(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년11월16일
(11) 등록번호 10-1676893
(24) 등록일자 2016년11월10일

(51) 국제특허분류(Int. Cl.)
H04W 8/04 (2009.01) *H04L 29/06* (2006.01)
H04W 12/06 (2009.01)
(21) 출원번호 10-2011-7028814
(22) 출원일자(국제) 2010년06월09일
심사청구일자 2015년04월06일
(85) 번역문제출일자 2011년12월01일
(65) 공개번호 10-2012-0037380
(43) 공개일자 2012년04월19일
(86) 국제출원번호 PCT/EP2010/058093
(87) 국제공개번호 WO 2010/145979
국제공개일자 2010년12월23일
(30) 우선권주장
10 2009 026 953.3 2009년06월16일 독일(DE)
(56) 선행기술조사문헌
WO2005119931 A1
US20060205388 A1
WO2008110597 A2

(73) 특허권자
분데스드룩커라이 게엠베하
독일 10969 베를린 코만단텐스트라쎄 18
(72) 발명자
쿠테르, 요아킴
독일 베를린 10179 암 크로겔 3
로에르, 토마스
독일 베를린 10961 빌름스트라쎄 21 비
란젠, 커스텐
독일 베를린 10178 로센탈레르스트라쎄 40
(74) 대리인
특허법인 무한

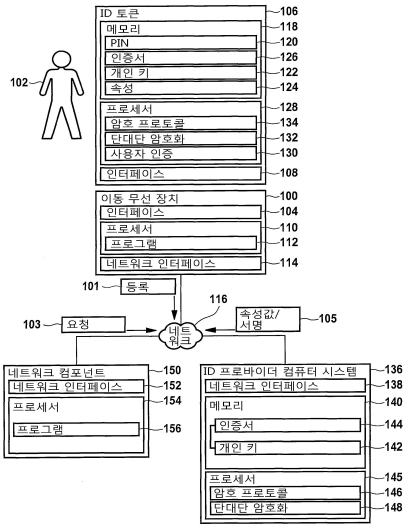
전체 청구항 수 : 총 19 항 심사관 : 장상배

(54) 발명의 명칭 **이동 무선 네트워크에 이동 무선 장치를 등록하기 위한 방법**

(57) 요 약

본 발명은 ID 토큰(106)에 저장된 하나 이상의 속성을 이용하여 이동 무선 네트워크(116)에 이동 무선 장치(100)를 등록하기 위한 방법으로서, ID 토큰이 사용자(102)에 할당된 조건에서, - ID 토큰에 대해 사용자를 인증하는 단계, - ID 토큰에 대해 제1 컴퓨터 시스템(136)을 인증하는 단계, - ID 토큰에 대한 사용자 및 제1 컴퓨터 시스템의 인증이 성공한 후 이동 무선 네트워크를 통해 ID 토큰에 저장된 하나 이상의 속성에 대해 제1 컴퓨터 시스템이 판독 접근하는 단계, - 등록을 위해 하나 이상의 속성을 이용하는 단계를 포함하는 상기 방법에 관한 것이다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

ID 토큰(106) 내에 저장된 하나 이상의 속성을 이용하여 이동 무선 네트워크(116)에 이동 무선 장치(100)를 등록하기 위한 방법에 있어서,

상기 ID 토큰이 사용자(102)에 할당된 조건에서,

- ID 토큰에 대해 사용자를 인증하는 단계와,

- ID 토큰에 대해 제1 컴퓨터 시스템(136)을 인증하는 단계와,

- ID 토큰에 대해 사용자 및 제1 컴퓨터 시스템이 성공적으로 인증받은 후에 이동 무선 네트워크를 통해 ID 토큰 내에 저장된 상기 하나 이상의 속성에 대해 제1 컴퓨터 시스템이 판독 접근하는 단계와,

- 등록을 위해 상기 하나 이상의 속성을 이용하는 단계를 포함하는 방법.

청구항 2

제1항에 있어서, ID 토큰에 대한 제1 컴퓨터 시스템의 인증은 제1 컴퓨터 시스템의 인증서(144)를 이용하여 이루어지되, 상기 인증서는 ID 토큰에 저장되어 있으면서 상기 제1 컴퓨터 시스템이 판독 접근과 관련하여 권한을 갖는 그런 속성들의 정보를 포함하는, 방법.

청구항 3

제2항에 있어서, ID 토큰은 속성들 중 하나 이상의 속성에 대한 판독 접근과 관련한 제1 컴퓨터 시스템의 판독 권한을 인증서를 이용하여 점검하는, 방법.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서,

- 제1 컴퓨터 시스템을 통해서, ID 토큰으로부터 판독된 하나 이상의 속성을 신호화하는 단계와,

- 등록을 실행하거나 초기화하기 위해 제2 컴퓨터 시스템(150; HLR 1, HLR 2, ..., HLR i, HLR I)이 이동 무선 네트워크와 결합된 조건에서, 신호화된 상기 하나 이상의 속성을 상기 제1 컴퓨터 시스템으로부터 제2 컴퓨터 시스템으로 전송하는 단계를 더 포함하는 방법.

청구항 5

제4항에 있어서, 상기 제2 컴퓨터 시스템은 이동 무선 네트워크의 이동 무선 네트워크 컴포넌트인, 방법

청구항 6

제4항에 있어서, 제1 컴퓨터 시스템에 의해 ID 토큰으로부터 판독된 하나 이상의 속성이 이동 무선 장치로 전송되고, 사용자에 의한 릴리스 후에, 상기 하나 이상의 속성은 상기 이동 무선 장치로부터 제2 컴퓨터 시스템으로 전송되는, 방법.

청구항 7

제6항에 있어서, 사용자는 상기 제2 컴퓨터 시스템으로 전송하기 전에 추가의 데이터로 속성들을 보충할 수 있는, 방법.

청구항 8

제1항에 있어서, 상기 이동 무선 장치는 이동 전화기, 스마트 폰, 이동 무선 인터페이스를 포함한 개인 정보 단말기, 이동 무선 인터페이스를 포함한 휴대용 컴퓨터, 또는 이동 무선 인터페이스를 포함한, 예컨대 디지털 카

메라와 같은 휴대용 전자 장치인, 방법.

청구항 9

제1항에 있어서, 식별자들이 저장되어 있는 데이터 베이스(158)에 대한 데이터 베이스 접근이 실행되되, 상기 식별자들 각각에 의해서는 홈 위치 등록기가 식별되고, 사용자에 할당된 홈 위치 등록기(HLR 1, HLR 2, ..., HLR i, ..., HLR I)의 식별자는 하나 이상의 속성을 이용하여 데이터 베이스로부터 판독되며, 그리고 데이터 베이스로부터 판독된 식별자에 의해 식별되는 홈 위치 등록기 내에 이동 무선 장치의 등록이 실행되는, 방법.

청구항 10

제9항에 있어서, 상기 데이터 베이스에 사용자들의 전화 번호가 저장되는, 방법.

청구항 11

제8항에 있어서, 제1 식별자는 이동 무선 장치에 저장되고, 홈 위치 등록기가 식별되도록 하는 제2 식별자는 사용자에게 할당되며, 하나 이상의 속성을 이용하여 상기 제1 식별자가 상기 제2 식별자인지 여부가 검사되며, 그리고 상기 제1 및 제2 식별자가 일치하면, 상기 제1 및 제2 식별자에 의해 식별된 홈 위치 등록기 내 등록이 이루어지는, 방법.

청구항 12

제1항에 있어서, 상기 하나 이상의 속성은 홈 위치 등록기가 식별되도록 하는 식별자이고, 상기 식별자에 의해 식별된 홈 위치 등록기 내 이동 무선 장치의 등록이 이루어지는, 방법.

청구항 13

제1항에 따르는 방법을 실행하기 위한 컴퓨터 프로그램이 기록된 컴퓨터로 판독 가능한 기록 매체.

청구항 14

ID 토큰으로서,

- 하나 이상의 속성을 저장하기 위한 보호되는 메모리 영역(124)과,

- ID 토큰에 대해 ID 토큰에 할당된 사용자(102)를 인증하기 위한 수단(120, 130)과,

- ID 토큰에 대해 제1 컴퓨터 시스템(136)을 인증하기 위한 수단(134)과,

- 이동 무선 장치를 통해 제1 컴퓨터 시스템으로 향하는 보호되는 링크를 구성하되, 상기 제1 컴퓨터 시스템이 상기 보호되는 링크를 통해 상기 하나 이상의 속성을 판독할 수 있게 하는 수단(132)을 포함하는 상기 ID 토큰에 있어서,

상기 제1 컴퓨터 시스템이 상기 ID 토큰으로부터 상기 하나 이상의 속성을 판독하기 위해 필요한 전제 조건은 상기 ID 토큰에 대한 사용자 및 제1 컴퓨터 시스템의 성공적인 인증이며, 그리고 상기 하나 이상의 속성을 통해 이동 무선 네트워크의 홈 위치 등록기(HLR 1, HLR 2, ..., HLR i, ..., HLR I)가 식별될 수 있는, ID 토큰.

청구항 15

제14항에 있어서, 속성들 중 하나 이상의 속성을 상기 제1 컴퓨터 시스템으로 보호되는 조건에서 전송하기 위한 링크를 단대단 암호화하기 위한 수단(132)을 포함하는 ID 토큰.

청구항 16

제14항 또는 제15항에 있어서, 전자 장치, USB 스틱이거나, 또는 증서, 가치 또는 보안 증서인 ID 토큰.

청구항 17

ID 토큰이 사용자(102)에 할당된 조건에서, ID 토큰(106)에 저장된 하나 이상의 속성을 이용하여 이동 무선 네트워크(116)에 이동 무선 장치(100)를 등록하기 위한 이동 무선 시스템으로서,

- 상기 ID 토큰에 대해 제1 컴퓨터 시스템(136)을 인증하기 위한 수단(142, 144, 146)과,

- 상기 ID 토큰에 저장된 상기 하나 이상의 속성에 대한 제1 컴퓨터 시스템의 판독 접근을 실행하되, 이 판독 접근은 사용자 및 제1 컴퓨터 시스템이 ID 토큰에 대해 인증받은 후에 실행될 수 있게 하는 수단(138, 148)과,

- 등록을 위해 상기 하나 이상의 속성을 이용하기 위한 수단(150)을 포함하는 이동 무선 시스템.

청구항 18

제17항에 있어서, 상기 제1 컴퓨터 시스템은 상기 하나 이상의 속성을 신호화하기 위한 수단(144)을 포함하며, 그리고 상기 제1 컴퓨터 시스템으로부터 상기 하나 이상의 신호화된 속성을 수신할 수 있도록 형성되는 네트워크 컴포넌트(150)가 구비되어 있는, 이동 무선 시스템.

