(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0033541
(43) 공개일자 2008년04월16일

(51) Int. Cl.
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
G06F 15/16 (2006.01) *G06F 21/00* (2006.01)
(21) 출원번호 10-2008-7005884
(22) 출원일자 2008년03월11일
심사청구일자 없음
번역문제출일자 2008년03월11일
(86) 국제출원번호 PCT/IL2006/000928
국제출원일자 2006년08월10일
(87) 국제공개번호 WO 2007/017878
국제공개일자 2007년02월15일
(30) 우선권주장
60/707,203 2005년08월11일 미국(US)

(71) 출원인
샌디스크 아이엘 엘티디
이스라엘 44425 크파 사바 아틸 예다 스트리트 7
(72) 발명자
바이치코브, 에얄
이스라엘 호드 하샤론 45204 샤롬 알리첼 13
(74) 대리인
박종혁, 김정욱, 정삼영, 송봉식

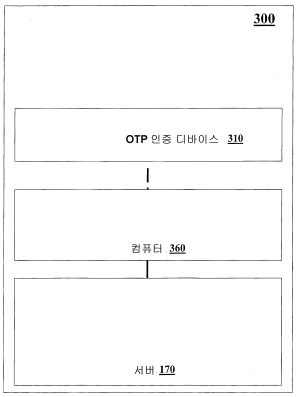
전체 청구항 수 : 총 36 항

(54) 확장된 일회용 암호 방법 및 장치

(57) 요 약

인터넷을 통해 서버와의 세션을 수행하는 클라이언트 워크스테이션의 인증을 보조하는 OTP 토큰이 개시된다. 적어도 부분적으로 서버를 식별하는 정보가 상기 OTP 토큰 및/또는 클라이언트 워크스테이션에 제공되고, 상기의 식별 정보를 이용하여, 상기 서버가 적법한 서버인지를 판정하는 것이 이루어진다. 상기 판정에 따라, OTP 토큰으로부터 클라이언트 워크스테이션으로 세션 OTP를 지시하는 데이터를 전송할지 여부를 결정한다. 일부 실시예에서, 상기 식별 정보가 적법한 서버임을 지시한다면, 상기 세션 OTP를 지시하는 데이터는 상기 OTP 토큰으로부터 클라이언트 워크스테이션으로 전송되고, 그렇지 않으면, 상기 세션 OTP를 지시하는 데이터는 상기 클라이언트 워크스테이션으로부터 보류된다. 세션 OTP를 지시하는 데이터는, 다양한 실시예에서, 사용자 인증 데이터로부터 도출된 멀티-팩터 인증 데이터, 또는 사용자 인증 데이터에 독립적인 세션 OTP 데이터 중 어느 하나를 포함한다.

대표도 - 도3A



특허청구의 범위

청구항 1

서버, 광역 네트워크를 통해 상기 서버와 통신하는 클라이언트 워크스테이션, 및 디바이스 인터페이스를 통해 상기 클라이언트 워크스테이션과 인터페이싱하는 OTP 토큰을 구비하는 시스템에서, 세션 OTP 전송을 핸들링하는 방법에 있어서,

(a) 적어도 부분적으로 상기 서버를 식별하는 정보를 서버로부터 수신하는 단계;

(b) 상기 식별 정보가 적법한 서버를 지시하는 지를 판정하는 단계; 및

(c) 상기 판정에 따라,

i) OTP 토큰으로부터 내부적으로 생성된 세션 OTP를 지시하는 데이터를 전송하는 단계, 및

ii) 상기 전송을 억제하는 단계;로

구성되는 그룹으로부터 선택된 하나의 동작을 수행하도록 결정하는 단계;를 포함하는 것을 특징으로하는 세션 OTP 전송을 핸들링하는 방법.

청구항 2

제 1 항에 있어서,

d) 상기 결정이 포지티브한 결정인 경우에만, 상기 OTP 토큰으로부터 상기 세션 OTP를 지시하는 데이터를 전송하는 단계를 더 포함하는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 3

제 2 항에 있어서,

상기 전송 단계는, 상기 결정이 포지티브한 경우에만, 상기 인터페이스를 통해 상기 OTP 토큰으로부터 상기 클라이언트 워크스테이션으로 상기 지시 데이터의 디바이스 상호간의 데이터 전송을 유효화하는 단계를 포함하는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 4

제 2 항에 있어서,

상기 전송 단계는, 상기 결정이 포지티브한 경우에만, 상기 OTP 토큰의 디스플레이 스크린 상에 상기 세션 OTP를 지시하는 데이터를 표시하는 단계를 포함하는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 5

제 1 항에 있어서,

상기 세션 OTP를 지시하는 데이터는 사용자 인증 데이터로부터 도출된 멀티-팩터 인증 데이터인 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 6

제 1 항에 있어서,

상기 세션 OTP를 지시하는 데이터는 사용자 인증 데이터에 독립적인 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 7

제 1 항에 있어서,

d) 상기 결정이 네거티브한 결정이라면, 상기 OTP 토큰에 의해 상기 세션 OTP를 생성하는 것을 방지하는 단계를 더 포함하는 것을 특징으로하는 세션 OTP 전송을 핸들링하는 방법.

청구항 8

제 1 항에 있어서,

d) 상기 결정이 네거티브한 결정이라면,

i) 내부적으로 상기 OTP 토큰내에서 상기 세션 OTP를 생성하는 단계; 및

ii) 상기 세션 OTP가 상기 OTP 토큰내에 남아있는 상태를 유지하는 단계를 더 포함하는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 9

제 1 항에 있어서,

(d) 상기 수신단계 전에, 상기 OTP 토큰 내의 내장된 보안 브라우저를 사용하는 단계, 및 상기 OTP 토큰과 상기 서버 사이에서 보안 세션을 오픈하는 단계를 더 포함하는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 10

제 9 항에 있어서,

(e) 상기 세션의 오픈하는 단계 후에, 상기 OTP 토큰으로부터 클라이언트 워크스테이션으로 상기 세션의 클라이언트 엔드를 전송하는 단계를 더 포함하고,

여기서 상기 수신 및 판정 단계 중 적어도 하나는 상기 클라이언트 워크스테이션에서 수행되는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 11

제 9 항에 있어서,

상기 세션의 클라이언트 엔드는 상기 식별 정보가 상기 서버로부터 상기 OTP 토큰에 의해 수신된 때에, 상기 내장된 브라우저에 유지되는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 12

제 1 항에 있어서,

상기 수신단계는 상기 서버와 상기 OTP 토큰 사이의 통신 링크를 통해 상기 OTP 토큰에 의해 수행되는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 13

제 1 항에 있어서,

상기 판정단계는 상기 OTP 토큰 내에서 수행되는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 14

제 1 항에 있어서,

상기 판정 단계는 상기 OTP 토큰내에 상주하는 데이터베이스로의 쿼리를 유효화하는 단계를 포함하는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 15

제 14 항에 있어서,

상기 쿼리는 상기 클라이언트 워크스테이션으로부터 유효화되는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 16

제 14 항에 있어서,

상기 판정 단계는 상기 OTP 토큰 내에서 수행되고, 상기 쿼리는 상기 OTP 토큰 내에 상주하는 데이터 베이스 클라이언트 코드에 의해 유효화되는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 17

제 14 항에 있어서,

상기 데이터베이스는 불변의 데이터베이스인 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 18

제 14 항에 있어서,

상기 데이터베이스는 수용가능한 URL의 미리 정해진 리스트, 수용가능한 IP 어드레스의 미리정해진 리스트, 및 공인인증 필드에 대한 수용가능한 값의 미리정해진 리스트를 포함하는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 19

제 1 항에 있어서,

상기 판정은 수신된 하나의 통신의 프로토콜 데이터, 수신 통신에서 전송된 공인인증 데이터, URL 데이터 및 IP 어드레스 데이터 중 적어도 하나에 따라 수행되는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 20

제 19 항에 있어서,

상기 판정 단계는 상기 서버로부터 수신된 공인인증의 일부 속성에 따라서만 수행되는 것을 특징으로 하는 세션 OTP 전송을 핸들링하는 방법.

청구항 21

광역 네트워크를 통해 서버와 통신하는 클라이언트 워크스테이션으로 사용하는 OTP 토큰에 있어서,

(a) 적어도 부분적으로 서버를 식별하는 정보를 포함하는 데이터를 클라이언트 워크스테이션으로부터 수신하는 디바이스 포트;

(b) 상기 정보가 적법한 서버를 지시하는 지를 판정하는 서버 적법성 엔진;

(c) 세션 OTP를 생성하도록 동작하는 OTP 생성기; 및

(d) 상기 판정의 결과에 따라,

ⅰ) OTP 토큰으로부터 상기 세션 OTP를 지시하는 데이터를 전송하는 단계, 및

ⅱ) 상기 전송을 억제하는 단계;

로 구성되는 그룹으로부터 선택된 하나의 동작을 수행하는 것을 결정하도록 동작하는 OTP 전송 결정 엔진;을 포함하는 것을 특징으로 하는 OTP 토큰.

청구항 22

제 21 항에 있어서,

e) 상기 결정에 따라 상기 OTP 토큰으로부터 세션 OTP를 지시하는 데이터를 전송하는 OTP 전송기를 더 포함하는 것을 특징으로 하는 OTP 토큰.

청구항 23

제 22 항에 있어서,

상기 OTP 전송기는, 상기 결정이 포지티브한 결정인 경우에만, 상기 데이터 포트를 통해 상기 세션 OTP를 지시하는 데이터의 디바이스 상호간의 데이터 전송을 유효화하도록 동작하는 것을 특징으로 하는 OTP 토큰.

청구항 24

제 22 항에 있어서,

(f) 상기 결정이 포지티브한 결정인 경우에만, 상기 OTP 전송기가 상기 데이터 디스플레이로 세션 OTP를 지시하는 데이터를 전송하도록 동작하는, 데이터 디스플레이를 더 포함하는 것을 특징으로 하는 OTP 토큰.

청구항 25

제 21 항에 있어서,

(e) 상기 내장된 브라우저가 상기 OTP 토큰과 상기 서버 사이의 보안 세션을 오픈하도록 동작하는, 상기 OTP 토큰 내에 설치된 내장된 보안 브라우저를 더 포함하는 것을 특징으로 하는 OTP 토큰.

청구항 26

제 25 항에 있어서,

상기 내장된 보안 브라우저는, 상기 보안 세션동안, 상기 식별 정보를 수신하도록 동작하는 것을 특징으로 하는 OTP 토큰.

청구항 27

제 21 항에 있어서, 상기 서버 적법성 엔진은,

(d) 상기 서버 적법성 엔진이 상기 데이터베이스의 컨텐츠에 따라 상기 판정을 수행하도록 동작하는, 미리정해진 데이터의 데이터베이스를 포함하는 것을 특징으로 하는 OTP 토큰.

청구항 28

제 27 항에 있어서,

상기 데이터베이스는 불변의 데이터베이스인 것을 특징으로 하는 OTP 토큰.

청구항 29

제 27 항에 있어서,

상기 데이터베이스는 수용가능한 URL의 미리정해진 리스트, 수용가능한 IP 어드레스의 미리정해진 리스트, 및 공인인증 필드의 수용가능한 값의 미리정해진 리스트를 포함하는 것을 특징으로 하는 OTP 토큰.

청구항 30

제 21 항에 있어서,

상기 서버 적법성 엔진은 상기 서버로부터의 통신에서 전송된 서버 공인인증 데이터로부터의 통신의 프로토콜 데이터, IP 어드레스 데이터, URL 데이터 중 적어도 하나에 따라 상기 판정을 수행하도록 동작하는 것을 특징으로 하는 OTP 토큰.

청구항 31

제 30 항에 있어서,

상기 서버 적법성 엔진은 상기 서버로부터 수신된 공인인증의 일부 속성에 따라서만 판정을 수행하도록 동작하는 것을 특징으로 하는 OTP 토큰.

청구항 32

제 21 항에 있어서,

상기 OTP 생성기는 사용자 인증 데이터에 따라 상기 세션 OTP를 생성하도록 동작하고, 그에 의해 멀티-팩터 인증 데이터로서 상기 세션 OTP를 생성하는 것을 특징으로 하는 OTP 토큰.

