(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년07월18일
(11) 등록번호 10-2001544
(24) 등록일자 2019년07월12일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)
(21) 출원번호 10-2012-0030957
(22) 출원일자 2012년03월27일
심사청구일자 2017년03월27일
(65) 공개번호 10-2013-0109322
(43) 공개일자 2013년10월08일
(56) 선행기술조사문헌
US20090307764 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
임한나
서울 서초구 서래로5길 102, 202호 (반포동)
이성원
경기 용인시 기흥구 덕영대로 1732, 전자정보대학관 MOBILE CONVERGENCE LAB (서천동, 경희대학교)
이지철
경기 수원시 영통구 효원로 363, 130동 906호 (매탄동, 매탄위브하늘채아파트)
(74) 대리인
이건주

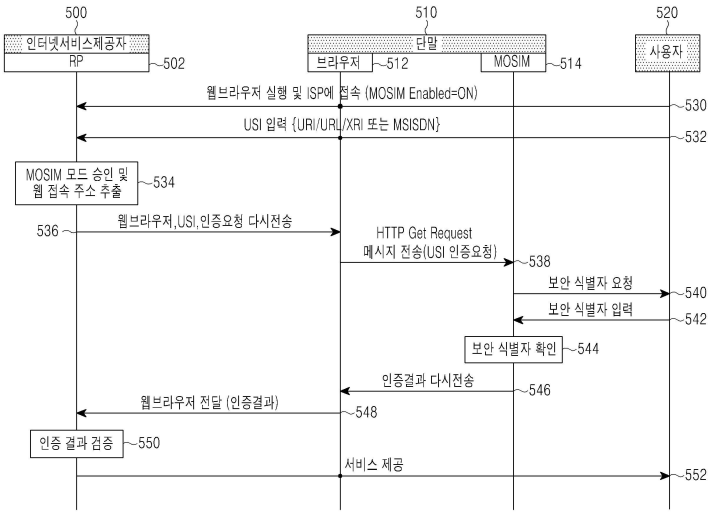
전체 청구항 수 : 총 10 항 심사관 : 양종필

(54) 발명의 명칭 **통신 시스템에서 사용자 인증을 대행하는 장치 및 방법**

(57) 요 약

본 발명은 통신 시스템에서 단말의 사용자 인증을 대행하는 방법에 있어서, 인터넷서비스 제공자로부터 상기 단말을 통해 사용자를 인증할 것을 요청하는 인증 요청을 수신하고, 상기 사용자에게 인증을 위한 보안 식별자 정보를 요청하고, 상기 사용자로부터 상기 보안 식별자 정보를 입력 받고, 상기 단말이 관리하는 보안이 요구되는 정보들을 통해 상기 보안 식별자 정보가 유효한 정보인지 확인하여 상기 사용자를 인증하고, 인증 결과를 상기 인터넷서비스 제공자에게 전송하고, 상기 인터넷서비스 제공자로부터 검증된 인증 결과를 수신하고 상기 검증된 인증 결과에 따른 서비스를 상기 사용자에게 제공한다.

대 표 도



명 세 서

청구범위

청구항 1

통신 시스템에서 단말의 사용자 인증을 대행하는 방법에 있어서,

인터넷서비스 제공자로부터 사용자의 인증을 위해 사용되는 사용자 식별 정보와 인터넷 사이트의 정보를 포함하는 인증 요청을 수신하는 과정과,

상기 단말에서 관리하는 데이터 베이스 정보를 통해, 상기 인터넷 사이트에 접속할 수 있는지 판단하는 과정과,

상기 인터넷 사이트에 접속할 수 있는 것으로 판단한 경우, 상기 사용자의 인증을 위한 보안 식별자 정보를 요청하는 과정과,

상기 보안 식별자 정보를 수신하는 과정과,

상기 사용자 식별 정보 및 상기 단말이 관리하는 보안이 요구되는 정보들을 통해 상기 보안 식별자 정보가 유효한 정보인지 확인하여 상기 사용자를 인증하는 과정과,

상기 인증 결과를 상기 인터넷서비스 제공자에게 전송하는 과정과,

상기 인터넷서비스 제공자로부터 검증된 인증 결과를 수신하는 과정과,

인증 성공 또는 인증 실패와 관련된 서비스를 제공하기 위해 상기 검증된 인증 결과를 표시하는 과정을 포함하는 단말의 사용자 인증 대행 방법.

청구항 2

제1항에 있어서,

상기 인증 요청을 수신하기 이전에, 상기 단말이 자체 정보만으로 사용자 인증을 수행할 수 있음을 지시하는 정보를 상기 인터넷서비스 제공자에게 전달하는 과정을 더 포함하는 단말의 사용자 인증 대행 방법.

청구항 3

제1항에 있어서,

상기 단말은 복수의 로컬 인터넷 프로토콜 주소/포트 번호를 가지며, 상기 인증 요청은 상기 인터넷서비스 제공자가 추출한 웹 접속 주소가 지시하는 로컬 인터넷 프로토콜(IP: Internet Protocol) 주소/포트 번호를 통해 수신되는 단말의 사용자 인증 대행 방법.

청구항 4

제1항에 있어서,

상기 보안이 요구되는 정보들은 검증된 응용 데이터 베이스 정보, 가입자 정보, IMS (internet protocol multimedia sybsystem) 인증 정보, 공인인증서 및 상기 데이터베이스 정보 중 적어도 하나를 포함하는 단말의 사용자 인증 대행 방법.

청구항 5

제1항에 있어서,

상기 데이터 베이스 정보는 접속이 허용되지 않는 인터넷 사이트들의 정보로 구성된 블랙 리스트와 접속이 허용되는 인터넷 사이트들의 정보로 구성된 화이트 리스트를 포함하며, 상기 블랙 리스트 및 상기 화이트 리스트는 이동통신 사업자와 단말 간에 설명된 별도의 통신 링크를 통해 업데이트되는 단말의 사용자 인증 대행 방법.

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

통신 시스템에서 사용자 인증을 대행하는 단말에 있어서,

사용자의 인증을 위한 보안 식별자 정보를 요청하고, 상기 보안 식별자 정보를 수신 사용자 인터페이스부와,

인터넷서비스 제공자로부터 사용자의 인증을 위해 사용되는 사용자 식별 정보와 인터넷 사이트의 정보를 포함하는 인증 요청을 수신하고, 상기 단말에서 관리하는 데이터 베이스 정보를 통해, 상기 인터넷 사이트에 접속할 수 있는지 판단하고, 상기 사용자 식별 정보 및 상기 단말이 관리하는 보안이 요구되는 정보들을 통해 상기 보안 식별자 정보가 유효한 정보인지 확인하여 상기 사용자를 인증하고, 상기 인증 결과를 상기 인터넷서비스 제공자에게 전송하고, 상기 인터넷서비스 제공자로부터 검증된 인증 결과를 수신하고, 인증 성공 또는 인증 실패와 관련된 서비스를 제공하기 위해 상기 검증된 인증 결과를 표시하는 보안 로컬 웹서버부를 포함하는 사용자 인증을 대행하는 단말.

청구항 14

제13항에 있어서,

상기 보안 로컬 웹서버부는 상기 인증 요청을 수신하기 이전에, 상기 단말이 자체 정보만으로 사용자 인증을 수행할 수 있음을 지시하는 정보를 상기 인터넷서비스 제공자에게 전달하는 사용자 인증을 대행하는 단말.

청구항 15

제13항에 있어서,

상기 보안 로컬 웹서버부는 복수의 로컬 인터넷 프로토콜 주소/포트 번호를 가지며, 상기 인증 요청은 상기 인터넷서비스 제공자가 추출한 웹 접속 주소가 지시하는 로컬 인터넷 프로토콜(IP: Internet Protocol) 주소/포트 번호를 통해 수신되는 사용자 인증을 대행하는 단말.

청구항 16

제13항에 있어서,

상기 보안이 요구되는 정보들은 검증된 응용 데이터 베이스 정보, 가입자 정보, IMS (internet protocol multimedia sybsystem) 인증 정보, 공인인증서 및 상기 데이터베이스 정보 중 적어도 하나를 포함하는 사용자 인증을 대행하는 단말.

청구항 17

제13항에 있어서,

상기 데이터 베이스 정보는 접속이 허용되지 않는 인터넷 사이트들의 정보로 구성된 블랙 리스트와 접속이 허용되는 인터넷 사이트들의 정보로 구성된 화이트 리스트를 포함하며, 상기 블랙 리스트 및 상기 화이트 리스트는 이동통신 사업자와 단말 간에 설명된 별도의 통신 링크를 통해 업데이트되는 사용자 인증을 대행하는 단말.

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 통신 시스템에 대한 것으로서, 특히 사용자 인증을 대행하는 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 최근 개인정보 보호에 대한 관심이 높아지면서 하나의 아이디(ID: identifier)로 여러 인터넷 사이트에 로그인(log-in)함으로써 개인정보 유출을 최소화할 수 있는 오픈아이디(OpenID: open identifier) 서비스에 대한 관심이 크게 증가하고 있다. 상기 오픈아이디 서비스는 사용자가 인터넷 사업자의 인터넷 사이트에 접속할 시, 제3

의 인터넷 사업자가 사용자 인증을 대행하는 서비스를 의미한다. 따라서 상기 오픈아이디 서비스를 지원하는 사이트에 접속하는 사용자들은 모든 사이트에 방문할 때마다 새로운 계정을 만들고 관리할 필요 없이 사용자가 신뢰하는 하나의 사이트에서만 인증이 완료되면 해당 사이트에 접속할 수 있게 된다.

[0003] 도 1a 및 1b는 일반적인 통신 시스템에서 오픈아이디 서비스를 이용하여 사용자를 인증하는 절차를 도시한 도면이다.

[0004] 도 1a 및 1b를 참조하면, 이동통신 사업자(100)는 가입자 정보를 관리하는 홈 가입자 서버부(HSS: Home Subscriber Server)/홈 위치 레지스터부(HLR: Home Location Register)(102)와, 실질적으로 사용자(user)(130)를 인증하는 부트스트랩핑 서버 기능부(BSF: Bootstrapping Server Function)(104)와, 오픈아이디 제공부(OP: OpenID Provider)/네트워크 응용 기능부(NAF: Network Application Function)(106)를 관리한다.

[0005] 인터넷 서비스 제공자(ISP: Internet Service Provider)(110)는 사용자의 인증을 제3의 기관과 연동하여 수행하는 중계부(RP: Relaying Party)(112)를 관리한다.

[0006] 단말(120)은 웹브라우저(web browser)를 제공하는 브라우징 에이전트부(BA: Browsing Agent)와 인증 서비스를 제공하는 인증 에이전트부(AA: Authentication Agent)를 관리하며, 이하에서는 편의상 상기 BA와 AA를 합쳐서 하나의 구성부, 즉 BA/AA(122)로 설명한다.

[0007] 사용자(130)는 BA/AA(122)를 통해 접속하고자 하는 인터넷 사이트의 웹 브라우저를 실행하여 ISP(110)에 접속한다.(140단계) 또한 사용자(130)는 상기 접속하고자 하는 인터넷 사이트로부터 접속 정보가 요구되면 오픈아이디 서비스를 이용하여 사용자를 인증하는 모드를 선택하고, 상기 오픈아이디 서비스를 통해 사용자 인증을 대행하는 제3기관에서 사용될 식별 정보(USI: User-supplied-identifier)를 입력한다.(142단계) 이때 상기 식별 정보는 URI(Uniform Resource Identifier), URL(Uniform Resource Locator), XRI(Extensible Resource Identifier) 또는 MSISDN(Mobile Station International Subscriber Directory Number) 등이 될 수 있다. 또한 도 1에서는 상기 제3기관을 도시된 이동통신사업자(100)라 가정한다.

[0008] ISP(110)의 RP(112)는 상기 사용자(130)가 입력한 식별 정보로부터 사용자 인증을 대행하는 제3기관의 OP 주소를 추출하고,(144단계) 상기 제3기관, 즉 이동통신사업자(100)와 보안이 제공되는 통신 링크를 설정한다.(146단계) 이때 선택 사항이긴 하나 상기 통신 링크 설정을 위해 디피 헬먼(DH: Diffie Hellman) 키 교환 방식이 사용될 수 있다.

[0009] 또한 ISP(110)의 RP(112)는 사용자(130)가 접속하고자 하는 인터넷 사이트의 웹브라우저, 사용자(130)가 입력한 식별 정보(USI) 및 오픈 아이디를 통한 인증 요청을 단말(120)에게 다시 전송하고,(148단계) 단말(120)은 사용자(130)가 입력한 식별 정보(USI) 및 오픈 아이디를 통한 인증 요청을 포함하는 HTTP(Hyper Text Transfer Protocol) Get Request 메시지를 이동통신사업자(100)의 OP(106)에게 전송한다.(150단계) 그런 다음 상기 OP(106)는 사용자(130)에 대한 인증을 시작한다.(152단계) 이때 상기 OP(106)는 이동통신사업자(100)의 NAF 기능을 겸한다고 가정한다.

[0010] 이동통신사업자(100)의 NAF(106)는 사용자(130)의 단말(120)에게 인증 시작을 알리는 HTTPS Response 401 Unauthorized 메시지를 전송하고,(154단계) 단말(120)은 상기 메시지에 대한 응답으로 HTTP Get Request 메시지를 이동통신사업자(100)의 BSF(104)에게 전송한다.(156단계) 이때 상기 HTTP Get Request 메시지에는 사용자(130)가 입력한 식별 정보(USI)가 포함된다.

[0011] 이동통신사업자(100)의 BSF(104)는 HSS/HLR(102)로부터 사용자(130) 인증을 위해 필요한 추가적인 정보를 획득하고,(158단계) BSF(104)는 인증 및 키 합의(AKA: Authentication and Key Agreement)를 요청하는 401 Unauthorized 메시지를 단말(120)에게 전송한다.(160단계)

[0012] 단말(120)은 상기 요청에 따라 AKA 알고리즘을 수행하고,(162단계) 상기 AKA 알고리즘 수행 결과를 Request Authorization Digest 메시지를 통해 이동통신사업자(100)의 BSF(104)로 전송한다. (164단계)

[0013] 이동통신사업자(100)의 BSF(104)는 상기 단말(120)로부터 수신한 AKA 알고리즘 수행 결과를 기반으로 하여 단말의 적합성을 판단하고,(166단계) 판단 결과에 따른 인증키 정보를 200 OK 메시지를 통해 단말(120)로 전달한다.(168단계) 이때 상기 200 OK 메시지에는 상기 인증키가 이후 절차에서 유효하게 사용되는 시간(lifetime) 정보가 포함된다. 단말(120)은 상기 인증키 정보를 HTTP Get Request 메시지를 통해 상기 이동통신사업자(100)의 OP/NAF(106)에 전달한다.(170단계)

[0014] 이동통신사업자(100)의 OP/NAF(106)는 BSF(104)에 접속하여 단말(120)로부터 수신한 인증키에 대한 정보를 요청

하고,(172단계) BSF(104)는 상기 인증키 정보를 OP/NAF(106)에 제공한다.(174단계)

[0015] 이동통신사업자(100)의 OP/NAF(106)는 단말(120)을 통해 확인한 인증키와 BSF(104)를 통해 확인한 인증키의 정보가 동일한지 확인하고, 동일할 경우 단말(120)의 사용자(130)가 접속하고자 하는 인터넷 사이트의 웹브라우저를 인증결과와 함께 단말(120)에게 다시 전송하고,(176단계) 단말(120)은 상기 인증 결과를 RP(112)로 전달한다.(178단계)

[0016] ISP(110)의 RP(112)는 상기 인증결과를 검증하고,(180단계) 검증된 인증결과를 사용자(130)에게 디스플레이하여 인증 성공 또는 인증 실패에 따른 서비스를 제공한다.(182단계)

[0017] 이와 같이 도 1에서는 일반적인 통신시스템에서 오픈아이디 서비스를 이용하여 사용자를 인증하는 절차에 대해 살펴보았다. 그러나 상기와 같은 절차를 수행하기 위해서는 ISP(110)의 인터넷 사이트와 단말(120)간에 수치적으로 총 13번의 메시지 송수신, 즉 140, 142, 148, 150, 154, 156, 160, 164, 168, 170, 176, 178, 182단계가 필요하며, 상기와 같은 메시지 송수신으로 인한 무선 트래픽 사용이 증가하고 이에 따라 사용자 입장에서 로그인을 위한 시간이 길어지는 문제점이 있다. 따라서 상기와 같은 메시지 송수신 절차를 최소화하여 사용자 입장에서 로그인 시간을 줄이는 방안이 요구된다. 이와 함께 오픈아이디 인증에 사용되는 무선 트래픽에 대한 경제적 보상을 이동통신사업자가 확보할 수 있는 방안이 요구된다.

