



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년11월15일
(11) 등록번호 10-1083863
(24) 등록일자 2011년11월09일

- (51) Int. Cl.
HO4L 12/22 (2006.01) *HO4L 29/06* (2006.01)
- (21) 출원번호 10-2009-7014572
 (22) 출원일자(국제출원일자) 2007년12월05일
 심사청구일자 2009년07월13일
- (85) 번역문제출일자 2009년07월13일
 (65) 공개번호 10-2009-0088958
 (43) 공개일자 2009년08월20일
 (86) 국제출원번호 PCT/US2007/086504
 (87) 국제공개번호 WO 2008/073780
 국제공개일자 2008년06월19일
- (30) 우선권주장
 11/609,760 2006년12월12일 미국(US)
- (56) 선행기술조사문헌
 KR1020030047874 A*
 KR1020060046771 A*
 KR1020060123134 A
 KR1020060045365 A
 *는 심사관에 의하여 인용된 문헌
- (73) 특허권자
칼컴 인코포레이티드
 미국 캘리포니아 샌디에고 모어하우스
 드라이브5775 (우 92121-1714)
- (72) 발명자
치메이텔리, 마젠
 미국 92121 캘리포니아 샌디에고 모어하우스 드라
 이브 5775
- (74) 대리인
남상선

전체 청구항 수 : 총 48 항

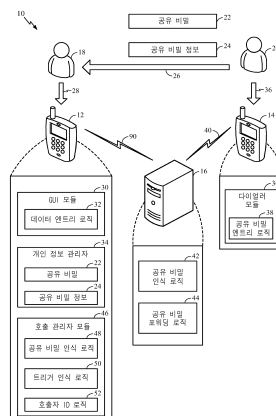
심사관 : 양찬호

(54) 호출자 식별 맞춤화 및 통신 디바이스들의 원격 관리를 위한 시스템들 및 방법들

(57) 요약

호출자들 및 피호출자들 사이의 공유 비밀 교환을 통해 통신 디바이스의 원격 기능 관리, 및 통신 디바이스에서 맞춤화된 호출자 ID를 구현하기 위한 방법들, 디바이스들, 시스템들, 및 컴퓨터 프로그램 물건들이 설명된다. 맞춤화된 호출자 ID는 호출자가 호출하기 위해 사용하는 디바이스와는 상관없이 자신들을 식별하도록 제공한다. 게다가, 호출 우선순위 태깅과 같은 다른 원격 기능 관리는 호출자가 호출의 우선 순위를 결정하거나, 또는 호출 ID 메시지를 피호출자에 맞춤화하도록 제공한다. 호출자들과 피호출자들 사이에서 공유 비밀들을 교환함으로써, 맞춤화된 호출자 ID 방법 및 원격 기능 관리는 보안되고, 그에 따라 알려지지 않은 자들에 의한 허가되지 않은 탬퍼링(tampering)의 가능성은 제거된다. 또한, 공유 비밀 교환은 예를 들어, 통신 디바이스를 오프 상태로 두거나 원격으로 로킹 다운시키는 것과 같이, 허가된 호출자들이 통신 디바이스에 원격으로 액세스하고 통신 디바이스를 관리하도록 제공한다.

대표도 - 도1



특허청구의 범위

청구항 1

통신 디바이스를 관리하기 위해 상기 통신 디바이스에 의해 수행되는 방법으로서,
 콘택(contact)과 연관된 공유 비밀을 포함하는 통신 호출을 수신하는 단계;
 상기 공유 비밀을 검증하는 단계; 및
 상기 검증된 공유 비밀과 연관된 통신 디바이스 기능을 수행하는 단계
 를 포함하는, 통신 디바이스를 관리하기 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 2

제 1 항에 있어서,
 상기 공유 비밀을 검증하는 단계는 상기 공유 비밀의 수신에 응답하여 미리 결정된 데이터베이스를 참조하는 단계, 및 상기 공유 비밀과 연관된 데이터베이스 내의 미리 결정된 엔트리를 참조하는 단계를 더 포함하는, 통신 디바이스를 관리하기 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 3

제 1 항에 있어서,
 상기 검증된 공유 비밀과 연관된 통신 디바이스 기능을 수행하는 단계는 상기 공유 비밀과 연관된 호출자를 식별하기 위해서 출력 신호를 제공하는 단계를 더 포함하는, 통신 디바이스를 관리하기 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 4

제 3 항에 있어서,
 상기 공유 비밀과 연관된 호출자를 식별하기 위해서 출력 신호를 제공하는 단계는 상기 공유 비밀과 연관된 호출자를 식별하기 위해서 호출자 식별을 디스플레이하는 단계를 더 포함하는, 통신 디바이스를 관리하기 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 5

제 3 항에 있어서,
 상기 공유 비밀과 연관된 호출자를 식별하기 위해서 출력 신호를 제공하는 단계는 상기 공유 비밀과 연관된 호출자를 식별하기 위해서 오디오 신호를 제공하는 단계를 더 포함하는, 통신 디바이스를 관리하기 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 6

제 1 항에 있어서,
 상기 검증된 공유 비밀과 연관된 통신 디바이스 기능을 수행하는 단계는 상기 호출의 우선순위를 식별하기 위해 출력 신호를 제공하는 단계를 더 포함하는, 통신 디바이스를 관리하기 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 7

제 6 항에 있어서,
 상기 호출의 우선순위를 식별하기 위해 출력 신호를 제공하는 단계는 상기 호출의 우선순위를 식별하기 위해 우선순위 메시지를 디스플레이하는 단계를 더 포함하는, 통신 디바이스를 관리하기 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 8

제 1 항에 있어서,

상기 검증된 공유 비밀과 연관된 통신 디바이스 기능을 수행하는 단계는 하나 이상의 통신 디바이스 기능들에 호출자 액세스를 제공하는 단계를 더 포함하는, 통신 디바이스를 관리하기 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 9

제 1 항에 있어서,

상기 검증된 공유 비밀과 연관된 통신 디바이스 기능을 수행하는 단계는 상기 디바이스를 오프 모드로 로킹(lock)하는 단계를 더 포함하는, 통신 디바이스를 관리하기 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 10

제 1 항에 있어서,

상기 공유 비밀을 포함하는 통신 호출을 수신하는 단계는 트리거 및 공유 비밀을 포함하는 통신 호출을 수신하는 단계를 더 포함하는, 통신 디바이스를 관리하기 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 11

제 10 항에 있어서,

상기 공유 비밀을 검증하는 단계는 상기 트리거와 연관된 미리 결정된 데이터베이스를 참조하는 단계, 및 상기 공유 비밀과 연관된 데이터베이스 내의 미리 결정된 엔트리를 참조하는 단계를 더 포함하는, 통신 디바이스를 관리하기 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 12

명령들의 시퀀스를 저장하는 컴퓨터 판독가능 매체로서,
 상기 명령들은 실행되는 경우, 컴퓨터 디바이스가,
 콘택과 연관된 공유 비밀을 포함하는 통신 호출을 수신하고;
 상기 공유 비밀을 검증하고; 그리고
 상기 공유 비밀의 검증에 기초하여 통신 디바이스 기능을 수행하는 동작들을 수행하도록 하는, 컴퓨터 판독가능 매체.

청구항 13

적어도 하나의 프로세서로서,
 콘택과 연관된 공유 비밀을 포함하는 통신 호출을 수신하고;
 상기 공유 비밀을 검증하고; 그리고
 상기 공유 비밀의 검증에 기초하여 통신 디바이스 기능을 수행하는 동작들을 수행하도록 구성된, 적어도 하나의 프로세서.

청구항 14

통신 디바이스로서,
 콘택과 연관된 공유 비밀을 포함하는 통신 호출을 수신하기 위한 수단;
 상기 공유 비밀을 검증하기 위한 수단; 및
 상기 검증된 공유 비밀과 연관된 통신 디바이스 기능을 수행하기 위한 수단

을 포함하는, 통신 디바이스.

청구항 15

통신 디바이스 상에서의 호출자 식별을 위해 상기 통신 디바이스에 의해 수행되는 방법으로서,
 콘택과 연관된 공유 비밀을 포함하는 통신 호출을 수신하는 단계;
 상기 공유 비밀과 연관된 콘택을 결정하기 위해서 데이터베이스에 액세스하는 단계; 및
 상기 공유 비밀과 연관된 콘택을 식별하는 출력 신호를 제공하는 단계
 를 포함하는, 통신 디바이스 상에서의 호출자 식별을 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 16

제 15 항에 있어서,
 상기 공유 비밀과 연관된 콘택을 식별하는 출력 신호를 제공하는 단계는 상기 공유 비밀과 연관된 콘택과 연관된 호출자 식별을 디스플레이하는 단계를 더 포함하는, 통신 디바이스 상에서의 호출자 식별을 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 17

제 15 항에 있어서,
 상기 공유 비밀과 연관된 콘택을 식별하는 출력 신호를 제공하는 단계는 상기 공유 비밀과 연관된 콘택과 연관된 오디오 신호를 제공하는 단계를 더 포함하는, 통신 디바이스 상에서의 호출자 식별을 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 18

제 15 항에 있어서,
 상기 공유 비밀을 포함하는 통신 호출을 수신하는 단계는 트리거 및 공유 비밀을 포함하는 통신 호출을 수신하는 단계를 더 포함하고,
 상기 공유 비밀과 연관된 콘택을 결정하기 위해서 데이터베이스에 액세스하는 단계는 상기 공유 비밀과 연관된 콘택을 결정하기 위해서 상기 트리거와 연관된 데이터베이스에 액세스하는 단계를 더 포함하는, 통신 디바이스 상에서의 호출자 식별을 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 19

제 15 항에 있어서,
 상기 공유 비밀과 연관된 통신 우선순위를 결정하기 위해서 데이터베이스에 액세스하는 단계를 더 포함하는, 통신 디바이스 상에서의 호출자 식별을 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 20

제 19 항에 있어서,
 상기 공유 비밀과 연관된 통신 우선순위를 식별하는 출력 신호를 제공하는 단계를 더 포함하는, 통신 디바이스 상에서의 호출자 식별을 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 21

제 20 항에 있어서,
 상기 공유 비밀과 연관된 통신 우선순위를 식별하는 출력 신호를 제공하는 단계는 상기 공유 비밀과 연관된 메시지를 식별하는 통신 우선순위를 디스플레이하는 단계를 더 포함하는, 통신 디바이스 상에서의 호출자 식별을 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 22

제 20 항에 있어서,

상기 공유 비밀과 연관된 통신 우선순위를 식별하는 출력 신호를 제공하는 단계는 상기 공유 비밀과 연관된 통신 우선순위를 식별하는 오디오 신호를 제공하는 단계를 더 포함하는, 통신 디바이스 상에서의 호출자 식별을 위해 상기 통신 디바이스에 의해 수행되는 방법.

청구항 23

통신 디바이스로서,

공유 비밀 정보와 공유 비밀들을 연관시키는 하나 이상의 데이터베이스들을 포함하는 개인 정보 관리자; 및

통신 호출에서의 콘택과 연관된 공유 비밀을 인식하고, 상기 공유 비밀과 연관된 공유 비밀 정보를 결정하기 위해서 적어도 하나의 데이터베이스에 액세스하도록 동작가능한 공유 비밀 인식 로직, 및 상기 공유 비밀 및 공유 비밀 정보 중 적어도 하나에 기초하여 통신 디바이스 기능을 수행하도록 동작가능한 공유 비밀 기능 로직을 포함하는 호출 관리자 모듈

을 포함하는, 통신 디바이스.

청구항 24

제 23 항에 있어서,

상기 공유 비밀 기능 로직은 상기 공유 비밀과 연관된 호출자를 식별하고, 상기 호출자를 식별하기 위해서 출력 신호를 제공하도록 동작가능한 호출자 식별 로직을 더 포함하는, 통신 디바이스.

청구항 25

제 24 항에 있어서,

상기 호출자를 식별하기 위해서 출력 신호를 제공하도록 동작가능한 호출자 식별 로직은 상기 공유 비밀과 연관된 호출자를 식별하기 위해서 호출자 식별을 디스플레이하도록 추가적으로 동작가능한, 통신 디바이스.

청구항 26

제 24 항에 있어서,

상기 호출자를 식별하기 위해서 출력 신호를 제공하도록 동작가능한 호출자 식별 로직은 상기 공유 비밀과 연관된 호출자를 식별하기 위해서 오디오 신호를 제공하도록 추가적으로 동작가능한, 통신 디바이스.

청구항 27

제 23 항에 있어서,

상기 공유 비밀 기능 로직은, 상기 공유 비밀에 기초하여 상기 통신 호출의 우선순위를 식별하고 우선순위 메시지를 디스플레이하도록 동작가능한 호출 우선순위 로직을 더 포함하는, 통신 디바이스.

청구항 28

제 23 항에 있어서,

상기 공유 비밀 기능 로직은, 상기 공유 비밀에 기초하여 상기 통신 호출의 우선순위를 식별하고 상기 식별된 우선순위와 연관된 오디오 신호를 제공하도록 동작가능한 호출 우선순위 로직을 더 포함하는, 통신 디바이스.

청구항 29

제 23 항에 있어서,

상기 공유 비밀 기능 로직은, 상기 공유 비밀에 기초하여 통신 디바이스 기능에 호출자 액세스를 제공하도록 동작가능한 통신 디바이스 관리 로직을 더 포함하는, 통신 디바이스.

청구항 30

제 23 항에 있어서,

상기 공유 비밀 기능 로직은 상기 공유 비밀에 기초하여 상기 통신 디바이스를 로킹 다운(lock down)하도록 동작가능한 통신 디바이스 로킹-다운 로직을 포함하는, 통신 디바이스.

청구항 31

통신 디바이스로서,

공유 비밀들 및 연관된 공유 비밀 정보를 저장하기 위한 수단;

통신 호출에서의 콘택과 연관된 공유 비밀을 인식하기 위한 수단;

상기 공유 비밀과 연관된 공유 비밀 정보를 결정하기 위해서 상기 저장하기 위한 수단에 액세스하기 위한 수단; 및

상기 공유 비밀 및 공유 비밀 정보 중 적어도 하나에 기초하여 통신 디바이스 기능을 수행하기 위한 수단을 포함하는, 통신 디바이스.

청구항 32

통신 디바이스로서,

공유 비밀과 콘택을 연관시키는 콘택 데이터베이스; 및

통신 호출에서의 콘택과 연관된 공유 비밀을 인식하고, 상기 공유 비밀과 연관된 콘택을 결정하기 위해서 상기 콘택 데이터베이스에 액세스하도록 동작가능한 공유 비밀 인식 로직, 및 상기 공유 비밀과 연관된 콘택을 호출자로서 식별하는 출력 신호를 제공하도록 동작가능한 호출자 식별 로직을 포함하는 호출 관리자 모듈

을 포함하는, 통신 디바이스.

청구항 33

제 32 항에 있어서,

상기 호출자 식별 로직은 상기 공유 비밀과 연관된 콘택과 연관된 호출자 식별을 디스플레이하도록 추가적으로 동작가능한, 통신 디바이스.

청구항 34

제 33 항에 있어서,

상기 호출자 식별 로직은 상기 공유 비밀과 연관된 콘택을 식별하는 오디오 신호를 제공하도록 추가적으로 동작가능한, 통신 디바이스.

청구항 35

제 32 항에 있어서,

상기 공유 비밀에 기초하여 호출 우선순위를 식별하도록 동작가능한 호출 우선순위 로직을 더 포함하는, 통신 디바이스.

청구항 36

네트워크 디바이스에서의 통신 디바이스 관리를 제공하기 위한 방법으로서,

호출 디바이스 식별 번호 및 콘택과 연관된 공유 비밀을 포함하는 통신 호출 요청을 상기 네트워크 디바이스에서 수신하는 단계; 및

상기 호출 디바이스 식별 번호 및 상기 공유 비밀을 포함하는 호출 요청을 피호출자에게 전달하는 단계를 포함하는, 통신 디바이스 관리를 제공하기 위한 방법.

청구항 37

제 36 항에 있어서,

상기 호출 디바이스 식별 번호 및 공유 비밀을 포함하는 통신 호출 요청을 네트워크 디바이스에서 수신하는 단계는, 호출 디바이스 식별 번호, 트리거, 및 공유 비밀을 포함하는 통신 호출 요청을 네트워크 디바이스에서 수신하는 단계를 더 포함하는, 통신 디바이스 관리 제공 방법.

청구항 38

제 37 항에 있어서,

상기 호출 디바이스 식별 번호 및 공유 비밀을 포함하는 호출 요청을 피호출자에게 전달하는 단계는, 상기 호출 디바이스 식별 번호, 상기 트리거, 및 상기 공유 비밀을 포함하는 호출 요청을 피호출자에게 전달하는 단계를 더 포함하는, 통신 디바이스 관리를 제공하기 위한 방법.

청구항 39

제 36 항에 있어서,

상기 피호출자는 상기 호출 요청을 수신하고, 상기 공유 비밀을 검증하고, 상기 공유 비밀과 연관된 통신 디바이스 기능을 수행하는, 통신 디바이스 관리를 제공하기 위한 방법.

청구항 40

제 36 항에 있어서,

상기 피호출자는 상기 호출 요청을 수신하고, 상기 공유 비밀을 검증하고, 상기 공유 비밀과 연관된 호출자를 식별하는 출력 신호를 제공하는, 통신 디바이스 관리를 제공하기 위한 방법.

청구항 41

명령들의 시퀀스를 저장하는 컴퓨터 판독가능 매체로서,

상기 명령들은 실행되는 경우, 컴퓨터 디바이스가,

호출 디바이스 식별 번호 및 콘택과 연관된 공유 비밀을 포함하는 통신 호출 요청을 네트워크 디바이스에서 수신하고; 그리고

상기 호출 디바이스 식별 번호 및 상기 공유 비밀을 포함하는 호출 요청을 피호출자에게 전달하는 동작들을 수행하도록 하는, 컴퓨터 판독가능 매체.

청구항 42

적어도 하나의 프로세서로서,

호출 디바이스 식별 번호 및 콘택과 연관된 공유 비밀을 포함하는 통신 호출 요청을 네트워크 디바이스에서 수신하고; 그리고

상기 호출 디바이스 식별 번호 및 상기 공유 비밀을 포함하는 호출 요청을 피호출자에게 전달하는 동작들을 수행하도록 구성된, 적어도 하나의 프로세서.