청구항 33

제 33 항에 있어서,

(e) 상기 사용자 인증 데이터를 인증하는 사용자 식별 모듈을 더 포함하는 것을 특징으로 하는 OTP 토큰.

청구항 34

제 33 항에 있어서,

상기 OTP 전송 결정 엔진은 상기 사용자 인증 데이터의 인증의 결과에 따라 상기 결정을 유효화하도록 동작하는 것을 특징으로 하는 OTP 토큰.

청구항 35

세션 OTP 데이터의 전송을 핸들링하는 시스템에 있어서,

a) 광역 네트워크를 통해 서버와 통신하는 클라이언트 워크스테이션;

b) 상기 클라이언트 워크스테이션과 인터페이싱하고,

ⅰ) 상기 클라이언트 워크스테이션과 인터페이싱하는 디바이스 포트, 및

ii) 세션 OTP를 생성하도록 동작하는 OTP 생성기를 구비하는 OTP 토큰;을 포함하고, 상기 OTP 토큰과 상기 클라이언트 워크스테이션 중 적어도 하나는 상기 서버를 식별하는 정보를 수신하도록 동작하는 시스템으로서, 상기 시스템은 또한,

c) 상기 정보가 적법한 서버를 지시하는지 여부를 판정하며, 상기 OTP 토큰 및 클라이언트 워크스테이션 중 적어도 하나에 적어도 부분적으로 상주하는 서버 적법성 엔진;

d) 상기 판정의 결과에 따라,

ⅰ) 상기 OTP 토큰으로부터 상기 세션 OTP를 지시하는 데이터를 전송하는 단계; 및

ii) 상기 전송을 억제하는 단계로

구성된 그룹으로부터 선택된 하나의 동작을 수행하는 것을 결정하도록 동작하는 OTP 전송 결정 엔진;을 더 포함하고,

상기 OTP 전송 결정 엔진은 상기 OTP 토큰과 상기 클라이언트 워크스테이션 중 적어도 하나에 적어도 부분적으로 상주하는 것을 특징으로 하는 시스템.

청구항 36

컴퓨터 판독가능 저장 매체에 내장된 컴퓨터 판독가능 코드를 가진 컴퓨터 판독가능 저장 매체로서, 상기 컴퓨터 판독가능 코드는,

a) 광역 네트워크를 통해 서버와 통신하는 클라이언트 워크스테이션과 상기 서버와 인터페이싱하는 OTP 토큰 중 적어도 하나에 의해 상기 서버를 적어도 부분적으로 식별하는 정보를 수신하고;

b) 상기 식별 정보가 적법한 서버를 지시하는지를 판정하고;

c) 상기 판정에 따라,

ⅰ) 상기 OTP 토큰으로부터 내부적으로 생성된 세션 OTP를 지시하는 데이터를 전송하는 단계, 및

ii) 상기 전송을 억제하는 단계로

구성되는 그룹으로부터 선택된 하나의 동작을 수행하는 것을 결정하는; 명령을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 코드를 가진 컴퓨터 판독가능 저장 매체.

명 세 서

기 술 분 야

<1> 본 발명은 인터넷 인증에 관한 것으로, 보다 특정하게는 일회용 암호를 사용하는 인증에 관한 것이다.

배 경 기 술

<2> 많은 인터넷 사용자들은 자신들의 서비스 공급자, 회사 네트워크, 유료 서비스, 또는 자신들의 은행 또는 신용 계좌로의 특정한 액세스 권한을 가진다. 그들의 권한을 실행하기 위해, 이러한 사용자들은 자기 자신을 증명할 필요가 있다. 가장 잘 알려지고 일반적으로 사용되는 사용자 인증 방법은 사용자 이름과 암호를 입력하는 것이다.

<3> 인터넷 사기의 성장속도와 교묘함으로, 상기 데이터가 통신 네트워크를 통해 쉽게 인터셉트될 수 있고 그런다음 원래 사용자의 신원과 권한의 위조 대리를 위해 상기 공격자에 의해 재사용될 수 있기 때문에, 사용자 이름과 암호 인증은 안전하지 않은 것으로 인식된다.

<4> 일회용암호(이하 "OTP")는 사용자 이름 및 암호의 체계의 취약성을 극복하기위해 다양한 벤더에 의해 제공되는 일반적인 방법이다. 그것은 한번의 로그인 또는 트랜잭션을 위해서만 암호를 사용하고, 그런다음 상기 암호는 소용없게 되도록하는 것에 기반을 둔다. 임의의 추가적인 로그인 또는 트랜잭션에는 상이한 암호를 요구하게 된다. 따라서, 어떠한 사람이 암호를 인터셉트한다고 하더라도, 차후의 트랜잭션에는 사용할 수 없게된다.

<5> 일회용 암호를 생성하고 관리하는 것에는 3 가지 기본적인 방법이 있다. 첫번째로는 종이 또는 전자 파일 상에 긴 리스트의 암호를 가지는 것이고; 둘째는 이러한 암호를 생성하기 위해 자신의 컴퓨터(데스크탑, 랩탑, 팜탑 또는 스마트폰)상에서 실행되는 소프트웨어를 사용하는 것이고; 세번째는 암호생성을 위한 전용 하드웨어 디바이스를 사용하는 것이다. 본 발명의 초점은 상기의 하드웨어 디바이스이다.

<6> 도 1A는 일회용 암호를 생성하는 전용 OTP 인증 디바이스(110)(일반적으로 OTP "토큰")를 사용하는 배경 기술의 시스템(100)을 기술한다. 컴퓨터(160)는 정보 또는 트랜잭션으로의 액세스와 같은 타겟 기능성을 얻기 위해, 서버(170) 상에서 실행되는 서버 애플리케이션(182)과 함께 클라이언트 애플리케이션(168)을 실행을 위한 처리 용량(도시되지 않음)을 포함한다. 클라이언트 애플리케이션(168)은 전용 프로그램 또는 범용 웹브라우저가 될 수 있다. 서버 애플리케이션(182)은 타겟 기능성을 제공하기 위해 OTP 검증기(178)로부터의 승인을 필요로한다. OTP 검증기(178)는 서버 애플리케이션(182)으로부터 (일회용) 암호를 수신하고 체크하도록 고안되고, 그런다음 클라이언트 애플리케이션(168)으로부터의 암호를 수신하는소프트웨어 모듈이다. 고려되는 구성에서, 상기 암호는 인증 디바이스 인터페이스(164)를 통해 OTP 인증 디바이스(110)에 의해 생성되고 그로부터 수신된 데이터로부터 도출된다. OTP 인증 디바이스(110)는 사용자에 의해 소지되고 복수의 컴퓨터(160)와 인터페이스하도록 적응된 보안 포터블 디바이스이다. OTP 인증 디바이스(110)의 핵심은 상기 OTP 인증 디바이스(110)에 기록된 트리거(120) 및 보안 사용자 키(132)에 기반을 둔 일회용암호를 생성하도록 고안된 마이크로프로세서기반 암호 소프트웨어 루틴인 OTP 생성기(130)이다. 일반적으로, 상기 OTP 디바이스(110)는 보안 사용자 키(132) 데이터로의 액세스 및/또는 상기 보안 사용자 키(132) 데이터를 변경하는 것을 방지하는 접근이 어렵고 조작이 방지되도록 구축된다.

<7> 트리거(120)는 OTP 생성기(130)에 의한 하나의 암호 생성 동작으로부터 다른 생성 세션으로 변하고, 그결과 암호의 "일회용" 측면을 제공하는 엘리먼트이다. 트리거(120) 생성을 위한 배경 기술에서의 3 개의 일반적인 접근 방식은 서버(170)로부터 수신된 랜덤 챌린지(120A), OTP 인증 디바이스(110)에 내장된 정확한 실시간 클록(120B)으로부터 수신된 풀 데이트 시간 스트링, 또는 각각의 연속적인 암호 생성에 대해 1 씩 증가하는 카운터(120C)이다.

<8> 이러한 개시를 통해, "세션 OTP 데이터"는 트리거(120) 및 보안 사용자 키(132)로부터 도출된 데이터라고 한다. 이러한 세션 OTP 데이터는 2 개의 팩터(또는 다수의 팩터) 인증 데이터를 제공하는 사용자 인증 데이터(즉, 암호, 생물학적 데이터 등)를 가지고 OTP 인증 디바이스(110) 및/또는 클라이언트 워크스테이션(160) 내에서 조합된다. 상기 조합이 상기 OTP 인증 디바이스(110)내에서 영향을 받는 특정한 경우, 상기 2 팩터 인증 데이터는 "세션 OTP 데이터"의 형태 그자체이다. 그럼에도 불구하고, 상기 세션 OTP 데이터가 상기 사용자키(132) 및 트리거(120)로부터 도출되는 한, 상기 OTP 디바이스(110)로부터 클라이언트 워크스테이션(160)에 제공된 상기 "세션 OTP 데이터"는 사용자-제공 데이터(즉, 암호/PIN 데이터 또는 생물학 데이터)로부터 도출된 멀티-팩터 인증

데이터가 될 수 있다는 명백한 요구조건이 없다.

<9> 선택적으로 그리고 일반적으로, 사용자 식별자(또는 사용자 식별 모듈)(134)가 OTP 인증 디바이스(110)를 찾아내거나 훔치는 사람에 의해 오용되는 것을 방지하기 위해 상기 OTP 인증 디바이스(110)에 제공될 수 있다. 다수의 구현에서, OTP 생성기(130)는 사용자 식별자(134)가 포지티브 사용자 인증을 제공하지 못한다면, 세션 OTP 데이터를 생성하지 않을 것이다(또는 전송하지 않을 것이다).

<10> 사용자 식별을 위한 일반적인 방법은 개인 식별 번호(PIN)를 수신하는 작은 키패드, 생물학 센서, PIN 또는 컴퓨터/클라이언트 워크스테이션으로부터 수신된 기타 데이터(일반적으로, 클라이언트 워크스테이션(160)의 키보드에 의한 클라이언트 워크스테이션(160)으로의 입력)를 체크하는 비교기이다.

<11> OTP 인터페이스(140)는 OTP 인증 디바이스(110)와 컴퓨터(160) 사이의 OTP 연관 데이터를 교환하기 위해 인증 디바이스 인터페이스(164)와 인터페이싱한다. 특히, OTP 생성기(130)가 세션 OTP를 생성할 때마다, OTP 전송기(도시되지 않음)가 상기 OTP 디바이스(110)으로부터 세션 OTP를 "전송"한다(즉, OTP 인터페이스(140)를 통해 세션 OTP 데이터를 컴퓨터(160)로 제공하도록 데이터 교환을 디스플레이하고 및/또는 데이터 교환을 실행한다).

<12> OTP 인터페이스(140)에 대한 일반적인 구현은: 암호를 판독하고 동일한 것을 인증 디바이스 인터페이스(164)로 기능하는 키보드로 수동으로 입력하기 위해 사용자에 의해 사용되는 디스플레이(140A)(그런다음 선호하는 트리거(120)가 실시간 클록(120B) 또는 카운터(120C)가 된다.); 양방향 시리얼 통신을 구축하기 위해 인증 디바이스 인터페이스(164)로서 기능하는 매칭 USB 인터페이스와 인터페이싱하는 USB 인터페이스(140B)(또는 기타 "접촉" 인터페이스), 또는 인증 디바이스 인터페이스(164)로서 기능하는 호환가능한 적외선/무선주파수 트랜시버와 인터페이싱하는 IR/RF 인터페이스(140C)(또는 기타 "무선 인터페이스")이다. USB(140B) 및 IR/RF 인터페이스(140C)의 경우, 트리거(120)에 대한 3개의 모든 접근 방식이 유효하다.

<13> OTP 인터페이스(140)가 디스플레이(140A)에 적용하는 경우는 OTP 인증 디바이스(110)와 컴퓨터(160) 사이에 직접적인 전자 통신링크를 필요로하지 않음을 유의하라. 다수의 예에서, 사용자는 사용자 인증 데이터(즉, 예를 들면 제 2의 "2-팩터" 인증을 위한 암호 및/또는 생물학적 데이터) 뿐만 아니라 상기 디스플레이(140B)로부터 판독된 세션 OTP 데이터(140) 모두를 상기 데이터가 2-팩터 인증 암호를 생성하기 위해(이것은 그 자체가 OTP 유형임) 조합되는 클라이언트 워크스테이션(160)으로 입력할 것이다.

