(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년09월06일
(11) 등록번호 10-1651607
(24) 등록일자 2016년08월22일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *H04W 12/08* (2009.01)
(21) 출원번호 10-2014-0060505
(22) 출원일자 2014년05월20일
심사청구일자 2014년09월03일
(65) 공개번호 10-2015-0133938
(43) 공개일자 2015년12월01일
(56) 선행기술조사문헌
KR1020100069398 A
KR1020090020778 A

(73) 특허권자
주식회사 케이티
경기도 성남시 분당구 불정로 90(정자동)
(72) 발명자
이종건
서울특별시 강동구 선사로 120 102동 1003호 (암사동,한솔솔파크더리버)
김봉기
충청북도 청주시 흥덕구 대농로 17 108동 2304호 (복대동,신영지웰시티1차)
(뒷면에 계속)
(74) 대리인
특허법인충정

전체 청구항 수 : 총 16 항 심사관 : 이상윤

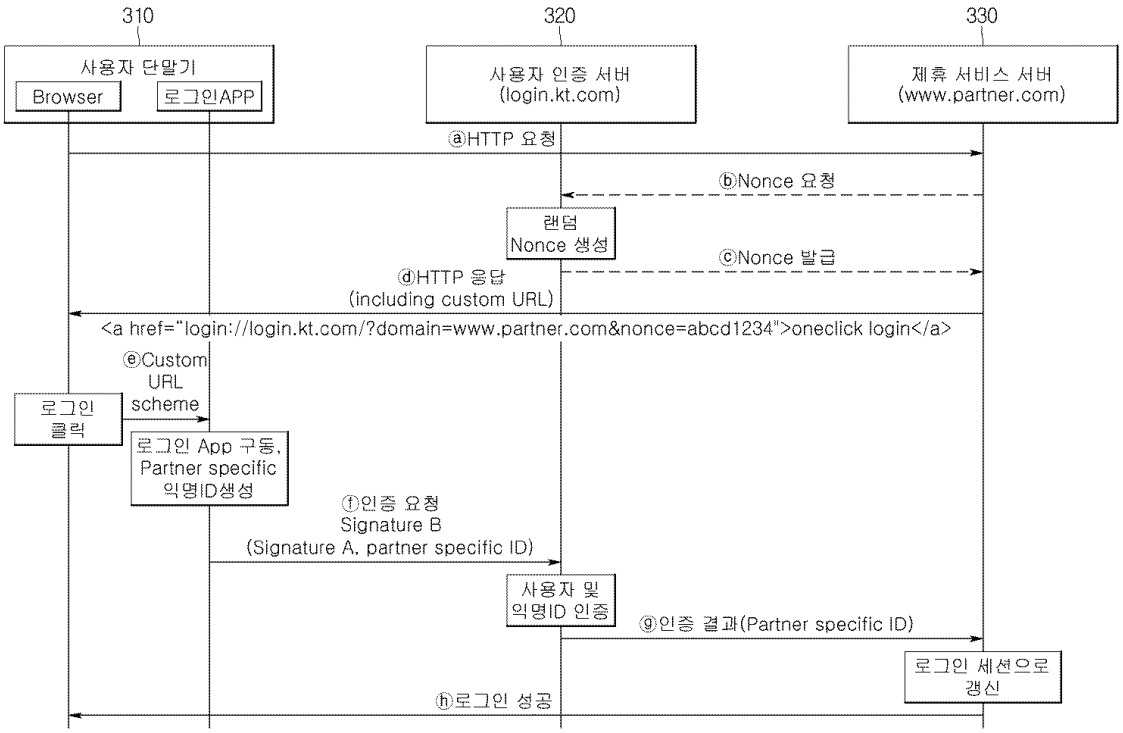
(54) 발명의 명칭 **익명 아이디를 사용하는 원클릭 사용자 인증 방법 및 시스템**

(57) 요 약

본 발명은 온라인 웹사이트 등을 포함하는 다양한 서비스에서의 사용자 인증 방법 및 시스템에 관한 것이다. 본 발명은 (a) 사용자 단말기가 제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하는 단계; (b) 사용자 인증 서버가 상기 제휴 서비스 서버로부터 상기 사용자에 대응하는 무작위 임시어(Nonce)를 요청받고, 이를 생성하여 상

(뒷면에 계속)

대 표 도



기 제휴 서비스 서버로 전달하는 단계; (c) 상기 사용자 단말기가 상기 제휴 서비스 서버로부터 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 인증 정보를 전달받는 단계; (d) 사용자가 사용자 인터페이스(User Interface)를 통하여 상기 제휴 서비스에서의 사용자 인증을 시도하면, 사용자 단말기가 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 단계; 및 (e) 사용자 인증 서버가 암호화되어 전달된 상기 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 각 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 (b) 단계에서 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법을 개시한다.

(72) 발명자

박재성

서울특별시 서대문구 홍제내길 168 101동 902호 (홍제동,남양아파트)

박태민

경기도 안양시 동안구 학의로 390 111동 2203호 (평촌동,푸른마을대우아파트)

명 세 서

청구범위

청구항 1

(a) 사용자 단말기가 제휴 서비스 서버로 소정의 서비스의 제공을 요청하는 단계;

(b) 사용자 인증 서버가 상기 제휴 서비스 서버로부터 상기 사용자에 대응하는 무작위 임시어(Nonce)를 요청받고, 이를 생성하여 상기 제휴 서비스 서버로 전달하는 단계;

(c) 상기 사용자 단말기가 상기 제휴 서비스 서버로부터 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 인증 정보를 전달받는 단계;

(d) 사용자가 사용자 인터페이스(User Interface)를 통하여 상기 제휴 서비스에서의 사용자 인증을 시도하면, 사용자 단말기가 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 단계; 및

(e) 사용자 인증 서버가 암호화되어 전달된 상기 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 각 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 (b) 단계에서 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 2

(a) 사용자가 사용자 인터페이스(User Interface)를 통하여 제휴 서비스 서버에서 제공하는 소정의 서비스에서의 사용자 인증을 시도하면, 사용자 단말기가 상기 제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하는 단계;

(b) 사용자 인증 서버가 상기 제휴 서비스 서버로부터 상기 사용자에 대응하는 무작위 임시어(Nonce)를 요청받고, 이를 생성하여 상기 제휴 서비스 서버로 전달하는 단계;

(c) 상기 사용자 단말기가 상기 제휴 서비스 서버로부터 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 일련의 정보를 전달받는 단계;

(d) 사용자 단말기가 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 단계; 및

(e) 사용자 인증 서버가 암호화되어 전달된 상기 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 각 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 (b) 단계에서 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 3

제1항 또는 제2항 중 어느 한 항에 있어서,

사용자가 한번의 클릭 동작만을 통하여 상기 소정의 서비스에서의 사용자 인증을 시도하는 것을 특징으로 하는 사용자 인증 방법.

청구항 4

제3항에 있어서,

상기 제휴 서비스 서버는 웹서버이고,

상기 사용자 단말기에서는 웹브라우저 프로그램이 구동되며,

이때 사용자가 상기 제휴 서비스 서버의 웹사이트에서의 사용자 인증을 위하여 마련된 소정의 버튼을 클릭하는 경우,

상기 사용자 단말기의 이미 구동되고 있던 또는 새롭게 구동되는 사용자 인증 어플리케이션이 사용자 인증 절차를 수행하는 것을 특징으로 하는 사용자 인증 방법.

청구항 5

제4항에 있어서,

상기 (c) 단계에 있어,

상기 사용자 단말기는 수정된 자원위치지정자 구조(custom URL scheme)를 이용하여 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 전달받는 것을 특징으로 하는 사용자 인증 방법.

