

명세서

발명의 명칭: 트러스트 플랫폼 기반의 개방형 아이디 인증 방법, 이를 위한 장치 및 시스템

기술분야

- [1] 본 발명은 개방형 아이디 인증 방법에 관한 것으로, 더욱 상세하게는 개방형 아이디 인증 시 반복되는 데이터 전송으로 인한 네트워크 과부하를 사전에 방지할 수 있는 트러스트 플랫폼 기반의 개방형 아이디 인증 방법, 이를 위한 장치 및 시스템에 관한 것이다.

배경기술

- [2] 일반적으로 사용자들은 특정 웹 서비스를 이용하기 위해 해당 웹 서비스를 제공하는 웹 서비스 제공 장치로 회원 가입을 통해 자신의 개인 정보를 등록한 후 아이디를 발급 받아 웹 서비스를 이용하게 된다.
- [3] 이때, 사용자들은 자신의 개인 정보, 예컨대 주민등록번호와 같은 개인 정보를 등록한 후 해당 웹 서비스를 이용하게 되는데, 다양한 웹 서비스를 제공하는 다양한 종류의 웹 서비스 제공 장치가 증가함에 따라, 사용자가 관리해야 할 아이디와 비밀번호의 수 또한 증가하고 있어, 사용자 입장에서 아이디 관리에 많은 어려움이 있으며, 보안의 취약한 웹 서비스 제공 장치가 해킹되어 사용자 개인 정보가 노출될 경우 자신의 개인 정보가 악용될 수 있는 불안감에 항상 노출되어 있다.
- [4] 이러한 문제점들을 해결하기 위해 최근 개방형 아이디(Open ID) 기술이 주목받고 있다. 개방형 아이디는 웹을 사용하는 사용자들의 정보를 한 곳에 등록하고, 개방형 아이디 서비스 방식으로 사용자의 로그인을 지원하는 어느 웹 사이트에서도 개방형 아이디를 이용하여 로그인을 가능하게 해주는 서비스를 의미한다.
- [5] 이러한 개방형 아이디 서비스는 웹에서 하나의 아이디와 비밀번호를 가지고 개방형 아이디 서비스 방식으로 로그인을 지원하는 모든 웹 서비스를 별도의 회원가입 없이 이용할 수 있다는 이점이 있으며, 별도의 회원 가입이 필요 없어 개인 정보 유출을 사전에 방지할 수 있다는 장점이 있다.
- [6] 또한, 웹 사이트 입장에서 복잡한 사용자 관리 프로세스를 별도로 구축할 필요 없이 인증된 사용자를 구분하여 차별화된 서비스를 제공할 수 있다는 장점이 있다.
- [7] 이러한, 개방형 아이디 서비스 방식은 하나의 사용자 아이디와 비밀번호로 개방형 아이디 서비스를 지원하는 여러 웹 서비스에 가입 및 인증을 할 수 있다는 장점이 있으나, 사용자 인증 시 사용자 단말과 웹 서비스를 제공하는 웹 서비스 제공 장치, 그리고 개방형 아이디 서비스를 지원하는 개방형 아이디 관리 장치 간의 반복적인 데이터 전송으로 인해 네트워크 과부하가 발생된다는

문제점이 있다.

- [8] 또한, 한정된 무선 자원을 이용하는 무선 통신 환경에서 개방형 아یدی 서비스를 적용하고자 할 경우, 반복적인 데이터 전송으로 인해 많은 무선 자원의 낭비를 초래한다는 문제점이 있다.

발명의 상세한 설명

기술적 과제

- [9] 본 발명은 상기한 종래의 문제점을 해결하기 위해 제안된 것으로서, 특히 개방형 아یدی 인증 시 반복되는 데이터 전송으로 인한 네트워크 과부하를 사전에 방지할 수 있는 트러스트드 플랫폼 기반의 개방형 아یدی 인증 방법, 이를 위한 장치 및 시스템을 제공하는 데 목적이 있다.
- [10] 본 발명의 다른 목적은 개방형 운영체제를 기반으로 동작하는 보안 영역 및 보안 운영체제를 기반으로 동작하는 보안 영역으로 구분되는 격리환경을 구비하는 사용자 단말에서, 개방형 아یدی 관리 장치로부터 사용자 인증에 대한 권한을 위임받아, 사용자 단말의 보안 영역에서 상기 개방형 아یدی에 대한 인증을 수행할 수 있는 트러스트드 플랫폼 기반의 개방형 아یدی 인증 방법, 이를 위한 장치 및 시스템을 제공하는 데 그 목적이 있다.

과제 해결 수단

- [11] 상술한 바와 같은 목적을 달성하기 위한 본 발명의 개방형 아یدی 인증 시스템은 특정 웹 서비스를 제공하며, 개방형 아یدی 관리 장치와의 상호 작용에 따라 개방형 아یدی 서비스 방식으로 사용자 단말의 로그인을 지원하는 웹 서비스 제공 장치 및 개방형 운영체제를 기반으로 동작하는 보안 영역 및 보안용 운영체제를 기반으로 동작하는 보안 영역으로 구분되는 격리환경을 구비하며, 웹 서비스 제공 장치가 제공하는 웹 서비스를 이용하여 위해 사용자 요청에 따라 보안 영역에서 동작하는 웹 브라우저를 통해 웹 서비스 제공 장치가 제공하는 웹 서비스에 접속한 후 웹 브라우저를 통해 입력된 개방형 아یدی를 웹 서비스 제공 장치로 전송한 후 웹 서비스 제공 장치로부터 리다이렉션 메시지가 수신되면, 보안 영역에서 개방형 아یدی에 대응하여 기 저장된 비밀번호를 기초로 사용자 인증을 수행한 후 사용자 인증 성공 메시지를 보안 영역의 웹 브라우저를 통해 웹 서비스 제공 장치로 전송하여 로그인을 수행하는 사용자 단말을 포함하여 구성될 수 있다.

- [12] 상술한 바와 같은 목적을 달성하기 위한 본 발명의 사용자 단말은 통신망을 통해 정보를 송수신하는 통신부 및 개방형 운영체제를 기반으로 동작하는 보안 영역 및 보안용 운영체제를 기반으로 동작하는 보안 영역으로 구분되는 격리환경을 구비하며, 웹 서비스 제공 장치가 제공하는 웹 서비스를 이용하여 위해 사용자 요청에 따라 보안 영역에서 동작하는 웹 브라우저를 통해 웹 서비스 제공 장치가 제공하는 웹 서비스에 접속한 후 웹 브라우저를 통해 입력된 개방형 아یدی를 웹 서비스 제공 장치로 전송한 후 웹 서비스 제공 장치로부터

리다이렉션 메시지가 수신되면, 보안 영역에서 개방형 아이디에 대응하여 기 저장된 비밀번호를 기초로 사용자 인증을 수행한 후 사용자 인증 성공 메시지를 보안 영역의 웹 브라우저를 통해 웹 서비스 제공 장치로 전송하여 로그인을 수행하는 제어부를 포함하여 구성될 수 있다.

[13] 이때, 제어부는 웹 서비스 제공 장치가 제공하는 웹 서비스에 로그인하기 위해 입력된 개방형 아이디 및 사용자 식별 번호를 더 포함하여 웹 서비스 제공 장치로 전송할 수도 있다.

[14] 이때, 리다이렉션 메시지는 개방형 아이디 관리 장치 주소 정보 및 개방형 아이디가 개방형 아이디 관리 장치로부터 발급된 아이디임을 나타내는 개방형 아이디 인증 정보 또는 개방형 아이디 관리 장치를 대신하여 사용자 인증을 수행해도 된다는 사용자 인증 권한 위임 정보 중 적어도 어느 하나로 구성되는 인증정보를 포함하여 구성될 수 있다.

[15] 또한, 제어부는 보안 영역에서 개방형 아이디에 대응하여 기 저장된 비밀번호가 존재하는 경우, 사용자 식별 번호를 이용하여 비밀번호를 복호화하여 사용자 인증을 수행할 수 있다.

[16] 또한, 제어부는 보안 영역에서 개방형 아이디에 대응하여 기 저장된 비밀번호가 존재하지 않는 경우, 개방형 아이디 관리 장치의 주소 정보에 대응하는 개방형 아이디 관리 장치로 사용자 인증을 요청한 후, 개방형 아이디 관리 장치의 요청에 따라 사용자로부터 입력된 비밀번호를 개방형 아이디 관리 장치로 전송한 후, 개방형 아이디 관리 장치로부터 사용자 인증 성공 메시지가 수신되면, 입력된 비밀번호를 보안 영역에서 사용자 식별 번호를 이용하여 암호화한 후 저장할 수도 있다.

[17] 상술한 바와 같은 목적을 달성하기 위한 본 발명의 웹 서비스 제공 장치는 개방형 아이디 서비스를 지원하는 개방형 아이디 관리 장치 및 개방형 운영체제를 기반으로 동작하는 보안 영역 및 보안 응용 운영체제를 기반으로 동작하는 보안 영역으로 구분되는 격리환경을 구비하는 적어도 어느 하나의 사용자 단말과 정보를 송수신하는 서비스 통신부; 및 어느 하나의 사용자 단말의 보안 영역으로부터 개방형 아이디가 수신되면, 개방형 아이디를 기초로 개방형 아이디 관리 장치의 주소 정보를 확인하여 개방형 아이디 관리 장치로 개방형 아이디에 대한 인증을 질의하며, 개방형 아이디 관리 장치로부터 인증 결과에 따른 인증 정보가 수신되면, 인증 정보 및 개방형 아이디 관리 장치의 주소 정보를 포함하는 리다이렉션 메시지를 사용자 단말의 보안 영역으로 전송하고, 사용자 단말의 보안 영역으로부터 사용자 인증 성공 메시지가 수신되면, 사용자 단말의 로그인을 허용하는 서비스 제어부를 포함하여 구성될 수 있다.

