

명세서

발명의 명칭: 브라우저의 웹스토리지를 이용한 간편인증 방법 및 시스템

기술분야

- [1] 본 발명은 브라우저의 웹스토리지를 이용한 간편인증 방법 및 시스템에 관한 것으로 보다 구체적으로 웹스토리지에 저장된 간편인증 데이터를 이용하여 사용기기 및 브라우저별 1회성 공개키 및 개인키를 발급하고, 발급된 공개키 및 개인키를 이용하여 간편 인증을 수행하는 방법 및 시스템에 관한 것이다.

배경기술

- [2] 인터넷 서비스의 발달로 인해 대부분의 사람들은 인터넷을 통해 정부기관, 교육기관, 의료기관, 통신회사, 금융회사, 여객회사, 자산관리, 신용정보, 포털, 소셜네트워크서비스(Social Network Service: SNS), 게임, 쇼핑, 발권, 택배, 전자투표 등의 수많은 온라인 서비스를 이용한다.
- [3] 따라서, 이러한 서비스를 이용하고자 하는 사용자는 자신의 실명 등을 포함한 개인정보를 입력하여 회원에 가입하거나, 특정 아이디와 비밀번호를 입력하여 가입된 사용자임을 인증해야 한다. 그런데 여러 사이트마다 이러한 인증 절차를 반복하는 것은 상당히 번거롭기 때문에, 최근에는 간편 인증이라고 하여 보다 쉽게 로그인을 도와주어 인터넷상에서 금융거래를 쉽게 진행할 수 있도록 하는 방법이 발전되고 있다.
- [4] 한편, 과거 이러한 사용자들을 인증하는 방법에 주로 사용되었던 방식은 대칭키를 이용하는 방법이었다. 그러나 이러한 대칭키방식은 하나의 비밀키를 서버와 단말 양쪽에서 같이 사용하기에 해커로부터 안전하지 못한 문제가 있었다.
- [5] 한편, 이러한 문제를 해결하고자 공개키(Public Key)와 개인키(Private Key) 조합을 이용하여 데이터를 암호화하고, 인증을 수행하는 방법으로 발전되었다.
- [6] 그러나, 기존의 사용자 인증을 위한 공개키(Public Key)와 개인키(Private Key)를 사용함에 있어서 브라우저 저장소(local storage)는 여전히 평문 저장방식을 사용하고 있어 보안의 문제가 많았다. 물론, 보안책으로 암호화 방식을 취하고 있기는 하지만 이러한 방법도 여전히 개인정보 유출이나 보안의 문제가 있다. 따라서, 이러한 문제 해결을 위해 공개키(Public Key)와 개인키(Private Key)의 안전 보관 및 그 사용방법이 필요로 하다.

발명의 상세한 설명

기술적 과제

- [7] 본 발명이 해결하고자 하는 과제는 웹 스토리지를 이용한 간편인증 방법 및 시스템에 있어서, 웹스토리지에 저장된 간편인증 데이터를 이용하여 사용기기 및 브라우저별 1회성 공개키를 발급하고, 발급된 공개키를 이용하여 간편

- 인증을 수행하여 개인정보의 보호화 보안을 강화할 수 있다.
- [8] 또한, 생성된 개인키를 서버의 세션에 저장하고, 저장된 세션에 대한 세션키 및 공개키를 단말에 전송하는 방식을 취함으로써 2차 인증을 수행하도록 할 수 있다.
- [9] 또한, 서버에 저장되는 공개키를 블록체인에 저장하여 공개키 위변조 방지 및 인증 로그 데이터를 블록체인에 저장하여 인증에 대한 부인방지 및 무결성을 확보할 수 있다.
- [10] 본 발명이 해결하고자 하는 과제들은 이상에서 언급된 과제로 제한되지 않으며, 언급되지 않은 또 다른 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.
- 과제 해결 수단**
- [11] 상술한 과제를 해결하기 위한 본 발명의 일 면에 따른 브라우저의 웹스토리지를 이용한 간편인증 방법은, 서버가 수신된 사용자키에 기초하여 인증토큰, 공개키 및 개인키를 생성하여 세션에 저장하고, 상기 세션에 대응하는 세션키, 상기 인증토큰 및 상기 공개키를 단말에 전송하는 단계; 상기 단말이 상기 수신한 공개키를 이용하여, 사용자가 입력한 PIN 번호 데이터를 암호화하고, 암호화된 데이터를 상기 수신된 세션키와 함께 상기 서버로 전송하는 단계; 및 상기 서버는 상기 수신된 세션키에 대응하는 상기 개인키를 이용하여 상기 PIN 번호 데이터를 복호화하여 간편인증을 수행하는 단계를 포함하고, 상기 사용자키는 단말의 웹스토리지에 저장되어 기기 또는 브라우저별로 다르게 설정되는 것일 수 있다.
- [12] 또한, 상기 공개키는 블록체인에 저장되어 변조 또는 위조가 되었는지 검증하는데 이용되는 것일 수 있다.
- [13] 또한, 상기 간편인증을 수행하는 단계는, 상기 서버가 상기 수신된 세션키를 통해 불러온 개인키를 기초로 암호화된 PIN 번호 데이터를 복원하여 1차 인증을 진행하는 단계; 상기 1차인증이 통과되면, 상기 단말에서 상기 인증토큰을 상기 공개키를 이용하여 암호화하고, 암호화된 데이터를 상기 수신된 세션키와 함께 서버로 전송하는 단계; 및 상기 서버에서 상기 개인키를 기초로 복원한 인증토큰과 상기 세션에 저장된 인증토큰을 비교하여 2차 인증을 수행한 뒤 상기 세션을 삭제하는 단계를 더 포함할 수 있다.
- [14] 또한, 상기 사용자키는 암호화 알고리즘으로 암호화되고, PIN번호는 해시 암호화되어 상기 웹스토리지에 저장되는 것일 수 있다.
- [15] 또한, 상기 공개키를 단말에 전송하는 단계는, 상기 서버의 인증정책을 조회하는 단계; 및 상기 서버의 인증정책에 따라 상기 단말에서 사용자키를 간편인증 방식 또는 사용자 공개키로 조회하는 단계를 포함할 수 있다.
- [16] 또한, 상기 공개키를 단말에 전송하는 단계는, 단말은 상기 웹스토리지에 상기 사용자키가 저장되어 있는지 판단하는 단계; 및 상기 사용자키가 저장되어 있지