청구항 6

제1항 또는 제2항 중 어느 한 항에 있어서,

상기 (e) 단계에 이어서,

(f) 제휴 서비스 서버가 상기 사용자 인증 서버로부터 전달받은 검증 결과를 바탕으로 상기 사용자 단말기로 서비스를 제공하는 단계를 더 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 7

제1항 또는 제2항 중 어느 한 항에 있어서,

상기 (d) 단계는,

(d1) 상기 제휴 서비스 서버의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하여 제1 개인키(Private key)와 제1 공용키(Public key)를 생성하는 단계;

(d2) 상기 무작위 임시어(Nonce)를 상기 제1 개인키(Private key)로 암호화하여 제1 전자서명을 생성하는 단계; 및

(d3) 상기 사용자 인증 서버의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하여 생성된 제2 개인키를 사용하여,

상기 제1 전자서명 및 제1 공용키를 묶은 하나의 데이터를 암호화하여 제2 전자서명을 생성하고, 이를 상기 사용자 인증 서버로 전달하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 8

제7 항에 있어서,

상기 (e) 단계는,

(e1) 상기 사용자 인증 서버의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하여 생성된 제2 공용키로서, 사용자가 상기 사용자 인증 서버의 인증 서비스에 가입할 때 등록된 상기 제2 공용키를 사용하여,

상기 사용자 인증 서버로 전달된 제2 전자서명을 복호화하여 제1 전자서명과 제1 공용키를 산출하는 단계;

(e2) 상기 제1 공용키를 사용하여 상기 제1 전자서명을 복호화하여 무작위 임시어(Nonce)를 산출한 후, 이를 상기 (b) 단계에서 생성된 무작위 임시어(Nonce)와 비교하여 일치 여부를 검증하는 단계를 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 9

제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하고,

상기 제휴 서비스 서버로부터 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 사용자 인증 서버의 식별 정보를 포함하는 일련의 정보를 전달받은 후,

사용자가 사용자 인터페이스(User Interface)를 통하여 상기 제휴 서비스 서버에서 제공하는 소정의 서비스에서

의 사용자 인증을 시도하는 경우, 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 사용자 단말기; 및

상기 제휴 서비스 서버로부터 상기 사용자에 대응하는 무작위 임시어(Nonce)를 요청받아, 이를 생성하여 상기 제휴 서비스 서버로 전달하며,

상기 사용자 단말기로부터 암호화되어 전달된 상기 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 각 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 사용자 인증 서버가 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 사용자 인증 서버를 포함하여 구성되는 것을 특징으로 하는 사용자 인증 시스템.

청구항 10

사용자가 사용자 인터페이스(User Interface)를 통하여 제휴 서비스 서버에서 제공하는 소정의 서비스에서의 사용자 인증을 시도하는 경우, 상기 제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하고,

상기 제휴 서비스 서버로부터 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 사용자 인증 서버의 식별 정보를 포함하는 일련의 정보를 전달받은 후,

상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 사용자 단말기; 및

상기 제휴 서비스 서버로부터 상기 사용자에 대응하는 무작위 임시어(Nonce)를 요청받아, 이를 생성하여 상기 제휴 서비스 서버로 전달하며,

상기 사용자 단말기로부터 암호화되어 전달된 상기 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 각 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 사용자 인증 서버가 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 사용자 인증 서버를 포함하여 구성되는 것을 특징으로 하는 사용자 인증 시스템.

청구항 11

제9항 또는 제10항 중 어느 한 항에 있어서,

상기 제휴 서비스 서버는 웹서버이고,

상기 사용자 단말기에서는 웹브라우저 프로그램이 구동되며,

이때 사용자가 상기 제휴 서비스 서버의 웹사이트에서의 사용자 인증을 위하여 마련된 소정의 버튼을 클릭하는 경우,

상기 사용자 단말기의 이미 구동되고 있던 또는 새롭게 구동되는 사용자 인증 어플리케이션이 사용자 인증 절차를 수행하는 것을 특징으로 하는 것을 특징으로 하는 사용자 인증 시스템.

청구항 12

제9항 또는 제10항 중 어느 한 항에 있어서,

상기 사용자 단말기가 상기 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달함에 있어,

상기 제휴 서비스 서버의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하여 제1 개인키(Private key)와 제1 공용키(Public key)를 생성하고,

상기 무작위 임시어(Nonce)를 상기 제1 개인키(Private key)로 암호화하여 제1 전자서명을 생성한 후,

상기 사용자 인증 서버의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하여 생성된 제2 개인키를 사용하여, 상기 제1 전자서명 및 제1 공용키를 묶은 하나의 데이터를 암호화하여 제2 전자서명을 생성하고, 이를 상기 사용자 인증 서버로 전달하는 것을 특징으로 하는 사용자 인증 시스템.

청구항 13

제12항에 있어서,

상기 사용자 인증 서버가 암호화되어 전달된 상기 인증 정보를 복호화함에 있어,

상기 사용자 인증 서버의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하여 생성된 제2 공용키로서, 사용자가 상기 사용자 인증 서버의 인증 서비스에 가입할 때 등록된 상기 제2 공용키를 사용하여,

상기 사용자 인증 서버로 전달된 제2 전자서명을 복호화하여 제1 전자서명과 제1 공용키를 산출하고,

상기 제1 공용키를 사용하여 상기 제1 전자서명을 복호화하여 무작위 임시어(Nonce)를 산출하는 것을 특징으로 하는 사용자 인증 시스템.

청구항 14

사용자 단말기에 있어서,

제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하고,

상기 제휴 서비스 서버로부터 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 사용자 인증 서버의 식별 정보를 포함하는 일련의 정보를 전달받은 후,

사용자가 사용자 인터페이스(User Interface)를 통하여 상기 제휴 서비스 서버에서 제공하는 소정의 서비스에서의 사용자 인증을 시도하는 경우, 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 것을 특징으로 하며,

이때 상기 사용자 인증 서버는,

상기 제휴 서비스 서버로부터 상기 사용자에 대응하는 무작위 임시어(Nonce)를 요청받아, 이를 생성하여 상기 제휴 서비스 서버로 전달하며,

상기 사용자 단말기로부터 암호화되어 전달된 상기 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 각 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 사용자 인증 서버가 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 서버인 것을 특징으로 하는 사용자 단말기.

청구항 15

사용자 단말기에 있어서,

사용자가 사용자 인터페이스(User Interface)를 통하여 제휴 서비스 서버에서 제공하는 소정의 서비스에서의 사용자 인증을 시도하는 경우, 상기 제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하고,

상기 제휴 서비스 서버로부터 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 사용자 인증 서버의 식별 정보를 포함하는 일련의 정보를 전달받은 후,

상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 것을 특징으로 하며,

이때 상기 사용자 인증 서버는,

상기 제휴 서비스 서버로부터 상기 사용자에 대응하는 무작위 임시어(Nonce)를 요청받아, 이를 생성하여 상기 제휴 서비스 서버로 전달하며,

상기 사용자 단말기로부터 암호화되어 전달된 상기 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 각 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 사용자 인증 서버가 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 서버인 것을 특징으로 하는 사용자 단말기.

청구항 16

사용자 인증 서버에 있어서,

제휴 서비스 서버로부터 사용자에 대응하는 무작위 임시어(Nonce)를 요청받아, 이를 생성하여 상기 제휴 서비스 서버로 전달하며,

상기 사용자의 단말로부터 암호화되어 전달된 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 사용자 인증 서버가 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 서버인 것을 특징으로 하며,

이때 상기 사용자의 단말은,

사용자가 사용자 인터페이스(User Interface)를 통하여 제휴 서비스 서버에서 제공하는 소정의 서비스에서의 사용자 인증을 시도하는 경우, 상기 제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하고,

상기 제휴 서비스 서버로부터 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 사용자 인증 서버의 식별 정보를 포함하는 일련의 정보를 전달받은 후,

상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하거나,

또는,

제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하고,

상기 제휴 서비스 서버로부터 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 사용자 인증 서버의 식별 정보를 포함하는 일련의 정보를 전달받은 후,

사용자가 사용자 인터페이스(User Interface)를 통하여 상기 제휴 서비스 서버에서 제공하는 소정의 서비스에서의 사용자 인증을 시도하는 경우, 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 것을 특징으로 하는 사용자 인증 서버.