청구항 43

통신 네트워크에서 호출자 식별을 식별하기 위한 방법으로서,

호출 디바이스 식별 번호 및 콘택과 연관된 공유 비밀을 포함하는 통신 호출 요청을 네트워크 디바이스에서 수신하는 단계; 및

상기 공유 비밀과 연관된 호출자 식별을 결정하기 위해서 클라이언트 데이터베이스를 참조하는 단계; 및
 상기 공유 비밀과 연관된 호출자 식별을 포함하는 호출 요청을 피호출자에게 전달하는 단계

를 포함하는, 호출자 식별을 식별하기 위한 방법.

청구항 44

제 43항에 있어서,

상기 공유 비밀과 연관된 호출 우선순위를 결정하기 위해서 미리 결정된 데이터베이스를 참조하는 단계를 더 포함하는, 호출자 식별을 식별하기 위한 방법.

청구항 45

제 44항에 있어서,

상기 공유 비밀과 연관된 호출자 식별을 포함하는 호출 요청을 피호출자에게 전달하는 단계는 상기 호출 우선순위를 포함하는 호출 요청을 피호출자에게 전달하는 단계를 더 포함하는, 호출자 식별을 식별하기 위한 방법.

청구항 46

네트워크 디바이스로서,

통신 호출 요청에서의 콘택과 연관된 공유 비밀을 인식하도록 동작가능한 공유 비밀 인식 로직, 및 상기 통신 호출 요청과 연관된 상기 공유 비밀을 피호출자에게 전달하도록 동작가능한 공유 비밀 포워딩 로직을 포함하는 공유 비밀 포워딩 로직을 포함하는, 네트워크 디바이스.

청구항 47

네트워크 디바이스로서,

호출자 식별과 공유 비밀들을 연관시키는 클라이언트 데이터베이스;

호출 요청에서의 콘택과 연관된 공유 비밀을 인식하고, 상기 공유 비밀과 연관된 호출자 식별을 결정하기 위해서 상기 클라이언트 데이터베이스를 참조하도록 동작가능한 공유 비밀 인식 로직을 포함하는 공유 비밀 모듈; 및

상기 공유 비밀과 연관된 호출자 식별을 포함하는 호출 요청을 피호출자에게 전달하도록 동작가능한 통신 모듈을 포함하는, 네트워크 디바이스.

청구항 48

네트워크 디바이스로서,

호출 디바이스 식별 번호 및 콘택과 연관된 공유 비밀을 포함하는 통신 호출 요청을 수신하기 위한 수단; 및

상기 호출 디바이스 식별 번호 및 상기 공유 비밀을 포함하는 호출 요청을 피호출자에게 전달하기 위한 수단을 포함하는, 네트워크 디바이스.

명세서

기술분야

[0001] 본 발명은 호출자 식별 시스템들에 관한 것이며, 특히, 호출자 식별의 주문형 맞춤화(on demand customization)를 위한 시스템들 및 방법들에 관한 것이다.

배경기술

[0002] 먼저, 호출자 ID 라고도 지칭되는, 호출자 식별은 1980년대 초에 처음 발명되었고, 1990년대에 상업적으로 널리 이용가능하게 되었다. 오늘날, 호출자 ID는 유선(즉, 지상통신선(landline)) 및 무선 통신 디바이스들 모두에 이용가능하다.

[0003] 종래의 호출자 ID에서, 전화 회사와 같은 서비스 제공자는 링 신호 데이터(ring signal data)와 인터트와인(intertwine)된 ASCII(American Standard Code for Information Interchange) 문자 데이터를 전송하기 위해서

주파수 편이(Frequency Key Shift: FSK) 기술을 구현한다. 호출 수신 디바이스 내의 모뎀은 링 신호 및 호출자 ID 정보와 같은 호출 전송에서의 비트들을 디코딩한다. 호출자 ID 정보는 호출 디바이스(calling device) 식별 번호(예를 들어, 호출 디바이스 전화 번호)를 포함할 수 있으며, 일부 양상들에서, 호출 디바이스 전화 번호와 연관된 사용자의 이름을 포함할 수 있다.

[0004] 이에 비해, 무선 통신 디바이스에서, 호출자 ID는 디바이스의 전화번호부 또는 콘택 목록들(contact listings) 내의 엔트리들과 무선으로 수신된 전화 번호(air phone number)를 매칭시킴으로써 구현된다. 전화번호부 또는 콘택 목록에서의 매치가 검색되는 경우, 전화 번호와 연관된 이름이 무선 디바이스에 디스플레이된다.

[0005] 그러나, 종래의 호출자 ID 서비스 및 무선 통신 호출자 ID 시스템 모두에서, 호출자 식별은 전화 번호와 전형적으로 연관된 호출자를 식별하는 것으로 한정된다. 예를 들어, 종래의 호출자 ID는 서비스 제공자에 등록된 자 (party)를 수신 디바이스의 전화번호부 또는 콘택 목록 내의 전화 번호의 "소유자" 또는 상기 전화 번호와 연관된 자로서 식별한다. 이로서, 공지된 호출자 ID 시스템들은 실제 호출자가 서비스 제공자에 등록된 자, 또는 수신 디바이스의 전화번호부 또는 콘택 목록 내의 전화 번호와 연관된 자와는 다른 누군가인 상황을 수용하지 않는다.

[0006] 예를 들어, 호출할 필요가 있는 누군가가 유선 또는 무선 전화를 차용한 상황에서, 호출 전화 번호가 수신 디바이스의 전화번호부에서 이름과 연관하여 존재하지 않을 것이므로, 호출을 수신하는 무선 디바이스는 전형적으로 호출 전화 번호만을 디스플레이할 것이다. 마찬가지로, 수신 디바이스가 유선 통신 디바이스인 경우, 호출자 ID 기능은 실제 호출자의 이름이 아닌 전화 번호와 연관된 자의 이름을 표시하는 데이터를 디스플레이할 것이다.

[0007] 따라서, 수신자가 디스플레이된 전화 번호 및/또는 전화 번호와 연관된 자의 이름을 알지 못하는 문제가 발생하고, 그에 따라 수신자는 해당 호출을 무시하기로 결정할 수 있다. 많은 예들에서, 이러한 문제는 호출이 가장 중요하며, 피호출자(called party)와 즉시 통신할 수 있는 것이 중요한 경우, 누군가가 전화를 차용하여 호출할 때 악화될 수 있다.

[0008] 추가적으로, 현재 호출자 ID 시스템들은 수신자가 호출에 응답하는 것을 보장하기 위해서 호출의 중요도에 대한 우선순위 결정을 제공하지 않는다. 이러한 통신들의 우선순위 결정은, 붉은 플래그들(red flags) 또는 느낌표들을 사용하여 메시지가 높은 우선순위를 가지고 있음을 나타내는, 전자 메일과 같은, 통신의 다른 형태들에서는 일반적인 일이다. 이에 관하여, 수신측으로 통신들의 중요도를 하이라이트하기 위해서 우선순위를 결정하는 것이 바람직할 수 있다. 가상의 지상통신선 전화(land-line telephone hypothetical)에서, 근무일 동안 빈번한 호출들에 의해 부담을 갖는 수신자는 일상적으로 이러한 호출들을 무시하도록 결정할 수 있고, 호출자가 음성 메일을 남기게 하도록 선택할 수 있다. 그러나, 호출의 중요도가 높은 우선순위를 보증한다는 것을 수신자에게 시그널링하기 위한 수단을 호출자가 제공받을 경우, 수신자는 이러한 시그널링을 고려하여 호출에 즉시 응답하기가 보다 쉬울 수 있다.

[0009] 그러나, 피호출자가 호출자들 신원을 아는 것을 보장하도록 호출자가 호출자 ID 정보를 맞춤화하기를 희망하는 상황에서, 그리고 피호출자가 호출에 응답하는 것을 보장하기 위해서 호출자가 호출의 우선순위를 결정하기를 희망하는 상황에서, 사기꾼들, 텔레마케터들 등과 같은, 허가되지 않은 호출자들이 자신의 호출자 ID 정보를 맞춤화하거나, 자신들의 호출들의 우선순위를 결정하기 위해 액세스하지 않는 것을 보장하는 것이 바람직할 수 있다. 이에 관하여, 보안은 사기꾼들이 자신들이 알려진 자 또는 중요한 호출자라는 것을 신뢰성 없는 정보에 기초하여 수신자가 믿도록 속이지 않는 것을 보장하는데 유용할 수 있다.

[0010] 따라서, 맞춤화된 호출자 식별을 제공하는 방법들 및 시스템들에 대한 필요성이 존재한다. 시스템의 맞춤화 양상은 호출자가 호출 통신 디바이스와 연관된 기존 호출자 ID 정보를 무시(override)하도록 제공할 수 있다. 게다가, 맞춤화는 호출이 중요도를 높였다는 것을 수신자에게 경고하기 위해서 호출자가 호출들의 우선순위를 결정하도록 제공할 수 있다.

발명의 상세한 설명

[0011] 무선 디바이스들의 원격 보안된 관리 및 맞춤화된 호출자 ID를 제공하는 시스템들, 방법들, 디바이스들, 및 컴퓨터 프로그램들이 제공된다. 본 양상들은 호출자와 피호출자 사이의 공유 비밀을 이용하여, 피호출 통신 디바이스의 원격 관리 및/또는 맞춤화된 호출자 식별을 허용한다. 이에 관하여, 호출자가 대안적인 통신 디바이스 (즉, 호출자 소유의 디바이스가 아닌 디바이스)를 사용하는 경우들에서, 호출자는 자신을 식별할 수 있다. 추가적으로, 호출자가 맞춤화된 메시지의 우선 순위를 결정하거나, 호출자에게 맞춤화된 메시지를 제공하도록 맞

축화된 호출자 ID가 제공된다. 또한, 공유 비밀들은 통신 디바이스의 보안된 원격 관리 및 제어를 제공하고, 통신 디바이스 사용자가 통신 디바이스에 원격으로 액세스하여, 디바이스에서 이용가능한 기능들을 수행하거나, 디바이스를 오프 모드(off mode)로 두거나, 로킹-다운(lock-down)할 권한을 허가할 수 있게 한다.

- [0012] 일 양상에서, 통신 디바이스의 원격 관리를 위한 방법이 정의된다. 상기 방법은 공유 비밀 데이터를 포함하는 통신 호출을 수신하는 단계, 공유 비밀을 검증하는 단계, 및 검증된 공유 비밀과 연관된 통신 디바이스 기능을 수행하는 단계를 포함한다. 공유 비밀 데이터를 포함하는 통신 호출을 수신하는 동작은 트리거 및 공유 비밀을 포함하는 통신을 수신하는 동작에 의해 추가적으로 정의될 수 있다. 공유 비밀을 검증하는 동작은 공유 비밀의 수신에 응답하여 미리 결정된 데이터베이스를 참조하는 동작, 및 공유 비밀과 연관된 데이터베이스 내의 미리 결정된 엔트리를 참조하는 동작에 의해 추가적으로 정의될 수 있다. 통신 호출이 트리거 및 공유 비밀 데이터를 포함하는 양상들에서, 공유 비밀을 검증하는 동작은 트리거와 연관된 미리 결정된 데이터베이스를 참조하는 동작, 및 공유 비밀과 연관된 데이터베이스 내의 미리 결정된 엔트리를 참조하는 동작에 의해 추가적으로 정의될 수 있다.
- [0013] 검증된 공유 비밀과 연관된 통신 디바이스 기능을 수행하는 동작은 공유 비밀과 연관된 호출자를 식별하기 위해서 시각적 디스플레이 또는 오디오 신호와 같은 출력 신호의 동작에 의해 추가적으로 정의될 수 있다. 추가적으로, 검증된 공유 비밀과 연관된 통신 디바이스 기능을 수행하는 동작은 높은 또는 긴급한 우선순위와 같은 호출의 우선순위를 식별하기 위해서 시각적 디스플레이 또는 오디오 신호와 같은 출력 신호의 동작에 의해 추가적으로 정의될 수 있다. 또한, 검증된 공유 비밀과 연관된 통신 디바이스 기능을 수행하는 동작은, 하나 이상의 통신 디바이스 기능들에 호출자 액세스를 제공하거나, 디바이스를 오프 모드로 로킹(locking)하는 기능을 호출자에게 제공하는 동작에 의해 추가적으로 정의될 수 있다.
- [0014] 다른 양상은 실행되는 경우, 컴퓨터 디바이스가 공유 비밀 데이터를 포함하는 통신 호출을 수신하고, 공유 비밀을 검증하며, 공유 비밀의 검증에 기초하여 통신 디바이스 기능을 수행하는 동작들을 수행하도록 하는 명령들의 시퀀스를 실제적으로(tangibly) 저장하는 컴퓨터 판독가능 매체에 의해 정의된다.
- [0015] 관련된 양상은 공유 비밀 데이터를 포함하는 통신 호출을 수신하고, 공유 비밀을 검증하며, 공유 비밀의 검증에 기초하여 통신 디바이스 기능을 수행하는 동작들을 수행하도록 구성된 적어도 하나의 프로세서에 의해 정의된다.
- [0016] 본 발명의 다른 양상은 통신 디바이스 상에서의 호출자 식별을 위한 방법을 포함한다. 상기 방법은 공유 비밀 데이터를 포함하는 통신 호출을 수신하는 단계, 공유 비밀과 연관된 콘택을 결정하기 위해서 데이터베이스에 액세스하는 단계, 및 공유 비밀과 연관된 콘택을 식별하는 출력 신호를 제공하는 단계를 포함한다. 출력 신호는 호출자 식별의 디스플레이, 오디오 신호, 또는 임의의 다른 적합한 출력 신호를 포함할 수 있다. 공유 비밀 데이터를 포함하는 통신 호출을 수신하는 동작은 트리거 및 공유 비밀을 포함하는 통신 호출을 수신하는 동작에 의해 추가적으로 정의될 수 있다. 이러한 양상들에서, 공유 비밀과 연관된 콘택을 결정하기 위해서 데이터베이스에 액세스하는 동작은 공유 비밀과 연관된 콘택을 결정하기 위해서 트리거와 연관된 데이터베이스에 액세스하는 것으로 추가적으로 정의된다. 콘택을 식별하기 위해 출력 신호를 제공하는 것 뿐만 아니라, 공유 비밀 데이터는 공유 비밀 데이터와 연관된 통신 우선순위를 결정하기 위해서 데이터베이스에 액세스하는 것, 및 공유 비밀과 연관된 통신 우선순위를 식별하는, 호출 우선순위의 디스플레이 또는 오디오 신호와 같은, 출력 신호를 제공하는 것을 추가적으로 제공할 수 있다.
- [0017] 다른 양상은 공유 비밀 정보와 공유 비밀들을 연관시키는 하나 이상의 데이터베이스들을 포함하는 개인 정보 관리자를 포함하는 통신 디바이스에 의해 제공된다. 통신 디바이스는 통신 호출에서의 공유 비밀을 인식하고, 공유 비밀과 연관된 공유 비밀 정보를 결정하기 위해서 콘택 데이터베이스에 액세스하도록 동작가능한 공유 비밀 인식 로직, 및 공유 비밀 및 공유 비밀 정보 중 적어도 하나에 기초하여 통신 디바이스 기능을 수행하도록 동작가능한 공유 비밀 기능 로직을 포함하는 호출 관리자 모듈을 더 포함한다. 공유 비밀 기능 로직은 공유 비밀과 연관된 호출자를 식별하고, 호출자를 식별하는, 시각적 디스플레이 또는 오디오 신호와 같은, 출력 신호를 제공하도록 동작가능한 호출자 식별 로직에 의해 정의될 수 있다. 다른 양상들에서, 공유 비밀 기능 로직은 공유 비밀에 기초하여 통신 호출의 우선순위를 식별하고, 호출의 우선순위를 식별하는, 시각적 디스플레이 또는 오디오 신호와 같은, 출력 신호를 제공하도록 동작가능한 호출 우선순위 로직에 의해 정의될 수 있다. 추가적으로, 공유 비밀 기능 로직은 공유 비밀에 기초하여 통신 디바이스 기능에 호출자 액세스를 제공하도록 동작가능한 통신 디바이스 관리 로직에 의해 정의될 수 있다. 추가적으로, 공유 비밀 기능 로직은 공유 비밀에 기초하여 통신 디바이스를 로킹 다운하도록 동작가능한 통신 디바이스 로킹-다운 로직에 의해 정의될 수 있다.

- [0018] 다른 양상에서, 공유 비밀과 콘택을 연관시키는 콘택 데이터베이스를 포함하는 통신 디바이스가 제공된다. 통신 디바이스는 통신 호출에서의 공유 비밀을 인식하고, 공유 비밀과 연관된 콘택을 결정하기 위해서 콘택 데이터베이스에 액세스하도록 동작가능한 공유 비밀 인식 로직, 및 공유 비밀과 연관된 콘택을 호출자로서 식별하는, 시각적 디스플레이 또는 오디오 신호와 같은, 출력 신호를 제공하고, 콘택을 호출자로서 식별하는 출력 신호를 제공하도록 동작가능한 호출자 식별 로직을 포함하는 호출 관리자 모듈을 더 포함한다. 추가적으로, 호출 관리자 모듈은 공유 비밀에 기초하여 호출 우선순위를 식별하는, 시각적 디스플레이 또는 오디오 신호와 같은, 출력 신호를 제공하도록 동작가능한 호출 우선순위 로직을 포함할 수 있다.
- [0019] 다른 양상들은 기지국 등에 상주하는 서버와 같은 네트워크 디바이스에 의하여 정의된다. 일 양상에서, 네트워크 디바이스를 통해 통신 디바이스에 원격 액세스를 제공하기 위한 방법이 정의된다. 상기 방법은 호출 디바이스 식별 번호 및 공유 비밀을 포함하는 통신 호출 요청을 네트워크 디바이스에서 수신하는 단계, 및 호출 디바이스 식별 번호 및 공유 비밀을 포함하는 호출 요청을 피호출자에게 전달하는 단계를 포함한다. 또한, 상기 방법은 호출 디바이스 식별 번호 및 공유 비밀 뿐만 아니라, 트리거를 수신하는 단계, 및 호출 요청과 함께 트리거를 피호출자에게 전달하는 단계를 제공하는 단계를 포함할 수 있다.
- [0020] 관련된 양상은 실행되는 경우, 컴퓨터 디바이스가 호출 디바이스 식별 번호 및 공유 비밀을 포함하는 통신 호출 요청을 네트워크 디바이스에서 수신하고, 호출 디바이스 식별 번호 및 공유 비밀을 포함하는 호출 요청을 피호출자에게 전달하는 동작들을 수행하도록 하는 명령들의 시퀀스를 실제로 저장하는 컴퓨터 판독가능 매체에 의해 정의된다.
- [0021] 다른 관련된 양상은 호출 디바이스 식별 번호 및 공유 비밀을 포함하는 통신 호출 요청을 네트워크 디바이스에서 수신하고, 호출 디바이스 식별 번호 및 공유 비밀을 포함하는 호출 요청을 피호출자에게 전달하는 동작들을 수행하도록 구성된 적어도 하나의 프로세서에 의해 정의된다.
- [0022] 다른 양상은 기지국 등에서 상주하는 서버와 같은 네트워크 디바이스에 의해 제공된다. 상기 디바이스는 통신 호출 요청에서의 공유 비밀을 인식하도록 동작가능한 공유 비밀 인식 로직, 및 통신 호출 요청과 연관된 공유 비밀을 피호출자에게 전달하도록 동작가능한 공유 비밀 포워딩 로직을 포함하는 공유 비밀 포워딩 모듈을 포함한다.
- [0023] 따라서, 설명된 양상들은 호출자들 및 피호출자들 사이에서 공유 비밀 교환을 구현함으로써 디바이스 기능의 원격 관리를 수행하거나, 호출자 ID를 맞춤화하기 위한 방법들, 디바이스들, 시스템들, 및 컴퓨터 프로그램 물건들(products)을 제공한다. 맞춤화된 호출자 ID는 호출자가 호출하기 위해 사용하는 디바이스와는 상관없이 자신들을 식별하도록 제공한다. 게다가, 호출 우선순위 태깅과 같은 다른 기능은 호출자가 호출의 우선 순위를 결정하거나, 또는 호출 식별 메시지를 피호출자에 맞춤화하도록 제공한다. 호출자들과 피호출자들 사이에서 공유 비밀들을 교환함으로써, 맞춤화된 호출자 ID 및 원격 기능 관리 방법은 보안되고, 알려지지 않은 자들에 의한 허가되지 않은 탬퍼링(tampering)의 가능성은 제거된다. 또한, 공유 비밀 교환은 예를 들어, 오프 상태로 통신 디바이스를 원격으로 로킹 다운시키는 것과 같이, 허가된 호출자들이 통신 디바이스에 원격으로 액세스하고 통신 디바이스를 관리하도록 제공한다.
- [0024] 이하, 기재된 양상들을 한정하는 것이 아니라 예시하는 첨부된 도면들과 관련하여 기재된 양상들을 설명할 것이고, 여기서 동일한 명칭들은 동일한 엘리먼트들을 나타낸다.

