(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0167366
(43) 공개일자 2022년12월20일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 21/34* (2013.01)
G06F 21/45 (2013.01) *H04L 9/06* (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3228 (2013.01)
G06F 21/34 (2013.01)
(21) 출원번호 10-2022-0173336(분할)
(22) 출원일자 2022년12월13일
심사청구일자 2022년12월13일
(62) 원출원 특허 10-2021-0123680
원출원일자 2021년09월16일
심사청구일자 2021년09월16일

(71) 출원인
(주)이스톰
서울특별시 금천구 디지털로 130, 남성프라자 에이스9차 1310호 1311호 (가산동)
(72) 발명자
우종현
서울특별시 영등포구 도신로29길 28, 108동 2001호 (영등포동, 영등포푸르지오)
(74) 대리인
강경돈

전체 청구항 수 : 총 4 항

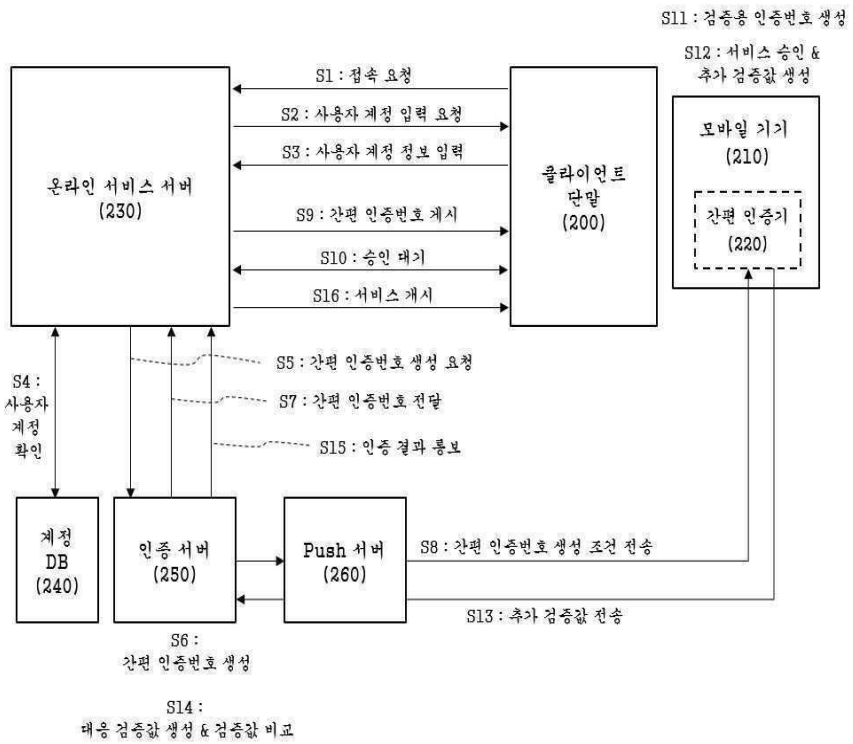
(54) 발명의 명칭 **온라인 서비스 서버와 클라이언트 간의 상호 인증 방법 및 시스템**

(57) 요 약

온라인 서비스 서버와 서비스 사용자 간의 상호 인증을 수행하는 컴퓨터 구현 방법(computer implemented method)으로서, (a) 인증 서버가, 상기 온라인 서버로부터 상기 온라인 서버에 접속하는 서비스 사용자의 사용자 계정 정보를 포함하는 간편 인증번호 생성 요청이 수신됨에 따라 간편 인증번호를 생성하는 단계; (b) 상기 인증

(뒷면에 계속)

대 표 도 - 도1



서버가, 상기 간편 인증번호의 생성에 사용된 생성 조건을 상기 사용자 계정 정보에 상응하는 사용자의 간편 인증기로 전송하는 단계; (c) 상기 간편 인증기가, 상기 간편 인증번호의 생성 조건을 이용하여 상기 간편 인증번호에 대응되는 검증용 인증번호를 생성하는 단계; 및 (d) 상기 인증 서버가, 상기 간편 인증번호 및 상기 검증용 인증번호를 통한 상기 온라인 서비스 서버에 관한 검증이 완료됨에 따라 상기 간편 인증기로부터 전달되는 추가 검증값에 대응하여 대응 검증값을 생성하고, 상기 추가 검증값과 상기 대응 검증값 간의 일치 여부를 비교함으로써 해당 서비스 사용자에 대한 인증을 수행하는 단계를 포함하는 상호 인증을 위한 컴퓨터 구현 방법이 제공된다.

(52) CPC특허분류
G06F 21/45 (2013.01)
H04L 9/0656 (2013.01)
H04L 9/0863 (2013.01)

명 세 서

청구범위

청구항 1

온라인 서비스 서버와 서비스 사용자 간의 상호 인증을 수행하는 컴퓨터 구현 방법(computer implemented method)으로서,

(a) 인증 서버가, 상기 온라인 서버로부터 상기 온라인 서버에 접속하는 서비스 사용자의 사용자 계정 정보를 포함하는 간편 인증번호 생성 요청이 수신됨에 따라 간편 인증번호를 생성하는 단계;

(b) 상기 인증 서버가, 상기 간편 인증번호의 생성에 사용된 생성 조건을 상기 사용자 계정 정보에 상응하는 사용자의 간편 인증기로 전송하는 단계;

(c) 상기 간편 인증기가, 상기 간편 인증번호의 생성 조건을 이용하여 상기 간편 인증번호에 대응되는 검증용 인증번호를 생성하는 단계; 및

(d) 상기 인증 서버가, 상기 간편 인증번호 및 상기 검증용 인증번호를 통한 상기 온라인 서비스 서버에 관한 검증이 완료됨에 따라 상기 간편 인증기로부터 전달되는 추가 검증값에 대응하여 대응 검증값을 생성하고, 상기 추가 검증값과 상기 대응 검증값 간의 일치 여부를 비교함으로써 해당 서비스 사용자에 대한 인증을 수행하는 단계

를 포함하는 상호 인증을 위한 컴퓨터 구현 방법.

청구항 2

제1항에 있어서,

상기 간편 인증번호 생성 요청은, 상기 서비스 사용자가 상기 온라인 서비스 서버가 제공하는 온라인 사이트에 입력한 상기 사용자 계정 정보가 사전 등록된 해당 사용자의 계정 정보와 일치하는 경우, 상기 온라인 서비스 서버로부터 상기 인증 서버로 전송되고,

상기 (b) 단계에서, 상기 간편 인증번호의 생성 조건은 푸시 메시지 또는 소켓 데이터 통신을 통해서 상기 인증 서버로부터 상기 사용자 계정 정보에 상응하는 사용자의 모바일 기기 또는 해당 모바일 기기에 설치된 상기 간편 인증기로 전송되는, 상호 인증을 위한 컴퓨터 구현 방법.

청구항 3

제1항에 있어서,

상기 단계 (a)에서, 상기 인증 서버는, 상기 온라인 서비스 서버로부터 상기 온라인 서비스 서버에 접속한 해당 서비스 사용자의 접속단말에 대한 클라이언트 접속환경정보를 더 수신하되, 상기 간편 인증번호를 생성할 때 상기 클라이언트 접속정보를 이용하고,

상기 단계 (b)에서, 상기 인증 서버는, 상기 클라이언트 접속환경정보를 포함하는 상기 간편 인증번호의 생성 조건을 상기 간편 인증기로 전송하고,

상기 클라이언트 접속환경정보는,

상기 온라인 서비스 서버에 접속한 접속단말과 관련된 서버 변수, 호스트 네임, 쿠키 정보, 이전 URL, 현재 접속 IP 주소, 한 단계 앞의 접속 IP 주소, 클라이언트 브라우저 정보, 클라이언트 언어 정보, 접속단말의 시스템 변수, 접속단말에 서비스를 제공하는 온라인 서비스 서버의 서버 호스트명, 서버 IP 주소, 세션 아이디, 세션 최대 유효시간 정보 중 적어도 하나인, 상호 인증을 위한 컴퓨터 구현 방법.

청구항 4

제3항에 있어서,

상기 단계 (a)에서, 상기 인증 서버는, 상기 클라이언트 접속환경정보를 제1 시드값, 사전 지정된 적어도 하나의 추가 정보를 제2 시드값으로 하되 시간 또는 시도횟수를 연산 조건으로 하여 상기 간편 인증번호를 생성하고,

상기 단계 (c)에서, 상기 간편 인증기는, 상기 간편 인증번호와 동일 생성 조건을 적용하여 상기 검증용 인증번호를 생성하고,

상기 간편 인증번호 및 상기 검증용 인증번호를 통해서 상기 온라인 서비스 서버에 관한 검증이 완료된 경우, 상기 간편 인증기는, 사전 지정된 조건에 따라 상기 추가 검증값을 생성하여 상기 인증 서버로 전송하고,

상기 인증 서버는 상기 사전 지정된 조건과 동일 조건을 적용하여 상기 대응 검증값을 생성하고, 상기 추가 검증값과 상기 대응 검증값이 일치하는 경우 상기 온라인 서비스 서버로 정상 인증을 통지하는, 상호 인증을 위한 컴퓨터 구현 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 인증 방법 및 시스템에 관한 것으로서, 보다 구체적으로는 온라인 서비스 서버와 클라이언트 간의 상호 인증 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 편리한 전자 금융 서비스나 중요한 온라인 서비스를 안전하게 활용하고자 할 때 온라인 서비스에서 사용되는 아이디와 암호 이외에 별도의 인증 방법을 구성하여 사용자 인증에 대한 안전성을 높이고 있다. 대표적으로 OTP 동글, SMS를 통한 일회용 비밀번호, ARS를 통한 일회용 비밀번호, 모바일 앱(Mobile App) 기반 본인 생체인증 등을 활용하여 아이디 패스워드 도용에 따른 본인 인증을 강화하고 있다.