발명의 설명

기 술 분 야

[0001] 본 발명은 온라인 웹사이트 등을 포함하는 다양한 서비스에서의 사용자 인증 방법 및 시스템에 관한 것으로서, 구체적으로는 사용자가 직접 아이디와 패스워드를 입력함이 없이 한번의 클릭만으로 익명의 아이디를 사용하여 온라인 웹사이트 등에서 사용자를 인증하는 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 근래 통신 기술과 서비스가 지속적으로 발전하면서, 수많은 사용자들이 개인용 컴퓨터(PC) 혹은 스마트폰 등의 휴대용 단말기를 이용하여 다양한 서비스를 이용하고 있다. 예를 들어, 종래 사용자들은 개인용 컴퓨터(PC) 혹은 스마트폰을 이용하여 채팅 서비스를 이용하거나, 특정 웹 서비스를 이용하거나, 타 사용자와 이메일을 주고받는 서비스를 이용하여 왔다.

[0003] 이때, 사용자는 개인용 컴퓨터(PC) 혹은 스마트폰을 기반으로 동작하는 다양한 어플리케이션들을 이용하여 특정 통신 서비스를 이용하게 된다. 그런데 이 과정에서 사용자는 각각의 어플리케이션이 제공하는 특정 통신 서비스 이용을 위해서는 해당 어플리케이션 운용을 지원하는 서비스 장치와 인증 과정을 수행하여 정당한 사용자인지를 확인하고 이용 권한을 획득해야 한다. 이러한 인증 과정은 각 사용자들의 정상적인 통신 서비스 이용 및 보안을 위해서 필수적으로 거쳐야 하는 과정이라 할 수 있다.

[0004] 그런데, 이러한 사용자 인증 과정은 때로는 사용자에게 매우 큰 불편함을 주는 경우가 있다. 이를테면 사용자는 복수의 특정 어플리케이션 기반의 통신 서비스 이용을 위하여 각각의 서비스 장치와 인증 정보를 송수신하고 이를 인증받는 과정을 개별적으로 수행해야 하므로, 사용자가 불편한 인증 정보 입력 과정을 반복적으로 수행하여야 한다는 문제가 있었다.

[0005] 이에 대하여, 오픈 아이디/싱글 사인온(Open ID/SSO) 등을 이용하여 복수의 웹 사이트 등을 한번의 로그인 과정

을 통하여 통합 로그인할 수 있도록 하는 방법이 시도되었다. 예를 들어 대한민국 공개특허 제 10-2010-0040413호(2010년 4월 20일 공개)에서는 오픈 아이디(Open ID)를 지원하는 단일 사용승인 아이디 인증 방법에 대하여 개시하고 있고, 도 1에서는 이에 따르는 오픈 아이디(Open ID)를 지원하는 단일 사용승인 아이디 인증 방법의 일실시예에 대한 흐름도를 보여주고 있다.

[0006] 그러나, 상기한 오픈 아이디/싱글 사인온(Open ID/SSO) 등을 이용하는 로그인 방법에도 여전히 여러가지 문제점이 존재하게 된다. 예를 들어, 오픈 아이디/싱글 사인온(Open ID/SSO)은 모든 사이트/어플리케이션에 대하여 하나의 계정(ID)를 사용하게 됨으로써 각 사이트/어플리케이션에서 동일 사용자임이 쉽게 드러날 수 있어 익명성을 보장하기 어렵게 되고, 또한 최소한 한번의 계정(ID) 및 비밀번호(Password)를 입력하여야 하므로 키스트로킹(keystroking) 등의 해킹 위험성에 노출될 수 있으며, 특히 스마트폰 등을 사용하는 경우 텍스트 기반의 사용자 인증 방식은 사용자 인터페이스(User Interface) 측면에서 상당한 불편함을 초래하게 된다.

[0007] 이에 따라, 복수의 사이트/어플리케이션에서의 익명성을 보장할 수 있고, 텍스트 기반의 사용자 인증 절차에 따르는 키스트로킹(keystroking) 등의 해킹 위험을 방지할 수 있으며, 나아가 스마트폰 등을 사용하는 경우에도 간편하게 사용자 인증 절차를 수행할 수 있는 사용자 인터페이스를 제공하는 사용자 인증 방법 및 시스템이 요구되고 있으나, 아직 이에 대한 적절한 해결책이 제시되지 못하고 있는 실정이다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 상기와 같은 종래 기술의 문제점을 해결하기 위해 창안된 것으로, 복수의 사이트/어플리케이션에서의 익명성을 보장할 수 있고, 텍스트 기반의 사용자 인증 절차에 따르는 키스트로킹(keystroking) 등의 해킹 위험을 방지할 수 있으며, 나아가 스마트폰 등을 사용하는 경우에도 간편하게 사용자 인증 절차를 수행할 수 있는 사용자 인터페이스를 제공하는 사용자 인증 방법 및 시스템을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0009] 상기 과제를 해결하기 위한 본 발명의 한 측면에 따른 사용자 인증 방법은 (a) 사용자 단말기가 제휴 서비스 서버로 서비스의 제공을 요청하는 단계; (b) 사용자 인증 서버가 상기 제휴 서비스 서버로부터 상기 사용자에 대응하는 무작위 임시어(Nonce)를 요청받고, 이를 생성하여 상기 제휴 서비스 서버로 전달하는 단계; (c) 상기 사용자 단말기가 상기 제휴 서비스 서버로부터 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 인증 정보를 전달받는 단계; (d) 사용자가 사용자 인터페이스(User Interface)를 통하여 상기 제휴 서비스에서의 사용자 인증을 시도하면, 사용자 단말기가 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 단계; 및 (e) 사용자 인증 서버가 암호화되어 전달된 상기 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 각 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 (b) 단계에서 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 단계를 포함하는 것을 특징으로 한다.

[0010] 본 발명의 다른 측면에 따른 사용자 인증 방법은 (a) 사용자가 사용자 인터페이스(User Interface)를 통하여 제휴 서비스 서버에서 제공하는 소정의 서비스에서의 사용자 인증을 시도하면, 사용자 단말기가 상기 제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하는 단계; (b) 사용자 인증 서버가 상기 제휴 서비스 서버로부터 상기 사용자에 대응하는 무작위 임시어(Nonce)를 요청받고, 이를 생성하여 상기 제휴 서비스 서버로 전달하는 단계; (c) 상기 사용자 단말기가 상기 제휴 서비스 서버로부터 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 일련의 정보를 전달받는 단계; (d) 사용자 단말기가 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 단계; 및 (e) 사용자 인증 서버가 암호화되어 전달된 상기 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 각 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 (b) 단계에서 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 단계를 포함하는 것을 특징으로 한다.

[0011] 여기서, 사용자는 한번의 클릭 동작만을 통하여 상기 소정의 서비스에서의 사용자 인증을 시도할 수 있다.

[0012] 또한, 상기 제휴 서비스 서버는 웹서버이고, 상기 사용자 단말기에서는 웹브라우저 프로그램이 구동되며, 이때

사용자가 상기 제휴 서비스 서버의 웹사이트에서의 사용자 인증을 위하여 마련된 소정의 버튼을 클릭하는 경우, 상기 사용자 단말기의 이미 구동되고 있던 또는 새롭게 구동되는 사용자 인증 어플리케이션이 사용자 인증 절차를 수행할 수 있다.

