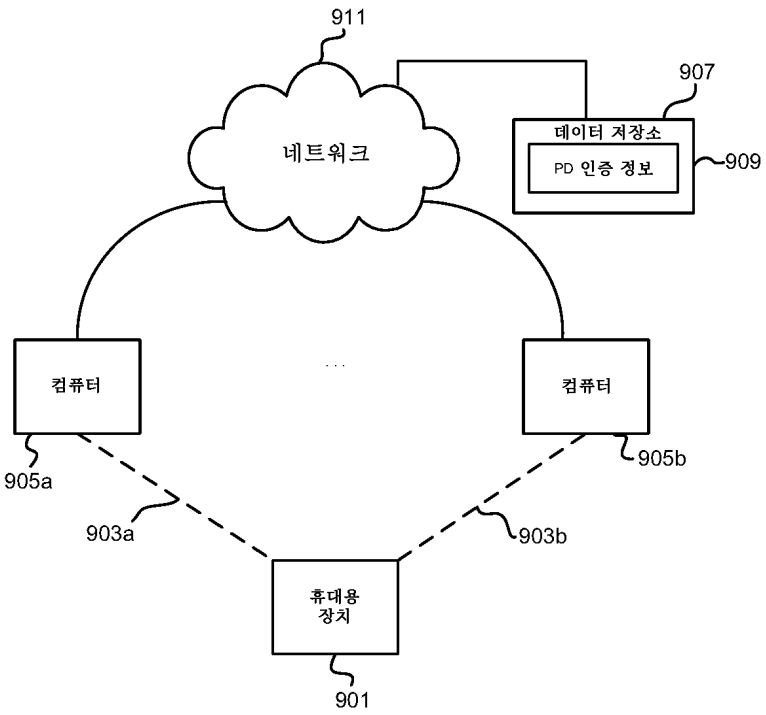
[0091] 이와 같이 본 발명의 적어도 하나의 실시예의 몇가지 측면에 대해 기술하였지만, 다양한 변경, 수정 및 개량이 당업자에 의해 용이하게 안출될 것이라는 것을 잘 알 것이다. 이러한 변경, 수정 및 개량은 본 발명의 사상 및 범위 내에 속하는 것으로 보아야 한다. 그에 따라, 이상의 설명 및 도면은 단지 일례에 불과하다.