[0003] 그러나 종래 추가 인증 수단들은 온라인 서비스와 인증 매체 간에 발생한 일회용 비밀번호를 사용자가 직접 입력하게 하거나, 별도의 생체 정보를 입력하는 등과 같이 사용자의 번잡한 입력을 요구하게 된다. 특히 모바일 폰으로 4~6자리의 임시 비밀번호를 재입력해야 되면, 모바일 폰 화면을 통해 확인되는 번호를 숙지하기도 어려울 뿐만 아니라 입력하기도 번잡하다.

[0004] 이러한 임시 비밀번호의 입력을 없애기 위해서 사용자가 서비스에 아이디와 패스워드로 로그 온하면 푸시 정보를 모바일 폰에 보내고, 사용자가 본인 확인 인증 앱을 구동하면 본인의 생체정보(지문, 얼굴, 홍채 등)를 모바일 앱에 입력하도록 함으로써, 본인이 맞으면 자동으로 온라인 서비스를 로그인 해주는 서비스가 있는데, 이 역시 생체정보를 입력하기 위한 번잡함이 발생한다.

[0005] 또 다른 간편 인증 방식으로는 사용자의 입력을 최소화 시키고자 사전에 사용자의 지정된 모바일 폰에 접속 승인 여부를 결정하는 접속 제어 앱을 설치한 상태에서, 사용자가 온라인 서비스에 아이디와 패스워드를 입력하면 모바일 푸시 메시지로 사용자 접속을 알려주고, 사용자가 접속 승인 앱을 구동하면 온라인 서비스의 접속 여부를 승인하거나 거절하는 접속 확인 방식도 있었다. 그러나 이 방식은 사용자가 접속한 서비스가 파밍(pharming)된 해커의 사이트인 경우, 사용자가 입력한 아이디와 패스워드를 해커가 역이용하여 실제 온라인 서비스에 전송하면 사용자는 자신의 모바일 폰에 접속 확인 요청이 왔을 때 본인의 접속으로 오해하고 해당 접속을 승인해 주게 되는 문제가 발생하게 된다. 뿐만 아니라 사용자의 아이디와 패스워드를 알고 있는 해커가 실제 사용자가 접속하자 마자, 해당 사용자의 아이디와 패스워드로 접속을 하게 되면 사용자는 자신의 스마트폰에 도착한 최종 접속 내용을 자신의 것으로 오해하고 해당 접속을 승인하게 해줄 수도 있다.

[0006] 따라서 사용자가 임시 비밀번호를 재입력하는 번잡함이 없으면서도, 해당 사이트가 정상인지 인지를 판단할 수도 있고, 자신의 접속인지 아닌지 까지 확인할 수 있는 개선된 방법과 기술이 필요하다.

발명의 내용

해결하려는 과제

[0007] 본 발명은 온라인 서비스의 안전한 사용을 위해 2팩트 인증(즉, 서비스 인증 및 사용자 인증에 따른 상호 간 인증)을 수행할 때, 별도의 일회용 암호나 생체 정보를 입력하지 않고도 올바른 서비스인지에 대해서 사용자가 확인한 후 편리하게 접속이 진행될 수 있도록 하는 간편 인증을 위한 방법 및 시스템을 제공한다.

과제의 해결 수단

[0008] 본 발명의 일 측면에 따르면, 온라인 서비스 서버와 서비스 사용자 간의 상호 인증을 수행하는 컴퓨터 구현 방법(computer implemented method)으로서,

[0009] (a) 인증 서버가, 상기 온라인 서버로부터 상기 온라인 서버에 접속하는 서비스 사용자의 사용자 계정 정보를 포함하는 간편 인증번호 생성 요청이 수신됨에 따라 간편 인증번호를 생성하는 단계;

[0010] (b) 상기 인증 서버가, 상기 간편 인증번호의 생성에 사용된 생성 조건을 상기 사용자 계정 정보에 상응하는 사용자의 간편 인증기로 전송하는 단계;

[0011] (c) 상기 간편 인증기가, 상기 간편 인증번호의 생성 조건을 이용하여 상기 간편 인증번호에 대응되는 검증용 인증번호를 생성하는 단계; 및

[0012] (d) 상기 인증 서버가, 상기 간편 인증번호 및 상기 검증용 인증번호를 통한 상기 온라인 서비스 서버에 관한 검증이 완료됨에 따라 상기 간편 인증기로부터 전달되는 추가 검증값에 대응하여 대응 검증값을 생성하고, 상기 추가 검증값과 상기 대응 검증값 간의 일치 여부를 비교함으로써 해당 서비스 사용자에 대한 인증을 수행하는 단계를 포함하는 상호 인증을 위한 컴퓨터 구현 방법이 제공된다.

[0013] 일 실시예에서, 상기 간편 인증번호 생성 요청은, 상기 서비스 사용자가 상기 온라인 서비스 서버가 제공하는 온라인 사이트에 입력한 상기 사용자 계정 정보가 사전 등록된 해당 사용자의 계정 정보와 일치하는 경우, 상기 온라인 서비스 서버로부터 상기 인증 서버로 전송될 수 있다.

[0014] 일 실시예에서, 상기 (b) 단계에서, 상기 간편 인증번호의 생성 조건은 푸시 메시지 또는 소켓 데이터 통신을 통해서 상기 인증 서버로부터 상기 사용자 계정 정보에 상응하는 사용자의 모바일 기기 또는 해당 모바일 기기에 설치된 상기 간편 인증기로 전송될 수 있다.

[0015] 일 실시예에서, 상기 단계 (a)에서, 상기 인증 서버는, 상기 온라인 서비스 서버로부터 상기 온라인 서비스 서버에 접속한 해당 서비스 사용자의 접속단말에 대한 클라이언트 접속환경정보를 더 수신하되, 상기 간편 인증번호를 생성할 때 상기 클라이언트 접속정보를 이용하고,

[0016] 상기 단계 (b)에서, 상기 인증 서버는, 상기 클라이언트 접속환경정보를 포함하는 상기 간편 인증번호의 생성 조건을 상기 간편 인증기로 전송할 수 있다.

[0017] 일 실시예에서, 상기 클라이언트 접속환경정보는,

[0018] 상기 온라인 서비스 서버에 접속한 접속단말과 관련된 서버 변수, 호스트 네임, 쿠키 정보, 이전 URL, 현재 접속 IP 주소, 한 단계 앞의 접속 IP 주소, 클라이언트 브라우저 정보, 클라이언트 언어 정보, 접속단말의 시스템 변수, 접속단말에 서비스를 제공하는 온라인 서비스 서버의 서버 호스트명, 서버 IP 주소, 세션 아이디, 세션 최대 유효시간 정보 중 적어도 하나일 수 있다.

[0019] 일 실시예에서, 상기 단계 (a)에서, 상기 인증 서버는, 상기 클라이언트 접속환경정보를 제1 시드값, 사전 지정된 적어도 하나의 추가 정보를 제2 시드값으로 하되 시간 또는 시도횟수를 연산 조건으로 하여 상기 간편 인증번호를 생성하고,

[0020] 상기 단계 (c)에서, 상기 간편 인증기는, 상기 간편 인증번호와 동일 생성 조건을 적용하여 상기 검증용 인증번호를 생성할 수 있다.

[0021] 일 실시예에서, 상기 간편 인증번호 및 상기 검증용 인증번호를 통해서 상기 온라인 서비스 서버에 관한 검증이 완료된 경우, 상기 간편 인증기는, 사전 지정된 조건에 따라 상기 추가 검증값을 생성하여 상기 인증 서버로 전송하고,

[0022] 상기 인증 서버는 상기 사전 지정된 조건과 동일 조건을 적용하여 상기 대응 검증값을 생성하고, 상기 추가 검

증값과 상기 대응 검증값이 일치하는 경우 상기 온라인 서비스 서버로 정상 인증을 통지할 수 있다.

[0023] 일 실시예에서, 상기 인증 서버가, 상기 간편 인증번호가 상기 온라인 서비스 서버에 의해 제공되는 인증번호 게시 화면을 통해 게시되도록 상기 간편 인증번호를 상기 온라인 서비스 서버로 전송하는 단계를 더 포함하고,

[0024] 상기 인증번호 게시 화면을 통한 상기 간편 인증번호의 검증 유효시간이 경과되기 전 또는 상기 서비스 사용자에 의한 상기 온라인 서비스 서버에 관한 검증이 완료되기 전에, 상기 서비스 사용자의 사용자 계정 정보와 동일한 계정 정보를 이용한 후순위의 접속이 시도된 경우,

[0025] 상기 인증 서버는, 상기 간편 인증번호의 검증 유효시간 동안 또는 상기 온라인 서비스 서버에 관한 검증이 완료되기 전까지, 선순위 접속에 따라 생성된 간편 인증번호를 그대로 유지하거나 또는 후순위 접속에 따른 간편 인증번호의 신규 생성을 금지할 수 있다.