[0013] 또한, 상기 사용자 단말기는 수정된 자원위치지정자 구조(custom URL scheme)를 이용하여 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 전달받을 수 있다.

[0014] 또한, 상기 (e) 단계에 이어서, (f) 제휴 서비스 서버가 상기 사용자 인증 서버로부터 전달받은 검증 결과를 바탕으로 상기 사용자 단말기로 서비스를 제공하는 단계를 더 포함할 수 있다.

[0015] 또한, 상기 (d) 단계는, (d1) 상기 제휴 서비스 서버의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하여 제1 개인키(Private key)와 제1 공용키(Public key)를 생성하는 단계; (d2) 상기 무작위 임시어(Nonce)를 상기 제1 개인키(Private key)로 암호화하여 제1 전자서명을 생성하는 단계; 및 (d3) 상기 사용자 인증 서버의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하여 생성된 제2 개인키를 사용하여, 상기 제1 전자서명 및 제1 공용키를 묶은 하나의 데이터를 암호화하여 제2 전자서명을 생성하여 상기 사용자 인증 서버로 전달하는 단계를 포함할 수 있다.

[0016] 또한, 상기 (e) 단계는, (e1) 상기 사용자 인증 서버의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하여 생성되어, 사용자가 상기 사용자 인증 서버의 인증 서비스에 가입할 때 등록된 제2 공용키를 사용하여, 상기 사용자 인증 서버로 전달된 제2 전자서명을 복호화하여 제1 전자서명과 제1 공용키를 산출하는 단계; (e2) 상기 제1 공용키를 사용하여 상기 제1 전자서명을 복호화하여 무작위 임시어(Nonce)를 산출한 후, 이를 상기 (b) 단계에서 생성된 무작위 임시어(Nonce)와 비교하여 일치 여부를 검증하는 단계를 포함할 수 있다.

[0017] 본 발명의 또 다른 측면에 따른 사용자 인증 시스템은, 제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하고, 상기 제휴 서비스 서버로부터 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 사용자 인증 서버의 식별 정보를 포함하는 일련의 정보를 전달받은 후, 사용자가 사용자 인터페이스(User Interface)를 통하여 상기 제휴 서비스 서버에서 제공하는 소정의 서비스에서의 사용자 인증을 시도하는 경우, 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 사용자 단말기; 및 상기 제휴 서비스 서버로부터 상기 사용자에 대응하는 무작위 임시어(Nonce)를 요청받아, 이를 생성하여 상기 제휴 서비스 서버로 전달하며, 상기 사용자 단말기로부터 암호화되어 전달된 상기 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 각 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 사용자 인증 서버가 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 사용자 인증 서버를 포함하여 구성되는 것을 특징으로 한다.

[0018] 본 발명의 또 다른 측면에 따른 사용자 인증 시스템은, 사용자가 사용자 인터페이스(User Interface)를 통하여 제휴 서비스 서버에서 제공하는 소정의 서비스에서의 사용자 인증을 시도하는 경우, 상기 제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하고, 상기 제휴 서비스 서버로부터 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 사용자 인증 서버의 식별 정보를 포함하는 일련의 정보를 전달받은 후, 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 사용자 단말기; 및 상기 제휴 서비스 서버로부터 상기 사용자에 대응하는 무작위 임시어(Nonce)를 요청받아, 이를 생성하여 상기 제휴 서비스 서버로 전달하며, 상기 사용자 단말기로부터 암호화되어 전달된 상기 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 각 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 사용자 인증 서버가 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 사용자 인증 서버를 포함하여 구성되는 것을 특징으로 한다.

[0019] 여기서, 상기 제휴 서비스 서버는 웹서버이고, 상기 사용자 단말기에서는 웹브라우저 프로그램이 구동되며, 이때 사용자가 상기 제휴 서비스 서버의 웹사이트에서의 사용자 인증을 위하여 마련된 소정의 버튼을 클릭하는 경우, 상기 사용자 단말기의 이미 구동되고 있던 또는 새롭게 구동되는 사용자 인증 어플리케이션이 사용자 인증 절차를 수행할 수 있다.

[0020] 또한, 상기 사용자 단말기가 상기 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달함에 있어, 상기 제휴 서비스 서버의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하

여 제1 개인키(Private key)와 제1 공용키(Public key)를 생성하고, 상기 무작위 임시어(Nonce)를 상기 제1 개인키(Private key)로 암호화하여 제1 전자서명을 생성한 후, 상기 사용자 인증 서버의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하여 생성된 제2 개인키를 사용하여, 상기 제1 전자서명 및 제1 공용키를 묶은 하나의 데이터를 암호화하여 제2 전자서명을 생성하여 상기 사용자 인증 서버로 전달할 수 있다.

[0021] 또한, 상기 사용자 인증 서버가 암호화되어 전달된 상기 인증 정보를 복호화함에 있어, 상기 사용자 인증 서버의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하여 생성되어, 사용자가 상기 사용자 인증 서버의 인증 서비스에 가입할 때 등록된 제2 공용키를 사용하여, 상기 사용자 인증 서버로 전달된 제2 전자서명을 복호화하여 제1 전자서명과 제1 공용키를 산출하고, 상기 제1 공용키를 사용하여 상기 제1 전자서명을 복호화하여 무작위 임시어(Nonce)를 산출할 수 있다.

[0022] 본 발명의 또 다른 측면에 따른 사용자 단말기는, 제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하고, 상기 제휴 서비스 서버로부터 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 사용자 인증 서버의 식별 정보를 포함하는 일련의 정보를 전달받은 후, 사용자가 사용자 인터페이스(User Interface)를 통하여 상기 제휴 서비스 서버에서 제공하는 소정의 서비스에서의 사용자 인증을 시도하는 경우, 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 것을 특징으로 하며, 이때 상기 사용자 인증 서버는, 상기 제휴 서비스 서버로부터 상기 사용자에 대응하는 무작위 임시어(Nonce)를 요청받아, 이를 생성하여 상기 제휴 서비스 서버로 전달하며, 상기 사용자 단말기로부터 암호화되어 전달된 상기 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 각 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 사용자 인증 서버가 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 서버인 것을 특징으로 한다.

[0023] 본 발명의 또 다른 측면에 따른 사용자 단말기는, 사용자가 사용자 인터페이스(User Interface)를 통하여 제휴 서비스 서버에서 제공하는 소정의 서비스에서의 사용자 인증을 시도하는 경우, 상기 제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하고, 상기 제휴 서비스 서버로부터 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 사용자 인증 서버의 식별 정보를 포함하는 일련의 정보를 전달받은 후, 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 것을 특징으로 하며, 이때 상기 사용자 인증 서버는, 상기 제휴 서비스 서버로부터 상기 사용자에 대응하는 무작위 임시어(Nonce)를 요청받아, 이를 생성하여 상기 제휴 서비스 서버로 전달하며, 상기 사용자 단말기로부터 암호화되어 전달된 상기 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 각 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 사용자 인증 서버가 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 서버인 것을 특징으로 한다.

