(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년11월14일
(11) 등록번호 10-1675880
(24) 등록일자 2016년11월08일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 21/34* (2013.01)
H04W 12/06 (2009.01)
(52) CPC특허분류
H04L 9/3228 (2013.01)
G06F 21/34 (2013.01)
(21) 출원번호 10-2015-0139775
(22) 출원일자 2015년10월05일
심사청구일자 2015년10월05일
(56) 선행기술조사문헌
KR101481101 B1*
KR1020120080283 A*
매일일보, LGU+, 유심 스마트OTP 서비스 출시, http://www.m-i.kr/news/articleView.html?idxno=151928 (2015.02.04.)
KR101508320 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 인포바인
서울특별시 마포구 마포대로 144 (공덕동)
(72) 발명자
권성준
서울특별시 마포구 토정로 158, 106동 2102호
김재수
서울특별시 마포구 독막로42길 2, 109동 1602호
(74) 대리인
한양특허법인

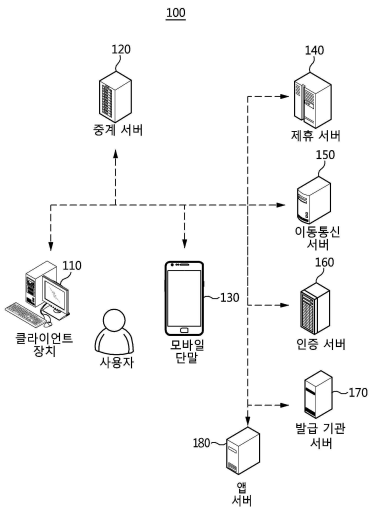
전체 청구항 수 : 총 14 항 심사관 : 양종필

(54) 발명의 명칭 **ＵＳＩＭ을 이용하는 ＯＴＰ 인증을 제공하는 인증 서비스 장치 및 이를 위한 방법**

(57) 요 약

USIM을 이용한 OTP 인증 서비스를 위한 장치 및 방법이 제공된다. 사용자의 클라이언트 장치는 사용자가 선택한 인증 방식에 따라 공인 인증서 전송 방식, 전자 서명 방식 및 USIM을 이용하는 OTP 방식 중 하나의 인증 방식을 자동으로 결정한다. 결정된 인증 방식에 따라 사용자의 모바일 단말은 인증 서비스를 제공한다. 인증 서비스를 통해 사용자에 대한 인증을 위한 인증용 데이터가 클라이언트 장치로 제공되고, 클라이언트 장치는 인증용 데이터를 사용하여 사용자에 대한 인증을 수행한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/3234 (2013.01)
H04W 12/06 (2013.01)

공지예외적용 : 있음

명 세 서

청구범위

청구항 1

사용자의 클라이언트 장치 및 중계 서버와의 상호 작용을 통해 상기 사용자에게 OTP 서비스를 포함하는 복수의 인증 서비스들을 제공하는 모바일 단말에 있어서,

모바일 프로그램을 저장하는 메모리; 및

상기 모바일 프로그램을 실행하는 프로세서

를 포함하고,

상기 모바일 프로그램은,

상기 모바일 단말에 장착된 모바일 유심(USIM)의 보안 토큰에 공인 인증서를 저장하고,

상기 공인 인증서에 대한 암호화를 수행함으로써 암호화된 공인 인증서를 생성하고, 상기 암호화된 공인 인증서를 상기 메모리에 저장하고,

상기 모바일 USIM에 의해 생성된 OTP를 출력하고,

상기 모바일 USIM은 OTP를 생성하기 위한 OTP 생성 정보 및 OTP 생성 알고리즘을 저장하고,

상기 모바일 USIM은 상기 OTP 생성 정보 및 상기 OTP 생성 알고리즘을 사용하여 상기 OTP를 생성하고,

상기 OTP 생성 정보의 적어도 일부는 발급 기관 서버에 의해 제공되고,

상기 OTP 생성 정보는 시드, 업체 코드, 일련 번호, 사용자 키, 상기 모바일 단말의 식별 정보 및 시간 정보를 포함하고,

상기 모바일 프로그램은 상기 모바일 단말의 상기 사용자에 대한 인증과 관련된 상기 복수의 인증 서비스들을 제공하고,

상기 복수의 인증 서비스들은 상기 메모리에 저장된 상기 암호화된 공인 인증서의 전송을 통해 상기 사용자를 인증하는 공인 인증서 전송 서비스, 상기 모바일 USIM에 저장된 상기 공인 인증서를 사용하여 상기 사용자의 전자 서명을 제공하는 전자 서명 서비스 및 상기 모바일 USIM에 의해 생성된 상기 OTP를 사용하는 상기 OTP 서비스를 포함하고,

상기 OTP 서비스는 상기 OTP 서비스를 사용하는 상기 사용자에 대한 인증 서비스 요청이 상기 클라이언트 장치로부터 상기 중계 서버를 경유하여 상기 모바일 단말로 전송되고, 상기 모바일 단말이 상기 인증 서비스 요청을 수신함에 따라 상기 OTP를 생성 및 출력하고, 상기 사용자에 의해 상기 클라이언트 장치로 입력된 OTP가 인증 서버에 의해 인증됨에 따라 이루어지는 모바일 단말.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 모바일 단말은 상기 복수의 인증 서비스들을 제공하는 상기 모바일 프로그램을 단일한 어플리케이션으로서 설치 및 관리하는 모바일 단말.

청구항 4

제1항에 있어서,

상기 중계 서버로부터 상기 사용자의 인증과 관련된 상기 인증 서비스 요청을 수신하는 통신부

를 더 포함하고,

상기 프로세서는 상기 통신부를 통해 상기 인증 서비스 요청이 수신되면 상기 모바일 프로그램을 실행하고,

상기 모바일 프로그램은 상기 복수의 인증 서비스들 중 상기 인증 서비스 요청이 나타내는 상기 사용자에 의해 선택된 인증 서비스에 따라 상기 공인 인증서 전송 서비스, 상기 전자 서명 서비스 및 상기 OTP 서비스 중 하나를 자동으로 제공하는 모바일 단말.

청구항 5

제4항에 있어서,

상기 인증 서비스는, 상기 클라이언트 장치에 의해 상기 사용자에 의해 선택된 상기 사용자에 대한 인증 방식이 인식되고, 상기 클라이언트 장치 및 상기 중계 서버 간에 형성된 보안 채널을 통해 상기 클라이언트 장치로부터 상기 중계 서버로 상기 인증 방식의 정보가 전송되면, 상기 중계 서버에서 상기 인증의 방식에 따라서 상기 공인 인증서 전송 서비스에 대응하는 공인 인증서 전송 모드, 상기 전자 서명 서비스에 대응하는 전자 서명 모드 및 상기 OTP 서비스에 대응하는 OTP 모드 중 하나로 자동으로 이루어지는 분기에 의해 결정되고,

상기 중계 서버에 의해 상기 전자 서명 모드 또는 상기 OTP 모드 중 하나로 자동으로 분기가 이루어지고, 상기 분기에 의해 결정된 인증 서비스의 요청의 내용이 상기 중계 서버로부터 상기 모바일 프로그램으로 전송되면, 상기 모바일 프로그램에서는 상기 중계 서버에서의 분기에 의해 선택된 인증 서비스에 따라 자동으로 분기가 이루어지는 모바일 단말.

청구항 6

삭제

청구항 7

제1항에 있어서,

상기 OTP를 생성함에 있어서 상기 모바일 프로그램은 상기 사용자에 의해 입력된 핀(PIN) 또는 패스워드를 수신하고, 상기 핀 또는 패스워드를 사용하여 상기 사용자에 대한 인증을 수행하는 모바일 단말.

청구항 8

삭제

청구항 9

제1항에 있어서,

상기 모바일 프로그램을 다운로드하기 위한 주소의 정보를 수신하는 통신부

를 더 포함하고,

상기 프로세서는 상기 주소의 정보를 사용하여 상기 모바일 프로그램을 다운로드 및 설치하는 모바일 단말.

청구항 10

제9항에 있어서,

상기 모바일 프로그램을 다운로드하기 위한 주소의 정보는 상기 모바일 단말의 사용자가 제휴사에 상기 제휴사의 제휴 서비스에 사용되는 모바일 OTP의 발급을 신청함에 따라 중계 서버로부터 상기 모바일 단말로 전송되는 모바일 단말.

청구항 11

제10항에 있어서,

상기 모바일 OTP의 발급은 1차 발급 및 2차 발급을 포함하고,

상기 1차 발급은 상기 모바일 프로그램을 설치하는 과정 및 상기 모바일 프로그램을 통해 상기 모바일 단말에게

이동통신 서비스를 제공하는 이동통신사의 이동통신 서버로부터 상기 모바일 OTP의 인증 모듈을 수신하고, 상기 인증 모듈을 상기 모바일 USIM에 설치하는 과정을 포함하고,

상기 2차 발급은 상기 발급 기관 서버로부터 상기 모바일 OTP의 상기 OTP 생성 정보를 수신하고, 상기 OTP 생성 정보를 상기 모바일 USIM에 저장하는 과정을 포함하는 모바일 단말.

청구항 12

제11항에 있어서,

상기 인증 모듈은 애플릿으로서 상기 모바일 USIM에 설치되고, 상기 애플릿은 상기 모바일 USIM의 보안 토큰의 기능을 수행하는 모바일 단말.

청구항 13

제11항에 있어서,

상기 모바일 OTP의 발급의 신청이 비대면 거래로 이루어질 경우 상기 OTP 생성 정보는 보안 채널을 통해 전송되는 모바일 단말.

청구항 14

사용자의 모바일 단말 및 중계 서버와의 상호 작용을 통해 상기 사용자에게 OTP 방식을 포함하는 복수의 인증 방식들을 제공하는 클라이언트 장치에 있어서,

프로그램을 저장하는 메모리; 및

상기 프로그램을 실행하는 프로세서

를 포함하고,

상기 프로그램은 상기 복수의 인증 방식들을 통해 상기 클라이언트 장치의 상기 사용자에 대한 인증을 처리하고,

상기 복수의 인증 방식들은 상기 모바일 단말의 모바일 USIM에 저장된 공인 인증서를 사용하여 생성된 상기 사용자의 전자 서명을 통해 상기 사용자를 인증하는 전자 서명 방식, 상기 모바일 단말의 메모리로부터 제공된 암호화된 공인 인증서의 전송을 통해 상기 사용자를 인증하는 공인 인증서 전송 방식 및 상기 모바일 USIM에 의해 생성된 OTP를 통해 상기 사용자를 인증하는 제공하는 상기 OTP 방식을 포함하고,

상기 OTP 방식의 인증은 상기 OTP 방식에 의한 상기 사용자에 대한 인증 서비스 요청이 상기 클라이언트로부터 상기 중계 서버를 경유하여 상기 모바일 단말로 전송되고, 상기 모바일 단말이 상기 인증 서비스 요청을 수신함에 따라 상기 모바일 단말에서 상기 OTP가 생성 및 출력되고, 상기 사용자에 의해 상기 클라이언트 장치로 입력된 상기 OTP가 인증 서버에 의해 인증됨에 따라 이루어지는 클라이언트 장치.

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

사용자의 클라이언트 장치 및 중계 서버와의 상호 작용을 통해 모바일 단말이 상기 사용자에게 OTP 서비스를 포함하는 복수의 인증 서비스들을 제공하는 방법에 있어서,

중계 서버로부터 상기 모바일 단말의 사용자의 인증과 관련된 인증 서비스 요청을 수신하는 단계; 및

복수의 인증 서비스들 중 상기 인증 서비스 요청이 나타내는 선택된 인증 서비스를 제공하는 단계

를 포함하고,

상기 복수의 인증 서비스들은 상기 모바일 단말의 모바일 USIM에 저장된 공인 인증서를 사용하여 상기 사용자의 전자 서명을 제공하는 전자 서명 서비스, 상기 모바일 단말의 메모리에 저장된 암호화된 공인 인증서의 전송을 통해 상기 사용자를 인증하는 공인 인증서 전송 서비스 및 상기 모바일 USIM에 의해 생성된 OTP를 사용하는 OTP 서비스를 포함하고,

상기 모바일 단말은 모바일 프로그램을 실행하고,

상기 모바일 프로그램은 상기 인증 서비스 요청이 나타내는 상기 선택된 인증 서비스에 따라 상기 공인 인증서 전송 서비스, 상기 전자 서명 서비스 및 상기 OTP 서비스 중 하나를 자동으로 제공하고,

상기 모바일 단말은 상기 모바일 단말의 메모리 및 상기 모바일 단말에 장착된 유심(USIM)의 각각에 공인 인증서를 저장하고,

상기 모바일 USIM은 OTP 생성 정보 및 OTP 생성 알고리즘을 사용하여 상기 OTP를 생성하고,

상기 OTP 생성 정보의 적어도 일부는 발급 기관 서버에 의해 제공되고,

상기 OTP 생성 정보는 사용자 키 및 상기 모바일 단말의 식별 정보를 포함하고,

상기 OTP 서비스는 상기 OTP 서비스를 사용하는 상기 사용자에 대한 상기 인증 서비스 요청이 상기 클라이언트 장치로부터 상기 중계 서버를 경유하여 상기 모바일 단말로 전송되고, 상기 모바일 단말이 상기 인증 서비스 요청을 수신함에 따라 상기 OTP를 생성 및 출력하고, 상기 사용자에 의해 상기 클라이언트 장치로 입력된 OTP가 인증 서버에 의해 인증됨에 따라 이루어지는 복수의 인증 서비스들을 제공하는 방법.

청구항 19

사용자의 모바일 단말 및 중계 서버와의 상호 작용을 통해 클라이언트 장치가 상기 사용자에게 OTP 방식을 포함하는 복수의 인증 방식들을 제공하는 방법에 있어서,

상기 복수의 인증 방식들 중 상기 클라이언트 장치의 상기 사용자에 의해 선택된 인증의 방식을 인식하는 단계;

상기 선택된 인증 방식의 정보를 포함하는 인증 요청을 보안 채널을 통해 중계 서버로 전송하는 단계; 및

상기 중계 서버에서 상기 선택된 인증 방식에 따라 자동으로 분기가 이루어지고, 상기 분기에 의해 결정된 인증 서비스의 요청의 내용이 상기 중계 서버로부터 상기 사용자의 모바일 단말의 모바일 프로그램으로 전송되면, 상기 인증 서비스에 관련하여 상기 모바일 프로그램으로부터 상기 사용자에 대한 인증에 관련된 인증용 데이터를 수신하는 단계

를 포함하고,

상기 복수의 인증 방식들은 상기 모바일 단말의 모바일 USIM에 저장된 공인 인증서를 사용하여 생성된 상기 사용자의 전자 서명을 통해 상기 사용자를 인증하는 전자 서명 방식, 상기 모바일 단말의 메모리로부터 제공된 암호화된 공인 인증서의 전송을 통해 상기 사용자를 인증하는 공인 인증서 전송 방식 및 상기 모바일 단말의 모바일 USIM에 의해 생성된 OTP를 통해 상기 사용자를 인증하는 제공하는 상기 OTP 방식을 포함하고,

상기 OTP 방식의 인증은 상기 OTP 방식에 의한 상기 사용자에 대한 인증 서비스 요청이 상기 클라이언트로부터 상기 중계 서버를 경유하여 상기 모바일 단말로 전송되고, 상기 모바일 단말이 상기 인증 서비스 요청을 수신함에 따라 상기 모바일 단말에서 상기 OTP가 생성 및 출력되고, 상기 사용자에 의해 상기 클라이언트 장치로 입력된 상기 OTP가 인증 서버에 의해 인증됨에 따라 이루어지는 복수의 인증 방식들을 제공하는 방법.

청구항 20

제18항 및 제19항 중 어느 한 항의 방법을 수행하는 프로그램을 수록한 컴퓨터 판독 가능 기록 매체.

발명의 설명

기 술 분 야

[0001] 아래의 실시예들은 인증 서비스 장치 및 이를 위한 방법에 관한 것으로, 특히 USIM을 이용하는 OTP 인증을 포함하는 적어도 하나의 인증 방식 중 사용자에 의해 선택된 인증 방식에 따라서 사용자에 대한 인증을 수행하는 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 최근 IT 기술의 발전에 따라 전자 상거래가 활발히 이루어지고 있다. 전자 상거래에 있어서, 피싱 등 개인 정보 유출에 따른 피해가 잇따르고 있다. 따라서, 거래 주체인 사용자 본인에 대한 인증의 중요성이 대두되고 있다.