실시예

- [0039] 본 발명의 디바이스들, 장치들, 방법들, 컴퓨터-판독 매체, 및 프로세서들은 본 발명의 양상들이 도시되어 있는 첨부된 도면들을 참조하여 설명된다. 그러나, 상기 디바이스들, 장치들, 방법들, 컴퓨터-판독가능 매체, 및 프로세서들은 다수의 상이한 형태로 실시될 수 있고, 본 발명에서 설명된 양상들에 한정되는 것으로 해석되어서는 안되며, 오히려 이러한 양상들이 제공되어 본 발명은 완전하게 완성될 것이며, 당업자에게 본 발명의 범위를 충분히 전달할 것이다. 또한, 이러한 설명에서, 동일한 번호들은 명세서 전반에 걸쳐 동일한 엘리먼트들을 지칭한다.
- [0040] 본 디바이스들, 장치들, 방법들, 컴퓨터-판독가능 매체, 및 프로세서들은 맞춤화된 호출자 식별(즉, 호출자 ID), 및 통신 디바이스들의 보안된 원격 액세스 및 관리를 제공한다. 본 양상들은 호출자 및 피호출자 사이의 공유 비밀을 이용하여, 맞춤화된 호출자 식별 및/또는 피호출 통신 디바이스의 원격 액세스 또는 관리를 허용한다. 이에 관하여, 호출자는 자신이 대안적인 통신 디바이스(즉, 자신의 디바이스가 아닌 디바이스)를 사용하고 있는 경우들에서, 자신을 식별할 수 있다. 추가적으로, 맞춤화된 호출자 ID는 호출자가 맞춤화된 메시지의 우

선순위를 결정하거나, 또는 호출자에게 맞춤화된 메시지를 제시하도록 제공한다. 또한, 공유 비밀들은 통신 디바이스의 보안된 원격 관리 및 제어를 제공하고, 통신 디바이스 사용자가 통신 디바이스에 원격으로 액세스하여, 디바이스에서 이용가능한 기능들을 수행하거나, 디바이스를 오프 모드(off mode)로 두거나, 로킹-다운(lock-down)할 권한을 허가할 수 있게 한다.

[0041] 도 1을 참조하면, 일 양상에 따라, 맞춤화된 호출자 ID, 및/또는 통신 디바이스들의 원격 액세스 및 관리를 위한 시스템(10)이 도시된다. 본 명세서에서 설명된 본 양상들의 맞춤화된 호출자 ID, 보안된 원격 액세스 및 통신 디바이스 관리 기능은 피호출 통신 디바이스 레벨, 네트워크 디바이스 레벨, 또는 피호출 디바이스와 네트워크 디바이스의 임의의 조합에 상주할 수 있다는 것에 유의하여야 한다. 도 1에 도시된 양상에서, 공유 비밀을 인식하고, 그것을 데이터베이스 내의 엔트리와 연관시키는 기능은 피호출 디바이스 레벨에 상주한다. 시스템은 이러한 예에서 피호출 통신 디바이스로서의 역할을 하는 제 1 통신 디바이스(12), 이러한 예에서 호출 통신 디바이스로서의 역할을 하는 제 2 통신 디바이스(14), 통신 네트워크 내의 기지국에 상주하는 서버 디바이스와 같은 네트워크 디바이스(16)를 포함한다. 도시된 양상에서, 통신 디바이스들은 무선 디바이스들이지만, 다른 양상들에서, 하나 이상의 통신 디바이스들은 지상통신선 전화들 등과 같은 유선 통신 디바이스들일 수 있고, 네트워크 디바이스는 지상 네트워크 내의 컴포넌트일 수 있다.

[0042] 시스템(10)은 통신 디바이스들의 원격 액세스 및 관리를 허용할 뿐만 아니라, 제 1 사용자(18) 및 제 2 사용자(20)가 호출자 ID 및/또는 호출 우선순위 정보를 맞춤화할 수 있게 한다. 제 1 사용자(18)는 제 1 통신 디바이스의 소유자 또는 전형적인 소유주가 되도록 제 1 통신 디바이스(12)와 연관된다. 또한, 제 2 사용자(20)는 제 2 사용자가 제 2 통신 디바이스의 차용자 또는 부소유주(secondary possessor)가 되도록 제 2 통신 디바이스(14)와 연관되지 않는다(즉, 제 2 통신 디바이스는 제 2 사용자에 의해 전형적으로 소유되는 디바이스가 아님). 제 2 사용자(20)는 공유 비밀(22)을 생성하고, 제 1 사용자(18)에게 상기 공유 비밀 및 임의의 관련된 공유 비밀 정보(24)를 전달할 것이다. 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)의 전달은 도 1의 화살표(26)에 의해 표현된다.

[0043] 공유 비밀(22)은 제 1 통신 디바이스(20)에 의해 인식가능할 수 있는 임의의 데이터 형태를 취할 수 있다. 많은 양상들에서, 공유 비밀은 둘 이상의 디지털 숫자 코드(digit numeric code)와 같은 숫자 코드일 것이다. 다른 양상들에서, 공유 비밀은 이미지와 같은 시각적 데이터(visual data), 링 톤 신호(ring tone signal)와 같은 오디오 데이터, 지문 데이터와 같은 생체 데이터, 음성 데이터 등일 수 있다. 관련된 공유 비밀 정보(24)는 우선순위 데이터와 같은, 공유 비밀과 연관된 데이터를 디스플레이될 시각적 메시지의 형태 또는 발생될 오디오 신호의 형태로 포함할 수 있거나, 또는 추가적인 공유 비밀 정보는 공유 비밀 교환에 기초하여, 원격으로 통신 디바이스에 액세스하고, 그리고/또는 통신 디바이스를 관리하기 위한 명령들을 포함할 수 있다.

[0044] 제 2 사용자(20)는 전자 통신, 직접 통신(in-person communication) 등과 같은 임의의 수용가능한 통신 수단에 의해 제 1 사용자(18)에게 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)를 전달할 것이다(화살표(26)). 전형적으로, 선택된 공유 비밀 통신 수단은, 공유 비밀(22)이 공유되지 않거나, 또는 허가된 사용자들의 소유가 되는 것을 보장하기 위해서, 필수적인 통신 보안 레벨을 제공할 것이다. 이에 관하여, 전자 통신은 암호화 또는 소정의 다른 형태의 보안 통신을 이용하여 공유 비밀(22)이 기밀로 유지되는 것을 보장할 수 있다.

[0045] 공유 비밀을 수신할 때, 제 1 사용자(18)는 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)를 제 1 통신 디바이스(12)로 입력할 것이다. 제 1 통신 디바이스로서의 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)의 입력은 도 1의 화살표(28)에 의해 표현된다. 일 양상에서, 그래픽 사용자 인터페이스(GUI) 모듈(30)은 제 1 통신 디바이스(12)에서 실행되며, 개인 정보 관리자(34)와 같은, 저장 디바이스에 공유 비밀 및 임의의 관련된 공유 비밀 정보를 입력하도록 동작가능한 데이터 엔트리 로직(32)을 포함하고, 상기 저장 디바이스는 콘택 데이터베이스, 전화번호부 데이터베이스 등 내의 공유 비밀 및 임의의 관련된 공유 비밀 정보가 제 2 사용자(20)와 연관되도록, 개인 전화번호부, 콘택 데이터베이스 등을 포함할 수 있다. 제 2 사용자(20)는 제 1 통신 디바이스 콘택 저장장치 또는 전화번호부 저장장치 내에 기존 엔트리(preexisting entry)를 가질 수 있거나, 또는 공유 비밀 및 임의의 관련된 공유 비밀 정보를 포함할 제 2 사용자(20)에 대한 새로운 콘택 엔트리를 생성하는 것이 필요할 수 있다. 콘택 또는 전화번호부 데이터베이스에 공유 비밀들을 입력하기 위한 절차를 하이라이트하는 GUI의 디스플레이에 대한 예들을 도시하는 도 5-8은 아래에서 상세하게 논의될 것이다. 또한, 콘택 또는 전화번호부 데이터베이스에 추가적인 공유 비밀 정보를 입력하기 위한 절차를 하이라이트하는 GUI의 디스플레이에 대한 예들을 도시하는 도 8-11은 아래에서 상세하게 논의될 것이다.

[0046] 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)가 제 2 사용자(20)로부터 제 1 통신 디바이스(12)로 전자

적으로 전달되는 대안적인 양상들에서, 제 1 통신 디바이스는 공유 비밀 및 관련된 정보를 자동으로 인식하고, 상기 비밀을 전송하는 사용자와 공유 비밀을 자동으로 연관시키며, 공유 비밀을 전송하는 사용자와 연관된 콘택 또는 전화번호부 데이터베이스 내에 대응하는 엔트리에 공유 비밀을 자동으로 저장하도록 구성될 수 있다. 이러한 양상들에서, 제 1 사용자가 공유 비밀 및 임의의 관련된 공유 비밀 정보를 수동으로 입력하도록 할 필요가 없어질 수 있다.

[0047] 공유 비밀이 제 1 통신 디바이스(12)에 저장되었을 때, 제 2 사용자(20)는 제 2 통신 디바이스(14)를 차용 또는 사용하여 제 1 통신 디바이스(12)에 호출할 수 있다. 전술한 바와 같이, 제 2 통신 디바이스는 제 2 사용자(20)에 의해 전형적으로 사용되거나 제 2 사용자(20)와 연관된 디바이스가 아니다. 이로서, 전형적인 호출자 ID 시스템들에서, 제 1 통신 디바이스(12)에 의한 제 2 통신 디바이스(14)로부터의 호출 수신은 전형적으로 호출자 ID 정보가 디스플레이되지 않도록 하거나, 또는 제 1 통신 디바이스(12)의 소유자에게 알려져 있지 않을 수 있는 제 2 통신 디바이스(14)의 실제 소유자의 전화 번호 및/또는 이름이 디스플레이되도록 할 것이다. 제 2 사용자에 의한 제 2 통신 디바이스(14)의 사용은 도 1의 화살표(36)에 의해 표현된다. 제 2 통신 디바이스(14)는 호출을 요청하기 위해서 전화 번호를 입력하도록 동작가능한 다이얼러 모듈(dialer module)(36)을 포함할 수 있다. 일부 양상들에서, 다이얼러 모듈(36)은 공유 비밀(22)을 입력하거나, 호출 요청에 공유 비밀을 첨부하도록 동작가능한 공유 비밀 엔트리 로직(38)을 포함할 수 있다. 일 양상에서, 공유 비밀 엔트리 로직(38)은 트리거 명령의 엔트리가 피호출자 전화 번호의 엔트리 후에 공유 비밀의 엔트리를 제공하도록 동작가능하다. 예를 들어, "*" 키 및 첨부한 숫자 코드는 트리거로서의 역할을 할 수 있고, 공유 비밀(22)은 트리거 입력 후에 숫자 코드의 형태로 입력될 수 있다. 도 17은 호출 요청 엔트리 시퀀스들에 대한 예들을 제공하며, 아래에서 상세하게 논의될 것이다. 그러나, 입력된 전화 번호, 하나 이상의 공유 비밀 트리거 명령들, 및 하나 이상의 공유 비밀들의 조합이 사용 중인 통신 네트워크에 의해 인식된 미리 결정된 수의 디지털트 내에 있는 경우와 같이, 공유 비밀 엔트리 로직(38)이 필요하지 않을 수 있다는 것에 유의하여야 한다.

[0048] 다이얼링된 전화 번호 및 공유 비밀(22)을 포함하는 호출 요청이 기지국으로 전달될 때, 호출 요청은 서버 등과 같은 네트워크 디바이스(16)에 의해 수신된다. 제 2 통신 디바이스(14)로부터 네트워크 디바이스(16)로의 호출 요청 전달은 무선 통신 볼트(bolt)(40)에 의해 표현된다. 네트워크 디바이스(16)는 호출 요청에서의 공유 비밀을 인식하고, 공유 비밀(22)을 포함하는 페이로드를 구문 분석(parse)하도록 동작가능한 공유 비밀 인식 로직(42)을 포함할 수 있다. 호출 요청이 트리거 및 공유 비밀(22)을 포함하는 양상들에서, 공유 비밀 인식 로직(42)은 트리거를 인식하고, 트리거 및 공유 비밀을 포함하는 페이로드를 구문 분석하도록 구성될 수 있다. 또한, 네트워크 디바이스는 공유 비밀 및 선택적인 트리거를 포함하는 구문 분석된 페이로드를 피호출자에게 포워딩하도록 동작가능한 공유 비밀 포워딩 로직(44)을 포함할 수 있다. 그러나, 입력된 전화 번호, 하나 이상의 공유 비밀 트리거 명령들, 및 하나 이상의 공유 비밀들의 조합이 사용 중인 통신 네트워크 및/또는 네트워크 디바이스(16)에 의해 인식 및 포워딩된 미리 결정된 수의 디지털트 내에 있을 경우와 같이, 공유 비밀 인식 로직(42) 및/또는 공유 비밀 포워딩 로직(44)이 필요하지 않을 수 있다는 것에 유의하여야 한다.

[0049] 네트워크 디바이스(16)는 제 1 통신 디바이스(12)로 호출 요청, 공유 비밀, 및 일부 양상들에서, 트리거를 포워딩한다. 호출 관리자 모듈(46)은 호출 요청을 수신하도록 동작가능하고, 공유 비밀 인식 로직(48)은 공유 비밀을 인식하고, 개인 정보 관리자(34) 내의 공유 비밀 데이터베이스(22)와 같은 디바이스 데이터베이스 내의 공유 비밀의 존재를 검증하며, 공유 비밀과 관련된 기능을 수행하거나, 공유 비밀과 관련된 애플리케이션을 실행하도록 동작가능할 수 있다. 일부 양상들에서, 호출 관리자 모듈(46)은 공유 비밀 인식 로직(48) 뿐만 아니라, 호출 요청에서의 공유 비밀이 다음에 나타날 것(forthcoming)임에 대한 표시자로서 트리거를 인식하도록 동작가능한 트리거 인식 로직(50)을 포함할 수 있다. 일부 양상들에서, 트리거는 공유 비밀과 관련된 기능 또는 애플리케이션을 표시할 수 있다. 이에 관하여, 트리거 인식은 공유 비밀과 관련된 기능 및/또는 실행에 대한 검증 및 명령들을 위해서 어떤 데이터베이스들이 다음에 나타날 공유 비밀과 연관되는지에 관한 정보를 제공할 수 있다.

[0050] 공유 비밀들의 사용이 맞춤형 호출자 식별을 제공하는 일 양상에서, 호출 제어 관리자는 호출 디바이스와 연관된 전화 번호 및/또는 이름을 디바이스 디스플레이에 디스플레이함으로써 호출자의 식별을 인식하도록 동작가능한 호출자 식별(ID) 로직(52)을 포함할 수 있다. 이러한 양상에서, 공유 비밀 인식 로직(48), 및 선택적으로, 트리거 인식 로직(50)은 공유 비밀을 인식하고, 선택적으로, 트리거를 인식하도록 동작가능할 수 있으며, 그 결과 호출 디바이스와 연관된 전화 번호 및/또는 이름의 디스플레이와 관련하여 호출자 ID 로직(52)은 무시된다. 대신에, 공유 비밀 인식 로직(48)은 개인 정보 관리자(34)의 공유 비밀 데이터베이스(22) 내의 공유 비밀을 검증하고, 이름, 전화 번호, 또는 다른 식별과 같은 공유 비밀과 연관된 개인 정보를 디스플레이하

기 위해 호출자 ID 로직(52)으로 전달하거나, 또는 이러한 정보를 직접 디스플레이한다. 이에 관하여, 이러한 양상은 호출 디바이스의 소유자의 식별을 디스플레이하기 보다는, 공유 비밀에 기초하여, "실제" 호출자의 식별을 디스플레이한다.