- 않은 경우, 사용자로부터 PIN 번호를 등록 받는 단계를 더 포함할 수 있다.
- [17] 또한, 상기 간편인증을 수행하는 단계는, 상기 PIN번호가 비매칭 될 때마다 인증시도 횟수를 갱신하고, 상기 인증시도 횟수가 소정 개수 이상 증가하는 경우 상기 서버 및/또는 단말에 저장된 PIN번호 데이터를 삭제하는 것일 수 있다.
- [18] 또한, 상기 생성된 공개키 및 개인키에서 계수(modulus), 개인 지수(private exponent) 및 공개 지수(public exponent)를 추출하는 단계; 상기 개인 지수가 단말에 저장되고, 상기 계수 및 공개 지수는 상기 서버에 저장되는 단계; 및 상기 단말에 저장된 개인 지수와 상기 서버에 저장된 계수를 이용하여 생성된 개인키 및 상기 서버에 저장된 공개 지수와 계수를 이용하여 생성된 공개키를 이용하여 간편인증을 수행하는 단계;를 더 포함할 수 있다.
- [19] 또한, 상기 간편인증을 수행하는 단계는, 상기 서버가 간편인증 요청에 따라 상기 단말로 상기 계수를 전송하는 단계; 상기 단말이 수신한 계수 및 상기 저장된 개인 지수를 이용하여 개인키를 생성하는 단계; 상기 생성된 개인키를 이용하여 데이터를 암호화 및 전자서명을 진행하는 단계; 상기 암호화된 데이터 및 전자서명을 서버로 전송하는 단계; 및 상기 개인키를 폐기하는 단계를 포함할 수 있다.
- [20] 또한, 상기 간편인증을 수행하는 단계는, 상기 서버가 상기 계수 및 상기 공개 지수를 이용하여 공개키를 생성하는 단계; 상기 생성된 공개키를 이용하여 상기 단말로부터 수신한 암호화된 데이터를 복호화하고, 상기 전자서명을 이용하여 검증하는 단계; 및 상기 공개키를 폐기하는 단계를 더 포함할 수 있다.
- [21] 상술한 과제를 해결하기 위한 본 발명의 다른 면에 따른 웹스토리지를 이용한 간편인증 시스템은, 수신된 사용자키에 기초하여 인증토큰, 공개키 및 개인키를 생성하여 세션에 저장하고, 상기 세션에 대응수신된 사용자키에 기초하여 인증토큰, 공개키 및 개인키를 생성하여 세션에 저장하고, 상기 세션에 대응하는 세션키, 상기 인증토큰 및 상기 공개키를 단말에 전송하고, 상기 단말로부터 암호화된 데이터와 세션키를 수신하면 수신된 세션키에 대응하는 개인키를 이용하여 상기 PIN 번호 데이터를 복호화하여 간편인증을 수행하는 서버; 및 사용자키에 기초하여 공개키 발행을 요청하고, 서버에서 수신한 공개키를 이용하여, 사용자가 입력한 PIN 번호 데이터를 암호화하고, 암호화된 데이터를 상기 수신된 세션키와 함께 서버로 전송하는 단말을 포함하고, 상기 사용자키는 단말의 웹스토리지에 저장되어 기기 또는 브라우저별로 다르게 설정될 수 있다.
- [22] 또한, 상기 공개키는 블록체인에 저장되어 변조 또는 위조가 되었는지 검증하는데 이용되는 것일 수 있다.
- [23] 또한, 상기 서버는 상기 수신된 세션키를 통해 불러온 개인키를 기초로 암호화된 PIN 번호 데이터를 복원하여 1차 인증을 진행하고, 상기 단말은 상기 1차인증이 통과되면, 상기 단말에서 상기 인증토큰을 상기 공개키를 이용하여 암호화하고, 암호화된 데이터를 상기 수신된 세션키와 함께 서버로 전송하며, 서버는 상기 개인키를 기초로 복원한 인증토큰과 상기 세션에 저장된

인증토큰을 비교하여 2차 인증을 수행한 뒤 상기 세션을 삭제하는 동작을 수행할 수 있다.

- [24] 또한, 상기 서버는, 상기 복원된 PIN번호가 비매칭 될 때마다 인증시도 횟수를 갱신하고, 상기 인증시도 횟수가 소정 개수 이상 증가하는 경우 상기 서버 및/또는 단말에 저장된 PIN번호 데이터를 삭제할 수 있다.

- [25] 본 발명의 기타 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

발명의 효과

- [26] 본 발명은 웹스토리지에 저장된 간편인증 데이터를 이용하여 기기 또는 브라우저별로 다르게 개인키를 발급하여 인증을 수행할 수 있다. 또한, 인증 요청시마다 공개키 기반의 1회성 키 생성을 지원함으로써 간편 인증 방식에 있어서 보다 강력한 보안을 제공할 수 기 때문에, 공인인증서를 대체할 수 있을 정도로 신뢰성이 높으면서도 간편한 인증방법을 제공할 수 있다.
- [27] 본 발명의 효과들은 이상에서 언급된 효과로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

- [28] 도 1은 본 발명에 따른 브라우저의 웹스토리지를 이용한 간편인증 시스템을 설명하기 위한 개념도이다.
- [29] 도 2는 본 발명에 따른 웹스토리지를 이용한 간편인증 방법을 설명하는 순서도이다.
- [30] 도 3은 본 발명에 따라 PIN 번호를 등록하는 일 예를 설명하는 도이다.
- [31] 도 4는 본 발명에 따라 웹스토리지를 이용한 간편인증을 수행하는 일 예를 설명하는 순서도이다.
- [32] 도 5는 본 발명에 따라 웹스토리지를 이용한 간편인증을 수행하는 다른 예를 설명하는 순서도이다.
- [33] 도 6은 본 발명에 따른 웹스토리지를 이용한 간편인증 과정을 수행하는 서버의 내부 구성을 개략적으로 나타낸 블록 도이다.
- [34] 도 7은 본 발명에 따른 웹스토리지를 이용한 간편인증 과정을 수행하는 단말의 내부 구성을 개략적으로 나타낸 블록 도이다.
- [35] 도 8은 본 발명에 따른 공개키 및 개인키의 구성요소 분산저장을 통한 간편인증 시스템을 설명하기 위한 개념도이다.
- [36] 도 9는 본 발명에 따른 공개키 및 개인키의 구성요소 분산저장을 통한 간편인증 방법을 설명하는 순서도이다.
- [37] 도 10은 본 발명에 따른 공개키 및 개인키의 구성요소 분산저장을 수행하는 방법의 일 예를 설명하는 도이다.
- [38] 도 11은 본 발명에 따른 단말에서 개인키를 생성하는 일 예를 설명하는 순서도이다.

- [39] 도 12는 본 발명에 따른 서버에서 공개키를 생성하는 일 예를 설명하는 순서도이다.
- [40] 도 13은 본 발명에 따른 공개키 및 개인키의 구성요소 분산저장을 통한 간편인증과정을 수행하는 서버의 내부 구성을 개략적으로 나타낸 블록 도이다.
- [41] 도 14는 본 발명에 따른 공개키 및 개인키의 구성요소 분산저장을 통한 간편인증과정을 수행하는 단말의 내부 구성을 개략적으로 나타낸 블록 도이다.
- 발명의 실시를 위한 최선의 형태**
- [42] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 제한되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술 분야의 통상의 기술자에게 본 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.
- [43] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소 외에 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다. 명세서 전체에 걸쳐 동일한 도면 부호는 동일한 구성 요소를 지칭하며, "및/또는"은 언급된 구성요소들의 각각 및 하나 이상의 모든 조합을 포함한다. 비록 "제1", "제2" 등이 다양한 구성요소들을 서술하기 위해서 사용되나, 이들 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 구성요소를 다른 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제1 구성요소는 본 발명의 기술적 사상 내에서 제2 구성요소일 수도 있음은 물론이다.
- [44] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술분야의 통상의 기술자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또한, 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않은 한 이상적으로 또는 과도하게 해석되지 않는다.
- [45] 공간적으로 상대적인 용어인 "아래(below)", "아래(beneath)", "하부(lower)", "위(above)", "상부(upper)" 등은 도면에 도시되어 있는 바와 같이 하나의 구성요소와 다른 구성요소들과의 상관관계를 용이하게 기술하기 위해 사용될 수 있다. 공간적으로 상대적인 용어는 도면에 도시되어 있는 방향에 더하여 사용시 또는 동작 시 구성요소들의 서로 다른 방향을 포함하는 용어로 이해되어야 한다. 예를 들어, 도면에 도시되어 있는 구성요소를 뒤집을 경우,

다른 구성요소의 "아래(below)" 또는 "아래(beneath)"로 기술된 구성요소는 다른 구성요소의 "위(above)"에 놓여 질 수 있다. 따라서, 예시적인 용어인 "아래"는 아래와 위의 방향을 모두 포함할 수 있다. 구성요소는 다른 방향으로도 배향될 수 있으며, 이에 따라 공간적으로 상대적인 용어들은 배향에 따라 해석될 수 있다.

