(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년01월22일
(11) 등록번호 10-1584510
(24) 등록일자 2016년01월06일

(51) 국제특허분류(Int. Cl.)
G06F 21/44 (2013.01) *G06F 21/33* (2013.01)
G06F 21/43 (2013.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2010-7017469
(22) 출원일자(국제) 2008년11월13일
심사청구일자 2013년10월29일
(85) 번역문제출일자 2010년08월05일
(65) 공개번호 10-2010-0126291
(43) 공개일자 2010년12월01일
(86) 국제출원번호 PCT/EP2008/065470
(87) 국제공개번호 WO 2009/089943
국제공개일자 2009년07월23일
(30) 우선권주장
10 2008 000 067.1 2008년01월16일 독일(DE)
(56) 선행기술조사문헌
KR1020060104268 A*
KR1020070012106 A*
US20050138421 A1
US20070204325 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
분데스드룩커라이 게엠베하
독일 10969 베를린 코만단텐스트라쎄 18
(72) 발명자
디트리히, 프랑크
독일 12437 베를린, 베어베리트첸웩 25
비스치오, 프랑크
독일 16348 반들리츠, 추어 하이데 19
패쉬크, 맨프레드
독일 16352 바스도르프, 안 데어 빌드반 61
(74) 대리인
임훈빈

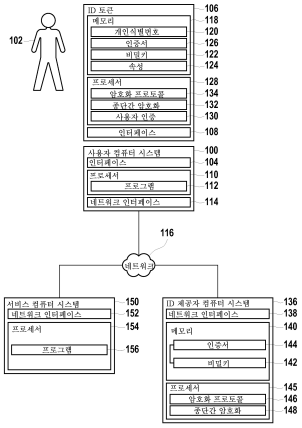
전체 청구항 수 : 총 11 항 심사관 : 서광훈

(54) 발명의 명칭 **아이디 토큰에서 속성을 판독하는 방법**

(57) 요 약

본 발명은 ID 토큰에서 적어도 하나의 속성을 판독하는 방법에 관한 것으로, ID 토큰은 사용자에게 할당된다. 본 발명의 방법은 ID 토큰에 대해 사용자를 인증하는 단계, ID 토큰에 대해 제 1 컴퓨터 시스템을 인증하는 단계, ID 토큰에 대한 사용자와 제 1 컴퓨터 시스템의 성공적인 인증 후에, 적어도 하나의 속성을 제 2 컴퓨터 시스템으로 전송하기 위해 제 1 컴퓨터 시스템이 ID 토큰에 저장된 적어도 하나의 속성으로 판독 액세스를 수행하는 단계를 포함한다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

ID 토큰(106, 106')에 저장된 적어도 하나의 속성을 판독하며 ID 토큰은 사용자(102)와 연관된 방법에 있어서,

사용자가 ID 토큰에 대해 인증되는 단계;

네트워크(116) 상에서 ID 토큰과 제 1 컴퓨터 시스템 간에 보호된 연결을 설정하는 단계;

상기 보호된 연결을 통해 제 1 컴퓨터 시스템(136)이 ID 토큰에 대해 인증되는 단계;

ID 토큰에 대한 사용자와 제 1 컴퓨터 시스템의 성공적인 인증 뒤에, 하나 이상의 판독 명령과 적어도 하나의 속성이 제 1 컴퓨터 시스템에 보호된 연결 상에서 종단간 암호화 수단을 포함하는 ID 토큰에서 제 1 컴퓨터 시스템으로 전송되고 제 1 컴퓨터 시스템에 의해 적어도 하나의 속성이 해독되게 하는 방법으로, ID 토큰에 저장된 적어도 하나의 속성에 대해 제 1 컴퓨터 시스템이 판독 액세스를 수행하는 단계;

를 포함하고,

ⅰ. 제 1 컴퓨터 시스템을 통하여 ID 토큰으로부터 판독된 적어도 하나의 속성을 서명하는 단계;

ii. 서명된 속성이 제 1 컴퓨터 시스템에서 제 2 컴퓨터 시스템으로 전송되는 단계;

를 더 포함하며,

상기 제 1 컴퓨터 시스템은 제 1 컴퓨터 시스템의 인증서(144)를 이용하여 ID 토큰에 대해 인증되며, 상기 인증서는 제 1 컴퓨터 시스템이 판독 액세스에 대한 권한을 부여받기 위하여 ID 토큰에 저장된 속성의 표시를 포함하고,

상기 ID 토큰은 인증서를 이용하여 적어도 하나의 속성으로의 판독 액세스에 대한 제 1 컴퓨터 시스템의 판독 권한을 검사하는,

ID 토큰(106, 106')에 저장된 적어도 하나의 속성을 판독하는 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

제 1 항에 있어서,

요구(164)가 제 3 컴퓨터 시스템(100)에서 제 2 컴퓨터 시스템으로 전송되는 단계;

제 2 컴퓨터 시스템이 하나 이상의 속성을 특정하는 단계; 및

속성의 상세(166)가 제 2 컴퓨터 시스템에서 제 1 컴퓨터 시스템으로 전송되는 단계를 더 포함하며,

제 1 컴퓨터 시스템에 의한 판독 액세스는 ID 토큰으로부터 속성의 상세에 특정된 하나 이상의 속성을 판독하기 위해 수행되는 ID 토큰(106, 106')에 저장된 적어도 하나의 속성을 판독하는 방법.

청구항 6

제 5 항에 있어서, 상기 요구(164)는 제 2 컴퓨터 시스템이 제 1 컴퓨터 시스템을 식별하기 위한 식별자를 포함하며, 상기 속성의 상세는 제 3 컴퓨터 시스템의 개입 없이 제 2 컴퓨터 시스템에서 제 1 컴퓨터 시스템으로 전송되는 ID 토큰(106, 106')에 저장된 적어도 하나의 속성을 판독하는 방법.

청구항 7

제 5 항에 있어서, 상기 제 3 컴퓨터 시스템은 복수의 미리 정의된 구성 데이터 레코드(158, 160, ...)를 포함하며, 각각의 구성 데이터 레코드는 속성의 부분 집합, 적어도 하나의 데이터 소스, 및 한 세트의 제 1 컴퓨터 시스템(136, 136', ...)으로부터의 제 1 컴퓨터 시스템을 특정하고, 속성의 상세는 우선 제 2 컴퓨터 시스템에서 제 3 컴퓨터 시스템으로 전송되어, 제 3 컴퓨터 시스템이 속성의 상세에서 특정된 적어도 하나의 속성을 포함하는 속성의 부분 집합을 특정하는 적어도 하나의 구성 데이터 레코드를 선택하기 위해 이용되며, 제 3 컴퓨터 시스템은 속성의 상세를 제 1 컴퓨터 시스템으로 전송하며, 그리고 제 1 컴퓨터 시스템과 선택된 구성 데이터 레코드에서의 데이터 소스의 표시에 의해 특정된 ID 토큰 사이의 연결이 제 3 컴퓨터 시스템을 통해 설정되는 ID 토큰(106, 106')에 저장된 적어도 하나의 속성을 판독하는 방법.

청구항 8

제 1 항, 제 5 항, 제 6 항 또는 제 7 항에 있어서, 제 1 컴퓨터 시스템에 의해 ID 토큰에서 판독된 적어도 하나의 속성은 제 3 컴퓨터 시스템으로 전송되는데, 상기 속성은 사용자에 의한 공개에 뒤이어 제 2 컴퓨터 시스템으로 전송되는 ID 토큰에 저장된 적어도 하나의 속성을 판독하는 방법.

청구항 9

삭제

청구항 10

삭제

청구항 11

제 1 항, 제 5 항, 제 6 항 또는 제 7 항에 있어서, 상기 제 3 컴퓨터 시스템은 네트워크(116)를 통해 제 3 컴퓨터 시스템에게 다른 속성(A)을 요구하는 외부 데이터 소스를 특정하는 적어도 하나의 구성 데이터 레코드(161)를 포함하며, 상기 다른 속성은, 적어도 하나의 속성이 ID 토큰으로부터 판독됨과 아울러, 제 3 컴퓨터 시스템이 제 1 컴퓨터 시스템으로부터 적어도 하나의 서명된 속성을 수신한 이후에 요구되며, 상기 요구는 적어도 하나의 서명된 속성을 포함하는 ID 토큰(106, 106')에 저장된 적어도 하나의 속성을 판독하는 방법.

청구항 12

삭제

청구항 13

제 1 항, 제 5 항, 제 6 항 또는 제 7 항에 따른 방법을 수행하기 위해 컴퓨터 시스템에 의해서 실행될 수 있는 명령어를 포함하는 컴퓨터 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

네트워크(116) 연결 수단에 의하여 보호된 연결 상에 구비되는 적어도 하나의 제 1 컴퓨터 시스템(136)과 ID 토큰(106, 106')을 포함하는 컴퓨터 시스템에 있어서, 상기 제 1 컴퓨터 시스템은:

네트워크(116)를 통해 적어도 하나의 속성을 특정하는 속성의 상세(166)를 수신하는 수단(138);

ID 토큰 (106)에 대해 인증하는 수단(142,144,146)으로서, 상기 제 1 컴퓨터 시스템이 제 1 컴퓨터 시스템의 인증서(144)를 이용하여 ID 토큰에 대해 인증되며, 상기 인증서는 제 1 컴퓨터 시스템이 판독 액세스에 대한 권한을 부여받는 ID 토큰에 저장된 속성의 표시를 포함하는 인증 수단;

보호된 연결을 통해 ID 토큰으로부터 적어도 하나의 속성을 판독하는 수단;

을 포함하며,

적어도 하나의 속성을 판독하기 위해 필요한 조건은 ID 토큰에 연관된 사용자와 컴퓨터 시스템의 ID 토큰에 대한 인증이며,

제 1 컴퓨터 시스템을 통하여 ID 토큰으로부터 판독된 적어도 하나의 속성을 서명하는 수단;

서명된 속성이 제 1 컴퓨터 시스템에서 제 2 컴퓨터 시스템으로 전송되도록 하는 수단;

를 더 포함하며,

상기 ID 토큰은:

적어도 하나의 속성을 저장하는 보호된 메모리 영역(124);

ID 토큰에 대해, ID 토큰과 연관된 사용자(102)를 인증하는 수단(120, 130);

적어도 하나의 속성을 판독하기 위해 사용될 수 있는 제 1 컴퓨터 시스템에 대해 보호된 연결을 설정하는 수단(132);

제 1 컴퓨터 시스템으로 적어도 하나의 속성의 보호된 전송을 위한 연결의 종단간 암호화 수단;

을 포함하며,

상기 ID 토큰은 인증서를 이용하여 적어도 하나의 속성으로의 판독 액세스에 대한 제 1 컴퓨터 시스템의 판독 권한을 검사하는,

컴퓨터 시스템.