<14> 서버(170)는 OTP 검증기(178)의 승인시에만 서버 애플리케이션(182)으로하여금 타겟 서비스를 클라이언트 애플리케이션(168)으로 제공하도록 한다. OTP 검증기(178)는 컴퓨터(160)를 통해 OTP 인증 디바이스(110)로부터 수신된 암호를 체크하고 사용자 키(132)와 트리거(120)를 고려하는 처리 및 암호 수단을 포함한다. 사용자 키(132)는 사용자 데이터베이스(176)로부터 검색되고, 이것은 자신들의 사용자 이름과 키를 포함하는 적합한 사용자의 기록을 포함한다. 트리거(120)의 값은 트리거 동기장치(174)로부터 OTP 검증기(178)에 의해 검색되고, 이는 챌린지 생성기, 실시간 클록 또는 카운터를 포함하며, 챌린지(120A), 실시간 클록(120B) 및카운터(120C) 각각으로부터 선택된 트리거(120)에 대한 방법에 대응한다.

<15> 도 1B는 도 1A의 동일한 종래기술 시스템을 도시한다. 도 1B에서, OTP 인증 디바이스(110), 컴퓨터(160)(즉, 클라이언트 워크스테이션), 서버(170)의 배치가 명확하게 도시된다. 보다 특정하게, 도 1B에 도시된 바와 같이, 클라이언트 워크스테이션/컴퓨터(160)는 ISP에 의해 제공된 WAN 게이트웨이(22)(ISP 액세스 포인트)를 가진 인터넷 액세스 링크(예를 들면, 광대역 링크, 다이얼업 링크, 소호링크, 또는 기타 ISP(인터넷 서비스 공급자) 액세스 링크, 또는 이동 디바이스로 서핑을 하기 위한 이동전화 인터넷 액세스 링크)를 통해 광역 네트워크(20)로 연결된다. 상기 서버(170)는 클라이언트 워크스테이션(160)으로 광역 네트워크(20)(일반적으로, 패킷 스위칭된 프로토콜을 이용하여)를 통해 세션 OTP에 대해 요청을 전송한다. 클라이언트 워크스테이션(160)에 의해 이러한 요청을 수신할 때, 상기 OTP 인증 디바이스(110)는 세션 OTP를 클라이언트 워크스테이션(160)으로 전송한다(자동 또는 사용자가 클라이언트 워크스테이션의 키보드를 통해 입력함으로써). 이러한 세션 OTP 데이터는 서버(170)로 직접 포워딩되거나 또는 인증 데이터(즉, 암호, 핀, 생물학적)와 결합되고, 그런다음 광역 네트워크(즉 인터넷)(20)를 통해 서버(170)로 전송된다.

<16> 도 2는 종래 일부 배경기술에 따라 도 1A-1B의 시스템(100)의 동작을 기술한다. 단계(201)에서, 컴퓨터(!60)의 사용자는 클라이언트 애플리케이션(168)을 런칭한다. 클라이언트 애플리케이션(168)은, 사용자에게 데이터에 대한 액세스 또는 트랜잭션을 하는 것과 같은 원하는 타겟 기능성을 제공하기 위해 서버 애플리케이션(182)과 통신하고 상호작용할 필요가 있다. 단계(221)에서, 서버 애플리케이션(182)은 OTP에 의한 사용자 인증에 대한 요청으로 클라이언트 애플리케이션(168)에 응답한다. 이러한 요청은 OTP 인증 디바이스(110)로 전송되고, 여기

서 OTP 생성기(130)는 단계(221)에서 OTP를 생성하기 위한 트리거를 트리거 유닛(120)으로부터 요청한다. 상기 트리거가 챌린지(120A)라면 서버(170)는 트리거 동기장치(174)에서 랜덤 챌린지 스트링을 생성하고 그것을 컴퓨터(160)를 통해 OTP 생성기(130)로 제공한다; 상기 트리거가 임의의 실시간 클록(120B) 또는 카운터(120C)라면, 그것은 OTP 인증 디바이스(110)내에서 스스로 생성된다. 단계(231)에서, OTP 생성기(130)는 OTP를 생성하기 위해 트리거(120)와 사용자 키(132)를 처리한다. 단계(241)에서, 단계(231)에서 생성된 OTP가, 상기 OTP로부터 서버(170)로 유도된 데이터를 포워딩하는 클라이언트 워크스테이션(160)으로 상기 OTP 디바이스(110)로부터 전송된다. 단계(251)에서, OTP 검증기(178)는 트리거 동기장치(174)로부터 검색된 트리거와 사용자 데이터 베이스(176)로부터 검색된 사용자 키에 기초하여 예측된 OTP를 연산하고, 그것을 컴퓨터(160)를 통해 OTP 인증 디바이스(110)로부터 수신된 OTP와 비교한다. 상기 검증이 포지티브하다면, 스텝(261)은 상기 프로세스를 스텝(271)로 라우팅하고, 여기서 클라이언트 서버 세션은 클라이언트 애플리케이션(168)과 서버 애플리케이션(182) 사이의 협력을 통해 원하는 타겟 서비스를 제공하는 것을 시작하고; 상기 검증이 네거티브라면, 그런다음 단계(261)는 상기 프로시저를 단계(281)로 라우팅하고, 여기서 서버(170)는 컴퓨터(160)로부터 수신된 서비스 요청을 거절하고, 사용자는 컴퓨터(160)에 의해 통지된다.

<17> 배경기술의 일반적인 사용자 인증 방법을 사용하는 상술한 시스템은 서비스 공급자(서버(170)를 운영하는)에 의한 사용자의 인증(컴퓨터(160)를 사용하는)에 초점을 맞춘다. 새로운 모드의 사기, 코인드 "피싱"이 소개되고 주된 사기 방법이 될 때까지, 이러한 단방향 인증 방법은 상당히 보호된 서비스 공급자와 사용자를 사용자 신분을 훔치는자로부터 상당히 보호하여왔다. 피싱에서, 사용자는 자신의 은행 또는 적법하고, 평판이 높은 인터넷 상업 사이트로부터 보내진 것으로 가장한 이메일 메시지에 의해 어드레스된다. 상기 메시지는 사용자에게 자신의 상세사항을 업데이트하거나 또는 상업 트랜잭션을 처리하도록 요청한다. 이러한 프로세스동안, 사용자는 자기자신을 인증하도록 요청받고, 그가 제공하는 정보는 상기 사용자의 신원정보를 훔치는 범죄자에 의해 사용되고, 사용자 앞으로의 다른 거래를 제공한다. 사용자에 의해 제공된 사용자이름과 암호는 상기 범죄자에 의해 보다 많은 트랜잭션에 재사용되기 때문에, 사용자 이름과 암호의 조합은 피싱에 대해 매우 취약하다. OTP의 사용은 피싱의 효과를 드라마틱하게 감소시키지만, 소위 "맨인더미들(man-in-the-middle)"이라고하는 피싱의 변종에 대해서는 완전한 보호를 제공하지는 못한다. 맨인더미들 공격에서, 위장 사이트로부터의 메시지는 사용자에게 적법한 뱅킹 또는 상업적 트랜잭션으로 보이게 하는 것을 시작한다. 트랜잭션이 발생하는 동안, 범죄자는 실제 사이트로 자신의 트랜잭션을 처리한다. 상기 범죄자는 OTP 기반 인증 세션을 통과하고 그런다음 돈을 이체하거나 또는 상품을 자신 또는 자신의 파트너에 전송하게하는 트랜잭션을 처리한다.

<18> 맨-인-더-미들 공격의 위험에 있는 환경에서 보안성을 증가시키는 기술에 연관된 공개된 다수의 문서가 있다. 잠재적으로 연관된 특허 및 공개된 특허 출원은 모두가 그 전체가 참조로 통합된, US20010045451, US20060041759, US6141752, WO2005098630, WO06018647, WO06062838을 포함한다.

<19> RSA Security, Inc.로부터의 백서 "Enhancing One-Time Passwords for Protection Against Real-Time Phishing Attacks"는 OTP 디바이스(즉, 전자 토큰)가 클라이언트 워크스테이션과 함께 사용되는 기술을 개시한다. 상기 OTP 디바이스는 클라이언트 워크스테이션(예를 들면 트리거-도출 데이터가 USB 인터페이스를 통해 제공된 USB 인터페이스를 통해 통신하는 "접촉" OTP 디바이스)과 통신하거나 또는 트라이거-도출 OTP-코드(즉, 트리거 도출 데이터)를 클라이언트 워크스테이션의 키보트로 타이핑하는 인간 사용자에 의해 사용된다. 상기 트리거-도출 OTP-코드(자동으로 제공되거나, 또는 OTP 토큰의 스크린으로부터 복사된)가 클라이언트 워크스테이션 상에서, "2-팩터" 암호를 제공하도록 클라이언트 워크스테이션으로 입력된 암호/PIN 데이터로 조합된다. 보다 특정하게, 이러한 암호/PIN 데이터를 브라우저로 입력하고 직접 상기 조합된 데이터 2-팩터 인증 데이터를 인터넷을 통해 전송하는 대신에, 상기 사용자 암호/PIN을 수신하기 위한 클라이언트 워크스테이션 상에 상주하는 소프트웨어 "암호 보호 모듈"(PPM)(일반적으로 상기 브라우저와는 독립된)이 제공된다. 클라이언트 워크스테이션 상에서, 상기 PPM 모듈은 사용자 암호/PIN을 상기 OTP 디바이스 토큰에 의해 제공된 OTP 데이터와 조합한다. 상기 클라이언트 워크스테이션으로부터 서버로 전송하기전에, 상기 조합된 데이터는 요청 서버의 신원확인에 따라 상기 PPM에 의해 암호화/해시된다. 이것은 아마도 상기 해싱된 암호에 액세스하고, 상기 OTP 데이터 및/또는 2-팩터 인증 데이터 및/또는 사용자 인증 데이터를 알게되는 것을 상기 "맨-인-미들"이 어렵도록한다.

<20> 상기 PPM이 일반적으로 상기 공격하기 쉬운 브라우저로부터의 독립 애플리케이션이더라도, 이러한 종래기술의 하나의 단점은, 상기 OTP 인증을 요청하는 서버가 적법하지 않은 위험이 있음에도 불구하고, 상기 잠재적으로 안전하지않은 클라이언트 워크스테이션에 대한 일반적으로 접근이 어려운 OTP 디바이스로부터의 상기 세션 OTP 데이터가 항상 제공되는(사용자 또는 디바이스 인터페이스를 통해)것이다.

<21> 피싱과 맨-인-더-미들의 위험에 기인하여, 인증된 파티에 의한 액세스로부터의 OTP 데이터를 보호하기 위한 개

선된 방법 및 장치에 대한 진행중이 요구가 있다.

발명의 상세한 설명

<22> 본 발명은 지금 피싱 공격을 효과적으로 방지하기 위한 일회용 암호(OTP) 설비에 의해 제공되는 보호를 확장하는 시스템 및 기능을 기술한다. 특정하게, 본 발명자는, 지금 세션 OTP 요청하는 서버가 적법한 서버임을 지시하는 경우에만, 클라이언트 워크스테이션으로 세션 OTP 데이터를 제공하는 것이 유리하다는 것을 기술한다. 그렇지 않다면, 상기 세션 OTP 데이터를 요청하는 서버가 적법한 서버인 것을 나타내지 않는다면(또는 충분히 지시하지 못한다면), 상기 OTP 디바이스가 상기 클라이언트 워크스테이션/단말로부터의 세션 OTP 데이터를 보류하는 것이 유리하다.

<23> 명확한 요구조건이 없다면, 일 실시예에서, 요청 서버가 적법한지 아닌지 여부를 판정하는 것에 연관된 특정한 기능은 또한 상기 접근이 어렵고 OTP 디바이스 내에서 구현되고, 그에 의해 상기 서버의 신원확인을 검증하기 위한 메커니즘을 조작하는 것(예를 들면, 크랙커 및/또는 사기꾼 및/또는 맨-인-더-미들에 의해)에 대한 추가적인 보호를 제공한다. 대안으로, 또는 추가로, 이러한 기능성이 클라이언트 워크스테이션에서 구현된다.