- [46] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세하게 설명한다.
- [47]
- [48] 도 1은 본 발명에 따른 브라우저의 웹스토리지를 이용한 간편인증 시스템을 설명하기 위한 개념도이다.
- [49] 도 1을 참조하면 본 발명에 따른 브라우저의 웹스토리지를 이용한 간편인증 시스템은 서버(100) 및 단말(200)을 포함할 수 있다.
- [50] 우선 서버(100)와 단말(200)은 SSL 암호화 방식을 통해 모든 통신구간(10)에 대해 종단간(End-to-End) 암호화가 수행될 수 있다. 먼저 서버(100)는 공개키 및 개인키를 생성하여 세션에 저장하고 있다가, 단계 101에서 공개키를 배포하면서, 공개키 대응하는 세션에 대한 세션키를 단말(200)에 전송할 수 있다.
- [51] 단말(200)은 단계 201에서 수신한 세션키에 대해서 암호화를 수행할 수 있으며, 단계 202에서 수신된 공개키를 이용하여 간편인증 데이터를 암호화한다. 여기서, 간편인증 데이터는 사용자키 및 PIN 번호 데이터를 포함할 수 있다. 단계 101에서 서버(100)는 수신된 인증 정보의 무결성을 검증하고, 단계 102에서 단말(200)로부터 암호화된 데이터와 세션키를 수신하면 세션키에 대응하는 개인키를 이용하여 상기 PIN 번호 데이터를 복호 함으로써, 간편인증을 수행할 수 있다. 한편 전달정보 무결성 검증에는 인증토큰이 별도로 이용될 수 있으며, 인증 토큰을 활용하여 2단계로 간편인증을 수행함으로써 보다 보안을 강화 할 수 있다.
- [52] 단계 203에서 최종적으로 단말(200)은 간편 인증 결과에 기초하여 로그인 등 동작을 수행하도록 할 수 있다.
- [53] 다른 실시예에 따른 간편인증 방법에서 간편인증을 위한 정보가 블록체인에 저장되고, 인증 단계에서 검증될 수 있다.
- [54] 예를 들면, 간편인증을 위한 공개키 정보는 블록체인에 저장될 수 있다. 간편인증 정보는 공개키 및 개인키 기반으로 암호화 및 복호화되는데, 사용자가 입력한 PIN 번호를 암호화하기 위한 공개키가 변조/조작된 경우가 발생할 수 있다. 따라서 이러한 경우를 막기 위해 공개키를 블록체인 방식으로 저장하여 신뢰성을 담보하고 서버(100)가 없이도 단말(200)에서 공개키를 획득하여 PIN 번호를 암호화할 수 있다.
- [55] 또 다른 예로, 공개키 기반으로 암호화된 인증 데이터(사용자키 및 PIN번호)가 블록체인에 저장될 수 있다. 따라서, 서버(100) 또는 단말은 블록체인을 기반으로 사용자가 입력한 PIN번호의 인증 및 검증을 수행하여 변조가능성을 낮춤으로써 신뢰성을 높일 수도 있다.

- [56] 상술한 바와 같이, 본 발명에 따른 브라우저의 웹스토리지를 이용한 간편인증 시스템은 웹스토리지에 저장된 간편인증 데이터를 이용하여 사용기기 및 브라우저별 1회성 공개키를 발급하고, 발급된 공개키를 이용하여 간편 인증을 수행하여 개인정보의 보호와 보안을 강화할 수 있다.
- [57] 또한, 생성된 개인키를 서버(100)의 세션에 저장하고, 저장된 세션에 대한 세션키 및 공개키를 단말(200)에 전송하는 방식을 취함으로써 2차 인증을 수행하도록 하여 보다 보안을 강화시킬 수 있다.
- [58] 나아가, 서버에 저장되는 공개키를 블록체인에 저장하여 공개키 위변조 방지 및 인증 로그 데이터를 블록체인에 저장하여 인증에 대한 부인방지 및 무결성을 확보할 수 있다.
- [59]
- [60] 도 2는 본 발명에 따른 웹스토리지를 이용한 간편인증 방법을 설명하는 순서도이다.
- [61] 도 2를 참조하면, 본 발명에 따른 웹스토리지를 이용한 간편인증 방법은, 단계 S200에서 서버(100)가 수신된 사용자키에 기초하여 인증토큰, 공개키 및 개인키를 생성하여 세션에 저장하고, 세션에 대응하는 세션키, 인증토큰 및 상기 공개키를 단말(200)에 전송한다. 여기서, 사용자키는 단말(200)의 웹스토리지에 저장되어 기기 또는 브라우저별로 다르게 설정될 수 있다.
- [62] 다음으로, 단계 S210에서, 본 발명에 따른 웹스토리지를 이용한 간편인증 방법은, 단말(200)이 수신한 공개키를 이용하여, 사용자가 입력한 PIN 번호 데이터를 암호화하고, 암호화된 데이터를 수신된 세션키와 함께 서버(100)로 전송한다.
- [63] 다음으로, 단계 S220에서, 본 발명에 따른 웹스토리지를 이용한 간편인증 방법에서, 서버(100)는 수신된 세션키에 대응하는 개인키를 이용하여 상기 PIN 번호 데이터를 복호화 하여 간편인증을 수행한다.
- [64] 보다 구체적으로, 서버(100)는 수신된 세션키를 통해 불러온 개인키를 기초로 암호화된 PIN 번호 데이터를 복원하여 1차 인증을 진행한다. 여기서 1차 인증은 사용자키에 대응하는 PIN번호 데이터를 서버가 저장하고 있는 경우 서버에서 인증이 수행되고, 단말이 가지고 있는 경우 단말에서 인증이 수행된다. 물론 서버와 단말에서 교차 검증이 수행될 수 있다. 1차인증이 통과되면, 단말(200)에서 상기 인증토큰을 상기 공개키를 이용하여 암호화하고, 암호화된 데이터를 상기 수신된 세션키와 함께 서버(100)로 전송한다. 만약 PIN번호가 비매칭되어 1차 인증을 통과하지 못하면 서버(100)는 사용자키별 인증시도 횟수를 카운트하고, 누적 카운트가 소정값 이상이면 해킹 가능성을 고려하여 서버(100) 및/또는 단말(200)에 저장된 PIN번호 데이터를 삭제한다.
- [65] 한편, 서버(100)는 개인키를 기초로 복원한 인증토큰과 세션에 저장된 인증토큰을 비교하여 2차 인증을 수행한 뒤 상기 세션을 삭제한다. 즉, 세션 및 세션키는 인증 요청시마다 1회성으로 생성되며 인증이 완료되면 삭제됨으로써

생성된 키가 유출되는 것을 방지할 수 있다.