[18] 상술한 바와 같은 목적을 달성하기 위한 본 발명의 개선된 보안 기능 기반의 개방형 아이디 인증 방법은 사용자 단말이 보안 영역에서 동작하는 웹 브라우저들 통해 웹 서비스 제공 장치가 제공하는 웹 서비스에 접속한 후 웹

서비스에 로그인하기 위해 웹 브라우저를 통해 입력된 개방형 아이디를 웹 서비스 제공 장치로부터 개방형 아이디 관리 장치 주소 정보 및 개방형 아이디 인증 정보 또는 사용자 인증 권한 위임 정보 중 적어도 어느 하나로 구성되는 인증 정보를 포함하는 리다이렉션 메시지를 수신하는 단계, 사용자 단말이 보안 영역에서 개방형 아이디에 대응하여 기 저장된 비밀번호를 기초로 사용자 인증을 수행하는 단계 및 사용자 인증에 성공하면, 사용자 단말이 비보안 영역의 웹 브라우저를 통해 웹 서비스 제공 장치로 사용자 인증 성공 메시지를 전송하고 웹 서비스에 로그인하는 단계를 포함하여 이뤄질 수 있다.

- [19] 이때, 사용자 단말이 개방형 아이디를 웹 서비스 제공 장치로 전송하는 단계는 사용자 단말의 사용자 식별 번호를 더 포함하여 웹 서비스 제공 장치로 전송할 수도 있다.

- [20] 또한, 사용자 단말이 개방형 아이디를 웹 서비스 제공 장치로 전송하는 단계 이후에, 웹 서비스가 제공 장치가 개방형 아이디를 기초로 개방형 아이디 관리 장치의 주소 정보를 확인하는 단계, 웹 서비스 제공 장치가 확인된 주소 정보에 대응하는 개방형 아이디 관리 장치로 인증을 질의하는 단계 및 웹 서비스 제공 장치가 개방형 아이디 관리 장치로부터 개방형 아이디 인증 정보, 사용자 식별 번호를 기초로 판단되며 개방형 아이디 관리 장치를 대신하여 사용자 인증을 수행해도 된다는 사용자 인증 권한 위임 정보 중 적어도 어느 하나로 구성되는 인증 정보를 수신하는 단계를 포함하여 이뤄질 수도 있다.

- [21] 또한, 리다이렉션 메시지를 수신하는 단계에서, 리다이렉션 메시지에 사용자 인증 권한 위임 정보가 포함되어 있지 않을 경우, 개방형 아이디 관리 장치 주소 정보에 대응하는 개방형 아이디 관리 장치로 사용자 인증을 수행하는 단계를 더 포함하여 이뤄질 수도 있다.

- [22] 또한, 사용자 인증을 수행하는 단계는 사용자 단말이 보안 영역에 개방형 아이디에 대응하는 비밀번호가 존재하는 지 판단하는 단계 및 판단 결과, 개방형 아이디에 대응하는 비밀번호가 존재하는 경우, 사용자 단말이 기 저장된 사용자 식별 번호를 이용하여 비밀번호를 복호화하여 사용자 인증을 수행하는 단계를 포함하여 이뤄질 수 있다.

- [23] 또한, 사용자 인증을 수행하는 단계는 사용자 단말이 보안 영역에 개방형 아이디에 대응하는 비밀번호가 존재하는 지 판단하는 단계, 판단 결과, 개방형 주소 정보에 대응하는 개방형 아이디 관리 장치로 사용자 인증을 요청하는 단계, 개방형 아이디 관리 장치의 요청에 따라 사용자 단말이 사용자로부터 입력된 비밀번호를 개방형 아이디 관리 장치로 전송하는 단계 및 개방형 아이디 관리 장치로부터 사용자 인증 성공 메시지가 수신되면, 사용자 단말이 비밀번호를 개방형 아이디에 대응하여 보안 영역에 사용자 식별 번호를 이용하여 암호화한 후 저장하는 단계를 포함하여 이뤄질 수도 있다.

- [24] 상술한 바와 같은 목적을 달성하기 위한 본 발명의 트러스티드 플랫폼 기반의 개방형 아이디 인증 방법은 웹 서비스 제공 장치가 사용자 단말로부터 수신된 개방형 아이디를 기초로 개방형 아이디 관리 장치의 주소 정보를 확인하는 단계; 웹 서비스 제공 장치가 확인된 주소 정보에 대응하는 개방형 아이디 관리 장치로 개방형 아이디에 대한 인증을 질의하는 단계; 웹 서비스 제공 장치가 개방형 아이디 관리 장치로부터 개방형 아이디 인증 정보, 개방형 아이디 관리 장치를 대신하여 사용자 인증을 수행해도 된다는 사용자 인증 권한 위임 정보 중 적어도 어느 하나로 구성되는 인증 정보를 수신하는 단계; 및 웹 서비스 제공 장치가 인증 정보 및 개방형 아이디 관리 장치의 주소 정보를 포함하는 리다이렉션 메시지를 사용자 단말로 전송하는 단계;를 포함하여 이뤄질 수 있다.
- [25] 더하여, 본 발명은 컴퓨터에 의해 실행되어, 사용자 단말의 비보안 영역에서 동작하는 웹 브라우저를 통해 웹 서비스 제공 장치가 제공하는 웹 서비스에 접속한 후 상기 웹 서비스에 로그인하기 위해 상기 웹 브라우저를 통해 입력된 개방형 아이디를 상기 웹 서비스 제공 장치로 전송하는 단계; 상기 웹 서비스 제공 장치로부터 개방형 아이디 관리 장치 주소 정보 및 개방형 아이디 인증 정보 또는 사용자 인증 권한 위임 정보 중 적어도 어느 하나로 구성되는 인증 정보를 포함하는 리다이렉션 메시지를 수신하는 단계; 상기 보안 영역에서 상기 개방형 아이디에 대응하여 기 저장된 비밀번호를 기초로 사용자 인증을 수행하는 단계; 및 상기 사용자 인증에 성공하면, 상기 비보안 영역의 웹 브라우저를 통해 상기 웹 서비스 제공 장치로 사용자 인증 성공 메시지를 전송하고 상기 웹 서비스에 로그인하는 단계를 실행하는 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체를 제공할 수 있다.

발명의 효과

- [26] 본 발명의 개방형 아이디 인증 방법, 이를 위한 장치 및 시스템에 의하면, 개방형 아이디 인증 시 개방형 아이디 관리 장치로부터 사용자 인증에 대한 권한을 위임 받아 사용자 단말에서 개방형 아이디 인증을 수행함으로써, 개방형 아이디 인증 시 과도한 정보 전송에 따른 네트워크 과부하를 사전에 방지할 수 있다는 장점이 있다.
- [27] 본 발명의 개방형 아이디 인증 방법, 이를 위한 장치 및 시스템에 의하면, 개방형 운영체제를 기반으로 동작하는 비보안 영역 및 보안 운영체제를 기반으로 동작하는 보안 영역으로 구분되는 격리환경을 구비하고 개방형 아이디 관리 장치로부터 사용자 인증에 대한 권한을 위임 받은 사용자 단말에서, 상기의 보안 영역에서 개방형 아이디에 대한 인증을 수행함으로써, 정보 노출의 문제가 없이 안정적으로 개방형 아이디 인증을 수행할 수 있다는 장점이 있다.

도면의 간단한 설명

- [28] 도 1은 본 발명의 실시 예에 따른 트러스티드 플랫폼 기반의 개방형 아이디 인증 시스템의 주요 구성을 도시한 개략적인 구성도이다.

- [29] 도 2는 일반적인 개방형 아이디 인증 방법을 설명하기 위한 데이터 흐름도이다.
- [30] 도 3은 본 발명의 실시 예에 따른 사용자 단말의 주요 구성을 도시한 블록도이다.
- [31] 도 4는 본 발명의 실시 예에 따른 제어부의 구성을 보다 상세히 나타낸 도면이다.
- [32] 도 5는 본 발명의 실시 예에 따른 웹 서비스 제공 장치의 주요 구성을 도시한 블록도이다.
- [33] 도 6은 본 발명의 실시 예에 따른 사용자 단말에서의 개방형 아이디 인증 방법을 설명하기 위한 흐름도이다.
- [34] 도 7은 본 발명의 실시 예에 따른 웹 서비스 제공 장치에서의 개방형 아이디 인증을 위한 리다이렉션 메시지 생성 방법을 설명하기 위한 흐름도이다.
- [35] 도 8은 본 발명의 실시 예에 따른 개방형 아이디 인증 방법을 설명하기 위한 데이터 흐름도이다.

발명의 실시를 위한 형태

- [36] 이하 첨부된 도면을 참조하여 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있는 바람직한 실시예를 상세히 설명한다. 다만, 본 발명의 바람직한 실시예에 대한 동작 원리를 상세하게 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략한다. 이는 불필요한 설명을 생략함으로써 본 발명의 핵심을 흐리지 않고 더욱 명확히 전달하기 위함이다. 또한, 도면 전체에 걸쳐 유사한 기능 및 작용을 하는 부분에 대해서는 동일한 도면 부호를 사용한다.
- [37] 이하, 본 발명의 실시 예에 따른 트러스티드 플랫폼 기반의 개방형 아이디 인증 시스템에 대해 설명한다.
- [38] 도 1은 본 발명의 실시 예에 따른 트러스티드 플랫폼 기반의 개방형 아이디 인증 시스템의 주요 구성을 도시한 개략적인 구성도이다.
- [39] 도 1을 참조하면, 본 발명의 개방형 아이디 인증 시스템은 사용자 단말(10), 웹 서비스 제공 장치(20) 및 개방형 아이디 관리 장치(30)를 포함하여 구성된다.
- [40] 먼저, 웹 서비스 제공 장치(20)는 사용자 단말(10)의 요청에 따라 특정한 웹 서비스, 예컨대 쇼핑, 게임, 영화 제공 등의 서비스를 제공하는 것으로, 특히 본 발명에 따른 웹 서비스 제공 장치(20)는 개방형 아이디 관리 장치(30)와의 상호 작용에 따라 개방형 아이디 서비스 방식으로 사용자 단말(10)의 로그인을 지원하게 된다.
- [41] 개방형 아이디 관리 장치(30)는 개방형 아이디 서비스 방식을 관리하고 지원하는 장치로, 사용자 단말(10)의 요청에 따라 사용자의 프로파일(profile) 정보가 입력되면, 해당 사용자에게 개방형 아이디 서비스를 이용할 수 있는 개방형 아이디를 발급하게 된다.