청구항 19

제18항에 있어서, 상기 네트워크 컴포넌트는 데이터 베이스(158)를 포함하되, 이 데이터 베이스에는 식별자들이 저장되어 있으며, 식별자들 각각에 의해서는 이동 무선 네트워크의 홈 위치 등록기(HLR 1, HLR 2, ..., HLR i, ..., HLR I)가 식별되며, 사용자에 할당된 식별자에 대한 판독 접근은 하나 이상의 속성에 의해 실행될 수 있는, 이동 무선 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은, 이동 무선 네트워크에 이동 무선 장치를 등록하기 위한 방법, 컴퓨터 프로그램 제품, ID 토큰, 및 이동 무선 시스템에 관한 것이다.

배 경 기 술

[0002] GSM 표준에 따라서는 국제 모바일 가입자 식별 번호(IMSI)를 이용하여 GSM 이동 무선 네트워크 내 이동 무선 장치의 등록이 이루어진다. IMSI는 가입자 식별 모듈(SIM) 내에 저장된다. IMSI를 통해서는 등록이 이루어져야 하는 홈 위치 등록기(HLR)가 식별된다. 유사한 유형 및 방식으로는 UMTS 표준 및 기타 이동 무선 표준에 따른 등록도 이루어진다.

[0003] US 2007/0294431로부터는 사용자 등록을 요구하는 디지털 식별 번호를 이용하기 위한 방법이 공지되었다.

[0004] 또한, 토큰 기반의 인증 방법은 예컨대 US 2001/0045451 A1 및 US 6 257 486 B1로부터 공지되었다.

[0005] 추가의 토큰 기반의 인증 방법은 출원 시점에 공개되지 않은 동일한 특허 출원인의 특허 출원 DE 10 2008 000 067.1-31, DE 10 2008 040 416.0-31 및 DE 10 2008 042 262.2-31에서 개시되었다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 목적은 이동 무선 네트워크에 이동 무선 장치를 등록하기 위한 개선된 방법, 컴퓨터 프로그램, ID 토큰 및 이동 무선 시스템을 제공하는 것에 있다.

과제의 해결 수단

[0007] 본 발명의 기초가 되는 상기 목적들은 각각 독립 청구항들의 특징들에 의해 달성된다. 본 발명에 따른 실시예들은 독립 청구항에서 지시된다.

[0008] 본 발명의 실시예들에 따라 ID 토큰에 저장된 하나 이상의 속성을 이용하여 이동 무선 네트워크 내 이동 무선 장치의 등록이 이루어지되, 이는 ID 토큰이 사용자에게 할당되는 조건에서, ID 토큰에 대해 사용자를 인증하는 단계, ID 토큰에 대해 제1 컴퓨터 시스템을 인증하는 단계, ID 토큰에 대해 사용자 및 제1 컴퓨터의 인증이 성공한 후 이동 무선 네트워크를 통해 ID 토큰에 저장된 하나 이상의 속성에 대해 제1 컴퓨터 시스템이 판독 접근하는 단계, 그리고 등록을 위해 하나 이상의 속성을 이용하는 단계로 실행된다.

[0009] 본 발명의 실시예들은 특히 바람직한데, 그 이유는 이동 무선 장치의 등록을 위해 SIM 카드가 요구되는 것이 아니라, 예컨대 사용자의 신분 증명서, 특히 전자 신분 증명 카드일 수 있는, 사용자에게 할당된 ID 토큰이 요구

되기 때문이다. 다시 말해 사용자가 상기 ID 토큰을 보유하고 있다면, 이동 무선 네트워크에 사용자의 이동 무선 장치를 등록하기 위해 SIM 카드는 추가로 소요되지 않는다. 따라서 SIM 카드의 제조, 개인화, 및 사용자 배포를 위한 기술, 물류 및 재정적 비용도 요구되지 않는다. 그러므로 추가로 특히 바람직하게는 신규 가입할 사용자, 다시 말해 소위 가입자는, SIM 카드의 발송을 기다릴 필요도 없이, 즉시 자신의 이동 무선 장치를 이동 무선 네트워크에 등록할 수 있다.

[0010] 본 발명의 실시예들은, 제1 컴퓨터 시스템을 통해서, ID 토큰에 저장된 속성들 중 하나 이상의 판독을 가능하게 하되, ID 토큰과 제1 컴퓨터 시스템 사이의 링크는 이동 무선 네트워크, 특히 인터넷을 통해 구성될 수 있다. 하나 이상의 속성은 ID 토큰에 할당된 사용자의 식별 번호와 관련한, 특히 사용자의 이른바 디지털 식별 번호와 관련한 데이터일 수 있다. 예컨대 성, 이름, 주소와 같은 속성들을 제2 컴퓨터 시스템에, 예컨대 이동 무선 네트워크의 이동 무선 네트워크 컴포넌트에, 특히 중앙 데이터 베이스 또는 홈 위치 등록기(HLR)로 전송하기 위해, 제1 컴퓨터 시스템에 의해 상기 속성들이 판독된다.

[0011] 본 발명의 실시예에 따라, ID 토큰에 저장된 속성은 식별자이다. 식별자는, 사용자와 이에 추가로 그 사용자에 대해 권한이 있는 이동 무선 네트워크의 홈 위치 등록기를 명확하게 식별하도록 형성될 수 있다. 특히 식별자는 전역 고유 식별자(GUID)로서 형성될 수 있다. 예컨대 식별자는 IMSI일 수 있다.

[0012] 본원에서 "홈 위치 등록기"는 이동 무선 네트워크에 이동 무선 장치를 등록하는 역할을 하는 이동 무선 네트워크의 모든 네트워크 컴포넌트를 의미한다.

[0013] 본원에서 이동 무선 네트워크에 이동 무선 장치를 "등록"하는 과정은, 이동 무선 장치의 사용자 식별 번호가 이동 무선 네트워크에 전달됨으로써, 사용자가 자신의 이동 무선 장치를 이용하여, 예컨대 음성 전화를 걸거나 수신할 수 있고, 메시지를 송신하거나 수신할 수 있고, 그리고/또는 예컨대 이동 무선 네트워크를 통한 데이터 다운로드와 같은 이동 무선 네트워크를 통해 제공되는 또 다른 서비스를 요청할 수 있는 실제 가입자로서 등록되는, 모든 과정을 의미한다.

[0014] ID 토큰은 예컨대 소위 USB 스틱 형태의 휴대용 전자 장치이거나, 또는 증서(document), 특히 가치 또는 보안 증서일 수 있다.

[0015] "증서"란 본 발명에 따라, 예컨대 신분 증명서, 특히 여권, 신분 증명 카드, 비자 또는 운전 면허증, 자동차 등록증, 자동차 등록 증서, 건강 보험 카드, 기타 ID 증서뿐 아니라, 칩 카드, 지불 수단, 특히 현금 인출 카드 및 신용 카드, 또는 그 외 하나 이상의 속성을 저장하기 위한 데이터 메모리가 통합되어 있는 신분 증명서처럼 종이 기반 및/또는 플라스틱 기반의 증서를 의미한다.

[0016] 또한, 본 발명의 실시예들은 특히 바람직한데, 그 이유는 하나 이상의 속성이 특히 신용할 수 있는 증서, 예컨대 관공서 공식 증서로부터 판독되기 때문이다. 또한, 본 발명은, 편리한 취급 조건에서 최적의 데이터 보호와 결부되어, 디지털 식별 번호에 속하는 속성의 전달과 관련한 특히 높은 정도의 신뢰성을 가능하게 한다.

[0017] 본 발명의 실시예에 따라, 제1 컴퓨터 시스템은 ID 토큰에 대해 제1 컴퓨터 시스템의 인증을 위해 이용되는 하나 이상의 인증서를 포함한다. 인증서는 제1 컴퓨터 시스템이 갖는 판독 권한의 대상이 되는 그런 속성의 데이터를 포함한다. ID 토큰은 상기 인증서에 따라, 속성에 대한 판독 접근이 제1 컴퓨터 시스템에 의해 실행될 수 있기 전에, 제1 컴퓨터 시스템이 그 속성에 대한 판독 접근을 위해 요구되는 판독 권한을 갖는지 여부를 검사한다.

[0018] 본 발명의 실시예에 따라, 제1 컴퓨터 시스템은 ID 토큰에 의해 판독되는 하나 이상의 속성을 제2 컴퓨터 시스템에 직접 전송한다. 제2 컴퓨터 시스템은 예컨대 이동 무선 네트워크의 이동 무선 네트워크 컴포넌트일 수 있되, 이 이동 무선 네트워크 컴포넌트를 통해 등록이 이루어진다.

[0019] 본 발명의 실시예에 따라, ID 토큰으로부터 판독된 속성들은 제1 컴퓨터 시스템으로부터 우선 사용자의 이동 무선 장치로 전송된다.

[0020] 본 발명의 실시예에 따라, ID 토큰으로부터 판독된 속성들은 제1 컴퓨터 시스템에 의해 신호화되고 그런 다음 이동 무선 장치로 전송된다. 다시 말해 이동 무선 장치의 사용자는 상기 속성들을 판독할 수 있지만, 변경하지는 못한다. 사용자에 의한 릴리스 후에 비로소 속성들은 이동 무선 장치로부터 제2 컴퓨터 시스템으로 전송된다.

[0021] 본 발명의 실시예에 따라, 사용자는 속성들의 전송 전에 예컨대 사용자가 요청하고 이동 무선 네트워크를 통해

제공될 서비스의 제공을 위해 필요한 속성들만큼 추가 데이터로 상기 속성들을 보충할 수 있다.

[0022] 본 발명의 실시예에 따라, 이동 무선 장치는 이동 전화기, 특히 스마트 폰, 이동 무선 인터페이스를 포함한 개인 정보 단말기(Personal Digital Assistant), 이동 무선 인터페이스를 포함한 휴대용 컴퓨터, 또는 기타 이동 무선 인터페이스를 포함한, 예컨대 디지털 카메라와 같은 휴대용 전자 장치("electronic appliance")이다.

[0023] 본 발명의 실시예에 따라, 예컨대 사용자의 IMSI와 같은 식별자들은 데이터 베이스에 저장된다. ID 토큰으로부터 판독된 하나 이상의 속성으로는, 사용자에 할당된 식별자를 데이터 베이스로부터 판독할 수 있도록 데이터 베이스에 대한 접근이 이루어진다. 또한, 식별자를 통해서는 사용자에 대한 권한이 있는 홈 위치 등록기가 식별된다. 그런 다음 이처럼 사용자에 대한 권한이 있는 홈 위치 등록기에서는 사용자의 이동 무선 장치가 등록된다. 그런 후에 사용자는 자신의 이동 무선 장치로 이동 무선 네트워크를 통해 임의의 전화를 걸거나 수신할 수 있고, 또는 예컨대 데이터 다운로드나 예컨대 인터넷 이용과 같은 또 다른 온라인 서비스와 같은 또 다른 용도로 이동 무선 네트워크를 이용할 수 있다.

