(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년01월02일
(11) 등록번호 10-1216545
(24) 등록일자 2012년12월21일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *H04L 9/32* (2006.01)
G07C 9/00 (2006.01)
(21) 출원번호 10-2009-7019889
(22) 출원일자(국제) 2008년02월25일
심사청구일자 2009년09월23일
(85) 번역문제출일자 2009년09월23일
(65) 공개번호 10-2009-0122968
(43) 공개일자 2009년12월01일
(86) 국제출원번호 PCT/US2008/054900
(87) 국제공개번호 WO 2008/103991
국제공개일자 2008년08월28일
(30) 우선권주장
12/035,309 2008년02월21일 미국(US)
60/891,230 2007년02월23일 미국(US)
(56) 선행기술조사문헌
KR1020020040779 A
US20060253894 A1
WO2001099369 A1
WO2001045319 A1
전체 청구항 수 : 총 70 항

(73) 특허권자
콸콤 인코포레이티드
미국 캘리포니아 샌디에고 모어하우스 드라이브5775 (우 92121-1714)
(72) 발명자
미셸리스, 올리버
미국 92121 캘리포니아 샌디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

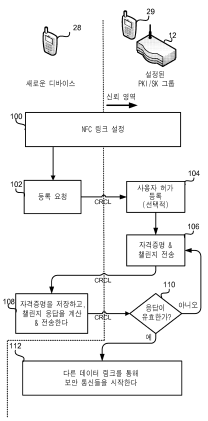
심사관 : 장상배

(54) 발명의 명칭 **접근에 기초한 동적 자격증명 인프라를 배치하기 위한 방법 및 장치**

(57) 요 약

본 발명의 디바이스들 및 방법들은 근거리 통신 링크들, 예를 들어, 니어 필드 통신(NFC) 링크들을 사용하여 통신 디바이스들을 서로 인증하여 신뢰 영역을 생성하거나 새로운 디바이스를 상기 신뢰 영역에 조인시킨다. 2개의 디바이스들이 근거리 통신 피어-투-피어 링크를 설정하면, 디바이스들은 상기 신뢰 영역에 대한 인프라(infrastructure)를 제공하는 자격증명 정보를 교환한다. 이후 매체 또는 원거리 무선 또는 유선 네트워크 통신 링크들은 보안되고 신뢰받은 통신들을 위해 사용된다. 근거리 통신 P2P 링크의 접근 제한들은 상호 신뢰가 신뢰 영역 확장 프로세스에 추가된 보안을 제공하고 보안 및 인증 시그널링에 대한 필요성을 감소시키는디바이스들 사이에 가정되도록 한다. 실시예들은 디바이스들 간의 자격증명 인프라를 확장시키기 위한 다양한 방법들을 제공한다. 또한 실시예들은 단지 두 개의 통신 디바이스들을 함께 터치시킴으로써 구성되는 보안 포인트-투-포인트 통신들을 제공하는 가상케이블들을 간단하게 사용할 수 있게 한다.

대 표 도 - 도2



특허청구의 범위

청구항 1

자격증명(credential) 인프라(infrastructure)를 배치하기 위한 방법으로서,

제 1 디바이스와 신뢰 영역 관리자 간의 초기 통신 링크를 설정하는 단계;

사전로딩(preload)된 자격증명 정보를 상기 초기 통신 링크를 통해 상기 제 1 디바이스로부터 상기 신뢰 영역 관리자로 전송하는 단계;

상기 사전로딩된 자격증명 정보를 확인하는 단계;

상기 제 1 디바이스 및 제 2 디바이스로 하여금 서로 간에 근거리(close range) 통신 링크를 설정하기 위한 명령들을 상기 신뢰 영역 관리자로부터 상기 제 1 디바이스 및 상기 제 2 디바이스에 전송하는 단계;

상기 제 1 디바이스과 상기 제 2 디바이스 간에 상기 근거리 통신 링크를 설정하는 단계;

상기 근거리 통신 링크를 통해 새로운 자격증명 정보를 전송하는 단계; 및

상기 근거리 통신 링크와는 상이한 또다른 통신 링크를 통해 전송되는, 상기 제 1 디바이스와 상기 제 2 디바이스 간의 통신들에 상기 새로운 자격증명 정보를 사용하는 단계를 포함하는,

자격증명 인프라를 배치하기 위한 방법.

청구항 2

제 1 항에 있어서,

상기 새로운 자격증명 정보의 수신을 사용자에게 통지하는 단계

를 추가로 포함하는, 자격증명 인프라를 배치하기 위한 방법.

청구항 3

제 1 항에 있어서,

또다른 별개의 자격증명을 사용하여 사용자의 신원을 확인하는 단계

를 추가로 포함하는, 자격증명 인프라를 배치하기 위한 방법.

청구항 4

제 3 항에 있어서,

상기 별개의 자격증명은 패스워드인,

자격증명 인프라를 배치하기 위한 방법.

청구항 5

제 3 항에 있어서,

상기 별개의 자격증명은 생체(biometric) 데이터인,

자격증명 인프라를 배치하기 위한 방법.

청구항 6

제 1 항에 있어서,

상기 근거리 통신 링크는 니어-필드 통신(near-field communication : NFC) 프로토콜 통신 링크인,

자격증명 인프라를 배치하기 위한 방법.

청구항 7

제 1 항에 있어서,

신뢰 영역에 등록하라는 요청을 상기 제 1 디바이스로부터 상기 제 2 디바이스로 전송하는 단계를 추가로 포함하고,

상기 제 2 디바이스는 이미 상기 신뢰 영역의 멤버이며,

상기 새로운 자격증명 정보는 상기 신뢰 영역 내에서의 통신을 보안하기 위해 사용되는,

자격증명 인프라를 배치하기 위한 방법.

청구항 8

제 7 항에 있어서,

상기 신뢰 영역에 등록하라는 상기 요청을 상기 제 2 디바이스로부터 상기 신뢰 영역 관리자로 포워딩하는 단계;

상기 새로운 자격증명 정보를 상기 신뢰 영역 관리자로부터 상기 제 2 디바이스로 전송하는 단계

를 추가로 포함하고,

상기 근거리 통신 링크를 통해 새로운 자격증명 정보를 전송하는 단계는, 상기 제 2 디바이스가 상기 근거리 통신 링크를 통해 상기 제 1 디바이스로 상기 수신된 새로운 자격증명 정보를 포워딩하는 단계를 포함하는,

자격증명 인프라를 배치하기 위한 방법.

청구항 9

제 8 항에 있어서,

상기 신뢰 영역 관리자에 대해 별개의 자격증명을 제공하도록 상기 제 2 디바이스의 사용자를 프롬프트(prompt)하는 단계;

상기 별개의 자격증명을 상기 신뢰 영역 관리자에게 전송하는 단계; 및

상기 신뢰영역 관리자에서 상기 별개의 자격증명을 검증하는 단계

를 추가로 포함하고,

상기 새로운 자격증명 정보를 상기 제 2 디바이스로 전송하는 단계는 상기 신뢰 영역 관리자에서 상기 별개의 자격증명을 검증하는 단계에 응답하여 성취되는,

자격증명 인프라를 배치하기 위한 방법.

청구항 10

제 1 항에 있어서,

디바이스 자격증명을 상기 제 1 디바이스로부터 상기 제 2 디바이스로 전송하는 단계; 및

상기 디바이스 자격증명을 검증하는 단계

를 추가로 포함하고,

상기 근거리 통신 링크를 통해 새로운 자격증명 정보를 전송하는 단계는 상기 디바이스 자격증명을 검증하는 단계에 응답하여 성취되는,

자격증명 인프라를 배치하기 위한 방법.

청구항 11

제 1 항에 있어서,

상기 제 1 디바이스와 제 3 디바이스 간의 근거리 통신 링크를 설정하는 단계; 및

상기 근거리 통신 링크를 통해 상기 새로운 자격증명 정보를 상기 제 1 디바이스로부터 상기 제 3 디바이스로

전송하는 단계

를 추가로 포함하는,

자격증명 인프라를 배치하기 위한 방법.

청구항 12

이동 디바이스로서,

프로세서;

상기 프로세서에 연결된 제 1 트랜시버;

상기 프로세서에 연결된 제 2 트랜시버 - 상기 제 2 트랜시버는 근거리 통신 트랜시버임 - ; 및

상기 프로세서에 연결된 메모리를 포함하고,

상기 프로세서는

상기 제 1 트랜시버를 통해, 상기 이동 디바이스와 신뢰 영역 관리자 간의 초기 통신 링크를 설정하는 단계;

상기 초기 통신 링크를 통해 상기 이동 디바이스로부터 상기 신뢰 영역 관리자로 사전로딩된 자격증명 정보를 전송하는 단계;

제 1 통신 디바이스와의 근거리 통신 링크를 설정하라는 명령을 상기 신뢰 영역 관리자로부터 수신하는 단계;

상기 제 2 트랜시버를 통해, 상기 이동 디바이스와 상기 제 1 통신 디바이스 간의 상기 근거리 통신 링크를 설정하는 단계;

상기 근거리 통신 링크를 통해 상기 제 1 통신 디바이스로부터 새로운 자격증명 정보를 수신하는 단계; 및

상기 이동 디바이스와 상기 제 1 통신 디바이스 사이에서 상기 제 1 트랜시버를 사용하는 통신 시에 상기 새로운 자격증명 정보를 사용하는 단계를 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

이동 디바이스.

청구항 13

제 12 항에 있어서,

상기 프로세서는 상기 새로운 자격증명 정보의 수신을 상기 이동 디바이스의 사용자에게 통지하는 단계를 추가로 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

이동 디바이스.

청구항 14

제 12 항에 있어서,

상기 프로세서는 상기 이동 디바이스의 사용자를 식별하기 위해 별개의 자격증명을 상기 근거리 통신 링크를 통해 상기 제 1 통신 디바이스로 전송하는 단계를 추가로 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

이동 디바이스.

청구항 15

제 12 항에 있어서,

상기 프로세서는

상기 이동 디바이스의 사용자로부터 패스워드를 수신하는 단계; 및

상기 근거리 통신 링크를 통해 상기 패스워드를 상기 제 1 통신 디바이스에 전송하는 단계를 추가로 포함하는 단계들을 수행하도록 구성되는,

이동 디바이스.

청구항 16

제 12 항에 있어서,

상기 프로세서는

상기 이동 디바이스의 사용자에 관한 생체 데이터를 수신하는 단계; 및

상기 근거리 통신 링크를 통해 상기 생체 데이터를 상기 제 1 통신 디바이스에 전송하는 단계를 추가로 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

이동 디바이스.

청구항 17

제 12 항에 있어서,

상기 프로세서에 연결된 지문 스캐너를 추가로 포함하고,

상기 프로세서는

상기 지문 스캐너로부터 지문 스캔 데이터를 수신하는 단계; 및

상기 근거리 통신 링크를 통해 상기 지문 스캔 데이터를 상기 제 1 통신 디바이스에 전송하는 단계

를 추가로 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

이동 디바이스.

청구항 18

제 12 항에 있어서,

상기 프로세서는

신뢰 영역에 등록하라는 요청을 상기 근거리 통신 링크를 통해 상기 이동 디바이스로부터 상기 제 1 통신 디바이스로 전송하는 단계

를 추가로 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

이동 디바이스.

청구항 19

제 12 항에 있어서,

상기 프로세서는

상기 근거리 통신 링크를 통해 상기 제 1 통신 디바이스로 상기 이동 디바이스의 디바이스 자격증명을 전송하는 단계

를 추가로 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

이동 디바이스.

청구항 20

제 12 항에 있어서,

상기 프로세서는

상기 이동 디바이스와 제 2 통신 디바이스 간의 근거리 통신 링크를 설정하는 단계; 및

상기 근거리 통신 링크를 통해 상기 이동 디바이스로부터 상기 제 2 통신 디바이스로 상기 새로운 자격증명 정보를 전송하는 단계

를 추가로 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

이동 디바이스.

청구항 21

제 20 항에 있어서,

상기 프로세서는

신뢰 영역에 등록하라는 요청을 상기 제 2 통신 디바이스로부터 수신하는 단계;

상기 등록하라는 요청을 상기 제 1 통신 디바이스에 포워딩하는 단계;

사용자 자격증명을 상기 제 1 통신 디바이스에 제공하라는 요청을 수신하는 단계; 및

상기 사용자 자격증명을 상기 제 1 통신 디바이스에 전송하는 단계

를 추가로 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

이동 디바이스.

청구항 22

프로세서-실행가능한 소프트웨어 명령들을 저장하는 컴퓨터-판독가능 매체로서, 상기 프로세서-실행가능한 소프트웨어 명령들은 이동 디바이스로 하여금,

상기 이동 디바이스와 신뢰 영역 관리자 간의 초기 통신 링크를 설정하는 단계;

상기 초기 통신 링크를 통해 상기 이동 디바이스로부터 상기 신뢰 영역 관리자로 사전로딩된 자격증명 정보를 전송하는 단계;

제 1 통신 디바이스와의 근거리 통신 링크를 설정하기 위한 명령을 상기 신뢰 영역 관리자로부터 수신하는 단계;

상기 이동 디바이스와 상기 제 1 통신 디바이스 간의 근거리 통신 링크를 설정하는 단계;

상기 근거리 통신 링크를 통해 상기 제 1 통신 디바이스로부터 새로운 자격증명 정보를 수신하는 단계; 및

상기 근거리 통신 링크와는 상이한 통신 링크를 통해 전송되는, 상기 이동 디바이스와 상기 제 1 통신 디바이스 간의 통신들에 상기 새로운 자격증명 정보를 사용하는 단계

를 포함하는 동작들을 수행하게 하도록 구성되는,

컴퓨터-판독가능 매체.

청구항 23

제 22 항에 있어서,

상기 프로세서-실행가능한 소프트웨어 명령들은 상기 이동 디바이스로 하여금,

상기 새로운 자격증명 정보의 수신을 상기 이동 디바이스의 사용자에게 통지하는 단계

를 포함하는 동작들을 추가로 수행하게 하도록 구성되는,

컴퓨터-판독가능 매체.

청구항 24

제 22 항에 있어서,

상기 프로세서-실행가능한 소프트웨어 명령들은 상기 이동 디바이스로 하여금,

상기 이동 디바이스의 사용자를 식별하기 위해 상기 제 1 통신 디바이스로 상기 근거리 통신 링크를 통해 별개의 자격증명을 전송하는 단계

를 포함하는 동작들을 추가로 수행하게 하도록 구성되는,

컴퓨터-판독가능 매체.

청구항 25

제 22 항에 있어서,

상기 프로세서-실행가능한 소프트웨어 명령들은 상기 이동 디바이스로 하여금,

상기 이동 디바이스의 사용자로부터 패스워드를 수신하는 단계; 및

상기 근거리 통신 링크를 통해 상기 패스워드를 상기 제 1 통신 디바이스에 전송하는 단계

를 포함하는 동작들을 추가로 수행하게 하도록 구성되는,

컴퓨터-판독가능 매체.

청구항 26

제 22 항에 있어서,

상기 프로세서-실행가능한 소프트웨어 명령들은 상기 이동 디바이스로 하여금,

상기 이동 디바이스의 사용자에 관한 생체 데이터를 수신하는 단계; 및

상기 근거리 통신 링크를 통해 상기 생체 데이터를 상기 제 1 통신 디바이스에 전송하는 단계

를 포함하는 동작들을 추가로 수행하게 하도록 구성되는,

컴퓨터-판독가능 매체.

청구항 27

제 22 항에 있어서,

상기 프로세서-실행가능한 소프트웨어 명령들은 상기 이동 디바이스로 하여금,

지문 스캐너로부터 지문 스캔 데이터를 수신하는 단계; 및

상기 근거리 통신 링크를 통해 상기 지문 스캔 데이터를 상기 제 1 통신 디바이스에 전송하는 단계

를 포함하는 동작들을 추가로 수행하게 하도록 구성되는

컴퓨터-판독가능 매체.

청구항 28

제 22 항에 있어서,

상기 프로세서-실행가능한 소프트웨어 명령들은 상기 이동 디바이스로 하여금,

신뢰 영역에 등록하라는 요청을 상기 근거리 통신 링크를 통해 상기 이동 디바이스로부터 상기 제 1 통신 디바이스로 전송하는 단계

를 포함하는 동작들을 추가로 수행하게 하도록 구성되는,

컴퓨터-판독가능 매체.

청구항 29

제 22 항에 있어서,

상기 프로세서-실행가능한 소프트웨어 명령들은 상기 이동 디바이스로 하여금,

상기 근거리 통신 링크를 통해 상기 제 1 통신 디바이스로 상기 이동 디바이스의 디바이스 자격증명을 전송하는 단계

를 포함하는 동작들을 추가로 수행하게 하도록 구성되는,

컴퓨터-판독가능 매체.

청구항 30

제 22 항에 있어서,

상기 프로세서-실행가능한 소프트웨어 명령들은 상기 이동 디바이스로 하여금,

상기 이동 디바이스와 제 2 통신 디바이스 간의 근거리 통신 링크를 설정하는 단계; 및

상기 이동 디바이스로부터 상기 제 2 통신 디바이스로 상기 근거리 통신 링크를 통해 상기 새로운 자격증명 정보를 전송하는 단계를 포함하는 동작들을 추가로 수행하게 하도록 구성되는,

컴퓨터-판독가능 매체.

청구항 31

제 22 항에 있어서,

상기 프로세서-실행가능한 소프트웨어 명령들은 상기 이동 디바이스로 하여금,

제 2 통신 디바이스로부터 신뢰 영역에 등록하라는 요청을 수신하는 단계;

상기 등록하라는 요청을 상기 제 1 통신 디바이스로 포워딩하는 단계;

사용자 자격증명을 상기 제 1 통신 디바이스에 제공하라는 요청을 수신하는 단계; 및

상기 사용자 자격증명을 상기 제 1 통신 디바이스에 전송하는 단계

를 포함하는 동작들을 추가로 수행하게 하도록 구성되는,

컴퓨터-판독가능 매체.

청구항 32

이동 디바이스로서,

상기 이동 디바이스와 신뢰 영역 관리자 간의 초기 통신 링크를 설정하기 위한 수단;

상기 초기 통신 링크를 통해 상기 이동 디바이스로부터 상기 신뢰 영역 관리자로 사전로딩된 자격증명 정보를 전송하기 위한 수단;

제 1 통신 디바이스와의 근거리 통신 링크를 설정하기 위한 명령을 상기 신뢰 영역 관리자로부터 수신하기 위한 수단;

상기 이동 디바이스와 상기 제 1 통신 디바이스 간의 상기 근거리 통신 링크를 설정하기 위한 수단;

상기 근거리 통신 링크를 통해 상기 제 1 통신 디바이스로부터 새로운 자격증명 정보를 수신하기 위한 수단; 및

상기 근거리 통신 링크와는 상이한 또다른 통신 링크를 통해 전송되는, 상기 이동 디바이스와 상기 제 1 통신 디바이스 간의 통신들에 상기 새로운 자격증명 정보를 사용하기 위한 수단을 포함하는,

이동 디바이스.

청구항 33

제 32 항에 있어서,

상기 새로운 자격증명 정보의 수신을 상기 이동 디바이스의 사용자에게 통지하기 위한 수단을 추가로 포함하는,

이동 디바이스.

청구항 34

제 32 항에 있어서,

상기 이동 디바이스의 사용자를 식별하기 위해 상기 제 1 통신 디바이스로 별개의 자격증명을 상기 근거리 통신 링크를 통해 전송하기 위한 수단을 추가로 포함하는,

이동 디바이스.

청구항 35

제 32 항에 있어서,

상기 이동 디바이스의 사용자로부터 패스워드를 수신하기 위한 수단; 및

상기 근거리 통신 링크를 통해 상기 패스워드를 상기 제 1 통신 디바이스에 전송하기 위한 수단을 추가로 포함하는,

이동 디바이스.

청구항 36

제 32 항에 있어서,

상기 이동 디바이스의 사용자에 관한 생체 데이터를 수신하기 위한 수단; 및

상기 근거리 통신 링크를 통해 상기 생체 데이터를 상기 제 1 통신 디바이스에 전송하기 위한 수단을 추가로 포함하는,

이동 디바이스.

청구항 37

제 32 항에 있어서,

지문 스캔 데이터를 획득하기 위해 사용자의 지문을 스캔하기 위한 수단; 및

상기 근거리 통신 링크를 통해 상기 지문 스캔 데이터를 상기 제 1 통신 디바이스에 전송하기 위한 수단을 추가로 포함하는,

이동 디바이스.

청구항 38

제 32 항에 있어서,

신뢰 영역에 등록하라는 요청을 상기 근거리 통신 링크를 통해 상기 이동 디바이스로부터 상기 제 1 통신 디바이스로 전송하기 위한 수단을 추가로 포함하는,

이동 디바이스.

청구항 39

제 32 항에 있어서,

상기 근거리 통신 링크를 통해 상기 제 1 통신 디바이스에 상기 이동 디바이스의 디바이스 자격증명을 전송하기 위한 수단을 추가로 포함하는,

이동 디바이스.

청구항 40

제 32 항에 있어서,

상기 이동 디바이스와 제 2 통신 디바이스 간의 근거리 통신 링크를 설정하기 위한 수단; 및

상기 이동 디바이스로부터 상기 제 2 통신 디바이스로 상기 근거리 통신 링크를 통해 상기 새로운 자격증명 정보를 전송하기 위한 수단을 추가로 포함하는,

이동 디바이스.

청구항 41

제 32 항에 있어서,

신뢰 영역에 등록하라는 요청을 제 2 통신 디바이스로부터 수신하기 위한 수단;

상기 등록하라는 요청을 상기 제 1 통신 디바이스로 포워딩하기 위한 수단;

사용자 자격증명을 상기 제 1 통신 디바이스에 제공하라는 요청을 수신하기 위한 수단; 및

상기 사용자 자격증명을 상기 제 1 통신 디바이스에 전송하기 위한 수단을 추가로 포함하는,

이동 디바이스.

청구항 42

컴퓨터로서,

프로세서;

상기 프로세서에 연결된 제 1 트랜시버;

상기 프로세서에 연결된 제 2 트랜시버 - 상기 제 2 트랜시버는 근거리 통신 트랜시버임 - ;

상기 프로세서에 연결된 메모리; 및

상기 프로세서에 연결된 네트워크 인터페이스를 포함하고,

상기 프로세서는

상기 제 1 트랜시버 또는 상기 네트워크 인터페이스를 통해 제 1 통신 디바이스로부터 사전로딩된 자격증명 정보를 수신하는 단계;

상기 사전로딩된 자격증명 정보를 확인하는 단계;

상기 제 2 트랜시버를 통해 상기 컴퓨터와 상기 제 1 통신 디바이스 간의 근거리 통신 링크를 설정하는 단계;

상기 근거리 통신 링크를 통해 상기 제 1 통신 디바이스에 대해 새로운 자격증명 정보를 제공하는 단계; 및

상기 컴퓨터와 상기 제 1 통신 디바이스 사이에서 상기 제 1 트랜시버를 사용하는 통신 시에 상기 새로운 자격증명 정보를 사용하는 단계

를 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

컴퓨터.

청구항 43

제 42 항에 있어서,

상기 프로세서는

상기 제 1 통신 디바이스의 사용자를 식별하는 별개의 자격증명을 상기 제 1 통신 디바이스로부터 상기 근거리 통신 링크를 통해 수신하는 단계; 및

상기 제 1 통신 디바이스에 대해 새로운 자격증명 정보를 제공하는 단계 이전에 상기 별개의 자격증명을 검증하는 단계

를 추가로 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

컴퓨터.

청구항 44

제 43 항에 있어서,

상기 별개의 자격증명은 패스워드이며,

상기 별개의 자격증명을 검증하는 단계는 디바이스들을 신뢰 영역에 등록하기 위해 허가된 사용자들의 패스워드들의 리스트와 수신된 패스워드를 비교하는 단계를 포함하는,

컴퓨터.

청구항 45

제 43 항에 있어서,

상기 별개의 자격증명은 생체 데이터이고,

상기 별개의 자격증명을 검증하는 단계는 디바이스들을 신뢰 영역에 등록하기 위해 허가된 사용자들의 생체 데이터와 수신된 생체 데이터를 비교하는 단계를 포함하는,

컴퓨터.

청구항 46

제 42 항에 있어서,

상기 프로세서는,

제 2 통신 디바이스를 신뢰 영역에 등록하라는 요청을 상기 제 1 트랜시버 또는 상기 네트워크 인터페이스를 통해 수신하는 단계;

상기 제 1 통신 디바이스에 관련된 별개의 자격증명을 위해 상기 제 1 통신 디바이스로 요청을 상기 제 1 트랜시버 또는 상기 네트워크 인터페이스를 통해 전송하는 단계;

상기 제 1 트랜시버 또는 상기 네트워크 인터페이스를 통해 상기 별개의 자격증명을 수신하는 단계;

상기 별개의 자격증명을 검증하는 단계; 및

상기 별개의 자격증명이 검증된 경우, 상기 제 2 통신 디바이스로의 릴레이를 위해 상기 제 1 트랜시버 또는 상기 네트워크 인터페이스를 통해 상기 제 1 통신 디바이스에 상기 새로운 자격증명 정보를 전송하는 단계

를 추가로 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

컴퓨터.

