(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0052560
(43) 공개일자 2013년05월22일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/30* (2006.01)
H04L 9/08 (2006.01) *H04W 12/02* (2009.01)
(21) 출원번호 10-2012-7029633
(22) 출원일자(국제) 2011년04월12일
심사청구일자 없음
(85) 번역문제출일자 2012년11월12일
(86) 국제출원번호 PCT/US2011/032118
(87) 국제공개번호 WO 2011/130274
국제공개일자 2011년10월20일
(30) 우선권주장
61/323,713 2010년04월13일 미국(US)

(71) 출원인
코넬 유니버시티
미국 뉴욕 14850 이타카 슈트 310 파인트리로드 395, 코넬 센터 포 테크놀로지, 엔터프라이즈 앤 커머셜리제이션("씨씨티이씨")
(72) 발명자
위커, 스티븐 비.
미국 14850 뉴욕주 이타카 엘름우드 애비뉴 201
(74) 대리인
백만기, 양영준, 정은진

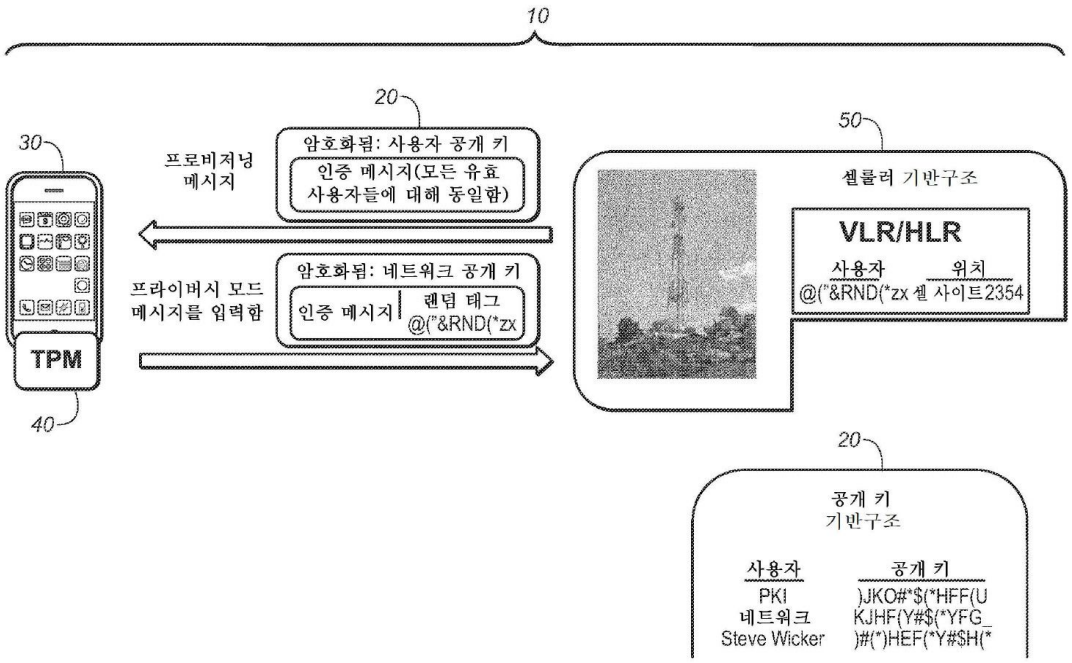
전체 청구항 수 : 총 60 항

(54) 발명의 명칭 **정보 네트워크들에 대한 사설 오버레이**

(57) 요 약

사설 오버레이는 사용자가 자신의 개인 정보의 책임을 지게 하는 정보 네트워킹을 위해 제공된다. 사용자 신원은 사용자 장비가 페이징될 수 있는 셀을 지정하는 숫자 태그로부터 분리된다. 사설 오버레이는 공개 키 기반구조 및 인증 기관(PKI)과 같은 등록 및 인증 기관의 추가에 의해 생성된다. 등록 및 인증 기관은 네트워크 및 모든 가입자들에게 네트워크 및 사용자들에 대한 공개 암호 키들을 제공한다. 개인 암호해독 키가 적절한 방식으로 로컬로 생성 및 저장된다. 이러한 추가를 통해, 기존의 셀룰러, 무선 또는 유틸리티 분배 기반구조에 대한 사설 오버레이가, 예를 들어, 셀룰러 또는 무선 네트워크에, 또는 유틸리티 분배 시스템에 등록한 디바이스에 대해 설정될 수 있다.

대 표 도



특허청구의 범위

청구항 1

네트워크에서 플랫폼의 사용자의 프라이버시를 보호하기 위한 시스템으로서,

공개 키 암호체계(20)에서 인증된 공개 키들을 분배하기 위한 시스템을 포함하는 사설 오버레이(10)

를 포함하고, 상기 플랫폼(40)은 사용자 장비(30)에 포함되고,

상기 인증된 공개 키들을 분배하기 위한 시스템은 상기 네트워크(50) 및 상기 네트워크의 각각의 허가된 사용자에게 상기 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공하는, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 2

제1항에 있어서,

상기 사용자 장비는 셀룰러 또는 이동 전화기, 컴퓨터 또는 고객 데이터 수집 시스템, 유틸리티 미터, 또는 유선 단말인, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 3

제2항에 있어서,

상기 고객 데이터 수집 시스템은 유틸리티 미터인, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 4

제1항에 있어서,

상기 인증된 공개 키들을 분배하기 위한 시스템은 공개 키 기반구조 및 인증 기관(Public Key Infrastructure and Certification Authority; PKI)인, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 5

제1항에 있어서,

상기 플랫폼은 셀룰러 플랫폼이고 상기 네트워크는 셀룰러 네트워크이고,

상기 플랫폼은 무선 플랫폼이고 상기 네트워크는 무선 네트워크이거나, 또는

상기 플랫폼은 유틸리티 플랫폼 또는 제3자 데이터 수신 및 관리 플랫폼이고, 상기 네트워크는 고객 데이터 수집 유닛과 통신하는 통신 네트워크인, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 6

제1항에 있어서,

개인 암호해독 키가 로컬로 생성되고 저장되는, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 7

제1항에 있어서,

상기 플랫폼은 셀룰러 플랫폼이고,

상기 네트워크는 셀룰러 네트워크이고,

상기 셀룰러 네트워크는 상기 사용자 장비를 난수와 연관시키고, 이에 의해 사용자 신원으로부터 상기 사용자 장비를 분리시키는, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 8

제1항에 있어서,

상기 플랫폼은 무선 플랫폼이고,

상기 네트워크는 무선 네트워크이고,

상기 무선 네트워크는 상기 사용자 장비를 사용자 계정 식별자가 아닌 난수와 연관시키고, 이에 의해 사용자 신원으로부터 상기 사용자 장비를 분리시키는, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 9

제1항에 있어서,

상기 플랫폼은 유틸리티 또는 제3자 데이터 수신 및 관리 플랫폼이고,

상기 네트워크는 통신 네트워크이고,

상기 통신 네트워크는 상기 사용자 장비를 난수와 연관시키고, 이에 의해 사용자 신원으로부터 상기 사용자 장비를 분리시키는, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 10

제1항에 있어서,

암호 칩(60)을 포함하고, 상기 플랫폼은 상기 암호 칩을 포함하고, 상기 암호 칩은 암호 보안 볼트(vault)에 인증 메시지를 보관하도록 프로그래밍되는, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 11

제10항에 있어서,

상기 암호 칩은 신뢰된 플랫폼 모듈(Trusted Platform Module; TPM)인, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 12

제10항에 있어서,

상기 플랫폼은 셀룰러이고, 상기 암호 칩은 상기 사용자 장비가 셀룰러 모드에 있는 동안 호출 시간(minute)들을 계속 추적하도록 프로그래밍되는, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 13

제12항에 있어서,

상기 호출 시간들은 선불되는, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 14

제10항에 있어서,

상기 플랫폼은 무선이고, 상기 암호 칩은 상기 사용자 장비가 무선 모드에 있는 동안 무선 사용 시간들을 계속 추적하도록 프로그래밍되는, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 15

제14항에 있어서,

상기 무선 사용 시간들은 선불되는, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 16

제10항에 있어서,

상기 암호 칩은 원격 증명(attestation)을 지원하도록 프로그래밍되어, 이에 의해 상기 네트워크가 상기 사용자

장비가 허가되는지의 여부를 원격으로 결정하는, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 17

제10항에 있어서,

상기 암호 칩은 원격 증명을 지원하도록 프로그래밍되어, 이에 의해 상기 네트워크가 상기 사용자 장비가 복제되었는지의 여부를 원격으로 결정하는, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 18

제10항에 있어서,

상기 암호 칩은 원격 증명을 지원하도록 프로그래밍되고, 이에 의해 상기 네트워크는 사용자 장비 하드웨어 및/또는 소프트웨어가 변경되었는지의 여부를 원격으로 결정하는, 사용자의 프라이버시를 보호하기 위한 시스템.

청구항 19

네트워크에서 플랫폼의 사용자의 프라이버시를 보호하기 위한 방법으로서,

공개 키 암호체계(20)에서 인증된 공개 키들을 분배하기 위한 시스템을 포함하는 사설 오버레이(10)를 제공하는 단계

를 포함하고, 상기 플랫폼(40)은 사용자 장비(30)에 포함되고,

상기 인증된 공개 키들을 분배하기 위한 시스템은 상기 네트워크 및 상기 네트워크의 각각의 허가된 사용자에게 상기 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 20

제19항에 있어서,

상기 사용자 장비는 셀룰러 또는 이동 전화기, 컴퓨터 또는 고객 데이터 수집 시스템인, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 21

제20항에 있어서,

상기 고객 데이터 수집 시스템은 유틸리티 미터인, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 22

제19항에 있어서,

상기 인증된 공개 키들을 분배하기 위한 시스템은 공개 키 기반구조 및 인증 기관(PKI)인, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 23

제19항에 있어서,

상기 플랫폼은 셀룰러 플랫폼이고 상기 네트워크는 셀룰러 네트워크이고,

상기 플랫폼은 무선 플랫폼이고 상기 네트워크는 무선 네트워크이거나, 또는

상기 플랫폼은 유틸리티 플랫폼 또는 제3자 데이터 수신 및 관리 플랫폼이고, 상기 네트워크는 고객 데이터 수집 유닛과 통신하는 통신 네트워크인, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 24

제19항에 있어서,

개인 암호해독 키가 로컬로 생성되고 저장되는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 25

제19항에 있어서,

상기 플랫폼은 셀룰러 플랫폼이고,

상기 네트워크는 셀룰러 네트워크이고,

상기 셀룰러 네트워크가 상기 사용자 장비를 난수와 연관시키고, 이에 의해 사용자 신원으로부터 상기 사용자 장비를 분리시키는 단계를 더 포함하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 26

제19항에 있어서,

상기 플랫폼은 무선 플랫폼이고,

상기 네트워크는 무선 네트워크이고,

상기 방법은 상기 무선 네트워크가 상기 사용자 장비를 난수와 연관시키고, 이에 의해 사용자 신원으로부터 상기 사용자 장비를 분리시키는 단계를 더 포함하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 27

제19항에 있어서,

상기 플랫폼은 유틸리티 또는 제3자 데이터 수신 및 관리 플랫폼이고,

상기 네트워크는 통신 네트워크이고,

상기 통신 네트워크는 상기 사용자 장비를 난수와 연관시키고, 이에 의해 사용자 신원으로부터 상기 사용자 장비를 분리시키는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 28

제19항에 있어서,

상기 사설 오버레이는 암호 칩을 포함하고, 상기 플랫폼은 상기 암호 칩을 포함하고, 상기 암호 칩은 암호 보안 볼트에 인증 메시지를 보관하도록 프로그래밍되는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 29

제19항에 있어서,

상기 암호 칩은 신뢰된 플랫폼 모듈(TPM)인, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 30

제19항에 있어서,

상기 플랫폼은 셀룰러이고, 상기 암호 칩은 상기 사용자 장비가 셀룰러 모드에 있는 동안 호출 시간(minute)들을 계속 추적하도록 프로그래밍되는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 31

제30항에 있어서,

상기 호출 시간들은 선불되는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 32

제19항에 있어서,

상기 플랫폼은 무선이고, 상기 암호 칩은 상기 사용자 장비가 무선 모드에 있는 동안 무선 사용 시간들을 계속

추적하도록 프로그래밍되는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 33

제32항에 있어서,

상기 무선 사용 시간들은 선불되는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 34

제19항에 있어서,

상기 암호 칩은 원격 증명을 지원하도록 프로그래밍되고, 상기 방법은 상기 네트워크가 상기 사용자 장비가 허가되는지의 여부를 원격으로 결정하는 단계를 포함하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 35

제19항에 있어서,

상기 암호 칩은 원격 증명을 지원하도록 프로그래밍되고, 상기 방법은 상기 네트워크가 상기 사용자 장비가 복제되었는지의 여부를 원격으로 결정하는 단계를 포함하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 36

제19항에 있어서,

상기 암호 칩은 원격 증명을 지원하도록 프로그래밍되고, 상기 방법은 상기 네트워크가 사용자 장비 하드웨어 및/또는 소프트웨어가 변경되었는지의 여부를 원격으로 결정하는 단계를 포함하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 37

제19항에 있어서,

개인 모드에서 상기 플랫폼을 동작시키는 단계

를 포함하고, 상기 네트워크는 상기 플랫폼이 상기 개인 모드에서 동작하는 경우 상기 플랫폼에 대한 위치 데이터를 특정 사용자와 연관시킬 수 없는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 38

제37항에 있어서,

상기 개인 모드에서 상기 플랫폼을 동작시키는 단계는:

개인 등록을 수행하는 단계

를 포함하고, 개인 등록은:

상기 네트워크가 상기 네트워크의 각각의 허가된 사용자에 동일한 인증 메시지를 주기적으로 전송하는 단계; 및

상기 네트워크가 사용자의 공개 암호 키를 사용하여 각각의 허가된 사용자에게 전송되는 상기 인증 메시지를 암호화하는 단계를 포함하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 39

제38항에 있어서,

상기 네트워크가 동일한 인증 메시지를 주기적으로 전송하는 단계는 매일 수행되는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 40

제37항에 있어서,

상기 개인 모드에서 상기 플랫폼을 동작시키는 단계는:

상기 플랫폼이 상기 네트워크에 프라이버시 인에이블 등록(Pravacy Enabling Registration; PER) 메시지를 송신하는 단계; 및

상기 플랫폼이 상기 네트워크의 공개 암호 키를 사용하여 상기 PER을 암호화하는 단계

를 포함하고, 상기 PER은 상기 인증 메시지 및 랜덤 장비 태그(RET)를 포함하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 41

제40항에 있어서,

상기 PER 내의 인증 메시지는:

상기 PER이 유효 사용자에 의해 송신되었던 네트워크를 보여주는 제로-지식 증명으로서 작용하고, 그리고

상기 사용자를 식별하지 않는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 42

제40항에 있어서,

상기 RET는 난수인, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 43

제40항에 있어서,

상기 RET를 상기 네트워크의 홈 위치 레지스터(HLR) 및 방문자 위치 레지스터(Visitor Location Register; VLR)에 입력하는 단계; 및

상기 RET를 전화 번호, 계정 식별자, 또는 사용자 ID 데이터 전송으로서 다루고, 이에 의해 상기 VLR 및 상기 HLR은 상기 플랫폼에 대한 셀룰러 전화 또는 데이터 호출, 무선 데이터 접속 또는 데이터 전송을 설정 및 유지하기 위해 요구되는 정보를 수집하지만, 상기 정보를 특정 사용자, 전화 번호, 계정 식별자 또는 사용자 ID와 연관시키지 않는 단계

를 포함하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 44

제43항에 있어서,

상기 셀룰러 전화 또는 데이터 호출, 상기 무선 데이터 접속 또는 데이터 전송은 인입(incoming) 또는 아웃고잉(outgoing)인, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 45

제43항에 있어서,

상기 RET를 임시 IP 어드레스와 연관시키는 단계를 포함하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 46

제44항에 있어서,

상기 셀룰러 전화 호출은 인입 호출이고, 상기 방법은:

상기 사용자가 셀룰러 전화 호출을 수신하려는 당사자들에게 상기 셀룰러 네트워크의 서비스 제공자의 신원 및 상기 사용자의 RET를 분배하는 단계

를 포함하고, 상기 분배하는 단계는 공개 키 암호화를 사용하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 47

제46항에 있어서,

상기 사용자는 상기 분배하는 단계를 수행하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 48

제46항에 있어서,

상기 인증된 공개 키들을 분배하기 위한 시스템은 상기 분배하는 단계를 수행하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 49

제19항에 있어서,

상기 셀룰러 플랫폼에 암호 칩을 구축하는 단계

를 포함하고, 상기 암호 칩은 암호 보안 볼트에 상기 인증 메시지를 보관하도록 프로그래밍되는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 50

제49항에 있어서,

상기 암호 칩은 신뢰된 플랫폼 모듈(TPM)인, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 51

제49항에 있어서,

상기 암호 칩은 상기 장비가 셀룰러 모드에 있는 동안 셀룰러 전화 호출 시간들을 계속 추적하도록 프로그래밍되는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 52

제51항에 있어서,

상기 호출 시간들은 선불되는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 53

제49항에 있어서,

상기 암호 칩은 원격 증명을 지원하도록 프로그래밍되고, 상기 방법은 상기 네트워크가 상기 장비가 허가되는지의 여부를 원격으로 결정하는 단계를 포함하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 54

제49항에 있어서,

상기 암호 칩은 원격 증명을 지원하도록 프로그래밍되고, 상기 방법은 상기 네트워크가 상기 장비가 복제되었는지의 여부를 원격으로 결정하는 단계를 포함하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 55

제49항에 있어서,

상기 TPM은 원격 증명을 지원하도록 프로그래밍되고, 상기 방법은 상기 네트워크가 장비 하드웨어 및/또는 소프트웨어가 변경되었는지의 여부를 원격으로 결정하는 단계를 포함하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 56

사용자 장비가 허가되는지의 여부를 결정하기 위한 방법으로서,

상기 사용자는 네트워크에서 플랫폼의 사용자이고, 상기 방법은 사설 오버레이를 제공하는 단계를 포함하고, 상기 사설 오버레이는 공개 키 암호체계에서 인증된 공개 키들을 분배하기 위한 시스템을 포함하고;

상기 플랫폼은 사용자 장비 내에 포함되고, 그리고

상기 인증된 공개 키들을 분배하기 위한 시스템은 상기 네트워크 및 상기 네트워크의 각각의 허가된 사용자에게 상기 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 57

사용자 장비가 복제되는지의 여부를 결정하기 위한 방법으로서,

상기 사용자는 네트워크에서 플랫폼의 사용자이고, 상기 방법은 사설 오버레이를 제공하는 단계를 포함하고, 상기 사설 오버레이는 공개 키 암호체계에서 인증된 공개 키들을 분배하기 위한 시스템을 포함하고,

상기 플랫폼은 사용자 장비에 포함되고, 그리고

상기 인증된 공개 키들을 분배하기 위한 시스템은 상기 네트워크 및 상기 네트워크의 각각의 허가된 사용자에게 상기 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 58

사용자 장비 하드웨어 또는 소프트웨어가 변경되거나 또는 조작되었는지의 여부를 결정하기 위한 방법으로서, 상기 사용자는 네트워크에서 플랫폼의 사용자이고, 상기 방법은 사설 오버레이를 제공하는 단계를 포함하고, 상기 사설 오버레이는 공개 키 암호체계 내의 인증된 공개 키들을 분배하기 위한 시스템을 포함하고;

상기 플랫폼은 사용자 장비 내에 포함되고, 그리고

상기 인증된 공개 키들을 분배하기 위한 시스템은 상기 네트워크 및 상기 네트워크의 각각의 허가된 사용자에게 상기 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 59

사용자에 요금청구하기 위한 방법으로서,

상기 사용자는 네트워크에서 플랫폼의 사용자이고, 상기 방법은 사설 오버레이를 제공하는 단계를 포함하고, 상기 사설 오버레이는 공개 키 암호체계에서 인증된 공개 키들을 분배하기 위한 시스템을 포함하고;

상기 플랫폼은 사용자 장비에 포함되고,

상기 인증된 공개 키들을 분배하기 위한 시스템은 상기 네트워크 및 상기 네트워크의 각각의 허가된 사용자에게 상기 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공하는, 사용자의 프라이버시를 보호하기 위한 방법.

