(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
G06F 17/00 (2006.01)

(11) 공개번호 10-2006-0112182
(43) 공개일자 2006년10월31일

(21) 출원번호 10-2005-7008764
(22) 출원일자 2005년05월16일
번역문 제출일자 2005년05월16일
(86) 국제출원번호 PCT/US2004/024370
국제출원일자 2004년07월29일
(87) 국제공개번호 WO 2005/045579
국제공개일자 2005년05월19일

(30) 우선권주장 10/693,172 2003년10월23일 미국(US)

(71) 출원인 마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이

(72) 발명자 카메론, 김
미국 98004 워싱턴주 벨리뷰 사우스이스트 쇼랜드 드라이브 9328
난다, 아룬
미국 90874 워싱턴주 삼마미시 사우스이스트 5번 스트리트 23902
하첼, 도날드 제이.
미국 98015 워싱턴주 노스 벤드 사우스이스트 129번 스트리트45668
사타고판, 멀리
미국 98074 워싱턴주 삼마미시 노스이스트 32번 코트 20535
콴, 스투어트
미국 98052 워싱턴주 레드몬드 노스이스트 117번 스트리트 15722
브라세, 콜린
미국 98112 워싱턴주 시애틀 이. 매디슨 스트리트 2620
스미스, 월터
미국 98144 워싱턴주 시애틀 32번 애비뉴 에스 539
던, 멜리사
미국 98072 워싱턴주 우드인빌 노스이스트 169번 플레이스 19435

(74) 대리인 주성민
백만기
이중희

심사청구 : 없음

(54) 아이덴티티 인식 방법 및 시스템

요약

다양한 양상에 따라, 본 발명은 아이덴티티 정보 문서에 포함시킬 아이덴티티 정보를 자기 아이덴티티 정보 저장부로부터 선택하는 과정을 포함하는 아이덴티티 정보 문서 송신 방법 및 시스템을 제공한다. 선택된 아이덴티티 정보가 자기 아이덴티티 정보 저장부로부터 판독된다. 그와 같이 선택된 아이덴티티 정보 및 하나 이상의 키들을 포함하는 아이덴티티 정보

문서가 생성되고, 이는 그 아이덴티티 정보 문서에 포함되어 있는 키들 중 하나와 연관된 키를 이용하여 서명된다. 그런 다음, 그 아이덴티티 정보 문서가 수신자에게 송신된다. 아이덴티티 정보 문서 수신은 발신자로부터 서명된 아이덴티티 정보 문서를 수신하는 과정을 포함한다. 아이덴티티 정보 문서에 포함되어 전달된 아이덴티티 정보가 신뢰할 수 있는지 것인지 여부에 대한 판단이 행해진다. 아이덴티티 정보가 신뢰할 수 있는 것이라고 판단된 경우 그 아이덴티티 정보가 인식 아이덴티티 정보 저장부에 저장된다. 아이덴티티 정보가 신뢰할 수 없는 것이라고 판단된 경우 송신자로부터 검색된 아이덴티티 인식 번호를 그 수신된 아이덴티티 정보 문서에 기초하여 수신자에 의해서 생성된 아이덴티티 인식 번호와 비교한다. 아이덴티티 인식 번호가 검증되면, 그 아이덴티티 정보가 인식 아이덴티티 정보 저장부에 저장된다.

대표도

도 1

색인어

아이덴티티 인식, 아이덴티티 정보, 공개키, 비밀키, 컴퓨터 보안, 네트워크 보안

명세서

기술분야

본 발명은 일반적으로 컴퓨터 및 네트워크 보안 분야에 관한 것으로, 특히 이종 컴퓨터 시스템들 간 사용자-제어형 아이덴티티 정보(user-controlled identity information) 교환에 관한 것이다.

배경기술

컴퓨터 상에서 그 컴퓨터의 어떤 자원이 공유되어야 하는지에 관하여 아무런 표시도 하지 않는 그와 같은 컴퓨터 리소스들을 네트워크 전체에 걸쳐 사용자들 간에 공유하는 것이 때로는 바람직하다. 예컨대, 회사, 대학, 기타 기관들은 종업원, 학생, 기타 개인들이 사용할 소정 타입의 네트워크에 연결된 하나 이상의 서버를 가질 수 있다. 각 개인을 비롯한 다양한 엔티티들은 인터넷 또는 기타 네트워크를 통해 정보나 자원을 공유한다. 가정에서의 이용을 위한 유무선 네트워크들이 더욱 더 널리 보급되고 있으며, 개인용 컴퓨터에서 가전 기기들에 이르는 광범위한 장치들은 현재 이러한 네트워크들에 연결되어 있고 또 이러한 네트워크를 통하여 액세스 가능하거나 장차 그리 될 예정이다. 다양한 자원에의 액세스가 점점 쉽게 이용 가능해짐에 따라, 이들 자원들의 안전한 공유 및 이들 간 협력이 더욱 중요해지고 있다.

이와 같은 자원의 공유 및 이들 간 협력에 있어서 한 가지 장애점은 제공된 자원에 액세스를 시도하는 여러 엔티티를 인식하고 인증(authenricating)하는 문제에 관한 것이다. 즉, 컴퓨터 상의 자원에 액세스를 시도하는 엔티티가 그와 같은 자원들에 액세스할 권리를 주장하고 그와 같은 자원들에 액세스하기 위하여 필요한 인가(authorization)를 받은 엔티티인지 확인하고 보장하는 것은 주의를 요한다. 어떤 엔티티를 인식하고 인가를 부여하는 방법에는 여러가지가 있다.

엔티티를 인식하고 그 엔티티에 인가를 부여하는 방법 중 하나는 보안 도메인(security domain)을 정의하도록 설정된 계정(account) 및 비밀 번호 시스템과 관련된다. 예컨대, 어떤 회사는 서버나 네트워크에 대하여, 그 회사의 전일제 종업원 모두로 이루어진 보안 도메인을 형성하고자 원할 수 있다. 이와 같은 보안 도메인을 운영하는 자, 예컨대 시스템 관리자 등은 종업원 개개인에게 통상적으로 사용자 이름과 비밀 번호를 포함하는 계정을 부여하고 이들 계정을 통한 자원에의 액세스를 제어하는 정책을 수립한다. 일단 보안 도메인이 설정되고 나면, 그 도메인 멤버들은 자원에 대한 액세스 권한을 부여받을 수 있고 동시에 계정이 없는 자들은 배제된다.

그러나, 사용자로 하여금 여러 사용자 이름과 비밀 번호들을 기억하도록 요구하는 계정 시스템에 기초한 보안 도메인은 번거러운 것일 수 있다. 더욱이, 계정 시스템에 기반을 둔 보안 도메인은 인터넷과 같은 네트워크를 통해 정보나 자원을 공유하고자 하는 각 개인들에게 있어서는 좋은 모델이 되지 못한다. 또한, 여러가지 사업상 이유로, 전통적인 폐쇄형 보안 도메인을 확장하거나 심지어는 인터넷을 통하여 선택된 개인들로 대체할 필요가 있을 수 있다. 예컨대, 종업원들, 외부 계약자들, 그리고 기타 다른 개인이나 엔티티들이 가상 팀의 일부를 이룰 수 있고, 공유 문서, 통신 및 기타 다른 자원에 액세스할 수 있는 프로젝트를 수립할 필요가 있을 수 있다.

자원에 액세스하기 위하여 유효한 사용자 이름과 비밀 번호를 구비한 계정을 이용하는 자를 그 계정의 소유자라고 가정하는 것은 비교적 쉬운 일이지만, 전통적 폐쇄형 보안 도메인의 일원이 아닌 자의 아이덴티티를 인식하는 것은 매우 어려운

일이었다. 엔티티의 아이덴티티를 확인하고 인증하는 한 가지 방법으로서 공개키 인프라구조가 이용되어 왔다. 공개키 인프라구조는 시스템의 사용자와, 그 확인(certifying) 즉 추천(recommending) 당국 간의 신뢰 관계에 기초를 두고 있다. 그러나, 이 공개키 인프라구조는 그 이해, 시동(bootstrap) 및 관리가 복잡하다. 그러므로, 공개키 인프라구조는 다양한 엔티티에 적용될 수 있는 아이덴티티 인식 시스템에 사용하기에 간단하지도 쉽지도 않기 때문에 컴퓨터 사용자 인식에 관하여 주류적 기술이 되지는 못하고 있다. 본 발명은 이와 같은 상황이나 기타 다른 상황들을 고려하여 창안된 것이다.

발명의 상세한 설명

전술한 문제점 및 기타 문제점들은, 수신자에 의한 송신자의 아이덴티티 인식 시스템 및 방법과, 송신자에 의해 서명된 아이덴티티 정보를 이용한 아이덴티티 정보의 교환 시스템 및 방법에 의해 해결된다. 어느 당사자에 관하여 선택된 아이덴티티 정보는, 컴퓨터 시스템들 간에 교환되어 그 당사자 인식에 이용될 수 있는 아이덴티티 정보 문서에 포함된다. 아이덴티티 인식이 인가를 포함하지는 않는다. 본 발명에서는, 송신자의 인증, 즉 아이덴티티 인식과, 수신자의 자원에 액세스하기 위한 송신자의 인가는 별개 사항이다.

또 다른 양상에 따르면, 본 발명은 아이덴티티 정보 문서를 송신하는 방법으로서, 그 아이덴티티 정보 문서에 포함시킬 아이덴티티 정보를 자기 아이덴티티 정보 저장부(self-identity information store)로부터 선택하는 단계를 포함하는 방법에 관한 것이다. 선택된 아이덴티티 정보를 자기 아이덴티티 정보 저장부로부터 판독하여, 그 선택된 아이덴티티 정보와 함께 적어도 하나의 제1 키(first key)(예컨대 공개키)를 포함하는 아이덴티티 정보 문서를 생성한다. 아이덴티티 정보 문서는 그 아이덴티티 정보 문서에 포함되어 있는 제1 키와 연관된, 제2 키(예컨대 비밀키)를 이용하여 송신자에 의해서 서명된 디지털 서명을 갖는다. 그런 다음에, 아이덴티티 정보 문서가 수신자에게 송신된다. 본 발명의 또 다른 양상에 따르면, 아이덴티티 정보 문서를 수신하는 방법은 발신자, 즉 송신자로부터 서명된 아이덴티티 정보 문서를 수신하는 단계를 포함한다. 아이덴티티 정보 문서에 의하여 전달되는 아이덴티티 정보가 신뢰할 수 있는지 여부에 대한 판단이 행해진다. 아이덴티티 정보가 신뢰할 수 있다고 판단되는 경우, 아이덴티티 정보는 인식 아이덴티티 정보 저장부(recognized identity information store)에 저장된다. 인식 아이덴티티 정보 저장부는 이후 발신자가 수신 컴퓨터 시스템에의 접속을 다시 시도할 때에 그 발신자에 대한 추후 인식과 인증을 위해 이용된다.