청구항 47

제 42 항에 있어서,

상기 컴퓨터는 네트워크에 연결된 서버인,

컴퓨터.

청구항 48

제 47 항에 있어서,

상기 서버는 증명서(certificate) 관리자로서 구성되는,

컴퓨터.

청구항 49

제 42 항에 있어서,

상기 컴퓨터는 의료 디바이스인,

컴퓨터.

청구항 50

프로세서-실행가능한 소프트웨어 명령들을 저장하는 컴퓨터-판독가능 매체로서,

상기 프로세서-실행가능한 소프트웨어 명령들은 프로세서로 하여금,

제 1 통신 디바이스로부터 사전로딩된 자격증명 정보를 수신하는 단계;

상기 사전로딩된 자격증명 정보를 확인하는 단계;

상기 프로세서와 제 1 통신 디바이스 간의 근거리 통신 링크를 설정하는 단계;

상기 근거리 통신 링크를 통해 상기 제 1 통신 디바이스에 새로운 자격증명 정보를 제공하는 단계; 및

상기 근거리 통신 링크와는 상이한 통신 링크를 통해 전송되는, 상기 프로세서와 상기 제 1 통신 디바이스 간의 통신에 상기 새로운 자격증명 정보를 사용하는 단계

를 포함하는 동작들을 수행하게 하도록 구성되는,

컴퓨터-판독가능 매체.

청구항 51

제 50 항에 있어서,

상기 프로세서-실행가능한 소프트웨어 명령들은 프로세서로 하여금,

상기 제 1 통신 디바이스의 사용자를 식별하는 별개의 자격증명을 상기 제 1 통신 디바이스로부터 상기 근거리 통신 링크를 통해 수신하는 단계; 및

상기 제 1 통신 디바이스에 새로운 자격증명 정보를 제공하는 단계 이전에 상기 별개의 자격증명을 검증하는 단계

를 추가로 포함하는 단계들을 수행하게 하도록 구성되는,

컴퓨터-판독가능 매체.

청구항 52

제 50 항에 있어서,

상기 프로세서-실행가능한 소프트웨어 명령들은 프로세서로 하여금,

패스워드를 상기 제 1 통신 디바이스로부터 상기 근거리 통신 링크를 통해 수신하는 단계; 및

상기 제 1 통신 디바이스에 새로운 자격증명 정보를 제공하는 단계 이전에, 디바이스들을 신뢰 영역에 등록하기 위해 허가된 사용자들의 패스워드들의 리스트와 수신된 패스워드를 비교함으로써 상기 패스워드를 검증하는 단계

를 추가로 포함하는 단계들을 수행하게 하도록 구성되는,

컴퓨터-판독가능 매체.

청구항 53

제 50 항에 있어서,

상기 프로세서-실행가능한 소프트웨어 명령들은 프로세서로 하여금,

생체 데이터를 상기 제 1 통신 디바이스로부터 상기 근거리 통신 링크를 통해 수신하는 단계; 및

상기 제 1 통신 디바이스에 새로운 자격증명 정보를 제공하는 단계 이전에, 디바이스들을 신뢰 영역에 등록하기 위해 허가된 사용자들의 생체 데이터와 수신된 생체 데이터를 비교함으로써 상기 생체 데이터를 검증하는 단계

를 추가로 포함하는 단계들을 수행하게 하도록 구성되는,

컴퓨터-판독가능 매체.

청구항 54

제 50 항에 있어서,

상기 프로세서-실행가능한 소프트웨어 명령들은 프로세서로 하여금,

제 2 통신 디바이스를 신뢰 영역에 등록하라는 요청을 수신하는 단계;

상기 제 1 통신 디바이스에 관련된 별개의 자격증명을 위해 상기 제 1 통신 디바이스로 요청을 전송하는 단계;

상기 별개의 자격증명을 수신하는 단계;

상기 별개의 자격증명을 검증하는 단계; 및

상기 별개의 자격증명이 검증된 경우, 상기 제 2 통신 디바이스로의 릴레이를 위해 상기 제 1 통신 디바이스로 상기 새로운 자격증명 정보를 전송하는 단계를 추가로 포함하는 단계들을 수행하게 하도록 구성되는,

컴퓨터-판독가능 매체.

청구항 55

컴퓨터로서,

제 1 통신 디바이스로부터 사전로딩된 자격증명 정보를 수신하기 위한 수단;

상기 사전로딩된 자격증명 정보를 확인하기 위한 수단;

상기 컴퓨터와 상기 제 1 통신 디바이스 간의 근거리 통신 링크를 설정하기 위한 수단;

상기 근거리 통신 링크를 통해 상기 제 1 통신 디바이스에 대해 새로운 자격증명 정보를 제공하기 위한 수단; 및

상기 근거리 통신 링크와는 상이한 또다른 통신 링크를 통해 전송되는, 상기 컴퓨터와 상기 제 1 통신 디바이스 간의 통신에 상기 새로운 자격증명 정보를 사용하기 위한 수단을 포함하는,

컴퓨터.

청구항 56

제 55 항에 있어서,

상기 제 1 통신 디바이스의 사용자를 식별하는 별개의 자격증명을 상기 제 1 통신 디바이스로부터 상기 근거리 통신 링크를 통해 수신하기 위한 수단; 및

상기 제 1 통신 디바이스에 대해 상기 새로운 자격증명 정보를 제공하기 이전에, 상기 별개의 자격증명을 검증하기 위한 수단을 추가로 포함하는,

컴퓨터.

청구항 57

제 56 항에 있어서,

상기 별개의 자격증명은 패스워드이며,

상기 별개의 자격증명을 검증하는 단계는, 디바이스들을 신뢰 영역에 등록하기 위해 허가된 사용자들의 패스워드들의 리스트와 수신된 패스워드를 비교하기 위한 수단을 추가로 포함하는,

컴퓨터.

청구항 58

제 56 항에 있어서,

상기 별개의 자격증명은 생체 데이터이며,

상기 별개의 자격증명을 검증하는 단계는, 디바이스들을 신뢰 영역에 등록하기 위해 허가된 사용자들의 생체 데이터와 수신된 생체 데이터를 비교하기 위한 수단을 추가로 포함하는,

컴퓨터.

청구항 59

제 55 항에 있어서,

신뢰 영역에 제 2 통신 디바이스를 등록하라는 요청을 수신하기 위한 수단;

상기 제 1 통신 디바이스와 관련된 별개의 자격증명을 위해 상기 제 1 통신 디바이스로 요청을 전송하기 위한 수단;

상기 별개의 자격증명을 수신하기 위한 수단;

상기 별개의 자격증명을 검증하기 위한 수단; 및

상기 별개의 자격증명이 검증되는 경우, 상기 제 2 통신 디바이스로의 릴레이를 위해 상기 제 1 통신 디바이스로 상기 새로운 자격증명 정보를 전송하기 위한 수단을 추가로 포함하는,

컴퓨터.

청구항 60

제 55 항에 있어서,

네트워크에 접속하기 위한 수단을 추가로 포함하며,

상기 컴퓨터는 서버로서 구성되는,

컴퓨터.

청구항 61

컴퓨터 및 의료 디바이스를 포함하는 의료 모니터링 시스템으로서,

상기 컴퓨터는,

컴퓨터 프로세서;

상기 컴퓨터 프로세서에 연결된 메모리;

상기 컴퓨터 프로세서에 연결된 제 1 트랜시버; 및

상기 컴퓨터 프로세서에 연결된 제 2 트랜시버 – 상기 제 2 트랜시버는 근거리 통신 트랜시버임 – 를 포함하고,

상기 컴퓨터 프로세서는

상기 제 2 트랜시버를 통해 상기 컴퓨터와 제 1 통신 디바이스 간의 근거리 통신 링크를 설정하는 단계,

상기 근거리 통신 링크를 통해 상기 제 1 통신 디바이스에 대해 자격증명 정보를 제공하는 단계, 및

상기 컴퓨터와 상기 제 1 통신 디바이스 사이에서 상기 제 1 트랜시버를 사용하는 통신 시에 상기 자격증명 정보를 사용하는 단계

를 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되고,

상기 의료 디바이스는,

의료 디바이스 프로세서;

상기 의료 디바이스 프로세서에 연결된 제 3 트랜시버; 및

상기 의료 디바이스 프로세서에 연결된 제 4 트랜시버 - 상기 제 4 트랜시버는 근거리 통신 트랜시버임 - 를 포함하고,

상기 의료 디바이스 프로세서는

상기 제 4 트랜시버를 통해 상기 의료 디바이스와 상기 컴퓨터 간의 근거리 통신 링크를 설정하는 단계;

상기 근거리 통신 링크를 통해 상기 컴퓨터로부터 자격증명 정보를 수신하는 단계; 및

상기 의료 디바이스와 상기 컴퓨터 사이에서 상기 제 3 트랜시버를 사용하는 통신 시에 상기 자격증명 정보를 사용하는 단계

를 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

의료 모니터링 시스템.

청구항 62

제 61 항에 있어서,

병원 서버를 추가로 포함하고,

상기 병원 서버는,

서버 프로세서; 및

상기 컴퓨터에 신호들을 전송하고 상기 컴퓨터로부터 데이터를 수신하도록 구성되고, 그리고 네트워크에 연결되는 네트워크 접속 회로를 포함하며,

상기 서버 프로세서는

상기 네트워크를 통해 상기 컴퓨터로 자격증명 정보를 제공하는 단계; 및

상기 네트워크를 통해 상기 병원 서버와 상기 컴퓨터 간의 통신에 상기 자격증명 정보를 사용하는 단계

를 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

의료 모니터링 시스템.

청구항 63

가상 케이블 디바이스로서,

케이블 소켓과의 전기적 접속을 설정하도록 구성된 케이블 커넥터 플러그;

상기 케이블 커넥터 플러그에 전자적으로 연결된 프로세서;

상기 프로세서에 연결된 무선 네트워크 트랜시버; 및

상기 프로세서에 연결된 니어-필드(near-field) 통신 무선 트랜시버를 포함하고,

상기 프로세서는

상기 니어-필드 통신 무선 트랜시버를 통해 상기 가상 케이블 디바이스와 다른 통신 디바이스 간의 니어-필드 통신 링크를 설정하는 단계;

상기 니어-필드 통신 링크를 통해 다른 통신 디바이스로부터 자격증명 정보를 수신하는 단계; 및

상기 가상 케이블 디바이스와 상기 다른 통신 디바이스 사이에서 상기 무선 네트워크 트랜시버를 사용하는 통신 시에 상기 자격증명 정보를 사용하는 단계

를 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

가상 케이블 디바이스.

청구항 64

제 63 항에 있어서,

상기 프로세서는

상기 무선 네트워크 트랜시버를 통해 수신된 자격증명 정보를, 상기 다른 통신 디바이스로부터 제 2 디바이스에 전달하는 단계 - 상기 제 2 디바이스에는 상기 케이블 커넥터 플러그가 삽입됨 -

를 추가로 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

가상 케이블 디바이스.

청구항 65

제 63 항에 있어서,

상기 프로세서는

상기 케이블 커넥터 플러그를 통해 수신된 정보를, 상기 무선 네트워크 트랜시버를 통해 제 2 디바이스로부터 상기 다른 통신 디바이스에 전달하는 단계 - 상기 제 2 디바이스에는 상기 케이블 커넥터 플러그가 삽입됨 -

를 추가로 포함하는 단계들을 수행하기 위한 소프트웨어 명령들로 구성되는,

가상 케이블 디바이스.

청구항 66

제 63 항에 있어서,

상기 다른 통신 디바이스는 또다른 가상 케이블 디바이스인,

가상 케이블 디바이스.

청구항 67

가상 케이블 디바이스로서,

무선 네트워크로 데이터를 무선으로 전달하기 위한 수단;

니어-필드 통신 무선 트랜시버를 통해 상기 가상 케이블 디바이스와 다른 통신 디바이스 간의 니어-필드 통신 링크를 설정하기 위한 수단;

상기 니어-필드 통신 링크를 통해 상기 다른 통신 디바이스로부터 자격증명 정보를 수신하기 위한 수단; 및

상기 무선 네트워크로 데이터를 무선으로 전달하기 위한 수단을 사용하여, 상기 가상 케이블 디바이스와 상기 다른 통신 디바이스 간의 통신에 상기 자격증명 정보를 사용하기 위한 수단을 포함하는,

가상 케이블 디바이스.

청구항 68

제 67 항에 있어서,

상기 제 1 트랜시버를 통해 수신된 정보를, 상기 다른 통신 디바이스로부터 제 2 디바이스로 전달하기 위한 수단 - 상기 제 2 디바이스에는 상기 케이블 커넥터 플러그가 삽입됨 - 을 추가로 포함하는,

가상 케이블 디바이스.

청구항 69

제 67 항에 있어서,

상기 무선 네트워크로 데이터를 무선으로 전달하기 위한 수단을 통해 제 2 디바이스로부터 상기 다른 통신 디바이스로, 상기 케이블 커넥터 플러그를 통해 수신된 정보를 전달하기 위한 수단 - 상기 제 2 디바이스에는 상기

케이블 커넥터 플러그가 삽입됨 - 을 추가로 포함하는,

가상 케이블 디바이스.

청구항 70

시스템으로서,

네트워크;

제 1 트랜시버 및 제 2 트랜시버를 포함하는 제 1 통신 디바이스 - 상기 제 1 트랜시버는 상기 네트워크를 통해 통신하도록 구성되고, 상기 제 2 트랜시버는 근거리 통신 트랜시버임 - ; 및

제 3 트랜시버 및 제 4 트랜시버를 포함하는 제 2 통신 디바이스 - 상기 제 3 트랜시버는 상기 네트워크를 통해 통신하도록 구성되고, 상기 제 4 트랜시버는 근거리 통신 트랜시버임 - 를 포함하고,

상기 제 1 통신 디바이스 및 상기 제 2 통신 디바이스는

상기 제 2 트랜시버 및 제 4 트랜시버를 통해 상기 제 1 통신 디바이스와 상기 제 2 통신 디바이스 간의 근거리 통신 링크를 설정하고;

상기 근거리 통신 링크를 통해 상기 제 1 통신 디바이스와 상기 제 2 통신 디바이스 간에 자격증명 정보를 교환하고;

상기 교환된 자격증명 정보에 기초하여 상기 제 1 트랜시버 및 상기 제 3 트랜시버를 통해 상기 제 1 통신 디바이스와 상기 제 2 통신 디바이스 간의 통신을 설정하도록 구성되는,

시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 컴퓨터 네트워크 통신에 관한 것이며, 더 구체적으로는 접근(proximity)에 기초한 동적 자격증명 인프라를 배치하기 위한 방법들에 관한 것이다.

배 경 기 술

[0002] 본 발명은 출원 번호가 60/891,230이고 출원일이 2008년 2월 23일이고 발명의 명칭이 "Method and Apparatus to Deploy Dynamic Credential Infrastructure Based on Proximity"이며 그 전체 내용이 여기에 참조로 포함되는 미국 가출원에 대한 우선권의 이익을 주장한다.

[0003] 인터넷과 같은 네트워크들을 통한 상거래 양이 계속 증가함에 따라 보안은 더 큰 이슈가 되고 있다. 불행히도, TCP/IP(전송 제어 프로토콜/ 인터넷 프로토콜)와 같은 인터넷에 기반한 프로토콜들은 보안 데이터 전송을 제공하도록 설계되지 않았다. 인터넷은 원래 학술 및 연구 커뮤니티들에서 의견으로 설계되었으며, 네트워크의 사용자들이 비-적대적이며, 협조적인 방식들로 작업한다는 점이 가정되었다. 인터넷이 공중 네트워크로 확산되기 시작함에 따라, 이들 커뮤니티들 외부에서의 사용이 상대적으로 제한되었으며, 새로운 사용자들의 대부분은 큰 회사에 위치한다. 이들 회사들은 인터넷 자체 내로 보안을 구축할 필요가 없었던 다양한 보안 프로시저들, 예를 들어 방화벽들을 사용하여 자신들의 사용자들의 데이터를 보호하기 위한 컴퓨팅 설비들을 가졌다. 그러나, 과거 수년동안, 인터넷 사용은 급증했다. 오늘날 수백만명의 사람들이 규칙적으로 인터넷 및 웹을 사용한다. (이하, 용어 "인터넷" 및 "웹"은 별도로 지시되지 않는 한 유사어로 사용된다.) 이들 사용자들은 전자 메일 메시지들의 교환에서 비즈니스 거래들을 수행하기 위한 정보 검색에 이르기까지 광범위한 작업들을 수행한다. 이들 사용자들은 가정으로부터, 그들의 셀룰러 전화로부터, 또는 다수의 다른 환경들로부터 인터넷에 액세스할 수 있으며, 여기서 보안 프로시저들은 일반적으로 사용가능하지 않다.

[0004] 종종 "전자상거래" 또는 간단히 "e-거래"라고도 지칭되는 인터넷 상에서의 비즈니스의 증가를 지원하기 위해, 용이하게 액세스 가능하면서 저렴한 보안 프로시저들이 개발되어야 했다. 최초의 일반적으로 사용된 보안 수단(measure)은 공개 키 인프라(이하 "PKI")를 포함한다. PKI는 보안 인프라에 대한 기반(basis)으로서 증명서(certificate)들을 사용한다. 증명서들은 공개 키들 및 제 3 자(third party) 검증 엔티티들을 사용하여 서버들이 클라이언트 전송들을 디코딩하고 클라이언트의 신원을 인증하게 한다. 동작시, 네트워크 내의 제 1 노드

는 자신만의 개인 키를 사용하여 메시지를 암호화할 수 있다. 상기 메시지는 제 1 노드의 공개 키를 사용하여 제 2 노드에 의해 판독될 수 있다. 공개 키는 오직 개인 키에 의해 생성된 메시지들을 암호해독하기 위해서만 사용될 수 있으며 메시지들을 암호화하는데 사용될 수 없다. 따라서, 제 1 노드는 자신의 공개 키를 분배하는데 자유롭다. 공개 키들이 분배되는 한 가지 방법은 상기 공개 키들을 증명서들에 포함시킴에 의해서이다. 증명서들에 대한 표준 포맷을 정의하는 X0.509 표준을 포함하는 증명서들에 대한 다수의 표준들이 존재한다. X0.509는 인증을 제공하기 위한 구성(framework)을 정의하는 ITU 제안 및 국제 표준 이다. (93년 11월 자인 "ITU Recommendation X0.509 (1997) Information Technology -- Open Systems Interconnection -- The Directory: "Authentication Framework"를 참조하라. 이 정보 역시 국제 표준 ISDO/IEC 9594-8 (1995)에 공개되어 있다.) 증명서 포맷은 이 표준으로 정의되어 있다. 이 국제 표준에 따라 상기 정의된 포맷으로 생성된 증명서들은 "X0.509 증명서"로 지칭된다.

발명의 상세한 설명

[0005] 다양한 실시예들에서, 접근에 기초하여 동적 자격증명 인프라를 배치하기 위한 방법들, 시스템들 및 디바이스들이 제공된다. 상기 실시예들은 근거리 또는 니어 필드(near-field) 통신 링크의 설정 및 상기 통신 링크를 통한 자격증명된(credentialed) 정보의 전송을 포함한다. 사용자의 신원은 패스워드 또는 생체 데이터와 같은 다른 별개의 자격증명(credential)을 사용하여 검증될 수 있다. 다양한 무선 접근-제한 통신 기술들이 피어-투-피어(P2P) 데이터 링크를 설정하기 위해 이동 디바이스들(예를 들어, 셀 폰, PDA, 및 다른 무선 디바이스들)에 대해 사용될 수 있다. P2P 링크가 무선 접근-제한 통신을 통해 구성된 이후, 보안 자격증명 정보는 원거리 통신을 위해 또는 더 대용량의 데이터의 전달을 위해 사용될 수 있는 BlueTooth® 또는 Wi-Fi와 같은 다른 무선 통신 기술들을 인증하거나 보안하기 위해 사용될 수 있는 링크를 통해 전달될 수 있다. 무선 접근-제한 통신 기술들이 단거리로 제한되므로, 이러한 무선 통신 링크의 자가 설정은 둘 이상의 이동 디바이스들을 근접하게 가져옴으로써 자격증명 정보의 전달 이전에 또는 전달 동안 사용자들이 이동 디바이스들을 인증하게 하는 지각 가능한(intuitive) 메커니즘을 제공한다.

[0006] 여기에 포함되고 본 명세서의 일부분을 구성하는 첨부 도면들은 전술된 일반적인 설명 및 후술될 상세한 설명과 함께 본 발명의 예시적인 실시예들을 설명하며, 본 발명의 특징들을 설명하는 역할을 한다.

실 시 예

[0028] 다양한 실시예들이 첨부 도면들을 참조하여 상세하게 설명될 것이다. 가능하다면, 동일한 참조번호들은 도면 전체에 걸쳐 동일한 또는 유사한 부분들을 지칭하도록 사용될 것이다. 특정 예시들 및 구현예들에 대해 이루어진 참조들은 예시적인 목적이며 본 발명 또는 청구항의 범위를 제한하도록 의도되지 않는다.

[0029] 용어 "예시적인"은 "예, 경우, 예시로서 작용하는" 것을 의미하도록 여기서 사용된다. 여기서 "예시적인" 것으로 설명된 임의의 구현예는 반드시 다른 구현예들보다 바람직하거나 유리한 것으로 해석될 필요는 없다.

[0030] 여기서 사용된 바와 같이, 용어 "이동 디바이스" 및 "핸드헬드 디바이스"는 셀룰러 전화들, 개인 휴대용 디지털 장비(PDA)들, 팜-톱(palm-top) 컴퓨터들, 무선 전자 메일 수신기들 및 셀룰러 전화 수신기들(예를 들어, Blackberry® 및 Treo® 디바이스들), 멀티미디어 인터넷 인에이블된 셀룰러 전화들(예를 들어, iPhone®), 및 프로그램가능 프로세서 및 메모리를 포함하는 유사한 개인용 전자 디바이스들, 근거리 통신 트랜시버 및 무선 네트워크로의 접속을 가능하게 하는 다른 통신 트랜시버 모두 또는 이들 중 임의의 것을 지칭한다. 여기에 사용된 바와 같이, 용어들 "디바이스","통신 디바이스", "무선 디바이스" 및 "무선 통신 디바이스"는 근거리 통신 트랜시버, (유선 또는 무선일 수 있는) 제 2 트랜시버, 및 상기 두 트랜시버들에 연결된 프로세서를 포함하는 전자 디바이스들을 지칭하도록 상호교환가능하게 사용되며, 상기 프로세서는 소프트웨어 명령들을 통해 실시예의 시스템들에 참여하고 실시예의 방법들의 몇몇 단계들을 수행하도록 구성된다. 적합한 디바이스들의 몇몇 예들은 도 1, 15-17 및 20을 참고하여 아래에 더 상세하게 설명되지만, 상기 용어들은 광범위하게 해석되도록 의도되는데, 왜냐하면 상기 실시예들이 예시적인 실시예들의 범위를 초과하는 애플리케이션들 및 구현예들의 넓은 범위에 적용가능하기 때문이다. 몇몇 실시예들은 셀룰러 전화 네트워크들의 셀 타워들을 포함하는 셀룰러 전화 네트워크 시스템을 지칭할 수 있으며, 본 발명 및 청구항의 범위는 예를 들어, 이더넷, WiFi, WiMax, 또는 다른 무선 데이터 네트워크 통신 기술들을 포함하는 임의의 유선 또는 무선 통신 시스템을 포함한다.

[0031] 여기서 사용된 바와 같이, 용어 "신뢰 영역"은 디바이스들이 비밀 정보를 공유하고 보안 방식으로 통신들을 교환하기 위해 서로 "신뢰"할 수 있도록 공통인 또는 관련된 자격증명들을 소유하는 디바이스들의 세트를 지칭한

다. 신뢰 영역의 일 예는 동일한 인증기관(CA; Certificate Authority)에 의해 사인(sign)된 X0.509 증명서들의 세트를 공유하는 한 쌍(또는 그 이상), 즉 PKI의 디바이스들이다. 신뢰영역의 또다른 예는 대칭인 자격증명들을 공유하는 한쌍(또는 그 이상)의 디바이스들이다. 신뢰 영역을 다른 디바이스로 확장하기 위해, 수신 디바이스는 유효한 새로운 멤버로서 검증받을 필요가 있으며, 자격증명들은 보안적으로 교환될 필요가 있다.