<24> 먼저 세션 OTP 데이터의 전송을 핸들링하는 방법이 기술된다(예를 들면, 세션 OTP에 대한 서버-생성 요청에 따라). 상기 현재 기술된 방법은 서버, 광역 네트워크(예를 들면 인터넷)를 통해 서버와 통신하는 클라이언트 워크스테이션, 및 디바이스 인터페이스(즉, '접촉' 또는 '무선 인터페이스'를 통해)를 통해 클라이언트 워크스테이션과 인터페이스하는 OTP 토큰을 구비하는 시스템에서 구현된다. 본 기술된 방법은 (a) 적어도 부분적으로 서버를 식별하는 정보를 서버로부터 수신하는 단계(OTP 디바이스 및/또는 클라이언트 워크스테이션에 의해); (b) 상기 식별 정보가 적법한 서버를 지시하는 지를 판정하는 단계; 및 (c) 상기 판정에 따라, i) OTP 토큰으로부터 내부적으로 생성된 세션 OTP를 지시하는 데이터(즉, 클라이언트 워크스테이션 내에서가 아니라 OTP 토큰 내에서 생성된 세션 OTP로서, 트리거와 보안 사용자 키, 그리고 옵션으로 사용자 인증 데이터에 따라 생성된 세션데이터)를 전송하는 단계, 및 ii) 상기 전송을 억제하는 단계;로 구성되는 그룹으로부터 선택된 하나의 동작을 수행하도록 결정하는(즉, 상기 OTP 트큰 및/또는 클라이언트 워크스테이션에 의해) 단계를 포함한다. 상기 결정이 포지티브한 결정(즉, 세션 OTP를 지시하는 데이터를 전송하는 결정)인 경우에만, 상기 OTP 토큰으로부터 상기 세션 OTP를 지시하는 데이터를 전송한다.

<25> 일부 실시예에 따라, 상기 전송 단계는 상기 결정이 포지티브한 경우에만, 상기 인터페이스를 통해 상기 OTP 토큰으로부터 상기 클라이언트 워크스테이션으로 상기 지시 데이터의 디바이스 상호간의 데이터 전송을 유효화하는 단계를 포함한다.

<26> 일부 실시예에 따라, 상기 전송 단계는 상기 결정이 포지티브한 경우에만, 상기 OTP 토큰의 디스플레이 스크린 상에 상기 세션 OTP를 지시하는 데이터를 표시하는 단계를 포함한다.

<27> 일부 실시예에 따라, 상기 세션 OTP를 지시하는 데이터는 사용자 인증 데이터로부터 도출된 멀티-팩터 인증 데이터이다.

<28> 또는, 상기 세션 OTP를 지시하는 데이터는 사용자 인증 데이터에 독립적이다.

<29> 일부 실시예에 따라, 상기 방법은, d) 상기 결정이 네거티브한 결정이라면, 상기 OTP 토큰에 의해 상기 세션 OTP를 생성하는 것을 방지하는 단계를 더 포함한다.

<30> 일부 실시예에 따라, 상기 방법은 d) 상기 결정이 네거티브한 결정이라면, i) 내부적으로 상기 OTP 토큰내에서 상기 세션 OTP를 생성하는 단계; 및 ii) 상기 세션 OTP가 상기 OTP 토큰내에 남아있는 상태를 유지하는 단계를 더 포함한다.

<31> 일부 실시예에 따라, 상기 방법은 (d) 상기 수신단계 전에, 상기 OTP 토큰 내에서 내장된 보안 브라우저를 사용하는 단계, 상기 OTP 토큰과 서버 사이에서 보안 세션을 오픈하는 단계를 더 포함한다.

<32> 일부 실시예에 따라, 상기 방법은 (e) 상기 세션의 오픈하는 단계 후에, 상기 OTP 토큰으로부터 클라이언트 워크스테이션으로 상기 세션의 클라이언트 엔드를 전송하고, 여기서 상기 수신 및 판정의 적어도 하나는 상기 클라이언트 워크스테이션에서 수행되는 단계를 더 포함한다.

<33> 일부 실시예에 따라, 클라이언트 말단 및/또는 세션의 엔드는 상기 식별 정보가 상기 서버로부터 상기 OTP 토큰에 의해 수신된 때에, 상기 내장된 브라우저에 유지된다(즉, 상기 클라이언트 워크스테이션은 ""데이터 관로"로 사용되고, 상기 통신은 상기 OTP 디바이스 내에서로부터 관리된다).

<34> 일부 실시예에서, 상기 수신단계는 상기 서버와 상기 OTP 토큰 사이의 통신 링크를 통해 상기 OTP 토큰(즉, 상기 OTP 토큰 내에 내장된 브라우저)에 의해 수행되고, 즉, 상기 OTP 토큰은 상기 세션의 클라이언트 엔드이고, 상기 클라이언트 워크스테이션은 "데이터 관로"로서만 사용되고, 상기 통신은 상기 OTP 디바이스내에서로부터 관리된다.

<35> 일부 실시예에서, 상기 판정단계는 상기 OTP 토큰 내에서 수행된다. 일부 실시예에 있어서, 이것은, 상기 OTP 토큰 내에서의 환경의 접근이 어렵고 및/또는 조작이 방지되는 속성에 따른 보안의 부가적 측정을 제공할 수 있다.

<36> 일부 실시예에서, 상기 판정단계는 상기 OTP 토큰 내에서 상주하는 데이터베이스로 쿼리(클라이언트 워크스테이션 및/또는 상기 OTP 토큰 내에 상주하는 데이터베이스 클라이언트 코드로부터)를 유효화하는 것을 포함한다.

<37> 일부 실시예에서, 상기 데이터베이스는 불변의 데이터베이스이다. 따라서, 일 실시예에 따라, 금융기관 또는 금융기관의 그룹은 디바이스 내에 내장된 적법한 서버(즉, 금융기관 또는 금융기관의 그룹에 연관된)의 "바람직한 리스트"를 가진 OTP 디바이스를 배포한다. 이러한 바람직한 리스트는 불변이고, 이것은 "포괄적인 해결안"을 제공하지 않지만, 배포 금융기관(및/또는 그들의 고객)에 대해 적절한 것이다. 서버에 대해 적법성을 인증하는 데이터베이스의 상기 불변의 속성은 또한 보안의 추가된 측정을 제공한다.

<38> 일부 실시예에 따라, 상기 데이터베이스는 수용가능한 URL의 미리 정해진 리스트, 수용가능한 IP 어드레스의 미리정해진 리스트, 및 공인인증 필드에 대한 수용가능한 값의 미리정해진 리스트를 포함한다.

<39> 일부 실시예에 따라, 상기 판정은 수신된 하나의 통신의 프로토콜 데이터(예를 들면, 서버의 IP 어드레스를 지시하는 전송된 패킷 데이터로부터 추출함으로써), 및 수신된 통신에서 전송된 공인인증 데이터, URL 데이터 및 IP 어드레스 데이터 중 적어도 하나에 따라 수행된다.

<40> 일부 실시예에 따라, 상기 판정은 상기 서버로부터 수신된 공인인증의 일부 속성에 따라서만 수행된다. 따라서, 일예에서, 공인인증은 다수의 필드를 가지지만, 일부이고 모든 공인인증 필드가 아닌 필드가 상기 서버의 적법성을 확인/판정하는 데에 사용된다. 이것은 다수의 예시적인 시나리오, 예를 들면, 서버의 "패밀리" 또는 서버 파라미터를 정의하는 것이 바람직한 경우(그에 의해 '부분적으로' 서버의 식별자를 정의)에 유용하다. 예를 들면, 발급자(예를 들면, 은행 또는 보안 서버의 기타 오퍼레이터)는 하나 이상의 공인인증 공급자와 작업하고, 그 결과 이러한 필드는 상기 공인인증을 검증할 것을 요청받지 않는다. 예를 들면, 은행은 특정한 그룹에 다수의 서버를 배치하고, 상기 그룹의 서버가 세션 OTP 요청을 발급하는 것을 지정하는 공인인증 필드 데이터는 사용되지 않는 반면, 다른 필드가 사용될 수 있다. 이것은 발급자(예를 들면 은행)가, 상기 OTP 디바이스가 발급되는 때에 서버 식별 파라미터(예를 들면, 불변의 데이터베이스를 포함하는)를 완벽하게 지정할 필요는 없는 유연성을 가지도록 한다.

<41> 상기 일부 상황에 보안을 제공하는 "불변의 데이터베이스"는 본 발명의 한정사항이 아님에 유의하라.

<42> 일실시예에서, 상기 전송된 데이터는 암호화 및/또는 해시된다.

<43> 먼저, 광역 네트워크를 통해 서버와 통신하는 클라이언트 워크스테이션으로 사용하는 OTP 토큰에 대해 개시된다. 본 개시된 OTP 디바이스는; (a) 적어도 부분적으로 서버를 식별하는 정보를 포함하는 데이터를 클라이언트 워크스테이션으로부터 수신하는 디바이스 포트(즉, USB 포트와 같은 것으로부터 연유한 '접촉' 및/또는 무선의 하나 이상의 디바이스 포트); (b) 상기 정보가 적법한 서버를 지시하는 지를 판정하는 서버 적법성 엔진; (c) 세션 OTP를 생성하도록 동작하는 OTP 생성기; 및 (d) 판정의 결과에 따라, i) OTP 토큰으로부터 세션 OTP를 지시하는 데이터를 전송하는 단계, 및 ii) 상기 전송을 억제하는 단계;로 구성되는 그룹으로부터 선택된 하나의 동작을 수행하는 것을 결정하도록 동작하는 OTP 전송 결정 엔진을 포함한다.

<44> 일실시예에서, 상기 디바이스는 c) 세션 OTP를 지시하는 데이터를 전송하는 OTP 전송기를 더 포함하고, 여기서 상기 OPT 전송기는 다음과 같은 특징을 가진다.

<45> 일부 실시예에 따라, 상기 OTP 전송기는 상기 결정이 포지티브하다면, 데이터 포트를 통해 클라이언트 워크스테이션으로 상기 세션 OTP를 지시하는 데이터를 전송하도록 동작한다.

<46> 일부 실시예에 따라, 상기 OTP 토큰은, (d) 상기 엔진이 상기 식별정보가 상기 적법한 서버를 지시하는 것으로 판정하는 경우에만, 상기 OTP 전송기가 데이터 디스플레이로 세션 OTP를 지시하는 데이터를 전송하도록 동작하는, 데이터 디스플레이를 더 포함한다.

<47> 일부 실시예에 따라, 상기 OTP 토큰은 (d) 상기 내장된 브라우저가 상기 OTP 토큰과 상기 서버 사이의 보안 세션을 오픈하도록 동작하는, 상기 OTP 토큰 내에 내장된 보안 브라우저를 더 포함한다.

<48> 일부 실시예에 따라, 상기 내장된 보안 브라우저는 상기 보안 세션동안, 상기 식별 정보를 수신하도록 동작한다.

<49> 일부 실시예에 따라, 상기 서버 적법성 엔진은, (d) 상기 서버 적법성 엔진이 상기 데이터베이스의 컨텐츠에 따라 판정하는 것을 수행하도록 동작하는, 미리정해진 데이터의 데이터베이스를 포함한다.

<50> 일부 실시예에 따라, 데이터베이스는 불변의 데이터베이스이다. 이것은 예를 들면, 미리정의된 서버 그룹으로 동작하는 특별한 OTP 디바이스(범용 OTP 디바이스가 아닌)가 배포되고, 사기꾼 및/또는 범죄자 및/또는 크래커가 서버를 추가하도록 데이터베이스를 변조하지 못하도록 추가된 보안을 제공하는 것이 바람직한 경우에, 유용하다.

<51> 일부 실시예에 따라, 상기 데이터베이스는 수용가능한 URL의 미리정해진 리스트, 수용가능한 IP 어드레스의 미리정해진 리스트, 및 공인인증 필드의 수용가능한 값의 미리정해진 리스트를 포함한다.

<52> 일부 실시예에 따라, 상기 서버 적법성 엔진은 상기 서버로부터의 통신의 프로토콜 데이터 및 상기 서버로부터의 통신에서 전송된 공인인증 데이터 중 적어도 하나에 다라 상기 판정을 수행하도록 동작한다.

<53> 일부 실시예에 따라, 상기 서버 적법성 엔진은 상기 서버로부터 수신된 공인인증의 일부 속성에 따라서만 판정을 수행하도록 동작된다.