[0026] 본 발명의 다른 측면에 따르면, 온라인 서비스 서버와 서비스 사용자 간의 상호 인증을 수행하는 인증 시스템으로서, 인증 서버; 및 상기 인증 서버와 통신하는 서비스 사용자 측의 간편 인증기를 포함하되,

[0027] 상기 인증 서버는,

[0028] 상기 온라인 서버로부터 상기 온라인 서버에 접속하는 서비스 사용자의 사용자 계정 정보를 포함하는 간편 인증번호 생성 요청이 수신됨에 따라 간편 인증번호를 생성하고,

[0029] 상기 간편 인증번호의 검증을 위한 검증용 인증번호가 생성될 수 있도록 상기 간편 인증번호의 생성에 사용된 생성 조건을 상기 사용자 계정 정보에 상응하는 상기 간편 인증기로 전송하며,

[0030] 상기 간편 인증번호 및 상기 검증용 인증번호를 통한 상기 온라인 서비스 서버에 관한 검증이 완료됨에 따라 상기 간편 인증기로부터 전달되는 추가 검증값에 대응하여 대응 검증값을 생성하고, 상기 추가 검증값과 상기 대응 검증값 간의 일치 여부를 비교함으로써 해당 서비스 사용자에 대한 인증을 수행하는, 상호 인증을 위한 인증 시스템이 제공된다.

[0031] 일 실시예에서, 상기 인증 서버는,

[0032] 상기 온라인 서비스 서버로부터 상기 온라인 서비스 서버에 접속한 해당 서비스 사용자의 접속단말에 대한 클라이언트 접속환경정보를 더 수신하되, 상기 간편 인증번호를 생성할 때 상기 클라이언트 접속정보를 이용하고,

[0033] 상기 클라이언트 접속환경정보를 포함하는 상기 간편 인증번호의 생성 조건을 상기 간편 인증기로 전송할 수 있다.

[0034] 일 실시예에서, 상기 클라이언트 접속환경정보는,

[0035] 상기 온라인 서비스 서버에 접속한 접속단말과 관련된 서버 변수, 호스트 네임, 쿠키 정보, 이전 URL, 현재 접속 IP 주소, 한 단계 앞의 접속 IP 주소, 클라이언트 브라우저 정보, 클라이언트 언어 정보, 접속단말의 시스템 변수, 접속단말에 서비스를 제공하는 온라인 서비스 서버의 서버 호스트명, 서버 IP 주소, 세션 아이디, 세션 최대 유효시간 정보 중 적어도 하나일 수 있다.

[0036] 일 실시예에서, 상기 인증 서버는, 상기 클라이언트 접속환경정보를 제1 시드값, 사전 지정된 적어도 하나의 추가 정보를 제2 시드값으로 하되 시간 또는 시도횟수를 연산 조건으로 하여 상기 간편 인증번호를 생성하고,

[0037] 상기 간편 인증기는, 상기 간편 인증번호와 동일 생성 조건을 적용하여 상기 검증용 인증번호를 생성할 수 있다.

[0038] 일 실시예에서, 상기 간편 인증번호 및 상기 검증용 인증번호를 통해서 상기 온라인 서비스 서버에 관한 검증이 완료된 경우, 상기 간편 인증기는, 사전 지정된 조건에 따라 상기 추가 검증값을 생성하여 상기 인증 서버로 전송하고,

[0039] 상기 인증 서버는 상기 사전 지정된 조건과 동일 조건을 적용하여 상기 대응 검증값을 생성하고, 상기 추가 검증값과 상기 대응 검증값이 일치하는 경우 상기 온라인 서비스 서버로 정상 인증을 통지할 수 있다.

[0040] 일 실시예에서, 상기 인증 서버는, 상기 간편 인증번호가 상기 온라인 서비스 서버에 의해 제공되는 인증번호 게시 화면을 통해 게시되도록 상기 간편 인증번호를 상기 온라인 서비스 서버로 전송하고,

[0041] 상기 인증번호 게시 화면을 통한 상기 간편 인증번호의 검증 유효시간이 경과되기 전 또는 상기 서비스 사용자에 의한 상기 온라인 서비스 서버에 관한 검증이 완료되기 전에, 상기 서비스 사용자의 사용자 계정 정보와 동

일한 계정 정보를 이용한 후순위의 접속이 시도된 경우,

[0042] 상기 인증 서버는, 상기 간편 인증번호의 검증 유효시간 동안 또는 상기 온라인 서비스 서버에 관한 검증이 완료되기 전까지, 선순위 접속에 따라 생성된 간편 인증번호를 그대로 유지하거나 또는 후순위 접속에 따른 간편 인증번호의 신규 생성을 금지할 수 있다.

발명의 효과

[0043] 본 발명의 실시예에 의하면, 사용자가 온라인 서비스에 아이디와 패스워드를 입력한 이후 추가 인증을 위해서 서비스에서 제공하는 간편 인증번호와 모바일 간편 인증기가 제공하는 간편 인증번호가 같은 경우 사용자의 서비스 접속을 승인함으로써, 사용자의 불필요한 인증번호 재입력을 없앨 수 있다.

[0044] 또한 본 발명의 실시예에 의하면, 타인이 사용자의 아이디와 패스워드로 온라인 서비스에 접근을 시도하면 간편 인증기를 갖고 있는 사용자는 본인이 아닌 타인에 의해서 접속 허가 요청이 있었다는 상황을 숙지할 수 있어, 사용자 아이디와 패스워드에 대한 보안 관리까지 가능하게 된다.

도면의 간단한 설명

[0045] 도 1은 본 발명의 실시예에 따른 온라인 서비스 서버와 서비스 사용자 간의 상호 인증 방법 및 시스템을 설명하기 위한 도면.

도 2는 본 발명의 실시예에 따른 상호 인증 방법을 구현하는 인증 서버에 관한 일 실시예의 블록도.

도 3은 본 발명의 실시예에 따른 상호 인증 방법을 구현하는 간편 인증기에 관한 일 실시예의 블록도.

도 4는 온라인 서비스 서버에 의해 운영되는 온라인 서비스 사이트에 간편 인증번호가 게시되는 화면과 관련된 예시.

도 5는 간편 인증기에 의해 생성된 검증용 인증번호가 표출되는 화면과 관련된 예시.

도 6은 도 1의 상호 인증 방법에 따른 인증 과정에서 해커에 의한 접속 시도시 처리 방법을 설명하기 위한 도면.

도 7은 도 6과 같은 해커에 의한 접속 시도시의 온라인 서비스 서버에 의해 운영되는 온라인 서비스 사이트에 게시되는 처리 결과를 예시한 도면.

도 8 및 도 9는 사용자의 모바일 기기를 통해 온라인 서비스 서버에 접속하였을 때의 본 발명의 실시예에 따른 상호 인증 방법의 구현 예시.

발명을 실시하기 위한 구체적인 내용

[0046] 본 발명은 다양한 변환을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변환, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0047] 본 발명을 설명함에 있어서, 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 본 명세서의 설명 과정에서 이용되는 숫자(예를 들어, 제1, 제2 등)는 하나의 구성요소를 다른 구성요소와 구분하기 위한 식별기호에 불과하다.

[0048] 또한, 명세서 전체에서, 일 구성요소가 다른 구성요소와 "연결된다" 거나 "접속된다" 등으로 언급된 때에는, 상기 일 구성요소가 상기 다른 구성요소와 직접 연결되거나 또는 직접 접속될 수도 있지만, 특별히 반대되는 기재가 존재하지 않는 이상, 중간에 또 다른 구성요소를 매개하여 연결되거나 또는 접속될 수도 있다고 이해되어야 할 것이다.

[0049] 또한, 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "부", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하나 이상의 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 조합으로 구현될 수 있음을 의미한다.

[0050] 또한 이하의 설명에서, 간편 인증기는 사용자 소유의 모바일 기기에 애플리케이션 프로그램의 형태로 설치된 소

프트웨어 방식의 인증 장치인 경우를 중심으로 설명하지만, 반드시 이에 한정되는 것은 아님은 물론이다. 예를 들어, 간편 인증기는 통신 기능을 갖춘 하드웨어 인증 디바이스일 수도 있다. 다만, 이하에서는 설명의 편의 및 집중을 위해 전자의 케이스를 가정하여 본 발명의 실시예를 설명하기로 한다.

[0051] 또한, 이하에서는 도 1을 기준으로 온라인 서비스 서버에 접속하는 접속단말인 클라이언트 단말과 간편 인증기가 물리적으로 별개로 구성된 경우를 가정하여 설명하지만, 간편 인증기는 클라이언트 단말과 일체적으로 구현될 수도 있다. 후자의 경우라면 도 1에 도시된 모바일 기기는 생략될 것이다. 또한, 클라이언트 단말 자체가 모바일 기기일 수도 있음은 자명하다.