[0024] 본 발명의 또 다른 측면에 따른 사용자 인증 서버는, 상기 제휴 서비스 서버로부터 상기 사용자에 대응하는 무작위 임시어(Nonce)를 요청받아, 이를 생성하여 상기 제휴 서비스 서버로 전달하며, 상기 사용자 단말기로부터 암호화되어 전달된 상기 인증 정보를 복호화하여 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 각 정보들을 산출한 후, 산출된 무작위 임시어(Nonce)가 상기 사용자 인증 서버가 생성한 무작위 임시어(Nonce)와 일치하는지 검증하고, 그 결과를 상기 제휴 서비스 서버로 전달하는 서버인 것을 특징으로 하며, 이때 상기 사용자 단말기는, 사용자가 사용자 인터페이스(User Interface)를 통하여 제휴 서비스 서버에서 제공하는 소정의 서비스에서의 사용자 인증을 시도하는 경우, 상기 제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하고, 상기 제휴 서비스 서버로부터 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 사용자 인증 서버의 식별 정보를 포함하는 일련의 정보를 전달받은 후, 상기 무작위 임시어(Nonce)와 상기 제휴 서비스 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하거나, 또는, 제휴 서비스 서버로 사용자 인증을 위한 정보를 요청하고, 상기 제휴 서비스 서버로부터 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 사용자 인증 서버의 식별 정보를 포함하는 일련의 정보를 전달받은 후, 사용자가 사용자 인터페이스(User Interface)를 통하여 상기 제휴 서비스 서버에서 제공하는 소정의 서비스에서의 사용자 인증을 시도하는 경우, 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 인증 정보를 암호화하여 상기 사용자 인증 서버로 전달하는 것을 특징으로 한다.

발명의 효과

[0025] 본 발명에 따르면, 사용자가 한번의 클릭 동작만으로 사용자 인증 요청을 할 수 있고, 이에 대하여 제휴 서비스 제공자와 원클릭 사용자 인증 서버가 익명 아이디를 사용하여 사용자 인증을 수행하도록 함으로써, 복수의 사이트/어플리케이션에서의 익명성을 보장할 수 있고, 텍스트 기반의 사용자 인증 절차에 따르는 키스트로킹(keystroking) 등의 해킹 위험을 방지할 수 있으며, 나아가 스마트폰 등을 사용하는 경우에도 편리하게 사용자 인증 절차를 수행할 수 있는 사용자 인터페이스를 제공하는 사용자 인증 방법 및 시스템을 구현하는 효과를 갖는다.

도면의 간단한 설명

[0026] 본 발명에 관한 이해를 돕기 위해 상세한 설명의 일부로 포함되는, 첨부도면은 본 발명에 대한 실시예를 제공하고, 상세한 설명과 함께 본 발명의 기술적 사상을 설명한다.

도 1은 종래 기술에 따른 오픈 아이디(Open ID)를 지원하는 단일 사용승인 아이디 인증 방법의 흐름도이다.

도 2는 종래 기술에 따른 텍스트 기반 로그인 사용자 인터페이스와 본 발명에 따른 원클릭 로그인 사용자 인터페이스의 비교도이다.

도 3은 본 발명의 일 실시예에 따른 익명 아이디를 사용하는 원클릭 사용자 인증 시스템의 구성 및 동작에 대한 설명도이다.

도 4는 본 발명의 일 실시예에 따른 익명 아이디를 사용하는 원클릭 사용자 인증 방법의 순서도이다.

도 5는 본 발명의 일 실시예에 따른 수정된 자원위치지정자 구조(custom URL scheme)의 예시도이다.

도 6은 본 발명의 일 실시예에 따른 원클릭 사용자 인증 방법에서의 인증 정보 암호화 및 복화화 과정에 대한 설명도이다.

발명을 실시하기 위한 구체적인 내용

[0027] 본 발명은 다양한 변환을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 이하에서는 특정 실시예들을 첨부된 도면을 기초로 상세히 설명하고자 한다.

[0028] 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0029] 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되는 것은 아니며, 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0030] 본 발명은, 종래 기술에 따라 오픈 아이디/싱글 사인온(Open ID/SSO) 등을 이용하는 통합 로그인 방법을 사용하는 경우 모든 사이트/어플리케이션에 대하여 하나의 계정(ID)를 사용하게 되어 각 사이트/어플리케이션에서 동일 사용자임이 쉽게 드러날 수 있어 익명성을 보장하기 어렵고, 또한 최소한 한번의 계정(ID) 및 비밀번호(Password)를 입력하여야 하므로 키스트로킹(keystroking) 등의 해킹 위험성에 노출될 수 있으며, 특히 스마트폰 등을 사용하는 경우 텍스트 기반의 사용자 인증 방식은 사용자 인터페이스(User Interface) 측면에서 상당한 불편함을 초래할 수 있다는 문제점에 착안하여, 사용자가 한번의 클릭 동작만으로 사용자 인증 요청을 할 수 있고, 이에 따라 제휴 서비스 제공자와 원클릭 사용자 인증 서버가 익명 아이디를 사용하여 사용자 인증을 수행하도록 함으로써, 복수의 사이트/어플리케이션에서의 익명성을 보장할 수 있고, 텍스트 기반의 사용자 인증 절차에 따르는 키스트로킹(keystroking) 등의 해킹 위험을 방지할 수 있으며, 나아가 스마트폰 등을 사용하는 경우에도 편리하게 사용자 인증 절차를 수행할 수 있는 사용자 인터페이스를 제공하는 사용자 인증 방법 및 시스템을 개시하는 것을 특징으로 한다.

[0031] 도 2에서는 종래 기술에 따른 텍스트 기반 로그인 사용자 인터페이스와 본 발명에 따른 원클릭 로그인 사용자 인터페이스의 비교도를 보여주고 있다. 도 2에서 볼 수 있는 바와 같이, 종래 기술에 따른 텍스트 기반 로그인 사용자 인터페이스(User Interface)의 경우 사용자가 계정(ID)와 비밀번호(Password)를 입력하여야 하는 불편함과 함께, 키스트로킹(keystroking) 등의 해킹 위험이 따르게 되지만, 본 발명에 따른 원클릭 로그인 사용자 인터페이스의 경우에는 스마트폰 등에서도 간편하게 한번의 클릭만으로 사용자 인증 절차를 수행할 수 있고, 사용

자가 직접 계정(ID)와 비밀번호(Password)를 입력할 필요가 없어 키스트로킹(keystroking) 등의 해킹 위험을 방지할 수 있게 된다.

[0032] 예를 들어, 통상의 웹사이트나 게임, 스마트폰 어플리케이션 등에서 사용되고 있는 종래 기술에 따른 텍스트 기반 로그인 사용자 인터페이스를 본 발명에 따른 원클릭 로그인 사용자 인터페이스로 대체하거나, 양 사용자 인터페이스를 병렬적으로 구성할 수도 있다.

[0033] 도 3에서는 본 발명의 일 실시예에 따른 익명 아이디를 사용하는 원클릭 사용자 인증 시스템(300)의 구성 및 동작에 대한 설명도를 도시하고 있다. 도 3에서 볼 수 있는 바와 같이, 본 발명의 일 실시예에 따른 익명 아이디를 사용하는 원클릭 사용자 인증 시스템(300)은 사용자 단말기(310), 사용자 단말기로 소정의 서비스를 제공하는 제휴 서비스 서버(330) 및 상기 사용자 단말기(310)와 제휴 서비스 서버(320)와 연결되어 상기 사용자 단말기(310)에 대한 사용자 인증을 수행하는 사용자 인증 서버(320)를 포함하여 구성될 수 있다.

[0034] 또한, 도 3에서 볼 수 있는 바와 같이, 본 발명의 일 실시예에 따른 익명 아이디를 사용하는 원클릭 사용자 인증 시스템(300)의 동작 원리를 웹 서비스의 경우를 예로 들어 간략하게 살펴보면 먼저 사용자 단말기(310)가 제휴 서비스 서버(330)로 사용자 인증을 위한 정보 요청에 대하여, ① 제휴 서비스 서버(330)가 사용자 단말기(310)로 HTTP 페이지의 전송 시에 수정된 자원위치지정자 구조(custom URL scheme)에 상기 사용자 인증을 위한 정보를 포함하는 방식으로 전달할 수 있고, ② 사용자가 웹사이트에 로그인하기 위하여 원클릭 로그인 사용자 인터페이스를 클릭하는 경우 ③ 사용자 단말기(310)상기 사용자 인증을 위한 정보를 암호화하여 사용자 인증 서버(320)로 전송하여 사용자 인증을 요청하고, ④ 사용자 인증 서버(320)는 상기 사용자 인증을 위한 정보를 복호화하여 사용자 인증을 수행한 후 인증 결과를 제휴 서비스 서버(330)로 전달하면, ⑤ 제휴 서비스 서버(330)는 그 인증 결과에 따라 사용자 단말기(310)로 적절한 서비스를 제공하게 된다.