[0003] 사용자 인증을 위해 다양한 방식들이 사용되고 있으나, 각 방식은 특유의 단점을 가지고 있다. 예를 들면, 사용자가 클라이언트 장치에 인증서를 저장하는 경우, 인증서가 저장된 사용자 클라이언트에서만 사용자에 대한 인증이 가능하다는 문제가 있다. 또한, 사용자가 모바일 단말에 인증서를 저장하는 경우, 인증서를 저장할 보안 토큰의 발급이 번거롭다는 문제가 있다. 또한, 사용자가 자금의 이체 및 포인트의 사용 등을 위해 공인 인증서 외에도 보안 카드 또는 오티피(One-Time Password; OTP)가 필요한 제휴 서비스를 사용할 경우, 사용자가 항상 보안 카드 또는 OTP 생성 장치를 소지해야 한다는 문제가 있다.

[0004] 만약, 하나의 프로그램을 통해 사용자의 선택에 따라 복수의 인증 방식들 중 하나의 인증 방식이 자동으로 결정된다면, 사용자에 대한 인증이 보다 용이하게 될 것이다.

[0005] 사용자에 대한 인증에 관련하여 한국등록특허 제10-1348079호(명칭: 휴대단말을 이용한 전자서명 시스템) 등이 공개된 바 있다.

발명의 내용

해결하려는 과제

[0006] 일 실시예는, 단일한 프로그램을 통해 사용자가 선택한 인증 방식에 따라 공인 인증서 전송 방식, 전자 서명 방식 및 OTP 방식 중 하나의 인증 방식이 자동으로 결정되고, 결정된 인증 방식에 따라 사용자에 대한 인증이 이루어지는 장치 및 방법을 제공할 수 있다.

[0007] 일 실시예는, 모바일 USIM에 의해 생성된 OTP를 사용하여 사용자에 대한 인증이 수행되는 장치 및 방법을 제공할 수 있다.

과제의 해결 수단

[0008] 일 측에 있어서, 모바일 단말에 있어서, 모바일 프로그램을 저장하는 메모리; 및 상기 모바일 프로그램을 실행하는 프로세서를 포함하고, 상기 모바일 프로그램은, 상기 메모리 및 상기 모바일 단말에 장착된 모바일 유심(USIM)의 각각에 공인 인증서를 저장하고, 상기 모바일 USIM에 의해 생성된 OTP를 출력하는 모바일 단말이 제공된다.

[0009] 상기 모바일 프로그램은 상기 모바일 단말의 사용자에 대한 인증과 관련된 적어도 하나의 인증 서비스를 제공할 수 있다.

[0010] 상기 적어도 하나의 인증 서비스는 상기 메모리에 저장된 상기 공인 인증서의 전송을 통해 상기 사용자를 인증하는 공인 인증서 전송 서비스, 상기 모바일 USIM에 저장된 상기 공인 인증서를 사용하여 상기 사용자의 전자 서명을 제공하는 전자 서명 서비스 및 상기 모바일 USIM에 의해 생성된 상기 OTP를 출력하는 OTP 서비스를 포함할 수 있다.

[0011] 상기 모바일 단말은 상기 적어도 하나의 서비스를 제공하는 상기 모바일 프로그램을 단일한 어플리케이션으로서 설치 및 관리할 수 있다.

[0012] 상기 모바일 단말은, 중계 서버로부터 상기 사용자의 인증과 관련된 인증 서비스 요청을 수신하는 통신부를 더 포함할 수 있다.

[0013] 상기 프로세서는 상기 통신부를 통해 상기 인증 서비스 요청이 수신되면 상기 모바일 프로그램을 실행할 수 있다.

[0014] 상기 모바일 프로그램은 상기 인증 서비스 요청이 나타내는 상기 사용자에 의해 선택된 인증 서비스에 따라 상기 공인 인증서 전송 서비스, 상기 전자 서명 서비스 및 상기 OTP 서비스 중 하나를 자동으로 제공할 수 있다.

[0015] 상기 인증 서비스는, 상기 클라이언트 장치에 의해 상기 사용자에 의해 선택된 상기 사용자에 대한 인증 방식이 인식되고, 상기 클라이언트 장치로부터 상기 중계 서버로 상기 인증의 방식의 정보가 전송되면, 상기 중계 서버에서 상기 인증의 방식에 따라서 자동으로 이루어지는 분기에 의해 결정될 수 있다.

[0016] 상기 모바일 USIM은 OTP를 생성하기 위한 OTP 생성 정보 및 OTP 생성 알고리즘을 저장할 수 있다.

[0017] 상기 모바일 USIM은 상기 OTP 생성 정보 및 상기 OTP 생성 알고리즘을 사용하여 상기 OTP를 생성할 수 있다.

[0018] 상기 OTP를 생성함에 있어서 상기 모바일 어플리케이션은 상기 모바일 단말의 사용자에 의해 입력된 핀(PIN) 또는 패스워드를 수신하고, 상기 핀 또는 패스워드를 사용하여 상기 사용자에 대한 인증을 수행할 수 있다.

[0019] 상기 OTP의 생성에 사용되는 인증 기술로서 시간 동기화 인증 기술, 이벤트 동기화 인증 기술, 질의-응답 인증 기술 또는 거래 연동 인증 기술 중 하나 이상의 인증 기술들이 이용될 수 있다.

[0020] 상기 모바일 단말은, 상기 모바일 프로그램을 다운로드하기 위한 주소의 정보를 수신하는 통신부를 더 포함할 수 있다.

[0021] 상기 프로세서는 상기 주소의 정보를 사용하여 상기 모바일 프로그램을 다운로드 및 설치할 수 있다.

[0022] 상기 모바일 프로그램을 다운로드하기 위한 주소의 정보는 상기 모바일 단말의 사용자가 제휴사에 상기 제휴사의 제휴 서비스에 사용되는 모바일 OTP의 발급을 신청함에 따라 중계 서버로부터 상기 모바일 단말로 전송될 수 있다.

[0023] 상기 모바일 OTP의 발급은 1차 발급 및 2차 발급을 포함할 수 있다.

[0024] 상기 1차 발급은 상기 모바일 프로그램을 설치하는 과정 및 상기 모바일 프로그램을 통해 상기 모바일 단말에게 이동통신 서비스를 제공하는 이동통신사의 이동통신 서버로부터 상기 모바일 OTP의 인증 모듈을 수신하고, 상기 인증 모듈을 상기 모바일 USIM에 설치하는 과정을 포함할 수 있다.

[0025] 상기 2차 발급은 발급 기관 서버로부터 상기 모바일 OTP의 OTP 생성 정보를 수신하고, 상기 OTP 생성 정보를 상기 모바일 USIM에 저장하는 과정을 포함할 수 있다.

[0026] 상기 사용자에 대한 본인 인증을 위한 하나 이상의 서로 다른 인증 기술들 중 상기 제휴 서비스의 이용 목적에 따라 선택된 인증 기술이 사용될 수 있다.

[0027] 상기 하나 이상의 서로 다른 인증 기술들은 대면 거래 시의 인증 기술 및 비대면 거래 시 인증 기술로 분류될 수 있다.

[0028] 상기 모바일 OTP의 발급의 신청이 비대면 거래로 이루어질 경우 상기 OTP 생성 정보는 보안 채널을 통해 전송될 수 있다.

[0029] 다른 일 측에 있어서, 클라이언트 장치에 있어서, 프로그램을 저장하는 메모리; 및 상기 프로그램을 실행하는 프로세서를 포함하고, 상기 프로그램은 적어도 하나의 인증 방식을 통해 상기 클라이언트 장치의 사용자에 대한 인증을 처리하는 클라이언트 장치가 제공될 수 있다.

[0030] 상기 적어도 하나의 인증 방식은 공인 인증서의 전송을 통해 상기 사용자를 인증하는 공인 인증서 전송 방식, 상기 사용자의 전자 서명을 통해 상기 사용자를 인증하는 전자 서명 방식 및 모바일 USIM에 의해 생성된 OTP를 통해 상기 사용자를 인증하는 제공하는 OTP 방식을 포함할 수 있다.

[0031] 상기 프로그램은 상기 적어도 하나의 인증 방식 중 상기 사용자에 의해 선택된 인증 방식을 인식할 수 있다.

[0032] 상기 프로그램은 상기 선택된 인증 방식의 정보를 포함하는 인증 요청을 중계 서버로 전송할 수 있다.

[0033] 상기 중계 서버에서 상기 선택된 인증 방식에 따라 자동으로 분기가 이루어지고, 상기 분기에 의해 결정된 인증 서비스의 요청의 내용이 상기 중계 서버로부터 상기 사용자의 모바일 단말의 모바일 프로그램으로 전송되고,

[0034] 상기 선택된 인증 방식이 상기 공인 인증서 전송 방식 또는 상기 전자 서명 방식이면, 상기 프로그램은 상기 인증 서비스에 관련하여 상기 모바일 프로그램으로부터 상기 사용자에 대한 인증에 관련된 인증용 데이터를 수신할 수 있다.

[0035] 상기 선택된 인증 방식이 상기 OTP 방식이면 상기 프로그램은 상기 클라이언트 장치의 사용자로부터 상기 인증용 데이터를 수신할 수 있고, 상기 인증용 데이터는 상기 모바일 단말에 출력된 OTP일 수 있다.

[0036] 상기 프로그램은 상기 인증용 데이터를 제휴 서버로 전송하고, 상기 제휴 서버로부터 상기 인증용 데이터를 사용하여 인증 서버에 의해 수행된 상기 사용자에 대한 인증의 결과를 수신할 수 있다.

[0037] 다른 일 측에 있어서, 모바일 단말의 인증 서비스 제공 방법에 있어서, 중계 서버로부터 상기 모바일 단말의 사용자의 인증과 관련된 인증 서비스 요청을 수신하는 단계; 및 적어도 하나의 인증 서비스 중 상기 인증 서비스 요청이 나타내는 선택된 인증 서비스를 제공하는 단계를 포함하고, 상기 적어도 하나의 인증 서비스는 상기 모바일 단말의 메모리에 저장된 공인 인증서의 전송을 통해 상기 사용자를 인증하는 공인 인증서 전송 서비스, 상기 모바일 단말의 모바일 USIM에 저장된 상기 공인 인증서를 사용하여 상기 사용자의 전자 서명을 제공하는 전자 서명 서비스 및 상기 모바일 USIM에 의해 생성된 OTP를 출력하는 OTP 서비스를 포함하고, 상기 모바일 단말은 모바일 프로그램을 실행하고, 상기 모바일 프로그램은 상기 인증 서비스 요청이 나타내는 상기 선택된 인증 서비스에 따라 상기 공인 인증서 전송 서비스, 상기 전자 서명 서비스 및 상기 OTP 서비스 중 하나를 자동으로 제공하는 인증 서비스 제공 방법이 제공될 수 있다.

[0038] 또 다른 일 측에 있어서, 클라이언트 장치의 인증 서비스 제공 방법에 있어서, 적어도 하나의 인증 방식 중 상기 클라이언트 장치의 사용자에 의해 선택된 인증의 방식을 인식하는 단계; 상기 선택된 인증 방식의 정보를 포함하는 인증 요청을 중계 서버로 전송하는 단계; 및 상기 중계 서버에서 상기 선택된 인증 방식에 따라 자동으로 분기가 이루어지고, 상기 분기에 의해 결정된 인증 서비스의 요청의 내용이 상기 중계 서버로부터 상기 사용자의 모바일 단말의 모바일 프로그램으로 전송되면, 상기 인증 서비스에 관련하여 상기 모바일 프로그램으로부터 상기 사용자에 대한 인증에 관련된 인증용 데이터를 수신하는 단계를 포함하고, 상기 적어도 하나의 인증 방식은 공인 인증서의 전송을 통해 상기 사용자를 인증하는 공인 인증서 전송 방식, 상기 사용자의 전자 서명을 통해 상기 사용자를 인증하는 전자 서명 방식 및 모바일 USIM에 의해 생성된 OTP를 통해 상기 사용자를 인증하는 제공하는 OTP 방식을 포함하는 인증 서비스 제공 방법이 제공될 수 있다.

발명의 효과

[0039] 단일한 프로그램을 통해 사용자가 선택한 인증 방식에 따라 공인 인증서 전송 방식, 전자 서명 방식 및 OTP 방식 중 하나의 인증 방식이 자동으로 결정되고, 결정된 인증 방식에 따라 사용자에 대한 인증이 이루어지는 장치 및 방법이 제공된다.

[0040] 모바일 USIM에 의해 생성된 OTP를 사용하여 사용자에 대한 인증이 수행되는 장치 및 방법이 제공된다.

도면의 간단한 설명

[0041] 도 1은 일 실시예에 따른 인증 서비스 시스템을 나타낸다.

도 2는 일 실시예에 따른 클라이언트 장치의 블록도이다.

도 3은 일 실시예에 따른 모바일 단말의 블록도이다.

도 4는 일 실시예에 따른 인증 서비스 시스템의 동작을 나타내는 신호 흐름도이다.

도 5는 일 예에 따른 모바일 프로그램 설치 단계를 나타내는 신호 흐름도이다.

도 6은 일 예에 따른 OTP 서비스 방법의 신호 흐름도이다.

도 7은 일 예에 따른 전자 서명 서비스 방법의 신호 흐름도이다.

도 8은 일 예에 따른 공인 인증서 전송 서비스 방법의 신호 흐름도이다.

도 9는 일 예에 따른 클라이언트 단말 및 모바일 단말에 표시되는 인터페이스 화면을 나타낸다.

도 10은 일 예에 따른 클라이언트 장치 및 모바일 단말에 표시되는 다른 인터페이스 화면을 나타낸다.

도 11은 일 예에 따른 클라이언트 장치 및 모바일 단말에 표시되는 또 다른 인터페이스 화면을 나타낸다.

도 12는 일 예에 따른 클라이언트 장치 및 모바일 단말에 표시되는 또 다른 인터페이스 화면을 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0042] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의

다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예에 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[0043] 이하에서는, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있도록 하기 위하여, 본 발명의 바람직한 실시예들에 관하여 첨부된 도면을 참조하여 상세히 설명하기로 한다.

[0044] 도 1은 일 실시예에 따른 인증 서비스 시스템을 나타낸다.

[0045] 인증 서비스 시스템(100)은 클라이언트 장치(110), 중계 서버(120), 모바일 단말(130), 제휴 서버(140), 이동통신 서버(150), 인증 서버(160), 발급 기관 서버(170) 및 앱 서버(180) 중 적어도 하나를 포함할 수 있다.

[0046] 사용자는 클라이언트 장치(110)를 통해 소정의 서비스를 제공받을 수 있다. 예를 들면, 사용자는 클라이언트 장치(110)를 통해 인터넷 서비스 및 웹 서비스 등을 제공받을 수 있다. 또한, 사용자는 모바일 단말(130)을 사용할 수 있다. 이하에서, 클라이언트 장치(110)의 사용자 및 모바일 단말(130)의 사용자는 동일인을 의미할 수 있다. 또한, 이하의 설명에서, 클라이언트 장치(110)의 사용자 및 모바일 단말(130)의 사용자는 서로 대체되어 사용될 수 있다.

[0047] 클라이언트 장치(110)는 개인용 컴퓨터(Personal Computer; PC), 노트북 컴퓨터, 휴대폰(mobile phone), 태블릿 PC, 네비게이션(navigation), 스마트폰(smart phone), PDA(Personal Digital Assistants), 또는 DVB(Digital Video Broadcasting)와 같은 통신 장치일 수 있다.

[0048] 서비스의 제공에 있어서, 사용자에 대한 인증이 요구될 수 있다. 사용자는 사용자에 대한 인증을 위해 클라이언트 장치(110) 및 모바일 단말(130)을 사용할 수 있다.

[0049] 클라이언트 장치(110)는 적어도 하나의 인증 방식을 통해 클라이언트 장치(110)의 사용자에 대한 인증을 처리할 수 있다. 사용자에 대한 인증을 처리하기 위해 사용되는 적어도 하나의 인증 방식은, 공인 인증서의 전송을 통해 사용자를 인증하는 공인 인증서 전송 방식, 사용자의 전자 서명을 통해 사용자를 인증하는 전자 서명 방식 및 모바일 유심(Universal Subscriber Identification Module; USIM)에 의해 생성된 오티피(One-Time Password; OTP)를 통해 상기 사용자를 인증하는 제공하는 OTP 방식을 포함할 수 있다.