- [66]
- [67] 이하 도 3 내지 도 5를 참조하여 본 발명에 따른 간편인증 방법에서 사용자의 PIN 번호를 등록하는 일 예 및 간편인증을 수행하는 예들을 상세히 살펴본다.
- [68] 도 3은 본 발명에 따라 PIN 번호를 등록하는 일 예를 설명하는 도이다.
- [69] 도 3을 참고하면, 단계 300에서 사용자가 PIN등록을 요청하면 단말(200)은 단계 301에서, PIN등록유무를 판단한다. 만약 PIN이 등록되어 있다면 바로 PIN인증 단계로 진행한다. 한편, PIN 인증단계는 도 4 및 도 5에 관한 설명에서 상세히 후술한다.
- [70] 단계 301에서 PIN등록이 되어있지 않다고 판단되면, 단말(200)은 단계 303으로 진행하여 본인인증 또는 ID/PW인증을 수행한다. 그리고, 인증 결과를 기반으로 획득된 사용자 정보를 서버(100)로 전송한다. 여기서 사용자 정보는 CI 또는 사용자 ID에 연동되거나 기간제 시스템을 통해 조회 되는 정보일 수 있다.
- [71] 단계 304에서 서버는 PIN 등록을 위한 사용자 정보를 기초로 등록토큰을 생성한다. 여기서 등록토큰은 사용자의 브라우저 정보에 호스트네임 및 타임스탬프가 결합된 형태로 해시 암호화된 데이터일 수 있다.
- [72] 그리고 단계 305에서 PIN번호 정책을 조회한다. 단계 306에서 사용자 정보를 이용하여 공개키 및 개인키를 생성한다. 그리고 단계 307에서 사용자 정보를 기초로 PIN사용자키를 생성한다. 예를 들면 PIN 사용자키는 사용자 정보에 브라우저 정보와 서비스도메인 정보가 추가된 데이터일 수 있다. 따라서, 사용자키는 단말(200)에서 생성되어 서버(100)로 전달될 수도 있다.
- [73] 단계 308에서, 서버는 생성된 등록토큰 및 개인키는 세션에 저장하고, PIN번호 정책, 공개키, 세션키 및 PIN 사용자키를 단말로 전송한다.
- [74] 단계 309에서 단말(200)은 사용자로부터 PIN 번호를 입력받는다. 단계 310에서 단말(200)은 수신한 PIN번호 정책에 따른 PIN번호가 입력되어 있는지 확인한다. 예컨대, 동일 숫자 또는 연속숫자가 기준에 부합하지 않는 경우 오류로 판단하여 단계 309를 반복한다.
- [75] 단계 311에서, PIN번호 정책에 부합하는 PIN번호 데이터는 공개키 기반으로 암호화된다. 또한 단말(200)은 공개키 기반으로 암호화된 PIN사용자키, PIN번호, 등록토큰 및 세션키를 다시 서버로 전달한다. 이때, 단말(200)과 서버(100) 사이에 SSL통신이 사용되어 보안이 강화 될 수 있다.
- [76] 단계 312에서 서버(100)는 수신된 세션키에 대응하는 개인키를 이용하여 수신한 데이터를 복호화 할 수 있다.
- [77] 단계 313에서 서버(100)는 등록토큰을 체크한다. 예를 들면, 브라우저, 호스트네임 등록 정보를 기초로 등록토큰이 재사용 되었는지 확인하거나, 타임스탬프를 이용하여 유효시간이 경과 되었는지 체크 한다. 만약 재사용이 확인된다면 단계 314로 진행하여 세션을 삭제하고 단계 315에서 PIN등록 절차를 종결한다.

- [78] 한편, 서버(100)는 단계 316에서 한 번 더 PIN 번호 정책을 확인한 뒤 단계 317에서 PIN번호 관련 기타 정책을 체크한다. 예컨대 생년월일, 휴대폰번호가 포함되어 있는지를 기간제 시스템의 등록 정보를 통해서 조회 할 수 있다.
- [79] PIN 번호 관련 기타정책 체크를 통과하면 단계 318에서 세션을 삭제하고 단계 319 및 단계 320으로 진행하여 PIN사용자키에 대한 등록토큰 및 PIN번호를 저장한다.
- [80] 다음으로 PIN사용자키, PIN번호, 인증정책은 단말(200)로 전달되며, 단계 321에서 웹스토리지의 지원 여부에 따라 웹스토리지에 저장되거나(322) 쿠키에 저장되며(323), 저장이 완료되면 단계 324에서 PIN등록 절차가 종료된다. 한편, PIN사용자키는 암호화 알고리즘으로 암호화 되고, PIN번호는 해시 암호화 될 수 있다.
- [81] 상술한 바에 따라서 PIN 번호 등록이 완료되면 다음으로, 도 4 또는 도 5를 후술하는 일 실시예에 따라 등록된 PIN번호로 인증이 수행될 수 있다. 도 4는 서버(100)가 1차 인증을 수행하고 단말(200)이 검증을 수행하는 방법을 나타내며, 도 5는 단말(200)이 1차 인증을 수행하고 서버(100)가 검증을 수행하는 방법을 설명한다. 한편, 후술하는 동작에서 일부 간편인증 절차는 블록체인을 이용하여 구현될 수 있음을 본 발명이 속하는 기술분야의 당업자에게는 자명할 것이다.
- [82] 도 4는 본 발명에 따라 웹스토리지를 이용한 간편인증을 수행하는 일 예를 설명하는 순서도이다.
- [83] 도 4를 참조하면, 단계 400에서 PIN 인증 절차가 시작된다. 단계 401 내지 단계 409를 통해 PIN번호 등록이 필요한지 판단한다. 우선 단계 401에서 서버(100)는 인증정책을 조회하여 단말(200)에 전달하고, 단말(200)은 사용자키를 조회하여 단계 403에서 PIN등록여부를 판단한다. 만약 PIN 번호가 웹스토리지에 등록되어 있다면 서버(100)에서는 PIN등록이 해지되었거나(404) 유효기간이 만료(405)되었는지 확인하고 이에 따라 PIN번호를 해지(406)하고 해지로그를 저장(407)한 뒤 최종적으로 단말(200)에서 PIN을 해지(408)하고 단계 409에서 PIN등록 절차를 다시 진행할 수 있다.
- [84] 단계 410에서는 PIN등록이 확인되면, 서버(100)는 간편인증을 위한 인증토큰을 생성하여 세션에 저장하고 또 단말(200)로 전달한다. 여기서 인증토큰은 호스트네임, 아이피, 타임스탬프가 결합된 형태의 데이터일 수 있다.
- [85] 단말(200)은 인증토큰이 수신되면 단계 411에서 사용자로부터 PIN번호를 입력받고, 단계 412에서 공개키를 요청한다.
- [86] 단계 413에서, 서버(100)는 사용자키를 기초로 공개키 및 개인키를 생성하되, 공개키 및 개인키를 생성하여 세션에 저장하고 세션에 대응하는 세션키 및 공개키를 단말(200)에 전달한다.
- [87] 단계 414에서, 단말(200)이 상기 수신한 공개키를 이용하여, 사용자가 입력한 PIN 번호 데이터를 암호화하고, 암호화된 데이터를 상기 수신된 세션키와 함께

서버로 전송한다.