청구항 60

제56항 내지 제59항 중 어느 한 항에 있어서,

상기 플랫폼은 셀룰러 플랫폼이고 상기 네트워크는 셀룰러 네트워크이고,

상기 플랫폼은 무선 플랫폼이고 상기 네트워크는 무선 네트워크이고, 또는

상기 플랫폼은 유틸리티 플랫폼 또는 제3자 데이터 수신 및 관리 플랫폼이고, 상기 네트워크는 고객 데이터 수집 유닛과 통신하는 통신 네트워크인, 사용자의 프라이버시를 보호하기 위한 방법.

명 세 서

기 술 분 야

[0001] 관련 출원들에 대한 교차-참조

[0002] 이 출원은, 그 전체가 여기에 참조로 포함되는, 2010년 4월 13일에 출원된 Private Overlay for Cellular Networks라는 명칭의 공동 계류중인 미국 가특허 출원 일련 제61/323,713호에 대한 우선권 및 이익을 청구한다.

[0003] 연방 후원 연구 또는 개발에 관한 언급

[0004] 개시된 발명은 미국 국가 과학 재단으로부터의 수여 번호 제 0424422호 하에서의 정부 지원으로 만들어졌다. 정부는 본 발명에 권한을 갖는다.

[0005] 기술 분야

[0006] 본 발명은 정보 네트워크에서 플랫폼의 사용자의 프라이버시를 보호하기 위한 시스템들 및 방법들에 관한 것이다. 본 발명은 또한 셀룰러, 무선 또는 제3자 데이터 수신 및 관리 시스템들의 사용자에 대한 사설(또는 프라이버시) 오버레이들에 관한 것이다.

배 경 기 술

[0007] 공개 키 암호방식

[0008] 공개 키 암호방식은 2개의 다른 키들을 허용하는데, 하나는 암호화를 위한 것이고 다른 하나는 암호해독을 위한 것이다. 암호 키를 사용하여 암호화된 플레인텍스트의 임의의 부분은 오직 누군가 암호해독 키를 가지는 경우에만 암호해독될 수 있다. 적절하게 설계된 경우, 매우 어려운 수학 문제를 풀지 않고 하나의 키로부터 다른 키를 획득하는 것은 가능하지 않다. 따라서, 아마도, 암호화 키를 온라인으로 게시함으로써 암호화 키를 공개할 수 있으며, 따라서, 누구라도 메시지를 암호화하여, 비밀 암호해독 키를 가지지 않은 사람에 의해 메시지가 판독가능할 것이라는 우려 없이 의도된 사용자에게 메시지를 송신할 수 있다. 메시지는 암호해독 키가 비밀로 유지되는 한 안전하게 유지될 것이다. Diffie 및 Hellman은 1976년 공개 키 암호방식을 소개하였다. 다음 중요한 단계가 1970년대 후반 Rivest, Shamir, 및 Adleman에 의해, 이들의 RSA 암호체계의 발명을 통해 취해졌다(두문자어는 각각의 발명자의 성들의 첫번째 문자를 포함한다). RSA 암호체계는 당해 기술분야에 공지된 알고리즘을 이용하여 공개 키 암호방식을 구현한다(구현은 지수화 모듈로 큰 수에 주로 의존한다). RSA 암호체계의 보안성은 A x B 형태의 매우 큰 수들을 계승화하는 어려움에 기초하는 것으로 추정되며, 여기서 A 및 B는 큰 소수들이다. 확정적으로 증명되지는 않았지만, 일반적으로, 대응하는 암호화 키로부터 적절하게 선택된 RSA 암호해독 키를 획득하는(또는 그 역인) 유일한 방식이 2개의 큰 소수들의 곱을 계승화하는 것이라고 여겨진다. 이는 매우 어려운 것으로 공지된 적절하게 이해된 문제이다. RSA 키들은 대칭 시스템 키들보다 훨씬 크지만 크게 실행불가능하지는 않다. 3072-비트 RSA 키들은 일반적으로 대칭 키 시스템 내의 128-비트 키들과 동일한 보안 레벨을 제공하는 것으로 당해 기술에서 여겨진다(예를 들어, http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf를 참조하라). 2개의 다른 키들을 갖는 것의 또다른 중요한 양상은 시스템이 보안 통신을 제공하는 것 뿐만 아니라 보안 디지털 서명들을 생성하기 위해 사용될 수 있다는 점이다.

[0009] 공개 키 암호방식은 신뢰된 통신에서 작용하는 강력한 규칙을 갖는다. 그러나, 한 부분은 여전히 빠져있다: 우리는 예를 들어, 온라인 판매자에게 예를 들어 우리의 신용 카드 정보를 송신하기 위해 공개 키를 사용할 때, 그것이 진짜 해당 온라인 판매자가 키를 제공한 것임을 확인하기를 원한다.

[0010] 당해 기술분야에 공지된 이러한 문제에 대한 해법은 공개 키 인증서의 형태를 취하는 것이다. 공개 키 인증서는 여권이 개인에 관한 정보(이름, 생년월일, 출생지 등)를 여권 사진에 바인딩하는 것과 거의 동일한 방식으로 공개 키를 개인 또는 회사 신원에 바인딩한다.

[0011] 현재, 전자상거래 판매자들이 등록 기관에 가서 자신의 회사 신원들을 증명하기 위한 충분한 문서들을 제시한다. 자신의 신원들이 검증되면, 연관된 인증 기관은 공개 키를 생성하여 이를 인증서에 배치하여, 그것을 키와 연관된 엔티티에 관한 정보에 바인딩한다. 인증 기관은 인증서가 인증된 엔티티의 고객들에 의해 검증될 수 있도록 인증서에 디지털로 서명할 것이다. 등록 및 인증 기관들 및 다른 관련 기능성들이 종종 공개 키 기반구조(PKI)라 명명되는 단일 엔티티의 헤드 아래에 발견된다. VeriSign과 같은 몇몇 큰 회사들은 인터넷 상거래를 위한 우세한 PKI들로서 부상하였다. 이들은 자신의 신뢰성, $250,000의 현금 담보를 포함한 다양한 수단(http://www.verisign.com/ssl/buy-ssl-certificates/index.html?tid=a_box를 참조하라), 및 회사로서의 자신들의 가치가 자신들이 그들에게 주어진 신뢰를 오용하는 경우 순식간에 사라질 것이라는 사실을 통해 신뢰를 구축한다. 많은 웹 브라우저들이 공지된 PKI들로부터의 인증서들을 자동으로 수용하도록 구성되어, 따라서, 인

간 사용자가 이러한 것들에 대해 걱정할 필요 없게 한다.

[0012] 예를 들어, 구매자가 온라인 북셀러의 웹사이트로 가서 책의 몇몇 제본들을 구매하기를 원한다고 가정한다. 구매자는 먼저 자신의 브라우저의 최상단의 URL 라인에 북셀러의 URL을 입력하여 북셀러의 홈페이지로 갈 것이다. 구매자는 이후 책의 제본들을 가상 쇼핑 카트에 넣고 계산을 진행할 것이다. 이때, 암호 동작이 대부분의 사용자들이 모르는 사이에 시작한다. 판매자는 공개 암호 키를 포함하는 인증서를 구매자의 브라우저에 송신할 것이다. 구매자가 원하는 경우, 그는 실제로 일부 브라우저들에서 안전한 브라우징을 표시하는 디스플레이된 잠금 아이콘을 클릭함으로써 인증서를 볼 수 있다. 이들 인증서들은, 서명 기관, 공개 암호 키, 및 의도된 암호화 알고리즘을 포함한 많은 정보를 포함한다. 이 예에 대해, 인증서는, 인증 서비스, 예를 들어, VeriSign에 의해 서명되고, 특정 길이의 키, 소위 2040 비트를 가지는 RSA 암호화를 요청한다. 인증서를 검증한 경우, 구매자의 브라우저는 대칭 키 암호체계에 대한 128 또는 256-비트 키를 생성할 것이다. 이 키는 인증서 상에 제공되는 RSA 공개 암호 키를 사용하여 암호화될 것이며, 결과적인 암호문이 온라인 판매자에게 송신될 것이다. 판매자 및 구매자는 이제 비밀 대칭 키를 공유하고, 이들은 이제 보안적으로 대화할 수 있다. 전자상거래의 성공은 공개 키 암호방식의 보안성 및 신뢰된 제3자들, 예를 들어, VeriSign과 같은 인증 서비스들을 통해 생성된 신뢰에 달려 있다.

[0013] 정보 네트워크들에서의 프라이버시의 보호

[0014] 그 시작에서부터, 지상 텔레포니는 감시 텔레포니였다. 감시에 대한 가능성들은, 등록 메시지가 위치 정보의 일정한 스트림을 제공하므로, 셀룰러 텔레포니와 함께 증가하였다. 가장 최근에는, 감시의 영향은 비-텔레포니 계산 및 비디오 기능성이 셀룰러 플랫폼으로 집중됨에 따라, 그리고 무선 플랫폼들 및 무선 네트워크들의 사용이 확장됨에 따라 점점 더 중요해지고 있다.

[0015] 사용자가 자신의 개인 정보의 책임을 지게 하는, 셀룰러 및 무선 네트워크들과 같은 정보 네트워크들에서 프라이버시를 보호하기 위한 시스템에 대한 당해 기술분야의 요구가 존재한다.

[0016] 섹션 2에서, 또는 이 출원의 임의의 다른 섹션에서의 임의의 참조의 인용 또는 식별은, 이러한 참조가 본 발명에 대한 종래 기술로서 사용가능하다는 허용으로 간주되지 않을 것이다.

발명의 내용

[0017] 발명의 요약

[0018] 네트워크에서 플랫폼의 사용자의 프라이버시를 보호하기 위한 시스템이 제공되며, 시스템은:

[0019] 공개 키 암호체계(20)에서 인증된 공개 키들을 분배하기 위한 시스템을 포함하는 사설 오버레이(10)

[0020] 를 포함하고, 플랫폼(40)은 사용자 장비(30)에 포함되고,

[0021] 인증된 공개 키들을 분배하기 위한 시스템은 네트워크(50) 및 네트워크의 각각의 허가된 사용자에게 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공한다.

[0022] 시스템의 일 실시예에서, 사용자 장비는 셀룰러 또는 이동 전화기, 컴퓨터 또는 고객 데이터 수집 시스템, 유틸리티 미터, 또는 유선 단말이다.

[0023] 시스템의 또다른 실시예에서, 고객 데이터 수집 시스템은 유틸리티 미터이다.

[0024] 시스템의 또다른 실시예에서, 인증된 공개 키들을 분배하기 위한 시스템은 공개 키 기반구조 및 인증 기관(PKI)이다.

[0025] 시스템의 또다른 실시예에서, 플랫폼은 셀룰러 플랫폼이고 네트워크는 셀룰러 네트워크이고, 플랫폼은 무선 플랫폼이고 네트워크는 무선 네트워크이고, 또는 플랫폼은 유틸리티 플랫폼 또는 제3자 데이터 수신 및 관리 플랫폼이고, 네트워크는 고객 데이터 수집 유닛과 통신하는 통신 네트워크이다.

[0026] 시스템의 또다른 실시예에서, 고객 데이터 수집 유닛은 전기 미터, 가스 미터 또는 유틸리티 미터이다.

[0027] 시스템의 또다른 실시예에서, 개인 암호해독 키가 로컬로 생성되고 저장된다.

[0028] 시스템의 또다른 실시예에서, 플랫폼은 셀룰러 플랫폼이고, 네트워크는 셀룰러 네트워크이고, 셀룰러 네트워크는 사용자 장비를 난수와 연관시키고, 이에 의해 사용자 신원으로부터 사용자 장비를 분리시킨다.

[0029] 시스템의 또다른 실시예에서, 플랫폼은 무선 플랫폼이고, 네트워크는 무선 네트워크이고, 무선 네트워크는 사용자 장비를 사용자 계정 식별자가 아닌 난수와 연관시키고, 이에 의해 사용자 신원으로부터 사용자 장비를 분리시킨다.

[0030] 시스템의 또다른 실시예에서, 플랫폼은 유틸리티 또는 제3자 데이터 수신 및 관리 플랫폼이고, 네트워크는 통신 네트워크이고, 통신 네트워크는 사용자 장비를 난수와 연관시키고, 이에 의해 사용자 신원으로부터 사용자 장비를 분리시킨다.

[0031] 또다른 실시예에서, 시스템은 암호 칩(60)을 포함하고, 플랫폼은 암호 칩을 포함하고, 암호 칩은 암호 보안 볼트(vault)에 인증 메시지를 보관하도록 프로그래밍된다.

[0032] 시스템의 또다른 실시예에서, 암호 칩은 신뢰된 플랫폼 모듈(TPM)이다.

[0033] 시스템의 또다른 실시예에서, 플랫폼은 셀룰러이고, 암호 칩은 사용자 장비가 셀룰러 모드에 있는 동안 호출 시간(minute)들을 계속 추적하도록 프로그래밍된다.

[0034] 시스템의 또다른 실시예에서, 호출 시간들은 선불된다.

[0035] 시스템의 또다른 실시예에서, 플랫폼은 무선이고, 암호 칩은 사용자 장비가 무선 모드에 있는 동안 무선 사용 시간들을 계속 추적하도록 프로그래밍된다.

[0036] 시스템의 또다른 실시예에서, 무선 사용 시간들은 선불된다.

[0037] 시스템의 또다른 실시예에서, 암호 칩은 원격 입증(attestation)을 지원하도록 프로그래밍되어, 이에 의해 네트워크가 사용자 장비가 허가되는지의 여부를 원격으로 결정한다.

[0038] 시스템의 또다른 실시예에서, 암호 칩은 원격 입증을 지원하도록 프로그래밍되어, 이에 의해 네트워크는 사용자 장비가 복제되었는지의 여부를 원격으로 결정한다.

[0039] 시스템의 또다른 실시예에서, 암호 칩은 원격 입증을 지원하도록 프로그래밍되고, 이에 의해 네트워크는 사용자 장비 하드웨어 및/또는 소프트웨어가 변경되었는지의 여부를 원격으로 결정한다.

[0040] 또한 네트워크에서 플랫폼의 사용자의 프라이버시를 보호하기 위한 방법이 제공되며, 방법은

[0041] 공개 키 암호체계(20)에서 인증된 공개 키들을 분배하기 위한 시스템을 포함하는 사설 오버레이(10)를 제공하는 단계

[0042] 를 포함하고, 플랫폼(40)은 사용자 장비(30)에 포함되고,

[0043] 인증된 공개 키들을 분배하기 위한 시스템은 네트워크 및 네트워크의 각각의 허가된 사용자에게 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공한다.

[0044] 방법의 일 실시예에서, 사용자 장비는 셀룰러 또는 이동 전화기, 컴퓨터 또는 고객 데이터 수집 시스템이다.

[0045] 방법의 또다른 실시예에서, 고객 데이터 수집 시스템은 유틸리티 미터이다.

[0046] 방법의 또다른 실시예에서, 인증된 공개 키들을 분배하기 위한 시스템은 공개 키 기반구조 및 인증 기관(PKI)이다.

[0047] 방법의 또다른 실시예에서, 플랫폼은 셀룰러 플랫폼이고 네트워크는 셀룰러 네트워크이고, 플랫폼은 무선 플랫폼이고 네트워크는 무선 네트워크이고, 또는 플랫폼은 유틸리티 플랫폼 또는 제3자 데이터 수신 및 관리 플랫폼이고, 네트워크는 고객 데이터 수집 유닛과 통신하는 통신 네트워크이다.

[0048] 방법의 또다른 실시예에서, 고객 데이터 수집 유닛은 전기 미터, 가스 미터 또는 유틸리티 미터이다.

[0049] 방법의 또다른 실시예에서, 개인 암호해독 키가 로컬로 생성되고 저장된다.

[0050] 방법의 또다른 실시예에서, 플랫폼은 셀룰러 플랫폼이고, 네트워크는 셀룰러 네트워크이고, 방법은 무선 네트워크가 셀룰러 네트워크가 사용자 장비를 난수와 연관시키고, 이에 의해 사용자 신원으로부터 사용자 장비를 분리시키는 단계를 더 포함한다.

[0051] 방법의 또다른 실시예에서, 플랫폼은 무선 플랫폼이고, 네트워크는 무선 네트워크이고, 방법은 사용자 장비를 난수와 연관시키고, 이에 의해 사용자 신원으로부터 사용자 장비를 분리시키는 단계를 더 포함한다.

[0052] 방법의 또다른 실시예에서, 플랫폼은 유틸리티 또는 제3자 데이터 수신 및 관리 플랫폼이고, 네트워크는 통신 네트워크이고, 통신 네트워크는 사용자 장비를 난수와 연관시키고, 이에 의해 사용자 신원으로부터 사용자 장비를 분리시킨다.

[0053] 방법의 또다른 실시예에서, 사설 오버레이는 암호 칩을 포함하고, 플랫폼은 암호 칩을 포함하고, 암호 칩은 암호 보안 볼트에 인증 메시지를 보관하도록 프로그래밍된다.

[0054] 방법의 또다른 실시예에서, 암호 칩은 신뢰된 플랫폼 모듈(TPM)이다.

[0055] 방법의 또다른 실시예에서, 플랫폼은 셀룰러이고, 암호 칩은 사용자 장비가 셀룰러 모드에 있는 동안 호출 시간(minute)들을 계속 추적하도록 프로그래밍된다.

[0056] 방법의 또다른 실시예에서, 호출 시간들은 선불된다.