도면

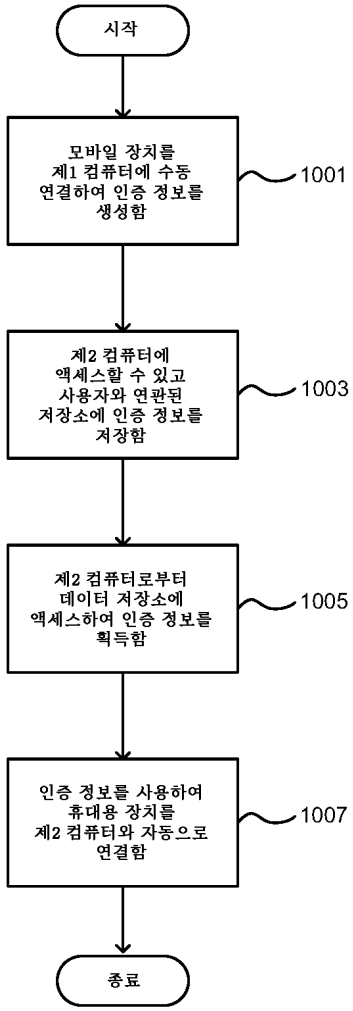
도면1


220
210
수동 연결
221
자동 연결
231
자동 연결
241
230
240

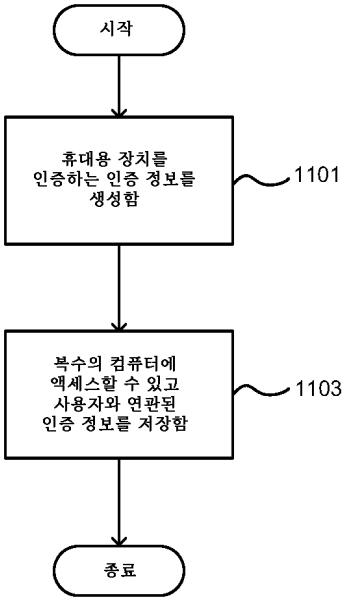
도면2


911
네트워크
907
데이터 저장소
PD 인증 정보
909
컴퓨터
컴퓨터
905a
905b
903a
903b
휴대용 장치
901

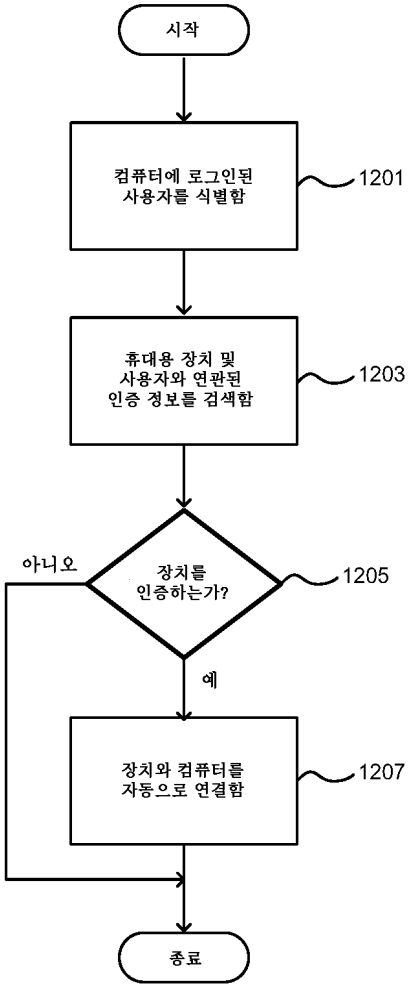
도면3


시작
모바일 장치를 제1 컴퓨터에 수동 연결하여 인증 정보를 생성함
1001
제2 컴퓨터에 액세스할 수 있고 사용자와 연관된 저장소에 인증 정보를 저장함
1003
제2 컴퓨터로부터 데이터 저장소에 액세스하여 인증 정보를 획득함
1005
인증 정보를 사용하여 휴대용 장치를 제2 컴퓨터와 자동으로 연결함
1007
종료