[0035] 도 4에서는 본 발명의 일 실시예에 따른 익명 아이디를 사용하는 원클릭 사용자 인증 방법의 순서도를 보여주고 있다. 아래에서는 웹 서비스에서 사용자 인증을 진행하는 경우에 대하여, 본 발명의 일 실시예에 따른 익명 아이디를 사용하는 원클릭 사용자 인증 방법을 도 4의 각 단계의 흐름에 따라 자세하게 살펴보도록 한다.

[0036] 먼저, 사용자 단말기(310)의 웹 브라우저에서 특정 웹사이트를 구동하는 제휴 서비스 서버(330)로 HTTP(hyper text transfer protocol)를 통하여 웹페이지의 서비스를 요청(도 4의 ⓐ)하게 된다. 물론, 웹페이지의 서비스를 요청하는 경우 외에도, 소정의 게임의 구동을 요청하거나, 특정한 어플리케이션의 구동을 요청할 수도 있다. 경우에 따라서는 특정한 서비스의 요청이 아닌 사용자 단말기가 제휴 서비스 서버로 사용자 인증만을 요청하거나 이를 위한 정보만을 요청할 수도 있다.

[0037] 상기 사용자 단말기(310)에서의 요청에 대하여, 제휴 서비스 서버(330)에서는 사용자 인증 서버(320)로 상기 사용자에 대응하는 무작위 임시어(Nonce)의 발급을 요청(도 4의 ⓑ)하게 되고, 이에 따라 상기 사용자 인증 서버(320)는 상기 제휴 서비스 서버(330)로 발급된 무작위 임시어(Nonce)를 전송(도 4의 ⓒ)하게 된다. 여기서, 제휴 서비스 서버(330)라 함은 상기 제휴 서비스 서버(330)와 사용자 인증 서버(320) 간에 사용자의 인증을 위하여 미리 정하여진 일련의 프로세스가 진행될 수 있도록 제휴 관계를 가진다는 것을 의미한다.

[0038] 다만, 상기한 바와 같이 제휴 관계를 가진다 하여 반드시 상기 사용자 인증 서버(320)와 상기 제휴 서비스 서버(330)가 독립되어 운영되어야 하는 것은 아니며, 양 서버가 하나의 운영 주체에 의하여 운영되거나 하나의 통합 서버에서 구동되더라도 본 발명의 일 실시예로서 포함될 수 있음은 자명하다.

[0039] 이어서, 상기 제휴 서비스 서버(330)는 상기 사용자 단말기(310)로 웹페이지의 서비스를 위한 정보를 전송(도 4의 ⓓ)하게 되는데, 여기에는 사용자 단말기(310)의 사용자 인증을 위한 정보가 포함될 수 있다. 예를 들어, 상기 사용자 인증을 위한 정보로서 상기 사용자에 대응하는 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보 등을 들 수 있다. 특히, HTTP(hyper text transfer protocol)를 통하여 웹페이지를 서비스하는 경우에는, 도 5에서 볼 수 있는 바와 같이, 수정된 자원위치지정자 구조(custom URL scheme)를 사용하여 상기 사용자에 대응하는 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보를 포함하는 일련의 사용자 인증을 위한 정보를 전달할 수 있게 된다.

[0040] iOS/Android/Windows 등의 다양한 운영체제는 사용자가 정의한 구조의 자원위치지정자(URL) 즉 수정된 자원위치지정자 구조(custom URL scheme)을 처리할 수 있는 어플리케이션을 등록하여 사용할 수 있으므로, 이를 활용하면 도 5에서 볼 수 있는 바와 같이, 상기 사용자에 대응하는 무작위 임시어(Nonce), 상기 제휴 서비스 서버의 식별 정보 및 상기 사용자 인증 서버의 식별 정보 등을 포함하는 일련의 사용자 인증을 위한 정보들을 웹페이지 정보와 함께 전달할 수 있게 된다.

[0041] 도 5에서 볼 수 있는 바와 같이, 본 발명의 일 실시예에 따른 원클릭 사용자 인증 방법에 수정된 자원위치지정자 구조(custom URL scheme)를 적용하면, 로그인을 위하여 임의로 정의된 수정된 자원위치지정자(custom URL)임을 나타내어 주는 구조 정의(scheme) 부분(도 5의 ⓐ Scheme), 사용자 인증 서버(320)의 식별 정보 부분(도 5의 ⓑ Host), 사용자 인증 서버(320)에 전달되어 인증에 사용되는 제휴 서비스 서버(330)의 식별 정보 및 상기 사용자에 대응하는 무작위 임시어(Nonce) 정보(도 5의 ⓒ Query)를 포함하는 질의어 부분을 포함하는 방식으로 일련의 사용자 인증을 위한 정보들을 포함하는 수정된 자원위치지정자 구조(custom URL scheme)를 구성하여 간편하게 정보를 전달할 수 있게 된다.

[0042] 이어서, 사용자가 상기 제휴 서비스 서버(330)의 웹사이트에서의 사용자 인증을 위하여 마련된 소정의 버튼을 클릭하는 경우, 웹브라우저는 상기 무작위 임시어(Nonce), 상기 제휴 서비스 서버(330)의 식별 정보 및 상기 사용자 인증 서버(320)의 식별 정보를 포함하는 인증 정보를 상기 사용자 단말기(310)에서 이미 구동되고 있던 또는 새롭게 구동되는 사용자 인증 어플리케이션으로 전달(도 4의ⓔ)하게 된다.

[0043] 나아가, 앞서 살핀 일련의 단계를 수정하여, 먼저 사용자가 웹페이지 등에 사용자 인증을 위하여 마련된 소정의 버튼을 클릭하는 등 사용자 인터페이스(User Interface)를 통하여 제휴 서비스 서버(330)에서 제공하는 소정의 서비스에서의 사용자 인증을 시도한 후에야, 사용자 단말기(310)가 상기 제휴 서비스 서버(330)로 웹페이지의 서비스를 요청하거나 사용자 인증을 위한 정보를 요청하는 절차를 개시하도록 할 수도 있다.

[0044] 다음으로, 상기 사용자 인증 어플리케이션에서는 상기 인증 정보를 암호화하여 상기 사용자 인증 서버(320)로 전달(도 4의ⓕ)하게 된다. 도 6에서는 본 발명의 일 실시예에 따른 원클릭 사용자 인증 방법에서의 인증 정보 암호화 및 복화화 과정을 설명하고 있다. 도 6에서 볼 수 있는 바와 같이, 먼저 상기 제휴 서비스 서버(330)의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하여 제1 개인키(Private key)와 제1 공용키(Public key)를 생성하고, 상기 무작위 임시어(Nonce)를 상기 제1 개인키(Private key)로 암호화하여 제1 전자서명을 생성한다.

[0045] 이어서, 상기 사용자 인증 서버(320)의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하여 생성된 제2 개인키를 사용하여, 상기 제1 전자서명 및 제1 공용키를 묶은 하나의 데이터를 암호화하여 제2 전자서명을 생성하고, 이를 상기 사용자 인증 서버(320)로 전송하게 된다.