- [42] 여기서, 개방형 아이디는 한글, 영문 또는 특정한 문자로 구성되며, 3개의 도메인으로 이뤄지는 영문 URL 형태일 수 있으나, 이에 한정되는 것은 아니고 개방형 아이디 관리 장치(30)가 지원하는 형태라면 그 어떠한 형태도 가능하다.
- [43] 상술한 과정에 따라 사용자로부터 개방형 아이디에 대응하는 비밀번호를 포함하는 사용자 프로파일이 입력되면, 개방형 아이디 관리 장치(30)는 사용자 단말(10)로 개방형 아이디, 예컨대 <http://iph1.openid.com>를 발급하고, 이를 발급받아 사용자 단말(10)은 개방형 아이디 관리 장치(30)와의 상호 약속에 따라 개방형 아이디 서비스를 이용하는 웹 사이트에 상기 개방형 아이디를 기초로 로그인을 수행할 수 있게 된다.
- [44] 본 발명의 실시 예에 따른 개방형 아이디 인증 방법을 설명하기에 앞서, 일반적인 개방형 아이디 인증 방법에 대해 도 2를 참조하여 간략하게 설명하도록 한다.
- [45] 도 2는 일반적인 개방형 아이디 인증 방법을 설명하기 위한 데이터 흐름도이다.
- [46] 도 2를 참조하면, 사용자 단말(10)을 이용하여 사용자가 웹 브라우저를 통해 웹 서비스 제공 장치(20)가 제공하는 개방형 아이디 서비스 방식으로 사용자 단말(10)의 로그인을 제공하는 특정 웹 서비스, 예컨대 사이트인 www.skplanet.co.kr로 접속한 후, 로그인을 위해 주소 창에 상기 개방형 아이디 관리 장치(30)로부터 발급받은 개방형 아이디인 URL, 예컨대 <http://iph1.openid.com>을 입력하여 로그인을 시도한다(S101).
- [47] 이후, 웹 서비스 제공 장치(20)는 사용자 단말(10)로부터 입력된 사용자의 개방형 아이디의 URL 주소, 즉 <http://iph1.openid.com>를 기초로 이를 발급한 개방형 아이디 관리 장치(30)의 주소 정보를 확인하게 된다(S103). 개방형 아이디 관리 장치(30)의 주소 정보는 URL 정보를 기초로 확인이 가능하다. 예컨대 상기의 개방형 아이디 URL 정보에서 [opened.com](http://iph1.openid.com)이 개방형 아이디 관리 장치(30)의 도메인이 될 수 있으며, 상기의 도메인 정보에 대응하여 기 저장된 IP 주소 정보를 통해 개방형 아이디 관리 장치(30)의 주소 정보 확인이 가능하다.
- [48] 상술한 과정을 통해 웹 서비스 제공 장치(20)는 개방형 아이디 관리 장치(30)의 주소 정보를 확인한 후 개방형 아이디 관리 장치(30)로 사용자 단말(10)로부터 입력된 개방형 아이디를 전송하고, 이 개방형 아이디가 개방형 아이디 관리 장치(30)가 발급한 정상적인 아이디인지를 질의하게 된다(S105).
- [49] 이후, 개방형 아이디 관리 장치(30)로부터 S105 단계에서의 인증 결과가 수신, 예컨대 사용자 단말(10)로부터 수신된 개방형 아이디는 자신이 발급한 아이디가 맞음을 인증하는 개방형 아이디 인증 정보를 생성하여 웹 서비스 제공 장치(20)로 전송하고, 이를 수신한 웹 서비스 제공 장치(20)는 사용자 단말(10)로 개방형 아이디 관리 장치(30) 주소 정보, 개방형 아이디 인증 정보를 포함하는 리다이렉션(redirection) 메시지를 전송하게 된다(S109).
- [50] 이후, 사용자 단말(10)은 수신된 개방형 아이디 관리 장치(30)의 주소 정보를 기초로 해당되는 개방형 아이디 관리 장치(30)로 개방형 아이디를 전송하여

사용자 인증을 요청하게 된다(S111).

- [51] 이후, 개방형 아이디 관리 장치(30)는 사용자 단말(10)의 웹 브라우저를 통해 개방형 아이디 생성 시에 입력했던 비밀번호를 입력할 수 있는 비밀번호 입력창이 표시되도록 사용자 단말(10)로 요청하고(S113), 사용자 단말(10)은 비밀번호 입력창을 통해 사용자로부터 비밀번호가 입력되면, 사용자로부터 입력된 비밀번호를 개방형 아이디 관리 장치(30)로 전송하고(S115), 개방형 아이디 관리 장치(30)는 이를 기초로 사용자 단말(10)의 사용자 인증을 수행하게 된다(S117).
- [52] 즉, 개방형 아이디 관리 장치(30)는 사용자 단말(10)로부터 수신된 비밀번호가 개방형 아이디 발급 당시 입력된 비밀번호와 일치하는 지를 비교하고, 일치하게 되면 사용자 인증에 성공한 것으로 판단하여(S117) 사용자 인증에 성공하였음을 알리는 사용자 인증 성공 메시지를 생성한 후 사용자 단말(10)로 전송하게 된다(S119).
- [53] 여기서, 상기 사용자 인증 성공 메시지에는 S107 단계에서의 개방형 아이디 인증 정보가 포함될 수 있으며, 사용자 단말(10)은 웹 서비스 제공 장치(20)로 개방형 아이디 인증 정보를 포함하는 사용자 인증 성공 메시지를 전송하고(S121), 웹 서비스 제공 장치(20)는 사용자 인증 성공 메시지에 포함된 개방형 아이디 인증 정보를 확인하여 상기 사용자 단말(10)로부터 입력된 개방형 아이디는 개방형 아이디 관리 장치(30)가 보장하는 인증된 아이디임을 확인한 후 사용자 단말(10)의 로그인을 허용하게 되고(S123), 사용자 단말(10)은 웹 서비스 제공 장치(20)가 제공하는 웹 서비스를 이용할 수 있게 된다.
- [54] 이러한, 일반적인 개방형 아이디 인증 방법의 경우, 개방형 아이디 서비스를 제공하는 웹 사이트에 단일 아이디를 이용해 사용자는 보다 편리하게 로그인을 수행하고, 웹 서비스를 이용할 수 있다는 장점이 있으나, 사용자 단말(10), 웹 서비스 제공 장치(20) 및 개방형 아이디 관리 장치(30)간의 로그인을 위한 반복적인 데이터 전송으로 인해, 네트워크 과부하가 발생될 수 있으며, 특히 한정된 무선 자원을 이용하는 무선 통신 환경에서 이러한 반복적인 데이터 전송은 무선 자원의 낭비로 이어지게 된다.
- [55] 본 발명은 이러한 문제점을 해결하기 위한 것으로, 특히, 개방형 운영체제를 기반으로 동작하는 비보안 영역 및 보안 운영체제를 기반으로 동작하는 보안 영역으로 구분되는 격리환경을 구비하는 사용자 단말(10)에서, 개방형 아이디 관리 장치(30)로부터 사용자 인증에 대한 권한을 위임 받아, 사용자 단말(10)의 보안 영역에서 상기 개방형 아이디에 대한 인증을 수행하고자 하는 것이다.
- [56] 상술한 본 발명의 실시 예에 따른 사용자 단말에서의 개방형 아이디 인증 방법에 대해서는 도 3 내지 도 8을 참조하여 보다 구체적으로 설명하도록 한다.
- [57] 상술한 바와 같은 본 발명의 사용자 단말(10)은 개방형 운영체제를 기반으로 동작하는 비보안 영역 및 보안용 운영체제를 기반으로 동작하는 보안 영역으로 구분되는 격리환경을 구비하며, 통신망(40)을 통해 웹 서비스 제공 장치(20) 및

개방형 아이디 관리 장치(30)와 정보를 송수신할 수 있는 사용자의 정보 처리 단말이다.

- [58] 이러한 사용자 단말(10)은 다양한 형태로 구현될 수 있다. 예를 들어, 스마트폰(smart phone), 태블릿 PC(Tablet PC), PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), MP3 Player 등의 이동 단말기는 물론, 스마트 TV(Smart TV), 데스크탑 컴퓨터 등과 같은 고정 단말기가 사용될 수 있으며 통신 기능을 포함하는 사용자 단말이라면 그 어느 것도 본 발명의 사용자 단말(10)로 적용 가능하다.
- [59] 또한, 본 발명의 실시 예에 따른 통신망(40)은 다양한 형태의 통신망이 이용될 수 있으며, 예컨대, WLAN(Wireless LAN), 와이파이(Wi-Fi), 와이브로(Wibro), 와이맥스(Wimax), HSDPA(High Speed Downlink Packet Access) 등의 무선 통신 방식 또는 이더넷(Ethernet), xDSL(ADSL, VDSL), HFC(Hybrid Fiber Coaxial Ca), FTTC(Fiber to The Curb), FTTH(Fiber To The Home) 등의 유선 통신 방식을 이용할 수 있으며, 상술한 통신 방식 이외에도 기타 널리 공지되었거나 향후 개발될 모든 형태의 통신 방식을 포함할 수 있다.
- [60] 이상으로 본 발명의 실시 예에 따른 개방형 아이디 인증 시스템(100)의 주요 구성에 대해 개략적으로 설명하였다.
- [61] 이하, 본 발명의 실시 예에 따른 사용자 단말의 주요 구성 및 동작 방법에 대해 설명하도록 한다.
- [62] 도 3은 본 발명의 실시 예에 따른 사용자 단말의 주요 구성을 도시한 블록도이다.
- [63] 도 1 및 도 3을 참조하면, 본 발명의 실시 예에 따른 사용자 단말(10)은 통신부(11), 제어부(12), 저장부(13), 입력부(14), 음원 처리부(15), 표시부(16)을 포함하여 구성될 수 있다.
- [64] 본 발명의 실시 예에 따른 사용자 단말(10)은 제어부(12)를 통해 일반적인 개방형 운영체제를 기반으로 동작하는 비보안 영역(130)과 별도의 보안용 운영체제를 기반으로 동작하는 보안 영역(140)으로 구분되는 격리환경이 구현되어 있으며, 상기의 격리환경은 물리적 또는 논리적으로 구현될 수 있다.
- [65] 이러한 환경에서 사용자 단말(10)은 개방형 아이디 서비스를 제공하는 개방형 아이디 관리 장치(30)로부터 사용자 인증에 대한 권한이 위임되면, 개방형 아이디에 대응하여 사용자로부터 입력되는 비밀번호, 또는 개방형 아이디 관리 장치(30)로부터 수신되는 비밀번호를 사용자 식별 번호를 이용하여 암호화한 후 보안 영역에 저장하고, 추후 사용자의 요청에 따라 로그인 시 보안 영역에서 사용자 식별 번호를 기초로 상기 비밀번호를 복호화한 후 복호화가 완료되면 사용자 인증에 성공한 것으로 판단하여 웹 서비스에 로그인할 수 있게 된다.
- [66] 이를 위한 각 구성 요소의 구체적인 동작을 살펴보면 다음과 같다.
- [67] 먼저, 통신부(11)는 통신망(40)을 통해 웹 서비스 제공 장치(20) 및 개방형 아이디 관리 장치(30) 사이의 정보 송수신을 위한 다양한 통신 채널을 형성하기

위해 다양한 형태의 통신 모듈을 포함하여 구현될 수 있다.