청구항 18

삭제

청구항 19

제 17 항에 있어서, 상기 수단(138)은 제 2 컴퓨터 시스템으로부터 속성의 상세를 수신하도록 설계되며, 제 2 컴퓨터 시스템으로의 전송을 위해 ID 토큰으로부터 판독된 적어도 하나의 속성을 제 3 컴퓨터 시스템(100)으로 전송하는 수단(138)을 포함하는 컴퓨터 시스템.

청구항 20

삭제

청구항 21

제 17 항 또는 제 19 항에 있어서, 다른 판독 권한을 갖는 다수의 인증서(144.1,144.2)를 포함하며, 상기 컴퓨터 시스템은 속성의 상세에서 특정된 속성을 판독하기에 충분한 판독 권한을 갖는 적어도 하나의 인증서의 선택의 기초로서 속성의 상세를 수신하도록 설계된 컴퓨터 시스템.

청구항 22

제 17 항 또는 제 19 항에 있어서, ID 토큰은 USB 스틱, 전자 기구, 가치 문서 또는 보안 문서인 컴퓨터 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 ID 토큰에서 적어도 하나의 속성을 판독하는 방법, 컴퓨터 프로그램 제품, ID 토큰 및 컴퓨터 시스템에 관한 것이다.

배 경 기 술

[0002] 종래의 기술은 사용자의 디지털 ID로 알려진 것을 관리하는 여러 가지 방법을 개시한다.

[0003] 마이크로소프트사의 Windows CardSpace는 인터넷 사용자가 그들의 디지털 ID를 온라인 서비스에 알리도록 해주는 클라이언트 기반 디지털 ID 시스템이다. 이에 관련된 결점은 특히 사용자가 자신의 디지털 ID를 조작할 수 있다는 것이다.

[0004] 이에 비해, OPENID는 서버 기반 시스템이다. ID 서버로 알려진 것은 등록된 사용자의 디지털 ID를 데이터베이스에 저장한다. 이의 하나의 결점은 특히 불충분한 데이터 보호인데, 이는 사용자의 디지털 ID가 중앙 집중적으로 저장되어 있으며 사용자의 행동도 기록 될 수 있기 때문이다.

[0005] 미국 특허 제 2007/0294431 A1호는 사용자 등록을 또한 요구하는 디지털 ID를 관리하는 다른 방법을 개시한다.

발명의 내용

해결하려는 과제

[0006] 이에 비해, 본 발명은 적어도 하나의 속성을 판독하는 향상된 방법, 적절한 컴퓨터 프로그램 제품, ID 토큰 및 컴퓨터 시스템을 제공하려는 목적에 기초한다.

[0007] 본 발명이 기초로 하는 목적들은 독립항의 특징에 의해 각각 달성된다. 본 발명의 실시예는 종속항에서 특정된다.

과제의 해결 수단

[0008] 본 발명은 사용자와 연관된 ID 토큰에 저장된 적어도 하나의 속성을 판독하는 방법을 제공한다. 상기 방법은 ID 토큰에 대해 사용자를 인증하는 단계; ID 토큰에 대해 제 1 컴퓨터 시스템을 인증하는 단계; ID 토큰에 대한 사용자와 제 1 컴퓨터 시스템의 성공적인 인증 뒤에, 적어도 하나의 속성이 서명되면 상기 적어도 하나의 속성을 제 2 컴퓨터 시스템으로 전송하기 위해, 제 1 컴퓨터 시스템이 ID 토큰에 저장된 적어도 하나의 속성으로 판독 액세스를 하는 단계를 포함한다. 이는 "신용 수단"이 제공되게 한다.

[0009] 본 발명은 ID 토큰에 저장된 하나 이상의 속성이 제 1 컴퓨터 시스템에 의해 판독되도록 한다. ID 토큰과 제 1 컴퓨터 시스템 사이의 연결은 네트워크 특히 인터넷을 통해 설정될 수 있다. 상기 적어도 하나의 속성은 ID 토큰과 연관된 사용자의 ID 특히 사용자의 디지털 ID의 표시 일수 있다. 일례로서, 제 1 컴퓨터 시스템은 이러한 속성을, 예를 들면 온라인 서비스로 제 2 컴퓨터 시스템에 전송하기 위하여, 성, 이름, 주소 같은 속성을 판독한다.

[0010] 그러나, 일례로서, 사용자의 ID를 규정하기 위해 사용되지 않으나, 특정 온라인 서비스를 사용하기 위해 사용자의 권한을 체크하는데 사용되는 사용자의 나이와 같은 단지 하나의 속성이 판독되는 것도 가능하다. 여기서, 사용자는 특정 나이 그룹을 위해 준비된 온라인 서비스를 사용하고 싶어 한다. 또는 온라인 서비스를 사용하도록 권한이 부여된 특정 그룹과 연관된 사용자임을 입증하는 다른 속성이 판독되는 것도 가능하다.

[0011] ID 토큰은 USB 스틱 같은 휴대용 전자 기구이거나, 특히 가치 문서나 보안 문서 같은 문서 일 수 있다.

[0012] 본 발명에 따라, "문서"는 특히 여권, ID 카드, 비자와 운전 면허증, 차량 등록 인증서, 차량 등록 문서, 기업 인식 카드, 건강 수첩, 또는 다른 ID 문서와 칩 카드 같은 신원 확인 자료, 특히 은행 카드와 신용 카드 같은 지불 수단, 화물 운송장이나 다른 신용 증명서 같은 종이-기반/또는 플라스틱-기반 문서를 의미한다고 이해할 수 있는데, 이는 적어도 하나의 속성을 저장하는 데이터 메모리를 포함한다.

[0013] 따라서 본 발명의 실시예들은 특히 유리한 이점이 있는데, 이는 적어도 하나의 속성이 특정 신용 가능한 문서, 예를 들어 사무실 문서로부터 판독되기 때문이다 . 또한 속성의 중앙 기억장치가 필요하지 않다는 것도 특히 유리한 이점이다. 따라서 본 발명은 최적의 데이터 보호에 의해 매우 편리한 처리를 수반하는 디지털 ID와 연관된 속성의 통신이 특히 높은 수준의 신용을 갖는다고 여긴다.

[0014] 본 발명의 일 실시예에 따르면, 제 1 컴퓨터 시스템은 ID 토큰에 대해 제 1 컴퓨터 시스템을 인증하기 위해 사용되는 적어도 하나의 인증서를 포함한다. 인증서는 제 1 컴퓨터 시스템이 판독 권한을 갖는다는 속성의 표시를 포함한다. ID 토큰은 제 1 컴퓨터 시스템에 의해 판독 액세스가 수행될 수 있기 전에, 제 1 컴퓨터 시스템이 속성으로의 판독 액세스에 대해 필요한 판독 권한을 갖는지 체크하기 위해 상기 인증서를 사용한다.

[0015] 본 발명의 일 실시예에 따르면, 제 1 컴퓨터 시스템은 ID 토큰으로부터 판독된 적어도 하나의 속성을 제 2 컴퓨터 시스템으로 직접 전송한다. 일례로서, 제 2 컴퓨터 시스템은 온라인 서비스나 뱅킹 서비스 같은 다른 서비스를 제공하거나 제품을 주문하는 서버일 수 있다. 일례로서, 사용자는 온라인으로 계좌를 개설할 수 있는데, 사용자의 ID를 포함하는 선단 속성들은 제 1 컴퓨터 시스템에서 은행의 제 2 컴퓨터 시스템으로 전송된다.

[0016] 본 발명의 일 실시예에 따르면, ID 토큰으로부터 판독된 속성들은 우선 제 1 컴퓨터 시스템에서 사용자의 제 3 컴퓨터 시스템으로 전송된다. 일례로서, 제 3 컴퓨터 시스템은 사용자가 제 2 컴퓨터 시스템에서 웹 페이지를 오픈하기 위해 사용할 수 있는 보통의 인터넷 브라우저를 포함한다. 사용자는 웹 페이지에 요구나 서비스나 제품에 대한 주문을 입력할 수 있다.

[0017] 그러면 제 2 컴퓨터 시스템은 예를 들어 사용자나 사용자의 ID 토큰의 속성들을 특정 하며, 이는 서비스를 제공하거나 주문을 하기 위해 요구된다. 이러한 속성의 명세 사항을 포함하는 해당 속성의 상세는 제 2 컴퓨터 시스템에서 제 1 컴퓨터 시스템으로 전송된다. 이는 제 3 컴퓨터 시스템의 간섭에 의해 또는 간섭 없이 행해 질 수 있다. 후자의 경우, 사용자는 예를 들어 제 1 컴퓨터 시스템의 URL을 제 3 컴퓨터 시스템으로부터 제 2 컴퓨터 시스템의 웹 페이지에 입력함으로써, 제 2 컴퓨터 시스템에 바람직한 제 1 컴퓨터 시스템을 특정할 수 있다.

[0018] 본 발명의 일 실시예에 따르면, 사용자로부터 제 2 컴퓨터 시스템으로의 서비스 요구는 식별자의 표시를 포함하며, 식별자는 제 1 컴퓨터 시스템을 식별한다. 일례로서, 식별자는 예를 들면 제 1 컴퓨터 시스템의 URL인 링크이다.

[0019] 본 발명의 일 실시예에 따르면, 속성의 상세는 제 2 컴퓨터 시스템에서 제 1 컴퓨터 시스템으로 직접 전송되지 않고, 우선 제 2 컴퓨터 시스템에서 제 3 컴퓨터 시스템으로 전송된다. 제 3 컴퓨터 시스템은 다수의 미리 정의된 구성 데이터 레코드를 포함하며, 제 3 컴퓨터는 다수의 미리 정의된 구성 데이터 레코드를 포함하고, 각각의 구성 데이터 레코드는 한 세트의 제 1 컴퓨터 시스템으로부터 속성, 적어도 하나의 데이터 소스 및 제 1 컴퓨터 시스템의 부분 집합을 특정하고, 속성의 상세는 우선 제 2 컴퓨터 시스템에서 제 3 컴퓨터 시스템으로 전송되어, 제 3 컴퓨터 시스템이 속성의 상세에 특정된 적어도 하나의 속성을 포함하는 속성의 부분 집합을 특정하는 적어도 하나의 구성 데이터 레코드를 선택하기 위해 이용되며, 제 3 컴퓨터는 속성의 상세를 제 1 컴퓨터 시스템으로 전송하고, 선택된 구성 데이터 레코드에서의 데이터 소스의 표시에 의해 특정된 ID 토큰으로의 연결이 설정된다.

[0020] 본 발명의 일 실시예에 따르면, ID 토큰으로부터 판독된 속성은 제 1 컴퓨터 시스템에 의해 서명되어 제 3 컴퓨터 시스템으로 전송된다. 따라서 제 3 컴퓨터 시스템의 사용자는 속성을 변경할 수 는 없으나 속성을 판독할 수 있다. 사용자에 의한 공개 후에, 속성은 제 3 컴퓨터 시스템에서 제 2 컴퓨터 시스템으로 전송된다.

[0021] 본 발명의 일 실시예에 따르면, 사용자는 속성이 전송되기 전에 속성에 다른 데이터를 추가할 수 있다.