[0032] 다양한 실시예들은 디지털 증명서들, 암호화 키들 및 둘 이상의 디바이스들 간의 보안된 유선 또는 무선 통신을 위해 자격증명 인프라(예를 들어, PKI들)를 배치하기 위해 사용될 수 있는 다른 자격증명 데이터와 같은 자격증명 정보를 인증하고 이후 교환하도록 할 필요성을 두 전자 디바이스들에 부과하기 위해 무선 접근-제한 통신 기술들을 사용한다. 다양한 무선 접근-제한 통신 기술들은 이 목적을 위해 사용될 수 있다. 예를 들어, 니어-필드 통신(NFC) 프로토콜 기술들이 사용될 수 있다. NFC 기술 디바이스들은 13.56MHz의 조절되지 않은(unregulated) RF 대역에서 동작하며 기존의 비접촉식 스마트 카드 기술들, 표준들, 및 프로토콜들, 예컨대 FeliCa 및 Mifare에 전적으로 따른다. NFC-인에이블된 디바이스들은 이들 프로토콜들에 따르는 비접촉식 스마트카드들 및 스마트 카드 판독기들과 상호 동작가능하다. NFC 프로토콜 통신들의 유효 범위는 대략 0-20cm(최대 8인치)이며 데이터 통신들은 링크를 사용하는 애플리케이션으로부터의 명령에 의해 또는 통신 디바이스들이 범위 밖으로 이동할 때 종료된다.

[0033] 비접촉식 식별 및 네트워킹 기술들의 조합으로부터의 발전으로, NFC 프로토콜들은 단거리 무선 접속 표준들이 되었다. 다수의 국제 표준들이 NFC 프로토콜들을 위해 설정되었으며, 이들은 예를 들어, ISO/IEC 14443; ISO/IEC 15693; ISO/IEC 18092; ISO/IEC 21481; ISO/IEC 22536; ISO/IEC 23917; ISO/IEC DIS 28361; NFCIP-I라고 지칭되는 ECMA-340; NFCIP-2라고 지칭되는 ECMA-352; ECMA-356; ECMA-362; ECMA-373; ECMA/TC32-TG19/2006/057; NFC-WI; 및 NFC-FEC를 포함한다.

[0034] 그러나, 실시예들 및 청구항들은 NFC 프로토콜들 중 임의의 하나 또는 모두에 반드시 제한되지 않으며, 대신 임의의 근거리(즉, 접근-제한) 무선 통신 링크를 포함할 수 있다. 임의의 무선 접근-제한 통신 기술은 상기 실시예들의 일부에서 사용될 수 있다. 상기 열거된 NFC 프로토콜들 뿐만 아니라, 무선 접근-제한 통신 링크들은 예를 들어 무선 주파수 식별 태그(RFID) 및 IrDA(Infrared Data Association) 프로토콜을 포함한 다른 근거리 통신 매체를 사용해 설정될 수 있다. 또한, 다른 근거리 무선 프로토콜들 및 표준들이 개발될 수 있으며, NFC 프로토콜 디바이스들과 동일한 방식으로 다양한 실시예들에 사용될 수 있다. 또한, 원거리 무선 기술들 및 프로토콜들은 전자 디바이스들을 서로 식별할 목적으로 자신들의 유효 범위들을 제한하는 수정들 및 추가사항들과 함께 사용될 수 있다. 예를 들어,(2.4 GHz 주파수 대역을 사용하여 통신하는) WiFi, BlueTooth® , UWB (초광대역), IEEE 802.15.4, 및 Zigbee® 무선 통신 프로토콜들 및 표준들 역시 범위-제한 특징들과 함께 사용될 수 있다. 예를 들어, 송신기들의 전력은 통신들을 전송하고 수신하기 위해서는 두 개의 디바이스들이 비교적 가까이 근접해(예를 들어, 각각 수 피트 이내에) 있어야 하도록, 인증 통신들에 대해 제한될 수 있다. 또다른 예로서, 인증 통신들이 오직 이러한 신호들의 왕복이 수십 피트 이상으로부터 전송된 신호들을 거절하도록 설정된 임계 미만인 경우에만 발생할 수 있도록 왕복 통신 지연 제한들이 부과될 수 있으며, 이는 2 내지 3피트 떨어진 만큼 짧을 수 있다.

[0035] 액세스, 결제, 발급과 같은 무선 주파수 식별(RFID) 비접촉식 스마트 카드들 지원형의 광범위한 애플리케이션들의 채택의 증가, 및 셀 폰들과 같은 NFC 프로토콜 디바이스들의 상거래 기능과 더불어, RFID를 구비한 이동 디바이스들의 컨버전스에 대한 관심이 증가하고 있다.

[0036] 참조의 간략함을 위해, 다양한 실시예들 및 청구항들은 임의의 그리고 모든 무선 접근-제한 통신 기술들을 포함하기 위해 "근거리 통신" 및 "니어 필드 통신"을 참조한다. 여기서 "근거리 통신 링크(CRCL)" 및 "니어 필드 통신"에 대한 참조는 통신 기술들이 약 3미터(약 12 피트)를 초과하여 자격증명 정보를 교환하지 않을 것을 제외한 어떠한 방식으로든 설명 및 청구항들의 범위를 제한하는 것으로 의도되지 않는다. 바람직한 실시예에서, 통신 범위는 약 1미터(약 3피트) 미만으로 제한되며, 더 바람직한 실시예에서 상기 통신 범위는 약 1 피트 미만으로 제한되며, 일부 실시예들에서 상기 통신 범위는 약 0-20cm(최대 8인치까지)로 제한된다. 이러한 구별을 반영하기 위해, 약 0-20 cm(최대 8인치까지)의 통신 범위를 가지는 링크를 사용하는 실시예들의 설명들은 "NFC 프로토콜" 링크들이라 지칭된다. 따라서, "니어 필드 통신 프로토콜" 및 "NFC 프로토콜" 통신들에 대한 참조는 위에서 열거된 다양한 NFC 프로토콜들 및 표준들에 의해 제공되는 범위를 가지는 통신 트랜시버들 및 기술들로 제한되도록 의도되지만, 또한 유사하게 제한된 통신 범위를 가지는 RFID 트랜시버들 및 기술들을 포함할 수 있다.

[0037] NFC 프로토콜 디바이스들과 같은 근거리 통신들을 사용하여, 용이하고 보안성 있게 정보를 교환하거나 컨텐츠

및 서비스들에 액세스하도록 임의의 두 디바이스들을 서로 접속시키는 것이 가능하다. 솔루션 벤더들은 NFC 프로토콜 시스템의 지각가능한 동작들은 소비자들이 사용하기에 특히 용이한("단순 터치 및 실행") 기술을 만들 것을 주장하지만, 매우 짧은 통신 범위로부터 야기되는 본질적인 보안성은 이러한 시스템들이 모바일 결제 및 금융 거래 애플리케이션들에 이상적이도록 한다. NFC 프로토콜 기술에 친화적인(familiar) 애플리케이션들은 보안 시스템들, 대용량 이체 요금 카드 시스템들, 및 거래를 완료하기 위해 세일 판독기의 포인트에 근접하게 오는 것만이 필요한 스마트 신용 카드들을 구축하는데 사용되는 전자 패스 키들이다.

[0038] 이동 디바이스들 및 소비자 전자 디바이스들을 더 많이 사용하게 되고 많은 서비스들이 사후-판매 형태로 제공될 수 있음에 따라, 자격증명된 인프라(예를 들어, PKI들) 및 유사한 자격증명 사후-제조 배치의 스케일링가능한 방법들가 점점 더 중요해지고 있다. 자격증명 정보의 교환은 다양한 검증된 방법들을 사용하여 처리될 수 있는데, 상기 검증된 방법은 도청, 사기 및 횡령을 방지하기 위한 복잡한 보호법들을 포함할 수 있다. 그러나, 사용자들이 본질적으로 신뢰받게 하도록 두 개의 디바이스들이 근접하여 위치될 수 있거나(즉, 올바른 디바이스 동작이 사용자의 관심사항임), 또는 접근 조건이 신뢰받는 환경(예를 들어, 은행에서의 텔러 창구)에서 설정되거나, 또는 부가적인 자격증명들이 새로운 디바이스로 신뢰 영역의 확장을 허용하도록 사용될 수 있는 시점들이 존재한다. 따라서, 다양한 실시예들은 접근에 의해 가능한 본질적인 보안에 영향을 줌으로써(leveraging) 기존의 자격증명된 인프라의 신뢰 영역을 확장하기 위한 더 간단한 시스템들 및 방법들을 제공한다.

[0039] 개략적으로, 다양한 실시예들은 신뢰 영역을 생성하거나 확장하기 이전에 물리적인 인식을 보장하기 위해 자격증명 정보를 교환하도록 근거리 통신에 영향을 준다. 근거리 니어-필드 통신 기술의 사용은 이미 신뢰 영역에 있는 디바이스와 추가될 새로운 디바이스 간의 물리적인 인식을 설정하는데, 왜냐하면 상기 디바이스들은 가까이에서(예를 들어, NFC 프로토콜 디바이스들을 통해서는 약 8인치 이내에) 접촉될 필요가 있기 때문이다. 이러한 접근 이벤트 시에, 신뢰 영역 내의 디바이스는 새로운 디바이스로 자격증명 정보를 전송하기 위해 무선 프로토콜을 사용한다. 근거리 통신들 및 NFC 프로토콜 링크들은 자격증명들이 인터셉트 또는 간섭에 대한 최소한의 리스크를 가지는 클리어(clear) 상태에서 교환되도록 하는 반면, 무결성-보호되는 그리고/또는 비밀-보호되는 통신들 역시 구현예에 따라 사용될 수 있다. NFC 프로토콜 기술들은 통신 링크를 설정하기 위해 사용자들이 두 개의 디바이스들을 함께 터치해야 하거나 거의(nearly) 터치해야 하는 이러한 단거리들에 제한된다. 따라서, 여기서 접근 이벤트라고 지칭되는 이러한 물리적 동작은 피어-투-피어(P2P) 무선 통신 링크를 설정하기 위한 지각가능한 메커니즘을 제공하며, 사용자들이 새로운 디바이스를 신뢰 영역으로 조인시키기를 원하는 경우, 그들은 새로운 디바이스를 상기 신뢰 영역의 멤버에 단지 터치한다. 다양한 실시예들에서, 이러한 터치-대-통신 메커니즘은 자격증명 데이터를 교환하기 이전에 또는 교환하는 동안 사용자들이 이동 디바이스들을 서로 인증하도록 하는 지각가능한 수단을 제공하도록 영향을 받는다. 두 개(또는 그 이상)의 디바이스들이 더 근거리의 P2P 링크를 설정하여 자격증명 데이터를 교환하면, 더 원거리의 무선(또는 유선) 네트워크 보안 및 신뢰받은 통신들이 상기 자격증명 인프라를 사용하여 설정될 수 있다. 보안 계층의 추가 뿐만 아니라, 다양한 방법들은 신뢰 그룹을 형성하거나 신뢰 그룹에 멤버들을 추가하기 위해 수반되는 보안 및 인증 프로토콜에 대한 필요성을 방지한다(obviate). 근거리 P2P 링크들의 제한된 범위는 일반적으로 상기 링크들이 도청에 의해 공격받지 않게 하고, 원거리 무선 링크들을 통해 신뢰받은 통신으로의 해킹을 시도하는 원치 않는 디바이스들의 발생(issue)들을 회피한다.

[0040] 자격증명 정보의 교환의 일부로서 또는 이에 추가하여, 근거리 통신 링크 역시 신뢰 영역에 의해 사용되는 제 2 유선 또는 무선 통신 링크를 설정하기 위해 요구되는 정보를 교환하는데 사용될 수 있다. 예를 들어, 2개의 디바이스들은 어떠한 추가적인 동기 액티비티 또는 사용자 동작도 없이 BlueTooth® 무선 데이터 링크를 즉시 설정하게 하는데 필요한 어드레스 및 디바이스 식별자 정보를 교환할 수 있다. 또다른 예로서, 2개의 디바이스들은 WiFi 무선 또는 이더넷-기반 네트워크들을 통해 통신을 가능하게 하기 위해 인터넷 프로토콜(IP) 또는 로컬 영역 네트워크 어드레스 정보를 교환할 수 있다. 이러한 방식으로, 접근 이벤트는 어떠한 추가적인 사용자 동작도 요구함이 없이 두 개의 디바이스들이 보안적으로 통신할 수 있음을 보장한다. 따라서, 다양한 실시예들은 둘 이상의 디바이스들이 단지 근접하게 가져옴으로써 사용자들이 보안 신뢰 영역 통신들을 개시하게 하도록 한다.

[0041] 일 실시예에서, 신뢰 영역은 접근 이벤트 및 연관된 근거리 통신 링크를 사용하여 유효 디바이스로서 새로운 멤버를 수용하여 상기 신뢰 영역을 상기 새로운 멤버로 확장할 수 있게 한다. 이는 사용자 통지를 포함할 수 있다. 대안적으로, 상기 신뢰 영역은 사용자 확인과 함께 접근 검출 방법을 사용하여 유효한 디바이스로서 새로운 멤버를 수용하여 상기 신뢰 영역을 상기 새로운 멤버로 확장할 수 있게 한다. 이러한 실시예는 도 2-3을 참조하여 아래에 더 상세하게 설명된다.

[0042] 또다른 실시예에서, 신뢰 영역은 접근 이벤트 및 연관된 근거리 통신 링크 및 또다른 별개의 자격증명을 사용하여 유효한 디바이스로서 새로운 멤버를 수용하여 상기 신뢰 영역을 상기 새로운 멤버로 확장한다. 이러한 실시예는 패스워드, 생체 측정들, 및 다른 외부적으로 제공된 자격증명들을 포함할 수 있다. 이러한 실시예는 도 4-5를 참조하여 아래에서 더 상세하게 설명된다.

[0043] 또다른 실시예에서, 신뢰 영역은 접근 이벤트 및 연관된 근거리 통신 링크 및 새로운 디바이스 상에 이미 설정된 또다른 자격 증명, 예를 들어, 새로운 멤버의 근원(origin)을 검증하기 위해 디바이스 제조자 또는 서비스 공급자의 PKI의 제공을 사용하는 반면, 접근 조건은 추가로 상기 새로운 디바이스를 인증하고 새로운 디바이스에 대한 자격증명들을 전달하는데 사용된다. 이러한 실시예는 도 6-8을 참조하여 아래에 상세하게 설명된다.

[0044] 또다른 실시예에서, 신뢰 영역은 접근 이벤트 및 (예를 들어, 특정 시간 제한 이내의) 두 개의 연속적인 디바이스들의 연관된 근거리 통신 링크를 사용하여 유효한 디바이스로서 새로운 멤버를 수용하고 상기 신뢰 영역을 상기 새로운 멤버로 확장한다. 제 1 디바이스 접촉은 물리적으로 보안된 환경(예를 들어, 은행 고객 서비스 데스크)을 설정하는 반면, 제 2 디바이스 접촉(즉, 접근 이벤트)은 신뢰 영역을 설정하기 위해 사용되는 자격증명을 설정한다. 이러한 실시예는 엔티티의 제공이 다른 비-전자적/비-암호화 수단을 통해(예를 들어, 계약상으로, 소유권 등을 통해) 서비스 엔티티에 의해 신뢰받는 경우 유용할 수 있다. 이러한 실시예는 도 9-10을 참조하여 아래에 더 상세하게 설명된다.

[0045] 다양한 실시예들에서, 접근 조건에서 새로운 멤버가 발견되는 경우, 신뢰 영역 내의 자격증명들의 세트는 이미 존재하고 있을 수 있다. 이러한 환경들에서, 신뢰 영역은 기존의 자격증명들의 세트를 새로운 디바이스로 확장할 수 있다. 대안적으로, 신뢰 영역의 멤버는 접근 조건에서 새로운 멤버의 발견에 의해 트리거링된 새로운 자격증명들의 세트를 생성할 수 있다. 이러한 대안은 도 11-12를 참조하여 아래에 더 상세하게 설명된다.

[0046] 다양한 실시예들에서, 접근 이벤트 역시 신뢰 영역으로부터 디바이스를 제거하는 일부분으로서 사용될 수 있다. 이러한 실시예는 도 13-14를 참조하여 아래에 더 상세하게 설명된다.

[0047] 다양한 실시예들이 예를 들어 셀룰러 데이터 통신 링크들을 채택하는 무선 네트워크를 포함하는, 다양한 유선 및 무선 네트워크들에서 사용될 수 있다. 예를 들어, 도 1은 셀룰러 네트워크를 포함하는 신뢰 영역 통신 네트워크(10)의 블록도를 도시하며, 상기 셀룰러 네트워크에서 일부 이동 셀룰러 디바이스들은 NFC 프로토콜 및 RFID 통신들과 같은 근거리 무선 통신들의 판독기들로서 작용(function)하는 부가 기능을 가진다. 네트워크(10)는 단말(12)을 포함할 수 있으며, 도시된 시스템 내의 상기 네트워크(10)는 셀룰러 베이스 사이트 또는 기지국(BS)(16)으로/으로부터 셀룰러 신호들(2)을 전송하고 수신하기 위한 네트워크 안테나 및 트랜시버로 구성된다. 단말(12)은 또한 근거리 통신 트랜시버를 포함한다. 이러한 예시적인 네트워크(10)에서, 기지국(16)은 이동 교환국(MSC)(18)과 같은 네트워크를 동작시키는데 필요한 엘리먼트들을 포함하는 셀룰러 네트워크의 일부분이다. 동작 시에, MSC(18)는 상기 단말(12)이 셀룰러 데이터 호출들을 발생시키고 수신하는 경우 기지국(16)을 통해 상기 단말(12)로 및 상기 단말(12)로부터 호출들 및 메시지들을 라우팅할 수 있다. 또한, MSC(18)는 상기 단말(12)이 호출에 관련되는 경우, 전화 지상통신선 트렁크(trunk)들(미도시)로의 접속을 제공한다. 또한, MSC는 인터넷(24)에 연결된 서버 게이트웨이(22)에 연결될 수 있지만, 반드시 연결될 필요는 없다.

[0048] 또한 MSC(18)는 유선 네트워크 접속(1)에 의해 네트워크(19), 예를 들어, 로컬 영역 네트워크(LAN), 도심 지역 네트워크(MAN), 및/또는 광역 네트워크(WAN)에 연결될 수 있다. MSC(18)는 유선 네트워크 접속(1)에 의해 직접 네트워크(19)에 연결될 수 있거나, 또는 시스템이 (도시된 바와 같이) 게이트웨이(22)를 포함하는 경우, 상기 MSC는 네트워크(19)로의 유선 네트워크 접속(1)을 가지는 게이트웨이(22)를 통해 네트워크(19)에 연결될 수 있다. 통상적인 실시예에서, MSC(18)는 게이트웨이(22)에 연결되고, 게이트웨이(22)는 인터넷(24)에 연결된다. 차례로, (도시된 바와 같은) 랩톱 컴퓨터(30) 또는 임의의 다른 프로세싱 엘리먼트들(예를 들어, 개인용 컴퓨터들, 서버 컴퓨터들 등)과 같은 전자 디바이스들은 단말 자신만의 고유한 인터넷 접속(9)을 통해 인터넷(24)을 통해 단말(10)에 연결될 수 있다. 추가적인 실시예에서, CA 서버(26)와 연관된 하나 이상의 프로세싱 엘리먼트들은 인터넷(24)을 통해 이러한 네트워크(10)로 연결될 수 있다.

[0049] 셀룰러 네트워크 통신(2) 뿐만 아니라, 단말(12)은 로컬 무선 네트워크(3) 및 근거리 통신 링크(4)를 통해 이동 디바이스들(28, 29, 30)과 같은 다른 디바이스들과 통신하기 위해 구비될 수 있다. 예를 들어, 도 1의 실시예에서, 단말(12)은 제 1 이동 디바이스(28), 제 2 이동 디바이스(29) 및 랩톱 컴퓨터(30)와 통신하도록 구성되고, 각각에는 내부 NFC 프로토콜 트랜시버(예를 들어, NFCIP-2 트랜시버)가 구비된다. 또한 단말(12)은 BlueTooth® 와 같은 다른 원거리 무선 통신 링크 또는 다른 로컬 영역 무선 링크(3)를 통해 이들 디바이스들

(28, 29, 30)과 통신하도록 구성된다. 예를 들어, 단말(12)은 NFCIP-2 NFC 트랜시버 및 IEEE 802.11g 무선 데이터 네트워크 트랜시버를 포함할 수 있다. 유사하게, 도시된 바와 같은 이동 디바이스들(28,29) 및 랩톱 컴퓨터(30)는 호환가능한 NFC 프로토콜 및 로컬 영역(또는 광역) 무선 트랜시버들로 구성된다.

[0050] 단말(12) 내의 근거리 통신 트랜시버들 및 다른 네트워크 디바이스들(28, 29, 30)은 예를 들어, 상기 열거된 NFC 프로토콜들 및 표준들로 정의된 바와 같은 다수의 상이한 근거리 기법들 중 임의의 기법에 따라 데이터를 전송 및/또는 수신할 수 있는 (예를 들어 RFID 태그들을 포함하는) 다수의 상이한 알려진 트랜시버들 중 임의의 트랜시버일 수 있다. 예를 들어, NFC 트랜시버는 NFCIP-1 또는 NFCIP-2 트랜시버, RFID 트랜시버 또는 RFID 태그일 수 있거나, 또는 BlueTooth®(즉, 2.4 GHz 주파수 대역에서의 통신), 적외선, IrDA(Infrared Data Association), UWB(초광대역) 또는 다른 무선 통신 링크들을 사용할 수 있다.

[0051] 또한 단말(12) 및 네트워크 디바이스들(28, 29, 30)은 신뢰 영역 내에서 데이터를 보안상으로 전송하기 위해 사용될 수 있는 제 2 데이터 통신 링크를 포함한다. 예를 들어, 도 1에 도시된 바와 같이, 예를 들어, 제 2 데이터 통신 링크는 IEEE 802.11g 표준에 따른 로컬 영역 무선 링크(3)일 수 있다. 이러한 제 2 데이터 통신 링크는 무선일 필요는 없으며, 예를 들어 링 토큰 네트워크 또는 이더넷 네트워크와 같은 유선 로컬 영역 네트워크(미도시)일 수 있다.

[0052] 이동 디바이스들(28,29) 및 랩톱 컴퓨터들(30) 뿐만 아니라, 네트워크(10) 역시 또는 대안적으로 다른 이동 단말들, 무선 액세서리들(예를 들어 대용량 저장 디바이스, 네트워킹된 프린터들, 모니터들 등), 개인 휴대용 전자 장비(PDA)들, 페이저들, 데스크 톱 컴퓨터들, 의료 디바이스들, 데이터 센서들 및 다른 타입들의 전자 시스템들을 포함하는 다수의 다른 전자 디바이스들 중 어느 하나를 포함할 수 있다.

[0053] 도 1은 신뢰 영역의 멤버들일 수 있는 디바이스들을 도시한다. 예를 들어, 신뢰 영역은 단말(12), 이동 디바이스들(28,29) 및 랩톱 컴퓨터(30) 사이에 설정될 수 있다. 이러한 신뢰 영역의 일 예는 상기 신뢰 영역을 관리하기 위한 허브로서 단말(12)을 사용하는 오피스 네트워킹된 컴퓨터 시스템일 수 있다. 또다른 예로서, 신뢰 영역은 중앙 데이터 프로세서 및 통신 허브(예를 들어, 단말(12))와 통신함으로써 신용 카드들을 원격으로 처리하기 위한 이동 디바이스들(28,29)을 포함할 수 있다. 추가적인 예로서, 신뢰 영역은 중앙 데이터 프로세서 및 통신 허브(예를 들어, 단말(12))로 환자 정보를 전송하고 상기 중앙 데이터 프로세서 및 통신 허브로부터 환자 기록들을 분배하기 위한 이동 의료 보조 PDA들(28, 29) 및 원격 단말들(30)을 포함할 수 있다. 이러한 예들에서, 상기 신뢰 영역은 무선 데이터 링크(3)에 의해 전송된 보안 메시지들을 통해 신뢰받은 디바이스들 내에서 데이터를 공유할 수 있다. 이러한 신뢰 영역 전송들은 이동 디바이스(28) 및 이동 디바이스(29) 간에 예시된 바와 같은 피어-투-피어 링크들일 수 있거나 또는 이동 디바이스들(28,29) 및 랩톱 컴퓨터(30) 사이에 예시된 바와 같이, 단말(12)을 통한 간접적 네트워크 통신들일 수 있다. 또한 이러한 신뢰 영역은 도시된 바와 같이 예를 들어, 인터넷(24)에 직접 접속된 랩톱 컴퓨터(30), 또는 인터넷(24)에 연결된 기지국(16)과 셀룰러 데이터 통신 링크(2)를 통해 통신하는 단말(12)에 의해, 외부 웹사이트들 및 데이터 소스들과 통신할 수 있다. 유사하게, 상기 이동 디바이스들(28,29) 중 하나 이상은 또한 예를 들어 셀룰러 데이터 통신 링크(2)에 의해서와 같이, 기지국(16)과 직접 통신할 수 있다.

