(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0015026
(43) 공개일자 2009년02월11일

(51) Int. Cl.
G06F 15/16 (2006.01) *H04L 9/30* (2006.01)
(21) 출원번호 10-2008-7025220
(22) 출원일자 2008년10월15일
심사청구일자 없음
번역문제출일자 2008년10월15일
(86) 국제출원번호 PCT/US2007/010092
국제출원일자 2007년04월23일
(87) 국제공개번호 WO 2007/124180
국제공개일자 2007년11월01일
(30) 우선권주장
11/408,894 2006년04월21일 미국(US)

(71) 출원인
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
시두, 구샤란 에스.
미국 98052-6399 워싱턴주 레드몬드 원 마이크로소프트 웨이 마이크로소프트 코포레이션 국제 특허부 내
호튼, 노아
미국 98052-6399 워싱턴주 레드몬드 원 마이크로소프트 웨이 마이크로소프트 코포레이션 국제 특허부 내
싱할, 산딥 케이.
미국 98052-6399 워싱턴주 레드몬드 원 마이크로소프트 웨이 마이크로소프트 코포레이션 국제 특허부 내
(74) 대리인
양영준, 백만기

전체 청구항 수 : 총 20 항

(54) 인덱스 저장소 사용 방법, 컴퓨터 시스템, 및 컴퓨터 판독가능 매체

(57) 요 약

시스템은 공개적으로 이용가능한 인덱스 저장소에서 인증된 연락처 정보를 게시할 수 있고, 이 연락처 정보를 검색할 수 있고, 그것에 대한 유효성 검사를 행할 수 있다. 청구하는 방법 및 시스템은, 게시(publishing)에 대한 서버는 선택적인(optional) 클라이언트 기반인 접근 방법을 제공할 수 있다. 이 공개적으로 이용가능한 인덱스 저장소는 피어-투-피어 네트워크에서 사용되는 분산된 해시 테이블일 수 있다. 시스템은 서버가 이용가능하지 않거나 또는 서버 신뢰도가 최소한일 수 있는 기타 보안 디렉토리 서비스 애플리케이션에서 사용될 수 있다.

대 표 도 - 도5

특허청구의 범위

청구항 1

보안 게시 시스템(secure publication system)을 위한 공개적으로 이용가능한 인덱스 저장소(index store)를 사용하는 방법으로서,

공개 키(public key)에 통계적으로 고유한 암호화 고유 식별자(cryptographically unique identifier)를 제공하는 단계;

게시자의 개인 키(private key)로 메시지에 서명하는 단계 -상기 메시지는 게시자의 공개 키를 포함함-

상기 메시지를 공개적으로 이용가능한 인덱스 저장소에 삽입하는 단계 -상기 메시지는 상기 암호화 고유 식별자에 의해 인덱스됨 -;

상기 암호화 고유 식별자에 기초하여 엔트리를 검색(retrieve)하는 단계;

상기 암호화 고유 식별자가 상기 공개 키에 관련된 것인지의 여부를 판정하는 단계;

상기 메시지가 상기 공개 키에 대응하는 개인 키에 의해 서명되어 있는지의 여부를 판정하는 단계

를 포함하는, 인덱스 저장소 사용 방법.

청구항 2

제1항에 있어서, 상기 메시지가 예상되는 포맷과 구문을 지니는지의 여부를 판정하는 단계를 더 포함하는 인덱스 저장소 사용 방법.

청구항 3

제1항에 있어서, 상기 인덱스 저장소는 분산된 해시 테이블(distributed hash table)과 디렉토리 서버(directory server) 중 하나인 인덱스 저장소 사용 방법.

청구항 4

제1항에 있어서, 상기 암호화 고유 식별자는 해시 함수를 사용하여 사용자의 공개 키로부터 도출되는(derived) 인덱스 저장소 사용 방법.

청구항 5

제1항에 있어서, 상기 검색 단계를 수행하는 컴퓨터가, 상기 암호화 고유 식별자가 상기 공개 키에 관련된 것으로 판정할 때, 상기 메시지가 상기 공개 키에 대응하는 개인 키로 서명된 것으로 판정할 때, 그리고 상기 메시지가 예상되는 포맷과 구문을 지니는 것으로 판정할 때, 상기 공개 키를 사용하는 것을 허용하는 단계를 더 포함하는 인덱스 저장소 사용 방법.

청구항 6

제1항에 있어서, 상기 메시지는 암호화 강도(encryption strength)에 비례하는 지속기간 파라미터(duration parameter)를 더 포함하는 인덱스 저장소 사용 방법.

청구항 7

제6항에 있어서, 상기 지속기간 파라미터에 의해 표시되는 지속기간이 만료되지 않은 것으로 판정할 때, 상기 암호화 고유 식별자가 상기 공개 키에 관련된 것으로 판정할 때, 상기 메시지가 상기 공개 키에 대응하는 개인 키로 서명된 것으로 판정할 때, 그리고 상기 메시지가 예상되는 포맷과 구문을 지니는 것으로 판정할 때, 상기 검색 단계를 수행하는 컴퓨터가, 상기 공개 키를 사용하는 것을 허용하는 단계를 더 포함하는 인덱스 저장소 사용 방법.

청구항 8

제1항에 있어서, 상기 암호화 고유 식별자는 그룹 공개 키를 포함하는 인덱스 저장소 사용 방법.

청구항 9

제1항에 있어서, 암호화 고유 식별자는 적어도 제1 사용자의 암호화 고유 식별자와 제2 사용자의 암호화 고유 식별자로부터 형성되는 인덱스 저장소 사용 방법.

청구항 10

피어-투-피어 네트워크를 형성하는 복수의 피어 노드;

상기 피어-투-피어 네트워크의 분산된 해시 테이블;

제1 피어 노드 -상기 제1 피어 노드는, 자신의 공개 키에 통계적으로 고유한 암호화 고유 식별자를 생성하며, 상기 공개 키를 포함하고 상기 공개 키에 대응하는 개인 키로 서명된 메시지를 상기 암호화 고유 식별자에 의해 인덱스되는 상기 분산된 해시 테이블 내로 삽입함-;

제2 노드 -상기 제2 노드는 상기 암호화 고유 식별자에 기초하여 상기 메시지를 검색하며, 상기 암호화 고유 식별자가 상기 공개 키에 관련된 것인지의 여부를 판정하고, 상기 메시지가 상기 공개 키에 대응하는 상기 개인 키로 서명되어 있는지의 여부를 판정하고, 상기 메시지가 예상되는 포맷과 구문을 지니는지의 여부를 판정함-

를 포함하는 컴퓨터 시스템.

청구항 11

제10항에 있어서, 상기 제2 노드는, 상기 암호화 고유 식별자가 상기 공개 키에 관련된 것으로 판정될 때, 상기 서명이 상기 공개 키에 대응하는 상기 개인 키로 서명된 것으로 판정될 때, 그리고 상기 메시지가 예상되는 포맷과 구문을 지니는 것으로 판정될 때, 상기 공개 키를 사용하여 상기 제1 노드와 통신하는 컴퓨터 시스템.

청구항 12

제10항에 있어서, 상기 암호화 고유 식별자는, 상기 제1 노드와 관련된 제1의 암호화 고유 식별자와 상기 제2 노드와 관련된 제2의 암호화 고유 식별자의 조합을 포함하는 컴퓨터 시스템.

청구항 13

제12항에 있어서, 상기 메시지는 상기 제2 노드의 공개 키를 사용하여 암호화되는 컴퓨터 시스템.

청구항 14

제10항에 있어서, 상기 메시지는 지속기간 파라미터를 포함하며, 상기 지속기간 파라미터는 상기 공개 키와 상기 공개 키에 대응하는 개인 키를 생성하는 데에 사용되는 암호화 알고리즘(encryption algorithm)의 강도에 비례하는 컴퓨터 시스템.

청구항 15

제14항에 있어서, 상기 제2 노드는, 상기 지속기간 파라미터에 의해 표시되는 지속기간이 만료되지 않은 것으로 판정할 때, 상기 암호화 고유 식별자가 상기 공개 키에 관련된 것으로 판정할 때, 상기 메시지가 상기 공개 키에 대응하는 개인 키로 서명된 것으로 판정할 때, 그리고 상기 메시지가 예상되는 포맷과 구문을 지니는 것으로 판정할 때, 상기 메시지를 받아들이는(accept) 컴퓨터 시스템.