[0022] 본 발명의 일 실시예에 따르면, 제 1 컴퓨터 시스템은 다른 판독 권한을 갖는 다수의 인증서를 포함한다. 속성의 상세 수신에 기초해서, 제 1 컴퓨터 시스템은 ID 토큰 또는 다수의 다른 ID 토큰으로부터 관련 속성을 판독하기 위하여 하나 이상의 인증서를 선택한다.

[0023] 본 발명의 일 실시예에 따르면, 제 3 컴퓨터 시스템은 네트워크를 통해 제 3 컴퓨터 시스템에게 다른 속성을 요구하는 외부 데이터 소스를 특정하는 적어도 하나의 구성 데이터 레코드를 포함한다.

[0024] 본 발명의 일 실시예에 따르면, 적어도 하나의 속성이 ID 토큰으로부터 판독되고 제 3 컴퓨터 시스템이 제 1 컴퓨터 시스템으로부터 적어도 하나의 속성을 수신한 후에, 상기 다른 속성이 요구되는데, 상기 요구는 적어도 하나의 속성을 포함한다.

[0025] 다른 면에서, 본 발명은 컴퓨터 프로그램 제품에 관한 것으로, 특히, 본 발명에 따른 방법을 수행하는 실행 가

능한 프로그램 명령을 포함하는 디지털 저장장치 매체에 관한 것이다.

[0026] 다른 면에서, 본 발명은 적어도 하나의 속성을 저장하는 보호된 메모리 영역; ID 토큰에 대해 ID 토큰과 연관된 사용자를 인증하는 수단; ID 토큰에 대해 제 1 컴퓨터 시스템을 인증하는 수단; 및 적어도 하나의 속성을 판독하기 위해 사용될 수 있는 제 1 컴퓨터 시스템에 대해 보호된 연결을 설정하는 수단을 포함하며, 제 1 컴퓨터 시스템에 의해 ID 토큰으로부터 적어도 하나의 속성을 판독하는 필요조건은 ID 토큰에 대한 사용자와 제 1 컴퓨터 시스템의 성공적인 인증인 ID 토큰에 관한 것이다

[0027] ID 토큰에 대한 제 1 컴퓨터 시스템의 인증 이외에, 본질적으로 "확장된 액세스 제어", 예를 들어 기계 판독 가능 여행 문서(MRTD)로 알려지고, 국제 민간 항공 기구(ICAO)에 의해 특정된 바와 같이, 사용자는 ID 토큰에 대해 자신을 인증해야 한다. 일례로서, ID 토큰에 대한 사용자의 성공적인 인증은 ID 토큰을 공개하고, 그에 따라 다음 단계, 즉 ID 토큰에 대한 제 1 컴퓨터 시스템의 인증 및/또는 속성 판독을 위한 보호된 연결 설정이 실행된다.

[0028] 본 발명의 실시예에 따르면, ID 토큰은 종단간 암호화 수단을 포함한다. 사용자는 종단간 암호화를 위하여 연결을 통해 전송되는 데이터에 어떤 변경도 가하지 못하기 때문에, 종단간 암호화 수단은 ID 토큰과 제 1 컴퓨터 시스템 사이에 사용자의 제 3 컴퓨터 시스템을 통해 연결이 설정되게 한다.

[0029] 다른 면에서, 본 발명은 제 1 컴퓨터 시스템과, 네트워크를 통해 적어도 하나의 속성을 특정하는 속성의 상세를 수신하는 수단; ID 토큰에 대해 인증하는 수단; 및 보호된 연결을 통해 ID 토큰으로부터 적어도 하나의 속성을 판독하는 수단을 포함하며, 적어도 하나의 속성을 판독하는 필요조건은 ID 토큰에 연관된 사용자와 컴퓨터 시스템의 ID 토큰에 대한 인증이라는 컴퓨터 시스템에 관한 것이다

[0030] 본 발명의 실시예에 따르면, 제 1 컴퓨터 시스템은 사용자에 대한 요구를 생성하는 수단을 포함할 수 있다. 제 1 컴퓨터 시스템이 제 2 컴퓨터 시스템으로부터 속성의 상세를 수신하면, 예를 들어 제 1 컴퓨터 시스템은 요구를 사용자의 제 3 컴퓨터 시스템으로 전송하여, 사용자에게 ID 토큰에 대해 인증할 것을 요구한다. ID 토큰에 대한 사용자의 인증이 성공적으로 수행되면, 제 1 컴퓨터 시스템은 제 3 컴퓨터 시스템으로부터 확인을 수신한다. 그러면 제 1 컴퓨터 시스템은 ID 토큰에 대해 자신을 인증하고, ID 토큰과 제 1 컴퓨터 시스템 사이에는 종단간 암호화를 이용하여 보안 연결이 설정된다.

[0031] 본 발명의 실시예에 따르면, 제 1 컴퓨터 시스템은 각각 다른 판독 권한을 특정하는 다수의 인증서를 포함한다. 속성의 상세의 수신 후에, 제 1 컴퓨터 시스템은 특정된 속성을 판독하기에 충분한 판독 권한을 갖는 적어도 하나의 인증서를 선택한다.

발명의 효과

[0032] 본 발명에 따른 제 1 컴퓨터 시스템의 실시예들은 특히 유리한 효과가 있는데, 이는 ID 토큰에 대한 사용자의 인증 필요성과 결합하여 위조되지 않은 사용자의 디지털 ID에 대한 신용수단을 형성하기 때문이다. 이에 관련한 특히 유리한 효과는 사용자와 컴퓨터 시스템 또는 디지털 ID를 형성하는 사용자의 속성을 저장하는 중앙 저장소의 사전등록을 필요로 하지 않는다는 것이다.

[0033] 본 발명의 일 실시예에 따르면, 제 1 컴퓨터 시스템은 속성의 명세와 함께 제 2 컴퓨터 시스템에 대한 식별자를 수신한다. 이 식별자를 이용하여, 제 2 컴퓨터 시스템에게 식별 서비스를 요구하기 위해, 컴퓨터 시스템은 식별 서비스를 이용하고자 하는 제 2 컴퓨터 시스템을 식별한다.

[0034] 본 발명의 일 실시예에 따르면, 컴퓨터 시스템은 공식적으로 인증된 신용 센터, 특히, 서명 행위에 준거하는 신용 센터이다.

도면의 간단한 설명

[0035] 이하, 도면을 참조하여 본 발명의 실시예들을 더욱 자세하게 설명한다.

도 1은 본 발명에 따른 컴퓨터 시스템의 제 1 실시예의 블록도이다.

도 2는 본 발명에 따른 방법의 실시예의 흐름도이다.

도 3은 본 발명에 따른 컴퓨터 시스템의 다른 실시예의 블록도이다.

도 4는 본 발명에 따른 방법의 또 다른 실시예의 UML(Unified Modeling Language) 도 이다.

발명을 실시하기 위한 구체적인 내용

[0036] 이하, 서로 상응하는 실시예의 요소는 동일한 도면 부호로 나타낸다.

[0037] 도 1은 사용자(102)의 사용자 컴퓨터 시스템(100)을 도시한다. 사용자 컴퓨터 시스템(100)은 퍼스널 컴퓨터, 랩탑이나 팜탑 컴퓨터와 같은 휴대용 컴퓨터, PDA, 특히 스마트 폰과 같은 이동 통신 기구일 수 있다. 사용자 컴퓨터 시스템(100)은 적절한 인터페이스(108)를 포함하는 ID 토큰(106)과의 통신을 위한 인터페이스(104)를 포함한다.

[0038] 사용자 컴퓨터 시스템(100)은 프로그램 명령(112)을 실행하는 적어도 하나의 프로세서(110) 및 네트워크(116)를 통한 통신을 위한 네트워크 인터페이스(114)를 포함한다. 네트워크는 인터넷과 같은 컴퓨터 네트워크일 수 있다.

[0039] ID 토큰(106)은 보호된 메모리 영역(120,122,124)을 갖는 전자 메모리(118)를 포함한다. 보호된 메모리 영역(120)은 ID 토큰(106)에 대해 사용자(102)를 인증하기 위해 요구되는 기준 값을 저장하는데 사용된다. 기준 값은, 예를 들어 특히, 개인 식별 번호(PIN)로 알려진 식별자이거나, ID 토큰(106)에 대해 사용자(102)를 인증하기 위해 사용될 수 있는 사용자(102)의 생체 인식 특징에 대한 기준 데이터 이다.

[0040] 보호된 영역(122)은 비밀키를 저장하기 위해 사용되고, 보호된 메모리 영역(124)은 예를 들어 사용자의 이름, 거주지, 생일, 성별과 같은 사용자(102)의 속성 및/또는 ID 토큰을 생성하거나 발행한 기관, ID 토큰의 유효 기간, 또는 여권번호나 신용 카드 번호와 같은 ID 토큰에 대한 식별자와 같은 ID 토큰 자체에 관한 속성을 저장하기 위해 사용된다.

[0041] 전자 메모리(118)는 또한 인증서를 저장하는 메모리 영역(126)을 포함할 수 있다. 인증서는 보호된 메모리 영역(122)에 저장된 비밀키와 연관된 공개키를 포함한다. 인증서는 예를 들어 X.509 표준에 기초한 공개키 기반(PKI) 표준에 기초하여 생성될 수 있다.

[0042] 인증서는 반드시 ID 토큰(106)의 전자 메모리(118)에 저장되어야 하는 것은 아니다. 대안적으로 또는 추가적으로, 인증서는 공개 디렉토리 서버에 저장될 수 있다.

[0043] ID 토큰(106)은 프로세서(128)를 포함한다. 프로세서(128)는 프로그램 명령(130,132,134)을 실행시키는데 사용된다. 프로그램 명령(130)은 사용자 인증, 즉, ID 토큰에 대한 사용자 인증에 사용된다.

[0044] 개인 식별 번호를 사용한 실시예에서, 사용자(102)는 자신을 인증하기 위하여, 예를 들어 사용자 컴퓨터 시스템(100)을 통해 자신의 개인 식별 번호를 ID 토큰(106)에 입력한다. 그러면 프로그램 명령(130)의 수행은, 입력된 개인 식별 번호와 보호된 메모리 영역에 저장된 개인 식별 번호에 대한 기준 값을 비교하기 위해서 보호된 메모리 영역(120)으로 액세스한다. 입력된 개인 식별 번호가 개인 식별 번호의 기준 값과 일치하면, 사용자(102)는 인증된 것으로 간주된다.

[0045] 대안적으로, 사용자(102)의 생체 인식 특징이 캡쳐된다. 일례로서, ID 토큰(106)은 이러한 목적을 위해 지문 센서를 포함한다, 즉, 지문 센서가 사용자 컴퓨터 시스템(100)에 연결된다. 본 실시예에서, 사용자(102)로부터 캡쳐된 생체 인식 데이터는 보호된 메모리 영역(120)에 저장된 생체 인식 기준 데이터와 프로그램 명령(130)을 실행함으로써 비교된다. 사용자(102)로부터 캡쳐된 생체 인식 데이터와 생체 인식 기준 데이터가 충분히 매치되면, 사용자(102)는 인증된 것으로 간주된다.

