(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년06월13일
(11) 등록번호 10-1746797
(24) 등록일자 2017년06월07일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *H04L 29/06* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04W 12/06 (2013.01)
H04L 63/0861 (2013.01)
(21) 출원번호 10-2015-7028754
(22) 출원일자(국제) 2014년03월14일
심사청구일자 2017년02월10일
(85) 번역문제출일자 2015년10월12일
(65) 공개번호 10-2015-0131209
(43) 공개일자 2015년11월24일
(86) 국제출원번호 PCT/US2014/029027
(87) 국제공개번호 WO 2014/144563
국제공개일자 2014년09월18일
(30) 우선권주장
61/800,518 2013년03월15일 미국(US)
14/040,213 2013년09월27일 미국(US)
(56) 선행기술조사문헌
US20050130634 A1
US20080041937 A1
US20100283682 A1
US20110109431 A1

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
수, 데이비드 쿠오치
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
창, 닝
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

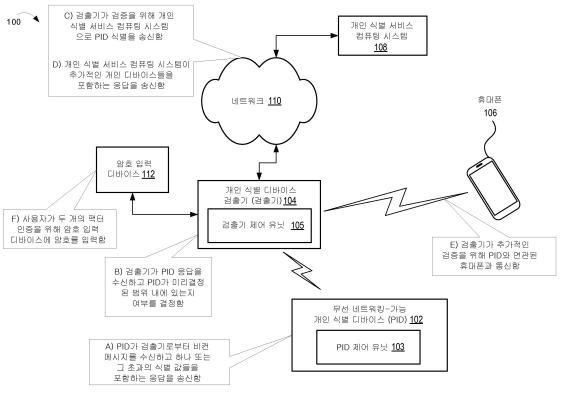
전체 청구항 수 : 총 42 항 심사관 : 이준석

(54) 발명의 명칭 **무선 네트워킹-가능 개인 식별 시스템**

(57) 요 약

비컨 메시지는 제1 디바이스로부터 무선으로 송신된다. 상기 제1 디바이스는 상기 비컨 메시지에 대한 제1 응답을 수신하고, 상기 제1 응답은 개인 식별 디바이스와 연관된 식별 값들을 포함한다. 상기 제1 디바이스는 상기 개인 식별 디바이스와 연관된 제2 디바이스와 통신한다. 상기 개인 식별 디바이스는 상기 제2 디바이스와의 통신 및 상기 식별 값들에 적어도 부분적으로 기초하여 인증된다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/12 (2013.01)
H04L 9/3213 (2013.01)
H04L 2209/80 (2013.01)

명 세 서

청구범위

청구항 1

방법으로서,

제1 디바이스로부터, 비컨 메시지(beacon message)를 송신하는 단계 – 상기 비컨 메시지는 무선으로 송신됨 –;

상기 제1 디바이스에서, 개인 식별 디바이스로부터, 상기 비컨 메시지에 대한 제1 응답을 수신하는 단계 – 상기 제1 응답은 상기 개인 식별 디바이스와 연관된 하나 이상의 식별 값들을 포함함 –;

식별 서비스와 통신하는 단계 – 상기 통신하는 단계는,

상기 제1 디바이스로부터, 상기 개인 식별 디바이스와 연관된 상기 하나 이상의 식별 값들을 상기 식별 서비스와 연관된 컴퓨팅 시스템에 송신하는 단계, 및

상기 제1 디바이스에서, 상기 컴퓨팅 시스템으로부터 제2 응답을 수신하는 단계를 포함하고, 상기 제2 응답은, 상기 개인 식별 디바이스가 인증되었다는 표시 및 상기 개인 식별 디바이스와 연관된 데이터로 구성된 그룹으로부터 선택된 적어도 하나의 멤버(member)를 포함함 –;

상기 제1 디바이스에 의해, 상기 컴퓨팅 시스템으로부터 수신된 상기 제2 응답에 적어도 부분적으로 기초하여 상기 개인 식별 디바이스와 연관된 제2 디바이스를 결정하는 단계;

상기 식별 서비스와 통신한 이후 상기 제2 디바이스와 통신하는 단계; 및

상기 개인 식별 디바이스를 인증하는 단계를 포함하고,

상기 인증하는 단계는 상기 컴퓨팅 시스템으로부터 수신된 상기 제2 응답 및 상기 제2 디바이스와 통신하는 단계에 적어도 부분적으로 기초하는,

방법.

청구항 2

제 1 항에 있어서,

상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리를 결정하는 단계를 더 포함하고,

상기 인증하는 단계는 추가로, 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 결정된 거리에 적어도 부분적으로 기초하는,

방법.

청구항 3

제 2 항에 있어서,

상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리는 상기 제1 디바이스와 상기 개인 식별 디바이스 사이에서 데이터를 이동(travel)시키기 위한 전파 시간(a time of flight)에 적어도 부분적으로 기초하여 결정되는,

방법.

청구항 4

제 2 항에 있어서,

상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리가 미리결정된 거리 내에 있음을 결정하는 단계를 더 포함하고,

상기 개인 식별 디바이스를 인증하는 단계는 추가로, 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리가 미리결정된 거리 내에 있음을 결정하는 단계에 적어도 부분적으로 기초하는,

방법.

청구항 5

제 1 항에 있어서,

상기 개인 식별 디바이스와 연관된 데이터는 상기 제2 디바이스의 표시를 포함하는,

방법.

청구항 6

제 1 항에 있어서,

상기 컴퓨팅 시스템에서, 상기 개인 식별 디바이스와 연관된 상기 하나 이상의 식별 값들을 수신하는 단계;

상기 컴퓨팅 시스템에서, 상기 개인 식별 디바이스와 연관된 상기 하나 이상의 식별 값들을 검증하는 단계; 및

상기 컴퓨팅 시스템으로부터, 상기 제2 응답을 송신하는 단계를 더 포함하는,

방법.

청구항 7

제 1 항에 있어서,

상기 제1 디바이스에서, 제1 인증 토큰(token)을 생성하는 단계 - 상기 제1 인증 토큰은 상기 개인 식별 디바이스와 연관된 상기 하나 이상의 식별 값들과 함께 상기 컴퓨팅 시스템으로 송신됨 -; 및

상기 컴퓨팅 시스템으로부터, 제2 인증 토큰을 수신하는 단계를 더 포함하고,

상기 개인 식별 디바이스를 인증하는 단계는 상기 제1 인증 토큰이 상기 제2 인증 토큰과 매칭(match)됨을 결정하는 단계를 더 포함하는,

방법.

청구항 8

제 1 항에 있어서,

상기 하나 이상의 식별 값들은 암호화된(encrypted) 식별 값 및 비암호화된(unencrypted) 식별 값으로 구성된 그룹으로부터 선택된 적어도 하나의 멤버를 포함하는,

방법.

청구항 9

제 8 항에 있어서,

상기 암호화된 식별 값은 상기 개인 식별 디바이스와 연관된 공개 키로 암호화된 랜덤 값을 포함하는,

방법.

청구항 10

제 1 항에 있어서,

상기 제1 디바이스에서, 상기 개인 식별 디바이스와 연관된 인증 데이터를 수신하는 단계를 더 포함하고,

상기 개인 식별 디바이스를 인증하는 단계는 추가로, 상기 인증 데이터에 적어도 부분적으로 기초하는,

방법.

청구항 11

제 10 항에 있어서,

상기 인증 데이터는 암호(password) 및 생체인식(biometric) 데이터로 구성된 그룹으로부터 선택된 적어도 하나의 멤버를 포함하는,

방법.

청구항 12

제 1 항에 있어서,

상기 제1 디바이스와 상기 제2 디바이스 사이의 거리를 결정하는 단계를 더 포함하고,

상기 개인 식별 디바이스를 인증하는 단계는 추가로, 상기 제1 디바이스와 상기 제2 디바이스 사이의 거리에 적어도 부분적으로 기초하는,

방법.

청구항 13

제 1 항에 있어서,

상기 개인 식별 디바이스와 상기 제2 디바이스 사이의 거리를 결정하는 단계를 더 포함하고,

상기 개인 식별 디바이스를 인증하는 단계는 추가로, 상기 개인 식별 디바이스와 상기 제2 디바이스 사이의 거리에 적어도 부분적으로 기초하는,

방법.

청구항 14

제 1 항에 있어서,

상기 제2 디바이스는 휴대폰(cellphone)인,

방법.

청구항 15

제 1 항에 있어서,

상기 개인 식별 디바이스에서, 상기 제1 디바이스로부터 상기 비컨 메시지를 수신하는 단계;

상기 개인 식별 디바이스에서, 상기 제1 디바이스로부터 상기 비컨 메시지를 수신하는 단계에 응답하여, 상기 개인 식별 디바이스에서, 상기 비컨 메시지에 대한 상기 제1 응답을 생성하는 단계; 및

상기 개인 식별 디바이스로부터, 상기 제1 응답을 송신하는 단계를 더 포함하는,

방법.

청구항 16

제 15 항에 있어서,

상기 개인 식별 디바이스에서, 상기 비컨 메시지에 대한 상기 제1 응답을 생성하는 단계는 적어도 하나의 식별 값을 암호화하는 단계를 포함하고,

상기 개인 식별 디바이스와 연관된 상기 하나 이상의 식별 값들은 상기 적어도 하나의 암호화된 식별 값을 포함하는,

방법.

청구항 17

제 1 항에 있어서,

상기 개인 식별 디바이스와 연관된 제3 디바이스와 통신하는 단계를 더 포함하고,

상기 인증하는 단계는 추가로, 상기 제3 디바이스와 통신하는 단계에 적어도 부분적으로 기초하는,

방법.

청구항 18

디바이스로서,

메모리; 및

상기 메모리와 커플링되는 프로세서를 포함하고,

상기 프로세서는:

비컨 메시지를 송신하고 - 상기 비컨 메시지는 무선으로 송신됨 -;

개인 식별 디바이스로부터 상기 비컨 메시지에 대한 제1 응답을 수신하고 - 상기 제1 응답은 상기 개인 식별 디바이스와 연관된 하나 이상의 식별 값들을 포함함 -;

식별 서비스와 통신하고 - 상기 프로세서는,

상기 개인 식별 디바이스와 연관된 상기 하나 이상의 식별 값들을 상기 식별 서비스와 연관된 컴퓨팅 시스템에 송신하고, 그리고

상기 컴퓨팅 시스템으로부터, 상기 개인 식별 디바이스가 인증되었다는 표시 및 상기 개인 식별 디바이스와 연관된 데이터로 구성된 그룹으로부터 선택된 적어도 하나의 멤버를 포함하는 제2 응답을 수신하도록 구성됨으로써 상기 식별 서비스와 통신하도록 구성됨 -;

상기 컴퓨팅 시스템으로부터 수신된 상기 제2 응답에 적어도 부분적으로 기초하여 상기 개인 식별 디바이스와 연관된 제2 개인 식별 디바이스를 결정하고;

상기 식별 서비스와 통신한 이후 상기 제2 개인 식별 디바이스와 통신하고; 그리고

상기 개인 식별 디바이스를 인증하도록 구성되고,

상기 인증은 상기 컴퓨팅 시스템으로부터 수신된 상기 제2 응답 및 상기 제2 개인 식별 디바이스와 통신하는 것에 적어도 부분적으로 기초하는,

디바이스.

청구항 19

제 18 항에 있어서,

상기 프로세서는, 상기 개인 식별 디바이스 및 상기 제2 개인 식별 디바이스로 구성된 그룹으로부터 선택된 적어도 하나의 멤버와 상기 디바이스 사이의 거리를 결정하도록 추가로 구성되고,

상기 개인 식별 디바이스를 인증하는 것은 추가로, 상기 개인 식별 디바이스 및 상기 제2 개인 식별 디바이스로 구성된 그룹으로부터 선택된 적어도 하나의 멤버와 상기 디바이스 사이의 거리 결정에 적어도 부분적으로 기초하는,

디바이스.

청구항 20

제 19 항에 있어서,

상기 개인 식별 디바이스 및 상기 제2 개인 식별 디바이스 중 적어도 하나와 상기 디바이스 사이의 거리는, 상기 개인 식별 디바이스 및 상기 제2 개인 식별 디바이스 중 적어도 하나와 상기 디바이스 사이에서 데이터를 이동시키기 위한 전파 시간에 적어도 부분적으로 기초하여 결정되는,

디바이스.

청구항 21

제 19 항에 있어서,

상기 프로세서는, 상기 개인 식별 디바이스 및 상기 제2 개인 식별 디바이스 중 적어도 하나와 상기 디바이스 사이의 거리가 미리결정된 거리 내에 있음을 결정하도록 추가로 구성되고,

상기 개인 식별 디바이스의 인증은 추가로, 상기 개인 식별 디바이스 및 상기 제2 개인 식별 디바이스 중 적어도 하나와 상기 디바이스 사이의 거리가 상기 미리결정된 거리 내에 있다는 결정에 적어도 부분적으로 기초하는,

디바이스.

청구항 22

제 18 항에 있어서,

상기 프로세서는, 상기 개인 식별 디바이스와 상기 제2 개인 식별 디바이스 사이의 거리를 결정하도록 추가로 구성되고,

상기 개인 식별 디바이스를 인증하는 것은 추가로, 상기 개인 식별 디바이스와 상기 제2 개인 식별 디바이스 사이의 거리 결정에 적어도 부분적으로 기초하는,

디바이스.

청구항 23

제 19 항에 있어서,

상기 개인 식별 디바이스와 연관된 데이터는 상기 제2 개인 식별 디바이스의 표시를 포함하는,

디바이스.

청구항 24

제 18 항에 있어서,

상기 프로세서는, 상기 개인 식별 디바이스와 연관된 인증 데이터를 수신하도록 추가로 구성되고,

상기 개인 식별 디바이스의 인증은 추가로, 상기 인증 데이터에 적어도 부분적으로 기초하는,

디바이스.

청구항 25

제 24 항에 있어서,

상기 인증 데이터는 암호 및 생체인식 데이터로 구성된 그룹으로부터 선택된 적어도 하나의 멤버를 포함하는,

디바이스.

청구항 26

저장된 명령들을 갖는 비-일시적인 기계 판독가능한 저장 매체로서,

상기 명령들은 제1 디바이스의 하나 이상의 프로세서들에 의해 실행되는 경우, 상기 제1 디바이스로 하여금,

비컨 메시지를 송신하는 것 - 상기 비컨 메시지는 무선으로 송신됨 -;

개인 식별 디바이스로부터 상기 비컨 메시지에 대한 제1 응답을 수신하는 것 - 상기 제1 응답은 상기 개인 식별 디바이스와 연관된 하나 이상의 식별 값들을 포함함 -;

식별 서비스와 통신하는 것 - 상기 통신하는 것은,

상기 개인 식별 디바이스와 연관된 상기 하나 이상의 식별 값들을 상기 식별 서비스와 연관된 컴퓨팅 시스템에 송신하는 것, 및

상기 컴퓨팅 시스템으로부터, 상기 개인 식별 디바이스가 인증되었다는 표시 및 상기 개인 식별 디바이스와 연관된 데이터로 구성된 그룹으로부터 선택된 적어도 하나의 멤버를 포함하는 제2 응답을 수신하는 것을 포함함 -;

상기 컴퓨팅 시스템으로부터 수신된 상기 제2 응답에 적어도 부분적으로 기초하여 상기 개인 식별 디바이스와 연관된 제2 디바이스를 결정하는 것;

상기 식별 서비스와 통신한 이후 상기 제2 디바이스와 통신하는 것; 및

상기 개인 식별 디바이스를 인증하는 것 - 상기 인증하는 것은 상기 컴퓨팅 시스템으로부터 수신된 상기 제2 응답 및 상기 제2 디바이스와 통신하는 것에 적어도 부분적으로 기초함 -

을 포함하는 동작들을 수행하게 하는,

비-일시적인 기계 판독가능한 저장 매체.

청구항 27

제 26 항에 있어서,

상기 동작들은, 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리를 결정하는 것을 더 포함하고,

상기 인증하는 것은 추가로, 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 결정된 거리에 적어도 부분적으로 기초하는,

비-일시적인 기계 판독가능한 저장 매체.

청구항 28

제 27 항에 있어서,

상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리는 상기 제1 디바이스와 상기 개인 식별 디바이스 사이에서 데이터를 이동시키기 위한 전파 시간에 적어도 부분적으로 기초하여 결정되는,

비-일시적인 기계 판독가능한 저장 매체.

청구항 29

제 27 항에 있어서,

상기 동작들은, 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리가 미리결정된 거리 내에 있음을 결정하는 것을 더 포함하고,

상기 개인 식별 디바이스를 인증하는 것은 추가로, 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리가 상기 미리결정된 거리 내에 있음을 결정하는 것에 적어도 부분적으로 기초하는,

비-일시적인 기계 판독가능한 저장 매체.

청구항 30

제 26 항에 있어서,

상기 개인 식별 디바이스와 연관된 데이터는 상기 제2 디바이스의 표시를 포함하는,

비-일시적인 기계 판독가능한 저장 매체.