청구항 16

공개 키로부터 암호화 고유 식별자를 도출하는(derive) 단계;

상기 암호화 고유 식별자에 기초하여 인덱스 저장소에서 엔트리를 검색하는 단계 -상기 엔트리는 메시지와 공개 키를 포함하며, 상기 메시지와 공개 키는 상기 공개 키에 대응하는 개인 키로 함께 서명됨-;

상기 암호화 고유 식별자가 상기 공개 키에 관련된 것인지의 여부를 판정하는 단계;

상기 메시지와 공개 키가 상기 개인 키로 서명되어 있는지의 여부를 판정하는 단계

를 포함하는 동작들을 수행하는 컴퓨터 실행가능 명령어들을 갖는 컴퓨터 판독가능 매체.

청구항 17

제16항에 있어서, 상기 메시지가 예상되는 포맷과 구문을 지니는지의 여부를 판정하는 단계를 더 포함하는 컴퓨터 판독가능 매체.

청구항 18

제16항에 있어서, 상기 메시지의 지속기간 파라미터가 만료되었는지의 여부를 판정하는 단계를 더 포함하는 컴퓨터 판독가능 매체.

청구항 19

제18항에 있어서, 상기 지속기간 파라미터에 의해 표시되는 지속기간은 상기 공개 키와 상기 개인 키를 생성하는 데에 사용되는 암호화 수준에 비례하는 컴퓨터 판독가능 매체.

청구항 20

제16항에 있어서, 상기 암호화 고유 식별자는, 제1의 암호화 고유 식별자와 제2의 암호화 고유 식별자를 조합함으로써 형성되며, 상기 메시지는 상기 제2의 암호화 고유 식별자와 관련된 컴퓨터의 공개 키를 사용하여 암호화되는 컴퓨터 판독가능 매체.

명 세 서

배 경 기 술

<1> 디렉토리 서비스는 통상적으로 네트워크 서버를 이용하여 제공될 수 있다. 디렉토리 서비스를 이용하기 위해, 사용자는 그 서버에 접속해야 하고, 디렉토리 서비스에 액세스하기 위해 사용자 계정을 지닐 것을 필요로 할 수 있다. 게다가, 사용자는 그 서버가 데이터 무결성(data integrity)과 데이터 인증(data authentication)을 제공한다는 것을 신뢰해야만 하는 경우가 있다. 디렉토리 서비스가 예를 들면 애드 혹 네트워크와 같은 접속된 엔티티들의 작은 그룹을 의도한 것이라면, 이 애드 혹 네트워크를 위한 디렉토리 서버를 생성하고 셋업하는 것은 비효율적일 수 있다. 예를 들면, 애드 혹 네트워크는 그 속성상 통상적으로 일시적(transient)일 수 있으며, 짧은 지속기간 동안 그리고 적은 수의 사용자를 위해 전용 서버를 셋업하는 비용은, 관리자 시간(administrator time), 장비 자원 용량(equipment resource capacity)(일부 서버는 재할당되거나 또는 추가되어야 함) 그리고 사용자 시간(계정 생성과 셋업에 사용자가 관련될 수 있음)으로 인해 과다 비용이 들 수 있다. 게다가, 서버 기반 시스템이 일반적일 수 있으나, 피어-투-피어(peer-to-peer) 네트워크와 같이 서버가 없는 새로운 시스템은 통신을 용이하게 하기 위한 전용 서버를 필요로 하지 않을 수 있으므로, 애드 혹 네트워크를 생성하는 데에 있어 더 큰 융통성을 제공할 수 있다. 그러나, 기존의 암호화 프로세스들을 이용하여 이들 애드 혹 네트워크상에서 보안 통신을 가능하게 하게 위해서는, 서버 기반 모델에 의존하지 않는 공개 키 교환을 용이하게 하기 위해 디렉토리 서비스가 필요할 수 있다.

발명의 상세한 설명

<2> 본 시스템은 공개적으로 이용가능한 인덱스 저장소(publicly available index store)에서 인증된 연락처 정보를 게시(publish)할 수 있다. 또한 본 시스템은, 이 연락처 정보를 검색(retrieve)하고, 그것에 대한 유효성 검사(validate)를 행하는 방법을 제공할 수 있다. 청구하는 방법 및 시스템은 서버는 선택적인(optional) 클라이언트 기반일 수 있다. 이 공개적으로 이용가능한 인덱스 저장소는 피어-투-피어 네트워크에서 사용되는 분산된 해시 테이블(distributed hash table)일 수 있다. 본 시스템은 서버가 사용가능하지 않거나 또는 서버 신뢰도가 최소한일 수 있는 기타 보안 디렉토리 서비스 애플리케이션에서 사용될 수 있다.

<3> 한 실시예에서, 본 시스템은 일반적인 메시지 게시 시스템으로서 사용될 수 있다. 또 다른 실시예에서, 본 시스템을 사용하여 게시된 레코드가 의도하는 수신인에 의해서만 검색되고 판독될 수 있는 선택적인 게시(selective publishing)를 제공할 수 있다.

실 시 예

<16> 이하에서는 다수의 상이한 실시예에 대한 상세한 설명을 개시하지만, 이러한 설명의 법률적 범위는 본 명세서의 끝 부분에 개시되는 특허청구범위의 용어들에 의해 제한된다는 점이 이해되어야 한다. 상세한 설명은 단지 예

시적인 것으로 고려되어야 하고, 모든 가능한 실시예들을 설명하는 것은 아니며, 이는 비록 불가능하지 않더라도 모든 가능한 실시예들을 설명한다는 것은 실용적이지 않기 때문이다. 현재의 기술 또는 본 특허의 출원일 이후에 개발된 기술들을 사용하여 다수의 대안적인 실시예들이 구현될 수 있지만, 이러한 것들도 역시 본 발명의 특허청구범위의 범위에 포함되는 것이다.

<17> "본 명세서에서 사용될 때, 용어 '____'는 ...을 의미하도록 여기에서 정의된다"라는 문장 또는 이와 유사한 문장을 사용하여 본 명세서에서 명시적으로 정의되지 않는 한, 이러한 용어는 명시적으로든 또는 암시적으로든, 그것의 일반적인 의미 또는 보통의 의미 이상으로, 그 용어의 의미를 제한하려는 의도는 아니며, 이러한 용어가 본 명세서의 임의의 섹션에 있는 임의의 문장(청구항의 언어가 아니라)에 기초하여 범위가 제한되도록 해석되어서는 안 된다는 것 또한 이해할 것이다. 본 명세서의 끝 부분에 있는 청구범위에 언급된 임의의 용어가 단일 의미로 일관된 방식으로 본 명세서에서 지칭되는 점에서, 이는 단지 독자들을 혼동시키지 않도록 단순 명료하게 기술한 것으로, 이러한 청구범위의 용어가 암시적으로든 또는 다르게든, 그 단일 의미로 제한되는 것은 아니다. 마지막으로, 임의의 구조의 언급 없이 "수단"이라는 단어와 기능을 언급함으로써 청구항의 구성요소가 정의되지 않는 한, 임의의 청구항의 구성요소의 범위가 U.S.C.§112, 6번째 항의 적용에 기초하여 해석되어야 하는 것은 아니다.

<18> 도 1은 청구하는 방법 및 장치의 블록들에 대한 시스템이 구현되기에 적합한 컴퓨팅 시스템 환경(100)의 일례를 도시하고 있다. 컴퓨팅 시스템 환경(100)은 적합한 컴퓨팅 환경의 일례에 불과하며, 청구항의 방법 및 장치의 용도 또는 기능성의 범위에 관해 어떤 제한을 암시하고자 하는 것이 아니다. 컴퓨팅 환경(100)이 예시적인 운영 환경(100)에 도시된 컴포넌트들 중 임의의 하나 또는 그 컴포넌트들의 임의의 조합과 관련하여 어떤 의존성 또는 요구사항을 갖는 것으로 해석되어서는 안 된다.

<19> 청구하는 방법 및 장치의 블록들은 많은 기타 범용 또는 특수 목적의 컴퓨팅 시스템 환경 또는 구성에서 동작할 수 있다. 청구항의 방법 또는 장치에서 사용하는 데 적합할 수 있는 잘 알려진 컴퓨팅 시스템, 환경 및/또는 구성의 예로는 퍼스널 컴퓨터, 서버 컴퓨터, 핸드-헬드 또는 랩톱 장치, 멀티프로세서 시스템, 마이크로프로세서 기반 시스템, 셋톱 박스, 프로그램가능한 가전제품, 네트워크 PC, 미니컴퓨터, 메인프레임 컴퓨터, 상기 시스템들이나 장치들 중 임의의 것을 포함하는 분산 컴퓨팅 환경, 기타 등등이 있지만 이에 제한되는 것은 아니다.