[0052] 도 1은 본 발명의 실시예에 따른 온라인 서비스 서버와 서비스 사용자 간의 상호 인증 방법 및 시스템을 설명하기 위한 도면이다. 또한, 도 2는 본 발명의 실시예에 따른 상호 인증 방법을 구현하는 인증 서버에 관한 일 실시예의 블록도이고, 도 3은 본 발명의 실시예에 따른 상호 인증 방법을 구현하는 간편 인증기에 관한 일 실시예의 블록도이다. 이하, 도 1을 중심으로 도 2 및 도 3을 참조하여, 본 발명의 실시예에 따른 상호 인증 방법 및 시스템을 설명한다.

[0053] 또한, 본 발명의 실시예의 설명 과정에서, 도 4 ~ 도 9를 함께 참조한다. 여기서, 도 4는 온라인 서비스 서버에 의해 운영되는 온라인 서비스 사이트에 간편 인증번호가 게시되는 화면과 관련된 예시이고, 도 5는 간편 인증기에 의해 생성된 검증용 인증번호가 표출되는 화면과 관련된 예시이며, 도 6은 도 1의 상호 인증 방법에 따른 인증 과정에서 해커에 의한 접속 시도시 처리 방법을 설명하기 위한 도면이고, 도 7은 도 6과 같은 해커에 의한 접속 시도시의 온라인 서비스 서버에 의해 운영되는 온라인 서비스 사이트에 게시되는 처리 결과를 예시한 도면이다. 또한 도 8 및 도 9는 사용자의 모바일 기기를 통해 온라인 서비스 서버에 접속하였을 때의 본 발명의 실시예에 따른 상호 인증 방법의 구현 예시이다.

[0054] 도 1의 단계 S1을 참조하면, 온라인 서비스 서버(230)가 제공하는 온라인 서비스 사이트에 의한 온라인 서비스를 이용하고자 하는 경우, 서비스 사용자는 온라인 서비스 서버(230)에 접속 요청을 한다.

[0055] 예를 들어, 이용하고자 하는 온라인 서비스가 온라인 뱅킹 서비스인 경우, 사용자는 해당 온라인 뱅킹 서비스를 제공하는 특정 온라인 서비스 서버(즉, 온라인 뱅킹 서비스를 제공하는 특정 은행 서버)에 접속할 수 있다. 온라인 서비스 서버(230)로의 접속은 사용자 자신이 소유하는 모바일 기기(210)(예를 들어, 스마트폰 등)를 통한 모바일 접속에 의할 수 있음은 물론이나, 도 1에서는 사용자 소유의 모바일 기기(210)와는 별개의 클라이언트 단말(200)(예를 들어, 회사 PC 등)을 통해서 접속하는 경우를 예시하였다.

[0056] 도 1의 단계 S2를 참조하면, 온라인 서비스 서버(230)로의 접속 요청에 따라, 온라인 서비스 서버(230)는 온라인 서비스를 이용하고자 하는 서비스 사용자에게 사용자 계정 정보의 입력을 요청할 수 있다. 여기서, 사용자 계정 정보는, 사용자 등록 절차(또는 서비스 가입 절차)를 통해서 해당 온라인 서비스 서버(230)에 미리 저장(등록)되어 있는 해당 사용자의 식별 정보를 의미한다. 통상적으로, 사용자 계정 정보로는 사용자 ID(Identifier)와 패스워드(password)가 활용될 수 있다. 다만, 해당 온라인 서비스를 이용하는 사용자를 식별할 수 있는 정보라면, 상기 사용자 계정 정보로서 이외에도 다양한 정보(예를 들어, 해당 사용자의 이메일 주소, 전화번호, PKI(Public Key Infrastructure) 기반의 인증서 상의 인증서 암호 등)가 대체 활용될 수 있음은 물론이다.

[0057] 도 1의 단계 S3을 참조하면, 사용자 계정 정보의 입력 요청에 따라, 서비스 사용자는 사용자 계정 정보를 해당 온라인 서비스 사이트에 입력한다. 도 1의 단계 S4를 참조하면, 서비스 사용자로부터 사용자 계정 정보가 입력되면, 온라인 서비스 서버(230)는 사용자로부터 입력된 사용자 계정 정보와 일치하는 계정이 존재하는지를 확인한다. 이러한 계정 정보의 확인에는 도 1에 도시된 바와 같은 계정 DB(240)가 활용될 수 있다. 계정 DB(240)에는 해당 온라인 서비스 서버(230)를 통한 온라인 서비스를 제공받을 수 있는 사용자들(즉, 회원들)에 관한 계정 정보들이 보관된다. 도 1에서는 계정 DB(240)가 온라인 서비스 서버(230)와 별개로 구비되는 경우를 예시하였지만, 계정 DB(240)는 온라인 서비스 서버(230)와 통합되어 구현될 수도 있음은 물론이다. 또한, 시스템 구현 방식에 따라, 계정 DB(240)는 인증 서버(250)와 통합되어 구현될 수도 있을 것이다.

[0058] 도 1의 단계 S5를 참조하면, 입력된 사용자 계정 정보가 계정 DB(240)에 보관된 사용자 계정과 일치하는 경우, 온라인 서비스 서버(230)는 인증 서버(250)로 간편 인증번호의 생성을 요청한다. 여기서, 간편 인증번호는 사용자가 현재 접속한 온라인 서비스 사이트가 진정한 온라인 서비스 제공자에 의해 제공된 것인지 여부를 사용자가 판별할 수 있도록 하기 위한 용도로서 활용된다.

[0059] 도 1의 단계 S5에서, 온라인 서비스 서버(230)가 인증 서버(250)로 간편 인증번호의 생성 요청을 할 때, 온라인

서비스 서버(230)는 해당 서비스 사용자의 사용자 계정 정보를 함께 인증 서버(250)로 전송할 수 있다. 예를 들어, 온라인 서비스 서버(230)는 사용자 계정 정보로서 해당 사용자의 사용자 ID를 포함하는 간편 인증번호 생성 요청을 인정 서버(250)로 전송할 수 있다.

[0060] 또한 일 실시예에 의할 때, 온라인 서비스 서버(230)는 도 1의 단계 S5를 통해서(혹은 별개의 단계를 통해서) 클라이언트 접속환경정보를 인증 서버(250)로 추가 전송할 수도 있다. 여기서, 클라이언트 접속환경정보란, 온라인 서비스 서버(230)에 접속한 해당 서비스 사용자의 접속단말에 관한 접속환경을 직접 또는 간접적으로 나타낼 수 있는 정보를 통칭한다. 이러한 클라이언트 접속환경정보는 서비스 서버에 따라 다양할 수 있다.

[0061] 예를 들어, 표준 웹 서버를 예로 들면 접속한 클라이언트 단말기의 값을 추출할 수 있는 다양한 서버 변수(Server Variables; 호스트 네임(REMOTE_HOST), 쿠키 정보(HTTP_COOKIE), 이전 URL(HTTP_PEFERER), 한 단계 앞의 IP 주소(HTTP_X_FORWARDED_FOR), 현재 IP 주소(REMOTE_ADDR), 클라이언트 브라우져(HTTP_USER_AGENT), 클라이언트 언어(HTTP_ACCEPT_LANGUAGE))이거나, 클라이언트 단말에 서비스를 제공하는 서비스 서버의 변수(서버 호스트명, 서버 IP, 세션 아이디값, 세션 최대 유효시간 등)로 구성될 수 있다. 다른 예로, 접속하는 클라이언트가 표준 웹 브라우저가 아니라 자체 클라이언트 프로그램인 경우 운영체제(OS)가 허용하는 범위 내에서 클라이언트 단말기의 다양한 시스템 변수(Mac Address, HDD UUID 등)를 클라이언트 접속환경정보로서 이용할 수 있을 것이다.

[0062] 상술한 바와 같은 간편 인증번호의 생성 요청은 인증 서버(250)의 통신 인터페이스부(251)를 통해 접수(수신)되며, 함께 전송된 사용자 계정 정보 또는/및 클라이언트 접속환경정보는 상기 간편 인증번호의 생성에 시드값으로서 활용될 수 있다.

[0063] 도 1의 단계 S6을 참조하면, 온라인 서비스 서버(230)로부터의 간편 인증번호 생성 요청에 따라, 인증 서버(250)는 간편 인증번호를 생성한다. 이때, 간편 인증번호의 생성은 인증 서버(250)의 간편 인증번호 생성부(253)에 의해 수행될 수 있다.

[0064] 이때, 간편 인증번호는 온라인 서비스 서버(230)로부터 전달된 클라이언트 접속환경정보를 이용하여 생성할 수 있음은 앞서 설명하였는 바, 이하에서는 이러한 클라이언트 접속환경정보를 대체하여 활용되거나 또는 클라이언트 접속환경정보와 함께 상기 간편 인증번호 생성을 위한 추가 시드값으로서 활용될 수 있는 기타 실시예들에 대하여 상세히 설명하기로 한다.