청구항 31

제 26 항에 있어서,

상기 동작들은,

제1 인증 토큰을 생성하는 것 – 상기 제1 인증 토큰은 상기 개인 식별 디바이스와 연관된 상기 하나 이상의 식별 값들과 함께 상기 컴퓨팅 시스템으로 송신됨 –; 및

제2 인증 토큰을 수신하는 것을 더 포함하고,

상기 개인 식별 디바이스를 인증하는 것은 상기 제1 인증 토큰이 상기 제2 인증 토큰과 매칭됨을 결정하는 것을 더 포함하는,

비-일시적인 기계 판독가능한 저장 매체.

청구항 32

제 26 항에 있어서,

상기 동작들은, 상기 개인 식별 디바이스와 연관된 인증 데이터를 수신하는 것을 더 포함하고,

상기 개인 식별 디바이스를 인증하는 것은 추가로, 상기 인증 데이터에 적어도 부분적으로 기초하는,

비-일시적인 기계 판독가능한 저장 매체.

청구항 33

제 32 항에 있어서,

상기 인증 데이터는 암호 및 생체인식 데이터로 구성된 그룹으로부터 선택된 적어도 하나의 멤버를 포함하는,

비-일시적인 기계 판독가능한 저장 매체.

청구항 34

제 26 항에 있어서,

상기 동작들은, 상기 제1 디바이스와 상기 제2 디바이스 사이의 거리를 결정하는 것을 더 포함하고,

상기 개인 식별 디바이스를 인증하는 것은 추가로, 상기 제1 디바이스와 상기 제2 디바이스 사이의 거리에 적어도 부분적으로 기초하는,

비-일시적인 기계 판독가능한 저장 매체.

청구항 35

제 26 항에 있어서,

상기 동작들은, 상기 개인 식별 디바이스와 상기 제2 디바이스 사이의 거리를 결정하는 것을 더 포함하고,

상기 개인 식별 디바이스를 인증하는 것은 추가로, 상기 개인 식별 디바이스와 상기 제2 디바이스 사이의 거리에 적어도 부분적으로 기초하는,

비-일시적인 기계 판독가능한 저장 매체.

청구항 36

시스템으로서,

인증 쿼리(query)들에 응답하도록 구성되는 제1 개인 식별 디바이스 – 상기 제1 개인 식별 디바이스는 사용자와 연관됨 –;

개인 식별 디바이스 검출기 – 상기 개인 식별 디바이스 검출기는,

상기 제1 개인 식별 디바이스를 검출하고, 그리고

상기 사용자와 연관된 제2 개인 식별 디바이스를 결정하기 위해 식별 서비스와 통신하도록 구성됨 –;

상기 식별 서비스를 포함하는 식별 서버 – 상기 식별 서버는,

상기 개인 식별 디바이스 검출기로부터 상기 제1 개인 식별 디바이스와 연관된 인증 데이터를

수신하고,

상기 제1 개인 식별 디바이스와 연관된 상기 인증 데이터에 적어도 부분적으로 기초하여 상기 제1 개인 식별 디바이스를 인증하고, 그리고

상기 제1 개인 식별 디바이스가 인증된다는 표시를 상기 개인 식별 디바이스 검출기에 송신하도록 구성됨 -;

를 포함하고,

상기 개인 식별 디바이스 검출기는,

상기 제1 개인 식별 디바이스가 인증된다는 표시를 수신하고,

상기 제1 개인 식별 디바이스가 인증된다는 표시의 수신 이후 상기 제2 개인 식별 디바이스와 통신하고, 그리고

상기 제1 개인 식별 디바이스가 인증된다는 표시의 수신 및 상기 제2 개인 식별 디바이스와의 통신에 적어도 부분적으로 기초하여 상기 제1 개인 식별 디바이스를 인증하도록 추가로 구성되는,

시스템.

청구항 37

제 36 항에 있어서,

상기 제1 개인 식별 디바이스가 인증된다는 표시는 상기 제2 개인 식별 디바이스의 표시를 포함하는,

시스템.

청구항 38

제 36 항에 있어서,

상기 개인 식별 디바이스 검출기와 통신하도록 구성되는 상기 제2 개인 식별 디바이스를 더 포함하고,

상기 개인 식별 디바이스 검출기와의 통신은 상기 제1 개인 식별 디바이스를 인증하는데 사용되는,

시스템.

청구항 39

제 38 항에 있어서,

상기 제1 개인 식별 디바이스는 상기 제2 개인 식별 디바이스와 상기 개인 식별 디바이스 검출기 사이의 통신들을 중계(relay)하는,

시스템.

청구항 40

제 38 항에 있어서,

상기 제1 개인 식별 디바이스는, 하나 이상의 동작들의 세트를 상기 제2 개인 식별 디바이스에 위임하도록 추가로 구성되고,

상기 제2 개인 식별 디바이스는,

상기 제1 개인 식별 디바이스로부터 상기 하나 이상의 동작들의 세트의 표시를 수신하고;

상기 하나 이상의 동작들의 세트를 수행하고; 그리고

상기 하나 이상의 동작들의 세트의 결과들을 상기 제1 개인 식별 디바이스 및 상기 개인 식별 디바이스 검출기 중 하나에 송신하도록 추가로 구성되는,

시스템.

청구항 41

제 40 항에 있어서,

상기 하나 이상의 동작들의 세트는, 인증 관련 데이터를 암호화하는 것 및 상기 인증 관련 데이터를 송신하는 것으로 구성된 그룹으로부터 선택된 적어도 하나의 멤버를 포함하는,

시스템.

청구항 42

제 36 항에 있어서,

제3 개인 식별 디바이스를 더 포함하고,

상기 개인 식별 디바이스 검출기는 상기 제3 개인 식별 디바이스와 통신하는 것에 적어도 부분적으로 기초하여 상기 제1 개인 식별 디바이스를 인증하도록 추가로 구성되는,

시스템.

청구항 43

삭제

청구항 44

삭제

청구항 45

삭제

청구항 46

삭제

청구항 47

삭제

청구항 48

삭제

청구항 49

삭제

청구항 50

삭제

청구항 51

삭제

청구항 52

삭제

청구항 53

삭제

청구항 54

삭제

청구항 55

삭제

청구항 56

삭제

발명의 설명

기 술 분 야

[0001] 관련 출원들

[0002] [0001] 본원은 2013년 3월 15일에 출원된 미국 가특허 출원 번호 제61/800,518호 및 2013년 9월 27일에 출원된 미국 출원 번호 제14/040,213호에 우선권을 주장한다.

[0003] [0002] 발명의 대상의 실시예들은 일반적으로 무선 디바이스들의 분야에 관한 것이고, 그리고 보다 구체적으로는, 무선 네트워킹-가능 개인 식별 디바이스들에 관한 것이다.

배 경 기 술

[0004] [0003] 디지털 세계에서 사용되는 가장 흔한 인증 기법은 아마도 사용자명 및 암호의 조합이다. 사용자명은 사용자를 식별하는데 반해, 암호는, 적어도 최적으로, 오직 상기 사용자에게만 알려진다. 시스템은, 암호에 관한 지식에 기초하여, 사용자가 그들이 주장하는 누군가라고 가정한다. 사용자의 고유한 신체적 양상들이 사용자의 신원을 확인하기 위해 이용될 수 있는 생체인식 인증 또는 키카드(keycard)에 내장된 무선 주파수(RF) 칩과 통신하는 것과 같은 다른 형태들의 인증이 또한 이용된다. 또한, 다양한 인증 기법들은 멀티-팩터(multi-factor) 인증을 생성하기 위해 조합될 수 있다.

[0005] [0004] 무선 통신들은, 전술한 내장된 RF 칩을 사용하는 통신들과 같은, 무선 인증 방법들을 허용한다. RF 칩들 및 회로들은 다른 것들 중에 신용 카드들 및 유료 도로(toll road)들을 위한 몇몇 식별 태그들 내에 또한 존재한다. 근거리 무선통신(NFC) 표준들과 같은 다른 기술은 전자 디바이스들 사이의 통신 및 인증을 허용한다. 다수의 이용가능한 인증 기법들 및 기술들은 디지털 세계에서 개인이 그들이 주장하는 누구인지 여부를 결정하는 것과 연관된 도전들을 강조한다.

발명의 내용

[0006] [0005] 무선 네트워킹-가능 개인 식별 시스템에 대한 다양한 실시예들이 개시된다. 몇몇 실시예들에서, 방법은: 제1 디바이스로부터, 비컨 메시지(beacon message)를 송신하는 단계 - 상기 비컨 메시지는 무선으로 송신됨 -; 상기 제1 디바이스에서, 상기 비컨 메시지에 대한 제1 응답을 수신하는 단계 - 상기 제1 응답은 개인 식별 디바이스와 연관된 식별 값들을 포함함 -; 제2 디바이스와 통신하는 단계 - 상기 제2 디바이스는 상기 개인 식별 디바이스와 연관됨 -; 및 상기 개인 식별 디바이스를 인증하는 단계 - 상기 인증하는 단계는 상기 제2 디바이스와 통신하는 단계 및 상기 식별 값들에 적어도 부분적으로 기초함 -를 포함한다.

[0007] [0006] 몇몇 실시예들에서, 상기 방법은 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리를 결정하는 단계를 더 포함하고, 상기 인증하는 단계는 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 상기 결정된 거리에 적어도 부분적으로 기초한다.

[0008] [0007] 몇몇 실시예들에서, 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리는 상기 제1 디바이스와 상기 개인 식별 디바이스 사이에서 데이터를 이동(travel)시키기 위한 전파 시간(a time of flight)에 적어도 부분적으로 기초하여 결정된다.

[0009] [0008] 몇몇 실시예들에서, 상기 방법은 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리가 미리결정된 거리 내에 있음을 결정하는 단계를 더 포함하고, 상기 개인 식별 디바이스를 인증하는 단계는 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리가 미리결정된 거리 내에 있음을 결정하는 단계에 적어도 부분적으

로 기초한다.

[0010] [0009] 몇몇 실시예들에서, 상기 개인 식별 디바이스를 인증하는 단계는 상기 제1 디바이스로부터, 컴퓨팅 시스템으로 상기 개인 식별 디바이스와 연관된 상기 식별 값들을 송신하는 단계; 및 상기 제1 디바이스에서, 상기 컴퓨팅 시스템으로부터의 제2 응답을 수신하는 단계 - 상기 제2 응답은 상기 개인 식별 디바이스가 인증되었다는 표시 및 상기 개인 식별 디바이스와 연관된 데이터 중 적어도 하나를 포함함 -를 더 포함하고, 상기 개인 식별 디바이스를 인증하는 단계는 상기 개인 식별 디바이스가 인증되었다는 표시 및 상기 개인 식별 디바이스와 연관된 데이터 중 적어도 하나에 적어도 부분적으로 기초한다.

[0011] [0010] 몇몇 실시예들에서, 상기 개인 식별 디바이스와 연관된 데이터는 상기 제2 디바이스의 표시를 포함한다.

[0012] [0011] 몇몇 실시예들에서, 상기 방법은 상기 컴퓨팅 시스템에서, 상기 개인 식별 디바이스와 연관된 상기 식별 값들을 수신하는 단계; 상기 컴퓨팅 시스템에서, 상기 개인 식별 디바이스와 연관된 상기 식별 값들을 검증하는 단계; 및 상기 컴퓨팅 시스템으로부터, 상기 제2 응답을 송신하는 단계를 더 포함한다.

[0013] [0012] 몇몇 실시예들에서, 상기 방법은 상기 제1 디바이스에서, 제1 인증 토큰(token)을 생성하는 단계 - 상기 제1 인증 토큰은 상기 개인 식별 디바이스와 연관된 상기 식별 값들과 함께 상기 컴퓨팅 시스템으로 송신됨 -; 및 상기 컴퓨팅 시스템으로부터, 제2 인증 토큰을 수신하는 단계를 더 포함하고, 상기 개인 식별 디바이스를 인증하는 단계는 상기 제1 인증 토큰이 상기 제2 인증 토큰과 매칭(match)됨을 결정하는 단계를 포함한다.

[0014] [0013] 몇몇 실시예들에서, 상기 식별 값들은 암호화된 식별 값 및 비암호화된 식별 값 중 적어도 하나를 포함한다.

[0015] [0014] 몇몇 실시예들에서, 상기 암호화된 식별 값은 상기 개인 식별 디바이스와 연관된 공개 키로 암호화된 랜덤 값을 포함한다.

[0016] [0015] 몇몇 실시예들에서, 상기 방법은 상기 제1 디바이스에서, 상기 개인 식별 디바이스와 연관된 추가적인 인증 데이터를 수신하는 단계를 더 포함하고, 상기 개인 식별 디바이스를 인증하는 단계는 상기 추가적인 인증 데이터에 적어도 부분적으로 기초한다.

[0017] [0016] 몇몇 실시예들에서, 상기 추가적인 인증 데이터는 암호 및 생체인식 데이터 중 적어도 하나를 포함한다.

[0018] [0017] 몇몇 실시예들에서, 상기 방법은 상기 제1 디바이스와 상기 제2 디바이스 사이의 거리를 결정하는 단계를 더 포함하고, 상기 개인 식별 디바이스를 인증하는 단계는 상기 제1 디바이스와 상기 제2 디바이스 사이의 거리에 적어도 부분적으로 기초한다.

[0019] [0018] 몇몇 실시예들에서, 상기 방법은 상기 개인 식별 디바이스와 상기 제2 디바이스 사이의 거리를 결정하는 단계를 더 포함하고, 상기 개인 식별 디바이스를 인증하는 단계는 상기 개인 식별 디바이스와 상기 제2 디바이스 사이의 상기 거리에 적어도 부분적으로 기초한다.

[0020] [0019] 몇몇 실시예들에서, 상기 제2 디바이스는 휴대폰(cellphone)이다.

[0021] [0020] 몇몇 실시예들에서, 상기 방법은 상기 개인 식별 디바이스에서, 상기 제1 디바이스로부터의 상기 비컨 메시지를 수신하는 단계; 상기 개인 식별 디바이스에서, 상기 제1 디바이스로부터의 상기 비컨 메시지를 수신하는 단계에 응답하여, 상기 개인 식별 디바이스에서, 상기 비컨 메시지에 대한 상기 제1 응답을 생성하는 단계; 및 상기 개인 식별 디바이스로부터, 상기 제1 응답을 송신하는 단계를 더 포함한다.

[0022] [0021] 몇몇 실시예들에서, 상기 개인 식별 디바이스에서, 상기 비컨 메시지에 대한 상기 제1 응답을 생성하는 단계는 적어도 하나의 식별 값을 암호화하는 단계를 포함하고, 상기 개인 식별 디바이스와 연관된 상기 식별 값들은 상기 적어도 하나의 암호화된 식별 값을 포함한다.

[0023] [0022] 몇몇 실시예들에서, 상기 방법은 제3 디바이스와 통신하는 단계 - 상기 제3 디바이스는 상기 개인 식별 디바이스와 연관됨 - 를 더 포함하고, 상기 인증하는 단계는 상기 제3 디바이스와 통신하는 단계에 적어도 부분적으로 기초한다.

[0024] [0023] 몇몇 실시예들에서, 방법은: 개인 식별 디바이스가 제1 디바이스와 통신할 수 있음을 결정하는 단계; 상기 개인 식별 디바이스에 의해 수행가능한 하나 또는 그 초과의 동작들의 세트가 전력 임계값보다 더 큰 전력의 양을 소모할 수 있음을 결정하는 단계; 및 상기 하나 또는 그 초과의 동작들의 세트를 상기 제1 디바이스에 위임(delegate)하는 단계 - 상기 위임하는 단계는 상기 개인 식별 디바이스가 상기 제1 디바이스와 통신할 수 있

음을 결정하는 단계 및 상기 개인 식별 디바이스에 의해 수행가능한 하나 또는 그 초과의 동작들의 세트가 상기 전력 임계값보다 더 큰 전력의 양을 소모할 수 있음을 결정하는 단계에 적어도 부분적으로 기초함 -를 포함한다.

[0025] [0024] 몇몇 실시예들에서, 상기 방법은 상기 개인 식별 디바이스가 제2 디바이스와 통신할 수 있음을 결정하는 단계; 및 상기 제1 디바이스가 상기 개인 식별 디바이스로부터의 상기 하나 또는 그 초과의 동작들의 세트를 위임하기 위해 선호되는(preferred) 디바이스임을 결정하는 단계를 더 포함하고, 상기 하나 또는 그 초과의 동작들의 세트를 상기 제1 디바이스에 위임하는 단계는 상기 제1 디바이스가 상기 개인 식별 디바이스로부터의 상기 하나 또는 그 초과의 동작들의 세트를 위임하기 위해 선호되는 디바이스임을 결정하는 단계에 응답하여 이루어진다.

[0026] [0025] 몇몇 실시예들에서, 상기 제1 디바이스가 상기 하나 또는 그 초과의 동작들의 세트를 위임하기 위해 선호되는 디바이스임을 결정하는 단계는 상기 제1 디바이스의 배터리 용량, 상기 제1 디바이스의 잔여 배터리 수명, 상기 제1 디바이스의 프로세싱 전력, 및 상기 제1 디바이스의 전력원 중 적어도 하나에 적어도 부분적으로 기초한다.

[0027] [0026] 몇몇 실시예들에서, 상기 하나 또는 그 초과의 동작들의 세트는 인증 관련 데이터를 암호화하는 것 및 상기 인증 관련 데이터를 송신하는 것 중 적어도 하나를 포함한다.