[68] 이러한 통신부(11)는 무선 또는 유선 그 어떠한 방식으로든 동작 가능하다.

[69] 제어부(12)는 사용자 단말(10)의 전반적인 제어를 수행하는 것으로 특히 상술한 바와 같이 개방형 운영체제를 기반으로 동작하는 비보안 영역 및 보안용 운영체제를 기반으로 동작하는 보안 영역으로 구분되는 격리환경, 예컨대 트러스티드 플랫폼(trusted platform, 120)을 구비할 수 있다.

[70] 이러한 제어부(12)의 구성에 도 4를 참조하여 보다 구체적으로 설명하도록 한다.

[71] 도 4는 본 발명의 실시 예에 따른 제어부의 구성을 보다 상세히 나타낸 도면이다.

[72] 도 4를 참조하면, 본 발명의 제어부(12)는 비보안 영역(130)과 보안 영역(140) 및 하드웨어 플랫폼(135)을 포함하여 구성될 수 있다

[73] 비보안 영역(130)은 사용자 단말(10)의 사용자 기능 운용 중 암호화된 정보를 필요로 하지 않는 사용자 기능 운용을 위한 개방형 운영체제(OS; Operating System)를 포함할 수 있다. 이러한 비보안 영역(130)은 입력부(14) 또는 터치스크린 기능을 포함하는 표시부(16)로부터 입력되는 입력 신호에 따른 사용자 기능을 운용을 위한 제어를 수행할 수 있다. 예를 들어 비보안 영역(130)은 사용자가 카메라 기능을 활성화하기 위한 입력 신호를 생성하는 경우, 카메라 활성화, 카메라 기반의 이미지 수집 기능, 수집된 이미지의 저장 기능 등을 제어할 수 있으며, 특히 본 발명의 실시 예에 따른 비보안 영역(130)은 웹 서비스 접속을 위한 웹 브라우저 구동 및 웹 브라우저를 통해 특정 웹 서비스에 로그인하기 위해 입력부(14)를 통해 입력되는 다양한 정보를 통신부(11)를 통해 웹 서비스 제공 장치(20) 및 개방형 아이디 관리 장치(30)로 전송될 수 있도록 제어부(12)의 제어 하에 동작하며, 제어부(12)의 제어 하에 수신되는 정보를 보안 영역(140)으로 전달하는 역할을 수행할 수 있다.

[74] 이러한 비보안 영역(130)은 도 4에 도시된 바와 같이, 응용 어플리케이션 레이어(131), TEE 기능 API 레이어(132), TEE 클라이언트 API 레이어(133), 범용 OS 레이어(134)로 구성될 수 있다.

[75] 반면, 보안 영역(140)은 비보안 영역(130)의 호출에 따라 저장된 암호화된 정보를 제어부(12)로 제공하는 역할을 수행한다. 예를 들어 비보안 영역(130)이 음악 파일 재생 기능을 수행하는 과정에서 음악 파일 구매나 음악 파일 사용 권한 획득을 위한 요금 지불 등을 위해 암호화된 정보가 필요한 경우 비보안 영역(130)의 호출에 따라 보안 영역(140)이 호출될 수 있다. 이 과정에서 비보안 영역(130)은 필요로 하는 암호화된 정보에 대한 호출 정보를 보안 영역(140)에 전달할 수 있다. 특히 본 발명의 실시 예에 따른 보안 영역(140)은 비보안 영역(130)을 통해 전달되는 개방형 아이디에 대응하는 비밀번호를 사용자 식별 번호를 기초로 암호화하여 저장한 후, 추후 비보안 영역(130)에서 동작되는 웹 브라우저의 요청에 따라 비보안 영역(130)으로부터 사용자 식별 번호가

전달되면, 보안 영역(140)은 보안 영역(140)에 사용자 식별 번호를 기초로 암호화하여 저장된 비밀번호를 복호화하기 위해, 전달받은 사용자 식별 번호가 암호화에 이용된 사용자 식별 번호인지를 확인하고, 일치하는 경우, 저장된 비밀번호를 복호화한 후 비보안 영역(130)으로 전달한다. 비보안 영역(130)의 웹 브라우저는 보안 영역(140)으로부터 복호화된 비밀번호가 전달되면, 사용자 인증에 성공한 것으로 판단하여, 사용자 인증 성공 메시지를 생성하고, 통신부(11)를 통해 웹 서비스 제공 장치(20)로 사용자 인증 성공 메시지를 전송하게 된다.

- [76] 이러한, 본 발명의 보안 영역(140)은 도 4에 도시된 바와 같이 트러스티드 어플리케이션 레이어(141), TEE 인터널 API 레이어(142), 트러스티드 코어 환경 레이어(143) 및 트러스티드 기능 레이어(144), 하드웨어 보안 리소스 레이어(146)를 포함하여 구성될 수 있다. 여기서 트러스티드 코어 환경 레이어(143), 트러스티드 기능 레이어(144) 및 TEE 인터널 API 레이어(142)는 TEE 커널 레이어(145) 상에 배치되며, 하드웨어 보안 리소스 레이어(146)는 하드웨어 플랫폼(135) 상에 배치될 수 있다.
- [77] 상술한 구성의 트러스티드 플랫폼 기반의 제어부(12)는 TEE 클라이언트 API 레이어(133)가 응용 어플리케이션 레이어(131)를 통하여 특정 사용자 기능 수행 중, 다시 말해 웹 브라우저 구동 중에 보안 영역(140)에 암호화되어 저장된 비밀번호가 요구되는 경우 TEE 기능 API 레이어(132)가 이에 대한 호출을 TEE 클라이언트 API 레이어(133)에 전달한다. 그러면 TEE 클라이언트 API 레이어(133)는 TEE 인터널 API 레이어(142)와의 메시지 송수신을 통하여 보안 기능 운용에 필요한 암호화되어 저장된 비밀번호를 요청한다. 이때, 사용자 식별 번호를 함께 전달하게 된다. 그러면 TEE 인터널 API 레이어(142)가 트러스티드 기능 레이어(144)를 통하여 하드웨어 보안 리소스에 저장된 암호화된 비밀번호를 수집하고, 수집된 암호화된 비밀번호를 비보안 영역(130)으로부터 인가받은 사용자 식별 번호를 기초로 복호화를 진행한다. 이때 비보안 영역(130)으로부터 인가 받은 사용자 식별 번호가 암호화하는데 사용된 사용자 식별 번호와 상이할 경우, TEE 인터널 API 레이어(142)는 다시 TEE 클라이언트 API 레이어(133)로 사용자 인증에 성공하지 못하였음을 알리는 정보를 전송하게 된다.
- [78] 반면, 인가 받은 사용자 식별 번호를 기초로 복호화를 진행하여 복호화에 성공할 경우, TEE 인터널 API 레이어(142)는 복호화된 비밀번호를 TEE 클라이언트 API 레이어(133)로 전송하여 사용자 인증에 성공하였음을 알릴 수 있다.
- [79] 결과적으로 보안 영역(140)에 장착된 트러스티드 플랫폼(120)을 통해서만 접근이 가능한 하드웨어 보안 리소스 레이어(146)에 저장된 암호화된 비밀번호를 비보안 영역(130)에서 호출하면, 비보안 영역(130)으로부터 인가받은 사용자 식별 번호를 기초로 보안 영역(140)에서 복호화한 후 이에 대한

결과를 비보안 영역(130)으로 반환하게 된다.