또 다른 양상에 따르면, 본 발명은 아이덴티티 정보 문서를 송신하는 시스템에 관한 것이다. 이 시스템은 프로세서, 프로세서에 접속된 통신 채널, 그리고 프로세서에 연결되고 프로세서에 의해 판독가능한 메모리를 포함한다. 메모리는 일련의 명령어들을 포함하고, 그 명령어들은 프로세서에 의해 실행될 경우 프로세서로 하여금 아이덴티티 정보 문서에 포함시킬 아이덴티티 정보를 자기 아이덴티티 정보 저장부로부터 선택하도록 한다. 선택된 아이덴티티 정보가 자기 아이덴티티 정보 저장부로부터 판독되고, 그 선택된 아이덴티티 정보 및 적어도 하나의 제1 키를 포함하는 아이덴티티 정보 문서가 생성된다. 아이덴티티 정보 문서는 아이덴티티 정보 문서에 포함되어 있는 제1 키와 쌍을 이루는 제2 키를 이용하여 서명된 디지털 서명을 갖는다. 그런 다음에, 아이덴티티 정보 문서는 통신 채널에 연결된 수신자에게 송신된다.

본 발명의 또 다른 양상에 따르면, 본 발명은 아이덴티티 정보 문서를 수신하는 시스템에 관한 것이다. 이 시스템은 프로세서, 프로세서에 접속된 통신 채널, 그리고 프로세서에 연결되고 프로세서에 의해 판독가능한 메모리를 포함한다. 메모리는 일련의 명령어들을 포함하고, 그 명령어들은 프로세서에 의해 실행될 경우 프로세서로 하여금 서명된 아이덴티티 정보 문서를 발신자, 즉 송신자로부터 수신하도록 한다. 아이덴티티 정보 문서에 의하여 전달된 아이덴티티 정보가 신뢰할 만한 것인지 여부에 대한 판단이 행해진다. 아이덴티티 정보가 신뢰할 만한 것이라고 판단된 경우, 아이덴티티 정보는 인식 아이덴티티 정보 저장부에 저장된다. 인식 아이덴티티 정보 저장부는 이후 발신자가 수신 컴퓨터 시스템에의 접속을 다시 시도할 때에 그 발신자에 대한 추후 인식과 인증을 위해 이용된다.

본 발명은 컴퓨터 프로세스, 컴퓨팅 시스템, 또는 컴퓨터 프로그램 제품이나 컴퓨터 판독가능 매체와 같은 제조품으로 구현될 수 있다. 컴퓨터 판독가능 매체는 컴퓨터 시스템에 의해 판독가능하고 컴퓨터 프로세스를 실행하기 위한 컴퓨터 프로그램 명령어들을 인코딩하는 컴퓨터 저장 매체일 수 있다. 컴퓨터 판독가능 매체는 컴퓨팅 시스템에 의해 판독가능하고 컴퓨터 프로세스 실행을 위하여 컴퓨터 프로그램 명령어들을 인코딩하는 반송파에 의하여 전파되는 신호일 수도 있다.

본 발명에 관한 이들 및 기타 특성과 이점들은 이하의 상세한 설명과 첨부 도면에 의하여 명백해질 것이다.

도면의 간단한 설명

도 1은 본 발명의 일 실시예에 따른 아이덴티티 인식 시스템의 개념도,

도 2는 본 발명의 실시예들이 구현될 수 있는 적합한 컴퓨팅 시스템 환경의 예를 도시한 도면,

도 3은 본 발명의 일 실시예에 따른 아이덴티티 인식 시스템의 예시적 소프트웨어 구성요소를 도시한 도면,

도 4는 본 발명의 일 실시예에 따른 아이덴티티 정보 교환의 개시에 관하여 나타낸 플로우차트,

도 5는 본 발명의 일 실시예에 따른 아이덴티티 정보 수신을 나타낸 플로우차트,

도 6은 본 발명의 일 실시예에 따른 아이덴티티 정보 문서의 예시적 포맷을 도시한 도면.

실시예

본 발명의 각종 실시예를 설명하기 전에, 본 명세서 전체에 걸쳐 사용될 몇 가지 용어들에 대해 정의한다.

"아이덴티티 정보(identity information)"라 함은 아이덴티티 정보 시스템에 속한 어느 당사자에 관한 정보 모음을 의미하는 것으로, 이 아이덴티티 정보 시스템을 통해 그 당사자나 에이전트는 어떤 정보를 수신 장치로 전달할 것인지 제어할 수 있고 그와 같은 정보의 사용 목적을 표시할 수 있다.

"아이덴티티 정보 문서"라 함은 장치 간에 전송되는 어느 당사자에 대한 아이덴티티 정보의 서브세트를 의미하며, 이에 의해서 수신 장치는 그 아이덴티티 정보 문서의 발신자를 표시할 수 있고 이어서 그 발신자가 개시했던 또는 응답했던 디지털 이벤트(digital event)를 인식할 수 있다.

"당사자"라 함은 디지털 방식으로 동작할 수 있는 임의의 엔티티를 의미한다. 당사자에는 각 개인과, 개인들 집단, 가족, 기관, 명시 그룹(explicit group), 공통 역활을 담당하는 사람들, 즉 소정 종류의 속성들과 다양한 전자 장치들(그 개인들은 이를 통하여 동작함)을 공유하는 사람들을 의미하는 사람들 그룹이나 모임이 포함된다.

도 1은 본 발명의 일 실시예에 따른 아이덴티티 인식 시스템의 개념도이다. 본 예는 네트워크(111) 기타 채널을 통해 서로 연결된 개시 시스템(initiating system)(101)과 수신 시스템(receiving system)(106)을 도시하고 있다. 분명히, 대부분의 장치는 때에 따라 개시 시스템(101)이자 수신 시스템(106) 모두로 기능할 수 있다. 그러나, 간단하게 하기 위해서, 여기서는 이들 기능을 분리하여 나타내었다. 또한, 네트워크(111)는 인터넷을 포함한 임의의 유형의 네트워크일 수도 있고, 또는 개시 시스템(101)과 수신 시스템(106) 사이에 통신을 설정하는데 적합한 임의의 유형의 채널일 수 있다.

개시 시스템(101)은 자기 아이덴티티 정보(self-identity information)(102) 세트를 보유한다. 자기 아이덴티티 정보(102)에는 개시 시스템(101)에 의하여 표시된 당사자 즉 그 개시 시스템(101)을 이용하는 당사자에 관한 각종 정보들이 포함될 수 있다. 이 정보는 예컨대 이름, 이메일 어드레스, 웹사이트 URL 및 기타 개인 정보는 물론이고 이러한 정보의 이용 방법을 기술하는 이용 정책도 포함할 수 있다. 이들 각기 다른 아이덴티티 확인 요소들을 본 명세서에서는 아이덴티티 클레임(claim)이라 부른다.

자기 아이덴티티 정보(102)의 일부 또는 전부를 포함하는 아이덴티티 정보 문서(105)가 작성된다. 일 실시예에서, 아이덴티티 정보 문서(105)는 수신 시스템(106)으로부터의 요구에 응답하여 작성된다. 그러므로, 개시 시스템(101)에 의해서 표시된 당사자 즉 그 시스템을 이용하는 당사자가 다른 시스템, 예컨대 수신 시스템(106)으로 아이덴티티 정보를 송신하고자 할 경우, 사용자는 전송할 정보를 자기 아이덴티티 정보(102) 중에서 선택한다. 즉, 당사자는 아이덴티티 정보 문서(105) 생성시 자기 아이덴티티 정보(102)로부터의 정보 개시에 관하여 제어할 능력을 갖고 있다. 그러므로, 당사자는 각기 다른 수신자에 대해 각기 다른 아이덴티티 데이터 서브세트를 선택적으로 개시할 수 있으며, 그 개시된 정보의 사용 방식에 대한 의사를 표현할 수 있다. 더욱이, 이것은 "순차적(progessive) 공개"를 가능하게 하는데, 이러한 순차적 공개의 경우 당사자는 약간의 정보만을 담고 있는 제1 아이덴티티 정보 문서를 송신하고, 좀 더 뒤의 시점에 보다 많은 정보를 공표할 만한 이유가 있을 경우 그와 같은 정보를 공표한다.

일 특정 실시예에서, 풀(full) 아이덴티티 정보 문서는 그 아이덴티티 정보 문서 생성시에 그 아이덴티티 정보 문서를 발신하는 당사자의 비밀키를 이용하여 디지털 서명된다. 그러므로, 그 아이덴티티 정보 문서는 자기 서명형(self-signed)이라고 불린다. 또 다른 실시예에서, 풀 아이덴티티 정보 문서는 그 아이덴티티 정보 문서 생성시에 그 아이덴티티 정보 문서를 발신하는 당사자를 위하여 아이덴티티 클레임을 발행했던 기관의 비밀키로 서명된 디지털 서명을 갖는다. 이 경우, 아이덴티티 정보 문서는 그 기관에 의하여 서명된 것이라고 말해진다. 마찬가지로, 이미 공유된 아이덴티티 정보 문서에 관한 갱신이나 순차적 공개에 대해서는 그 원래 공유된 아이덴티티 정보를 서명하는데 사용되었던 비밀키를 이용하여 서명이 이

루어질 것이다. 그 서명에 이용되는 비밀키와 한 쌍을 이루는 공개키는 아이덴티티 정보 문서의 일부로서 포함되는 등 여러 가지 방식으로 분배될 수 있다. 이와 달리, 공개/비밀키 방식 이외의 키 구성도 이용될 수 있다. 예컨대, 비밀키 세트가 이용될 수도 있다.

개시 시스템(101)은 자기 아이덴티티 정보(102)로부터 서명형 아이덴티티 정보 문서(105)를 생성하여 이것을 네트워크(111)를 통해서 수신 시스템으로 전송한다. 일 실시예에 따르면, 아이덴티티 정보는 확장형 마크업 언어(XML) 파일 또는 임의의 채널을 이용하여 수신 시스템(106)으로 전송될 수 있는 텍스트 파일을 포함할 수 있다. 아이덴티티 정보 문서(105)에 대하여 가능한 한 가지 포맷의 세부 사항에 대해서는 도 6을 참조하여 후술할 것이다. 그러나, 일반적으로 말하자면, 아이덴티티 정보(105)는 각종 채널을 통하여 이종 시스템들 간에 정보를 전달하는데 적합한 임의의 포맷일 수 있다. 전술한 바와 같이, 개시 시스템(101)으로부터 수신 시스템(106)으로 아이덴티티 정보 문서(105)를 전달하는데 이용되는 채널은 여러 가지 가능한 매체들 중 어느 것이라도 좋다. 예컨대, 이메일, 인스턴트 메시지 전달(instant messaging), 빔 전송(beaming), 전용 라인 및 기타 다른 많은 수단이 채널로 이용될 수 있다. 또한, 그 채널은 안전할 수도 안전하지 않을 수도 있다.