[0018] 또한 오픈아이디는 컴퓨터 중심의 웹브라우저 환경에 주로 적용되므로 스마트폰 또는 테블릿 컴퓨터와 같은 단말에서 응용프로그램(application) 중심의 환경에서도 사용될 수 있도록 오픈아이디 서비스에 대한 개선이 필요하다.

발명의 내용

해결하려는 과제

[0019] 본 발명은 간소화된 절차를 통해 사용자를 인증을 대행하는 장치 및 방법을 제안한다.

과제의 해결 수단

[0020] 본 발명에서 제안하는 방법은; 통신 시스템에서 단말의 사용자 인증을 대행하는 방법에 있어서, 인터넷서비스 제공자로부터 상기 단말을 통해 사용자를 인증할 것을 요청하는 인증 요청을 수신하는 과정과, 상기 사용자에게 인증을 위한 보안 식별자 정보를 요청하는 과정과, 상기 사용자로부터 상기 보안 식별자 정보를 입력 받는 과정과, 상기 단말이 관리하는 보안이 요구되는 정보들을 통해 상기 보안 식별자 정보가 유효한 정보인지 확인하여 상기 사용자를 인증하고, 인증 결과를 상기 인터넷서비스 제공자에게 전송하는 과정과, 상기 인터넷서비스 제공자로부터 검증된 인증 결과를 수신하고 상기 검증된 인증 결과에 따른 서비스를 상기 사용자에게 제공하는 과정을 포함한다.

[0021] 본 발명에서 제안하는 다른 방법은; 통신 시스템에서 단말의 사용자 인증을 대행하는 방법에 있어서, 인터넷서비스 제공자의 인터넷 사이트와의 인증 정보가 존재하는지 여부를 확인하는 과정과, 상기 인증 정보가 존재하지 않을 경우, 이동통신 사업자의 요청에 따라 미리 정해진 인증 알고리즘을 수행하고 그 수행 결과를 상기 이동통신 사업자에게 전송하는 과정과, 상기 이동통신 사업자로부터 상기 인증 알고리즘 수행 결과에 따라 생성된 상기 단말과 상기 인터넷 사이트를 인증하는 항구적 인증키를 수신하여 저장하는 과정과, 상기 이동통신 사업자로부터 상기 항구적 인증키를 통한 사용자 인증 결과를 수신하는 과정과, 상기 인터넷서비스 제공자로부터 검증된 인증 결과를 수신하고 상기 검증된 인증 결과에 따른 서비스를 상기 사용자에게 제공하는 과정을 포함한다.

[0022] 본 발명에서 제안하는 장치는; 통신 시스템에서 사용자 인증을 대행하는 단말에 있어서, 사용자에게 인증을 위한 보안 식별자 정보를 요청하고 상기 사용자로부터 상기 보안 식별자 정보를 입력 받는 보안 사용자 인터페이스부와, 인터넷서비스 제공자로부터 상기 단말을 통해 사용자를 인증할 것을 요청하는 인증 요청을 수신하고, 상기 단말이 관리하는 보안이 요구되는 정보들을 통해 상기 보안 식별자 정보가 유효한 정보인지 확인하여 상기 사용자를 인증하고, 인증 결과를 상기 인터넷서비스 제공자에게 전송하고, 상기 인터넷서비스 제공자로부터 검증된 인증 결과를 수신하고 상기 검증된 인증 결과에 따른 서비스를 상기 사용자에게 제공하는 보안 로컬 웹서버부를 포함한다.

[0023] 본 발명에서 제안하는 다른 장치는; 통신 시스템에서 사용자 인증을 대행하는 단말에 있어서, 인터넷서비스 제공자의 인터넷 사이트와의 인증 정보가 존재하는지 여부를 확인하고, 상기 인증 정보가 존재하지 않을 경우, 이동통신 사업자의 요청에 따라 미리 정해진 인증 알고리즘을 수행하고 그 수행 결과를 상기 이동통신 사업자에게

전송하고, 상기 이동통신 사업자로부터 상기 인증 알고리즘 수행 결과에 따라 생성된 상기 단말과 상기 인터넷 사이트를 인증하는 항구적 인증키를 수신하여 저장하고, 상기 이동통신 사업자로부터 상기 항구적 인증키를 통한 사용자 인증 결과를 수신하고, 상기 인터넷서비스 제공자로부터 검증된 인증 결과를 수신하고 상기 검증된 인증 결과에 따른 서비스를 상기 사용자에게 제공하는 보안 로컬 웹서버부를 포함한다.

발명의 효과

[0024] 본 발명은 기존의 사용자 인증 방안대비 무선통신 링크에서의 트래픽 부하와 인증 절차에 소요되는 시간을 감소시키는 효과가 있다.

[0025] 첫째로 기존의 오픈아이디 서비스가 이동통신망에서 적용되어 이동통신사업자가 인터넷서비스의 인증대행기관으로서 역할을 수행하는 경우, 해당 인증에 요구되는 기존 방안의 무선 링크 메시지 송수신은 13번에 이르지만, 본 발명에서 제안하는 방안들은 최소 5번 정도의 메시지 송수신으로 인증을 수행함으로써, 사용자나 인터넷서비스사업자로부터 인증 트래픽에 대한 별도의 과금 없이 동작할 수 있도록 한다.

[0026] 둘째로 유선대비 상대적으로 저속인 무선링크에서, 줄어든 메시지 송수신을 지원함으로써, 인증 메시지 송수신에 따른 (인증 시) 지연 시간을 줄이도록 한다. 따라서, 제3의 인증기관을 통한 인증이 무선에서 활발하게 사용되더라도 사용자가 불편함을 최소화하는 방안을 지원한다.

[0027] 셋째로 이동통신사업자가 자체의 서비스가 아닌 타 인터넷서비스에 대한 인증을 수행함으로써 발생할 수 있는 인증 관련 장비의 부하를 줄이도록 한다. 기존의 방안 대비 본 발명에서 제안한 방안들은 이동통신망의 장비가 인증에 개입하는 시간(횟수)을 작게 함으로써, 오픈아이디 서비스와 같은 인증을 이동통신 사업자가 대행하는 경우에도 기존 망에 부하가 적도록 한다.

[0028] 넷째로 인터넷서비스제공자가 요구하는 신뢰성을 차별화된 수준으로 구분하여, 저 수준에서 고 수준까지 차별화된 인증 레벨을 제공할 수 있도록 한다. 즉, 본 발명에서 제안하는 방안은 완전히 신뢰 가능한 MOSIM을 가정하는 경우, MOSIM과 인터넷서비스사업자가 사전에 인증한 인증키 값을 활용하여 인증 강도를 강화한 방안, 이동통신망의 개입을 통해서 단말의 MOSIM 기반 인증에 추가적인 이동통신망 인증을 복수로 지원하는 방안, 그리고 마지막으로 인터넷사이트에 대한 접속의 허용/거절 데이터베이스를 단말이 관리하며 인증 시 활용하는 다양한 방안을 제공하여, 다양한 인증의 요구수준을 만족하도록 한다.

도면의 간단한 설명

[0029] 도 1a 및 1b는 일반적인 통신 시스템에서 오픈아이디 서비스를 이용하여 사용자를 인증하는 절차를 도시한 도면,

도 2는 본 발명의 일 실시예에 따른 통신시스템에서 단말에 포함되는 이동 보안 정보 매니저의 구조를 도시한 도면,

도 3은 본 발명의 일 실시예에 따른 통신시스템에서 단말에 포함되는 MOSIM의 특정 응용 프로그램의 합법성 여부를 인증하는 동작을 도시한 도면,

도 4는 본 발명의 일 실시예에 따른 통신시스템에서 단말에 포함되는 MOSIM의 해당 응용 프로그램이 지속적으로 보안이 보장되는 정보에 접근하는 것을 허락하는 동작을 도시한 도면,

도 5는 본 발명의 일 실시예에 따른 통신시스템에서 MOSIM을 구비하는 단말이 자체적으로 사용자를 인증하는 절차를 도시한 도면,

도 6a 및 6b는 본 발명의 일 실시예에 따른 통신시스템에서 MOSIM을 제공하는 단말이 사용자 인증을 위해 항구적 인증키를 생성하는 절차를 도시한 도면,

도 7은 본 발명의 일 실시예에 따른 통신시스템에서 MOSIM을 제공하는 단말이 기 생성한 항구적 인증키를 이용하여 사용자를 인증하는 절차를 도시한 도면,

도 8a 및 8b는 본 발명의 일 실시예에 따른 통신시스템에서 MOSIM을 제공하는 단말이 AKA 인증 알고리즘 접근 방식에 따른 이중 체크를 통해 사용자를 인증하는 절차를 도시한 도면,

도 9a 및 9b는 본 발명의 일 실시예에 따른 통신시스템에서 MOSIM을 제공하는 단말이 무선 구간의 부하를 줄이는 접근 방식에 따른 이중 체크 방식을 통해 사용자를 인증하는 절차를 도시한 도면,

도 10은 본 발명의 일 실시예에 따른 통신시스템에서 MOSIM을 제공하는 단말이 검증된 응용 데이터베이스 정보를 기반으로 사용자 접속을 허용하는 절차를 도시한 도면,

도 11은 본 발명의 일 실시예에 따른 통신시스템에서 MOSIM을 제공하는 단말이 검증된 응용 데이터베이스 정보를 기반으로 사용자 접속을 거절하는 절차를 도시한 도면.

발명을 실시하기 위한 구체적인 내용

[0030] 이하, 본 발명의 바람직한 실시예를 첨부된 도면을 참조하여 상세히 설명한다. 하기의 설명에서는 본 발명의 동작을 이해하는데 필요한 부분만을 설명하며 그 이외의 배경 기술은 본 발명의 요지를 흩트리지 않도록 생략한다.

[0031] 도 2는 본 발명의 일 실시예에 따른 통신시스템에서 단말에 포함되는 이동 보안 정보 매니저의 구조를 도시한 도면이다.

[0032] 도 2를 참조하면, 도시된 이동 보안 정보 매니저(MOSIM: MObile Secure Information Manager)(200)는 보안 사용자 인터페이스부(Secure User Interface)(210)와, 보안 로컬 웹서버부(Secure Local Web-server)(220)를 포함하며, 상기 보안 로컬 웹서버부는 검증된 응용 데이터 베이스(Authorized Application Database) 정보(230)와, UICC(Universal Integrated Circuit Card) 및 USIM(universal Subscriber Identity Module)과 같이 단말에 탑재되어 관리되는 가입자 정보(240)와, 인터넷 프로토콜 멀티미디어 서브시스템(IMS: Internet Protocol Multimedia Subsystem) 인증 정보(250)와, 공인인증서(Secured Signature) 및 데이터베이스 정보(260)를 관리한다.

[0033] 보안 로컬 웹서버부(220)는 하나의 대표(representative) 인터넷 프로토콜(IP: Internet Protocol)/포트와 적어도 두 개의 전용 IP/포트를 가진다.

[0034] 대표 IP/포트는 고정의 특정 IP 주소와 포트 번호를 가지는 것으로, 특히 어떤 응용 프로그램이든지 단말의 보안이 보장되는 정보에 접근할 수 있도록 공개된 주소 값을 가진다. 즉 해당 IP 주소와 포트 번호를 통해서 보안이 보장되는 HTTPS 프로토콜 메시지가 송수신된다.

[0035] 응용 프로그램에서 보안이 보장되는 정보에 접근하고자 하면, 해당 요청은 보안이 보장되는 보안 사용자 인터페이스부(210)를 통해 사용자에게 확인을 거치는 작업을 수행할 수 있다. 이는 부가적인 기능으로서 반드시 필요한 것은 아니며, 보안이 보장되는 정보에 대한 접근에 대해서 사용자에게 보다 신뢰성 있는 접근제어를 수행하는 경우에 사용된다.

[0036] 또한 검증된 응용 데이터 베이스 정보(230)에는 일례로 접근이 허용되는 응용 프로그램 정보 및 접근이 거절되는 응용 프로그램 정보 등이 포함된다.

[0037] 전용 IP/포트는 지속적으로 보안이 보장되는 정보에 접근하고자 하는 응용 프로그램을 위해 할당되며, 해당 특정 IP 주소와 포트 번호를 특정 응용 프로그램에 할당함으로써 특정 응용 프로그램의 보안 정보 활용에 대해 보다 세심한 관리가 가능하다.

[0038] 도 3은 본 발명의 일 실시예에 따른 통신시스템에서 단말에 포함되는 MOSIM의 특정 응용 프로그램의 합법성 여부를 인증하는 동작을 도시한 도면이다.

[0039] 도 3을 참조하면, 합법성을 인증 받고자 하는 응용 프로그램(300)은 대표 IP/포트를 통해 보안 로컬 웹서버부(320)에 접속하여 보안이 보장되는 보안 인증을 요청하고,(302단계) 보안 로컬 웹서버부(320)는MOSIM 내에 보안이 보장되는 보안 사용자 인터페이스부(310)를 활성화시킨다.(304단계) 그런 다음 보안 사용자 인터페이스부(310)는 사용자(370)에게 인증을 위한 보안 식별자, 일례로 아이디 및 패스워드를 요청하여(306단계) 해당 응용 프로그램의 접근이 합법적인 지를 확인하는 절차를 수행한다. 즉 사용자(370)가 현재 상기 응용 프로그램(300)을 사용하고자 하는지 여부 및 상기 응용 프로그램(300)이 합법적인 프로그램인지 여부를 확인하고, 아울러 상기 응용 프로그램(300)이 보안이 제공되는 주요한 단말의 정보를 합법적으로 사용하는 것을 허락하는지 여부를 확인한다.

[0040] 보안 사용자 인터페이스부(310)는 사용자(370)로부터 인증을 위한 보안 식별자가 입력되면,(308단계) 상기 식별자 정보를 보안 로컬 웹서버부(320)로 전달한다. (312단계) 이때 보안 사용자 인터페이스부(310)는 타 응용 프로그램의 키보드 해킹 등을 방지하기 위해 그림화된 서명을 사용자(370)에게 디스플레이하여 사용자 인증을 위한 해당 정보를 입력 받을 수도 있다.

[0041] 보안 로컬 웹서버부(320)는 자신이 관리하는 보안이 요구되는 정보, 즉 검증된 응용 데이터 베이스 정보(330), 가입자 정보(340), IMS 인증 정보(350), 공인인증서 및 데이터베이스 정보(360)를 통해 사용자(370)가 입력한 식별자가 올바른지를 확인한다.(322단계) 여기서 상기 보안 로컬 웹서버부(320)가 관리하는 보안이 요구되는 정보에는 사용자(370)가 입력한 식별자 정보가 올바른지를 확인할 수 있는 정보가 포함되는 것으로 가정한다.

[0042] 그런 다음 보안 로컬 웹서버부(320)는 대표 IP/포트를 통해 응용 프로그램(300)에게 상기 확인한 인증 결과를 포함하는 보안 인증 응답을 전송한다.(324단계) 즉 보안 로컬 웹서버부(320)는 사용자(370)가 올바른 식별자를 입력하여 특정 응용 프로그램의 보안이 보장되는 정보로의 접근을 허락하면, 해당 응용 프로그램에 대한 인증이 성공적으로 이루어진 것으로 판단하여 성공적인 응답을 응용 프로그램(300)에 전달한다. 그러나 만약 사용자가 잘못된 식별자를 입력하거나 불법적인 요청에 의한 것으로 사용자가 알지 못하는 응용 프로그램이 인증을 요청한다면 해당 인증 요청은 거부된다.

[0043] 도 4는 본 발명의 일 실시예에 따른 통신시스템에서 단말에 포함되는 MOSIM의 해당 응용 프로그램이 지속적으로 보안이 보장되는 정보에 접근하는 것을 허락하는 동작을 도시한 도면이다.