[0057] 방법의 또다른 실시예에서, 플랫폼은 무선이고, 암호 칩은 사용자 장비가 무선 모드에 있는 동안 무선 사용 시간들을 계속 추적하도록 프로그래밍된다.

[0058] 방법의 또다른 실시예에서, 무선 사용 시간들은 선불된다.

[0059] 방법의 또다른 실시예에서, 암호 칩은 원격 입증을 지원하도록 프로그래밍되고, 방법은 네트워크가 사용자 장비가 허가되는지의 여부를 원격으로 결정하는 단계를 포함한다.

[0060] 방법의 또다른 실시예에서, 암호 칩은 원격 입증을 지원하도록 프로그래밍되고, 방법은 네트워크가 사용자 장비가 복제되었는지의 여부를 원격으로 결정하는 단계를 포함한다.

[0061] 방법의 또다른 실시예에서, 암호 칩은 원격 입증을 지원하도록 프로그래밍되고, 방법은 네트워크가 사용자 장비 하드웨어 및/또는 소프트웨어가 변경되었는지의 여부를 원격으로 결정하는 단계를 포함한다.

[0062] 또다른 실시예에서, 방법은 개인 모드에서 플랫폼을 동작시키는 단계를 포함하고, 네트워크는 플랫폼이 개인 모드에서 동작하는 경우 플랫폼에 대한 위치 데이터를 특정 사용자와 연관시킬 수 없다.

[0063] 방법의 또다른 실시예에서, 개인 모드에서 플랫폼을 동작시키는 단계는:

[0064] 개인 등록을 수행하는 단계

[0065] 를 포함하고, 개인 등록은:

[0066] 네트워크가 네트워크의 각각의 허가된 사용자에 동일한 인증 메시지를 주기적으로 전송하는 단계; 및

[0067] 네트워크가 사용자의 공개 암호 키를 사용하여 각각의 허가된 사용자에게 전송되는 인증 메시지를 암호화하는 단계를 포함한다.

[0068] 방법의 또다른 실시예에서, 네트워크가 동일한 인증 메시지를 주기적으로 전송하는 단계는 매일 수행된다.

[0069] 방법의 또다른 실시예에서, 개인 모드에서 플랫폼을 동작시키는 단계는:

[0070] 플랫폼이 네트워크에 프라이버시 인에이블 등록(PER) 메시지를 송신하는 단계; 및

[0071] 플랫폼이 네트워크의 공개 암호 키를 사용하여 PER을 암호화하는 단계

[0072] 를 포함하고, PER은 인증 메시지 및 랜덤 장비 태그(RET)를 포함한다.

[0073] 방법의 또다른 실시예에서, PER 내의 인증 메시지는 PER이 유효 사용자에 의해 송신되었던 네트워크를 보여주는 제로-지식 증명으로서 작용하고, 그리고 사용자를 식별하지 않는다.

[0074] 방법의 또다른 실시예에서, RET는 난수이다.

[0075] 또다른 실시예에서, 방법은 RET를 네트워크의 홈 위치 레지스터(HLR) 및 방문자 위치 레지스터(VLR)에 입력하는 단계; 및 RET를 전화 번호, 계정 식별자, 또는 사용자 ID 데이터 전송으로서 다루고, 이에 의해 VLR 및 HLR은 플랫폼에 대한 셀룰러 전화 또는 데이터 호출, 무선 데이터 접속 또는 데이터 전송을 설정 및 유지하기 위해 요구되는 정보를 수집하지만, 정보를 특정 사용자, 전화 번호, 계정 식별자 또는 사용자 ID와 연관시키지 않는 단계를 포함한다.

[0076] 방법의 또다른 실시예에서, 셀룰러 전화 또는 데이터 호출, 무선 데이터 접속 또는 데이터 전송은 인입

(incoming) 또는 아웃고잉(outgoing)이다.

[0077] 또다른 실시예에서, 방법은 RET를 임시 IP 어드레스와 연관시키는 단계를 포함한다.

[0078] 방법의 또다른 실시예에서, 셀룰러 전화 호출은 인입 호출이고, 방법은 사용자가 셀룰러 전화 호출을 수신하려는 당사자들에게 셀룰러 네트워크의 서비스 제공자의 신원(예를 들어, 네트워크 ID) 및 사용자의 RET를 분배하는 단계를 포함하고, 분배 단계는 공개 키 암호화를 사용한다.

[0079] 방법의 또다른 실시예에서, 사용자는 분배 단계를 수행한다.

[0080] 방법의 또다른 실시예에서, 인증된 공개 키들을 분배하기 위한 시스템은 분배 단계를 수행한다.

[0081] 또다른 실시예에서, 방법은 셀룰러 플랫폼에 암호 칩을 구축하는 단계를 포함하고, 암호 칩은 암호 보안 볼트에 인증 메시지를 보관하도록 프로그래밍된다.

[0082] 방법의 또다른 실시예에서, 암호 칩은 신뢰된 플랫폼 모듈(TPM)이다.

[0083] 방법의 또다른 실시예에서, 암호 칩은 장비가 셀룰러 모드에 있는 동안 셀룰러 전화 호출 시간들을 계속 추적하도록 프로그래밍된다.

[0084] 방법의 또다른 실시예에서, 호출 시간들은 선불된다.

[0085] 방법의 또다른 실시예에서, 암호 칩은 원격 입증을 지원하도록 프로그래밍되고, 방법은 네트워크가 장비가 허가되는지의 여부를 원격으로 결정하는 단계를 포함한다.

[0086] 방법의 또다른 실시예에서, 암호 칩은 원격 입증을 지원하도록 프로그래밍되고, 방법은 네트워크가 장비가 복제되었는지의 여부를 원격으로 결정하는 단계를 포함한다.

[0087] 방법의 또다른 실시예에서, TPM은 원격 입증을 지원하도록 프로그래밍되고, 방법은 네트워크가 장비 하드웨어 및/또는 소프트웨어가 변경되었는지의 여부를 원격으로 결정하는 단계를 포함한다.

[0088] 또한, 사용자 장비가 허가되는지의 여부를 결정하기 위한 방법이 제공되며, 사용자는 네트워크 내의 플랫폼의 사용자이다. 일 실시예에서, 방법은 사설 오버레이를 제공하는 단계를 포함하고, 사설 오버레이는 공개 키 암호체계에서 인증된 공개 키들을 분배하기 위한 시스템을 포함하고;

[0089] 플랫폼은 사용자 장비 내에 포함되고, 그리고

[0090] 인증된 공개 키들을 분배하기 위한 시스템은 네트워크 및 네트워크의 각각의 허가된 사용자에게 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공한다.

[0091] 또한, 사용자 장비가 복제되었는지의 여부를 결정하기 위한 방법이 제공되고, 사용자는 네트워크 내의 플랫폼의 사용자이다. 일 실시예에서, 방법은 사설 오버레이를 제공하는 단계를 포함하고, 사설 오버레이는 공개 키 암호체계에서 인증된 공개 키들을 분배하기 위한 시스템을 포함하고,

[0092] 플랫폼은 사용자 장비에 포함되고, 그리고

[0093] 인증된 공개 키들을 분배하기 위한 시스템은 네트워크 및 네트워크의 각각의 허가된 사용자에게 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공한다.

[0094] 또한, 사용자 장비 하드웨어 또는 소프트웨어가 변경되거나 또는 조작되었는지의 여부를 결정하기 위한 방법이 제공되며, 사용자는 네트워크에서 플랫폼의 사용자이다. 일 실시예에서, 방법은 사설 오버레이를 제공하는 단계를 포함하고, 사설 오버레이는 공개 키 암호체계에서 인증된 공개 키들을 분배하기 위한 시스템을 포함하고;

[0095] 플랫폼은 사용자 장비 내에 포함되고, 그리고

[0096] 인증된 공개 키들을 분배하기 위한 시스템은 네트워크 및 네트워크의 각각의 허가된 사용자에게 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공한다.

[0097] 또한 사용자에 요금청구하기 위한 방법이 제공되며, 사용자는 네트워크 내의 플랫폼의 사용자이다. 일 실시예에서, 방법은 사설 오버레이를 제공하는 단계를 포함하고, 사설 오버레이는 공개 키 암호체계에서 인증된 공개 키들을 분배하기 위한 시스템을 포함하고;

[0098] 플랫폼은 사용자 장비에 포함되고,

[0099] 인증된 공개 키들을 분배하기 위한 시스템은 네트워크 및 네트워크의 각각의 허가된 사용자에게 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공한다.

[0100] 특정 실시예들에서, 플랫폼은 셀룰러 플랫폼이고 네트워크는 셀룰러 네트워크이고, 플랫폼은 무선 플랫폼이고 네트워크는 무선 네트워크이고, 또는 플랫폼은 유틸리티 플랫폼 또는 제3자 데이터 수신 및 관리 플랫폼이고, 네트워크는 고객 데이터 수집 유닛과 통신하는 통신 네트워크이다.

[0101] 본 발명은 첨부 도면들을 참조하여 여기에 기술되며, 여기서 유사한 참조 기호들은 몇몇 도면들에 걸쳐 유사한 엘리먼트들을 참조한다. 일부 경우들에서, 본 발명의 다양한 양상들이 본 발명의 이해를 용이하게 하기 위해 강조되거나 확대되어 도시될 수 있다는 점이 이해되어야 한다.

도면의 간단한 설명

[0102] 도 1a는 셀룰러 시스템에 대한 사설(또는 프라이버시) 오버레이(10)의 일 실시예의 개략도이다. 사설 오버레이(10)는 사용자에게 속박된 위치 및 사용 기록을 생성하지 않고 서비스들(예를 들어, 셀룰러 음성 및 데이터 서비스들)을 제공하기 위해 기존 통신, 정보 및 데이터 네트워크(예를 들어, 셀룰러 네트워크)(50)의 기반구조를 사용한다. 공개 키 암호체계(20)에서 인증된 공개 키들을 분배하기 위한 시스템에 대한 기반구조의 상세항목이 오른쪽 하단부에 있다. 이 실시예에서, 인증된 공개 키들을 분배하기 위한 시스템은 공개 키 기반구조 및 인증 기관(PKI)이다. TPM(Trusted Platform Module: 신뢰된 플랫폼 모듈) 또는 암호 칩(60). VLR(visitor location register: 방문자 위치 레지스터). HLR(홈 위치 레지스터). 사용자 랜덤 태그, @(*&RND(*zx.

도 2는 신뢰된 플랫폼 모듈(TPM) 다양한 서비스들 이후에 수정된 표; 신뢰된 컴퓨팅 그룹(TCG) 사양 아키텍쳐 개요, 개정 1.4, pg. 36. 상세항목에 대해 섹션 5.3을 참조하라.

도 3은 TPM 컴포넌트 아키텍쳐, TPM 메인 파트 1 이후에 수정된 다이어그램. 상세항목에 대해 섹션 5.3을 참조하라.

도 4는 셀룰러 또는 무선 시스템에 대한 사설 오버레이의 일 실시예의 개략도. 서비스 제공자는, 예를 들어, 셀룰러 또는 무선 서비스 제공자일 수 있다. TPM, 신뢰된 플랫폼 모듈 또는 암호 칩(60).

도 5는 수요 반응에 대한 잠재력의 평가. 연방 에너지 규제 위원회 이후 수정됨(2009년 6월). 수요 반응 잠재력의 국가 평가, 스태프 대표, http://www.ferc.gov/legal/staff-reports/06-09-demand-response.pdf. 상세항목들에 대해 섹션 6.3을 참조하라.

도 6은 시나리오 가정들에서의 키 차이들. 연방 에너지 규제 위원회 이후 수정됨(2009년 6월). 수요 반응 잠재력의 국가 평가, 스태프 대표. http://www.ferc.gov/legal/staff-reports/06-09-demand-response.pdf. 상세항목들에 대해 섹션 6.3을 참조하라.

도 7a-d는 행동-추출 알고리즘. (a) 전력 소모-데이터 수집, (b) 유도된 스위치 이벤트들, (c) 몇몇 식별된 로드 이벤트들, 및 (d) 기준 및 추정된 구간들 사이의 비교. M. Lisovich, D. Mulligan, 및 S. B. Wicker의 요구-응답 시스템들로부터의 개인 정보의 추론, IEEE 보안 프라이버시 매거진, vol. 8, no. 1, pp. 11-20, 2010년 1월/2월 이후 수정됨. 상세항목들에 대해 섹션 6.3을 참조하라.

도 8은 어드밴스드 계측 기반구조(AMI) 구축 블록들. 엔지니어링 전력 연구 위원회, 어드밴스드 계측 기반구조 이후 수정됨, http://www.ferc.gov/eventcalendar/Files/20070423091846-EPRI%20-%20Advanced%20Metering.pdf. 상세항목들에 대해 섹션 6.3을 참조하라.

도 9는 프라이버시-인지 수요 반응 아키텍쳐. 상세항목들에 대해 섹션 6.3을 참조하라.

발명을 실시하기 위한 구체적인 내용

[0103] 사용자가 자신의 개인 정보의 책임을 지게 하는 정보 네트워크들 또는 네트워킹 시스템들(예를 들어, 셀룰러 전화 네트워크, 무선 컴퓨터 네트워크, 유선 컴퓨터 네트워크, 통신 네트워크, 제3자 데이터 수신 및 관리 시스템 또는 유틸리티 분배 시스템)에 대한 사설 오버레이(10)가 제공된다. 사용자의 신원은 사용자 장비(30)가 페이징될 수 있는 셀을 지정하는 숫자 태그로부터 분리된다. 사설 오버레이(10)는 공개 키 기반구조 및 인증 기관(PKI) 및 다른 등록 및 인증 기관(20)의 추가에 의해 생성된다. 이러한 등록 및 인증 기관들은 당해 기술분야에 공지되어 있다. PKI(또는 다른 등록 및 인증 기관)(20)는 셀룰러 전화, 무선 컴퓨팅, 또는 유틸리티 분배 시스템 또는 네트워크 및 그것의 모든 가입자들에게 네트워크 및 사용자들에 대한 공개 암호 키들을 제공한다.

개인 암호해독 키들은 적절한 방식으로 로컬로 생성 및 저장된다. 개인 암호해독 키 생성 및 저장을 위한 이러한 방법들은 당해 기술분야에 공지되어 있다. 이러한 추가를 통해, 기존의 셀룰러, 무선, 제3자 데이터 수신 및 관리에 대한 사설 오버레이(10), 또는 유틸리티 분배 기반구조(50)는 셀룰러 또는 무선 네트워크에, 또는 유틸리티 또는 제3자 데이터 수신 및 관리 시스템에 등록된 디바이스에 대해 설정될 수 있다.

[0104] 제한으로서가 아니라 개시내용의 명료함을 위해, 본 발명의 상세한 설명은 하기에 설명되는 서브섹션들로 나누어진다.

[0105] 5.1. 사용자의 프라이버시를 보호하기 위한 시스템

[0106] 네트워크에서 플랫폼(40)의 사용자의 프라이버시를 보호하기 위한 시스템이 제공된다. 시스템은:

[0107] 공개 키 암호체계(20)에서 인증된 공개 키들을 분배하기 위한 시스템을 포함하는 사설 오버레이(10)

[0108] 를 포함하고, 플랫폼(40)은 사용자 장비(30)에 포함되고,

[0109] 인증된 공개 키들(20)을 분배하기 위한 시스템은 네트워크 및 네트워크의 각각의 허가된 사용자에게 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공한다.

[0110] 일 실시예에서, 사용자 장비(30)는 셀룰러 전화, 컴퓨터 또는 고객 데이터 수집 유닛이다. 당해 기술 분야에 공지된 임의의 고객 데이터 수집 유닛이 사용될 수 있다. 예를 들어, 일 실시예에서, 고객 데이터 수집 유닛은 유틸리티 미터, 예를 들어, 전기 미터, 가스 미터 또는 수도 미터와 같은 유틸리티 관리 및 분배를 위한 것이다.

[0111] 특정 실시예에서, 사설 오버레이(10)는 3G 및 4G 셀룰러 시스템에 대한 것일 수 있다.

[0112] 또다른 실시예에서, 플랫폼(40)은 셀룰러 플랫폼이고, 네트워크는 셀룰러 네트워크이다(도 1 및 4). 또다른 실시예에서, 플랫폼은 무선 플랫폼이고, 네트워크는 무선 네트워크이다(도 4). 또다른 실시예에서, 플랫폼은 고객 데이터 수집 플랫폼이고, 네트워크는 통신 네트워크(도 8)이다.

[0113] 또다른 실시예에서, 인증된 공개 키들(20)을 분배하기 위한 시스템은 공개 키 기반구조 및 인증 기관(PKI) 또는 당해 기술분야에 공지된 다른 등록 및 인증 기관이다.

[0114] 또다른 실시예에서, 개인 암호해독 키는 로컬로 생성 및 저장된다.

[0115] 또다른 실시예에서, 셀룰러 네트워크(50)는 사용자 장비(예를 들어, 셀룰러 또는 이동 전화기)를 전화 번호가 아닌 난수와 연관시키고, 이에 의해 사용자 장비를 사용자 신원으로부터 분리한다(도 1).

[0116] 또다른 실시예에서, 플랫폼(40)은 무선 플랫폼이고, 네트워크(50)는 무선 네트워크이고, 무선 네트워크는 사용자 장비(30)를 사용자 계정 식별자가 아닌 난수와 연관시키고, 이에 의해 사용자 장비를 사용자 신원으로부터 분리한다(도 4).

[0117] 또다른 실시예에서, 플랫폼(40)은 유틸리티 또는 제3자 데이터 수신 및 관리 플랫폼이고, 네트워크(50)는 통신 네트워크이고, 통신 네트워크는 사용자 장비(30)(예를 들어, 전기 미터, 가스 미터 또는 수도 미터)를 난수와 연관시키고, 이에 의해, 사용자 장비(30)를 사용자 신원으로부터 분리한다.

[0118] 또다른 실시예에서, 시스템은 암호 칩(60)을 포함하고, 암호 칩은 플랫폼(40) 내에 구축되고 암호 보안 볼트(vault)에 인증 메시지를 보관하도록 프로그래밍된다.

[0119] 또다른 실시예에서, 암호 칩(60)은 신뢰된 플랫폼 모듈(TPM)이다.

[0120] 또다른 실시예에서, 플랫폼(40)은 셀룰러이고, 암호 칩(60)은 사용자 장비가 셀룰러 모드인 동안 호출 시간들을 계속 추적하도록 프로그래밍된다.

[0121] 또다른 실시예에서, 셀룰러 전화 호출 시간들은 선불된다.

[0122] 또다른 실시예에서, 플랫폼(40)은 무선이고, 암호 칩(60)은 사용자 장비가 무선 모드에 있는 동안 무선 사용 시간들을 계속 추적하도록 프로그래밍된다.

[0123] 또다른 실시예에서, 무선 사용 시간들은 선불된다.

