

청구범위

- [청구항 1] 브라우저의 웹스토리지를 이용한 간편인증 방법에 있어서,
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 복호화 하여 간편인증을 수행하는 단계를
포함하고,
상기 사용자키는 단말의 웹스토리지에 저장되어 기기 또는 브라우저별로
다르게 설정되는 것인 방법.
- [청구항 2] 제 1항에 있어서,
상기 공개키는 블록체인에 저장되어 변조 또는 위조가 되었는지
검증하는데 이용되는 것인 방법.
- [청구항 3] 제 1항에 있어서, 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 포함하는 방법.
- [청구항 4] 제 1항에 있어서, 상기 사용자키는 암호화 알고리즘으로 암호화되고,
PIN번호는 해시 암호화되어 상기 웹스토리지에 저장되는 것인 방법.
- [청구항 5] 제 1항에 있어서, 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 포함하는 방법.
- [청구항 6] 제 1항에 있어서, 상기 공개키를 단말에 전송하는 단계는,
단말은 상기 웹스토리지에 상기 사용자키가 저장되어 있는지 판단하는
단계; 및
상기 사용자키가 저장되어 있지 않은 경우, 사용자로부터 PIN 번호를
등록받는 단계를 더 포함하는 방법.
- [청구항 7] 제 1항에 있어서, 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 것인 방법.

- [청구항 8] 제 1항에 있어서,
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 포함하는 것인 방법.
- [청구항 9] 제 8항에 있어서, 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 포함하는 것인 방법.
- [청구항 10] 제 9항에 있어서, 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 검증을 수행하는 단계; 및
상기 공개키를 폐기하는 단계를 더 포함하는 것인 방법.
- [청구항 11] 웹스토리를 이용한 간편인증 시스템에 있어서,
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 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 설정되는 것인 시스템.
- [청구항 12] 제 11항에 있어서,
상기 공개키는 블록체인에 저장되어 변조 또는 위조가 되었는지 검증하는데 이용되는 것인 시스템.
- [청구항 13] 제 11항에 있어서,
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 수행하는 것을 특징으로 하는 시스템.
- [청구항 14] 제 11항에 있어서, 상기 서버는,
상기 복원된 PIN번호가 비매칭 될때마다 인증시도 횟수를 갱신하고, 상기 인증시도 횟수가 소정 개수 이상 증가하는 경우 상기 서버 및/또는 단말에 저장된 PIN번호 데이터를 삭제하는 시스템.
- [청구항 15] 하드웨어인 컴퓨터와 결합되어, 제1항 내지 제10항 중 어느 한 항의 방법을 실행시키기 위하여 매체에 저장된, 간편인증 프로그램.