[0028] [0027] 몇몇 실시예들에서, 상기 하나 또는 그 초과의 동작들의 세트를 상기 제1 디바이스에 위임하는 단계는 상기 제1 디바이스에 대한 상기 하나 또는 그 초과의 동작들의 세트의 제1 동작을 나타내는 데이터를 송신하는 단계를 포함하고, 상기 하나 또는 그 초과의 동작들의 세트의 상기 제1 동작을 나타내는 상기 데이터는 수행할 상기 동작의 표시, 상기 동작에 대한 입력 데이터, 및 상기 동작의 결과들이 상기 제1 디바이스 또는 제2 디바이스 중 하나에 송신될 것이라는 표시 중 적어도 하나를 포함한다.

[0029] [0028] 몇몇 실시예들에서, 상기 제1 디바이스는 휴대폰이다.

[0030] [0029] 몇몇 실시예들에서, 디바이스는 프로세서; 및 검출기 제어 유닛을 포함하고, 상기 검출기 제어 유닛은: 비컨 메시지를 송신하고 - 상기 비컨 메시지는 무선으로 송신됨 -; 상기 비컨 메시지에 대한 제1 응답을 수신하고 - 상기 제1 응답은 개인 식별 디바이스와 연관된 식별 값들을 포함함 -; 2차(secondary) 개인 식별 디바이스와 통신하고 - 상기 2차 개인 식별 디바이스는 상기 개인 식별 디바이스와 연관됨 -; 그리고 상기 개인 식별 디바이스를 인증하도록 - 상기 인증은 상기 식별 값들 및 상기 2차 개인 식별 디바이스와 통신하는 것에 적어도 부분적으로 기초함 -; 구성된다.

[0031] [0030] 몇몇 실시예들에서, 상기 검출기 제어 유닛은 상기 디바이스와, 개인 식별 디바이스 및 상기 2차 개인 식별 디바이스 중 적어도 하나 사이의 거리를 결정하도록 추가로 구성되고, 상기 개인 식별 디바이스를 인증하는 것은 상기 디바이스와, 상기 개인 식별 디바이스 및 상기 2차 개인 식별 디바이스 중 적어도 하나 사이의 거리의 결정에 적어도 부분적으로 기초한다.

[0032] [0031] 몇몇 실시예들에서, 상기 디바이스와, 상기 개인 식별 디바이스 및 상기 2차 개인 식별 디바이스 중 적어도 하나 사이의 거리는 상기 디바이스와, 상기 개인 식별 디바이스 및 상기 2차 개인 식별 디바이스 중 적어도 하나 사이에서 데이터를 이동시키기 위한 전파 시간에 적어도 부분적으로 기초하여 결정된다.

[0033] [0032] 몇몇 실시예들에서, 상기 검출기 제어 유닛은 상기 디바이스와, 상기 개인 식별 디바이스 및 상기 2차 개인 식별 디바이스 중 적어도 하나 사이의 거리가 미리결정된 거리 내에 있음을 결정하도록 추가로 구성되고, 상기 개인 식별 디바이스의 인증은 상기 디바이스와, 상기 개인 식별 디바이스 및 상기 2차 개인 식별 디바이스 중 적어도 하나 사이의 거리가 미리결정된 거리 내에 있다는 상기 결정에 응답하여 이루어진다.

[0034] [0033] 몇몇 실시예들에서, 상기 검출기 제어 유닛은 상기 개인 식별 디바이스와 상기 2차 개인 식별 디바이스 사이의 거리를 결정하도록 추가로 구성되고, 상기 개인 식별 디바이스를 인증하는 것은 상기 개인 식별 디바이스와 상기 2차 개인 식별 디바이스 사이의 거리의 결정에 적어도 부분적으로 기초한다.

[0035] [0034] 몇몇 실시예들에서, 상기 검출기 제어 유닛은 상기 개인 식별 디바이스와 연관된 상기 식별 값들을 컴퓨팅 시스템에 송신하고; 그리고 상기 컴퓨팅 시스템으로부터 제2 응답을 수신하도록 - 상기 제2 응답은 상기 개인 식별 디바이스가 인증되었다는 표시, 상기 개인 식별 디바이스와 연관된 데이터, 및 상기 2차 개인 식별 디바이스의 표시 중 적어도 하나를 포함함 - 추가로 구성되고, 상기 개인 식별 디바이스의 인증은 상기 개인 식별 디바이스가 인증되었다는 표시 및 상기 개인 식별 디바이스와 연관된 데이터 중 적어도 하나에 적어도 부분

적으로 기초한다.

[0036] [0035] 몇몇 실시예들에서, 상기 검출기 제어 유닛은 상기 개인 식별 디바이스와 연관된 추가적인 인증 데이터를 수신하도록 추가로 구성되고, 상기 개인 식별 디바이스의 인증은 상기 추가적인 인증 데이터에 적어도 부분적으로 기초한다.

[0037] [0036] 몇몇 실시예들에서, 상기 추가적인 인증 데이터는 암호 및 생체인식 데이터 중 적어도 하나를 포함한다.

[0038] [0037] 몇몇 실시예들에서, 개인 식별 디바이스는 프로세서; 및 개인 식별 디바이스 제어 유닛을 포함하고, 상기 개인 식별 디바이스 제어 유닛은: 상기 개인 식별 디바이스가 제1 디바이스와 통신할 수 있음을 결정하고; 상기 개인 식별 디바이스에 의해 수행가능한 하나 또는 그 초과의 동작들의 세트가 전력 임계값보다 더 큰 전력의 양을 소모할 수 있음을 결정하고; 그리고 상기 하나 또는 그 초과의 동작들의 세트를 상기 제1 디바이스에 위임하도록 – 상기 위임하는 것은 상기 개인 식별 디바이스가 상기 제1 디바이스와 통신할 수 있다는 결정 및 상기 개인 식별 디바이스에 의해 수행가능한 하나 또는 그 초과의 동작들의 세트가 상기 전력 임계값보다 더 큰 전력의 양을 소모할 수 있다는 결정에 적어도 부분적으로 기초함 – 구성된다.

[0039] [0038] 몇몇 실시예들에서, 상기 개인 식별 디바이스 제어 유닛은 상기 개인 식별 디바이스가 제2 디바이스와 통신할 수 있음을 결정하고; 그리고 상기 제1 디바이스가 상기 개인 식별 디바이스로부터의 상기 하나 또는 그 초과의 동작들의 세트를 위임하기 위해 선호되는 디바이스임을 결정하도록 추가로 구성되고, 상기 하나 또는 그 초과의 동작들의 세트의 상기 제1 디바이스로의 위임은 상기 제1 디바이스가 상기 개인 식별 디바이스로부터의 상기 하나 또는 그 초과의 동작들의 세트를 위임하기 위해 선호되는 디바이스라는 결정에 응답하여 이루어진다.

[0040] [0039] 몇몇 실시예들에서, 상기 제1 디바이스가 상기 하나 또는 그 초과의 동작들의 세트를 위임하기 위해 선호되는 디바이스라는 결정은 상기 제1 디바이스의 배터리 용량, 상기 제1 디바이스의 배터리 수명, 상기 제1 디바이스의 프로세싱 전력, 및 상기 제1 디바이스의 전력원 중 적어도 하나에 적어도 부분적으로 기초한다.

[0041] [0040] 몇몇 실시예들에서, 상기 하나 또는 그 초과의 동작들의 세트는 인증 관련 데이터를 암호화하는 것 및 상기 인증 관련 데이터를 송신하는 것 중 적어도 하나를 포함한다.

[0042] [0041] 몇몇 실시예들에서, 상기 하나 또는 그 초과의 동작들의 세트의 상기 제1 디바이스로의 위임은 상기 제1 디바이스에 대한 상기 하나 또는 그 초과의 동작들의 세트의 제1 동작을 나타내는 데이터의 송신을 포함하고, 상기 하나 또는 그 초과의 동작들의 세트의 상기 제1 동작을 나타내는 상기 데이터는 수행할 상기 동작의 표시, 상기 동작에 대한 입력 데이터, 및 상기 동작의 결과들이 상기 제1 디바이스 또는 제2 디바이스 중 하나에 송신될 것이라는 표시 중 적어도 하나를 포함한다.

[0043] [0042] 몇몇 실시예들에서, 명령들이 저장된 기계-판독가능 저장 매체는 상기 명령들이 하나 또는 그 초과의 프로세서들에 의해 실행될 때 상기 하나 또는 그 초과의 프로세서들로 하여금: 비컨 메시지를 송신하는 것 – 상기 비컨 메시지는 제1 디바이스로부터 무선으로 송신됨 –; 상기 비컨 메시지에 대한 제1 응답을 수신하는 것 – 상기 제1 응답은 개인 식별 디바이스와 연관된 식별 값들을 포함함 –; 제2 디바이스와 통신하는 동작 – 상기 제2 디바이스는 상기 개인 식별 디바이스와 연관됨 –; 및 상기 개인 식별 디바이스를 인증하는 것 – 상기 인증하는 것은 상기 제2 디바이스와 통신하는 것 및 상기 식별 값들에 적어도 부분적으로 기초함 –을 포함하는 동작들을 수행하게 한다.

[0044] [0043] 몇몇 실시예들에서, 상기 동작들은 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리를 결정하는 것을 더 포함하고, 상기 인증하는 것은 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 상기 결정된 거리에 적어도 부분적으로 기초한다.

[0045] [0044] 몇몇 실시예들에서, 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리는 상기 제1 디바이스와 상기 개인 식별 디바이스 사이에서 데이터를 이동시키기 위한 전파 시간에 적어도 부분적으로 기초하여 결정된다.

[0046] [0045] 몇몇 실시예들에서, 상기 동작들은 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리가 미리결정된 거리 내에 있음을 결정하는 것을 더 포함하고, 상기 개인 식별 디바이스를 인증하는 것은 상기 제1 디바이스와 상기 개인 식별 디바이스 사이의 거리가 상기 미리결정된 거리 내에 있음을 결정하는 것에 적어도 부분적으로 기초한다.

[0047] [0046] 몇몇 실시예들에서, 상기 개인 식별 디바이스를 인증하는 동작은 컴퓨팅 시스템으로 상기 개인 식별 디바이스와 연관된 상기 식별 값들을 송신하는 것; 및 상기 컴퓨팅 시스템으로부터의 제2 응답을 수신하는 것 –

상기 제2 응답은 상기 개인 식별 디바이스가 인증되었다는 표시 및 상기 개인 식별 디바이스와 연관된 데이터 중 적어도 하나를 포함함 -; 을 더 포함하고, 상기 개인 식별 디바이스를 인증하는 것은 상기 개인 식별 디바이스가 인증되었다는 표시 및 상기 개인 식별 디바이스와 연관된 데이터 중 적어도 하나에 적어도 부분적으로 기초한다.

[0048] [0047] 몇몇 실시예들에서, 상기 개인 식별 디바이스와 연관된 데이터는 상기 제2 디바이스의 표시를 포함한다.

[0049] [0048] 몇몇 실시예들에서, 상기 동작들은 제1 인증 토큰을 생성하는 것 - 상기 제1 인증 토큰은 상기 개인 식별 디바이스와 연관된 상기 식별 값들과 함께 상기 컴퓨팅 시스템으로 송신됨 -; 및 제2 인증 토큰을 수신하는 것을 더 포함하고, 상기 개인 식별 디바이스를 인증하는 것은 상기 제1 인증 토큰이 상기 제2 인증 토큰과 매칭됨을 결정하는 것을 포함한다.

[0050] [0049] 몇몇 실시예들에서, 상기 동작들은 상기 개인 식별 디바이스와 연관된 추가적인 인증 데이터를 수신하는 것을 더 포함하고, 상기 개인 식별 디바이스를 인증하는 것은 상기 추가적인 인증 데이터에 적어도 부분적으로 기초한다.

[0051] [0050] 몇몇 실시예들에서, 상기 추가적인 인증 데이터는 암호 및 생체인식 데이터 중 적어도 하나를 포함한다.

[0052] [0051] 몇몇 실시예들에서, 상기 동작들은 상기 제1 디바이스와 상기 제2 디바이스 사이의 거리를 결정하는 것을 더 포함하고, 상기 개인 식별 디바이스를 인증하는 것은 상기 제1 디바이스와 상기 제2 디바이스 사이의 상기 거리에 적어도 부분적으로 기초한다.

[0053] [0052] 몇몇 실시예들에서, 상기 동작들은 상기 개인 식별 디바이스와 상기 제2 디바이스 사이의 거리를 결정하는 것을 더 포함하고, 상기 개인 식별 디바이스를 인증하는 것은 상기 개인 식별 디바이스와 상기 제2 디바이스 사이의 상기 거리에 적어도 부분적으로 기초한다.

[0054] [0053] 몇몇 실시예들에서, 시스템은: 인증 쿼리(query)들에 응답하도록 구성된 개인 식별 디바이스 - 상기 제1 개인 식별 디바이스는 사용자와 연관됨 -; 및 개인 식별 디바이스 검출기를 포함하고, 상기 개인 식별 디바이스 검출기는 상기 제1 개인 식별 디바이스를 검출하고, 그리고 제2 개인 식별 디바이스와 통신하는 것에 적어도 부분적으로 기초하여 상기 제1 개인 식별 디바이스를 인증하도록 - 상기 제2 개인 식별 디바이스는 상기 사용자와 연관됨 -구성된다.

[0055] [0054] 몇몇 실시예들에서, 상기 시스템은 식별 서버를 더 포함하고, 상기 식별 서버는, 상기 개인 식별 디바이스 검출기로부터 상기 제1 개인 식별 디바이스와 연관된 인증 데이터를 수신하고; 상기 제1 개인 식별 디바이스와 연관된 상기 인증 데이터에 적어도 부분적으로 기초하여 상기 제1 개인 식별 디바이스를 인증하고; 그리고 상기 제1 개인 식별 디바이스가, 상기 제1 개인 식별 디바이스와 연관된 상기 인증 데이터에 적어도 부분적으로 기초하여 인증된 표시를 상기 개인 식별 디바이스 검출기로 송신하도록 구성되고, 상기 개인 식별 디바이스 검출기는, 상기 제1 개인 식별 디바이스가 상기 제1 개인 식별 디바이스와 연관된 상기 인증 데이터에 적어도 부분적으로 기초하여 인증된 표시를 수신하도록 추가로 구성되고, 상기 제2 개인 식별 디바이스와 통신하는 것은 상기 제1 개인 식별 디바이스가, 상기 제1 개인 식별 디바이스와 연관된 상기 인증 데이터에 적어도 부분적으로 기초하여 인증된 표시의 수신에 응답하여 이루어진다.

[0056] [0055] 몇몇 실시예들에서, 상기 제1 개인 식별 디바이스가 인증된 표시는 상기 제2 개인 식별 디바이스의 표시를 포함한다.

[0057] [0056] 몇몇 실시예들에서, 상기 시스템은 상기 개인 식별 디바이스 검출기와 통신하도록 구성된 상기 제2 개인 식별 디바이스를 더 포함하고, 상기 개인 식별 디바이스 검출기와의 상기 통신은 상기 제1 개인 식별 디바이스를 인증하기 위해 이용된다.

[0058] [0057] 몇몇 실시예들에서, 상기 제1 개인 식별 디바이스는 상기 제2 개인 식별 디바이스와 상기 개인 식별 디바이스 검출기 사이의 통신들을 중계(relay)한다.

[0059] [0058] 몇몇 실시예들에서, 상기 제1 개인 식별 디바이스는 하나 또는 그 초과의 동작들의 세트를 상기 제2 개인 식별 디바이스에 위임하도록 추가로 구성되고, 상기 제2 개인 식별 디바이스는 상기 제1 개인 식별 디바이스로부터 상기 하나 또는 그 초과의 동작들의 세트의 표시를 수신하고; 상기 하나 또는 그 초과의 동작들의 세트를 수행하고; 그리고 상기 하나 또는 그 초과의 동작들의 세트의 결과들을 상기 제1 개인 식별 디바이스 및 상기 개인 식별 디바이스 검출기 중 하나에 송신하도록 추가로 구성된다.

[0060] [0059] 몇몇 실시예들에서, 상기 하나 또는 그 초과의 동작들의 세트는 인증 관련 데이터를 암호화하는 것 및 상기 인증 관련 데이터를 송신하는 것 중 적어도 하나를 포함한다.

[0061] [0060] 몇몇 실시예들에서, 상기 시스템은 제3 개인 식별 디바이스를 더 포함하고, 상기 개인 식별 디바이스 검출기는 상기 제3 개인 식별 디바이스와 통신하는 것에 적어도 부분적으로 기초하여 상기 제1 개인 식별 디바이스를 인증하기 위해 추가로 구성된다.

도면의 간단한 설명

[0062] [0061] 첨부한 도면들을 참조함으로써 본 실시예들은 더 잘 이해될 수 있으며, 많은 목적들, 특징들 및 장점들은 통상의 기술자에게 명백하도록 이루어졌다.

[0062] 도 1은 개인 식별 디바이스를 활용하는 시스템의 상호 작용들을 도시하는 예시적인 다이어그램이다.

[0063] 도 2는 멀티-디바이스 인증 및 개인 식별 디바이스를 구현하는 시스템을 활용하기 위한 예시적인 동작들의 흐름도를 도시한다.

[0064] 도 3은 동작들을 또 다른 디바이스로 오프로드(offload)하는 개인 식별 디바이스를 활용하는 시스템의 상호 작용들을 도시하는 예시적인 다이어그램이다.