[0044] 도 4를 참조하면, 자신의 합법성을 인증 받고자 하는 응용 프로그램(400)은 대표 IP/포트를 통해 보안 로컬 웹서버부(420)에 접속하여 보안이 보장되는 보안 접속 정보를 요청하고,(402단계) 보안 로컬 웹서버부(420)는 MOSIM 내에 보안이 보장되는 보안 사용자 인터페이스부(410)를 활성화시킨다.(404단계) 그런 다음 보안 사용자 인터페이스부(410)는 사용자(470)에게 인증을 위한 식별자, 일례로 아이디 및 패스워드를 요청하여(406단계) 해당 응용 프로그램의 접근이 합법적인 지를 확인하는 절차를 수행한다. 즉 사용자(470)가 현재 상기 응용 프로그램(400)을 사용하고자 하는지 여부 및 상기 응용 프로그램(400)이 합법적인 프로그램인지 여부를 확인하고, 아울러 상기 응용 프로그램(400)이 보안이 제공되는 주요한 단말의 정보를 합법적으로 사용하는 것을 허락하는지 여부를 확인한다.

[0045] 보안 사용자 인터페이스부(410)는 사용자(470)로부터 인증을 위한 식별자가 입력되면,(408단계) 상기 식별자 정보를 보안 로컬 웹서버부(420)로 전달한다. (412단계) 이때 보안 사용자 인터페이스부(410)는 타 응용 프로그램의 키보드 해킹 등을 방지하기 위해 그림화된 서명을 사용자(470)에게 디스플레이하여 사용자 인증을 위한 해당 정보를 입력 받을 수도 있다.

[0046] 보안 로컬 웹서버부(420)는 자신이 관리하는 보안이 요구되는 정보, 즉 검증된 응용 데이터 베이스 정보(430), 가입자 정보(440), IMS 인증 정보(450), 공인인증서 및 데이터베이스 정보(460)를 통해 사용자(470)가 입력한 식별자가 올바른지를 확인한다.(422단계) 여기서 상기 보안 로컬 웹서버부(420)가 관리하는 보안이 요구되는 정보에는 사용자(470)가 입력한 식별자 정보가 올바른지를 확인할 수 있는 정보가 포함되는 것으로 가정한다.

[0047] 그런 다음 보안 로컬 웹서버부(420)는 대표 IP/포트를 통해 응용 프로그램(400)에 상기 확인한 인증 결과를 포함하는 보안 접속 정보 응답을 전송한다.(424단계) 즉 보안 로컬 웹서버부(420)는 사용자(470)가 올바른 식별자를 입력하여 특정 응용 프로그램의 보안이 보장되는 정보로의 접근을 허락하면, 해당 응용 프로그램에 대한 인증이 성공적으로 이루어진 것으로 판단하여 성공적인 응답을 응용 프로그램(400)에 전달한다. 도 4에서는 해당 응용 프로그램이 지속적으로 보안이 보장되는 정보에 접근하는 것을 허락하는 동작을 가정하므로, 해당 프로그램에 대한 인증이 성공적으로 이뤄진 경우만을 가정하여 설명한다.

[0048] 또한 보안 로컬 웹서버부(420)는 응용 프로그램(400)의 보안이 보장되는 정보로의 접근을 허락한 이후, 응용 프로그램(400)이 전용으로 사용하게 되는 적어도 두 개의 전용 IP/포트를 상기 응용 프로그램(400)에게 할당한다. 응용 프로그램(400)은 상기 할당된 적어도 두 개의 전용 IP/포트를 통해 보안 로컬 웹서버부(420)로 보안 정보를 요청하고,(432단계) 보안 로컬 웹서버부(420)는 검증된 응용 데이터 베이스 정보(430), 가입자 정보(440), IMS 인증 정보(450), 공인인증서 및 데이터베이스 정보(460)를 통해 해당 정보를 검색하여(434단계) 보안 정보 응답을 통해 응용 프로그램(400)에게 전송한다.(436단계)

[0049] 도 5는 본 발명의 일 실시예에 따른 통신시스템에서 MOSIM을 구비하는 단말이 자체적으로 사용자를 인증하는 절차를 도시한 도면이다.

[0050] 도 5를 참조하면, ISP(500)는 사용자 인증을 수행하는 RP(502)를 관리하고, 단말(510)은 브라우저(512)와 MOSIM(514)을 관리한다.

[0051] 사용자(520)는 브라우저(512)를 통해 접속하고자 하는 인터넷 사이트의 웹 브라우저를 실행하여 ISP(500)에 접속한다.(530단계) 이때 사용자(520)는 상기 ISP(500)에 접속함과 동시에 자신의 단말(510)이 MOSIM(514)을 가지

고 있으며 따라서 MOSIM(514)에서 관리되는 자체 정보만으로 인증을 수행할 수 있음을 지시하는 MOSIM Enabled=ON과 같은 정보를 입력한다.(530단계) 여기서는 MOSIM(514)에서 관리되는 자체 정보만으로 인증을 수행할 수 있음을 알리는 정보가 MOSIM Enabled=ON 형태로 구현되는 것을 일례로 설명하였으나, 상기 정보는 어떠한 형태로도 구현될 수 있음은 물론이다.

[0052] 또한 사용자(520)는 상기 접속하고자 하는 인터넷 사이트로부터 접속 정보가 요구되면 MOSIM을 이용하여 사용자를 인증하는 MOSIM 모드를 선택하고, 상기 MOSIM 모드를 통해 사용자 인증 시 사용될 식별 정보(USI)를 입력한다.(532단계) 이때 상기 식별자는 URI, URL, XRI 또는 MSISDN 등이 될 수 있다.

[0053] ISP(500)의 RP(502)는 MOSIM 모드를 승인하고 고정 값으로 정의된 MOSIM의 웹 접속 주소, 즉 로컬 IP 주소와 포트 번호를 추출한다.(534단계)

[0054] 또한 ISP(500)의 RP(502)는 사용자(520)가 접속하고자 하는 인터넷 사이트의 웹브라우저, 사용자(520)가 입력한 식별 정보(USI) 및 MOSIM을 통한 인증 요청을 단말(510)의 브라우저(512)에게 다시 전송한다.(536단계) 단말(510)은 사용자(520)가 입력한 식별 정보(USI) 및 인증 요청을 포함하는 HTTP Get Request 메시지를 534단계에서 추출한 로컬 IP 주소와 포트 번호를 통해 MOSIM(514)에게 전송한다.(538단계)

[0055] 그런 다음 MOSIM(514)은 사용자(520)에게 인증을 위한 보안 식별자, 일례로 아이디 및 패스워드를 요청하고,(540단계) 사용자(520)는 MOSIM(514)을 통해 상기 요청된 보안 식별자를 입력한다.(542단계) 이때 상기 MOSIM(514)은 타 응용 프로그램의 키보드 해킹 등을 방지하기 위해 그림화된 서명을 사용자(520)에게 디스플레이하여 사용자 인증을 위한 해당 정보를 입력 받을 수도 있다.

[0056] 상기 보안 식별자를 입력 받은 MOSIM(514)은 상기 보안 식별자가 유효한 정보인지 확인하여(544단계) 상기 아이디를 입력한 사용자(520)를 인증하고, 그 인증결과를 단말(510)의 브라우저(512)로 다시 전송한다.(546단계) 단말(510)의 브라우저(512)는 사용자(520)가 접속하고자 하는 인터넷 사이트의 웹브라우저를 인증결과와 함께 ISP(500)의 RP(502)로 전달하고,(548단계) ISP(500)의 RP(502)는 상기 인증결과를 검증한다.(550단계) 또한 ISP(500)의 RP(502)는 검증된 인증결과를 사용자(520)에게 디스플레이하여 인증 성공 또는 인증 실패에 따른 서비스를 제공한다.(552단계)

[0057] 도 5에서는 통신시스템에서 MOSIM을 제공하는 단말이 자체적으로 사용자를 인증하는 절차를 살펴보았다. 이와 같이 MOSIM을 제공하는 단말이 자체적으로 사용자를 인증하는 절차는 기존의 오픈아이디 서비스를 이용하여 사용자를 인증하는 절차에서 총 14번의 메시지 송수신을 수행하는 것과 달리 5개의 메시지 송수신 만으로 사용자를 인증할 수 있다.

[0058] 도 5에 도시된 인증 절차는 MOSIM이 보안 실행 환경(SEE: Secure Execution Environment)과 같이 하드웨어/소프트웨어가 결합하여 보안이 제공되는 모듈로 구현될 경우에는 별문제 없이 사용될 수 있다. 그러나 만약 해커가 의도적으로 단말의 브라우저 및 MOSIM을 모두 가짜로 개발했을 경우 상기 인증 절차만으로는 정확한 인증을 수행하기 어려운 문제가 있다. 즉 해커가 의도적으로 가짜 MOSIM을 구현하고 브라우저가 가짜 MOSIM으로 인증을 요청하는 HTTP Get Request 메시지를 전송할 경우, 가짜 MOSIM은 상기 인증 요청을 합법적인 인증으로 판단하여 처리할 수 있는 문제가 있다.

[0059] 상기와 같은 문제점을 개선하는 방안으로서, 이하에서는 도 6 및 도 7을 통해 단말과 인터넷 서비스 제공자(ISP)가 최초의 서비스 개시 시점에서 서로를 인증하는 인증키를 생성하고, 이후 모든 사용자 인증 절차에서 상기 생성한 인증키를 이용함으로써 인증 절차에 소용되는 시간을 줄이고 보안을 더욱 강화시킬 수 있는 개선된 인증 방안을 설명하도록 한다.

[0060] 또한 상기 개선된 인증 방안은 단말이 처음으로 특정 ISP의 인터넷 사이트에 접속하는 경우에 도 6의 절차를 수행하여 항구적 인증키를 최초 한번만 생성하여 사용자를 인증하고, 이후에는 도 7의 절차를 수행하여 기 생성한 항구적 인증키를 이용하여 사용자를 인증한다.

[0061] 도 6a 및 6b는 본 발명의 일 실시예에 따른 통신시스템에서 MOSIM을 제공하는 단말이 사용자 인증을 위해 항구적 인증키를 생성하는 절차를 도시한 도면이다. 도 6에서 설명할 절차는 단말이 처음으로 특정 ISP의 인터넷 사이트에 접속하는 경우에 수행되며 최초 한번만 수행된다.

[0062] 도 6a 및 6b를 참조하면, 이동통신 사업자(600)는 가입자 정보를 관리하는 HSS/HLR(602)와, 실질적으로 사용자(630)를 인증하는 BSF(604)와, OP/NAF(606)을 관리한다. 인터넷 서비스 제공자(ISP)(610)는 사용자 인증을 수행하는 RP(612)를 관리하고, 단말(620)은 브라우저/MOSIM(622)를 관리한다.

[0063] 사용자(630)는 브라우저/MOSIM(622)을 통해 접속하고자 하는 인터넷 사이트의 웹 브라우저를 실행하여 ISP(610)에 접속한다.(640단계) 이때 사용자(630)는 상기 ISP(610)에 접속함과 동시에 자신의 단말(620)이 MOSIM을 가지고 있으며 따라서 MOSIM에서 관리되는 자체 정보만으로 인증을 수행할 수 있음을 지시하는 MOSIM Enabled=ON 정보와, 단말(620)과 네트워크가 상호 공유하는 인증코드를 생성하고 관리함을 지시하는 USE_SIGCODE=YES 정보와, 단말(620)이 ISP(610)의 인터넷 사이트와의 인증 정보를 가지고 있지 않음을 지시하는 SignatureCode=NO와 같은 정보를 입력한다.(640단계) 상기 MOSIM Enabled=ON 정보와, USE_SIGCODE=YES 정보와, SignatureCode=NO 정보는 일례로서 구현된 것이며, 그 밖의 어떠한 형태로도 구현될 수 있음은 물론이다.

[0064] 또한 사용자(630)는 상기 접속하고자 하는 인터넷 사이트로부터 접속 정보가 요구되면 MOSIM을 이용하여 사용자를 인증하는 MOSIM 모드를 선택하고, 상기 MOSIM 모드를 통해 사용자 인증 시 사용될 식별 정보(USI)를 입력한다.(642단계) 이때 상기 식별자는 URI, URL, XRI 또는 MSISDN 등이 될 수 있다.

[0065] ISP(610)의 RP(612)는 MOSIM 모드를 승인하고, 상기 사용자(630)가 입력한 식별자로부터 사용자 인증을 대행하는 제3기관의 OP 주소를 추출하고,(644단계) 상기 제3기관, 즉 이동통신사업자(600)와 보안이 제공되는 통신 링크를 설정한다.(646단계) 이때 선택 사항이긴 하나 상기 통신 링크 설정을 위해 DH 키 교환 방식이 사용될 수 있다.

[0066] 또한 ISP(610)의 RP(612)는 사용자(630)가 접속하고자 하는 인터넷 사이트의 웹브라우저, 사용자(630)가 입력한 식별 정보(USI) 및 오픈 아이디를 통한 인증 요청을 단말(620)의 브라우저/MOSIM(622)에게 다시 전송하고,(648단계) 단말(620)은 사용자(630)가 입력한 식별 정보(USI) 및 MOSIM을 통한 인증 요청을 포함하는 HTTP Get Request 메시지를 이동통신사업자(600)의 OP에게 전송한다.(650단계) 그런 다음 상기 OP는 사용자(630)에 대한 인증을 시작한다.(652단계) 이때 상기 OP는 이동통신사업자(600)의 NAF 기능을 겸한다고 가정한다.

[0067] 이동통신사업자(600)의 NAF는 사용자(630)의 단말(620)에게 인증 시작을 알리는 HTTPS Response 401 Unauthorized 메시지를 전송하고,(654단계) 단말(620)은 상기 메시지에 대한 응답으로 HTTP Get Request 메시지를 이동통신사업자(600)의 BSF(604)에게 전송한다.(656단계) 이때 상기 HTTP Get Request 메시지에는 사용자(630)가 입력한 식별 정보(USI)가 포함된다.

[0068] 이동통신사업자(600)의 BSF(604)는 HSS/HLR(602)로부터 사용자(630) 인증을 위해 필요한 추가적인 정보를 획득하고,(658단계) BSF(604)는 인증 및 키 합의(AKA: Authentication and Key Agreement)를 요청하는 401 Unauthorized 메시지를 단말(620)에게 전송한다.(660단계)

[0069] 단말(620)은 상기 요청에 따라 AKA 알고리즘을 수행하고,(662단계) 상기 수행 결과를 Request Authorization Digest 메시지를 통해 이동통신사업자(600)의 BSF(604)로 전송한다. (664단계)

[0070] 이동통신사업자(600)의 BSF(604)는 상기 단말(620)로부터 수신한 AKA 알고리즘 수행 결과를 기반으로 하여 단말의 적합성을 판단하고, 단말(620)과 ISP(610) 서로를 인증하는 인증키를 생성한다.(666단계) 또한 이동통신사업자(600)의 BSF(604)는 상기 판단 결과에 따른 인증키를 200 OK 메시지를 통해 단말(620)로 전송한다.(668단계) 이때 상기 200 OK 메시지에는 상기 인증키가 이후 절차에서 유효하게 사용되는 시간 정보가 포함되며, 상기 인증키는 이후 절차에서 영구적으로 사용되므로, 이후에서는 상기 666단계에서 생성한 인증키를 항구적 인증키라 칭한다. 상기 항구적 인증키는 코드 형태로 구현될 수 있다.

[0071] 단말(620)은 이동통신사업자(600)의 BSF(604)로부터 수신한 항구적 인증키를 저장하고,(670단계) 항구적 인증키 정보를 HTTP Get Request 메시지를 통해 상기 이동통신사업자(600)의 OP/NAF(606)에 전달한다.(672단계) 이동통신사업자(600)의 OP/NAF(606)는 단말(620)로부터 수신한 항구적 인증키를 저장한다. (674단계)

[0072] 이동통신사업자(600)의 OP/NAF(606)는 BSF(604)에 접속하여 단말(620)로부터 수신한 항구적 인증키에 대한 정보를 요청하고,(676단계) BSF(104)는 상기 항구적 인증키 정보를 OP/NAF(106)에 제공한다.(678단계)

[0073] 이동통신사업자(600)의 OP/NAF(606)는 단말(620)을 통해 확인한 인증키와 BSF(604)를 통해 확인한 인증키 정보가 동일한지 확인하고, 동일할 경우 단말(620)의 사용자(630)가 접속하고자 하는 인터넷 사이트의 웹브라우저를 인증결과와 함께 단말(620)에게 전달하고,(680단계) 단말(120)은 상기 인증 결과를 RP(112)로 전달한다.(682단계)

[0074] ISP(610)의 RP(612)는 항구적 인증키를 저장하고, 상기 인증결과를 검증한다,(684단계) 또한 ISP(610)의 RP(612)는 검증된 인증결과를 사용자(630)에게 디스플레이하여 인증 성공 또는 인증 실패에 따른 서비스를 제공한다.(686단계)

[0075] 도 7은 본 발명의 일 실시예에 따른 통신시스템에서 MOSIM을 제공하는 단말이 기 생성한 항구적 인증키를 이용하여 사용자를 인증하는 절차를 도시한 도면이다. 도 7에서 설명할 절차는 기 생성한 항구적 인증키가 존재할 경우에만 적용된다.