[0050] 클라이언트 장치(110)는 사용자에 대한 인증을 처리하기 위해 사용되는 적어도 하나의 인증 방식 중 사용자에 의해 선택된 인증 방식을 인식할 수 있다. 선택된 인증 방식이 인식되면, 클라이언트 장치(110)에서는 선택된 인증 방식에 따라 자동으로 분기가 이루어질 수 있다. 예를 들면, 클라이언트 장치(110)는 선택된 인증 방식이 공인 인증서 전송 방식일 경우 공인 인증서 전송 모드로 분기할 수 있다. 클라이언트 장치(110)는 선택된 인증 방식이 전자 서명 방식일 경우 전자 서명 모드로 분기할 수 있다. 클라이언트 장치(110)는 선택된 인증 방식이 OTP 방식일 경우 OTP 모드로 분기할 수 있다.

[0051] 클라이언트 장치(110)는 선택된 인증 방식의 정보를 중계 서버(120)로 전송할 수 있다.

[0052] 선택된 인증 방식의 정보가 전송되면, 중계 서버(120)에서는 선택된 인증 방식에 따라 자동으로 분기가 이루어질 수 있다. 예를 들면, 중계 서버(120)는 선택된 인증 방식이 공인 인증서 전송 방식일 경우 공인 인증서 전송 모드로 분기할 수 있다. 중계 서버(120)는 선택된 인증 방식이 전자 서명 방식일 경우 전자 서명 모드로 분기할 수 있다. 중계 서버(120)는 선택된 인증 방식이 OTP 방식일 경우 OTP 모드로 분기할 수 있다.

[0053] 중계 서버(120)에서 선택된 인증 방식에 따른 분기가 이루어지면, 분기에 의해 적어도 하나의 인증 서비스 중 요청될 인증 서비스가 선택될 수 있다. 예를 들면, 중계 서버(120)가 공인 인증서 전송 모드로 분기한 경우, 선택된 인증 서비스는 공인 인증서 전송 서비스일 수 있다. 중계 서버(120)가 전자 서명 모드로 분기한 경우, 선택된 인증 서비스는 전자 서명 서비스일 수 있다. 중계 서버(120)가 OTP 모드로 분기한 경우, 선택된 인증 서비스는 OTP 서비스일 수 있다.

[0054] 중계 서버(120)는 선택된 인증 서비스의 정보를 모바일 단말(130)로 전송할 수 있다.

[0055] 모바일 단말(130)은 사용자에 대한 인증과 관련된 적어도 하나의 인증 서비스를 제공할 수 있다. 적어도 하나의 인증 서비스는 모바일 단말(130)의 메모리에 저장된 공인 인증서의 전송을 통해 사용자를 인증하는 공인 인증서 전송 서비스, 모바일 단말(130)에 장착된 모바일 USIM에 저장된 공인 인증서를 사용하여 사용자의 전자 서명을 제공하는 전자 서명 서비스 및 모바일 USIM에 의해 생성된 OTP를 출력하는 OTP 서비스를 포함할 수 있다.

[0056] 선택된 인증 서비스의 정보가 전송되면, 모바일 단말(130)의 모바일 프로그램에서는 선택된 인증 서비스에 따라 자동으로 분기가 이루어질 수 있다. 예를 들면, 모바일 단말(130)의 모바일 프로그램은 선택된 인증 서비스가 공인 인증서 전송 서비스일 경우 공인 인증서 전송 모드로 분기할 수 있다. 모바일 단말(130)의 모바일 프로그램은 선택된 인증 서비스가 전자 서명 서비스일 경우 전자 서명 모드로 분기할 수 있다. 모바일 단말(130)의 모바일 프로그램은 선택된 인증 서비스가 OTP 서비스일 경우 OTP 모드로 분기할 수 있다.

[0057] 선택된 인증 서비스의 정보가 전송되고, 선택된 인증 서비스에 따른 분기가 이루어지면, 모바일 단말(130)은 모바일 단말(130)에 의해 제공되는 적어도 하나의 인증 서비스 중 선택된 인증 서비스를 제공할 수 있다. 모바일 단말(130)은 선택된 인증 서비스에 따라, 공인 인증서 전송 서비스, 전자 서명 서비스 및 OTP 서비스 중 하나를 자동으로 제공할 수 있다.

[0058] 클라이언트 장치(110), 중계 서버(120) 및 모바일 단말(130)은 통신, 특히 보안 채널의 형성에 있어서, 암호화 통신을 사용할 수 있다. 예를 들면, 보안 채널은 보안 소켓 레이어(Secure Socket Layer; SSL) 채널일 수 있다.

[0059] 제휴 서버(140)는 제휴사에 의해 운영될 수 있다. 제휴사는 클라이언트 장치(110)를 통해 제공되는 소정의 서비스를 제공하는 주체일 수 있다. 예를 들면, 제휴사는 금융사일 수 있다.

[0060] 인증 서비스의 제공에 있어서, 클라이언트 장치(110), 중계 서버(120) 및 모바일 단말(130) 간의 상호 작용이 이루어질 수 있다. 또한, 인증 서비스의 제공을 위해 제휴 서버(140), 이동통신 서버(150) 및 인증 서버(160)와의 상호 작용이 사용될 수 있다.

[0061] 인증 서버(160)는 복수일 수 있다. 적어도 하나의 인증 방식의 일부에 대해 별개의 인증 서버가 사용될 수 있다. 예를 들면, 공인 인증서 전송 방식 및 전자 서명 인증 서버에 대해서는 동일한 공인 인증서 인증 서버가 사용될 수 있다. OTP 방식에 대해서는 OTP 인증 서버가 사용될 수 있다.

[0062] 발급 기관 서버(170)는 OTP의 2차 발급 과정에서, OTP 생성 정보를 모바일 단말(130)에게 제공할 수 있다.

[0063] 앱 서버(180)는 모바일 단말(130)을 위한 다양한 모바일 프로그램들을 제공하는 앱 스토어일 수 있다. 앱 서버(180)는 이동통신 서버(150)를 운영하는 이동통신사에 의해 운영될 수 있다. 또는, 앱 서버(180)는 모바일 단말(130)을 제조하는 업체에 의해 운영될 수 있으며, 모바일 단말(130)의 운영 체제를 제조하는 업체에 의해 운영될 수 있다.

[0064] 인증 서비스를 위한 클라이언트 장치(110), 중계 서버(120), 모바일 단말(130), 제휴 서버(140), 이동통신 서버(150), 인증 서버(160), 발급 기관 서버(170) 및 앱 서버(180)의 기능 및 동작이 아래의 실시예들에서 보다 상세하게 설명된다.

[0065] 도 2는 일 실시예에 따른 클라이언트 장치의 블록도이다.

[0066] 클라이언트 장치(110)는 프로세서(210), 메모리(220) 및 통신부(230)를 포함할 수 있다.

[0067] 프로세서(210)는 프로그램을 실행할 수 있다. 메모리(220)는 프로그램을 저장할 수 있다. 여기에서, 프로그램은 사용자에 대한 인증을 제공하는 인증 서비스 프로그램을 포함할 수 있다.

[0068] 통신부(230)는 외부의 다른 장치로부터 데이터 또는 정보를 수신할 수 있고, 외부의 다른 장치로 데이터 또는 정보를 전송할 수 있다.

[0069] 프로그램은 적어도 하나의 인증 방식을 통해 클라이언트 장치(110)의 사용자에 대한 인증을 처리할 수 있다. 적어도 하나의 인증 방식은 공인 인증서의 전송을 통해 사용자를 인증하는 공인 인증서 전송 방식, 상기 사용자의 전자 서명을 통해 사용자를 인증하는 전자 서명 방식 및 모바일 USIM에 의해 생성된 OTP를 통해 사용자를 인증하는 제공하는 OTP 방식을 포함할 수 있다.

[0070] 또한, 프로그램은 공인 인증서의 선택 및 공인 인증서의 패스워드의 입력을 위한 인터페이스를 클라이언트 장치(110)의 사용자에게 제공할 수 있고, 사용자로부터 공인 인증서의 선택 및 공인 인증서의 패스워드를 수신할 수

있다.

[0071] 프로그램은 하나의 동적 링크 라이브러리(Dynamic-link Library; DLL)를 이용할 수 있다.

[0072] 클라이언트 장치(110) 및 프로그램의 기능 및 동작이 아래의 실시예들에서 보다 상세하게 설명된다.

[0073] 도 3은 일 실시예에 따른 모바일 단말의 블록도이다.

[0074] 모바일 단말(130)은 프로세서(310), 메모리(320) 및 통신부(330)를 포함할 수 있다.

[0075] 프로세서(310)는 모바일 프로그램을 실행할 수 있다. 메모리(320)는 모바일 프로그램을 저장할 수 있다. 메모리(320)는 모바일 단말(130)의 내장 메모리일 수 있다. 또는, 메모리(320)는 메모리 카드(card) 등과 같은 모바일 단말(130)에 장착된 메모리일 수 있다.

[0076] 통신부(330)는 외부의 다른 장치로부터 데이터 또는 정보를 수신할 수 있고, 외부의 다른 장치로 데이터 또는 정보를 전송할 수 있다.

[0077] 모바일 단말(130)에는 모바일 USIM(340)이 장착될 수 있다. 또는, 모바일 단말(130)은 모바일 USIM(340)을 포함할 수 있다.

[0078] 모바일 프로그램은 모바일 단말(130)의 사용자에 대한 인증과 관련된 적어도 하나의 인증 서비스를 제공할 수 있다. 적어도 하나의 인증 서비스는 모바일 단말(130)의 메모리(320)에 저장된 공인 인증서의 전송을 통해 사용자를 인증하는 공인 인증서 전송 서비스, 모바일 단말(130)에 장착된 모바일 USIM(340)에 저장된 공인 인증서를 사용하여 사용자의 전자 서명을 제공하는 전자 서명 서비스 및 모바일 USIM(340)에 의해 생성된 OTP를 출력하는 OTP 서비스를 포함할 수 있다.

[0079] 모바일 USIM(340)은 USIM 보안 토큰을 제공할 수 있다. USIM 보안 토큰은 모바일 USIM(340) 내의 보안 모듈을 구비한 보안 토큰일 수 있다. 이하에서, USIM 보안 토큰은 보안 토큰으로 약술될 수 있다. 모바일 프로그램은 USIM 보안 토큰에 인증서를 저장할 수 있다.

[0080] 모바일 프로그램은 메모리(320) 및 모바일 USIM(340)의 각각에 공인 인증서를 저장할 수 있다.

[0081] 모바일 프로그램은 메모리(320)에 사용자의 공인 인증서를 저장할 수 있다. 모바일 프로그램은 공인 인증서에 대한 암호화를 수행함으로써 암호화된 공인 인증서를 생성할 수 있고, 암호화된 공인 인증서를 메모리(320)에 저장할 수 있다. 메모리(320)에 저장된 공인 인증서는 공인 인증서 전송 서비스를 위해 사용될 수 있다.

[0082] 또한, 모바일 프로그램은 모바일 USIM(340)에 사용자의 공인 인증서에 대한 정보를 저장할 수 있다.

[0083] 공인 인증서에 대한 정보는 공인 인증서 중 적어도 일부의 정보를 포함할 수 있다. 예를 들면, 공인 인증서에 대한 정보는 사용자의 개인 키를 포함할 수 있다. USIM에 저장된 공인 인증서는 전자 서명 서비스를 위해 사용될 수 있다.

[0084] 모바일 USIM(340)은 OTP를 생성하기 위한 OTP 생성 정보 및 OTP 생성 알고리즘을 저장할 수 있다. 모바일 USIM(340)은 OTP 생성 정보 및 OTP 생성 알고리즘을 사용하여 OTP를 생성할 수 있다. OTP 생성 정보는 OTP 생성 시드(seed) 정보를 포함할 수 있으며, 기타 OTP 생성을 위한 부가 정보를 포함할 수 있다.

[0085] OTP의 생성에 사용되는 인증 기술로서 시간 동기화 인증 기술, 이벤트 동기화 인증 기술, 질의-응답 인증 기술 또는 거래 연동 인증 기술 중 하나 이상의 인증 기술들이 이용될 수 있다. 이러한 인증 기술들은 모바일 USIM(340) 및 인증 서버(160)에 의해 사용될 수 있다.

[0086] OTP를 생성함에 있어서, 모바일 프로그램은 사용자에 대한 인증을 요구할 수 있다. 사용자에 대한 인증을 위해, 모바일 프로그램은 사용자에 의해 입력된 개인 정보를 수신할 수 있다. 개인 정보는 사용자의 패스워드 또는 사용자의 핀(Personal Identification Number; PIN)일 수 있다. 모바일 프로그램은 핀 또는 패스워드를 사용하여 사용자에 대한 인증을 수행할 수 있다.

[0087] 모바일 프로그램은 모바일 USIM(340)에게 OTP 인증 요청을 전송할 수 있다. OTP 인증 요청이 전송되면, 모바일 USIM(340)은 OTP를 생성할 수 있고, 생성된 OTP를 모바일 프로그램으로 전송할 수 있다. 생성된 OTP가 전송되면 모바일 프로그램은 OTP를 출력할 수 있다. OTP가 출력되면, 모바일 단말(130)의 사용자는 출력된 OTP를 인식할 수 있고, OTP를 사용할 수 있다.

[0088] OTP 생성 정보는 비밀키(또는, 시드(seed)), 업체 코드, 일련 번호, 사용자 키, 모바일 단말(130)의 식별 정보, 이벤트 발생 정보 및 시간 정보 등을 포함할 수 있다. 모바일 단말(130)의 식별 정보는, 모바일 디렉토리 번호(Mobile Directory Number; MDN) 및 모바일 식별 번호(Mobile Identification Number; MIN) 등과 같은, 모바일 단말(130)을 고유하게 식별할 수 있는 정보 중 어느 하나일 수 있다.

[0089] 또한, OTP 생성 정보는 OTP의 생성에 관련된 부가 정보를 포함할 수 있다. OTP 생성 정보는 발급 기관 서버(170) 에 의해 생성 또는 관리될 수 있다.

[0090] 모바일 단말(130) 또는 모바일 단말(130)의 운영 체제(Operating System)은 적어도 하나의 서비스를 제공하는 모바일 프로그램을 단일한 어플리케이션으로서 설치 및 관리할 수 있다.

[0091] 모바일 프로그램에 의해 다양한 인증 서비스들이 제공됨에 따라, 사용자는 자신이 항상 휴대하고 있는 모바일 단말(130)을 통해 자신에게 필요한 인증 서비스들을 제공받을 수 있다. 또한, 다양한 인증 서비스들이 단일한 어플리케이션으로서 설치 및 관리되는 모바일 어플리케이션에 의해 제공됨에 따라, 인증 서비스 별로 어플리케이션을 설치 및 관리하는 불편함이 해소될 수 있다. 또한, 모바일 어플리케이션을 통해 다양한 인증 서비스들에 대하여 통일된 사용자 인터페이스(user interface) 및 사용자 경험(user experience)이 제공될 수 있다.

[0092] 또한, 단일한 모바일 프로그램에 의해 다양한 인증 서비스들이 제공됨에 따라, 어플리케이션의 설치에 따른 저장 공간의 문제 및 보안 문제들이 해결될 수 있다.

[0093] 도 4는 일 실시예에 따른 인증 서비스 시스템의 동작을 나타내는 신호 흐름도이다.

[0094] 단계(405)에서, 보안 채널이 형성될 수 있다. 클라이언트 장치(110), 중계 서버(120) 및 모바일 단말(130) 간의 통신은 보안 채널을 통해 이루어질 수 있다.

[0095] 클라이언트 장치(110)의 프로그램은 클라이언트 장치(110) 및 중계 서버(120) 간의 보안 채널을 형성할 수 있다. 또한, 모바일 단말(130)의 모바일 프로그램은 모바일 단말(130) 및 중계 서버(120) 간의 보안 채널을 형성할 수 있다.

[0096] 단계(405)의 실행 순서는 단지 예시적인 것이다. 예를 들면, 보안 채널의 형성은 단계(405)는 후술될 단계(430) 및 단계(460)에서 이루어지거나, 단계(430) 및 단계(460)의 이전에 이루어질 수 있고, 단계(430) 및 단계(460) 등과는 별도의 단계로서 이루어질 수 있다.

[0097] 클라이언트 장치(110) 및 중계 서버(120) 간의 보안 채널의 형성에 있어서, 클라이언트 장치(110)의 프로그램은 사용자에 의해 입력된 모바일 단말(130)의 식별자를 중계 서버(120)로 전송할 수 있다. 클라이언트 장치(110)의 프로그램은 비밀 키를 생성할 수 있고, 생성된 비밀 키를 중계 서버(120)로 전송함으로써 비밀 키를 중계 서버(120)와 공유할 수 있다. 비밀 키의 전송 전, 클라이언트 장치(110)의 프로그램은 중계 서버(120)의 공개 키를 사용하여 비밀 키를 암호화함으로써 암호화된 비밀 키를 생성할 수 있고, 암호화된 비밀 키를 중계 서버(120)로 전송할 수 있다. 중계 서버(120)는 중계 서버(120)의 개인 키를 사용하여 암호화된 비밀 키를 복호화함으로써 비밀 키를 생성할 수 있다.