[0051] 도 2를 참조하면, 대안적인 일 양상에 따라, 맞춤형된 호출자 ID, 및/또는 통신 디바이스들의 원격 액세스 및 관리를 위한 시스템(10)이 도시된다. 도 2에 도시된 양상에서, 공유 비밀을 인식하고, 그것을 데이터베이스 내의 엔트리와 연관시키는 것에 관한 기능은 네트워크 디바이스 레벨에 상주한다. 시스템은 이러한 예에서 피호출 통신 디바이스로서의 역할을 하는 제 1 통신 디바이스(12), 이러한 예에서 호출 통신 디바이스로서의 역할을 하는 제 2 통신 디바이스(14), 통신 네트워크 내의 기지국에 상주하는 서버 디바이스와 같은 네트워크 디바이스(16)를 포함한다. 도 1과 유사하게, 도 2의 도시된 양상에서, 통신 디바이스들은 무선 디바이스들이지만, 다른 양상들에서, 하나 이상의 통신 디바이스들은 지상통신선 전화들 등과 같은 유선 통신 디바이스들일 수 있고, 네트워크 디바이스는 지상 네트워크 내의 컴포넌트일 수 있다.

[0052] 시스템(10)은 통신 디바이스들의 원격 액세스 및 관리를 허용할 뿐만 아니라, 제 1 사용자(18) 및 제 2 사용자(20)가 호출자 ID 및/또는 호출 우선순위 정보를 맞춤형할 수 있게 한다. 제 1 사용자(18)는 제 1 통신 디바이스의 소유자 또는 전형적인 소유주가 되도록 제 1 통신 디바이스(12)와 연관된다. 또한, 제 2 사용자(20)는 제 2 사용자가 제 2 통신 디바이스의 차용자 또는 부소유주(secondary possessor)가 되도록 제 2 통신 디바이스(14)와 연관되지 않는다(즉, 제 2 통신 디바이스는 제 2 사용자에 의해 전형적으로 소유되는 디바이스가 아님). 제 2 사용자(20)는 공유 비밀(22)을 생성하고, 공유 비밀 및 임의의 관련된 공유 비밀 정보(24)를 직접 네트워크 디바이스(16)로 전달하고, 그리고/또는 네트워크 디바이스(16)로의 후속적인 전달을 위하여 제 1 사용자(18)에게 전달할 것이다. 제 2 사용자(20)로부터 네트워크 디바이스(16)로의 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)의 직접 전달은 화살표(36)(제 2 통신 디바이스(14)로의 입력) 및 무선 통신 볼트(40)(제 2 통신 디바이스(14)로부터 네트워크 디바이스(16)로의 전자 통신)에 의해 표현된다. 대안적으로, 제 2 사용자로부터 제 1 사용자로의 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)의 전달은 도 2의 화살표(26)에 의해 표현된다.

[0053] 제 2 사용자(20)는 전자 통신, 직접 통신(in-person communication) 등과 같은 임의의 수용가능한 통신 수단에 의해 제 1 사용자(18)에게 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)를 전달할 수 있다(화살표(26)에 의해 표현됨). 게다가, 제 2 사용자(20)는 전자 통신, 직접 통신 등과 같은 임의의 수용가능 통신 수단에 의해 네트워크 디바이스(16)로 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)를 전달할 수 있다(화살표(36) 및 볼트(40)에 의해 표현됨). 전형적으로, 선택된 공유 비밀 통신 수단은, 공유 비밀(22)이 공유되지 않거나, 또는 허가되지 않은 사용자들의 소유가 되는 것을 보장하기 위해서 필수적인 통신 보안 레벨을 제공할 것이다. 이에 관하여, 전자 통신은 암호화 또는 소정의 다른 형태의 보안 통신을 이용하여 공유 비밀(22)이 기밀로 유지되는 것을 보장할 수 있다.

[0054] 제 2 사용자(20)가 공유 비밀(22) 및 임의의 추가적인 공유 비밀 정보(24)를 네트워크 디바이스(16)로 직접 전달하는 양상들에서, 공유 비밀 및 임의의 관련된 정보를 제 1 사용자(18)에게 전송할 필요가 없어질 수 있다. 제 2 사용자(20)가 공유 비밀(22) 및 임의의 관련된 비밀 정보를 제 1 사용자(18)에게 전달하지 않고, 네트워크 디바이스(16)로 직접 전달하는 양상들에서, 맞춤형된 호출자 ID, 원격 액세스 및/또는 통신 디바이스 관리는 제 1 사용자(18)에게 알리지 않고 수행될 수 있다.

[0055] 그러나, 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)가 제 1 사용자(18)에게 전달되고 후속적으로 네트워크 디바이스(16)로 전달되는 양상들에서, 제 1 사용자(18)는 네트워크 디바이스(16)로의 후속적인 전달을 위하여 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)를 제 1 통신 디바이스(12)로 입력한다. 제 1 통신 디바이스로서의 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)의 입력은 도 1의 화살표(28)에 의해 표현된다. 일 양상에서, 그래픽 사용자 인터페이스(GUI) 모듈(30)은 제 1 통신 디바이스(12)에서 실행되며, 공유 비밀 및 임의의 관련된 공유 비밀 정보를 입력하도록, 그리고 선택적으로, 공유 비밀 및 관련된 정보를 로컬로 저장하도록 동작가능한 데이터 엔트리 로직(32)을 포함한다. 또한, GUI 모듈(30)은 네트워크 디바이스(16)로 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)를 업로드 또는 전달하도록 동작가능한 네트워크 업로드 로직(51)을 포함할 수 있다. 대안적인 일 양상에서, 제 1 통신 디바이스는 제 1 사용자(18)가 네트워크 디바이스(16)와 연관된 웹 페이지에 액세스하고, 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)를 입력하며, 이후에 인터넷을 통해 네트워크 디바이스(16)로 공유 비밀 및 관련된 정보를 전달할 수 있게 하는 웹 브라우저 애플리케이션(53)을 포함할 수 있다.

- [0056] 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)가 제 2 사용자(20)로부터 제 1 통신 디바이스(12)로 전자적으로 전달되는 대안적인 양상들에서, 제 1 통신 디바이스는 공유 비밀 및 관련된 정보를 자동으로 인식하고, 네트워크 디바이스(16)로 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보를 자동으로 업로드 또는 전달하도록 구성될 수 있다. 이러한 양상들에서, 제 1 사용자가 공유 비밀 및 임의의 관련된 공유 비밀 정보를 수동으로 입력하도록 할 필요가 없어질 수 있다.
- [0057] 공유 비밀이 네트워크 디바이스(16)에 저장되었을 때, 제 2 사용자(20)는 제 2 통신 디바이스(14)를 차용 또는 사용하여 제 1 통신 디바이스(12)에 호출할 수 있다. 전술한 바와 같이, 제 2 통신 디바이스는 제 2 사용자(20)에 의해 전형적으로 사용되는 또는 제 2 사용자(20)와 연관된 디바이스가 아니다. 제 2 통신 디바이스(14)는 호출을 요청하기 위해서 전화 번호를 입력하도록 동작가능한 다이얼러 모듈(36)을 포함할 수 있다. 일부 양상들에서, 다이얼러 모듈(36)은 공유 비밀(22)을 입력하거나, 호출을 요청하기 위해서 공유 비밀을 첨부하도록 동작가능한 공유 비밀 엔트리 로직(38)을 포함할 수 있다. 일 양상에서, 공유 비밀 엔트리 로직(38)은 트리거 명령의 엔트리가 피호출자 전화 번호의 엔트리 후에, 공유 비밀의 엔트리를 제공하도록 동작가능하다. 예를 들어, "*" 키 및 첨부한 숫자 코드는 트리거로서의 역할을 할 수 있고, 공유 비밀(22)은 트리거 입력 후에 숫자 코드의 형태로 입력될 수 있다. 도 17은 호출 요청 엔트리 시퀀스들에 대한 예를 제공하며, 아래에서 상세하게 논의될 것이다. 그러나, 입력된 전화 번호, 하나 이상의 공유 비밀 트리거 명령들, 및 하나 이상의 공유 비밀들의 조합이 사용 중인 통신 네트워크에 의해 인식된 미리 결정된 수의 디지털들 내에 있는 경우와 같이, 공유 비밀 엔트리 로직(38)이 필요하지 않을 수 있다는 것에 유의하여야 한다.
- [0058] 다이얼링된 전화 번호 및 공유 비밀(22)을 포함하는 호출 요청이 기지국으로 전달될 때, 호출 요청은 서버 등과 같은 네트워크 디바이스(16)에 의해 수신된다. 제 2 통신 디바이스(14)로부터 네트워크 디바이스(16)로의 호출 요청 전달은 무선 통신 볼트(40)에 의해 표현된다. 또한, 네트워크 디바이스는 공유 비밀을 인식하고, 클라이언트 정보 관리자(59) 내의 공유 비밀(22)과 같은 네트워크 데이터베이스 내의 공유 비밀의 존재를 검증하고, 검증 시 공유 비밀과 관련된 기능을 수행하거나 공유 비밀과 관련된 애플리케이션을 실행시키도록 동작가능한 공유 비밀 인식 로직(42)을 포함할 수 있다. 클라이언트 정보 관리자는 네트워크 디바이스에 저장되거나 네트워크 디바이스에 액세스가능한 임의의 다른 네트워크 위치에 저장된 데이터베이스이다. 클라이언트 정보 관리자는 클라이언트/사용자 정보의 데이터베이스이고, 특히, 클라이언트/사용자와 연관된 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)를 포함할 수 있다. 또한, 호출 요청에 트리거가 포함된 양상들에서, 네트워크 디바이스(16)는 호출 요청에서의 공유 비밀이 다음에 나타날 표시자로서 트리거를 인식하도록 동작가능한 트리거 인식 로직(92)을 포함할 수 있다. 일부 양상들에서, 트리거는 공유 비밀과 관련된 기능 또는 애플리케이션을 표시할 수 있다. 이에 관하여, 트리거 인식은 공유 비밀과 관련된 기능 및/또는 실행에 대한 검증 및 명령들을 위해서 어떤 데이터베이스들이 다음에 나타날 공유 비밀과 연관되는지에 관한 정보를 제공할 수 있다.
- [0059] 공유 비밀과 관련된 기능이 맞춤형 호출자 ID인 특정 양상들에서, 클라이언트 정보 관리자(59) 내에서의 공유 비밀(22)의 검증은 호출 요청의 페이로드에서 호출 디바이스(즉, 제 2 통신 디바이스(14)) 호출자 ID 정보를 공유 비밀 소유자(즉, 실제 호출자)와 연관된 호출자 ID 정보로 대체시키도록 동작가능한 호출자 ID 오버라이드 로직(caller ID override logic)(55)에 인보크(invoke)할 것이다. 이에 관하여, 피호출 디바이스 즉, 제 1 통신 디바이스(12)로 이후에 포워딩되는 호출 요청은 제 2 통신 디바이스와 연관된 전화 번호, 및 제 2 사용자(20)(즉, 공유 비밀의 소유자)와 연관된 호출자 ID 정보를 포함할 것이다. 이로서, 이러한 양상은 호출 디바이스의 소유자의 식별을 디스플레이하기 보다는, 공유 비밀에 기초하여, "실제" 호출자의 식별을 디스플레이한다.
- [0060] 공유 비밀과 관련된 기능이 원격 액세스, 통신 디바이스 관리 등과 관련되는 대안적인 양상들에서, 네트워크 디바이스는 원격 액세스, 통신 디바이스 관리 등을 위한 명령들 및/또는 호출 요청 페이로드 식별에 삽입시키도록 동작가능한 추가적인 공유 비밀 관련 삽입 로직(57)을 포함할 수 있다. 특정 양상들에서, 삽입 로직(57)은 제 1 통신 디바이스(12)(즉, 피호출자)에 의해 인식가능할 페이로드 내에 코드와 같은 식별을 삽입할 수 있고, 필수적인 원격 액세스, 통신 디바이스 관리 등과 연관될 수 있다. 대안적인 양상들에서, 삽입 로직(57)은 필수적인 원격 액세스, 통신 디바이스 관리 등을 수행하기 위해서 제 1 통신 디바이스(12)에 의해 실행될 페이로드에 루틴, 애플리케이션들, 애플릿 등과 같은 명령들을 삽입할 수 있다.
- [0061] 네트워크 디바이스(16)는 호출 요청, 호출자와 연관된 호출자 ID 정보, 및/또는 원격 액세스/통신 디바이스 관리 식별 또는 명령들을 제 1 통신 디바이스(12)로 포워딩한다. 호출 관리자 모듈(46)은 호출 요청을 수신하도록 동작가능하고, 호출자 ID 로직(52)은 호출 요청에 포함된 호출자 ID 정보를 디스플레이하거나, 사용자에게 제공하도록 동작가능하다. 이러한 양상에서, 호출 요청은 제 2 통신 디바이스(14)의 전화 번호, 및 제 2 사용자(20)(즉, 공유 비밀(22)과 연관된 사용자)와 연관된 호출자 ID 정보를 포함할 수 있다. 호출 관리자 모듈

(46)은, 호출 요청에서의 원격 액세스/디바이스 관리 코드를 인식하고 상기 코드와 연관된 기능을 수행하도록 동작가능한 원격 액세스/디바이스 관리 로직(61)을 추가로 포함할 수 있다. 대안적으로, 원격 액세스/디바이스 관리 로직(61)은 호출 요청에서의 명령들을 실행시켜 필수적인 원격 액세스/디바이스 관리 기능들을 수행하도록 동작가능할 수 있다.

[0062] 도 3을 참조하면, 일 양상에 따라, 제 1 통신 디바이스(12)와 같은 통신 디바이스를 나타내는 블록 다이어그램이 도시된다. 도시된 통신 디바이스는 임의의 타입의 컴퓨터화된, 무선 디바이스, 예를 들어, 셀룰러 전화, 개인용 디지털 보조기(PDA), 양방향 텍스트 페이지, 휴대용 컴퓨터, 심지어 무선 통신 포털을 포함하는 개별 컴퓨터 플랫폼과 같은 무선 통신 디바이스이고, 상기 통신 디바이스는 네트워크 또는 인터넷에 유선 접속할 수도 있다. 무선 디바이스는 원격 슬레이브, 또는 최종 사용자를 가지고 있지는 않지만, 원격 센서들, 진단 도구들, 데이터 릴레이들 등과 같은 무선 또는 유선 네트워크를 통해 단순히 데이터를 전달하는 다른 디바이스일 수 있다. 대안적인 양상들에서, 통신 디바이스(12)는 지상통신선 전화, 개인용 컴퓨터, 셋-탑 박스 등과 같은 유선 통신 디바이스일 수 있다. 따라서, 맞춤형된 호출자 식별 및/또는 원격 디바이스 관리를 위한 장치 및 방법은 무선 모듈들, PCMCIA 카드들, 액세스 단말들, 개인용 컴퓨터들, 전화들, 또는 이들의 임의의 조합 또는 서브-조합들을 포함하지만 이에 한정되지 않는 유선 또는 무선 통신 포털을 구비하는 임의의 형태의 유선 또는 무선 디바이스 또는 컴퓨터 모듈에서 수행될 수 있다.

[0063] 추가적으로, 통신 디바이스(12)는 무선 디바이스로의 입력들을 발생시키기 위한 입력 메커니즘(54), 및 무선 디바이스의 사용자에게 의한 소비를 위한 정보를 발생시키기 위한 출력 메커니즘(56)을 포함한다. 예를 들어, 입력 메커니즘(54)은 키패드 또는 키보드, 마우스, 터치-스크린 디스플레이, 음성 인식 모듈 등과 관련된 마이크로폰과 같은 메커니즘을 포함할 수 있다. 특정 양상들에서, 입력 메커니즘들(54)은 그래픽 사용자 인터페이스 모듈(30)을 활성화시키고, 디바이스 메모리에 공유 비밀들을 입력시키기 위해서 사용자 입력을 제공한다. 또한, 예를 들어, 출력 메커니즘(56)은 디스플레이, 오디오 스피커, 햅틱 피드백 메커니즘 등을 포함할 수 있다. 디스플레이와 같은 출력 메커니즘들은 맞춤형된 호출자 ID들이 전형적으로 디스플레이 또는 오디오 스피커를 통해 디바이스 사용자에게 전달되는 이러한 양상들에서 구현될 수 있다.

[0064] 또한, 통신 디바이스(12)는 컴퓨터 플랫폼(58)을 포함하고, 컴퓨터 플랫폼(58)은 무선 네트워크, 또는 일부 양상들에서, 유선 네트워크를 통해 데이터를 전송할 수 있고, 루틴들 및 애플리케이션들을 수신 및 실행시키고, 서버 또는 무선 또는 유선에 접속된 다른 컴퓨터 디바이스와 같은 네트워크 디바이스(16)로부터 전송된 데이터를 디스플레이할 수 있다. 컴퓨터 플랫폼(58)은 판독-전용 및/또는 랜덤-액세스 메모리(RAM 및 ROM), EPROM, EEPROM, 플래시 카드들, 또는 컴퓨터 플랫폼들에 공통된 임의의 메모리와 같은 휘발성 및 비휘발성 메모리를 포함할 수 있는 데이터 레지스트리(60)를 포함한다. 또한, 데이터 레지스트리(60)는 하나 이상의 플래시 메모리 셀들을 포함할 수 있거나, 또는 자기 매체, 광학 매체, 테이프, 또는 소프트 또는 하드 디스크와 같은 임의의 2차 또는 3차 저장 디바이스일 수 있다.

[0065] 또는, 컴퓨터 플랫폼(58)은 주문형 집적 회로("ASIC"), 또는 다른 칩셋, 프로세서, 논리 회로, 또는 다른 데이터 프로세싱 디바이스일 수 있는 프로세싱 엔진(62)을 더 포함한다. 프로세싱 엔진(62) 또는 ASIC와 같은 다른 프로세서는 통신 디바이스(12)의 데이터 레지스트리(60) 내의 GUI 모듈(30) 및/또는 호출 관리자 모듈(46)과 같은 임의의 상주 프로그램들과 인터페이싱하는 애플리케이션 프로그래밍 인터페이스("API") 계층(64)을 실행시킬 수 있다. 전형적으로, API(64)는 각각의 무선 디바이스에서 실행시키는 런타임 환경(runtime environment)이다. 이러한 한 가지의 런타임 환경은 캘리포니아 샌디에고의 Qualcomm, Inc.에 의해 개발된 Wireless[®] (BREW[®]) 소프트웨어를 위한 바이너리 런타임 환경(Binary Runtime Environment)이다. 예를 들어, 무선 컴퓨팅 디바이스들 상에서 애플리케이션들의 실행을 제어하도록 동작하는 다른 런타임 환경들이 이용될 수 있다.