[0046] 프로그램 명령(134)은, ID 토큰(106)에 대해 ID 제공자 컴퓨터 시스템(136)을 인증하기 위하여, ID 토큰(106)에 관련된 암호화 프로토콜 단계를 실시하기 위해 사용된다. 암호화 프로토콜은 한 쌍의 대칭키 또는 비대칭키에 기초한 도전/응답(challenge/응답) 프로토콜일 수 있다.

[0047] 일례로서, 국제 민간 항공 기구(ICAO)에 의해 기계 판독 가능 여행 문서(MRTD)로 특정되는 바와 같이, 암호화 프로토콜은 확장된 액세스 컨트롤 방법을 실현한다. 암호화 프로토콜의 성공적인 실행은 ID 제공자 컴퓨터 시스템(136)을 ID 토큰에 대해 인증되게 하며, 그에 따라 보호된 메모리 영역(124)에 저장된 속성을 판독하는 판독 권한을 입증한다. 인증은 상호적으로 이루어질 수 있는데, 즉 ID 토큰(106) 또한 동일한 또는 다른 암호화 프로토콜에 기초하여 ID 제공자 컴퓨터 시스템(136)에 대해 인증될 필요가 있다.

[0048] 프로그램 명령(132)은 보호된 메모리 영역(124)으로부터 ID 제공자 컴퓨터 시스템(136)에 의해 판독된 최소한의 속성을 제외한 ID 토큰(106)과 ID 제공자 컴퓨터 시스템(136) 사이에 전달된 데이터의 종단간 암호화를 위해 사용된다. 종단간 암호화는, 예를 들어 암호화 프로토콜이 실행될 경우, ID 토큰(106)과 ID 제공자 컴퓨터 시스템

(136) 사이에서 일치된 대칭키를 사용하는 것이 가능하다.

[0049] 도 1에서 보여진 실시예의 대안으로서, 사용자 컴퓨터 시스템(100)은, ID 토큰(106)에 대해서, 인터페이스(108)와 직접적인 방법이 아닌 인터페이스(104)에 연결된 리더를 통해서 통신하기 위한 인터페이스(104)를 사용할 수 있다. 예를 들어 제 2 칩 카드 단말로 알려진 이 리더는 또한 개인 식별 번호를 입력하기 위해 사용될 수 있다.

[0050] ID 제공자 컴퓨터 시스템(136)은 네트워크(116)를 통한 통신을 위해 네트워크 인터페이스(138)를 포함한다. ID 제공자 컴퓨터 시스템(136)은 또한 ID 제공자 컴퓨터 시스템(136)에 대한 비밀키(142)와 적절한 인증서(144)를 저장하는 메모리(140)를 포함한다. 이 인증서는 예를 들어 X.509와 같은 공개키 기반(PKI) 표준에 기초한 인증서일 수 있다.

[0051] 또한, ID 제공자 컴퓨터 시스템(136)은 프로그램 명령(146,148)을 실행하는 적어도 하나의 프로세서(145)를 포함한다. 프로그램 명령(146)을 실행함으로써, ID 제공자 컴퓨터 시스템(136)에 관련된 암호화 프로토콜 단계가 실행된다. 결국, ID 토큰(106)의 프로세서(128)에 의한 프로그램 명령(134)의 실행을 통해서 그리고 ID 제공자 컴퓨터 시스템(136)의 프로세서(145)에 의한 프로그램 명령(146)의 실행을 통해서, 암호화 프로토콜이 실현된다.

[0052] 프로그램 명령(148)은 예를 들어 암호화 프로토콜이 실행될 때, ID 토큰(106)과 ID 제공자 컴퓨터 시스템(136) 사이에서 일치된 대칭키에 기초해서 ID 제공자 컴퓨터 시스템(136)에서 종단간 암호화를 실현하기 위해 사용된다. 원칙적으로, 본래 Diffie-Hellman 키 교환과 같이 미리 알려진 종단간 암호와에 대한 대칭키를 승인하는 어떤 방법도 사용 가능하다.

[0053] 바람직하게 ID 제공자 컴퓨터 시스템(136)은, 특히, 신용 센터로 알려진, 특별하게 보호된 환경에 놓여지고, 그 결과 ID 제공자 컴퓨터 시스템(136)은 ID 토큰(106)에 대한 사용자(102)의 인증의 필요성과 결합된 ID 토큰(106)으로부터 판독된 속성의 신뢰성에 대한 신용 수단을 형성하는 것이다.

[0054] 서비스 컴퓨터 시스템(150)은 서비스 또는 제품, 특히, 온라인 서비스에 대한 주문이나 명령 을 받도록 설계되었다. 일례로서, 사용자(102)는 네트워크(116)를 통해 은행계좌를 개설하거나 온라인으로 다른 금융 또는 뱅킹 서비스를 사용할 수 있다. 또한, 서비스 컴퓨터 시스템(150)은 온라인 보관소의 형식을 가질 수 있어서, 사용자(102)는 예를 들어 온라인으로 모바일 폰 등을 구매할 수 있다. 게다가, 서비스 컴퓨터 시스템(150)은 또한 예를 들어 음악 데이터 및/또는 비디오 데이터의 다운로드를 위한 디지털 컨텐츠를 운반하도록 설계될 수 있다.

[0055] 이러한 목적을 달성하기 위하여, 서비스 컴퓨터 시스템(150)은 네트워크(116)을 연결하기 위한 네트워크 인터페이스(152)를 포함한다. 게다가, 서비스 컴퓨터 시스템(150)은 프로그램 명령(156)을 실행하는 적어도 하나의 프로세서(154)를 포함한다. 프로그램 명령(156)의 실행으로, 예를 들어 사용자(102)가 그의 명령이나 주문을 입력할 수 있는 다이나믹 HTML 페이지를 생성한다.

[0056] 명령되거나 주문된 제품이나 서비스의 특질에 따라, 서비스 컴퓨터 시스템(150)은 하나 이상의 규정된 기준을 사용하여 사용자(102) 및/또는 그의 ID 토큰(106)의 하나이상의 속성을 검사할 필요가 있다. 이러한 검사가 통과된 경우에만, 사용자(102)로부터의 주문이나 명령이 받아들여지거나/또는 실행된다.

[0057] 일례로서, 은행 계좌의 개설이나 관련된 계약에 따른 모바일 폰 구매는 사용자로 하여금 서비스 컴퓨터 시스템(150)으로의 신분 기재와 기재된 신분의 검사를 요구한다. 종래 기술에서, 사용자(102)는 신분증을 제시함으로서 이를 행해야 했다. 이 과정은 사용자의 ID 토큰(106)으로부터 사용자(102)의 디지털 ID를 판독하는 것으로 바뀌었다.

[0058] 그러나, 응용의 실례에 따라서, 사용자(102)는 그의 신분을 서비스 컴퓨터 시스템(150)에 기재할 필요가 없고, 예를 들어 속성 중 하나만을 전달하는 것으로 충분하다. 일례로서, 사용자(102)는 다운로드를 하기 위해 서비스 컴퓨터 시스템(150)에 저장된 데이터로의 접근이 승인된 사람들의 특정 그룹에 속한다는 증거를 제시하는 속성 중 하나를 사용할 수 있다. 일례로서, 이러한 기준은 사용자(102)의 최소 연령이나, 특정 기밀 데이터에 대한 접근 권한을 갖는 사람들의 그룹과 사용자(102)의 연관성일 수 있다.

[0059] 서비스 컴퓨터 시스템(150)에 의해 제공되는 서비스를 사용하기 위한 절차는 다음과 같다.

[0060] 1. ID 토큰(106)에 대한 사용자(102) 인증

[0061] 사용자(102)는 ID 토큰(106)에 대해 자신을 인증한다. 개인 식별 번호를 이용한 실행에서, 사용자(102)는 예를

들어 사용자 컴퓨터 시스템(100) 또는 이에 연결된 칩 카드 단말을 이용하여 개인 식별 번호를 입력함으로써 인증을 수행한다. 프로그램 명령(130)을 실행함에 의해, ID 토큰(106)은 입력된 개인 식별 번호의 정확성을 검사한다. 입력된 개인 식별 번호가 보호된 메모리 영역(120)에 저장된 개인 식별 번호의 기준값과 매치되면, 사용자(102)는 인증된 것으로 간주된다. 상술된 바와 같이 사용자(102)의 생체 인식 특징이 사용자를 인증하기 위해 사용되면, 인증 절차는 유사하다.

[0062] 2. ID 토큰(106)에 대한 ID 제공자 컴퓨터 시스템(136) 인증

[0063] 이 목적을 달성하기 위하여, 사용자 컴퓨터 시스템(100)과 네트워크(116)를 통해서 ID 토큰(106)과 ID 제공자 컴퓨터 시스템(136) 사이에 연결이 설정된다. 일례로서, ID 제공자 컴퓨터 시스템(136)은 이 연결을 통하여 인증서(144)를 ID 토큰(106)으로 전송한다. 그러면, 프로그램 명령(134)은 예를 들어 도전이라고 알려진 임의의 숫자를 생성한다. 이 임의의 숫자는 ID 제공자 컴퓨터 시스템(136)의 공개키를 이용하여 암호화 되는데, 공개키는 인증서(144)에 포함된다. 그 결과로 생기는 암호는 ID 토큰(106)으로부터 이 연결을 통하여 ID 제공자 컴퓨터 시스템(136)으로 전송된다. ID 제공자 컴퓨터 시스템(136)은 비밀키(142)를 이용하여 암호를 해독하고, 이러한 방식으로 임의의 숫자를 획득한다. 임의의 숫자는 ID 제공자 컴퓨터 시스템(136)에 의해 연결을 통하여 ID 토큰(106)으로 리턴된다. 프로그램 명령(134)을 실행함으로써, 상기 ID 토큰은 ID 제공자 컴퓨터 시스템(136)으로부터 수신한 임의의 숫자가 처음에 생성된 임의의 숫자, 즉, 도전과 매치되는지 검사한다. 이러한 경우, ID 제공자 컴퓨터 시스템(136)은 ID 토큰(106)에 대해 인증된 것으로 간주된다. 임의의 숫자는 종단간 암호화를 위해 대칭키로 이용될 수 있다.

[0064] 3. 사용자(102)가 ID 토큰(106)에 대해 사용자 자신을 성공적으로 인증하고 ID 제공자 컴퓨터 시스템(136)이 ID 토큰(106)에 대해 그 자신을 성공적으로 인증하면, ID 제공자 컴퓨터 시스템(136)은 속성을 판독하는 판독 권한과, 보호된 메모리 영역(124)에 저장된 다수의 속성 또는 모든 속성을 제공 받는다. ID 제공자 컴퓨터 시스템(136)이 연결을 통해 ID 토큰(106)으로 전송하는 관련된 판독 명령에 기초해서, 요구된 속성은 보호된 메모리 영역(124)으로부터 판독되고, 프로그램 명령(132)을 실행함으로써 암호화 된다. 암호화된 속성은 연결을 통해 ID 제공자 컴퓨터 시스템(136)으로 전송되는데, ID 제공자 컴퓨터 시스템(136)에서 암호화된 속성은 프로그램 명령(148)을 실행함으로써 해독 된다. 이는 ID 제공자 컴퓨터 시스템(136)에 ID 토큰(106)으로부터 판독된 속성에 대한 지식을 제공한다.