[0098] 모바일 단말(130) 및 중계 서버(120) 간의 보안 채널의 형성에 있어서, 모바일 단말(130)의 모바일 프로그램은 비밀 키를 생성할 수 있고, 생성된 비밀 키를 중계 서버(120)로 전송함으로써 비밀 키를 중계 서버(120)와 공유할 수 있다. 비밀 키의 전송 전, 모바일 단말(130)의 모바일 프로그램은 중계 서버(120)의 공개 키를 사용하여 비밀 키를 암호화함으로써 암호화된 비밀 키를 생성할 수 있고, 암호화된 비밀 키를 중계 서버(120)로 전송할 수 있다. 중계 서버(120)는 중계 서버(120)의 개인 키를 사용하여 암호화된 비밀 키를 복호화함으로써 비밀 키를 생성할 수 있다.

[0099] 보안 채널의 형성에 있어서, 클라이언트 장치(110), 중계 서버(120) 및 모바일 단말(130)는 유도 키를 이용한 세션 키 생성 방식을 사용할 수 있다. 유도 키를 이용한 세션 키 생성 방식을 통해 보다 보안이 강화된 인증 서비스가 제공될 수 있다.

[0100] 또한, 모바일 단말(130)의 모바일 프로그램은 USIM 보안 토큰에 공인 인증서를 저장하기 위해, 공인 인증서의 저장을 위한 보안 채널을 형성할 수 있다.

[0101] 모바일 단말(130)의 모바일 프로그램은 통신부(330)를 통해 중계 서버(120)에게 USIM 보안 토큰에 공인 인증서를 저장하기 위한 세션 키를 생성할 것을 요청할 수 있다. 또한, 세션 키의 요청과 함께, 모바일 단말(130)의

모바일 프로그램은 통신부(330)를 통해 유도 키를 생성하기 위한 모바일 USIM(340)의 USIM 고유 값을 중계 서버(120)로 전송할 수 있다. 중계 서버(120)는 USIM 고유 값을 사용하여 유도 키를 생성할 수 있고, 유도 키를 사용하여 공인 인증서를 저장하기 위한 세션 키를 생성할 수 있다. 중계 서버(120)는 세션 키를 모바일 단말(130)의 통신부(330)로 전송할 수 있다. 모바일 단말(130)의 모바일 프로그램은 통신부(330)를 통해 세션 키를 수신할 수 있다. 세션 키를 통해 모바일 프로그램 및 USIM 보안 토큰 간의 보안 채널이 형성될 수 있다. 모바일 단말(130)의 모바일 프로그램은 생성된 보안 채널을 통해 USIM 보안 토큰에 공인 인증서를 저장할 수 있다.

[0102] 또한, 모바일 단말(130)의 모바일 프로그램은 USIM 보안 토큰으로부터 공인 인증서를 발급받기 위해, USIM 보안 토큰의 애플릿과의 보안 채널을 형성할 수 있다.

[0103] 모바일 단말(130)의 모바일 프로그램은 통신부(330)를 통해 중계 서버(120)에게 인증서 발급을 위한 세션 키를 생성할 것을 요청할 수 있다. 여기에서, 세션 키는 USIM 보안 토큰에 저장된 유도 키를 이용하여 생성된 것일 수 있다. 또한, 세션 키의 요청과 함께, 모바일 단말(130)의 모바일 프로그램은 통신부(330)를 통해 유도 키를 생성하기 위한 모바일 USIM(340)의 USIM 고유 값을 중계 서버(120)로 전송할 수 있다. 중계 서버(120)는 USIM 고유 값을 사용하여 유도 키를 생성할 수 있고, 유도 키를 사용하여 공인 인증서를 발급하기 위한 세션 키를 생성할 수 있다. 중계 서버(120)는 세션 키를 모바일 단말(130)의 통신부(330)로 전송할 수 있다. 모바일 단말(130)의 모바일 프로그램은 통신부(330)를 통해 세션 키를 수신할 수 있다.

[0104] 또한, 모바일 단말(130)의 모바일 프로그램은 클라이언트 장치(110)의 프로그램으로부터 USIM 보안 토큰에 공인 인증서의 발급을 하기 위해, 모바일 USIM 보안 토큰의 애플릿 및 클라이언트 장치(110)의 프로그램 간의 보안 채널을 형성할 수 있다.

[0105] 모바일 단말(130)의 모바일 프로그램은 통신부(330)를 통해 중계 서버(120)에게 유도 키를 생성하기 위한 모바일 USIM(340)의 USIM 고유 값을 전송할 수 있다. 중계 서버(120)는 USIM 고유 값을 사용하여 유도 키를 생성할 수 있고, 유도 키를 사용하여 공인 인증서를 발급하기 위한 세션 키 및 클라이언트 장치(110)의 접근 용 인증 키를 생성할 수 있다. 중계 서버(120)는 클라이언트 장치(110)의 접근 용 인증 키를 모바일 장치(130)의 통신부(330)로 전송할 수 있다. 모바일 단말(130)의 모바일 프로그램은 통신부(330)를 통해 클라이언트 장치(110)의 접근 용 인증 키를 수신할 수 있고, 통신부(330)를 통해 클라이언트 장치(110)의 접근 용 인증 키를 클라이언트 장치(110)의 통신부(230)로 전송할 수 있다. 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 클라이언트 장치(110)의 접근 용 인증 키를 수신할 수 있다.

[0106] 클라이언트 장치(110)의 프로그램은 클라이언트 장치(110)의 접근 용 인증 키를 사용하여 중계 서버(120)에 접근할 수 있고, 중계 서버(120)로부터 공인 인증서를 발급하기 위한 세션 키를 수신할 수 있다. 상술된 것과 같은 과정을 통해, 모바일 단말(130)의 모바일 프로그램은 USIM 보안 토큰의 애플릿 및 클라이언트 장치(110)의 프로그램 간의 보안 채널을 형성할 수 있고, 형성된 보안 채널을 통해 USIM 보안 토큰에 인증서를 발급할 수 있다.

[0107] 상술된 보안 채널에 관련된 내용은, 전자 서명의 결과 값을 전송하는 경우에도 적용될 수 있다.

[0108] 단계(410)에서, 클라이언트 장치(110)의 프로그램은 프로그램에 의해 제공되는 사용자에 대한 적어도 하나의 인증 방식을 출력할 수 있다. 말하자면, 클라이언트 장치(110)의 프로그램은 사용자에게 가용한 인증 방식의 목록을 출력할 수 있다.

[0109] 사용자는 출력된 적어도 하나의 인증 방식 중 하나의 인증 방식을 선택할 수 있고, 선택된 인증 방식을 클라이언트 장치(110)의 프로그램에 입력할 수 있다.

[0110] 단계(420)에서, 입력을 통해, 클라이언트 장치(110)의 프로그램은 사용자에 대한 인증을 처리하기 위해 사용되는 적어도 하나의 인증 방식 중 사용자에 의해 선택된 인증 방식을 인식할 수 있다.

[0111] 선택된 인증 방식이 인식되면, 클라이언트 장치(110)의 프로그램에서는 선택된 인증 방식에 따라 자동으로 분기가 이루어질 수 있다. 예를 들면, 클라이언트 장치(110)의 프로그램은 선택된 인증 방식이 공인 인증서 전송 방식일 경우 공인 인증서 전송 모드로 분기할 수 있다. 클라이언트 장치(110)는 선택된 인증 방식이 전자 서명 방식일 경우 전자 서명 모드로 분기할 수 있다. 클라이언트 장치(110)는 선택된 인증 방식이 OTP 방식일 경우 OTP 모드로 분기할 수 있다.

[0112] 단계(430)에서, 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 인증 요청을 중계 서버(120)로 전송할 수 있다. 인증 요청은 선택된 인증 방식의 정보를 포함할 수 있다. 인증 요청을 통해, 선택된 인증 방식의 정보

가 중계 서버(120)로 전송될 수 있다.

[0113] 인증 요청은 모바일 단말(130)의 식별자를 포함할 수 있다. 모바일 단말(130)의 식별자는 클라이언트 장치(110)의 사용자에 의해 클라이언트 장치(110)에 입력될 수 있다. 클라이언트 장치(110)의 프로그램은 사용자에 의해 입력된 모바일 단말(130)의 식별자를 인식할 수 있고, 모바일 단말(130)의 식별자를 인증 요청에 포함시킬 수 있다.

[0114] 단계(440)에서, 선택된 인증 방식의 정보가 전송되면, 중계 서버(120)에서는 선택된 인증 방식에 따라 자동으로 분기가 이루어질 수 있다. 예를 들면, 중계 서버(120)는 선택된 인증 방식이 공인 인증서 전송 방식일 경우 공인 인증서 전송 모드로 분기할 수 있다. 중계 서버(120)는 선택된 인증 방식이 전자 서명 방식일 경우 전자 서명 모드로 분기할 수 있다. 중계 서버(120)는 선택된 인증 방식이 OTP 방식일 경우 OTP 모드로 분기할 수 있다.

[0115] 단계(450)에서, 중계 서버(120)에서 선택된 인증 방식에 따른 분기가 이루어지면, 중계 서버(120)는 분기에 따라 자동으로 결정된 모드에 따라 중계를 수행할 수 있다.

[0116] 또한, 중계 서버(120)에서 선택된 인증 방식에 따른 분기가 이루어지면, 중계 서버(120)는 모바일 단말(130)에 의해 제공되는 적어도 하나의 인증 서비스 중 요청될 인증 서비스를 선택할 수 있다. 예를 들면, 중계 서버(120)가 공인 인증서 전송 모드로 분기한 경우, 선택된 인증 서비스는 공인 인증서 전송 서비스일 수 있다. 중계 서버(120)가 전자 서명 모드로 분기한 경우, 선택된 인증 서비스는 전자 서명 서비스일 수 있다. 중계 서버(120)가 OTP 모드로 분기한 경우, 선택된 인증 서비스는 OTP 서비스일 수 있다.

[0117] 중계 서버(120)는 인증 요청 내의 모바일 단말(130)의 식별자를 사용하여 모바일 단말(130)을 식별할 수 있다.

[0118] 단계(460)에서, 중계 서버(120)는 클라이언트 장치(110)의 사용자에 대한 인증과 관련된 인증 서비스 요청을 모바일 단말(130)의 통신부(330)로 전송할 수 있다. 모바일 단말(130)의 통신부(330)는 중계 서버(120)로부터 인증 서비스 요청을 수신할 수 있다.

[0119] 인증 서비스 요청은 선택된 인증 서비스의 정보를 포함할 수 있다. 인증 서비스 요청을 통해 선택된 인증 서비스의 정보가 모바일 단말(130)로 전송될 수 있다.

[0120] 인증 서비스 요청은 모바일 단말(130)에서 출력될 설치 안내 메시지 및/또는 실행 안내 메시지에 대한 정보를 포함할 수 있다. 말하자면, 인증 서비스 요청은 설치 안내 메시지 또는 실행 안내 메시지일 수 있다.

[0121] 설치 안내 메시지는 기정의된 형태로 전송될 수 있다. 예를 들면, 설치 안내 메시지는 URL(Uniform Resource Locator) 주소를 포함할 수 있다. 또는, 설치 안내 메시지는 단문 메시지 서비스(Short Message Service; SMS) 또는 푸쉬(push) 알림 메시지일 수 있다. 중계 서버(120)는 모바일 단말(130)의 타입(type) 또는 구성(configuration)에 따라 하나 이상의 형태들 중 모바일 단말(130)에 적합한 형태의 설치 안내 메시지를 선택할 수 있다.

[0122] 실행 안내 메시지는 기정의된 형태로 전송될 수 있다. 예를 들면, 실행 안내 메시지는 URL 주소를 포함할 수 있다. 또는, 실행 안내 메시지는 SMS 또는 푸쉬 알림 메시지일 수 있다. 중계 서버(120)는 모바일 단말(130)의 타입 또는 구성에 따라 하나 이상의 형태들 중 모바일 단말(130)에 적합한 형태의 실행 안내 메시지를 선택할 수 있다.

[0123] 설치 안내 메시지의 형태 및 실행 안내 메시지의 형태는 서로 동일할 수 있으며, 서로 상이할 수도 있다.

[0124] 단계(470)에서, 통신부(330)를 통해 인증 서비스 요청이 수신되면, 프로세서(310)는 모바일 프로그램을 실행할 수 있다. 또한, 프로세서(310)는 인증 서비스 요청을 모바일 프로그램으로 전달할 수 있다.

[0125] 인증 서비스 요청이 설치 안내 메시지인 경우, 프로세서(310)는 설치 안내 메시지에 의해 모바일 프로그램의 설치에 대한 사용자의 확인이 이루어진 후 모바일 프로그램을 설치할 수 있다. 예를 들면, 인증 서비스 요청이 수신되면, 프로세서(310)는 설치 안내 메시지에 대한 정보를 사용하여 설치 안내 메시지를 출력할 수 있다. 모바일 단말(130)의 사용자는 출력된 설치 안내 메시지를 확인할 수 있고, 사용자에 의해 설치 안내 메시지에 대한 확인이 모바일 단말(130)로 입력되면 프로세서(310)는 모바일 프로그램을 모바일 단말(130)에 설치할 수 있다.

[0126] 인증 서비스 요청이 실행 안내 메시지인 경우, 프로세서(310)는 실행 안내 메시지에 의해 모바일 프로그램의 실행에 대한 사용자의 확인이 이루어진 후 모바일 프로그램을 실행할 수 있다. 예를 들면, 인증 서비스 요청은 모바일 단말(130)에서 출력될 실행 안내 메시지에 대한 정보를 포함할 수 있다. 인증 서비스 요청이 수신되면, 프로세서(310)는 실행 안내 메시지에 대한 정보를 사용하여 실행 안내 메시지를 출력할 수 있다. 모바일 단말

(130)의 사용자는 출력된 실행 안내 메시지를 확인할 수 있고, 사용자에 의해 실행 안내 메시지에 대한 확인이 모바일 단말(130)로 입력되면 프로세서(310)는 모바일 프로그램을 실행할 수 있다.

[0127] 단계(480)에서, 선택된 인증 서비스의 정보가 전송되면, 모바일 단말(130)의 모바일 프로그램에서는 선택된 인증 서비스에 따라 자동으로 분기가 이루어질 수 있다. 예를 들면, 모바일 단말(130)의 모바일 프로그램은 선택된 인증 서비스가 공인 인증서 전송 서비스일 경우 공인 인증서 전송 모드로 분기할 수 있다. 모바일 단말(130)의 모바일 프로그램은 선택된 인증 방식이 전자 서명 서비스일 경우 전자 서명 모드로 분기할 수 있다. 모바일 단말(130)의 모바일 프로그램은 선택된 인증 방식이 OTP 서비스일 경우 OTP 모드로 분기할 수 있다.

[0128] 단계(490)에서, 선택된 인증 서비스의 정보가 전송되고, 선택된 인증 서비스에 따른 분기가 이루어지면, 모바일 단말(130)의 모바일 프로그램은 모바일 프로그램에 의해 제공되는 적어도 하나의 인증 서비스 중 선택된 인증 서비스를 제공할 수 있다. 모바일 단말(130)의 모바일 프로그램은 인증 서비스 요청이 나타내는 사용자에 의해 선택된 인증 서비스에 따라 공인 인증서 전송 서비스, 전자 서명 서비스 및 OTP 서비스 중 하나를 자동으로 제공할 수 있다.

[0129] 전술된 것과 같이, 인증 서비스는, 클라이언트 장치(110)에 의해 사용자에 의해 선택된 사용자에 대한 인증 방식이 인식되고, 클라이언트 장치(110)로부터 중계 서버(120)로 인증 방식의 정보가 전송되면, 중계 서버(120)에서 인증 방식에 따라서 자동으로 이루어지는 분기에 의해 결정될 수 있다.

[0130] 또한, 인증 서비스는, 중계 서버(120)에 의해 선택된 인증 서비스의 정보가 모바일 단말(130)로 전송되면, 모바일 단말(130)의 모바일 프로그램에서 선택된 인증 서비스에 따라서 자동으로 이루어지는 분기에 의해 결정될 수 있다.

[0131] 단계(490)에서의 인증 서비스는, 클라이언트 장치(110), 중계 서버(120) 및 모바일 단말(130) 간의 상호 작용에 의해 이루어질 수 있다.