<54> 일부 실시예에 따라, 상기 OTP 생성기는 사용자 인증 데이터에 따라 상기 세션 OTP를 생성하도록 동작하고, 그에 의해 멀티-팩터 인증 데이터로서 세션 OTP를 생성한다.

<55> 일부 실시예에 따라, 상기 디바이스는 (e) 상기 사용자 인증 데이터를 인증하는 사용자 식별 모듈을 더 포함한다.

<56> 일부 실시예에 따라, 상기 OTP 전송 결정 엔진은 상기 사용자 인증 데이터의 인증의 결과에 따라 결정을 수행하도록 동작한다.

<57> 세션 OTP 데이터의 전송을 핸들링하는 시스템을 먼저 개시한다. 본 기술된 시스템은, a) 광역 네트워크를 통해 서버와 통신하는 클라이언트 워크스테이션; b) 상기 클라이언트 워크스테이션과 인터페이싱하고, i) 상기 클라이언트 워크스테이션과 인터페이싱하는 디바이스 포트, 및 ii) 세션 OTP를 생성하도록 동작하는 OTP 생성기를 포함하는 OTP 토큰을 포함하고; 상기 OTP 토큰과 클라이언트 워크스테이션 중 적어도 하나는 상기 서버를 식별하는 정보를 수신하도록 동작하는 시스템이고, 상기 시스템은, 또한 c) 상기 정보가 적법한 서버를 지시하는지 여부를 판정하며, 상기 OTP 토큰 및 클라이언트 워크스테이션 중 적어도 하나에 적어도 부분적으로 상주하는 서버 적법성 엔진; d) 상기 판정의 결과에 따라, i) 상기 OTP 토큰으로부터 상기 세션 OTP를 지시하는 데이터를 전송하고; ii) 상기 전송을 억제하는 단계로 구성된 그룹으로부터 선택된 하나의 동작을 수행하는 것을 결정하도록 동작하며, 상기 OTP 토큰과 상기 클라이언트 워크스테이션 중 적어도 하나에 적어도 부분적으로 상주하는 OTP 전송 결정 엔진을 더 포함하는 시스템이다.

<58> 먼저, 컴퓨터 판독가능 저장 매체에 내장된 컴퓨터 판독가능 코드를 가진 컴퓨터 판독가능 저장 매체로서, 상기 컴퓨터 판독가능 코드는, a) 광역 네트워크를 통해 서버와 통신하는 클라이언트 워크스테이션과 상기 서버와 인터페이싱하는 OTP 토큰 중 적어도 하나에 의해 상기 서버를 적어도 부분적으로 식별하는 정보를 수신하고; b) 상기 식별 정보가 적법한 서버를 지시하는지를 판정하고; c) 상기 판정에 따라, i) 상기 OTP 토큰으로부터 내부적으로 생성된 세션 OTP를 지시하는 데이터를 전송하는 단계, 및 ii) 상기 전송을 억제하는 단계로 구성되는 그룹으로부터 선택된 하나의 동작을 수행하는 것을 결정하는; 명령을 포함하는 컴퓨터 판독가능 저장 매체가 개시된다.

<59> 이러한 그리고 추가적인 실시예는 하기의 상세한 설명과 예시에 의해 명확하게 될 것이다.

실 시 예

<69> 본 발명은 특정한 예시적인 실시예로 기술될 것이다. 본 발명이 기술된 예시적 실시예에 한정되는 것이 아니라는 것이 이해될 것이다. 또한 본 개시된 세션 데이터를 핸들링하는 장치, 디바이스, 및 컴퓨터 판독가능한 코드의 모든 특징이 첨부된 청구범위 중 특정한 하나에서 주장되는 본 발명을 구현하기 위해 필요한 것은 아니라

는 것이 이해되어야한다. 디바이스의 다양한 엘리먼트 및 특징이 본 발명을 완전히 이네이블하게 하기 위해 기술된다. 하나의 단계가 먼저 실시된 다른 단계에 따른다는 것이 문맥에서 명확하지 않다면, 프로세스 또는 방법이 도시되거나 기술된 본 설명을 통해, 상기 방법의 단계들은 임의의 순서로 또는 동시에 수행될 수도 있다는 것이 또한 이해되어야한다. 명확한 반대의 문구가 없다면, 클라이언트 워크스테이션, 서버, 또는 OTP 토큰의 임의의 개시된 컴포넌트는 하드웨어 및/또는 소프트웨어 및/또는 펌웨어의 임의의 조합으로 구현될 수 있다.

<70> 도 3A-3E를 참조하면, 이는 본 발명의 바람직한 실시예에 따라 구축된 시스템(300)을 기술한다. 상기 시스템(300)의 특정한 블록 및 기능이 도 1A-1B의 시스템(100)의 상당하는 블록 및 기능과 유사 또는 동일하다는 것에 유의하라. 따라서, 도 3A-3D의 OTP 인증 디바이스(310)는 사용자 키 리포지토리(132)의 컨텐츠 및 트리거(120)의 출력에 따라 세션 OTP 데이터를 생성하는 트리거(120) 및 OTP 생성기(330)를 포함한다. 선택적으로, 상기 세션 OTP 데이터는 또한 사용자 인증 데이터(예를 들면, 사용자 식별자(134)에 의해 핸들링되는)에 따라 생성된다. 또는, 상기 세션 OTP 데이터는 사용자 인증 데이터에 독립적이며, 트리거(120)의 출력과 사용자 키 리포지토리(132)(일반적으로, 사용자 키 데이터가 상주하는 접근이 어렵고 조작이 방지되는 비휘발성 메모리)의 컨텐츠에만 의존한다.

<71> OTP 세션 데이터는 인터페이스(140)를 통해 OTP 전송기(342)에 의해, 상기 OTP 토큰 디바이스(310)로부터 상기 디스플레이 인터페이스(140A)의 일부로서 제공된 디스플레이 스크린으로, 또는 접촉 인터페이스(140B) 또는 무선 디바이스 인터페이스(140C)를 통해 클라이언트 워크스테이션(360)으로 전송된다.

<72> 상기 OTP 세션 데이터는 OTP 세션에 대한 요청이 수신될 때마다 상기 OTP 토큰(310)으로부터 무조건적으로 전송되는 것은 아니다. 오히려, 상기 전송은 OTP 전송 결정 엔진(344)에 의해 유효화되는 "진행/진행준비가 안됨" 결정에 따라 수행된다. 도 3A-3E에서, 특정한 컴포넌트(예를 들면, OTP 전송 결정 엔진(344), 사용자 식별자(134), 브라우저(350), 및 서버 적법성 엔진(340))가, 상기 컴포넌트 중 하나 이상이 OTP 토큰의 외부에 일부 또는 그 전체가 상주하는 실시예가 또한 본 발명자에 의해 고려되었음에도 불구하고, 상기 OTP 토큰(310) 내에 상주하는 것으로 도시된다.

<73> 상기 전송 결정 엔진(344)은 하나 이상의 팩터에 따라 상술한 "진행/진행준비가 안됨" 전송 결정을 수행한다. 일반적으로, 상기 OTP 토큰(310)은, 서버 적법성 엔진(340)이 세션 OTP에 대한 요청에 연관된 서버 식별자가 상기 요청 서버(170)가 적법한 것 같다고(사기꾼 또는 피셔 또는 "맨-인-더-미들"일 가능성이 더 적다고) 지시하는 것으로 판정할 때에만, 상기 안전한 OTP 토큰으로부터(덜 안전한 클라이언트 워크스테이션(360) 또는 디스플레이 스크린으로) 세션 OTP를 전송한다.

<74> 따라서, 도 3D를 참조하면, 예시적인 실시예에서, 서버 적법성 엔진(340)은 데이터베이스(362)와, 예를 들면 상기 데이터베이스(검색할 정도로 간단할 수 있는)에 "쿼리"하도록 동작하는 로직(360)을 포함한다는 것에 유의하라. 상기 데이터베이스는 "신뢰할 수 있는 서버"를 지시하는 미리정해진 데이터를 포함한다. 상기 서버 적법성 엔진(340)은 따라서 본 세션 OTP가 적법한 서버로 이루어지고, 전형적인 피싱에서와 같이 적법한 서버로 가장하는 위장 서버로 이루어지는 것은 아니라는 것을 검증하도록 동작한다. 상기 신뢰할 수 있는 서버의 데이터베이스(360)는, 각각의 신뢰할 수 있는 서버에 대해, 예를 들면, IP(인터넷 프로토콜) 어드레스, URL(고유 리소스 로케이터) 또는 공인인증 데이터(예를 들면, 상세한 설명에서 논의된 것과 같은 '부분적' 공인인증 데이터) 중 적어도 하나를 포함하는 기록으로부터 형성된다.

<75> 예시적인 실시예에서, 상기 데이터베이스는 OTP 인증 디바이스(310)의 공급자(예를 들면, 자신의 고객들에게 그에 연관된 보안 세션을 위한 디바이스를 제공하는 은행)에 의하거나, 또는 상기 사용자에 의해 만들어진 엔트리를 통해, 또는 신뢰할 수 있는 파티로부터 상기 신뢰할 수 있는 서버의 파일을 수신하는 것 중 어느 하나에 의해 점유된다. 일부 실시예에서, 상기 데이터베이스는 불변이고, 상기 OTP 인증 토큰(310)의 "시핑" 전에 구성된다.

<76> 도 3E를 참조하면, 컴퓨터(360)(즉, 클라이언트 "워크스테이션")는 도 1A-1B의 컴퓨터(160)의 인증 디바이스 인터페이스와 동일한 인증 디바이스 인터페이스(164)를 가지고, 클라이언트 애플리케이션(368)은 자신의 신원을 검색(연결된 파티의 IP, URL, 및/또는 공인인증을 식별하기 위한 당업자에 공지된 표준 식별 서비스를 이용하여)하고 그 서버 신원을 입력으로서 OTP 인증 디바이스(310)의 서버 ID 검사기(334)로 전송하기 위한 문의 서버(170)의 추가적인 기능성을 가지며, 도 1A-1B의 클라이언트 애플리케이션(168)과 유사하다. 본 발명은 컴퓨터(360) 또는 서버(170)에 대한 변형을 필수적으로 요구하지는 않는다. 컴퓨터("클라이언트 워크스테이션")(360)는 서버(170)와 통신하는 데에 사용되는 임의의 컴퓨터화된 사용자 디바이스가 될 수 있음에 유의하라. 예를 들면, 컴퓨터(360)는 개인용 데스크탑, 랩탑, 또는 팜탑 컴퓨터, 휴대 전화 또는 양방향 페이

저가 될 수 있다. OTP 인증 디바이스(310)는, 하나 이상의 컴퓨터(360)에 연결될 수 있는 자율적인 포터블 디바이스(전자 "토큰")이고, 디스플레이, USB 토큰, 토큰 기능을 가진 USB 디스크, 착탈가능 카드(예를들면 보안 디지털(SD), 멀티미디어카드(MMC), 메모리스틱, 또는 SIM 카드) 등을 가진 키 팝과 같은 다양한 폼 팩터를 가질 수 있고; 또는 그것은 개인용 컴퓨터와 같은 다른 컴퓨터와 함께 사용된다면, 휴대전화가 될 수도 있다.

<77> 서버(170)가 본 발명을 "인지"할 필요는 없다는 것에 또한 유의하라. 이것은 기존 서버(170)를 공격하는 피싱의 위험을 감소시키기 위해 본 개시된 방법 및 장치 사이의 호환성을 제공한다.