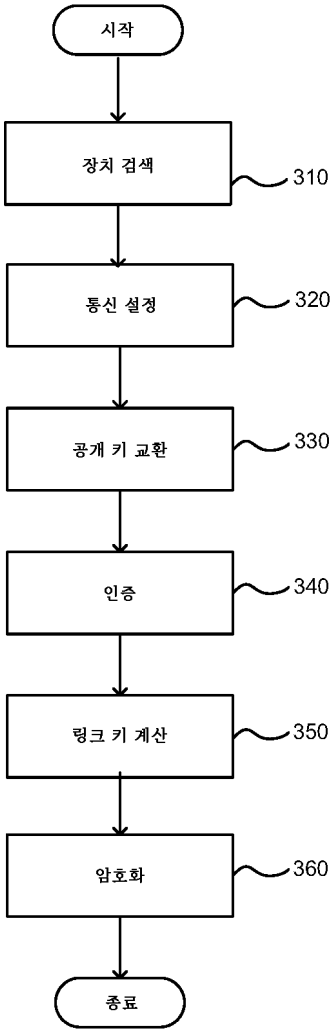
도면4


시작
휴대용 장치를 인증하는 인증 정보를 생성함
1101
복수의 컴퓨터에 액세스할 수 있고 사용자와 연관된 인증 정보를 저장함
1103
종료

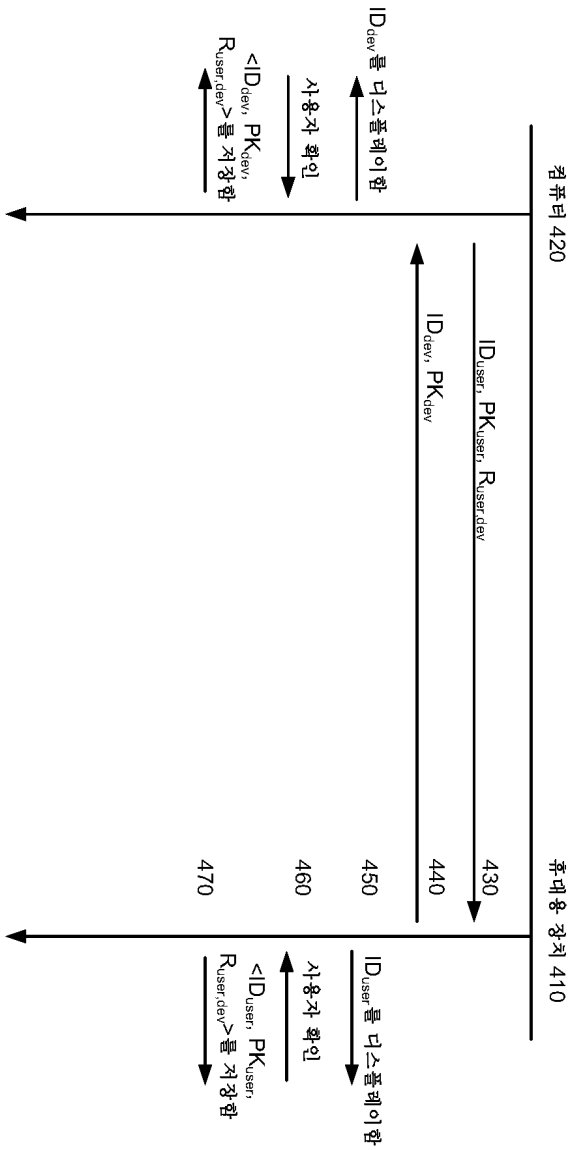
도면5


시작
컴퓨터에 로그인된 사용자를 식별함
1201
휴대용 장치 및 사용자와 연관된 인증 정보를 검색함
1203
장치를 인증하는가?
1205
아니오
예
장치와 컴퓨터를 자동으로 연결함
1207
종료

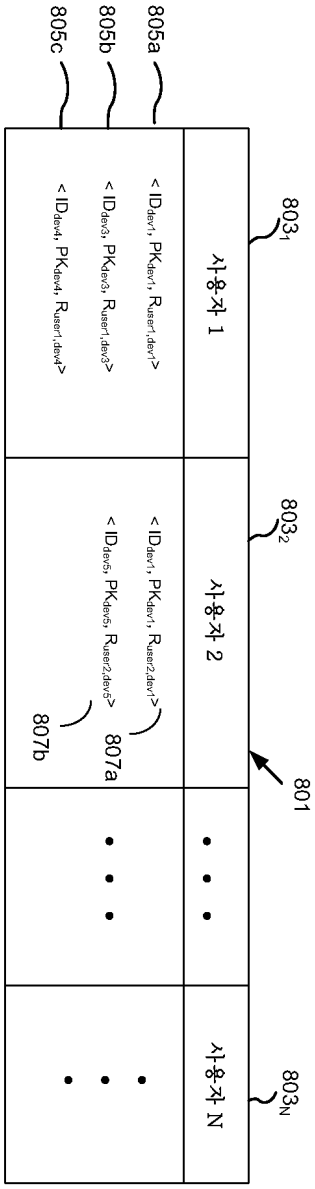
도면6



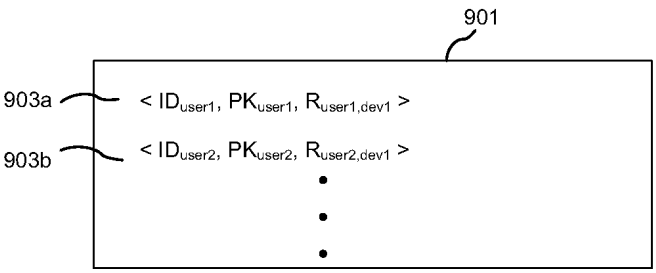
도면7


컴퓨터 420
휴대용 장치 410
ID_{user}, PK_{user}, $R_{user,dev}$
430
ID_{dev}, PK_{dev}
440
ID_{user}를 디스플레이함
450
사용자 확인
460
<ID_{user}, PK_{user}, $R_{user,dev}$>를 저장함
470
ID_{dev}를 디스플레이함
사용자 확인
<ID_{dev}, PK_{dev}, $R_{user,dev}$>를 저장함