[0065] 본 발명의 일 실시예에서, 간편 인증번호의 생성을 위한 시드 값으로는 서비스 사용자의 사용자 계정 정보에 대응하여 사전 등록된 고정키가 이용될 수 있다.

[0066] 일 예로, 사용자 계정 정보에 대응하는 고정키는, 전술한 사용자 ID, 패스워드, 사용자의 이메일 주소, 전화번호, 인증서 암호 등과 같은 다양한 사용자 식별 정보 중 어느 하나 또는 적어도 2개의 조합이 사전 등록되어 이용될 수 있다. 다른 예로, 사용자 계정 정보에 대응하는 고정키는, 사용자 소유의 모바일 기기(예를 들어, 스마트폰 등)의 폰 번호, 제품 일련번호, 유심(USIM) 카드번호, 맥 어드레스(MAC address) 등과 같은 식별자 중 어느 하나 또는 적어도 2개의 조합이 사전 등록되어 이용될 수도 있다. 또 다른 예로, 사용자 계정 정보에 대응하는 고정키는, 사용자가 간편 인증 서비스에 등록할 때에 자신이 직접 선택하여 등록한 또는 간편 인증 서비스 등록시에 부여된 개인키가 이용될 수도 있다.

[0067] 본 발명의 다른 실시예에서, 인증번호 생성을 위한 시드 값으로는 사용자가 해당 온라인 서비스 서버에 접속하는 시점에 동적으로 할당되는 동적 할당키가 이용될 수 있다.

[0068] 일 예로, 상기 동적 할당키로는, 해당 온라인 서비스 서버로 접속하는 서비스 사용자의 접속단말 연결정보가 이용될 수 있다. 이때, 접속단말 연결정보로는 서비스 사용자의 접속시 해당 온라인 서비스 서버에서 서비스 사용자의 접속단말에 할당하는 세션 정보(예를 들어, 세션 ID(Session ID) 등) 또는 소켓 정보(예를 들어, 소켓 핸들(Socket handle) 등)가 이용될 수 있다.

[0069] 여기서, 세션 ID는 서버와 접속단말 간의 연속적인 데이터 송수신을 관리하기 위해 해당 서버에 의해 부여되는 값이고, 소켓 핸들 정보는 서버와 접속단말 간에 네트워크를 통해 데이터를 송수신하는 단위인 소켓을 관리하기 위해 해당 서버가 자체적으로 할당한 임의의 연결 고유값이다. 이러한 세션 ID 또는 소켓 핸들 정보는 동적으로 할당됨은 물론 해당 서버에 의해 자체적으로 부여되는 값으로서, 서버 외부에서 해커에 의해 탈취되기 어렵기 때문에, 이를 이용하는 경우 보안 상 유리한 효과가 있다.

[0070] 다른 예로, 상기 동적 할당키로는, 서비스 사용자 소유의 모바일 기기에 이동통신사가 동적으로 할당한 모바일

IP 주소(IP 주소 전체 또는 일부분일 수 있음)가 이용될 수도 있다. 예를 들어, 서비스 사용자가 자신의 모바일 기기를 통해서 해당 온라인 서비스 서버로 접속하는 경우를 가정하면, 이때 이동통신사에 의해 동적으로 할당된 모바일 IP 주소를 시드값으로 이용할 수 있을 것이다.

[0071] 또한 이상에서는 시드값으로서 특정 값이 이용되는 경우를 중심으로 설명하였지만, 간편 인증번호 생성을 위한 시드값으로는 인증 서버(250)에서 자체적으로 랜덤하게 생성하는 랜덤값이 이용될 수도 있음은 물론이다.

[0072] 이에 따라, 인증 서버(250)의 간편 인증번호 생성부(253)는 상술한 바와 같은 적어도 하나의 시드값들을 이용하되, 시간 또는 시도 횟수(즉, 간편 인증번호 발급 시도 횟수)를 연산 조건으로 하여 간편 인증번호를 생성할 수 있다. 예를 들어, 간편 인증번호 생성부(253)는 상술한 적어도 하나의 시드값에 시간 또는 시도횟수를 곱한 값을 특정 해시 함수(hash function)에 따라 암호화한 값으로 생성될 수 있다. 이에 따라 간편 인증번호는 일회성을 갖는 값으로 생성될 수 있다.

[0073] 또한 여기서, 타임 OTP 방식은 연산 조건으로서 생성 시간을 이용하여 OTP를 생성하는 방식이다. 이에 의할 때, OTP는 결정된 특정 OTP 생성키에 연산 조건인 생성 시간을 곱한 값을 특정 해시 함수에 따라 암호화한 값으로 생성될 수 있다.

[0074] 상술한 바와 같이, 간편 인증번호가 생성되면, 인증 서버(250)는 통신 인터페이스부(251)를 통해서 앞선 단계 S6을 통해서 생성된 간편 인증번호를 온라인 서비스 서버(230)로 전달한다. 전달된 간편 인증번호는 도 1의 단계 S9에 따라 온라인 서비스 서버(230)에 의해 운영되는 온라인 서비스 사이트의 화면을 통해 사용자가 확인할 수 있도록 게시된다. 이에 관한 일 예가 도 4에 도시되고 있다. 도 4를 참조하면, 온라인 뱅킹 사이트의 우측의 인증번호 게시 화면을 통해서 간편 인증번호(도 4의 도면부호 30A 참조)가 게시되고 있음을 확인할 수 있다. 간편 인증번호가 화면 상에 게시된 이후, 사용자로부터의 확인이 완료되기 전까지는 승인 대기 상태가 지속될 수 있다[도 1의 단계 S10 참조].

[0075] 또한, 도 1의 단계 S8을 참조하면, 인증 서버(250)는 통신 인터페이스부(251)를 통해서 간편 인증번호의 생성 조건이 서비스 사용자 소유의 모바일 기기(110)에 설치된 간편 인증기(220)로 전송되도록 한다.

[0076] 도 1에서 단계 S8의 간편 인증번호 생성 조건의 전송은 푸시 서버(260)를 통해서 수행되는 것으로 예시하고 있지만, 반드시 이와 같을 필요는 없으며, 인증 서버(250)에서 직접 간편 인증기(220)로 전송될 수도 있음은 물론이다. 또한, 도 1에서는 푸시 메시지를 통해서 간편 인증번호의 생성 조건을 전송하는 케이스를 중심으로 도시하였지만, 간편 인증번호 생성 조건의 전송은 소켓 데이터 통신에 의한 전송 방식에 의할 수도 있다.

[0077] 푸시 서버(260)를 통해 간편 인증번호 생성 조건을 전송하는 경우, 인증 서버(250)는 그 생성 조건을 푸시 서버(260)로 전달하고, 이때 푸시 서버(260)는 푸시 메시지를 통해서 간편 인증번호 생성 조건을 간편 인증기(220)로 전송할 수 있다. 여기서, 푸시 메시지는 특정 모바일 운영체제에서 앱(App) 별로 제공하는 메시지 서비스일 수 있다. 다만, 간편 인증번호 생성 조건의 전송을 반드시 푸시 메시지에 의할 필요는 없음은 자명하며, SMS, MMS 등의 상용의 다양한 메시징 서비스에 의할 수도 있고, 특정 통신 프로토콜에 의하여도 무방하다. 간편 인증번호 생성 조건의 전송을 푸시 메시지에 의하지 않는 다른 예시적 케이스들에서, 전술한 푸시 서버(260)는 일반적인 통신 서버로서 그 기능이 대체될 수 있다.

[0078] 또한 도 1에서는 간편 인증번호 생성 조건이 간편 인증기(220)로 직접 전송되는 케이스를 중심으로 설명하였지만, 반드시 이와 같을 필요는 없다. 예를 들어, 간편 인증번호 생성 조건은 푸시 메시지 등을 통해서 모바일 기기(210)로 전송되고, 간편 인증기(220)가 이를 읽어들여 간편 인증번호 생성 조건을 수신(취득)할 수 있음은 자명하다. 이러한 간편 인증번호 생성 조건의 수신은 간편 인증기(220)의 통신 인터페이스부(221)에 의해 이루어질 수 있다.

[0079] 상술한 도 1의 단계 S8을 통해 전송될 간편 인증번호 생성 조건은, 도 1의 단계 S6에서 간편 인증번호의 생성에 활용된 시드값 및 연산 조건 전부일 수도 있지만, 그 일부 일 수도 있다. 예를 들어, 인증 서버(250)와 간편 인증기(220)가 각각 간편 인증번호 생성에 활용되는 시드값 및 연산 조건 중 일부를 사전에 보관하고 이를 공통적으로 사용하는 경우라면, 그와 같이 사전 보관된 조건은 별도로 전송해줄 필요가 없기 때문이다.

[0080] 이에 따라, 간편 인증기(220)는 수신한 생성 조건을 이용하여 온라인 서비스 서버(230)의 온라인 서비스 사이트 화면을 통해 표출된 간편 인증번호의 검증을 위한 검증용 인증번호를 생성할 수 있다[도 1의 단계 S11 참조]. 이와 같은 검증용 인증번호의 생성은 간편 인증기(220)의 검증용 인증번호 생성부(223)에 의해 수행될 수 있다.