<78> 도 4A는 본 발명의 일부 실시예에 따른 도 3A-3E의 시스템(300)의 운영을 기술한다. 대부분의 단계는 도 2의 것과 동일하며, 단계(401, 411, 421, 431)가 추가되었다. 따라서, 클라이언트 애플리케이션(368)이 단계(201)에서 런칭된 후에, 단계(401)에서 클라이언트 애플리케이션(368)하에서, 서버(170)의 ID는 컴퓨터(360)에 의해 검색되고, 서버 ID 검사기(334)의 일부를 형성하는 적법한 서버의 데이터베이스에 대해 서버 ID 검사기(334)에 의해 단계(411)에서 검증되도록 OTP 인증 디바이스(310)로 전송된다. 서버가 포지티브하게 검증된다면, 단계(421)는 상기 프로세스를 도 2에서 처럼 단계(211, 221, 231, 241, 251, 261, 271, 281)로 라우팅하고, 여기서 OTP는 OTP 인증 디바이스(310)의 OTP 생성기(330)에 의해 생성되고, 클라이언트-서버 세션을 실행하는 전제조건으로서 서버(170)에 의해 검증된다. 단계(411)에서 상기 검증이 네거티브하게 종료하면, 단계(421)는 상기 프로세스를 단계(431)에서의 거절로 라우팅하고, 여기서 OTP 인증 디바이스(310)의 OTP 생성기(330)는 유효한 OTP를 생성하지 못하고, 프로시저는 클라이언트 애플리케이션(368) 또는 서버 애플리케이션(182)에 의해 종료될 것이다.

<79> 도 3 및 4의 구성은 OTP 인증 디바이스(310)와 양방향 통신을 요구하기 때문에, USB(140B) 또는 IR/RF 인터페이스(140C)의 사용이 바람직하다는 것에 유의하라. 그러나, OTP 인터페이스(140)가 OTP 인증 디바이스(310)와 컴퓨터(360) 사이에 통신 링크가 없는 디스플레이(140A)를 사용한다면, 상기 서버 ID의 엔트리는 키패드(사용자 식별자(134)에 대한 PIN 엔트리에 대해 사용할 수도 있는)와 같은 수동 입력 디바이스를 OTP 인증 디바이스(310)에서 필수적이 되도록 할 것이다. 따라서, 이경우에, 사용자는 OTP 인증 디바이스(310)로 메시지에 표시된 서버 ID를 타이핑하도록 컴퓨터(360)의 디스플레이 상의 메시지에 의해 프롬프트되고, 그런다음 디스플레이(140A) 상에 도시된 OTP를 컴퓨터(360)로 타이핑한다.

<80> 도 4B는 도 4A에 기술된 예시적인 인증 루틴의 서브-루틴을 기술한다. 따라서, 루틴(4B)은 도 4B에 기술된 것인 아닌 인증 루틴에 따라 수행된다.

<81> 도 4B를 참조하면, 먼저 적어도 국부적으로 서버를 식별하는 정보가 수신된다(385)(OTP 디바이스(110) 및/또는 클라이언트 워크스테이션에서). 그런다음, 식별 정보가 적법한 서버(387)를 지시하는지(즉, 서버(170)가 적법한/신뢰할 수 있는/진짜인지) 여부를 판정하는 것이 이루어진다(387)(예를 들면 서버 적법성 엔진(340)에 의해). 상기의 판정의 결과에 따라, "진행/진행준비가 안됨" 전송 결정(389)(덜 안전한 클라이언트 워크스테이션으로 OTP 세션 데이터를 전송하기 위한- 광역 네트워크를 통해 서버(170)로 OTP 세션 데이터를 전송하는 것에 관한 결정이 필수적인 것은 아님)이 이루어진다(예를 들면 OTP 전송 결정 엔진(344)에 의해). 포지티브 결정(즉, 전송)의 이벤트(391)에서, OTP 세션을 지시하는 데이터가 "전송된다"(즉, 디바이스 인터페이스 또는 디스플레이 스크린 중 어느 하나를 통해). 그렇지않다면, 이것들은 상기 OTP 토큰(310)의 "외부"의 보다 덜 안전한 환경으로 상기 OTP 세션 데이터를 전송하는 것을 억제(431)한다.

<82> 본 출원서의 상세한 설명 및 청구범위에서, 동사 "구비한다", "포함한다", "갖는다", 및 그의 활용형 각각은, 상기 동사의 목적어 또는 목적어들이 상기 동사의 주어 또는 주어들의 멤버, 컴포넌트, 엘리먼트 또는 부분들의 완전한 목록을 제시하는 것이 필수적인 것이 아니라는 것을 지시하도록 사용된다.

<83> 본문에 인용된 모든 참조문헌은 그 전체가 참조에 의해 통합되었다. 참조문헌의 인용은 상기 참조문헌이 종래기술이라는 것을 자인하는 것은 아니다.

<84> 관사인 "a" 및 "an"은 상기 관사의 하나 이상(즉, 적어도 하나)의 문법적인 목적어를 지시하도록 본문에서 사용된다. 예시의 방식에 의해, "엘리먼트"는 하나의 엘리먼트 또는 하나 이상의 엘리먼트를 의미한다.

<85> "포함하는"이라는 단어는 본문에서 "포함하지만 한정되는 것은 아님"이라는 어구를 의미하고, 그와 상호교환가능하게 사용된다.

<86> "또는"이라는 단어는 본문에서 명확하게 달리 지시하지 않으면, "및/또는"이라는 단어를 의미하고 그와 상호교환가능하게 사용된다.

<87> "~와 같은"이라는 단어는 본문에서 "~와 같지만 그에 한정되는 것은 아님"이라는 의미의 어구를 의미하고, 그와 상호교환가능하게 사용된다.

<88> 본 발명은 예시의 방식으로 제공되고, 본 발명의 범위를 한정하지 않도록 의도된 그의 실시예의 상세한 설명을 이용하여 기술되었다. 상기 기술된 실시예는 상이한 특징을 구비하지만, 그의 모두가 본 발명의 모든 실시예에서 필수적인 것은 아니다. 본 발명의 일부 실시예는 상기 특징 중 일부 또는 그 특징들의 가능한 조합을 활용한다. 기술된 본 발명의 실시예의 변형과 기술된 실시예의 상술한 특징의 상이한 조합을 구비하는 본 발명의 실시예가 당업자에게는 자명할 것이다.

도면의 간단한 설명

<60> 도 1A-1B(종래 기술)는 세션 OTP 요청 서버(170), 인터넷(20)을 통해 상기 서버(170)와 통신하는 컴퓨터/클라이언트 워크스테이션(160), 및 상기 클라이언트 워크스테이션(160)으로 사용하는 OTP 디바이스/토큰(110)을 포함하는 예시적인 시스템의 각각의 블록도를 제공한다.

<61> 도 2는 OTP 디바이스(110)에 의해 생성된 OTP로 클라이언트-서버 세션을 시작하는 종래 기술의 루틴의 플로우도를 제공한다.

<62> 도 3A-3B는 본 발명의 실시예에 따라 세션 OTP 요청 서버(170), 인터넷(20)을 통해 상기 서버(170)와 통신하는 컴퓨터/클라이언트 워크스테이션(360), 및 상기 클라이언트 워크스테이션(160)으로 사용하는 OTP 디바이스/토큰(310)을 포함하는 예시적인 시스템(300)의 각각의 블록도를 제공한다.

<63> 도 3C는 예시적인 OTP 인증 디바이스/토큰(310)의 블록도를 제공한다.

<64> 도 3D는 예시적인 서버 적법성 엔진(340)의 블록도를 제공한다.

<65> 도 3E는 예시적인 클라이언트 워크스테이션/컴퓨터(360)의 블록도를 제공한다.

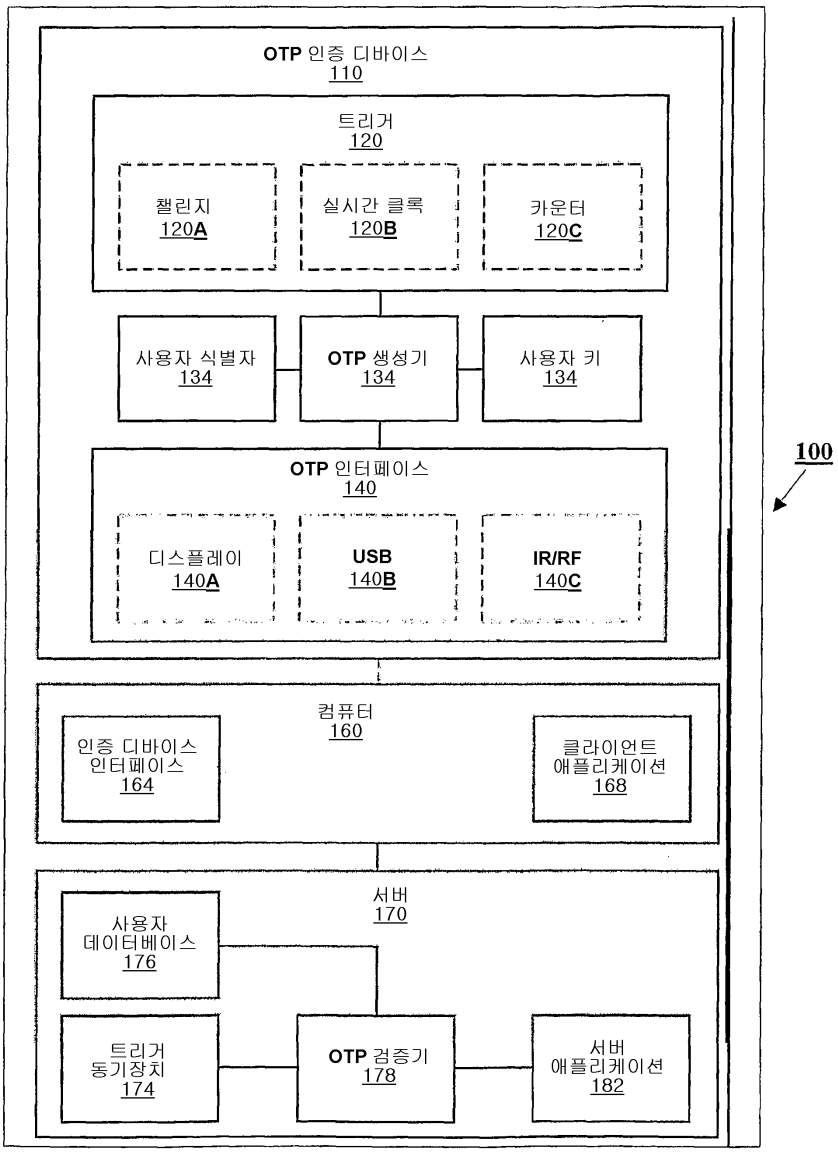
<66> 도 4A는 본 발명의 일실시예에 따라 OTP 디바이스(110)에 의해 생성된 OTP로 클라이언트-서버 세션을 시작하는 루틴의 플로우 도를 제공한다.

<67> 도 4B는 OTP 토큰으로부터의 세션 OTP 전송을 핸들링하는 루틴의 플로우도를 제공한다.

<68> 본 발명이 다수의 실시예와 예시적인 도면으로 본문에서 예시의 방식에 의해 기술되었지만, 당업자는 본 발명이 기술된 실시예 또는 도면에 한정되지 않음을 이해할 것이다. 그에 대한 도면과 상세한 설명은 기술된 특정한 형태로 본 발명을 한정하는 것을 의도하지 않고, 본 발명은 본 발명의 취지와 범위 내에서 모든 변형, 등가물, 및 대안을 포함한다는 것을 이해해야한다. 본 출원서 전체에서 사용되는, "할수있다"는 단어는 허용의 의미(즉, "~을 할 가능성이 있다")로 사용되고, 강제적인 의미(즉, "~해야한다")로 사용되는 것은 아니다.