- [80] 이러한 과정에서 트러스티드 기능 레이어(144)는 암호화된 정보 호출에 대한 신뢰성 확보를 위하여 사전 정의된 사용자 식별 번호를 다시 확인하는 과정을 수행하도록 지원할 수도 있으며, 비보안 영역(130)은 웹 브라우저를 통해 이러한 확인 과정 수행을 지원하기 위한 사용자 식별 번호 입력 화면을 표시부(16)에 출력하도록 지원할 수도 있다.
- [81] 이후 사용자 식별 번호가 정상적으로 보안 영역(140)으로 인가되어 복호화가 완료되면, 복호화된 비밀번호를 비보안 영역(130)에 전달할 수 있다. 또는 보안 영역(140)은 상술한 개방형 아이디 인증을 위한 비밀번호 복호화 과정에 필요한 다양한 기능 수행을 비보안 영역(130)으로부터 일시적으로 위임받고, 통신부(11) 직접 제어를 통하여 웹 서비스 제공 장치(20) 및 개방형 아이디 관리 장치(30)와의 데이터 송수신을 직접 제어할 수도 있다.
- [82] 이하, 본 발명의 실시 예에 따른 제어부(12)의 보다 구체적인 동작 방법에 대해서도 4를 참조하여 설명하였다
- [83] 다시 도 3을 참조하여 나머지 구성 요소인 저장부(13), 입력부(14), 음원 처리부(15), 표시부(16)에 대해 설명하도록 한다.
- [84] 본 발명의 실시 예에 따른 저장부(13)는 사용자 단말(10)의 동작 제어 시 필요한 프로그램과 그 프로그램 수행 중에 발생하는 데이터를 저장한다. 특히 본 발명의 저장부(13)는 웹 서비스 제공 장치(20)가 제공하는 웹 사이트 접속을 위한 웹 브라우저(110)를 저장할 수 있다. 사용자 단말(10)은 웹 브라우저(110) 활성화를 위한 아이콘이나 메뉴 항목을 제공할 수 있으며, 해당 항목 선택 시 웹 브라우저(110)는 제어부(12)에 로드되어 웹 사이트 접속을 위한 다양한 기능 수행을 지원할 수 있다. 특히 웹 브라우저(110)는 본 발명의 개방형 아이디 인증을 위한 개방형 아이디 입력, 비밀번호 입력 등의 인증 과정을 지원하기 위한 정보들의 송수신을 지원할 수 있으며, 웹 브라우저(110)를 통해 송수신되는 다양한 정보들을 일시 또는 영구적으로 저장할 수 있다.
- [85] 또한, 본 발명의 저장부(13)는 사용자 식별 번호를 더 저장할 수도 있다. 여기서 사용자 식별 번호는 사용자 단말(10)을 식별할 수 있는 형태의 정보로, 예컨대, 이동 통신 단말기의 경우 이동통신 사업자로부터 할당된 사용자 고유 번호를 사용자 식별 번호로 이용할 수 있으며, 또는 단말기전화번호(MIN; Mobile Identification Number)를 사용자 식별 번호로 이용할 수도 있다. 또한 네트워크와 연결된 고정 단말기의 경우 IP 주소 정보를 사용자 식별 번호로 이용할 수도 있으며, 사용자 단말(10)을 식별할 수 있는 형태의 정보라면 그 어떠한 것도 본 발명의 사용자 식별 번호로 이용 가능하다.
- [86] 이러한, 저장부(13)는 플래시 메모리(flash memory), 하드디스크(hard disk), 멀티미디어 카드 마이크로(multimedia card micro) 타입의 메모리(예컨대, SD 또는 XD 메모리 등), 램(RAM), 롬(ROM) 등의 저장매체를 포함하여 구성될 수 있다.

- [87] 입력부(14)는 숫자 및 문자 정보 등의 다양한 정보를 입력 받고, 각종 기능을 설정 및 사용자 단말(10)의 기능 제어와 관련하여 입력되는 신호를 제어부(12)로 전달한다. 특히, 본 발명의 입력부(14)는 웹 브라우저 구동을 위한 사용자 입력을 지원하며, 웹 브라우저의 주소 창을 또는 특정 입력 창을 통해 사용자로부터 입력되는 개방형 아이디 또는 비밀번호를 제어부(12)로 전송하는 역할을 수행한다.
- [88] 이러한 입력부(14)는 사용자의 터치 또는 조작에 따른 입력 신호를 발생하는 키패드와 터치패드 중 적어도 하나를 포함하여 구성될 수 있다. 이때, 입력부(14)는 후술할 표시부(16)와 함께 하나의 터치패널(또는 터치스크린)의 형태로 구성되어 입력과 표시 기능을 동시에 수행할 수 있다. 또한, 입력부(14)는 키보드나 키패드와 같은 키 입력 수단, 터치센서나 터치 패드와 같은 터치 입력 수단, 자이로 센서, 지자기 센서, 가속도 센서와 근접 센서, 그리고 카메라 중 적어도 하나 이상을 포함하여 이루어지는 제스처 입력 수단 또는 음성 입력 수단 중 하나 이상을 포함할 수 있다. 이 외에도 현재 개발 중이거나 향후 개발될 수 있는 모든 형태의 입력 수단이 포함될 수 있다.
- [89] 음원 처리부(15)는 전기적인 신호인 음원을 아날로그 신호로 변환하여 외부로 출력하는 것으로, 본 발명의 실시 예에 따른 음원 처리부(15)는 사용자 인증에 성공하지 못하면, 이에 대한 특정 음원을 출력하는 기능을 수행할 수도 있다.
- [90] 표시부(16)는 사용자 단말(10)의 기능 수행 중에 발생하는 일련의 동작상태 및 동작결과 등에 대한 정보를 표시한다. 특히, 본 발명의 실시 예에 따른 표시부(16)는 웹 브라우저를 통해 제공되는 다양한 정보들을 표시하거나 개방형 아이디 및 이에 대응하는 비밀번호 입력을 위한 화면을 표시할 수도 있다. 표시부(16)은 LCD(Liquid Crystal Display), TFT-LCD(Thin Film Transistor LCD), OLED(Organic Light Emitting Diodes), 발광다이오드(LED), AMOLED(Active Matrix Organic LED), 플렉시블 디스플레이(Flexible display) 및 3차원 디스플레이(3 Dimension) 등으로 구성될 수 있다.
- [91] 이상으로 본 발명의 실시 예에 따른 사용자 단말(10)의 주요 구성요소에 대해 설명하였다. 그러나 도 3을 통해 도시된 구성요소가 모두 필수 구성요소인 것은 아니며, 도시된 구성요소보다 많은 구성 요소에 의해 사용자 단말(10)이 구현될 수도 있고, 그 보다 적은 구성요소에 의해서 사용자 단말(10)이 구현될 수도 있다.
- [92] 이하, 본 발명의 실시 예에 따른 웹 서비스 제공 장치(20)의 주요 구성 및 동작 방법에 대해 설명하도록 한다.
- [93] 도 5는 본 발명의 실시 예에 따른 웹 서비스 제공 장치의 주요 구성을 도시한 블록도이다.
- [94] 도 1 및 도 5를 참조하면, 본 발명의 실시 예에 따른 웹 서비스 제공 장치(20)는 서비스 통신부(21), 서비스 제어부(22) 및 서비스 저장부(23)를 포함하여 구성될 수 있다.
- [95] 서비스 통신부(21)는 개방형 아이디 서비스를 지원하는 개방형 아이디 관리

장치(30) 및 적어도 어느 하나의 사용자 단말(10)과 정보를 송수신하는 것으로, 이때의 서비스 통신부(21)는 사용자 단말(10)의 통신부를 통해 개방형 운영체제를 기반으로 동작하는 비보안 영역과 정보를 송수신하게 된다.

- [96] 일반적으로, 사용자 단말(10)은 개방형 운영체제를 기반으로 동작하게 되나, 본 발명의 실시 예에 따른 사용자 단말(10)은 개방형 운영체제를 기반으로 동작하는 영역, 즉 비보안 영역 이외에 별도의 보안용 운영체제를 기반으로 동작하는 영역, 즉 보안 영역으로 구분되는 격리환경을 구비하며, 사용자 단말(10)의 비보안 영역의 정보를 서비스 통신부(21)가 수신하여, 후술할 서비스 제어부(22)로 전달하는 역할을 수행하게 된다.
- [97] 서비스 제어부(22)는 사용자 단말(10)로 특정 웹 서비스, 예컨대, 게임, 뉴스, 영화, 포털 등 웹을 통해 특정 서비스를 사용자 단말(10)로 제공하는 전반적인 과정을 제어하는 것으로, 웹 서비스를 이용하기 위한 사용자 단말(10)의 로그인 전반을 제어할 수도 있다.
- [98] 보다 구체적으로 본 발명의 서비스 제어부(22)는 개방형 아이디 관리 장치(30)가 지원하는 개방형 아이디 서비스를 이용하여 사용자 단말(10)의 로그인 전반을 제어하게 되는 데, 즉, 사용자 단말(10)의 비보안 영역에서 동작하는 웹 브라우저로부터 사용자 단말(10)을 통해 사용자로부터 입력된 개방형 아이디가 수신되면, 수신된 개방형 아이디를 기초로 개방형 아이디를 발급한 개방형 아이디 관리 장치(30)의 주소 정보를 확인하게 된다.
- [99] 예컨대, 사용자 단말(10)의 비보안 영역에서 동작하는 웹 브라우저로부터 수신된 사용자의 개방형 아이디가 <http://iph1.openid.com>일 경우, iph1은 사용자의 개방형 아이디 식별 정보, openid.com은 상기의 개방형 아이디를 발급한 개방형 아이디 관리 장치(30)의 도메인 정보가 될 수 있다.
- [100] 따라서, 수신되는 개방형 아이디를 기초로 개방형 아이디 관리 장치(30)의 도메인 정보를 확인하고, 기 저장된 상기 도메인 정보에 대응하는 개방형 아이디 관리 장치(30)의 IP 주소 정보를 확인하여, 해당되는 개방형 아이디 관리 장치(30)로 사용자 단말(10)로부터 수신된 개방형 아이디에 대한 인증을 질의하게 된다.
- [101] 즉, 서비스 제어부(22)는 사용자 단말(10)로부터 수신된 개방형 아이디가 실제 개방형 아이디 관리 장치(30)가 발급한 정상적인 개방형 아이디인지를 질의하고, 여기에 더하여, 사용자 단말(10)로부터 개방형 아이디와 함께 수신된 사용자 식별 번호를 기초로, 사용자 인증에 대한 권한 위임 정보가 존재하는 지 질의할 수도 있다.
- [102] 질의 결과, 서비스 제어부(22)는 개방형 아이디 관리 장치(30)로부터 인증 결과가 수신되면, 수신된 인증 결과 및 개방형 아이디 관리 장치(30)의 주소 정보를 포함하는 리다이렉션 메시지를 서비스 통신부(21)를 통해 사용자 단말(10)로 전송하게 된다.
- [103] 이후, 사용자 단말(10)의 비보안 영역에서 동작하는 웹 브라우저로부터 사용자

인증 성공 메시지가 수신되면, 서비스 제어부(22)는 사용자 단말(10)의 로그인을 허용하게 된다.