[0076] 도 7을 참조하면, 인터넷 서비스 제공자(ISP)(700)는 사용자 인증을 수행하는 RP(702)를 관리하고, 단말(710)은 브라우저(712)와 MOSIM(714)을 관리한다.

[0077] 사용자(720)는 브라우저(712)를 통해 접속하고자 하는 인터넷 사이트의 웹 브라우저를 실행하여 ISP(700)에 접속한다.(730단계) 이때 사용자(720)는 상기 ISP(700)에 접속함과 동시에 자신의 단말(710)이 MOSIM(714)을 가지고 있으며 따라서 MOSIM(714)에서 관리되는 자체 정보만으로 인증을 수행할 수 있음을 지시하는 MOSIM Enabled=ON 정보와, 단말(610)과 네트워크가 상호 공유하는 인증코드를 생성하고 관리함을 지시하는 USE_SIGCODE=YES 정보와, 단말(710)이 ISP(700)의 인터넷 사이트와의 인증 정보를 가지고 있음을 지시하는 SignatureCode=YES와 같은 정보를 입력한다.(730단계) 상기 MOSIM Enabled=ON 정보와, USE_SIGCODE=YES 정보와, SignatureCode=YES 정보는 일례로서 구현된 것이며, 그 밖의 어떠한 형태로도 구현될 수 있음은 물론이다.

[0078] 또한 사용자(720)는 상기 접속하고자 하는 인터넷 사이트로부터 접속 정보가 요구되면 MOSIM(714)을 이용하여 사용자를 인증하는 MOSIM 모드를 선택하고, 상기 MOSIM 모드를 통해 사용자 인증 시 사용될 식별 정보(USI)를 입력한다.(732단계) 이때 상기 식별자는 URI, URL, XRI 또는 MSISDN 등이 될 수 있다.

[0079] ISP(700)의 RP(702)는 MOSIM 모드를 승인하고 고정 값으로 정의된 MOSIM의 웹 접속 주소, 즉 로컬 IP 주소와 포트 번호를 추출한다.(734단계) 또한 ISP(700)의 RP(702)는 사용자(720)가 접속하고자 하는 인터넷 사이트의 웹 브라우저, 사용자(720)가 입력한 식별 정보(USI) 및 MOSIM을 통한 인증 요청을 단말(710)의 브라우저(712)에게 다시 전송한다.(736단계) 단말(710)은 사용자(720)가 입력한 식별 정보(USI) 및 인증 요청을 포함하는 HTTP Get Request 메시지를 734단계에서 추출한 로컬 IP 주소와 포트 번호를 통해 MOSIM(714)에게 전송한다.(738단계)

[0080] 그런 다음 MOSIM(714)은 사용자(720)에게 인증을 위한 보안 식별자, 일례로 아이디 및 패스워드를 요청하고,(740단계) 사용자(720)는 MOSIM(714)을 통해 상기 요청된 보안 식별자를 입력한다.(742단계) 이때 상기 MOSIM(714)은 타 응용 프로그램의 키보드 해킹 등을 방지하기 위해 그림화된 서명을 사용자(720)에게 디스플레이하여 사용자 인증을 위한 해당 정보를 입력 받을 수도 있다.

[0081] 상기 보안 식별자를 입력 받은 MOSIM(714)은 상기 보안 식별자가 유효한 정보인지 확인하여(744단계) 상기 아이디를 입력한 사용자(720)를 인증하고, 그 인증결과와 함께 추가적으로 단말(710)과 ISP(700)의 인터넷 사이트가 이전에 서로를 인증하여 생성한 항구적 인증키, 즉 도 6의 670단계에서 저장한 항구적 인증키를 단말(710)의 브라우저(712)로 다시 전송한다.(746단계)

[0082] 단말(710)의 브라우저(712)는 사용자(720)가 접속하고자 하는 인터넷 사이트의 웹브라우저를 인증결과 및 항구적 인증키와 함께 ISP(700)의 RP(702)로 전달하고,(748단계) ISP(700)의 RP(702)는 상기 인증결과 및 항구적 인증키를 검증한다.(750단계) 또한 ISP(700)의 RP(702)는 검증된 인증결과를 사용자(720)에게 디스플레이하여 인증 성공 또는 인증 실패에 따른 서비스를 제공한다.(752단계)

[0083] 도 7에서 기 생성한 항구적 인증키를 이용하여 사용자를 인증할 시, 인터넷서비스 제공자가 요구하는 단말의 인증에 대한 신뢰성, 또는 단말이 요구하는 인터넷서비스 제공자의 신뢰성이 보다 높은 수준일 경우 추가적으로 사용되는 이중 체크 방식에 대해 이하의 도 8 및 도 9를 통해 설명하도록 한다.

[0084] 도 8a 및 8b는 본 발명의 일 실시예에 따른 통신시스템에서 MOSIM을 제공하는 단말이 AKA 인증 알고리즘 접근 방식에 따른 이중 체크를 통해 사용자를 인증하는 절차를 도시한 도면이다.

[0085] 도 8a 및 8b를 참조하면, 이동통신 사업자(800)는 사용자(830)를 인증하는 BSF(802)와, OP/NAF(804)를 관리한다. 인터넷 서비스 제공자(ISP)(810)는 사용자 인증을 수행하는 RP(812)를 관리하고, 단말(820)은 브라우저(822)와 MOSIM(824)을 관리한다.

[0086] 사용자(830)는 브라우저(822)를 통해 접속하고자 하는 인터넷 사이트의 웹 브라우저를 실행하여 ISP(810)에 접속한다.(840단계) 이때 사용자(830)는 상기 ISP(810)에 접속함과 동시에 자신의 단말(820)이 MOSIM(824)을 가지고 있으며 따라서 MOSIM(824)에서 관리되는 자체 정보만으로 인증을 수행할 수 있음을 지시하는 MOSIM Enabled=ON 정보와, 단말(820)과 네트워크가 상호 공유하는 인증코드를 생성하고 관리함을 지시하는 USE_SIGCODE=YES 정보와, 단말(820)이 ISP(810)의 인터넷 사이트와의 인증 정보를 가지고 있음을 지시하는

SignatureCode=YES와, 상기 인증 정보를 입력한다.(840단계) 여기서 상기 단말(820)과 ISP(810)의 인터넷 사이트간의 인증 정보는 일례로 항구적 인증키라 가정한다. 또한 상기 MOSIM Enabled=ON 정보와, USE_SIGCODE=YES 정보와, SignatureCode=YES 정보는 일례로서 구현된 것이며, 그 밖의 어떠한 형태로도 구현될 수 있음은 물론이다.

[0087] 또한 사용자(830)는 상기 접속하고자 하는 인터넷 사이트로부터 접속 정보가 요구되면 MOSIM(824)을 이용하여 사용자를 인증하는 MOSIM 모드를 선택하고, 상기 MOSIM 모드를 통해 사용자 인증 시 사용될 식별 정보(USI)를 입력한다.(842단계) 이때 상기 식별자는 URI, URL, XRI 또는 MSISDN 등이 될 수 있다.

[0088] ISP(810)의 RP(812)는 MOSIM 모드를 승인하고 고정 값으로 정의된 MOSIM의 웹 접속 주소, 즉 로컬 IP 주소와 포트 번호를 추출하고, 이중체크 방식을 적용하는 이중체크 모드를 설정한다.(844단계) 상기 이중체크 모드는 접근 방식에 따라 복수의 모드들로 정의될 수 있으며, 여기서는 AKA 인증 알고리즘 접근 방식이 적용되는 제1이중체크 모드를 일례로 설명한다.

[0089] 또한 ISP(810)의 RP(812)는 사용자(830)가 접속하고자 하는 인터넷 사이트의 웹브라우저, 사용자(830)가 입력한 식별 정보(USI), MOSIM을 통한 인증 요청 및 상기 제1이중체크 모드가 설정되었음을 지시하는 DualCheck=YES1 정보를 단말(820)의 브라우저(822)에게 다시 전송한다.(846단계) 단말(820)의 브라우저(822)는 사용자(830)가 입력한 식별 정보(USI) 및 인증 요청을 포함하는 HTTP Get Request 메시지를 844단계에서 추출한 로컬 IP 주소와 포트 번호를 통해 MOSIM(824)에게 전송한다.(848단계)

[0090] 그런 다음 MOSIM(824)은 사용자(830)에게 인증을 위한 보안 식별자, 일례로 아이디 및 패스워드를 요청하고,(850단계) 사용자(830)는 MOSIM(824)을 통해 상기 요청된 보안 식별자를 입력한다.(852단계) 이때 상기 MOSIM(824)은 타 응용 프로그램의 키보드 해킹 등을 방지하기 위해 그림화된 서명을 사용자(830)에게 디스플레이하여 사용자 인증을 위한 해당 정보를 입력 받을 수도 있다.

[0091] 상기 보안 식별자를 입력 받은 MOSIM(824)은 상기 보안 식별자가 유효한 정보인지 확인하여(854단계) 상기 아이디를 입력한 사용자(830)를 인증하고, 그 인증결과와 함께 추가적으로 단말(820)과 ISP(810)의 인터넷 사이트가 이전에 서로를 인증하여 생성한 항구적 인증키, 즉 도 6의 670단계에서 저장한 항구적 인증키를 단말(820)의 브라우저(822)로 다시 전송한다.(856단계)

[0092] 단말(820)의 브라우저(822)는 사용자(830)가 접속하고자 하는 인터넷 사이트의 웹브라우저를 인증결과 및 항구적 인증키와 함께 ISP(810)의 RP(812)로 전달하고,(858단계) ISP(810)의 RP(812)는 사용자(830)가 입력한 식별자로부터 사용자 인증을 대행하는 제3기관의 OP 주소를 추출하고,(860단계) 상기 제3기관, 즉 이동통신사업자(800)와 보안이 제공되는 통신 링크를 설정한다.(862단계) 이때 선택 사항이긴 하나 상기 통신 링크 설정을 위해 DH 키 교환 방식이 사용될 수 있다.

[0093] 그런 다음 ISP(810)의 RP(812)는 AKA 인증 알고리즘 접근 방식을 적용하여 이중체크를 수행하도록 요청하는 확인 요청을 이동통신사업자(800)의 BSF(802)에게 전송하고,(864단계) BSF(802)는 인증 및 키 합의(AKA)를 요청하는 401 Unauthorized 메시지를 단말(820)에게 전송한다.(866단계)

[0094] 단말(820)은 상기 요청에 따라 AKA 알고리즘을 수행하고,(868단계) 상기 수행 결과를 Request Authorization Digest 메시지를 통해 이동통신사업자(800)의 BSF(802)로 전송한다.(870단계)

[0095] 이동통신사업자(800)의 BSF(802)는 상기 단말(820)로부터 수신한 AKA 알고리즘 수행 결과를 기반으로 하여 단말의 적합성을 판단하고, 상기 판단 결과에 따른 인증키를 200 OK 메시지를 통해 단말(820)의 MOSIM(824)에게 전송한다.(872단계) 이때 상기 200 OK 메시지에는 상기 인증키가 이후 절차에서 유효하게 사용되는 시간 정보가 포함된다. 또한 상기 BSF(802)는 상기 864단계에서 수신한 확인 요청에 대한 응답을 나타내는 확인 응답을 ISP(810)의 RP(812)에게 전송한다.(874단계) 상기 확인 응답에는 인증 결과가 포함된다.

[0096] ISP(810)의 RP(812)는 상기 인증 결과를 검증하고,(876단계) 검증된 인증결과를 사용자(830)에게 디스플레이하여 인증 성공 또는 인증 실패에 따른 서비스를 제공한다.(878단계)

[0097] 이 경우 도 1에서의 13개의 무선구간 메시지 송수신은 8개로 줄어드는 효과를 보인다. 비록 도 5 및 도 7에 비교하여 무선구간 메시지 송수신은 증가하였나, 단말까지 경유하는 인증을 수행함으로써 인증의 안정도는 훨씬 증가하였다.

[0098] 도 9a 및 9b는 본 발명의 일 실시예에 따른 통신시스템에서 MOSIM을 제공하는 단말이 무선 구간의 부하를 줄이

는 접근 방식에 따른 이중 체크 방식을 통해 사용자를 인증하는 절차를 도시한 도면이다.

[0099] 도 9a 및 9b를 참조하면, 이동통신 사업자(900)는 가입자 정보를 관리하는 HSS/HLR(902)와, OP/HSS-FE(904)를 관리한다. 인터넷 서비스 제공자(ISP)(910)는 사용자 인증을 수행하는 RP(912)를 관리하고, 단말(920)은 브라우저(922)와 MOSIM(924)을 관리한다.

[0100] 사용자(930)는 브라우저(922)를 통해 접속하고자 하는 인터넷 사이트의 웹 브라우저를 실행하여 ISP(910)에 접속한다.(940단계) 이때 사용자(930)는 상기 ISP(910)에 접속함과 동시에 자신의 단말(920)이 MOSIM(924)을 가지고 있으며 따라서 MOSIM(924)에서 관리되는 자체 정보만으로 인증을 수행할 수 있음을 지시하는 MOSIM Enabled=ON 정보와, 단말(920)과 네트워크가 상호 공유하는 인증코드를 생성하고 관리함을 지시하는 USE_SIGCODE=YES 정보와, 단말(920)이 ISP(910)의 인터넷 사이트와의 인증 정보를 가지고 있음을 지시하는 SignatureCode=YES와, 상기 인증 정보를 입력한다.(840단계) 여기서 상기 단말(920)과 ISP(910)의 인터넷 사이트간의 인증 정보는 일례로 항구적 인증키라 가정한다. 또한 상기 MOSIM Enabled=ON 정보와, USE_SIGCODE=YES 정보와, SignatureCode=YES 정보는 일례로서 구현된 것이며, 그 밖의 어떠한 형태로도 구현될 수 있음은 물론이다.

[0101] 또한 사용자(930)는 상기 접속하고자 하는 인터넷 사이트로부터 접속 정보가 요구되면 MOSIM(924)을 이용하여 사용자를 인증하는 MOSIM 모드를 선택하고, 상기 MOSIM 모드를 통해 사용자 인증 시 사용될 식별 정보(USI)를 입력한다.(942단계) 이때 상기 식별자는 URI, URL, XRI 또는 MSISDN 등이 될 수 있다.

[0102] ISP(910)의 RP(912)는 MOSIM 모드를 승인하고 고정 값으로 정의된 MOSIM의 웹 접속 주소, 즉 로컬 IP 주소와 포트 번호를 추출하고, 이중체크 방식을 적용하는 이중체크 모드를 설정한다.(944단계) 상기 이중체크 모드는 접근 방식에 따라 복수의 모드들로 정의될 수 있으며, 여기서는 단말이 무선 구간의 부하를 줄이는 접근 방식이 적용되는 제2이중체크 모드를 일례로 설명한다.

[0103] 또한 ISP(910)의 RP(912)는 사용자(930)가 접속하고자 하는 인터넷 사이트의 웹브라우저, 사용자(930)가 입력한 식별 정보(USI), MOSIM을 통한 인증 요청 및 상기 제2이중체크 모드가 설정되었음을 지시하는 DualCheck=YES2 정보를 단말(920)의 브라우저(922)에게 다시 전송한다.(946단계) 단말(920)의 브라우저(922)는 사용자(930)가 입력한 식별 정보(USI) 및 인증 요청을 포함하는 HTTP Get Request 메시지를 944단계에서 추출한 로컬 IP 주소와 포트 번호를 통해 MOSIM(924)에게 전송한다.(948단계)

[0104] 그런 다음 MOSIM(924)은 사용자(930)에게 인증을 위한 보안 식별자, 일례로 아이디 및 패스워드를 요청하고,(950단계) 사용자(930)는 MOSIM(924)을 통해 상기 요청된 보안 식별자를 입력한다.(952단계) 이때 상기 MOSIM(924)은 타 응용 프로그램의 키보드 해킹 등을 방지하기 위해 그림화된 서명을 사용자(930)에게 디스플레이하여 사용자 인증을 위한 해당 정보를 입력 받을 수도 있다.