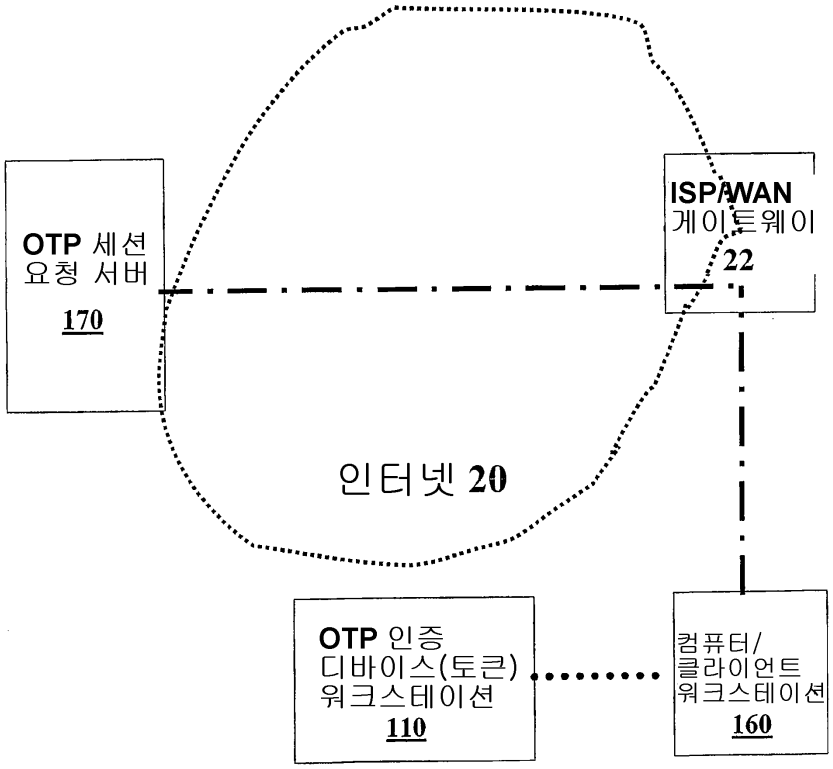
도면

도면1A


OTP 인증 디바이스
110
트리거
120
챌린지
120A
실시간 클록
120B
카운터
120C
사용자 식별자
134
OTP 생성기
134
사용자 키
134
OTP 인터페이스
140
디스플레이
140A
USB
140B
IR/RF
140C
100
컴퓨터
160
인증 디바이스
인터페이스
164
클라이언트
애플리케이션
168
서버
170
사용자
데이터베이스
176
트리거
동기장치
174
OTP 검증기
178
서버
애플리케이션
182

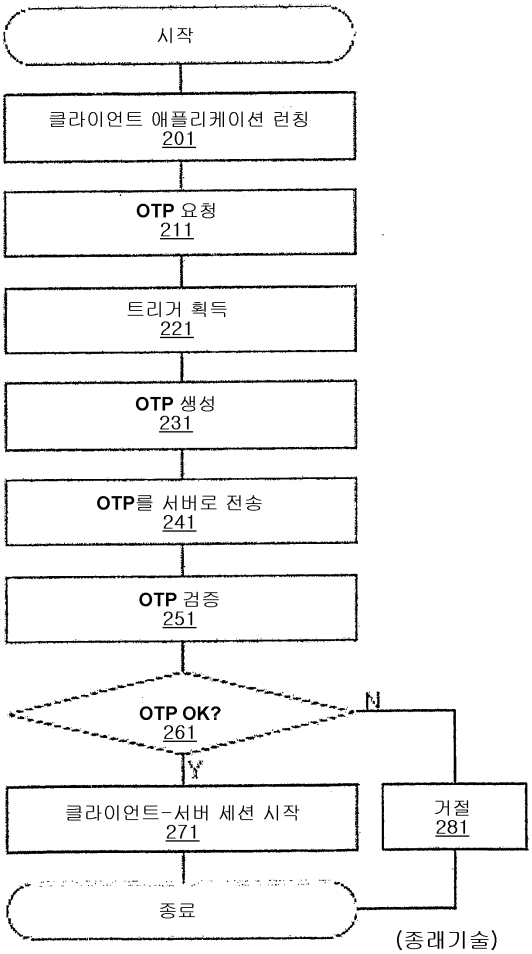
(종래기술)

도면1B


OTP 세션
요청 서버
170
ISP/WAN
게이트웨이
22
인터넷 20
OTP 인증
디바이스(토큰)
워크스테이션
110
컴퓨터/
클라이언트
워크스테이션
160

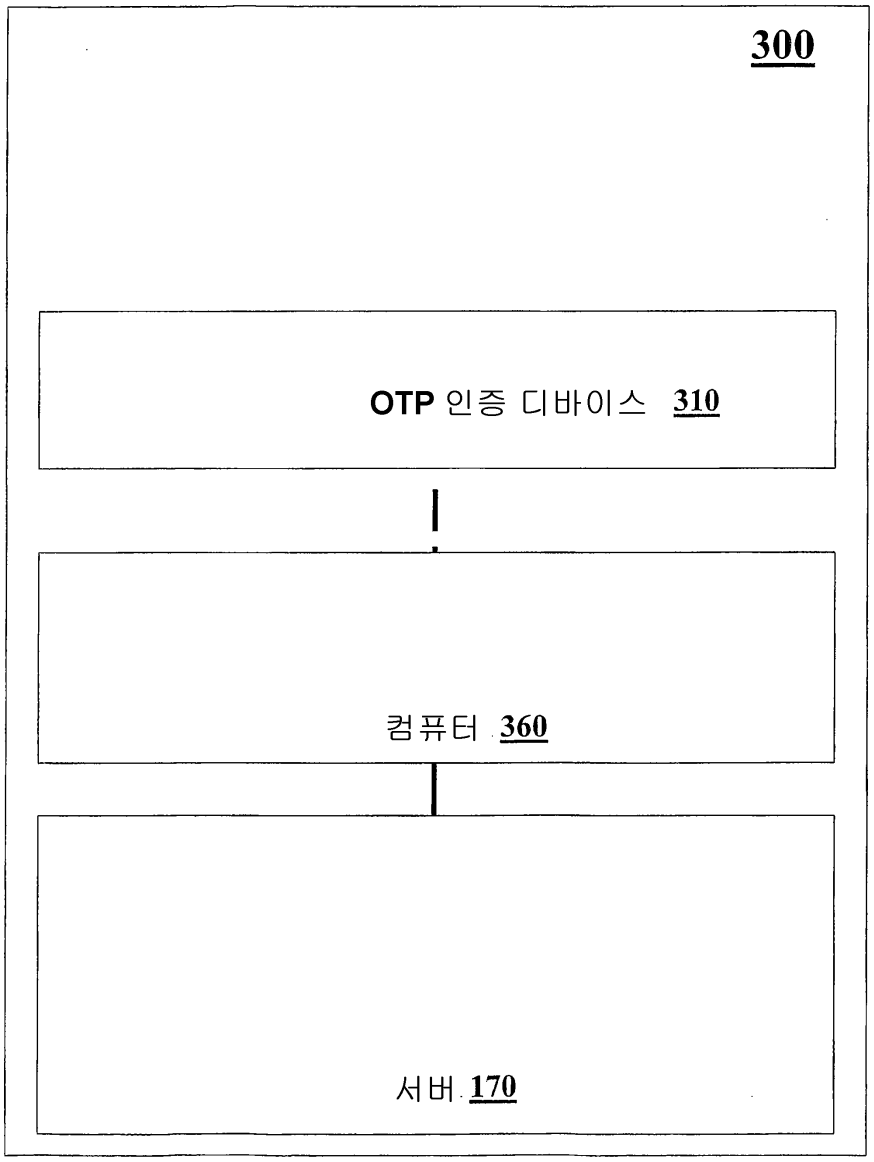
(종래기술)

도면2

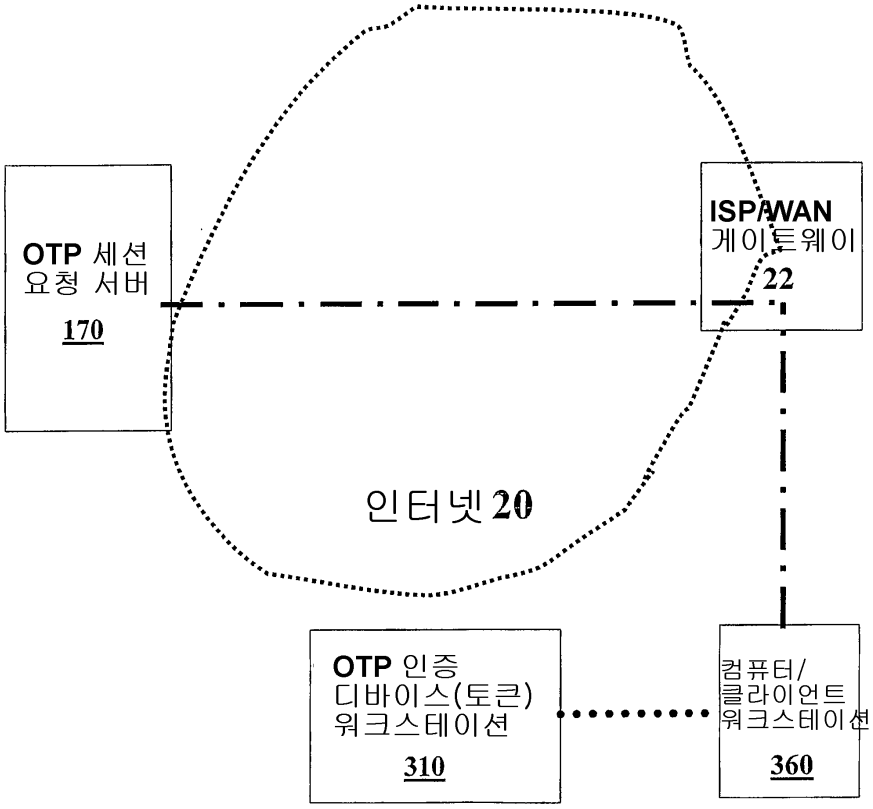

시작
클라이언트 애플리케이션 런칭
201
OTP 요청
211
트리거 획득
221
OTP 생성
231
OTP를 서버로 전송
241
OTP 검증
251
OTP OK?
261
N
Y
클라이언트-서버 세션 시작
271
거절
281
종료

(종래기술)