[0065] 이러한 속성은 인증서(144)를 이용하여 ID 제공자 컴퓨터 시스템에 의해 서명되어 사용자 컴퓨터 시스템(100)을 통하여 전송되거나, 서비스 컴퓨터 시스템(150)으로 직접 전송된다. 이는 서비스 컴퓨터 시스템(150)에게 ID 토큰(106)에서 판독된 속성을 알림으로써, 서비스 컴퓨터 시스템(150)이 사용자(102)에 의해 요구된 서비스를 가능하게 제공하기 위하여 규정된 하나 이상의 기준을 사용하여 이러한 속성을 검사 할 수 있다.

[0066] ID 토큰(106)에 대해 사용자(102)를 인증하기 위한 필요성과 ID 토큰(106)에 대해 ID 제공자 컴퓨터 시스템(136)을 인증하기 위한 필요성은 필요한 신용 수단을 제공하여, 서비스 컴퓨터 시스템(150)이 ID 제공자 컴퓨터 시스템(136)에 의해 서비스 컴퓨터 시스템에 전달된 사용자(102)의 속성은 정확하며 왜곡된 것이 아니라는 것을 확신할 수 있게 한다.

[0067] 실시예에 따라서, 인증의 순서는 다를 수 있다. 일례로서, 우선 첫 번째로, ID 토큰(106)에 대해 자신을 인증해야 하는 사용자(102)에 대한 제공이 이루어지고, ID 제공자 컴퓨터 시스템(136)이 그 뒤를 따를 수 있다. 그러나, 원칙상, ID 토큰(106)에 대해 자신을 인증해야 하는 ID 제공자 컴퓨터 시스템(136)이 우선 먼저이고, 사용자(102)가 그 뒤를 따르는 것도 가능하다.

[0068] 첫 번째의 경우, 일례로서, ID 토큰(106)은 사용자(102)에 의한 정확한 개인 식별 번호 또는 정확한 생체 인식 특징의 입력을 통해서만 열리도록 (unlock) 설계된다. 이러한 열림만이 프로그램 명령(132,134)이 시작되고, 그에따라 ID 제공자 컴퓨터 시스템(136)이 인증되게 한다.

[0069] 두 번째의 경우, 사용자(102)가 ID 토큰(106)에 대해서 자신을 인증하지 않았더라도, 프로그램 명령(132,134)을 시작할 수 있다. 이 경우, 일례로서서, 사용자(102)가 성공적으로 인증되었다고 프로그램 명령(130)이 알릴 때까지, ID 제공자 컴퓨터 시스템(136)은 하나 이상의 속성을 판독하기 위해 보호된 메모리 영역(124)에 대한 판독 액세스를 할 수 없도록 프로그램 명령(134)이 형성된다.

[0070] 전자 상거래와 전자 정부 어플리케이션에 대한 ID 토큰(106)의 활용이라는 특정 효과는, 예를 들면, 특히 미디어 분열없이, ID 토큰(106)에 대해 인증될 사용자(102)와 ID 제공자 컴퓨터 시스템(136)에 대한 필요성에 의해 형성된 신용 수단에 합법적으로 기초한다. 다양한 사용자(102)의 속성에 대한 중앙 기억장치가 필요하지 않다는

특정 효과는, 종래의 기술에 존재하는 데이터 보호 문제가 해결됨을 의미한다. 본 방법의 응용의 편의와 관련되어서는, ID 제공자 컴퓨터 시스템(136)을 사용하기 위해 사용자(102)의 사전등록이 필요 없다는 효과가 있다.

[0071] 도 2는 본 발명에 따른 방법의 실시예를 보여준다. 단계 200에서, 서비스 요구가 사용자 컴퓨터 시스템으로부터 서비스 컴퓨터 시스템으로 전송된다. 일례로서, 사용자는 사용자 컴퓨터 시스템에서 인터넷 브라우저를 시작하고 서비스 컴퓨터 시스템에서 웹 페이지를 호출하기 위하여 URL을 입력함으로써 이를 실행한다. 그리고 사용자는 예를 들어 서비스나 제품을 주문 또는 명령하기 위해, 사용자의 서비스 요구를 호출된 웹 페이지에 입력한다.

[0072] 그러면, 단계 202에서, 서비스 컴퓨터 시스템(150)은 서비스 요구에 대한 사용자의 권한을 검사하기 위해 컴퓨터 시스템이 요구하는 하나 이상의 속성을 특정한다. 특히, 서비스 컴퓨터 시스템은 사용자(102)의 디지털 ID를 결정하는 속성을 특정 할 수 있다. 서비스 컴퓨터 시스템(150)에 의한 속성의 상세는 확고하게 규정되거나, 서비스 요구에 따라 규정된 규칙을 이용하여 서비스 컴퓨터 시스템(150)이 개별적으로 결정할 수 있다.

[0073] 단계 204에서, 속성의 상세, 즉, 단계 202에서 실시된 하나 이상의 속성에 대한 상세는 직접적으로 또는 서비스 컴퓨터 시스템에서 ID 제공자 컴퓨터 시스템으로 사용자 컴퓨터 시스템을 통해서 전송된다.

[0074] 단계 206에서, 사용자의 ID 토큰으로부터 속성을 판독할 기회를 ID 제공자 컴퓨터 시스템에게 제공하기 위해, 사용자는 ID 토큰에 대해 그 자신을 인증한다.

[0075] 단계 208에서, ID 토큰과 ID 제공자 컴퓨터 시스템 사이의 연결이 설정된다. 바람직하게, 이는, 예를 들어 안전한 메시징 방법에 기초한, 보호된 연결이다.

[0076] 단계 210에서, ID 제공자 컴퓨터 시스템은 단계 208에서 설정된 연결을 통해 ID 토큰에 대해 적어도 인증된다. 게다가, ID 제공자 컴퓨터 시스템에 대해 인증될 ID 토큰이 제공될 수 있다.

[0077] 사용자와 ID 제공자 컴퓨터 시스템 모두가 성공적으로 ID 토큰에 대해 인증되면, ID 제공자 컴퓨터 시스템은 ID 토큰에 의해 속성을 판독하는 접근 권한을 제공 받는다. 단계 212에서, ID 제공자 컴퓨터 시스템은 속성의 상세에 따라 ID 토큰에게 요구되는 속성의 판독을 위한 하나 이상의 판독 명령을 전송한다. 그러면 속성은 보호된 연결을 통하여 ID 제공자 컴퓨터 시스템으로 종단간 암호화를 이용하여 전송되는데, ID 제공자 컴퓨터 시스템에서 속성의 암호가 해독된다.

[0078] 단계 214에서, 판독된 속성 값이 ID 제공자 컴퓨터 시스템에 의해 서명된다. 단계 216에서, ID 제공자 컴퓨터 시스템은 서명된 속성 값을 네트워크를 통해 전송한다. 서명된 속성 값은 직접적으로 또는 사용자 컴퓨터 시스템을 통해 서비스 컴퓨터 시스템에 도달한다. 후자의 경우, 사용자는 서명된 속성 값을 메모하거나 및/또는 다른 데이터를 속성에 추가할 기회를 가질 수 있다. 사용자에 의한 공개 뒤에, 사용자 컴퓨터 시스템에서 서비스 컴퓨터 시스템으로 전송될 추가된 데이터와 함께 서명된 속성 값들이 제공될 수 있다. 이는 ID 제공자 컴퓨터 시스템에서 서비스 컴퓨터 시스템으로 전송된 속성에 관해서는 사용자에 대한 최대한의 투명성을 제공한다.

[0079] 도 3은 본 발명에 따른 ID 토큰과 본 발명에 따른 컴퓨터 시스템의 실시예를 보인다. 도 3의 실시예에서, ID 토큰(106)은 통합 전자 회로 상태의 종이 기반 및/또는 플라스틱 기반 문서 형식인데, 통합 전자 회로는 인터페이스(108), 메모리(118) 및 프로세서(128)를 형성한다. 일례로서, 통합 전자 회로는 무선 태그일 수 있는데, 무선 태그는 또한 RFID 태그 또는 RFID 라벨이라 불린다. 또한, 인터페이스(108)는 중개자를 갖추거나, 듀얼 모드 인터페이스 형식 일 수 있다.

[0080] 특히, 문서(106)는 전자 여권이나 전자 식별 카드 같은 기계 판독 가능 여행 문서와 같은 가치 문서 또는 보안 문서이거나, 신용 카드와 같은 지불 수단일 수 있다.

[0081] 현재의 상황을 고려한 실시예에서, 보호된 메모리 영역(124)은 속성(i, $1 \leq i \leq n$)를 저장한다. 이어서, 일반적 성질의 제한 없이, 도 3에서 일례로 도시된 ID 토큰(106)은 전자 식별 카드라고 가정한다. 일례로서, 속성 i가 1인 경우는 별명이고, 속성 i가 2인 경우는 이름이며, 속성 i가 3인 경우는 주소이고, 속성 i가 4인 경우는 생일이다.

[0082] 이를 고려한 실시예에서, 사용자 컴퓨터 시스템(100)의 인터페이스(104)는 RFID 리더 형식일 수 있는데, RFID 리더는 사용자 컴퓨터 시스템의 필수적인 부분을 형성하거나, 개별 부품으로서 사용자 컴퓨터에 연결될 수 있다.

[0083] 사용자(102)는 신용카드인 ID 토큰(106')과 같은 기본적으로 동일 디자인의 하나 이상의 ID 토큰을 가진다.

[0084] 사용자 컴퓨터 시스템(100)은 다수의 구성 데이터 레코드(158, 160,....)를 저장할 수 있다. 각각의 구성 데이터 레코드는 특정한 속성의 세트 , 데이터 소소 및 열거된 데이터 소스를 판독할 수 있는 ID 제공자 컴퓨터 시스템을 나타낸다. 본 실시예에서, 사용자 컴퓨터 시스템(100)은 각각 다른 신용 센터와 연관된 ID 제공자 컴퓨터 시스템(136, 136', ..)을 어드레스하기 위해 네트워크(116)를 사용할 수 있다. 일례로서, ID 제공자 컴퓨터 시스템(136)은 신용 센터 A와 연관되고, 원칙적으로 동일한 디자인의 ID 제공자 컴퓨터 시스템(136)'은 또 다른 신용 센터 B와 연관될 수 있다.