[0066] 프로세싱 엔진(62)은 통신 디바이스(12)의 기능성, 및 무선 또는 유선 네트워크 상의 통신 디바이스의 운용성을 인에이블시키는 하드웨어, 펌웨어, 소프트웨어, 및 이들의 조합들로 구현되는 다양한 프로세싱 서브시스템들(66)을 포함한다. 예를 들어, 프로세싱 서브시스템들(66)은 통신 개시 및 유지, 및 네트워킹된 디바이스들과의 데이터 교환을 허용한다. 일 양상에서, 예를 들어 셀룰러 전화에서, 통신 프로세싱 엔진(62)은 소리, 비휘발성 메모리, 파일 시스템, 송신, 수신, 검색기, 계층 1, 계층 2, 계층 3, 메인 제어, 원격 절차, 핸드셋(handset), 전력 관리, 진단, 디지털 신호 프로세서, 보코더(vocoder), 메시징, 호출 매니저, Bluetooth[®] 시스템, Bluetooth[®] LPOS, 위치 결정, 위치 엔진, 사용자 인터페이스, 휴면, 데이터 서비스들, 보안, 인증 USIM/SIM, 음성 서비스들, 그래픽스, USB, MPEG와 같은 멀티미디어, GPRS 등과 같은 프로세싱 서브시스템들(66) 중의 하나

또는 이들의 조합을 포함할 수 있다. 기술한 양상들에 대하여, 프로세싱 엔진(62)의 프로세싱 서브시스템들(66)은 컴퓨터 플랫폼(58) 상에서 실행하는 애플리케이션들과 상호작용하는 임의의 서브시스템 컴포넌트들을 포함할 수 있다. 예를 들어, 프로세싱 서브시스템들(66)은 GUI 모듈(30)을 대신하여 API(64)로부터 데이터 관독들 및 데이터 기록들을 수신하거나, 호출 관리자 모듈(46)을 지원하는 임의의 서브시스템 컴포넌트들을 포함할 수 있다.

[0067] 컴퓨터 플랫폼(58)의 데이터 레지스트리(60)는 공유 비밀(22) 및 임의의 관련된 공유 비밀 정보(24)를 개인 정보 관리자(34)와 같은 통신 디바이스 메모리/데이터 레지스트리(60)에 입력하도록 동작가능한 데이터 엔트리 로직(32)을 포함하는 그래픽 사용자 인터페이스(GUI) 모듈(30)을 추가적으로 저장할 수 있다. 전형적으로, GUI 모듈은 디바이스의 사용자에게 공유 비밀 및 임의의 관련된 공유 비밀 정보를 입력하기 위한 데이터 엔트리 필드들의 시각적 디스플레이를 제공하도록 동작가능하다. 공유 비밀(22) 및/또는 관련된 공유 비밀 정보(24)가 디바이스로 전자적으로 전달되는 대안적인 양상들에서, 공유 비밀은 메모리에 자동으로 입력될 수 있고, 공유 비밀 엔트리를 위하여 GUI 모듈(30)에 인보크할 필요가 없어진다. 공유 비밀(22) 및 관련된 공유 비밀 정보(24)를 저장하는 개인 정보 관리자(34)는 개인 전화번호부 등과 같은 콘택 정보 데이터베이스(68)를 포함할 수 있다. 콘택 정보 데이터베이스는 이름, 전화 번호 등과 같은 콘택들과 관련된 개인 정보를 저장하고, 공유 비밀, 및 선택적으로, 관련된 공유 비밀 정보를 콘택과 연관시킨다. 대안적인 양상들에서, 공유 비밀(22) 및 관련된 공유 정보는 개인 정보 관리자(34) 내의, 또는 다른 경우에서, 데이터 레지스트리(60) 내의 다른 파일들 또는 디렉토리들 내에 저장될 수 있고, 이것은 호출자들/콘택들 및 공유 비밀들 사이의 연관(association)을 제공한다.

[0068] 컴퓨터 플랫폼(58)의 데이터 레지스트리(60)는 호출 관리자 모듈(46)을 더 포함할 수 있고, 호출 관리자 모듈(46)은 호출 요청에서의 공유 비밀(22)을 인식하고, 공유 비밀이 호출자/콘택과 연관됨을 검증하며, 공유 비밀과 연관되거나, 관련된 공유 비밀 정보(24)에 의해 규정된 기능 또는 애플리케이션을 수행하도록 동작가능한 공유 비밀 인식 로직(48)을 포함할 수 있다. 공유 비밀이 호출자/콘택과 연관됨을 검증하는 것은 개인 정보 관리자(34)에 액세스하는 것, 및 공유 비밀이 데이터베이스 내의 호출자/콘택과 연관됨을 검증하는 것을 포함할 수 있다. 공유 비밀이 검증되었으면, 로직(48)은 공유 비밀 또는 관련된 공유 정보와 연관된 기능 또는 애플리케이션을 수행할 수 있다. 예를 들어, 공유 비밀은 고객 호출자-ID 기능과 연관될 수 있고, 이로써 공유 비밀과 연관된 호출/콘택 식별이 호출 디바이스의 식별 대신에 호출자로서 디스플레이되거나, 또는 전송될 수 있다. 다른 예들에서, 공유 비밀은 유실되거나 도난당한 디바이스의 허가되지 않은 사용을 방지하기 위해서 디바이스를 디스에이블하거나, 디바이스를 로킹-다운시키는 것과 같은 디바이스 기능과 연관될 수 있다.

[0069] 호출 관리자 모듈(46)은 호출 요청에서의 트리거(70)를 인식하도록 동작가능한 트리거 인식 로직(50)을 더 포함할 수 있다. 트리거(70)는 공유 비밀이 호출 요청에 첨부된다는 것을 호출 제어 관리자에게 통지하는 숫자 코드 동일 수 있다. 일부 양상들에서, 트리거(70)는 공유 비밀과 연관된 기능 또는 애플리케이션을 표시할 수 있다. 예를 들어, "88"의 숫자 값을 가지는 트리거는 고객 호출자 ID 기능이 첨부된 공유 비밀과 연관된다는 것을 표시할 수 있는 반면, "89"의 숫자 값을 가지는 트리거는 "긴급" 메시지 디스플레이, 또는 호출 표시자 신호를 통한 "긴급" 메시지 전달과 같은, 호출 우선순위 태깅(call priority tagging)이 첨부된 공유 비밀과 연관된다는 것을 표시할 수 있다. 이러한 양상들에서, 공유 비밀들(22) 및 선택적인 관련된 공유 비밀 정보(24)와 트리거들(70)을 연관시키는 개인 정보 관리자(34) 또는 다른 디바이스 데이터베이스는 데이터를 저장할 수 있다.

[0070] 공유 비밀이 호출자 식별 기능과 연관되는 일 양상에서, 호출 관리자 모듈(46)은 호출자 ID 로직(52)을 포함할 수 있다. 호출자 ID 로직은 이름, 전화 번호 등과 같은 호출자 식별을 디스플레이하거나 또는 전달하도록 동작가능할 수 있다. 종래의 호출 ID 로직은 호출자 식별, 전형적으로, 호출 디바이스와 연관된 이름, 전화 번호의 디스플레이 또는 다른 전달을 제공한다. 그러나, 본 양상들에서, 호출자 ID 로직은 공유 비밀의 인식이 호출 디바이스와 연관된 호출자 식별의 디스플레이 또는 전달 대신에, 공유 비밀과 연관된 콘택/호출자의 디스플레이 또는 전달을 제공하도록 구성될 수 있다. 또한, 호출 우선순위 등과 같은, 관련된 공유 비밀 정보에 전형적으로 저장되는 추가적인 정보가 디스플레이 또는 전달될 수 있다. 이로서, 전형적으로 호출자와 연관된 디바이스가 아닌 디바이스(예를 들어, 차용한 디바이스)로부터 호출하는 호출자는 피호출자가 호출에 응답하거나, 또는 호출에 확인 응답할 가능성을 증가시키기 위해서 실제 소유자 정보보다는, 호출자의 식별 정보가 디스플레이되거나 피호출자에게 전달되는 것을 보장할 수 있다. 공유 비밀 인식 및 연관이 네트워크 디바이스에서 수행되는 대안적인 양상들에서, 호출자 ID 로직(52)은 호출 요청 페이로드 내의 호출자 ID 정보를 인식하고, 호출자 ID 정보를 디스플레이하거나 출력하도록 동작가능할 수 있다.

[0071] 공유 비밀이 원격 액세스 및/또는 디바이스 관리 기능과 연관되는 다른 양상들에서, 호출 관리자 모듈(46)은 원

격 액세스/디바이스 관리 로직(61)을 포함할 수 있다. 공유 비밀 인식 및 연관이 피호출 통신 디바이스에서 수행되는 양상들에서, 원격 액세스/디바이스 관리 로직(61)은 원격 액세스 기능 또는 디바이스 관리 기능과 연관된 공유 비밀 또는 트리거를 인식하고, 원격 액세스 또는 디바이스 관리를 수행하도록 동작가능할 수 있다. 공유 비밀 인식 및 연관이 네트워크 디바이스에서 수행되는 대안적인 양상들에서, 원격 액세스/디바이스 관리 로직(61)은 호출 요청에서의 원격 액세스/디바이스 관리 코드를 인식하고, 상기 코드와 연관된 기능을 수행하도록 동작가능할 수 있거나, 또는 원격 액세스/디바이스 관리 로직(61)은 호출 요청에서의 명령들을 실행시켜 필수적인 원격 액세스/디바이스 관리 기능들을 수행하도록 동작가능할 수 있다.

[0072] 컴퓨터 플랫폼(58)은 통신 디바이스(12)와 유선 또는 무선 네트워크 사이의 통신들 뿐만 아니라, 통신 디바이스(12)의 다양한 컴포넌트들 사이의 통신들을 가능하게 하는, 하드웨어, 펌웨어, 소프트웨어, 및 이들의 조합들로 구현되는 통신 모듈(72)을 더 포함할 수 있다. 통신 모듈은 유선 또는 무선 통신 접속을 설정하기 위한 필수적인 하드웨어, 펌웨어, 소프트웨어, 및/또는 이들의 조합들을 포함할 수 있다.

[0073] 도 4를 참조하면, 일 양상에서, 공유 비밀들을 인식하고, 공유 비밀들을 호출자 또는 기능과 연관시키고, 그리고/또는 호출 요청들을 포워딩하도록 동작가능한 네트워크 디바이스(16)의 블록 다이어그램 도면이 제시된다. 네트워크 디바이스는 임의의 타입의 하드웨어, 서버, 개인용 컴퓨터, 미니 컴퓨터, 메인프레임 컴퓨터, 또는 전용 또는 범용 컴퓨팅 디바이스 중 어느 하나인 임의의 컴퓨팅 디바이스 중 적어도 하나를 포함할 수 있다. 또한, 네트워크 디바이스(16) 상에서 동작되거나 네트워크 디바이스(16)에 의해 실행되는 것으로 본 명세서에서 설명된 모듈들 및 애플리케이션들은 네트워크 디바이스(16)에서 완전히 실행될 수 있거나, 대안적으로, 다른 양상들에서, 개별적인 서버들 또는 컴퓨터 디바이스들은 당사자들에게 사용가능한 포맷들로 데이터를 제공하기 위해서, 그리고/또는 무선 디바이스(12)와 네트워크 디바이스(16)에 의해 실행되는 모듈들 및 애플리케이션들 사이의 데이터 플로우의 개별적인 제어 계층을 제공하기 위해서 함께 동작할 수 있다.

[0074] 네트워크 디바이스(16)는 컴퓨터 플랫폼(80)을 포함할 수 있고, 컴퓨터 플랫폼(80)은 무선 또는 유선 네트워크를 통해 데이터를 전송 및 수신할 수 있고, 루틴들 및 애플리케이션들을 실행시킬 수 있다. 컴퓨터 플랫폼(80)은 판독-전용 및/또는 랜덤-액세스 메모리(RAM 및 ROM), EPROM, EEPROM, 플래시 카드들, 또는 컴퓨터 플랫폼들에 공통적인 임의의 메모리와 같은 휘발성 및 비휘발성 메모리를 포함할 수 있는, 데이터 저장장치(82)를 포함할 수 있다. 또한, 데이터 저장장치(82)는 하나 이상의 플래시 메모리 셀들을 포함할 수 있거나, 또는 자기 매체, 광학 매체, 테이프, 또는 소프트 또는 하드 디스크와 같은, 임의의 2차 또는 3차 저장 디바이스일 수 있다. 또한, 컴퓨터 플랫폼(80)은 또한 주문형 집적 회로("ASIC"), 또는 다른 칩셋, 프로세서, 논리 회로, 또는 다른 데이터 프로세싱 디바이스일 수 있는 프로세싱 엔진(84)을 포함할 수 있다. 컴퓨터 플랫폼(80)은 네트워크 디바이스(16)와 무선 또는 유선 네트워크 사이의 통신들 뿐만 아니라, 네트워크 디바이스(16)의 다양한 컴포넌트들 사이의 통신들을 가능하게 하는, 하드웨어, 펌웨어, 소프트웨어, 및 이들의 조합들로 구현되는 통신 모듈(86)을 더 포함할 수 있다. 예를 들어, 설명된 양상들에서, 통신 모듈은 호출자 무선 디바이스들로부터 호출 요청들을 수신하고, 호출 요청들을 피호출자 무선 디바이스들로 포워딩하도록 구성된다. 통신 모듈은 무선 통신 접속을 설정하기 위한 필수적인 하드웨어, 펌웨어, 소프트웨어 및/또는 이들의 조합들을 포함할 수 있다.

[0075] 데이터 저장장치(82)는 공유 비밀 인식 로직(42)을 구현할 수 있는 공유 비밀 모듈(90)을 포함할 수 있다. 공유 비밀 인식 및 연관이 피호출 통신 디바이스에서 수행되는 양상들에서, 공유 비밀 인식 로직(42)은 호출 요청에서의 하나 이상의 공유 비밀들을 인식하고 공유 비밀들(22)을 포함하는 페이로드를 구문 분석하도록 동작가능할 수 있다. 추가적으로, 이러한 양상들에서, 호출 요청은 트리거를 포함할 수 있고, 그에 따라, 데이터 저장장치(82)는 호출 요청에서의 하나 이상의 트리거들을 인식하고, 트리거(들) 및 연관된 공유 비밀(들)을 포함하는 페이로드를 구문 분석하도록 동작가능한 트리거 인식 로직(92)을 포함할 수 있다. 추가적으로, 공유 비밀 인식 및 연관이 피호출 통신 디바이스에서 수행되는 양상들에서, 네트워크 디바이스는 또한 호출 요청의 부분으로서 공유 비밀, 및 선택적인 트리거를 포함하는 구문 분석된 페이로드를 피호출자에게 포워딩하도록 동작가능한 공유 비밀 포워딩 로직(44)을 포함할 수 있다.

[0076] 공유 비밀 인식 및 연관이 네트워크 디바이스에서 수행되는 대안적인 양상들에서, 공유 비밀 인식 로직(42)은 공유 비밀을 인식하고, 클라이언트 정보 관리자(59) 내의 공유 비밀(22)과 같은 디바이스 데이터베이스 내의 공유 비밀의 존재를 검증하며, 검증하면, 공유 비밀과 관련된 기능을 수행하거나 공유 비밀과 관련된 애플리케이션을 실행시키도록 동작가능할 수 있다. 클라이언트 정보 관리자는 네트워크 디바이스(16) 내에 저장되거나 네트워크 디바이스에 액세스가능한 임의의 다른 네트워크 위치에 저장되는 데이터베이스이다. 클라이언트 정보 관리자는 클라이언트/사용자 정보(63)의 데이터베이스이며, 특히, 공유 비밀(22), 및 데이터베이스 내의 각각의

클라이언트/사용자와 연관된 임의의 관련된 공유 비밀 정보(24)를 포함할 수 있다.

[0077] 공유 비밀 인식 및 연관이 네트워크 디바이스에서 수행되며, 공유 비밀과 관련된 기능이 맞춤형 호출자 ID인 특정 양상들에서, 공유 비밀 모듈(90)은 호출자 ID 오버라이드 로직(55)을 포함할 수 있다. 호출자 ID 오버라이드 로직(55)은 호출 요청의 페이로드에서, 호출 디바이스(즉, 제 2 통신 디바이스(14)) 호출자 ID 정보를 공유 비밀 소유자(즉, 실제 호출자)와 연관된 호출자 ID 정보로 대체하도록 동작가능하다. 공유 비밀(22)과 연관된 호출자 ID 정보는 클라이언트 정보 관리자(59)로부터 검색될 수 있다.

[0078] 공유 비밀 인식 및 연관이 네트워크 디바이스에서 수행되며, 공유 비밀과 관련된 기능이 원격 액세스, 통신 디바이스 관리 등에 관한 것인 대안적인 양상들에서, 공유 비밀 모듈(90)은 원격 액세스/디바이스 관리 삽입 로직(57)을 포함할 수 있다. 원격 액세스/디바이스 관리 삽입 로직(57)은 원격 액세스, 통신 디바이스 관리 등을 위한 명령들 및/또는 호출 요청 페이로드 식별 내에 삽입하도록 구성가능하다. 특정 양상들에서, 삽입 로직(57)은, 제 1 통신 디바이스(12)(즉, 피호출자)에 의해 인식가능하며 필수적인 원격 액세스, 통신 디바이스 관리 등과 연관된 페이로드 내에 코드와 같은 식별을 삽입할 수 있다. 대안적인 양상들에서, 삽입 로직(57)은 필수적인 원격 액세스, 통신 디바이스 관리 등을 수행하기 위해서 제 1 통신 디바이스(12)에 의해 실행될 페이로드 내에 루틴, 애플리케이션들, 애플릿 등과 같은 명령들을 삽입할 수 있다.

[0079] 도 5, 6, 7 및 8은 전화번호부 또는 콘택 목록 데이터 엔트리, 특히 연관된 콘택 목록에 대한 공유 비밀의 엔트리의 GUI 디스플레이들에 대한 예들을 제공한다. 도 5-8에 도시된 GUI 디스플레이들은 예시일 뿐이며, 전체 사용자 경험 플로우를 미리 정의된 디바이스 사용자 인터페이스들과 동화(assimilate)시킬 뿐만 아니라, 본 명세서에서 설명된 태스크들을 수행하기 위해서 예를 들어, 그래픽상으로의, 청취가능한 또는 그 외의 다양한 다른 사용자 인터페이스 구현들이 통신 디바이스의 제조자에 의해 채택될 수 있다는 것에 유의하여야 한다. 도 5는 개인 전화번호부 또는 콘택 목록 데이터베이스 내에 리스팅된 콘택들(102A-102F)의 디스플레이(100)를 제공한다. 예시된 양상에서, GUI의 사용자는 콘택 이름 "Davis"(102C)와 연관되는 공유 비밀을 입력하기를 희망한다. 사용자는 키패드 키 또는 다른 미리 결정된 디바이스 입력 메커니즘을 사용하여 "Davis" 콘택(102C)을 선택할 수 있다. "Davis" 콘택(102C)의 선택은 예를 들어, 도 6에 도시되는 콘택과 관련된 개인 정보가 디스플레이되도록 할 수 있다. 도 6에 도시된 바와 같이, 개인 정보에 대한 디스플레이(110)는 연락 이름(112), 연락 집 전화 번호(114), 연락 휴대 전화 번호(116), 연락 이메일 주소(118), 연락 집 주소(120), 및 연락 공유 비밀(122)과 같은 데이터 필드들 중 하나 또는 이들의 임의의 조합을 포함할 수 있다. 공유 비밀(122)과 연관된 공백(blank) 데이터 엔트리 필드(124)는 콘택이 연관된 공유 비밀을 현재 가지고 있지 않다는 것을 표시한다. 또한, 디스플레이(110)는 편집가능한 데이터 및/또는 데이터 엔트리 필드들을 제공하기 위해서 사용자에게 의해 사용(engage)되도록 동작가능한 "편집" 키(126)를 포함한다. 사용자는 "편집" 키(126)를 사용하는 것 뿐만 아니라, 개인 정보를 추가 또는 편집할 권한이 허가되도록 프로그래밍 보안 코드 또는 소정의 다른 형태의 허가를 입력할 수 있다.