<20> 청구하는 방법 및 장치의 블록들은 일반적으로 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터 실행가능 명령어와 관련하여 기술될 것이다. 일반적으로, 프로그램 모듈은 특정 태스크를 수행하거나 특정 추상 데이터 유형을 구현하는 루틴, 프로그램, 객체, 컴포넌트, 데이터 구조 등을 포함한다. 방법 및 장치는 또한 통신 네트워크를 통해 연결되어 있는 원격 처리 장치들에 의해 태스크가 수행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 메모리 저장 장치를 비롯한 로컬 및 원격 컴퓨터 저장 매체 둘 다에 위치할 수 있다.

<21> 도 1과 관련하여, 청구하는 방법 및 장치의 블록들을 구현하는 예시적인 시스템은 컴퓨터(110) 형태의 범용 컴퓨팅 장치를 포함한다. 컴퓨터(110)의 컴포넌트들은 처리 장치(120), 시스템 메모리(130), 및 시스템 메모리를 비롯한 각종 시스템 컴포넌트들을 처리 장치(120)에 연결시키는 시스템 버스(121)를 포함하지만 이에 제한되는 것은 아니다. 시스템 버스(121)는 메모리 버스 또는 메모리 컨트롤러, 주변 장치 버스 및 각종 버스 아키텍처 중 임의의 것을 이용하는 로컬 버스를 비롯한 몇몇 유형의 버스 구조 중 어느 것이라도 될 수 있다. 예로서, 이러한 아키텍처는 ISA(industry standard architecture) 버스, MCA(micro channel architecture) 버스, EISA(Enhanced ISA) 버스, VESA(video electronics standard association) 로컬 버스, 그리고 메자닌 버스(mezzanine bus)로도 알려진 PCI(peripheral component interconnect) 버스 등을 포함하지만 이에 제한되는 것은 아니다.

<22> 컴퓨터(110)는 통상적으로 각종 컴퓨터 판독가능 매체를 포함한다. 컴퓨터(110)에 의해 액세스 가능한 매체는 그 어떤 것이든지 컴퓨터 판독가능 매체가 될 수 있고, 이러한 컴퓨터 판독가능 매체는 휘발성 및 비휘발성 매체, 이동식 및 비이동식 매체를 포함한다. 예로서, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 포함하지만 이에 제한되는 것은 아니다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보를 저장하는 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성, 이동식 및 비이동식 매체를 포함한다. 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술, CD-ROM, DVD(digital versatile disk) 또는 기타 광 디스크 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 또는 컴퓨터(110)에 의해 액세스되고 원하는 정보를 저장할 수 있는

임의의 기타 매체를 포함하지만 이에 제한되는 것은 아니다. 통신 매체는 통상적으로 반송파(carrier wave) 또는 기타 전송 메커니즘(transport mechanism)과 같은 피변조 데이터 신호(modulated data signal)에 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터 등을 구현하고 모든 정보 전달 매체를 포함한다. "피변조 데이터 신호"라는 용어는, 신호 내에 정보를 인코딩하도록 그 신호의 특성들 중 하나 이상을 설정 또는 변경시킨 신호를 의미한다. 예로서, 통신 매체는 유선 네트워크 또는 직접 배선 접속(direct-wired connection)과 같은 유선 매체, 그리고 음향, RF, 적외선, 기타 무선 매체와 같은 무선 매체를 포함하지만 이에 제한되는 것은 아니다. 상술된 매체들의 모든 조합이 또한 컴퓨터 판독가능 매체의 영역 안에 포함되는 것으로 한다.

<23> 시스템 메모리(130)는 판독 전용 메모리(ROM)(131) 및 랜덤 액세스 메모리(RAM)(132)와 같은 휘발성 및/또는 비휘발성 메모리 형태의 컴퓨터 저장 매체를 포함한다. 시동 중과 같은 때에, 컴퓨터(110) 내의 구성요소들 사이의 정보 전송을 돕는 기본 루틴을 포함하는 기본 입/출력 시스템(BIOS)(133)은 통상적으로 ROM(131)에 저장되어 있다. RAM(132)은 통상적으로 처리 장치(120)가 즉시 액세스 할 수 있고 및/또는 현재 동작시키고 있는 데이터 및/또는 프로그램 모듈을 포함한다. 예로서, 도 1은 운영 체제(134), 애플리케이션 프로그램(135), 기타 프로그램 모듈(136) 및 프로그램 데이터(137)를 도시하고 있지만 이에 제한되는 것은 아니다.

<24> 컴퓨터(110)는 또한 기타 이동식/비이동식, 휘발성/비휘발성 컴퓨터 저장 매체를 포함한다. 단지 예로서, 도 1은 비이동식·비휘발성 자기 매체에 기록을 하거나 그로부터 판독을 하는 하드 디스크 드라이브(141), 이동식·비휘발성 자기 디스크(152)에 기록을 하거나 그로부터 판독을 하는 자기 디스크 드라이브(151), CD-ROM 또는 기타 광 매체 등의 이동식·비휘발성 광 디스크(156)에 기록을 하거나 그로부터 판독을 하는 광 디스크 드라이브(155)를 포함한다. 예시적인 운영 환경에서 사용될 수 있는 기타 이동식/비이동식, 휘발성/비휘발성 컴퓨터 저장 매체로는 자기 테이프 카세트, 플래시 메모리 카드, DVD, 디지털 비디오 테이프, 고상(solid state) RAM, 고상 ROM 등이 있지만 이에 제한되는 것은 아니다. 하드 디스크 드라이브(141)는 통상적으로 인터페이스(140)와 같은 비이동식 메모리 인터페이스를 통해 시스템 버스(121)에 접속되고, 자기 디스크 드라이브(151) 및 광 디스크 드라이브(155)는 통상적으로 인터페이스(150)와 같은 이동식 메모리 인터페이스에 의해 시스템 버스(121)에 접속된다.

<25> 위에서 설명되고 도 1에 도시된 드라이브들 및 이들과 관련된 컴퓨터 저장 매체는, 컴퓨터(110)를 위해, 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 및 기타 데이터를 저장한다. 도 1에서, 예를 들어, 하드 디스크 드라이브(141)는 운영 체제(144), 애플리케이션 프로그램(145), 기타 프로그램 모듈(146), 및 프로그램 데이터(147)를 저장하는 것으로 도시되어 있다. 여기서 주의할 점은 이들 컴포넌트가 운영 체제(134), 애플리케이션 프로그램(135), 기타 프로그램 모듈(136), 및 프로그램 데이터(137)와 동일하거나 그와 다를 수 있다는 것이다. 이에 관해, 운영 체제(144), 애플리케이션 프로그램(145), 기타 프로그램 모듈(146) 및 프로그램 데이터(147)에 다른 번호가 부여되어 있다는 것은 적어도 이들이 다른 사본(copy)이라는 것을 나타내기 위한 것이다. 사용자는 키보드(162), 및 마우스, 트랙볼(trackball) 또는 터치 패드와 같은 포인팅 장치(161) 등의 입력 장치를 통해 명령 및 정보를 컴퓨터(110)에 입력할 수 있다. 다른 입력 장치(도시 생략)로는 마이크, 조이스틱, 게임 패드, 위성 안테나, 스캐너 등을 포함할 수 있다. 이들 및 기타 입력 장치는 종종 시스템 버스에 결합된 사용자 입력 인터페이스(160)를 통해 처리 장치(120)에 접속되지만, 병렬 포트, 게임 포트 또는 USB(universal serial bus) 등의 다른 인터페이스 및 버스 구조에 의해 접속될 수도 있다. 모니터(191) 또는 다른 유형의 디스플레이 장치도 비디오 인터페이스(190) 등의 인터페이스를 통해 시스템 버스(121)에 접속될 수 있다. 모니터 외에, 컴퓨터는 스피커(197) 및 프린터(196) 등의 기타 주변 출력 장치를 포함할 수 있고, 이들은 출력 주변장치 인터페이스(195)를 통해 접속될 수 있다.

<26> 컴퓨터(110)는 원격 컴퓨터(180)와 같은 하나 이상의 원격 컴퓨터로의 논리적 접속을 사용하여 네트워크화된 환경에서 동작할 수 있다. 원격 컴퓨터(180)는 또 하나의 퍼스널 컴퓨터, 서버, 라우터, 네트워크 PC, 피어 장치 또는 기타 통상의 네트워크 노드일 수 있고, 통상적으로 컴퓨터(110)와 관련하여 상술된 구성요소들의 대부분 또는 그 전부를 포함하지만, 도 1에는 메모리 저장 장치(181) 만이 도시되어 있다. 도 1에 도시된 논리적 접속으로는 LAN(171) 및 WAN(173)이 있지만, 기타 네트워크를 포함할 수도 있다. 이러한 네트워킹 환경은 사무실, 전사적 컴퓨터 네트워크(enterprise-wide computer network), 인트라넷, 및 인터넷에서 일반적인 것이다.