[0065] 도 4는 개인 식별 디바이스로부터 또 다른 디바이스로 동작들을 위임하기 위한 예시적인 동작들의 흐름도를 도시한다.

[0066] 도 5는 전자 디바이스의 일 실시예의 블록 다이어그램을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0063] 아래의 설명은 본 발명의 대상의 기법들을 구현하는 예시적인 시스템들, 방법들, 기법들, 명령 시퀀스들 및 컴퓨터 프로그램 물건들을 포함한다. 그러나, 설명된 실시예들은 이들 특정한 세부사항들 없이도 실시될 수 있음이 이해된다. 예를 들어, 예시들이 암호 및 생체인식 인증 기법들을 언급하고 있을지라도, 임의의 인증 기법이 본 발명의 대상과 조합될 수 있다. 다른 예들에서, 잘 알려진 명령 인스턴스들, 프로토콜들, 구조들 및 기법들은 상기 설명을 혼란스럽게 하지 않기 위해 상세히 나타내지 않았다.

[0064] [0067] 인증 기법들은, 완전한 확실성으로, 인증하는 개인이 그들이 주장하는 누구인지를 입증하지 않는다. 예를 들어, 암호가 정당한 사용자 외에는 아무에게도 알려지지 않았을지라도, 악의적인 사용자는 정확한 암호가 찾아질 때까지 문자들의 임의의 조합들을 시도함으로써 폭력적인(brute force) 공격을 수행하기 위해 컴퓨터를 사용할 수 있다. 지문들 및 심지어 유전 형질과 같은 생체인식 데이터는 동일한 생체인식 데이터를 가진 두 사람들을 이론적으로 낳을 수 있는 프로세스들에 의존한다. 그러므로, 인증의 목표는 인증하는 개인이, 그들이 주장하는 누구인지를 입증하는 데 있는 것이 아니라, 그들이, 용인되는 확률(acceptable probability)로 그들이 주장하는 누구임을 입증하는데 있다. "용인되는 확률"은 보호되는 중인 것의 민감성 또는 위반의 영향에 기초하여 규정될 수 있다. 예를 들어, 개인 파일들에 제한되는 컴퓨팅 시스템에 로그인하는 것은 암호만을 요구할 수 있지만, 매우 민감한 데이터를 가진 컴퓨팅 시스템에 로그인하는 것은 암호를 요구하는 것뿐만 아니라, 컴퓨팅 시스템에 접근하기 위해 지문 스캔과 같은 인증 및 암호화(cryptographic) 원리들에 기초하여 패스코드를 정기적으로 변경할 것을 또한 요구할 수 있다.

[0065] [0068] 그러나, 더 안전한 인증 기법들은 더 번거로운(cumbersome) 경향이 있다. 심지어 암호들만으로도 상당히 번거로우며, 그리고 일반적으로, 적어도 실제적으로는, 매우 안전한 것으로 여겨지지도 않는다. 예를 들어, 최적의 보안을 위해, 암호들은 랜덤해야 하며, 다수의 로그인들을 위해 이용되어서는 안 된다. 그러나, 사용자들은 암호들(예를 들어, 시간의 연장된 기간 동안 이용되는 암호들에 기초한 사전)을 가진 바로가기(shortcut)들을 취하는 경향이 있으며, 그들의 유효성을 감소시킨다. 암호에 덧붙여 추가적인 랜덤 패스코드를 입력하는 것과 같은 두 개의 팩터 인증은 추가된 보안을 제공할 수 있지만, 사용자에 대한 인증의 복잡도를 증가시킨다. 그러나, 동글(dongle) 또는 키 포브(key fob)와 같이, 개인 식별 디바이스에 무선 네트워킹 능력들을 통합시키는 것은 인증과 연관된 복잡도를 감소시킬 수 있는 한편, 제공되는 보안의 레벨을 또한 증가시킬 수 있다.

[0066] [0069] 그러므로, 시스템은 오직 무선 네트워킹-가능 개인 식별 디바이스(이하에서는 "개인 식별 디바이스(personal identification device)" 또는 PID)만을 사용하도록 또는 사용자를 안전하게 인증하기 위해 다른 개인 디바이스들과 조합하여 사용하도록 구현될 수 있다. 암호화 기법들은 개인 식별 디바이스를 안전하게 인증하

기 위해 사용될 수 있다. 인증의 안전도는 개인 식별 디바이스를 사용하는 인증과, 내장된 RF 칩을 갖는 신용 카드 또는 휴대폰과 같은 추가적인 개인 디바이스들을 이용한 인증을 조합함으로써 더욱 개선될 수 있다. "레인징(ranging)"으로서 지칭되는, 개인 식별 디바이스와 추가적인 개인 디바이스 사이의 거리의 결정은 인증의 안전도를 개선하기 위해 또한 사용될 수 있는 한편, 관심 있는 개인 식별 디바이스들을 식별하기 위해 또한 사용될 수 있다. 나아가, 제3자 컴퓨팅 시스템과의 통신은 개인 식별 디바이스의 사용을 용이하게 할 수 있고, 간소화할 수 있다. 계산적 업무들의 오프로딩(offloading)과 같은 추가적인 기법들은 개인 식별 디바이스의 전력 소비를 더 낮추기 위해 이용될 수 있다.

[0067] [0070] 도 1은 개인 식별 디바이스를 활용하는 시스템의 상호작용들을 도시하는 예시적 다이어그램이다. 도 1은 개인 식별 디바이스(102), 개인 식별 디바이스 검출기(이후, 검출기"; 104) 및 휴대폰(106)을 포함하는, 인증-연관된 컴포넌트들(100)의 세트를 도시한다. 개인 식별 서비스 컴퓨팅 시스템(이후 "컴퓨팅 시스템"; 108)은 네트워크(110)에 의해 검출기(104)에 접속된다. 네트워크(110)는 근거리 네트워크, 광역 네트워크, 인터넷 등을 포함하는 다수의 네트워크들의 조합일 수 있다. 암호 입력 디바이스(112)는 검출기(104)에 접속된다. 추가적으로, 개인 식별 디바이스(102) 및 휴대폰(106)은 네트워크(110)를 통해 검출기(104)에 연결될 수 있다. 개인 식별 디바이스(102) 및 휴대폰(106)은 검출기(104)에 무선으로 접속되는 것처럼 도시된다. 그러나, 개인 식별 디바이스(102) 및 휴대폰(106)은 하드웨어를 통해(예를 들어, 유선들에 의해) 접속될 수 있다. 개인 식별 디바이스(102)는, 여기서 설명된 개인 식별 디바이스(102)의 기능성의 일부 또는 전부를 구현하는 개인 식별 디바이스 제어 유닛(103)을 포함한다. 검출기(104)는, 여기서 설명된 검출기(104)의 기능성의 일부 또는 전부를 구현하는 검출기 제어 유닛(105)을 포함한다.

[0068] [0071] 단계 A에서, 개인 식별 디바이스(102)는 검출기(104)로부터 비컨 메시지를 수신하고 하나 또는 그 초과의 식별 값들을 포함하는 응답을 송신한다. 개인 식별 디바이스(102)에 의해 수신된 메시지는 비컨 메시지일 수 있고, 상기 비컨 메시지는, 검출기(104)가 이용가능한 범위 내에서의 임의의 디바이스를 표시하는 방송 메시지일 수 있다. 비컨 메시지는 검출기(104)와 호환될 뿐만 아니라, 프로토콜 버전 숫자, 지원되는 옵션들 등과 같은 다른 메타데이터와도 호환될 수 있는 통신 프로토콜들의 유형을 표시할 수 있다. 이후에서 "비컨 메시지"는, 송신될 수 있는 추가적인 메시지들과 초기 메시지를 구별하기 위해, 검출기(104)에 의해 전송되는 초기 메시지를 말하도록 사용될 것이지만, 실시예들은 그렇게 제한되지 않는다.

[0069] [0072] 검출기(104)로부터 비컨 메시지가 수신되면, 개인 식별 디바이스(102)는 응답을 생성하고, 상기 응답을 검출기(104)로 송신한다. 개인 식별 디바이스(102) 응답은 두 개의 식별 값들: 비암호화된 식별 값 및 암호화된 식별 값을 포함할 수 있다. 이하에서 설명되는 것처럼, 식별 값들은 개인 식별 디바이스(102)를 인증하기 위해 사용될 수 있다. 개인 식별 디바이스(102) 응답은 또한 특정 구현에서 규정되는 다른 데이터를 포함할 수 있다. 개인 식별 디바이스(102)는 배터리 수명을 보존하기 위해 검출기로부터의 비컨 메시지를 수신하기 전까지 낮은 전력 상태를 유지하도록 구현될 수 있다.

[0070] [0073] 몇몇 구현예들에서, 비컨 메시지는, 휴대폰(106)과 같은 또 다른 디바이스에 의해 중계될 수 있다. 예를 들어, 검출기(104)는 초기 비컨 메시지를 송신할 수 있고, 상기 초기 비컨 메시지는 휴대폰(106)에 의해 수신된다. 휴대폰(106)은 그 후 동일한 비컨 메시지 또는 수정된 비컨 메시지를 송신할 수 있다. 예를 들어, 휴대폰(106)은, 검출기(104) 대신에 휴대폰(106)으로 송신될 임의의 응답을 표시하기 위해 비컨 메시지를 수정할 수 있다. 개인 식별 디바이스(102)는 그 후 검출기(104) 대신에 휴대폰(106)으로 응답을 송신할 수 있다. 그러므로, 예를 들어, 휴대폰(106)이 검출기(104)보다 개인 식별 디바이스(102)에 더 가까이 있는 경우, 개인 식별 디바이스(102)는 휴대폰(106)으로 응답을 송신함으로써 더 낮은 전력을 이용할 수 있다. 응답을 송신하기 위해 더 낮은 전력을 이용함으로써, 개인 식별 디바이스(102)는 더 적은 배터리 용량으로 구현될 수 있을 뿐만 아니라, 임의의 배터리의 배터리 수명도 증가시킬 수 있다. 개인 식별 디바이스(102)가 검출기(104) 및 휴대폰(106)뿐만 아니라, 다른 것들과 같은 다수의 디바이스들로부터 비컨 메시지를 수신하는 경우, 개인 식별 디바이스(102)는 가장 근접한 디바이스로 답신(reply)을 송신할 수 있다.

[0071] [0074] 단계 B에서, 검출기(104)는 개인 식별 디바이스(102) 응답을 수신하고, 개인 식별 디바이스(102)가 미리 결정된 범위 내에 있는지 여부를 결정한다. 검출기(104)는, 다양한 기법들을 사용하여 개인 식별 디바이스(102)의 거리를 결정할 수 있다. 예를 들어, 첫 번째 기법으로, 프로토콜은, 응답을 송신하기 위해 개인 식별 디바이스(102)가 사용하는 전력의 양을 규정할 수 있거나, 또는 개인 식별 디바이스(102)는 응답을 송신하기 위해 사용되는 전력 레벨을 응답 내에 표시할 수 있다. 검출기(104)는 응답을 송신하기 위해 사용되는 전력 및 측정된 신호 강도에 기초하여 검출기(104)와 개인 식별 디바이스(102) 사이의 거리를 계산할 수 있다. 그러나, 검출기(104)에 의해 예상된 것보다 더 많은 전력을 사용하는 개인 식별 디바이스(102)는, 개인 식별 디바이스

(102)가 실제보다 더 가까이 있는 것으로 결정하도록 검출기(104)를 속일 수 있다. 검출기(104)는 대신에 검출기(104)와 개인 식별 디바이스(102) 사이의 거리를 결정하기 위해 응답 및/또는 메시지의 "전파 시간(a time of flight)"을 계산할 수 있다.

[0072] [0075] 검출기(104)와 개인 식별 디바이스(102) 사이의 "전파 시간"은 메시지 또는 응답이 검출기(104)와 개인 식별 디바이스(102) 사이에서 이동(travel)하는데 걸리는 시간이다. 전파 시간은 다수의 방식들로 결정될 수 있다. 예를 들어, 검출기(104) 및 개인 식별 디바이스(102)는 전파 시간을 결정하기 위해 시계들을 동기화할 수 있고 그리고 메시지 타임스탬프(timestamp)들을 활용할 수 있다. 몇몇 실시예들에서, 검출기(104)는 검출기(104)와 개인 식별 디바이스(102) 사이의 메시지에 대한 응답의 출발 시간(a time of departure; TOD)과 도착 시간(a time of arrival; TOA) 사이의 차이에 주목함(note)으로써 전파 시간을 결정할 수 있다. SIFS(Short Interframe Space) 시간을 계산에 넣지 않은(less) TOD와 TOA 사이의 시간 차이는 검출기(104)와 개인 식별 디바이스(102) 사이의 거리를 결정하기 위해 이용될 수 있다. 통신하기 위해 사용되는 신호들은 일정 속도(constant rate)로 이동하고 그리고 검출기(104)는 개인 식별 디바이스(102)로부터의 정보에 의존하지 않기 때문에, 개인 식별 디바이스(102)는 실제보다 더 가까이 있는 것처럼 보일 수 없다. 그러므로, 전파 시간을 계산하는 것은 개인 식별 디바이스(102)를 도용하는(spoof) 악의적 디바이스의 확률을 감소시킬 수 있고, 이에 의해 보안을 강화시킬 수 있다.

[0073] [0076] 미리결정된 범위는 몇몇 팩터들에 기초하여 구성될 수 있다. 예를 들어, 개인 식별 디바이스(102)의 성공적인 인증이 문을 여는(unlock) 경우, 미리결정된 범위는 문의 약간의 피트(feet) 내로 구성될 수 있고, 그러므로 사용자가 문을 무심코 열 가능성들을 감소시킬 수 있다. 그러나, 특정한 개인이 빌딩 내로 걸어들어올 때, 개인 식별 디바이스(102)가 식별하기 위해 사용되는 경우, 미리결정된 범위는 더 큰 거리로 구성될 수 있다.

[0074] [0077] 단계 C에서, 검출기(104)는 인증을 위하여 컴퓨팅 시스템(108)으로 단계 A에서의 응답에서 수신된 개인 식별 디바이스(102) 식별 값들을 송신한다. 컴퓨팅 시스템(108)은 개인 식별 디바이스들의 데이터베이스를 포함할 수 있고, 개인 식별 디바이스들 각각은 시리얼 번호와 같이, 표현(representation)들의 고유한 번호 또는 다른 유형들에 의해 식별된다. 개인 식별 디바이스(102) 비암호화된 식별 값은 컴퓨팅 시스템(108) 데이터베이스 내에서 특정 개인 식별 디바이스(102)를 식별하는 고유한 숫자일 수 있다. 개인 식별 디바이스(102) 암호화된 식별 값은 개인 식별 디바이스(102)의 식별의 암호화 "증거"일 수 있다. 예를 들어, 공개 키 암호화는 개인 식별 디바이스(102)를 인증하기 위한 메커니즘을 제공할 수 있다. 검출기(104)는 비컨 메시지에서의 랜덤 값을 포함할 수 있다. 개인 식별 디바이스(102)는, 오직 개인 식별 디바이스(102) 상에만 저장된 개인 키를 사용하여 랜덤 값을 암호화한다. 암호화된 랜덤 값은 개인 식별 디바이스(102) 응답에서의 암호화된 식별 값이 되고, 이는 후속적으로 컴퓨팅 시스템(108)으로 송신된다. 컴퓨팅 시스템(108)은, 암호화된 식별 값을 해독하기 위해 개인 식별 디바이스(102)와 연관된 공개 키를 사용한다. 컴퓨팅 시스템(108)은 그 후, 해독된 식별 값을 (검출기(104)에 의해 제공된) 비컨 메시지로부터의 랜덤 값과 비교할 수 있다. 값들이 매칭되는 경우, 개인 식별 디바이스(102)는 인증된다.

[0075] [0078] 인증의 실제 구현은 달라질 수 있다. 예를 들어, 컴퓨팅 시스템(108)은, 검출기(104)로 개인 식별 디바이스(102)와 연관된 공개 키를 제공하도록 구현될 수 있고, 검출기는 개인 식별 디바이스(102)로부터의 암호 값을 해독할 수 있다. 개인 식별 디바이스(102)와 연관된 공개 키는, 개인 식별 디바이스(102)의 구성 동안과 같은, 사용 이전의 컴퓨팅 시스템(108)과 교환될 수 있다. 개인 식별 디바이스(102)와 연관된 공개 키는 또한 컴퓨팅 시스템(108)에 액세스가능한 공개 키들의 데이터베이스 내에 저장될 수 있다. 또한, 개인 키(private key) 교환들과 같은 다른 유형들의 암호화 기법들이 활용될 수 있다.

[0076] [0079] 단계 D에서, 컴퓨팅 시스템(108)은 검출기(104)로 응답을 송신한다. 컴퓨팅 시스템(108)이 개인 식별 디바이스(102)를 인증한 경우, 컴퓨팅 시스템(108) 응답은 인증이 성공적이었는지 여부를 포함한다. 검출기(104)가 인증을 수행하는 경우, 컴퓨팅 시스템(108) 응답은, 개인 식별 디바이스(102)와 연관된 공개 키와 같은, 인증을 위한 검출기(104)에 대한 임의의 데이터를 포함할 수 있다. 또한, 응답은, 개인 식별 디바이스(102)와 연관된, 휴대폰(106)과 같은, 추가적인 개인 디바이스들에 관한 정보를 포함할 수 있다. 아래에서 설명되는 것처럼, 추가적인 개인 디바이스들은 사용자를 추가적으로 인증하도록 사용될 수 있고, 따라서 보안을 강화시킨다.