수신 시스템(106)은 입력되는 아이덴티티 정보 문서(105)를 판독하여 이것을 수용하거나 거부한다. 전형적인 시나리오에서는, 아이덴티티 정보 문서(105)가 이미 알려져 있는 당사자로부터 발신되고, 수신 시스템(106)은 그 아이덴티티 정보 문서(105)의 신뢰성(authenticity)에 대해 매우 잘 판단할 것이다. 그러나, 만일 아이덴티티 정보 문서(105)가 미지의 당사자로부터 온 것이거나, 당사자를 사칭하는 자가 그 아이덴티티 정보 문서(105)를 오픈하고 변경하거나 위조할 충분한 동기를 가질 염려가 있다면, 수신 시스템(106)은 그 아이덴티티 정보 문서(105)를 거부하거나 그 신뢰성에 대한 추가적 검증 절차를 시도할 수 있다. 이 검증 절차에 대해 자세한 것은 도 3 내지 도 6을 참조하여 후술할 것이다.

아이덴티티 정보 문서가 일단 수용되고 나면, 이 문서가 포함하는 정보가 수신 시스템(106)의 인식 아이덴티티 정보(recognized identity information)(107)에 추가된다. 아이덴티티 정보 문서(105)가 인식 아이덴티티 정보(107) 리스트에 추가되고 나면, 수신 시스템(106)은 그 아이덴티티 정보 문서(105)가 포함하고 있는 정보를 이용하여 장차 개시 시스템(101)을 인증할 수 있고, 또 인증없이는 신뢰되지 않을 당사자와 대화하는 채널을 이용할 수 있다. 그러면, 예컨대 아이덴티티 정보 문서(105)에 의해서 표시된 당사자에게 수신 시스템(106) 상의 자원, 예컨대 캘린더(calender) 또는 문서 등에 대한 액세스 권한이 주어질 수 있다. 이와 달리, 당사자는 과제를 부여받을 수 있고, 그 과제가 충족될 경우 수신 시스템 상의 자원에 대한 액세스에 대해 인증받을 수 있다. 거꾸로 말하면, 수신 시스템(106)에 의해 수용된 아이덴티티 정보 문서를 제공하지 않은 아이덴티티 미확인 시스템(110)에 의해 표시된, 즉 이 시스템을 이용하는 아이덴티티 미확인 당사자는 수신 시스템(106)의 자원들로부터 배척될 수 있다. 마찬가지로, 수신 시스템(106)에 의해 수용된 아이덴티티 정보 문서를 제공한 아이덴티티 확인 시스템(110)에 의해 표시된, 즉 이 시스템을 이용하는 아이덴티티 확인 당사자도 의도에 따라서는 수신 시스템(106)의 자원으로부터 배척될 수 있다.

아이덴티티 정보 문서(105) 이용을 통한 당사자 인식과 인식 아이덴티티 정보 리스트(107)로의 아이덴티티 정보 반입(importing)이 그 당사자에게 임의의 자격이나 수신 시스템(106)에 대한 액세스 권한 등을 자동적으로 제공하는 것은 아니다. 이는 단지 수신 시스템(106)이 장래에 그 당사자를 인식하고 인증할 수 있는 능력을 제공할 뿐이다. 인식 또는 인증은 파일 공유, 암호화된 메일의 송신, 이미 공유된 아이덴티티 정보의 자동 갱신 등에 대한 인가의 가능성을 제공한다. 누구라도 인식될 수 있다. 인식이란 단지 수신 시스템(106)이 누가 그 시스템과 현재 상대하고 있는지를 안다는 것을 의미할 뿐이고, 그 당사자에게 어떤 액세스권이 주어진다는 것을 의미하는 것은 아니다. 어떤 당사자를 인식한다는 것은 그에게 무엇인가에 대한 액세스권을 준다는 것을 의미하는 것은 아니다. 인증을 거친 후에 또는 그렇게 하는 것이 유용하거나 안전할 때에 당사자에게 액세스권이 주어질 수 있다.

따라서, 아이덴티티 인식은 일방향으로만 이루어진다. 그러므로, 또 다른 방향으로도 유효하게 아이덴티티 인식이 이루어지기 위해서는 개시 시스템(101)과 수신 시스템(106) 간에 아이덴티티 정보의 양방향 교환을 요구할 필요가 있다. 수신 시스템(106)이 개시 시스템(101)에 의해 표시되는, 즉 이 시스템을 이용하는 당사자를 인식하고 그 당사자를 적절한 당사자로 취급하는데에는 개시 시스템(101)으로부터 수신 시스템(106)으로의 일방향 아이덴티티 정보 문서(105)의 교환으로 충분하다.

당사자의 아이덴티티가 인식될 수 있고 액세스권이 적절하게 주어지거나 거부될 수 있는 경우, 또는 추가적 인증 프로세스가 요구될 수 있는 경우, 아이덴티티 정보 문서(105)와 인식 아이덴티티 리스트(107)에 기초하여 수신 시스템(106)의 자원에 대한 액세스를 허용하는 것이 보안을 위태롭게 하는 것은 아니다. 또한, 임의의 미인식 당사자가 배척될 수 있다.

도 2는 본 발명의 실시예들이 구현될 수 있는 적합한 컴퓨팅 시스템 환경의 일 예를 도시한 도면이다. 이 시스템(200)은 전술한 개시 시스템 및/또는 수신 시스템으로 기능하도록 이용될 수 있는 대표적 시스템이다. 가장 기본적 구성으로서, 시스

템(200)은 통상적으로 적어도 하나의 처리부(202)와 메모리(204)를 포함한다. 컴퓨팅 장치의 정확한 구성과 타입에 따라서 메모리(104)는 휘발성(RAM 등)이나 비휘발성(ROM, 플래시메모리 등) 메모리 또는 이들 둘의 조합일 수 있다. 이와 같은 가장 기본적 구성이 도 2에서 점선(206)으로 도시되어 있다. 또한, 시스템(200)은 추가적 특성/기능성을 가질 수도 있다. 예컨대, 장치(200)는 자기 또는 광헉 디스크나 테이프(단 이로써 제한되는 것은 아님)를 포함한 (착탈식 및/또는 고정식) 추가 저장 장치들을 포함할 수 있다. 그와 같은 추가 저장 장치가 도 2에서는 착탈식 저장 장치(208)와 고정식 저장 장치(210)로 도시되어 있다. 컴퓨터 저장 매체에는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터 등의 정보 저장을 위한 임의의 방법이나 기술로 구현된 휘발성 및 비휘발성, 착탈식 및 고정식 매체가 포함된다. 메모리(204), 착탈식 저장 장치(208) 및 고정식 저장 장치(210)는 모두 컴퓨터 저장 매체의 예이다. 컴퓨터 저장 매체로는 RAM, ROM, EEPROM, 플래시메모리 기타 메모리 기술, CD-ROM, DVD 기타 광gkr 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 기타 자기 저장 장치, 그리고 원하는 정보를 저장하는데 사용될 수 있고 시스템(200)에 의해 액세스될 수 있는 임의의 기타 매체가 포함되고, 다만 이로써 한정되는 것은 아니다.

시스템(200)은 그 시스템이 다른 장치와 통신할 수 있게 하는 통신 접속부(212)도 포함할 수 있다. 통신 접속부(212)는 통신 매체의 일 예이다. 통신 매체는 대개 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조형 데이터 신호나 기타 전송 메카니즘에 의한 데이터를 구체화하며, 이에는 임의의 정보 전달 매체가 포함된다. "변조형 데이터 신호"라는 용어는 신호 안에 정보를 인코딩하도록 그 하나 이상의 특성을 설정 또는 변화시킨 신호를 의미한다. 제한이 아니라 예로서, 통신 매체로는 유선 네트워크나 직접 유선 접속부 등의 유선 매체와, 음향, 무선(RF), 적외선 및 기타 무선 매체와 같은 무선 매체가 포함된다. 본 명세서에서 사용된 "컴퓨터 판독가능 매체"라는 용어는 저장 매체와 통신 매체 모두를 포함한다.

또한, 시스템(200)은 키보드, 마우스, 펜, 음성 입력 장치, 접촉식 입력 장치 등과 같은 입력 장치(214)를 가질 수 있다. 디스플레이, 스피커, 프린터 등과 같은 출력 장치(216)도 포함될 수 있다. 이들 모든 장치는 본 기술분야에서 공지된 것이며 여기서는 상세히 설명하지 않는다.

시스템(200)과 같은 컴퓨팅 장치는 일반적으로 적어도 소정 형태의 컴퓨터 판독가능 매체를 포함한다. 컴퓨터 판독가능 매체는 시스템(200)이 액세스할 수 있는 임의의 이용 가능 매체일 수 있다. 제한이 아니라 예로서, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체와 통신 매체를 포함할 수 있다.

도 3은 본 발명의 일 실시예에 따른 아이덴티티 인식용 시스템의 주요 소프트웨어 컴포넌트를 도시한 도면이다. 이 예는 도 1에 도시된 것과 마찬가지로, 채널(306)을 통해 서로 연결된 개시 시스템(301)과 수신 시스템(306)을 도시하고 있다. 또한, 전술한 바와 같이, 시스템은 시점에 따라 개시 시스템(301)과 수신 시스템(306) 두 가지 모두로서 기능할 수 있다. 그러나, 간단하게 하기 위해서, 여기서는 이들 기능을 별도로 도시하였다.

개시 시스템(301)은 자기 아이덴티티 정보 저장부(302), 자기 아이덴티티 정보 제어 모듈(303), 아이덴티티 정보 처리부(304) 및 아이덴티티 인식 번호(IRN) 처리 모듈(305)을 포함한다. 자기 아이덴티티 정보 저장부(302)는 개시 시스템(301)에 의해서 표시되는, 즉 이 시스템을 이용하는 당사자에게 특정된 데이터베이스, 리스트 또는 기타 정보 모음을 포함한 정보를 저장할 수 있다. 자기 아이덴티티 정보 저장부(302)는 당사자 이름, 이메일 어드레스, 공개키 및/또는 인증서 등의 정보와, 후술될 아이덴티티 정보 문서에서 이용될 있는 기타 개인 정보를 저장할 수 있다.

자기 아이덴티티 정보 제어 모듈(303)은 자기 아이덴티티 정보 저장부(302)로부터 아이덴티티 정보를 판독한다. 어느 당사자가 아이덴티티 정보를 다른 시스템으로 보내고자 한다면, 그 당사자는 보낼 정보를 자기 아이덴티티 정보 제어 모듈(303)을 통해서 자기 아이덴티티 정보 저장부(302)로부터 선택한다. 예컨대, 당사자가 아이덴티티 정보 문서를 보내고자 할 경우, 자기 아이덴티티 정보 제어 모듈(303)에 의하여 그래픽 유저 인터페이스(GUI)가 제시될 수 있고 당사자는 이 GUI를 통하여 보내고자 하는 정보를 자기 아이덴티티 정보 저장부(302)로부터 선택할 수 있다.