<27> LAN 네트워킹 환경에서 사용될 때, 컴퓨터(110)는 네트워크 인터페이스 또는 어댑터(170)를 통해 LAN(171)에 접속된다. WAN 네트워킹 환경에서 사용될 때, 컴퓨터(110)는 통상적으로 인터넷과 같은 WAN(173)을 통해 통신을 설정하기 위한 모뎀(172) 또는 기타 수단을 포함한다. 내장형 또는 외장형일 수 있는 모뎀(172)은 사용자 입력 인터페이스(160) 또는 기타 적절한 메커니즘을 통해 시스템 버스(121)에 접속된다. 네트워크화된 환경에서, 컴

퓨터(110) 또는 그의 일부와 관련하여 기술된 프로그램 모듈은 원격 메모리 저장 장치에 저장될 수 있다. 예로서, 도 1은 원격 애플리케이션 프로그램(185)이 원격 메모리 장치(181)에 있는 것으로 도시하고 있지만 이에 제한되는 것은 아니다. 도시된 네트워크 접속은 예시적인 것이며 이 컴퓨터들 사이에 통신 링크를 설정하는 기타 수단이 사용될 수 있다는 것을 이해할 것이다.

<28> 피어-투-피어(Peer-to-Peer;P2P) 시스템은 중앙 서버의 도움 없이, 비중앙화(decentralized) 방식으로 서로 통신하는 노드들의 네트워크를 채용한다. 피어-투-피어 네트워크의 각 노드(예를 들면, 애플리케이션 또는 장치)는 직접 접속을 통해 네트워크 상의 다른 노드와 통신할 수 있거나, 또는 각 노드는 하나 이상의 중간 노드들을 이용하여 의도하는 노드로 통신을 중계하여(relay) 간접적으로 통신할 수 있다.

<29> 도 2는 P2P 시스템(200)의 하이 레벨의 도면이다. 시스템(200)은 피어 엔티티(202-212)의 컬렉션(collection)을 포함한다. 피어 엔티티(202-212)는 하나의 네트워크 또는 네트워크들의 조합을 통하여 서로 결합되는 퍼스널 컴퓨터 장치들일 수 있다. 도 2는 각 피어 엔티티(202-212)가 나머지 모든 피어 엔티티(202-212)와 접속되어 있는 예를 도시한다. 다른 경우에서, 하나 이상의 피어 엔티티(202-212)는 하나 이상의 중간 참가자(202-212)를 통해 다른 피어 엔티티(202-212)에 접속될 수 있다. 그러나, 피어-투-피어 네트워크상에서 보안 통신(secure communication)을 제공하기 위해, 피어 노드들 간에 우선 보안 접속이 확립될 필요가 있을 수 있다.

<30> 접속 보안(connection security)은 본 기술분야에서 통상적으로 알려져 있는 바와 같이, 대칭 키 암호화 프로세스(symmetric key encryption process)에 기초할 수 있다. 그러나, 이 암호화 보안을 구현하기 위해, 피어 엔티티는, 초기에 보안 접속이 확립되는 것을 가능하게 하는 증명서(certificate) 및/또는 공개 키를 먼저 교환할 필요가 있을 수 있다. 도 3에 도시된 바와 같은 일부 기존의 시스템에서, 이러한 교환은, 사용자(301, 302, 303)가 자신의 증명서(304, 305, 306) 및/또는 공개 키를 디렉토리 서버(300)에 게시할(post) 수 있는 중앙 디렉토리 서버(300)를 이용하여 용이하게 될 수 있다. 디렉토리 서비스(307)는, 키(309)로 사용되는 사용자명(username) 또는 다른 식별자로 인덱스된(indexed) 증명서 및/또는 공개 키 레코드(308)를 포함하는 데이터베이스 테이블일 수 있다. 디렉토리 서버(300)로 접속하여 디렉토리 서비스(307)로의 액세스가 허용되는 사용자는, 목표 사용자의 식별자를 이용하여 목표 사용자를 검색(lookup)하고, 그 목표 사용자에 대응하는 공개 키를 획득할 수 있다. 이 접근 방법은 서버(300)로의 접속성(connectivity), 디렉토리 서버(300)에의 명시적인 등록(explicit signup with the directory server) 및 디렉토리 서버(300)에서의 신뢰를 필요로 할 수 있다. 게다가, 누군가는 서버와 같은 호스팅 비용을 져야만 한다. 사용자(303)가 원격 장소로부터 접속하고 있는 경우, 인터넷 접속성(301)이 추가로 요구될 수 있다. 서버 등록 프로세스는 디렉토리 서버(300)에서의 신뢰를 증진시키는 데에 사용되는 사용자 계정을 수반할 수 있다. 예를 들어, 임의의 사용자가 서버(300)에 액세스할 수 있으면, 특히 공개 키와 같은 보안 정보가 게시되어 교환된다면, 서버(300)는 좀 더 위태로운(compromised) 것으로 보일 수 있다. 게다가, 임시적인 네트워크인 애드 혹을 위해 디렉토리 서버를 생성하는 것은, 이들 네트워크의 일시적인 속성과 디렉토리 서버를 셋업하는 데 있어서의 곤란성으로 인해 실용적이지 않을 수 있다. 애드 혹 피어-투-피어 네트워크에 대한 가능한 차선책은, 이메일을 통해, 또는 증명서/공개 키를 포함하는 디스켓을 목표 멤버에게 물리적으로 전송하거나 또는 메일링하는 것과 같은 오프 네트워크 프로세스(off network process)를 통해 공개 키를 교환하는 것일 수 있다. 이것은 피어 엔티티가 서버에 독립적이며 보안 링크를 확립하는 것을 가능하게 한다. 그러나, 이것은 번거롭고(cumbersome) 에러를 일으키기 쉬울(error-prone)일 수 있다.

<31> 청구하는 서버-독립적인 인덱싱 프로세스(claimed server-independent indexing process)의 실시예는 도 4에 도시되어 있는 분산된 해시 테이블(distributed hash table:DHT)(400)과 같은 서버가 없는 인덱스 저장소를 이용할 수 있다. 이 분산된 해시 테이블(400)은 피어-투-피어 네트워크(405)를 형성하는 피어 엔티티들(401-404)의 그룹을 통해 유지될 수 있다. 분산된 해시 테이블 내의 엔트리들은 예를 들면 해시 함수를 이용하여 논리적으로 분할되거나 또는 그룹핑(grouping)될 수 있다. 해시 함수는 특정한 조직화된 방식으로 레코드들을 함께 묶어서(clump), 더 효율적으로 검색할 수 있게 한다. DHT는 두 개의 주요 속성 : 1) 복수의 노드(예를 들면, 노드(401-404))에 걸친 테이블(예를 들면, 테이블(400))의 분산 및 2) 레코드들을 게시(publish)하고 검색하기 위한 방법을 제공하는 라우팅 메커니즘(도시 생략)을 지닐 수 있다. 라우팅 메커니즘 및 분산은 Chord, PNRP, Pastry, Tapestry 등과 같은 오버레이 프로토콜(overlay protocol)에 의해 다루어질(managed) 수 있다. 청구항들의 실시예에 따른 인덱스 저장소를 제공하기 위해 DHT가 사용될 수 있으나, 서버 기반 인덱스를 비롯하여 피어 엔티티들 그룹에 의해 쉽게 액세스될 수 있는 것이라면 어떠한 인덱스 저장소도 사용될 수 있음을 강조한다. 서버 기반 인덱스의 경우, 청구하는 시스템은 보안되지 않은 인덱스 저장소에 대해 필수 보안 수준을 제공할 수 있기 때문에 서버 단독(alone)으로부터 요구되는 신뢰 수준(level of trust)을 줄일 수 있다.