[0124] 또다른 실시예에서, 암호 칩(60)은 원격 입증(attestation)을 지원하도록 프로그래밍되고, 이에 의해 네트워크(50)는 사용자 장비(30)가 허가되는지의 여부를 원격으로 결정한다.

[0125] 또다른 실시예에서, 암호 칩은 원격 입증을 지원하도록 프로그래밍되고, 이에 의해 네트워크는 사용자 장비가 복제되었는지 또는 그렇지 않은 경우 조작되었는지의 여부를 원격으로 결정한다.

[0126] 또다른 실시예에서, 암호 칩은 원격 입증을 지원하도록 프로그래밍되고, 이에 의해, 네트워크는 사용자 장비 하드웨어 및/또는 소프트웨어가 변경되었는지의 여부를 원격으로 결정한다.

[0127] 여기서 제공되는 사설 오버레이는 예를 들어, 무선 네트워크 내의 무선 디바이스 또는 셀룰러 네트워크 내의 셀룰러 플랫폼(예를 들어, 셀룰러 전화)의 사용자의 프라이버시를 보호하기 위해 사용될 수 있다. 시스템은 공개 키 암호체계에서 인증된 공개 키들을 분배하기 위한 시스템을 포함할 수 있고, 여기서 공개 키 암호체계에서 인증된 공개 키들을 분배하기 위한 시스템은 네트워크 및 셀룰러 네트워크의 허가된 사용자들에게 네트워크 및 허가된 사용자들에 대한 공개 암호 키들을 제공한다. 개인 암호해독 키들은 당해 기술분야에 공지된 기법들을 통해 네트워크 및 허가된 사용자들에 의해 생성되고 안전하게 저장될 수 있다.

[0128] 도 1은 셀룰러(또는 무선) 네트워크와 같은 네트워크에서 플랫폼(40)의 사용자의 프라이버시를 보호하기 위한 시스템의 일 실시예에 대한 사설 오버레이(10)의 개략도를 도시한다. 사설 오버레이(10)는 공개 키 암호체계(20)에서 인증된 공개 키들을 분배하기 위한 시스템을 포함한다. 이러한 시스템들은 당해 기술분야에 공지되어 있다. 플랫폼(40)은 사용자 장비(30)(이 실시예에서 셀룰러 전화)에 포함되고, 인증된 공개 키들(20)을 분배하기 위한 시스템은 네트워크 및 네트워크의 각각의 허가된 사용자에게 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공한다.

[0129] 사설 오버레이는 사용자에게 속박된 위치 및 사용 기록을 생성하지 않고 셀룰러 음성 및 데이터 서비스들을 제공하기 위해 기존 셀룰러 기반구조를 사용한다. 도 1에 도시된 바와 같이, 동일한 인증 메시지("암호화됨: 사용자 공개 키")가 모든 허가된 사용자들에게 송신된다.

[0130] 도 1에 도시된 바와 같이, 사용자는 프라이버시 모드("암호화됨: 네트워크 공개 키")를 입력하기 위해 사용자 장비(30)로부터 인증 메시지(이는 모든 유효 사용자들에 대해 동일함) 및 랜덤 태그(@(*&RND(*zx로서 도 1에 도시됨)를 송신한다. 인증 메시지는 제로-지식 증명으로서 작용한다. 암호 칩, 이 실시예에서, 신뢰된 플랫폼 모듈(TPM)(60)은 오직 유효 사용자만이 인증 메시지를 알지만, 네트워크는 어느 사용자가 메시지를 송신했는지를 알지 못함을 보장한다. 랜덤 태그는 프라이버시-인에이블 사용자의 전화 번호로서 역할을 한다. 프라이버시-인에이블 전화들은 TPM을 포함할 수 있다. TPM은 필수 공개-키 암호 기능들을 수행할 수 있고, 호출 시간 제한들을 추적하고 강제할 수 있다. 복제는 원격 입증을 통해 방지될 수 있다.

[0131] 또한 도 1에 도시된 바와 같이, 랜덤 태그는 등록 및 호출 라우팅을 위한 사용자 ID 대신 기존의 셀룰러 기반구조에서 사용될 수 있다. 네트워크 기반구조(50)(이 실시예에서, 셀룰러 네트워크 기반구조)에 대한 어떠한 변경도 필요하지 않다. PKI 또는 인증 기관(20)은 개인 메시징(텍스트 및 호출 제어)을 지원한다. 사용자들은 공개 암호 키들을 생성하고, 이들을 인증 기관 또는 PKI(20)에 송신한다. 대응하는 암호해독 키들은 TPM과 같은 암호 칩(60)에 비밀로 유지된다. 이는 사용자들로 하여금 이들이 서로 호출할 수 있도록 랜덤 태그들을 안전하게 교환하게 하고, 보안 호출 그룹들을 허용한다.

[0132] 도 1에 상세하게 도시된 바와 같이, 다음은 인증 기관의 공개 키 기반구조에 의해 제공되는 공개 키들의 예이다.

[0133] 공개 키 기반구조

사용자	공개 키
PKI	)JKO#*$(*HFF(U
네트워크	KJHF(Y#$(*YFG_
개별 사용자	)#(*)HEF(*Y#$H(*

[0134] (“Steve Wicker”)

[0135] 여기서 제공되는 사설 오버레이의 일 실시예에서, 사용자의 신원은 사용자 장비(30)가 페이징될 수 있는 셀을 지시하는 숫자 태그로부터 분리된다. 사설 오버레이(10)는 공개 키 기반구조 및 인증 기관(PKI)(20)와 같은 인증 기관의 네트워크에 대한 추가만을 요구한다. PKI는 네트워크 및 모든 가입자들에게 공개 암호 키 및 개인 암호해독 키를 제공한다. 추가로, 기존의 셀룰러 기반구조에 대한 사설 오버레이는 다음과 같이 설정될 수 있

다. 누군가 셀룰러 네트워크에 등록한 셀룰러 전화를 가지고 시작할 수 있다. 개인 등록은 네트워크가 각각의 허가된 가입자에게 동일한 인증 메시지를 하루에 한번(또는 일부 적절한 간격으로) 전송하게 함으로써 인에이블된다. 모든 가입자들에 송신된 공통 인증 메시지는 각각의 가입자의 공개 암호 키를 사용하여 암호화된다.

[0136] 위의 실시예가 무선 네트워크 내의 임의의 무선 디바이스(도 4를 참조)와 함께, 또는 제3자 데이터 수신 및 관리 시스템의 통신 네트워크 내의(도 8을 참조) 또는 유틸리티 분배 시스템 내의 고객 데이터 수집 유닛(예를 들어, 유틸리티 미터)과 함께 사용되도록 용이하게 수정될 수 있다는 점이 당업자에게 명백할 것이다.

[0137] 5.2 네트워크 내의 플랫폼의 사용자의 프라이버시를 보호하기 위한 방법

[0138] 네트워크에서 플랫폼(40)의 사용자의 프라이버시를 보호하기 위한 방법이 또한 제공된다. 방법은 사설 오버레이(10)를 제공하는 단계를 포함하고, 사설 오버레이(10)는 공개 키 암호 시스템(20) 내의 인증된 공개 키들을 분배하기 위한 시스템을 포함하고, 플랫폼(40)은 사용자 장비(30) 내에 포함되고, 인증된 공개 키들(20)을 분배하기 위한 시스템은 네트워크(50) 및 네트워크의 각각의 허가된 사용자에게 네트워크 및 각각의 허가된 사용자에 대한 공개 암호 키를 제공한다.

[0139] 사용자 장비는 예를 들어, 셀룰러 전화, 컴퓨터 또는 고객 데이터 수집 유닛일 수 있다.

[0140] 방법의 또다른 실시예에서, 인증된 공개 키들을 분배하기 위한 시스템은 공개 키 기반구조 및 인증 기관(PKI)이다.

[0141] 방법의 또다른 실시예에서, 플랫폼은 셀룰러 플랫폼이고, 네트워크는 셀룰러 네트워크이다. 또다른 실시예에서, 플랫폼은 무선 플랫폼이고, 네트워크는 무선 네트워크이다. 또다른 실시예에서, 플랫폼은 고객 데이터 수집 플랫폼이고, 네트워크는 통신 네트워크이다.

[0142] 방법의 또다른 실시예에서, 개인 암호해독 키가 로컬로 생성 및 저장된다. 개인 암호해독 키들은 당해 기술분야에 공지된 기법들을 통해 네트워크 및 허가된 사용자들에 의해 보안적으로 생성 및 저장될 수 있다. 네트워크는 사용자 장비를 전화 번호가 아닌 난수와 연관시키고, 따라서, 사용자 장비와 사용자 신원을 분리한다.

[0143] 방법의 또다른 실시예에서, 플랫폼은 셀룰러 플랫폼이고, 네트워크는 셀룰러 네트워크이고, 방법은 셀룰러 네트워크가 사용자 장비를 전화 번호가 아닌 난수와 연관시키고 이에 의해 사용자 장비를 사용자 신원으로부터 분리하는 단계를 더 포함한다.

[0144] 방법의 또다른 실시예에서, 플랫폼은 무선 플랫폼이고, 네트워크는 무선 네트워크이고, 방법은 무선 네트워크가 사용자 장비를 개인과 연관된 계정이 아닌 난수와 연관시켜서, 이에 의해 사용자 장비를 사용자 신원으로부터 분리하는 단계를 더 포함한다.

[0145] 방법의 또다른 실시예에서, 플랫폼은 유틸리티 또는 제3자 데이터 수신 및 관리 플랫폼이고, 네트워크는 통신 네트워크이고, 통신 네트워크는 사용자 장비(예를 들어, 전기 미터, 가스 미터 또는 수도 미터)를 난수와 연관시키고, 이에 의해 사용자 장비를 사용자 신원으로부터 분리시킨다.

[0146] 방법의 또다른 실시예에서, 사설 오버레이는 암호 칩을 포함하고, 암호 칩은 셀룰러 플랫폼 내에 구축되고, 암호 보안 볼트 내에 인증 메시지를 보관하도록 프로그래밍된다.

[0147] 방법의 또다른 실시예에서, 암호 칩은 신뢰된 플랫폼 모듈(TPM)이다.

[0148] 방법의 또다른 실시예에서, 플랫폼은 셀룰러이고, 암호 칩은 사용자 장비가 셀룰러 모드에 있는 동안 호출 시간들을 계속 추적하도록 프로그래밍된다.

[0149] 방법의 또다른 실시예에서, 호출 시간들은 선불된다.

[0150] 방법의 또다른 실시예에서, 플랫폼은 무선이고, 암호 칩은 사용자 장비가 무선 모드에 있는 동안 무선 사용 시간들을 계속 추적하도록 프로그래밍된다.

[0151] 방법의 또다른 실시예에서, 무선 사용 시간들은 선불된다.

[0152] 방법의 또다른 실시예에서, 암호 칩은 원격 입증을 지원하도록 프로그래밍되고, 방법은 네트워크가 사용자 장비가 허가되는지의 여부를 원격으로 결정하는 단계를 포함한다.

[0153] 방법의 또다른 실시예에서, 암호 칩은 원격 입증을 지원하도록 프로그래밍되고, 방법은 네트워크가 사용자 장비가 복제되었는지의 여부를 원격으로 결정하는 단계를 포함한다.

[0154] 방법의 또다른 실시예에서, 암호 칩은 원격 입증을 지원하도록 프로그래밍되고, 방법은 네트워크가 사용자 장비 하드웨어 및/또는 소프트웨어가 변경되었는지의 여부를 원격으로 결정하는 단계를 포함한다.

[0155] 또다른 실시예에서, 방법은 개인 모드(예를 들어, 개인 셀룰러 또는 무선 모드)에서 플랫폼을 동작시키는 단계를 포함하고, 여기서, 네트워크는 플랫폼이 개인 모드에서 동작하는 경우, 플랫폼에 대한 위치 데이터를 특정 사용자와 연관시킬 수 없다.

[0156] 방법의 또다른 실시예에서, 개인 모드에서 플랫폼을 동작시키는 단계는 개인 등록을 수행하는 단계를 포함하고, 개인 등록은:

[0157] 네트워크가 네트워크의 각각의 허가된 사용자에게 동일한 인증 메시지를 주기적으로(예를 들어, 시간 단위 간격으로, 12시간 간격으로, 매일, 매주 등) 전송하는 단계; 및 네트워크가 사용자의 공개 암호 키를 사용하여 각각의 허가된 사용자에게 전송되는 인증 메시지를 암호화하는 단계를 포함한다.

[0158] 방법의 또다른 실시예에서, 네트워크가 동일한 인증 메시지를 주기적으로 전송하는 단계는 매일 수행된다.

[0159] 방법의 또다른 실시예에서, 개인 모드에서 플랫폼(예를 들어, 셀룰러 또는 무선 플랫폼)을 동작시키는 단계는:

[0160] 플랫폼이 네트워크에 개인 인에이블 등록(PER) 메시지를 송신하는 단계; 및

[0161] 플랫폼이 네트워크의 공개 암호 키를 사용하여 PER을 암호화하는 단계를 포함하고, PER은 인증 메시지 및 랜덤 장비 태그(RET)를 포함한다.

[0162] 방법의 또다른 실시예에서, PER에서의 인증 메시지는 PER이 유효 사용자에 의해 송신된 네트워크를 도시하는 제로-지식 증명으로서 작용하며, PER 내의 인증 메시지는 사용자를 식별하지 않는다.

[0163] 방법의 또다른 실시예에서, RET는 난수이다.

[0164] 또다른 실시예에서, 방법은:

[0165] RET를 네트워크의 방문자 위치 레지스터(VLR) 및 홈 위치 레지스터(HLR)에 입력하는 단계; 및

[0166] RET를 전화 번호 및 계정 식별자로서 다루는 단계를 포함하고, 이에 의해 VLR 및 HLR은 셀룰러 전화 또는 데이터 호출 또는 플랫폼에 대한 무선 데이터 접속을 설정 및 유지하기 위해 필요한 정보를 수집하지만, 정보를 특정 사용자, 전화 번호 또는 사용자 계정 식별자와 연관시키지 않는다.

[0167] 방법의 또다른 실시예에서, 셀룰러 전화 또는 데이터 호출 또는 무선 데이터 접속은 인입(incoming) 또는 아웃고잉(outgoing)이다.

[0168] 또다른 실시예에서, 방법은 RET를 임시 IP 어드레스와 연관시키는 단계를 포함한다.

[0169] 방법의 또다른 실시예에서, 셀룰러 전화 호출은 인입 호출이고, 방법은:

[0170] 사용자가 셀룰러 전화 호출을 수신하려는 당사자들에게 사용자의 RET 및 셀룰러 네트워크의 서비스 제공자의 신원(예를 들어, 네트워크 ID)을 분배하는 단계를 포함하고, 분배 단계는 공개 키 암호화를 사용한다.

[0171] 방법의 또다른 실시예에서, 사용자는 분배 단계를 수행한다.

[0172] 방법의 또다른 실시예에서, 인증 기관은 분배 단계를 수행한다.

[0173] 또다른 실시예에서, 방법은 셀룰러 플랫폼 내에 암호 칩(예를 들어, TPM)을 구축하는 단계를 포함하고, 암호 칩은 암호 보안 볼트에 인증 메시지를 보관하도록 프로그래밍된다.

[0174] 방법의 또다른 실시예에서, 암호 칩(예를 들어, TPM)은 장비가 셀룰러 모드에 있는 동안 셀룰러 전화 호출 시간들을 계속 추적하도록 프로그래밍된다.

[0175] 방법의 또다른 실시예에서, 호출 시간들은 선불된다. 암호 칩(예를 들어, TPM)은 허용된 수의 시간(minute)들이 만료된 경우 프라이버시 모드를 종료하도록 인에이블될 수 있다.

[0176] 방법의 또다른 실시예에서, 암호 칩(예를 들어, TPM)은 원격 입증을 지원하고, 방법은 네트워크가 장비가 허가되는지의 여부를 원격으로 결정하는 단계를 포함할 수 있다. 예를 들어, 네트워크는 암호 칩에 접촉하고, 암호 칩으로 하여금 장비가 유효한지의 여부(즉, 그것이 복제인지의 여부), 및 하드웨어 및/또는 소프트웨어가 조작되었는지의 여부를 결정하기 위해 프라이버시 소프트웨어 및 장비 ID에 대한 계산들을 수행하게 할 수 있다.

[0177] 방법의 또다른 실시예에서, 암호 칩은 원격 입증을 지원하도록 프로그래밍되고, 방법은 네트워크가 장비가 복제되었는지의 여부를 원격으로 결정하는 단계를 포함한다.

[0178] 방법의 또다른 양상에서, 암호 칩은 원격 입증을 지원하도록 프로그래밍되고, 방법은 네트워크가 장비 하드웨어 및/또는 소프트웨어가 변경되었는지의 여부를 원격으로 결정하는 단계를 포함한다.

[0179] 5.3 암호 칩 또는 신뢰된 플랫폼 모듈(TPM)

[0180] 셀룰러 또는 무선 디바이스의 복제를 방지하기 위해, 사용자 장비는 암호 보안 볼트에 인증 메시지를 보관하도록 프로그래밍되는 신뢰된 플랫폼 모듈(TPM)과 같은 암호 칩(60)이 구비될 수 있다. TPM 및 다른 적절한 암호 칩들이 당해 기술분야에 공지된다. 사용자가 개인 셀룰러(또는 무선) 모드에 입력하기를 원하는 경우, 사용자는 사용자 장비로 하여금 네트워크에 프라이버시 인에이블 등록(PER) 메시지를 송신하게 할 수 있다. PER은 인증 메시지 및 랜덤 장비 태그(RET)를 포함하고, 네트워크의 공개 암호 키를 사용하여 암호화된다. PER 내의 인증 메시지는, PER이 유효 사용자에 의해 송신되었음을 네트워크에 보여주지만, 실제로 사용자를 식별하지는 않는, 제로-지식 증명으로서 작용한다. RET는 홈 위치 레지스터(HLR) 및 방문자 위치 레지스터(VLR)에 입력될 것이며, 마치 그것이 전화 번호 또는 사용자 계정 식별자(개인 계정)인 것처럼 다루어지는 난수이다. 이러한 HLR/VLR 레코드는 개인 셀룰러 또는 무선 상황으로서 참조될 것이다. 이는 표준 HLR 또는 VLR 레코드에서 발견되지만 특정 개인 또는 그의 전화 번호 또는 개인 계정과 연관되지 않을 모든 정보를 포함할 것이다. 사용자 장비가 개인 셀룰러 또는 무선 모드에서 유지되는 한, 후속적인 등록 메시지들은 사용자의 전화 번호 또는 개인 계정이 아닌 RET를 포함할 것이다.

[0181] 셀룰러 전화 호출 설정, 이동도 관리, 및 로밍은, HLR 및 VLR 위치 정보가 전화 번호가 아닌 RET와 연관된다는 차이점을 가지고, 모두 이전처럼 정확하게 핸들링될 것이다. 데이터 호출들은 RET를 임시 IP 어드레스와 연관시킴으로써 개인적인 것으로 유지될 수 있다.