[0024] 본 발명의 실시예에 따라, 데이터 베이스에는 사용자에게 할당된 전화 번호도 저장된다. 다시 말해 하나 이상의 속성을 이용하여 식별자뿐 아니라, 사용자에게 할당된 전화 번호가 데이터 베이스로부터 판독된다. 그런 다음 상기 전화 번호는 사용자에 대한 권한이 있으면서 식별자를 통해 식별된 홈 위치 등록기로 전송되고, 그런 다음 상기 홈 위치 등록기에서 적어도 이동 무선 장치가 이동 무선 네트워크에 등록되는 시간 기간 동안 저장된다. 또한, 전화 번호는 사용자에 대한 권한이 있는 홈 위치 등록기 내에 영구적으로 저장될 수도 있다.

[0025] 여기서 특히 바람직하게는 전화 번호는 이동 무선 네트워크의 관리자에 의해 사전 설정되지 않아도 될 뿐더러, 원하는 전화 번호가 이미 어느 것에도 할당되지 않은 점에 한해서 사용자가 자신의 전화 번호를 직접 결정할 수도 있다. 사용자가 원하는 전화 번호는 데이터 베이스 및/또는 권한 있는 HLR에 입력 및 저장되며, 그에 따라 상기 전화 번호는 추가 상세 내역(futher details)을 위한 용도로 결정된다. 데이터 베이스 및/또는 권한 있는 HLR 내 전화 번호의 등록은 사용자의 측에서 예컨대 이동 무선 네트워크의 관리자에 의해 자유롭게 이용할 수 있도록 제공된 인터넷 플랫폼을 통해 이루어질 수 있다.

[0026] 본 발명의 실시예에 따라, 제1 식별자는 사용자의 이동 무선 장치에 저장된다. 데이터 베이스 접근을 이용하여 제2 식별자가 데이터 베이스로부터 판독되되, 데이터 베이스 접근에 대한 키로서는 사용자의 ID 토큰으로부터 판독된 하나 이상의 속성이 이용된다. 그런 다음 제1 및 제2 식별자는 네트워크 측에서 서로 비교된다. 두 식별자가 일치하면, 사용자에 대해 권한이 있으면서 제1 및 제2 식별자에 의해 식별된 홈 위치 등록기에서 이동 무선 장치의 등록이 이루어진다.

[0027] 본 발명의 실시예에 따라, ID 토큰에 저장된 하나 이상의 속성은 사용자뿐 아니라 사용자에 대한 권한이 있는 이동 무선 네트워크의 홈 위치 등록기가 분명하게 식별되게 하는 식별자이다. 예컨대 식별자는 IMSI로서 형성된다. 제1 컴퓨터 시스템은 ID 토큰으로부터 판독된 식별자를 권한 있는 홈 위치 등록기로 전송하며, 이 홈 위치 등록기는 식별자에 의해 식별됨으로써, 해당하는 사용자의 이동 무선 장치의 등록은 상기 홈 위치 등록기를 통해 이루어질 수 있게 된다.

[0028] 본 발명의 실시예에 따라, 이동 무선 장치와 ID 토큰 사이의 통신은 비접촉 방식으로 특히 RFID 또는 근거리 무선 통신(NFC) 표준에 의해 이루어진다. 바람직하게는 이동 무선 장치와 ID 토큰 사이의 데이터 교환을 위해 이용되는 통신 방법의 커버리지(coverage)는 50㎝ 미만의 범위, 특히 최대 30㎝의 범위이다. 특히 RFID 또는 NFC 표준에 따라 무선 신호로 이루어지는 이동 무선 장치와 ID 토큰 사이의 데이터 교환은 사용자에게 관리 장점을 제공한다.

[0029] 예컨대 사용자는 호주머니, 특히 지갑에 ID 토큰을 넣어 소지하고 다닌다. 이동 무선 장치의 등록을 위해 사용자는 호주머니로부터 ID 토큰을 꺼낼 필요가 없는데, 그 이유는 이는 무선 신호를 이용한 통신을 위해 요구되지 않기 때문이다. 동시에 데이터 교환을 위해 사용되는 통신 방법의 적은 커버리지를 바탕으로, 사용자의 이동 무선 장치와 근처에 있는 또 다른 사용자의 ID 토큰 사이의 통신이 이루어지지 않는 점이 보장된다.

[0030] 추가의 관점에서 본 발명은 본 발명에 따른 방법을 실행하기 위해 컴퓨터 시스템에 의해 실행될 수 있는 명령어를 이용하는 컴퓨터 프로그램 제품에 관한 것이다. 컴퓨터 프로그램 제품은 모듈러 형식으로 구성될 수 있으며, 그럼으로써 소정의 모듈은 제1 컴퓨터 시스템에 의해 실행되고 또 다른 모듈은 제2 컴퓨터 시스템에 의해 실행된다.

[0031] 추가의 관점에서 본 발명은 예컨대 신분 증명서, 특히 하나 이상의 속성을 저장하기 위한 보호되는 메모리 영역, ID 토큰에 대해 ID 토큰에 할당된 사용자를 인증하기 위한 수단, ID 토큰에 대해 제1 컴퓨터 시스템을 인

증하기 위한 수단, 이동 무선 장치를 통해 제1 컴퓨터 시스템으로 향하는 보호되는 링크를 구성하기 위한 수단을 포함하는 전자 신분 증명 카드와 같은 ID 토큰에 관한 것으로서, 제1 컴퓨터 시스템은 보호되는 링크를 통해 하나 이상의 속성을 판독할 수 있고, 제1 컴퓨터 시스템을 통해 ID 토큰으로부터 하나 이상의 속성을 판독하기 위해 필요한 전제 조건은 ID 토큰에 대한 사용자 및 제1 컴퓨터 시스템의 성공적인 인증이며, 그리고 하나 이상의 속성을 통해서는 이동 무선 네트워크의 홈 위치 등록기가 식별될 수 있다.

[0032] 추가의 관점에서 본 발명은, ID 토큰이 사용자에 할당되는 조건에서, ID 토큰에 저장된 하나 이상의 속성을 이용하여 이동 무선 네트워크에 이동 무선 장치를 등록하기 위한 이동 무선 시스템에 있어서, ID 토큰에 대해 제1 컴퓨터 시스템(136)을 인증하기 위한 수단과, 이동 무선 네트워크를 통해 ID 토큰에 저장된 하나 이상의 속성에 대한 제1 컴퓨터 시스템의 판독 접근을 실행하면서, 판독 접근은 사용자 및 제1 컴퓨터 시스템이 ID 토큰에 대해 인증된 후에 실행될 수 있도록 하는 수단과, 그리고 등록을 위해 하나 이상의 속성을 이용하기 위한 수단을 포함하는 상기 이동 무선 시스템에 관한 것이다.

[0033] 본 발명의 실시예에 따라, ID 토큰은 단대단 암호화를 위한 수단을 포함한다. 이는 이동 무선 장치를 통해 ID 토큰과 제1 컴퓨터 시스템 사이의 링크를 구성할 수 있게 하는데, 그 이유는 사용자가 단대단 암호화를 바탕으로 링크를 통해 전송되는 데이터를 변경할 수 없기 때문이다.

[0034] 다음에서 본 발명의 실시예들은 도면과 관련하여 더욱 상세하게 설명된다.

발명의 효과

[0035] 본 발명에 따르면, 편리한 취급 조건에서 최적의 데이터 보호와 결부되어, 디지털 식별 번호에 속하는 속성의 전달과 관련한 특히 높은 정도의 신뢰성을 가능하게 한다.

도면의 간단한 설명

[0036] 도 1은 본 발명에 따른 ID 토큰 및 본 발명에 따른 이동 무선 시스템의 실시예를 도시한 블록선도이다.

도 2는 본 발명에 따른 방법의 실시예를 나타낸 흐름도이다.

도 3은 본 발명에 따른 방법의 실시예를 나타낸 UML 다이어그램이다.

도 4는 본 발명에 따른 ID 토큰 및 본 발명에 따른 이동 무선 시스템의 추가 실시예를 도시한 블록선도이다.

도 5는 본 발명에 따른 ID 토큰 및 본 발명에 따른 이동 무선 시스템의 추가 실시예를 도시한 블록선도이다.

도 6은 본 발명에 따른 ID 토큰 및 본 발명에 따른 이동 무선 시스템의 추가 실시예를 도시한 블록선도이다.

발명을 실시하기 위한 구체적인 내용

[0037] 서로 상응하는 다음 실시예들의 부재들은 동일한 도면 부호로 식별 표시된다.

[0038] 도 1에는 사용자(102)의 이동 무선 장치(100)가 도시되어 있다. 이동 무선 장치(100)는 예컨대 랩탑이나 팜탑 컴퓨터와 같은 휴대용 컴퓨터, 개인 정보 단말기, 이동 통신 장치, 특히 이동 전화기, 스마트 폰 등일 수 있다. 이동 무선 장치(100)는 대응하는 인터페이스(108)를 포함하는 ID 토큰(106)과의 통신을 위한 인터페이스(104)를 포함한다. 인터페이스(104)는 무선 인터페이스, 특히 RFID 또는 NFC 인터페이스일 수 있다.

[0039] 특히 ID 토큰(106)은 증서, 특히 예컨대 전자 여권 같은 기계 판독 가능 여행 증서(MRTD), 또는 전자 신분 증명 카드, 또는 예컨대 신용 카드 같은 지불 수단과 같은 가치 또는 보안 증서일 수 있다.

[0040] 이동 무선 장치(100)는 프로그램 명령어(112)를 실행하기 위한 하나 이상의 프로세서(110)뿐 아니라, 이동 무선 네트워크(116)를 통한 통신을 위한 이동 무선 네트워크 인터페이스(114)를 포함한다. 이동 무선 네트워크는 GSM, UMTS, CDMA 2000 네트워크, 또는 예컨대 3GPP 롱 텀 에볼루션(LTE) 또는 4G 같은 또 다른 이동 무선 표준에 따른 이동 무선 네트워크일 수 있다.

[0041] ID 토큰(106)은 보호되는 메모리 영역들(120, 122, 124)을 보유하는 전자 메모리(118)를 포함한다. 보호되는 메모리 영역(120)은 ID 토큰(106)에 대한 사용자(102)의 인증을 위해 필요한 기준 값을 저장하는 역할을 한다. 상기 기준 값은 예컨대 식별 코드, 특히 이른바 개인 식별 번호(PIN)이거나, 또는 ID 토큰(106)에 대한 사용자의 인증을 위해 이용될 수 있는 사용자의 바이오인식 특징에 대한 기준 데이터이다.

[0042] 보호되는 영역(122)은 개인 키를 저장하는 역할을 하고, 보호되는 메모리 영역(124)은 예컨대 사용자(102)의 이

름, 주소, 생년월일, 성별과 같은 상기 사용자의 속성, 및/또는 예컨대 ID 토큰을 제조 또는 지급한 기관, ID 토큰의 유효 기간, 여권 번호 또는 신용 가드 번호처럼 ID 토큰 자체에 관계하는 속성들을 저장하는 역할을 한다.