- [104] 이를 위해, 웹 서비스 제공 장치(20)는 웹 서비스 제공 장치(20)가 제공하는 웹 서비스에 대한 콘텐츠를 저장하고 있는 서비스 저장부(23)를 포함하여 구성될 수 있다.
- [105] 서비스 저장부(23)는 사용자 단말(10)로 웹 서비스를 제공하기 위한 전반적인 정보를 저장하고 관리하며, 특히 본 발명의 실시 예에 따른 서비스 저장부(23)는 개방형 아이디 관리 장치(30)의 주소 정보를 도메인 정보에 대응하여 저장하게 된다.
- [106] 상술한 바와 같이, 본 발명의 웹 서비스 제공 장치(20)는 서비스 저장부(23)에 사용자 단말(10)의 사용자 인증에 필요한 정보 대신 개방형 아이디 관리 장치(30)에 대한 정보만을 저장하고 관리하므로, 시스템 구축이 보다 용이하고, 사용자 인증 성공 메시지가 수신된 사용자 단말(10)의 로그인만을 지원하므로, 보안에 대한 위협 없이 안정적으로 사용자 단말(10)의 로그인을 지원할 수 있게 된다.
- [107] 상술한 본 발명의 웹 서비스 제공 장치(20)와 여기에 더하여 개방형 아이디 관리 장치(30)는 서버 기반 컴퓨팅 방식 또는 클라우드 방식으로 동작하는 하나 이상의 서버로 구현될 수 있다. 특히, 본 발명의 실시 예에 따른 개방형 아이디 인증 시스템을 통해 송수신되는 정보는 인터넷 상의 클라우드 컴퓨팅 장치에 영구적으로 저장될 수 있는 클라우드 컴퓨팅(Cloud Computing) 기능을 통해 제공될 수 있다. 여기서, 클라우드 컴퓨팅은 데스크톱, 태블릿 컴퓨터, 노트북, 넷북 및 스마트폰 등의 디지털 단말기에 인터넷 기술을 활용하여 가상화된 IT(Information Technology) 자원, 예를 들어, 하드웨어(서버, 스토리지, 네트워크 등), 소프트웨어(데이터베이스, 보안, 웹 서버 등), 서비스, 데이터 등을 온 디맨드(On demand) 방식으로 서비스하는 기술을 의미한다. 본 발명에 있어서, 사용자 단말(10), 웹 서비스 제공 장치(20) 및 개방형 아이디 관리 장치(30) 사이에 송수신되는 모든 정보는 인터넷 상의 클라우드 컴퓨팅 장치에 저장되고, 언제 어디서든 전송될 수 있다.
- [108] 이하, 본 발명의 실시 예에 따른 개방형 아이디 인증 방법에 대해 보다 구체적으로 설명하도록 한다.
- [109] 도 6은 본 발명의 실시 예에 따른 사용자 단말에서의 개방형 아이디 인증 방법을 설명하기 위한 흐름도이다.
- [110] 도 1 및 도 6을 참조하면, 먼저, 사용자 단말(10)의 비보안 영역에서 구동되는 웹 브라우저를 통해 웹 서비스 제공 장치(20)가 제공하는 웹 서비스에 접속한 후 웹 서비스에 로그인하기 위해 사용자로부터 개방형 아이디가 입력되면, 입력된 개방형 아이디를 웹 서비스 제공 장치로 전송하게 된다(S301).
- [111] 이후, 웹 서비스 제공 장치(20)로부터 인증 결과를 포함하는 리다이렉션 메시지를 수신하게 된다(S303).

- [112] 여기서, 인증 결과는 사용자가 입력한 개방형 아이디가 정상적으로 발행된 아이디인지에 대한 개방형 아이디 인증 정보 및 개방형 아이디 관리 장치(30)를 대신하여 사용자 인증을 수행해도 된다는 사용자 인증 권한 위임 정보로 구성되는 인증 정보를 의미하며, 비보안 영역에서 동작하는 웹 브라우저는 이러한 인증 정보와 개방형 아이디 관리 장치(30)의 주소 정보를 포함하는 리다이렉션 메시지를 수신하게 된다.
- [113] 이후, 웹 브라우저는 수신된 리다이렉션 메시지에 사용자 인증 권한 위임 정보가 존재하는 지 판단하여(S305), 그렇지 않을 경우, 주소 정보에 대응하는 개방형 아이디 관리 장치(30)로 사용자 인증을 요청하게 되고(S307), 사용자 인증 권한 위임 정보가 존재하는 경우, 비보안 영역에서 동작하는 웹 브라우저는 보안 영역으로 사용자 인증을 요청하게 된다(S309).
- [114] 이후, 보안 영역에서 사용자 인증을 수행하는 별도의 API를 통해, 예컨대 도 4를 참조하여 설명한 바와 같이, TEE 인터널 API(142)가 개방형 아이디에 대응하여 사용자 식별 번호를 기초로 암호화된 비밀번호가 존재하는 지 확인하여, 존재할 경우, 사용자 식별 번호를 이용하여 암호화된 비밀번호를 복호화하게 된다(S309).
- [115] 보안 영역의 TEE 인터널 API(142)는 복호화 과정이 정상적으로 수행되면, 비보안 영역에서 동작하는 웹 브라우저로 사용자 인증 성공 메시지를 전송(S313)하고, 비보안 영역의 웹 브라우저는 이를 웹 서비스 제공 장치(20)로 전송하여 로그인을 수행하게 된다.
- [116] 이하, 본 발명의 실시 예에 따른 웹 서비스 제공 장치(20)의 동작 방법에 대해 도 7을 참조하여 보다 구체적으로 설명하도록 한다.
- [117] 도 7은 본 발명의 실시 예에 따른 웹 서비스 제공 장치에서의 개방형 아이디 인증을 위한 리다이렉션 메시지 생성 방법을 설명하기 위한 흐름도이다.
- [118] 도 1 및 도 7을 참조하면, 웹 서비스 제공 장치(20)는 사용자 단말(10)로부터 개방형 아이디가 수신되면(S401), 수신된 개방형 아이디를 기초로 개방형 아이디 관리 장치(30)의 주소 정보를 확인하게 된다(S403).
- [119] 이후, 확인된 주소 정보에 대응하는 개방형 아이디 관리 장치(30)로 개방형 아이디에 대한 인증을 질의하고(S405), 개방형 아이디 관리 장치(30)로부터 인증 결과가 수신되면(S407), 사용자 단말로 인증 결과를 포함하는 리다이렉션 메시지를 전송하게 된다(S409).
- [120] 여기서, 인증 결과는 사용자 단말(10)로부터 수신된 개방형 아이디가 개방형 아이디 관리 장치(30)로부터 정상적으로 발급된 아이디인지를 나타내는 개방형 아이디 인증 정보 및 개방형 아이디 관리 장치(30)를 대신하여 사용자 인증을 수행해도 된다는 사용자 인증 권한 위임 정보를 포함하는 인증 정보로, 웹 서비스 제공 장치(20)는 개방형 아이디 관리 장치(30)로부터 상기의 인증 정보가 수신되면, 수신된 인증 정보와 더불어 S403 단계에서 확인된 개방형 아이디 관리 장치(30)의 주소 정보를 포함하는 리다이렉션 메시지를 생성하여 사용자

단말(10)로 전송한다.

- [121] 이때, S407 단계에서 정상적으로 인증 결과가 수신되지 않을 경우, 사용자 단말(10)로 인증에 실패하였다는 메시지를 더 전송할 수도 있다.
- [122] 이하, 본 발명의 실시 예에 따른 개방형 아이디 인증 방법에 대해 보다 구체적으로 설명하도록 한다.
- [123] 도 8는 본 발명의 실시 예에 따른 개방형 아이디 인증 방법을 설명하기 위한 데이터 흐름도이다.
- [124] 도 8을 참조하면, 먼저, 사용자 단말(10)의 비보안 영역(130)에서 구동되는 웹 브라우저를 통해 웹 서비스 제공 장치(20)가 제공하는 웹 서비스에 접속한 후 웹 서비스에 로그인하기 위해 웹 브라우저를 통해 사용자로부터 개방형 아이디가 입력되면, 입력된 개방형 아이디를 웹 서비스 제공 장치(20)로 전송하게 된다(S201).
- [125] 예컨대, 웹 서비스 제공 장치(20)가 제공하는 특정 웹 서비스를 이용하기 위해 이를 위한 웹 사이트인 www.skplanet.co.kr에 속한 후, 로그인을 위해 웹 브라우저 주소 창에 상기 개방형 아이디 관리 장치(30)로부터 미리 발급받은 개방형 아이디, 예컨대 <http://iph1.openid.com>을 입력하여 로그인을 시도한다(S201).
- [126] 이후, 웹 서비스 제공 장치(20)는 사용자 단말(10)로부터 입력된 사용자의 URL, 즉 <http://iph1.openid.com> 상기의 아이디를 발급한 개방형 아이디 관리 장치(30)의 주소 정보를 확인하게 된다(S203). 개방형 아이디 관리 장치(30)의 주소 정보는 URL 정보를 기초로 확인이 가능하다. 예컨대 상기의 개방형 아이디 URL 정보에서 opened.com이 개방형 아이디 관리 장치(30)의 도메인이 될 수 있으며, 상기의 도메인 정보에 대응하여 기 저장된 IP 주소 정보를 통해 개방형 아이디 관리 장치(30)의 주소 정보 확인이 가능하다.
- [127] 상술한 과정을 통해 웹 서비스 제공 장치(20)는 개방형 아이디 관리 장치(30)의 주소 정보를 확인한 후 개방형 아이디 관리 장치(30)로 사용자 단말(10)로부터 입력된 개방형 아이디를 전송하고, 이 개방형 아이디가 개방형 아이디 관리 장치(30)가 발급한 정상적인 아이디인지를 질의하게 된다(S205).
- [128] 이후, 개방형 아이디 관리 장치(30)로부터 S205 단계에서의 인증 결과가 수신, 예컨대 사용자 단말(10)로부터 수신된 개방형 아이디는 자신이 발급한 아이디가 맞음을 인증하는 개방형 아이디 인증 정보를 생성하여 웹 서비스 제공 장치(20)로 전송하게 된다(S207).
- [129] 이때, S201 단계에서 사용자 단말(10)은 사용자 식별 번호를 더 포함하여 웹 서비스 제공 장치(20)로 전송할 수 있으며, 웹 서비스 제공 장치(20)는 수신된 사용자 식별 번호를 다시 개방형 아이디 관리 장치(30)로 전송하여, 개방형 아이디 관리 장치(30)가 사용자 식별 번호를 기초로 사용자 단말(10)에 사용자 인증에 대한 권한을 위임할지의 여부를 결정할 수도 있다.
- [130] 예컨대, 사용자 단말(10)이 이동통신 단말의 경우, 이동통신 사업자로부터 할당된 사용자 번호를 사용자 식별 번호로 사용하는 경우, 개방형 아이디 관리

장치(30)는 사용자 식별 번호를 기초로 대응하는 이동통신 사업자의 서비스 장치로 해당 사용자 단말(10)에 대한 보증 여부를 질의할 수도 있다. 이때, 이동통신 사업자의 서비스 장치는 사용자 단말(10)이 트러스티드 플랫폼을 구비한 사용자 단말(10)인지에 대한 정보를 미리 저장하고 있을 수 있으며, 보안이 강화된 트러스티드 플랫폼을 구비한 사용자 단말(10)일 경우 이동통신 사업자 서비스 장치는 사용자 단말(10)을 보증할 수 있다는 정보를 생성하여 개방형 아이디 관리 장치(30)로 전송하고, 개방형 아이디 관리 장치(30)는 웹 서비스 제공 장치(20)를 통해 사용자 단말(10)로 개방형 아이디 관리 장치(30)를 대신하여 사용자 인증을 수행해도 된다는 사용자 인증 권한 위임 정보를 전송할 수도 있다.