자기 아이덴티티 정보 제어 모듈(303)은 당사자에게 아이덴티티 정보 문서(307) 생성시 자기 아이덴티티 정보 저장부(302)로부터의 정보 공개를 통제할 수 있는 능력을 부여한다. 자기 아이덴티티 정보가 GUI를 통해 제시되는 경우, 자기 아이덴티티 정보는 판독이 쉽고 사용하기 쉬운 다양한 포맷으로 제시될 수 있다. 예컨대, 아이덴티티 정보 문서에 포함된다는 것을 나타내기 위하여 사용자가 체크 표시, 즉 선택할 수 있는 정보 리스트가 제시될 수 있다. 그러므로, 자기 아이덴티티 정보 제어 모듈(303)은 당사자로 하여금 각기 다른 수신 시스템(309)마다 서로 다른 아이덴티티 정보 서브세트를 선택적으로 공개할 수 있도록 하고 그 공개 정보가 어떻게 이용될 것인가에 대한 의사를 표시할 수 있도록 한다. 더욱이, 자기 아이덴티티 정보 제어 모듈(303)은 "순차적 공개"를 가능하게 하는데, 이러한 순차적 공개의 경우 당사자는 약간의 정보만을 담고 있는 제1 아이덴티티 정보 문서를 송신하고, 좀 더 뒤의 시점에 보다 많은 정보를 공표할 만한 이유가 있을 때 그와 같은 정보를 공표한다.

아이덴티티 정보 처리부(304)는 자기 아이덴티티 정보 제어 모듈(303)이 제공한 정보로부터 아이덴티티 정보 문서(307)를 생성하고, 이것을 채널(306)을 통해 수신 시스템(309)으로 송신한다. 일 실시예에 따르면, 아이덴티티 정보 문서(307)는 XML 파일이나 임의의 채널을 이용하여 수신 시스템(309)으로 전송될 수 있는 텍스트 파일을 포함할 수 있다. 아이덴티티 정보에 대하여 가능한 한 가지 포맷에 있어서의 세부 사항에 대해서 도 6을 참조하여 후술할 것이다. 그러나, 일반적으로 말하자면, 아이덴티티 정보(307)는 이종 시스템들 간에 정보를 전달하는데 적합한 임의의 포맷일 수 있다.

개시 시스템(301)으로부터 수신 시스템(309)으로 아이덴티티 정보 문서(307)를 전달하는데 이용된 채널(306)은 여러 가지 가능한 매체들 중 임의의 것일 수 있다. 예컨대, 이메일, 인스턴트 메시지 전달, 빔 전송, 전용 라인 및 기타 많은 메카니즘이 채널(306)로 이용될 수 있다. 이 채널(306)은 안전할 수도 안전하지 않을 수도 있다.

수신 시스템(309)은 아이덴티티 정보 처리부(312), 수신 아이덴티티 정보 제어 모듈(311), 인식 아이덴티티 정보 저장부(310) 및 IRN 처리 모듈(314)을 포함한다. 수신 시스템(309)의 아이덴티티 정보 처리부(312)는 채널(306)로부터 입력되는 아이덴티티 정보(307)를 수신한다. 아이덴티티 정보 처리부(312)는 아이덴티티 정보를 아이덴티티 정보 문서(307)로부터 수신 아이덴티티 정보 제어 모듈(311)로 전달한다.

수신 아이덴티티 정보 제어 모듈(311)은 그 아이덴티티 정보 문서(307)를 수용할 것인지 거부할 것인지를 결정한다. 소정의 경우에, 이와 같은 결정은 GUI를 통하여 사용자에게 그 수신된 정보를 수용 또는 거부할 것인지 질의하는 방식으로 이루어질 수 있다. GUI를 통하여 제시될 경우, 아이덴티티 정보 문서로부터의 아이덴티티 정보는 판독이 쉬운 여러 가지 포맷으로 제시될 수 있다. 예컨대, 정보가 신속하고 용이한 검토를 가능하게 하는 롤로덱스(rolodex) 형태나 "접촉" 엔트리 형태로 제시될 수 있다.

아이덴티티 정보 문서(307)가 이미 알려져 있는 당사자로부터 발신된 경우에는, 수신 시스템(309)은 그 아이덴티티 정보 문서(307)의 신뢰성을 매우 잘 판단할 수 있을 것이다. 그러나, 만일 아이덴티티 정보가 미지의 당사자으로부터 온 것이거나, 당사자를 사칭하는 자가 메일을 오픈하고 변경할 충분한 동기를 가질 염려가 있다면, 수신 시스템(309)은 아이덴티티 인식 번호(IRN) 처리 모듈(314)을 이용하여 그 아이덴티티 정보 문서(307)를 검증할 수 있다.

아이덴티티 정보 문서(307)는 다양한 매체를 통해 교환될 수 있다. 일부 매체는 다른 매체에 비해 스푸핑(spoofing)에 더 취약하다. 아이덴티티 정보 문서(307)가 이메일과 같이 보다 취약한 매체를 통해 교환된 경우나 그 외에도 아이덴티티 정보 문서(307)가 의심이 드는 것이라면, 아이덴티티 정보 문서(307)의 무결성(integrity)에 관하여 대역외(out-of-band) 검증을 수행하여 그 문서가 스푸핑이나 MITM 공격(man-in-the middle attacks)을 받지 않았음을 보증하는 것이 바람직할 수 있다. 대역외 검증이 요구되는 정도는 아이덴티티 정보가 얻어진 방법 및 송신측과의 공유가 의도되는 정보의 감도에 따라 달라진다.

아이덴티티 정보 문서(307)와 당사자의 결속에 대한 대역외 검증을 지원하기 위하여, 아이덴티티 인식 번호(IRN)가 이용될 수 있다. IRN은 당사자의 공개키를 아이덴티티 정보 문서에 포함된 판독가능한 문자열로 만드는 적합한 변환 기능을 갖는 당사자 공개키의 해시(hash)이다. 이와 같은 변환 기능을 통해서 IRN은 용이하게 판독 가능하고 기억 가능한 일련의 숫자들로 표시될 수 있다. 예컨대, IRN은 전화 번호와 유사할 수 있다.

대역외 검증을 수행하기 위하여, 수신 시스템(309)의 IRN 처리 모듈(314)은 아이덴티티 정보 문서(307)에 대한 IRN을 계산하여 디스플레이한다. 수신 시스템이나 그 사용자는, 예컨대 전화로 또는 인스턴트 메시지 전달(IM)을 통해 발신자를 호출하는 것과 같이 또 다른 채널(308)에 의해서 발신자와 접촉하여 그 발신자에게 자신의 IRN을 확인할 것을 요청한다. 그런 다음, IRN 처리 모듈(314)은 그 확인된 IRN이 수신된 아이덴티티 정보 문서(307)에 기초하여 수신자측에서 계산된 것과 매칭되는지를 검증할 수 있다.

MITM 공격이 송신자를 스푸핑하도록 공개키 정보를 교체함으로써 수신 시스템(309)에 의해 수신된 아이덴티티 정보 문서(307)를 함부로 변경시킨 경우라면, 그 계산된 IRN은 대역외 검증 프로세스에서 명백해질 실제 송신자의 IRN과 매칭되지 않을 것이다. IRN은 공개키로부터 계산되므로 공개 정보가 될 수 있고, 따라서 개인의 아이덴티티에 대한 증거로서 비즈니스 카드 등에 포함시키기 적합할 수 있음을 알아야 한다.

일단 아이덴티티 정보 문서(307)가 수용되고 나면, 그 문서가 포함하고 있는 정보는 인식 아이덴티티 정보 저장부(107)에 저장된다. 그런 다음, 아이덴티티 정보 문서(307)를 발신한 당사자에게 수신 시스템(309) 상의 자원에 대한 액세스권이 부여될 수 있다. 장래에 그 당사자가 그와 같은 자원에 액세스하려고 할 경우, 그 당사자의 컴퓨터는 아이덴티티 정보 문서

(307) 내에 공개키와 관련된 비밀키를 알고 있음을 표시하도록 요구받게 될 것이다. 당사자가 신뢰할 수 있는 당사자인 경우라면, 컴퓨터는 이와 같이 비밀키를 알고 있다는 증거를 제공하여 당사자 인식 및 자원에의 액세스 허가를 가져올 것이다.

이와 달리, 거부된 아이덴티티 정보까지도 인식 아이덴티티 정보 저장부(107)에 저장될 수 있다. 예컨대, 소정의 아이덴티티 정보 세트가 거부된 경우라 하더라도, 장래의 참고를 위하여 이를 저장하고 아울러 신뢰할 수 없는 것이라고 표시할 수 있다. 이와 같이 인식은 되었으되 신뢰할 수 없는 아이덴티티 정보는 인식 아이덴티티 정보 저장부의 특별한 부분에 저장하거나 소정의 방식으로 태그(tag) 또는 플래그(flag)하여 표시할 수 있다. 그와 같은 정보는 장래에 신뢰할 수 없는 아이덴티티 정보에 대한 아이덴티티 확인에 유용할 수 있다.

또한, 수신 시스템의 사용자가 검토할 수 있도록, 예컨대 GUI를 통해서, 인식 아이덴티티 정보 저장부(107)에 저장되어 있는 아이덴티티 정보가 액세스 가능해질 수 있다. GUI를 통하여 제시될 경우, 인식 아이덴티티 정보 저장부(107)로부터의 아이덴티티 정보는 판독이 쉬운 여러 가지 포맷으로 제시될 수 있다. 예컨대, 아이덴티티 정보는 신속하고 용이한 검토가 가능하게 하는 롤로덱스 형태나 "접촉" 엔트리 형태로 제시될 수 있다.

도 3에 도시된 시스템을 이용하여, 주체에 관한 기밀 정보를 포함한 아이덴티티 정보 문서들을 서로 교환하는 것은 아이덴티티 정보의 순차적 공개 프로세스를 이용함으로써 안전하게 달성될 수 있다. 이와 같은 프로세스에서, 예컨대 발신자와 수신자는 먼저 X509v3 인증서 등의 인증서에 캡슐화될 수 있는 공개키를 교환하고, 아이덴티티 정보 문서를 통해 최소한의 필요한 아이덴티티 클레임을 교환한다. 그런 다음, 양측은 해당 정보의 수신자측의 공개키로 암호화하여 나머지 공개되는 속성들 전체 세트를 교환한다. 이에 의해서 기밀 데이터는 의도된 수신자만이 볼 수 있게 되고 그 이외의 자들은 볼 수 없게 된다. 물론 순차적 공개 방법을 이용하기 위하여 반드시 아이덴티티 정보 문서의 교환이 필요로 되는 것은 아니다. 순차적 공개는 일방향 공유에도 역시 이용될 수 있다. 이와 같은 순차적 공개 교환은 무상태(stateless) 방식으로 비동기적으로 일어날 수 있으며 한 세션(session)으로 래핑되거나(wrapped) 특정 프로토콜에 구속될 필요가 없다.

본 발명의 여러 실시예들에 있어서의 논리적 동작들은 (1) 컴퓨팅 시스템 상에서 실행되는 컴퓨터 구현 동작이나 프로그램 모듈의 시퀀스 및/또는 (2) 컴퓨팅 시스템 내의 상호 접속형 기계 논리 회로 또는 회로 모듈로 구현된다. 이와 같은 구현은 본 발명을 구현하는 컴퓨팅 시스템의 성능 요구 조건에 따른 선택의 문제이다. 따라서, 본 명세서에 개시된 본 발명의 실시예를 구성하는 논리적 동작은 동작, 구조적 장치, 행위 또는 모듈과 같이 다양하게 지칭된다. 당업자라면 이러한 동작, 구조적 장치, 행위 또는 모듈이 첨부된 청구범위에 기재된 본 발명의 사상과 범위를 벗어나지 않고서 소프트웨어, 펌웨어, 특수 목적 디지털 논리 및 이들로 이루어진 임의의 조합으로 구현될 수 있다는 점을 알 것이다.

