(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년05월31일
(11) 등록번호 10-1270323
(24) 등록일자 2013년05월27일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *H04L 9/32* (2006.01)
H04W 80/12 (2009.01) *H04W 84/02* (2009.01)
(21) 출원번호 10-2010-7026325
(22) 출원일자(국제) 2009년03월10일
심사청구일자 2010년11월24일
(85) 번역문제출일자 2010년11월24일
(65) 공개번호 10-2011-0008272
(43) 공개일자 2011년01월26일
(86) 국제출원번호 PCT/FI2009/050189
(87) 국제공개번호 WO 2009/130370
국제공개일자 2009년10월29일
(30) 우선권주장
12/109,644 2008년04월25일 미국(US)
(56) 선행기술조사문헌
US7296290 B1
Security Assertion Markup Language(SAML) V2.0 Technical Overview(John Hughes et al, 2005)
US20030149781 A1
전체 청구항 수 : 총 25 항

(73) 특허권자
노키아 코포레이션
핀랜드핀-02150 에스푸 카일알라덴티에 4
(72) 발명자
카잘라 자리
핀랜드 에프아이-01610 반타아 아프라민티에 1 씨 27
벱살라이넨 아리
핀랜드 에프아이-02200 에스푸 티카스니틴티에 11
마키 주씨
핀랜드 에프아이-02340 에스푸 오라카스켄마키 16 에이 1
(74) 대리인
제일특허법인, 김원준

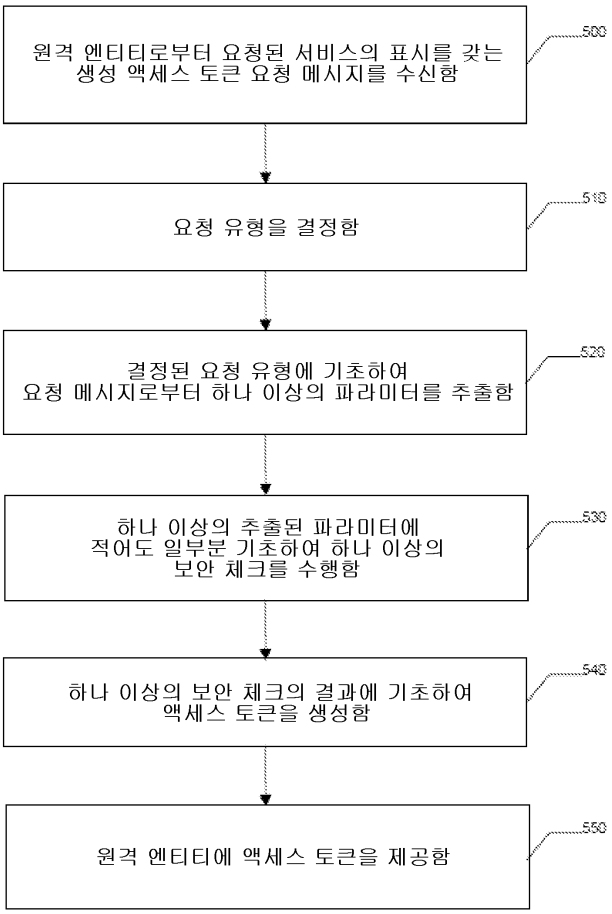
심사관 : 장상배

(54) 발명의 명칭 **단일 서비스 사인 온을 제공하는 방법, 장치 및 컴퓨터 판독가능 저장 매체**

(57) 요 약

장치는 원격 엔티티로부터 액세스 토큰에 대한 요청을 수신하도록 구성된 프로세서를 포함할 수 있으며(500), 요청은 요청된 서비스의 표시를 포함한다. 프로세서는 요청 유형을 결정하도록 또한 구성될 수 있으며(510), 요청 유형은 사용자 식별정보 및 암호 조합, 요청 토큰 교환 또는 액세스 토큰 교환일 수 있다. 프로세서는 결정된 요청 유형에 기초하여 요청 내에 포함된 하나 이상의 파라미터를 추출하고(520), 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 하나 이상의 보안 체크를 수행하도록(530) 추가적으로 구성될 수 있다. 프로세서는 하나 이상의 보안 체크의 결과에 적어도 일부분 기초하여 액세스 토큰을 생성하고(540), 원격 엔티티에 액세스 토큰을 제공하도록(550) 또한 구성될 수 있다.