[0182] 사용자에 대한 프라이머리 동작 차이점은 인입 호출(셀룰러 플랫폼의 경우) 또는 인입 데이터 접속들(무선 플랫폼의 경우)에 있다. 인입 호출이 개인 셀룰러 모드에서 사용자 장비에 대해 완료될 수 있는 유일한 방식은 호출 당사자가 호출된 당사자의 RET 및 네트워크 ID를 알고 있는 경우이다. (후자는 호출 설정 요청들이 적절한 HLR에 대한 것일 수 있도록 요구된다). 따라서, 개인 셀룰러 모드에서의 사용자는 사용자가 호출을 수신하려고 하는 해당 당사자들에게 자신의 RET를 공개 키 암호화를 사용하여 분배해야 한다. 이러한 분배는 또한 인증 기관을 통해 핸들링될 수 있다. 명백하게, 해결될 과금 및 CALEA(Communications Assistance for Law Enforcement Act) 이슈들이 존재한다. 서비스 제공자는 각각의 PER에 대해 허용된 호출 시간들의 수를 제한하기를 원할 수 있다. 또한, 사용자 장비가 개인 셀룰러 모드에 있는 경우, 매일 또는 매달 제한들을 강제하기 위해 사용자 장비에서 TPM에 의존하는 것이 가능할 것이다. CALEA 우려들은 개인 셀룰러 시간들에 대한 사용자 선불을 가지고, 따라서 전화가 선불 셀룰러 폰인 것처럼 동작하게 함으로써 부분적으로 완화될 수 있다.

[0183] 신뢰 플랫폼 모듈(TPM)은 Trusted Computing Group™ (TCG)에 의해 표준들의 세트로서 개발되었다. 이들 표준들은 당해 기술분야에 공지되어 있다(예를 들어, 2007년 8월 2일 TCG 규격 아키텍쳐 개요, 규격, 개정 1.4; 2007년 7월 9일 TPM 메인: 파트 1 설계 원리들, 규격 버전 1.2, 레벨 2 개정 103, 2005년 12월 1일, Trusted Computing Group Design, Implementation, and Usage Principles, Version 2.01, Authorship: TCG Best Practices Committee을 참조하라; 이들 모두는 www.trustedcomputinggroup.org에서 또는 Trusted Computing Group™, Beaverton, OR로부터 다운로드가능한 PDF들로서 사용가능함)

[0184] TPM은 암호 키들의 보안 생성 및 사용을 포함한, 광범위한 기능들을 수행한다. 이들 키들은 원격 입증, 바인딩, 서명 및 봉인을 포함하는, 몇몇 표준화된 목적들을 위해 사용된다.

[0185] 원격 입증은 종종 위조 불가능한 해시 알고리즘을 통해, 컴퓨팅 디바이스의 하드웨어 및 소프트웨어 상태를 증명하기 위한 메커니즘이다.

[0186] TCG 규격 아키텍쳐 개요, 개정 1.4(www.trustedcomputinggroup.org 에서 또는 Trusted Computing Group™, Beaverton, OR로부터 다운로드 가능한 PDF로서 사용가능)에 따라, "입증은 정보의 정확성에 대한 보장의 프로세스이다. 외부 엔티티들은 차폐된 위치들, 보호된 능력들, 및 신뢰 루트를 증명할 수 있다. 플랫폼은 플랫폼의 무결성(신뢰성)에 영향을 주는 플랫폼 특성들에 대한 자신의 기재를 증명할 수 있다. 모든 형태들의 증명은 증명 엔티티의 신뢰가능한 증거를 요구한다. 증명은 몇몇 디멘젼들, TPM에 의한 증명, 플랫폼에 대한 증명, 플랫폼의 증명 및 플랫폼의 인증에 따라 이해될 수 있다". (TCG 규격 아키텍쳐 개요, 개정 1.4, pg. 5)

[0187] TPM 자체에 대한 입증은 플랫폼 구성 레지스터(PCR)들의 세트의 유지를 통해 수행된다. TPM 기능성의 "스냅샷들"이 측정 및 저장된다. 이들 특정들의 해싱된 버전들은 "다이제스트"들로서 참조된다. PCR은 측정 다이제스트들을 포함한다.

[0188] TCG 규격 아키텍쳐 개요, 개정 1.4에 따라, "측정 커넬은 측정 이벤트들을 생성한다. 측정 이벤트는 데이터의 2개 클래스들로 구성된다; 1) 측정된 값들 - 임베디드 데이터 또는 프로그램 코드의 표현 및 2) 측정 다이제스트들 - 해당 값들의 해시. 데이터는 메시지 다이제스트를 생성하는 측정 커넬에 의해 스캐닝된다. 다이제스트들은 기계 동작 상태의 스냅샷이다. 2개의 데이터 엘리먼트들(측정된 값들 및 측정 다이제스트)은 별개로 저장된다. 측정 다이제스트는 RTR 및 RTS 기능성을 사용하여 TPM에 저장된다. 측정된 값들은 측정 커넬의 자유재량으로 가상으로 어느 곳에나 저장될 수 있다. 실제로, 이것은 전혀 저장되지 않을 수 있지만, 직렬화된 표현이 요구될 때마다 재계산될 수 있다... TPM은 측정 다이제스트들을 포함하는 플랫폼 구성 레지스터(PCR)들로 명명되는 레지스터들의 세트를 포함한다. 대수적으로, PCR에 대한 업데이트들은 다음과 같다: PCR[n] ← SHA-1(PCR[n] + 측정된 데이터). PCR 값들은 일시적이며 시스템 재부팅시에 리셋된다. 측정 이벤트들의 검증은 측정 다이제스트의 재생성을 요구한다".(TCG 규격 아키텍쳐 개요, 개정 1.4, pg. 8)

[0189] 바인딩은 공개 키를 사용하는 메시지의 암호화이다. 공개 키 암호방식은 보안 키 전송에 대한 필요 없이 정보 보안을 용이하게 하기 위해 하나는 공개이고 하나는 개인인 한 쌍의 키들을 사용한다. TPM이 "이동 불가능한" 키로서 개인 키를 저장한다는 점에 유의한다 - 개인 키는 또다른 디바이스에 전달될 수 없다. TPM은 조작되거나 액세스될 수 없는 보안 위치들을 유지함으로써 이러한 키들의 보안성을 보장한다.

[0190] TCG 규격 아키텍쳐 개요, 개정 1.4에 따라, "TCG는 보호된 메시지 교환의 4개 클래스들; 바인딩, 서명, 봉인된-바인딩(봉인이라고도 알려짐) 및 봉인된 서명을 정의한다... 바인딩은 공개 키를 사용하여 메시지를 암호화하는 통상적인 동작이다. 즉, 송신자는 메시지를 암호화하기 위해 의도된 수신측의 공개 키를 사용한다. 메시지는 오직 수신측의 개인 키를 사용하는 암호해독에 의해서만 복원가능하다. 개인 키가 이동 불가능한 키로서 TPM에 의해 관리되는 경우, 오직 키를 생성한 TPM 만이 그것을 사용할 수 있다. 따라서, 공개 키를 이용하여 암호화된 메시지는 TPM의 특정 경우에 "바인딩되었다". 다수의 TPM 디바이스들 사이에서 전달가능한 이동가능한 개인 키들을 생성하는 것이 가능하다. 따라서, 바인딩은 암호화 이상의 어떠한 특수한 중요성도 가지지 않는다".(TCG 규격 아키텍쳐 개요, 개정 1.4, pg. 15)

[0191] 서명은 디지털 서명의 생성이다. 위에서 논의된 바와 같이, 디지털 서명들은 종종 비-거절을 강제하기 위해 사용된다; 다른 사람들이 메시지를 판독하는 것을 방지하는 것이 아니라 메시지에 서명한 당사자가 그들이 자신들이라고 말한 사람들임을 보장하는 것에 대해 더욱 초점을 둔다.

[0192] TCG 규격 아키텍쳐 개요, 개정 1.4에 따라 "종래의 관점에서의 서명은 또한 메시지의 무결성을 서명을 생성하기 위해 사용되는 키와 연관시킨다. TPM은 일부 관리되는 키들을 오직 키들만을 서명하는 것으로서 태그처리하는데, 이는 이들 키들이 오직 서명된 데이터의 해시를 계산하고 해시를 암호화하기 위해 사용됨을 의미한다. 따라서, 이들은 암호화 키들로서 잘못 해석될 수 없다".(TCG 규격 아키텍쳐 개요, 개정 1.4, pg. 15)

[0193] 봉인은 수신측 사용자가 필요한 개인 키를 가지는 것 뿐만 아니라, 암호해독 하드웨어가 특정 상태에 있어야 함을 요구한다. 이러한 상태는 플랫폼 구성 레지스터(PCR)들의 사용을 통해 입증된다.

[0194] TCG 규격 아키텍쳐 개요, 개정 1.4에 따라, "봉인은 바인딩을 한 단계 더 취한다. 봉인된 메시지들은 메시지 송신자에 의해 특정된 플랫폼 메트릭들의 세트에 바인딩된다. 플랫폼 메트릭들은 암호해독이 허가되기 전에 존재해야 하는 플랫폼 구성 상태를 특정한다. 봉인은 암호화된 메시지(실제로 메시지를 암호화하기 위해 사용되는 대칭 키)를 PCR 레지스터 값들의 세트 및 이동 불가능한 비대칭 키와 연관시킨다. 봉인된 메시지는 PCR 레지스터 값들의 범위를 선택하고 메시지들을 암호화하기 위해 사용되는 대칭 키 더하기 PCR 값들을 비대칭으로 암호화함으로써 생성된다. 비대칭 암호해독 키를 가지는 TPM은 플랫폼 구성이 송신자에 의해 특정된 PCR 레지스터 값들을 매칭시키는 경우 오직 대칭 키를 암호해독할 수 있다. 봉인은 TPM의 강력한 특징이다. 이것은 보호된 메시지들이 오직 플랫폼이 매우 특정적인 공지된 구성에서 기능하는 경우에만 복원가능하다는 보장을 제공한다".(TCG 규격 아키텍쳐 개요, 개정 1.4, pg. 15 - 16)

[0195] 서명이 또한 봉인될 수 있는데, 즉, PCR 레지스터들의 상태에 속박될 수 있다. TCG 규격 아키텍쳐 개요, 개정 1.4에 따라, "봉인된 서명... 서명 동작은 또한 메시지를 서명한 플랫폼이 특정 구성 요건을 만족시킨다는 보장을 증가시키는 방식으로서 PCR 레지스터들에 링크될 수 있다. 검증자는 서명이 PCR 레지스터들의 특정 세트를 포함해야 함을 지시한다. 서명자는, 서명 동작 동안, 특정된 PCR 레지스터들에 대한 값들을 수집하고, 이들

을 메시지에, 그리고 서명된 메시지 다이제스트의 계산의 일부분으로서 포함시킨다. 검증자는 이후 서명이 생성되었을 때 서명 플랫폼의 구성을 조사하는 것과 등가인 서명된 메시지에 공급되는 PCR 값들을 조사할 수 있다". (TCG 규격 아키텍처 개요, 개정 1.4, pg. 15)

[0196] TPM은 다수의 다른 서비스들을 제공한다. 표준화된 TPM 커맨드들은 TCG 규격 아키텍처 오버뷰의 섹션 4.6.3에 요약된다. 도 2에 예시된 인용은 Sign, GetRandom, 및 StirRandom 커맨드들이 키들의 생성과 같은 일반적인 암호 목적들에 사용가능해짐을 주지한다.

[0197] TPM GetRandom 커맨드는, TPM 메인 파트 3 커맨드들, 규격 버전으로부터의 인용에 후속하여 보여지는 바와 같이, 난수 생성기로부터 요구되는 바이트 수를 리턴시킨다:

[0198] "13.6 TPM_GetRandom

[0199] 정보 코멘트의 시작:

[0200] GetRandom은 난수 생성기로부터 호출자에게로 다음 bytesRequested 바이트들을 리턴시킨다.

[0201] TPM이, 사용가능한 바이트 수보다 더 적은 bytesRequested의 빈도수가 덜 자주 발생하도록 이것이 RNG 바이트들을 리턴하게 하는 방식으로 RNG를 구현하는 것이 추천된다.

[0202] ...

[0203] 동작들

[0204] 1. TPM은 bytesRequested양이 TPM으로부터 사용가능한지의 여부를 결정한다.

[0205] 2. randomBytesSize를 RNG로부터 사용가능한 바이트 수로 설정한다. 이 수는 randomBytesSize보다 더 적을 수 있다.

[0206] 3. randomBytes를 RNG로부터 다음 randomBytesSize로 설정한다"

[0207] (TPM 메인 파트 3 커맨드들, 규격 버전 1.2, pg. 91)

[0208] StirRandom 커맨드는 난수 생성기의 상태를 업데이트함으로써 난수 생성기의 상태에 엔트로피를 추가한다:

[0209] "13.7 TPM_StirRandom

[0210] 정보 코맨트의 시작:

[0211] StirRandom는 RNG 상태에 엔트로피를 추가한다.

[0212] ...

[0213] 동작들

[0214] TPM은 적절한 믹싱 함수를 사용하여 현재 RNG의 상태를 업데이트한다".(TPM 메인 파트 3 커맨드들. 규격 버전 1.2, pg. 92)

[0215] 설계 원리들에 초점을 두는 표준의 일부분이 "TPM 메인: 파트 1 설계 원리들, 규격 버전 1.2, 레벨 2, 개정 103, 2007년 7월 9일, www.trustedcomputinggroup.org에서, 또는 Trusted Computing Group™, Beaverton OR로부터 다운로드가능한 PDF로서 사용가능하며 여기서 "TPM 메인 파트 1"로서 참조됨"로부터 획득될 수 있다. 하기에 기술되는 바와 같이, TPM 메인 파트 1은 결과적인 TPM이 표준에 순응해야 할 경우 따라야 하는 설계자에 대한 구현 요건들을 배치한다:

[0216] "TPM 설계자는 TPM 메인 규격(파트 1-4) 내의 정보를 검토 및 구현하고 의도된 플랫폼에 대한 플랫폼 특정 문서를 검토해야 한다. 플랫폼 특정 문서는 TPM의 설계 및 구현예에 영향을 주는 규범적 선언들을 포함할 것이다".(TPM 메인 파트 1, pg. 1)

[0217] TPM의 기본 엘리먼트들이 도 3에 도시된다. 위의 다이어그램의 왼쪽 상단 부분에 도시된 암호 공동프로세서는 하기에 기술되는 바와 같이, 아키텍처의 다른 엘리먼트들과 함께 다양한 암호 기능들을 구현하도록 설계된다.

[0218] TPM 메인 파트 1은 다음을 언급한다 "암호 공동-프로세서, 도 2: C1이 TPM 내에서 암호 동작들을 수행한다. TPM은 종래의 방식들로 종래의 암호 동작들을 사용한다. 해당 동작들은 다음을 포함한다:

[0219] 비동기 키 생성(RSA)

[0220] 비동기 암호화/암호해독(RSA)

[0221] 해싱(SHA-1)

[0222] 난수 생성(RNG)

[0223] TPM은 랜덤 데이터의 생성, 비대칭 키들의 생성, 저장된 데이터의 서명 및 비밀을 수행하기 위해 이들 능력들을 사용한다.

[0224] TPM은 내부 TPM에 대해 대칭 암호화를 사용할 수 있지만, TPM의 일반적인 사용자들에게 어떠한 대칭 알고리즘 함수들도 노출하지 않는다.

[0225] TPM은 추가적인 비대칭 알고리즘을 구현할 수 있다. 상이한 알고리즘들을 구현하는 TPM 디바이스들은 상이한 알고리즘들이 서명 및 랩핑(wrap)을 수행하게 할 수 있다.

[0226] (TPM 메인 파트 1, pg. 12)

[0227] 위에 논의된 바와 같이, 암호화 알고리즘은 대칭 및 비대칭 (공개 키) 모두일 수 있다. 이들 알고리즘에 대한 키들은 또한 대칭 또는 비대칭으로서 참조될 수 있다. 하기에 논의되는 바와 같이, TPM은 노출된 대칭 키 암호 방식을 제공하도록 설계되지 않는다. 그것은 또다른 디바이스에 의해 사용하기 위한 이들 키들의 생성, 저장 및 보호에 제한된다. 대칭 키들의 생성은 난수 생성기(RNG)를 사용하여 수행될 수 있다. 바인딩 및 봉인은 일단 생성되면 이들 키들의 전달을 위해 사용될 수 있다.

[0228] TPM 메인 파트 1은 "TPM이 노출된 대칭 알고리즘을 가지지 않음에 따라, TPM은 오직 대칭 키들의 생성기, 저장 디바이스 및 보호기이다. 대칭 키의 생성은 TPM RNG를 사용할 것이다. 저장 및 보호는 TPM의 바인드 및 봉인 능력들에 의해 제공될 것이다. 호출자가 대칭 키의 릴리즈가 호출자로의 전달에 대한 언바인드/봉인 해제 이후에도 노출되지 않음을 보장하기를 원하는 경우, 호출자는 비밀성 세트를 가지는 전송 세션을 사용해야 한다... 비대칭 알고리즘에 대해, TPM은 RSA 키들을 생성하여 이에 대해 동작한다. 키들은 오직 TPM에 의해 또는 TPM의 호출자와 함께 유지될 수 있다. 키의 개인 부분이 TPM의 외부에서 사용중인 경우, 키의 보호들을 보장하는 것은 해당 키의 호출자 및 사용자의 책임이다"라고 언급한다. (TPM 메인 파트 1, pg. 13)

[0229] 후속하는 예들은 제한으로서가 아닌 예시로써 공급된다.

[0230] 6. 예들

[0231] 6.1 예 1: 사설 셀룰러 오버레이

[0232] 이 예는 사용자 신원으로부터 장비 신원을 엄격하게 분리함으로써 사용자 프라이버시를 보호하는 셀룰러 시스템들에 대한 사설 오버레이를 보여준다.