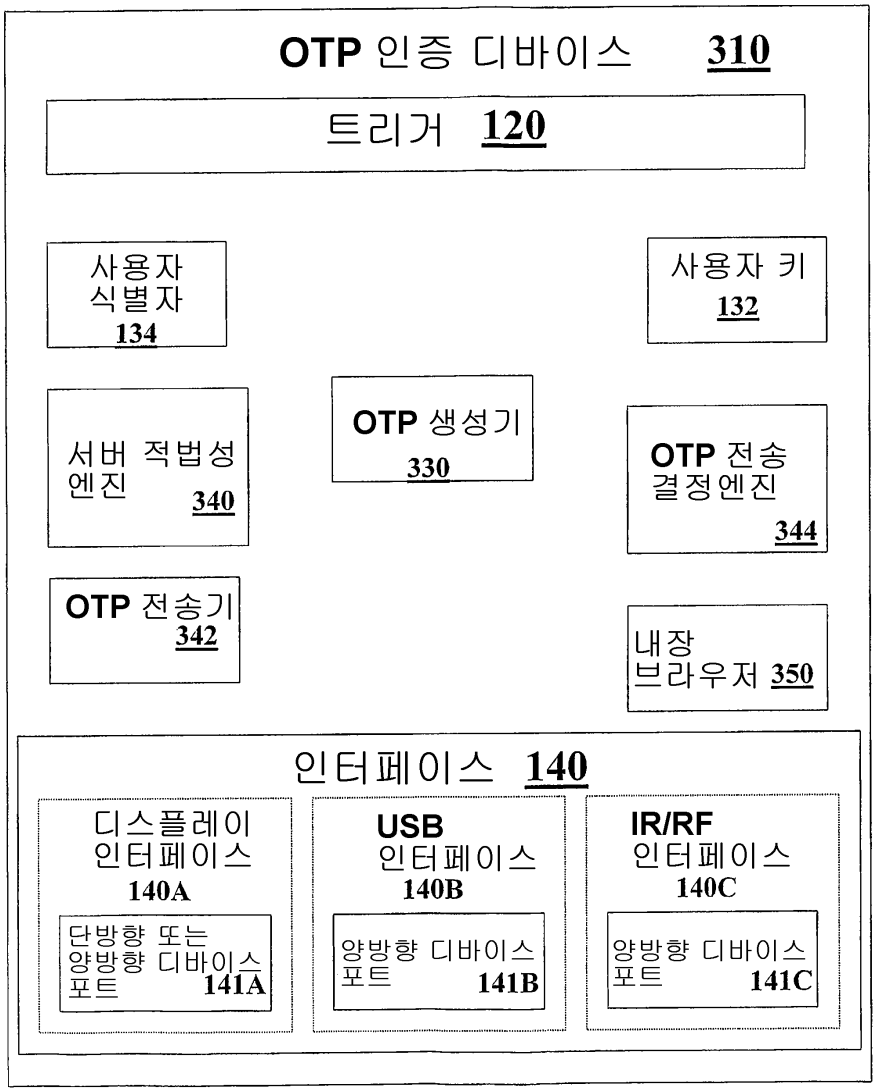
도면3A



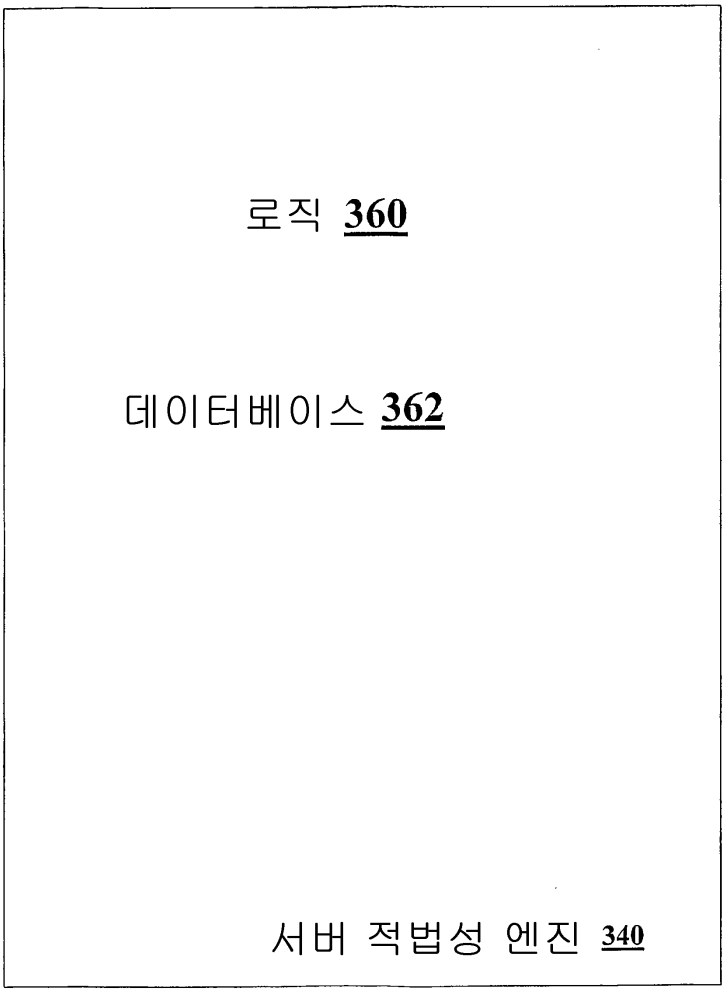
도면3B


OTP 세션
요청 서버
170
ISP/WAN
게이트웨이
22
인터넷 20
OTP 인증
디바이스(토큰)
워크스테이션
310
컴퓨터/
클라이언트
워크스테이션
360

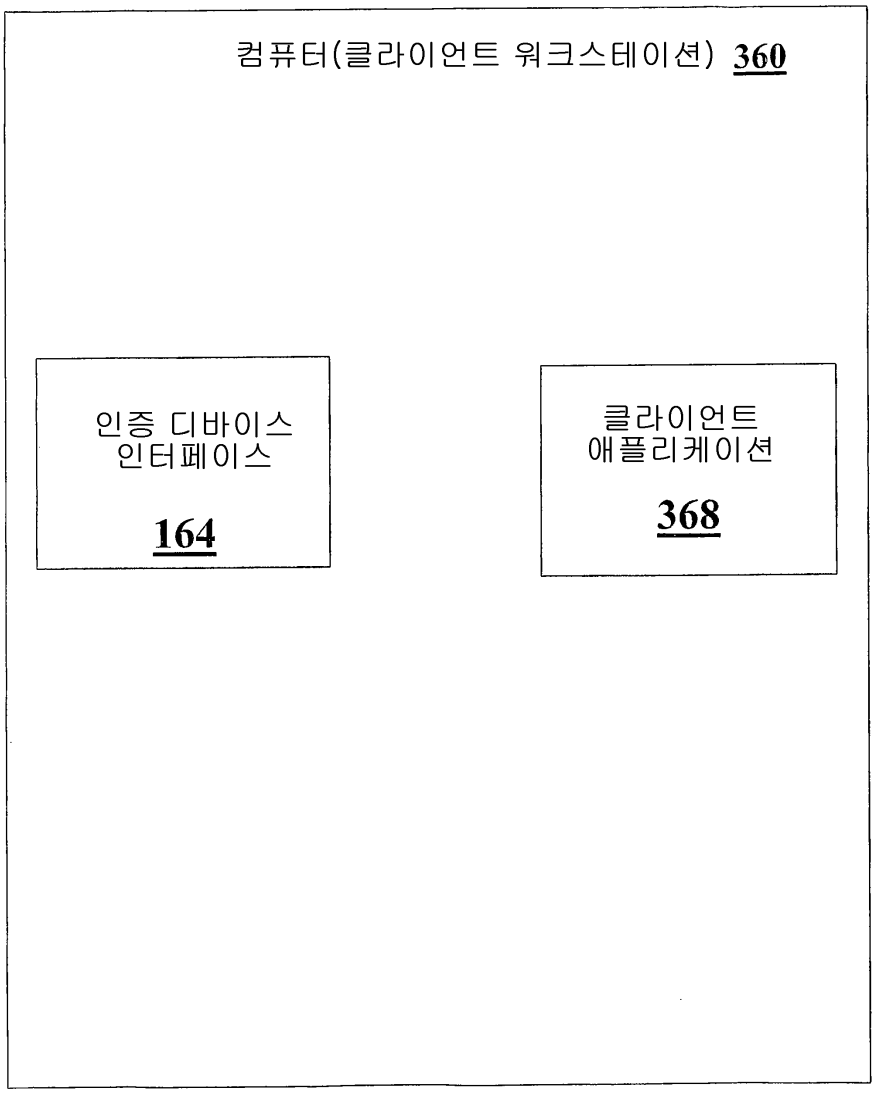
도면3C


OTP 인증 디바이스 310
트리거 120
사용자 식별자 134
사용자 키 132
서버 적법성 엔진 340
OTP 생성기 330
OTP 전송 결정엔진 344
OTP 전송기 342
내장 브라우저 350
인터페이스 140
디스플레이 인터페이스 140A
단방향 또는 양방향 디바이스 포트 141A
USB 인터페이스 140B
양방향 디바이스 포트 141B
IR/RF 인터페이스 140C
양방향 디바이스 포트 141C

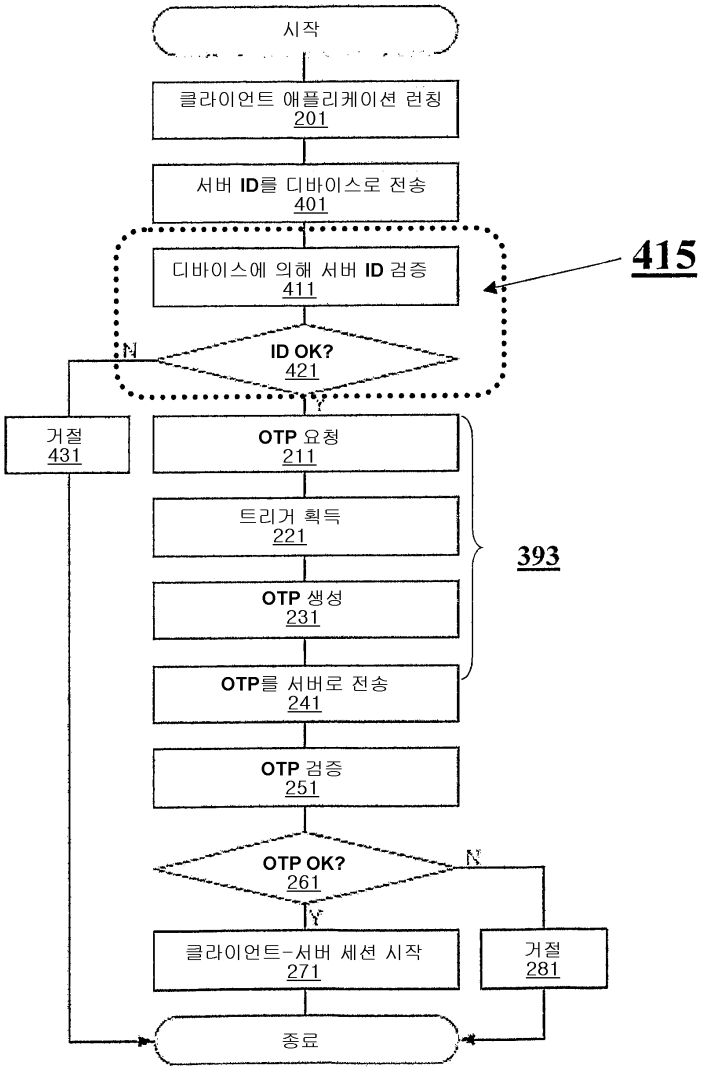
도면3D



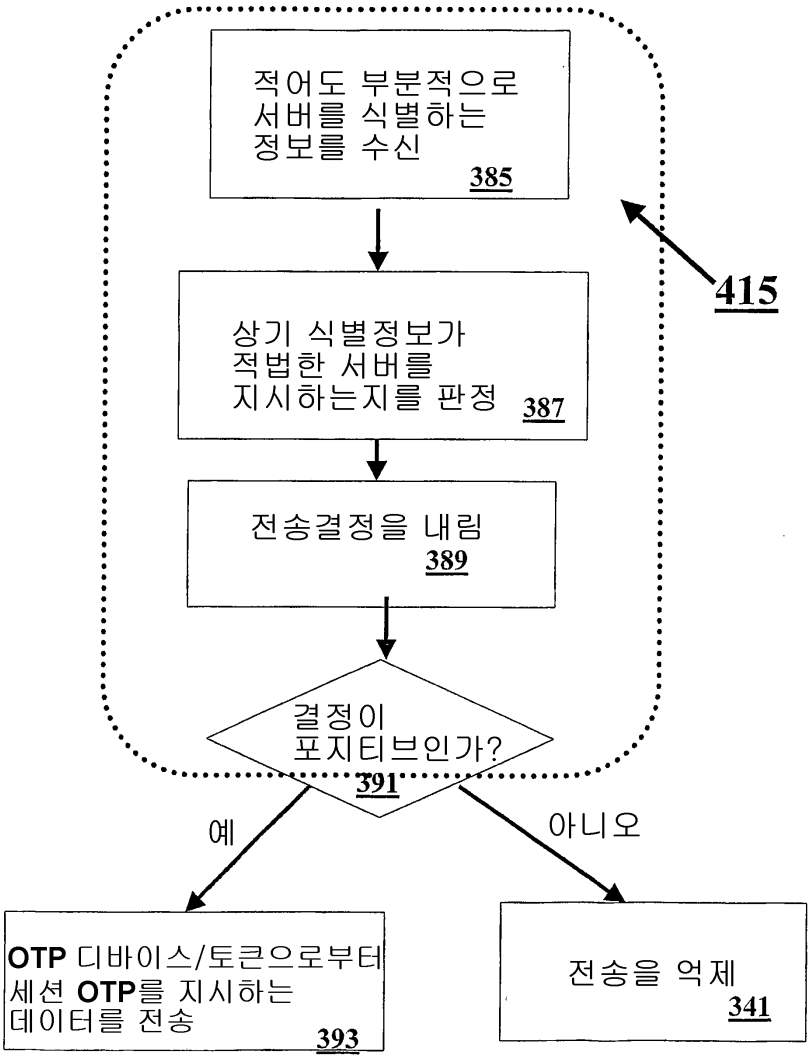
도면3E



도면4A


시작
클라이언트 애플리케이션 런칭
201
서버 ID를 디바이스로 전송
401
디바이스에 의해 서버 ID 검증
411
415
ID OK?
421
N
Y
거절
431
OTP 요청
211
트리거 획득
221
393
OTP 생성
231
OTP를 서버로 전송
241
OTP 검증
251
OTP OK?
261
N
Y
클라이언트-서버 세션 시작
271
거절
281
종료

도면4B


적어도 부분적으로 서버를 식별하는 정보를 수신
385
415
상기 식별정보가 적법한 서버를 지시하는지를 판정
387
전송결정을 내림
389
결정이 포지티브인가?
391
예
아니오
OTP 디바이스/토큰으로부터 세션 OTP를 지시하는 데이터를 전송
393
전송을 억제
341