[0085] ID 컨테이너라 불리는 구성 데이터 레코드(158)는 그 안에 정의된 한 세트의 속성(i, i는 1 내지 4)를 포함한다. 이러한 속성은 각각 ID 토큰(106)인 데이터 소스 "ID카드"와 그들과 연관된 ID 제공자 컴퓨터 시스템(136)인 신용 센터 A를 포함한다. 후자의 경우, 예를 들어 구성 데이터 레코드(158)와 같은 URL형식으로 특정될 수 있다.

[0086] 한편, 구성 데이터 레코드(116)는 그 안에 정의된 한 세트의 속성(I, II, III)을 포함한다. 이러한 속성을 나타내는 데이터 소스는 각각의 신용카드, 즉 ID 토큰(106')이다. ID 토큰(106')은 속성(I, II, III)을 저장하는 보호된 메모리 영역(124')을 포함한다. 예를 들어, 속성(I)은 신용 카드 소지자의 이름, 속성(II)은 신용 카드 번호 및 속성(III)은 신용 카드의 유효 기간일 수 있다.

[0087] 구성 데이터 레코드(160)에서 나타나는 ID 제공자 컴퓨터 시스템은 신용 센터 B의 ID 제공자 컴퓨터 시스템(136')이다.

[0088] 도 3에서 보여지는 실시예의 대안으로서, 다른 데이터소스 및/또는 다른 ID 제공자 컴퓨터 시스템을 다른 속성에 대해 동일한 구성 데이터 레코드로 나타낼 수 있다.

[0089] 도 3의 실시예에서, 각각의 ID 제공자 컴퓨터 시스템(136, 136', ..)은 각각 다수의 인증서를 포함 할 수 있다.

[0090] 일례로서, 도 3에 예시되어있는 ID 제공자 컴퓨터 시스템(136)의 메모리(140)는, 각각의 연관된 비밀키(142.1,142.2)와 함께 저장된 인증서(144.1,144.2)와 같은, 다수의 인증서를 저장한다. 인증서(144.1)에서 ID 제공자 컴퓨터 시스템(136)에 대한 판독 권리는 속성(i, i는 1 내지 4)에 대해 정의되고, 그에 반해, 인증서(144.2)에서 판독 권리는 속성(I 내지 III)에 대해 정의된다.

[0091] 서비스 컴퓨터 시스템(150)이 제공하는 서비스를 이용하기 위해, 예를 들어 원하는 서비스에 대한 요구를 서비스 컴퓨터 시스템(150)의 웹 페이지에 입력하기 위해, 사용자(102)는 우선 사용자 컴퓨터 시스템(100)으로 사용자 입력(162)을 실시한다. 상기 서비스 요구(164)는 사용자 컴퓨터 시스템(100)에서 네트워크(116)를 통해 서비스 컴퓨터 시스템(150)으로 전송된다. 그러면 서비스 컴퓨터 시스템(150)은 속성의 상세(166)로 응답한다, 즉, 사용자(102)로부터의 서비스 요구(164)를 처리하기위해 서비스 컴퓨터 시스템(150)이 요구하는 속성을 특정함으로써 응답한다. 일례로서, 속성의 상세는 성, 이름, 주소, 신용 카드 번호와 같은 속성 이름 형식으로 만들어 질 수 있다.

[0092] 사용자 컴퓨터 시스템(100)이 사용자(102)에게 속성의 상세(166)의 수신을 알린다. 사용자(102)는 하나 또는 필요에 따라 속성의 상세(166)에 따른 속성을 포함하는 한 세트의 속성을 각각 정의하는 다수의 구성 데이터 레코드(158, 160, ...)를 적어도 부분 집합으로서 선택할 수 있다.

[0093] 속성의 상세(166)가 단지 사용자(102)의 성, 이름 및 주소만을 알려주길 요구한다면, 예를 들어, 사용자(102)는 구성 데이터 레코드(158)를 선택할 수 있다. 반면, 속성의 상세(166)에 신용카드 번호가 추가적으로 명시되어 있다면, 사용자(102)는 구성 데이터 레코드(160)를 추가적으로 선택 할 수 있다. 이 과정은 또한 사용자 컴퓨터 시스템(100)에 의해서, 예를 들어 프로그램 명령(112)을 실행함으로써, 완전히 자동으로 실시될 수 있다.

[0094] 다음으로, 우선 구성 데이터 레코드(158)와 같이 구성 데이터 레코드 중 오직 하나만이 속성의 상세(166)에 기초하여 선택된다고 가정한다.

[0095] 그러면 사용자 컴퓨터 시스템(100)은, 예를 들어 신용 센터 A의 ID 제공자 컴퓨터 시스템(136)을 고려하여, 선택된 구성 데이터 레코드에서 지정된 ID 제공자 컴퓨터 시스템으로 요구(168)를 전송한다. 상기 요구(168)는 속성의 상세(166)에 따른 속성의 지시를 포함며, 이는 ID 제공자 컴퓨터 시스템(136)에 의해 구성 데이터 레코드(158)에서 나타난 데이터 소스로부터 판독될 필요가 있다.

[0096] 그러면 ID 제공자 컴퓨터 시스템(136)은 이러한 속성을 판독하기 위해 요구되는 판독 권한을 갖는 하나 이상의 인증서를 선택한다. 일례로서, ID 카드로부터 속성(i)는 1 내지 3이라고 판독된다면, ID 제공자 컴퓨터 시스템(136)은 인증서(144.1)를 선택하며, 이는 속성에 대해 요구되는 판독 권한을 정의한다. 프로그램 명령(149)을

실행함에 의해 이인증서가 선택된다.

[0097] 다음으로, 암호화 프로토콜의 수행이 시작된다. 일례로서, 이러한 목적을 달성하기 위하여, ID 제공자 컴퓨터 시스템(136)은 사용자 컴퓨터 시스템(100)으로 응답을 전송한다. 그러면 사용자 컴퓨터 시스템(100)은 사용자(102)에게 특정된 데이터 소스, 즉, 이 경우 ID 카드에 대한 인증을 요구한다.

[0098] 그러면 사용자(102)는 자신의 ID 카드, 즉, ID 토큰(106)을 RFID 리더(104)의 유효 범위로 가져가서, 예를 들어 자신을 인증하기 위해, 개인 식별 번호를 입력한다. ID 토큰(106)에 대한 사용자(102)의 성공적인 인증은 암호화 프로토콜의 수행, 즉. 프로그램 명령(134)의 수행을 위해 ID 토큰을 공개한다.

[0099] 다음으로, ID 제공자 컴퓨터 시스템(136)은 선택된 인증서(144.1), 예를 들어 도전/응답 방법을 이용하여 ID 토큰(106)에 대해 자신을 인증한다. 이 인증은 또한 상호간에 이루어질 수 있다. ID 토큰(106)에 대한 ID 제공자 컴퓨터 시스템(136)의 성공적인 인증 다음에, ID 제공자 컴퓨터 시스템은 사용자 컴퓨터 시스템(100)로 필요한 속성을 판독하기 위한 판독 요구를 전송하고, 사용자 컴퓨터 시스템은 이를 RFID 리더(104)를 통해 ID 토큰(106)으로 전송한다. ID 토큰(106)은 ID 제공자 컴퓨터 시스템(136)이 필요한 판독 권한을 갖는지 검사하기 위해 인증서(144.1)를 사용한다. 이 경우, 보호된 메모리 영역(124)에서 바람직한 속성이 판독되고, 종단간 암호화에 의해 사용자 컴퓨터 시스템(100)을 통해 ID 제공자 컴퓨터 시스템으로 전송된다.

[0100] 그러면 ID 제공자 컴퓨터 시스템(136)은 판독된 속성을 포함하는 응답(170)을 네트워크(116)를 통해 서비스 컴퓨터 시스템(150)으로 전송한다. 응답(170)은 디지털 방식으로 인증서(144.1)로 서명된다.

[0101] 반면, ID 제공자 컴퓨터 시스템(136)은 응답(170)을 사용자 컴퓨터 시스템(100)으로 전송한다. 그러면 사용자(102)는 응답(170)에 포함된 속성을 판독하고 정말로 이러한 속성을 서비스 컴퓨터 시스템(150)으로 보내고 싶은지 결정하는 기회를 제공 받는다. 사용자로부터의 공개 명령이 사용자 컴퓨터 시스템(100)에 입력되면, 응답(170)은 서비스 컴퓨터 시스템(150)으로 전송된다. 본 실시예에서는, 또한 사용자(102)가 응답(170)에 다른 데이터를 추가 하는 것이 가능하다.

[0102] 다수의 ID 제공자 컴퓨터 시스템(136, 136', ..)이 포함되면, ID 제공자 컴퓨터 시스템으로부터의 개별적인 응답은 사용자 컴퓨터 시스템(100)에 의해서 속성의 상세(166)에 따른 모든 속성이 포함되어있는 하나의 응답으로 결합될 수 있는데, 그러면 상기 응답은 사용자 컴퓨터 시스템(100)에서 서비스 컴퓨터 시스템(150)으로 전송된다.

[0103] 본 발명의 일 실시예에 따르면, 예를 들어 서비스 요구(164)의 일부로서 사용자 속성을 네트워크(116)를 통해 서비스 컴퓨터 시스템으로 전송함으로써, 사용자(102)는 서비스 요구(164)에 따라서 서비스 컴퓨터 시스템(150)으로 하나 이상의 사용자 속성을 개시 할 수 있다. 특히, 사용자(102)는 상기 속성을 서비스 컴퓨터 시스템(150)의 웹 페이지에 입력 할 수 있다. 그러면 이러한 속성의 정확성이 응답(170)에 의해 확인된다, 즉, 서비스 컴퓨터 시스템(150)은 사용자(102)로부터 수신한 속성과 ID 제공자 컴퓨터(136)에 의해 ID 토큰(106)으로부터 판독된 속성을 비교할 수 있으며, 그들이 일치하는지 검사 할 수 있다.

[0104] 본 발명의 다른 일 실시예에 따르면, 적어도 하나의 다른 속성이 속성의 상세(166)에서 나타 날 수 있는데, 상기 속성은 사용자(102)의 ID 토큰 중 하나에 저장되지 않으나 외부 데이터 소스로부터 요구 될 수 있다. 일례로서, 이는 사용자(102)의 신용 가치에 관련된 속성을 포함 할 수 있다. 이러한 목적을 달성하기 위하여, 사용자 컴퓨터 시스템(100)은 데이터 소스의 표시와 속성(A)에 대한 ID 제공자 컴퓨터 시스템의 표시, 예를 들면, 신용 가치를 포함하는 또 다른 구성 데이터 레코드(161)를 포함 할 수 있다. 데이터 소스는 신용 조사소, Dun & Bradstreet와 같은 온라인 신용 조사기관일 수 있다. 예를 들어 도 3의 실시예에서와 같이, 표시된 ID 제공자 컴퓨터 시스템은 신용 센터 C 이다. 이 경우, 데이터 소스는 신용 센터 C에 위치한다.