[0233] 도입: 공개 키 암호방식

[0234] 공개 키 암호방식은 2개의 다른 키들을 허용하는데, 하나는 암호화를 위한 것이고, 다른 하나는 암호해독을 위한 것이다. 암호 키를 사용하여 암호화되는 플레인 텍스트의 임의의 부분은 누군가 암호해독 키를 가지는 경우에만 오직 암호해독될 수 있다. 적절하게 설계되는 경우, 매우 어려운 수학 문제를 풀지 않고 하나의 키를 다른 하나로부터 획득하는 것이 가능하지 않다. 따라서, 누군가 암호 키를, 아마도, 이를 온라인에 게시함으로써 공개적인 것으로 만들 수 있고, 따라서, 임의의 누군가는 메시지를 암호화하고, 메시지가 비밀 암호해독 키를 가지지 않는 누군가에 의해 판독가능하다는 우려 없이 이를 의도된 사용자에게 송신할 수 있다. 메시지는 암호해독 키가 비밀로 유지되는 한 안전하게 유지될 것이다. Diffie 및 Hellman은 1976년 공개 키 암호방식을 도입하였다. 다음 중요한 단계는 1970년대 후반, Rivest, Shamir, 및 Adleman에 의해, RSA 암호체계의 발명을 사용하여 취해졌다(두문자어는 발명자의 성들 각각의 첫문자를 포함한다). RSA 암호체계가 당해 기술분야에 공지된 알고리즘을 이용하여 공개 키 암호방식을 구현한다(구현예는 주로 지수 모듈로 큰 수에 의존한다). RSA 암호체계의 보안성은 A x B 형태의 매우 큰 수들을 계승하는 어려움에 기초하며, 여기서, A 및 B는 큰 소수들이다. 이는 확정적으로 증명되지는 않았지만, 일반적으로, 대응하는 암호 키로부터 적절하게 선택된 RSA 암호해독 키를 획득하는 유일한 방식은 2개의 큰 소수들의 곱을 계승화하는 것이라고 여겨진다. 이는 매우 어려운 것으로 공지된 적절하게 이해된 문제이다. RSA 키들은 대칭 시스템 키들보다 훨씬 더 크지만 크게 실행불가능하지는 않다. 3072-비트 RSA 키들은 일반적으로 대칭 키 시스템 내의 128-비트 키들과 동일한 보안 레벨을 제공

하는 것으로 당해 기술에서 여겨진다(예를 들어, http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf를 참조하라). 2개의 다른 키들의 또다른 중요한 양상은 시스템이 보안 통신을 제공하는 것 뿐만 아니라 보안 디지털 서명들을 생성하기 위해 사용될 수 있다는 점이다.

[0235] 예를 들어, 구매자가 단일 책 제목의 수백 권의 제본들을 주문하는 편지를 온라인 북셀러에게 쓴다고 가정한다. 편지를 수신할 시에, 판매자는 편지를 송신한 사람이 실제 해당 개인 구매자였음을 검증하기를 원할 수 있다. 추가로, 구매자가 대응하는 암호 키를 비밀로 유지하는 동안 RSA 암호해독 키를 발행했다고 가정한다. 편지의 플레인텍스트 카피와 함께, 구매자는 암호화된 카피를 판매자에게 송신할 수 있는데, 이는 구매자의 비밀 암호 키를 사용하여 암호화된 것이다. 판매자가 구매자의 공개 암호해독 키를 적용하는 경우, 판매자는 플레인텍스트를 복원하여, 그것이 판매자의 편지와 동일한 것임을 알게 될 것이다. 판매자는 이후 구매자가 실제로 편지를 송신했음을 확신할 것인데, 왜냐하면, 오직 판매자만이 암호화된 카피를 생성하기 위해 요구되는 암호 키를 소유하기 때문이다. 이러한 보증은 하기에 논의되는 바와 같이 공식화될 수 있다. 이 예에서의 암호문은 누구라도 판독할 수 있지만 오직 구매자만이 생성할 수 있는 디지털 서명이다. 많은 방식들에 있어서, 디지털 서명은 실제로 구식의 다양한 서명보다 더 안전한데, 왜냐하면 디지털 서명은 상이한 문서에 전달될 수 없기 때문이다 - 이는 항상 생성시 암호화되었던 텍스트와 연관된다.

[0236] 추가 단계를 취하자면, 개인들의 그룹이 키들의 2개 세트들을 생성하며, 제1 세트는 컨텐츠를 암호화하기 위한 것이고, 제2 세트는 디지털 서명들을 생성하기 위한 것이라고 가정한다. 그룹은, 각각의 키 쌍의 다른 절반을 비밀로 유지하는 동안, 제1 세트로부터 암호 키를, 그리고 제2 세트로부터 암호해독 키를 발행한다. 그룹의 한 멤버인 Alice는 서명된 비밀 메시지를 Bob이라는 이름을 가진 그룹의 또다른 멤버에게 송신하기를 원한다고 가정한다. Alice는 먼저 메시지를 자신의 비밀 암호 키를 이용하여 암호화함으로써 메시지를 서명으로 변환할 것이다. 그녀는 이후 Bob의 공개 암호 키를 사용하여 서명을 암호화할 것이다. 따라서 원래 메시지는 이제, 처음에는 Alice의 비밀 암호키를 이용하여, 그후에는 Bob의 공개 암호 키를 이용하여, 2번 암호화되었다. Bob이 암호문을 수신하는 경우, 그는 서명을 복원하기 위해 먼저 자신의 비밀 암호해독 키를 적용해야 한다. 그는 이후, 원래 메시지를 복원하는 동시에 편지가 실제로 Alice로부터 온 것임을 동시에 스스로 확인하기 위해 Alice의 공개 암호해독 키를 적용할 것이다.

[0237] 따라서, 공개 키 암호방식은 신뢰된 통신에서 강력한 역할을 수행한다. 그러나, 한 부분은 여전히 빠져있는데, 위의 Alice와 Bob 사이의 통신에서, Alice는 Bob의 공개 암호 키가 실제로 Bob에 의해 생성되었다고 가정한다. 그러나, 만약 Eve(엿듣는 자)가 Bob인 척하면서 키를 발행하였다면 어떻게 되는가? 만약 그녀가 이를 수행할 수 있는 경우, Bob에 대해 의도된 임의의 비밀 메시지가 Eve에 의해 판독가능하게 될 것이다. 이를 방지하기 위해, 공개 키들은 인증되어야 한다. 다시 말해, Bob의 서명된 비밀 메시지의 수신측은 Bob의 키가 실제로 Bob에 의해 생성되었으며, 오직 Bob만이 대응하는 개인 키를 가질 것임을 확신해야 한다. 또는 이를 더욱 현대적인 면으로 보면, 우리는 예를 들어, 온라인 판매자에게 우리의 신용 카드 정보를 송신하기 위해 공개 키를 사용하는 경우, 이것이 실제로 해당 온라인 판매자가 제공한 키임을 확인하기를 원한다.

[0238] 이러한 문제에 대한 현재 당해 기술분야에 공지된 해법은 공개 키 인증서의 형태를 취한다. 공개 키 인증서는, 여권이 개인에 대한 정보(이름, 생년월일, 출생지 등)를 여권 사진에 바인딩하는 것과 거의 동일한 방식으로 공개 키를 개인의 신원에 바인딩한다. 여권은 신뢰된 제3자인 연방 정부에 의해 발행된 공식 문서이다.

[0239] 연방 정부는 사용자가 그가 자신이라고 말한 사람임을 보장하기 위해 요청측 사용자가 충분한 문서를 제공할 때까지 여권을 발행하지 않을 것이다. 연방 여권 에이전시가 모든 필요한 서류 및 몇 장의 사진들 모두를 수신하면, 에이전시는 문서들을 검증하고 여권을 발행할 것이다. 공항 및 출입국 관리 당국은 아마 이러한 프로세스에 친숙하다. 이들이 여권을 보고 포함된 사진을 소지자의 얼굴과 비교하는 경우, 이들은 이후 문서에 대한 데이터를 소지자와 연관시키려 한다. 공개 키 인증서들이 거의 동일한 방식으로 생성되어 사용된다.

[0240] 현재, 전자상거래 소매자들은 등록 기관으로 가서 자신의 회사 신원들을 증명하기 위해 충분한 문서를 제시한다. 이들의 신원들이 검증되면, 연관된 인증 기관은 공개 키를 생성하고, 이를 인증서 상에 배치하여, 이를 키와 연관된 엔티티에 대한 정보에 바인딩한다. 인증 기관은 인증서가 인증된 엔티티의 고객들에 의해 검증될 수 있도록 인증서를 디지털로 서명할 것이다. 등록 및 인증 기관들 및 다른 관련된 기능성은 종종 공개 키 기반구조(PKI)라 명명되는 단일 엔티티의 헤드 하에서 발견된다. 몇몇 큰 회사들, 예를 들어, VeriSign는 인터넷 상거래를 위해 우세한 PKI들로서 부상하였다. 이들은 이들의 신뢰도, $250,000의 현금 보증들을 포함하는 다양한 수단(http://www.verisign.com/ssl/buy-ssl-certificates/index.html?tid=a_box를 참조하라), 및 회사로서의 이들의 가치가 이들이 자신들에게 주어진 신뢰를 오용하는 경우 순식간에 사라질 것이라는 사실을 통

해 신뢰를 구축한다. 많은 웹 브라우저들은 알려진 PKI들로부터 인증서들을 자동으로 수용하고, 따라서, 휴먼 사용자가 이러한 것들에 대해 걱정할 필요가 없도록 구성된다.

[0241] 예를 들어, 구매자가 온라인으로 온라인 북셀러의 웹 사이트로 가서 책의 몇 권의 제본들을 구매하기를 원한다고 가정한다. 구매자는 자신의 브라우저의 최상단에 있는 URL 라인에 먼저 북셀러의 URL을 입력하여 북셀러의 홈페이지로 갈 것이다. 구매자는 이후 책의 제본들을 가상 쇼핑 카트에 넣고 계산을 진행할 것이다. 이때, 암호 동작이 대부분의 사용자들이 모르는 사이에 시작한다. 판매자는 공개 암호 키를 포함하는 인증서를 구매자의 브라우저에 송신할 것이다. 구매자가 원하는 경우, 그는 실제로 안전한 브라우징을 표시하는 디스플레이된 잠금 아이콘을 클릭함으로써 인증서를 볼 수 있다. 이들 인증서들은, 서명 기관, 공개 암호 키, 및 의도된 암호화 알고리즘을 포함한 많은 정보를 포함한다. 이 예에 대해, 인증서는, 인증 서비스, 예를 들어, VeriSign에 의해 서명되고, 2040 비트 키를 가지는 RSA 암호화를 요청한다. 인증서를 검증한 경우, 구매자의 브라우저는 대칭 키 암호체계에 대한 128 또는 256-비트 키를 생성할 것이다. 이 키는 인증서 상에 제공되는 RSA 공개 암호 키를 사용하여 암호화될 것이며, 결과적인 암호문이 온라인 판매자에게 송신될 것이다. 판매자 및 구매자는 이제 비밀 대칭 키를 공유하고, 이들은 이제 보안적으로 대화할 수 있다. 전자상거래가 공개 키 암호방식의 보안성 및 신뢰된 제3자들, 예를 들어, VeriSign과 같은 인증 서비스들을 통해 생성된 신뢰에 달려 있다는 점은 의심의 여지가 없다.

[0242] 일부 정부 기관들의 노력에도 불구하고, 상업 섹터는 시장의 확대를 즐기는 반면 대중은 더 큰 구매 기회들을 즐긴다. 후속하는 예는, 여기서 개시된 방법들을 사용하여, 공개 키 암호방식이 개인들의 프라이버시 이익들을 지원하기 위해 수정될 수 있다는 것을 보여준다.

[0243] 사설 셀룰러 오버레이

[0244] 셀룰러 개념이 장비의 일부분이 특정 셀 내에 위치되어야 함을 요구하는 한, MSC가 하나 또는 적은 개수의 셀 사이트들의 레벨에서 사용자 장비를 위치시킬 수 있다는 셀룰러 시스템들 내의 요건들이 존재할 것이다. 그러나, 그것은 위치될 필요가 있으며 특정 명칭의 가입자일 필요는 없는 장비라는 점에 주목하는 것이 중요하다. 사용자 신원으로부터 장비 신원을 엄격하게 분리시킴으로써 사용자 프라이버시를 보호하는 셀룰러 시스템에 대한 사설 오버레이가 여기(도 1 및 4)에 제공된다. 이 예에서 기술된 사설 셀룰러 오버레이의 실시예는 공개 키 암호 시스템 내의 인증된 공개 키들을 분배하기 위한 시스템을 사용한다. 당업자에 의해 이해될 바와 같이, 키들은 PKI-타입 프로세스를 사용하여 인증된다.

[0245] 공개 키 암호 시스템, 인증 기관, 또는 PKI(또는 그것의 기능적 등가물)에서 인증된 공개 키들을 분배하기 위한 시스템은 네트워크 및 모든 가입자들에게 공개 암호 키 및 개인 암호해독 키를 제공한다. 이러한 추가를 통해, 기존의 셀룰러 기반구조에 대한 사설 오버레이는 다음과 같이 설정될 수 있다.

[0246] 이러한 예는 셀룰러 전화가 개인 모드, 즉 네트워크가 전화에 대한 위치 데이터를 특정 사용자와 연관시킬 수 없는 모드에서 동작하기 위한 능력이 추가된 표준 능력들을 가지고 사용되는 실시예를 기술한다. 당해 기술분야에 공지된 다른 셀룰러 또는 무선 플랫폼들을 사용하는 다른 실시예들이 또한 예상될 수 있다는 점이 당업자에게 명백할 것이다.

[0247] 개인 모드는 네트워크가 각각의 허가된 가입자에 동일한 인증 메시지를 하루에 한번(또는 일부 적당한 간격으로) 전송하게 함으로써 인에이블되는 개인 등록 프로세스 상에서 예측된다. 각각의 가입자에게 송신된 인증 메시지는 해당 가입자의 공개 암호 키를 사용하여 암호화된다.

[0248] 사용자가 개인 셀룰러 모드에 들어가기를 원하는 경우, 사용자는 셀룰러 플랫폼으로 하여금 네트워크에 개인 인에이블 등록(PER) 메시지를 송신하게 한다. 인증 메시지 및 랜덤 장비 태그(RET)로 구성된 PER은 네트워크의 공개 암호 키를 사용하여 암호화된다. PER 내의 인증 메시지는, PER이 유효 사용자에 의해 송신되었지만 실제로 사용자를 식별하지 않는 네트워크를 보여주는 제로-지식 증명으로서 작용한다(복제의 문제는 하기에서 다루어질 것이다).

[0249] RET는 방문자 위치 레지스터(VLR) 및 홈 위치 레지스터(HLR)에 입력되어 마치 전화 번호인 것처럼 다루어질 수 있는 난수이다. 따라서, VLR 및 HLR은 셀룰러 플랫폼에 대한 전화 호출을 설정하고 유지하기 위해 요구되는 모든 정보를 수집할 수 있지만, 이 정보를 특정 개인 및 전화 번호와 연관시키지 않을 것이다. 사용자 장비가 개인 셀룰러 모드에서 유지되는 한, 후속적인 등록 메시지들은 사용자의 전화 번호가 아닌 RET를 포함할 것이다.

[0250] 호출 설정, 이동도 관리 및 로밍은, HLR 및 VLR 위치 정보가 전화 번호가 아닌 RET와 연관된다는 차이점을 가지고, 모두 이전처럼 정확히 핸들링될 수 있다. 데이터 호출들은 RET를 임시 IP 어드레스와 연관시킴으로써 개인

적인 것으로 유지될 수 있다. 당해 기술분야에 공지된 일반 패킷 무선 서비스(GPRS) 표준의 한가지 버전은 익명의 패킷 데이터 프로토콜(PDP) 상황을 허용하였다. 이러한 상황은 SGSN에서 PDP 어드레스를 임시 논리 링크 식별자와 연관시켰는데, IMSI는 PDP 어드레스와 연관되지 않았고, 따라서 상황은 익명이었다. 상세 항목들은 추후 표준에서 삭제된 ETSI GSM 03.60의 섹션 9.2.2.3의 조기 버전에 기술되었다.

[0251] 인입 호출들은 호출 당사자들이 RET를 알고 있을 것을 요구한다. RET가 정확한 HLR과 연관되도록 하기 위해, 호출 당사자는 호출된 당사자로서 역할을 하는 서비스 제공자를 식별할 수 있다. 따라서, 개인 셀룰러 모드에 있는 사용자는 공개 키 암호화를 사용하여, 자신이 호출을 수신하려고 하는 해당 당사자들에게 자신의 RET 및 서비스 제공자의 신원을 분배할 수 있다. 호출들은 인입 호출들에 대해 전개된 개인 상황을 사용하여 셀룰러 플랫폼으로부터 개인 모드에 놓일 수 있거나, 또는 대안적으로, 아웃고잉 호출들은 다른 랜덤 스트링들을 사용하여 호출 단위 기반으로 등록될 수 있다. 이는 단일 랜덤 스트링과 연관된 정보의 양을 감소시키고, 따라서, 개인 상황을 특정 사용자와 연관시키기 위한 서비스 제공자의 능력을 감소시킬 것이다.

[0252] 복제 및 요금청구 모두는 신뢰된 플랫폼 모듈(TPM)을 셀룰러 플랫폼 내에 구축함으로써 다루어질 수 있다. TPM(또는 등가 디바이스)은 인증 메시지를 암호 보안 볼트에 유지하고, 따라서, 이를 또다른 플랫폼에 전달하기를 원하는 어떤 사람에게도 사용불가능하게 하도록 프로그래밍될 수 있다. 네트워크가 PER 메시지를 수신하는 경우, 따라서, 전송측 전화가 실제로 네트워크로부터 인증 메시지를 수신했음이 보증될 수 있다. 원격 입증은 TPM을 제어하는 소프트웨어가 변경되지 않았음을 보장하기 위해 사용될 수 있다.

[0253] 요금청구에 대해, 서비스 제공자는 알려지지 않은 당사자에 서비스를 제공하는 불편한 작업에 당면한다. 해법은 다시 한번 TPM에 있다. 플랫폼에 대해 사용가능한 개인 호출 시간의 수는 플랫폼 내의 소프트웨어를 통해 제어될 수 있고, 소프트웨어는 원격 입증에 의해 인증된다. 일 실시예에서, 개인 호출 시간들은 선불될 수 있다. 개인 모드를 선불된 서비스로서 간주하기 위한 잠재력은, CALEA(Communications Assistance for Law Enforcement Act)가 현재 선불된 셀룰러 전화들을 커버하지 않으므로, CALEA에 대해 상당한 장점을 가진다. 미국 및 많은 다른 국가들에서, 사람들은 자신의 이름을 전화와 연관시키지 않고 선불된 셀룰러 전화를 구매하고 사용할 수 있다. 따라서, 여기서 개시된 프라이버시 오버레이는 선불된 셀룰러의 프라이버시 이점들을 후불 셀룰러 전화 사용자들에게 제공할 것이다.

[0254] 6.2 예 2: 익명 인증

[0255] 이 예 및 예 6.3은 프라이버시-인지 설계 구현들이 정보 네트워킹에 적용되는 경우들을 고려한다. 이러한 예는 정보 네트워킹(예를 들어, 셀룰러, 무선)에 대한 포괄적인 문제점, 사용자 인증에 대한 필요성을 해결하는 동시에, 개인들과의 데이터 식별을 최소화하도록 노력하는 프라이버시 오버레이를 보여준다. 이러한 예는 비속성(nonattribution) 요건이 자신의 프라이버시-인지 시스템들의 개발시에 실제 엔지니어를 지원할 수 있는 툴들에 대한 필요성을 생성함을 보여준다. 섹션 6.3, 예 3에서, 프라이버시-인지 수요 반응 시스템이 개시된다. 예 3에서, 분배된 프로세싱 요건들의 중요성을 강조하는 몇몇 아키텍쳐 이슈들이 또한 다루어진다.