[0043] 대체되거나 추가되는 실시예에 따라, 메모리 영역(124) 내에는 ID 토큰(106)이 할당된 사용자(102)가 분명하게 식별되게 하는 식별자가 저장될 수 있다. 또한, 식별자를 통해서는 이동 무선 네트워크(116)의 네트워크 컴포넌트(150)가 식별될 수도 있다. 이런 네트워크 컴포넌트(15)를 통해서 이동 무선 네트워크(116) 내 이동 무선 장치(100)의 등록이 활성화되거나 실행된다. 특히 식별자는 IMSI로서 형성될 수 있다. 특히 식별자는 다중 숫자의 번호로서 형성될 수 있되, 상기 다중 숫자 번호 중 사전 지정된 자릿수는 HLR 번호를 형성하며, 이 HLR 번호를 통해 사용자(102)에 대해 권한이 있는 HLR이 식별된다.

[0044] 또한, 전자 메모리(118)는 인증서를 저장하기 위한 메모리 영역(126)을 포함할 수 있다. 인증서는 공개 키 기반 구조(PKI) 표준에 따라, 예컨대 X.509 표준에 따라 생성될 수 있다.

[0045] 인증서는 반드시 ID 토큰(106)의 전자 메모리(118)에 저장될 필요는 없다. 대체되거나 추가되는 실시예에 따라 인증서는 또한 공용 디렉터리 서버(public directory server)에도 저장될 수 있다.

[0046] ID 토큰(106)은 프로세서(128)를 포함한다. 프로세서(128)는 프로그램 명령어들(130, 132, 134)을 실행하는 역할을 한다. 프로그램 명령어들(130)은 사용자 인증을 위해 이용되며, 다시 말하면 ID 토큰에 대해 사용자(102)를 인증하는 역할을 한다.

[0047] PIN을 이용한 실시예의 경우, 사용자(102)는 예컨대 이동 무선 장치(100)를 통해 ID 토큰(106)에 자신을 인증하기 위한 자신의 PIN을 입력한다. 그런 다음 프로그램 명령어들(130)의 실행을 통해, 보호되는 메모리 영역(120)에 저장된 PIN의 기준 값과 입력된 PIN을 비교할 수 있도록, 상기 보호되는 메모리 영역(120)에 대한 접근이 이루어진다. 입력된 PIN이 PIN의 기준 값과 일치하는 경우 사용자(102)는 인증받은 것으로서 간주된다.

[0048] 대체되는 실시예에 따라, 사용자(102)의 바이오인식 특징이 검출된다. 이를 위해 예컨대 ID 토큰(106)은 지문 센서를 포함하거나, 또는 지문 센서가 이동 무선 장치(100)에 연결되거나 이 이동 무선 장치 내에 통합된다. 본 실시예의 경우 사용자(102)로부터 검출된 바이오인식 데이터는, 프로그램 명령어들(130)의 실행을 통해, 보호되는 메모리 영역(120)에 저장된 바이오인식 기준 데이터와 비교된다. 바이오인식 기준 데이터와 사용자(102)로부터 검출된 바이오인식 데이터가 충분히 일치할 경우 사용자(102)는 인증받은 것으로서 간주된다.

[0049] 프로그램 명령어들(134)은 ID 토큰(106)에 대해 ID 프로바이더 컴퓨터 시스템(136)을 인증하기 위한 암호 프로토콜의 단계이면서 ID 토큰(106)에 관련하는 단계를 실행하는 역할을 한다. 암호 프로토콜은 대칭 키 또는 비대칭 키 쌍을 기반으로 하는 시도-응답 프로토콜(challenge-response protocol)일 수 있다.

[0050] 예컨대 암호 프로토콜을 통해서는, 기계 판독 여행 증서(machine-readable travel documents - MRTD)에 대해 국제 민간 항공 기구(ICAO)에 의해 명시된 것처럼 확장 접근 제어 방법이 구현된다. 암호 프로토콜을 성공적으로 실행한 후에 ID 프로바이더 컴퓨터 시스템(136)은 ID 토큰에 대해 인증을 받고, 그에 따라 보호되는 메모리 영역(124)에 저장된 속성을 판독하기 위한 판독 권한을 입증한다. 또한, 인증은 서로 상호 간에 이루어질 수 있는데, 다시 말하면 그런 다음 ID 토큰(106)이 동일한 암호 프로토콜, 또는 또 다른 암호 프로토콜에 따라 ID 프로바이더 컴퓨터 시스템(136)에 대해 인증을 받아야 한다.

[0051] 프로그램 명령어들(132)은, ID 토큰(106)과 ID 프로바이더 컴퓨터 시스템(136) 사이에서 전송되는 데이터를, 그러나 적어도 보호되는 메모리 영역(124)으로부터 ID 프로바이더 컴퓨터 시스템(136)에 의해 판독된 속성을 단대단 암호화하는 역할을 한다. 단대단 암호화의 경우 대칭 키가 이용될 수 있으며, 이런 대칭 키는 예컨대 ID 토큰(106)과 ID 프로바이더 컴퓨터 시스템(136) 사이에서 암호 프로토콜을 실행할 때 결정된다.

[0052] 도 1에 도시된 실시예에 대체되는 실시예에 따라, 이동 무선 장치(100)는 자체의 인터페이스(104)로 인터페이스(108)와 직접 통신하는 것이 아니라, ID 토큰(106)을 위해 인터페이스(104)에 연결된 판독 장치를 통해 통신할 수 있다. 예컨대 소위 클래스 2 칩카드 단말기와 같은 상기 판독 장치를 통해서는 PIN의 입력도 이루어질 수 있다.

[0053] ID 프로바이더 컴퓨터 시스템(136)은, 이동 무선 네트워크(116)를 통한 통신, 또는 이 이동 무선 네트워크(116)의 네트워크 컴포넌트와의 통신을 위한, 특히 이동 무선 네트워크(116)의 코어 네트워크 또는 이른바 백본(backbone)을 통한 통신을 위한 이동 무선 네트워크 인터페이스(138)를 포함한다. 또한, ID 프로바이더 컴퓨터 시스템(136)은 ID 프로바이더 컴퓨터 시스템(136)의 개인 키(142)뿐 아니라 대응하는 인증서(144)가 저장되어

있는 메모리(140)를 포함한다. 또한, 상기 인증서는 예컨대 X.509처럼 PKI 표준에 따른 인증서일 수 있다.

[0054] 또한, ID 프로바이더 컴퓨터 시스템(136)은 프로그램 명령어들(146 및 148)을 실행하기 위한 하나 이상의 프로세서(145)를 포함한다. 프로그램 명령어들(146)의 실행을 통해, 암호 프로토콜의 단계이면서 ID 프로바이더 컴퓨터 시스템(136)에 관계하는 단계들이 실행된다. 다시 말해 전체적으로 암호 프로토콜은 ID 토큰(106)의 프로세서(128)에 의해 프로그램 명령어들(134)이 실행되는 것을 통해, 그리고 ID 프로바이더 컴퓨터 시스템(136)의 프로세서(145)에 의해 프로그램 명령어들(146)이 실행되는 것을 통해 구현된다.

[0055] 프로그램 명령어들(148)은, 예컨대 ID 토큰(106)과 ID 프로바이더 컴퓨터 시스템(136) 사이에서 암호 프로토콜을 실행할 때 결정되었던 대칭 키를 기반으로, ID 프로바이더 컴퓨터 시스템(136)의 측에서 단대단 암호화의 구현을 위해 이용된다. 기본적으로 앞서 공지된 대칭 키를 결정하기 위한 모든 방법은 예컨대 디플-헬만(Diffle-Hellman) 키 교환처럼 단대단 암호화를 위해 이용될 수 있다.

[0056] ID 프로바이더 컴퓨터 시스템(136)은 바람직하게는 특별히 보호되는 환경에, 특히 이른바 트러스트 센터(Trust center)에 위치하며, 그럼으로써 ID 프로바이더 컴퓨터 시스템(136)은 ID 토큰(106)에 대한 사용자(102)의 인증 필요성과 결합되어 ID 토큰(106)으로부터 판독된 속성의 진정성에 대한 신뢰의 상징을 형성하게 된다.

[0057] 또한, 본 발명의 추가 실시예에 따라, ID 프로바이더 컴퓨터 시스템(136)은 네트워크 컴포넌트(150)의 통합 구성 요소를 형성할 수 있다.

[0058] 네트워크 컴포넌트(150)는 홈 위치 등록기로서 형성될 수 있거나, 또는 네트워크 컴포넌트(150)는, 이동 무선 장치의 등록을 실행하거나 활성화할 수 있도록, 이동 무선 네트워크(116)의 홈 위치 등록기와 상호 작용하도록 형성될 수 있다.

[0059] 네트워크 컴포넌트(150)는 특히 이동 무선 네트워크(116)의 코어 네트워크 또는 이른바 백본을 통해, 이동 무선 네트워크(116), 또는 이 이동 무선 네트워크(116)의 또 다른 네트워크 컴포넌트와의 링크를 위한 이동 무선 네트워크 인터페이스(152)를 포함한다. 특히 네트워크 컴포넌트(150)와 ID 프로바이더 컴퓨터 시스템(136) 사이의 통신은 이동 무선 네트워크(116)의 코어 네트워크 또는 백본을 통해 이루어질 수 있다.

[0060] 또한, 네트워크 컴포넌트(150)는 프로그램 명령어들(156)을 실행하기 위한 하나 이상의 프로세서(154)를 포함한다. 프로그램 명령어들(156)의 실행을 통해 예컨대 하나 이상의 속성에 따라 이동 무선 네트워크(116) 내 이동 무선 장치의 등록이 이루어지거나, 또는 상기 실행에 의해 등록이 초기화된다.

[0061] 이동 무선 네트워크(116) 내 이동 무선 장치(100)의 등록을 위해 다음과 같이 진행된다.

[0062] 1. ID 토큰(106)에 대한 사용자(102)의 인증.

[0063] 사용자(102)는 ID 토큰(106)에 대해 인증을 받는다. 이를 위해 PIN을 이용한 구현의 경우 사용자(102)는 예컨대 이동 무선 장치(100) 또는 이 이동 무선 장치에 연결되거나 통합된 칩카드 단말기를 통해 자신의 PIN을 입력한다. 그런 다음 프로그램 명령어들(130)의 실행을 통해 ID 토큰(106)은 입력된 PIN의 정확성을 검사한다. 입력된 PIN이 보호되는 메모리 영역(120)에 저장된 PIN의 기준 값과 일치하면, 사용자(102)는 인증받은 것으로서 간주된다. 이와 유사하게 사용자(102)의 바이오인식 특징이 사용자의 인증을 위해 이용될 때에도 앞서 기재한 바대로 진행될 수 있다.

[0064] 2. ID 토큰(106)에 대한 ID 프로바이더 컴퓨터 시스템(136)의 인증.