[0105] 속성 A를 요청하기 위해서, 사용자 컴퓨터 시스템(100)은 적절한 요구(도 3에 미도시)를 신용 센터 C, 즉 ID 제공자 컴퓨터 시스템(136)''으로 전송한다. 그러면 C 신용 센터는 속성 A를 운반하며, 속성 A는 사용자 컴퓨터 시스템(100)이 사용자(102)의 ID 토큰으로부터 판독된 다른 속성과 함께 서비스 컴퓨터 시스템(150)으로 전달한다.

[0106] 바람직하게, 속성 A는, 예를 들어 사용자(102)의 디지털 ID에 관련된 속성이 이미 사용자(102)의 ID 토큰 중 하나로부터 요구되고 사용자 컴퓨터 시스템(100)에 의해서 서명된 응답으로 수신된 후에 요청된다. 그러면 사용자 컴퓨터 시스템(100)에 의한 ID 제공자 컴퓨터 시스템(136'')으로부터의 속성 A에 대한 요구는 서명된 응답(170)을 포함하여, ID 제공자 컴퓨터 시스템(136'')은 사용자(102)의 신분에 관한 믿을만한 정보를 갖게 된다.

[0107] 도 4는 본 발명에 따른 방법의 다른 실시예를 보인다. 사용자(102)로부터의 사용자 컴퓨터 시스템(100)으로의 사용자 입력은, 사용자가 이용하고자 하는 서비스 컴퓨터 시스템에서 서비스를 특정하기 위하여 사용자에 의해 이용된다. 예를 들어, 서비스 컴퓨터 시스템에서 인터넷 페이지를 호출하거나 서비스 컴퓨터 시스템에 제공되는 서비스 중 하나를 선택함으로써 사용자 입력이 수행 된다. 사용자(102)로부터의 서비스 요구는 사용자 컴퓨터 시스템(100)에서 서비스 컴퓨터 시스템(150)으로 전송된다.

[0108] 서비스 컴퓨터 시스템(150)은 속성의 상세, 즉, 예를 들어 속성 이름 리스트로 서비스 요구에 응답한다. 속성의 상세가 수신되면, 사용자 컴퓨터 시스템(100)은, 예를 들어 입력 요구의 수단으로 사용자(102)에게 ID 토큰(106)에 대해 인증할 것을 요구한다.

[0109] 그러면 사용자(102)는, 예를 들어 개인 식별 번호를 입력함으로써, ID 토큰(106)에 대해 자신을 인증한다. 성공적인 인증의 뒤를 따라, 속성의 상세가 사용자 컴퓨터 시스템(100)에서 ID 제공자 컴퓨터 시스템(136)으로 전송된다. 그러면 ID 제공자 컴퓨터 시스템(136)은 ID 토큰(106)에 대해 인증하고, ID 토큰(106)에 대한 속성의 상세에 따라 속성을 판독하기 위한 판독 요구를 전송한다.

[0110] 사용자(102)와 ID 제공자 컴퓨터 시스템(136)이 사전에 성공적으로 인증된다고 가정하면, ID 토큰(106)은 바람직한 속성으로 판독 요구에 응답한다. ID 제공자 컴퓨터 시스템(136)은 속성을 서명하고 서명된 속성을 사용자 컴퓨터 시스템(100)으로 전송한다. 사용자(102)에 의한 공개 후에, 서명된 속성은 서비스 컴퓨터 시스템(150)으로 전송되어, 필요에 따라 바람직한 서비스를 제공할 수 있다.

부호의 설명

[0111] 100 사용자 컴퓨터 시스템

102 사용자

104 인터페이스

106 ID 토큰

108 인터페이스

110 프로세서

112 프로그램 명령

114 네트워크 인터페이스

116 네트워크

118 전자 메모리

120 보호된 메모리 영역

122 보호된 메모리 영역

124 보호된 메모리 영역

126 메모리 영역

128 프로세서

130 프로그램 명령

132 프로그램 명령

134 프로그램 명령

136 ID 제공자 컴퓨터 시스템

138 네트워크 인터페이스

140 메모리

142 비밀키

144 인증서

145 프로세서

146 프로그램 명령

148 프로그램 명령

149 프로그램 명령

150 서비스 컴퓨터 시스템

152 네트워크 인터페이스

154 프로세서

156 프로그램 명령

158 구성 데이터 레코드

160 구성 데이터 레코드

161 구성 데이터 레코드

162 사용자 입력

164 서비스 요구

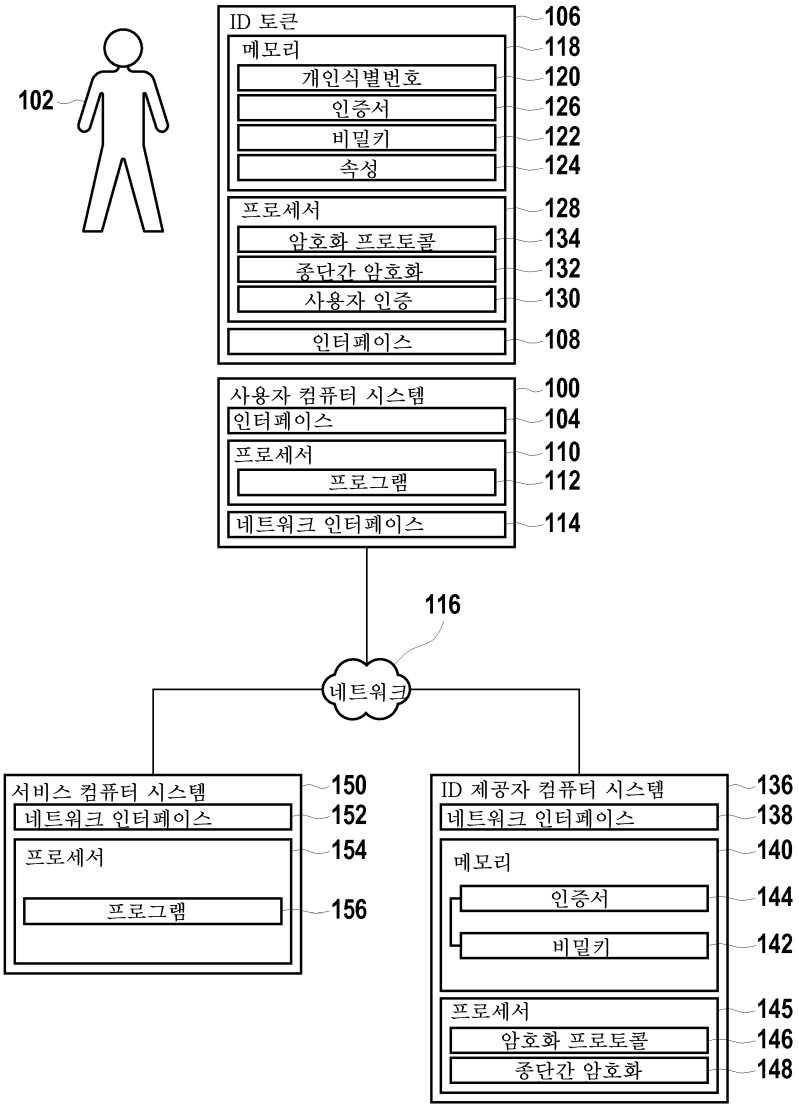
166 속성의 상세

168 요구

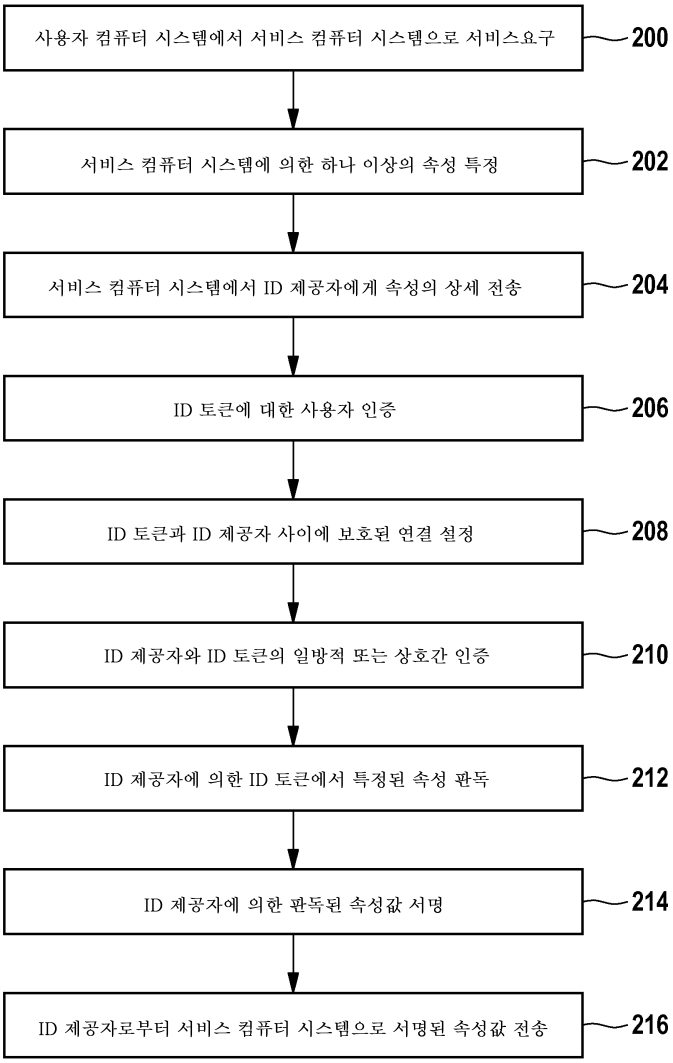
170 응답

도면

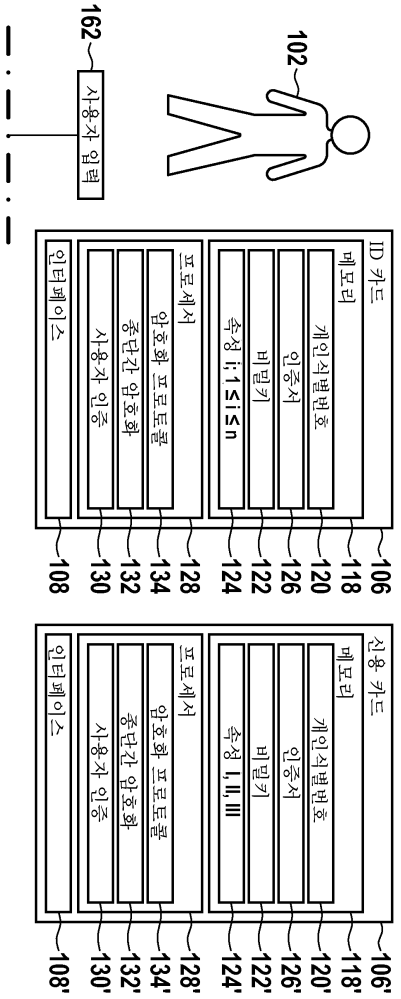
도면1


102
ID 토큰
106
메모리
118
개인식별번호
120
인증서
126
비밀키
122
속성
124
프로세서
128
암호화 프로토콜
134
종단간 암호화
132
사용자 인증
130
인터페이스
108
사용자 컴퓨터 시스템
100
인터페이스
104
프로세서
110
프로그램
112
네트워크 인터페이스
114
116
네트워크
서비스 컴퓨터 시스템
150
네트워크 인터페이스
152
프로세서
154
프로그램
156
ID 제공자 컴퓨터 시스템
136
네트워크 인터페이스
138
메모리
140
인증서
144
비밀키
142
프로세서
145
암호화 프로토콜
146
종단간 암호화
148