- [131] 개방형 아이디 관리 장치(30)는 웹 서비스 제공 장치(20)로 사용자 단말(10)로부터 수신된 개방형 아이디는 자신이 발급한 개방형 아이디임을 인증하는 정보인 개방형 아이디 인증 정보, 상술한 바와 같은 사용자 인증 권한 위임 정보를 전송하고, 이를 수신한 웹 서비스 제공 장치(20)는 수신된 인증 정보와 더불어 개방형 아이디 관리 장치(30)에 대한 주소 정보를 포함하는 리다이렉션 메시지를 사용자 단말(10)의 웹 브라우저로 전송하게 된다(S209).
- [132] 비보안 영역(130)에서 동작하는 웹 브라우저는 수신되는 리다이렉션 메시지에 사용자 인증 권한 위임 정보가 포함되어 있는지 판단하고(S211), 포함되어 있지 않을 경우 수신된 개방형 아이디 관리 장치(30)의 주소 정보에 대응하여 해당되는 개방형 아이디 관리 장치(30)로 사용자 인증을 요청하게 된다(S213). 이후의 동작 과정은 도 2를 참조하여 설명한 바와 동일하다.

- [133] 그러나 S211 단계에서 사용자 인증 권한 위임 정보가 리다이렉션 메시지에 포함될 경우, 비보안 영역(130)에서 동작하는 웹 브라우저는 보안 영역(140)으로 사용자 인증 요청(S215), 즉 암호화된 비밀번호를 호출하게 된다.

- [134] 이후, 보안 영역(140)에서 동작하는 예컨대 그림 4를 참조하여 설명한 바와 같이 TEE 인터넷 API(142)는 웹 브라우저가 호출한 비밀번호가 보안 영역(140)이 관리하는 영역에 저장되어 있는지를 확인하고(S217), 저장되어 있을 경우, 웹 브라우저를 통해 수신된 사용자 식별 번호를 기초로 복호화를 진행하게 된다(S219).

- [135] 여기서, 웹 브라우저를 통해 수신된 사용자 식별 번호와 비밀번호 저장 시 암호화에 이용된 사용자 식별 번호가 일치하지 않을 경우, 사용자 인증에 실패한 것이며, 일치하여 정상적으로 복호화가 이뤄지면 사용자 인증에 성공한 것으로, 사용자 인증 성공 메시지를 비보안 영역(130)의 웹 브라우저로 전송하고(S221), 이를 수신한 비보안 영역(130)의 웹 브라우저는 웹 서비스 제공 장치(20)로 사용자 인증 성공 메시지를 전송하게 된다(S223).

- [136] 이때의 사용자 인증 성공 메시지는 S207 단계에서 수신한 개방형 아이디 인증 정보가 포함되어 있으며, 사용자 단말(10)을 통해 입력된 개방형 아이디는 개방형 아이디 관리 장치(30)가 보장하고 있으므로, 웹 서비스 제공 장치(20)는

보안에 대한 위험 없이 사용자 단말(10)의 웹 서비스 로그인을 허용하게 된다(S225).

- [137] 만일 S217 단계에서 개방형 아이디에 대응하는 비밀번호가 존재하지 않을 경우, 개방형 아이디 관리 장치(30)의 주소 정보에 대응하는 개방형 아이디 관리 장치(30)로 사용자 인증을 요청하고, 개방형 아이디 관리 장치(30)로부터 사용자 인증 성공 메시지가 수신되면, 비보안 영역(130)의 웹 브라우저를 통해 사용자로부터 입력된 비밀번호를 사용자 식별 번호를 이용하여 암호화한 후 보안 영역(140)에 저장할 수 있다.
- [138] 이와 같이, 한 번 보안 영역(140)에 개방형 아이디에 대응하는 비밀번호가 암호화되어 저장되어 있을 경우, 사용자 단말(10)은 웹 서비스 제공 장치(20) 및 개방형 아이디 관리 장치(30)와의 복잡한 정보의 송수신 없이 바로 보안 영역(140)에 저장된 비밀번호를 호출하여 사용자 인증을 수행하게 된다.
- [139] 이처럼, 사용자 단말(10)의 보안 영역(140)을 통해 개방형 아이디를 인증함으로써, 종래의 개방형 아이디 인증 시 반복적인 데이터 전송으로 인한 네트워크 과부하를 사전에 방지할 수 있다는 장점이 있다.
- [140] 또한, 개방형 운영체제를 기반으로 동작하는 비보안 영역(130) 및 보안 운영체제를 기반으로 동작하는 보안 영역(130)으로 구분되는 격리환경을 구비하고 개방형 아이디 관리 장치로부터 사용자 인증에 대한 권한을 위임 받은 사용자 단말(10)을 통해 개방형 아이디에 대한 사용자 인증을 수행함으로써, 사용자 정보 노출의 문제가 없이 안정적으로 개방형 아이디 인증을 수행할 수 있다는 장점이 있다.
- [141] 이상으로 본 발명의 실시 예에 따른 트러스티드 플랫폼 기반의 개방형 아이디 인증 방법에 대해 설명하였다.
- [142] 이러한, 본 발명의 실시 예에 따른 개방형 아이디 인증 방법은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있으며, 컴퓨터 시스템에 의해 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media) 및 롬(ROM, Read Only Memory), 램(RAM, Random Access Memory), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함한다.
- [143] 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고, 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및

코드 세그먼트들은 본 발명이 속하는 기술분야의 프로그래머들에 의해 용이하게 추론될 수 있다.

- [144] 이상으로 본 발명의 기술적 사상을 예시하기 위한 바람직한 실시예와 관련하여 설명하고 도시하였지만, 본 발명은 이와 같이 도시되고 설명된 그대로의 구성 및 작용에만 국한되는 것은 아니며, 기술적 사상의 범주를 이탈함이 본 발명에 대해 다수의 변경 및 수정이 가능함을 당업자들은 잘 이해할 수 있을 것이다. 따라서 그러한 모든 적절한 변경 및 수정과 균등물들도 본 발명의 범위에 속하는 것으로 간주되어야 할 것이다.

산업상 이용가능성

- [145] 본 발명은 개방형 아이디 인증 방법에 관한 것으로, 더욱 상세하게는 개방형 아이디 인증 시 반복되는 데이터 전송으로 인한 네트워크 과부하를 방지할 수 있는 트러스트드 플랫폼 기반의 개방형 아이디 인증 방법, 이를 위한 장치 및 시스템에 관한 것이다.

- [146] 본 발명에 개방형 아이디 인증 방법, 이를 위한 장치 및 시스템에 의하면, 개방형 운영체제를 기반으로 동작하는 비보안 영역 및 보안 운영체제를 기반으로 동작하는 보안 영역으로 구분되는 격리환경을 구비하고 개방형 아이디 관리 장치로부터 사용자 인증에 대한 권한을 위임 받은 사용자 단말의 보안 영역에서 개방형 아이디에 대한 인증을 수행함으로써, 정보 누출의 문제가 없이 안정적으로 개방형 아이디 인증을 수행할 수 있다는 장점이 있으며, 이를 통해 보안 산업 및 웹 서비스 산업 발전에 이바지할 수 있다는 산업상 이용가능성이 존재한다.

청구범위

[청구항 1]

특정 웹 서비스를 제공하며, 개방형 아이디 관리 장치와의 상호 약속에 따라 개방형 아이디 서비스 방식으로 사용자 단말의 로그인을 지원하는 웹 서비스 제공 장치; 및
 개방형 운영체제를 기반으로 동작하는 비보안 영역 및 보안용 운영체제를 기반으로 동작하는 보안 영역으로 구분되는 격리환경을 구비하며, 상기 웹 서비스 제공 장치가 제공하는 웹 서비스를 이용하기 위해 사용자 요청에 따라 비보안 영역에서 동작하는 웹 브라우저를 통해 웹 서비스 제공 장치가 제공하는 웹 서비스에 접속한 후 상기 웹 브라우저를 통해 입력된 개방형 아이디를 상기 웹 서비스 제공 장치로 전송한 후 상기 웹 서비스 제공 장치로부터 리다이렉션 메시지가 수신되면, 상기 보안 영역에서 상기 개방형 아이디에 대응하여 기 저장된 비밀번호를 기초로 사용자 인증을 수행한 후 사용자 인증 성공 메시지를 상기 비보안 영역의 웹 브라우저를 통해 상기 웹 서비스 제공 장치로 전송하여 로그인을 수행하는 사용자 단말;

[청구항 2]

을 포함하는 것을 특징으로 하는 개방형 아이디 인증 시스템.
 통신망을 통해 정보를 송수신하는 통신부; 및
 개방형 운영체제를 기반으로 동작하는 비보안 영역 및 보안용 운영체제를 기반으로 동작하는 보안 영역으로 구분되는 격리환경을 구비하며, 상기 웹 서비스 제공 장치가 제공하는 웹 서비스를 이용하기 위해 사용자 요청에 따라 비보안 영역에서 동작하는 웹 브라우저를 통해 웹 서비스 제공 장치가 제공하는 웹 서비스에 접속한 후 상기 웹 브라우저를 통해 입력된 개방형 아이디를 상기 웹 서비스 제공 장치로 전송한 후 상기 웹 서비스 제공 장치로부터 리다이렉션 메시지가 수신되면, 상기 보안 영역에서 상기 개방형 아이디에 대응하여 기 저장된 비밀번호를 기초로 사용자 인증을 수행한 후 사용자 인증 성공 메시지를 상기 비보안 영역의 웹 브라우저를 통해 상기 웹 서비스 제공 장치로 전송하여 로그인을 수행하는 제어부;

[청구항 3]

상기 제어부는
 상기 웹 서비스 제공 장치가 제공하는 웹 서비스에 로그인하기 위해 입력된 상기 개방형 아이디 및 사용자 식별 번호를 더 포함하여 상기 웹 서비스 제공 장치로 전송하는 것을 특징으로 하는 사용자 단말.