<32> 청구하는 서버-독립적인 인덱싱 프로세스의 실시예는 도 5에 도시되는 것과 같은 특정 레코드 포맷을 사용할 수 있다. 도 5는, 게시자(publisher)가 연락처 정보(contact information)(501), 게시자의 공개 키(502) 및, 게시자의 개인 키를 이용한 연락처 정보의 서명(signature)(503)을 포함하는 레코드(500)를 인덱스 저장소에 게시할 수 있다. 대안으로, 서명은 연락처 정보와 공개 키의 조합일 수 있다. 이 레코드는 레코드 키(504)로 인덱싱될 수 있다. 한 실시예에서, 레코드의 키(504)는 CUI(cryptographically unique identifier)일 수 있다. CUI는 두 개의 주요 속성을 갖는다. 첫 번째로는, CUI는 통계적으로 고유하며, 두 번째로, CUI는 게시자 공개 키(502)와 같은 특정 사용자의 공개 키에 해당할 수 있다는 것이다. 일반적인 데이터베이스 인덱싱 방식과 마찬가지로, 레코드 키는 엔티티 엔트리들의 중복을 막기 위해 고유해야 한다. 따라서, CUI는 특정 상황 또는 특정 애플리케이션에 고유할 가능성이 높게 되도록 도출된 것일 수 있다. 예를 들면, 몇몇 멤버들만이 있는 피어 그룹에서는, 그룹 사이즈로 봐서 CUI가 동일한 멤버의 공개 키로부터 도출될 수 있는 확률이 있을 것 같지 않을 경우(if the probability that a cryptographically unique identifier may be derived from the same member public key is unlikely for the group size), CUI는 통계적으로 고유할 수 있다.

<33> CUI는 해시 또는 암호화 알고리즘과 같은 알고리즘을 이용하여 공개 키로부터 도출될 수 있다. 이 알고리즘을 이용하여 CUI가 그 공개 키에 해당하는지 또는 그 공개 키와 일치하는지를 검증(verify)할 수 있다. 한 실시예에서, CUI는, 발명의 명칭이 "Callsigns"인 미국 특허 출원 제10/882079호에 개시되어 있는 P2P 시스템에서 사용되는 피어 이름과 같은 더 짧으며 사용자가 더 관리하기 쉬운 형태로 공개 키와 같은 더 긴 사용자 식별자를 나타내는 데에 사용될 수 있다.

<34> 도 5의 레코드는, 도 4의 DHT(400)와 같은 인덱스 저장소에 연락처 정보를 게시하는 데에 사용될 수 있다. CUI 키(504)는 각 레코드(500)를 찾아(locate) 그 연락처 정보(501)와 공개 키(502)를 검색하는 데에 사용될 수 있다. 이 실시예에서, 게시된 정보는 공개적일 수 있으며, 즉 서명을 제외하고는, 암호화되어 있지 않은 경우가 있다. 그러나, 이하에 설명된 다른 실시예는 게시된 정보 중 일부를 암호화할 수 있다. 또한, 이 실시예에서는 레코드(500)를 이용하여 공개 키(502)의 교환을 용이하게 하는 것을 도시하지만, 고유 메시지 게시가 사용될 수 있다면 어떠한 애플리케이션에서도 본 시스템이 사용될 수 있음을 강조한다. 예를 들면, 연락처 정보(501) 대신, 사용자 CUI(504)에 대하여 임의의 메시지가 게시될 수 있다.

<35> 도 6은 청구항들의 실시예에 따른 일반적인 게시 프로세스를 도시한다. 해시 함수와 같은 알고리즘을 이용하여, 소정의 사용자의 공개 키(601)에 대해 CUI가 생성될 수 있다. 무슨 알고리즘이 사용되었는지, CUI는, 그것을 생성하기 위해 사용되었던 공개 키에 대응하도록, 유효성 검사될 수 있다는 것을 유의하는 것이 중요하다. 연락처 정보 또는 기타 메시지 데이터 및 게시자의 공개 키의 레코드가 구축될 수 있으며(602), 연락처 정보 및/또는 게시자의 공개 키는 (공개 키에 대응할 수 있는) 게시자의 개인 키에 의해 서명될 수 있다(603). 연락처 정보, 공개 키 및 서명을 포함하는 레코드는 공개적으로 이용가능한 인덱스 내에 삽입될 수 있다(604). 레코드는 게시자의 공개 키에 대응하는 CUI에 의해 인덱스될 수 있다.

<36> 도 7은 청구항들의 실시예에 따른 검색 프로세스를 도시한다. 제2 피어와 접속하기를 원하는 사용자는 제2 피어의 CUI를 획득할 수 있다(701). CUI는 이메일을 통해 또는 오프 네트워크 프로세스(예를 들면, 일반 우편 서비스(snail mail), 구두 통신, 명함 등)를 통해 대역 외에서(out of band) 획득될 수 있다. 이후, CUI를 이용하여 그 CUI에 매핑된 레코드를 인덱스 저장소에서 검색(lookup)할 수 있다(702). 상술된 바와 같이, 레코드는 키, 특정 메시지 정보(연락처 정보) 및 서명을 포함할 수 있다.

<37> 이후 사용자는 인덱스 저장소에 질의하여 CUI에 기초하여 레코드를 검색(retrieve)할 수 있다(703). 일단 CUI가 검색(retrieve)되면, CUI와 공개 키가 서로 대응하도록 보장하기 위해, 레코드에 포함된 공개 키를 이용하여 CUI를 검증할 수 있다(704). 이 프로세스 블록은 레코드가 CUI에 대응하는지를 검증하는 데에 사용될 수 있다. CUI는 임의의 방식으로 공개 키에 통계적으로 고유하도록 만들어질 수 있다. 한 실시예에서, 피어 통신 시스템은, 예컨대, 인지된 해시 함수를 이용하여 공통 매핑 프로세스를 사전 확립할 수 있다. 이러한 초기의 검증 프로세스는 레코드가 실제로 소정의 CUI에 대응할 수 있다는 것을 보장하는 것을 돕는다.

<38> CUI가 제대로 매핑되면, 레코드의 서명을 사용하여, 이 서명이 게시자의 대응하는 개인 키에 의해 서명되어 있는지의 여부를 판정한다(705). 이것은 게시자가 암호화에 사용된 공개 키에 대응하는 개인 키를 소유한다고 가정했을 때, 메시지가 게시자로부터 비롯되었다는 증거를 제공함으로써 메시지를 인증할 수 있다.

<39> 레코드/메시지가 제대로 서명되면, 레코드의 연락처 정보에 관하여 메시지 포맷 및/또는 구문(syntax) 점검이 수행될 수 있다(706). 이것은, 예를 들면, 메시지가 해킹되지 않아서 서명과 일치함을 보장하는 데에 사용될 수 있다. 암호화된 서명과 일치하는 해킹된 메시지를 제공하는 것은 통계적으로 어려울 수는 있으나 불가능하

지는 않다. 그러나, 해킹에 의해 의도하는 포맷 또는 예상되는 포맷에 따르지 않는 메시지가 초래될 수 있다. 따라서, 메시지 포맷이 예상되는 포맷에 부합하는지의 여부를 판정하기 위해 메시지의 제1 점검이 행해질 수 있다. 예를 들면, 연락처 정보가 통신되는 경우, 이 연락처 정보는 10개 문자 포맷(ten character format)을 필요로 할 수 있다. 레코드 포맷이 이 10개 문자 포맷을 제공하지 않는다면, 누군가가 또는 무엇인가가 이 메시지에 간섭(tamper)했을 수 있다(711).

<40> 대안으로 또는 추가로, 메시지의 의미론이 점검될 수 있다. 예를 들면, 연락처 정보가 옵션들의 리스트와 이들 옵션들 간의 특별한 관계로 한정될 수 있다. 그러므로, 포맷이 두 개의 엔트리를 필요로 하고 제1 엔트리가 제2 엔트리(의미론)에 관련된 것이며, 이 엔트리들이 이 예상되는 포맷과 일치하지 않는다면, 누군가가 또는 무엇인가가 이 메시지에 간섭했을 수 있다(711).

<41> 모든 검증 프로세스(704, 705, 706)를 성공적으로 완료했으면, 레코드는 진짜이므로(authentic), 사용될 수 있고(707), 예를 들면 통신 링크를 확립하는 데에 공개 키가 사용될 수 있다. 검증 단계(704, 705, 706) 중 하나라도 실패하면, 누군가가 또는 무엇인가가 이 메시지에 간섭했을 수 있다(711). 공개 키 교환 시스템의 경우, 접속이 거절될 수 있다.