[0065] 이를 위해 이동 무선 장치(100) 및 이동 무선 네트워크(116)를 통해 ID 토큰(106)과 ID 프로바이더 컴퓨터 시스템(136) 사이에 링크가 이루어진다. 예컨대 ID 프로바이더 컴퓨터 시스템(136)은 상기 링크를 통해 자체의 인증서(144)를 ID 토큰(106)으로 전송한다. 그런 다음 프로그램 명령어들(134)을 통해 이른바 챌린지(challenge), 다시 말해 예컨대 난수가 생성된다. 이런 난수는 인증서(144)에 포함된 ID 프로바이더 컴퓨터 시스템(136)의 공개 키와 함께 암호화된다. 그리고 그 결과에 따른 사이퍼 텍스트(cipher text)는 ID 토큰(106)으로부터 링크를 통해 ID 프로바이더 컴퓨터 시스템(136)으로 전송된다. ID 프로바이더 컴퓨터 시스템(136)은 자체 개인 키(142)를 이용하여 사이퍼 텍스트를 복호화하고 그에 따라 난수를 획득한다. 난수는 ID 프로바이더 컴퓨터 시스템(136)으로부터 링크를 통해 ID 토큰(106)으로 다시 전송된다. ID 토큰에서 프로그램 명령어들(134)의 실행을 통해, ID 프로바이더 컴퓨터 시스템(136)이 수신한 난수가 원래 생성된 난수와, 다시 말해 챌린지와 일치하는지 여부가 검사된다. 만일 일치한다면, ID 프로바이더 컴퓨터 시스템(136)은 ID 토큰(106)에 대해 인증받은 것으로서 간주된다. 난수는 대칭 키로서 단대단 암호화를 위해 이용될 수 있다.

[0066] 3. 하나 이상의 속성의 판독.

[0067] 사용자(102)가 ID 토큰(106)에 대해 성공적으로 인증을 받은 후에, 그리고 ID 프로바이더 컴퓨터 시스템(136)이 ID 토큰(106)에 대해 성공적으로 인증을 받은 후에, ID 프로바이더 컴퓨터 시스템(136)은 보호되는 메모리 영역(124)에 저장된 속성 하나, 다수, 또는 모두를 판독할 판독 권한을 수신한다. 그런 다음 ID 프로바이더 컴퓨터 시스템(136)이 링크를 통해 ID 토큰(106)으로 전송하는 대응하는 판독 명령어를 바탕으로 요청되는 속성들이 보호되는 메모리 영역(124)으로부터 판독되며, 프로그램 명령어들(132)의 실행을 통해 암호화된다. 암호화된 속성들은 링크를 통해 ID 프로바이더 컴퓨터 시스템(136)으로 전송되고, 이 컴퓨터 시스템에서 프로그램 명령어들(148)의 실행을 통해 복호화된다. 그럼으로써 ID 프로바이더 컴퓨터 시스템(136)은 ID 토큰(106)으로부터 판독된 속성들의 정보를 수신하게 된다.

[0068] 상기 속성들은 ID 프로바이더 컴퓨터 시스템에 의해 이 컴퓨터 시스템의 인증서(144)를 이용하여 신호화되고, 이동 무선 장치(100)를 통해, 또는 직접적으로 네트워크 컴포넌트(150)로 전송된다. 그럼으로써 네트워크 컴포넌트(150)는 ID 토큰(106)으로부터 판독된 속성들에 대한 정보를 수신하며, 그럼으로써 네트워크 컴포넌트(150)는 상기 속성들에 따라 이동 무선 네트워크(116)에 이동 무선 장치(100)를 등록할 수 있거나, 상기 속성들에 따른 등록을 활성화할 수 있게 된다.

[0069] ID 토큰(106)에 대한 사용자(102)의 인증, 및 ID 토큰(106)에 대한 ID 프로바이더 컴퓨터 시스템(136)의 인증의 필요성을 통해 필요한 신뢰 상징이 제공되며, 그럼으로써 네트워크 컴포넌트(150)는 ID 프로바이더 컴퓨터 시스템(136)으로부터 자체에 통지된 사용자(102)의 속성들이 적절하며 위조되지 않은 것임을 확실하게 신뢰할 수 있게 된다.

[0070] 각각의 실시예에 따라, 인증의 시퀀스는 서로 다를 수 있다. 예컨대 최초 사용자(102)가 ID 토큰(106)에 대해 인증을 받아야 한다면, 후속하여 ID 프로바이더 컴퓨터 시스템(136)이 인증을 받을 수 있다. 그러나 기본적으로 최초 ID 프로바이더 컴퓨터 시스템(136)이 ID 토큰(106)에 대해 인증을 받아야 하고 그런 후에 비로소 사용자(102)가 인증을 받을 수도 있다.

[0071] 위의 단락에서 첫 번째의 경우 ID 토큰(106)은 사용자(102)에 의한 정확한 PIN 또는 정확한 바이오인식 특징의 입력을 통해서만 잠금 해제되도록 형성된다. 이런 잠금 해제만이 비로소 프로그램 명령어들(132 및 134)의 시작과 그에 따른 ID 프로바이더 컴퓨터 시스템(136)의 인증을 가능하게 한다.

[0072] 두 번째의 경우 프로그램 명령어들(132 및 134)의 시작은 또한 사용자(102)가 아직 ID 토큰(106)에 대해 인증을 받지 않았을 때에도 이미 가능하다. 이런 경우 예컨대 프로그램 명령어들(134)은, 프로그램 명령어들(130)에 의해 사용자(102)의 성공적인 인증이 신호화된 이후에 비로소 ID 프로바이더 컴퓨터 시스템(136)이 하나 이상의 속성을 판독하기 위해 보호되는 메모리 영역(124)에 대한 판독 접근을 실행할 수 있도록 형성된다.

[0073] 이동 무선 장치(100)의 등록을 위해, 이동 무선 장치(100)는 자체의 네트워크 인터페이스(114)를 통해 예컨대 신호(101)를 이동 무선 네트워크(116)로 전송할 수 있다. 이런 신호(101)의 전송은 또한 이동 무선 장치(100)가 이동 무선 네트워크(116)에 등록되지 않은 때에도 이미 가능할 수 있다.

[0074] 신호(101)는, 네트워크 컴포넌트(150)가 ID 프로바이더 컴퓨터 시스템(136)으로 요청(103)을 보내면서, 이동 무선 네트워크(116)의 네트워크 컴포넌트(150)에 의해 처리된다. 상기 요청(103)을 바탕으로, 사용자(102) 및 ID 프로바이더 컴퓨터 시스템(136)의 인증이 이루어진 후에, ID 프로바이더 컴퓨터 시스템(136)은 ID 토큰(106)으로부터 하나 이상의 속성값을 판독한다. 그런 다음 ID 프로바이더 컴퓨터 시스템(136)은 요청(103)에 대해 하나 이상의 속성값과 이 속성값의 서명을 포함하는 메시지(105)로 응답한다. 이런 메시지는 이동 무선 네트워크(116)의 네트워크 컴포넌트(150) 또는 다른 네트워크 컴포넌트에 의해 수신되고 사용자(102)의 이동 무선 장치(100)의 등록을 위해 이용된다.

[0075] 또한, ID 토큰(106)과 ID 프로바이더 컴퓨터 시스템(136) 사이의 통신은 이동 무선 장치(100)의 등록 전에 이미 이동 무선 네트워크(116)를 통해 이루어질 수 있다. 예컨대 이를 위해, 이동 무선 네트워크(116)의 측에서 신호(101)의 수신을 바탕으로, 이동 무선 장치(100)가 아직 등록되지 않은 점에 한해서, 이동 무선 네트워크(116)를 통한 이동 무선 장치(100)와의 통신을 위해 이용되는 임시 식별 코드가 이동 무선 장치(100)에 할당된다.

[0076] 도 2에는 본 발명에 따른 방법의 실시예가 도시되어 있다.

[0077] 사용자(102)의 ID 토큰(106)을 이용하여 사용자(102)의 이동 무선 장치(100)를 등록하기 위해 예컨대 다음과 같이 진행된다. 단계 200에서 사용자는 ID 토큰에 대해 인증을 받는다. 이는 사용자가 이동 무선 장치의 키 버

튼을 통해, 이동 무선 장치로부터 이 이동 무선 장치의 인터페이스를 통해 ID 토큰의 인터페이스로 전송되는 사용자 자신의 PIN을 입력하도록 이루어질 수 있다. ID 토큰에 대한 사용자의 인증이 성공했다면, 단계 202에서 ID 토큰과 ID 프로바이더 컴퓨터 시스템 사이의 링크가 구성된다.

[0078] 상기 링크는 바람직하게는 이른바 보안 메시지 기법에 따라 보안된 링크이다.

[0079] 단계 204에서는 단계 202에서 구성된 링크를 통해 적어도 ID 토큰에 대한 ID 프로바이더 컴퓨터 시스템의 인증이 이루어진다. 이에 추가로 ID 프로바이더 컴퓨터 시스템에 대한 ID 토큰의 인증도 제공될 수 있다.

[0080] 사용자뿐 아니라 ID 프로바이더 컴퓨터 시스템이 ID 토큰에 대해 성공적으로 인증받은 후에, ID 프로바이더 컴퓨터 시스템은 ID 토큰으로부터 속성들 중 하나 이상을 판독하기 위한 접근 권한을 수신한다. 단계 206에서는 ID 프로바이더 컴퓨터 시스템이 ID 토큰으로부터 필요한 속성들을 판독하기 위한 하나 이상의 판독 명령어를 전송한다. 그런 다음 속성들은 단대단 암화호에 의해 보안된 링크를 통해 ID 프로바이더 컴퓨터 시스템으로 전송되어 이 컴퓨터 시스템에서 복호화된다.

[0081] 판독된 속성값들은 단계 208에서 ID 프로바이더 컴퓨터 시스템에 의해 신호화된다. 단계 210에서는 ID 프로바이더 컴퓨터 시스템이 신호화된 속성값들을 네트워크 컴포넌트로 전송한다. 상기 하나 이상의 속성값의 전송은 이동 무선 네트워크를 통해 이루어질 수 있다. 대체되는 실시예에 따라, ID 프로바이더 컴퓨터 시스템은 네트워크 컴포넌트의 부분이며, 그럼으로써 전송이 요구되지 않을 수 있다.

[0082] 신호화된 속성값들은 직접적으로 또는 이동 무선 장치를 통해 네트워크 컴포넌트에 도달한다. 이동 무선 장치를 통하는 경우 사용자는 신호화된 속성값들에 대한 정보를 알 수 있고, 그리고/또는 추가 데이터를 보충할 수 있다. 신호화된 속성값들은 경우에 따라 보충된 데이터와 함께 사용자에 의한 릴리스 후에 비로소 이동 무선 장치로부터 네트워크 컴포넌트로 전송될 수 있다. 그럼으로써 ID 프로바이더 컴퓨터 시스템으로부터 네트워크 컴포넌트로 전송된 속성들과 관련하여 사용자에 대해 가능한 최대의 투명성이 달성된다.

[0083] 그런 다음 단계 212에서는 이동 무선 장치가 ID 토큰으로부터 판독된 속성값들에 따라 네트워크 컴포넌트에 의해 이동 무선 네트워크에 등록된다.

[0084] 도 3에는 본 발명에 따른 방법의 추가 실시예가 도시되어 있다.