도 4는 본 발명의 일 실시예에 따른 아이덴티티 정보 교환을 개시하는 과정을 나타낸 플로우차트이다. 이 플로우차트에서 프로세스는 선택 동작(405)으로 시작한다. 선택 동작(405)은 아이덴티티 정보 문서에 포함될 아이덴티티 정보를 자기 아이덴티티 정보 저장부로부터 선택하는 과정을 포함한다. 선택 동작은 소정의 상황에 있어서 미리 선택된 아이덴티티 정보 세트가 그 아이덴티티 확인된 경우 자동으로나 GUI를 통한 사용자 입력에 기초하여 아이덴티티 정보 문서에 포함시킬 아이덴티티 정보를 선택한다. 그런 다음, 제어가 판독 동작(410)으로 진행한다.

판독 동작(410)은 선택된 아이덴티티 정보를 자기 아이덴티티 정보 저장부로부터 판독하는 과정을 포함한다. 이러한 판독 동작은 선택된 아이덴티티 정보의 위치를 찾고 그 정보를 자기 아이덴티티 정보 저장부로부터 검색해 낸다. 그런 다음, 제어가 생성 동작(415)으로 진행한다.

생성 동작(415)은 선택되어 자기 아이덴티티 정보 저장부로부터 판독된 정보를 포함하는 아이덴티티 정보 문서를 생성하는 과정을 포함한다. 생성 동작(415)은 선택된 정보로부터 아이덴티티 정보 문서를 구성해낸다. 후술하는 바와 같이, 아이덴티티 정보 문서는 XML 파일을 포함할 수 있다. 이와 달리, 아이덴티티 정보 문서는 각종 매체를 통해서 이종 시스템들로 정보를 전달하기에 적합한 임의의 형태일 수 있다. 또한, 아이덴티티 정보 문서는 적어도 하나의 제1 키, 예컨대 하나 이상의 공개키(예컨대, 인증서로 캡슐화되어 있을 수 있음)를 포함한다. 아이덴티티 정보 문서는 그 아이덴티티 정보 문서에 포함된 공개키들 중 하나와 쌍을 이루는 비밀키 등의 제2 키를 이용하여 디지털 서명이 이루어진다. 그런 다음, 제어는 송신 동작(420)으로 넘어간다.

송신 동작(420)은 아이덴티티 정보 문서를 채널을 통해 수신 시스템으로 송신하는 과정을 포함한다. 이 송신 동작은 아이덴티티 정보 문서를 수신 시스템으로의 발신(outgoing) 신호로써 전송, 전달 또는 송신한다. 전술한 바와 같이, 채널은 안전할 수도 안전하지 않을 수도 있다. 아이덴티티 정보 문서가 송신될 수 있는 채널의 예로는 이메일, 인스턴트 메시지 전달, 빔 전송, 전용선 등이 있으나, 이에 한정되는 것은 아니다.

도 5는 본 발명의 일 실시예에 따른 아이덴티티 정보 수신을 도시한 플로우차트이다. 이 예에서 프로세스는 수신 동작(505)으로 시작한다. 수신 동작(505)은 전술한 것과 같은 채널로부터 아이덴티티 정보 문서를 수신하는 과정을 포함한다. 수신 동작은 개시 시스템으로부터의 입력 신호를 처리하여 그 입력 신호로부터 아이덴티티 정보 문서를 복구한다. 그런 다음, 제어는 질의 동작(510)으로 넘어간다.

질의 동작(510)은 아이덴티티 정보 문서로써 수신된 아이덴티티 정보가 믿을 수 있는 것인지 여부를 판단한다. 질의 동작은 정보 수신 방법에 관한 많은 상황들에 기초하여 아이덴티티 정보의 신뢰성을 테스트한다. 일부 경우에는, 그와 같은 신뢰성 판단이 그 정보를 수용할지 또는 거부할지 여부에 관한 GUI를 통해서 이루어지는 사용자에 대한 질의에 의존할 수 있다. 다른 경우에는, 휴리스틱 알고리즘을 이용하여, 정보 전달에 이용된 매체, 정보의 감도, 그리고 임의의 수의 기타 기준에 근거해서 자동으로 판단을 내릴 수 있다. 정보가 신뢰할 수 있는 것이라고 판단되면, 제어는 저장 동작(530)으로 넘어가고, 저장 동작은 아이덴티티 정보 문서에서 수신된 아이덴티티 정보를 인식 아이덴티티 정보 저장부에 저장한다. 저장 동작에 의하여 아이덴티티 정보를 인식 아이덴티티 정보 저장부에 기록한 후에는 동작 플로우가 메인 프로그램 플로우로 복귀한다.

만일 질의 동작(510)에서 아이덴티티 정보가 신뢰할 수 없는 것이라고 판단되면, 제어는 질의 동작(515)으로 넘어간다. 검증 질의 동작(515)은 그 아이덴티티 정보 문서를 검증할 것인지 여부를 결정하는 과정을 포함한다. 이러한 판단은 디폴트로써 자동으로 이루어지거나, GUI를 통한 사용자 입력에 따라 행해지거나, 사용자가 프로그램할 수 있는 많은 수의 기타 기준에 따라 행해질 수 있다. 만일 검증 질의 동작(515)에서 그 아이덴티티 정보를 검증하지 않을 것이라고 결정되면, 더 이상 프로세스가 수행되지 않고 동작 플로우는 메인 프로그램 플로우로 복귀한다. 그러나 아이덴티티 정보를 검증할 것이라고 결정하면, 제어는 검색 동작(520)로 넘어간다.

IRN 검색 동작(520)은 개시 시스템, 즉 발신자로부터 IRN을 검색하는 과정을 포함한다. 검색 동작은 또 다른 채널을 통하여 개시 시스템, 즉 발신자와 접촉하도록 수신 시스템에게 명령을 내리거나, 수신 시스템 사용자를 촉구한다. 예컨대, 사용자는 전화로 발신자를 호출하거나 IM(인스턴트 메시지 전달)을 통해 발신자에게 메시지를 송신하여 그 발신자로 하여금 자신의 IRN을 확인할 것을 요청할 수 있다.

IRN 생성 동작(523)은 아이덴티티 정보 문서로써 수신된 공개키에 기초하여 수신 시스템에서 IRN을 재작성한다. IRN을 계산하기 위하여 IRN 생성 동작(523)에서는 아이덴티티 정보 문서로써 전송된 공개키를 해시한다. 이와 달리, 발신자의 디스플레이 이름(도 6)이 공개키와 조합되고 그 조합이 해시될 수도 있다. 그런 다음 해시 동작의 결과에 대해 마스킹 알고리즘이 수행되어 AAA-AA-AA-AAA 형태의 영숫자 서명을 생성할 수 있다(여기서, 'A'는 영숫자를 나타낸다). IRN 생성 동작(523)에서 계산된 IRN은 예컨대 732-AB-5H-XVQ와 같이 보일 수 있다. 그런 다음, 두 개의 IRN이 IRN 테스트 동작(525)에서 비교된다.

IRN 테스트 동작(525)은 IRN이 올바른 것인지 여부를 판단하는 과정을 포함한다. IRN 테스트 동작(525)은 수신 시스템에서 생성된 계산 IRN을 개시 시스템으로부터 검색된 검색 IRN과 비교한다. MITM 공격이 송신자를 스푸핑하도록 공개키 정보를 교체함으로써 수신자에 의해 수신된 아이덴티티 정보를 함부로 변경시킨 경우라면, 그 계산 IRN은 발신자 또는 개시 시스템, 즉 진정한 송신자로부터의 검색 IRN과 매칭되지 않을 것이다.

IRN이 올바른 것으로 판정되면, 제어는 저장 동작(530)으로 넘어간다. 저장 동작(530)은 아이덴티티 정보 문서로써 수신된 아이덴티티 정보를 인식 아이덴티티 정보 저장부에 저장한다. 그런 다음 동작 플로우는 수신 시스템에서의 메인 제어 프로그램으로 복귀한다.

이와 달리, 거부된 아이덴티티 정보라 하더라도 인식 아이덴티티 정보 저장부에 저장될 수 있다. 예컨대, 소정의 아이덴티티 정보 세트가 거부된 경우라 하더라도, 장래의 참고를 위하여 이를 저장하고 아울러 신뢰할 수 없는 것이라고 표시할 수 있다. 이와 같이 인식은 되었으되 신뢰할 수 없는 아이덴티티 정보는 인식 아이덴티티 정보 저장부의 특별한 부분에 저장되거나 소정의 방식으로 태그 또는 플래그하여 표시할 수 있다. 그와 같은 정보는 장래에 신뢰할 수 없는 아이덴티티 정보에 대한 아이덴티티 확인에 유용할 수 있다.

도 6은 본 발명의 일 실시예에 따른 아이덴티티 정보 문서의 예시적 포맷을 도시한 도면이다. 데이터 구조로서, 인식 정보 문서(600)는 하나의 키로 묶이고 내포된 이용 정책에 의해 관리되는 아이덴티티 클레임 및 속성/특성 클레임의 모음이다. 아이덴티티 정보에 대한 인코딩 언어로서 XML이 이용될 것이다. 그러나, 다른 포맷도 마찬가지로 적합한 것으로 생각할 수 있다. 또한 아이덴티티 정보 문서(600)가 기밀이 유지되어야 하는 기밀 정보를 포함하고 있다면 그 아이덴티티 정보 문서(600)의 구성 요소들이 선택적으로 암호화될 수 있다.

아이덴티티 정보 문서(600)의 데이터는 두 개의 범주로 분류될 수 있다. 이들 범주에는 일련의 논리 컴포넌트(601)와 일련의 속성 태그(608)가 포함된다. 아이덴티티 정보 문서는 6개의 주요 논리 컴포넌트들, 즉 1) 아이덴티티 정보 주체 식별자(602), 2) 그 주체에 관한 하나 이상의 아이덴티티 클레임(603), 3) 그 주체에 관한 디스플레이 이름과 0개 이상의 선택적으로 공개되는 속성(604), 4) 임의 의 수용 가능한 포맷으로 구성된 해당 주체에 관한 하나 이상의 키(예컨대, X509v3 인증서에서의 공개키)(605), 5) 해당 주체의 프라이버시 요구 조건을 표시하는 이용 정책(606) 및 6) 아이덴티티 정보 갱신의 경우에 송신자를 인증하고 데이터의 무결성을 보호하는 아이덴티티 정보의 전체 내용에 대한 디지털 서명(607)을 갖는다. 이들 6개의 논리 컴포넌트(601)에 대해 차례로 설명한다.

주체 식별자(602)는 이름 식별자로 표현되는 아이덴티티 클레임들 중 하나에 의해서 식별되는 엔티티로서 그 아이덴티티 정보의 주체를 나타낸다. 주체 타입이 사람인 경우 아이덴티티 정보 주체에 대한 바람직한 이름 식별자 또는 아이덴티티 클레임은 이메일 어드레스이다.