[0132] 다음으로, 중계 서버(120)는 클라이언트 장치(110)의 통신부(230)로 접속 완료 메시지를 전송할 수 있다. 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 중계 서버(120)로부터 접속 완료 메시지를 수신할 수 있다.

[0133] 접속 완료 메시지는 1) 모바일 단말(130)의 모바일 프로그램이 최신 버전인지 여부를 나타내는 정보 및 2) 모바일 단말(130)에 만료되지 않은 공인 인증서가 저장되어 있는 가를 나타내는 정보 등을 포함할 수 있다.

[0134] 다음으로, 접속 완료 메시지가 전송되면, 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 모바일 단말(130)의 통신부(330)로 클라이언트 장치(110)의 사용자에 대한 인증과 관련된 인증용 데이터 요청을 전송할 수 있다. 모바일 단말(130)의 모바일 프로그램은 통신부(330)를 통해 클라이언트 장치(110)의 프로그램으로부터 인증용 데이터 요청을 수신할 수 있다.

[0135] 선택된 인증 방식이 공인 인증서 전송 방식 또는 전자 서명 방식이면, 모바일 단말(130)의 모바일 프로그램은 통신부(330)를 통해 클라이언트 장치(110)의 프로그램으로 인증용 데이터를 전송할 수 있다. 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 모바일 단말(130)의 모바일 프로그램으로부터 인증용 데이터를 수신할 수 있다.

[0136] 선택된 인증 방식이 OTP 방식이면, 모바일 단말(130)의 모바일 프로그램은 모바일 단말(130)에 인증용 데이터를 출력할 수 있다. 모바일 단말(130) 및 클라이언트 장치(110)의 사용자는 출력된 OTP를 클라이언트 장치(110)에 입력할 수 있다. 클라이언트 장치(110)의 프로그램은 클라이언트 장치(110)의 사용자로부터 인증용 데이터를 수신할 수 있다.

[0137] 여기서, 인증용 데이터는 클라이언트 장치(110)의 선택된 인증 방식에 상응하는 데이터일 수 있으며, 모바일 단말(130)의 선택된 인증 서비스에 상응하는 데이터일 수 있다. 예를 들면, 선택된 인증 방식이 공인 인증서 전송 방식이면 인증용 데이터는 모바일 단말(130)에 저장된 공인 인증서일 수 있다. 선택된 인증 방식이 전자 서명 방식이면 인증용 데이터는 전자 서명 결과 값일 수 있다. 선택된 인증 방식이 OTP 방식이면 인증용 데이터는 모바일 단말(130)에 출력된 OTP일 수 있다.

[0138] 전술된 것과 같이, 중계 서버(120)에서 선택된 인증 방식에 따라 자동으로 분기가 이루어지고, 분기에 의해 결정된 인증 서비스 요청이 중계 서버(120)로부터 모바일 단말(130)의 모바일 프로그램으로 전송되면, 클라이언트 장치(110)의 프로그램은 인증 서비스에 관련하여 모바일 단말(130)의 모바일 프로그램으로부터 사용자에 대한 인증에 관련된 인증용 데이터를 수신할 수 있다.

[0139] 클라이언트 장치(110)의 프로그램은 인증용 데이터를 사용하여 클라이언트 장치(110)의 사용자에 대한 인증을 수행할 수 있다. 사용자에 대한 인증에 있어서, 제휴 서버(140) 및 인증 서버(160)와의 상호작용이 수행될 수 있다. 예를 들면, 클라이언트 장치(110)의 프로그램은 인증용 데이터를 인증 서버(160)로 전송할 수 있고, 인증 서버(160)로부터 인증용 데이터를 사용하여 수행된 사용자에 대한 인증의 결과를 수신할 수 있다.

[0140] 선택된 인증 방식 및 선택된 인증 서비스에 대하여 아래에서 도 6, 도 7 및 도 8을 참조하여 상세하게 설명된다.

[0141] 도 5는 일 예에 따른 모바일 프로그램 설치 단계를 나타내는 신호 흐름도이다.

[0142] 모바일 단말(130)에 모바일 프로그램이 설치되지 않은 경우, 모바일 프로그램 설치 단계(500)가 수행될 수 있다. 모바일 프로그램 설치 단계(500)는 도 4를 참조하여 전술된 단계(410)의 이전에 수행될 수 있으며, 또는 단계(470)의 이전에 수행될 수도 있다. 단계(500)는 후술될 모바일 OTP 발급 신청 알림 단계(505), 보안 채널 형성 단계(510), 모바일 프로그램 다운로드 메시지 수신 단계(515), 1차 발급 단계(520) 및 2차 발급 단계(530)을 포함할 수 있다.

[0143] 예를 들면, 클라이언트 장치(110) 및 모바일 단말(130)의 사용자가 제휴사에 모바일 OTP의 발급 신청을 함에 따라 모바일 프로그램 설치 단계(500)가 시작될 수 있다. 제휴사에 의해 사용자의 신원이 확인되면, 제휴 서버(140)는 통해 모바일 OTP의 생성을 위해 요구되는 작업을 수행할 수 있다.

[0144] 사용자가 모바일 OTP의 발급 신청을 할 경우, 사용자에 대한 본인 인증이 요구될 수 있다. 사용자에 대한 본인 인증을 위한 하나 이상의 서로 다른 인증 기술들 중 제휴 서비스의 이용 목적에 따라 선택된 인증 기술이 사용될 수 있다.

[0145] 하나 이상의 서로 다른 인증 기술들은 대면 거래 시의 인증 기술 및 비대면 거래 시 인증 기술로 분류될 수 있다. 예를 들면, 비대면 거래 시 공인 인증서, 아이핀(IPIN), 모바일 단말(130), 패스워드, 신용카드 및 신분증 등을 사용하는 인증 기술을 통해 본인 확인이 이루어질 수 있다.

[0146] 단계(500)에서, 통신부(330)는 모바일 프로그램을 다운로드하기 위한 주소의 정보를 수신할 수 있고, 프로세서(310)는 주소의 정보를 사용하여 모바일 프로그램을 다운로드 및 설치할 수 있다.

[0147] 단계(505)에서, 제휴 서버(140)는 모바일 OTP 발급 신청 알림 메시지를 중계 서버(120)로 전송할 수 있다.

[0148] 단계(510)에서, 도 4를 참조하여 전술된 보안 채널이 형성될 수 있다.

[0149] 예를 들면, 모바일 OTP의 발급의 신청이 비대면 거래로 이루어질 경우, 도 5를 참조하여 전술된 보안 채널이 사용될 수 있다. 모바일 OTP의 발급의 신청이 비대면 거래로 이루어질 경우, 모바일 프로그램 다운로드 메시지, 모바일 프로그램, 인증 모듈 및 OTP 생성 정보 중 적어도 하나가 보안 채널을 통해 전송될 수 있다.

[0150] 단계(515)에서, 중계 서버(120)는 모바일 프로그램 다운로드 메시지를 모바일 단말(130)의 통신부(330)로 전송할 수 있다. 모바일 프로그램 다운로드 메시지는 모바일 프로그램을 다운로드하기 위한 주소의 정보를 포함할 수 있다. 통신부(330)는 모바일 프로그램 다운로드 메시지를 통해 모바일 프로그램을 다운로드하기 위한 주소의 정보를 수신할 수 있다.

[0151] 모바일 프로그램 다운로드 메시지는 에스엠에스(Short Message Service; SMS) 메시지, 엠엠에스(Multimedia Messaging Service; MMS) 메시지 또는 푸쉬(push) 메시지일 수 있다.

[0152] 모바일 프로그램을 다운로드하기 위한 주소의 정보는 모바일 단말(130)의 사용자가 제휴사에 제휴사의 제휴 서비스에 사용되는 모바일 OTP의 발급을 신청함에 따라 중계 서버로부터 모바일 단말(130)의 통신부(330)로 전송될 수 있다.

[0153] 모바일 OTP의 발급은 1차 발급 및 2차 발급을 포함할 수 있다.

[0154] 1차 발급 단계(520)에서의 1차 발급은, 1) 앱 서버(180)로부터 모바일 OTP의 구동 모듈인 모바일 프로그램을 수신하고, 모바일 프로그램을 모바일 단말(130)에 설치하는 과정 및 2) 모바일 프로그램을 통해 모바일 단말(130)에게 이동통신 서비스를 제공하는 이동통신사의 이동통신 서버(150)로부터 모바일 OTP의 인증 모듈을 수신하고, 인증 모듈을 모바일 USIM(340)에 설치하는 과정을 포함할 수 있다.

[0155] 1차 발급 단계(520)는 단계들(521, 522, 523, 524, 525 및 526)을 포함할 수 있다.

[0156] 단계(521)에서, 통신부(330)는 모바일 프로그램 요청을 앱 서버(180)로 전송할 수 있다.

[0157] 단계(522)에서, 앱 서버(180)는 모바일 프로그램을 통신부(330)로 전송할 수 있다.

[0158] 단계(523)에서, 프로세서(310)는 모바일 단말(130)에 모바일 프로그램을 설치할 수 있다.

[0159] 모바일 프로그램이 설치되면, 모바일 프로그램에 의해 인증 모듈이 설치될 수 있다.

[0160] 단계(524)에서, 통신부(330)는, 모바일 프로그램의 요청에 따라, 인증 모듈 요청을 이동통신 서버(150)로 전송할 수 있다.

[0161] 단계(525)에서, 이동통신 서버(150)는 인증 모듈을 통신부(330)로 전송할 수 있다.

[0162] 단계(526)에서, 프로세서(310)는 모바일 단말(130)에 인증 모듈을 설치할 수 있다.

[0163] 또한, 프로세서(310) 또는 모바일 단말(130)의 모바일 프로그램은 인증 모듈을 모바일 USIM(340)에 설치할 수 있다.

[0164] 인증 모듈은 애플릿(applet)의 형태로 모바일 USIM(340)에 설치될 수 있다.

[0165] 2차 발급 단계(530)에서의 2차 발급은 발급은 발급 기관 서버(170)로부터 모바일 OTP의 OTP 생성 정보를 수신하고, OTP 생성 정보를 모바일 USIM(340)에 저장하는 과정을 포함할 수 있다.

[0166] 2차 발급 단계(530)는 단계들(531, 532 및 533)을 포함할 수 있다.

[0167] 단계(531)에서, 통신부(330)는 OTP 생성 정보 요청을 발급 기관 서버(170)로 전송할 수 있다.

[0168] OTP 생성 정보 요청은 모바일 단말(130)의 사용자에 대한 정보를 포함할 수 있다. 사용자에 대한 정보는 사용자의 식별자일 수 있다. 또한, 단계(531)에서의 OTP 생성 정보 요청은 모바일 단말(130)의 식별자를 포함할 수 있다.

[0169] 단계(532)에서, 발급 기관 서버(170)는 OTP 생성 정보를 모바일 단말(130)의 통신부(330)로 전송할 수 있다. 통신부(330)는 발급 기관 서버(170)로부터 OTP 생성 정보를 수신할 수 있다.

[0170] 단계(533)에서, 프로세서(310) 또는 모바일 단말(130)의 모바일 프로그램은 OTP 생성 정보를 모바일 USIM(340)에 설치할 수 있다.

[0171] 예를 들면, 제휴 서버(140) 및 발급 기관 서버(170)는 OTP 생성 정보와 관련된 정보를 공유할 수 있다. 제휴 서버(140)는 OTP 생성 정보의 발급을 위해 요구되는 정보를 발급 기관 서버(170)를 전송할 수 있다. 여기에서, OTP 생성 정보의 발급을 위해 요구되는 정보는 OTP 생성 정보와 쌍(pair)를 이루는 시리얼 넘버(Serial Number; S/N)일 수 있다.

[0172] 도 6은 일 예에 따른 OTP 서비스 방법의 신호 흐름도이다.

[0173] OTP 서비스 단계(600)는 도 4를 참조하여 전술된 단계(490)에 대응할 수 있다. 말하자면, OTP 서비스 단계(600)는 도 4를 참조하여 전술된 단계(460)에서 요청된 인증 서비스가 OTP 서비스일 경우에서의 단계(490)를 나타낼 수 있다.

[0174] 요청된 인증 서비스가 OTP 서비스일 경우 OTP 서비스 단계(600)가 수행될 수 있다. 또한, 단계(600)는 단계들(610, 620, 630, 640, 650, 660, 670 및 680)을 포함할 수 있다.

[0175] 단계(610)에서, 모바일 USIM(340)은 OTP를 생성할 수 있다.

[0176] 단계(620)에서, 모바일 단말(130)의 모바일 프로그램은 생성된 OTP를 출력할 수 있다.

[0177] OTP가 출력됨에 따라 모바일 단말(130)의 사용자는 OTP를 인식할 수 있고, 인식된 OTP를 클라이언트 장치(110)의 프로그램에 입력할 수 있다.

[0178] 단계(630)에서, 인식된 OTP가 클라이언트 장치(110)의 프로그램에 입력되면, 클라이언트 장치(110)의 프로그램은 입력된 OTP를 수신할 수 있다.

[0179] 단계(640)에서, 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 OTP를 제휴 서버(140)로 전송할 수 있다.

[0180] 단계(650)에서, 제휴 서버(140)는 OTP를 인증 서버(160)로 전송할 수 있다.

[0181] 단계(660)에서, 인증 서버(160)는 OTP에 대한 인증을 수행할 수 있다.

[0182] 인증 서버(160)는 모바일 단말(130)의 사용자에 대한 OTP 생성 정보를 이용하여 OTP를 생성할 수 있다. 여기에서, OTP 생성 정보의 전부 또는 일부는 OTP 생성 정보의 2차 발급과 관련하여 발급 기관 서버(170)로부터 인증 서버(160)로 제공된 정보일 수 있다. OTP의 생성에 있어서, 모바일 USIM(340)에 대해 설명된 내용이 인증 서버(160)에 대해서도 적용될 수 있다.

[0183] 인증 서버(160)는 인증 서버(160)가 생성한 OTP 및 제휴 서버(140)로부터 전송된 OTP를 비교함으로써 OTP에 대한 인증을 수행할 수 있다. 여기에서, 제휴 서버(140)로부터 전송된 OTP는 사용자가 클라이언트 장치(110)를 통해 제휴사의 사이트에 입력한 OTP일 수 있다. 제휴사의 사이트는 제휴 서버(140)에 의해 제공될 수 있다.

[0184] 예를 들면, 인증 서버(160)는 인증 서버(160)가 생성한 OTP 및 제휴 서버(140)로부터 전송된 OTP가 동일할 경우 제휴 서버(140)로부터 전송된 OTP가 인증된 것으로 결정할 수 있다. 인증 서버(160)는 인증 서버(160)가 생성한 OTP 및 제휴 서버(140)로부터 전송된 OTP가 동일하지 않을 경우 제휴 서버(140)로부터 전송된 OTP가 인증되지 않은 것으로 결정할 수 있다.

[0185] 단계(670)에서, 인증 서버(160)는 OTP에 대한 인증의 결과를 제휴 서버(140)로 전송할 수 있다. OTP에 대한 인증의 결과는 OTP가 인증된 것을 나타내거나, OTP가 인증되지 않은 것을 나타낼 수 있다.

[0186] 인증 서버(160)는 OTP에 대한 인증의 결과가 OTP가 인증된 것을 나타내는 경우 인증 성공과 관련된 소정의 작업을 처리할 수 있다. 또한, 인증 서버(160)는 OTP에 대한 인증의 결과가 OTP가 인증되지 않은 것을 나타내는 경우 인증 실패와 관련된 소정의 작업을 처리할 수 있다.

[0187] 단계(680)에서, 제휴 서버(140)는 OTP에 대한 인증의 결과를 클라이언트 장치(110)의 통신부(230)로 전송할 수 있다. 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 OTP에 대한 인증의 결과를 수신할 수 있고, OTP에 대한 인증의 결과를 출력할 수 있다.

[0188] 도 7은 일 예에 따른 전자 서명 서비스 방법의 신호 흐름도이다.

[0189] 전자 서명 서비스 단계(700)는 도 4를 참조하여 전술된 단계(490)에 대응할 수 있다. 말하자면, 전자 서명 서비스 단계(700)는 도 4를 참조하여 전술된 단계(460)에서 요청된 인증 서비스가 전자 서명 서비스일 경우에서의 단계(490)를 나타낼 수 있다.

[0190] 요청된 인증 서비스가 전자 서명 서비스일 경우 전자 서명 서비스 단계(700)가 수행될 수 있다. 또한, 단계(700)는 단계들(710, 720, 730, 740, 750, 760, 770 및 780)을 포함할 수 있다.