<42> 도 8에 도시된 또 다른 실시예에서는, 레코드(800)에 지속기간 파라미터(duration parameter)(801)가 포함될 수 있다. 이 지속기간 파라미터(801)는 상술된 인증 프로세스에서 사용되는 암호화 수준에 대응할 수 있다. 예를 들면, 암호화 수준은 청구하는 시스템에서 사용되는 공개/개인 키 쌍을 생성하는 데에 사용되는 암호화 강도(encryption strength)에 대응할 수 있다. 암호화 강도가 높으면, 지속기간이 길 수 있고 그 반대일 수도 있다. 지속기간 파라미터(801)는 레코드의 유효함(validity)의 지속기간을 나타낼 수 있다. 따라서, 지속기간 파라미터(801)는 도 9에 도시된 검색(retrieval) 프로세스에서 사용될 수 있다. 도 9는 도 7과 동일한 프로세스를 도시하지만, 블록(908)이 추가되어 있으며, 이 블록(909)에서 지속기간 파라미터(801)에 의해 표시되는 지속기간(901)은 지속기간이 만료되었는지 여부에 관하여 점검된다. 지속기간 파라미터(801)가 만료된 경우, 레코드는 타협될(compromised) 수 있다(911). 그렇지 않을 경우, 레코드는 유효할 수 있다(907).

<43> 도 10 내지 도 12는, 목표로 하는(targeted) 제2 사용자만이 검색(retrieve)할 수 있는 데이터를 제1 사용자가 게시하는 것을 가능하게 하는 선택적인 게시(selective publication)이 사용될 수 있는 또 다른 실시예를 도시한다. 이 선택적인 게시 실시예에서, 도 10에 도시된 레코드(1001)가 사용될 수 있다. 레코드(1001)는 두 개의 CUI(1003, 1004)의 조합으로부터 형성된 키(1002)를 포함할 수 있다. 제1 CUI(1003)는 제1 사용자와 관련될 수 있고, 제2 CUI(1004)는 제2 사용자와 관련될 수 있다. 이 조합은 단순히 제2 CUI를 제1 CUI에 첨부함으로써 형성될 수 있다. 이 레코드는 메시지 부(1005)와 지속기간 파라미터(1006)를 포함할 수 있다. 메시지(1005)는 게시자의 연락처 정보, 게시자의 공개 키 및 서명에 대한 데이터를 포함할 수 있다.

<44> 도 11은 도 10의 레코드(1001)를 이용하는 선택적인 게시 프로세스를 도시한다. 게시자은 공개 키로부터 자신의 CUI를 도출할 수 있고(1101), 선택된 수신인의 CUI의 획득할 수 있고(1102), 메시지를 구축할 수 있고(1103), 게시자의 개인 키를 이용하여 메시지를 서명할 수 있고(1104) 및 CUI 조합 키(1101)에 기초하는 인덱스 내로 메시지를 삽입할 수 있다(1105). 게다가, 메시지는 의도하는 수신인의 공개 키를 이용하여 암호화될 수 있다(1106).

<45> 도 12는 블록(1201, 1202, 1203)이 추가되어 있는, 도 7과 유사한 선택적인 게시 프로세스에 대한 검색(retrieval) 프로세스를 도시한다. 게시된 레코드를 검색(retrieve)하기를 원하는 수신인은 우선 게시자의 CUI를 획득하고(1201), 조합된 CUI 키로 인덱스 저장소에서 레코드를 검색(lookup)한다(1202). 추가의 개선된 실시예에서, 메시지는 수신인의 공개 키를 이용하여 암호화될 수 있다. 따라서, 수신인만이 의도되는 데이터를 복호화(decrypt)할 수 있다. 수신인이 CUI 조합 키를 이용하여 메시지를 검색(retrieve)한 후, 수신인은 개인 키를 이용하여 우선 레코드를 복호화하고(1203), 그 후 검증 및 유효성 검사 프로세스는 도 7의 검증 및 유효성 검사 프로세스를 따른다. 이 선택적인 게시 실시예에서, (레코드를 암호화하는 데에 사용되었던) 수신인의 공개 키는, 게시자가 조합 키를 생성하기 위해 사용했던 수신인의 CUI로부터 결정될 수 있다.

<46> 상술된 실시예의 또 다른 개선에서, 키는 한 그룹의 피어에 의해 소유되는 그룹 공개 키일 수 있다. 이 실시예에서, 그룹의 임의의 멤버는 그룹 공개 키로 레코드를 검색(lookup)할 수 있으며, 인증 프로세스를 수행할 수 있다. 사용자 그룹은 레코드로 액세스할 수 있으며, 사용자 그룹은 게시된 메시지의 수신인으로서 특별이 목표로 될 수 있다.

<47> 상술된 특정 실시예가 공개 키 교환 디렉토리와 관련될 수 있으며, 연락처 정보가 다른 데이터를 나타낼 수 있

음을 강조해야 한다. 예를 들면, 연락처 정보 대신, 레코드는 일반적인 메시지 게시물(posting)일 수 있다. 따라서, 청구하는 시스템은 임의의 공개적으로 액세스가능한 인덱스 저장소 상의 일반적인 게시 시스템으로서 사용될 수 있다. 청구하는 시스템은 또한 공개 키 검색(lookup) 외에 디렉토리 서비스를 제공하는 데에 사용될 수 있다. 청구하는 시스템은 분산된 해시 테이블과 같은 기존의 분산된 인덱스 저장소들이 서버에 의존하지 않고 보안 디렉토리 서비스 워크(secured directory service work)로서 기능할 수 있게 한다.

<48> 게다가, 청구하는 시스템은 서버 보안이 최소한이어서 청구하는 시스템에 의해 제공되는 인증 프로세스를 필요로 할 수 있는 기존의 서버 기반 디렉토리에서도 사용될 수 있다. 피어 그룹 및 피어-투-피어 네트워크와 같은 애드 혹 네트워크에서, 서버 없는 공개 키 게시 및 검색(retrieval) 프로세스는, 호스트되며 전용인 서버가 디렉토리 서비스를 제공해야 하는 필요성을 줄임으로써, 이러한 네트워크의 생성을 더욱 효과적이 되게 할 수 있다. 청구하는 방법 및 시스템은 또한, 공개/개인 키 암호화 프로세스가 사용자가 서버에 명시적으로 서명해야 하는 필요성을 없앨 수 있기 때문에 사용자의 관여(involvement)를 최소화할 수 있다.

도면의 간단한 설명

<4> 도 1은 청구항에 따라 동작할 수 있는 컴퓨팅 시스템의 블록도를 도시하는 도면.

<5> 도 2는 일반적인 피어-투-피어 네트워크를 도시하는 도면.

<6> 도 3은 일반적인 디렉터 서버 및 서비스를 도시하는 도면.

<7> 도 4는 분산된 해시 테이블을 도시하는 도면.

<8> 도 5는 청구항의 실시예에서 사용되는 레코드를 도시하는 도면.

<9> 도 6은 게시 프로세스(publishing process) 실시예를 도시하는 도면.

<10> 도 7은 검색 프로세스(retrieval process) 실시예를 도시하는 도면.

<11> 도 8은 지속 기간 파라미터를 포함하는 수정된 레코드를 도시하는 도면.

<12> 도 9는 지속 기간 파라미터를 이용하는 또 다른 유효성 검사(validation) 프로세스를 도시하는 도면.

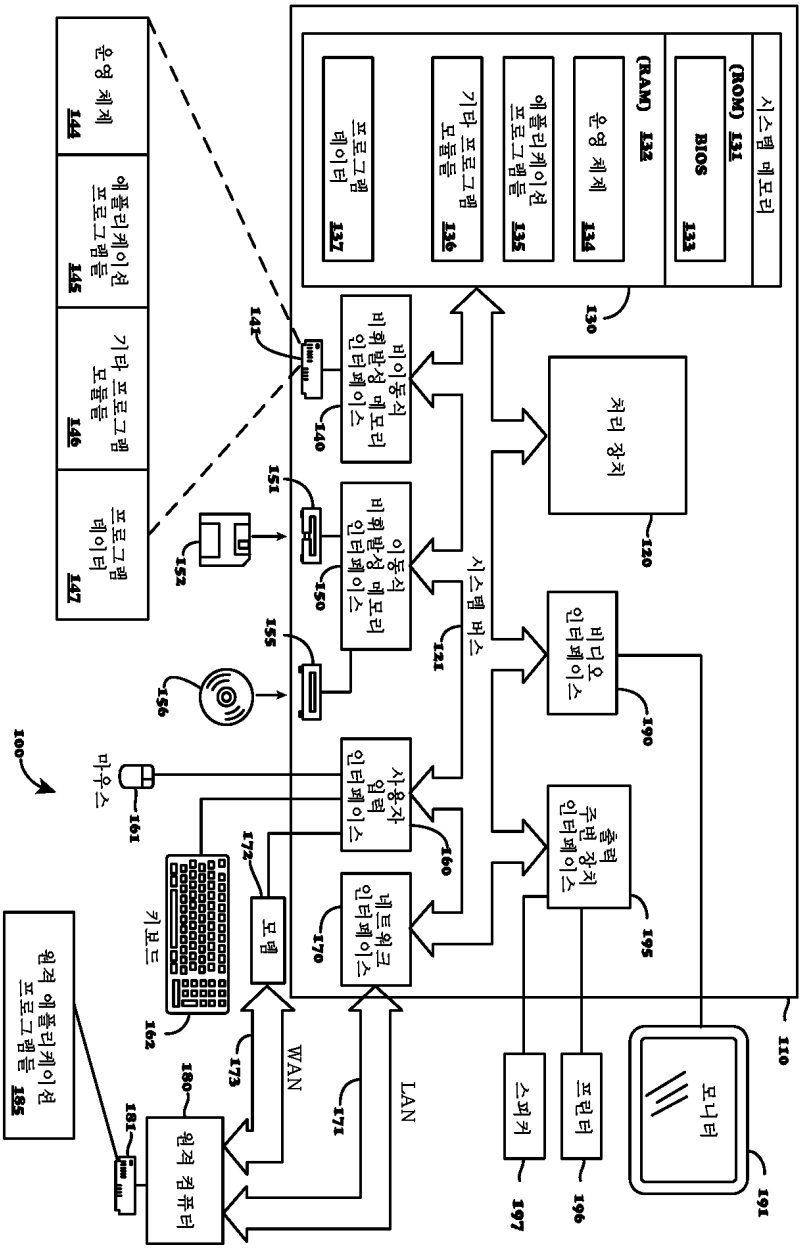
<13> 도 10은 선택적인 게시를 위한 수정된 레코드를 도시하는 도면.