아이덴티티 클레임(603)은 아이덴티티 정보 문서의 주체를 고유하게 식별시키는 구조화된 정보를 포함한다. 아이덴티티 클레임은 소정 기간 동안 단일 당사자의 아이덴티티를 확인하기 위하여 소정 타입의 기관에 의해서 할당된 값이다. 아이덴티티 정보 문서 내의 아이덴티티 클레임은 다양한 네임스페이스(namespace)에 속한 당사자의 아이덴티티를 확인하고, 당사자의 아이덴티티가 일단 확인되고 나면 디스플레이 이름과 물리적 메일링 어드레스와 같은 기타 공개 정보가 그 당사자에 대한 추가적 정황(context)을 제공한다.

디스플레이 이름(604)은 검색과 동작 중에 수신자 시스템 상에서 이용될 수 있다. 그러나, 반드시 이에 한정될 필요는 없다. 아이덴티티 정보의 주체 명세 사항(specification)에 의하여 당사자가 일단 아이덴티티 확인되고 나면 디스플레이 이름과 기타 공개 정보(물리적 메일링 어드레스 등)가 그 당사자에 대한 추가적 정황을 제공한다. 공개 정보는 그 주체에 대한 기술적(descriptive) 정보로 구성된다. 이는 일련의 특성으로 표현될 수 있다. 소정의 특성들은 표준화될 수 있으며, 확장 메커니즘이 있을 수 있다.

키(605)에는 아마도 인증서 포맷(예컨대, X509v3 인증서) 내에 캡슐화되어 있을 하나 이상의 키가 포함된다. 키(605)는 공개키일 수 있으며, 아이덴티티 정보의 주체에 대한 인식 정보로서 아이덴티티 정보에 포함될 수 있다. 인증서가 이용되는 경우, 이는 인증 기관에 의해 발행되거나 자기 서명될 수 있다.

이용 정책(606)은 아이덴티티 정보의 내용에 대하여 가해질 수 있는 이용에 관한 발신자의 명령을 수신자에게 전달한다. 예컨대, 이것은 아이덴티티 정보의 내용이 다른 사람에게 누설되어서는 안된다는 것을 나타낼 수 있다. 인식 아이덴티티 정보 저장부는 당사자를 규정하는 나머지 정보들과 함께 이와 같은 이용 정책을 저장할 것이며, 사용자가 예컨대 공유될 것으로 의도하지 않은 당사자에게 사본을 제공하고자 시도한다면, 시스템은 그 사용자에게 발신자의 의도를 나타내는 경고를 디스플레이할 것이다.

디지털 서명(607)은 아이덴티티 정보 문서 내의 데이터 서명을 제공한다. XML 서명은 서명을 문서와 관련시키는 3가지 방식, 즉 엔벌로핑 방식(enveloping), 엔벨로프형 방식(enveloped), 그리고 분리형 방식(detached)을 갖고 있다. 본 발명의 일 실시예에 따르면, 아이덴티티 정보 문서는 아이덴티티 정보 내용에 대한 서명시 XML 엔벨로프형 서명을 이용한다.

아이덴티티 정보 문서(600)는 6가지 속성 태그(608), 즉 1) 아이덴티티 정보 ID(609), 2) 메이저 버전(610), 3) 마이너 버전(611), 4) 주체 타입(612), 5) 정보 타입(613) 및 6) 이슈 인스턴트(issue instant)(614)를 가질 수 있다. 이들 속성 태그(608) 각각에 대해 아래에서 설명한다.

아이덴티티 정보 ID(609)는 아이덴티티 정보 문서에 대한 식별자이다. 이는 아이덴티티 정보 문서가 그 문서의 다른 부분으로부터 참조될 수 있는 식별자를 제공한다.

메이저 버전(610)은 이 아이덴티티 정보 문서의 메이저 버전 번호이다. 마이너 버전(611)은 이 아이덴티티 정보 문서의 마이너 버전 번호이다.

주체 타입(612)은 이 아이덴티티 정보 문서의 주체인 당사자 타입이다. 개인, 컴퓨터, 기관 등과 같이 여러 가지 타입의 당사자가 있을 수 있다.

정보 타입(613)은 이 아이덴티티 정보의 타입이다. 예컨대, "신규(New)" 아이덴티티 정보가 인식 아이덴티티 정보 저장부로 반입되어 새로운 당사자를 생성할 수 있고, 또는 "갱신(Update)" 아이덴티티 정보가 이용되어 기존의 당사자에 대해 최근 변화를 반영하여 개선할 수 있다.

이슈 인스턴트 속성(614)은 아이덴티티 정보가 발행 즉 생성되었을 때의 타임 인스턴트로서 UTC로 표현된 것이다. 아이덴티티 정보의 주체에 관한 기존의 표시가 구식인지 새로운 것인지를 판단하는데 갱신 아이덴티티 정보 상의 타임 스탬프가 이용될 수 있다.

지금까지 컴퓨터의 구조적 특성과 방법론적 행위에 대하여, 그리고 컴퓨터 판독가능 매체에 의하여 특정적인 언어로 본 발명을 설명하였지만, 첨부된 청구범위에서 정의되는 본 발명은 개시된 특정한 구조, 행위 또는 매체에 한정되는 것이 아님을 알아야 한다. 예컨대, XML 이외의 다른 포맷도 아이덴티티 정보를 인코딩하는데 이용될 수 있다. 그러므로, 이러한 특정적인 구조적 특성, 행위 및 매체는 청구되는 본 발명을 구현하는 예시적인 실시예로서 개시된 것이다.

전술한 여러 가지 실시예들은 단지 예시적인 것이며 본 발명을 한정하는 것으로 해석되어서는 안된다. 당업자라면 전술한 예시적인 실시예와 그 응용에 따르지 않고서도 첨부된 청구범위에 기재된 본 발명의 본질과 범위로부터 벗어남이 없이 본 발명을 여러 가지로 변경 및 수정할 수 있음을 잘 알 것이다.

(57) 청구의 범위

청구항 1.

아이덴티티 정보 문서(identity information document)를 송신하는 방법으로서,

상기 아이덴티티 정보 문서에 포함시킬 아이덴티티 정보를 자기 아이덴티티 정보 저장부(self-identity information store)로부터 선택하는 단계와,

상기 선택된 아이덴티티 정보를 상기 자기 아이덴티티 정보 저장부로부터 판독하는 단계와,

상기 선택된 아이덴티티 정보와 적어도 하나의 제1 키 - 상기 아이덴티티 정보 문서는 상기 아이덴티티 정보 문서 내의 상기 제1 키와 연관된 제2 키를 이용하여 서명됨 - 를 포함하도록 상기 아이덴티티 정보 문서를 생성하는 단계와,

상기 아이덴티티 정보 문서를 수신자에게 송신하는 단계

를 포함하는 아이덴티티 정보 문서 송신 방법.

청구항 2.

제1항에 있어서,

상기 아이덴티티 정보 선택 단계는 그래픽 유저 인터페이스(GUI)로부터의 사용자 입력에 기초하여 상기 자기 아이덴티티 정보 저장부로부터 아이덴티티 정보 서브세트를 선택하는 단계를 포함하는 아이덴티티 정보 문서 송신 방법.

청구항 3.

제1항에 있어서,

상기 아이덴티티 정보 선택 단계는 상기 자기 아이덴티티 정보 저장부로부터 미리 정해진 정보 서브세트를 선택하는 단계를 포함하는 아이덴티티 정보 문서 송신 방법.

청구항 4.

제1항에 있어서,

상기 아이덴티티 정보 문서 생성 단계는 상기 선택된 아이덴티티 정보를 확장형 마크업 언어(XML) 문서로 인코딩하는 단계를 포함하는 아이덴티티 정보 문서 송신 방법.

청구항 5.

제1항에 있어서,

상기 선택된 아이덴티티 정보는 상기 아이덴티티 정보 문서를 발신하는 당사자(principal)의 아이덴티티 클레임들(claims)을 포함하는 아이덴티티 정보 문서 송신 방법.

청구항 6.

제1항에 있어서,

상기 선택된 아이덴티티 정보는 상기 아이덴티티 정보의 내용에 대해 이루어질 수 있는 이용에 관하여 규정하는 이용 정책들(use policies)을 포함하는 아이덴티티 정보 문서 송신 방법.

청구항 7.

아이덴티티 정보 문서를 수신하는 방법으로서,

발신자로부터 서명된 아이덴티티 정보 문서를 수신하는 단계와,

상기 아이덴티티 정보 문서 내의 아이덴티티 정보가 신뢰할 수 있는 것인지(reliable) 판단하는 단계와,

상기 아이덴티티 정보가 신뢰할 수 있는 것이라고 판단된 경우, 상기 아이덴티티 정보를 인식 아이덴티티 정보 저장부(recognized identity information store)에 저장하는 단계

를 포함하는 아이덴티티 정보 문서 수신 방법.

청구항 8.

제7항에 있어서,

상기 아이덴티티 정보가 신뢰할 수 없는 것이라는 판단에 응답하여, 상기 아이덴티티 정보를 검증(verify)할 것인지 여부를 판단하는 단계와,

상기 아이덴티티 정보를 검증하기로 판단함에 응답하여, 상기 아이덴티티 정보 문서의 상기 발신자로부터 아이덴티티 인식 번호(Identification Recongnition Number : IRN)를 검색하고, 상기 IRN이 정확한 것인지 여부를 판단하고, 상기 IRN이 정확하다는 판단에 응답하여, 상기 아이덴티티 정보를 상기 인식 아이덴티티 정보 저장부에 저장하는 단계

를 더 포함하는 아이덴티티 정보 문서 수신 방법.

청구항 9.

제8항에 있어서,

상기 아이덴티티 정보가 신뢰할 수 있는 것인지 판단하는 단계가 그래픽 유저 인터페이스를 통한 사용자 입력에 기초하는 아이덴티티 정보 문서 수신 방법.

청구항 10.

제8항에 있어서,

상기 아이덴티티 정보를 검증할 것인지 여부를 판단하는 단계가 그래픽 유저 인터페이스를 통한 사용자 입력에 기초하는 아이덴티티 정보 문서 수신 방법.

청구항 11.

아이덴티티 정보 문서를 송신하는 시스템으로서,

프로세서와,

상기 프로세서에 접속된 통신 채널과,

상기 프로세서에 연결되고 상기 프로세서에 의해서 판독 가능한 메모리

를 포함하고,

상기 메모리는 일련의 명령어들을 포함하는데, 상기 명령어들은 상기 프로세서에 의해 실행될 경우 상기 프로세서로 하여금 상기 아이덴티티 정보 문서에 포함시킬 아이덴티티 정보를 자기 아이덴티티 정보 저장부로부터 선택하게 하고, 상기 선택된 아이덴티티 정보를 상기 자기 아이덴티티 정보 저장부로부터 판독하게 하며, 상기 선택된 아이덴티티 정보와 적어도 하나의 제1 키 - 상기 아이덴티티 정보 문서는 상기 제1 키와 쌍을 이루는 제2 키를 이용하여 서명됨 - 를 포함하도록 상기 아이덴티티 정보 문서를 생성하게 하고, 상기 아이덴티티 정보 문서를 상기 통신 채널에 접속된 수신자에게 송신하도록 하는

아이덴티티 정보 문서 송신 시스템.