[0054] 또한, 도 1에 예시된 아키텍처는 인터넷(24)에 연결된 서버(26)와 같은 원격(distant) 엘리먼트들을 포함하는 신뢰 영역들을 지원한다. 예를 들어, 신뢰 영역은 인터넷(24)을 통해 CA 서버(26)에 의해 관리될 수 있다. 예시된 바와 같이, 상기 신뢰 영역에 대해 의도된 메시지들은 CA 서버(26)로부터 인터넷(24)을 통해 기지국(16)으로 그 다음에 단말(12)로 전송될 수 있다. 단말(12)로부터, 상기 신뢰 영역 메시지들은 로컬 무선 통신 링크들(3)을 통해 다른 그룹 멤버들(28, 29, 30)로 재방송될 수 있다. 이후 상기 신뢰 영역의 임의의 멤버로부터의 메시지들은 반대 방식으로 CA 서버(26)에 라우팅될 수 있다. 유사하게, 상기 신뢰 영역은 인터넷(24)에 연결된 컴퓨터와 같은 단말(12)의 범위를 벗어나 있는 컴퓨팅 디바이스들을 포함할 수 있다. 신뢰 영역 멤버들로의 그리고 상기 신뢰 영역 멤버들 간의 메시지들은 인터넷 분야에 잘 알려진 어드레스지정 방식들 및 IP 어드레스들을 사용하여 각각의 멤버 디바이스에 지시될 수 있다.

[0055] 신뢰 영역으로, 신뢰 영역으로부터, 그리고 신뢰 영역 내에서의 통신을 위한 프로토콜들 및 방법들이 잘 알려져 있지만, 다양한 실시예들은 신뢰 영역을 설정하기 위한 또는 기존의 신뢰 영역에 새로운 멤버들을 조인시키기 위한 새로운 메커니즘들을 제공한다. 근거리 통신 트랜시버들을 단말(12) 및 멤버 이동 디바이스들(28, 29, 30)에 추가함으로써, 이러한 트랜시버들의 접근 제한은 2개의 관련없는 디바이스들, 예를 들어, 단말(12) 및 이동 디바이스(28)가 서로를 인지하게 한다. 따라서, 제 1 이동 디바이스(28)를 상기 단말(12)을 포함하는 신뢰 영역에 추가하기 위해, 상기 제 1 이동 디바이스는 상기 단말(12)에 매우 근접해 오게 된다. 공지된 근거리 통

신 기법들 중 하나를 사용하여, 상기 제 1 이동 디바이스(28) 및 상기 단말(12)은 근거리 데이터 링크(4)를 설정한다. 근거리 데이터 링크(4)를 사용하여, 제 1 이동 디바이스(28)는 신뢰 영역에 조인하라는 요청을 단말(12)에 전송할 수 있다. 디바이스 어드레스지정, 사용자 통지, 및/또는 신뢰 영역 참여 확인과 같은 부가 정보 역시 이 포인트에서 처리될 수 있다.

[0056] 일 실시예에서, 제 1 이동 디바이스(28) 및 단말(12)은 근거리 링크(4) 뿐만 아니라 다른 물리적 링크들, 예를 들어, 802.11g 무선 링크(3) 및 CDMA 셀룰러 데이터 통신 링크(2)를 통한 데이터 접속성을 가진다. 이러한 실시예에서, 신뢰 영역은 802.11g 무선 링크(3), CDMA 셀룰러 데이터 통신 링크(2) 또는 이들 모두를 사용하여 설정될 수 있다. 추가적인 실시예에서, 그룹 디바이스들(예를 들어, 랩톱 컴퓨터(30)) 중 하나 이상은 신뢰 영역 통신들을 위해 사용될 수 있는 유선 네트워크 링크(1)를 포함할 수 있다.

[0057] 각각의 디바이스(12, 28, 29, 30)는 자신의 근거리 통신 트랜시버를 사용하여 새로운 디바이스와 통신하고, 자신의 보안된 통신 링크(예를 들어, 유선, 무선 및/또는 셀룰러 링크들(1, 2 또는 3))를 사용하여 새로운 디바이스가 신뢰 영역에 조인했음을 또는 조인하도록 요청받았음을 상기 신뢰 영역의 다른 멤버들에게 통지하고, 따라서 상기 신뢰 영역을 확장할 수 있다. 따라서, 신뢰 영역이 설정되면, 근거리 통신 성능을 가지는 그룹의 임의의 멤버가 근거리 통신 링크(4)를 설정하기에 충분하도록 새로운 디바이스에 근접하여 위치됨으로써 또다른 디바이스를 상기 그룹에 조인시킬 수 있다. 네트워킹 인증이 두 개의 디바이스들을 근접하게 가져옴으로써 설정되고, 자격증명들, 네트워크 및 신뢰 영역 어드레스들 및 설정 정보가 근거리 통신 링크(4)를 통해 전달되므로, 설정된 신뢰 영역으로 새로운 디바이스를 조인시키는 것은 사용자에게 완전히 명백(transparent)할 수 있다.

[0058] 도 1에 도시된 네트워크(10)는 이동 디바이스들(28,29) 및 네트워크 상의 다른 컴퓨팅 디바이스들, 예를 들어, 랩톱(30) 간의 다양한 접속들을 인에이블시킨다. 예를 들어, 신뢰 영역은 셀룰러 통신 네트워크들(2)에 의해, 로컬 무선 네트워크들(3)에 의해, MSC(18) 및 네트워크(19)를 통해 기지국(16)으로 셀룰러 통신 링크들(2)을 통해 액세스되는 유선 네트워크 접속들(1)에 의해, 그리고 인터넷 접속(9)에 의해 인터넷(24)을 통해 통신할 수 있다. 네트워크 접속들에서의 이러한 유연성은 점선 표기된 통신 심볼들을 사용하여 랩톱(30)에 대해 예시된다. 신뢰 영역이 여기서 설명된 단거리 통신 링크(4)에 의해 인증된 경우, 상기 신뢰 영역 디바이스들은 보안 피어-투-피어 링크들을 통해 직접적으로, 또는 네트워크들(1, 2, 3, 9, 또는 24)을 통해 간접적으로 서로 통신할 수 있다.

[0059] 도 1은 단말(12)이 비이동식 단말임을 도시하지만, 이 디바이스 자체가 이동 디바이스, 예를 들어, 이동 디바이스(29), 랩톱 컴퓨터 또는 이동 카트 상의 개인용 컴퓨터일 수 있다. 예를 들어, 이동 디바이스(29)는 자신, 이동 디바이스(28) 및 랩톱(30)을 포함하는 신뢰 영역의 허브로서 동작할 수 있고, 네트워크 통신들은 셀룰러 데이터 네트워크 링크(2) 및 로컬 영역 무선 링크(3)를 포함한다. 이러한 예에서, 근거리 통신 링크(4)를 설정하기 위해 제 1 이동 디바이스(29)에 충분히 가깝도록 제 2 이동 디바이스(28)를 가져옴으로써 신뢰 영역 멤버십이 확인되면, 상기 신뢰 영역 멤버들로, 상기 신뢰 영역 멤버들로부터, 그리고 상기 신뢰 영역 멤버들 간의 통신들은 잘 알려진 신뢰 영역 통신 방법들 및 프로토콜들에 따라 진행할 수 있다.

[0060] 신뢰 영역으로 조인될 수 있는 각각의 디바이스는 임의의 두 개의 디바이스들이 근접하게 될 때 신뢰 영역의 생성을 자동으로 협상하는 애플리케이션 소프트웨어로 구성될 수 있다. 유사하게, 디바이스들은 설정된 신뢰 영역으로 하나의 디바이스를 자동으로 조인시키기 위한 애플리케이션 소프트웨어로 구성될 수 있으며, 상기 신뢰 영역의 다른 디바이스는 상기 두 개의 디바이스들이 근접하게 될 때의 멤버이다. 근거리 통신 트랜시버들의 통신 성능들을 사용하는 이러한 애플리케이션들은 보안 신뢰 영역들의 설정에 대한 복잡성을 많이 제거할 수 있다. 사용자들이 그룹 식별 및 통신 링크 정보를 하나 이상의 디바이스들로 입력할 필요성은 두 개의 디바이스들이 함께 터치되어야(또는 거의 터치 되어야) 한다는 요건으로 대체된다. 이러한 방식으로, 확장적인 신뢰 영역은 단순히 다양한 멤버 디바이스들을 순차적으로 함께 터치함으로써 신속하게 구성될 수 있다.

[0061] 신뢰 영역을 설정하거나 확장하기 위한 단순한 메커니즘의 제공 뿐만 아니라, 상기 다양한 실시예들은 신뢰 영역 통신, 식별 및 어드레스 정보를 교환하기 위한 보안 메커니즘을 제공한다. 정의에 의해 근거리 통신 링크들(4)은 매우 짧은 거리까지이므로, 상기 통신 링크들은 다른 디바이스들로부터의 도청 및 간섭을 방지한다. 예를 들어, 도 1은 NFC 링크(4)를 설정하기 위해 단말(12)에 충분히 가까운 이동 디바이스(28)를 도시하는 한편, 상기 그룹의 다른 멤버들(예를 들어, 이동 디바이스(29) 및 랩톱 컴퓨터(30))는 상기 통신을 수신하거나 간섭할 수 없다. 자격증명 보안 및 어드레스지정 정보가 광역 통신 링크들(2,3)을 통해 교환되지 않으므로, 디바이스들의 악의적인 조인, 또는 자격증명 정보의 도청자들에의 노출에 대한 낮은 위험성이 존재한다. 따라서, 보안 신뢰 영역은 사용자가 과도한(cumbersome) 보안 프로시저들에 참여해야 할 필요 없이 공개 위치에 신속하게 형

성될 수 있다.

[0062] 도 1은 셀룰러 데이터 네트워크에 기초하는 것으로서 위에서 설명되지만, 동일한 기본 아키텍처가 다른 무선 네트워크 기술들, 예를 들어, WiFi 또는 WiMax 네트워크를 사용하여 구현될 수 있다. 이러한 대안적인 무선 기술들에서, 기지국(16)은 (예를 들어) WiFi 또는 WiMax 기지국일 것이다. 이러한 네트워크(10)의 다른 엘리먼트들은, 단말(12) 및 다른 네트워크 엘리먼트들(28, 29, 30)이 WiFi(또는 다른) 무선 통신 프로토콜을 사용하여 통신하도록 구성될 것인 점을 제외하고는, 상기 설명된 것 그리고 도 1에 도시된 것과 실질적으로 동일할 것이다. 따라서, 대안적인 무선 및 유선 통신 기술 네트워크들을 도시하기 위한 별개의 도면은 불필요하며, 도 1에 도시된 참조 번호들을 사용하는 후속적인 도면들에 있는 컴포넌트들에 대한 참조들은 셀룰러 및 다른 유무선 네트워크 엘리먼트들 모두를 포함하도록 의도된다. 유사하게, 단말(12)은 (랩톱(30)에 연결되어 도시된 유선 네트워크 접속(1)과 유사한) 유선 접속에 의해 로컬 영역 네트워크(19)에 연결될 수 있으며, 셀룰러 네트워크 트랜시버를 포함할 필요는 없다.

[0063] 도 2 및 도 3에 예시된 제 1 실시예에서, 새로운 디바이스(28)는 이동 디바이스(29) 및 단말(12) 사이의 기존의 신뢰 영역에 접속된다. 이러한 신뢰 영역은 당해 기술분야에 잘 알려진 바와 같이 공유된 자격증명 정보(예를 들어, 암호화 키 자격증명들의 PKI 세트)에 기초할 수 있다. 새로운 디바이스(28)가 신뢰 그룹에 조인할 예정인 경우, 상기 새로운 디바이스(28)는 단말(12) 또는 다른 이동 디바이스(29)와 근접하게 되어 근거리 통신 링크가 자동으로 설정된다(단계 100, 메시지 34). 근거리 통신 링크(4)를 설정하는 프로세스는 메시지(34) 내에 포함된 일련의 핸드쉐이킹 통신 교환들을 포함할 수 있다. 예를 들어, 알려진 NFC 프로토콜 링크 설정 방법들 중 임의의 방법이 채택될 수 있다. 설정된 근거리 통신 링크(4)를 통해, 새로운 디바이스(28)가, 예를 들어, 자신의 디바이스 ID 및 표준 요청 메시지인 메시지(36)를 전송함으로써, 신뢰 영역으로의 등록을 요청할 수 있다(단계 102). 응답으로, 수신 디바이스인 단말(12) 또는 이동 디바이스(29)는 근거리 통신 링크(4)를 통해 챌린지 메시지(challenge message)와 함께 보안 자격증명을 상기 새로운 디바이스(28)로 전송할 수 있다(단계 106, 메시지 38). 또한, 이러한 메시지는 이러한 암호화 기술이 사용되는 경우, 보안 자격증명들에 대한 시드 데이터(seed data)를 포함할 수 있다. 자격 증명 및 챌린지 메시지를 수신할 때, 새로운 디바이스는 상기 자격증명 정보를 저장하고, 이후 상기 챌린지에 대한 적절한 응답을 계산하여 상기 응답을 단말 또는 이동 디바이스(29)로 근거리 통신 링크(4)를 통해 다시 전송할 수 있다(단계 108, 메시지 40). 수신 디바이스인 단말(12) 또는 이동 디바이스(29)는 상기 값이 올바른지를 확인하기 위해 상기 챌린지 응답 메시지를 체크한다(테스트 110). 상기 값이 올바른 경우, 이는 상기 자격증명이 정확하게 수신되었으며, 새로운 디바이스(28)에 의해 적절하게 처리되어, 상기 신뢰 영역이 상기 새로운 디바이스(28)로 확장되도록 하여 보안 통신들이 신뢰 영역 데이터 링크를 통해 시작할 수 있음을 나타낸다(단계 112). 그러나, 챌린지 응답이 올바르지 않는 경우, 상기 자격증명이 적절하게 수신되지 못했음을 나타내며, 단말(12) 또는 이동 디바이스(29)는 상기 자격증명을 재전송하고, 단계(106)를 반복하며, 메시지(38)를 재전송할 수 있다.

[0064] 신뢰 영역 자격증명을 전송(단계 106)하기 이전에, 단말(12) 또는 이동 디바이스(29)의 사용자는 등록을 확인응답하고 허가하라는 동작을 수행하도록 요청받을 수 있다(선택 단계 104). 이는 사용자가 예를 들어, 키패드 상의 문자 "Y"를 누름으로써, 또는 패스워드를 입력함으로써, 또는 생체 스캐너를 제출함으로써 사용자가 신뢰 영역을 새로운 디바이스(28)로 확장하는 것을 허가할 수 있는 사람임을 확인하여 새로운 디바이스(28)를 수용하려는 의도를 확인하려는 요청의 형태일 수 있다.

[0065] 이러한 프로세서의 일부, 예를 들어, 신뢰 영역 통신 링크를 통한 통신들의 설정 프로세스에서의 단계(단계 112)로서, 새로운 디바이스(28)의 사용자는 상기 디바이스가 신뢰 영역에 추가되고 있음을 통지받을 수 있다. 이러한 통지는 이동 디바이스 디스플레이 상에 제공된 메시지의 형태일 수 있다. 유사하게, 새로운 디바이스(28)를 신뢰 그룹으로 수용하는 디바이스는, 예컨대 각 디바이스들의 디스플레이 상에 제공될 메시지를 전송함으로써, 상기 새로운 디바이스가 추가되고 있음을 사용자에게 통지할 뿐만 아니라, 상기 신뢰 영역 내의 다른 디바이스들에도 알릴 수 있다.

[0066] 일 실시예에서, 수신 디바이스(즉, 단말(12) 또는 이동 디바이스(29))는 새로운 디바이스(28)로부터의 등록 요청을 수신함이 없이 단계(106) 및 메시지(38)에서, 자격증명 및 챌린지를 제공할 수 있다. 이러한 실시예에서, 근거리 통신 링크를 설정하는 프로세스(단계 100 및 메시지들 34)는 수신 디바이스가 신뢰 영역 자격증명을 확장하게 한다.

[0067] 사용자들의 관점으로부터, 새로운 디바이스(28)를 신뢰 그룹으로 조인시키는 단계들은 예를 들어 단말(12) 또는 이동 디바이스(29)와 같은 신뢰 그룹의 일부분인 디바이스에 새로운 디바이스(28)를 터치하거나 거의 터치하는

단계로만 구성된다(단계 100). 이후 신속하게, 새로운 디바이스(28)의 사용자는 보안 통신들이 인에이블되었다는 통지(예를 들어, 상기 디바이스의 선택적 디스플레이 통지 또는 동작)를 수신한다(단계 112). 따라서, 상기 사용자에게, 새로운 디바이스(28)를 신뢰 그룹으로 조인시키는 프로세스는 더 용이하지 않을 수 있다. 아래에 더 상세하게 설명된 실시예에서와 같이 사용자에게 패스워드 또는 생체 스캔의 입력이 프롬프트된다 할지라도, 자격증명들을 배치하고 검증하며 보안 통신 기능들을 확인하는 복잡성은 사용자에게 노출되지 않는다.

[0068] 일 실시예에서, 신뢰 영역은 예를 들어 CA 서버(26)와 같은 신뢰 영역 내의 서버에 의해 관리될 수 있다. 새로운 디바이스(28)를 이러한 신뢰 영역으로 수용하기 위한 예시적인 프로세스들 및 메시지들이 도 4 및 도 5에 설명된다. 이러한 예에서, 보안된 통신들은 신뢰 영역의 멤버들(예를 들어, 단말(12) 및 이동 디바이스(29)) 및 CA 서버(26)들 사이에 이미 설정된다(메시지 42a). 위에서 설명된 실시예와 유사하게, 새로운 디바이스(28)가 설정된 신뢰 영역에 추가될 예정인 경우, 새로운 디바이스(28)는 근거리 또는 NFC 통신 링크를 설정하기 위해 상기 신뢰 영역의 멤버(예를 들어, 단말(12) 및 이동 디바이스(29))에 근접하게 된다(단계 100, 메시지 34). 근거리 통신 링크가 설정되면, 새로운 디바이스(28)는 신뢰 영역으로의 등록을 요청한다(단계 102, 메시지 36). 이러한 실시예에서, 신뢰 영역 내의 멤버십은 CA 서버(26)에 의해 관리되며, 따라서, 등록 요청의 수신시, 수신 디바이스(예를 들어, 단말(12) 또는 이동 디바이스(29))는 상기 요청을 CA 서버(26)에 포워딩한다(단계 114, 메시지 44). 수신 디바이스가 신뢰 영역 내에 있었으므로, 등록 요청을 포워딩하는 메시지는 보안된 무선 또는 유선 네트워크 통신을 사용하여 CA 서버(26)로 전송될 수 있다. CA 서버(26)는 상기 요청을 수신하고, 상기 요청과 함께 제공된 임의의 디바이스 정보를 확인하고, 새로운 디바이스(28)를 신뢰 영역에 추가하라는 상기 요청을 확인한다(단계 116).

[0069] CA 서버(26)가 새로운 통신 디바이스(28)와 통신 접촉 상태 또는 근접 상태가 아니므로, 상기 CA 서버(26)는 새로운 디바이스(28)의 조인에 대한 동의를 표시하기 위해 다른 자격증명을 입력하도록 상기 디바이스의 사용자에게 요구하는 요청을 상기 등록 요청을 포워딩했던 디바이스(예를 들어, 단말(12) 및 이동 디바이스(29))로 전송할 수 있다(단계 118, 메시지(46)). 이러한 신뢰 영역 내의 사용자로부터의 제 2 자격증명에 대한 요청은 신뢰 그룹의 보안 통신 링크를 사용하여 전송될 수 있다. 이러한 요청은 단순히 사용자 확인 동작(예를 들어, 사용자가 동의하는 경우 문자 "Y" 키를 누르라는 요청)에 대한 것, CA 서버(26)에 알려진 패스워드의 엔트리, 생체 스캔의 엔트리(예를 들어, 사용자의 디바이스 내에 포함된 지문 스캐너를 통해 사용자의 지문을 스캔하라는 요청)에 대한 것, 또는 CA 서버(26)가 새로운 디바이스(28)를 신뢰 영역에 추가하는 것에 사용자가 동의함을 표시하는 것으로 인식할 수 있는 일부 다른 자격증명에 대한 것일 수 있다. 응답으로, 단계 118에서, 사용자는 CA 서버(26)에 전송된 요청된 동작을 수행한다(메시지 48). 다시, 이러한 제 2 사용자 자격증명은 신뢰 영역의 보안된 통신 네트워크를 통해 전송될 수 있다.

[0070] CA 서버(26)는 이후 사용자의 제 2 자격증명을 확인한다(단계 120). 제 2 자격증명은 다양한 알려진 방법들을 사용하여 확인될 수 있다. 예를 들어, 상기 제 2 자격증명이 패스워드인 경우, CA 서버(26)는 새로운 디바이스들을 신뢰 영역으로 수용하기 위해 허가된 개인들에 할당된 패스워드들의 리스트(예를 들어, 데이터베이스 리스팅)와 수신된 패스워드를 비교할 수 있다. 예를 들어, 예를 들어, 은행 내에 대출 관계자들과 같은, 기관 내의 특정 개인들 또는 회사 내의 정보 기술(IT) 전문가들은 랩톱 컴퓨터들 또는 새로운 하드웨어 설비들과 같은 새로운 디바이스들에 대한 자격증명 정보를 분배하도록 허가될 수 있다. 새로운 디바이스를 신뢰 영역에 추가하는 것이 신뢰받은 개인에 의해 시작되는 중임을 보장하기 위해, CA 서버는 이러한 개인들에 할당된 할당된 패스워드들의 리스트로 구성될 수 있다. 더 높은 보안 레벨을 제공하기 위해, 이러한 신뢰받은 개인들에 할당된 이동 디바이스들은 지문 스캐너(179)(도 15 참조)와 같은 생체 센서들로 구성될 수 있으며, 허가된 사용자들의 생체 데이터는 CA 서버(26) 상의 데이터베이스에 저장된다. 이러한 구현예들에서, CA 서버(26)는 새로운 디바이스(28)의 신뢰 영역으로의 추가를 요청하는 사용자가 상기 사용자의 이동 디바이스(29)로부터 수신된 생체 데이터와 CA 서버(26) 상에서 유지되거나 상기 CA 서버(26)에 의해 액세스 가능한 데이터베이스에 저장된 허가된 사용자들의 생체 데이터를 비교함으로써 상기 추가를 수행하도록 허가됨을 검증할 수 있다.

[0071] CA 서버(26)가 사용자의 제 2 자격증명을 확인하는 경우, 상기 CA 서버(26)는 새로운 디바이스(28)로 전달될 상기 자격증명을 전송한다(단계 122, 메시지 50). 이러한 자격증명 메시지는 예를 들어, 단말(12) 또는 이동 디바이스(29)와 같은 초기 레지스터들 요청을 수신했던 신뢰 영역의 멤버에게 전송된다. 대안적으로, CA 서버(26)는 단순히 수신 디바이스(예를 들어, 단말(12) 및 이동 디바이스(29))가 신뢰 영역을 설정하기 위해 사용된 자격증명에 대해 포워딩하도록 허가할 수 있다. 이후, 상기 디바이스는 상기 자격증명을 챌린지 메시지와 함께 새로운 디바이스(28)에 전송한다(단계 106, 메시지 38). 새로운 디바이스(28)가 아직 상기 신뢰 영역의 멤버가 아니므로, 자격증명 및 챌린지 메시지는 근거리 통신 링크를 통해 전송된다. 도 2를 참조하여 위에서 설명된

바와 같이, 새로운 디바이스(28)는 상기 자격증명을 저장하고, 상기 챌린지에 대한 적절한 응답을 계산하고, 상기 챌린지 응답을 근접한 신뢰 영역의 멤버(예를 들어, 단말(12) 또는 이동 디바이스(29))에게 다시 전송한다(단계 108, 메시지 40). 수신 디바이스는 상기 값이 올바른지를 확인하기 위해 챌린지 응답 메시지를 체크한다(테스트 110). 상기 값이 올바른 경우, 이는 자격증명이 정확하게 수신되었으며, 새로운 디바이스(28)에 의해 적절히 처리되어, 상기 신뢰 영역이 새로운 디바이스(28)로 확장되도록 하여 보안 통신들이 신뢰 영역 데이터 링크를 통해 시작될 수 있음을 나타낸다(단계 112, 메시지들 42a, 42b). 그러나, 챌린지 응답이 올바르지 않는 경우, 상기 자격증명이 적절히 수신되지 않았음을 나타내며, 단말(12) 또는 이동 디바이스(29)는 상기 자격증명을 재전송하고, 단계(106)를 반복하고, 메시지(38)를 재전송할 수 있다.