[0191] 단계(710)에서, 모바일 단말(130)의 모바일 프로그램은 보안 토큰 인증을 수행할 수 있다.

[0192] 단계(720)에서, 모바일 단말(130)의 모바일 프로그램은 통신부(330)를 통해 보안 토큰 인증 완료 알림을 클라이언트 장치(110)의 통신부(230)로 전송할 수 있다. 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 모바일 단말(130)로부터 보안 토큰 인증 완료 알림을 수신할 수 있다.

[0193] 단계(730)에서, 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 전자 서명 결과 값 요청을 모바일 단말(130)의 통신부(330)로 전송할 수 있다. 모바일 단말(130)의 모바일 프로그램은 통신부(330)를 통해 클라이언트 장치(110)로부터 전자 서명 결과 값 요청을 수신할 수 있다.

[0194] 전사 서명 결과 값 요청은 서명 데이터를 포함할 수 있다. 서명 데이터는 전자 서명의 대상일 수 있다.

[0195] 단계(740)에서, 모바일 단말(130)의 모바일 프로그램은 모바일 USIM(340)을 이용해서 전자 서명 결과 값을 생성할 수 있다.

[0196] 전자 서명 결과 값은 전술된 서명 데이터에 대하여 전자 서명이 적용된 결과일 수 있다.

[0197] 단계(750)에서, 모바일 단말(130)의 모바일 프로그램은 통신부(330)를 통해 전자 서명 결과 값을 클라이언트 장치(110)의 통신부(230)로 전송할 수 있다. 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 모바일 단말

(130)로부터 전자 서명 결과 값을 수신할 수 있다.

[0198] 단계(760)에서, 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 전자 서명 결과 값을 인증 서버(160)로 전송할 수 있다.

[0199] 단계(770)에서, 인증 서버(160)는 전자 서명 결과 값을 사용하여 클라이언트 장치(110)의 사용자에 대한 인증을 수행할 수 있다.

[0200] 단계(780)에서, 인증 서버(160)는 사용자에 대한 인증의 결과를 클라이언트 장치(110)의 통신부(230)로 전송할 수 있다. 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 사용자에 대한 인증의 결과를 수신할 수 있고, 사용자에 대한 인증의 결과를 출력할 수 있다.

[0201] 도 8은 일 예에 따른 공인 인증서 전송 서비스 방법의 신호 흐름도이다.

[0202] 공인 인증서 전송 서비스 단계(800)는 도 4를 참조하여 전술된 단계(490)에 대응할 수 있다. 말하자면, 공인 인증서 전송 서비스 단계(800)는 도 4를 참조하여 전술된 단계(460)에서 요청된 인증 서비스가 공인 인증서 전송 서비스일 경우에서의 단계(490)를 나타낼 수 있다.

[0203] 요청된 인증 서비스가 공인 인증서 전송 서비스일 경우 공인 인증서 전송 서비스 단계(800)가 수행될 수 있다. 또한, 단계(800)는 단계들(810, 820, 830, 835, 840, 850 및 860)을 포함할 수 있다.

[0204] 단계(810)에서, 클라이언트 장치(110) 및 모바일 단말(130) 간의 보안 채널이 형성될 수 있다.

[0205] 보안 채널의 형성을 위해, 클라이언트 장치(110)의 프로그램 및 모바일 단말(130)의 모바일 프로그램 간의 난수 검증이 수행될 수 있다. 난수 검증에서 사용되는 난수는 16자리일 수 있다.

[0206] 단계(820)에서, 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 공인 인증서 요청을 모바일 단말(130)의 통신부(330)로 전송할 수 있다. 모바일 단말(130)의 모바일 프로그램은 통신부(330)를 통해 클라이언트 장치(110)로부터 공인 인증서 요청을 수신할 수 있다. 이하에서, 공인 인증서는 인증서로 약술될 수 있다.

[0207] 단계(830)에서, 모바일 단말(130)의 모바일 프로그램은 통신부(330)를 통해 인증서를 클라이언트 장치(110)의 통신부(230)로 전송할 수 있다. 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 모바일 단말(130)로부터 인증서를 수신할 수 있다.

[0208] 모바일 단말(130)의 모바일 프로그램은 모바일 단말(130)의 메모리(320)에 저장된 클라이언트 장치(110)의 사용자의 인증서를 클라이언트 장치(110)의 통신부(230)로 전송할 수 있다. 인증서는 암호화된 인증서일 수 있다.

[0209] 단계(835)에서, 클라이언트 장치(110)의 프로그램은 인증서를 사용하여 전자 서명 결과 값을 생성할 수 있다.

[0210] 단계(840)에서, 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 전자 서명 결과 값을 인증 서버(160)로 전송할 수 있다.

[0211] 단계(850)에서, 인증 서버(160)는 전자 서명 값을 사용하여 클라이언트 장치(110)의 사용자에 대한 인증을 수행할 수 있다.

[0212] 단계(860)에서, 인증 서버(160)는 사용자에 대한 인증의 결과를 클라이언트 장치(110)의 통신부(230)로 전송할 수 있다. 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 사용자에 대한 인증의 결과를 수신할 수 있고, 사용자에 대한 인증의 결과를 출력할 수 있다.

[0213] 도 9는 일 예에 따른 클라이언트 단말 및 모바일 단말에 표시되는 인터페이스 화면을 나타낸다.

[0214] 도 9를 참조하면, 클라이언트 단말(110) 및 모바일 단말(130)은 OTP의 제공 및 OTP의 입력을 위한 인터페이스 화면을 제공할 수 있다.

[0215] OTP의 제공을 위한 화면은 모바일 단말(130)에서 제공되는 화면(910)을 포함할 수 있다. 또한, OTP의 입력을 위한 화면은 클라이언트 장치(110)에서 제공되는 화면(920)을 포함할 수 있다.

[0216] 특히, 화면(910)은 모바일 단말(130)의 모바일 프로그램에서 제공되는 화면일 수 있다. 또한, 화면(920)은 클라이언트 장치(110)의 프로그램에서 제공되는 화면일 수 있다.

[0217] 화면(910)을 통해 모바일 단말(130)의 사용자는 생성된 OTP를 인식할 수 있고, 생성된 OTP를 클라이언트 장치(110)에 입력해야 한다는 것을 알 수 있다. 화면(920)을 통해 클라이언트 장치(110)의 사용자는 생성된 OTP를 입력할 수 있다. 예를 들면, 도 9에서 도시된 것과 같이, OTP는 6자리일 수 있다.

[0218] 도 10은 일 예에 따른 클라이언트 장치 및 모바일 단말에 표시되는 다른 인터페이스 화면을 나타낸다.

[0219] 도 10을 참조하면, 클라이언트 장치(110) 및 모바일 단말(130)은 자동 분기 접속 인터페이스 화면을 제공할 수 있다.

[0220] 자동 분기 접속 인터페이스 화면은 클라이언트 장치(110)에서 제공되는 화면들(1011 및 1012) 및 모바일 단말(130)에서 제공되는 화면들(1031 및 1032)을 포함할 수 있다.

[0221] 특히, 화면(1011)은 클라이언트 장치(110)의 프로그램을 통해 제공되는 화면일 수 있다.

[0222] 예를 들면, 화면(1011)에서, 클라이언트 장치(110)의 사용자는 보안 토큰 메뉴 및 휴대폰 메뉴 중 어느 하나를 선택할 수 있다.

[0223] 화면(1011)에서, 사용자가 보안 토큰 메뉴를 선택하는 경우, 클라이언트 장치(110)의 프로그램은 인증 방식을 전자 서명 방식으로 결정할 수 있다. 사용자가 휴대폰 메뉴를 선택하는 경우, 클라이언트 장치(110)의 프로그램은 인증 방식을 공인 인증서 전송 방식으로 결정할 수 있다.

[0224] 화면(1012)에서, 사용자는 사용자가 이용하는 모바일 단말(130)의 식별자를 입력할 수 있다.

[0225] 화면(1012)에서 사용자가 모바일 단말(130)의 식별자를 입력한 경우, 클라이언트 장치(110)의 프로그램은 통신부(230)를 통해 클라이언트 장치(110)의 식별자를 중계 서버(120)로 전송할 수 있다.

[0226] 선택된 인증 방식이 전자 서명 방식인 경우, 모바일 단말(130)에서, 보안 토큰 인증을 수행하기 위한 화면(1031)이 제공될 수 있다. 선택된 인증 방식이 OTP 인증 방식인 경우, 모바일 단말(130)에서, 도 9를 참조하여 전술된 OTP 인증을 위한 화면(910)이 제공될 수 있다. 또한, 선택된 인증 방식이 공인 인증서 전송 방식인 경우, 도 12를 참조하여 후술될 공인 인증서 전송을 위한 화면(1211)이 제공될 수 있다.

[0227] 도 11은 일 예에 따른 클라이언트 장치 및 모바일 단말에 표시되는 또 다른 인터페이스 화면을 나타낸다.

[0228] 도 11을 참조하면, 클라이언트 장치(110) 및 모바일 단말(130)은 전자 서명 방식에 대한 인터페이스 화면을 제공할 수 있다.

[0229] 전자 서명 방식에 대한 인터페이스 화면은 클라이언트 장치(110)에서 제공되는 화면(1111) 및 모바일 단말(130)에서 제공되는 화면들(1131 및 1132)을 포함할 수 있다.

[0230] 특히, 화면(1111)은 클라이언트 장치(110)의 프로그램을 통해 제공되는 화면일 수 있다.

[0231] 화면(1111)에서, 클라이언트 장치(110)의 사용자는 보안 토큰 인증을 위한 보안 토큰 비밀번호를 입력할 수 있다.

[0232] 화면(1120)에서, 사용자는 사용자가 이용하는 모바일 단말(130)의 식별자를 입력할 수 있다.

[0233] 화면(1111) 및 화면(1120)을 통해, 사용자가 보안 토큰 비밀번호 및 모바일 단말(130)의 식별자를 입력하여 보안 토큰 인증이 완료되면, 클라이언트 장치(110)는 모바일 단말(130)로부터 전자 서명 결과 값을 수신할 수 있다. 또한, 클라이언트 장치(110)가 전자 서명 결과 값을 인증 서버(160)에 전송하고, 인증 서버(160)에 의해 사용자에 대한 인증이 수행 및 완료되면, 모바일 단말(130)의 모바일 프로그램은 화면(1132)과 같이 사용자에 대한 인증이 완료되었음을 나타내는 메시지를 출력할 수 있다.

[0234] 또한, 화면(1111)에서 및 화면(1120)을 통해, 클라이언트 장치(110)의 사용자가 보안 토큰 비밀번호 및 모바일 단말(130)의 식별자를 입력하고, 화면(1131)을 통해 전자 서명 과정의 진행 여부에 대하여 확인하면, 모바일 단말(130)은 전자 서명 결과 값을 클라이언트 장치(110)로 전송할 수 있다. 클라이언트 장치(110)의 프로그램은 사용자에 대한 인증을 진행할 것인지 여부를 확인하는 확인 메시지를 출력할 수 있다.

[0235] 또한, 화면(1111) 및 화면(1131)의 사이 또는 화면(1111) 및 화면(1130)의 사이에서는 사용자의 모바일 단말

(130)의 전화 번호를 수신하는 화면이 출력될 수 있다. 전화 번호를 수신하는 화면은 도 10을 참조하여 전술된 화면(1012)에 대응할 수 있다.

[0236] 도 12는 일 예에 따른 클라이언트 장치 및 모바일 단말에 표시되는 또 다른 인터페이스 화면을 나타낸다.

[0237] 도 12를 참조하면, 클라이언트 장치(110) 및 모바일 단말(130)은 공인 인증서 전송 방식에 대한 인터페이스 화면을 제공할 수 있다.

[0238] 공인 인증서 전송 방식에 대한 인터페이스 화면은 클라이언트 장치(110)에서 제공되는 화면들(1211 및 1212) 및 모바일 단말(130)에서 제공되는 화면들(1231 및 1232)을 포함할 수 있다.

[0239] 특히, 화면(1212)은 클라이언트 장치(110)의 프로그램을 통해 제공되는 인증서 전달에 대한 화면일 수 있다.

[0240] 화면(1211)에서, 사용자는 화면(1032)에 표시된 16자리 난수를 입력할 수 있다.

[0241] 화면(1211)에서, 사용자에 의해 16자리 난수가 입력되고, 입력된 16자리 난수를 사용하는 보안 채널의 형성이 완료되면, 클라이언트 장치(110)는 모바일 단말(130)로부터 인증서를 수신할 수 있다. 또한, 모바일 단말(130)은 인증서가 전송 중임을 나타내는 화면(1231) 및 인증서가 전송 완료되었음을 나타내는 화면(1232)을 출력할 수 있다.

[0242] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPA(field programmable array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0243] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0244] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 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. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