청구항 12.

제11항에 있어서,

상기 아이덴티티 정보 선택의 과정은 그래픽 유저 인터페이스(GUI)로부터의 사용자 입력에 기초하여 상기 자기 아이덴티티 정보 저장부로부터 아이덴티티 정보 서브세트를 선택하는 과정을 포함하는 아이덴티티 정보 문서 송신 시스템.

청구항 13.

제11항에 있어서,

상기 아이덴티티 정보 선택의 과정은 상기 자기 아이덴티티 정보 저장부로부터 미리 정해진 정보 서브세트를 선택하는 과정을 포함하는 아이덴티티 정보 문서 송신 시스템.

청구항 14.

제11항에 있어서,

상기 아이덴티티 정보 문서 생성의 과정은 상기 선택된 아이덴티티 정보를 확장형 마크업 언어(XML) 문서로 인코딩하는 과정을 포함하는 아이덴티티 정보 문서 송신 시스템.

청구항 15.

제11항에 있어서,

상기 선택된 아이덴티티 정보는 상기 아이덴티티 정보 문서를 발신하는 당사자의 아이덴티티 클레임들을 포함하는 아이덴티티 정보 문서 송신 시스템.

청구항 16.

제11항에 있어서,

상기 선택된 아이덴티티 정보는 상기 아이덴티티 정보의 내용에 대해 이루어질 수 있는 이용에 관하여 규정하는 이용 정책들을 포함하는 아이덴티티 정보 문서 송신 시스템.

청구항 17.

발신자로부터 장래의 상기 발신자 인식에 이용하기 위한 아이덴티티 정보 문서를 수신하는 시스템으로서,

프로세서와,

상기 프로세서에 접속된 통신 채널과,

상기 프로세서와 연결되고 상기 프로세서에 의해 판독 가능한 메모리

를 포함하고,

상기 메모리는 일련의 명령어들을 포함하는데, 상기 명령어들은 상기 프로세서에 의해 실행될 경우 상기 프로세서로 하여금 상기 발신자로부터 서명된 아이덴티티 정보 문서를 수신하도록 하고, 상기 아이덴티티 정보 문서에 포함된 아이덴티티 정보가 신뢰할 수 있는 것인지 판단하게 하며, 상기 아이덴티티 정보가 신뢰할 수 있는 것이라고 판단된 경우 상기 아이덴티티 정보를 인식 아이덴티티 정보 저장부 - 상기 인식 아이덴티티 정보 저장부는 장래의 상기 발신자 인식에 이용됨 - 에 저장하도록 하는

아이덴티티 정보 문서 수신 시스템.

청구항 18.

제17항에 있어서,

상기 아이덴티티 정보가 신뢰할 없는 것이라는 판단에 응답하여, 상기 아이덴티티 정보를 검증할 것인지 여부를 판단하도록 하고,

상기 아이덴티티 정보를 검증하기로 판단함에 응답하여, 상기 아이덴티티 정보 문서의 상기 발신자로부터 아이덴티티 인식 번호(IRN)를 수신하게 하고, 상기 IRN이 정확한 것인지 여부를 판단하도록 하며, 상기 IRN이 정확하다는 판단에 응답하여, 상기 아이덴티티 정보를 상기 인식 아이덴티티 정보 저장부에 저장하도록 하는 아이덴티티 정보 문서 수신 시스템.

청구항 19.

제18항에 있어서,

상기 아이덴티티 정보가 신뢰할 수 있는 것인지 판단하는 과정이 그래픽 유저 인터페이스를 통한 사용자 입력에 기초하는 아이덴티티 정보 문서 수신 시스템.

청구항 20.

제18항에 있어서,

상기 아이덴티티 정보를 검증할 것인지 여부를 판단하는 과정이 그래픽 유저 인터페이스를 통한 사용자 입력에 기초하는 아이덴티티 정보 문서 수신 시스템.

청구항 21.

아이덴티티 인식을 위한 컴퓨터 프로세스를 실행하는 명령어들로 이루어진 컴퓨터 프로그램을 인코딩하는 컴퓨터 판독가능 매체에 있어서,

상기 컴퓨터 프로세스는

아이덴티티 정보 문서에 포함시킬 아이덴티티 정보를 자기 아이덴티티 정보 저장부로부터 선택하는 단계와,

상기 선택된 아이덴티티 정보를 상기 자기 아이덴티티 정보 저장부로부터 판독하는 단계와,

상기 선택된 아이덴티티 정보와 적어도 하나의 제1 키 - 상기 아이덴티티 정보 문서는 상기 아이덴티티 정보 문서 내의 상기 제1 키와 연관된 제2 키로 서명됨 - 를 포함하도록 상기 아이덴티티 정보 문서를 생성하는 단계와,

상기 아이덴티티 정보 문서를 수신자에게 송신하는 단계

를 포함하는 컴퓨터 판독가능 매체.

청구항 22.

제21항에 있어서,

상기 아이덴티티 정보 선택 단계는 그래픽 유저 인터페이스(GUI)로부터의 사용자 입력에 기초하여 상기 자기 아이덴티티 정보 저장부로부터 아이덴티티 정보 서브세트를 선택하는 단계를 포함하는 컴퓨터 판독가능 매체.

청구항 23.

제21항에 있어서,

상기 아이덴티티 정보 선택 단계는 상기 자기 아이덴티티 정보 저장부로부터 미리 정해진 정보 서브세트를 선택하는 단계를 포함하는 컴퓨터 판독가능 매체.

청구항 24.

제21항에 있어서,

상기 아이덴티티 정보 문서 생성 단계는 상기 선택된 아이덴티티 정보를 확장형 마크업 언어(XML) 문서로 인코딩하는 단계를 포함하는 컴퓨터 판독가능 매체.

청구항 25.

제21항에 있어서,

상기 선택된 아이덴티티 정보는 상기 아이덴티티 정보 문서를 발신하는 당사자의 아이덴티티 클레임들을 포함하는 컴퓨터 판독가능 매체.

청구항 26.

제21항에 있어서,

상기 선택된 아이덴티티 정보는 상기 아이덴티티 정보의 내용에 대해 이루어질 수 있는 이용에 관하여 규정하는 이용 정책들을 포함하는 컴퓨터 판독가능 매체.

청구항 27.

제21항에 있어서,

발신자로부터 서명된 아이덴티티 정보 문서를 수신하는 단계와,

상기 아이덴티티 정보 문서에 포함된 아이덴티티 정보가 신뢰할 수 있는 것인지 판단하는 단계와,

상기 아이덴티티 정보가 신뢰할 수 있는 것이라고 판단된 경우, 상기 아이덴티티 정보를 장래의 상기 발신자 인식을 위한 인식 아이덴티티 정보 저장부에 저장하는 단계를 포함하는 컴퓨터 판독가능 매체.

청구항 28.

제27항에 있어서,

상기 아이덴티티 정보가 신뢰할 없는 것이라는 판단에 응답하여, 상기 아이덴티티 정보를 검증할 것인지 여부를 판단하는 단계와,

상기 아이덴티티 정보를 검증하기로 판단함에 응답하여, 상기 아이덴티티 정보 문서의 발신 시스템으로부터 검색 아이덴티티 인식 번호(IRN)를 검색하고, 상기 아이덴티티 정보 문서 내의 정보에 기초하여 상기 수신 시스템에서 계산 IRN을 생성하고, 상기 검색 IRN을 상기 계산 IRN과 비교하여 상기 계산 IRN이 검증되는지 판정하고, 상기 계산 IRN이 검증됨에 응답하여 상기 아이덴티티 정보를 상기 인식 아이덴티티 정보 저장부에 저장하는 단계를 더 포함하는 컴퓨터 판독가능 매체.

청구항 29.

제28항에 있어서,

상기 아이덴티티 정보가 신뢰할 수 있는 것인지 판단하는 단계가 그래픽 유저 인터페이스를 통한 사용자 입력에 기초하는 컴퓨터 판독가능 매체.

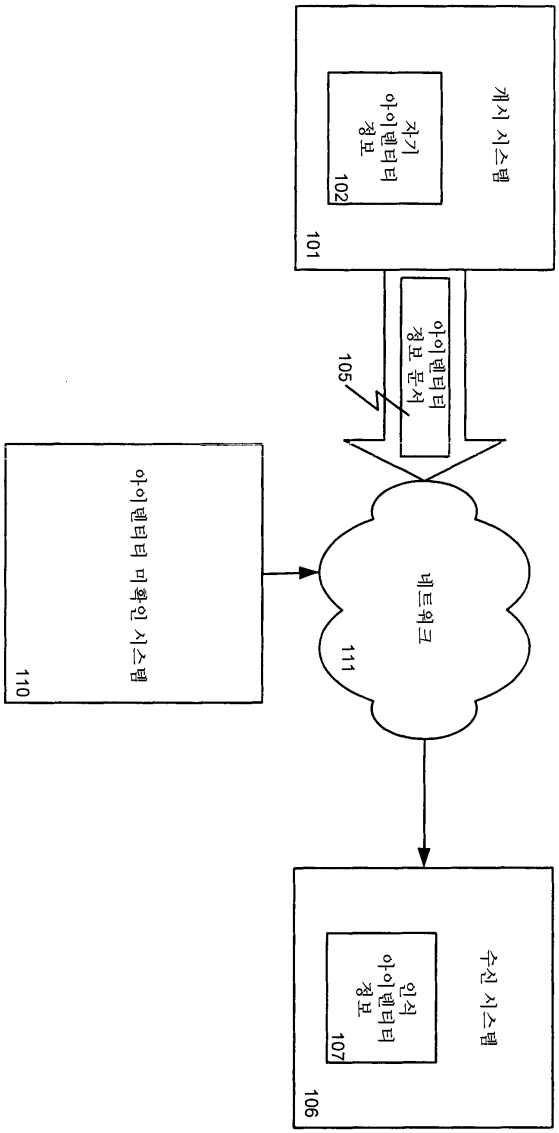
청구항 30.