[0081] 이와 같이 생성된 검증용 인증번호는 간편 인증기(220)의 인증번호 표출부(227)을 통해서 모바일 기기(210)의

앱 화면을 통해 표시될 수 있다. 이때, 앱 화면을 통해 검증용 인증번호(도 5의 도면부호 30B 참조)가 표출된 예가 도 5에 도시되고 있다.

[0082] 이상에서 전술한 단계 S7 ~ 단계 S11은, 반드시 도 1에 도시된 순서에 한정될 필요는 없으며, 서로 선후를 달리하거나 동시에 이루어질 수도 있다.

[0083] 상술한 과정을 통해서 앱 화면을 통해서 검증용 인증번호가 표출되면, 사용자는 이와 같이 표출된 검증용 인증번호와 온라인 서비스 사이트 화면을 통해 표출된 간편 인증번호 간을 비교함으로써 해당 온라인 서비스 서버가 진정한 서비스 서버임(즉, 서비스 서버의 진위)을 판별해낼 수 있다.

[0084] 비교 결과, 간편 인증번호와 검증용 인증번호가 일치하는 경우, 사용자는 도 5에 도시된 앱 화면 상의 승인 버튼을 선택함으로써, 해당 서비스에 관한 승인 처리(즉, 해당 온라인 서비스 서버가 진정한 서비스 서버임을 검증 완료 처리)를 할 수 있다[도 1의 단계 S12 참조].

[0085] 도 5에서는 앱 화면에 표출된 검증용 인증번호의 하단에 해당 서비스에 대한 승인 처리를 할 수 있는 승인 버튼이 구비된 경우를 예시하였지만, 이 외에도 다양한 변형이 가능함은 물론이다. 예를 들어, 해당 서비스에 대한 승인 또는 취소 처리는 사용자의 특정 제스처에 의할 수도 있다. 예를 들어, 사용자가 모바일 기기의 앱 화면을 위쪽 방향으로 밀어올리는 터치 제스처를 취하면 승인 처리되고, 아래쪽 방향으로 밀어 내리는 터치 제스처를 취하면 취소 처리되도록 구현될 수도 있는 것이다.

[0086] 상술한 바와 같이, 해당 서비스에 관한 승인이 이루어지는 경우, 간편 인증기(220)의 추가 검증값 생성부(225)는 추가 검증값을 생성하고, 이를 통신 인터페이스부(221)를 통해서 인증 서버(250)로 전송한다[도 1의 단계 S12 및 단계 S13 참조].

[0087] 여기서, 추가 검증값은 사용자 인증을 위한 용도로서 사용된다. 즉, 본 발명의 실시예에서는 간편 인증번호의 검증을 통해서 해당 서비스의 진위 여부를 먼저 확인한 이후에, 추가 검증값을 통해서 해당 서비스를 이용하고자 하는 사용자가 정당한 사용자인지 여부를 확인하는 방식이 이용된다. 특이한 점은, 본 발명의 실시예에 의할 때, 사용자 인증을 위한 추가 검증값은 앞선 간편 인증번호의 검증을 통한 승인 처리가 완료됨과 동시에 간편 인증기(220)에 의해 자동으로 생성되어 곧바로 인증 서버(250)로 전달된다는 점이다. 이에 의하면, 사용자 인증 과정에서 사용자가 그 사용자 인증값을 온라인 서비스 서버로 직접 입력해야 하는 불편함을 없앨 수 있다.

[0088] 이때, 추가 검증값은 다양한 방법으로 생성될 수 있다. 추가 검증값의 생성 방법은 앞서 설명한 간편 인증번호의 생성 방식들과 본질적으로 상이하지 않을 것이므로, 이에 관한 구체적인 설명은 생략하기로 한다. 물론, 추가 검증값의 생성은 앞서 설명한 간편 인증번호의 생성 방식을 따를 필요는 없으며, 시스템에서 정의하는 사전 지정된 조건에 따라 생성하여도 무방하다. 그 생성 방식은 후술할 인증 서버(250)에서의 확인용 검증값(즉, 위 추가 검증값에 대응되게 생성된 검증값)의 생성에도 동일하게 적용될 것이다. 따라서, 추가 검증값의 생성 과정에서 인증 서버(250)에 보관되지 않은 정보가 활용된 경우, 해당 정보도 도 1의 단계 S13을 통해서 인증 서버(250)로 전달될 필요는 있다.

[0089] 또한 도 1에서는 단계 S13에 따른 추가 검증값의 전송이 푸시 서버(260)를 경유하여 이루어지는 것으로 도시되고 있지만, 반드시 이에 의할 필요는 없으며, 인증 서버(250)로 직접 전송되는 방식에 의해도 무방하다.

[0090] 이에 따라, 인증 서버(250)의 확인용 검증값 생성부(255)는 전송된 추가 검증값을 검증하기 위한 확인용 검증값을 생성하고, 인증 서버(250)의 인증 처리부(257)는 생성된 확인용 검증값과 전송된 추가 검증값 간의 일치 여부를 비교함으로써 해당 서비스 사용자에 대한 사용자 인증을 수행할 수 있다[도 1의 단계 S14 참조]. 이때, 인증 결과는 온라인 서비스 서버(230)로 통보되며[도 1의 단계 S15 참조], 인증이 정상적으로 이루어진 경우 온라인 서비스 서버(230)는 해당 서비스 사용자에게 해당 서비스를 개시할 수 있다[도 1의 단계 S16 참조].

[0091] 상술한 바에 따르는 본 발명의 실시예에 의하면, 서비스 사용자는 간편 인증번호를 통한 서비스 검증만을 하면 되고 이후의 사용자 인증 과정은 자동으로 수행되므로, 사용자 인증번호 입력 과정이 생략될 수 있어, 전체 인증 절차가 간결하고 편리해지는 효과가 있다.

[0092] 이상에서는 도 1의 단계 S12를 통해 해당 서비스가 정상 승인되는 경우를 중심으로 설명하였다. 그러나 만일 도 1의 단계 S12를 통해 해당 서비스가 사용자에 의해 승인 불허되는 경우, 간편 인증기(220)는 도 1의 단계 S13을 통해 승인 불허 통지를 할 수 있다.

[0093] 또한 본 발명의 실시예에 의하면, 인증 서버(250)는 서비스 사용자에 의한 온라인 서비스 서버로의 접속 시도에 따라 간편 인증번호가 생성된 이후, 그 간편 인증번호에 관한 검증 유효시간(예를 들어, 60초) 동안 또는 사용

자에 의한 서비스 검증이 완료되기 전까지, 그 생성된 간편 인증번호를 그대로 유지할 수 있다. 이에 관하여 도 6을 참조하여 설명하면 다음과 같다.

[0094] 도 6을 참조하면, 정상적인 사용자에 의한 서비스 접속에 따라 간편 인증번호가 생성된 이후, 해당 사용자의 사용자 계정 정보를 탈취한 해커에 의한 후순위 접속이 이루어진 경우[도 6의 단계 S21 참조], 온라인 서비스 서버(230)에 의한 간편 인증번호의 생성 요청이 추가 접수되더라도[도 6의 단계 S22 참조], 인증 서버(250)는 인증번호의 재생성을 금지하고 있다[도 6의 단계 S23 참조].

[0095] 이와 같이, 인증 서버(250)는 간편 인증번호의 검증 유효시간 동안 또는 상기 온라인 서비스 서버에 관한 검증이 완료되기 전까지는 선순위 접속에 따라 생성된 간편 인증번호를 그대로 유지하거나 또는 후순위 접속에 따른 간편 인증번호의 신규 생성을 금지할 수 있다. 이와 같은 후순위 접속자에 대해서는 도 7과 같이 온라인 서비스 사이트의 화면을 통해서 중복 접속이 불가함을 안내하는 화면(도 7의 도면부호 30C 참조)이 표출될 수 있다. 이에 의하면, 해커에 의한 후순위 접속에 따른 불법적인 사용자 인증 및 이에 의한 정보 탈취를 방지할 수 있다.

[0096] 이상에서는 사용자가 자신 소유의 모바일 기기와 별개의 클라이언트 단말을 통해서 온라인 서비스 서버에 접속한 케이스를 중심으로 설명하였다. 그러나 간편 인증기가 설치된 모바일 기기를 이용해서 직접 온라인 서비스 서버에 접속할 수도 있음은 앞서도 설명한 바이다. 이러한 경우, 간편 인증번호와 검증용 인증번호는 도 8 및 도 9에 도시된 바와 같이 모바일 기기의 화면을 통해 표출될 수 있다. 도 8을 참조하면, 간편 인증기(220)에 의한 앱 화면이 모바일 기기의 화면 상단부(40A)에 표출되고, 온라인 서비스 서버(230)에 의해 제공되는 사이트 화면이 모바일 기기의 화면 하단부(40B)에 표출되고 있다. 그리고 그 화면 화단부(40B)에는 간편 인증번호(40C)가 표출되고 있다. 또한, 도 9를 참조하면, 그 화면 상단부(40A)에 간편 인증기(220)에 의해 생성되는 검증용 인증번호(40D)가 표출되고 있다. 이와 같이 간편 인증기가 설치된 모바일 기기를 이용하여 직접 온라인 서비스 서버에 접속하는 경우에는, 간편 인증기에 의한 앱 화면과 온라인 서비스 서버에 의한 사이트 화면이 서로 다른 화면 영역에 분리되어 표출될 수 있다. 이러한 예로서, 특히 도 8 및 도 9에는 앱 화면이 사이트 화면 상부에 띄워진 형태로 표출(즉, layered type의 화면 표출)되는 경우를 도시하고 있지만, 화면 분할 방식은 이 외에도 다양한 방식이 적용될 수 있음은 물론이다.