[0080] 도 7은 도 6에 도시된 바와 같이 사용자가 "편집" 키(126)를 사용함으로써 발생할 수 있는 편집가능한 데이터 엔트리 필드들의 디스플레이(130)를 제공한다. 사용자는 연락 이름(112), 연락 집 전화 번호(114), 연락 휴대 전화 번호(116), 연락 이메일 주소(118) 및/또는 연락 집 주소(120)와 같은 이전에 입력된 데이터를 편집할 수 있다. 도시된 도면에서, 밑줄 그어진 데이터는 편집가능한 데이터를 표시한다. 도시된 바와 같이, 사용자는 공유 비밀(122)에 대한 엔트리 필드(124)에 공유 비밀 "009999"를 입력하였다. 또한, 데이터 엔트리 디스플레이(130)는 콘택 데이터베이스에 편집 및/또는 입력된 데이터를 세이브하기 위해서 사용자에게 의해 사용되도록 동작가능한 "세이브(save)" 키(132)를 포함한다. 데이터 엔트리 로직(32)은 입력된 공유 비밀이 데이터베이스 내의 다른 엔트리에 의해 이미 사용되고 있다는 디스플레이가능한 표시를 제공하도록 구성될 수 있음에 유의하여야 한다. 데이터 엔트리 로직이 이러한 표시를 제공하는 경우, 데이터 엔트리 로직(32)은 사용자가 공유 비밀의 이전 할당을 무시하도록 하거나, 또는 상이한 공유 비밀의 선택을 제공하도록 추가적으로 구성될 수 있다. 도 8은 사용자가 공유 비밀 코드를 입력함으로써 발생할 수 있는 개인 정보에 대한 디스플레이(140)를 제공한다. 공유 비밀 코드가 콘택 데이터베이스 메모리에 입력 또는 세이브되어 있으면, 콘택과 관련된 개인 정보의 후속적인 디스플레이는 공유 비밀이 존재한다는 것을 표시하기 위해서 예를 들어, 별표들 또는 소정의 다른 일반적 심볼/문자/숫자 디스플레이를 사용함으로써 공유 비밀 필드(124)를 제공할 수 있지만, 공유 비밀에 추가적인 보안을 제공하기 위해서 실제 디스플레이에서 가려진다. 개인 정보를 보거나 편집하기 위해서 "편집" 키(126) 또는 소정의 다른 액세스 키를 사용하고, 프로그래밍 보안 코드 또는 소정의 다른 형태의 허가를 입력함으로써, 공유 비밀의 실제 디스플레이가 보여질 수 있다.

[0081] 도 9, 10, 11, 및 12는 전화번호부 또는 콘택 목록 데이터 엔트리, 특히 연관된 콘택 목록에 대한 공유 비밀 및

관련된 공유 비밀 정보에 대한 GUI 디스플레이들에 대한 예들을 제공한다. 도 9는 개인 전화번호부 또는 콘택 목록 데이터베이스 내에 리스팅된 콘택들(202A-202F)의 디스플레이(200)를 제공한다. 예시된 양상에서, GUI 사용자는 콘택 이름 "Davis"(202C)와 연관되는 공유 비밀을 입력하기를 희망한다. 사용자는 키패드 키 또는 다른 미리 결정된 디바이스 입력 메커니즘을 사용하여 "Davis" 콘택(202C)을 선택할 수 있다. "Davis" 콘택(202C)의 선택은 예를 들어, 도 10에 도시되는 콘택과 관련된 개인 정보가 디스플레이되도록 할 수 있다. 도 10에 도시된 바와 같이, 개인 정보에 대한 디스플레이(210)는 콘택 이름(212), 콘택 집 전화 번호(214), 콘택 휴대 전화 번호(216), 콘택 이메일 주소(218), 콘택 집 주소(220), 콘택 공유 비밀(222), 및 공유 비밀 정보(226)와 같은 데이터 필드들 중 하나 또는 이들의 임의의 조합을 포함할 수 있다. 공유 비밀(222)과 연관된 공백 데이터 엔트리 필드(224) 및 공유 비밀 정보(226)와 연관된 공백 데이터 엔트리 필드(228)는 콘택이 연관된 공유 비밀 또는 관련된 공유 비밀 정보를 현재 가지고 있지 않다는 것을 표시한다. 또한, 디스플레이(210)는 편집가능한 데이터 및/또는 데이터 엔트리 필드들을 제공하기 위해서 사용자에게 의해 사용되도록 동작가능한 "편집" 키(230)를 포함한다. 사용자는 "편집" 키(230)를 사용하는 것 외에, 개인 정보를 추가 또는 편집할 권한이 허가되도록 프로그래밍 보안 코드 또는 소정의 다른 형태의 허가를 입력할 수 있다.

[0082] 도 11은 도 10에 도시된 바와 같이 사용자가 "편집" 키(230)를 사용함으로써 발생할 수 있는 편집가능한 데이터 엔트리 필드들의 디스플레이(240)를 제공한다. 사용자는 콘택 이름(212), 콘택 집 전화 번호(214), 콘택 휴대 전화 번호(216), 콘택 이메일 주소(218) 및/또는 콘택 집 주소(220)와 같은 이전에 입력된 데이터를 편집할 수 있다. 도시된 도면에서, 밑줄 그어진 데이터는 편집가능한 데이터를 표시한다. 도시된 바와 같이, 사용자는 공유 비밀(222)에 대한 엔트리 필드(224)에 공유 비밀 "009999"를 입력하였고, 공유 비밀 정보(226)에 대한 엔트리 필드(228)에 관련된 공유 비밀 정보 "URGENT"를 입력하였다. 또한, 데이터 엔트리 디스플레이(240)는 콘택 데이터베이스에 편집 및/또는 입력된 데이터를 저장하기 위해서 사용자에게 의해 사용되도록 동작가능한 "저장" 키(242)를 포함한다. 동작 중에, 사용자가 연관된 공유 비밀을 포함하는 호출 요청을 수신하는 경우, 관련된 공유 비밀 정보가 디스플레이되거나 디바이스 사용자에게 전달될 수 있다는 것에 유의하여야 한다. 따라서, 상기 예에서, 공유 비밀 정보는 호출 우선순위 정보를 포함한다. 공유 비밀에 의해 트리거되는 바와 같이, 공유 비밀 정보는 임의의 타입의 메시지의 디스플레이 또는 전달을 허용한다는 것에 유의하여야 한다. 추가적으로, 관련된 공유 비밀 정보는 또한 그래픽, 문자숫자식 문자(alphanumeric character), 및 비디오 파일 또는 오디오 파일 등과 같은 실행가능한 프로그램을 포함할 수 있고, 이들은 디스플레이되거나 디바이스 사용자에게 전달될 수 있다는 것에 유의하여야 한다. 대안적인 양상들에서, 공유 비밀 트리거 이외의 트리거될 수 있는 연관된 정보 트리거가 수신된 호출 요청에 포함되는 경우, 관련된 공유 비밀 정보만이 디스플레이될 수 있다. 다른 대안적인 양상들에서, 콘택과 연관된 개인 정보는 다수의 공유 비밀들의 엔트리 및/또는 다수의 관련된 공유 비밀 정보를 제공할 수 있다. 이러한 양상들에서, 콘택은 이름 및 전화 번호와 같은 콘택 정보에 대한 디스플레이를 제공하는 하나의 공유 비밀을 가질 수 있고, 다른 공유 비밀은 이름 및 전화번호와 같은 콘택 정보에 대한 디스플레이 및 호출 우선순위 정보 등과 같은 관련된 공유 비밀 정보에 대한 디스플레이를 제공할 수 있다.

[0083] 도 12는 사용자가 공유 비밀 코드 및 관련된 공유 비밀 정보를 입력함으로써 발생할 수 있는 개인 정보에 대한 디스플레이(250)를 제공한다. 공유 비밀 코드가 콘택 데이터베이스 메모리에 입력 또는 저장되어 있으면, 콘택과 관련된 개인 정보의 후속적인 디스플레이는 공유 비밀이 존재한다는 것을 표시하기 위해서 예를 들어, 별표들 또는 소정의 다른 일반적 심볼 디스플레이를 사용함으로써 공유 비밀 필드(224)를 제공할 수 있지만, 공유 비밀에 추가적인 보안을 제공하기 위해서 실제 디스플레이에서 가려진다. 개인 정보를 보거나 편집하기 위해서 "편집" 키(230) 또는 소정의 다른 액세스 키를 사용하고, 프로그래밍 보안 코드 또는 소정의 다른 형태의 허가를 입력함으로써, 공유 비밀의 실제 디스플레이가 보여질 수 있다. 예시된 양상에서, 공유 비밀 정보 필드(228)는 공유 비밀 정보에 대한 시각적 디스플레이를 제공한다. 대안적인 양상들에서, GUI 모듈은 공유 비밀 정보 필드(228) 내의 데이터를 가리거나 숨기도록 구성될 수 있다.

[0084] 도 13-16은 본 명세서에서 논의된 양상들에 따른, 호출자 ID 정보에 대한 GUI 디스플레이들을 제공한다. 도 13은 수신된 호출 요청이 공유 비밀을 포함하고 있지 않는 호출자 ID 정보에 대한 GUI 디스플레이(300)를 도시한다. 이러한 경우, 호출자 ID 로직은 호출 요청에서 식별 번호, 전형적으로 전화번호와 연관된 콘택 목록 또는 전화번호부로부터 개인 정보를 검색할 수 있다. 디스플레이된 정보는 호출 식별자(302), 및 호출 디바이스 전화 번호(304) 및/또는 호출자 이름(306)의 형태인 호출자 ID 정보를 포함할 수 있다. 예시되는 호출자 ID 예에서, 호출자는 전형적으로 호출자와 연관되고, 그리고/또는 호출자에 의해 소유되고, 그리고/또는 호출자에 등록되는 통신 디바이스로부터 호출하고 있으므로, 호출자는 호출 요청에서의 공유 비밀을 입력하지 않았다.

[0085] 도 14는 수신된 호출 요청이 공유 비밀을 포함하는 호출자 ID 정보에 대한 GUI 디스플레이(310)를 도시한다.

이러한 경우, 호출자 ID 로직, 공유 비밀 인식 로직, 또는 트리거 인식 로직은 호출 요청에서의 공유 비밀, 또는 선택적으로 트리거를 인식하고, 공유 비밀과 연관된 콘택 정보를 검색하며, 공유 비밀과 연관된 콘택 정보를 디스플레이할 수 있다. 디스플레이된 정보는 호출 식별자(302), 및 호출 디바이스 전화 번호(304) 및/또는 호출자 이름(306)의 형태인 호출자 ID 정보 중 하나 또는 이들의 임의의 조합을 포함할 수 있다. 이러한 양상에서, 호출 디바이스 전화 번호(304)는 호출을 요청하기 위해 사용되는 디바이스의 번호를 반영하는 반면, 호출자 번호(306)는 호출하고 있는 자(즉, 공유 비밀과 연관된 자)의 실제 이름을 반영한다. 예시된 호출자 ID 예에서, 호출자는 전형적으로 호출자와 연관된 통신 디바이스와 다른 통신 디바이스로부터 호출하고 있으므로, 호출자는 호출 요청에서의 공유 비밀을 입력하였다.

[0086] 도 15는 수신된 호출 요청이 공유 비밀을 포함하고, 공유 비밀은 공유 비밀 정보와 연관된 호출자 ID 정보에 대한 GUI 디스플레이(320)를 도시한다. 이러한 경우, 호출자 ID 로직, 공유 비밀 인식 로직, 또는 트리거 인식 로직은 호출 요청에서의 공유 비밀, 또는 선택적으로 트리거를 인식하고, 관련된 공유 비밀 정보를 검색하며, 공유 비밀과 연관된 관련된 공유 비밀 정보를 디스플레이할 수 있다. 공유 비밀 자체는 관련된 공유 비밀 정보의 디스플레이를 제공할 수 있거나, 선택적으로, 트리거는 관련된 공유 비밀 정보의 디스플레이를 제공한다. 디스플레이된 정보는 호출 식별자(302), 호출 디바이스 전화 번호(304) 및/또는 호출자 이름(306)의 형태인 호출자 ID 정보, 및 관련된 공유 비밀 정보(308) 중 하나 또는 이들의 임의의 조합을 포함할 수 있다. 이러한 경우, 관련된 공유 비밀 정보(308)는 "URGENT" 메시지의 형태인 호출 우선순위 태깅이다. 예시된 호출 ID 예에서, 호출자가 전형적으로 호출자와 연관된 통신 디바이스로부터 호출하고 있으므로, 호출 ID 기능을 무시하기 위해서 공유 비밀이 요구되지는 않지만, 호출자 ID 정보 내에 호출 우선순위 태깅을 포함하기 위해서 공유 비밀, 및 선택적으로 트리거가 입력되었다.

[0087] 도 16은 수신된 호출 요청이 연관되지 않은 공유 비밀을 포함하는 호출자 ID 정보에 대한 GUI 디스플레이(330)를 도시한다. 이러한 경우, 호출자 ID 로직, 공유 비밀 인식 로직, 또는 트리거 인식 로직은 호출 요청에서의 공유 비밀, 또는 선택적으로 트리거를 인식하고, 공유 비밀과 연관된 콘택 정보의 검색을 시도할 수 있다. 그러나, 공유 비밀이 디바이스 데이터베이스 내의 임의의 콘택과 연관되지 않으므로, 디바이스는 수신된 공유 비밀과 데이터베이스 내의 콘택들 사이에 매치가 존재하지 않는다는 것을 디바이스 사용자에게 통지하는 메시지를 호출자 ID 정보 내에 디스플레이한다. 이로서, 디스플레이된 정보는 호출 식별자(302), 호출 디바이스 전화 번호(304)의 형태인 호출자 ID 정보 및 "비-매치(no match)" 메시지(332) 중 하나 또는 이들의 임의의 조합을 포함할 수 있다. 전형적으로, 연관되지 않은 공유 비밀을 포함하는 호출 수신은 호출자가 정확하지 않은 전화 번호 또는 정확하지 않은 공유 비밀을 입력함으로써 발생한다.

[0088] 도 17은 공유 비밀들, 및 일부 예들에서 선택적인 트리거들을 포함하는 호출 요청 시퀀스들의 4가지 예들을 도시한다. 제 1 예(350)는 피호출자의 전화 번호 및 공유 비밀을 포함하는 호출 요청 시퀀스를 도시한다. 호출자는 호출받을 자의 전화 번호를 입력하고, 전형적으로 호출 지연 기간 이후, 공유 비밀 코드를 입력한다. 전술한 바와 같이, 공유 비밀은 숫자 코드의 형태를 취할 수 있고, 호출자와 피호출자 사이에 비밀로 공유되었던 호출 요청에 첨부된 임의의 다른 데이터는 공유 비밀로서의 역할을 할 수 있다. 제 2 예(360)에서, 호출 요청 시퀀스는 피호출자, 트리거, 및 공유 비밀의 전화 번호를 포함한다. 트리거는 호출 네트워크 내에서, 그리고 피호출자 디바이스에서 공유 비밀 인식을 제공하고, 선택적으로, 트리거는 공유 비밀과 연관된 기능 또는 애플리케이션을 식별할 수 있다. 예를 들어, 트리거는 둘 이상의 디지털 숫자 코드에 선행하는 키패드 상의 "*" 키를 이용하는 것을 포함할 수 있다. 트리거가 공유 비밀과 연관된 기능 또는 애플리케이션을 식별하는 양상들에서, "*88"은 맞춤형 호출자 ID 기능과 연관될 수 있고, "*89"는 호출 우선순위 태깅 기능 등과 연관될 수 있다.

[0089] 제 3 예(370)는 공유 비밀 인식을 제공하고, 일부 양상들에서, 공유 비밀과 연관된 기능 또는 애플리케이션을 식별하기 위해서 다수의 고유의 트리거들의 사용을 구현하는 호출 요청 시퀀스를 도시한다. 제 3 예(370)에서, 호출 요청 시퀀스는 피호출자의 전화 번호, 및 공유 비밀에 선행하는 각 트리거를 가지는 다수의 고유의 트리거들을 포함한다. 이러한 예에서, 각 트리거는 고유의 디바이스 기능 또는 애플리케이션을 통해 식별된다. 예를 들어, 사용자의 공유 비밀 "009999"에 선행하는 제 1 트리거 "*88"의 입력은 맞춤형 호출자 ID 기능을 제공할 수 있고, 사용자의 공유 비밀 "009999"에 선행하는 제 2 트리거 "*89"는 호출 우선순위 태깅을 제공할 수 있고, 사용자의 공유 비밀 "009999"에 선행하는 제 3 트리거 "*90"의 입력은 피호출 통신 디바이스 상에서 시작될 추가적인 기능 또는 애플리케이션을 제공할 수 있다. 이러한 구현에서, 호출자는 피호출 디바이스 상에서 다수의 원격 기능들을 수행하기 위해서 하나의 공유 비밀만을 요구한다. 트리거 코드들은 호출 디바이스 상에 저장될 수 있고, GUI 디스플레이를 통해 사용자에게 액세스가능할 수 있다.