[0077] [0080] 단계 E에서, 검출기(104)는, 실제 사용자가 개인 식별 디바이스(102)와 연관된 정당한 사용자라는 인증을 추가적으로 제공하기 위해 휴대폰(106)과 통신한다. 개인 식별 디바이스(102)가 인증되었음을 것을 표시하

는 컴퓨팅 시스템(108) 응답을 수신하거나 또는 컴퓨팅 시스템(108) 응답에 기초하여 인증을 수행하면, 검출기(104)는 개인 식별 디바이스(102)를 인증한다. 그러나, 임의의 추가적인 개인 디바이스들과 통신하기 전에, 인증은 오로지 개인 식별 디바이스(102)에만 기초한다. 그러므로, 개인 식별 디바이스(102)의 단순한 소유는 개인 식별 디바이스(102)와 연관된 정당한 사용자의 위장(impersonation)을 허용할 수 있다. 몇몇 시나리오들에서, 이러한 보안의 레벨은 충분하다. 예를 들어, 추가적 인증이 수행되지 않는 경우, 보안의 레벨은 RF 키카드의 보안의 레벨과 기능적으로 유사하다. 그러나, 다른 시나리오들에서, 추가적 인증이 사용될 수 있다.

[0078] [0081] 보안의 레벨을 강화시키기 위해 사용될 수 있는 하나의 기법은 개인 식별 디바이스(102)와 추가적인 개인 디바이스들을 연관시키는 것에 의할 수 있다. 예를 들어, 개인 식별 디바이스(102)를 구성할 때, 사용자는 그들의 휴대폰(106)을 개인 식별 디바이스(102)와 연관시킬 수 있다. 단계 D에서 설명된 것처럼, 컴퓨팅 시스템(108)이 검출기(104)로부터의 인증 요청에 응답할 때, 컴퓨팅 시스템(108)은, 휴대폰(106)을 포함하는, 연관된 개인 디바이스들의 리스트를 제공할 수 있다. 검출기(104)는 그 후 휴대폰(106)과의 통신을 설정하기 위한 시도를 할 수 있다. 휴대폰(106)을 사용하여 수행되는 인증은 구현들 사이에서 달라질 수 있다. 예를 들어, 휴대폰(106)은 개인 식별 디바이스(102)와 유사한 공개/개인 키 쌍을 가질 수 있거나 또한, 검출기(104)는 오로지, 적절한 식별로 응답하는 휴대폰(106)에만 의존할 수 있다. 추가적으로, 더욱 복잡한 상호작용들이 가능하다. 예를 들어, 개인 식별 디바이스(102) 및 휴대폰(106)은 이전에 페어링될(paired) 수 있고, 이는 개인 식별 디바이스(102)와 휴대폰(106) 사이의 보안 통신을 가능케한다. 개인 식별 디바이스(102)를 인증한 후에, 검출기(104)는 그 후 추가적인 인증이 사용되어야 한다는 것을 개인 식별 디바이스(102)에 표시할 수 있다. 개인 식별 디바이스(102)는 그 후, 검출기(104)에 메시지를 전송하도록 휴대폰(106)에 지시(direct)하기 위해 휴대폰(106)과 보안적으로 통신할 수 있다. 개인 식별 디바이스(102)와 관련하여 위 단계 B에서 설명된 것처럼, 검출기(104)는 또한 검출기(104)와 휴대폰(106) 사이의 거리를 결정할 수 있다. 또한, 개인 식별 디바이스(102)는 개인 식별 디바이스(102)와 휴대폰(106) 사이의 거리, 또는 휴대폰(106)과 개인 식별 디바이스(102) 사이의 거리를 결정할 수 있고, 따라서, 개인 식별 디바이스(102)와 휴대폰(106)이 사용자에게 소지되어 서로 근접하게 위치되는 것을 보장하는 범위 제한을 가능케한다.

[0079] [0082] 그러므로, 예를 들어, 악의적 사용자가 빌딩으로의 액세스를 획득하기 위해 정당한 사용자의 복제된 개인 식별 디바이스(102)를 사용한다고 가정해보자. 정상적인 동작 하에서, 위에서 설명된 것처럼, 검출기(104)는 개인 식별 디바이스(102)를 검출하고, 그리고 정당한 사용자의 신원을 추가적으로 인증하기 위해 휴대폰(106)과 통신한다. 정당한 사용자가 빌딩 내에 있었고, 검출기(104)가 휴대폰(106)과 통신할 수 있었다면, 악의적인 사용자는 빌딩으로의 입장을 획득하기 위해 복제된 개인 식별 디바이스를 사용할 수 있을 것이다. 그러나, 휴대폰(106)과 복제된 개인 식별 디바이스 사이의 거리가 결정되었다면, 악의적 사용자가 휴대폰(106)에 또한 충분히 가까이 있는 경우가 아니라면 악의적 사용자는 액세스를 획득하는 것이 가능하지 않을 것이다. 개인 식별 디바이스(102)와 휴대폰(106) 사이의 범위 제한이 오직 몇 피트(few feet)라면, 악의적 사용자는 복제된 개인 식별 디바이스를 활용하기 위해 휴대폰(106) 및/또는 정당한 사용자의 몇 피트 내에 있어야 할 것이고, 따라서 복제된 개인 식별 디바이스의 유효성을 감소시킨다.

[0080] [0083] 두 개의 개인 디바이스들(이 예에서는, 개인 식별 디바이스(102) 및 휴대폰(106))을 인증하는 것에 의해, 검출기(104)는, 사용자가 개인 식별 디바이스(102)와 연관된 정당한 사용자인 확률을 증가시키고, 따라서 보안의 레벨을 강화시킨다. 사기꾼(imposter)은 개인 식별 디바이스(102)뿐만 아니라, 휴대폰(106)도 필요로 하기 때문에, 사용자가 정당한 사용자인 확률은 증가된다. 도난당한 또는 복제된 개인 식별 디바이스(102)는 정당한 사용자를 대신하여 액세스를 획득하기 위해 홀로 사용될 수 없다. 다수의 개인 디바이스들의 인증은 단순히 두 개의 개인 디바이스들에 제한되지 않는다. 또한, 검출기(104)는 개인 식별 디바이스(102)와 연관된 개인 디바이스들의 리스트를 수신하기 때문에, 검출기(104)가 휴대폰(106)과 통신하는 것을 실패하는 경우 (리스트 상에 표시된 것과 같은) 제3 개인 디바이스를 인증하기 위해 시도할 수 있다. 그러나, 개인 디바이스들은 특정 개인과 연관된 모든 물품들이기 때문에, 다수의 개인 디바이스들의 인증은 진정한 멀티-팩터 인증은 아니다. 그러나, 진정한 멀티-팩터 인증은 이하에서 설명된 것처럼 구현될 수 있다.

[0081] [0084] 단계 F에서, 사용자는 암호 입력 디바이스(112)에 암호를 입력한다. 개인 식별 디바이스(102)와 연관된 암호는 추가적인 개인 디바이스들을 구성하는 것과 유사하게 정당한 사용자에 의해 구성될 수 있다. 암호(또는 암호의 해시(hash))는 연관된 개인 디바이스들의 리스트에 덧붙여 컴퓨팅 시스템(108)에 의해 검출기(104)로 제공될 수 있다. 검출기(104)는 컴퓨팅 시스템(108) 상에 저장된 암호와 입력된 암호를 비교함으로써 입력된 암호를 검증한다. 생체인식 데이터는 또한, 암호를 대신해서 또는 암호에 덧붙여 사용될 수 있다. 암호에 덧붙여 사용될 때, 생체인식 데이터는 세 개의 팩터 인증을 가능케한다. 몇몇 구현들에서, 휴대폰(106)과 같은, 개

인 식별 디바이스(102)와 연관된 추가적인 개인 디바이스들 중 하나는, 키보드와 같은, 데이터 입력 메커니즘을 포함하고, 개인 식별 디바이스는 암호 입력 디바이스(112)처럼 동작할 수 있다. 유사하게, 몇몇 구현들에서, 개인 식별 디바이스(102)는 암호 입력 디바이스(112)이다.

[0082] [0085] 추가적 개인 디바이스의 인증이 실패하는 경우, 검출기(104)는 예비(fallback) 인증 기법으로서 암호 또는 생체인식 데이터를 또한 이용할 수 있다. 예를 들어, 휴대폰(106) 상의 배터리는 자신의 충전을 잃을 수 있어 개인 디바이스로 하여금 실패하도록 야기하고 정당한 사용자에 의한 액세스를 막을 수 있다. 검출기(104)가, 하나 초과의 개인 디바이스(예를 들어, 휴대폰(106)보다 많은)를 사용하여 개인 식별 디바이스(102)를 인증하도록 구성되는 경우, 검출기(104)는 백업 옵션으로서 암호 입력 디바이스(112) 상에 암호를 입력하는 옵션을 제공할 수 있다.

[0083] [0086] 도 1에 도시된 일반적인 동작들의 세트는 많은 특정 구현들에 적응될 수 있다. 예를 들어, 검출기(104)는 컴퓨팅 시스템 내에 구현될 수 있거나, 또는 컴퓨팅 시스템(108)과 같은 컴퓨팅 시스템 또는 주변부로서 도 1에 도시되지 않은 것에 접속될 수 있다. 개인 식별 디바이스(102)는 그러니까 일상적인 처리(transaction) 주변의 보안을 강화하는데 활용될 수 있는 동시에, 사용자의 부담을 최소화한다. 예를 들어, 보안 웹사이트를 네비게이팅(navigate)하는 경우, 개인 식별 디바이스(102)가 컴퓨터로부터의 미리결정된 거리에 있는지 여부를 결정하기 위해 웹 브라우저는 검출기(104)를 사용할 수 있다. 검출기(104)는 사용자를 인증하고 그리고 사용자의 정보를 브라우저로, 그리고 후속하여, 보안 웹사이트로 전달할 수 있다. 보안 웹사이트는, 사용자가 사용자명 및 암호를 입력하지 않고도 사용자를 자동으로 로그인시킬 수 있다. 상기 컴퓨팅 시스템(108)과 함께 설명된 것처럼, 온라인 서비스와의 통합은 구현될 추가적 특징들을 허용한다. 예를 들어, 위에서 설명된 것과 같은 자동 로그인 기능성 또는 아래에서 논의되는 것과 같은 표준 사용자명/암호 인증 기법에 덧붙인 추가적 보안과 같은 것 중 하나와 함께 "롤링 코드들(rolling codes)"로서 구현되는 인증 토큰들은 보안을 강화시키기 위해 사용될 수 있다. 그러나, 개인 식별 디바이스(102)는 사용자에 의한 추가적인 상호작용없이 웹사이트로 임의의 인증 토큰들을 전함으로써(communicate) 사용자의 부담을 감소시킨다.

[0084] [0087] "롤링 코드"는 상이한 디바이스들 상에서 생성될 수 있는 패스코드 또는 인증 토큰을 랜덤하게 변경시킨다. "롤링 코드"를 구현하기 위해, 인증 토큰들은, 특정된 시간 기간들, 입력 카운트들, 또는 챌린지(challenge) 코드 입력들에 의해 결정되는 규칙적인 간격들에서 생성될 수 있다. 인증 토큰들은 컴퓨팅 시스템(108)에 공지된 기법을 사용하여 생성되고, 이는 컴퓨팅 시스템(108)으로 하여금 동일한 인증 토큰을 생성하는 것을 허용한다. 동일한 기법 및 동일한 입력 파라미터들(예를 들어, 시드 값들 및 간격들의 개수)을 사용함으로써, 개인 식별 디바이스(102) 및 컴퓨팅 시스템(108)은 동일한 랜덤 인증 토큰을 생성할 수 있다. 그러나, 다음 인증 토큰은 입력 파라미터들에 관한 지식이 없이 이전의 인증 토큰들에 기초하여 결정될 수 없어, 악의적 사용자로 하여금 개인 식별 디바이스(102)를 "도용(spoof)"하는 것을 어렵게 한다. 컴퓨팅 시스템(108)이 개인 식별 디바이스(102)로부터 인증 토큰을 수신할 때, 컴퓨팅 시스템(108)은 이를 컴퓨팅 시스템(108) 상에서 생성된 인증 토큰과 비교한다. 인증 토큰들이 매칭되고, 임의의 다른 인증 전제 조건(prerequisite)들이 만족될 때, 컴퓨팅 시스템(108)은 개인 식별 디바이스(102)를 인증한다.

[0085] [0088] 최소 사용자 인터페이스를 가지는 것이 유리할 때, 유사한 시나리오들이 발생한다. 예를 들어, 검출기(104)는 비접촉 지불, 단일 팩터 또는 두 개의 팩터 식별 인증, 주머니 또는 지갑으로부터 개인 식별 디바이스(102)를 제거하지 않는 모든 것을 제공하기 위해 판매 시점 관리(point-of sale) 시스템에서 구현될 수 있다. 제공되는 보안의 레벨은 사용자의 적은 부담과 함께, 현재 이용가능한 것과 동일하거나 또는 더 크다. 예를 들어, 두 개의 팩터 인증을 사용하는 것은 현재 지불 방법들보다 더 빠른 처리를 제공한다. 출납원이 모든 사용자의 물품들을 스캐닝한 이후에, 검출기(104)는 사용자의 개인 식별 디바이스(102)를 검출한다. 검출기(104)는 전술한 것처럼 개인 식별 디바이스(102)를 인증하고 그리고 사용자에게 완전히 투명한(transparent) 롤링 코드 기능성을 이용한다. 사용자는 현재의 데빗 카드 처리들과 유사한, 개인 식별 번호(PIN)에 대해 유도된다. 그러나, 사용자는 어떠한 카드도 제거하고 대지(swipe) 않아, 데빗/신용 카드 번호가 도난당할 위험을 제거할 수 있는 한편, 패스코드들을 랜덤하게 변경하는 것을 활용하고, 이렇게 하여 위조 데빗/신용 카드가 사용되는 것을 방지할 수 있다. 유사하게, 개인 식별 디바이스(102)는 사용자를 인증하고 제한된 구역들에 액세스하는 것을 허용하는데 이용될 수 있는 한편, 그들의 액세스를 추적하는데 또한 이용될 수 있다. 그러나, 위에서 논의된 다양한 구현들 중 많은 것들을 조합한 보다 많은 동적 구현들이 가능하다.

[0086] [0089] 예를 들어, 그의/그녀의 선호하는 호텔 체인과 관계를 맺고 있는(established with) 계정(account)을 가진 사용자가 출장을 계획중이다. 방을 예약하기 위해, 사용자는 호텔의 웹사이트를 네비게이팅하고, 이는 사용자를 웹사이트에 자동으로 로그인시키기 위해 그의/그녀의 컴퓨터에 접속된 검출기(104)를 사용한다. 사용자

는 그의/그녀의 여행 정보를 입력하고, 방을 예약한다. 사용자가 호텔에 도착할 때, 또 다른(another) 검출기는 그의/그녀의 개인 식별 디바이스(102)를 검출한다. 사용자의 정보는 호텔 프론트 데스크에 있는 컴퓨터상으로 자동으로 로딩되고, 이는 스테프로 하여금 그/그녀가 프론트 데스크에 도달한 시간에 사용자를 체크-인하게 하는 것을 가능케한다. 스테프는 방 번호를 제공하고, 그리고 사용자는 방으로 곧장 향한다. 호텔 방 문쪽으로 걸어가면, 또 다른(yet another) 검출기가 사용자의 개인 식별 디바이스(102)를 검출하고, 호텔 방 문을 연다. 이후에, 사용자는 스낵을 구입하기 위해 자판기로 향하고, 스낵을 구입하기 위해 PIN 번호를 입력한다. 유사하게, 집으로 복귀할 시간일 때, 사용자는 호텔 로비의 키오스크(kiosk) 쪽으로 걸어가고, 그/그녀의 PIN 번호를 입력하고, 방에 대한 대금을 지불한다. 전체 프로세스는, 개인 식별 디바이스(102)가 없는 프로세스와 비교하여 각 단계에서 동일한 또는 더 나은 보안을 갖고, 도중에 추가적인 편의들과 함께, 매끄럽게 이루어진다.

[0087] [0090] 컴퓨팅 시스템(108)에 의해 제공되는 서비스는, 개인 식별 디바이스(102)를 인증하려고 시도하는 입력과 개인 식별 디바이스(102) 사이의 관계의 확립 또는 "사전인증"을 허용한다. 예를 들어, 위에서 설명된 것처럼, 사용자는 그들의 계정을 그들의 개인 식별 디바이스(102)에 연결시킬 수 있다. 개인 식별 디바이스(102)가 적절히 인증될 때, (호텔 회사와 같은) 인증 주체(identity)는 그 후, 구입 이력 및 선호도들과 같은, 사용자에 관한 정보를 제공하기 위해 컴퓨팅 시스템(108)을 활용할 수 있다.