[0072] 일 실시예에서, 수신 디바이스(즉, 단말(12) 또는 이동 디바이스(29))는 새로운 디바이스(28)로부터의 등록 요청의 수신 없이 새로운 디바이스(28)의 등록 요청을 CA 서버(26)로 포워딩할 수 있다(단계 114, 메시지 44). 이 실시예에서, 근거리 통신 링크 설정의 프로세스(단계 100, 메시지들 34)은 수신 디바이스로 하여금 새로운 디바이스(28)가 신뢰 영역으로 조인하려고 시도함을 CA 서버(26)에 통지하도록 할 수 있다. 이러한 자동 통지는 CA 서버(26)가 새로운 디바이스(28)의 추가를 확인하도록 하고(단계 116), 상기 디바이스(28)의 상기 신뢰 영역으로의 추가에 동의하기 위해 자격증명을 입력하도록 상기 수신 디바이스에 요청하기에 충분할 수 있다(단계 118).

[0073] 일부 경우들에서, 새로운 이동 디바이스(28)는 원래의 장비 제조자 또는 서비스 공급자에 의해 디바이스에 저장된 자격증명 정보, 예를 들어, 디지털 서명을 포함할 수 있다. 이러한 자격증명 정보는 새로운 디바이스가 신뢰 영역에 추가되어야할지의 여부를 결정하기 위해 신뢰 영역 관리자(예를 들어 CA 서버(26))를 인에이블시키는데 유용할 수 있다. 이러한 자격증명 정보는 예를 들어 PKI 방법들을 포함하는 임의의 알려진 방법을 사용하여 검증될 수 있다. 따라서, 도 6-8에서 예시된 실시예에서, 새로운 디바이스(28) 상에 저장된 자격증명은 디바이스를 신뢰 영역으로 추가할지의 여부를 결정하는 프로세스의 일부분으로서 확정된다. 도 6을 참조하여, 일 실시예에서, 새로운 이동 디바이스(28)는 근거리 통신 링크를 설정하기 위해 설정된 신뢰 영역의 멤버에 근접하도록 오게 된다(단계 100). 상기 새로운 디바이스(28)는 이후 자신의 사전로딩된 자격정보를 등록 요청과 함께 근거리 통신 링크를 통해 상기 설정된 신뢰 영역의 멤버에게 전송한다(단계 102). 이러한 메시지는 디바이스의 자격증명 정보의 추가와 함께 도 3에 예시된 등록 요청 메시지(36)와 유사하다. 자격증명의 수신시, CA 서버(26)와 같은 신뢰 영역의 멤버는 PKI 방법들과 같은 알려진 방법들을 사용하여 상기 자격증명을 확인한다(단계 124). 상기 자격증명이 유효한 경우, CA 서버(26)와 같은 신뢰 영역은 상기 새로운 디바이스(28)의 근원을 확인할 수 있고 챌린지 요청과 함께 자격증명 정보를 발생하도록 진행할 수 있다(단계 106). 이후 이러한 방법은 단계들(108, 110 및 112)에 대해 도 2 및 3을 참조하여 위에서 설명된 방식으로 계속한다.

[0074] 제 2 실시예에서, 새로운 디바이스(28)는 자신의 사전로딩된 자격증명 정보를 사용하여 CA 서버(26)와의 제 1 통신 링크를 보안할 수 있으며, 이후 새로운 서비스를 수신하기 위해 신뢰 영역으로의 엔트리를 요청할 수 있다. 도 7 및 8에 예시된 바와 같이, 새로운 디바이스(28)는 CA 서버(26)와 보안된 유선 및 무선 통신 링크를 사전 로딩된 자격증명을 사용하여 설정할 수 있다(단계 126, 메시지 52). 이후 이러한 보안 링크를 사용하여, 새로운 디바이스(28)는 새로운 서비스에 대한 등록을 요청할 수 있다(단계 128, 메시지 54). 응답으로, CA 서버(26)는 새로운 디바이스(28)의 자격증명을 확인할 수 있다(단계 130). 새로운 디바이스(28) 자격증명이 확인되는 경우, CA 서버(26)는 새로운 디바이스(28) 및 새로운 서비스를 포함하는 신뢰 영역 내의 다른 디바이스 예를 들어, 단말(12)로 근거리 통신 링크로 진입하라는 명령을 전송할 수 있다(단계 132, 메시지들 56a 및 56b). 이후 근거리 통신 링크를 설정하기 위한 명령을 수신하는 새로운 디바이스의 사용자(및/또는 단말(12)의 사용자)는 상기 디바이스가 단말(12)에 근접하게 오게 할 수 있다(단계 100, 메시지들 34). 근거리 통신 링크가 설정되면, 새로운 디바이스(28)는 근거리 통신 링크를 통해 단말(12)로 등록 요청을 전송할 수 있다(단계 102, 메시지 36). 이후 상기 단말(12)은 접근 이벤트가 새로운 디바이스(28)를 통해 발생했음을 나타내는 확인 메시지를 CA 서버(26)로 포워딩할 수 있다(단계 115, 메시지 58). 그 응답으로, CA 서버(26)는 새로운 디바이스(28)에 의해 사용될 자격증명을 상기 단말(12)에 제공할 수 있다(단계 122, 메시지 60). 이러한 점에서, 상기 방법 및 메시지들은 도 4 및 5를 참조하여 실질적으로 위에서 설명된 바와 같이 새로운 디바이스(28)를 포함하는 신뢰 영역을 확장하도록 진행한다.

[0075] 추가적인 실시예에서, 여기서 설명된 방법들 및 시스템들은 CA 서버(26)로부터 제 1 디바이스(29)로, 이후 제 2 디바이스(28) 상으로 (등등) 신뢰 영역을 확장시키기 위해 사용될 수 있다. 도 9-10에서 예시된 바와 같이, 제 1 이동 디바이스(29)는 근거리 통신 링크를 설정하기 위해 상기 CA 서버(26)와 근접할 수 있다(단계 100a, 메시지들 34a). 제 1 디바이스(29)는 CA 서버(26)로의 등록을 요청할 수 있으며(단계 102a 및 메시지 36a), 그 응

답으로, CA 서버(26)는 자격증명 및 챌린지 메시지를 전송한다(단계 106a 및 메시지 38a). 신뢰 영역(26)은 제 1 디바이스(29)로부터의 프롬프트 없이, 대신 근거리 통신 링크의 설정(단계 100a)에 의존하여, 자격증명 및 챌린지 메시지를 전송할 수 있다(단계 106a, 메시지 38a). 도 2 및 3을 참조하여 위에서 설명된 바와 같이, 제 1 이동 디바이스(29)는 상기 자격증명을 저장하고 상기 챌린지 요청에 대한 응답을 계산하고 상기 챌린지 응답을 상기 신뢰 서버(26)로 다시 전송한다(단계 108a, 메시지 40a). 신뢰 서버(26)는 상기 챌린지 응답이 유효함을 검증하고(테스트 110a), 응답이 유효하지 않는 경우 상기 자격증명 및 챌린지 요청을 전송하는 단계를 반복한다(단계 106a).

[0076] 새로운 디바이스(29)가 자격증명을 성공적으로 수신한 경우(즉, 테스트 110a = "예"), 새로운 디바이스(29)는 신뢰 영역 내에서 이동하며, 이제 상기 신뢰 영역을 다른 디바이스들로 확장하는데 사용될 수 있다. 예를 들어, 제 1 디바이스(29)의 사용자는 또다른 근거리 통신 링크를 설정하기 위해 상기 제 1 디바이스(29)를 제 2 디바이스(28)에 근접하게 가져올 수 있다(단계 100b, 메시지 34b). 등록 요청, 자격증명들의 전송, 자격증명들이 적절하게 수신되었다는 확인 및 신뢰 영역 통신 링크를 통한 보안 통신들의 개시의 프로세스(단계 102b 내지 112)는 이후, 도 2 및 3을 참조하여 전술된 유사하게 라벨링된 단계들과 실질적으로 동일한 방식으로 진행한다.

[0077] 이 실시예는 다수의 다른 디바이스들을 신뢰 영역으로 링크시키기 위한 수단으로서 이동 디바이스(29)를 사용하여 자격증명들을 분배하기 위한 다수의 유용한 애플리케이션들을 가진다.

[0078] 전술된 실시예들은 기존의 자격증명을 설정된 신뢰 영역으로부터 새로운 디바이스(28)로 확장하는 것으로서 설명되었다. 그러나, 다른 실시예에서, CA 서버(26)는 새로운 디바이스(28)가 상기 신뢰 영역으로 조인할 것을 요청할 때 새로운 자격증명을 발생시킬 수 있다. 이러한 실시예는 새로운 디바이스(28)의 엔트리가 다른 보안 레벨을 요구하는 경우 또는 이전 자격증명을 새로운 디바이스(28)에 공개하는 것을 회피할 필요가 있는 경우 유용할 수 있다.

[0079] 도 11 및 12에 예시된 이러한 실시예에서, 도 4 및 5를 참조하여 전술된 것과 유사한 방식으로, 새로운 디바이스(28)는 근거리 통신 링크를 설정하고(단계 100 및 메시지들 34) 등록 요청을 신뢰 영역의 멤버에게 전송하고(단계 102, 메시지 36)함으로써 상기 신뢰 영역에 조인하려고 한다. 새로운 디바이스(28)로부터 등록 요청을 수신하는 멤버 디바이스(예를 들어, 단말(12) 또는 이동 디바이스(29))는 CA 서버(26)로 상기 요청을 전달한다(단계 114, 메시지 44). 릴레이된 등록 요청을 수신할 때, 상기 CA 서버(26)는 신뢰 영역을 설정하기 위해 사용될 새로운 자격증명을 생성할 수 있다(단계 134). 이러한 새로운 자격증명(들)은 새로운 디바이스(28)가 신뢰 영역으로 수용될 수 있도록 상기 신뢰 영역의 멤버들에 의해 사용되는 현재의 자격증명(들)을 대체할 것이다. 이를 수행하기 위해, CA 서버(26)는 상기 새로운 자격증명을 챌린지 요청과 함께 상기 신뢰 영역의 각각의 멤버에 전송한다(단계 106a 및 메시지 62). 도 11은 CA 서버(26)로부터 상기 신뢰 영역의 멤버, 예컨대 단말(12)로 전달되는 새로운 자격증명 정보의 전달을 도시하지만, 새로운 자격증명 역시 도 9 및 도 10을 참조하여 전술된 것과 유사한 방식으로 한 멤버로부터 다른 멤버로 전달될 수 있다. 다른 실시예들에 대해 전술된 바와 같이, 새로운 자격증명을 수신하는 각각의 디바이스는 자격증명을 저장하고, 챌린지 요청에 대한 적절한 응답을 계산하고, 상기 자격증명을 제공한 디바이스로 상기 챌린지 응답을 다시 전송한다(단계 108a 및 메시지 64). 챌린지 응답은 유효성에 대해 체크되며(테스트 110a), 따라서 자격증명이 적절하게 수신되지 않았으면 상기 자격증명은 재전송될 수 있다(단계 106a). 신뢰 영역의 멤버들이 이미 보안 통신을 설정하도록 했으므로, 새로운 자격증명의 전송은 도 12에 도시된 바와 같이 신뢰 영역 내의 각각의 디바이스들의 쌍들 간에 근거리 통신 링크들을 설정할 필요 없이 해당 링크를 사용하여 이루어질 수 있다. 도 11 및 12가 오직 신뢰 영역의 단일 멤버로의 자격증명들의 전달을 도시하지만, 다양한 단계들은 상기 신뢰 영역의 모든 멤버들이 새로운 자격증명을 수신할 때까지 반복될 수 있다.

[0080] 새로운 자격증명이 신뢰 영역 내에 배치되면, 상기 신뢰 영역의 멤버들 중 하나는 설정된 근거리 통신 링크를 사용하여 새로운 디바이스(28)로 상기 자격증명을 전달할 수 있다. 이는 유사 번호의 단계들 및 메시지들에 대해 도 9 및 10을 참조하여 전술된 것과 실질적으로 동일한 방식으로 단계들(106b - 112) 및 메시지들(38 및 40)에서 달성될 수 있다.

[0081] 전술된 실시예들 중 임의의 실시예에서, 새로운 디바이스(28)를 신뢰 영역에 수용하는 프로세스의 일부분으로서, 상기 새로운 디바이스(28)의 사용자는 상기 신뢰 영역에 조인하도록 상기 사용자의 신원 또는 이전 허가를 확인하기 위해, 식별(identifying) 자격증명, 예를 들어, 패스워드 또는 생체 식별자를 입력하도록 프롬프트될 수 있다. 이러한 프롬프트는 근거리 통신 링크를 설정하는 프로세스의 일부분으로서 생성될 수 있으며(단계 100), 새로운 디바이스(28)의 디스플레이를 통해 상기 사용자에게 제공될 수 있다. 사용자가 패스워

드를 입력하도록 프롬프트되는 경우, 상기 사용자는 새로운 디바이스(28) 상의 키보드 또는 키패드를 사용함으로써 패스워드를 입력할 수 있다. 상기 사용자가 생체 식별자를 입력하도록 프롬프트되는 경우, 상기 사용자는 새로운 디바이스로 하여금 상기 새로운 디바이스가 요청 디바이스로 포워딩할 수 있는 생체 정보를 획득하도록 하기 위해 상기 새로운 디바이스(28) 상의 생체 센서를 사용할 수 있다. 예를 들어, 새로운 디바이스(28)는 사용자가 지문 이미지 또는 스캔을 생체 식별자로서 제공할 수 있게 하는 지문 스캐너(179)를 포함할 수 있다(도 15 참조). 다른 예로서, 사용자는 성문(voice print) 식별에 적합한 오디오 파일 또는 성문을 제공하기 위해 새로운 디바이스(28)의 마이크로폰으로 패스워드 구문을 말할 수 있다. 다른 생체 자격증명들 역시 사용될 수 있다. 사용자 식별자 정보(패스워드, 생체 식별자 또는 다른 자격증명)은 등록 요청의 일부분으로서, 또는 별개의 단계 및 메시지(미도시)로서, 근거리 통신 링크(4)를 통해 신뢰 영역 내의 요청 디바이스로 전달될 수 있다(단계 102 및 메시지 36). 도 4를 참조하여 전술된 바와 같이, CA 서버(26)는 신뢰 영역에 등록하기 위해 허가된 개인들에게 할당된 패스워드들의 리스트와 수신된 패스워드를 비교함으로써, 패스워드에 기초하여 사용자의 신원을 확인할 수 있다. 유사하게, CA 서버(26)는 신뢰 영역에 등록하기 위해 허가된 개인들의 생체 데이터와 수신된 생체 데이터를 비교함으로써, 생체 데이터에 기초하여 사용자의 신원을 확인할 수 있다.

[0082] 일 실시예에서, 접근 이벤트 역시 신뢰 영역으로부터 디바이스를 제거하는 프로세스의 일부분으로서 사용될 수 있다. 예를 들어, 도 13 및 14에 도시된 바와 같이, 신뢰 영역의 멤버인 이동 디바이스(28)는 영역 암호화 자격증명들에 의해 인에이블된 유선 또는 무선 통신 링크를 통해 보안 통신들에 참여할 수 있다(단계 134 및 메시지들 66). 이동 디바이스(28)를 제거하기 위해, 사용자는 상기 디바이스를 단말(12)과 같은 신뢰 영역의 다른 멤버에 근접하게 가져올 수 있으며, 이는 근거리 통신 링크의 설정을 자동으로 야기한다(단계 136 및 메시지들 68). 이후 이동 디바이스(28)는 신뢰 영역을 벗어나려는 희망을 선언(announce)하는 메시지를 근거리 통신 링크를 통해 단말(12)로 전송할 수 있다(단계 138 및 메시지 70). 상기 메시지의 수신시, 단말(12)은 상기 이동 디바이스(28)가 막 벗어나려고 함을 상기 신뢰 영역의 다른 멤버들에게 알리는 메시지들을 상기 신뢰 영역 통신 링크를 통해 전송할 수 있다(단계 140). 또한 단말(12)은 이동 디바이스(28)가 떠나는 것이 허용가능하다는 확인을 상기 CA 서버(26)로부터 수신할 수 있다. 이때, 단말(12)은 상기 출발 요청이 수신되었음을 확인 또는 확인응답하는 메시지를 떠나는 이동 디바이스(28)로 전송할 수 있다(단계 142 및 메시지 72). 이때, 상기 이동 디바이스(28)는 키 자격증명을 삭제할 수 있으며(단계 144), 이에 의해 자신이 신뢰 영역에서 벗어나게 할 수 있다. 일 실시예에서, CA 서버(26)는 상기 떠나는 이동 디바이스(28)가 다양한 실시예들의 자격증명 배치 방법들을 반복함이 없이 보안 통신들을 재설정할 수 없음을 보장하기 위해, 상기 신뢰 영역 내의 나머지 멤버들에게 새로운 자격증명을 전송할 것을 원할 수 있다. 이러한 실시예에 대한 변형에서, 상기 신뢰 영역을 벗어나려는 희망에 대한 표시가 보안 통신 링크를 사용하여 상기 떠나는 이동 디바이스(28)에 의해 상기 신뢰 영역의 다른 멤버들에게 전송될 수 있다. 이후 상기 신뢰 영역을 떠나려는 희망은 근거리 통신 링크(4)를 사용하여 상기 떠나는 이동 디바이스(28)에 의해 상기 단말(12)로 전달될 수 있다. 상기 단말(12)은 이후 제 1 이동 디바이스(28)가 더 이상 상기 그룹의 멤버가 아님을 상기 신뢰 영역의 나머지들에게 통지할 수 있다.

[0083] 상기 신뢰 영역으로부터 디바이스를 제거하기 위해 근거리 통신 링크를 생성하는 단계를 포함하는 것은 물리적 이동 형태로 추가된 보안 계층을 제공한다(즉, 상기 떠나는 디바이스를 상기 단말(12)에 근접하게 가져옴). 이러한 추가된 단계는 상기 디바이스들이 신뢰 영역으로부터 비고의적으로 떨어질 기회를 감소시킨다. 물론, 디바이스들 역시 설정된 신뢰 영역 통신 링크를 통해 상기 영역을 떠나려는 희망을 전달하는 메시지들을 전달하거나 턴오프됨으로써 신뢰 영역을 벗어날 수 있다.

[0084] 전술된 실시예들은 예를 들어, 랩톱 컴퓨터들, 셀룰러 전화들, 셀룰러 전화가 구비된 개인 휴대용 디지털 장비(PDA), 이동 전자 메일 수신기들, 이동 웹 액세스 디바이스들, 및 무선 네트워크에 접속하는 차후 개발될 수 있는 다른 프로세서가 구비된 디바이스들과 같은 다양한 이동 핸드셋들 중 임의의 이동 핸드셋 상에서 구현될 수 있다. 통상적으로, 이러한 이동 핸드셋들은 도 15에 도시된 컴포넌트들을 공통적으로 가질 것이다. 예를 들어, 이동 핸드셋(170)은 내부 메모리(172) 및 디스플레이(173)에 연결된 프로세서(171)를 포함할 수 있다. 추가적으로, 이동 핸드셋(170)은 프로세서(171)에 연결된 셀룰러 전화 트랜시버(175) 및/또는 무선 데이터 링크에 접속되어 전자기 복사를 전송하고 수신하기 위한 안테나(174)를 가질 것이다. 몇몇 실시예들에서, 셀룰러 전화 통신들을 위해 사용된 트랜시버들(175) 및 상기 프로세서(171)와 메모리(172)의 일부분들은 그것이 무선 데이터 링크를 통해 데이터 인터페이스를 제공하므로 무선 인터페이스라고도 지칭된다. 추가적으로, 이동 핸드셋(170)은 예를 들어, 니어 필드 통신 프로토콜들 중 하나를 사용하여, 근거리 통신 링크를 설정하고 전달할 수 있는 근거리 트랜시버(178)를 포함할 것이다. 몇몇 실시예들에서, 이동 핸드셋(170)은 사용자의 생체 이미지를 획득하고 그 데이터를 프로세서(177)에 전달할 수 있는 생체 센서들, 예를 들어 지문 스캐너(179)를 포함할 것이다. 이동 핸드셋들은 통상적으로 사용자 입력들을 수신하기 위한 키패드(176) 또는 미니 키보드 및 메뉴 선

택 버튼들 또는 자물쇠 스위치들(177)을 포함한다.

[0085] 또한 전술된 실시예들은 다양한 다른 컴퓨팅 디바이스들, 예를 들어, 도 16에 예시된 개인용 컴퓨터(180), 프로세서가 장착된 컴포넌트들(예를 들어, 도 18에 도시된 IV 펌프(214) 또는 ECG 모니터(216)), 또는 다른 스마트 디바이스들 중 임의의 디바이스 상에서 구현될 수 있다. 이러한 개인용 컴퓨터(180)는 통상적으로 메모리(182) 및 디스크 드라이브(183)와 같은 대용량 메모리에 연결된 프로세서(181)를 포함할 수 있다. 또한, 상기 컴퓨터(180)는 상기 프로세서를 유선 네트워크에 연결하기 위한 네트워크 접속 회로(184)를 포함할 수 있다. 추가적으로, 상기 컴퓨터(180)는 무선 데이터 네트워크를 통해 데이터를 전송하고 수신하기 위해 프로세서(181)에 연결된 중장거리 무선 트랜시버(185), 예를 들어, WiFi 또는 BlueTooth® 트랜시버로의 매체를 포함할 수 있다. 또한, 다양한 실시예들에서 사용된 컴퓨터(180)는 초단거리 무선 데이터 링크를 통해 데이터를 전송하고 수신하도록 구성된 근거리 통신 트랜시버(188)를 포함한다. 예를 들어, 근거리 통신 트랜시버(188)는 NFC 프로토콜 트랜시버 또는 RFID 판독기일 수 있다. 이와 같이 구성되어, 컴퓨터(180)는 다양한 실시예들의 방법들을 실행하기 위해, 다른 디바이스들, 예를 들어, 도 15에 도시된 이동 디바이스(170)와 근거리 통신 링크들을 설정할 수 있다.

[0086] 또한 전술된 실시예들은 다양한 서버 및 네트워크 관리자 시스템들 중 임의의 시스템, 예를 들어, 도 17에 도시된 네트워크 서버(190) 상에서 구현될 수 있다. 이러한 서버(190)는 통상적으로 메모리(192) 및 대용량 메모리, 예를 들어, 디스크 드라이브(193)에 연결된 프로세서(191)를 포함할 수 있다. 또한, 서버(190)는 프로세서를 인터넷과 같은 유선 네트워크에 연결시키기 위한 다수의 네트워크 접속 회로들(194a - 194d)을 포함할 수 있다. 선택적으로, 상기 서버(190)는 또한 무선 데이터 네트워크를 통해 데이터를 전송하고 수신하기 위해 상기 프로세서(191)에 연결된 WiFi 트랜시버와 같은 중장거리 무선 트랜시버(195)를 포함할 수 있다. 또한, 상기 서버(190)는 초단거리 무선 데이터 링크를 통해 데이터를 전송 및 수신하도록 구성된 근거리 통신 트랜시버(198)를 선택적으로 포함할 수 있다. 예를 들어, 상기 근거리 통신 트랜시버(198)는 NFC 프로토콜 트랜시버 또는 RFID 판독기일 수 있다. 이와 같이 구성되어, 상기 서버(190)는 다양한 실시예들의 방법들을 실행하기 위해, 다른 디바이스들, 예를 들어 도 15에 도시된 이동 디바이스(180) 또는 도 16에 도시된 컴퓨터(180)와 근거리 통신 링크를 설정할 수 있다.

[0087] 다양한 실시예들은 단순히 암호화된 통신들을 지원하는 것 이외에 다양한 애플리케이션들을 인에이블시킨다. 예시적인 애플리케이션은 도 18에 도시되어 있으며,도 18은 병원 내에서 예컨대 집중 치료 유닛에서 채택될 수 있는 센서, 데이터 수집 및 데이터베이스 시스템을 도시한다. 다양한 실시예들은 플렉시블한 무선 통신 링크들을 사용하여 다양한 의료 디바이스들을 네트워크에 링크시키기 위해 가상 케이블들(여기서 "V-케이블들"이라 지칭됨)의 생성을 인에이블시키고, 이에 의해 디바이스들로부터 모니터들로 데이터를 전달하는데 현재 사용되는 케이블들을 데이터 수집 노드들로 대체한다. 이러한 시스템은 근거리 통신 링크(224) 뿐만 아니라, BlueTooth® 프로토콜 데이터 링크와 같은 중거리 무선 데이터 링크(222)와 통신하도록 구성된 도 16을 참조하여 전술된 컴포넌트를 포함하는 환자 모니터링 컴퓨터(212)를 포함할 수 있다. 또한, 상기 환자 모니터링 컴퓨터(212)는 병원 메인프레임 컴퓨터(220)에 접속하기 위해 WiFi 데이터 링크와 같은 장거리 무선 데이터 링크(226), 예를 들어, WiFi 데이터 링크를 통해 통신할 수 있는 장거리 무선 트랜시버가 구비될 수 있다. 대안적으로, 환자 모니터링 컴퓨터는 유선 네트워크(224)에 의해 병원 메인프레임 컴퓨터(220)에 연결될 수 있다. 환자들의 집중 치료 유닛은 예를 들어, 정맥(IV) 펌프(214) 및 심전도(ECG) 모니터(216)와 같은 특정 환자 모니터링 장비일 수 있다. 이러한 환자 모니터링 장비(214,216)는 통상적으로 메모리 D에 연결된 프로세서 A, 중거리 무선 트랜시버 B, 및 근거리 무선 트랜시버 C를 포함할 것이다. 이와 같이 구비되어, 각각의 의료 디바이스는 중거리 무선 네트워크(222)를 통해 보안 통신을 설정하기에 충분한 자격증명 정보를 수신하기 위해, 다양한 실시예들에 채택된 상기 근거리 통신 링크(224)를 설정할 수 있을 것이다. 다양한 실시예들은 상기 다양한 실시예들에서 채택된 중거리 무선 네트워크(222) 및 근거리 통신 링크(224) 모두를 사용하여 센서들, 예를 들어 휴대용 전극(218)으로부터 환자 데이터를 전달하기 위해 추가로 사용될 수 있다. 근거리 및 중거리 통신 트랜시버들이 구비되지 않은 의료 디바이스들을 접속시키기 위해, 가상 케이블 커넥터(200)는 이러한 디바이스들을 환자 모니터 컴퓨터(212)에 접속시키기 위해 사용될 수 있다. 가상 케이블 커넥터(200)에 대한 더 상세한 내용들은 도 20을 참조하여 아래에 제공된다.