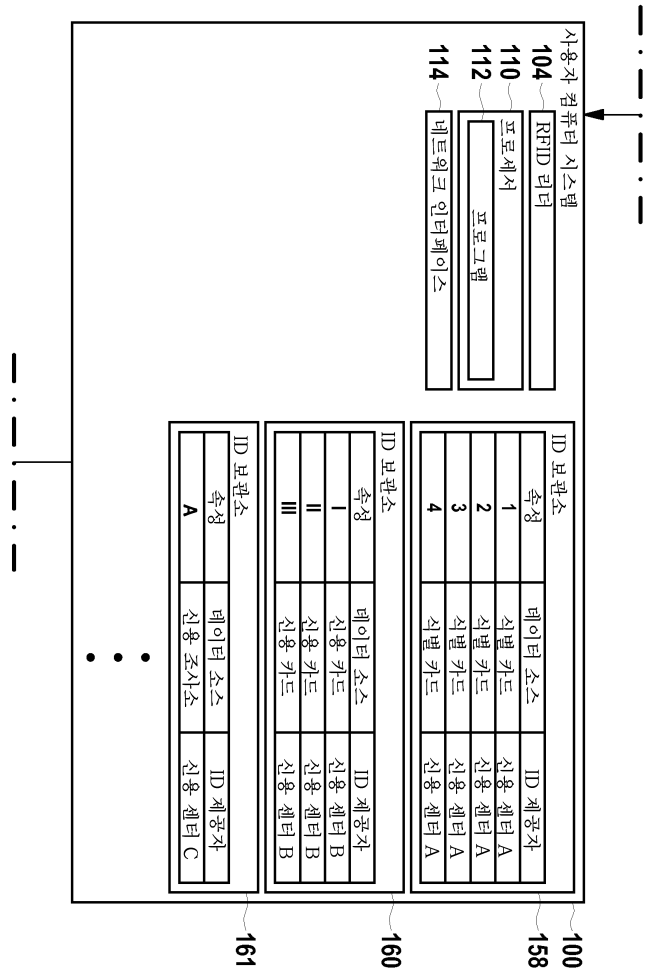
도면2


사용자 컴퓨터 시스템에서 서비스 컴퓨터 시스템으로 서비스요구
200
서비스 컴퓨터 시스템에 의한 하나 이상의 속성 특정
202
서비스 컴퓨터 시스템에서 ID 제공자에게 속성의 상세 전송
204
ID 토큰에 대한 사용자 인증
206
ID 토큰과 ID 제공자 사이에 보호된 연결 설정
208
ID 제공자와 ID 토큰의 일방적 또는 상호간 인증
210
ID 제공자에 의한 ID 토큰에서 특정된 속성 판독
212
ID 제공자에 의한 판독된 속성값 서명
214
ID 제공자로부터 서비스 컴퓨터 시스템으로 서명된 속성값 전송
216

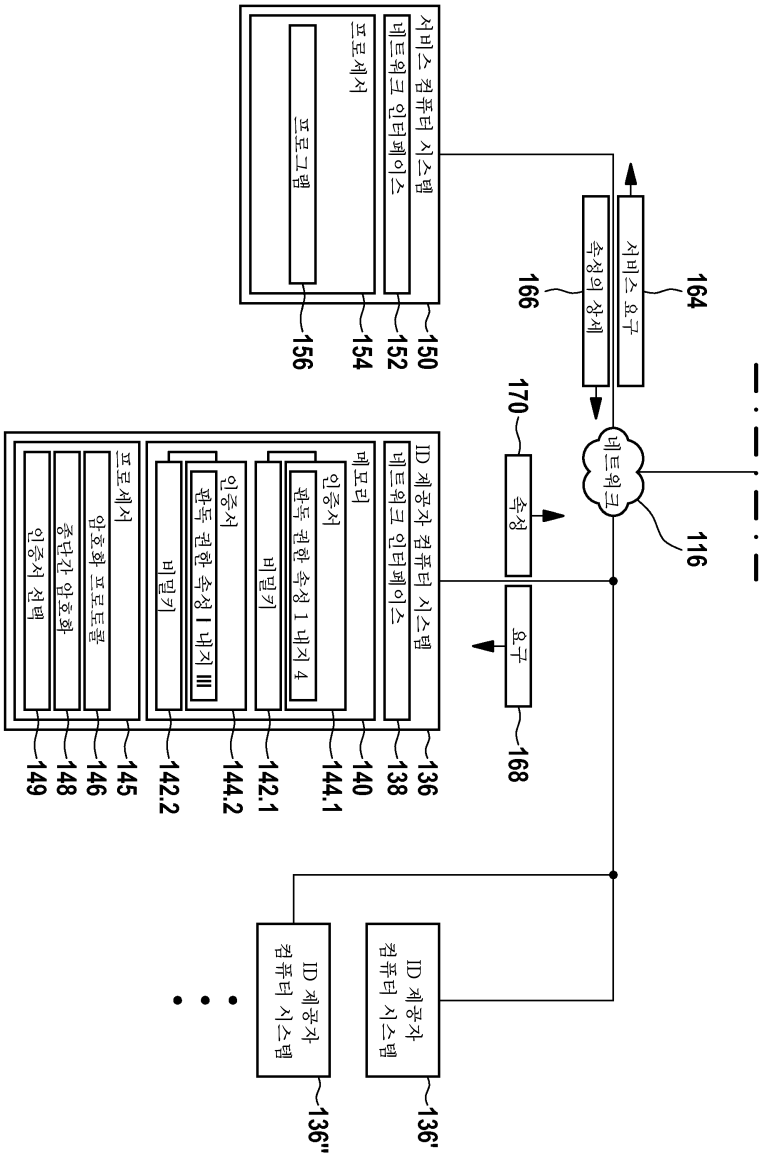
도면3a


102
162
사용자 입력
ID 카드
메모리
개인식별번호
인증서
비밀키
속성 i; 1≤i≤n
프로세서
암호화 프로토콜
종단간 암호화
사용자 인증
인터페이스
106
118
120
126
124
122
128
134
132
130
108
신용 카드
메모리
개인식별번호
인증서
비밀키
속성 I, II, III
프로세서
암호화 프로토콜
종단간 암호화
사용자 인증
인터페이스
106'
118'
120'
126'
124'
122'
128'
134'
132'
130'
108'

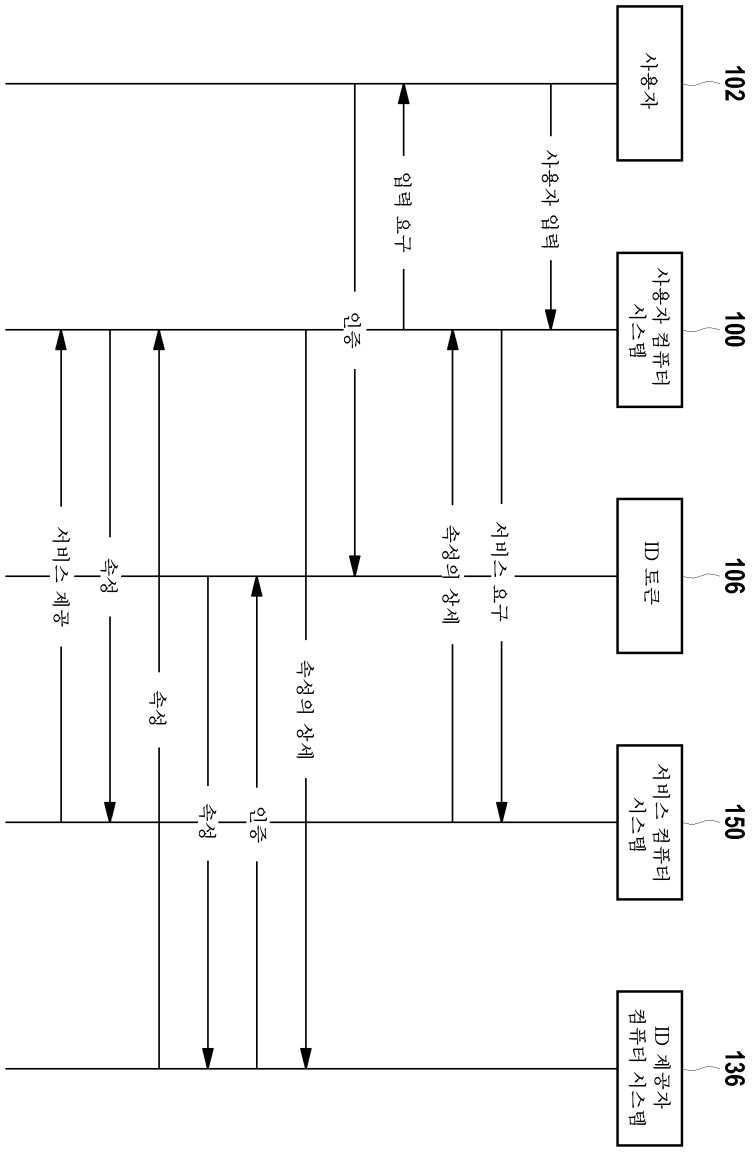
도면3b


사용자 컴퓨터 시스템
104
RFID 리더
110
프로세서
112
프로그램
114
네트워크 인터페이스
ID 보관소
속성
데이터 소스
ID 제공자
1
식별 카드
신용 센터 A
2
식별 카드
신용 센터 A
3
식별 카드
신용 센터 A
4
식별 카드
신용 센터 A
158
100
ID 보관소
속성
데이터 소스
ID 제공자
I
신용 카드
신용 센터 B
II
신용 카드
신용 센터 B
III
신용 카드
신용 센터 B
160
ID 보관소
속성
데이터 소스
ID 제공자
A
신용 조사소
신용 센터 C
161

도면3c


서비스 요구
164
속성의 상세
166
네트워크
116
속성
170
요구
168
서비스 컴퓨터 시스템
네트워크 인터페이스
150
프로세서
152
프로그램
154
156
ID 제공자 컴퓨터 시스템
네트워크 인터페이스
136
메모리
138
인증서
140
팬독 권한 속성 1 내지 4
144.1
비밀키
142.1
인증서
144.2
팬독 권한 속성 I 내지 III
142.2
비밀키
프로세서
145
암호화 프로토콜
146
종단간 암호화
148
인증서 선택
149
ID 제공자 컴퓨터 시스템
136'
ID 제공자 컴퓨터 시스템
136"

도면4



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제13항

【변경전】

'컴퓨터 프로그램 기록매체'

【변경후】

'컴퓨터 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체'