[0088] [0091] 나아가, 개인 식별 디바이스(102)에 의해 제공되는 가상 주체 및 허가들을 가상 주체에 결부시키는 능력은 위치들 사이의 매끄러운 천이들을 허용할 수 있는 한편, 각 장소가 사용자를 "인지"하는 것을 허용할 수 있다. 예를 들어, 오피스 빌딩 도처에 위치된 (검출기(104)와 같은) 검출기들은 그/그녀의 개인 식별 디바이스(102)를 검출하는 것에 기초하여 사용자의 위치를 결정할 수 있다. 사용자가 특정 컨퍼런스 룸에 들어갔을 때, 예를 들어, 검출기(104)는 모든 컨퍼런스 룸 디바이스들이 사용자와 연관된 허가들을 로딩하도록 트리거링(trigger)할 수 있다. 그러므로, 사용자가 컨퍼런스 룸 내에서 폰을 사용하기 위한 허가는 갖고 있지만, 컴퓨터를 사용하기 위한 허가는 갖고 있지 않을 때, 폰은 자동으로 인에이블(enable)되는 반면, 컴퓨터는 자동으로 디스에이블(disable)된다. 나아가, 사용자는 단일 폰 번호를 가질 수 있고, 사용자 폰 번호로의 전화는 사용자의 개인 식별 디바이스(102)를 인증하는 검출기(104)에 기초하여 사용자에게 가장 가까운 폰으로 라우팅될 수 있다. 추가적으로, 사용자의 컴퓨터로부터의 데이터는, 컴퓨팅 시스템(108)에 의해 제공되는 것처럼, 클라우드-기반 서비스를 사용하여 동기화될 수 있다. 그러므로, 사용자가 컨퍼런스 룸 내에서 컴퓨터를 사용하도록 허용된다면, 개인 식별 디바이스(102)의 검출 시 그/그녀의 데이터는 컨퍼런스 룸 컴퓨터 상에서 자동으로 이용가능할 것이다.

[0089] [0092] 개인 식별 디바이스(102)는 많은 상이한 형태들로 구현될 수 있다. 예를 들어, 개인 식별 디바이스(102)는, 흔히 키 포브로서 지칭되는, 키체인 부가물(attachment)로서 구현될 수 있다. 시계에 내장되거나 또는 또 다른 전자 디바이스 내부에 통합되는, 신용 카드와 유사한 것처럼, 다른 형태 팩터들로 개인 식별 디바이스(102)가 또한 구현될 수 있다.

[0090] [0093] 여기서 설명된 예시들은 쿼리에 응답하여 컴퓨팅 시스템(108)으로부터 데이터를 수신하는 검출기(104)를 언급하지만, 컴퓨팅 시스템(108)으로부터의 데이터는 검출기(104)로 "푸시(push)"될 수 있다. 예를 들어, 개인 식별 디바이스(102)와 연관된 사용자가 검출기(104)와 연관된 컨퍼런스 룸을 사용하도록 예정되어 있는지 여부를 결정하기 위해 컴퓨팅 시스템(108)에 질의하는 것 대신에, 컴퓨팅 시스템(108)은 컨퍼런스 룸 스케쥴이 변경될 때 또는 규칙적인 간격들에서 컨퍼런스 룸 스케쥴을 나타내는 데이터를 전송할 수 있다. 검출기(104)는 사용하기 위한 데이터를 저장할 수 있고, 개인 식별 디바이스(102)가 검출될 때 응답 시간을 잠재적으로 감소시킬 수 있다.

[0091] [0094] 도 2는 개인 식별 디바이스 및 멀티-디바이스 인증을 구현하는 시스템을 활용하기 위한 예시적인 동작들의 흐름도를 도시한다. 블록(202)에서 시작하여, 개인 식별 디바이스는 검출기로부터 비컨 메시지를 수신하고 응답을 송신한다. 개인 식별 디바이스는 검출기로부터 비컨 메시지를 수신하기 전까지 저 전력 상태를 유지하도록 구현될 수 있다. 비컨 메시지는 검출기가 근처의 개인 식별 디바이스들을 능동적으로 검색하는 중이라는 것을 표시한다. 비컨 메시지에 응답하여, 개인 식별 디바이스가 비컨 메시지를 수신하였으며, 인증을 위하여 이용가능하다는 것을 표시하는 응답을 개인 식별 디바이스가 송신한다. 통신 디바이스들이 호환성 레벨들 및 지원되는 피처(feature)들을 결정하는 것을 가능케 하는 프로토콜 정보와 같은, 추가적인 메타데이터가 비컨 메시지 및 응답 모두에 포함될 수 있다. 또한, 응답은, 개인 식별 디바이스를 식별하고 그리고 인증하기 위해 사용되는 데이터를 포함한다. 응답이 송신된 이후에, 제어는 그 다음에 블록(204)으로 흘러간다.

[0092] [0095] 블록(204)에서, 검출기는 개인 식별 디바이스로부터 응답을 수신하고 그리고 개인 식별 디바이스가 미리 결정된 범위 내에 있는지 여부를 결정한다. 검출기와 개인 식별 디바이스 사이의 범위(거리)를 결정하는 것은 검출기로 하여금, 관련된 행동을 트리거링하기에 검출기에 충분히 가까이 있지 않은 개인 식별 디바이스를 무시하는 것을 허용한다. 예를 들어, 오피스 빌딩에서, 문은 검출기에 접속된 잠금 메커니즘을 가질 수 있다. 문을 열기 위한 허가를 가진 사용자와 연관된 개인 식별 디바이스를 검출기가 인증할 때, 검출기는 문을 열기 위해 잠금 메커니즘을 트리거링한다. 그러나, 많은 사람들은 문을 지나쳐 걸어갈 수 있지만, 문을 여는 것을 의도하지 않을 수 있다. 그러므로, 오직 특정 거리 내에 있는 사람만이 잠금 메커니즘을 트리거링하도록 검출기는 미리결정된 범위를 갖도록 구성될 수 있다. 미리결정된 범위들은 상이한 구현들을 위해 상이하게 규정될 수 있다. 예를 들어, 일 구현은, 특정 거리를 넘어 떨어져 있는 검출기들과의 통신들이 발생하지 않도록 개인 식별 디바이스의 전력 레벨 출력을 제한할 수 있다. 검출기는, 위에서 설명된 것처럼, 전파 시간을 계산하거나 또는 개인 식별 디바이스로부터의 응답의 신호 강도를 사용하는 것 중 하나에 의해 거리를 결정할 수 있다. 개인 식별 디바이스가 미리결정된 범위 내에 있는지 여부를 결정한 후에, 제어는 그 다음에 블록(206)으로 흘러간다.

[0093] [0096] 블록(206)에서, 검출기는 개인 식별 디바이스로부터 수신된 식별 값들을, 인증을 위한 식별 서비스로 송신한다. 식별 값들은 특정 개인 식별 디바이스를 식별하는 고유 번호뿐만 아니라, 개인 식별 디바이스를 인증하기 위해 식별 서비스가 사용하는 임의의 추가적인 데이터를 포함한다. 위에서 설명된 것처럼, 이는 식별 서비스 또는 검출기 중 하나에 의해 해독되고 그리고 원본 값과 비교되는 암호화된 값을 포함할 수 있다. 식별 서비스에 식별 값들을 송신한 후에, 제어는 그 다음 블록(208)으로 흘러간다.

[0094] [0097] 블록(208)에서, 검출기는, 식별 서비스로부터 개인 식별 디바이스와 연관된 임의의 추가적인 개인 디바이스들에 관한 데이터 및 개인 식별 디바이스 식별 값들의 인증을 수신한다. 식별 값들의 성공적인 인증은, 개인 식별 디바이스의 인증을 나타낸다. 다시 말해, 개인 식별 디바이스가 그것을 식별하는 고유한 번호를 송신할 때, 개인 식별 디바이스는, 개인 식별 디바이스가 그 고유한 번호와 연관된 특정 개인 식별 디바이스임을 "주장(claim)"하는 중이다. 위에서 설명된 바와 같은, 암호화 인증은, 고유한 식별 번호와 연관된 개인 식별 디바이스가, 실제로, 개인 식별 디바이스라는 매우 강한 검증을 제공한다. 개인 식별 디바이스와 연관된 임의의 추가적인 개인 디바이스들에 관한 데이터 및 개인 식별 디바이스의 인증을 수신한 후에, 제어는 그 다음에 블록(210)으로 흘러간다.

[0095] [0098] 블록(210)에서, 검출기는 개인 식별 디바이스와 연관된 추가적인 개인 디바이스와 통신하거나, 또는 통신하기 위해 시도한다. 검출기는, 인증에 추가적인 보안을 추가하기 위해 개인 식별 디바이스와 연관된 임의의 추가적인 개인 디바이스들에 관한 식별 서비스에 의해 제공되는 데이터를 사용한다. 검출기는, 추가적인 개인 디바이스와 통신하는 것에 의해, 사용자를 가장하는 누군가로부터의 거짓 인증을 방지할 수 있다. 검출기가 추가적인 개인 디바이스와 통신한 이후에, 제어는 그 다음에 블록(212)으로 흘러간다.

[0096] [0099] 블록(212)에서, 사용자는 선택적으로 암호 입력 디바이스로 암호를 입력하고, 따라서, 두 개의 팩터 인증을 제공한다. 개인 식별 디바이스를 인증하기 위한 암호화 기법들 활용하는 것 및 사용자와 연관된 또 다른 개인 디바이스와 통신하는 것을 넘어선 인증 방법의 사용은 필요한 경우 훨씬 큰 보안을 제공한다. 추가적으로, 블록(210)에서 추가적인 개인 디바이스와의 통신이 실패하는 경우, 두 개의 팩터 인증은 예비 옵션으로서 기능할 수 있다. 나아가, 생체인식 및 다른 인증 방법들은 암호 대신에 사용될 수 있거나, 또는 보안의 추가적인 레벨들을 제공하기 위해 암호에 덧붙여 사용될 수 있다. 추가적인 인증 방법(들)을 사용하는 인증은 위에서 설명된 것처럼 수행된다. 추가적 인증 방법(들)을 사용하는 인증 이후에, 프로세스는 종료된다.

[0097] [0100] 개인 식별 디바이스의 동작에 대한 중요한 양상은 적절한 배터리 수명을 보장하는 것이다. 따라서, 개인 식별 디바이스는 전력 소모를 감소시키기 위한 기법들을 활용할 수 있다. 예를 들어, 개인 식별 디바이스는 그것과 통신하는 또 다른 개인 디바이스에 응답하여 통신하도록 구현될 수 있다. 많은 무선 디바이스들이 위에서 설명된 비컨 메시지와 유사한 메시지들을 정기적으로 송신할 수 있는 반면, 개인 식별 디바이스는 비컨 메시지를 정기적으로 송신하지 않고, 송신된 비컨 메시지들에 대한 수신된 메시지들을 모니터링만 하도록 구현될 수 있다.

[0098] [00101] 추가적으로, 개인 식별 디바이스는 더욱 파워풀한 디바이스들(이러한 디바이스들이 이용가능 하다면)로 프로세서-집중 업무를 오프로드하도록 구현될 수 있다. 예를 들어, 암호화 및 해독화는, 심지어 특정 목적을 위하여 특별히 고안된 하드웨어를 이용하더라도, 상당한 계산 전력을 사용할 수 있다. 계산 전력의 상당한 양들의 사용은 개인 식별 디바이스의 배터리 수명을 상당히 감소시킬 수 있다. 나아가, 배터리가 방전되었을 때

처럼, 낮은 이용가능 전력은 개인 식별 디바이스로부터의 데이터가 송신될 수 있는 거리를 감소시킬 수 있다. 그러나, 위에서 설명된 것처럼, 개인 식별 디바이스는 다른 개인 디바이스들과 페어링될 수 있다. 예를 들어, 스마트폰은, 개인 식별 디바이스보다, 복잡한 계산들(암호화 애플리케이션들에서 이용되는 것과 같은)에 대해 더욱 적합한 하드웨어 및 더 큰 배터리를 가지고 있을 수 있고, 그리고 개인 식별 디바이스가 충분한 전력이 부족할 때 데이터를 중계하기 위해 사용될 수 있다. 또한, 개인 식별 디바이스는, 스마트폰보다 많은 계산 전력을 가질 수 있는, 태블릿 컴퓨터들 및 개인 컴퓨터들과 같은, 많은 다른 디바이스들과 페어링될 수 있다. 개인 식별 디바이스가 더 큰 계산 전력, 더 큰 배터리 또는 지속적인 전력원을 갖는 디바이스와 페어링되는 경우, 개인 식별 디바이스는 페어링된 디바이스에 업무를 위임할 수 있다.

[0099] [00102] 도 3은 또 다른 디바이스에 동작들을 오프로드하는 개인 식별 디바이스를 활용하는 시스템의 상호작용을 도시하는 예시적인 다이어그램이다. 도 3은, 개인 식별 디바이스(302), 검출기(304) 및 휴대폰(306)을 포함하는 인증-관련 컴포넌트(300)의 세트를 도시한다. 개인 식별 디바이스(302), 검출기(304), 및 휴대폰(306) 사이의 통신들은 무선 통신들일 수 있다.

[0100] [00103] 단계 A에서, 개인 식별 디바이스(302)는 검출기(304)로부터의 비컨 메시지를 수신한다. 비컨 메시지는 도 1의 단계 A에서 설명된 것처럼 송신될 수 있다. 비컨 메시지는 또한, 개인 식별 디바이스(302)가 검출기(304)로부터의 비컨 메시지에 언제나 응답해야하는지 여부를 포함하는, 위에서 설명된 바와 동일한 또는 유사한 정보를 포함할 수 있다.

[0101] [00104] 단계 B에서, 개인 식별 디바이스(302)는 휴대폰(306)으로 하나 또는 그 초과의 동작들을 위임한다. 위에서 설명된 것처럼, 개인 식별 디바이스(302)를 인증하기 위한 여러 가지의 가능한 구현들이 있다. 몇몇 구현들은, 데이터를 암호화 또는 해독화하는 것과 같은, 계산적으로 비싼 동작들을 포함할 수 있다. 배터리 수명을 보존하거나 또는 전력 소모를 일반적으로 감소시키기 위하여, 개인 식별 디바이스(302)는, 계산적으로 비싼 동작들과 같은, 하나 또는 그 초과의 동작들을 휴대폰(306)에 위임한다. 동작들의 위임을 위하여 이용될 수 있는 휴대폰(306) 또는 다른 디바이스들은 더 파워풀한 하드웨어, 더 큰 배터리들을 포함할 수 있거나 또는 로컬 전력 그리드와 같은, 지속적인 전력원들에 연결될 수 있다. 그러므로, 휴대폰(306) 및 다른 이용가능한 디바이스들은 개인 식별 디바이스(302)보다 동작들을 수행하는데 있어서 더욱 적합할 수 있다.

[0102] [00105] 또한, 단지 계산적으로 비싼 동작들만이 아니라, 다른 동작들도 휴대폰(306)에 위임될 수 있다. 위임되도록 이용가능한 특정 동작들은 구현에 의존하여 변경될 수 있다. 예를 들어, 개인 식별 디바이스(302) 하드웨어(전력원을 포함하는) 및 동작을 위하여 사용되는 데이터를 휴대폰(306)으로 송신하기 위해 사용되는 전력의 양은 어떤 동작들이 위임될 것인지를 결정할 수 있다. 다시 말해, 몇몇 구현들에서, 데이터를 송신하기 위해 사용되는 전력은 특정 동작을 수행하기 위해 사용되는 전력보다 더 클 수 있고, 따라서, 보다 효율적이게 되도록 개인 식별 디바이스(302) 상에서 동작을 수행한다. 몇몇 구현들에서는, 반대가 옳을 수 있고, 따라서 보다 효율적이게 되도록 동작을 휴대폰(306)에 위임한다. 개인 식별 디바이스(302)에 이용가능한 전력의 양과 같은, 다양한 다른 팩터들이 또한 고려될 수 있다. 그러므로, 개인 식별 디바이스(302)가 특정 거리에서 데이터를 송신하기에 충분한 전력만을 갖고 있는 경우, 개인 식별 디바이스(302)는 데이터를 더 멀리 송신할 수 있는 디바이스에 데이터의 송신을 위임할 수 있다.

[0103] [00106] 동작들의 위임을 표시하는, 개인 식별 디바이스(302)로부터 휴대폰(306)으로 송신되는 데이터는 구현들 사이에서 변경될 수 있다. 예를 들어, 송신된 데이터는, 수행할 동작의 표시, 동작에 대한 입력 데이터, 및 위임된 동작의 결과가 송신되어야 하는 곳의 표시를 포함할 수 있다. 몇몇 구현들에서, 입력 데이터는 이미 휴대폰(306) 내에 상주할 수 있다. 예를 들어, 개인 식별 디바이스(302)는 위에서 설명된 것과 같은 "롤링 코드" 기능성을 포함할 수 있다. 휴대폰(306)은 또한 동일한 롤링 코드 기능성을 구현할 수 있고 그리고 개인 식별 디바이스(302)와 동기화 될 수 있어, 두 디바이스들은 주어진 시간에 동일한 코드를 생성한다. 그러므로, 개인 식별 디바이스(302)는 단지, 위임된 동작들로부터 기인하는 데이터가 개인 식별 디바이스(302)에 의해(by)/대하여(for) 사용되어야 함을 휴대폰(306)에 표시할 필요가 있다. 개인 식별 디바이스(302)로부터의 요청에 응답하여, 아래에 설명되는 바와 같이 휴대폰(306)은 데이터를 암호화하고 그리고 이를 개인 식별 디바이스(302)에 송신한다.