<14> 도 11은 선택적인 게시를 위한 게시 프로세스 실시예를 도시하는 도면.

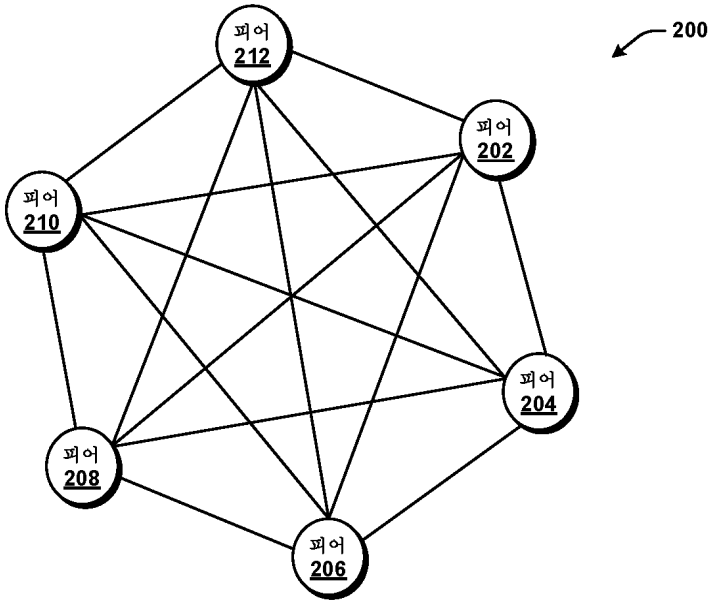
<15> 도 12는 선택적인 게시를 위한 검색 프로세스 실시예를 도시하는 도면.

도면

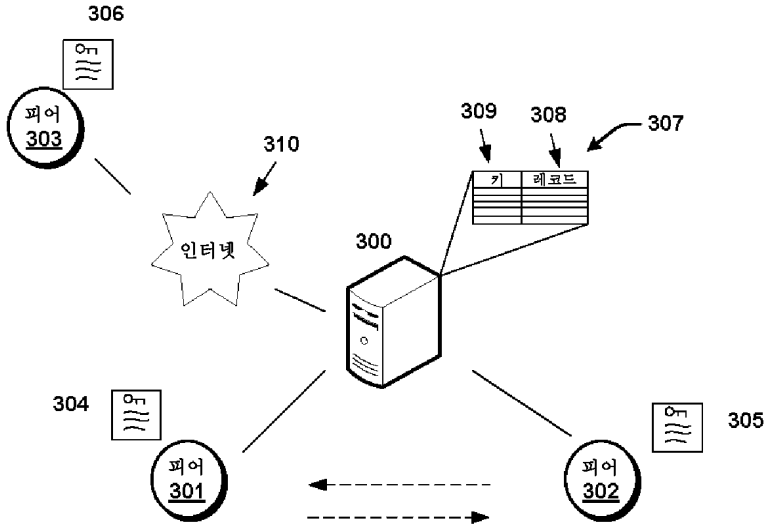
도면1


시스템 메모리
(ROM) 131
BIOS 133
(RAM) 132
운영 체제 134
에플리케이션 프로그램들 135
기타 프로그램 모듈들 136
프로그램 데이터 137
130
운영 체제 144
에플리케이션 프로그램들 145
기타 프로그램 모듈들 146
프로그램 데이터 147
비휘발성 메모리 인터페이스
140
141
이동식 비휘발성 메모리 인터페이스
150
151
152
155
156
처리 장치
120
시스템 버스
121
비디오 인터페이스
190
출력 주변 장치 인터페이스
195
사용자 입력 인터페이스
160
네트워크 인터페이스
170
모뎀
172
173
WAN
LAN
171
100
마우스
161
키보드
162
원격 에플리케이션 프로그램들 185
원격 컴퓨터
180
181
모니터
191
프린터
196
스피커
197
110

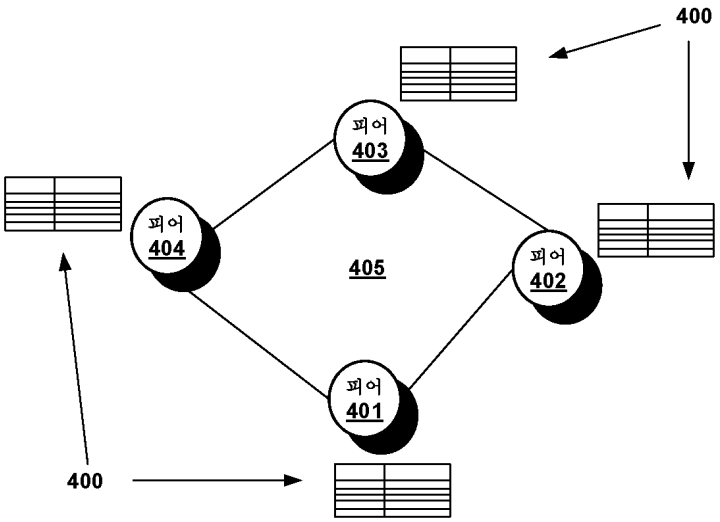
도면2


200
피어
212
피어
202
피어
210
피어
204
피어
208
피어
206

도면3


306
피어
303
310
309
308
307
키
레코드
인터넷
300
304
305
피어
301
피어
302

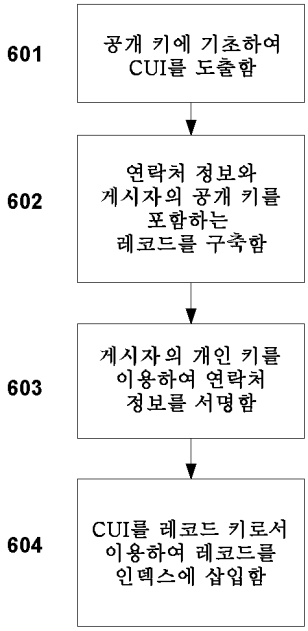
도면4


400
피어
403
피어
404
405
피어
402
피어
401
400

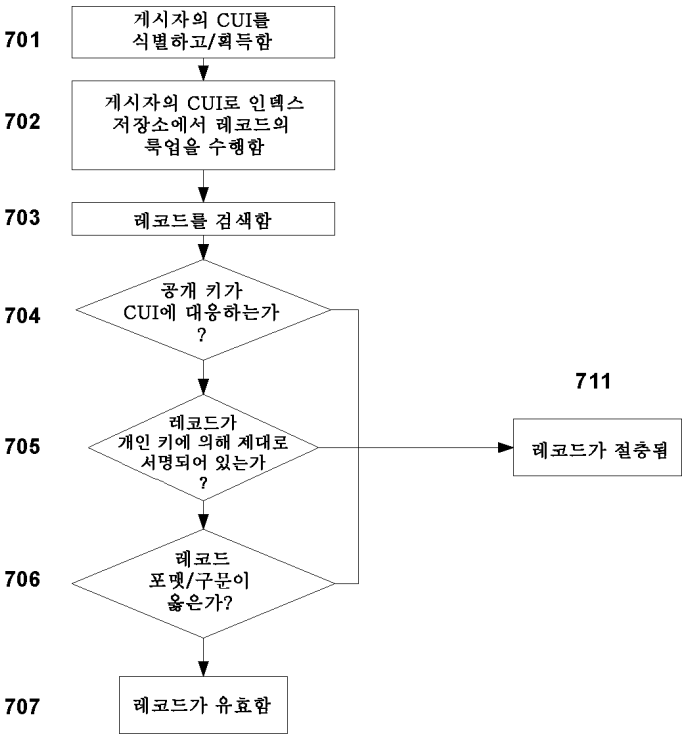
도면5


504
501
502
503
500
CUI
연락처 정보
게시자의 공개 키
서명

도면6


601
공개 키에 기초하여 CUI를 도출함
602
연락처 정보와 게시자의 공개 키를 포함하는 레코드를 구축함
603
게시자의 개인 키를 이용하여 연락처 정보를 서명함
604
CUI를 레코드 키로서 이용하여 레코드를 인덱스에 삽입함