- [88] 단계 415에서, 서버(100)는 상기 수신된 세션키에 대응하는 개인키를 이용하여 상기 PIN 번호 데이터를 복호화하고, 단계 416에서 PIN 인증시도 횟수가 초과되었는지 확인한다. 만약 PIN인증시도 횟수가 초과되었다면 단계 417 내지 421을 수행하여 PIN 인증을 종료한다.
- [89] 단계 422에서, PIN 인증 시도 횟수를 증가시키고 단계 423에서 PIN번호가 서버(100)에 저장된 PIN번호와 일치하는지 확인하는 1차 인증을 수행한다. 동일한 동작은 단계 425의 단말(200) 및/또는 서버(100)에서 수행될 수 있다. 만약 PIN번호가 일치하지 않는다면 단계 424에서 인증 실패로그를 저장하고 다시 단계 411의 PIN번호 입력 단계를 반복한다. 만약 1차인증이 통과되면, 단말(200)은 인증토큰을 서버에서 수신하였던 공개키를 이용하여 암호화하고, 암호화된 데이터를 기 수신한 세션키와 함께 서버로 전송한다.
- [90] 단계 426에서 서버(100)는 인증 토큰을 체크한다. 예를 들면 인증토큰 재사용 또는 인증 유효시간이 경과하였는지 2차 인증을 수행한다.
- [91] 만약 체크를 통과하지 못하면 세션을 삭제하고(단계 427) 인증실패로그를 저장한 뒤(단계 428) PIN인증을 종료한다(단계 429). 서버(100)는 인증 토큰 체크가 통과되면 세션을 삭제(단계 430)하되 인증토큰을 별도로 저장(단계 431)하고, 인증시도 횟수를 초기화(단계 432)한다. 단계 433에서, 최종적으로 PIN번호 간편인증을 통한 단말(200)의 로그인이 완료된다.
- [92] 도 5는 본 발명에 따라 웹스토리지를 이용한 간편인증을 수행하는 다른 예를 설명하는 순서도이다.
- [93] 단계 500에서 PIN 인증이 시작되면, 단계 501에서 PIN등록 유무를 판단하고 PIN 등록이 되어 있지 않다면 단계 502로 진행하여 도 3에 상술된 등록단계를 진행한다.
- [94] 단계 503에서, PIN 등록이 된 것으로 확인되면 웹스토리지 또는 쿠키에 저장되어 있는 사용자키를 조회하여 서버로 전달한다. 서버(100)는 단계 504에서 PIN 등록이 해지되었는지 체크하고, 단계 505에서 PIN번호 유효기간을 체크한다.
- [95] 만약 PIN 등록이 해지되었거나 해지되었다면 단계 506 내지 509를 통해 PIN 등록 절차를 수행한다.
- [96] 단계 510에서는 PIN등록이 확인되면, 서버(100)는 간편인증을 위한 인증토큰을 생성하여 세션에 저장하고 또 단말(200)로 전달한다. 여기서 인증토큰은 호스트네임, 아이피, 타임스탬프가 결합된 형태의 데이터일 수 있다.
- [97] 단말(200)은 인증토큰이 수신되면 단계 511에서 사용자로부터 PIN번호를 입력받고, 단계 512에서 공개키를 요청한다.
- [98] 단계 513에서, 서버(100)는 사용자키를 기초로 공개키 및 개인키를 생성하되, 공개키 및 개인키를 생성하여 세션에 저장하고 세션에 대응하는 세션키 및 공개키를 단말(200)에 전달한다.

- [99] 단계 514에서, 단말(200)이 상기 수신한 공개키를 이용하여, 사용자가 입력한 PIN 번호 데이터를 암호화하고, 암호화된 데이터를 상기 수신된 세션키와 함께 서버로 전송한다.
- [100] 단계 515에서, 서버(100)는 상기 수신된 세션키에 대응하는 개인키를 이용하여 상기 PIN 번호 데이터를 복호화하고, 단계 516에서 PIN 인증 시도 횟수가 초과되었는지 확인한다. 만약 PIN인증 시도 횟수가 초과되었다면 단계 517 내지 522를 수행하여 PIN 인증을 종료한다.
- [101] 단계 523에서 서버(100)는 복호화된 PIN번호를 해시 암호화하여 단말(200)로 전송한다. 단계 524에서 단말(200)은 수신된 PIN번호와 저장된 PIN번호가 일치하는지 체크한다. 만약 PIN번호가 일치하지 않는다면 단계 532에서 인증 실패로그를 저장하고 다시 단계 511의 PIN번호 입력 단계를 반복한다. 만약 1차인증이 통과되면, 단말(200)은 서버에서 수신하였던 사용자키, PIN번호, 인증토큰을 공개키를 이용하여 암호화하고, 암호화된 데이터를 기 수신한 세션키와 함께 서버로 전송한다.
- [102] 단계 526에서 서버(100)는 세션키에 대응하는 개인키를 이용하여 인증 토큰, 사용자키, PIN번호를 복호화하고 단계 527에서 서버(100)는 인증 토큰을 체크한다. 예를 들면 인증토큰 재사용 또는 인증 유효시간이 경과하였는지 2차 인증을 수행한다.
- [103] 만약 체크를 통과하지 못하면 세션을 삭제하고(단계 528) 인증실패로그를 저장한 뒤(단계 529) PIN인증을 종료한다(단계 530). 서버(100)는 인증 토큰 체크가 통과되면, PIN번호 체크를 수행한 뒤(단계 531), 체크를 통과하지 못한다면 인증실패 로그를 저장(단계 532)하고 체크를 통과한다면 세션을 삭제(단계 533)한다. 서버(100)는 인증토큰을 별도로 저장(단계 534)하고, 인증 시도 횟수를 초기화(단계 535)한다. 단계 536에서, 최종적으로 PIN번호 간편인증을 통한 단말(200)의 로그인이 완료된다.
- [104]
- [105] 도 6은 본 발명에 따른 웹스토리지를 이용한 간편인증 과정을 수행하는 서버(100)의 내부 구성을, 도 7은 본 발명에 따른 웹스토리지를 이용한 간편인증 과정을 수행하는 단말(200)의 내부 구성을 개략적으로 나타낸 블록 도이다.
- [106] 도 6 및 도 7에는 본 발명을 설명하기 위해 필요한 구성만이 도시되었으나, 디스플레이 장치 등 다양한 구성이 더 포함될 수 있다. 또한 도 6 및 도 7에 대한 설명에서 생략되더라도 도 1 내지 5에서 상술된 방법을 수행하기 위해 필요한 구성이 더 포함될 수 있음을 본 발명이 속하는 분야의 통상의 기술자에게는 자명하다.
- [107] 도 6을 참조하면 본 발명에 따른 서버(100)는, 프로세서(130), 메모리(140) 및 통신부(150)를 포함할 수 있다. 간편인증을 수행하는 서버(100)의 동작은 메모리(140)에 저장된 프로그램을 프로세서(130)를 통해서 실행시킴으로써 수행될 수 있다.

- [108] 본 발명에 따른 프로세서(130)에서 수행되는 연산은, 수신된 사용자키에 기초하여 인증토큰, 공개키 및 개인키를 생성하여 세션에 저장하고, 상기 세션에 대응하는 세션키, 상기 인증토큰 및 상기 공개키를 단말에 전송하고, 상기 단말로부터 암호화된 데이터와 세션키를 수신하면 수신된 세션키에 대응하는 개인키를 이용하여 상기 PIN 번호 데이터를 복호화 하여 간편인증을 수행할 수 있다.
- [109] 또한, 프로세서(130)는 수신된 세션키를 통해 불러온 개인키를 기초로 암호화된 PIN 번호 데이터를 복원하여 1차 인증을 진행 할수도 있다.
- [110] 또한, 프로세서(130)는 개인키를 기초로 복원한 인증토큰과 상기 세션에 저장된 인증토큰을 비교하여 2차 인증을 수행한 뒤 세션을 삭제하는 동작을 수행할 수 있다.
- [111] 또한, 프로세서(130)는 상기 복원된 PIN번호가 비매칭 될때마다 인증시도 횟수를 갱신하고, 상기 인증시도 횟수가 소정 개수 이상 증가하는 경우 상기 서버 및/또는 단말에 저장된 PIN번호 데이터를 삭제할 수 있다.
- [112] 본 발명에서, 통신부(150)는, 단말(200)과 또는 다른 서버 또는 다른 외부 장치 간의 무선 또는 유선 통신을 수행할 수 있다. 예를 들면 통신부(150)는 단말(200)과 SSL방식으로 암호화 통신을 수행할 수 있으며, 공개키 및 암호화된 데이터를 전달할 수 있다.
- [113]
- [114] 도 7을 참조하면 본 발명에 따른 단말(200)은, 프로세서(230), 메모리(240), 통신부(250) 및 입력부(260)를 포함할 수 있다. 간편인증 단말(200)의 동작은 메모리(240)에 저장된 프로그램을 프로세서(230)를 통해서 실행시킴으로 수행될 수 있다.
- [115] 본 발명에 따른 프로세서(230)에서 수행되는 연산은, 사용자키에 기초하여 공개키 발행을 요청하고, 서버에서 수신한 공개키를 이용하여, 사용자가 입력한 PIN 번호 데이터를 암호화하고, 암호화된 데이터를 상기 수신된 세션키와 함께 서버로 전송하는 연산을 포함할 수 있다. 상기 사용자키 및 PIN번호는 단말의 웹스토리지에 저장되어 기기 또는 브라우저별로 다르게 설정될 수 있다.
- [116] 다른 예로, 프로세서(230)는 인증토큰을 공개키를 이용하여 암호화하고, 암호화된 데이터를 서버(100)로부터 수신된 세션키와 함께 서버로 전송 할 수 있다.
- [117] 또 다른 예로, 공개키 기반으로 암호화된 인증 데이터(사용자키 및 PIN번호)가 블록체인에 저장될 수 있다. 따라서, 프로세서(230)는 블록체인을 기반으로 사용자가 입력한 PIN번호의 인증 및 검증을 수행하여 변조가능성을 낮춤으로써 신뢰성을 높일 수도 있다.
- [118] 또 다른 예로, 프로세서(230)는 블록체인에 저장된 공개키를 이용하여 사용자가 입력한 PIN번호 데이터를 암호화 할 수 있다.
- [119]