[0097] 본 발명의 실시 예에 따른 방법 및 장치는 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.

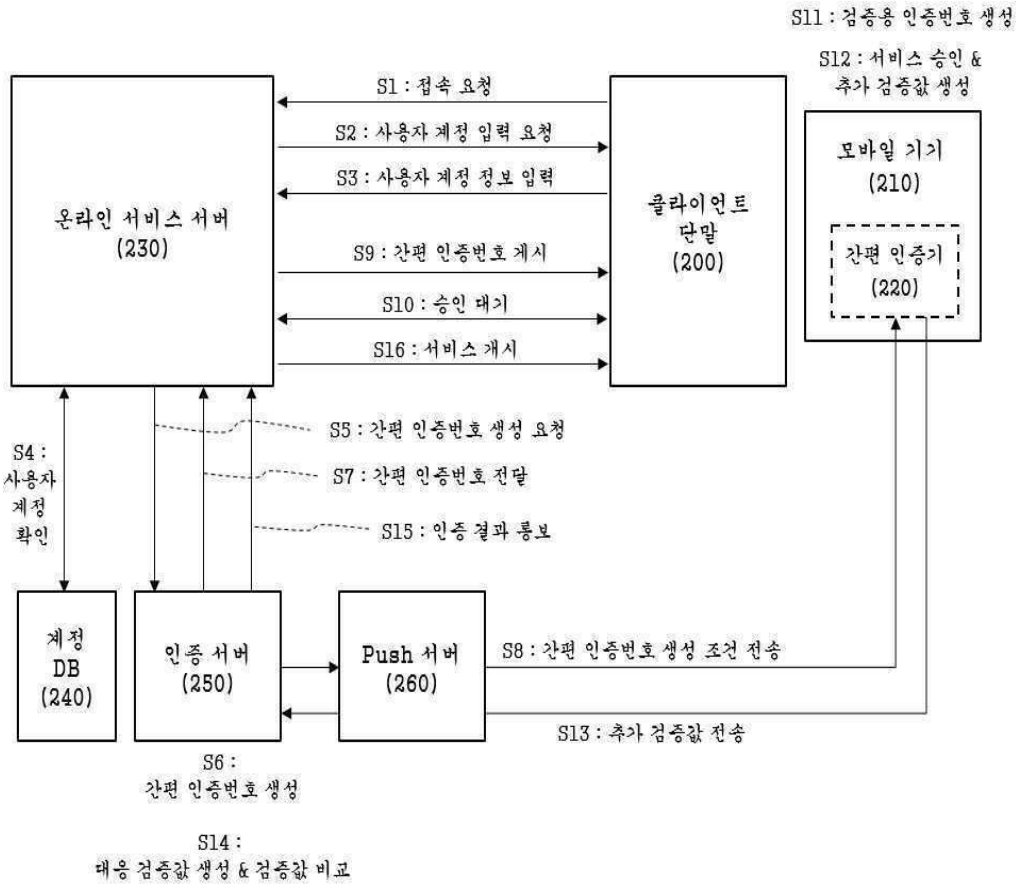
[0098] 컴퓨터 판독 가능 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media) 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0099] 상술한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

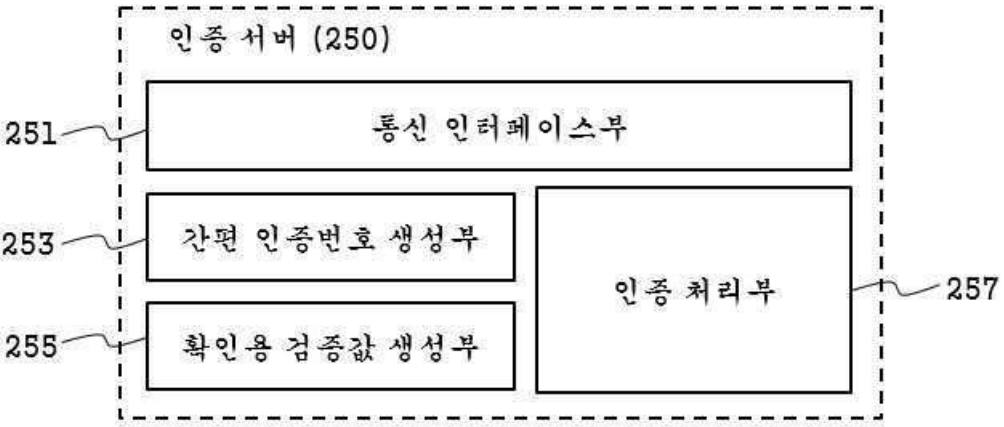
[0100] 이상에서는 본 발명의 실시예를 참조하여 설명하였지만, 해당 기술 분야에서 통상의 지식을 가진 자라면 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 쉽게 이해할 수 있을 것이다.

도면

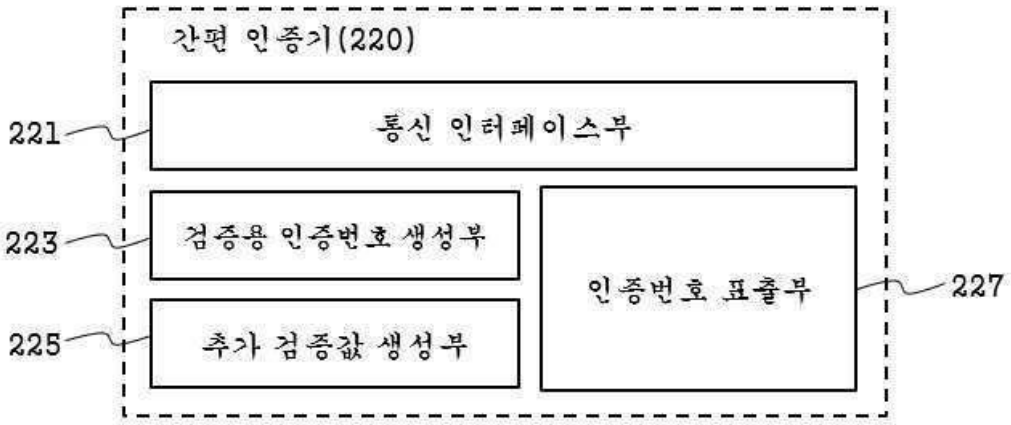
도면1


S11 : 검증용 인증번호 생성
S12 : 서비스 승인 & 추가 검증값 생성
S1 : 접속 요청
S2 : 사용자 계정 입력 요청
S3 : 사용자 계정 정보 입력
S9 : 간편 인증번호 게시
S10 : 승인 대기
S16 : 서비스 개시
온라인 서비스 서버 (230)
클라이언트 단말 (200)
모바일 기기 (210)
간편 인증기 (220)
S5 : 간편 인증번호 생성 요청
S7 : 간편 인증번호 전달
S15 : 인증 결과 통보
S4 : 사용자 계정 확인
계정 DB (240)
인증 서버 (250)
Push 서버 (260)
S8 : 간편 인증번호 생성 조건 전송
S13 : 추가 검증값 전송
S6 : 간편 인증번호 생성
S14 : 대응 검증값 생성 & 검증값 비교