[0256] 인증 문제점들이, 셀룰러 전화 호출의 배치로부터 커피숍에서의 인터넷 액세스의 획득까지, 많은 상이한 시나리오들에서 모바일 컴퓨팅 및 통신 네트워크들에서 발생한다. 따라서, 인증 문제는 당신이 바로 자신이 말하는 사람이라는 점을 서비스 제공자에게 증명하는 것이다. 그러나, 누군가 개인과의 장비의 식별을 최소화하려는 마음을 가지고 표면을 조금 파헤치면, 서비스 제공자의 관점으로부터의 문제점의 참 속성이 제공된 서비스들에 대한 지불이 수신될 것임을 보장하는 것임을 알 수 있다. 따라서, 비속성 요건이 만족될 수 있으며, 지불 보증이 마련되는 한, 서비스 제공자는 서비스가 누구에게 제공되는지를 아는 것이 필요하지 않다. 익명 인증이 설정되는 경우, 서비스의 동작에 의해 포함되는 임의의 데이터 수집(예를 들어, 셀룰러 전화에 대한 인입 호출들의 라우팅을 위해 요구되는 위치 데이터)은 익명일 것이다.

[0257] 익명 인증은 제로-지식 증명을 특징으로 할 수 있다. 사용자는, 임의의 개인 식별 정보를 제공하지 않고, 자신이 허가된 사용자들의 풀(pool)의 하나임을 서비스 제공자에게 증명하기를 원한다. 한가지 가능한 해법은 섹션 6.1, 예 1(도 1)에 개시된 셀룰러 텔레포니의 특정 적용예에 대한 방식에 있지만, 이는 당업자에게 명백할 바와 같이, 많은 적용예들, 예를 들어, 유틸리티 또는 제3자 데이터 수신 및 관리를 위한 무선 네트워크들 또는 통신 네트워크들에 적용될 수 있다. 네트워크 및 자신의 사용자들에 대한 공개 키들을 분배할 수 있는 공개 키 기반 구조(PKI)가 제공될 수 있다. 서비스 제공자는 네트워크를 사용하도록 허가되는 모든 사용자들에게 인증 메시지들을 주기적으로 분배한다. 특정 메시지는 모든 사용자들에 대해 동일하지만, 각각의 특정 사용자의 공개 키를 사용하여 암호화된다. 암호화된 인증 메시지는 이메일, 무선 제어 채널, 또는 애플리케이션에 대해 적절한 어떤 수단이라도 사용하여 전송될 수 있다. 일부 실시예들에서, 인증 메시지는 전송가능하지 않을 수 있으며,

어느 경우든 신뢰된 플랫폼 모듈(TPM)과 같은 암호 금고 기술이 사용될 수 있다.

[0258] 사용자가 서비스를 획득하기 위해 인증하기를 원하는 경우, 인증 메시지는 장비를 식별하기 위해 사용될 수 있는 랜덤 태그와 함께 네트워크에 다시 송신된다. 인증 메시지는 네트워크의 공개 키를 사용하여 암호화된다. 이 메시지를 수신할 시에, 네트워크는, 사용자가 인증 메시지를 알고 있으므로, 액세스를 요청하는 사용자가 유효함을 알고 있다. 그러나, 네트워크는 사용자의 신원을 알고 있지 않다. 네트워크는 이후 필요한 경우 사용자 장비에 접촉하여 사용자 장비에 대한 액세스를 제공하기 위해 랜덤 태그를 사용할 수 있다.

[0259] 프라이버시 오버레이에 대한 위의 예는 비속성 요건의 적용을 보여주는데, 즉 사용자 프라이버시를 보호하기 위한 시스템이 설정되어, 이에 의해, 네트워크가 상호작용할 수 있으며, 필요한 경우, 장비가 누구에게 속하는지 알지 않고 사용자 장비를 추적할 수 있다. 이러한 설계는 사용자의 프라이버시를 보호하는 역할을 하며, 개인 및 익명 소모를 가능하게 한다.

[0260] 6.3 예 3: 수요 반응 및 분배 프로세싱

[0261] 유틸리티들은 전력 생성시 비용 절감을 제공하고, 그리드 신뢰성 및 유연성을 증가시키고, 고객-유틸리티 상호작용의 새로운 모드들을 생성할 마이크로그리드들 및 다른 시스템들을 채택한다(예를 들어, 연방 에너지 규제 위원회(2009년 9월), 2009 수요 반응 및 어드밴스드 미터링의 평가, 스태프 대표 http://www.ferc.gov/legal/staff-reports/sep-09-demand-response.pdf를 참조하라). 수요 반응 시스템들은 이러한 노력에 있어서 중요한 역할을 수행할 것이다. 일반적으로 말해서, 수요 반응 시스템들은 시간 경과에 따른 전기료의 변경들에 응답하여 최종-사용 고객들에 의한 전기 소모 행동을 수정한다(M. H. Albadi 및 E. F. El-Saadany, A summary of demand response in electricity markets, Electric Power Syst. Res., vol. 78, pp. 1989-1996, 2008). 고객에게 가격책정 정보를 제시함으로써, 또는 유틸리티에 의한 가전제품들의 직접 제어를 통해 유도되는 수정들은 수요 타이밍, 즉각적 수요의 레벨, 또는 주어진 시간 기간 동안의 전체 수요를 변경시킬 수 있다(OECD, International Energy Agency, The Power to Choose - Demand Response in Liberalized Electricity Markets, Paris, France, 2003). 전체 목표는 시간 경과에 따른 에너지 소모의 균형을 맞추어서, 유틸리티들이 생성기들을 온라인 또는 오프라인으로 취할 (고가의) 필요성을 경감시키는 것이다.

[0262] 수요 반응 시스템들은 월별 요금청구를 위해 요구되는 것보다 훨씬 더 미세한 입도 레벨에서 전력 소모 정보를 요구한다. 그 이유는 간단하다: 소모가 하루 코스에 대한 가격에 따라 수정되는 경우, 소모 정보는 고객에게 적절하게 요금 청구하기 위해 가격책정 정보와 동일한 입도 레벨에서 사용가능해져야 한다. 해법은 어드밴스드 미터링 기반구조(AMI), 즉, 과거의 한 달에 한번 미터 판독이 아닌 분 단위 기반으로 전력 소모를 샘플링 및 기록할 수 있는 기술에 있다. AMI 배치는 수년간 진행되어 왔다. 연방 에너지 규제 위원회는 2009년 전국적으로 795만 개의 어드밴스드 미터들이 설치되었다고 추정한다(연방 에너지 규제 위원회(2009년 9월). 수요 반응 및 어드밴스드 미터링의 2009년 평가, 스태프 대표 http://www.ferc.gov/legal/staff-reports/sep-09-demand-response.pdf). 2009년 19개 주에서 26개의 유틸리티들이 어드밴스드 미터링 파일럿들 및 전체-배치 프로그램들을 선언하거나 추구하였다.

[0263] 수요 반응의 잠재적 영향이 크다. (2009년 6월, 연방 에너지 규제 위원회, 로부터 취해지는, 수요 반응 잠재력의 국가 평가, 스태프 대표. 다운로드: http://www.ferc.gov/legal/staff-reports/06-09-demand-response.pdf) 도 5에서 알 수 있는 바와 같이, AMI의 분배의 범위에 따라, 전기 수요에 대한 피크 여름 기간 동안 미국에서 에너지의 잠재적 절감들은 전체 로드의 4% 내지 20%를 범위로 한다. 외국의 오일 및 관련 자원들에 대한 미국의 필요성에 대한 후속적인 긍정적 영향은 과장하기 어려울 것이다.

[0264] 도 5를 더 상세하게 살펴보면, 전력 절감의 범위가 AMI 참여의 함수라는 점을 알 수 있다. 다양한 시나리오들의 설명이 도 6에 제공된다.

[0265] 도 6을 도 5와 비교하면, Bopt-in[참여 시나리오로부터의 에너지 절감들이 9%에서 추정되는 반면, 의무적인 유니버셜 방식의 에너지 절감은 20%라는 점에 유의한다. 따라서, 피크 소모에서의 추가적인 11% 감소는 규제자들이 고객이 자신의 홈에 설치된 어드밴스드 미터링을 가질 것을 요구하는 경우 가능하다. 이는 AMI가 적절하게 사용되지 않는 경우 심각한 프라이버시 위협을 가할 수 있으므로, 국가적 중요성이 이슈가 될 것이다.

[0266] Lisovich 등은 어드밴스드 미터링 시스템들에 의해 수집된 상세화된 전력 소모 데이터가 홈-내 활동들에 관한 정보를 노출함을 보여준다(M. Lisovich, D. Mulligan, and S. B. Wicker, Inferring personal information from demand-response systems, IEEE Security Privacy Mag., vol. 8, no. 1, pp. 11-20, 2010년 1월/2월을 참조하라). 또한, 이러한 데이터는 참여자의 활동들에 대해 훨씬 더 많이 발견하기 위해 다른 용이하게 사용가

능한 정보와 결합될 수 있다(M. Lisovich, D. Mulligan, and S. B. Wicker, Inferring personal information from demand-response systems, IEEE Security Privacy Mag., vol. 8, no. 1, pp. 11-20, 2010년 1월/2월). 이러한 결과는 (적절한 프라이버시 안전가드들 및 거주자의 명시적 허용을 가지고) 표준 학생 거주지에서 수행되는 실험으로부터 초래되었다. 제조된 에너지 사용 모니터는 실시간 전력 소모 데이터를 수집하기 위해 거주자의 브레이커 패널에 부착되었다. 1 W의 분해능을 가지고 1 또는 15초의 간격들로 획득되는 데이터는 워크스테이션 상에서 실행하는 NILM(nonintrusive load monitor) 애플리케이션에 전송되었다. 행동 추출 알고리즘은 이후 단독으로 전력 소모에만 기초하여 행동을 예측하려는 시도 시에 워크스테이션 상에서 실행되었다. 비디오 데이터는 실험에 대한 제어를 설정하기 위해 사용되었다.

[0267] 실험으로부터의 결과들 중 일부는 도 7a-d에서 재생된다. 도 7(a)는 며칠의 코스 동안 전력 소모 데이터의 수집을 도시한다. 수직 축은 와트로 라벨링되는 반면, 수평 축은 며칠의 코스 동안 시간 경과를 도시한다. 거주지 내에서의 활동을 표시하는, 매일의 코스 동안의 몇몇 상당한 전력 소모 피크들이 존재한다.

[0268] 도 7(b)는 수백 초 동안 수집된 전력 소모 데이터에 적용된 에지 검출 알고리즘의 결과들을 예시한다. 에지 검출 알고리즘은 다소 단순하며, 당해 기술분야에 공지되어 있으며, 그래프는 시간상으로 인접한 전력 소모 샘플들 사이의 차이를 도시한다. 수직축은 $\Delta(t) = P(t) - P(t-1)$를 도시하며, 여기서, $P(t)$는 시간 t에서 샘플링된 전력 소모이다. 수평 축은 시간을 반영한다. 특정 스위칭 이벤트들이 이제 격리될 수 있다는 점에 주목한다; 냉장고 및 마이크로파 오븐에 의해 생성된 전력 소모 과도들이 쉽게 보인다.

[0269] 도 7(c)는 로드-식별 프로그램으로부터 찍힌 스크린 샷이다. 이는 이벤트들이 하루 코스 동안(수평 축의 단위들은 일(day)들임) 격리되고 분류될 수 있다는 점을 보여준다. 이러한 정보 타입을 가지고, 집 내에서의 개인들의 행동을 추정하도록 진행할 수 있다.

[0270] 도 7(d)는 전력 소모 데이터가 개인 행동에 관련된 변수들을 추정하기 위해 사용됨을 도시한다. 기준선들은 실제 동작들을 도시한다. "기준 슬립웨이크" 선에서, 제로는 점유자가 잠들었음을 표시하고, 1은 그가 깨었음을 표시한다. "기준 존재" 라인 상에서, 제로는 거주지의 점유자가 집에 없었음을 표시하고, 1은 그가 집에 있었음을 표시한다. 추정된 라인들은 이들 이벤트들에 대한 추정들을 표시한다. 기준 데이터가 추정들에 얼마나 가까운지에 유의한다.

[0271] 전력 소모 데이터가 프라이버시 문제를 생성한다면, 중앙화된 수집이 이를 구현하는 유틸리티들의 고객들에 대해 미해결된 것으로 증명할 수 있다는 점이 명백하다. 아직 중앙화되지 않은 수집은 취해지는 방향인 것으로 나타날 것이다. 2006년 FERC "Assessment of Demand Response and Advanced Metering"로부터의 후속하는 인용에서, AMI는 중앙화된 수집을 제공하는 시스템으로서 정의된다. 고객의 프라이버시 요구들에 대해 더 민감한 아키텍처 옵션들에 대한 허용이 존재하지 않을 수 있다.

[0272] 이러한 보고의 목적으로, 위원회 스태프는 "어드밴스드 미터링"을 다음과 같이 정의한다:"어드밴스드 미터링은 시간마다 또는 더 빈번하게 고객 소모[및 가능하게는 다른 파라미터들]를 레코딩하고, 중앙 수집 포인트에 통신 네트워크 상에서의 일간 또는 더 빈번한 측정들의 전송을 제공하는 미터링 시스템이다"(연방 에너지 규제 위원회, Assessment of demand response and advanced metering, Washington, DC, Staff Rep., Docket No. AD06-2-000, 2006년 8월, p. vi).

[0273] 위의 정의는 유틸리티들에 의해 인용된 이후 존재하며, 당해 기술 분야에서 인지된다(E. Steel 및 J. Angwin, On the web's cutting edge, anonymity in name only, Wall Street J., 2010년 8월 4일). 또한, 이는, 도 8에 보여지는 바와 같이, FERC에 의해 분배된 어드밴스드 미터링 기반구조(AMI) 문헌에서 그래프로 표현되었다(엔지니어링 전력 연구 협회, 어드밴스드 미터링 기반구조, http://www.ferc.gov/eventcalendar/Files/20070423091846-EPRI%20-%20Advanced%20Metering.pdf). 기준이 제3자 데이터 수신 및 관리에 대한 잠재력에 대해 만들어진다는 점에 유의한다. 이는 마케터들 등에 의한 상업화 및 후속적인 재사용을 포함하는, 요구되는 데이터의 비규제 사용에 대한 잠재력을 틀림없이 증가시킨다.

[0274] 수요 반응 프로그램의 장기적 미래는 위험할 수 있다. 고객들은 프라이버시의 잠재적 침해시에 경고받을 수 있고, 이는 시스템의 고가의 리툴링을 요구하는 입법에 동기를 부여한다. 사법 처리가 또한 프로그램을 위험에 둘 수 있다. 대중의 격한 반응으로부터든 또는 사법 처리로부터든 간에, 프라이버시 인지를 중단하는 시스템들은 스스로 셧 다운함을 알 수 있다.

[0275] 그러나, 수요 반응 시스템들이 프라이버시-인지 설계의 렌즈를 통해 보여지는 경우, 프라이버시 보존 해법은 명

백하다. 수요 반응 시스템들의 목적은, 미세-입도의 가격책정 정보를 사용함으로써, 유도 또는 직접 제어를 통해, 소모 행동을 수정하는 것이다. 관심있는 행동 - 소모 - 이 고도로 배포된다. 분배 프로세싱 요건을 염두에 두면, 그것이 수집될 필요가 있는 전력 소모 데이터가 아니라, 대신 그것이 분배될 필요가 있는 가격 데이터라는 점이 명백해진다. 미세-입도의 소모 정보는 바로 이웃을 결코 남겨둘 필요가 없으며, 따라서, 대부분의 프라이버시 우려들을 완화시킨다.

[0276] 프라이버시-인지 수요 반응 아키텍쳐는 몇몇 상이한 데이터 흐름들을 고려해야 한다. 이들 각각에 대해, 프라이버시 분석이 수행되어야 하고 필요한 경우 프라이버시-인지 설계가 채택되어야 한다. 먼저, 고객 행동을 변경시키려 하는 시스템들에서, 가격책정 데이터는 고객이 소비 결정들을 하려는 기반을 가지도록 고객에게 제시되어야 한다. 이는 프라이버시 우려를 제시하지 않는데, 왜냐하면, 유틸리티가 주거용 미터에 및/또는 고객의 집 컴퓨터 상의 애플리케이션에 가격책정을 브로드캐스트 할 수 있기 때문이다.

[0277] 둘째, 직접 제어 시스템들에서, 유틸리티는 하루의 코스 동안 자신의 전기 소모를 제어하기 위해 가전제품들에 신호들을 송신해야 한다. 이것이 상당한 보안 이슈를 생성할 수 있지만, 이는 집 내에서의 고객 행동 및 선호도들에 대한 정보를 제공하지 않는다.

[0278] 제3 흐름은 더 많은 문제가 있다. 고객-특정 소모 데이터는 요금청구 목적으로 유틸리티에 제공되어야 한다. 여기에 이슈가 존재하는데, 왜냐하면, 전술된 프라이버시 이슈를 생성하지 않고 유틸리티에 소모 데이터를 스트리밍할 수 없기 때문이다. 또한 실시간 비용 데이터를 스트리밍할 수 없는데, 왜냐하면, 이러한 정보를 다시 소모 데이터로 변환하는 것이 사소한 것이기 때문이다. 해법은 거주지에서 가격-가중 소모 데이터를 누적하고 이후 주 단위 또는 월 단위로 유틸리티에 수집 비용을 송신하는 것에 있다. 이는 신뢰된 플랫폼 모듈 또는 등가물을 요구하는 미터에서 보안 레벨을 내포한다.

[0279] 마지막으로, 유틸리티는, 수요를 예측하고 가격책정 모델을 유지하기 위해, 시간상으로 정교하지만 고객 레벨에서 수집되는 소모 데이터를 요구한다. 통상적으로, 변전소 레벨에서의 수집된 실제 전력 소모 데이터는 예측된 수요를 서비스하는데 필요한 새로운 전송 및 분배 라인들 및 생성을 위한 요구를 예측하기에 충분하다. 이웃 수집기는 데이터를 결합하고 익명화하기 위해 사용될 수 있고, 따라서, 요구되는 시간 입도는 개인 행동에 대한 정보를 생성하지 않고 제공된다. 익명화는 단일 고객의 데이터가 격리될 수 없도록 충분한 수의 고객들에 대한 전력 소모 데이터를 합산함으로써 수행될 수 있다. 위의 해법들은 도 9에 도시된 아키텍쳐에 포함된다.