[0088] 도 18에 도시된 시스템의 동작은 새로운 환자를 모니터링하기 시작하도록 요구된 단계들의 예를 고려함으로써 이해될 수 있다. 도 19에 예시된 바와 같이, 환자 모니터 컴퓨터(212)는 턴 온되어 병원 네트워크 및 메인프레임 컴퓨터(220)로 로깅될 수 있다(단계 250). 구현에 따라, 병원 메인프레임 컴퓨터(220)는 무선 전송들의 암

호화를 위해 사용되는 임의의 시드 데이터와 함께 자격증명 정보를 환자 모니터 컴퓨터(212)에 전송할 수 있다. ECG 모니터(216)를 환자 모니터 컴퓨터(212)에 접속시키기 위해, 상기 모니터는 전술된 실시예들에서 설명된 바와 같이 근거리 통신 링크를 설정하고 자격증명 정보를 수신하도록 상기 컴퓨터에 근접해올 수 있다(단계 254). ECG 모니터(216)를 환자 모니터 컴퓨터(212)에 데이터 링크 접속시키는 적절한 동작이 확인될 수 있으며(단계 256), 필요한 경우 상기 프로세스가 반복된다(단계 258). 이후, 각각의 ECG 센서(218)는 각각의 센서(218)를 모니터에 단순히 터치시킴으로써 ECG 모니터(216)로 데이터를 전송하도록 구성될 수 있다(단계 260). ECG 센서-대-모니터 데이터 링크의 적절한 동작이 확인될 수 있으며(단계 262), 필요한 경우 프로세스가 반복된다(단계 264). 유사하게, IV 펌프(214)는 단지 컴퓨터에 근접하게 가져옴으로써 환자 모니터 컴퓨터(212)에 연결될 수 있다(단계 266). 다시, 펌프-대-컴퓨터 데이터 링크가 확인될 수 있고(단계 268), 필요한 경우 프로세스가 반복된다(단계 270). 다양한 의료 디바이스들을 접속시키는 이러한 터치 프로세스는 모든 디바이스들이 환자 모니터 컴퓨터(212)에 링크될 때까지 계속될 수 있다. 이때, 도 18에 도시된 시스템을 사용하는 환자 모니터링이 시작될 수 있다(단계 272).

[0089] 도 19에 예시된 방법은 각각의 의료 디바이스가 근거리 무선(예를 들어, NFC) 및 중거리 무선(예를 들어, BlueTooth®) 트랜시버들을 모두 포함한다고 가정한다. 그러나, 상기 시스템은 또한 도 20에 예시된 일 예인 V-케이블 커넥터(200)를 사용함으로써 종래의 케이블 접속들에 대해 구성된 의료 디바이스를 통해 구현될 수 있다. V-케이블 커넥터(200)는 메모리(202) 및 배터리(203)와 같은 전원에 연결된 프로세서(201)를 포함할 수 있다. V-케이블 커넥터(200)는 예를 들어 BlueTooth® 프로토콜을 사용하여 중거리 무선 통신을 설정하도록 구성된 안테나(202) 및 프로세서(201)에 연결된 중거리 트랜시버(205)를 포함할 수 있다. 추가적으로, V-케이블 커넥터(200)는 프로세서(201) 및 안테나(209)에 접속된 근거리 통신 트랜시버(208)를 포함할 수 있다. 예를 들어, 근거리 트랜시버(208)는 RFID 디바이스 또는 NFC 프로토콜 트랜시버일 수 있다. 추가적으로, V-케이블 커넥터(200)는 동축 케이블(207)을 통해 커넥터에 연결된 커넥터 플러그(206)를 포함할 수 있다. 커넥터 플러그(206)는 환자 모니터 컴퓨터(212)에, 그리고 의료 디바이스들을 함께 접속시키기 위해 사용된 케이블들의 표준 플러그 구성을 매치시키도록 구성된다. V-케이블 커넥터(200)는 단지 케이블인 것처럼 의료 디바이스들의 케이블 포트에 단순히 플러그인할 수 있는 단일 디바이스를 제공하기 위해 하우징(210) 내에 포함될 수 있다. 프로세서(201)는 다양한 실시예들에 따라 단계들을 수행하도록 상기 프로세서가 트랜시버들(205, 208)을 동작시키도록 하기 위해, 메모리(202)에 저장될 수 있는 소프트웨어 명령들과 함께 구성될 수 있다. 이와 같이 구성되어, V-케이블 커넥터(200)는 마치 접속이 케이블에 의해 이루어진 것처럼, 보안 무선 통신 네트워크들을 사용하여 하나의 이동 디바이스를 V-케이블 커넥터(200) 또는 내부 트랜시버들을 가지는 또다른 디바이스로 접속시킬 수 있을 필요가 있는 통신 엘리먼트들 모두를 포함한다.

[0090] V-케이블 커넥터들(200)을 사용하는 병원 시스템의 동작은 새로운 환자를 모니터링하기 위해 상기 시스템을 어셈블링하도록 요구되는 단계들의 일 예를 고려함으로써 이해될 수 있다. 도 21에 예시된 바와 같이, 환자 모니터 컴퓨터(212)가 턴 온되어 병원 네트워크 및 메인프레임 컴퓨터(220)로 로깅될 수 있다(단계 250). 상기 구현에 따라, 병원 메인프레임 컴퓨터(220)는 무선 전송들을 암호화하기 위해 사용되는 임의의 시드 데이터와 함께 자격증명 정보를 상기 환자 모니터 컴퓨터(212)에 전송할 수 있다(단계 252). V-케이블 커넥터들(200)을 사용하여 다양한 의료 디바이스들을 접속시키기 위해, 하나의 커넥터는 자격증명 정보를 수신하도록 근거리 통신 링크(222)를 설정하기 위해 상기 환자 모니터 컴퓨터(212)에 터치된다(단계 280). 커넥터-대-컴퓨터 데이터 링크가 확인될 수 있고(단계 282), 필요한 경우 상기 프로세스가 반복된다(단계 284). 데이터 링크가 설정되면, V-케이블 커넥터(200)는 의료 디바이스, 예를 들어, ECG 모니터(216)로 플러그인된다(단계 286). 이후, 다수의 ECG 센서들을 ECG 모니터(216)로 접속시키기 위해, 동일한 개수의 V-케이블 커넥터들(200)이 ECG 모니터(216)로 플러그인된다(단계 288). ECG 센서들(218)에 무선 트랜시버들이 구비되는 경우, 도 18에 예시된 바와 같이, 센서들은 ECG 모니터(216)에 플러그인된 V-케이블 커넥터들(200)의 개별 커넥터에 각각의 센서(218)를 터치시킴으로써 ECG 모니터(216)에 링크될 수 있다(단계 290). 센서-대-커넥터 데이터 링크가 확정될 수 있고(단계 292), 필요한 경우 프로세스가 반복된다(단계 294). 센서들이 모니터에 전자적으로 링크되면, 이후 상기 센서들은 환자들에게 적용될 수 있다(단계 294). IV 펌프는 V-케이블 커넥터(200)를 컴퓨터에 터치시키고(단계 296), 커넥터-대-컴퓨터 데이터 링크를 검증하고(단계 298)(그리고 필요한 경우 상기 프로세스를 반복함(단계 300)), 이후 상기 V-케이블 커넥터(200)를 IV 펌프로 플러그인함으로써(단계 302), 환자 모니터 컴퓨터(212)에 유사하게 접속될 수 있다. 이러한 점에서, 환자 모니터링이 시작될 수 있다(단계 272).

[0091] 설명될 수 있는 바와 같이, 다양한 실시예들이 물리적 케이블들을 신속하고 간편하게 대체하도록 가상 케이블들을 사용하기 위해 다양한 다른 애플리케이션들을 인에이블 할 수 있다. 중-장거리 통신 링크에 의한 암호화 자

격증명들의 사용은 다른 V-케이블 접속들에 의한 간섭을 방지할 것이며 또한 단지 물리적 케이블들이 도청을 방지하는 것과 같이 데이터를 도청으로부터 보호할 것이다. 다양한 실시예들을 사용하여, 이러한 애드 혹 신뢰 영역들을 설정하기 위한 프로세스는 원하는 데이터 링크 및 보안 장치를 설정하기 위해 컴포넌트들 및 가상 커넥터들을 단순히 함께 터치시키는 지각가능한 프로세스로 간략화될 수 있다.

[0092] 다양한 디바이스들, 컴포넌트들 및 서버들에서, 프로세서(171, 181, 191 및 201)는 임의의 프로그램 가능한 마이크로프로세서, 전술된 다양한 실시예들의 기능들을 포함한 다양한 기능들을 수행하도록 소프트웨어 명령들(애플리케이션들)에 의해 구성될 수 있는 마이크로컴퓨터 또는 다수의 프로세서 칩 또는 칩들일 수 있다. 몇몇 디바이스들에서, 다수의 프로세서들(171, 181, 191, 201)에는, 예를 들어, 무선 통신 기능들에 전용으로 사용되는 하나의 프로세서 및 다른 애플리케이션들의 실행에 전용으로 사용되는 하나의 프로세서가 제공될 수 있다. 통상적으로, 소프트웨어 애플리케이션들은 이들이 프로세서(171, 181, 191, 201)에 액세스되고 로딩되기 전에 내부 메모리(172, 182, 192, 202)에 저장될 수 있다. 일부 디바이스들에서, 프로세서(171, 181, 191, 201)는 애플리케이션 소프트웨어 명령들을 저장하기에 충분한 내부 메모리를 포함할 수 있다. 이러한 설명의 목적으로, 용어 메모리는 내부 메모리(172, 182, 192, 202) 및 프로세서(171, 181, 191, 201) 자체 내의 메모리를 포함한, 프로세서(171, 181, 191, 201)에 의해 액세스 가능한 모든 메모리를 지칭한다. 사용자 데이터 파일들은 통상적으로 메모리(172, 182, 192, 202)에 저장된다. 많은 이동 디바이스들에서, 메모리(172, 182, 192, 202)는 플래시 메모리와 같은 휘발성 또는 비휘발성 메모리, 또는 이들의 조합일 수 있다.

[0093] 하나 이상의 예시적인 실시예들에서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어 또는 이들의 임의의 조합으로 구현될 수 있다. 소프트웨어로 구현되는 경우, 상기 기능들은 컴퓨터-판독가능 매체상에 하나 이상의 명령들 또는 코드들로서 저장되거나 전송될 수 있다. 컴퓨터-판독가능 매체는 한 장소에서 다른 장소로의 컴퓨터 프로그램의 전송을 용이하게 하는 임의의 매체를 포함하는 통신 매체 및 컴퓨터 저장 매체 모두를 포함한다. 저장 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 사용가능한 매체일 수 있다. 제한이 아닌 예시로서, 이러한 컴퓨터-판독가능 매체는 RAM, ROM, EEPROM, CD-ROM 또는 다른 광학 디스크 저장소, 자기 디스크 저장소 또는 다른 자기 저장 디바이스, 또는 명령들 또는 데이터 구조들의 형태로 원하는 프로그램 코드를 반송하거나 저장하는데 사용될 수 있고 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 또한, 임의의 접속은 컴퓨터-판독가능 매체라고 적절히 지칭된다. 예를 들어, 소프트웨어가 동축 케이블, 광섬유 케이블, 연선(twisted pair), 디지털 가입자 회선(DSL), 또는 자외선, 라디오, 및 마이크로파와 같은 무선 기술들을 사용하여 웹사이트, 서버, 또는 다른 원격 소스로부터 전송되는 경우, 이러한 적외선, 라디오, 마이크로파는 매체의 정의 내에 포함된다. 여기에 설명된 바와 같이 디스켓(disk) 및 디스크(disc)는 컴팩트 디스크(CD), 레이저 디스크, 광학 디스크, 디지털 다용도 디스크(DVD), 플로피 디스켓 및 블루레이 디스크를 포함하며, 여기서 디스켓들은 일반적으로 데이터를 자기적으로 재생하는 반면 디스크들은 데이터를 레이저를 사용하여 광학적으로 재생한다. 전술 항목들의 조합 역시 컴퓨터-판독가능 매체의 범위내에 포함되어야 한다.

[0094] 개시된 실시예들의 이전 설명은 당업자가 본 발명을 제작하거나 사용하도록 제공된다. 이들 실시예들에 대한 다양한 수정들은 당업자에게 자명할 것이며, 여기에 정의된 일반 원리들은 본 발명의 사상 또는 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 따라서, 본 발명은 여기에 나타난 실시예들에 제한되도록 의도되는 것이 아니라, 여기에 개시된 원리들 및 신규한 특징들에 부합하는 최광의의 범위에 따라야 한다.

도면의 간단한 설명

[0007] 도 1은 다수의 이동 디바이스들 상에서 구현되는 단거리 무선 통신을 포함하는 무선 셀룰러 네트워크의 시스템 블록도이다.

[0008] 도 2는 디바이스를 신뢰 영역에 조인(join)시키기에 적합한 실시예의 방법의 프로세스 흐름도이다.

[0009] 도 3은 도 2에 예시된 신뢰 영역을 설정하기 위한 상기 실시예의 메시지 흐름도이다.

[0010] 도 4는 신뢰 영역을 설정하기에 적합한 또다른 실시예의 방법의 프로세스 흐름도이다.

[0011] 도 5는 도 4에 예시된 신뢰 영역을 설정하기 위한 실시예의 메시지 흐름도이다.

[0012] 도 6은 신뢰 영역을 설정하기에 적합한 또다른 실시예의 방법의 프로세스 흐름도이다.

[0013] 도 7은 신뢰 영역을 설정하기에 적합한 또다른 실시예의 방법의 프로세스 흐름도이다.

[0014] 도 8은 도 7에 예시된 신뢰 영역을 설정하기 위한 실시예의 메시지 흐름도이다.

[0015] 도 9는 다수의 디바이스들 사이에 신뢰 영역을 설정하기에 적합한 실시예의 방법의 프로세스 흐름도이다.

[0016] 도 10은 도 9에 설명된 신뢰 영역을 설정하기 위한 실시예의 메시지 흐름도이다.

[0017] 도 11은 신뢰 영역을 설정하기에 적합한 또다른 실시예의 방법의 프로세스 흐름도이다.

[0018] 도 12는 도 11에 설명된 신뢰 영역을 설정하기 위한 실시예의 메시지 흐름도이다.

[0019] 도 13은 신뢰 영역으로부터 디바이스를 제거하기에 적합한 실시예의 방법의 프로세스 흐름도이다.

[0020] 도 14는 도 13에 예시된 신뢰 영역으로부터 디바이스를 제거하기 위한 실시예의 메시지 흐름도이다.

[0021] 도 15는 다양한 실시예들과 함께 사용하기에 적합한 예시적인 이동 디바이스의 회로 블록도이다.

[0022] 도 16은 다양한 실시예들과 함께 사용하기에 적합한 예시적인 컴퓨터 또는 다른 프로그래밍된 디바이스의 회로 블록도이다.

[0023] 도 17은 다양한 실시예들과 함께 사용하기에 적합한 예시적인 서버의 회로 블록도이다.

[0024] 도 18은 일 실시예에 따른 무선 환자(patient) 모니터링 시스템의 시스템 블록도이다.

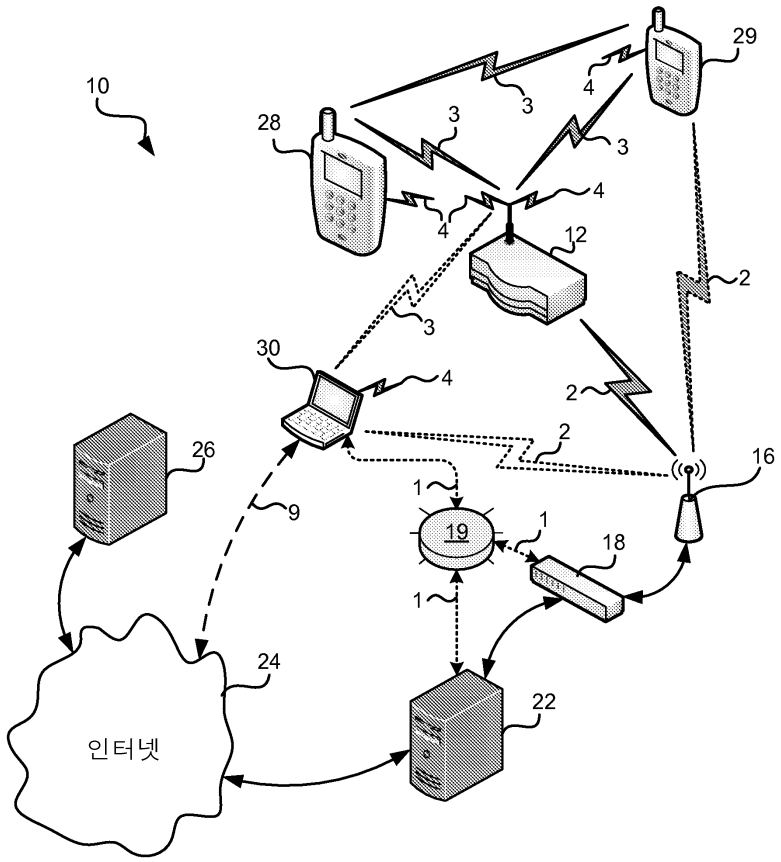
[0025] 도 19는 도 18에 도시된 환자 모니터링 시스템 내의 컴포넌트들을 접속시키기에 적합한 일 실시예의 방법의 프로세스 흐름도이다.

[0026] 도 20은 다양한 실시예들과 함께 사용하기에 적합한 예시적인 가상 케이블 커넥터 디바이스의 회로 블록도이다.

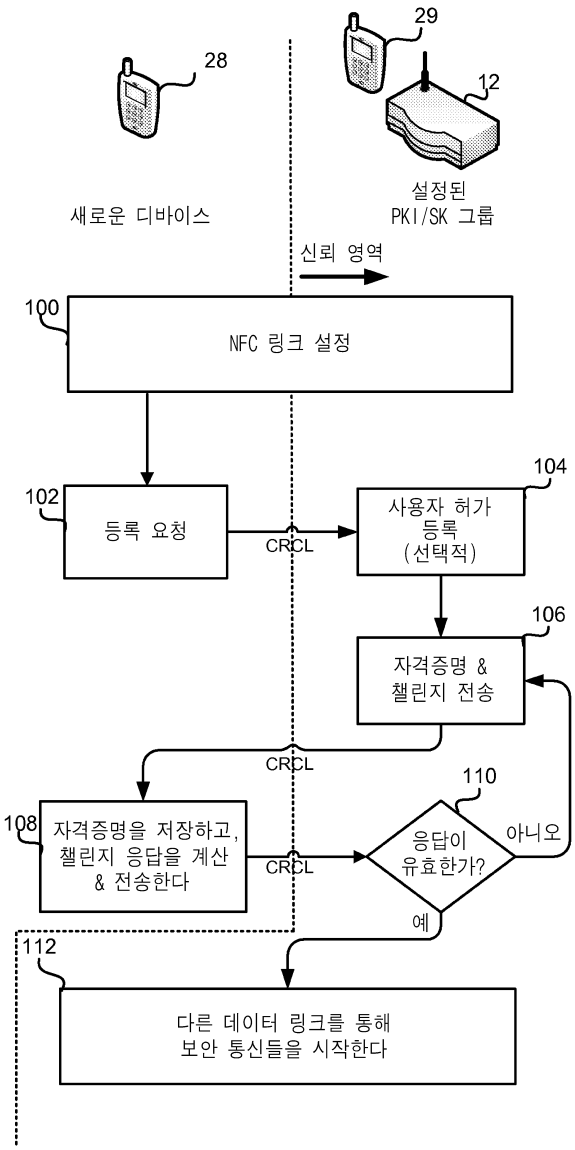
[0027] 도 21은 도 20에 도시된 가상 케이블 커넥터 디바이스를 사용하여 도 18에 도시된 환자 모니터링 시스템 내에서 컴포넌트들을 접속시키기에 적합한 일 실시예의 방법들의 프로세스 흐름도이다.