[0046] 사용자 인증 서버(320)에서는 암호화되어 전달된 인증 정보를 복호화하여 무작위 임시어(Nonce)를 산출하고, 이를 앞서 사용자 인증 서버(320)에서 생성하였던 무작위 임시어(Nonce)와 비교하여 일치 여부를 검증하여 제휴 서비스 서버(330)로 검증 결과를 전송(도 4의 ⓖ)하게 된다.

[0047] 이때 상기 암호화된 인증 정보를 복호화하기 위해서는, 상기 사용자 인증 서버(320)의 식별 정보와 소정의 비밀키(secret key)를 사용하고 해쉬 기반 메시지 인증 코드(HMAC)를 이용하여 생성되어, 사용자가 상기 사용자 인증 서버(320)의 인증 서비스에 가입할 때 등록된 제2 공용키를 사용하여, 상기 사용자 인증 서버(320)로 전달된 제2 전자서명을 복호화하여 제1 전자서명과 제1 공용키를 산출하게 된다.

[0048] 이어서, 상기 제휴 서비스 서버(330)에서는 상기 사용자 인증 서버(320)로부터 사용자 인증의 결과를 전달받아, 그 인증 여부에 따라 적절한 서비스를 사용자 단말기(310)로 제공(도 4의 ⓗ)하게 된다.

[0049] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서 본 발명에 기재된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의해서 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

[0050] 300 : 원클릭 사용자 인증 시스템

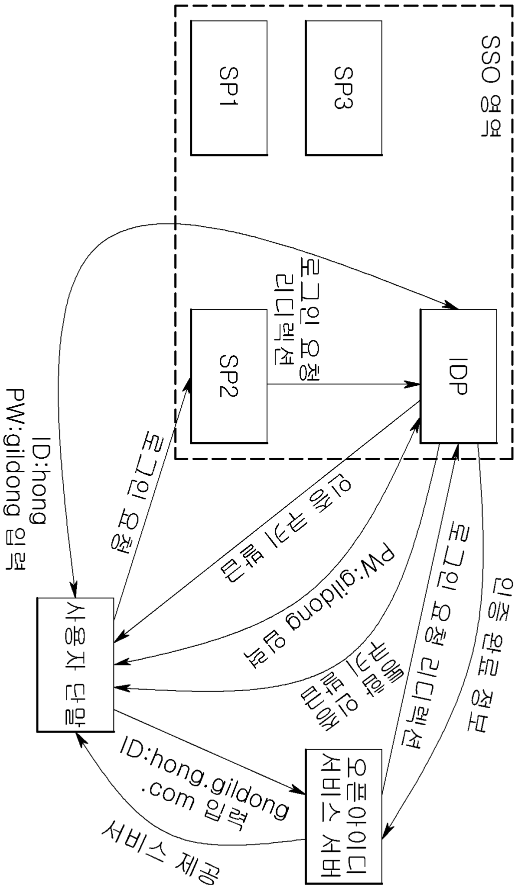
310 : 사용자 단말기

320 : 사용자 인증 서버

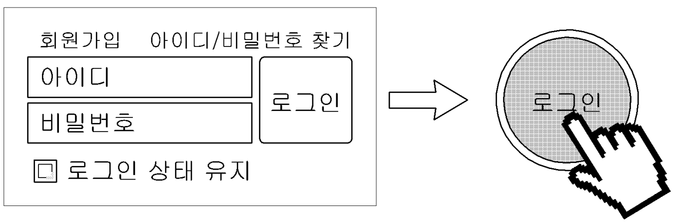
330 : 제휴 서비스 서버

도면

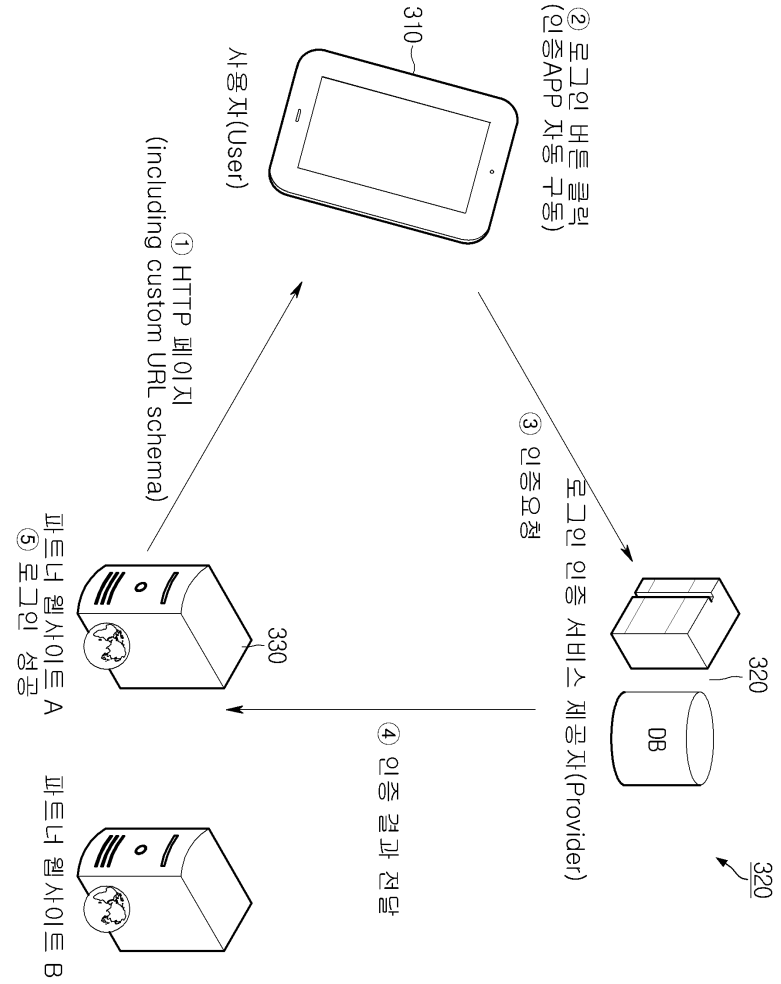
도면1


SSO 영역
SP1
SP3
SP2
IDP
로그인 요청 리디렉션
ID:hong
PW:gildong 입력
로그인 요청
PW:gildong 입력
로그인 요청 리디렉션
인증 완료 정보
사용자 단말
오픈아이디 서비스 서버
ID:hong.gildong .com 입력
서비스 제공