- [120] 한편, 상술한 서버(100) 및 단말(200)은 하나 이상의 프로세서(130, 230) 및/또는 하나 이상의 메모리(140, 240)를 포함할 수 있다. 또한, 메모리(140, 240)는, 휘발성 및/또는 비휘발성 메모리를 포함할 수 있다. 하나 이상의 메모리(140, 240)는, 하나 이상의 프로세서(130, 230)에 의한 실행 시, 하나 이상의 프로세서(130, 230)가 연산을 수행하도록 하는 명령들을 저장할 수 있다. 본 개시에서, 프로그램 내지 명령은 메모리(140, 240)에 저장되는 소프트웨어로서, 서버(100)의 리소스를 제어하기 위한 운영체제, 어플리케이션 및/또는 어플리케이션이 장치의 리소스들을 활용할 수 있도록 다양한 기능을 어플리케이션에 제공하는 미들웨어 등을 포함할 수 있다.
- [121] 하나 이상의 프로세서(130, 230)는, 소프트웨어(예: 프로그램, 명령)를 구동하여 프로세서(130, 230)에 연결된 서버(100) 및 단말(200)의 적어도 하나의 구성요소를 제어할 수 있다. 또한 프로세서(130, 230)는 본 개시와 관련된 다양한 연산, 처리, 데이터 생성, 가공 등의 동작을 수행할 수 있다. 또한 프로세서(130, 230)는 데이터 등을 메모리(140, 240)로부터 로드하거나, 메모리(140, 240)에 저장할 수 있다.
- [122] 본 발명에서는, 서버(100) 및 단말(200)의 구성요소들 중 적어도 하나가 생략되거나, 다른 구성요소가 추가될 수 있다. 또한 추가적으로(additionally) 또는 대체적으로(alternatively), 일부의 구성요소들이 통합되어 구현되거나, 단수 또는 복수의 개체로 구현될 수 있다.
- [123] 상술한, 통신부(150, 250)는 eMBB(enhanced Mobile Broadband), URLLC(Ultra Reliable Low-Latency Communications), MMTC(Massive Machine Type Communications), LTE(long-term evolution), LTE-A(LTE Advance), UMTS(Universal Mobile Telecommunications System), GSM(Global System for Mobile communications), CDMA(code division multiple access), WCDMA(wideband CDMA), WiBro(Wireless Broadband), WiFi(wireless fidelity), 블루투스(Bluetooth), NFC(near field communication), GPS(Global Positioning System) 또는 GNSS(global navigation satellite system) 등의 방식에 따른 무선 통신을 수행할 수 있다.
- [124] 상술한 입력부(260)는, 키보드, 마우스, 터치패드, 카메라 모듈 등 사용자의 간편인증 정보(PIN 번호)를 단말(200)에 입력하는 수단을 포함할 수 있다.
- [125] 한편, 본 발명과 관련하여 설명된 방법 또는 알고리즘의 단계들은 하드웨어로 직접 구현되거나, 하드웨어에 의해 실행되는 소프트웨어 모듈로 구현되거나, 또는 이들의 결합에 의해 구현될 수 있다. 소프트웨어 모듈은 RAM(Random Access Memory), ROM(Read Only Memory), EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM), 플래시 메모리(Flash Memory), 하드 디스크, 착탈형 디스크, CD-ROM, 또는 본 발명이 속하는 기술 분야에서 잘 알려진 임의의 형태의 컴퓨터 추출가능 기록매체에 상주할 수도 있다.
- [126]

- [127] 또한, 본 발명은 모바일웹이나 PC웹에서 간편인증을 하기 위해 공개키 기반으로 1회성 키를 생성하고 사용 후 이를 바로 포기하는 간편인증 방법을 제공할 수 있고, 특히, 웹스토리지를 이용하여 사용기기 및 브라우저별 개인키를 발급할 수 있다.
- [128] 또한, 본 발명은 공개키(Public key) 및 개인키(Private key) 요소들의 단말 및 서버에 분산저장하는 방법을 통해 개인정보와 보안을 강화할 수 있다.
- [129] 또한, 본 발명은 분산 저장된 공개키(Public key) 및 개인키(Private key) 요소들을 이용하여 1회성 키 생성을 지원함으로써 간편 인증 방식에 있어서 보다 강력한 보안을 제공할 수 있다. 즉, 키값을 보관하지 않고 필요시마다 생성 및 폐기할 수 있어 키값이 유출되는 것을 방지할 수 있다. 또한, 웹스토리지를 활용하여 하나의 플랫폼에서 사용기기 및 브라우저별 개인 키를 발급하여 저장할 수 있기 때문에 구현비용 및 관리비용을 효율화 할 수 있다.
- [130] 나아가, 브라우저 저장소 및 서버에 보관된 요소를 이용하여 보안이 강력해진 공개키 및 개인키를 이용할 수 있기 때문에, 공인인증서를 대체할 수 있을 정도로 신뢰성이 높으면서도 간편한 인증방법을 제공할 수 있다.
- [131] 이하, 도 8 내지 14를 참조하여, 본 발명에 따라 공개키 및 개인키 요소들의 분산저장을 통한 간편인증 과정에 대해 상세히 설명한다.
- [132] 도 8은 본 발명에 따른 공개키 및 개인키의 구성요소 분산저장을 통한 간편인증 시스템을 설명하기 위한 개념도이다.
- [133] 도 8을 참조하면, 본 발명에 따른 간편인증 시스템은 서버(1000)와 단말(2000)을 포함할 수 있다. 구체적으로, 간편인증 시스템에서는 인터넷을 통해 정부기관, 교육기관, 의료기관, 통신회사, 금융회사, 여객회사, 자산관리, 신용정보, 포털, 소셜네트워크서비스(Social Network Service: SNS), 게임, 쇼핑, 발권, 택배, 전자투표 등의 수많은 온라인 서비스를 이용하기 위한 사용자 인증에 필요한 데이터를 단말(2000)이 개인키를 기반으로 데이터를 암호화하여 서버(1000)로 보내면, 서버(1000)는 공개키 기반으로 데이터를 복호화하여 사용자를 인증할 수 있다. 반대로, 서버(1000)는 공개키 기반 암호화 데이터를 단말로 보내 단말(2000)에서 이를 개인키 기반으로 복호화할 수도 있다. 한편, 상술한 간편인증을 위해 개인키를 통해서 암호화 되는 데이터는 PIN사용자키 및 PIN번호를 포함할 수 있다.
- [134] 그런데, 이러한 사용자 인증 방식에 필요한 공개키 및 개인키는 브라우저 저장소(local storage)에 평문 저장방식을 사용하여 저장되고 있는 경우가 많아 보안의 문제가 발생하기 쉽다. 물론 보안책으로 암호화 방식을 취하고 있지만 이러한 방법도 여전히 개인정보 유출이나 보안의 문제가 많을 수 있다.
- [135] 따라서, 본 발명에 따른 간편인증 시스템은, 서버(1000)에서 생성된 공개키 및 개인키에서, 계수(modulus, 1100), 개인 지수(private exponent, 2100) 및 공개 지수(public exponent, 1200)를 추출한 뒤, 상기 개인 지수(2100)를 단말(2000)에 저장하고, 상기 계수(1100) 및 공개 지수(1200)를 서버(1000)에 저장하여

보안성을 강화할 수 있다.