- [0090] 제 4 예(380)는 단일 트리거 및 다수의 공유 비밀들의 사용을 구현하는 호출 요청 시퀀스를 도시하고, 각각의 공유 비밀은 피호출자 디바이스 상의 고유의 기능 또는 애플리케이션과 연관된다. 제 4 예(380)에서, 호출 요청 시퀀스는 피호출자의 전화번호, 트리거, 및 다수의 고유의 공유 비밀들을 포함한다. 예를 들어, "*88" 등과 같은 트리거의 입력은 호출 요청이 하나 이상의 공유 비밀들을 포함한다는 것을 네트워크 및 피호출 디바이스로 통지한다. 상기 트리거는 맞춤형 호출자 ID 기능과 연관된 제 1 공유 비밀 "009999", 호출 우선순위 태깅 기능과 연관된 제 2 공유 비밀 "009998", 및 피호출 통신 디바이스 상에서 시작될 추가적인 기능 또는 애플리케이션과 연관된 제 3 공유 비밀 "009997"과 같은 다수의 공유 비밀들에 선행한다.
- [0091] 도 17에 도시된 호출 시퀀스들의 예들은 임의의 방식으로 제한되는 것으로 간주되지 않는다는 것에 유의하여야 한다. 공유 비밀들, 및 선택적인 트리거들을 포함하는 다른 호출 요청 시퀀스들은 또한 본 양상들의 개념 내에서 참조되고 포함된다. 전술한 바와 같이, 공유 비밀들 및 선택적인 트리거들은 호출 요청 동안 호출 디바이스 키패드 상에 입력된 숫자 코드들에 제한되지 않는다. 공유 비밀들은 텍스트 데이터, 오디오 데이터, 시각적 데이터 등을 포함하지만 이에 제한되지 않는 당사자들 사이에서 공유된 임의의 비밀 데이터를 포함할 수 있다. 트리거는 다음에 나타날 공유 비밀을 네트워크 및 피호출 디바이스로 통지하기 위해서 호출 요청과 함께 전달될 수 있는 호출 디바이스 상의 임의의 입력을 포함할 수 있다.
- [0092] 도 18은 일 양상에 따라, 클라이언트-기반의 고객 호출자 ID, 및/또는 피호출 통신 디바이스의 원격 기능 관리를 구현하기 위한 방법을 구현하는 흐름 다이어그램이다. 이벤트(400)에서, 공유 비밀들, 및 선택적인 트리거들 및/또는 선택적인 관련된 공유 비밀 정보는 통신 디바이스에 저장된다. 공유 비밀들, 트리거들, 및 관련 공유 비밀 정보는 적절한 GUI 모듈의 구현을 통하여 디바이스 사용자에게 의해 수동으로 입력될 수 있거나, 또는 전자 통신을 통해 수신된 공유 비밀들, 트리거들, 및 관련 공유 비밀 정보는 자동으로 입력 및 저장될 수 있다. 전술한 바와 같이, 공유 비밀들은 전형적으로 콘택 또는 전화번호부 엔트리와 연관되며, 콘택 또는 전화번호부 엔트리와 관련하여 저장된다. 따라서, 공유 비밀들, 및 선택적인 트리거들 및/또는 선택적인 관련 공유 비밀 정보는 콘택 데이터베이스, 전화번호부 등에 저장될 수 있다.
- [0093] 이벤트(410)에서, 통신 디바이스는 호출 ID 번호, 공유 비밀, 및, 선택적으로 트리거를 포함하는 호출 요청을 수신한다. 트리거는 호출 요청이 공유 비밀을 포함한다는 것을 통신 디바이스로 통지하도록 작용할 수 있다. 추가적으로, 트리거는 공유 비밀과 연관된 기능 또는 애플리케이션을 식별하도록 작용할 수 있다. 이벤트(420)에서, 통신 디바이스는 공유 비밀과 연관되거나, 선택적으로, 트리거와 연관된 기능 또는 애플리케이션을 결정할 수 있다. 일부 양상들에서, 공유 비밀들의 사용이 하나의 기능에 제한될 수 있음에 따라, 공유 비밀, 또는 선택적인 트리거와 연관된 기능 또는 애플리케이션의 결정이 요구되지 않을 수 있다. 그러나, 다수의 기능들 또는 애플리케이션들이 공유 비밀들의 사용과 연관되는 대안적인 양상들에서, 공유 비밀 또는 트리거는 공유 비밀과 관련된 기능 또는 애플리케이션과 관련된 정보를 제공할 수 있다. 예를 들어, 숫자 트리거 코드들은 공유 비밀의 기능을 표시할 수 있다.
- [0094] 이벤트(430)에서, 통신 디바이스는 공유 비밀이 콘택 또는 전화번호부 엔트리와 연관된다는 것을 검증하기 위해서 콘택 목록 데이터베이스, 개인 전화번호부 데이터베이스 등과 같은 데이터베이스에 액세스한다. 이벤트(440)에서, 공유 비밀이 검증되었다면, 콘택 목록 또는 전화번호부 엔트리 내의 데이터는 결정된 기능 또는 애플리케이션에 따라 액세스 및 검색된다. 예를 들어, 맞춤형 호출자 ID 기능이 공유 비밀 또는 트리거와 연관되는 경우, 콘택과 관련된 이름 또는 다른 개인 정보는 통신 디바이스 상에서의 후속적인 디스플레이를 위하여 검색된다. 대안적으로, 호출 우선순위 태깅이 공유 비밀 또는 트리거와 연관되는 경우, 우선순위 태그 즉, "urgent" 등과 같은 공유 비밀과 관련된 정보는 통신 디바이스 상에서의 후속적인 디스플레이를 위하여 검색된다. 대안적인 양상들에서, 디바이스가 데이터베이스에 액세스하고 임의의 관련된 공유 비밀 정보를 결정하면, 통신 디바이스는 공유 비밀 또는 트리거와 연관된 기능 또는 애플리케이션을 결정하도록 구성될 수 있다.
- [0095] 도 19는 네트워크 디바이스에서의 공유 비밀, 및 선택적으로, 트리거 인식 및 포워딩을 위한 방법을 제공한다. 이벤트(500)에서, 네트워크 디바이스는 호출자 ID 번호, 공유 비밀, 및 선택적으로, 트리거를 포함하는 호출 요청을 수신한다. 이벤트(510)에서, 네트워크 디바이스는 공유 비밀을 구문 분석하고, 선택적으로, 선택적인 트리거를 구문 분석할 수 있다. 트리거가 공유 비밀을 피호출 디바이스로 통지하도록 작용하거나, 트리거가 공유 비밀과 연관된 기능 또는 애플리케이션을 식별하도록 작용하는 경우, 선택적인 트리거를 분석하는 것 및 이후에 포함하는 것은 필요할 수 있다. 이벤트(520)에서, 분석된 데이터 즉, 호출자 ID 번호, 공유 비밀, 및 선택적으로 트리거를 포함하는 호출 요청은 피호출 디바이스로 포워딩된다.
- [0096] 도 20은 일 양상에 따라, 네트워크-기반의 고객 호출자 ID, 및/또는 피호출 통신 디바이스의 원격 기능 관리를

위한 방법에 대한 흐름 다이어그램을 제공한다. 이벤트(600)에서, 공유 비밀들, 및 선택적인 트리거들 및/또는 선택적인 관련된 공유 비밀 정보는 클라이언트 데이터베이스와 같은 네트워크 데이터베이스에 저장된다. 공유 비밀들, 트리거들, 및 관련된 공유 비밀 정보는 공유 비밀 홀더(shared secret holder)에 의해 네트워크 데이터 베이스로 전달될 수 있거나, 공유 비밀이 신뢰되는(trusted)/공유되는 자에 의해 네트워크로 전달될 수 있다. 일 양상에서, 공유 비밀들, 트리거들, 및 임의의 관련 정보는 네트워크에서의 각 클라이언트에 대한 개별적인 엔트리들을 제공하는 클라이언트 데이터베이스에 저장될 수 있다. 클라이언트 데이터베이스는 호출 요청들을 이후에 수신하는 동일한 디바이스 내에, 또는 호출 요청-수신 네트워크 디바이스에 액세스가능한 임의의 다른 네트워크 위치에 저장될 수 있다.

[0097] 이벤트(610)에서, 네트워크 디바이스는 호출 ID 번호, 공유 비밀, 및 선택적으로 트리거를 포함하는 호출 요청을 수신한다. 트리거는 호출 요청이 공유 비밀을 포함한다는 것을 네트워크 디바이스로 통지하도록 작용할 수 있다. 추가적으로, 트리거는 공유 비밀과 연관된 기능 또는 애플리케이션을 식별하도록 작용할 수 있다. 이벤트(620)에서, 통신 디바이스는 공유 비밀과 연관된, 또는 선택적으로, 트리거와 연관된 기능 또는 애플리케이션을 결정할 수 있다. 일부 양상들에서, 공유 비밀들의 사용이 하나의 기능에 제한될 수 있음에 따라, 공유 비밀, 또는 선택적인 트리거와 연관된 기능 또는 애플리케이션의 결정이 요구되지 않을 수 있다. 그러나, 다수의 기능들 또는 애플리케이션들이 공유 비밀들의 사용과 연관되는 대안적인 양상들에서, 공유 비밀 또는 트리거는 공유 비밀과 관련된 기능 또는 애플리케이션과 관련된 정보를 제공할 수 있다. 예를 들어, 숫자 트리거 코드들은 공유 비밀의 기능을 표시할 수 있다.

[0098] 이벤트(630)에서, 통신 디바이스는 공유 비밀이 콘택 또는 전화번호부 엔트리와 연관된다는 것을 검증하기 위해서 클라이언트 등과 같은 네트워크 데이터베이스에 액세스한다. 이벤트(640)에서, 공유 비밀이 검증되었다면, 클라이언트 엔트리 내의 데이터는 결정된 기능 또는 애플리케이션에 따라 액세스 및 검색된다. 예를 들어, 맞춤형 호출자 ID 기능이 공유 비밀 또는 트리거와 연관되는 경우, 클라이언트와 관련된 이름 또는 다른 개인 정보는 통신 디바이스로의 후속적인 전달을 위하여 검색된다. 대안적으로, 호출 우선순위 태깅이 공유 비밀 또는 트리거와 연관되는 경우, 우선순위 태그 즉, "urgent" 등과 같은 공유 비밀과 관련된 정보는 통신 디바이스 상에서의 후속적인 디스플레이를 위하여 검색된다. 대안적인 양상들에서, 디바이스가 데이터베이스에 액세스하고 임의의 관련된 공유 비밀 정보를 결정하면, 네트워크 디바이스는 공유 비밀 또는 트리거와 연관된 기능 또는 애플리케이션을 결정하도록 구성될 수 있다.

[0099] 이벤트(650)에서, 수행될 기능이 호출자 ID를 맞춤화하는 경우, 네트워크 디바이스는, 클라이언트 데이터베이스로부터 검색되고 공유 비밀과 연관된 호출자 ID 정보와 호출 요청에서의 호출자 ID 정보를 무시할 것이다. 추가적으로, 수행될 기능이 원격 액세스/디바이스 관리와 관련되는 경우, 네트워크 디바이스는 호출 요청 페이로드 내에 코드들 등과 같은 원격 액세스/디바이스 관리 식별자들을 삽입하거나, 호출 요청의 페이로드 내에 애플리케이션들, 루틴들, 애플릿들 등과 같은 명령들을 삽입할 수 있다. 이벤트(660)에서, 맞춤형 호출자 ID 정보 및/또는 원격 액세스/디바이스 관리 식별자 또는 명령들을 포함하는 호출 요청은 피호출 통신 디바이스로 포워딩된다.

[0100] 따라서, 설명된 양상들은 호출자들 및 피호출자들 사이의 공유 비밀 교환을 구현함으로써 디바이스 기능의 원격 관리를 수행하거나, 호출자 ID를 맞춤화하기 위한 방법들, 디바이스들, 시스템들, 및 컴퓨터 프로그램 물건들을 제공한다. 맞춤형 호출자 ID는 호출자가 호출하기 위해 사용하는 디바이스와는 상관없이 호출자가 자신을 식별하도록 제공한다. 게다가, 호출 우선순위 태깅과 같은 다른 기능은 호출자가 호출의 우선 순위를 결정하거나, 또는 호출 식별 메시지를 피호출자에 맞춤화하도록 제공한다. 호출자들과 피호출자들 사이에서 공유 비밀들을 교환함으로써, 맞춤형 호출자 ID 및 원격 기능 관리 방법은 보안되고, 알려지지 않은 자들에 의한 허가되지 않은 탬퍼링(tampering)의 가능성이 제거된다. 또한, 공유 비밀 교환은 예를 들어, 오프 상태로 통신 디바이스를 원격으로 로킹 다운시키는 것과 같이, 허가된 호출자들이 통신 디바이스에 원격으로 액세스하고 통신 디바이스를 관리하도록 제공한다.

[0101] 본 명세서에 기재된 실시예들과 관련하여 설명된 다양한 예시적인 논리들, 논리 블록들, 모듈들, 및 회로들이 범용 프로세서, 디지털 신호 처리기(DSP), 주문형 집적회로(ASIC), 필드 프로그래머블 게이트 어레이(FPGA), 또는 다른 프로그래머블 논리 디바이스, 이산 게이트 또는 트랜지스터 논리, 이산 하드웨어 컴포넌트들, 또는 이러한 기능들을 수행하도록 설계된 이들의 조합을 통해 구현 또는 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안적 실시예에서, 이러한 프로세서는 기존 프로세서, 제어기, 마이크로 제어기, 또는 상태 머신일 수 있다. 프로세서는 예를 들어, DSP 및 마이크로프로세서, 복수의 마이크로프로세서들, DSP 코어와 결합된 하나 이상의 마이크로프로세서들, 또는 이러한 임의의 다른 구성들의 조합과 같이 컴퓨팅 디바이스들

의 조합으로서 구현될 수도 있다.

- [0102] 본 명세서에 기재된 실시예들과 관련하여 설명된 알고리즘 또는 방법의 동작들은 하드웨어에서, 프로세서에 의해 실행되는 소프트웨어 모듈에서, 또는 이들의 조합에 의해 직접 실시될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드디스크, 휴대용 디스크, CD-ROM, 또는 공지된 저장 매체의 임의의 다른 형태로서 상주할 수 있다. 예시적인 저장 매체는 프로세서와 결합되어, 프로세서는 저장 매체로부터 정보를 판독하여 저장 매체에 정보를 기록할 수 있다. 대안적으로, 저장 매체는 프로세서의 구성요소일 수 있다. 이러한 프로세서 및 저장 매체는 ASIC 에 상주할 수 있다. ASIC 는 사용자 단말에 상주할 수 있다. 대안적으로, 프로세서 및 저장 매체는 사용자 단말에서 이산 컴포넌트들로서 상주할 수 있다.
- [0103] 전술한 내용은 예시적인 양상들 및/또는 실시예들을 나타내지만, 첨부되는 청구항들에 의해 정의되는 바와 같이 설명된 양상들 및/또는 실시예들의 범위를 벗어나지 않고 다양한 변경들 및 변형들이 이루어질 수 있다는 점에 유의하여야 한다. 또한, 설명된 실시예들의 엘리먼트들이 단수의 형태로 설명 또는 청구될 수 있지만, 단수에 대한 명백한 한정이나 기재되지 않는 한 복수의 형태로 고려될 수 있다. 또한, 다르게 설명되지 않는다면, 임의의 양상 및/또는 실시예의 전부 또는 일부는 임의의 다른 양상 및/또는 실시예의 전부 또는 일부와 함께 이용될 수 있다.
- [0104] 따라서, 본 발명의 다양한 변형들 및 다른 실시예들은 전술한 설명들 및 연관된 도면들에서 제시되는 설명 내용들의 이점을 가지는 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 생각할 수 있다. 따라서, 본 발명이 설명된 특정 실시예들에 한정되지 않고, 변형들 및 다른 실시예들이 첨부되는 청구항들의 범위에 벗어나지 않는 것으로 해석된다는 것을 이해하여야 한다. 본 명세서에서 특정 용어들이 사용되지만, 이러한 용어들은 일반적으로, 그리고 기술적인 의미에서 사용될 뿐이며, 한정을 위해서 사용되는 것은 아니다.