도면

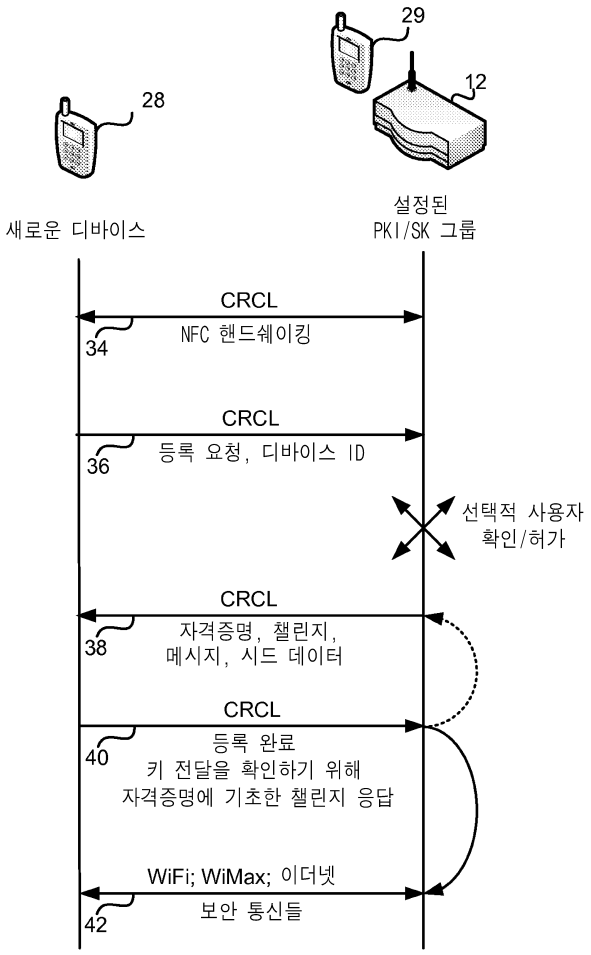
도면1



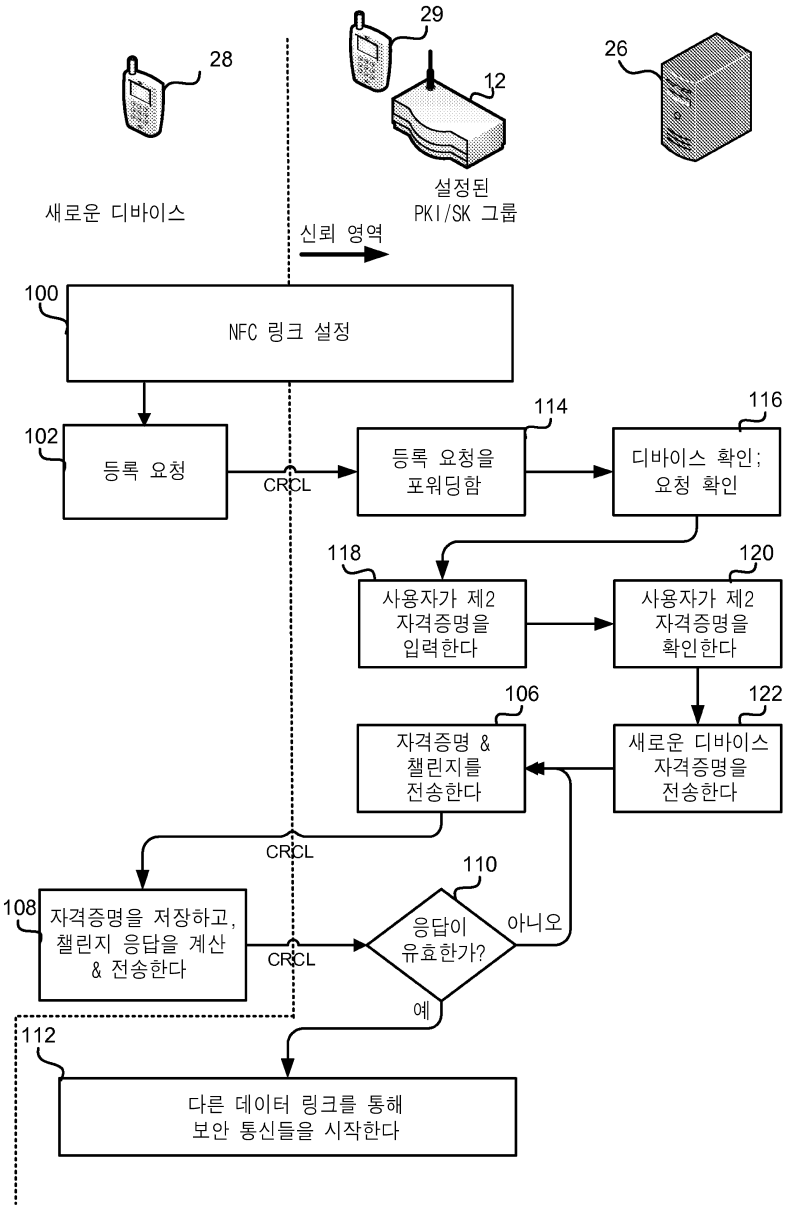
도면2


28
29
12
새로운 디바이스
설정된
PKI/SK 그룹
신뢰 영역
100
NFC 링크 설정
102
등록 요청
CRCL
104
사용자 허가
등록
(선택적)
106
자격증명 &
챌린지 전송
CRCL
108
자격증명을 저장하고,
챌린지 응답을 계산
& 전송한다
CRCL
110
응답이
유효한가?
아니오
예
112
다른 데이터 링크를 통해
보안 통신들을 시작한다

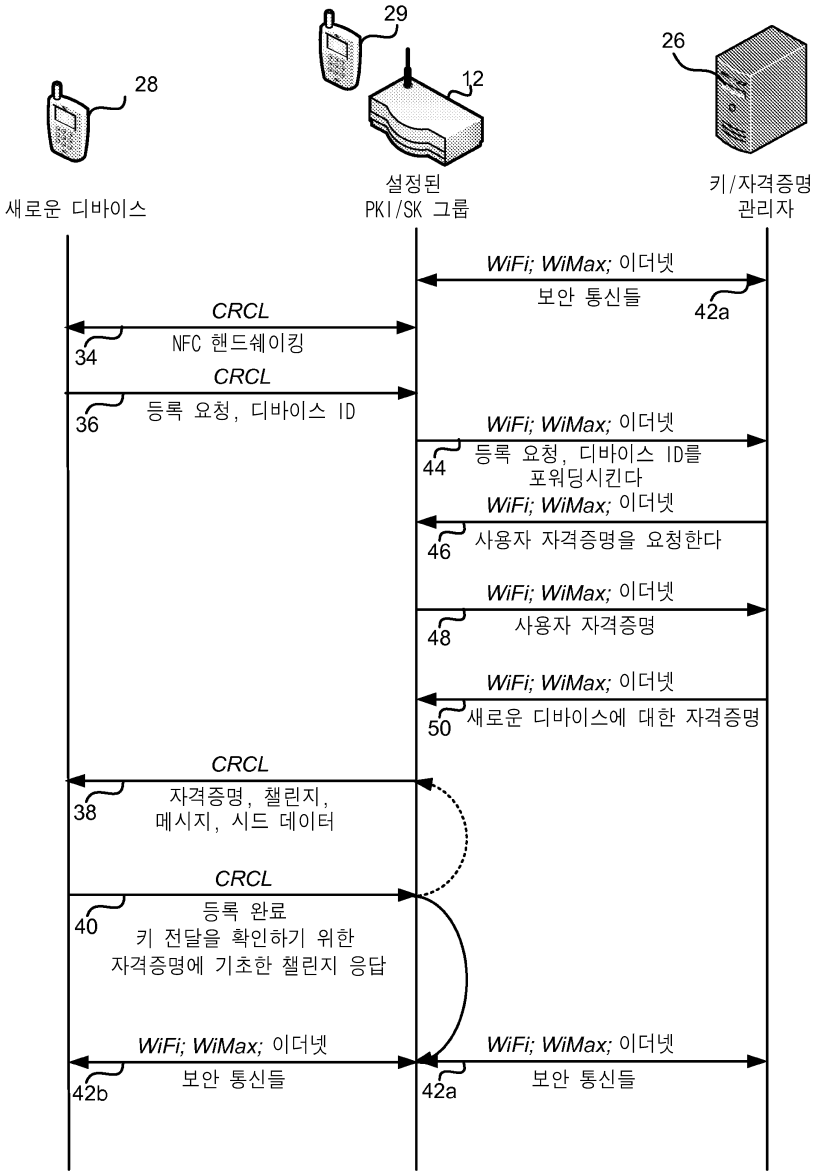
도면3


29
12
28
새로운 디바이스
설정된
PKI/SK 그룹
CRCL
NFC 핸드쉐이킹
34
CRCL
등록 요청, 디바이스 ID
36
선택적 사용자
확인/허가
CRCL
자격증명, 챌린지,
메시지, 시드 데이터
38
CRCL
등록 완료
키 전달을 확인하기 위해
자격증명에 기초한 챌린지 응답
40
WiFi; WiMax; 이더넷
보안 통신들
42

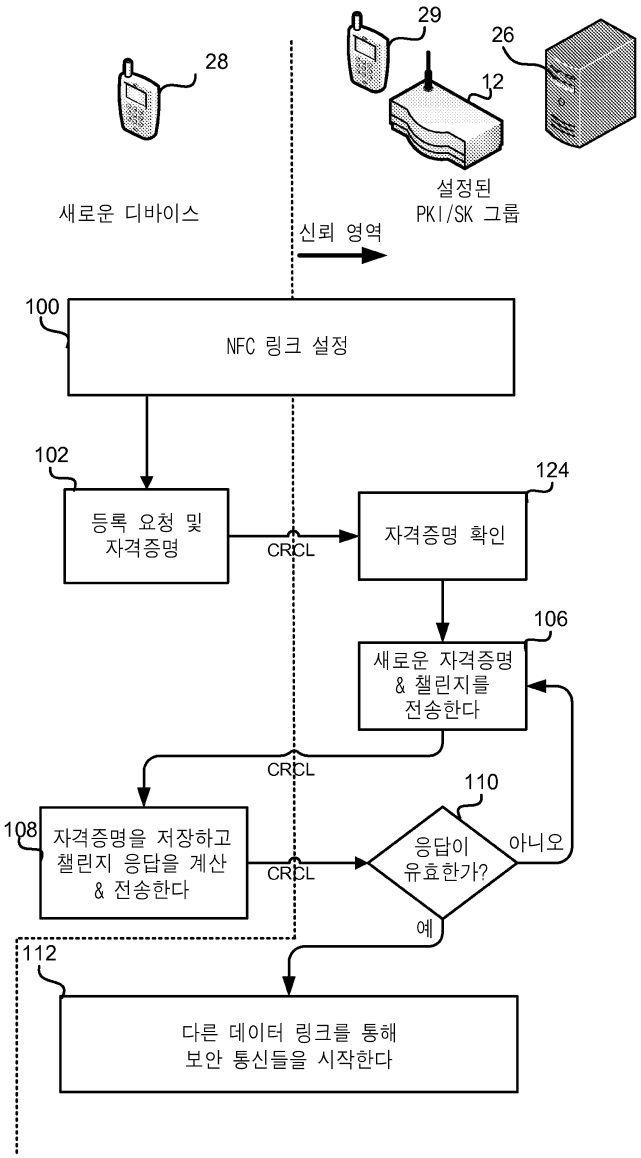
도면4


28
29
12
26
새로운 디바이스
설정된
PKI/SK 그룹
신뢰 영역
100
NFC 링크 설정
102
등록 요청
CRCL
114
등록 요청을
포워딩함
116
디바이스 확인;
요청 확인
118
사용자가 제2
자격증명을
입력한다
120
사용자가 제2
자격증명을
확인한다
106
자격증명 &
챌린지를
전송한다
122
새로운 디바이스
자격증명을
전송한다
CRCL
110
108
자격증명을 저장하고,
챌린지 응답을 계산
& 전송한다
CRCL
응답이
유효한가?
아니오
예
112
다른 데이터 링크를 통해
보안 통신들을 시작한다

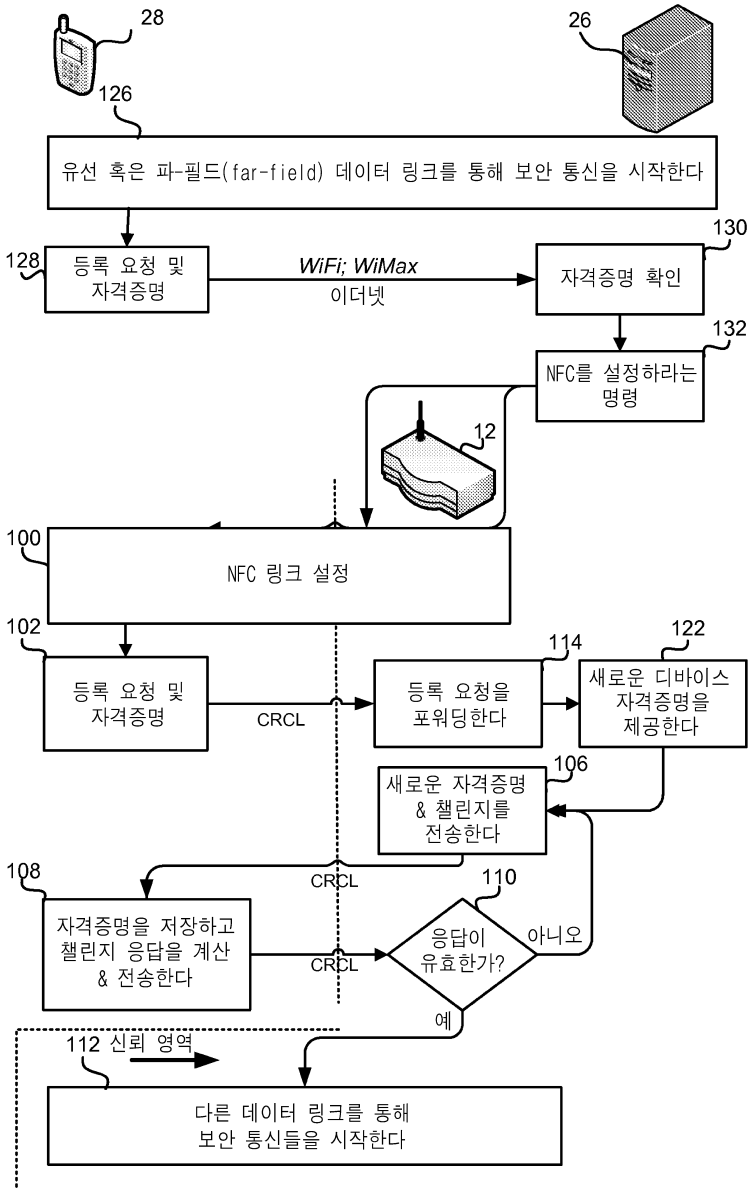
도면5


29
28
12
26
새로운 디바이스
설정된
PKI/SK 그룹
키/자격증명
관리자
WiFi; WiMax; 이더넷
보안 통신들
42a
CRCL
NFC 핸드쉐이킹
34
CRCL
등록 요청, 디바이스 ID
36
WiFi; WiMax; 이더넷
등록 요청, 디바이스 ID를
포워딩시킨다
44
WiFi; WiMax; 이더넷
사용자 자격증명을 요청한다
46
WiFi; WiMax; 이더넷
사용자 자격증명
48
WiFi; WiMax; 이더넷
새로운 디바이스에 대한 자격증명
50
CRCL
자격증명, 챌린지,
메시지, 시드 데이터
38
CRCL
등록 완료
키 전달을 확인하기 위한
자격증명에 기초한 챌린지 응답
40
WiFi; WiMax; 이더넷
보안 통신들
42b
WiFi; WiMax; 이더넷
보안 통신들
42a

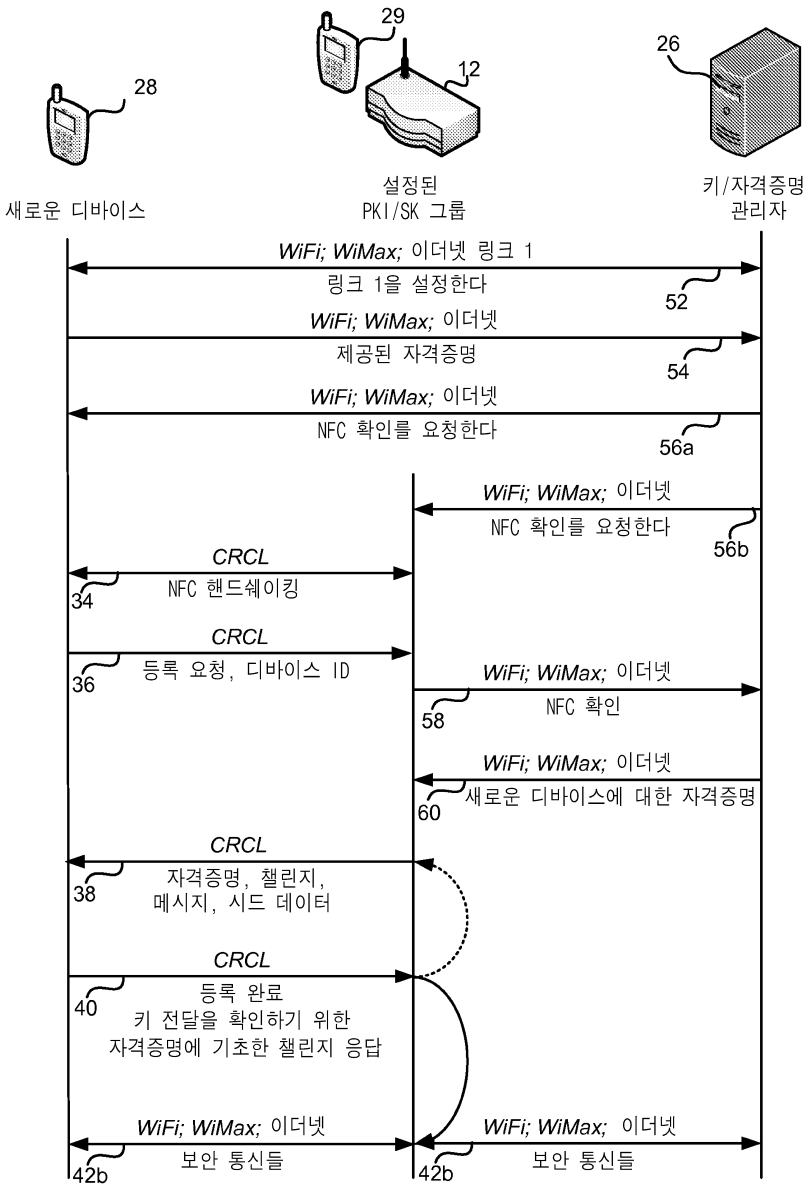
도면6


29
26
28
12
새로운 디바이스
설정된
PKI/SK 그룹
신뢰 영역
100
NFC 링크 설정
102
등록 요청 및
자격증명
CRCL
124
자격증명 확인
106
새로운 자격증명
& 챌린지를
전송한다
CRCL
110
108
자격증명을 저장하고
챌린지 응답을 계산
& 전송한다
CRCL
응답이
유효한가?
아니오
예
112
다른 데이터 링크를 통해
보안 통신들을 시작한다

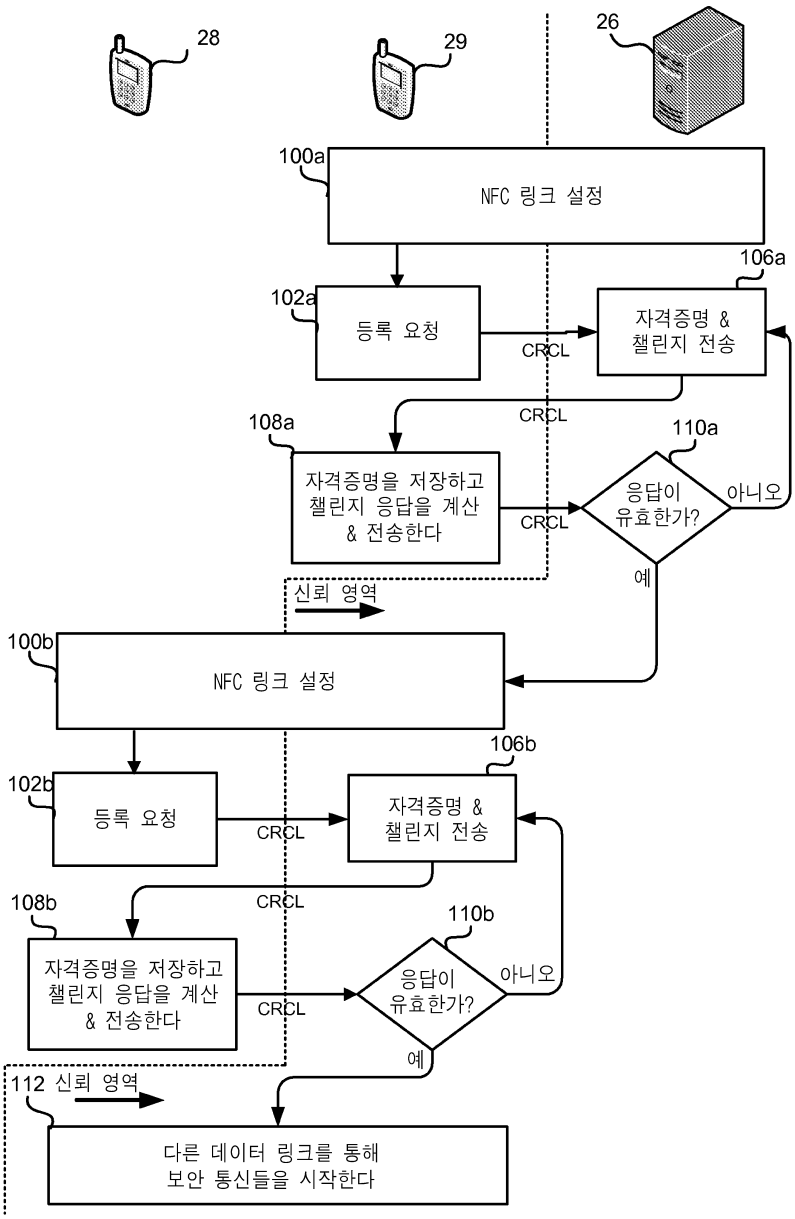
도면7


28
126
26
유선 혹은 파-필드(far-field) 데이터 링크를 통해 보안 통신을 시작한다
128
등록 요청 및 자격증명
WiFi; WiMax
이더넷
130
자격증명 확인
132
NFC를 설정하라는 명령
12
100
NFC 링크 설정
102
등록 요청 및 자격증명
CRCL
114
등록 요청을 포워딩한다
122
새로운 디바이스 자격증명을 제공한다
106
새로운 자격증명 & 챌린지를 전송한다
CRCL
108
자격증명을 저장하고 챌린지 응답을 계산 & 전송한다
CRCL
110
응답이 유효한가?
아니오
예
112 신뢰 영역
다른 데이터 링크를 통해 보안 통신들을 시작한다

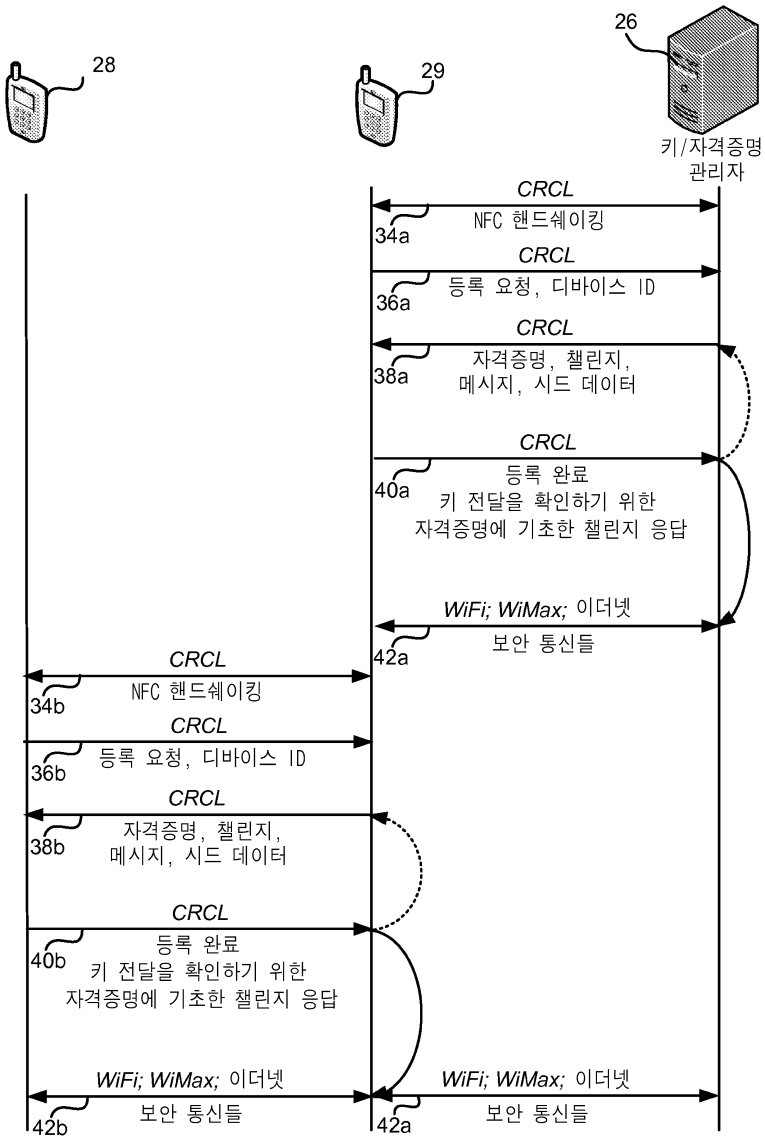
도면8


29
12
28
26
새로운 디바이스
설정된
PKI/SK 그룹
키/자격증명
관리자
WiFi; WiMax; 이더넷 링크 1
링크 1을 설정한다
52
WiFi; WiMax; 이더넷
제공된 자격증명
54
WiFi; WiMax; 이더넷
NFC 확인를 요청한다
56a
WiFi; WiMax; 이더넷
NFC 확인를 요청한다
56b
CRCL
NFC 핸드쉐이킹
34
CRCL
등록 요청, 디바이스 ID
36
WiFi; WiMax; 이더넷
NFC 확인
58
WiFi; WiMax; 이더넷
새로운 디바이스에 대한 자격증명
60
CRCL
자격증명, 챌린지,
메시지, 시드 데이터
38
CRCL
등록 완료
키 전달을 확인하기 위한
자격증명에 기초한 챌린지 응답
40
WiFi; WiMax; 이더넷
보안 통신들
42b
WiFi; WiMax; 이더넷
보안 통신들
42b