도면7


701
게시자의 CUI를 식별하고/획득함
702
게시자의 CUI로 인덱스 저장소에서 레코드의 룩업을 수행함
703
레코드를 검색함
704
공개 키가 CUI에 대응하는가 ?
705
레코드가 개인 키에 의해 제대로 서명되어 있는가 ?
711
레코드가 절충됨
706
레코드 포멧/구문이 옳은가?
707
레코드가 유효함

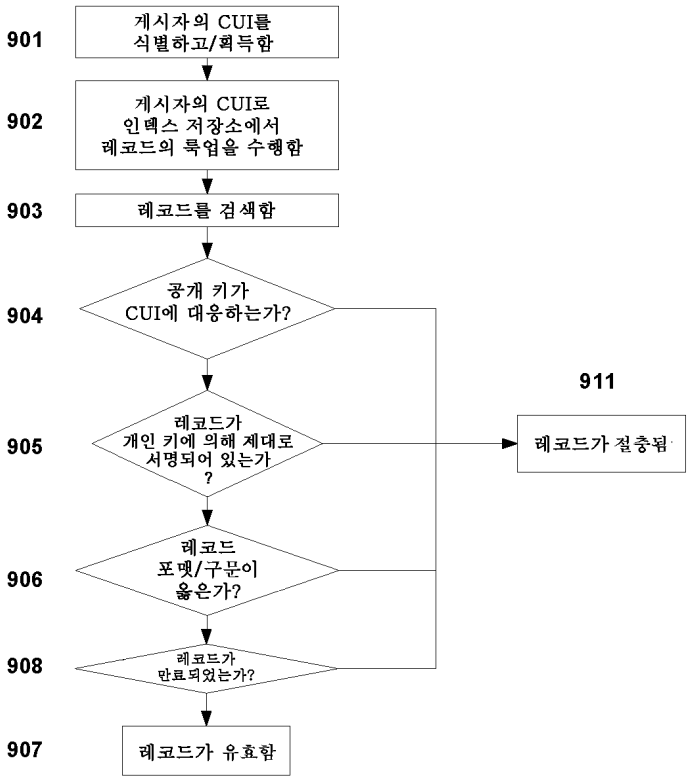
도면8

800 →

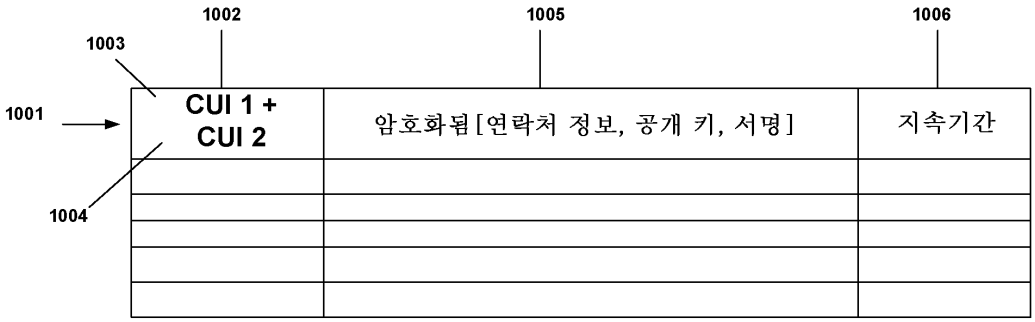
801 →

CUI	연락처 정보	공개 키	서명	지속기간

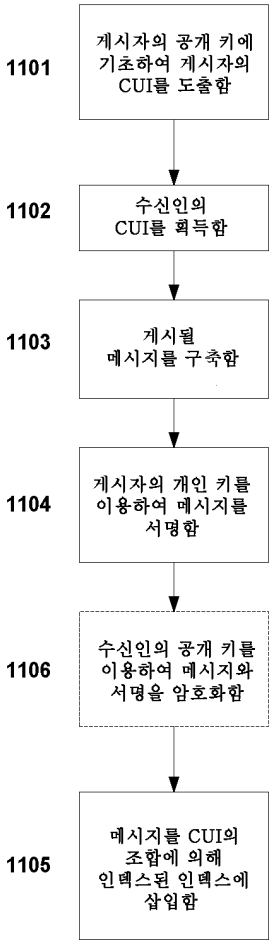
도면9



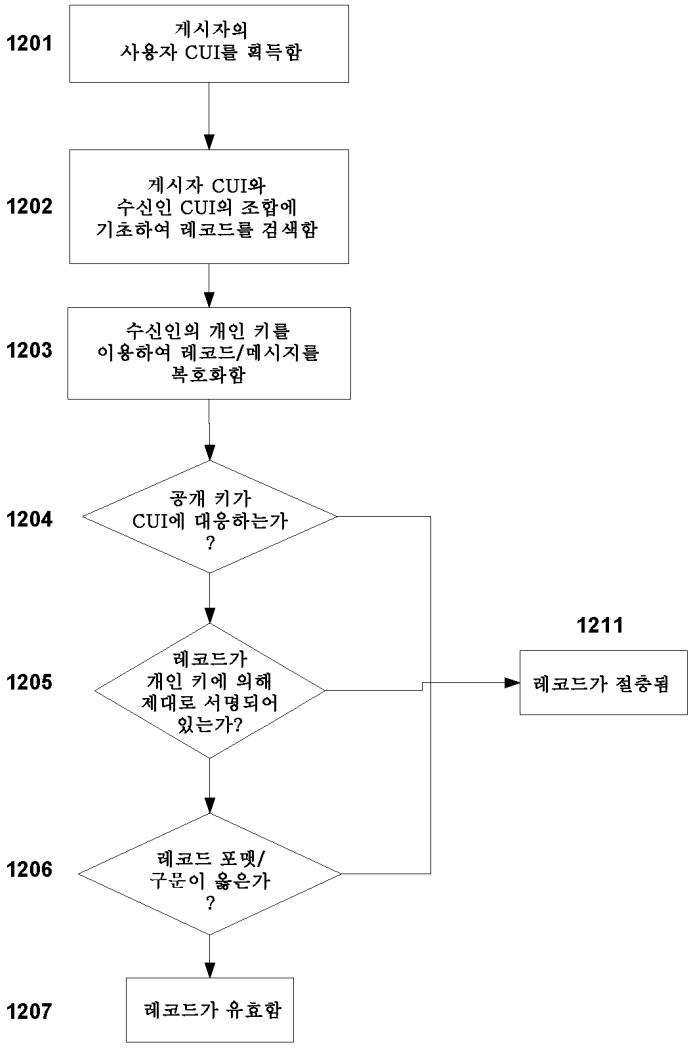
도면10


1002
1005
1006
1003
1001
CUI 1 +
CUI 2
암호화됨[연락처 정보, 공개 키, 서명]
지속기간
1004

도면11


1101
게시자의 공개 키에 기초하여 게시자의 CUI를 도출함
1102
수신인의 CUI를 획득함
1103
게시될 메시지를 구축함
1104
게시자의 개인 키를 이용하여 메시지를 서명함
1106
수신인의 공개 키를 이용하여 메시지와 서명을 암호화함
1105
메시지를 CUI의 조합에 의해 인덱스된 인덱스에 삽입함

도면12


1201
게시자의
사용자 CUI를 획득함
1202
게시자 CUI와
수신인 CUI의 조합에
기초하여 레코드를 검색함
1203
수신인의 개인 키를
이용하여 레코드/메시지를
복호화함
1204
공개 키가
CUI에 대응하는가
?
1205
레코드가
개인 키에 의해
제대로 서명되어
있는가?
1206
레코드 포맷/
구문이 옳은가
?
1207
레코드가 유효함
1211
레코드가 절충됨