[0105] 상기 보안 식별자를 입력 받은 MOSIM(924)은 상기 보안 식별자가 유효한 정보인지 확인하여(954단계) 상기 아이디를 입력한 사용자(930)를 인증하고, 그 인증결과와 함께 추가적으로 단말(920)과 ISP(910)의 인터넷 사이트가 이전에 서로를 인증하여 생성한 항구적 인증키, 즉 도 6의 670단계에서 저장한 항구적 인증키를 단말(920)의 브라우저(922)로 다시 전송한다.(956단계) 단말(920)의 브라우저(922)는 사용자(930)가 접속하고자 하는 인터넷 사이트의 웹브라우저를 인증결과 및 항구적 인증키와 함께 ISP(910)의 RP(912)로 전달한다.(958단계)

[0106] 한편, MOSIM(924)은 선택 사항으로써 상기 954단계에서 사용자 정보와 현재 시간 값에 따른 인증시간을 이용하여 인증 결과값인 확인키를 생성할 수 있으며, 상기 생성된 확인키 정보, 즉 상기 확인키를 나타내는 코드와 상기 인증시간 값은 단말(920)의 브라우저(922)를 통해 ISP(910)의 RP(912)로 전달될 수 있다.

[0107] ISP(910)의 RP(912)는 사용자(930)가 입력한 식별자로부터 사용자 인증을 대행하는 제3기관의 OP 주소를 추출하고,(960단계) 상기 제3기관, 즉 이동통신사업자(900)와 보안이 제공되는 통신 링크를 설정한다.(962단계) 이때 선택 사항이긴 하나 상기 통신 링크 설정을 위해 DH 키 교환 방식이 사용될 수 있다.

[0108] 그런 다음 ISP(910)의 RP(912)는 단말이 무선 구간의 부하를 줄이는 접근 방식을 적용하여 이중체크를 수행하도록 요청하는 확인 요청을 이동통신사업자(900)의 OP/HSS-FE(904)에게 전송하고,(964단계) 상기 확인 요청에는 항구적 인증키 및 확인키 정보가 포함되며, 경우에 따라 상기 확인키 정보는 확인 요청에 포함되지 않을 수도 있다.

[0109] 이동통신사업자(900)의 HSS/HLR(902)는 OP/HSS-FE(904)와 사용자 정보를 공유한다.(966단계) OP/HSS-FE(904)는 항구적 인증키를 검증하고, 사용자 정보와 인증시간 값을 이용하여 인증 결과값인 확인키를 생성하여 앞서 956

및 960단계를 통해 전달 받은 확인키와 동일한지 비교한다.(968단계) 또한 OP/HSS-FE(904)는 상기 964단계에서 수신한 확인 요청에 대한 응답을 나타내는 확인 응답을 ISP(910)의 RP(912)에게 전송한다.(970단계) 상기 확인 응답에서 인증 결과가 포함된다.

[0110] ISP(910)의 RP(912)는 상기 인증 결과를 검증하고,(972단계) 검증된 인증결과를 사용자(930)에게 디스플레이하여 인증 성공 또는 인증 실패에 따른 서비스를 제공한다.(974단계)

[0111] 이하에서는 도 10 및 도 11을 통해 이동통신사업자 또는 기업용 단말을 관리하는 관리자가 블랙 리스트(Black List) 및 화이트 리스트(White List)를 고려하여 해당 단말이 접속하는 인터넷 사이트에 대한 접속 허용 여부를 결정하는 방안을 설명하도록 한다. 여기서 상기 블랙 리스트는 해당 단말의 접속이 허용되지 않는 인터넷 사이트들의 목록을 의미하고, 상기 화이트 리스트는 해당 단말의 접속이 허용되는 인터넷 사이트들의 목록을 의미한다.

[0112] 도 10은 본 발명의 일 실시예에 따른 통신시스템에서 MOSIM을 제공하는 단말이 검증된 응용 데이터베이스 정보를 기반으로 사용자 접속을 허용하는 절차를 도시한 도면이다.

[0113] 도 10을 참조하면, 인터넷 서비스 제공자(ISP)(1000)는 사용자 인증을 수행하는 RP(1002)를 관리하고, 단말(1010)은 브라우저(1012)와 MOSIM(1014)을 관리한다.

[0114] 사용자(1020)는 브라우저(1012)를 통해 접속하고자 하는 인터넷 사이트의 웹 브라우저를 실행하여 ISP(1000)에 접속한다.(1030단계) 이때 사용자(1020)는 상기 ISP(1000)에 접속함과 동시에 자신의 단말(1010)이 MOSIM(1014)을 가지고 있으며 따라서 MOSIM(1014)에서 관리되는 자체 정보만으로 인증을 수행할 수 있음을 지시하는 MOSIM Enabled=ON 정보를 입력한다.(1030단계) 상기 MOSIM Enabled=ON 정보는 일례로서 구현된 것이며 그 밖의 어떠한 형태로도 구현될 수 있음은 물론이다.

[0115] 또한 사용자(1020)는 상기 접속하고자 하는 인터넷 사이트로부터 접속 정보가 요구되면 MOSIM(1014)을 이용하여 사용자를 인증하는 MOSIM 모드를 선택하고, 상기 MOSIM 모드를 통해 사용자 인증 시 사용될 식별 정보(USI)를 입력한다.(1032단계) 이때 상기 식별자는 URI, URL, XRI 또는 MSISDN 등이 될 수 있다.

[0116] ISP(1000)의 RP(1002)는 MOSIM 모드를 승인하고 고정 값으로 정의된 MOSIM의 웹 접속 주소, 즉 로컬 IP 주소와 포트 번호를 추출한다.(1034단계) 또한 ISP(1000)의 RP(1002)는 사용자(1020)가 접속하고자 하는 인터넷 사이트의 웹브라우저, 사용자(1020)가 입력한 식별 정보(USI) 및 MOSIM(1014)을 통한 인증 요청을 단말(1010)의 브라우저(1012)에게 다시 전송한다.(1036단계) 단말(1010)은 어플리케이션 식별자, 사용자(1020)가 입력한 식별 정보(USI) 및 인증 요청을 포함하는 HTTP Get Request 메시지를 1034단계에서 추출한 로컬 IP 주소와 포트 번호를 통해 MOSIM(1014)에게 전송한다.(1038단계) 여기서 상기 어플리케이션 식별자 브라우저(1012)가 제공하는 인터넷 사이트 자체를 나타낼 수도 있고, 그 밖의 해당 응용 프로그램의 개발자(creator) 정보와 해당 응용 프로그램의 식별자 정보의 조합을 나타낼 수도 있다.

[0117] 단말(1010)의 MOSIM(1014)은 검증된 응용 데이터베이스가 관리하는 블랙 리스트 및 화이트 리스트를 통해 어플리케이션 식별자가 나타내는 인터넷 사이트로의 접속을 허용할지 여부를 결정한다. 여기서는 MOSIM(1014)이 상기 인터넷 사이트로의 접속을 허용하는 경우를 가정하여 설명한다. 즉 단말(1010)의 MOSIM(1014)은 검증된 응용 데이터베이스가 관리하는 블랙 리스트 및 화이트 리스트를 확인한다. 이후 상기 어플리케이션 식별자가 나타내는 인터넷 사이트가 화이트 리스트에 포함될 경우,(1040단계) MOSIM(1014)은 사용자(1020)에게 인증을 위한 보안 식별자, 일례로 아이디 및 패스워드를 요청하고,(1042단계) 사용자(1020)는 MOSIM(1014)을 통해 상기 요청된 보안 식별자를 입력한다.(1044단계) 이때 상기 MOSIM(1014)은 타 응용 프로그램의 키보드 해킹 등을 방지하기 위해 그림화된 서명을 사용자(1020)에게 디스플레이하여 사용자 인증을 위한 해당 정보를 입력 받을 수도 있다.

[0118] 상기 보안 식별자를 입력 받은 MOSIM(1014)은 상기 보안 식별자가 유효한 정보인지 확인하여(1046단계) 상기 아이디를 입력한 사용자(1020)를 인증하고, 그 인증결과를 단말(1010)의 브라우저(1012)로 다시 전송한다.(1048단계) 단말(1010)의 브라우저(1012)는 사용자(1020)가 접속하고자 하는 인터넷 사이트의 웹브라우저를 인증결과와 함께 ISP(1000)의 RP(1002)로 전달한다.(1050단계)

[0119] ISP(1000)의 RP(1002)는 상기 인증 결과를 검증하고,(1052단계) 검증된 인증결과를 사용자(1020)에게 디스플레이하여 인증 성공 또는 인증 실패에 따른 서비스를 제공한다.(1054단계)

[0120] 도 11은 본 발명의 일 실시예에 따른 통신시스템에서 MOSIM을 제공하는 단말이 검증된 응용 데이터베이스 정보를 기반으로 사용자 접속을 거절하는 절차를 도시한 도면이다.

[0121] 도 11을 참조하면, 인터넷 서비스 제공자(ISP)(1100)는 사용자 인증을 수행하는 RP(1102)를 관리하고, 단말(1110)은 브라우저(1112)와 MOSIM(1114)을 관리한다.

[0122] 사용자(1120)는 브라우저(1112)를 통해 접속하고자 하는 인터넷 사이트의 웹 브라우저를 실행하여 ISP(1100)에 접속한다.(1130단계) 이때 사용자(1120)는 상기 ISP(1100)에 접속함과 동시에 자신의 단말(1110)이 MOSIM(1114)을 가지고 있으며 따라서 MOSIM(1114)에서 관리되는 자체 정보만으로 인증을 수행할 수 있음을 지시하는 MOSIM Enabled=ON 정보를 입력한다.(1130단계) 상기 MOSIM Enabled=ON 정보는 일례로서 구현된 것이며 그 밖의 어떠한 형태로도 구현될 수 있음은 물론이다.

[0123] 또한 사용자(1120)는 상기 접속하고자 하는 인터넷 사이트로부터 접속 정보가 요구되면 MOSIM(1114)을 이용하여 사용자를 인증하는 MOSIM 모드를 선택하고, 상기 MOSIM 모드를 통해 사용자 인증 시 사용될 식별 정보(USI)를 입력한다.(1132단계) 이때 상기 식별자는 URI, URL, XRI 또는 MSISDN 등이 될 수 있다.

[0124] ISP(1100)의 RP(1102)는 MOSIM 모드를 승인하고 고정 값으로 정의된 MOSIM의 웹 접속 주소, 즉 로컬 IP 주소와 포트 번호를 추출한다.(1134단계) 또한 ISP(1100)의 RP(1102)는 사용자(1120)가 접속하고자 하는 인터넷 사이트의 웹브라우저, 사용자(1120)가 입력한 식별 정보(USI) 및 MOSIM(1114)을 통한 인증 요청을 단말(1110)의 브라우저(1112)에게 다시 전송한다.(1036단계) 단말(1010)은 어플리케이션 식별자, 사용자(1020)가 입력한 식별 정보(USI) 및 인증 요청을 포함하는 HTTP Get Request 메시지를 1134단계에서 추출한 로컬 IP 주소와 포트 번호를 통해 MOSIM(1114)에게 전송한다.(1138단계) 여기서 상기 어플리케이션 식별자 브라우저(1112)가 제공하는 인터넷 사이트 자체를 나타낼 수도 있고, 그 밖의 해당 응용 프로그램의 개발자 정보와 해당 응용 프로그램의 식별자 정보의 조합을 나타낼 수도 있다.

[0125] 단말(1110)의 MOSIM(1114)은 검증된 응용 데이터베이스가 관리하는 블랙 리스트 및 화이트 리스트를 통해 어플리케이션 식별자가 나타내는 인터넷 사이트로의 접속을 허용할지 여부를 결정한다. 여기서는 MOSIM(1114)이 상기 인터넷 사이트로의 접속을 거절하는 경우를 가정하여 설명한다. 즉 단말(1010)의 MOSIM(1014)은 검증된 응용 데이터베이스가 관리하는 블랙 리스트 및 화이트 리스트를 확인한다. 이후 상기 어플리케이션 식별자가 나타내는 인터넷 사이트가 블랙 리스트에 포함될 경우,(1140단계) MOSIM(1014)은 인터넷 사이트로의 접속이 거절되었음을 나타내는 인증결과를 브라우저(1112)에게 다시 전송한다.(1142단계)

[0126] 단말(1110)의 브라우저(1112)는 사용자(1120)가 접속하고자 하는 인터넷 사이트의 웹브라우저를 인증결과와 함께 ISP(1100)의 RP(1102)로 전달한다.(1114단계)

[0127] ISP(1100)의 RP(1102)는 상기 인증 결과를 검증하고,(1146단계) 검증된 인증결과를 사용자(1120)에게 디스플레이하여 인증 실패에 따른 서비스를 제공한다.(1148단계)

[0128] 도시하지는 않았으나 도 10 및 도 11에서 설명한 사용자 접속의 허용 또는 거절 절차에서 사용되는 검증된 응용 데이터베이스가 관리하는 블랙 리스트 및 화이트 리스트는, 이동통신 사업자가 관리하는 모듈들 중 단말을 관리하는 모듈과 상기 단말의 MOSIM 간에 보안이 보장되는 별도의 통신 링크를 설정하고, 상기 설정한 통신 링크를 통해 블랙 리스트 및 화이트 리스트에 포함되는 인터넷 사이트들의 목록을 업데이트한다. 즉 상기 단말을 관리하는 모듈은 블랙 리스트 및 화이트 리스트에 포함될 인터넷 사이트 정보를 단말의 MOSIM으로 전달하고, 단말의 MOSIM은 실제 인터넷 사이트에 접근하여 통신을 수행한 경우의 통계 정보를 상기 단말을 관리하는 모듈에게 전달한다. 또한 상기와 같은 해당 정보들의 송수신이 완료되면, 앞서 설명한 별도의 통신 링크를 해제한다.

[0129] 한편 본 발명의 상세한 설명에서는 구체적인 실시 예에 관해 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시 예에 국한되어 정해져서는 안되며 후술하는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

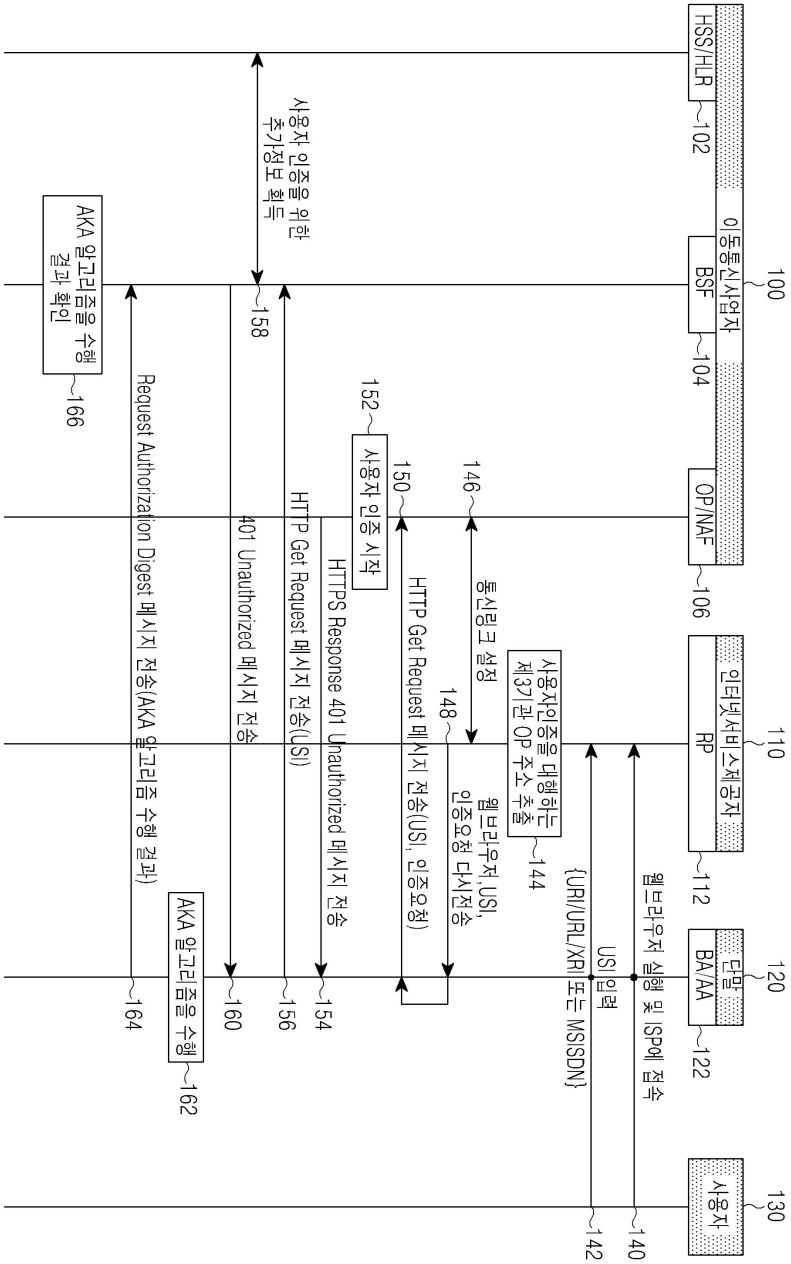
[0130] 또한 본 발명의 실시예에 따른 간소화된 절차를 통해 사용자를 인증을 대행하는 방법은 하드웨어, 소프트웨어 또는 하드웨어 및 소프트웨어의 조합의 형태로 실현 가능하다는 것을 알 수 있을 것이다. 이러한 임의의 소프트웨어는 예를 들어, 삭제 가능 또는 재기록 가능 여부와 상관없이, ROM 등의 저장 장치와 같은 휘발성 또는 비휘발성 저장 장치, 또는 예를 들어, RAM, 메모리 칩, 장치 또는 집적 회로와 같은 메모리, 또는 예를 들어 CD, DVD, 자기 디스크 또는 자기 테이프 등과 같은 광학 또는 자기적으로 기록 가능함과 동시에 기계(예를 들어, 컴퓨터)로 읽을 수 있는 저장 매체에 저장될 수 있다. 본 발명의 그래픽 화면 갱신 방법은 제어부 및 메모리를 포함하는 컴퓨터 또는 휴대 단말에 의해 구현될 수 있고, 상기 메모리는 본 발명의 실시 예들을 구현하는 지시들을 포함하는 프로그램 또는 프로그램들을 저장하기에 적합한 기계로 읽을 수 있는 저장 매체의 한 예임을 알 수 있을 것이다.