[0085] 이동 무선 네트워크(116)에 사용자 자신의 이동 무선 장치(100)를 등록하기 위해 사용자(102)는 우선 ID 토큰(106)에 대해 인증을 받는다. ID 토큰(106)에 대한 사용자(102)의 성공적인 인증 후에 이동 무선 장치(100)는, 이동 무선 네트워크에 대해 이동 무선 장치(100)가 이동 무선 네트워크에 등록되어야 하는 점을 신호화하기 위해, 이동 무선 네트워크(116)를 통해 신호를 이동 무선 네트워크의 네트워크 컴포넌트(150)로 전송한다.

[0086] 그에 이어서 네트워크 컴포넌트(150)는 ID 프로바이더 컴퓨터 시스템(136)으로 요청을 전송한다. 상기 요청은 이동 무선 네트워크(116)를 통해 전송될 수 있다. 또한, 상기 요청은, 특히 ID 프로바이더 컴퓨터 시스템(136)이 네트워크 컴포넌트(150)의 통합 구성 요소인 경우라면, 네트워크 컴포넌트(150)로부터 직접 ID 프로바이더 컴퓨터 시스템(136)으로 전달될 수도 있다.

[0087] 네트워크 컴포넌트(150)에 의해 수신된 요청을 바탕으로 ID 프로바이더 컴퓨터 시스템(136)은 ID 토큰(106)에 대해 인증을 받고 속성들 중 하나 이상을 판독하기 위한 권한 요청을 ID 토큰(106)으로 전송한다.

[0088] 이전에 사용자(102) 및 ID 프로바이더 컴퓨터 시스템(136)의 성공적인 인증이 이루어진 전제 조건 하에서, ID 토큰(106)은 원하는 속성들로 판독 요청에 응답한다. ID 프로바이더 컴퓨터 시스템(136)은 속성들을 신호화하여 이 신호화된 속성들을 이동 무선 장치(100)로 전송한다. 그런 다음 이동 무선 장치(100)에서 사용자(102)에 의한 릴리스 후에 신호화된 속성들은 네트워크 컴포넌트(150)로 전송된다. 그런 다음 네트워크 컴포넌트(150)는 이동 무선 장치(100)의 등록을 활성화한다.

[0089] 도 4에는 데이터 베이스(158)를 포함하는 본 발명에 따른 이동 무선 시스템의 실시예가 도시되어 있다. 데이터 베이스(158)는 이동 무선 네트워크(116)의 각각의 등록된 사용자에 대해 분명한 식별자 및 전화 번호가 저장되어 있는 하나 이상의 데이터 베이스 도표(160)를 포함한다. 사용자(102)의 식별자 및 전화 번호의 판독을 위해서는 사용자(102)의 ID 토큰(106)으로부터 ID 프로바이더 컴퓨터 시스템(136)에 의해 판독되어야 하는 하나 이상의 속성값의 정보가 요구된다.

[0090] 데이터 베이스(158)는 프로그램 명령어들(164)을 실행하기 위한 하나 이상의 프로세서(162)를 포함한다. 프로그램 명령어들(164)의 실행을 통해서는, 사용자(102)의 ID 토큰(106)으로부터 판독된 속성값을 이용하여 사용자

(102)의 식별자 및 전화 번호를 판독하기 위해 데이터 베이스 도표(160)에 대한 접근이 이루어질 수 있다.

[0091] 식별자를 통해서는 사용자(102)가 분명하게 식별될 뿐 아니라, 사용자(102)에 대해 권한이 있는 홈 위치 등록기도 식별된다. 여기서 고려되는 실시예의 경우 이동 무선 네트워크(116)는 I 개수의 홈 위치 등록기(HLR 1, HLR 2, ..., HLR i, ... HLR I)를 포함한다.

[0092] 이동 무선 네트워크(116)의 등록된 사용자 각각에 대해 데이터 베이스 도표(160)에 저장된 식별자들은 예컨대 IMSI로서 형성될 수 있다.

[0093] 이동 무선 장치(100)의 등록을 위해, 여기서 고려되는 실시예의 경우, 사용자(102) 및 ID 프로바이더 컴퓨터 시스템(136)이 예컨대 도 1, 도 2 및 도 3과 관련하여 앞서 설명한 바와 같이 ID 토큰(106)에 대해 인증을 받은 후에, 하나 이상의 속성값이 ID 토큰(106)으로부터 ID 프로바이더 컴퓨터 시스템(136)에 의해 판독되도록 진행된다. 그런 다음 ID 프로바이더 컴퓨터 시스템(136)은 속성값을 포함하는 메시지(105)를 데이터 베이스(158)로 전송한다. 그런 다음 프로그램 명령어들(164)의 실행을 통해, 키로서 속성값을 이용하는 조건에서 데이터 베이스 도표(160)로부터, 사용자(102)에 할당된 식별자와 사용자(102)의 전화 번호를 판독하기 위해, 속성값을 이용하여 데이터 베이스 접근이 실행된다. 그런 다음 데이터 베이스(158)는, 이동 무선 네트워크(116)에 대해 상기 식별자 및 사용자(102)의 전화 번호를 통지하기 위해, 메시지(107)를 전송한다. 메시지(107)는 식별자에 의해 식별된 홈 위치 등록기에 의해 수신되고, 그에 이어서 홈 위치 등록기는 이동 무선 장치(100)를 등록한다.

[0094] 도 5에는 식별자가 이동 무선 장치(100)의 메모리(166)에 저장되어 있는 대체되는 실시예가 도시되어 있다. 상기 식별자는 예컨대 사용자(102)에 의해 수동으로 이동 무선 장치(100)에 입력될 수 있으며, 그럼으로써 그 식별자는 메모리(166)에 저장된다. 대체되는 실시예에 따라 식별자는 OTA(Over-the-Air) 기술에 의해 이동 무선 장치(100)의 메모리(166)에 자동으로 저장될 수 있다.

[0095] 도 4에 따른 실시예에 보충되는 실시예에서, 이동 무선 장치(100)는 등록 실행을 위해 자체 메모리(166)에 저장된 식별자를 이동 무선 네트워크(116)를 통해 데이터 베이스(158)로 전송한다.

[0096] 데이터 베이스 도표(160) 내에는 여기서 고려되는 실시예의 경우 식별자들만이 저장되고 전화 번호는 저장되지 않는다. 그와 반대로 등록된 사용자들의 전화 번호는 개별 홈 위치 등록기들의 지역 데이터 베이스에 저장된다. 도 5에는 홈 위치 등록기 1이 권한을 갖는 그런 등록 사용자들의 전화 번호가 저장되어 있는 홈 위치 등록기 1의 데이터 베이스(168)가 예시로서 도시되어 있다. 이런 전화 번호에 대한 접근은 해당하는 사용자의 식별자로 이루어진다.

[0097] 데이터 베이스(158)의 프로세서(162)는 여기서 고려되는 실시예의 경우 추가로 프로그램 명령어들(170)을 실행하는 역할을 한다. 프로그램 명령어들(170)의 실행을 통해, 이동 무선 장치(100)에 의해 수신된 식별자가 데이터 베이스 도표(160)로부터 판독된 식별자와 동일한지 여부가 검사된다. 동일한 경우에만, 데이터 베이스(158)는 메시지(107)를 전송하고, 동일하지 않은 경우라면 등록이 거부된다.

[0098] 또한, 여기서는 이동 무선 장치(100)의 등록을 위해 다음과 같이 진행된다.

[0099] 이동 무선 장치(100)가 신호(101)를 이동 무선 네트워크(116)로 전송하되, 신호(101)는 본 실시예의 경우 메모리(166)에 저장된 식별자를 운반한다. ID 프로바이더 컴퓨터 시스템(136)은, 앞서 도 1 내지 도 4와 관련하여 설명한 바와 같이 사용자(102) 및 ID 프로바이더 컴퓨터 시스템(136)이 ID 토큰(106)에 대해 인증을 받은 후에, ID 토큰(106)으로부터 하나 이상의 속성값을 판독한다. 그런 다음 ID 프로바이더 컴퓨터 시스템(136)은 속성값을 포함하는 메시지(105)를 데이터 베이스(158)로 전송한다.

[0100] 프로그램 명령어들(164)의 실행을 통해 데이터 베이스(158)는 데이터 베이스 도표(160)로부터 속성값을 이용하여 사용자(102)의 식별자를 판독한다. 또한, 데이터 베이스(158)는 프로그램 명령어들(170)의 실행을 통해 이동 무선 장치(100)에 의해 수신된 식별자가 데이터 베이스 도표(160)로부터 판독된 식별자와 일치하는지 여부를 점검한다. 일치하는 경우에만, 데이터 베이스(158)가 메시지(107)를 전공하고, 그럼으로써 예컨대 홈 위치 등록기 1과 같은 권한 있는 홈 위치 등록기 내 등록이 이루어질 수 있게 된다. 권한 있는 홈 위치 등록기는, 사용자(102)의 전화 번호를 검출하기 위해, 키로서 식별자를 이용하여 자체의 지역 데이터 베이스(168)에 접근한다. 그런 다음 이와 같이 검출된 전화 번호에 대해 이동 무선 네트워크 내 등록이 실행된다.

[0101] 도 6에는 본 발명에 따른 이동 무선 시스템의 추가 실시예가 도시되어 있다. 본 실시예의 경우 사용자(102)의 식별자는, 다시 말해 예컨대 IMSI는 속성값으로서 ID 토큰(106)의 보호되는 메모리 영역(124)에 저장된다.

[0102] 그런 다음 이동 무선 장치(100)의 등록을 위해, 앞서 설명한 도 1 내지 도 5의 실시예와 유사하게 사용자(102)

및 ID 프로바이더 컴퓨터 시스템(136)이 ID 토큰(106)에 대해 인증을 받은 후에, ID 프로바이더 컴퓨터 시스템(136)이 ID 토큰(106)으로부터 식별자를 판독하도록 진행된다. 그런 다음 ID 프로바이더 컴퓨터 시스템(136)은, 예컨대 HLR 1처럼 식별자를 통해 식별되는 이동 무선 네트워크(116)의 홈 위치 등록기가 수신하는 식별자를 포함한 메시지(105)를 전송한다. 권한 있는 홈 위치 등록기는 메시지(105)에 포함된 식별자로 사용자(102)의 전화 번호를 검출하기 위해 자체 지역 데이터 베이스(168)에 대한 데이터 베이스 접근을 실행하며, 그런 다음 상기 전화 번호로 이동 무선 장치(100)의 등록이 이루어진다.