부호의 설명

[0245] 110: 클라이언트 장치

120: 중계 서버

130: 모바일 단말

140: 제휴 서버

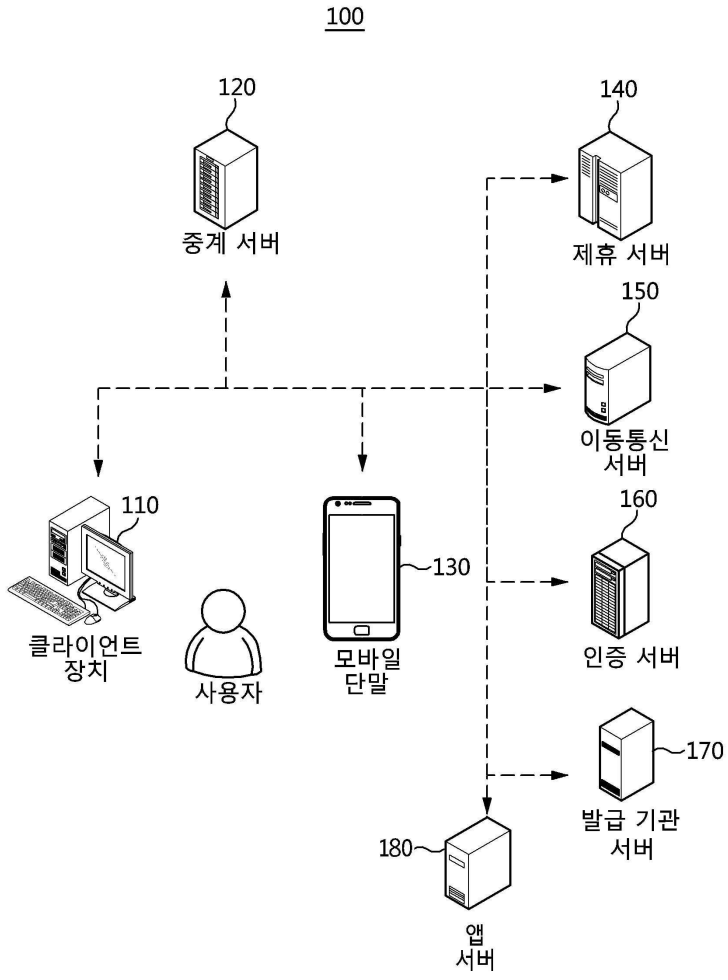
150: 이동통신 서버

160: 인증 서버

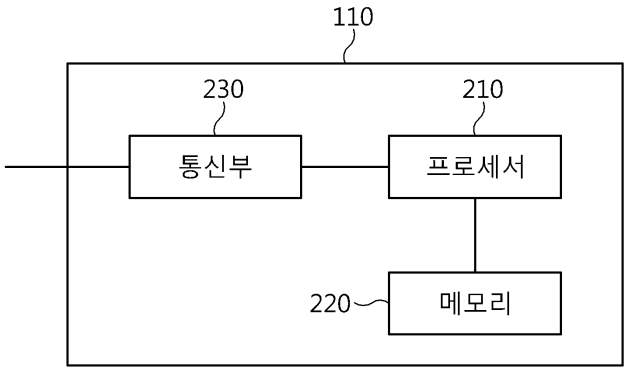
170: 발급 기관 서버

도면

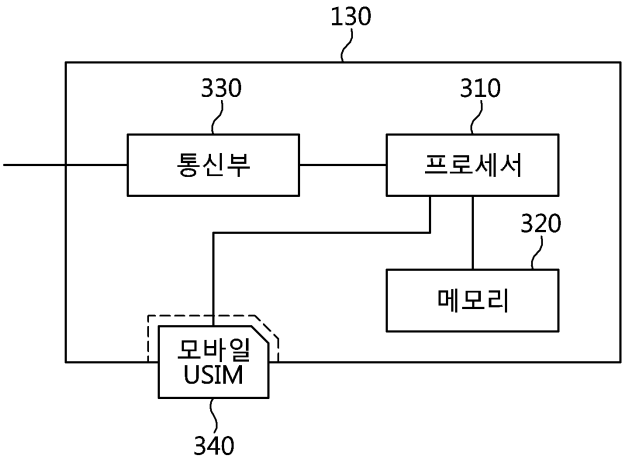
도면1



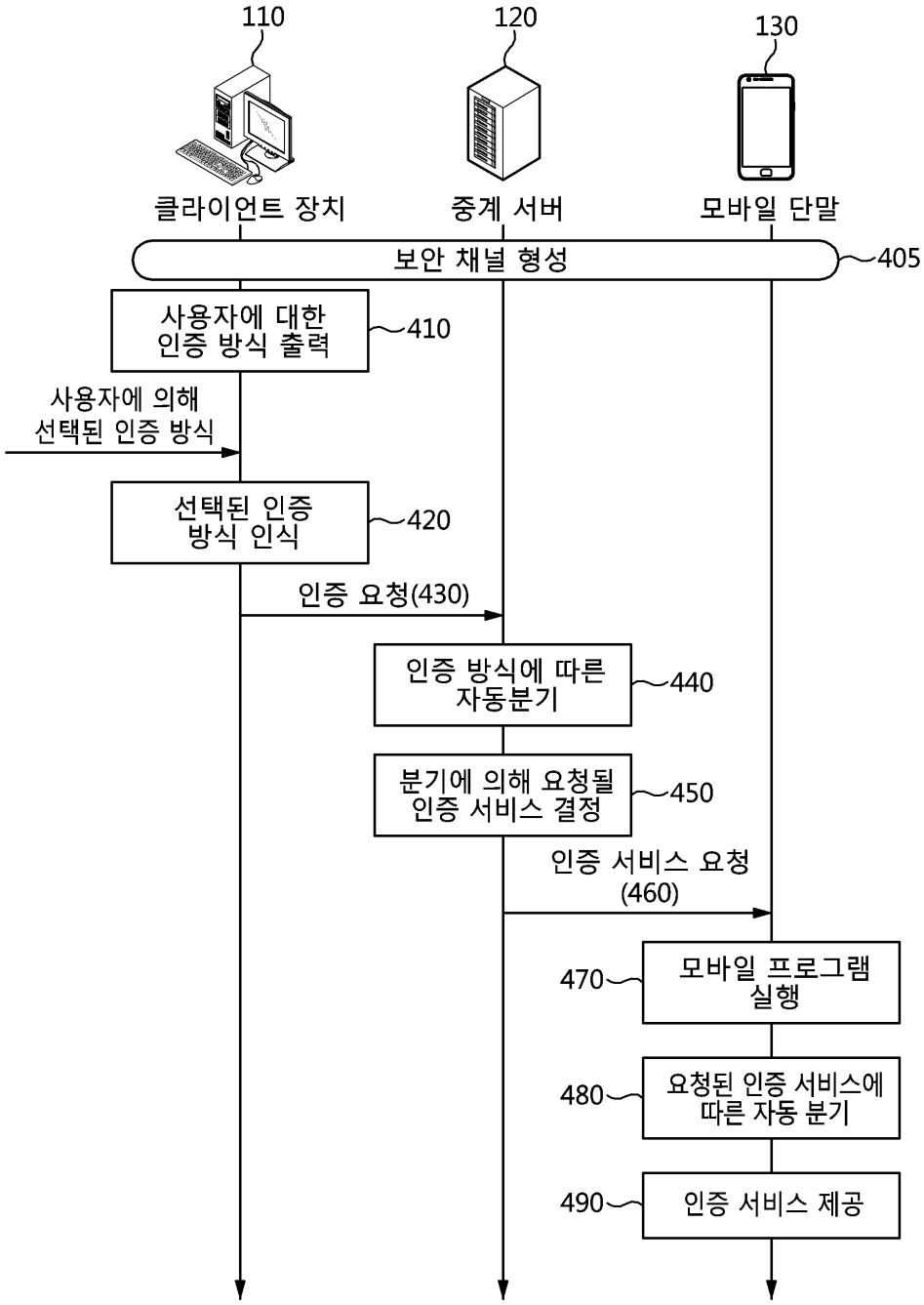
도면2


110
230
210
통신부
프로세서
220
메모리

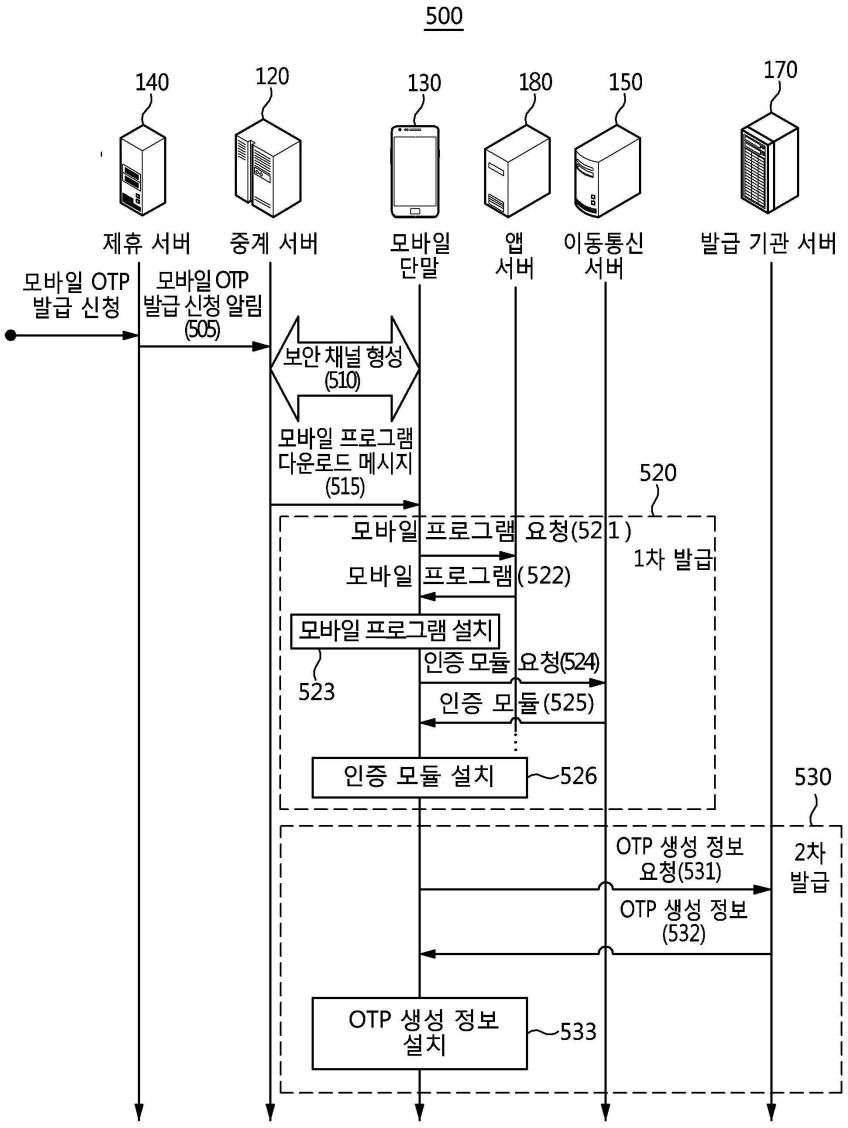
도면3


130
330
310
통신부
프로세서
320
메모리
모바일
USIM
340

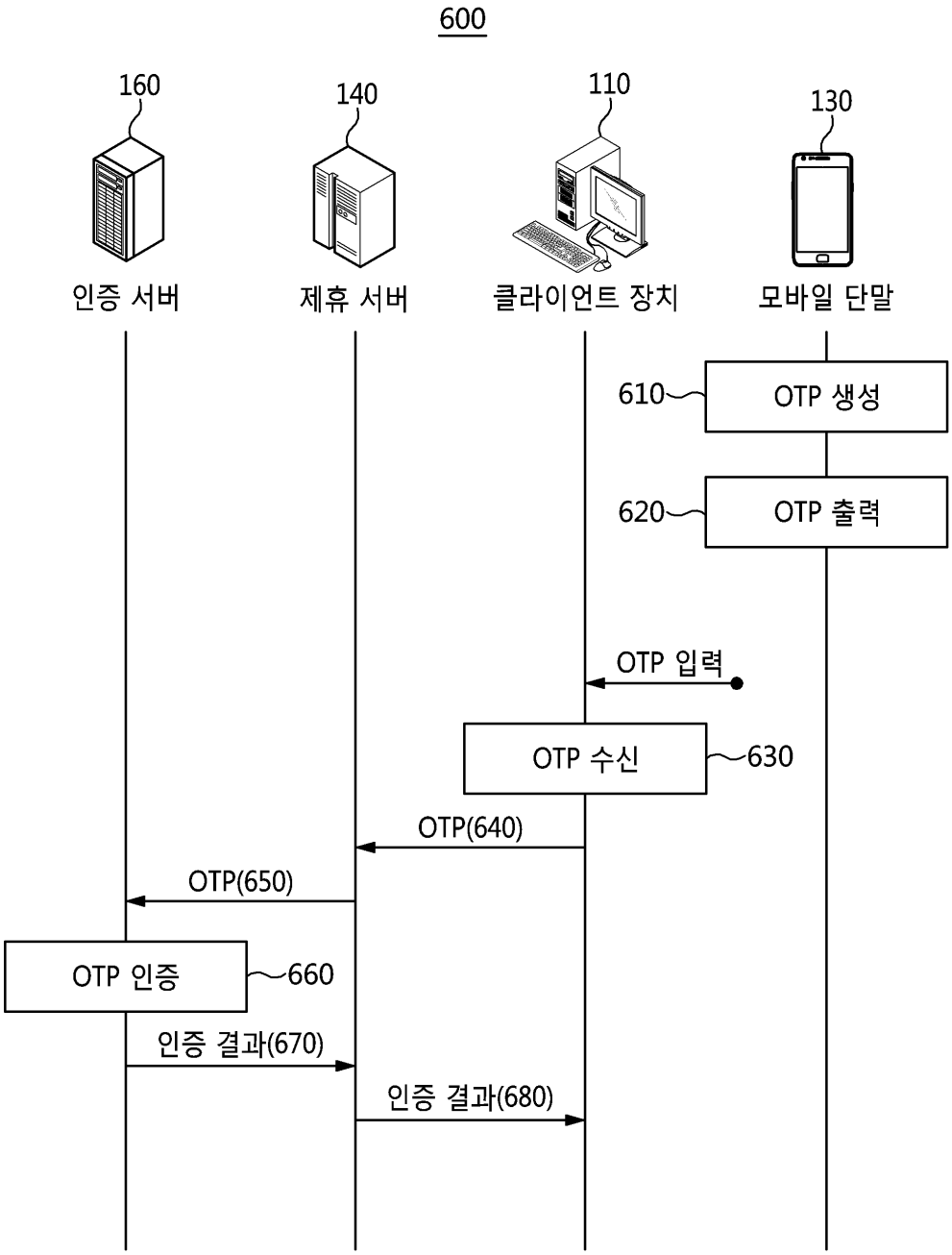
도면4


110
120
130
클라이언트 장치
중계 서버
모바일 단말
보안 채널 형성
405
사용자에 대한
인증 방식 출력
410
사용자에 의해
선택된 인증 방식
선택된 인증
방식 인식
420
인증 요청(430)
인증 방식에 따른
자동분기
440
분기에 의해 요청될
인증 서비스 결정
450
인증 서비스 요청
(460)
470
모바일 프로그램
실행
480
요청된 인증 서비스에
따른 자동 분기
490
인증 서비스 제공

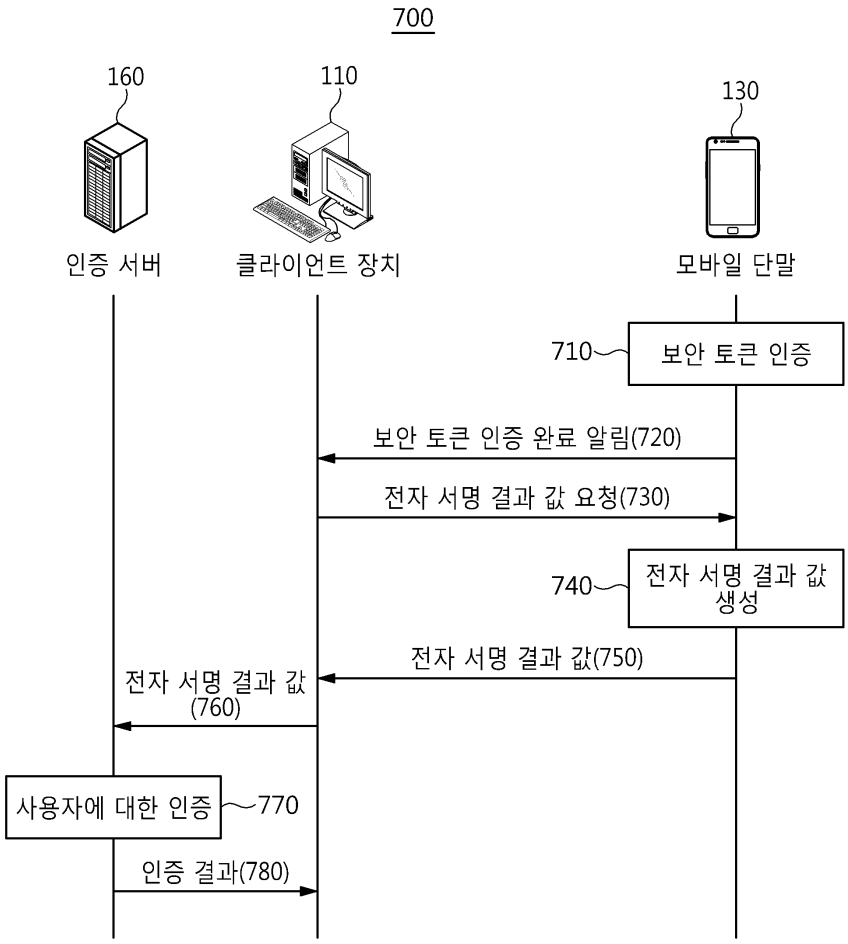
도면5


500
140
120
130
180
150
170
제휴 서버
중계 서버
모바일 단말
앱 서버
이동통신 서버
발급 기관 서버
모바일 OTP 발급 신청
모바일 OTP 발급 신청 알림 (505)
보안 채널 형성 (510)
모바일 프로그램 다운로드 메시지 (515)
520
모바일 프로그램 요청(521)
1차 발급
모바일 프로그램(522)
모바일 프로그램 설치
523
인증 모듈 요청(524)
인증 모듈(525)
인증 모듈 설치
526
530
OTP 생성 정보 요청(531)
2차 발급
OTP 생성 정보 (532)
OTP 생성 정보 설치
533

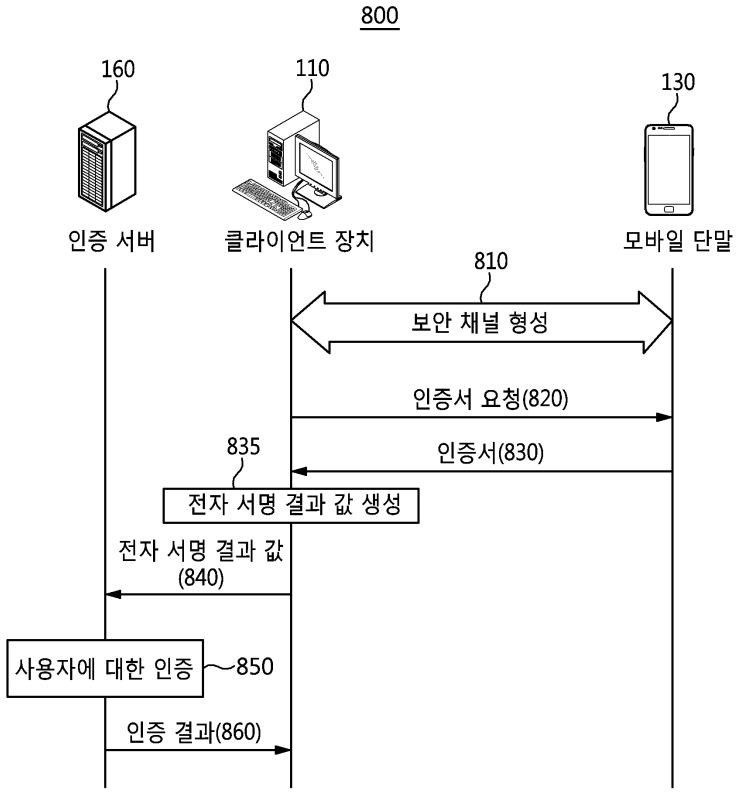
도면6


600
160
140
110
130
인증 서버
제휴 서버
클라이언트 장치
모바일 단말
610
OTP 생성
620
OTP 출력
OTP 입력
OTP 수신
630
OTP(640)
OTP(650)
OTP 인증
660
인증 결과(670)
인증 결과(680)