[0131] 따라서, 본 발명은 본 명세서의 임의의 청구항에 기재된 장치 또는 방법을 구현하기 위한 코드를 포함하는 프로그램 및 이러한 프로그램을 저장하는 기계(컴퓨터 등)로 읽을 수 있는 저장 매체를 포함한다. 또한, 이러한 프로그램은 유선 또는 무선 연결을 통해 전달되는 통신 신호와 같은 임의의 매체를 통해 전자적으로 이송될 수 있고, 본 발명은 이와 균등한 것을 적절하게 포함한다

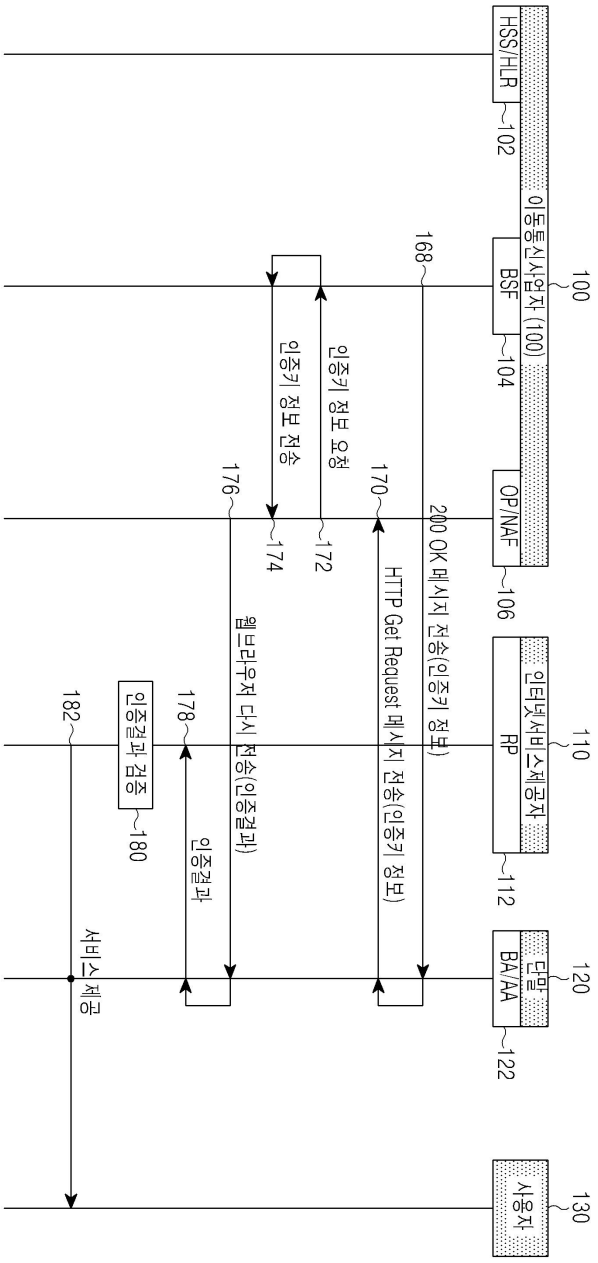
[0132] 또한 본 발명의 실시예에 따른 간소화된 절차를 통해 사용자를 인증을 대행하는 장치는 유선 또는 무선으로 연결되는 프로그램 제공 장치로부터 상기 프로그램을 수신하여 저장할 수 있다. 상기 프로그램 제공 장치는 상기 그래픽 처리 장치가 기설정된 컨텐츠 보호 방법을 수행하도록 하는 지시들을 포함하는 프로그램, 컨텐츠 보호 방법에 필요한 정보 등을 저장하기 위한 메모리와, 상기 그래픽 처리 장치와의 유선 또는 무선 통신을 수행하기 위한 통신부와, 상기 그래픽 처리 장치의 요청 또는 자동으로 해당 프로그램을 상기 송수신 장치로 전송하는 제어부를 포함할 수 있다.

도면

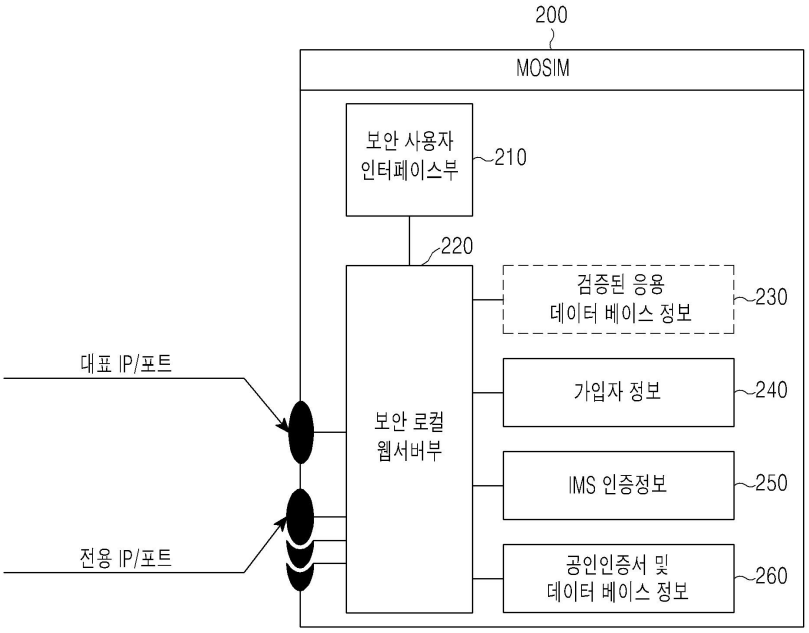
도면1



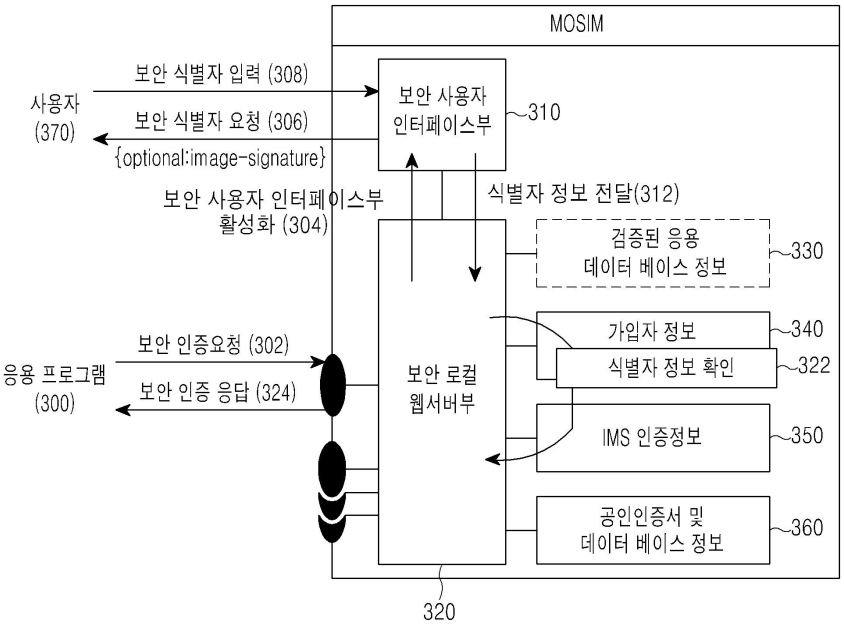
도면1b


HSS/HLR
102
이동통신사업자 (100)
BSF
104
OP/NAF
106
100
인터넷서비스제공자
RP
112
110
단말
BA/AA
122
120
사용자
130
168
인증키 정보 요청
172
인증키 정보 전송
174
176
200 OK 메시지 전송(인증키 정보)
170
HTTP Get Request 메시지 전송(인증키 정보)
웹브라우저 다시 전송(인증결과)
178
인증결과
인증결과 검증
180
182
서비스 제공

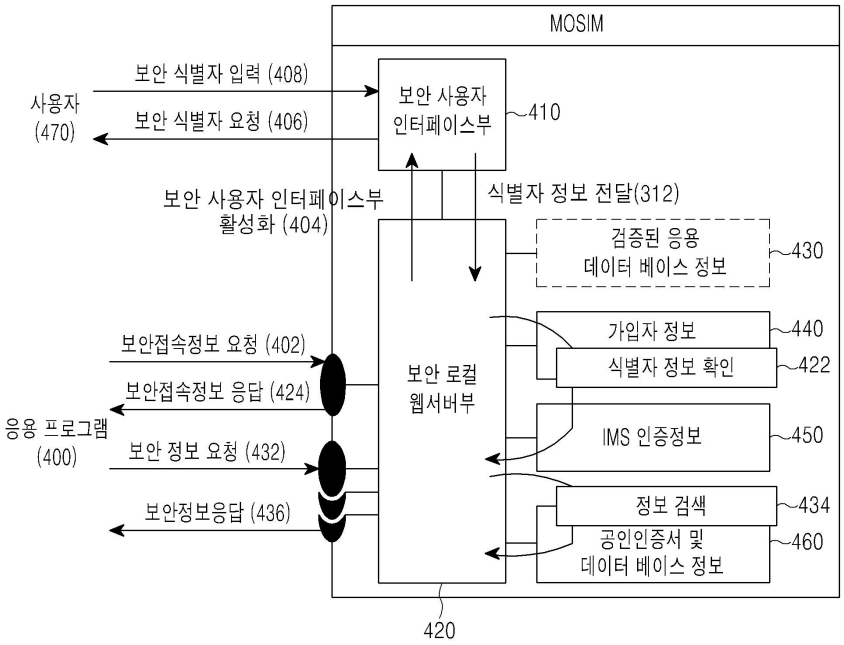
도면2


200
MOSIM
보안 사용자
인터페이스부
210
220
검증된 응용
데이터 베이스 정보
230
대표 IP/포트
보안 로컬
웹서버부
가입자 정보
240
IMS 인증정보
250
전용 IP/포트
공인인증서 및
데이터 베이스 정보
260

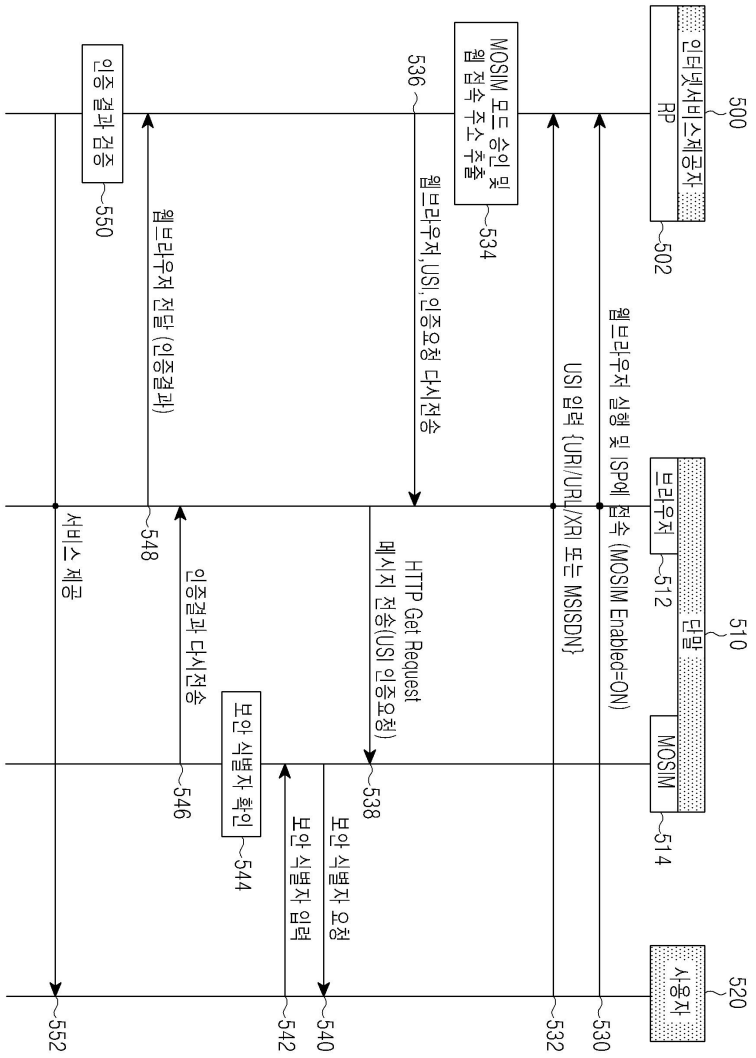
도면3


MOSIM
보안 식별자 입력 (308)
사용자
(370)
보안 식별자 요청 (306)
{optional:image-signature}
보안 사용자
인터페이스부
310
보안 사용자 인터페이스부
활성화 (304)
식별자 정보 전달(312)
검증된 응용
데이터 베이스 정보
330
보안 인증요청 (302)
응용 프로그램
(300)
보안 인증 응답 (324)
보안 로컬
웹서버부
가입자 정보
340
식별자 정보 확인
322
IMS 인증정보
350
공인인증서 및
데이터 베이스 정보
360
320