부호의 설명

[0103] 100: 이동 무선 장치

101: 신호

102: 사용자

103: 요청

104: 인터페이스

105: 메시지

106: ID 토큰

107: 메시지

108: 인터페이스

110: 프로세서

112: 프로그램 명령어

114: 이동 무선 네트워크 인터페이스

116: 이동 무선 네트워크

118: 전자 메모리

120: 보호되는 메모리 영역

122: 보호되는 메모리 영역

124: 보호되는 메모리 영역

126: 메모리 영역

128: 프로세서

130: 프로그램 명령어

132: 프로그램 명령어

134: 프로그램 명령어

136: ID 프로바이더 컴퓨터 시스템

138: 이동 무선 네트워크 인터페이스

140: 메모리

142: 개인 키

144: 인증서

145: 프로세서

146: 프로그램 명령어

148: 프로그램 명령어

149: 프로그램 명령어

150: 네트워크 컴포넌트

152: 이동 무선 네트워크 인터페이스

154: 프로세서

156: 프로그램 명령어

158: 데이터 베이스

160: 데이터 베이스 도표

162: 프로세서

164: 프로그램 명령어

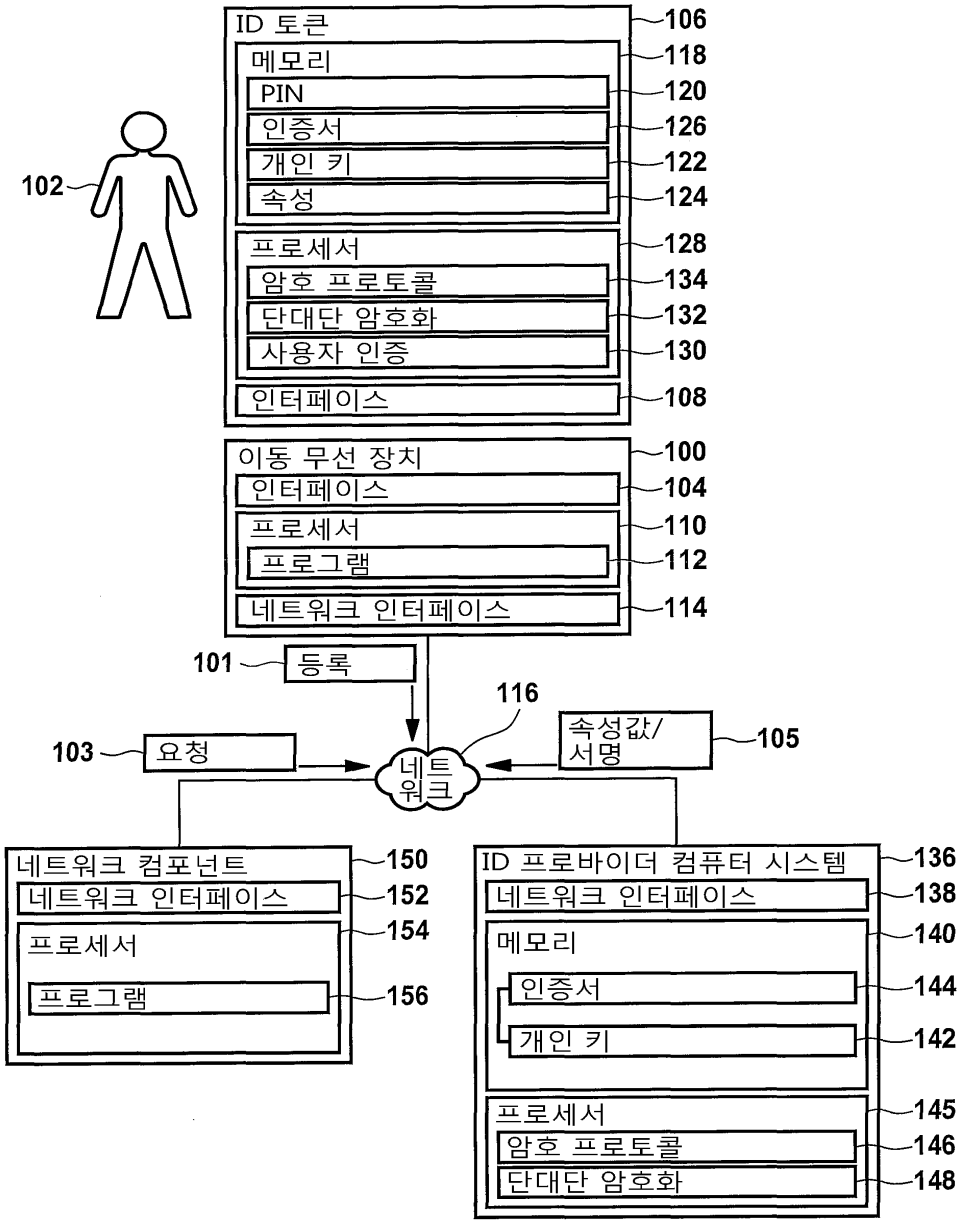
166: 메모리

168: 데이터 베이스

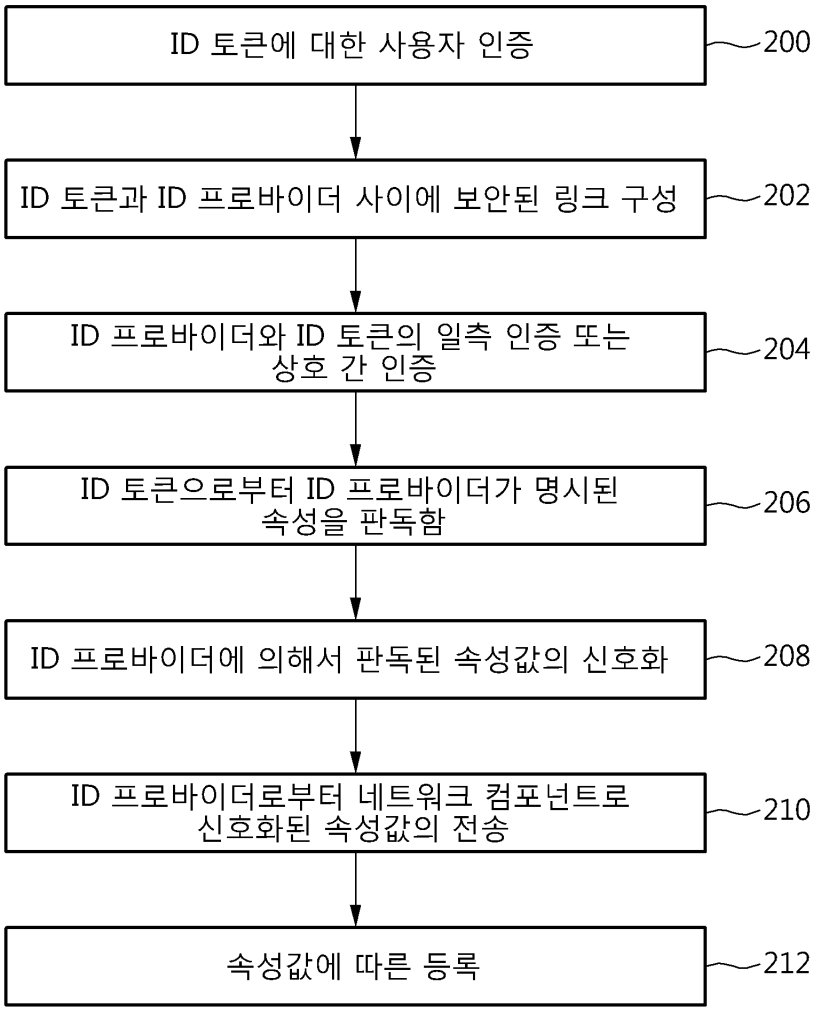
170: 프로그램 명령어

도면

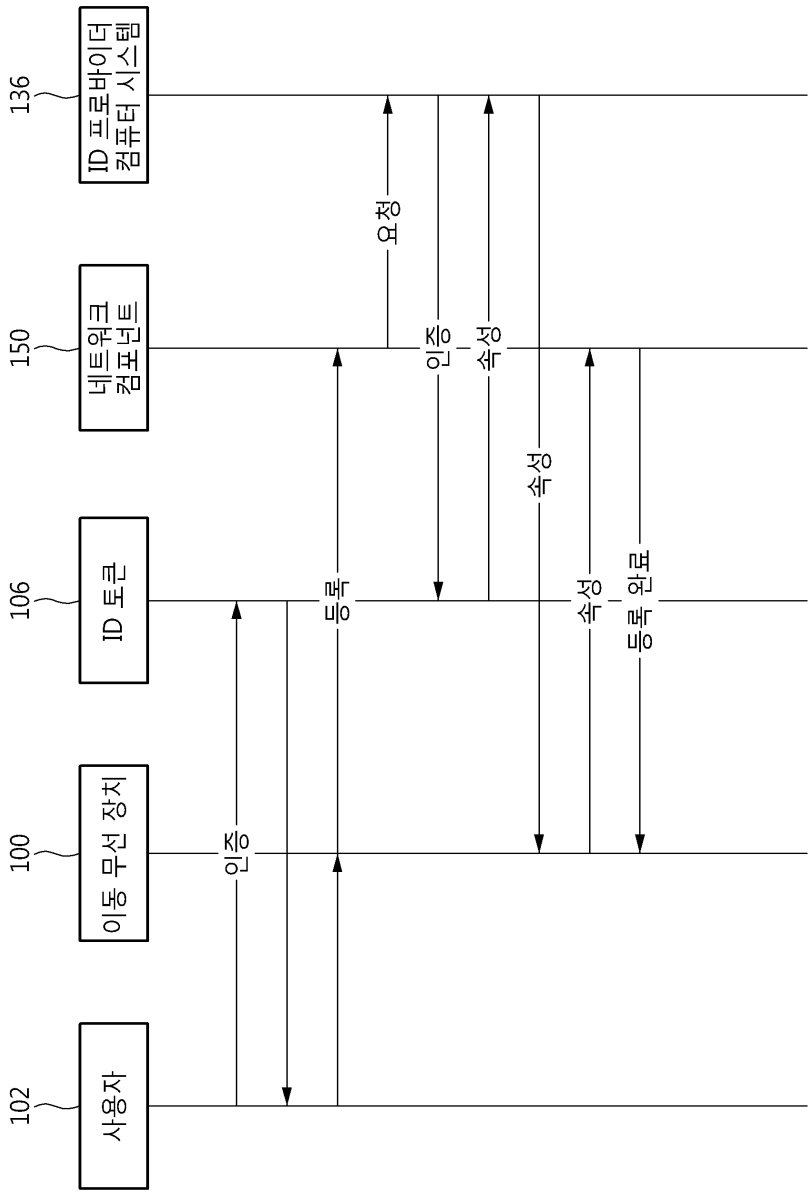
도면1


ID 토큰
106
메모리
118
PIN
120
인증서
126
개인 키
122
속성
124
프로세서
128
암호 프로토콜
134
단대단 암호화
132
사용자 인증
130
인터페이스
108
102
이동 무선 장치
100
인터페이스
104
프로세서
110
프로그램
112
네트워크 인터페이스
114
101
등록
116
103
요청
네트
워크
속성값/
서명
105
네트워크 컴포넌트
150
네트워크 인터페이스
152
프로세서
154
프로그램
156
ID 프로바이더 컴퓨터 시스템
136
네트워크 인터페이스
138
메모리
140
인증서
144
개인 키
142
프로세서
145
암호 프로토콜
146
단대단 암호화
148