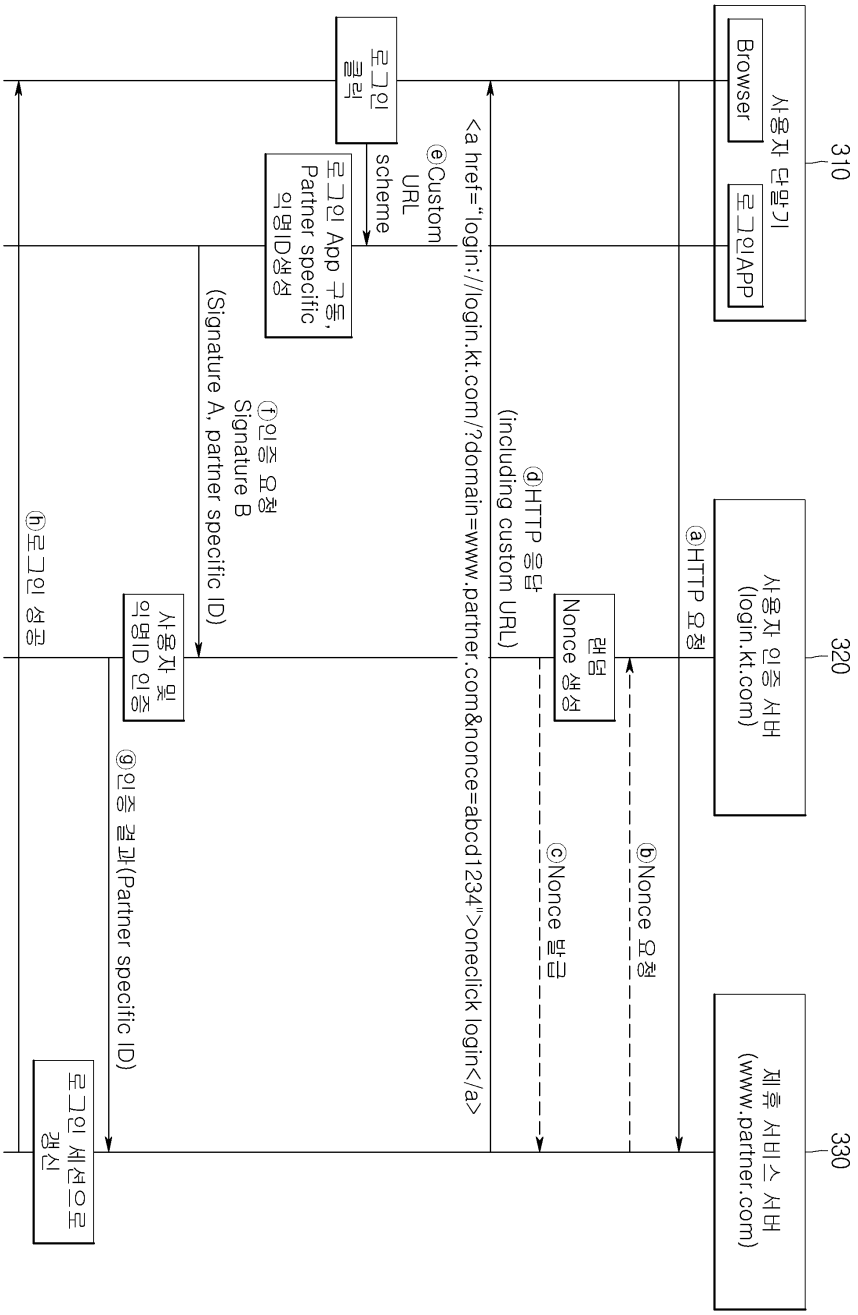
도면2


회원가입
아이디/비밀번호 찾기
아이디
비밀번호
로그인
로그인 상태 유지
로그인

도면3


310
사용자(User)
② 로그인 버튼 클릭
(인증APP 자동 구동)
① HTTP 페이지
(including custom URL schema)
③ 인증요청
로그인 인증 서비스 제공자(Provider)
320
DB
320
330
파트너 웹사이트 A
⑤ 로그인 성공
④ 인증 결과 전달
파트너 웹 사이트 B

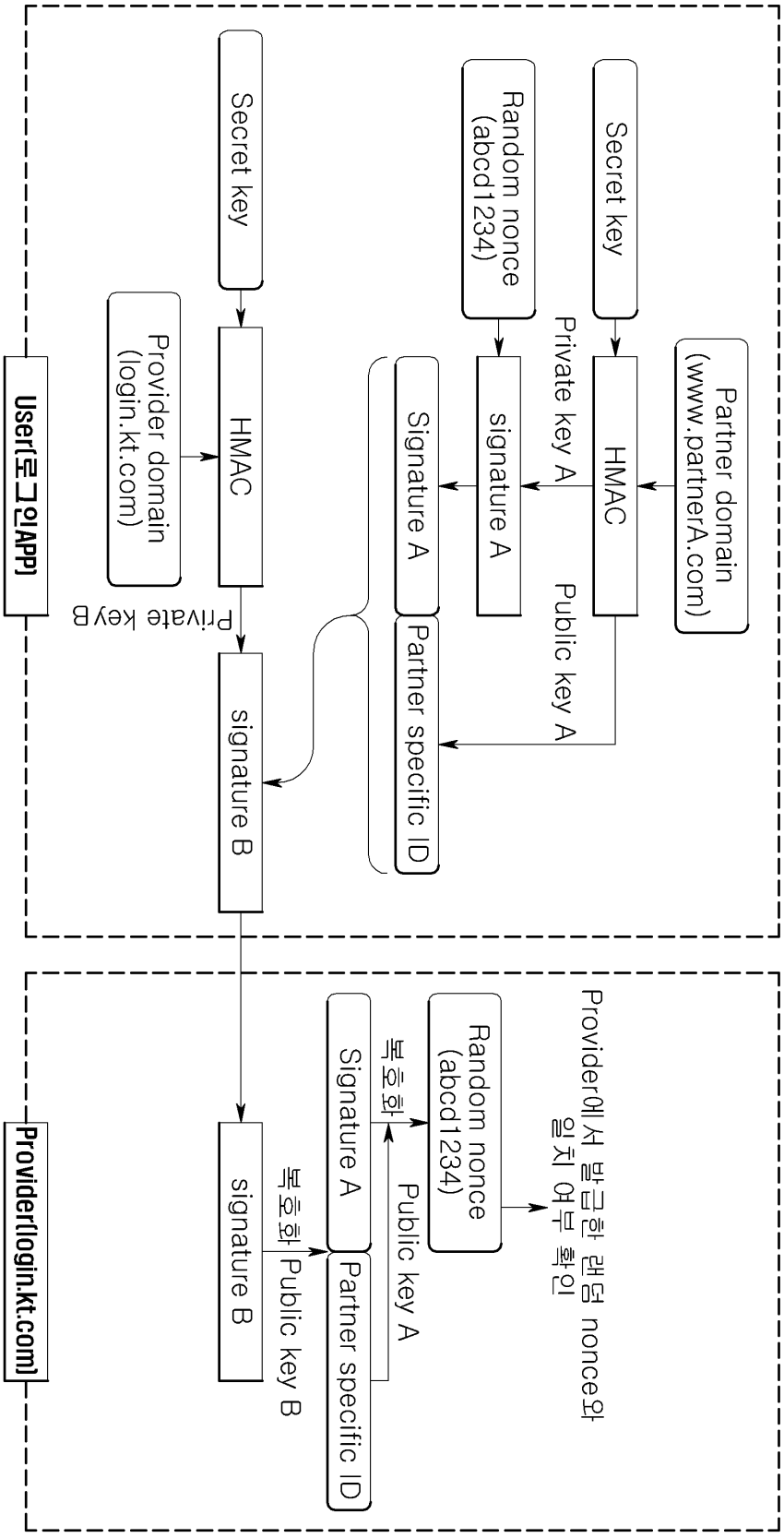
도면4


310
사용자 단말기
Browser
로그인APP
320
사용자 인증 서버
(login.kt.com)
330
제휴 서비스 서버
(www.partner.com)
ⓐHTTP 요청
ⓑNonce 요청
랜덤
Nonce 생성
ⓒNonce 발급
ⓓHTTP 응답
(including custom URL)
oneclick login
ⓔCustom
URL
scheme
로그인
클릭
로그인 App 구동,
Partner specific
익명ID생성
ⓕ인증 요청
Signature B
(Signature A, partner specific ID)
사용자 및
익명ID 인증
ⓖ인증 결과(Partner specific ID)
ⓗ로그인 성공
로그인 세션으로
갱신

도면5

Login://login.kt.com/?domain=www.partnerA.com&nonce=abcd1234
ⓐScheme
(본 발명에서 임의로 정의함)
ⓑHost
(인증서버)
ⓒQuery
(domain: 파트너사의 domain,
Nonce: 인증을 위한 랜덤 challenge value)

도면6



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 16

【변경전】

상기 사용자 단말기는,

【변경후】

상기 사용자의 단말은,