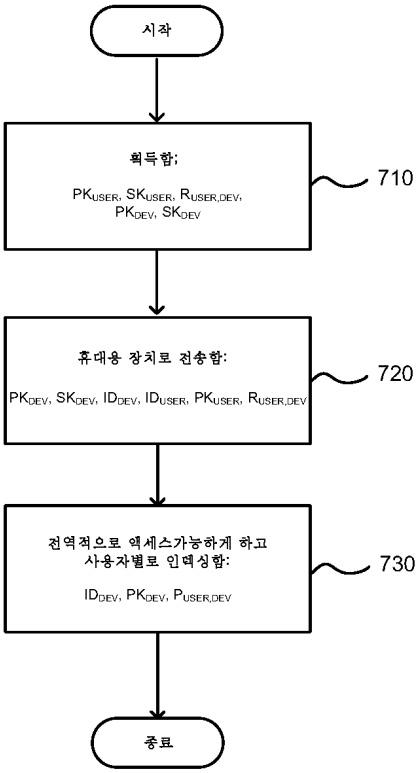
도면8


805a
805b
805c
803₁
803₂
803N
사용자 1
사용자 2
사용자 N
801
807a
807b

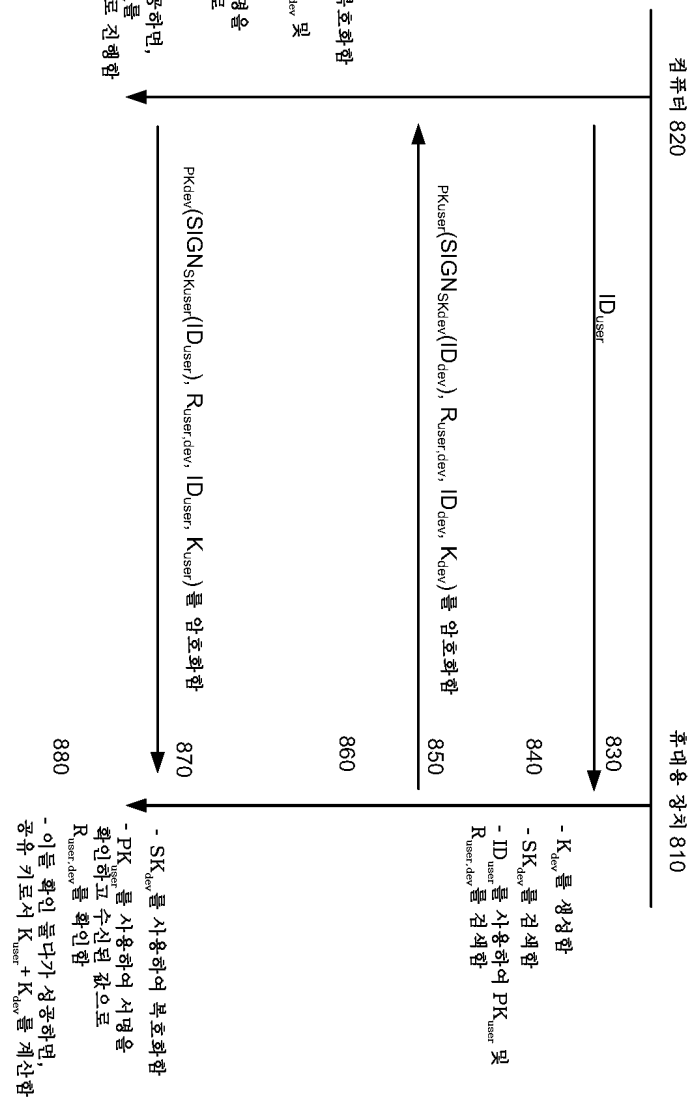
도면9


901
903a
903b

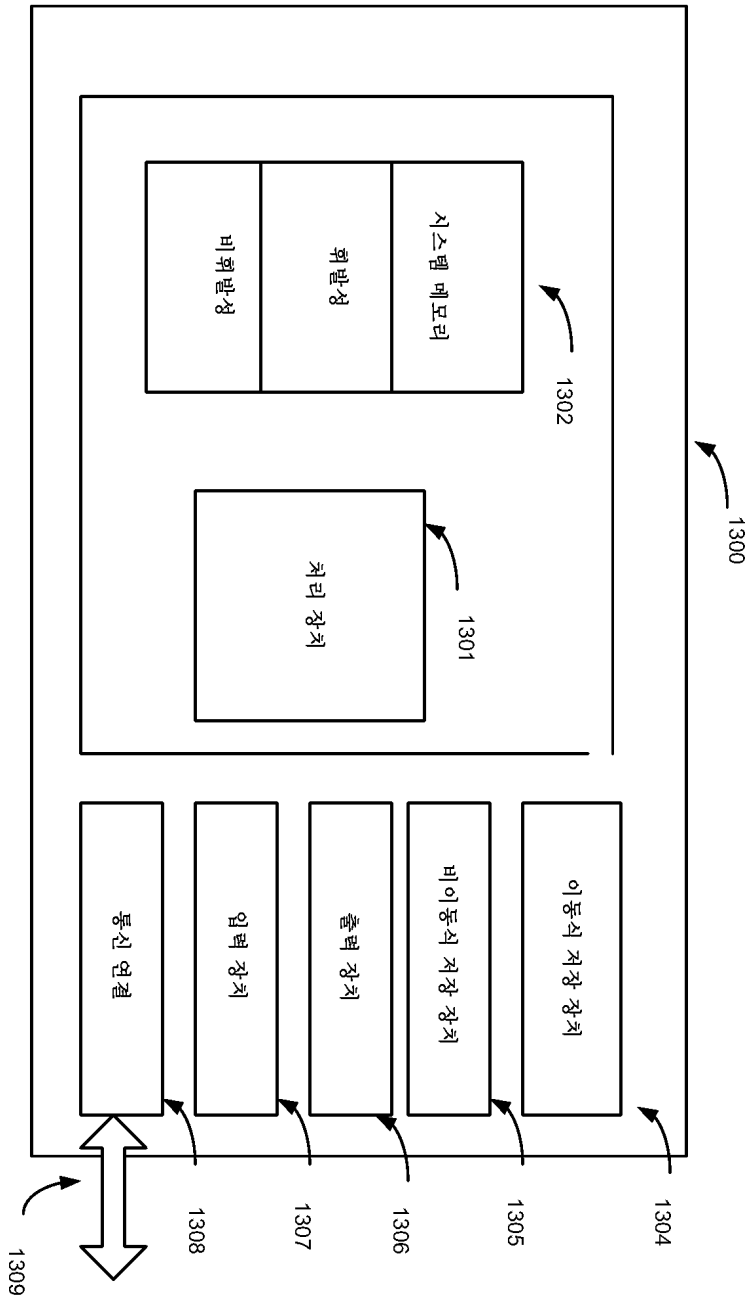
도면10


시작
획득함:
PK_{USER}, SK_{USER}, $R_{USER,DEV}$, PK_{DEV}, SK_{DEV}
710
휴대용 장치로 전송함:
PK_{DEV}, SK_{DEV}, ID_{DEV}, ID_{USER}, PK_{USER}, $R_{USER,DEV}$
720
전역적으로 액세스가능하게 하고 사용자별로 인덱싱함:
ID_{DEV}, PK_{DEV}, $P_{USER,DEV}$
730
종료

도면11


컴퓨터 820
휴대용 장치 810
IDuser
830
- Kdev 를 생성함
- SKdev 를 검색함
- IDuser 를 사용하여 PKuser 및 Ruser.dev 를 검색함
840
PKuser(SIGNSKdev(IDdev, Ruser.dev, IDdev, Kdev)를 암호화함
850
- Kuser 를 생성함
- SKuser 를 검색함
- SKuser 를 사용하여 복호화함
- IDdev 를 사용하여 PKdev 및 Ruser.dev 를 검색함
860
PKdev(SIGNSKuser(IDuser), Ruser.dev, IDuser, Kuser)를 암호화함
870
- SKdev 를 사용하여 복호화함
- PKuser 를 사용하여 서명을 확인하고 수신된 값으로 Ruser.dev 를 확인함
880
- PKdev 를 사용하여 서명을 확인하고 수신된 값으로 Ruser.dev 를 확인함
- 이들 확인 둘다가 성공하면, 공유 키로서 Kuser + Kdev 를 계산함
- 이들 확인 둘다가 성공하면, 공유 키로서 Kuser + Kdev 를 계산하고 동작(870)으로 진행함

도면12



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제7항

【변경전】

상기 제2 인증 정보

【변경후】

상기 보안화된 제2 인증 정보