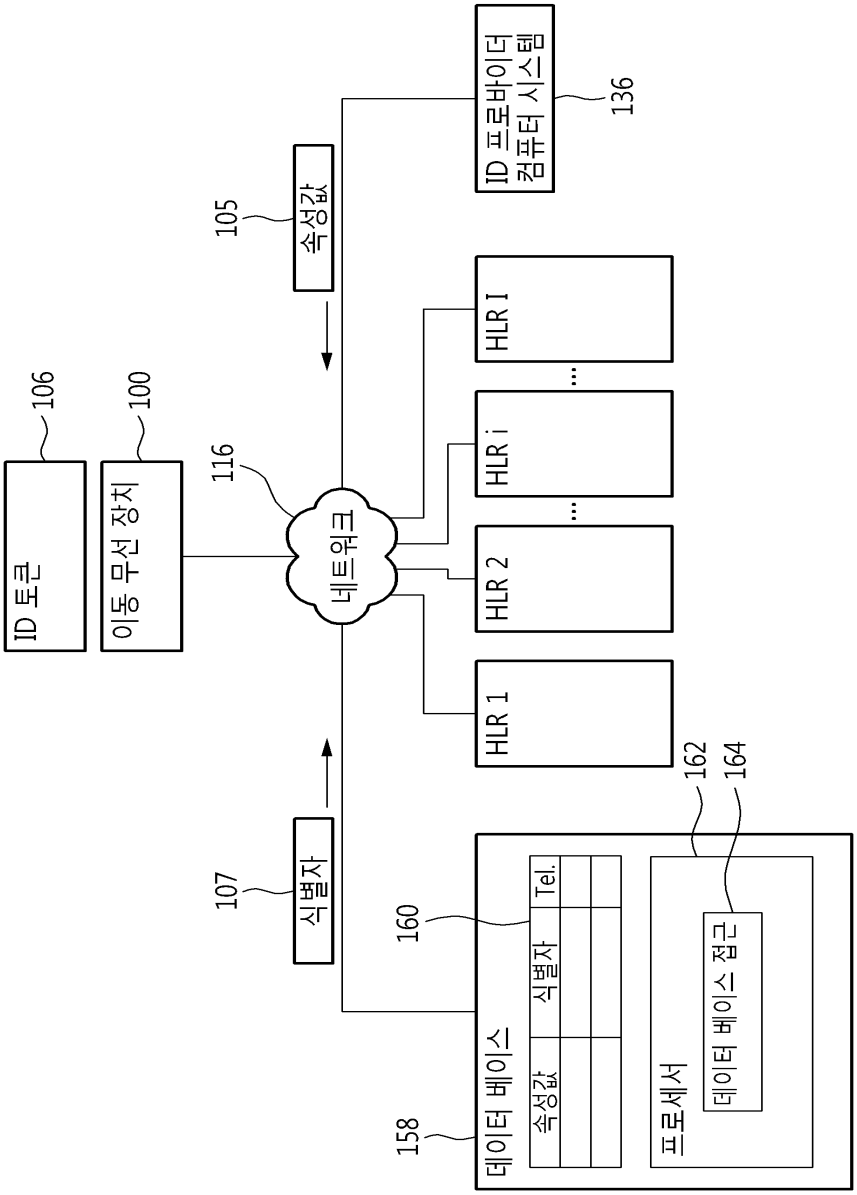
도면2


ID 토큰에 대한 사용자 인증
200
ID 토큰과 ID 프로바이더 사이에 보안된 링크 구성
202
ID 프로바이더와 ID 토큰의 일측 인증 또는 상호 간 인증
204
ID 토큰으로부터 ID 프로바이더가 명시된 속성을 판독함
206
ID 프로바이더에 의해서 판독된 속성값의 신호화
208
ID 프로바이더로부터 네트워크 컴포넌트로 신호화된 속성값의 전송
210
속성값에 따른 등록
212

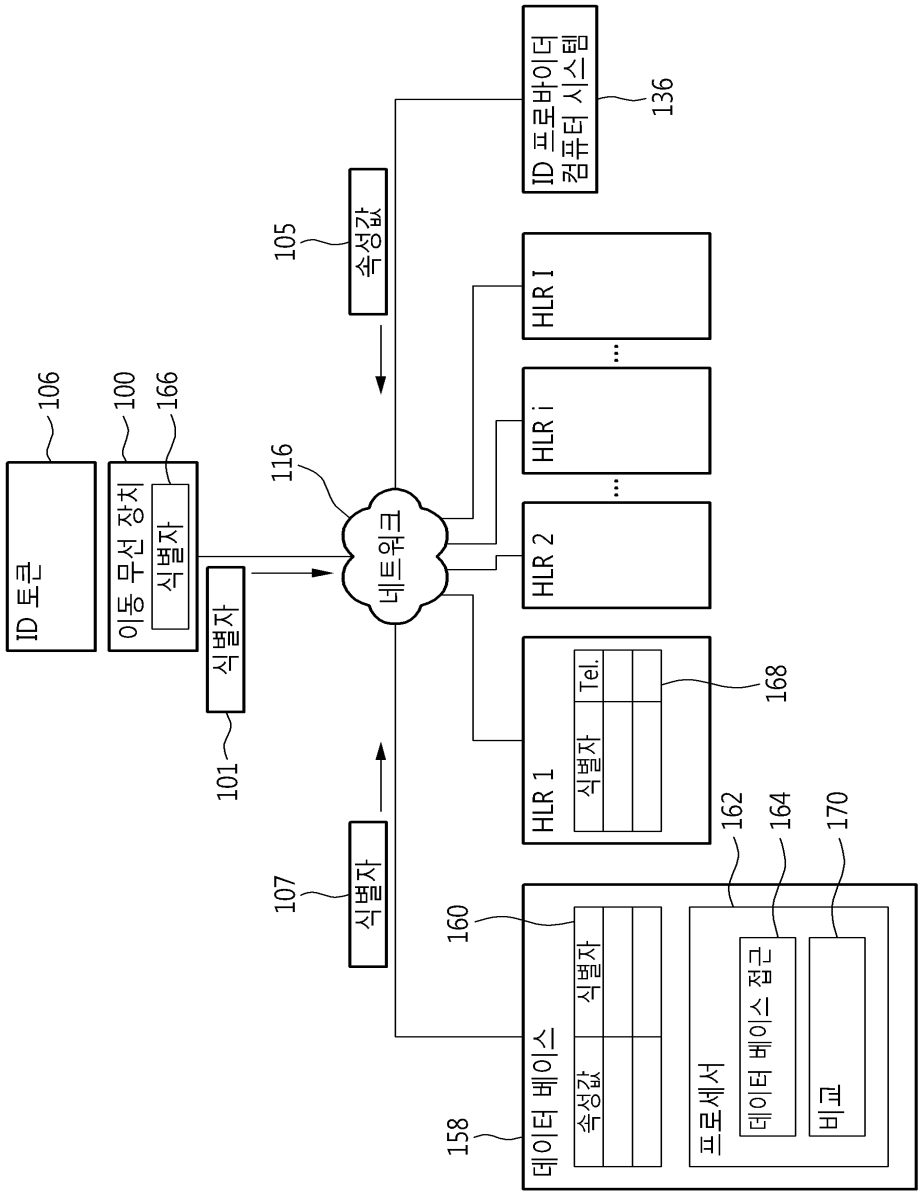
도면3


136
ID 프로바이더 컴퓨터 시스템
150
네트워크 컴포넌트
106
ID 토큰
100
이동 무선 장치
102
사용자
요청
인증
속성
속성
인증
등록
속성
등록 완료

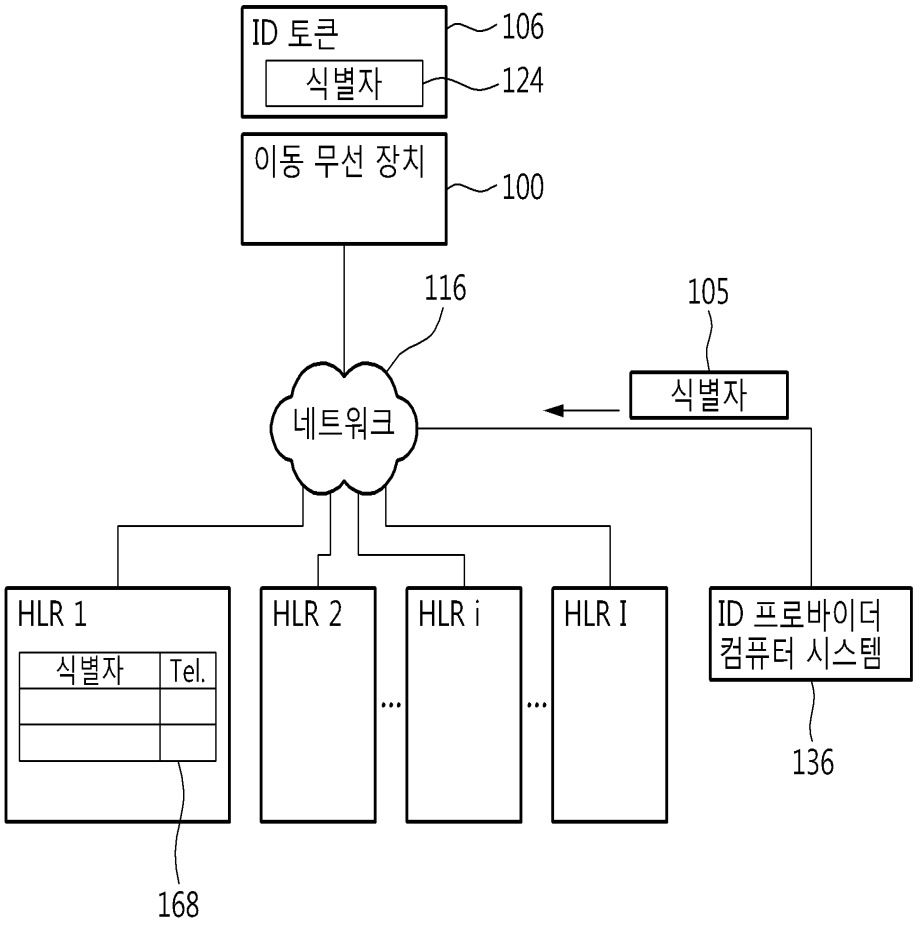
도면4


ID 토큰
106
이동 무선 장치
100
116
네트워크
105
속성값
107
식별자
ID 프로바이더 컴퓨터 시스템
136
HLR 1
HLR 2
HLR i
HLR I
162
164
160
158
데이터 베이스
속성값
식별자
Tel.
프로세서
데이터 베이스 접근

도면5


ID 토큰
106
이동 무선 장치
식별자
100
166
식별자
101
네트워크
116
속성값
105
식별자
107
ID 프로바이더 컴퓨터 시스템
136
HLR I
HLR i
HLR 2
HLR 1
식별자
Tel.
168
162
164
170
160
데이터 베이스
속성값
식별자
158
프로세서
데이터 베이스 접근
비교

도면6


ID 토큰
106
식별자
124
이동 무선 장치
100
116
105
식별자
네트워크
HLR 1
식별자
Tel.
HLR 2
HLR i
HLR I
ID 프로바이더
컴퓨터 시스템
136
168