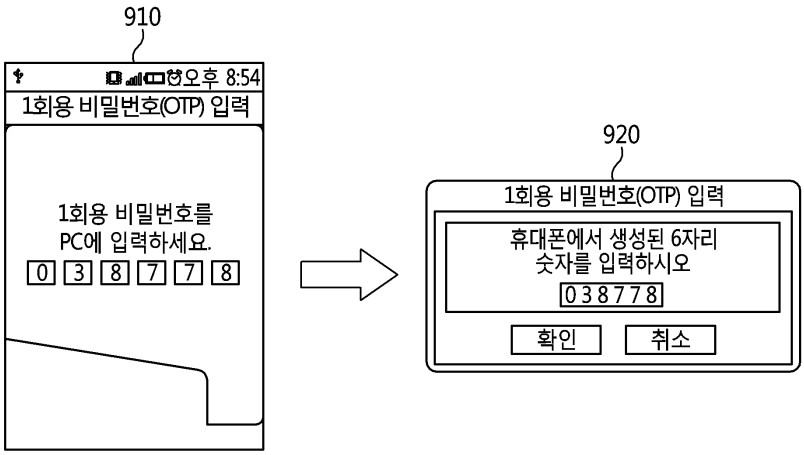
도면7


700
160
110
130
인증 서버
클라이언트 장치
모바일 단말
710
보안 토큰 인증
보안 토큰 인증 완료 알림(720)
전자 서명 결과 값 요청(730)
740
전자 서명 결과 값 생성
전자 서명 결과 값(750)
전자 서명 결과 값 (760)
사용자에 대한 인증
770
인증 결과(780)

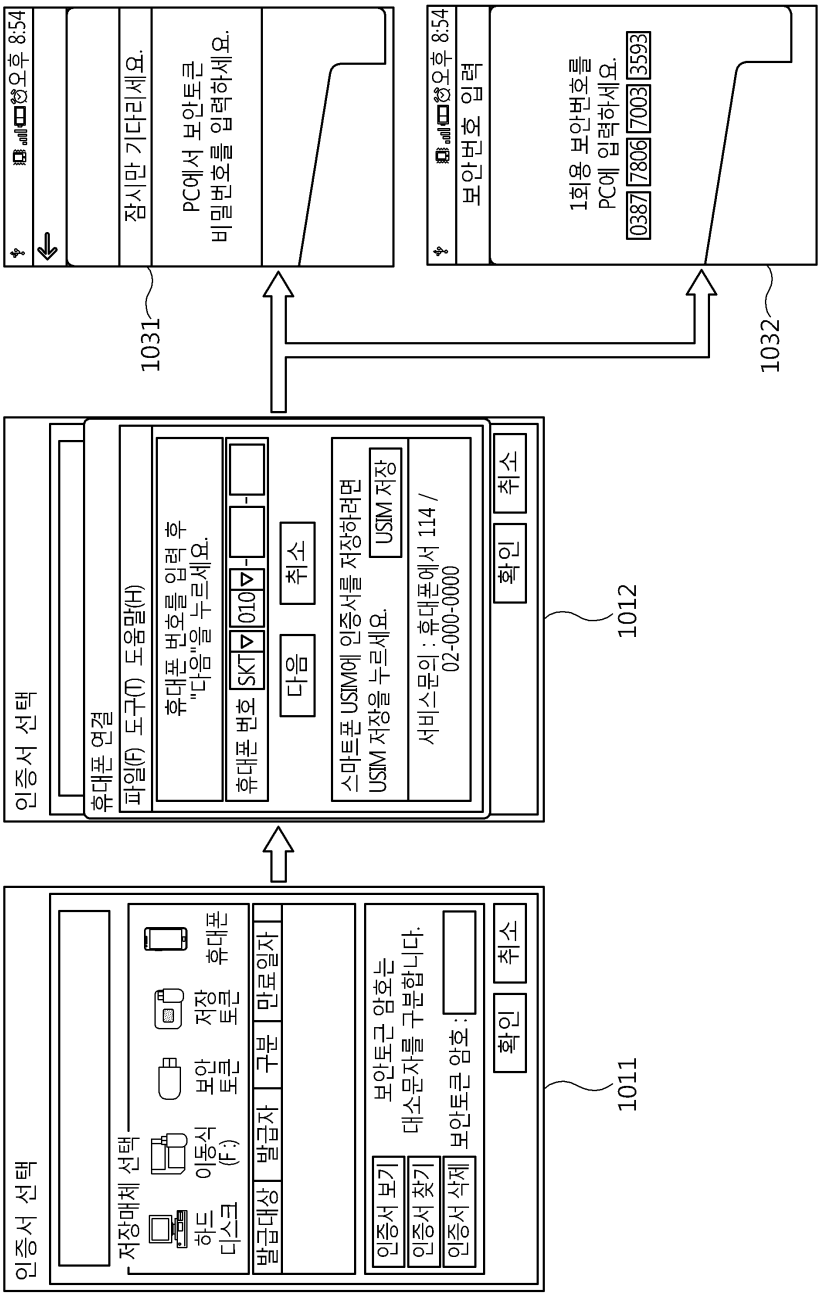
도면8


800
160
110
130
인증 서버
클라이언트 장치
모바일 단말
810
보안 채널 형성
인증서 요청(820)
835
인증서(830)
전자 서명 결과 값 생성
전자 서명 결과 값
(840)
사용자에 대한 인증
850
인증 결과(860)

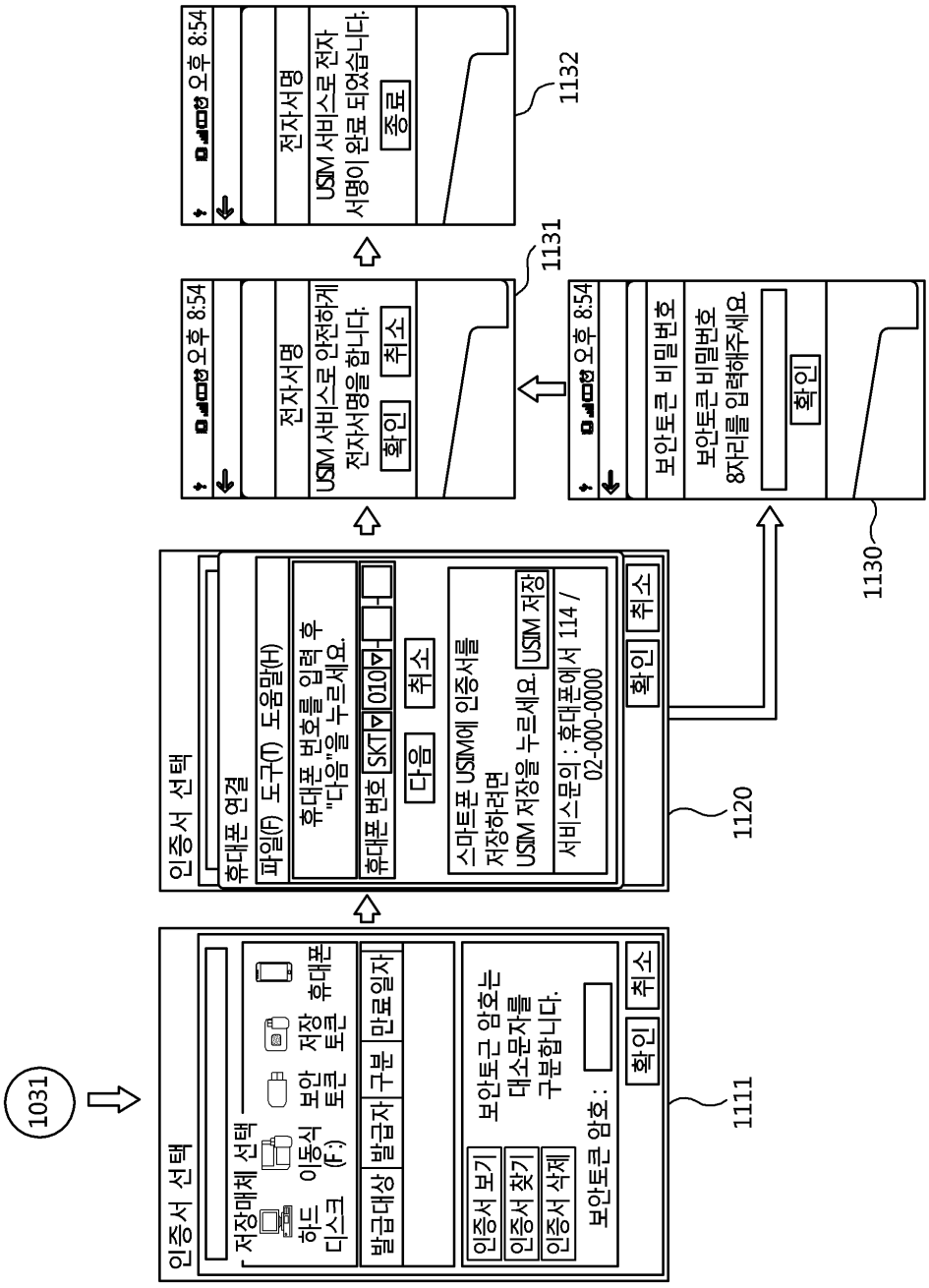
도면9


910
오후 8:54
1회용 비밀번호(OTP) 입력
1회용 비밀번호를
PC에 입력하세요.
0 3 8 7 7 8
920
1회용 비밀번호(OTP) 입력
휴대폰에서 생성된 6자리
숫자를 입력하시오
038778
확인
취소

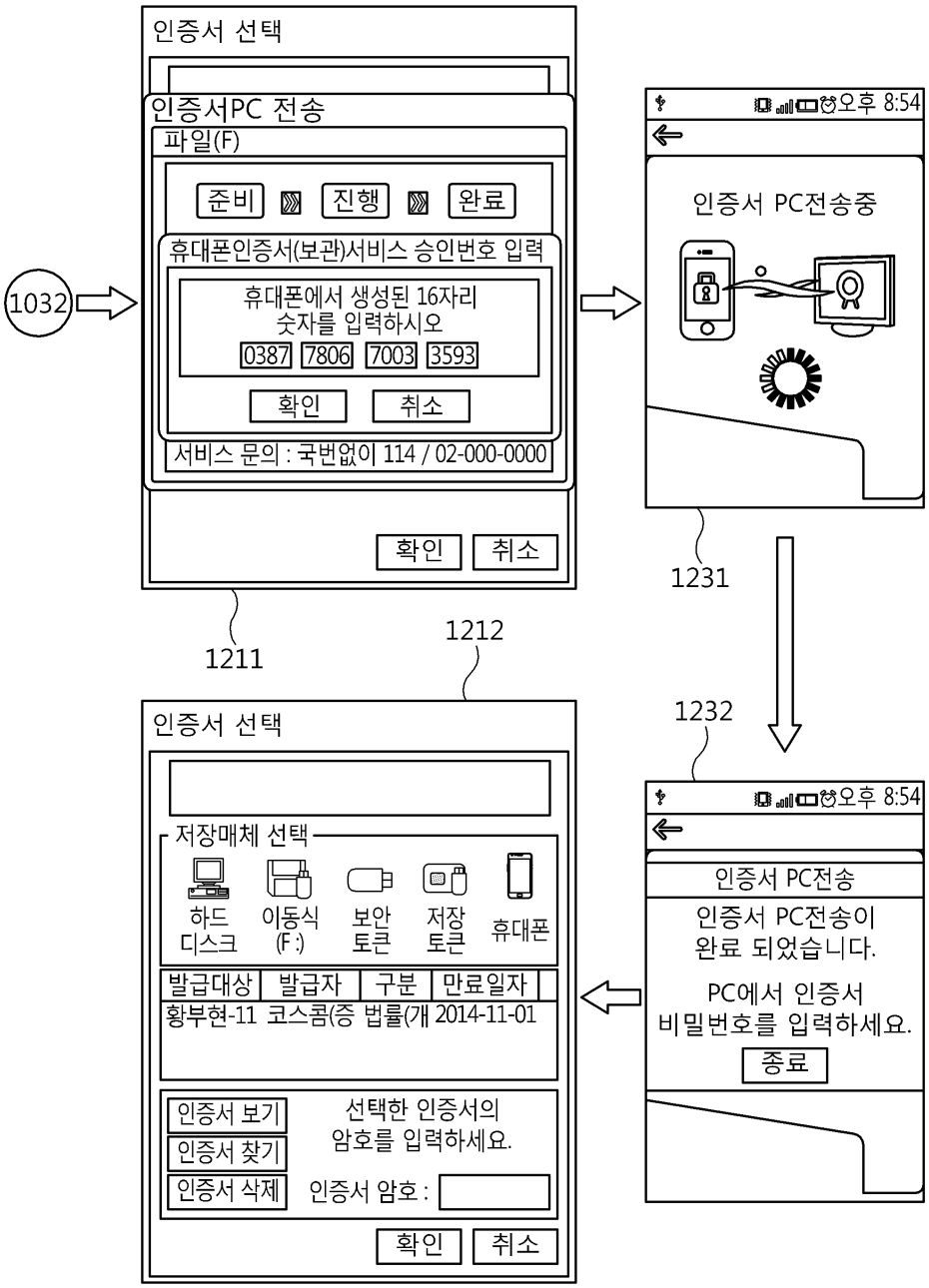
도면10


인증서 선택
저장매체 선택
하드 디스크
이동식 (F:)
보안 토큰
저장 토큰
휴대폰
발급대상
발급자
구분
만료일자
인증서 보기
인증서 찾기
인증서 삭제
보안토근 암호는
대소문자를 구분합니다.
보안토큰 암호 :
확인
취소
1011
인증서 선택
휴대폰 연결
파일(F) 도구(T) 도움말(H)
휴대폰 번호를 입력 후
"다음"을 누르세요.
휴대폰 번호
SKT
010
다음
취소
스마트폰 USIM에 인증서를 저장하려면
USIM 저장을 누르세요.
USIM 저장
서비스문의 : 휴대폰에서 114 /
02-000-0000
확인
취소
1012
오후 8:54
잠시만 기다리세요.
PC에서 보안토큰
비밀번호를 입력하세요.
1031
오후 8:54
보안번호 입력
1회용 보안번호를
PC에 입력하세요.
0387 7806 7003 3593
1032

도면11


1031
인증서 선택
저장매체 선택
하드 디스크
이동식 보안 토큰 (F:)
휴대폰 저장 토큰
발급대상
발급자
구분
만료일자
인증서 보기
인증서 찾기
인증서 삭제
보안토큰 암호는 대소문자를 구분합니다.
보안토큰 암호 :
확인
취소
1111
인증서 선택
휴대폰 연결
파일(F) 도구(T) 도움말(H)
휴대폰 번호를 입력 후 "다음"을 누르세요.
휴대폰 번호
SKT
010
다음
취소
스마트폰 USIM에 인증서를 저장하려면 USIM 저장을 누르세요.
USIM 저장
서비스문의 : 휴대폰에서 114 / 02-000-0000
확인
취소
1120
보안토큰 비밀번호
보안토큰 비밀번호 8자리를 입력해주세요.
확인
1130
오후 8:54
전자서명
USIM 서비스로 안전하게 전자서명을 합니다.
확인
취소
1131
전자서명
USIM 서비스로 전자서명이 완료 되었습니다.
종료
1132

도면12


인증서 선택
인증서PC 전송
파일(F)
준비
진행
완료
휴대폰인증서(보관)서비스 승인번호 입력
휴대폰에서 생성된 16자리
숫자를 입력하시오
0387 7806 7003 3593
확인
취소
서비스 문의 : 국번없이 114 / 02-000-0000
확인
취소
1032
1211
1212
오후 8:54
인증서 PC전송중
1231
1232
인증서 선택
저장매체 선택
하드 디스크
이동식 (F:)
보안 토큰
저장 토큰
휴대폰
발급대상
발급자
구분
만료일자
황부현-11 코스콤(증 법률(개 2014-11-01
인증서 보기
인증서 찾기
인증서 삭제
선택한 인증서의
암호를 입력하세요.
인증서 암호 :
확인
취소
오후 8:54
인증서 PC전송
인증서 PC전송이
완료 되었습니다.
PC에서 인증서
비밀번호를 입력하세요.
종료