[0104] [00107] 단계 C에서, 휴대폰(306)은 위임된 동작들을 수행하고 그리고 위임된 동작의 결과들을 개인 식별 디바이스(302)로 다시 송신한다. 휴대폰(306)은, 특정 네트워킹 프로토콜을 구현하는 것과 유사하게, 표준 피쳐로서 위임된 동작들을 수행하기 위한 기능성을 포함하도록 구현될 수 있다. 몇몇 구현들에서, 휴대폰(306)은, 휴대폰(306) 상에 설치되는 추가적인 소프트웨어 애플리케이션으로서(by way of) 위임된 동작들을 수행하기 위한

기능성을 구현한다.

[0105] [00108] 휴대폰(306)이 개인 식별 디바이스(302)로부터 동작들의 위임을 용이하게 하는 데이터(위임 데이터)를 수신할 때, 휴대폰(306)은 어떤 동작들이 수행되어야하는지를 결정하기 위해 위임 데이터를 분석한다. 예를 들어, 위임 데이터는 특정 값이 특정 암호화 방식을 사용하여 암호화되어야 함을 표시할 수 있다. 그 후 휴대폰(306)은 개인 식별 디바이스(302)에 의해 요청된 것처럼 암호화를 수행할 수 있다. 동작을 수행한 이후에, 휴대폰(306)은 동작들의 결과들을 개인 식별 디바이스(302)로 다시 송신한다.

[0106] [00109] 단계 D에서, 개인 식별 디바이스(302)는 휴대폰(306)으로부터 위임된 동작들의 결과들을 수신한다. 개인 식별 디바이스(302)는, 휴대폰(306)으로부터 수신되는 데이터에 기초하거나 또는 포함하여 검출기(304)로부터 수신되는 비컨 메시지에 대한 응답을 생성한다. 아래에서 설명되는 바와 같이 개인 식별 디바이스(302)는 검출기(304)에 대한 응답을 송신한다.

[0107] [00110] 선택적으로, 단계 E에서, 휴대폰(306)은 개인 식별 디바이스(302)로 결과들을 송신하는 것 대신에 검출기(304)로 위임된 동작들로부터의 결과들을 송신한다. 위에서 설명된 것처럼, 개인 식별 디바이스(302)는 결과들이 송신되어야 하는 곳을 휴대폰(306)에 표시할 수 있다. 예를 들어, 개인 식별 디바이스(302)는 검출기(304)와 연관된 특정 식별기, 검출기(304)와 호환가능한 프로토콜 등을 표시할 수 있다. 위임된 동작들을 수행한 후에, 휴대폰은 결과들을 직접 검출기(304)로 송신할 수 있고, 따라서, 단계들 C 및 D를 제거할 수 있다. 이는 개인 식별 디바이스(302)의 배터리 수명을 더욱 개선할 수 있다. 다시 말해, 몇몇 구현들은 비컨 메시지 응답의 실제 송신을 휴대폰(306)으로 위임하기 위해 개인 식별 디바이스(302)를 위한 능력을 제공할 수 있다. 예를 들어, 개인 식별 디바이스(302)가 데이터를 송신할 수 있는 거리가 낮은 이용가능한 배터리 전력에 의해 제한되는 경우, 개인 식별 디바이스(302)는 데이터의 송신을 휴대폰(306)으로 위임할 수 있다. 그러므로, 휴대폰(306)은 개인 식별 디바이스(302)와 검출기(304) 사이에서 중계기로서 동작할 수 있다.

[0108] [00111] 도 4는 개인 식별 디바이스로부터 또 다른 디바이스로 동작들을 위임하기 위한 예시적인 동작들의 흐름도를 도시한다. 블록(400)에서 시작하여, 개인 식별 디바이스는 현재 동작들이 상당한 전력(예를 들어, 임계값을 넘어서는 전력의 양)을 소모할 것임을 결정한다. 개인 식별 디바이스는, 범용 컴퓨팅 시스템과 비교할 때, 감소된 계산 능력과 같은, 제한된 기능성을 갖도록 설계될 수 있다. 그러므로, 개인 식별 디바이스가 수행하는 동작들의 특정 서브세트가 특히 전력의 상당한 양들을 소모함이 미리 공지될 수 있다. 예를 들어, 특정 암호화 기능성은 프로세싱 전력의 많은 양을 소모할 수 있고, 다른 일반적인 동작들보다 배터리로부터 전력을 더 많이 빼내갈 수 있다. 그러므로, 개인 식별 디바이스는 특정 동작들이 임계값을 넘어서는 전력을 소모할 때를 결정할 수 있다. 개인 식별 디바이스는 또한, 전압 레벨들과 같은, 배터리와 관련된 다양한 통계들을 추적하고 그리고 기록함으로써 동적으로 어떤 동작들이 전력의 상대적으로 많은 양들을 소모하는지 결정하도록 구현될 수 있다. 나아가, 개인 식별 디바이스는 단순히 전력의 많은 양을 소모하는 동작들만이 아니라, 위임을 위한 후보들로서 다른 위임가능 동작들을 고려하도록 구현될 수 있다. 현재 동작들이 상당한 전력을 소모할 것임을 결정한 이후에, 제어는 그 다음에 블록(402)으로 흘러간다.

[0109] [00112] 블록(402)에서, 개인 식별 디바이스는 어떤 디바이스들이 개인 식별 디바이스와 현재 페어링되어 있는지 그리고 페어링된 디바이스들 중 어떤 것이 이용가능한지를 결정한다. 페어링된 디바이스는 개인 식별 디바이스와의 정보 처리 상호 운용(interoperability)을 허용하는 소프트웨어 및/또는 하드웨어를 가지는 디바이스이며, 개인 식별 디바이스와 통신가능하도록 구성된다. 비록 페어링된 디바이스가 개인 식별 디바이스와 통신하는 임의의 디바이스일 수 있지만, 몇몇 동작들의 위임들은, 개인 식별 디바이스의 개인 키와 같은, 민감한 데이터의 전달을 포함할 수 있다. 그러므로, 페어링된 디바이스는 개인 식별 디바이스와 "신뢰성 있는" 접속을 수립해온 디바이스일 수 있고, 여기서 개인 식별 디바이스와 페어링된 디바이스 사이의 통신들은 개인적(private)이다. 그러나, 개인 식별 디바이스는 신뢰성 있는 그리고 신뢰성 없는 디바이스들 모두와 페어링되도록 그리고 신뢰성 없는 디바이스들과 페어링될 때 민감한 데이터를 전달하는 것을 포함하는 동작들을 위임하지 않도록 구현될 수 있다. 추가적으로, 개인 식별 디바이스는 끄는 것에 의해서 또는 범위 밖에 있는 것에 의해서 현재 이용가능하지 않은 디바이스들과 페어링될 수 있다. 그러므로, 개인 식별 디바이스는 페어링된 디바이스들 중 어떤 것이 현재 이용가능한지를 결정한다. 어떤 디바이스들이 현재 페어링되었는지 그리고 이용가능한지를 결정한 이후에, 제어는 그 다음에 블록(404)으로 흘러간다.

[0110] [00113] 블록(404)에서, 개인 식별 디바이스는 어떤 페어링된 디바이스가 위임된 동작들을 수신하기 위하여 가장 적절한지 결정한다. 개인 식별 디바이스는 다수의 팩터들에 기초하여 어떤 페어링된 디바이스가 가장 적절한지 결정할 수 있다. 예를 들어, 배터리에서 전력을 공급받는 것과 지속적인 전력원으로의 접속을 갖는 다른

것, 두 개의 페어링된 디바이스들이 이용가능한 경우, 지속적인 전력원을 갖는 페어링된 디바이스가 가장 적절한 것으로 고려될 수 있다. 개인 식별 디바이스는 또한 페어링된 디바이스들의 프로세싱 전력을 고려할 수 있다. 다시 말해, 랩탑은 휴대폰보다 현재 동작을 위임하기에 보다 적절할 수 있다. 페어링된 디바이스의 현재 선택적인 상태는 어떤 페어링된 디바이스가 위임된 동작들을 수신하는데 가장 적절한지의 결정에 또한 고려될 수 있다. 개인 식별 디바이스는 이미 배터리 수명이 낮은 페어링된 디바이스가 완충된 배터리 수명을 가진 것보다 덜 적절함을 결정할 수 있다. 개인 식별 디바이스에 이용가능한 데이터는 구현들 사이에서 변경될 수 있다. 예를 들어, 개인 식별 디바이스가 상이한 페어링된 디바이스들의 사양들을 상세히 비교할 수 있도록, 몇몇 구현들은 개인 식별 디바이스와 페어링된 디바이스들 사이에서 많은 양들의 메타데이터의 교환을 허용하도록 규정될 수 있다. 반면에, 몇몇 구현들은 매우 적은 메타데이터를 교환하거나 또는 메타데이터를 교환하지 않는 것을 포함하도록 규정될 수 있다. 어떤 페어링된 디바이스가 위임된 현재 동작들을 수신하기 위하여 가장 적절한지 결정한 이후에, 제어는 그 다음에 블록(406)으로 흘러간다.

[0111] [00114] 블록(406)에서, 개인 식별 디바이스는 가장 적절한 페어링된 디바이스로 하나 또는 그 초과의 동작들을 위임한다. 동작들의 위임은 구현들 사이에서 변경될 수 있다. 예를 들어, 페어링된 디바이스 상의 소프트웨어는 개인 식별 디바이스 상에서 수행될 수 있는 동작들을 복제(replicate)하는 기능들을 포함할 수 있다. 그러므로, 개인 식별 디바이스는 기능들에 대한 입력들로서 쓰일 수 있는 데이터를 전송할 수 있고, 페어링된 디바이스로 하여금, 그렇지 않았다면 개인 식별 디바이스가 수행하도록 요구되었을 업무를 수행하는 것을 가능케한다. 다른 구현들은, 페어링된 디바이스 상의 소프트웨어에 의해 실행되는 프로그램 명령들의 세트를 동적으로 생성하는 개인 식별 디바이스를 포함할 수 있다. 하나 또는 그 초과의 동작들을 가장 적절한 페어링된 디바이스에 위임한 이후에, 제어는 그 다음에 블록(408)으로 흘러간다.

[0112] [00115] 블록(408)에서, 개인 식별 디바이스는 선택적으로 위임된 동작들의 결과(들)를 수신한다. 예를 들어, 위임된 동작들이 데이터의 암호화를 포함하는 경우, 개인 식별 디바이스로 리턴되는 결과들은 일반적으로 암호화된 데이터를 포함할 것이다. 몇몇 동작들은 어떠한 데이터도 리턴시키지 않을 수 있다. 예를 들어, 개인 식별 디바이스는 단순히 암호화를 위임하는 것 대신에 암호화 및 암호화된 데이터의 후속적인 송신을 위임할 수 있고, 페어링된 디바이스로부터 데이터를 수신하고, 그 후 개인 식별 디바이스로부터 그것을 송신할 수 있다. 선택적으로 위임된 동작들의 결과들을 수신한 이후에, 프로세스는 종료한다.

[0113] [00116] 예시적인 흐름도들로서, 흐름도들은 예시적인 순서로 상기 본 동작들을 도시하였으며, 실시예들은 상기 예시적인 순서로부터 벗어날 수 있다 (예를 들어, 동작들은 도시된 것과 상이한 순서로 그리고/또는 병렬적으로 수행될 수 있음). 예를 들어, 도 2는 단일 비컨을 전송하고 그리고 개인 식별 디바이스로부터 단일 응답을 수신하는 검출기를 도시한다. 그러나, 특정 구현에 의해 규정된 바와 같이 다수의 메시지들이 주고 받아질 수 있다.

[0114] [00117] 용어 "접속된"이 본원에서 사용된다. 용어 "접속된"은 직접적으로 또는 비직접적으로 커플링된 것을 의미할 뿐만 아니라, 통신적으로 또는 물리적으로 커플링된 것을 의미할 수 있다. 용어 "접속된"은 명시적으로 언급되지 않는 한 접속의 특정 유형으로 제한되지 않는다. 예를 들어, 통신을 가능케하기 위하여 접속되는 컴포넌트들을 설명하기 위해 사용될 때, 그들은 하나 또는 그 초과의 선(wire)들에 직접적으로 연결되거나, 무선 접속을 이용하여 직접적으로 연결되거나, 하나 또는 그 초과의 중간 컴포넌트들을 통하여 연결되거나, 임의의 거리에 걸쳐져 있는 하나 또는 그 초과의 네트워크들을 통해 연결되는 것 등 일 수 있다. 컴포넌트들이 서로 통신할 수 있는 한, 그들은 "접속된"다. 나아가, "접속된" 컴포넌트들은 또한 서로 통합될 수 있으며, 따라서 물리적으로뿐만 아니라 통신적으로도 접속된다.

[0115] [00118] 본원에서 설명된 예제들이 배터리 전력을 포함하는 개인 식별 디바이스를 언급하긴 하지만, 개인 식별 디바이스들은 이에 제한되지 않는다. 몇몇 구현들에서, 개인 식별 디바이스는, 검출기와 같은, 또 다른 디바이스에 의해 송신되는 전자기 신호들에 의해 전력을 공급받는다. 몇몇 구현들에서, 개인 식별 디바이스는, 몇몇 동작들을 대해서는 배터리 전력을 활용하면서, 다른 동작들에 대해서는 또 다른 디바이스에 의해 송신되는 전자기 신호들에 의해 생성된 전력을 사용한다.

[0116] [00119] 나아가, 예시들은 인증을 위하여 사용되는 추가적인 개인 디바이스의 예시로서 휴대폰을 사용하지만, 추가적인 개인 디바이스는, 추가적인 개인 식별 디바이스를 포함하는, 임의이 유형의 디바이스일 수 있다. 다시 말해, 사용자를 인증하기 위해 사용되는 각 디바이스는 "개인 식별 디바이스"로 칭해질 수 있고, 여기서 검출기는 사용자의 진위(authenticity)를 결정하기 위해 하나 또는 그 초과의 개인 식별 디바이스들의 세트와 통신할 수 있다. 인증을 개시하는 개인 식별 디바이스는 1차 개인 식별 디바이스이고, 임의의 제2 개인 식별 디

바이스는 2차 개인 식별 디바이스이고, 임의의 제3 개인 식별 디바이스는 3차 개인 식별 디바이스이고, 이렇게 계속된다.

[0117] [00120] 실시예들은, 전체적으로 하드웨어 실시예, 전체적으로 소프트웨어 실시예(펌웨어, 상주 소프트웨어, 마이크로-코드 등을 포함함) 또는 모두 일반적으로 "회로", "모듈" 또는 "시스템"으로 본원에서 지칭될 수 있는 소프트웨어 양상과 하드웨어 양상을 조합하는 실시예의 형태를 취할 수 있다. 게다가, 발명의 대상의 실시예들은, 임의의 유형의(tangible) 매체로 구현된 컴퓨터 이용가능 프로그램 코드를 갖는 임의의 유형의 매체의 표현으로 구현되는 컴퓨터 프로그램 물건의 형태를 취할 수 있다. 설명된 실시예들은, 모든 상상가능한(conceivable) 변화가 본원에 열거되지는 않았기 때문에, 지금 설명되었건 또는 설명되지 않았건 간에, 실시예들에 따라서 프로세스를 수행하도록 컴퓨터 시스템(또는 다른 전자 디바이스(들))을 프로그래밍하는데 이용될 수 있는 명령들이 저장된 기계-판독가능 매체를 포함할 수 있는 컴퓨터 프로그램 물건 또는 소프트웨어로서 제공될 수 있다. 기계 판독가능 매체는, 기계(예를 들어, 컴퓨터)에 의해 판독가능한 형태(예를 들어, 소프트웨어, 프로세싱 애플리케이션)로 정보를 저장 또는 송신하기 위한 임의의 메커니즘을 포함한다. 기계-판독가능 매체는, 자기 저장 매체(예를 들어, 플로피 디스켓); 광 저장 매체(예를 들어, CD-ROM); 자기-광 저장 매체; ROM(read only memory); RAM(random access memory); 삭제가능한 프로그래머블 메모리(예를 들어, EPROM 및 EEPROM); 플래시 메모리; 또는 전자 명령들을 저장하기에 적합한 다른 유형들의 매체를 포함할 수 있지만, 이에 한정되지 않는다. 또한, 실시예들은, 전기, 광, 음향, 또는 다른 형태의 전파 신호(예를 들어, 캐리어 파형들, 적외선 신호들, 디지털 신호들 등), 또는 유선, 무선, 또는 다른 통신 매체로 구현될 수 있다.