[청구항 4]

제 2항에 있어서,
 상기 리더이택션 메시지는
 상기 개방형 아이디 관리 장치 주소 정보 및 개방형 아이디가 상기
 개방형 아이디 관리 장치로부터 발급된 아이디임을 나타내는
 개방형 아이디 인증 정보 또는 상기 개방형 아이디 관리를
 대신하여 사용자 인증을 수행해도 된다는 사용자 인증 권한 위임
 정보 중 적어도 어느 하나로 구성되는 인증정보를 포함하는 것을
 특징으로 하는 사용자 단말.

제 3항에 있어서,

상기 제어부는

상기 보안 영역에서 상기 개방형 아이디에 대응하여 기 저장된
 비밀번호가 존재하는 경우, 상기 사용자 식별 번호를 이용하여
 상기 비밀번호를 복호화하여 사용자 인증을 수행하는 것을
 특징으로 하는 사용자 단말.

제 3항에 있어서,

상기 제어부는

상기 보안 영역에서 상기 개방형 아이디에 대응하여 기 저장된
 비밀번호가 존재하지 않는 경우, 상기 개방형 아이디 관리 장치의
 주소 정보에 대응하는 개방형 아이디 관리 장치로 사용자 인증을
 요청한 후, 상기 개방형 아이디 관리 장치의 요청에 따라
 사용자로부터 입력된 비밀번호를 상기 개방형 아이디 관리 장치로
 전송한 후, 상기 개방형 아이디 관리 장치로부터 사용자 인증 성공
 메시지가 수신되면, 상기 입력된 비밀번호를 상기 보안 영역에서
 사용자 식별 번호를 이용하여 암호화한 후 저장하는 것을
 특징으로 하는 사용자 단말.

[청구항 5]

개방형 아이디 서비스를 지원하는 개방형 아이디 관리 장치 및
 개방형 운영체제를 기반으로 동작하는 보안 영역 및 보안용
 운영체제를 기반으로 동작하는 보안 영역으로 구분되는
 격리환경을 구비하는 적어도 어느 하나의 사용자 단말과 정보를
 송수신하는 서비스 통신부; 및

어느 하나의 사용자 단말의 비보안 영역으로부터 개방형 아이디가
 수신되면, 상기 개방형 아이디를 기초로 개방형 아이디 관리
 장치의 주소 정보를 확인하여 상기 개방형 아이디 관리 장치로
 상기 개방형 아이디에 대한 인증을 질의하며, 상기 개방형 아이디
 관리 장치로부터 인증 결과에 따른 인증 정보가 수신되면, 상기
 인증 정보 및 상기 개방형 아이디 관리 장치의 주소 정보를
 포함하는 리더이택션 메시지를 상기 사용자 단말의 비보안
 영역으로 전송하고, 상기 사용자 단말의 비보안 영역으로부터

[청구항 8]

사용자 인증 성공 메시지가 수신되면, 상기 사용자 단말의 로그인을 허용하는 서비스 제어부;
 를 포함하는 것을 특징으로 하는 웹 서비스 제공 장치.
 사용자 단말이 비보안 영역에서 동작하는 웹 브라우저를 통해 웹 서비스 제공 장치가 제공하는 웹 서비스에 접속한 후 상기 웹 서비스에 로그인하기 위해 상기 웹 브라우저를 통해 입력된 개방형 아이디를 상기 웹 서비스 제공 장치로 전송하는 단계;
 상기 사용자 단말이 상기 웹 서비스 제공 장치로부터 개방형 아이디 관리 장치 주소 정보 및 개방형 아이디 인증 정보 또는 사용자 인증 권한 위임 정보 중 적어도 어느 하나로 구성되는 인증 정보를 포함하는 리다이렉션 메시지를 수신하는 단계;
 상기 사용자 단말이 보안 영역에서 상기 개방형 아이디에 대응하여 기 저장된 비밀번호를 기초로 사용자 인증을 수행하는 단계; 및
 상기 사용자 인증에 성공하면, 상기 사용자 단말이 상기 비보안 영역의 웹 브라우저를 통해 상기 웹 서비스 제공 장치로 사용자 인증 성공 메시지를 전송하고 상기 웹 서비스에 로그인하는 단계;
 를 포함하는 것을 특징으로 하는 트러스티드 플랫폼 기반의 개방형 아이디 인증 방법.

[청구항 9]

제 8항에 있어서,
 상기 사용자 단말이 상기 개방형 아이디를 상기 웹 서비스 제공 장치로 전송하는 단계는
 상기 사용자 단말의 사용자 식별 번호를 더 포함하여 상기 웹 서비스 제공 장치로 전송하는 것을 특징으로 하는 트러스티드 플랫폼 기반의 개방형 아이디 인증 방법.

[청구항 10]

제 8항에 있어서,
 상기 리다이렉션 메시지를 수신하는 단계에서,
 상기 리다이렉션 메시지에 사용자 인증 권한 위임 정보가 포함되어 있지 않을 경우, 상기 개방형 아이디 관리 장치 주소 정보에 대응하는 개방형 아이디 관리 장치로 사용자 인증을 수행하는 단계;
 를 더 포함하는 것을 특징으로 하는 트러스티드 플랫폼 기반의 개방형 아이디 인증 방법.

[청구항 11]

제 8항에 있어서,
 상기 사용자 인증을 수행하는 단계는
 상기 사용자 단말이 보안 영역에 상기 개방형 아이디에 대응하는 비밀번호가 존재하는 지 판단하는 단계; 및
 상기 판단 결과, 개방형 아이디에 대응하는 비밀번호가 존재하는

경우, 상기 사용자 단말에 기 저장된 사용자 식별 번호를 이용하여 상기 비밀번호를 복호화하여 사용자 인증을 수행하는 단계; 를 포함하는 것을 특징으로 하는 트리스티드 플랫폼 기반의 개방형 아이디 인증 방법.

[청구항 12]

제 8항에 있어서,

상기 사용자 인증을 수행하는 단계는

상기 사용자 단말이 보안 영역에 상기 개방형 아이디에 대응하는 비밀번호가 존재하는 지 판단하는 단계;

상기 판단 결과, 개방형 아이디에 대응하는 비밀번호가 존재하지 않는 경우, 상기 개방형 아이디 관리 장치 주소 정보에 대응하는 개방형 아이디 관리 장치로 사용자 인증을 요청하는 단계;

상기 개방형 아이디 관리 장치의 요청에 따라 상기 사용자 단말이 사용자로부터 입력된 비밀번호를 상기 개방형 아이디 관리 장치로 전송하는 단계; 및

상기 개방형 아이디 관리 장치로부터 사용자 인증 성공 메시지가 수신되면, 상기 사용자 단말이 상기 비밀번호를 상기 개방형 아이디에 대응하여 상기 보안 영역에 사용자 식별 번호를 이용하여 암호화한 후 저장하는 단계;

를 포함하는 것을 특징으로 하는 트리스티드 플랫폼 기반의 개방형 아이디 인증 방법.

[청구항 13]

웹 서비스 제공 장치가 사용자 단말로부터 수신된 개방형 아이디를 기초로 개방형 아이디 관리 장치의 주소 정보를 확인하는 단계;

상기 웹 서비스 제공 장치가 상기 확인된 주소 정보에 대응하는 개방형 아이디 관리 장치로 개방형 아이디에 대한 인증을 질의하는 단계;

상기 웹 서비스 제공 장치가 상기 개방형 아이디 관리 장치로부터 개방형 아이디 인증 정보, 상기 개방형 아이디 관리 장치를 대신하여 사용자 인증을 수행해도 된다는 사용자 인증 권한 위임 정보 중 적어도 어느 하나로 구성되는 인증 정보를 수신하는 단계; 및

상기 웹 서비스 제공 장치가 상기 인증 정보 및 상기 개방형 아이디 관리 장치의 주소 정보를 포함하는 리다이렉션 메시지를 상기 사용자 단말로 전송하는 단계;

를 포함하는 것을 특징으로 하는 트리스티드 플랫폼 기반의 개방형 아이디 인증 방법.

[청구항 14]

컴퓨터에 의해 실행되어,

사용자 단말의 비보안 영역에서 동작하는 웹 브라우저를 통해 웹

서비스 제공 장치가 제공하는 웹 서비스에 접속한 후 상기 웹 서비스에 로그인하기 위해 상기 웹 브라우저를 통해 입력된 개방형 아이디를 상기 웹 서비스 제공 장치로 전송하는 단계; 상기 웹 서비스 제공 장치로부터 개방형 아이디 관리 장치 주소 정보 및 개방형 아이디 인증 정보 또는 사용자 인증 권한 위임 정보 중 적어도 어느 하나로 구성되는 인증 정보를 포함하는 리다이렉션 메시지를 수신하는 단계;

상기 보안 영역에서 상기 개방형 아이디에 대응하여 기 저장된 비밀번호를 기초로 사용자 인증을 수행하는 단계; 및 상기 사용자 인증에 성공하면, 상기 비밀번호 영역의 웹 브라우저를 통해 상기 웹 서비스 제공 장치로 사용자 인증 성공 메시지를 전송하고 상기 웹 서비스에 로그인하는 단계;를 실행하는 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체.