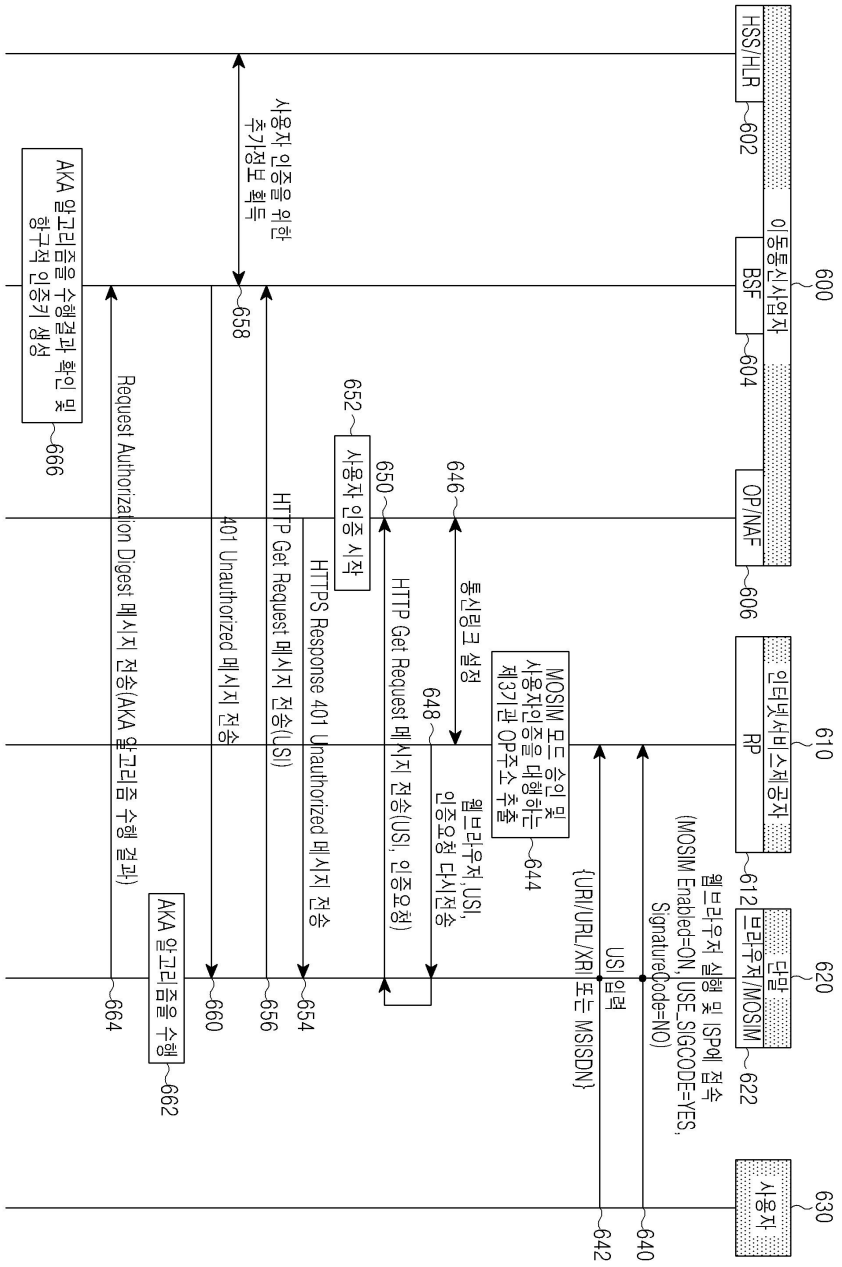
도면4


MOSIM
보안 식별자 입력 (408)
사용자
(470)
보안 식별자 요청 (406)
보안 사용자
인터페이스부
410
보안 사용자 인터페이스부
활성화 (404)
식별자 정보 전달(312)
검증된 응용
데이터 베이스 정보
430
가입자 정보
440
식별자 정보 확인
422
보안접속정보 요청 (402)
보안접속정보 응답 (424)
응용 프로그램
(400)
보안 정보 요청 (432)
보안 로컬
웹서버부
IMS 인증정보
450
정보 검색
434
보안정보응답 (436)
공인인증서 및
데이터 베이스 정보
460
420

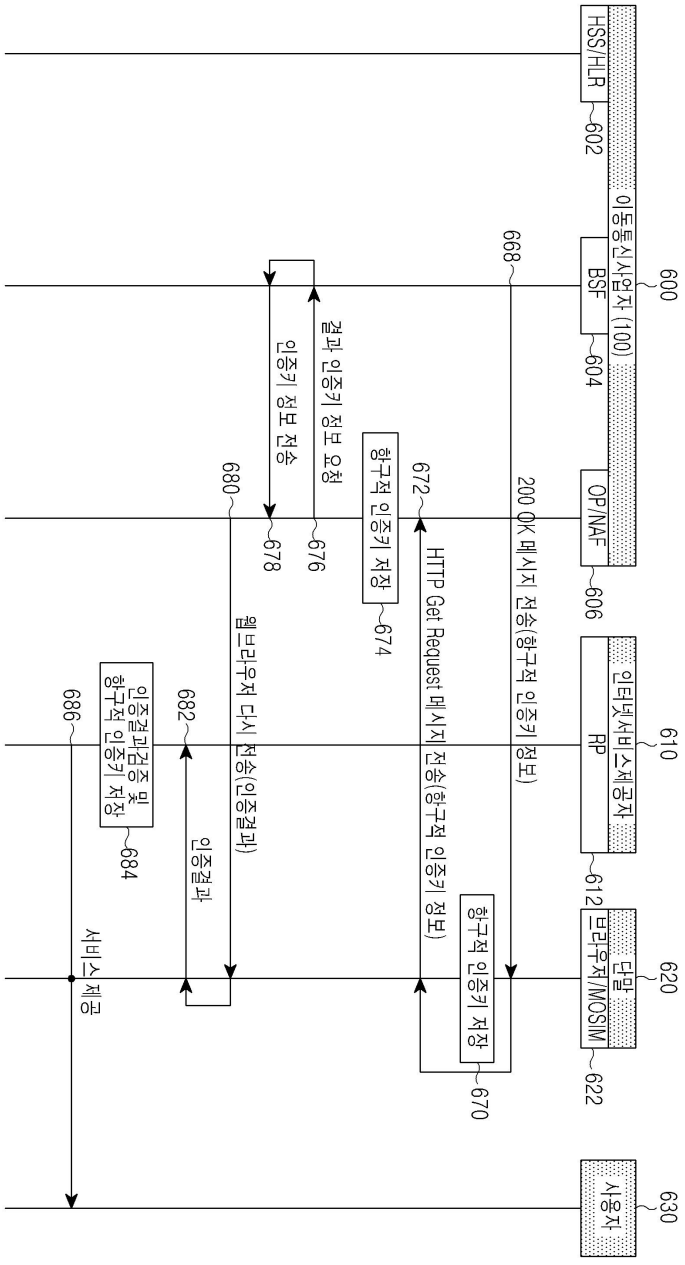
도면5


인터넷서비스제공자
RP
500
502
MOSIM 모드 승인 및
웹 접속 주소 추출
534
536
인증 결과 검증
550
웹브라우저,USI,인증요청 다시전송
웹브라우저 전달 (인증결과)
웹브라우저 실행 및 ISP에 접속 (MOSIM Enabled=ON)
USI 입력 {URI/URL/XRI 또는 MSISDN}
브라우저
512
단말
510
MOSIM
514
548
서비스 제공
HTTP Get Request
메시지 전송(USI 인증요청)
538
인증결과 다시전송
546
보안 식별자 확인
544
보안 식별자 입력
542
보안 식별자 요청
540
사용자
520
552
532
530

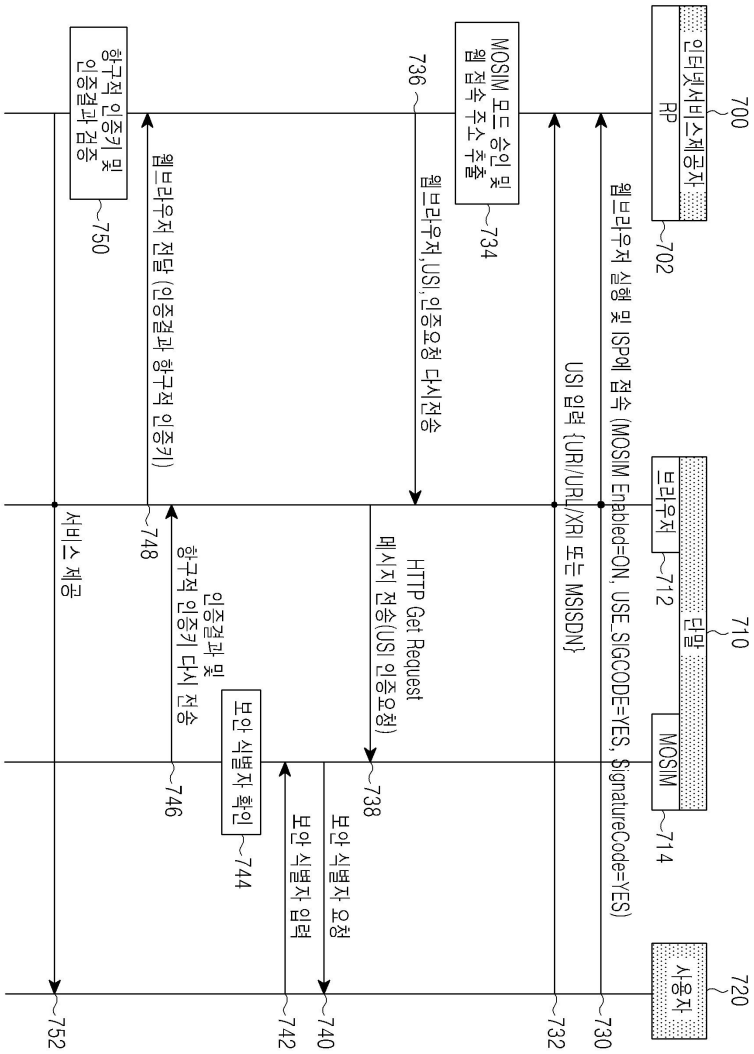
도면6a


HSS/HLR
602
이동통신사업자
BSF
604
OP/NAF
606
600
인터넷서비스제공자
RP
610
612
단말
브라우저/MOSIM
620
622
사용자
630
AKA 알고리즘을 수행결과 확인 및 향구적 인증키 생성
666
사용자 인증을 위한 추가정보 획득
658
652
사용자 인증 시작
650
646
통신링크 설정
MOSIM 모드 승인 및 사용자인증을 대행하는 제3기관 OP주소 추출
644
648
웹브라우저 USI, 인증요청 다시전송
HTTP Get Request 메시지 전송(USI, 인증요청)
HTTPS Response 401 Unauthorized 메시지 전송
654
HTTP Get Request 메시지 전송(USI)
656
401 Unauthorized 메시지 전송
660
Request Authorization Digest 메시지 전송(AKA 알고리즘 수행 결과)
664
AKA 알고리즘을 수행
662
웹브라우저 실행 및 ISP에 접속 (MOSIM Enabled=ON, USE_SIGCODE=YES, SignatureCode=NO)
640
USI 입력
{URI/URL/XRI 또는 MSISDN}
642

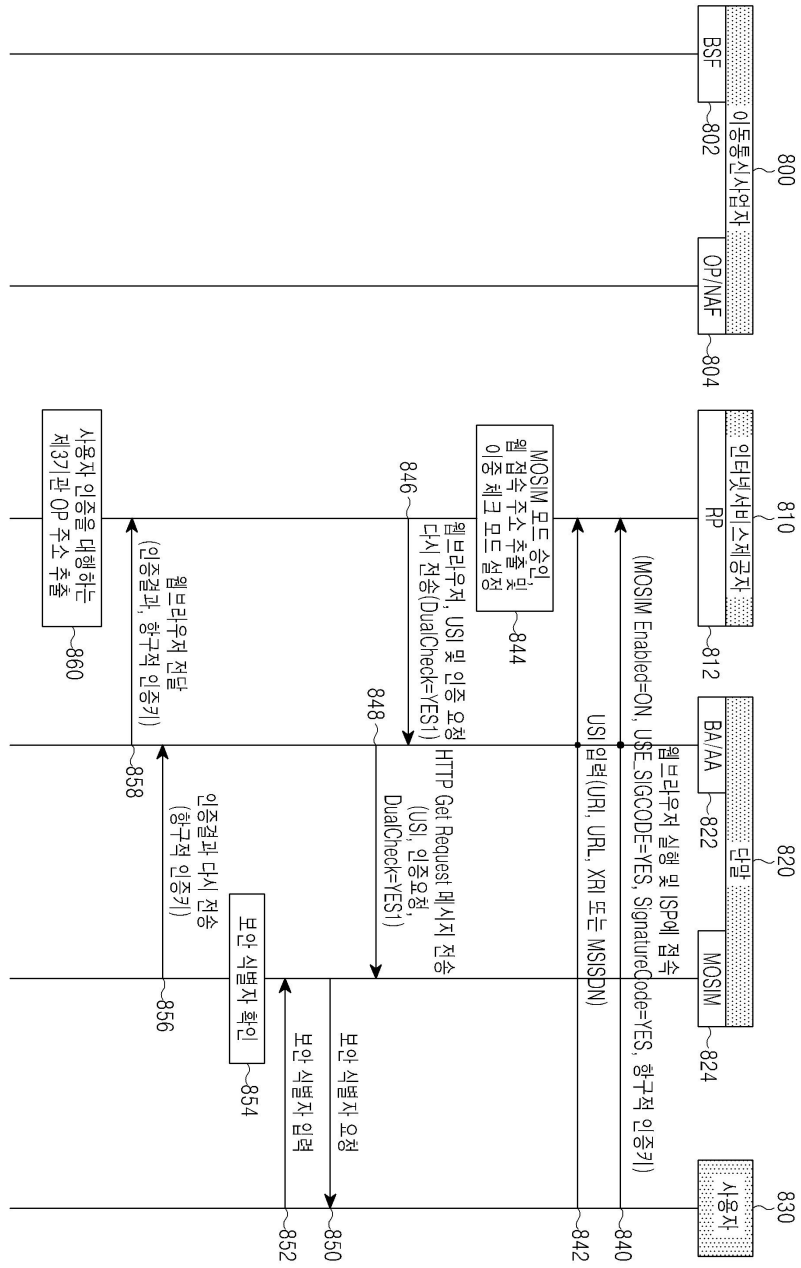
도면6b


HSS/HLR
602
이동통신사업자 (100)
BSF
604
OP/NAF
606
600
인터넷서비스제공자
RP
612
610
브라우저/MOSIM
622
620
단말
사용자
630
668
200 OK 메시지 전송(항구적 인증키 정보)
680
678
인증키 정보 전송
676
결과 인증키 정보 오청
672
항구적 인증키 저장
674
HTTP Get Request 메시지 전송(항구적 인증키 정보)
670
항구적 인증키 저장
웹브라우저 다시 전송(인증결과)
682
인증결과
686
서비스 제공
인증결과검증 및 항구적 인증키 저장
684

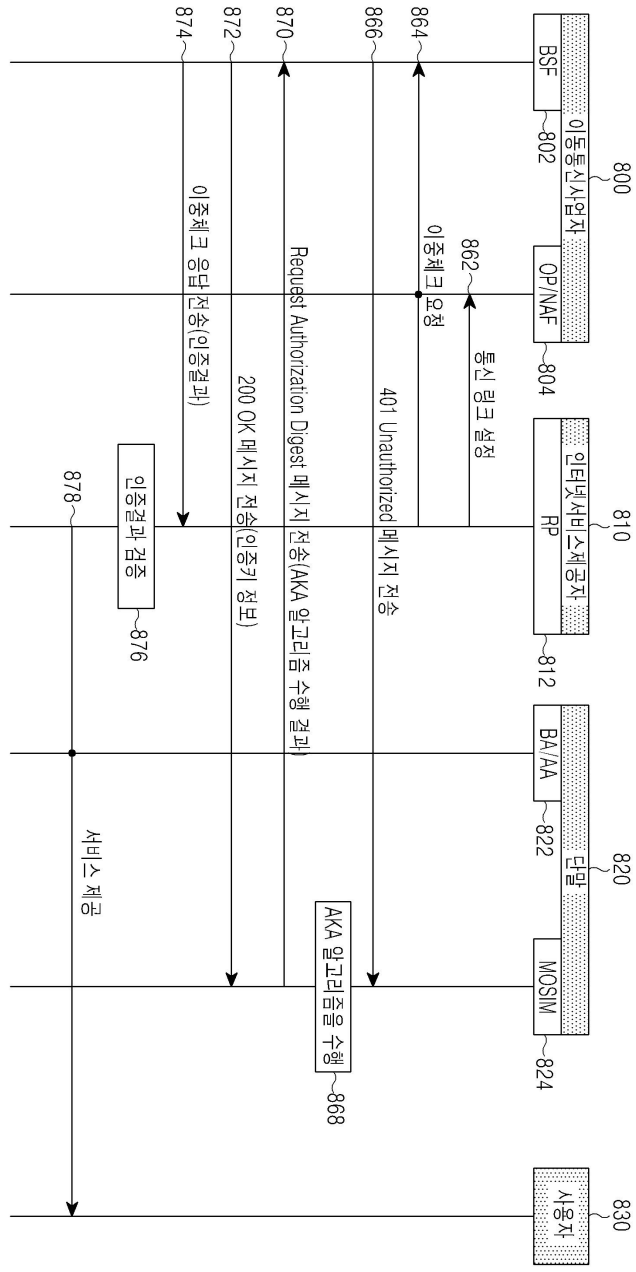
도면7


700
인터넷서비스제공자
RP
702
710
단말
브라우저
712
MOSIM
714
720
사용자
웹브라우저 실행 및 ISP에 접속 (MOSIM Enabled=ON, USE_SIGCODE=YES, SignatureCode=YES)
730
USI 입력 {URI/URL/XRI 또는 MSISDN}
732
736
MOSIM 모드 승인 및 웹 접속 주소 추출
734
웹브라우저,USI,인증요청 다시전송
HTTP Get Request
메시지 전송(USI 인증요청)
738
보안 식별자 요청
740
보안 식별자 입력
742
보안 식별자 확인
744
인증결과 및 항구적 인증키 다시 전송
746
748
웹브라우저 전달 (인증결과 항구적 인증키)
항구적 인증키 및 인증결과 검증
750
서비스 제공
752