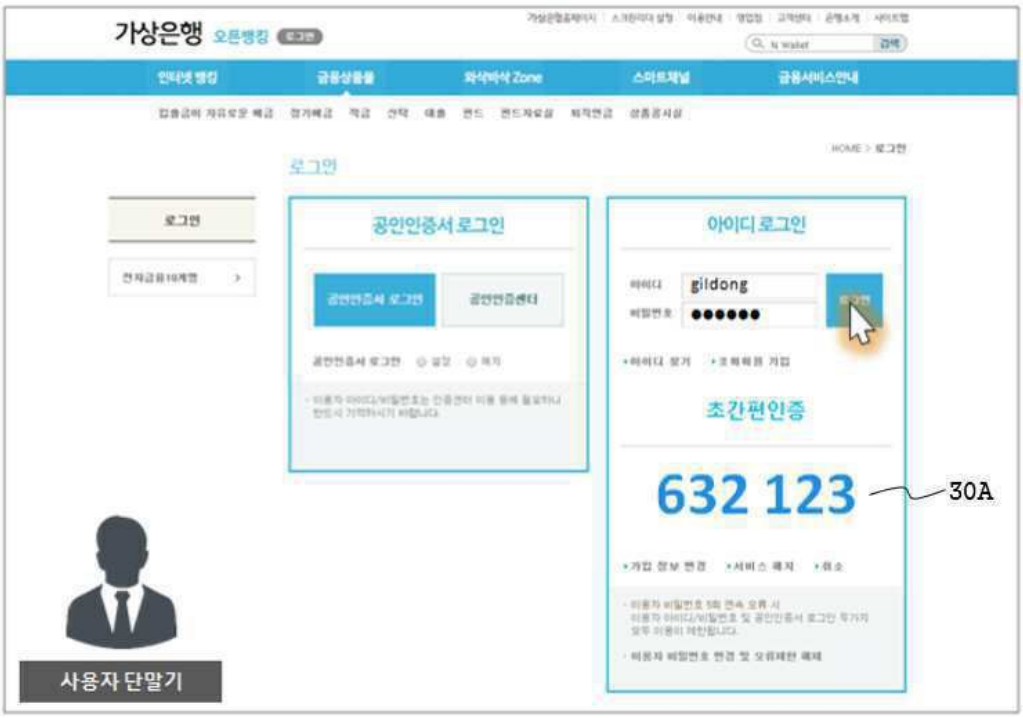
도면2


인증 서버 (250)
251
통신 인터페이스부
253
간편 인증번호 생성부
255
확인용 검증값 생성부
인증 처리부
257

도면3


간편 인증기(220)
221
통신 인터페이스부
223
검증용 인증번호 생성부
225
추가 검증값 생성부
인증번호 표출부
227

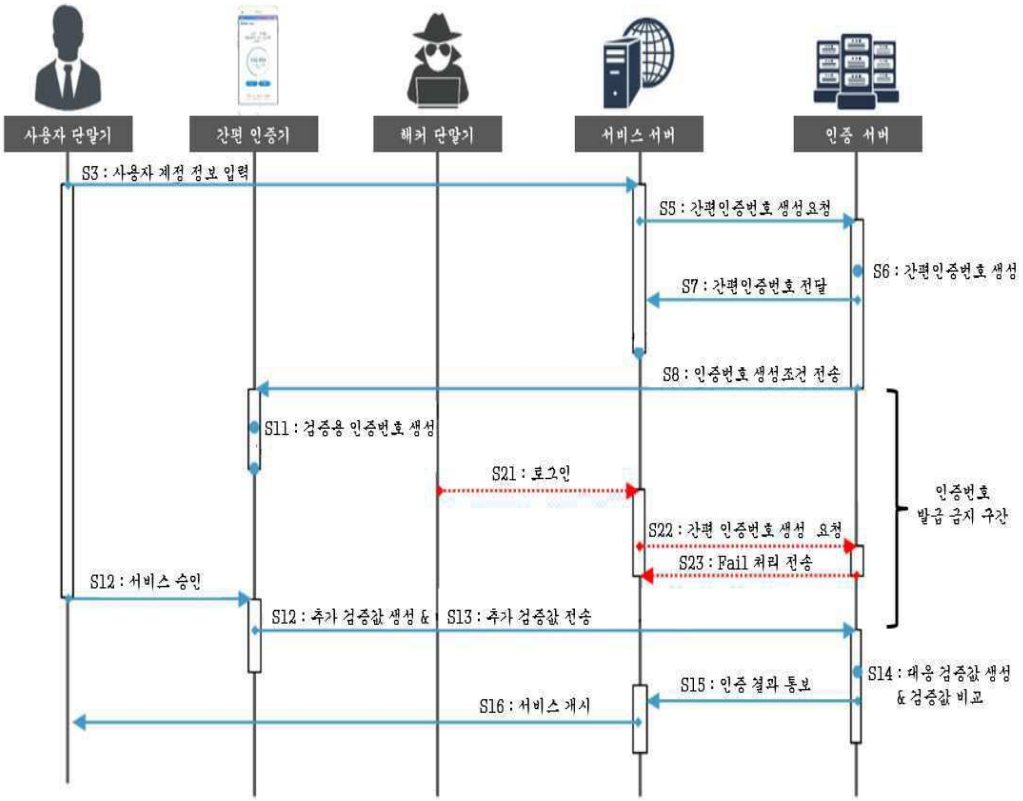
도면4


가상은행
로그인
공인인증서 로그인
아이디 로그인
gildong
초간편인증
632 123
30A
사용자 단말기

도면5


4:21 PM
100%
자동 로그인 인증 앱
2015년 12월 23일
오전 9시30분에
가상은행에서 홍길동님의
로그인 인증 요청이
왔습니다.
632 123
30B
간편인증번호 비교 후
승인 버튼을
눌러주세요.
취소
승인
사용자 인증 앱

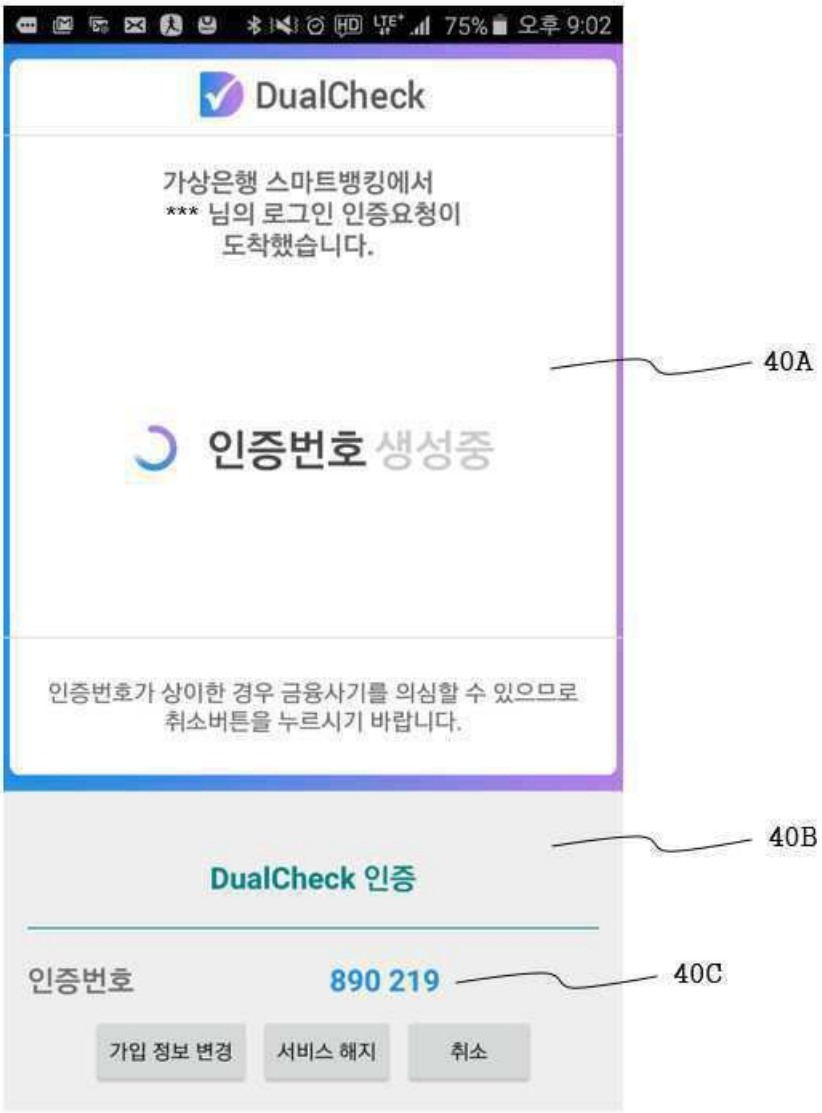
도면6


사용자 단말기
간편 인증기
해커 단말기
서비스 서버
인증 서버
S3 : 사용자 계정 정보 입력
S5 : 간편인증번호 생성요청
S6 : 간편인증번호 생성
S7 : 간편인증번호 전달
S8 : 인증번호 생성조건 전송
S11 : 검증용 인증번호 생성
S21 : 로그인
S22 : 간편 인증번호 생성 요청
S23 : Fail 처리 전송
인증번호
발급 금지 구간
S12 : 서비스 승인
S12 : 추가 검증값 생성 &
S13 : 추가 검증값 전송
S14 : 대응 검증값 생성
& 검증값 비교
S15 : 인증 결과 통보
S16 : 서비스 개시

도면7


가상은행
로그인
공인인증서 로그인
아이디 로그인
gildong
로그인 인증
홍길동님이 다른 곳에서
이미 접속 중 입니다.
30C
해커 단말기

도면8


75% 오후 9:02
DualCheck
가상은행 스마트뱅킹에서
*** 님의 로그인 인증요청이
도착했습니다.
인증번호 생성중
인증번호가 상이한 경우 금융사기를 의심할 수 있으므로
취소버튼을 누르시기 바랍니다.
DualCheck 인증
인증번호
890 219
가입 정보 변경
서비스 해지
취소
40A
40B
40C

도면9


75% 오후 9:02
DualCheck
가상은행 스마트뱅킹에서
*** 님의 로그인 인증요청이
도착했습니다.
40A
890 219
40D
인증번호 비교 후 승인버튼을 눌러주세요.
취소
승인
인증번호가 상이한 경우 금융사기를 의심할 수 있으므로
취소버튼을 누르시기 바랍니다.
DualCheck 인증
40B
인증번호
890 219
가입 정보 변경
서비스 해지
취소