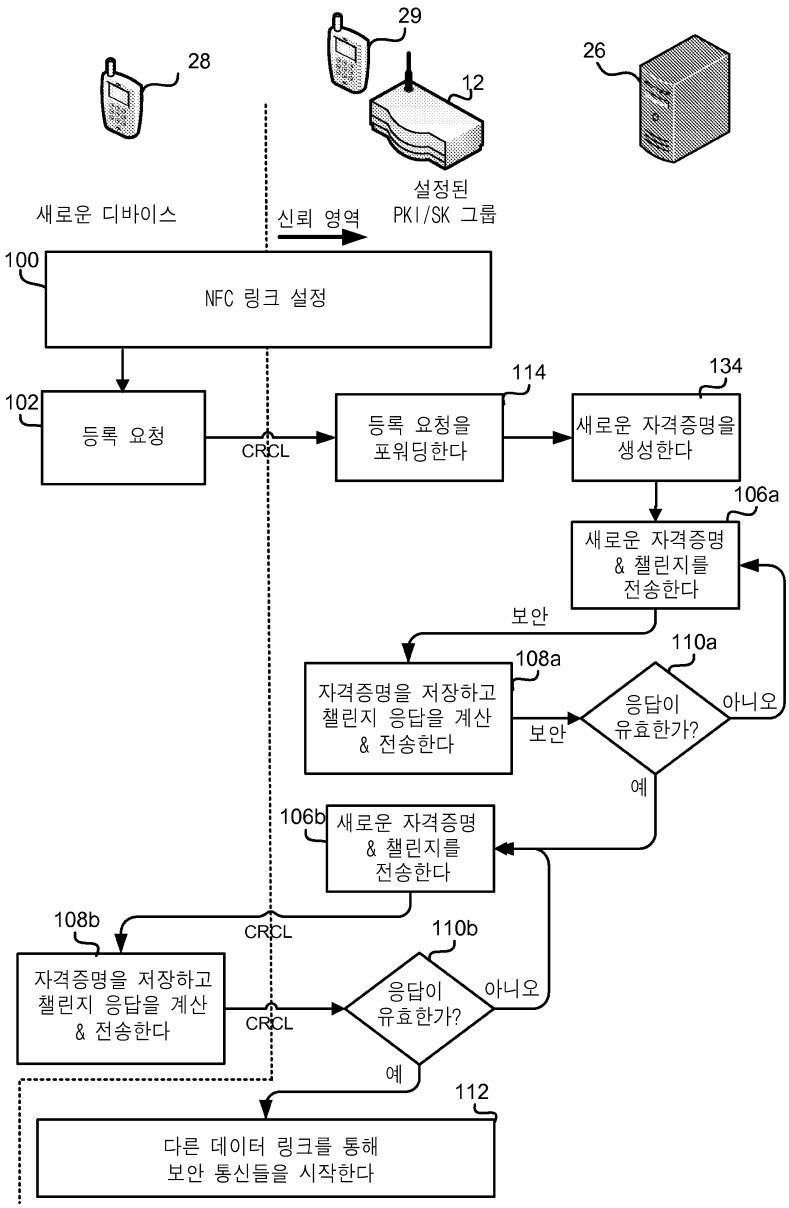
도면9


28
29
26
100a
NFC 링크 설정
102a
등록 요청
CRCL
106a
자격증명 &
챌린지 전송
CRCL
108a
자격증명을 저장하고
챌린지 응답을 계산
& 전송한다
CRCL
110a
응답이
유효한가?
아니오
예
신뢰 영역
100b
NFC 링크 설정
102b
등록 요청
CRCL
106b
자격증명 &
챌린지 전송
CRCL
108b
자격증명을 저장하고
챌린지 응답을 계산
& 전송한다
CRCL
110b
응답이
유효한가?
아니오
예
112 신뢰 영역
다른 데이터 링크를 통해
보안 통신들을 시작한다

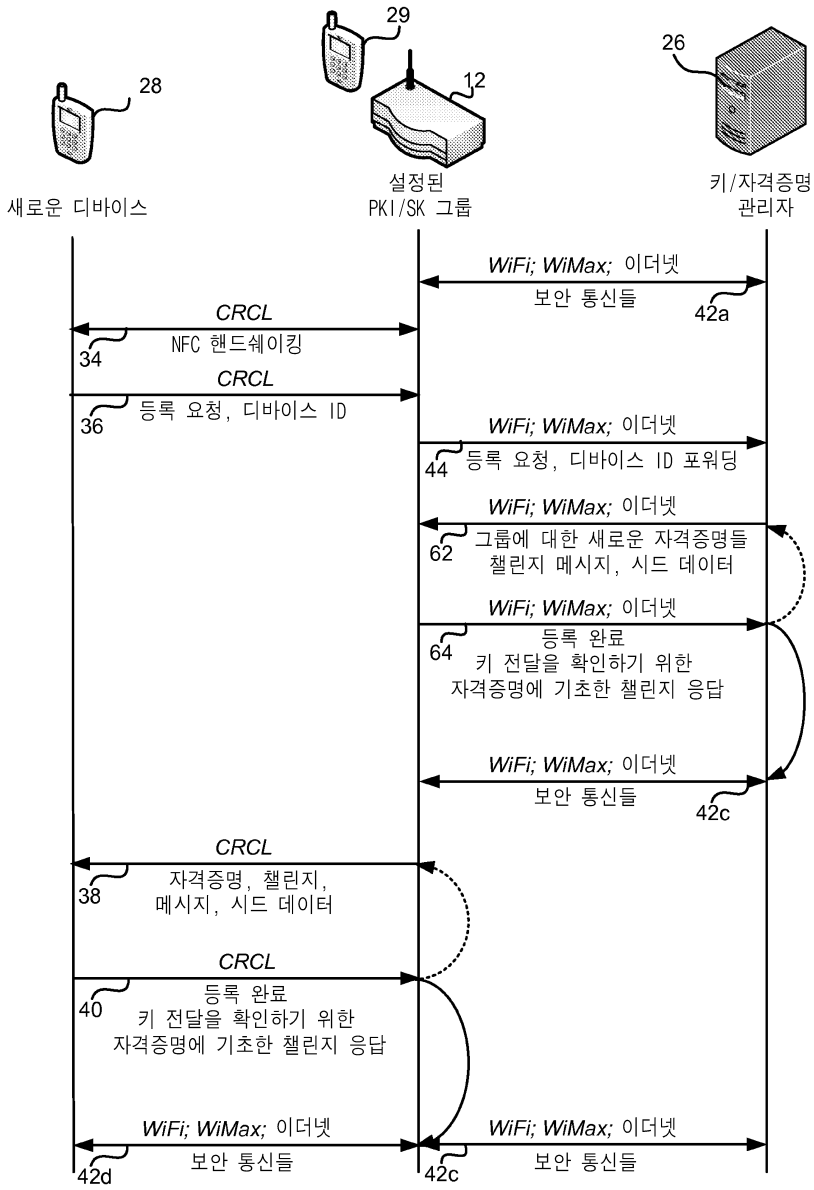
도면10


28
29
26
키/자격증명
관리자
CRCL
NFC 핸드쉐이킹
34a
CRCL
등록 요청, 디바이스 ID
36a
CRCL
자격증명, 챌린지,
메시지, 시드 데이터
38a
CRCL
등록 완료
키 전달을 확인하기 위한
자격증명에 기초한 챌린지 응답
40a
WiFi; WiMax; 이더넷
보안 통신들
42a
CRCL
NFC 핸드쉐이킹
34b
CRCL
등록 요청, 디바이스 ID
36b
CRCL
자격증명, 챌린지,
메시지, 시드 데이터
38b
CRCL
등록 완료
키 전달을 확인하기 위한
자격증명에 기초한 챌린지 응답
40b
WiFi; WiMax; 이더넷
보안 통신들
42b
WiFi; WiMax; 이더넷
보안 통신들
42a

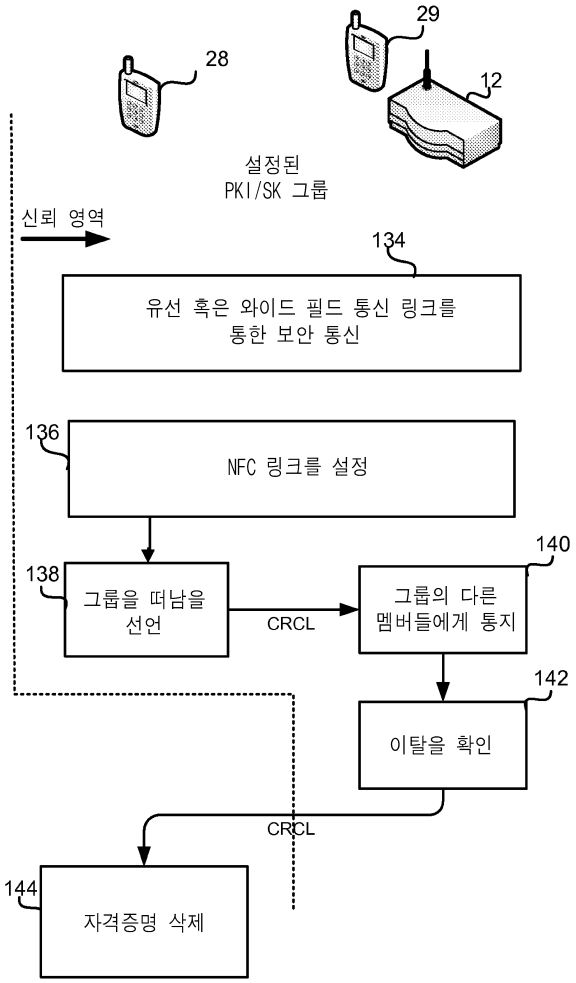
도면11


29
28
12
26
새로운 디바이스
신뢰 영역
설정된
PKI/SK 그룹
100
NFC 링크 설정
102
등록 요청
CRCL
114
등록 요청을
포워딩한다
134
새로운 자격증명을
생성한다
106a
새로운 자격증명
& 챌린지를
전송한다
보안
108a
자격증명을 저장하고
챌린지 응답을 계산
& 전송한다
보안
110a
응답이
유효한가?
아니오
예
106b
새로운 자격증명
& 챌린지를
전송한다
CRCL
108b
자격증명을 저장하고
챌린지 응답을 계산
& 전송한다
CRCL
110b
응답이
유효한가?
아니오
예
112
다른 데이터 링크를 통해
보안 통신들을 시작한다

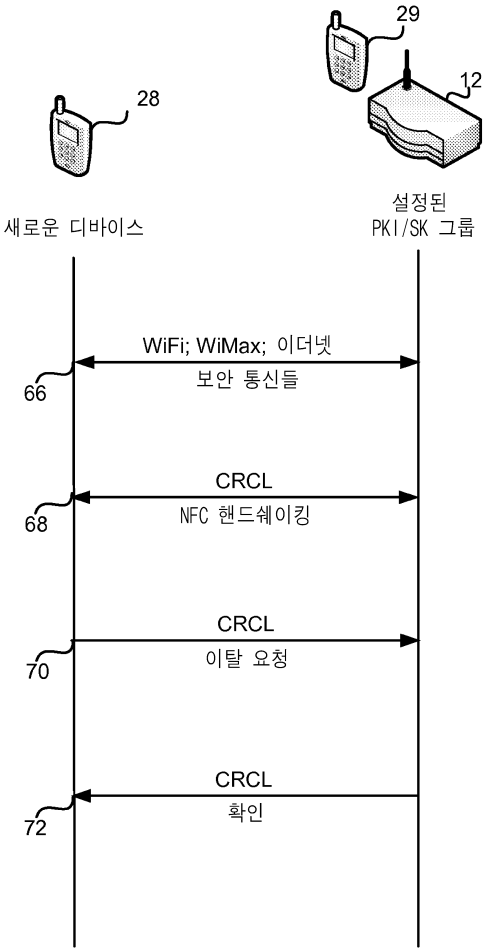
도면12


29
28
12
26
새로운 디바이스
설정된
PKI/SK 그룹
키/자격증명
관리자
WiFi; WiMax; 이더넷
보안 통신들
42a
CRCL
NFC 핸드쉐이킹
34
CRCL
등록 요청, 디바이스 ID
36
WiFi; WiMax; 이더넷
44
등록 요청, 디바이스 ID 포워딩
WiFi; WiMax; 이더넷
62
그룹에 대한 새로운 자격증명들
챌린지 메시지, 시드 데이터
WiFi; WiMax; 이더넷
64
등록 완료
키 전달을 확인하기 위한
자격증명에 기초한 챌린지 응답
WiFi; WiMax; 이더넷
보안 통신들
42c
CRCL
자격증명, 챌린지,
메시지, 시드 데이터
38
CRCL
40
등록 완료
키 전달을 확인하기 위한
자격증명에 기초한 챌린지 응답
WiFi; WiMax; 이더넷
보안 통신들
42d
WiFi; WiMax; 이더넷
보안 통신들
42c

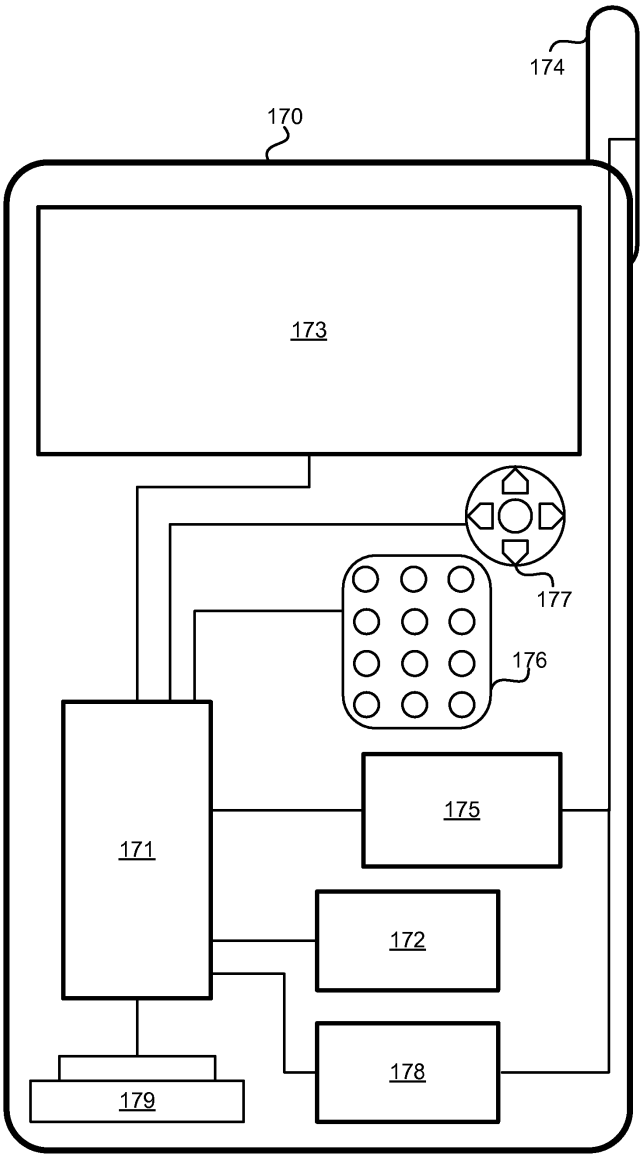
도면13


29
28
12
설정된
PKI/SK 그룹
신뢰 영역
134
유선 혹은 와이드 필드 통신 링크를
통한 보안 통신
136
NFC 링크를 설정
140
138
그룹을 떠남을
선언
CRCL
그룹의 다른
멤버들에게 통지
142
이탈을 확인
CRCL
144
자격증명 삭제

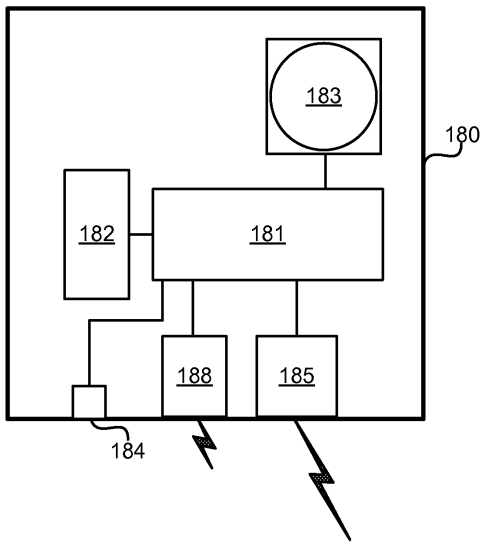
도면14


29
12
28
새로운 디바이스
설정된
PKI/SK 그룹
WiFi; WiMax; 이더넷
보안 통신들
66
CRCL
NFC 핸드쉐이킹
68
CRCL
이탈 요청
70
CRCL
확인
72

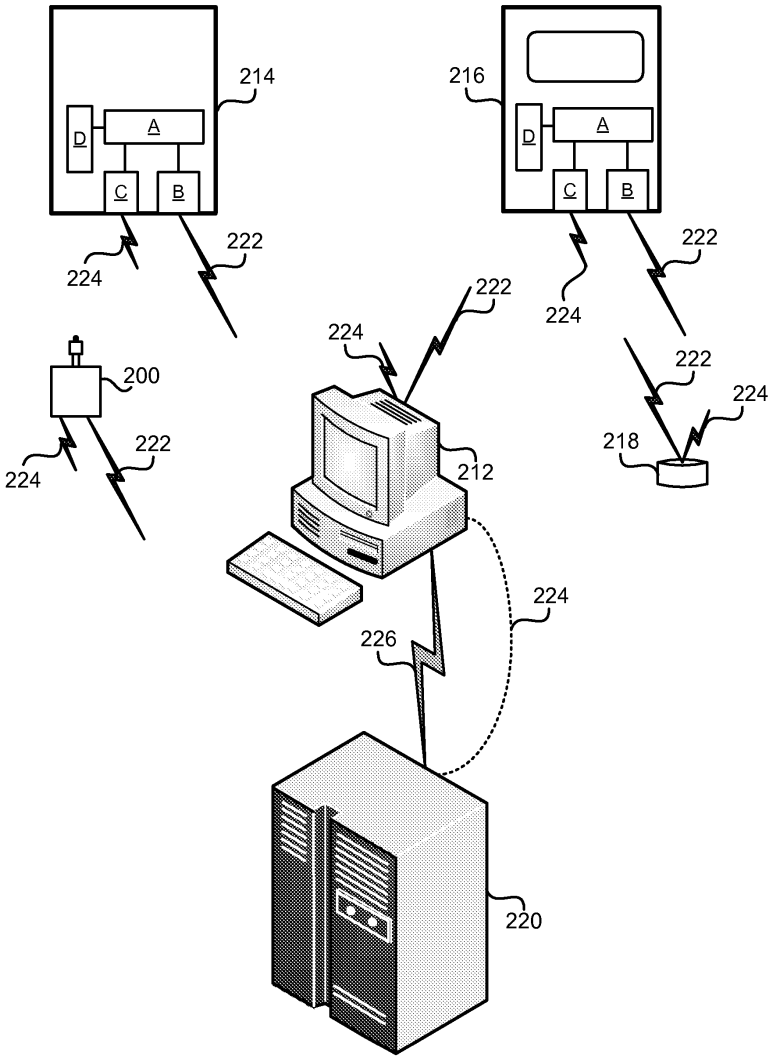
도면15



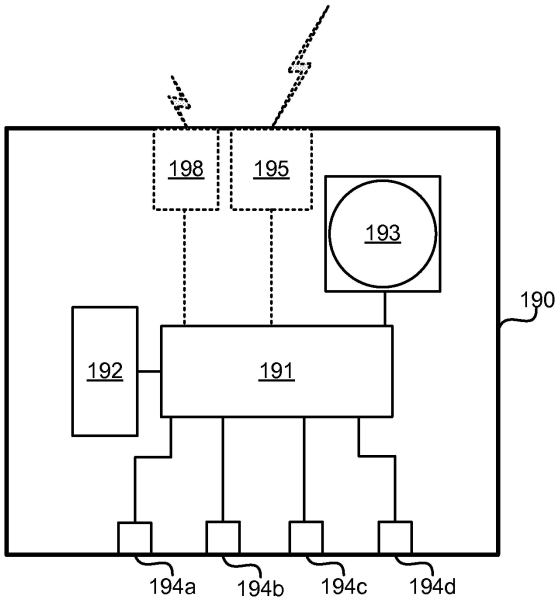
도면16



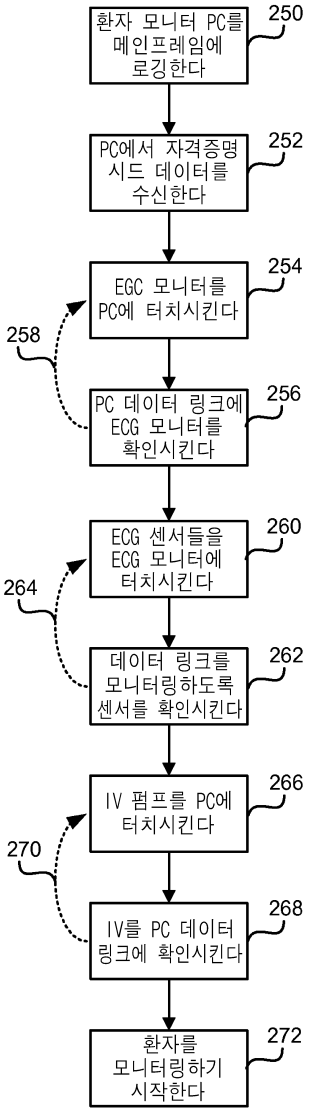
도면17


214
D
A
C
B
222
224
216
D
A
C
B
222
224
222
224
200
222
224
222
224
218
212
224
226
220

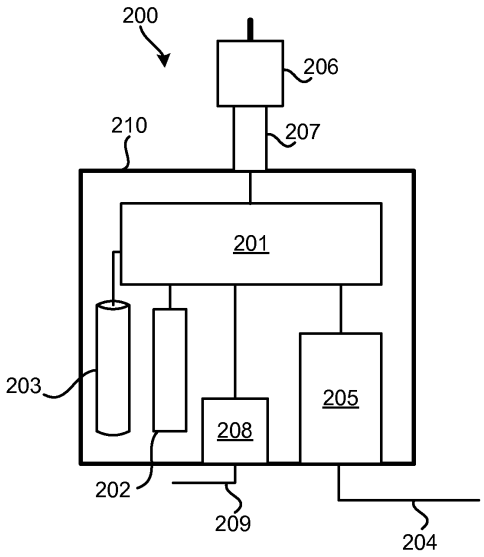
도면18



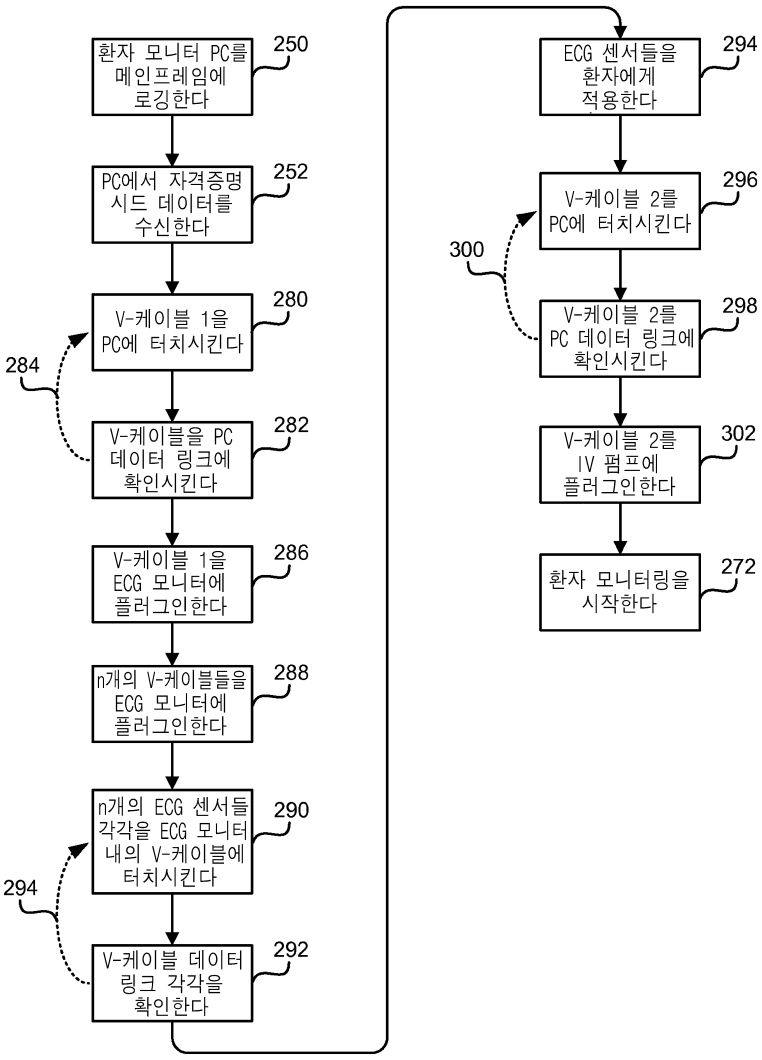
도면19


환자 모니터 PC를 메인프레임에 로깅한다
250
PC에서 자격증명 시드 데이터를 수신한다
252
EGC 모니터를 PC에 터치시킨다
254
258
PC 데이터 링크에 ECG 모니터를 확인시킨다
256
ECG 센서들을 ECG 모니터에 터치시킨다
260
264
데이터 링크를 모니터링하도록 센서를 확인시킨다
262
IV 펌프를 PC에 터치시킨다
266
270
IV를 PC 데이터 링크에 확인시킨다
268
환자를 모니터링하기 시작한다
272

도면20



도면21


환자 모니터 PC를 메인프레임에 로깅한다
250
PC에서 자격증명 시드 데이터를 수신한다
252
V-케이블 1을 PC에 터치시킨다
280
284
V-케이블을 PC 데이터 링크에 확인시킨다
282
V-케이블 1을 ECG 모니터에 플러그인한다
286
n개의 V-케이블들을 ECG 모니터에 플러그인한다
288
n개의 ECG 센서들 각각을 ECG 모니터 내의 V-케이블에 터치시킨다
290
294
V-케이블 데이터 링크 각각을 확인한다
292
ECG 센서들을 환자에게 적용한다
294
V-케이블 2를 PC에 터치시킨다
296
300
V-케이블 2를 PC 데이터 링크에 확인시킨다
298
V-케이블 2를 IV 펌프에 플러그인한다
302
환자 모니터링을 시작한다
272