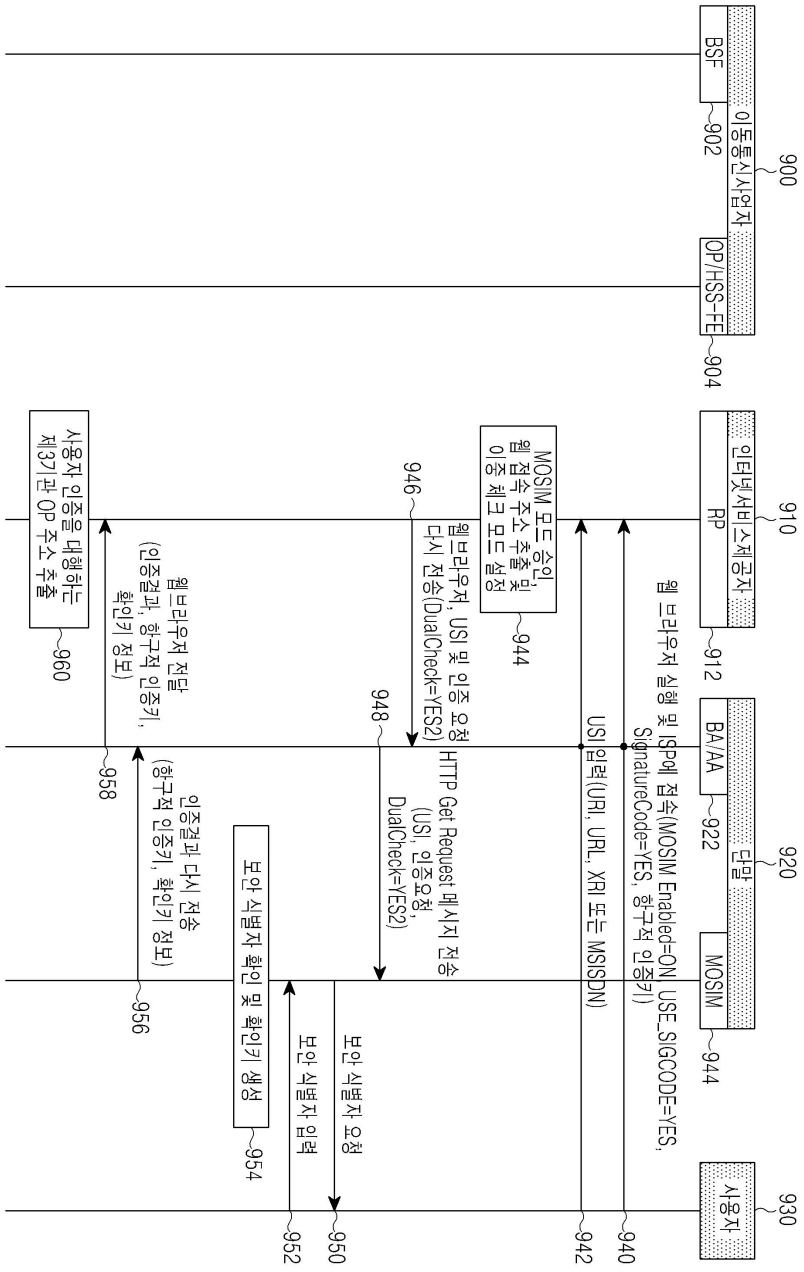
도면8a


800
이동통신사업자
BSF
802
OP/NAF
804
810
인터넷서비스제공자
RP
812
820
단말
BA/AA
822
MOSIM
824
830
사용자
842
840
850
852
854
856
858
860
846
848
844
웹브라우저 실행 및 ISP에 접속
(MOSIM Enabled=ON, USE_SIGCODE=YES, SignatureCode=YES, 항구적 인증키)
USI 입력(URI, URL, XRI 또는 MSISDN)
HTTP Get Request 메시지 전송
(USI, 인증요청,
DualCheck=YES1)
웹브라우저, USI 및 인증 요청
다시 전송(DualCheck=YES1)
MOSIM 모드 승인,
웹 접속 주소 추출 및
이중 체크 모드 설정
보안 식별자 요청
보안 식별자 입력
보안 식별자 확인
인증결과 다시 전송
(항구적 인증키)
웹브라우저 전달
(인증결과, 항구적 인증키)
사용자 인증을 대행하는
제3기관 OP 주소 추출

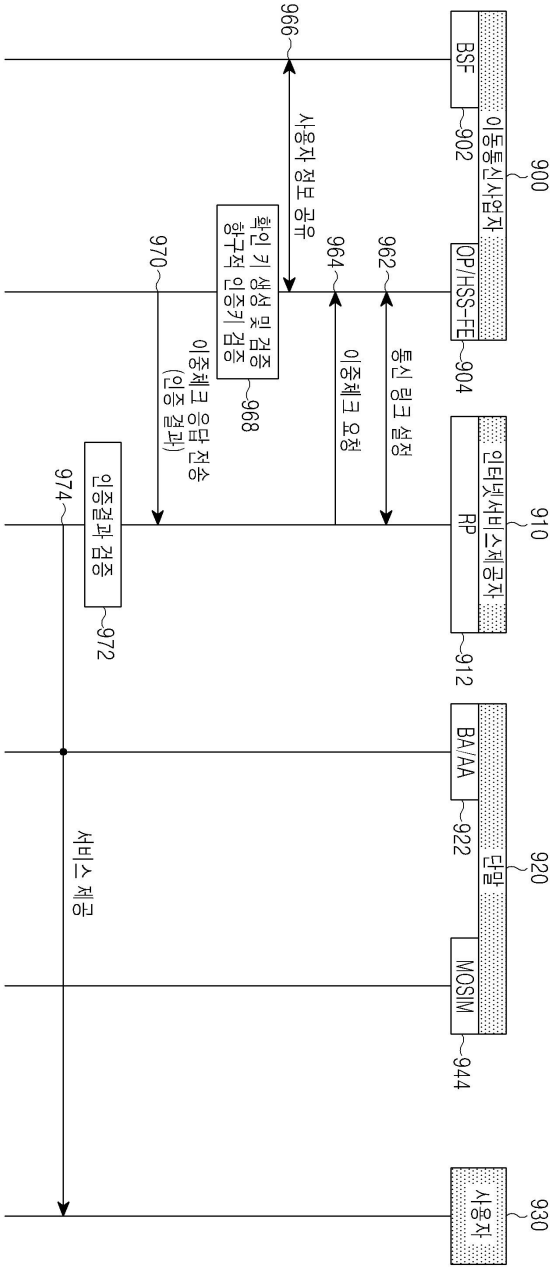
도면8b


800
이동통신사업자
BSF
802
OP/NAF
804
810
인터넷서비스제공자
RP
812
820
단말
BA/AA
822
MOSIM
824
830
사용자
862
이중체크 요청
통신 링크 설정
864
866
401 Unauthorized 메시지 전송
870
Request Authorization Digest 메시지 전송(AKA 알고리즘 수행 결과)
872
200 OK 메시지 전송(인증키 정보)
874
이중체크 응답 전송(인증결과)
876
인증결과 검증
878
868
AKA 알고리즘을 수행
서비스 제공

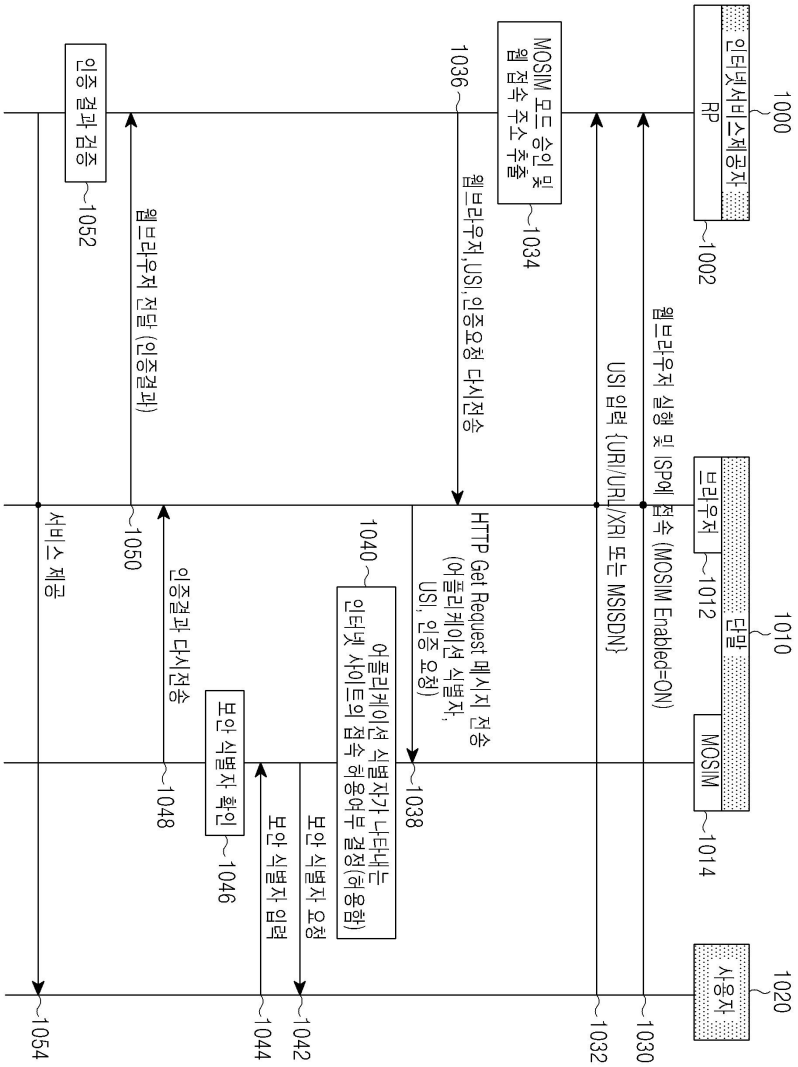
도면9a


900
이동통신사업자
902
BSF
904
OP/HSS-FE
910
인터넷서비스제공자
912
RP
920
단말
922
BA/AA
944
MOSIM
930
사용자
940
웹 브라우저 실행 및 IdP에 접속(MOSIM Enabled=ON, USE_SIGCODE=YES, SignatureCode=YES, 항구적 인증키)
942
USI 입력(URI, URL, XRI 또는 MSISDN)
944
MOSIM 모드 승인, 웹 접속 주소 추출 및 이중 체크 모드 설정
946
웹브라우저, USI 및 인증 요청 다시 전송(DualCheck=YES2)
948
HTTP Get Request 메시지 전송 (USI, 인증요청, DualCheck=YES2)
950
보안 식별자 요청
952
보안 식별자 입력
954
보안 식별자 확인 및 확인키 생성
956
인증결과 다시 전송 (항구적 인증키, 확인키 정보)
958
웹브라우저 전달 (인증결과, 항구적 인증키, 확인키 정보)
960
사용자 인증을 대행하는 제3기관 OP 주소 추출

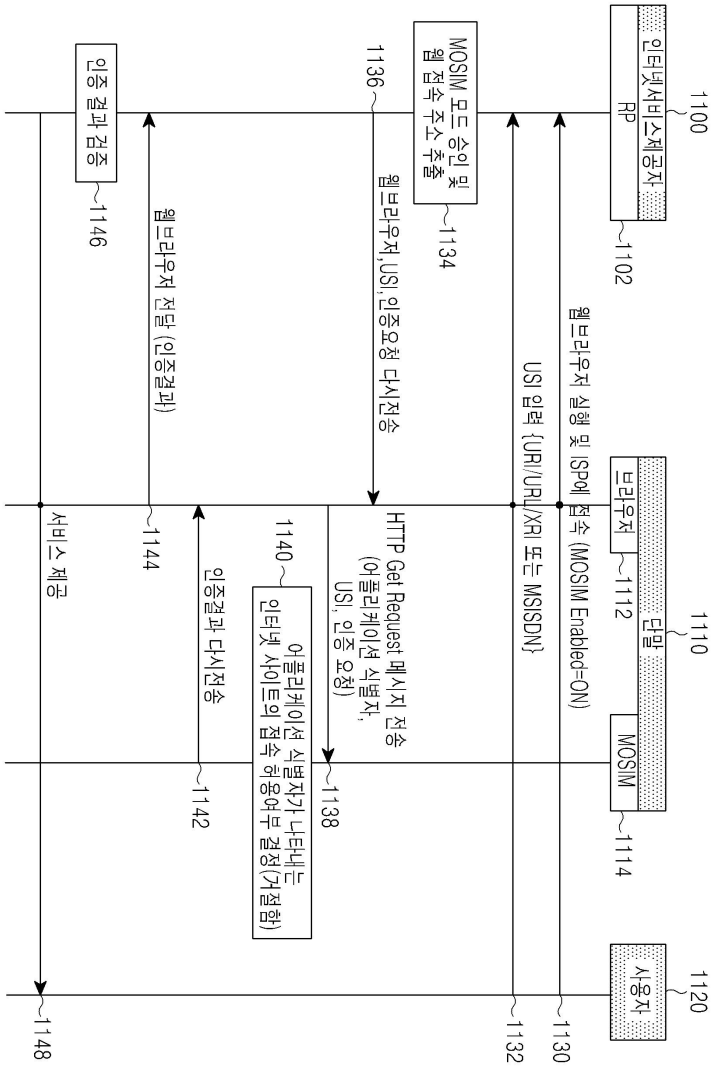
도면9b


900
이동통신사업자
902
BSF
904
OP/HSS-FE
910
인터넷서비스제공자
912
RP
920
단말
922
BA/AA
944
MOSIM
930
사용자
966
사용자 정보 공유
962
통신 링크 설정
964
이중체크 요청
970
확인 키 생성 및 검증
항구적 인증키 검증
968
이중체크 응답 전송
(인증 결과)
974
인증결과 검증
972
서비스 제공

도면10


인터넷서비스제공자
RP
1000
1002
MOSIM 모드 승인 및
웹 접속 주소 추출
1034
1036
인증 결과 검증
1052
단말
1010
브라우저
1012
MOSIM
1014
사용자
1020
웹브라우저 실행 및 ISP에 접속 (MOSIM Enabled=ON)
USI 입력 {URI/URL/XRI 또는 MSISDN}
웹브라우저,USI,인증요청 다시전송
웹브라우저 전달 (인증결과)
HTTP Get Request 메시지 전송
(어플리케이션 식별자,
USI, 인증 요청)
1038
어플리케이션 식별자가 나타내는
인터넷 사이트의 접속 허용여부 결정(허용함)
1040
보안 식별자 요청
보안 식별자 입력
보안 식별자 확인
1046
인증결과 다시전송
1048
1050
서비스 제공
1030
1032
1042
1044
1054

도면11


1100
인터넷서비스제공자
RP
1102
1110
단말
브라우저
1112
MOSIM
1114
1120
사용자
1130
1132
1134
MOSIM 모드 승인 및
웹 접속 주소 추출
1136
웹브라우저,USI,인증요청 다시전송
웹브라우저 실행 및 ISP에 접속 (MOSIM Enabled=ON)
USI 입력 {URI/URL/XRI 또는 MSISDN}
HTTP Get Request 메시지 전송
(어플리케이션 식별자,
USI, 인증 요청)
1138
1140
어플리케이션 식별자가 나타내는
인터넷 사이트의 접속 허용여부 결정(거절함)
1142
인증결과 다시전송
1144
웹브라우저 전달 (인증결과)
인증 결과 검증
1146
서비스 제공
1148