제28항에 있어서,

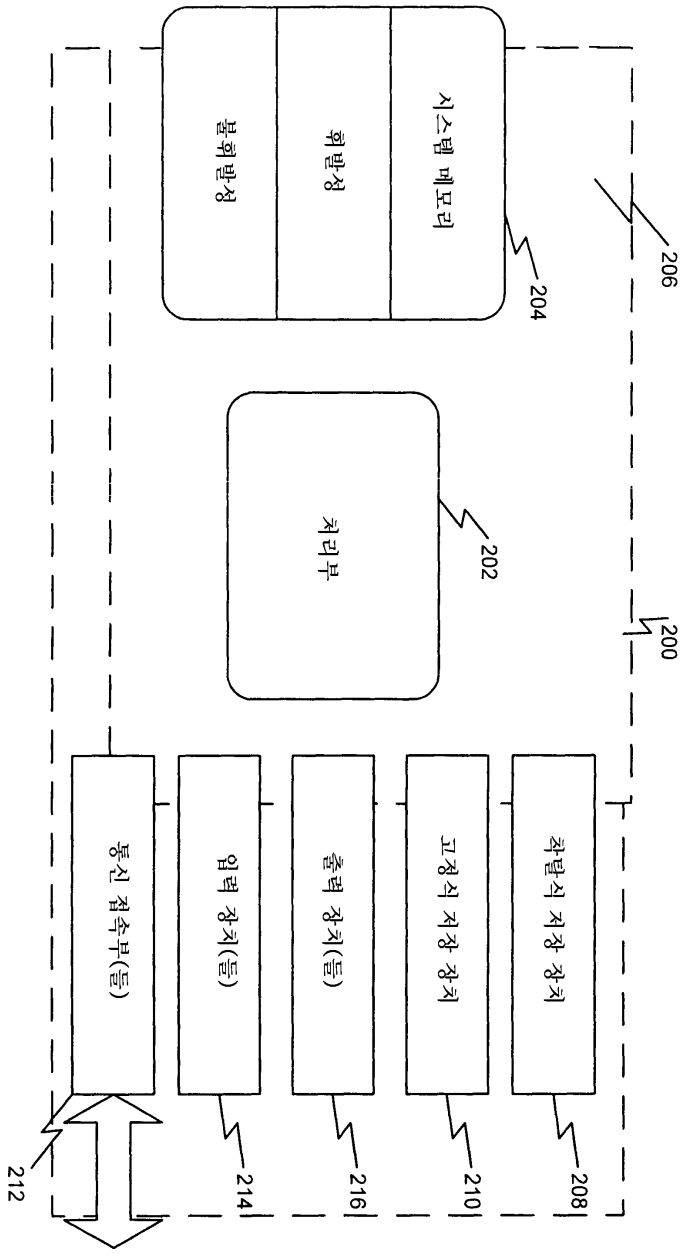
상기 아이덴티티 정보를 검증할 것인지 여부를 판단하는 단계가 그래픽 유저 인터페이스를 통한 사용자 입력에 기초하는 컴퓨터 판독가능 매체.

도면

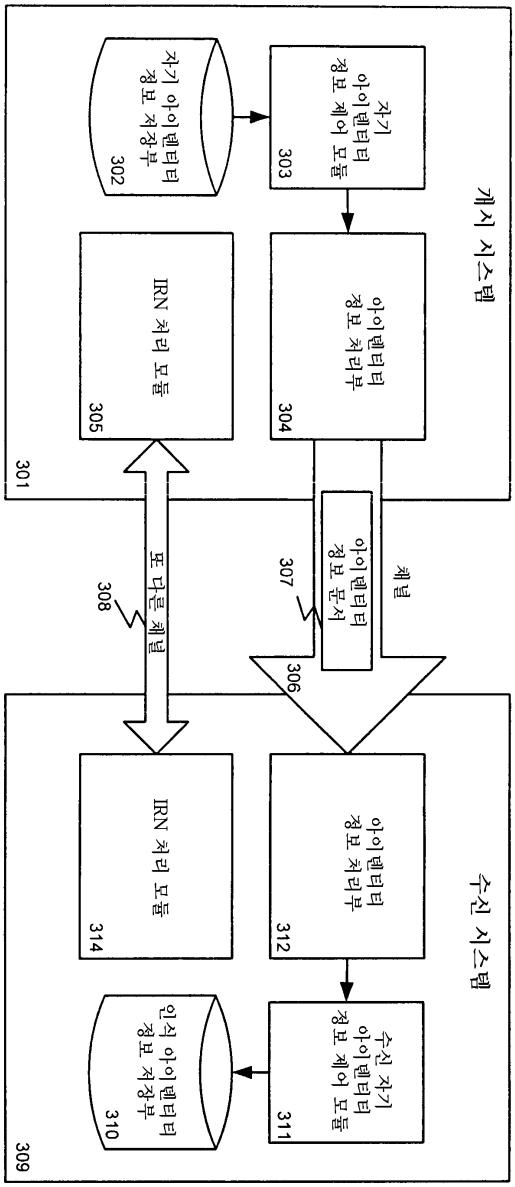
도면1


게시 시스템
101
자기 아이덴티티 정보
102
아이덴티티 정보 문서
105
네트워크
111
아이덴티티 미 확인 시스템
110
수신 시스템
106
인식 아이덴티티 정보
107

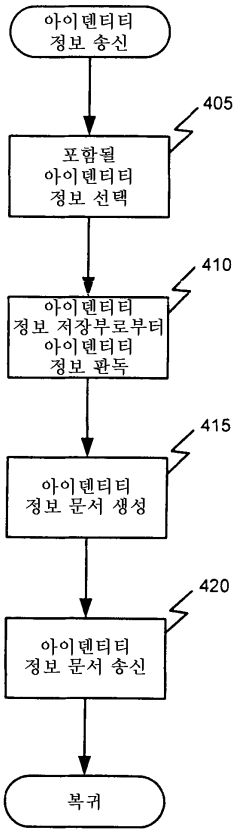
도면2


시스템 메모리
휘발성
불휘발성
204
206
처리부
202
200
착탈식 저장 장치
고정식 저장 장치
출력 장치(들)
입력 장치(들)
통신 접속부(들)
208
210
216
214
212

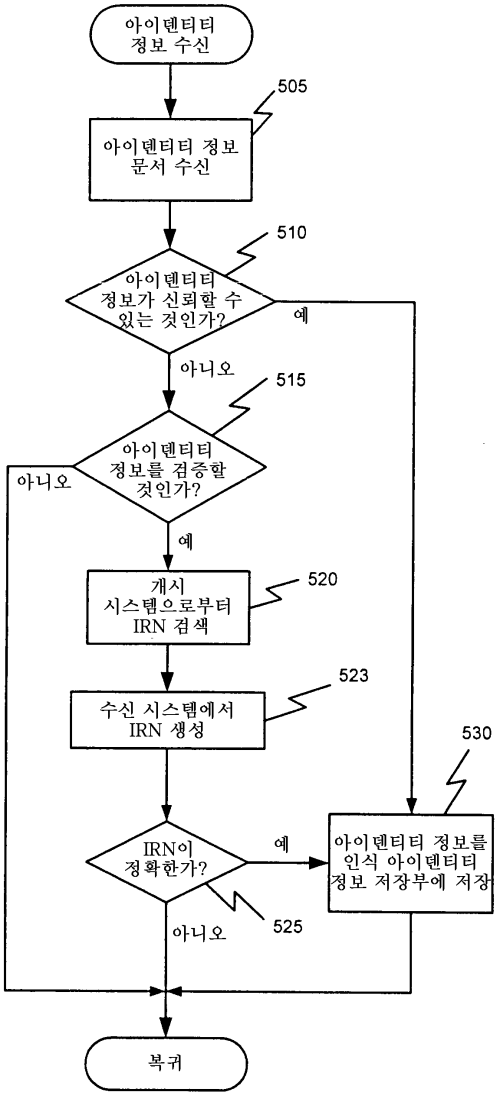
도면3


게시 시스템
301
자기 아이덴티티 정보 저장부
302
자기 아이덴티티 정보 제어 모듈
303
아이덴티티 정보 처리부
304
IRN 처리 모듈
305
아이덴티티 정보 문서
307
또 다른 채널
308
채널
306
수신 시스템
309
인식 아이덴티티 정보 저장부
310
수신 자기 아이덴티티 정보 제어 모듈
311
아이덴티티 정보 처리부
312
IRN 처리 모듈
314

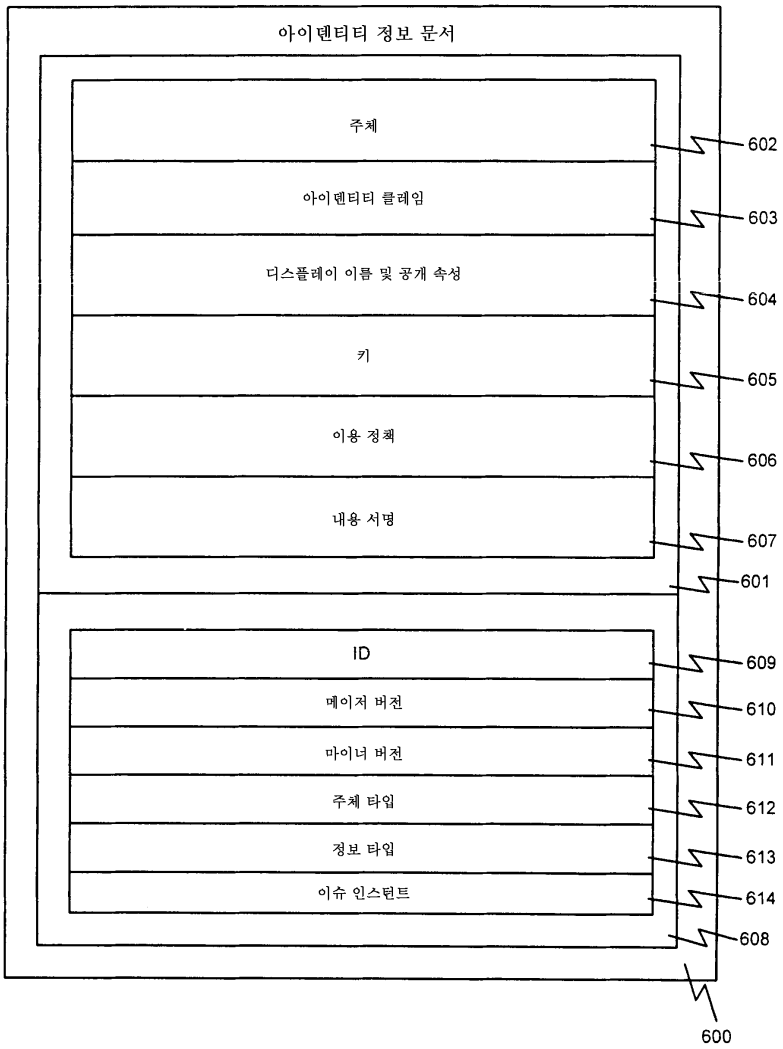
도면4


아이덴티티
정보 송신
405
포함될
아이덴티티
정보 선택
410
아이덴티티
정보 저장부로부터
아이덴티티
정보 판독
415
아이덴티티
정보 문서 생성
420
아이덴티티
정보 문서 송신
복귀

도면5


아이덴티티 정보 수신
505
아이덴티티 정보 문서 수신
510
아이덴티티 정보가 신뢰할 수 있는 것인가?
예
아니오
515
아이덴티티 정보를 검증할 것인가?
아니오
예
520
개시 시스템으로부터 IRN 검색
523
수신 시스템에서 IRN 생성
530
IRN이 정확한가?
예
아이덴티티 정보를 인식 아이덴티티 정보 저장부에 저장
525
아니오
복귀

도면6


아이덴티티 정보 문서
주체
아이덴티티 클레임
디스플레이 이름 및 공개 속성
키
이용 정책
내용 서명
ID
메이저 버전
마이너 버전
주체 타입
정보 타입
이슈 인스턴트
602
603
604
605
606
607
601
609
610
611
612
613
614
608
600