[0118] [00121] 실시예들의 동작들을 수행하기 위한 컴퓨터 프로그램 코드는, Java, Smalltalk, 또는 C++ 등과 같은 객체 지향형 프로그래밍 언어, 및 "C" 프로그래밍 언어 또는 유사한 프로그래밍 언어들과 같은 종래의 절차적 프로그래밍 언어들을 포함하는 하나 또는 그 초과의 프로그래밍 언어들의 임의의 조합으로 기록될 수 있다. 프로그램 코드는, 전체적으로 사용자의 컴퓨터 상에서, 부분적으로 사용자의 컴퓨터 상에서, 독립형(stand-alone) 소프트웨어 패키지로서, 부분적으로는 사용자의 컴퓨터 상에서 그리고 부분적으로는 원격 컴퓨터 상에서, 또는 전체적으로 원격 컴퓨터 또는 서버 상에서 실행할 수 있다. 후자의 시나리오에서, 원격 컴퓨터는 LAN(local area network), PAN(personal area network), 또는 WAN(wide area network)을 포함하는 임의의 타입의 네트워크를 통해서 사용자의 컴퓨터에 접속될 수 있거나, 또는 외부 컴퓨터에 대해 접속이 (예를 들어, 인터넷 서비스 제공자(Internet Service Provider)를 이용하여 인터넷을 통해서) 이루어질 수도 있다.

[0119] [00122] 도 5는 전자 디바이스(500)의 일 실시예의 블록 다이어그램을 도시한다. 몇몇 실시예들에서, 전자 디바이스(500)는, 랩탑 컴퓨터, 태블릿 컴퓨터, 넷북, 모바일 폰, 스마트 기기, 게이밍 콘솔, 라우터, 데스크탑 컴퓨터, 또는 유선 및/또는 무선 통신 능력들을 포함하는 다른 적절한 전자 디바이스일 수 있다. 디바이스(500)는 프로세서 유닛(501)(가능하게는, 다수의 프로세서들, 다수의 코어들, 다수의 노드들을 포함하고, 그리고/또는 멀티-스레딩을 구현하는 등)을 포함한다. 디바이스(500)는 메모리 유닛(507)을 포함한다. 메모리 유닛(507)은 시스템 메모리(예를 들어, 캐시, SRAM, DRAM, 제로 커패시터 RAM, 트윈 트랜지스터 RAM, eDRAM, EDO RAM, DDR RAM, EEPROM, NRAM, RRAM, SONOS, PRAM 등 중 하나 또는 그 초과) 또는 기계-판독가능 저장 매체들의 앞서 이미 설명된 가능한 실현들 중 임의의 하나 또는 그 초과일 수 있다. 디바이스(500)는 또한 버스(503)(예를 들어, PCI, ISA, PCI-Express, HyperTransport®, InfiniBand®, NuBus 등), 및 네트워크 인터페이스(예를 들어, ATM 인터페이스, 이더넷 인터페이스, 프레임 릴레이(Frame Relay) 인터페이스, SONET 인터페이스, 무선 인터페이스 등)를 포함할 수 있는 통신 유닛(505) 및 저장 디바이스(들)(509) (예를 들어, 광학 저장소, 자기 저장소, 등)를 포함한다. 디바이스(500)는 개인 식별 디바이스/검출기 제어 유닛(511)을 포함한다. 몇몇 실시예들에서, 개인 식별 디바이스/검출기 제어 유닛(511)은 위에서 설명한 바와 같은 개인 식별 디바이스의 실시예들을 시행하기 위해 기능성들을 구체화한다. 개인 식별 디바이스/검출기 제어 유닛(511)은 개인 식별 디바이스의 동작들을 용이하게 하는 하나 또는 그 초과의 기능성들을 포함할 수 있다. 몇몇 구현들에서, 개인 식별 디바이스/검출기 제어 유닛(511)은 위에서 설명한 바와 같이 개인 식별 디바이스 검출기의 실시예들을 시행하기 위한 기능성을 구체화한다. 개인 식별 디바이스/검출기 제어 유닛(511)은 개인 식별 디바이스 검출기의 동작을 용이하게 하는 하나 또는 그 초과의 기능성들을 포함할 수 있다. 디바이스(500)는 또한, 개인 식별 디바이스/검출기 제어 유닛(511)과 유사한 제어 유닛을 사용하여, 개인 식별 서비스 컴퓨팅 시스템 또는 본원에서 설명된 임의의 다른 디바이스를 구체화할 수 있다. 이들 기능성들 중 임의의 하나는 하드웨어 내에 그리고/또는 프로세서 유닛(501) 상에서 부분적으로(또는 전체적으로) 시행될 수 있다. 예를 들어, 기능성은 주문형 집적 회로(application specific integrated circuit)로, 프로세서 유닛(501)에 구현된 로직으로, 주변 디바이스 또는 카드 상의 공동-프로세서 등으로 구현될 수 있다. 나아가, 실현들은, 도 5에서 도시되지 않은 적거나 또는 추가적인 컴포넌트들(예를 들어, 비디오 카드들, 오디오 카드들, 추가적 네트워크 인터페이스들, 주변

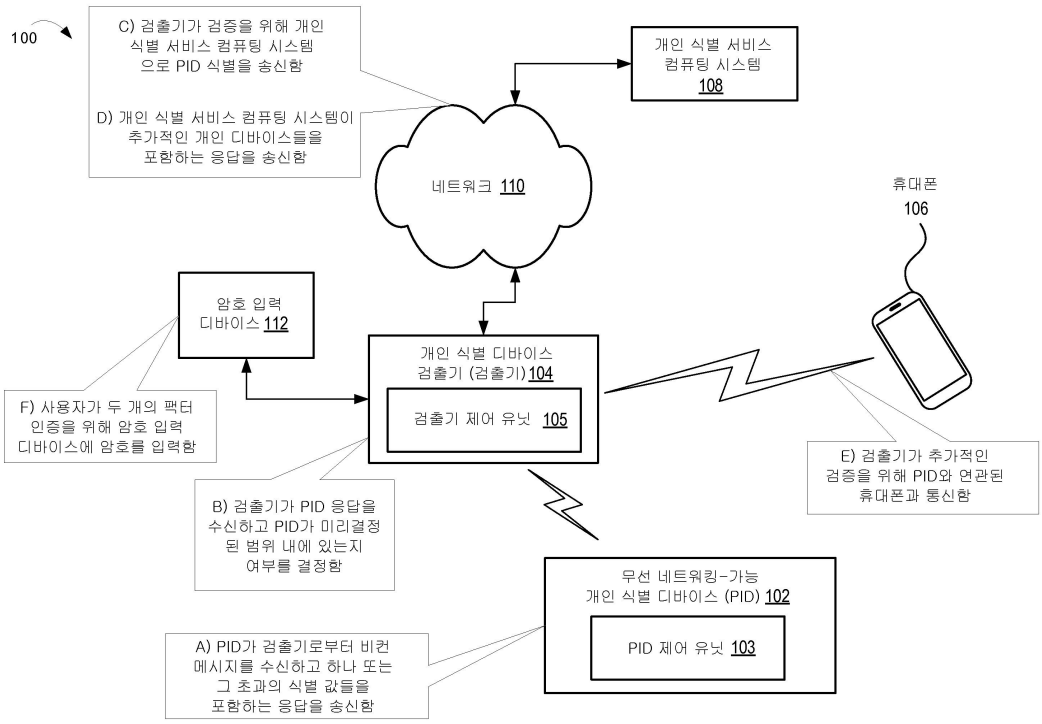
디바이스들, 등)을 포함할 수 있다. 프로세서 유닛(501), 저장 디바이스(들)(509), 및 통신 유닛(505)은 버스(503)에 커플링된다. 버스(503)에 커플링된 것으로 도시되었지만, 메모리 유닛(507)은 프로세서 유닛(501)에 커플링될 수 있다.

[0120] [00123] 실시예들이 다양한 구현들 및 이용들을 참조하여 설명되지만, 이러한 실시예들은 예시적이며, 발명의 대상의 범위는 이들로 제한되지 않는다는 것이 이해될 것이다. 일반적으로, 본원에서 설명된 무선 디바이스들을 위한 기법들은 임의의 하드웨어 시스템 또는 하드웨어 시스템들과 일치하는 설비들로 구현될 수 있다. 수많은 변화들, 변형들, 부가들, 및 개선들이 가능하다.

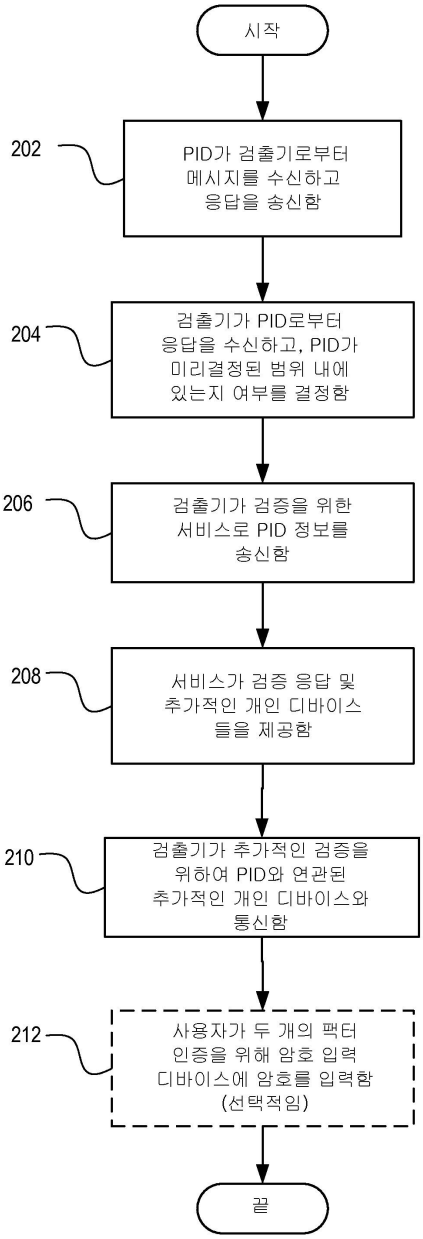
[0121] [00124] 단일의 예시로서 본원에서 설명된 컴포넌트들, 동작들 또는 구조들에 대해 복수의 예시들이 제공될 수 있다. 마지막으로, 다양한 컴포넌트들, 동작들 및 데이터 저장소들 사이의 경계들은 다소 임의적이며, 그리고 특정 동작들은 특정 예시적인 구성들의 맥락에서 예시된다. 기능성의 다른 할당들이 구상되고 그리고 발명의 대상의 범위 내에 포함될 수 있다. 일반적으로, 예시적인 구성들에서 별도의 컴포넌트들로서 제시된 구조들 및 기능성이 조합된 구조 또는 컴포넌트로서 구현될 수 있다. 유사하게, 단일 컴포넌트로서 제시된 구조들 및 기능이 별도의 컴포넌트들로서 구현될 수 있다. 이러한 그리고 다른 변화들, 변형들, 부가들, 및 개선들이 발명의 대상의 범위 내에 포함될 수 있다.

도면

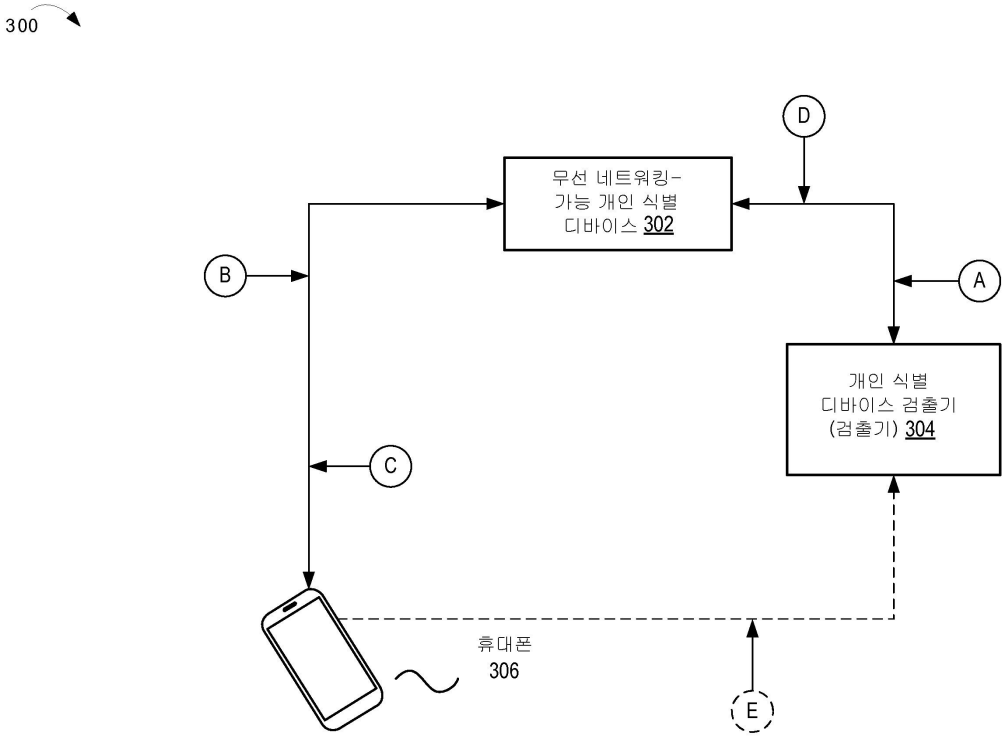
도면1



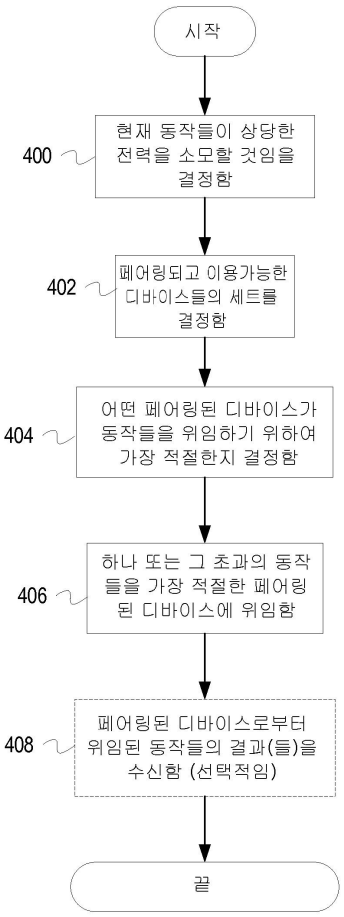
도면2


시작
202
PID가 검출기로부터 메시지를 수신하고 응답을 송신함
204
검출기가 PID로부터 응답을 수신하고, PID가 미리결정된 범위 내에 있는지 여부를 결정함
206
검출기가 검증을 위한 서비스로 PID 정보를 송신함
208
서비스가 검증 응답 및 추가적인 개인 디바이스들을 제공함
210
검출기가 추가적인 검증을 위하여 PID와 연관된 추가적인 개인 디바이스와 통신함
212
사용자가 두 개의 펙터 인증을 위해 암호 입력 디바이스에 암호를 입력함 (선택적임)
끝

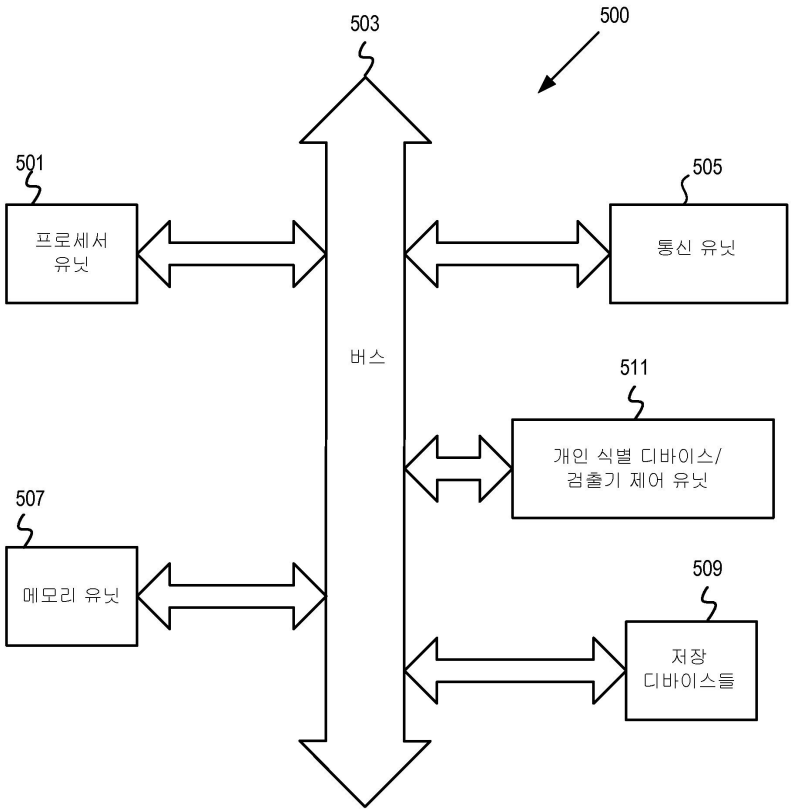
도면3


300
D
무선 네트워킹-
가능 개인 식별
디바이스 302
B
A
개인 식별
디바이스 검출기
(검출기) 304
C
휴대폰
306
E

도면4


시작
400
현재 동작들이 상당한 전력을 소모할 것임을 결정함
402
페어링되고 이용가능한 디바이스들의 세트를 결정함
404
어떤 페어링된 디바이스가 동작들을 위임하기 위하여 가장 적절한지 결정함
406
하나 또는 그 초과의 동작들을 가장 적절한 페어링된 디바이스에 위임함
408
페어링된 디바이스로부터 위임된 동작들의 결과(들)을 수신함 (선택적임)
끝

도면5


503
500
501
프로세서
유닛
505
통신 유닛
버스
511
개인 식별 디바이스/
검출기 제어 유닛
507
메모리 유닛
509
저장
디바이스들