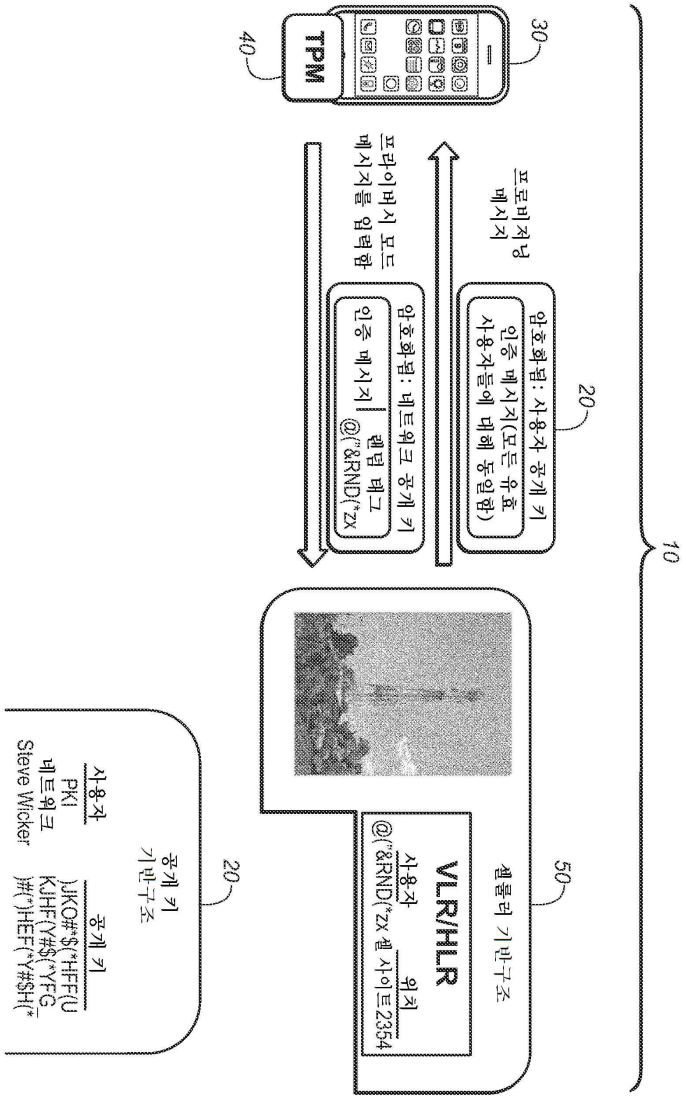
[0280] 본 발명은 여기서 기술된 특정 실시예들에 의한 범위에 제한되지 않을 것이다. 실제로, 여기서 기술된 것들에 추가하여 본 발명의 다양한 수정들이 이전 설명으로부터 당업자에 대해 명백할 것이다. 이러한 수정들은 첨부된 청구항들의 범위 내에 들도록 의도된다.

[0281] 여기서 인용된 모든 참조들은 그 전체가 참조로, 그리고 마치 각각의 개별 공보, 특허 또는 특허 출원이 모든 목적으로 그 전체내용이 참조로 포함되도록 구체적으로 그리고 개별적으로 나타내는 경우와 동일한 범위에 대해 모든 목적으로 여기에 포함된다.

[0282] 임의의 공보의 인용은 출원일 이전의 그것의 개시물에 대한 것이며, 본 발명이 이전 발명으로 인해 이러한 공보에 선행하도록 자격이 주어지지 않음을 허용하는 것으로서 해석되지 않아야 한다.

도면

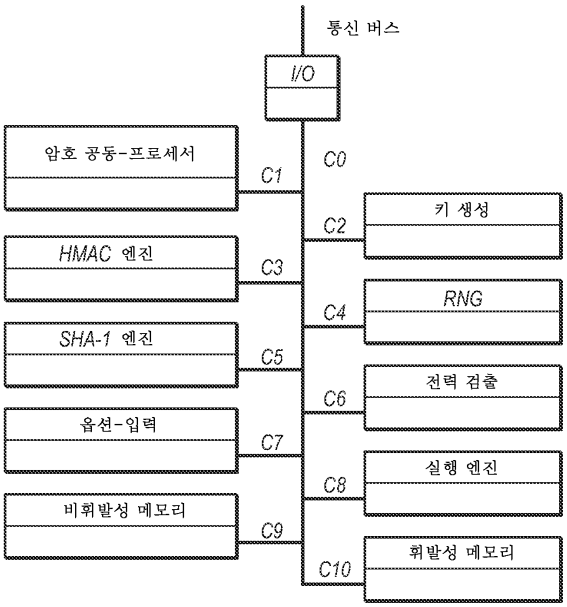
도면1



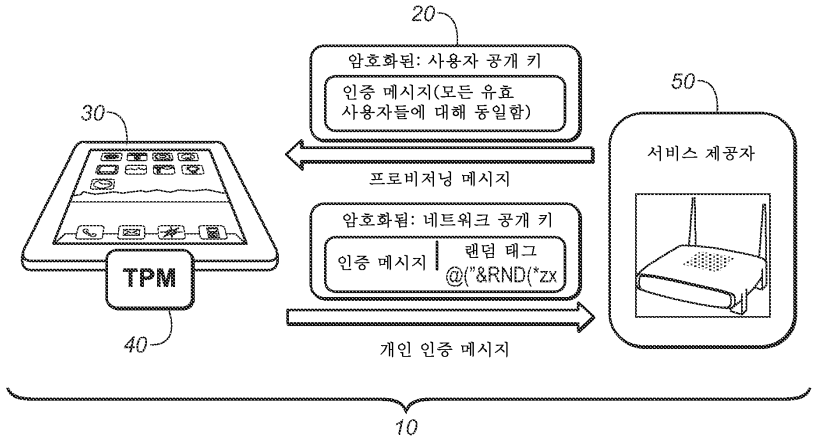
도면2

TPM 다양한 서비스	암호 커맨드들	*TPM_Sign* *TPM_GetRandom* *TPM_StirRandom*	이들 커맨드들은 일반적인 목적의 암호 서비스들을 제공한다.
	회계 커맨드들	*TPM_GetAuditEvent* *TPM_GetAuditEventSigned* *TPM_SetOrdinalAuditStatus* *TPM_GetOrdinalAuditStatus*	이들 커맨드들은 회계 트레일 데이터를 수집하고 회계 특징들을 제어하기 위해 사용된다.
	능력 보고 커맨드들	*TPM_GetCapability* *TPM_GetCapabilitySigned* *TPM_GetCapabilityOwner*	이들 커맨드들은 TPM 부분 및 구현된 기능성에 관한 정보를 제공한다.

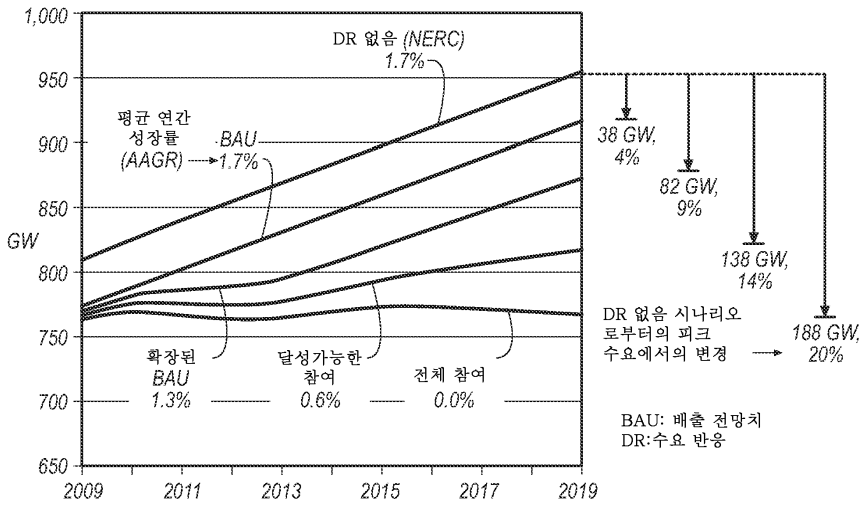
도면3


통신 버스
I/O
암호 공동-프로세서
C1
C0
키 생성
C2
HMAC 엔진
C3
RNG
C4
SHA-1 엔진
C5
전력 검출
C6
옵션-입력
C7
실행 엔진
C8
비휘발성 메모리
C9
휘발성 메모리
C10

도면4


20
암호화됨: 사용자 공개 키
인증 메시지(모든 유효 사용자들에 대해 동일함)
50
30
서비스 제공자
프로비저닝 메시지
암호화됨: 네트워크 공개 키
인증 메시지
랜덤 태그 @("&RND(*zx
TPM
40
개인 인증 메시지
10

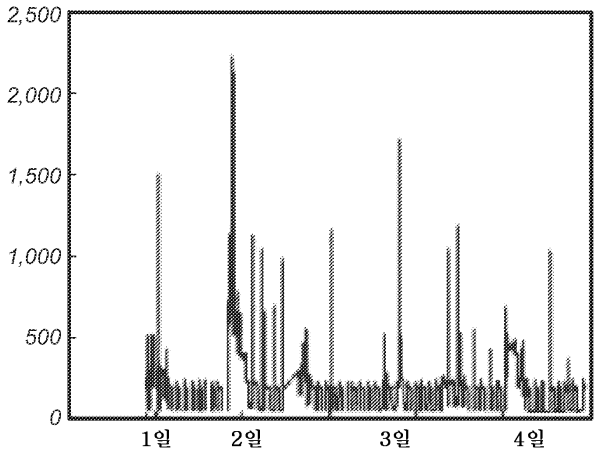
도면5


1,000
950
900
850
GW
800
750
700
650
2009
2011
2013
2015
2017
2019
DR 없음 (NERC)
1.7%
평균 연간 성장률 (AAGR)
BAU
1.7%
38 GW, 4%
82 GW, 9%
138 GW, 14%
188 GW, 20%
DR 없음 시나리오 로부터의 피크 수요에서의 변경
확장된 BAU 1.3%
달성가능한 참여 0.6%
전체 참여 0.0%
BAU: 배출 전망치
DR:수요 반응

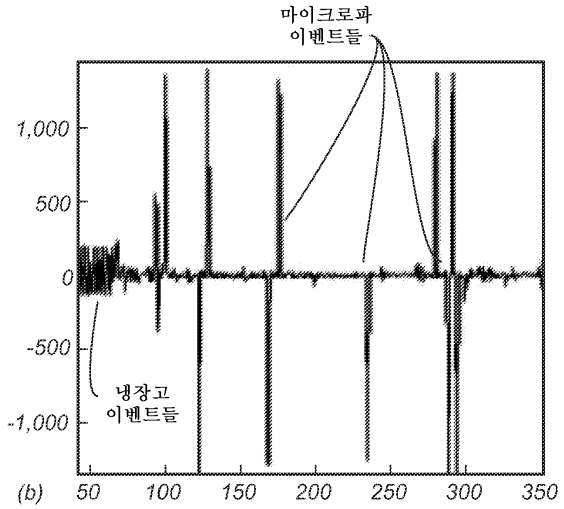
도면6

가정	배출 전망치	확장된 BAU	달성가능한 참여	전체 참여
AMI 배치	부분 배치	부분 배치	전체 배치	전체 배치
동적 가격책정 참여 (적합함)	오늘의 레벨	자발적 (옵션-입력); 5%	디폴트(옵션-출력) 60% 내지 70%	유니버셜 (의무적); 100%
적절한 고객 공급 인에이블 기술	없음	없음	95%	100%
적절한 고객 수용 인에이블 기술	없음	없음	60%	100%
비-가격책정 참여율에 대한 기반	오늘의 레벨	"최상의 구현들" 추정	"최상의 구현들" 추정	"최상의 구현들" 추정

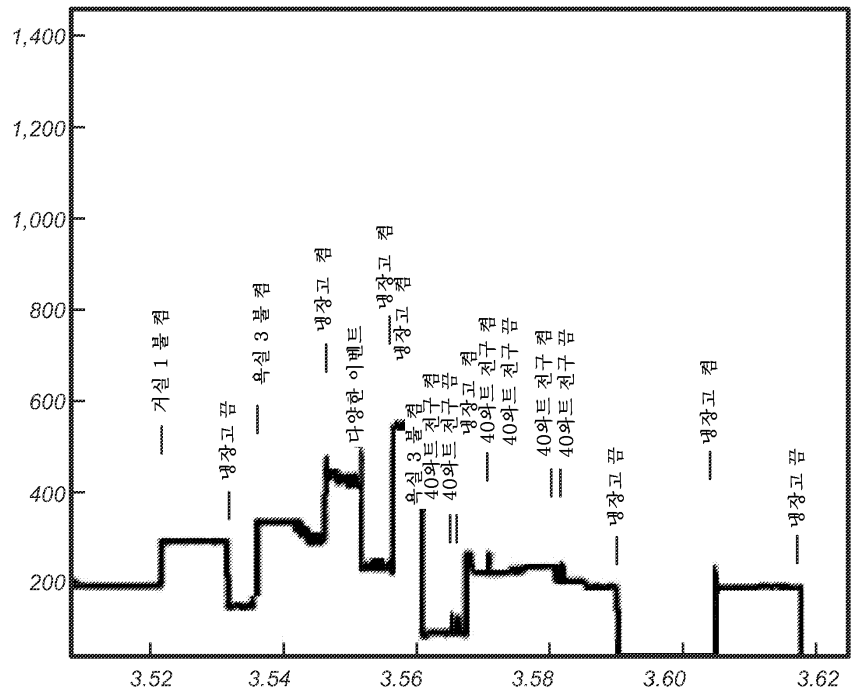
도면7a



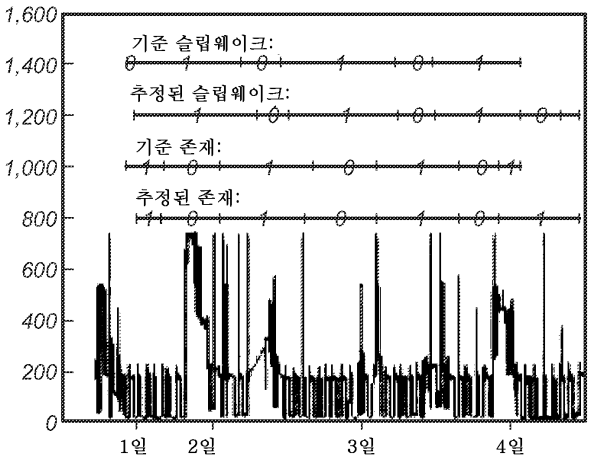
도면7b



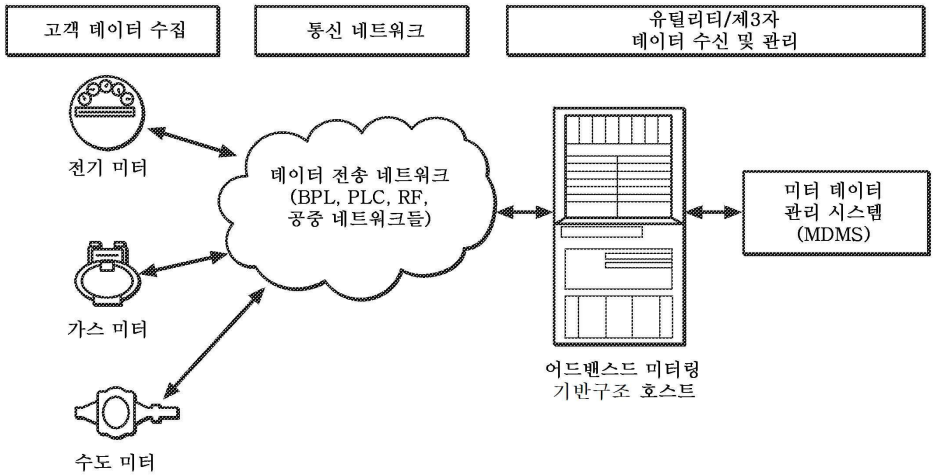
도면7c


1,400
1,200
1,000
800
600
400
200
3.52
3.54
3.56
3.58
3.60
3.62
거실 1 불 켬
냉장고 끔
욕실 3 불 켬
냉장고 켬
다양한 이벤트
냉장고 켬
냉장고 켬
욕실 3 불 켬
40와트 전구 끔
40와트 전구 켬
냉장고 켬
40와트 전구 켬
40와트 전구 끔
40와트 전구 켬
40와트 전구 끔
냉장고 끔
냉장고 켬
냉장고 끔

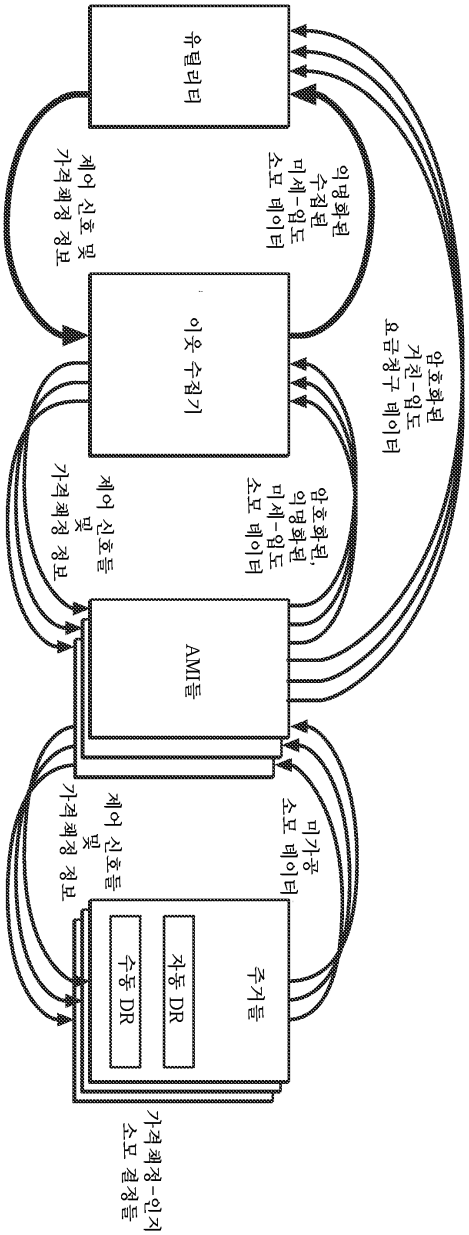
도면7d


1,600
1,400
1,200
1,000
800
600
400
200
0
기준 슬립웨이크:
추정된 슬립웨이크:
기준 존재:
추정된 존재:
1일
2일
3일
4일

도면8


고객 데이터 수집
통신 네트워크
유틸리티/제3자
데이터 수신 및 관리
전기 미터
가스 미터
수도 미터
데이터 전송 네트워크
(BPL, PLC, RF,
공중 네트워크들)
어드밴스드 미터링
기반구조 호스트
미터 데이터
관리 시스템
(MDMS)

도면9


유틸리티
이웃 수집기
AMI들
주거들
자동 DR
수동 DR
익명화된 수집된 미세-입도 소모 데이터
제어 신호 및 가격책정 정보
암호화된 거친-입도 요금청구 데이터
암호화된, 익명화된 미세-입도 소모 데이터
제어 신호들 및 가격책정 정보
미가공 소모 데이터
제어 신호들 및 가격책정 정보
가격책정-인지 소모 결정들