- [136] 즉, 간편인증 시스템은, 간편인증 시에 단말(2000)에 저장된 개인 지수(2100)와 서버(1000)에 저장된 계수(1100)를 이용하여 개인키를 생성하거나, 서버(1000)에 저장된 공개 지수(1200)와 계수(1100)를 이용하여 공개키를 생성할 수 있다.
- [137] 한편, 또 본 발명에 따른 간편인증 시스템은 이러한 개인키 및 공개키를 생성하기 위한 계수(1100), 공개 지수(1200)를 블록체인을 이용하여 분산 저장함으로써, 중앙 서버(1000) 없이도 상술한 간편인증 시스템을 구현할 수도 있다.
- [138] 따라서, 상술한 간편인증 시스템은 분산 저장된 공개키(Public key) 및 개인키(Private key) 요소들을 이용하여 1회성 키 생성을 지원함으로써 간편 인증 방식에 있어서 보다 강력한 보안을 제공할 수 있다. 즉, 키값을 보관하지 않고 필요시마다 생성 및 폐기할 수 있어 키값이 유출되는 것을 방지할 수 있다. 또한, 웹스토리지를 활용하여 개인키 요소를 저장한다면 하나의 플랫폼에서 사용기기 및 브라우저별 개인 키를 발급하여 저장할 수 있기 때문에 구현비용 및 관리비용을 효율화할 수도 있다.
- [139] 나아가, 브라우저 저장소 및 서버에 보관된 요소를 이용하여 보안이 강력해진 공개키 및 개인키를 이용할 수 있기 때문에, 공인인증서를 대체할 수 있을 정도로 신뢰성이 높으면서도 간편한 인증방법을 제공할 수 있다.
- [140] 이하 도 9 내지 도 14를 참조하여 공개키 및 개인키의 구성요소 분산저장을 통한 간편인증 방법 및 장치에 대해 보다 상세히 후술한다.
- [141]
- [142] 도 9는 본 발명에 따른 공개키 및 개인키의 구성요소 분산저장을 통한 간편인증 방법을 설명하는 순서도이다.
- [143] 도 9를 참조하면, 단계 S900에서 본 발명에 따른 간편인증 시스템은 사용자 간편인증을 위해 서버(1000)에서 공개키 및 개인키를 생성한다. 여기서, 상기 공개키는 사용자 식별 데이터와 연계하여 RSA 방식으로 생성된 것일 수 있다.
- [144] 다음으로, 단계 S910에서, 간편인증 시스템은 생성된 공개키 및 개인키에서, 계수(modulus), 개인 지수(private exponent) 및 공개 지수(public exponent)를 추출한다. 여기서 공개 지수는 16진수로 변환되어 컴파일될 수 있으며, 따라서 추후 공개키 생성시 컴파일 된 상태의 데이터가 이용될 수도 있다.
- [145] 단계 S920에서, 간편인증 시스템은 개인 지수는 단말(2000)에 저장되고, 계수 및 공개 지수는 서버(1000)에 저장되도록 한다.
- [146] 단계 S930에서, 간편인증 시스템은 단말(2000)에 저장된 개인 지수와 서버(1000)에 저장된 계수를 이용하여 생성된 개인키 및 서버(1000)에 저장된 공개 지수와 계수를 이용하여 생성된 공개키를 이용하여 간편인증을 수행한다.
- [147] 한편, 단말(2000)에 저장된 개인 지수와 서버(1000)에 저장된 계수를 이용하여 생성된 개인키 및 상기 서버에 저장된 공개 지수와 계수를 이용하여 생성된 공개키 각각 암호화 또는 복호화에 1회 사용된 뒤 폐기될 수 있다.

- [148]
- [149] 이하 도 10 내지 도 12를 참고하여 상술한 간편인증 시스템에서 서버(1000) 및 단말(2000)이 동작하는 것에 대해 보다 상세히 설명한다.
- [150] 도 10은 본 발명에 따른 공개키 및 개인키의 구성요소 분산저장을 수행하는 방법의 일 예를 설명하는 도이다.
- [151] 도 10을 참조하면, 단계 S1010에서 서버(1000)는 공개키 및 개인 키를 생성한다. 여기서 생성되는 공개키는 사용자 식별 데이터와 연계하여 RSA 방식으로 생성되는 것일 수 있다.
- [152] 다음으로 단계 S1020에서, 서버(1000)는 생성된 공개키 및 개인키에서, 계수(modulus), 개인 지수(private exponent) 및 공개 지수(public exponent)를 추출한다. 상기 공개 지수는 16진수로 변환되어 컴파일될 수 있으며, 따라서 추후 공개키 생성시 컴파일 된 상태의 데이터가 이용될 수도 있다.
- [153] 단계 S1030에서, 서버(1000)는 추출된 개인 지수를 단말(2000)로 전송하고, 단계 S1040으로 진행하여, 서버(1000)에 계수 및 공개 지수를 저장한다. 여기서 공개 지수는 16진수로 변환되어 컴파일 될 수 있다.
- [154] 한편, 단계 S1050에서, 단말(2000)은 수신한 개인 지수를 브라우저 저장소에 저장한다.
- [155] 도 11은 본 발명에 따라 단말에서 개인키를 생성하는 일 예를 설명하는 순서도이다.
- [156] 도 11을 참조하면, 단계 S1110에서 단말(2000)로부터 간편인증을 수행하겠다는 요청을 수신하면, 서버(1000)는 도 10의 단계 S1040에서 저장한 계수를 단말(2000)로 전송한다(S1120).
- [157] 단계 S1130에서 단말(2000)은 수신한 계수 및 저장된 개인지수(2100)를 이용하여 개인키를 생성한다.
- [158] 단계 S1140에서는 단말(2000)은 생성된 개인키를 이용하여 데이터 암호화 및 전자서명을 수행한다. 그리고 단계 S1150으로 진행하여, 단말은 암호화된 데이터 및 전자서명을 서버(1000)로 전송한다. 한편 개인키는 1회 사용된 뒤 바로 폐기된다(S1160).
- [159] 단계 S1170에서는, 이렇게 서버(1000)로 전송된 암호화된 데이터 및 전자서명은 공개키를 이용하여 복호화되고, 복호화된 데이터가 전송된 전자서명을 이용하여 검증받게 된다.
- [160] 예를 들면, 도 12는 본 발명에 따라 서버에서 공개키를 생성하는 일 예를 설명하는 순서도이다.
- [161] 도 12를 참조하면, 단계 S1171에서 서버(1000)는 저장된 계수(1100)와 컴파일된 공개지수(1200)를 이용하여 공개키를 생성한다.
- [162] 단계 S1172에서 서버(1000)는 생성된 공개키를 이용하여 복호화 및 검증을 수행하고, 1회 사용된 공개키는 폐기된다(S1173).
- [163] 따라서, 본 발명에 따라 분산 저장된 공개키(public key) 및 개인키(private key)

요소들을 이용하여 1회성 키 생성을 지원함으로써 간편 인증 방식에 있어서 보다 강력한 보안을 제공할 수 있다.