도면의 간단한 설명

- [0025] 도 1은 맞춤형 호출자 식별 및/또는 원격 통신 디바이스 액세스를 제공하기 위한 통신 디바이스 기반의 시스템의 일 양상에 대한 개략적인 다이어그램이다.
- [0026] 도 2는 맞춤형 호출자 식별 및/또는 원격 통신 디바이스 액세스를 제공하기 위한 네트워크 기반의 시스템의 일 양상에 대한 개략적인 다이어그램이다.
- [0027] 도 3은 맞춤형 호출자 식별 및/또는 원격 통신 디바이스 액세스를 제공하기 위한 통신 디바이스의 일 양상에 대한 블록 다이어그램이다.
- [0028] 도 4는 맞춤형 호출자 식별 및/또는 원격 통신 디바이스 액세스를 제공하기 위한 네트워크 디바이스의 일 양상에 대한 블록 다이어그램이다.
- [0029] 도 5-8은 콘택 또는 전화번호부 데이터베이스에 공유 비밀들을 입력하기 위한 절차를 하이라이트하는 그래픽 사용자 인터페이스의 디스플레이에 대한 예들이다.
- [0030] 도 9-12는 콘택 또는 전화번호부 데이터베이스에 호출 우선순위와 같은 공유 비밀들 및 관련된 공유 비밀 정보를 입력하기 위한 절차를 하이라이트하는 그래픽 사용자 인터페이스의 디스플레이에 대한 예들이다.
- [0031] 도 13은 호출자가 자신의 통신 디바이스로부터 호출하고 있는 호출자 ID 모드를 하이라이트하는 그래픽 사용자 인터페이스의 디스플레이이다.
- [0032] 도 14는 호출자가 자신의 디바이스가 아닌 통신 디바이스로부터 호출하고 있는 맞춤형 호출자 ID 모드를 하이라이트하는 그래픽 사용자 인터페이스의 디스플레이이다.
- [0033] 도 15는 호출자가 호출에 대한 우선순위를 식별하는 맞춤형 호출자 ID 모드를 하이라이트하는 그래픽 사용자 인터페이스의 디스플레이이다.
- [0034] 도 16은 통신 디바이스가 호출 요청에서 검색된 공유 비밀을 매치시킬 수 없는 맞춤형 호출자 ID 모드를 하이라이트하는 그래픽 사용자 인터페이스의 디스플레이이다.
- [0035] 도 17은 트리거들 및 공유 비밀 코드들을 이용하여 맞춤형 호출자 ID 및/또는 원격 통신 디바이스 액세스를 실행시키는 호출 엔트리 시퀀스들에 대한 예들을 제공한다.
- [0036] 도 18은 맞춤형 호출자 ID 및/또는 피호출 통신 디바이스의 원격 기능 관리를 위한 통신 디바이스 기반의 방

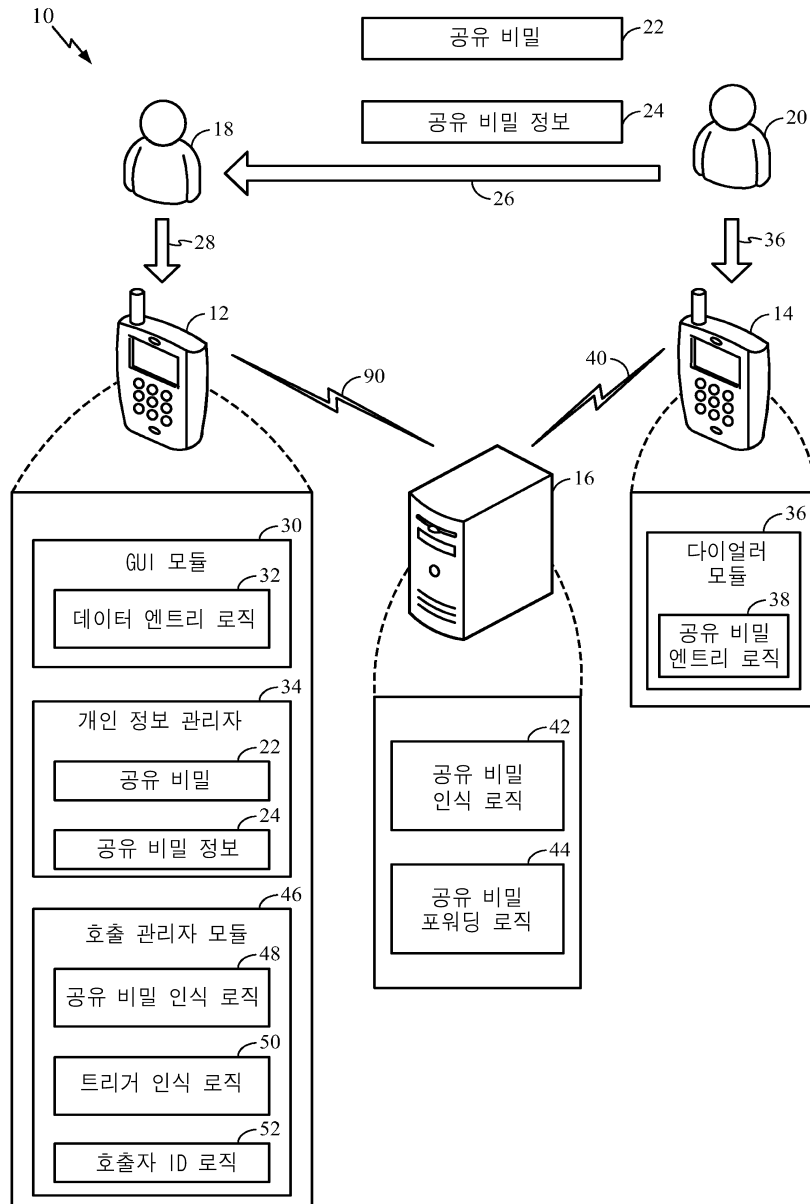
법의 일 양상에 대한 흐름 다이어그램이다.

[0037] 도 19는 네트워크 디바이스에서의 공유 비밀, 및 선택적으로, 트리거 인식 및 포워딩을 위한 방법의 일 양상에 대한 흐름 다이어그램이다.

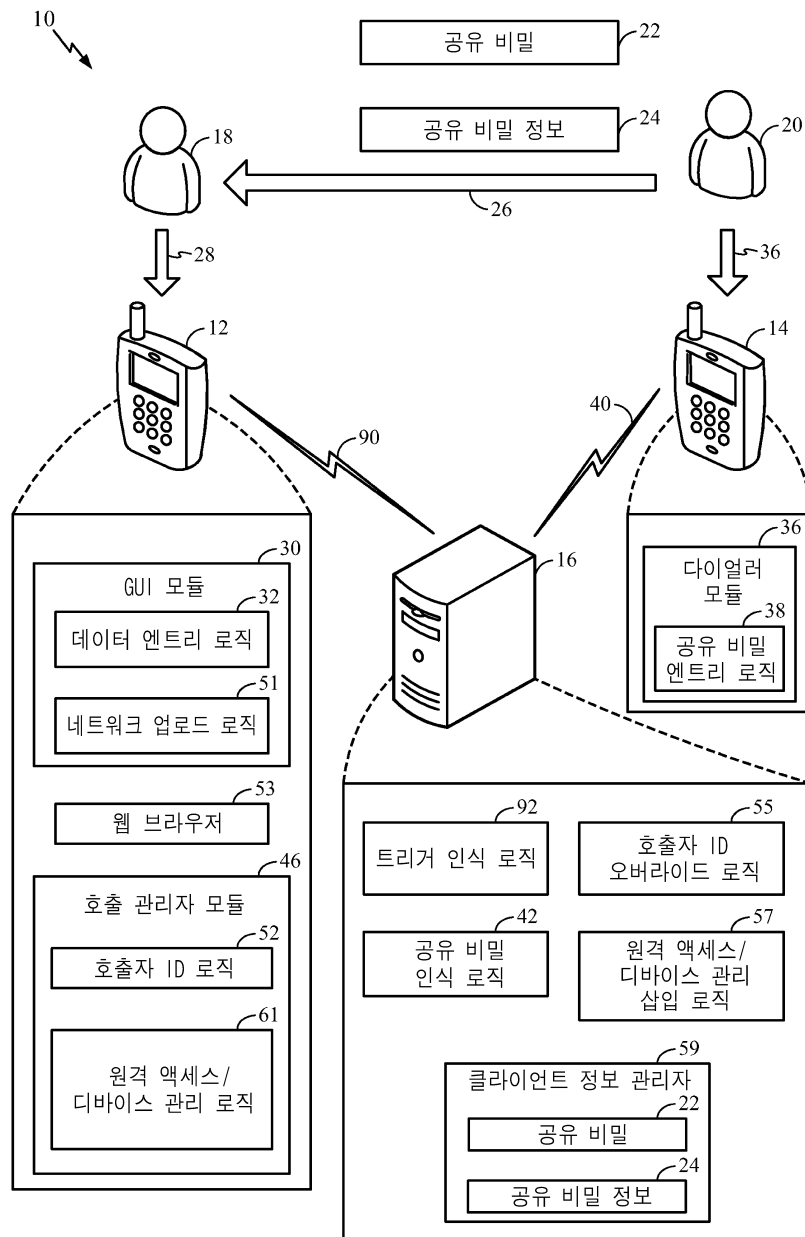
[0038] 도 20은 맞춤형 호출자 ID 및/또는 피호출 통신 디바이스의 원격 기능 관리를 위한 네트워크 디바이스 기반의 방법에 대한 흐름 다이어그램이다.

도면

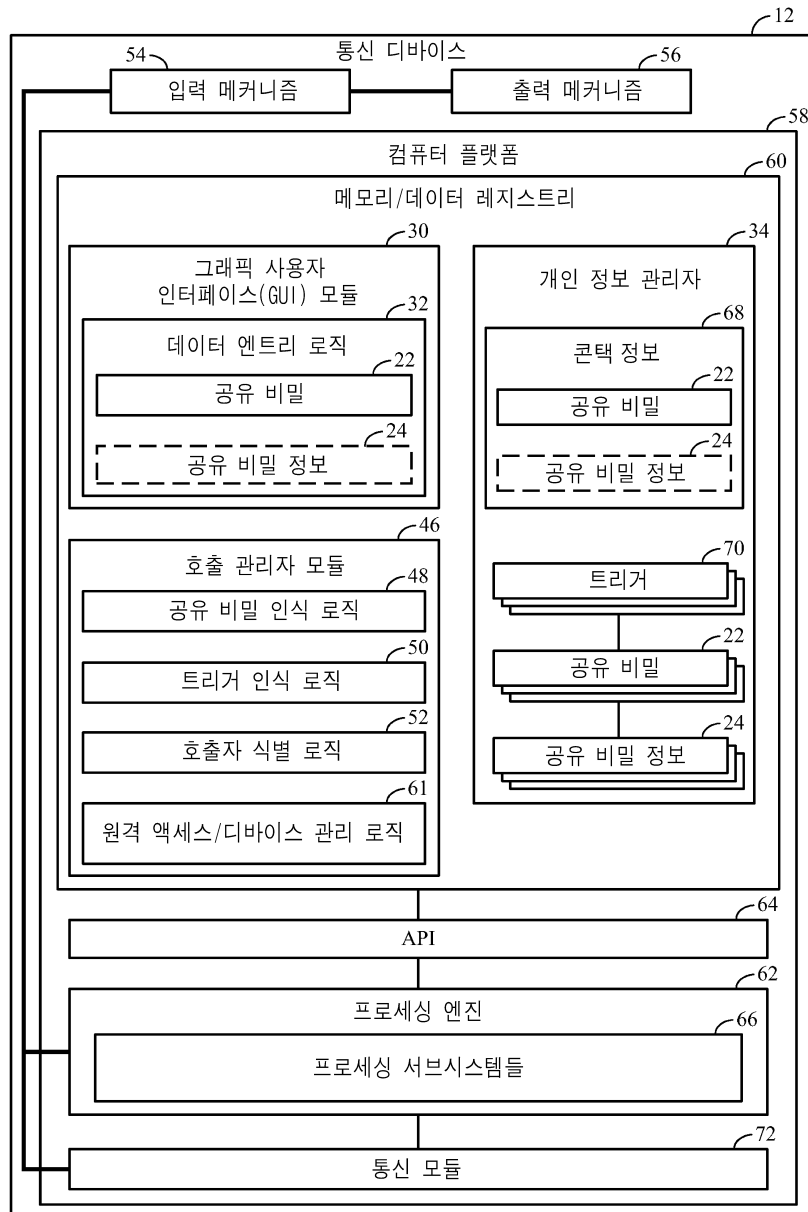
도면1



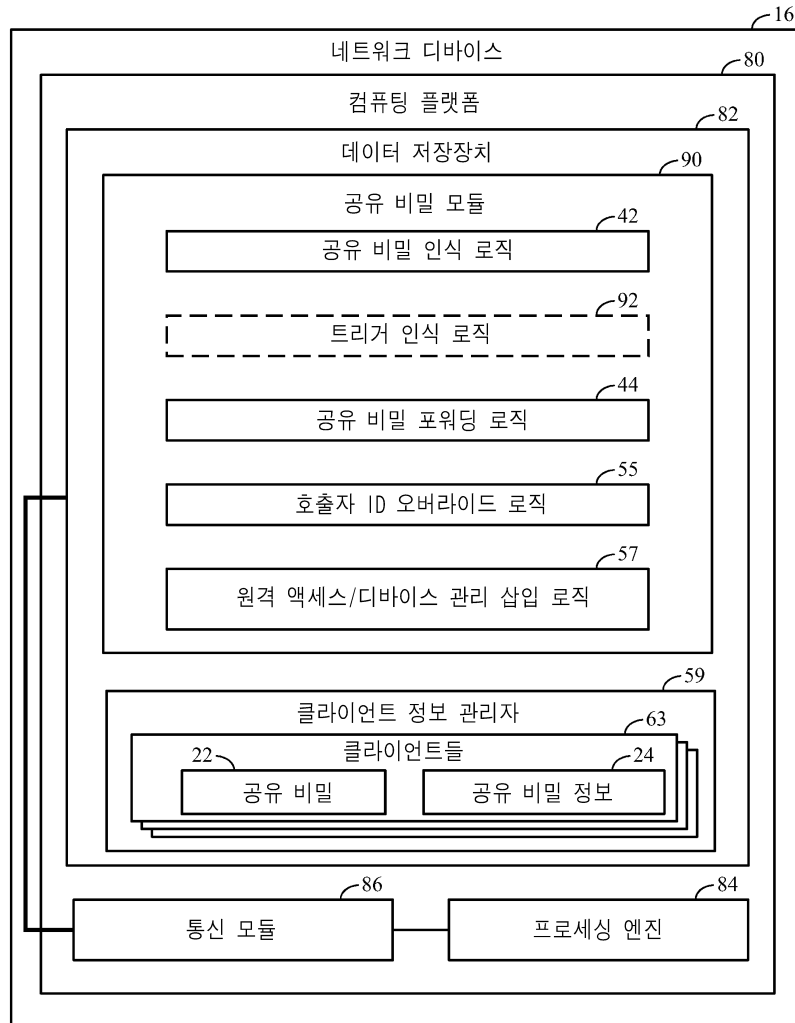
도면2



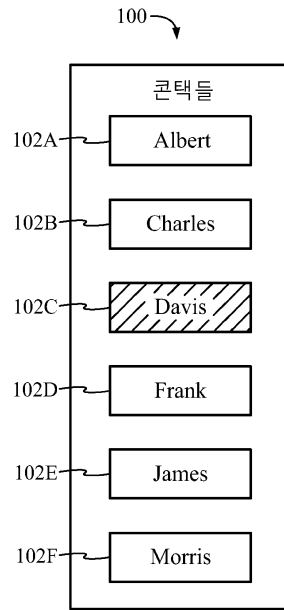
도면3



도면4



도면5



도면6



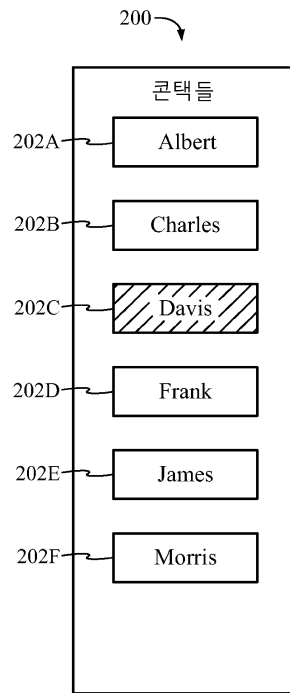
도면7



도면8



도면9



도면10



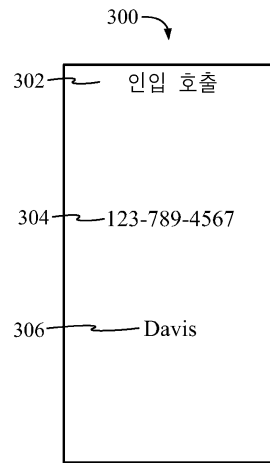
도면11



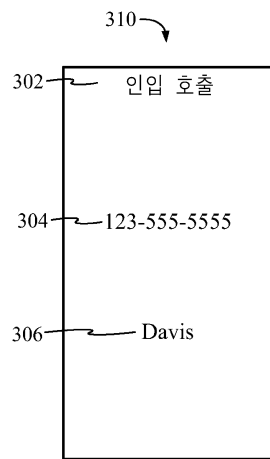
도면12



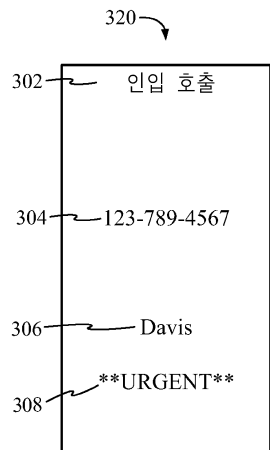
도면13



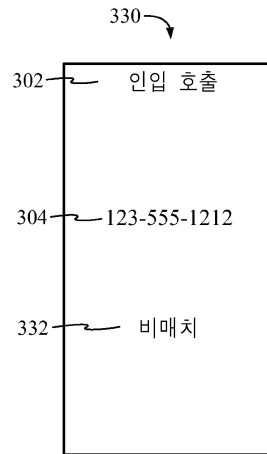
도면14



도면15



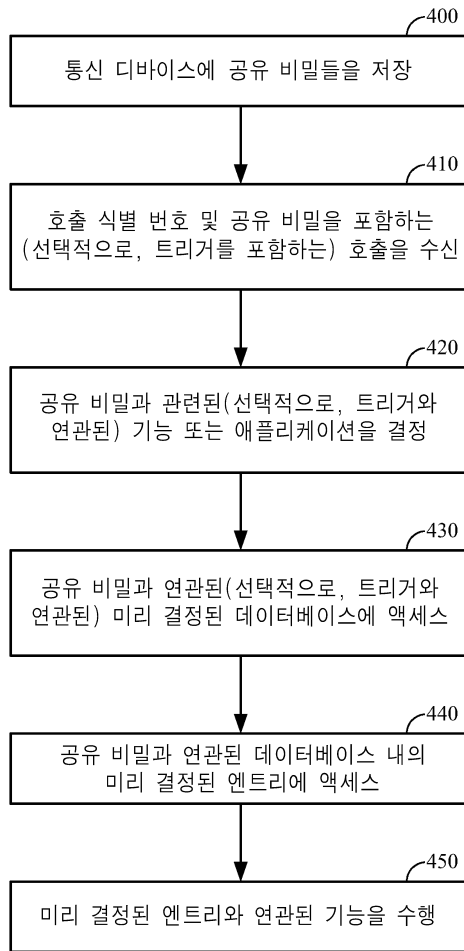
도면16



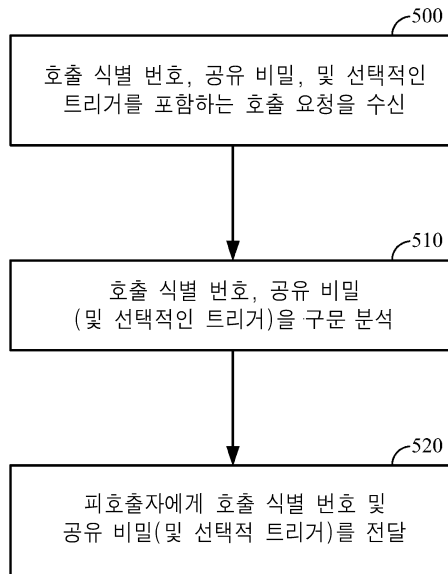
도면17

- 호출 요청 엔트리 시퀀스 예들
- 350 → 1. (피호출자 전화 번호)…(공유 비밀 코드)
 - 360 → 2. (피호출자 전화 번호)…(트리거)…(공유 비밀 코드)
 - 370 → 3. (피호출자 전화 번호)…(제 1 트리거 코드)…(공유 비밀 코드)…
(제 2 트리거 코드)…(공유 비밀 코드)…(제 n 트리거 코드)…(공유 비밀 코드)
 - 380 → 4. (피호출자 전화 번호)…(트리거 코드)…(제 1 공유 비밀 코드)…
(제 2 공유 비밀 코드)…(제 n 공유 비밀 코드)

도면18



도면19



도면20