[164]

[165] 도 13은 본 발명에 따른 공개키 및 개인키의 구성요소 분산저장을 통한 간편인증과정을 수행하는 서버(1000)의 내부 구성을, 도 14는 본 발명에 따른 공개키 및 개인키의 구성요소 분산저장을 통한 간편인증과정을 수행하는 단말(2000)의 내부 구성을 개략적으로 나타낸 블록 도이다.

[166] 도 13 및 도 14에는 본 발명을 설명하기 위해 필요한 구성만이 도시되었으나, 디스플레이 장치 등 다양한 구성이 더 포함될 수 있다. 또한 도 13 및 도 14에 대한 설명에서 생략되더라도 도 8 내지 12에서 상술된 방법을 수행하기 위해 필요한 구성이 더 포함될 수 있음을 본 발명이 속하는 분야의 통상의 기술자에게는 자명하다.

[167]

[168] 도 13을 참조하면 본 발명에 따른 서버(1000)는, 프로세서(1300), 메모리(1400) 및 통신부(1500)를 포함할 수 있다. 간편인증 서버(1000)의 동작은 메모리(1400)에 저장된 프로그램을 프로세서(1300)를 통해서 실행시킴으로써 수행될 수 있다.

[169] 본 발명에 따른 프로세서(1300)에서 수행되는 연산은, 사용자 간편인증을 위해 생성된 공개키 및 개인키에서 계수(modulus), 상기 개인 지수 및 공개 지수(public exponent)를 추출하여, 상기 개인 지수를 단말로 전송하고, 상기 계수 및 공개 지수를 저장하고, 공개 지수와 계수를 이용하여 생성된 공개키를 생성하도록 하는 연산을 수행할 수 있다. 여기서, 하나 이상의 메모리(1400)는 계수 및 공개 지수를 저장할 수 있다.

[170] 본 발명에 따른 프로세서(1300)는 저장된 계수 및 공개 지수를 이용하여 공개키를 생성하고 생성된 공개키로 단말로부터 수신한 암호화 된 데이터를 복호화 한뒤, 공개키를 다시 폐기하도록 하는 연산을 수행할 수도 있다.

[171] 여기서, 공개 지수는 16진수로 변환되어 컴파일되는 것이며, 상기 공개키는 사용자 식별 데이터와 연계하여 RSA 방식으로 생성된 것일 수 있다.

[172]

[173] 또한, 통신부(1500)는, 단말(2000)과 또는 다른 서버 또는 다른 외부 장치 간의 무선 또는 유선 통신을 수행할 수 있다. 예를 들면 통신부(1500)는 단말(2000)에 개인 지수 또는 계수를 전달할 수 있다.

[174]

[175] 도 14를 참조하면 본 발명에 따른 단말(2000)은, 프로세서(2300), 메모리(2400), 통신부(2500) 및 입력부(2600)를 포함할 수 있다. 간편인증 단말(2000)의 동작은 메모리(2400)에 저장된 프로그램을 프로세서(2300)를 통해서 실행시킴으로써 수행될 수 있다.

[176] 본 발명에 따른 프로세서(2300)에서 수행되는 연산은, 개인 지수(private

exponent)를 저장하고, 사용자 간편인증시에 서버에 저장된 계수를 수신하여 개인키 생성하도록 하는 연산을 포함 할 수 있다.

- [177] 예를 들면, 프로세서(2300)는 입력부(2600)를 통해 입력된 사용자의 간편인증 정보(예컨대 PIN 번호)를 암호화하기 위해 서버(1000)에서 계수를 수신하고 개인 지수와 결합시켜 개인키를 생성할 수 있다.
- [178] 또한, 프로세서(2300)는 개인키를 이용하여 암호화한 데이터 및 전자서명 정보를 서버(1000)로 전달하여 간편인증을 수행하도록 할 수 있다.
- [179] 한편, 상술한 서버(1000) 및 단말(2000)은 하나 이상의 프로세서(1300, 2300) 및/또는 하나 이상의 메모리(1400, 2400)를 포함할 수 있다. 또한, 메모리(1400, 2400)는, 휘발성 및/또는 비휘발성 메모리를 포함할 수 있다. 하나 이상의 메모리(1400, 2400)는, 하나 이상의 프로세서(1300, 2300)에 의한 실행 시, 하나 이상의 프로세서(1300, 2300)가 연산을 수행하도록 하는 명령들을 저장할 수 있다. 본 개시에서, 프로그램 내지 명령은 메모리(1400, 2400)에 저장되는 소프트웨어로서, 서버(1000)의 리소스를 제어하기 위한 운영체제, 어플리케이션 및/또는 어플리케이션이 장치의 리소스들을 활용할 수 있도록 다양한 기능을 어플리케이션에 제공하는 미들 웨어 등을 포함할 수 있다.
- [180] 하나 이상의 프로세서(1300, 2300)는, 소프트웨어(예: 프로그램, 명령)를 구동하여 프로세서(1300, 2300)에 연결된 서버(1000) 및 단말(2000)의 적어도 하나의 구성요소를 제어할 수 있다. 또한 프로세서(1300, 2300)는 본 개시와 관련된 다양한 연산, 처리, 데이터 생성, 가공 등의 동작을 수행할 수 있다. 또한 프로세서(1300, 2300)는 데이터 등을 메모리(1400, 2400)로부터 로드하거나, 메모리(1400, 2400)에 저장할 수 있다.
- [181] 본 발명에서는, 서버(1000) 및 단말(2000)의 구성요소들 중 적어도 하나가 생략되거나, 다른 구성요소가 추가될 수 있다. 또한 추가적으로(additionally) 또는 대체적으로(alternatively), 일부의 구성요소들이 통합되어 구현되거나, 단수 또는 복수의 개체로 구현될 수 있다.
- [182] 상술한, 통신부(1500, 2500)는 eMBB(enhanced Mobile Broadband), URLLC(Ultra Reliable Low-Latency Communications), MMTC(Massive Machine Type Communications), LTE(long-term evolution), LTE-A(LTE Advance), UMTS(Universal Mobile Telecommunications System), GSM(Global System for Mobile communications), CDMA(code division multiple access), WCDMA(wideband CDMA), WiBro(Wireless Broadband), WiFi(wireless fidelity), 블루투스(Bluetooth), NFC(near field communication), GPS(Global Positioning System) 또는 GNSS(global navigation satellite system) 등의 방식에 따른 무선 통신을 수행할 수 있다.
- [183] 상술한 입력부(2600)는, 키보드, 마우스, 터치패드, 카메라 모듈 등 사용자의 간편인증 정보를 단말(2000)에 입력하는 수단을 포함할 수 있다.
- [184] 한편, 본 발명과 관련하여 설명된 방법 또는 알고리즘의 단계들은 하드웨어로 직접 구현되거나, 하드웨어에 의해 실행되는 소프트웨어 모듈로 구현되거나,

또는 이들의 결합에 의해 구현될 수 있다. 소프트웨어 모듈은 RAM(Random Access Memory), ROM(Read Only Memory), EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM), 플래시 메모리(Flash Memory), 하드 디스크, 착탈형 디스크, CD-ROM, 또는 본 발명이 속하는 기술 분야에서 잘 알려진 임의의 형태의 컴퓨터 추출가능 기록매체에 상주할 수도 있다.

- [185] 이상, 첨부된 도면을 참조로 하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야의 통상의 기술자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며, 제한적이 아닌 것으로 이해해야만 한다.