대 표 도


원격 엔티티로부터 요청된 서비스의 표시를 갖는 생성 액세스 토큰 요청 메시지를 수신함
500
요청 유형을 결정함
510
결정된 요청 유형에 기초하여 요청 메시지로부터 하나 이상의 파라미터를 추출함
520
하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 하나 이상의 보안 체크를 수행함
530
하나 이상의 보안 체크의 결과에 기초하여 액세스 토큰을 생성함
540
원격 엔티티에 액세스 토큰을 제공함
550

특허청구의 범위

청구항 1

원격 엔티티로부터 액세스 토큰(token)에 대한 요청을 수신하는 단계 - 상기 요청은 요청된 서비스의 표시를 포함함 - 와,

프로세서를 이용하여 상기 수신된 요청의 요청 유형을 결정하는 단계 - 상기 결정된 요청 유형은 사용자 식별정보 및 암호 조합(a user identification and password combination), 요청 토큰 교환, 또는 액세스 토큰 교환 중 하나임 - 와,

상기 결정된 요청 유형에 적어도 일부분 기초하여 상기 요청 내에 포함된 하나 이상의 파라미터를 추출하는 단계와,

상기 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 한번 이상의 보안 체크를 수행하는 단계와,

상기 한번 이상의 보안 체크의 결과에 적어도 일부분 기초하여 액세스 토큰을 생성하는 단계 - 상기 액세스 토큰은 적어도 상기 요청된 서비스 및 상기 원격 엔티티와 연관됨 - 와,

상기 원격 엔티티에 상기 액세스 토큰이 제공되도록 하는 단계를 포함하는

방법.

청구항 2

제 1 항에 있어서,

상기 결정된 요청 유형에 적어도 일부분 기초하여 상기 요청 내에 포함된 하나 이상의 파라미터를 추출하는 단계는,

상기 결정된 요청 유형이 사용자 식별정보 및 암호 조합인 경우, 사용자 식별정보, 암호의 해시(hash), 및 클라이언트 키와 클라이언트 시크릿(secret)을 포함하는 시그니처(signature)를 추출하는 단계와,

상기 결정된 요청 유형이 요청 토큰 교환인 경우, 요청 토큰, 및 클라이언트 키와 클라이언트 시크릿을 포함하는 시그니처를 추출하는 단계, 또는

상기 결정된 요청 유형이 액세스 토큰 교환인 경우, 이전에 발행된 액세스 토큰, 및 클라이언트 시크릿과 토큰 시크릿을 포함하는 시그니처를 추출하는 단계를 포함하는

방법.

청구항 3

제 2 항에 있어서,

상기 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 한번 이상의 보안 체크를 수행하는 단계는,

상기 사용자 식별정보 및 상기 암호의 해시가 알려져 있고 서로에 대응하는지를 확인하고, 상기 시그니처를 확인하며, 또한 상기 결정된 요청 유형이 사용자 식별정보 및 암호 조합인 경우 클라이언트 식별정보, 사용자 식별정보, 및 상기 요청된 서비스 사이의 연관성을 확인하는 단계와,

상기 시그니처를 확인하고, 상기 결정된 요청 유형이 요청 토큰 교환인 경우 상기 요청 토큰, 클라이언트 키, 및 클라이언트 시크릿 사이의 연관성을 확인하는 단계, 또는

상기 시그니처를 확인하고, 상기 결정된 요청 유형이 액세스 토큰 교환인 경우 상기 이전에 발행된 액세스 토큰, 토큰 시크릿, 및 클라이언트 시크릿 사이의 연관성을 확인하는 단계를 포함하는

방법.

청구항 4

제 1 항에 있어서,

상기 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 한번 이상의 보안 체크를 수행하는 단계는, 상기 원격 엔티티가 상기 요청된 서비스에 액세스하기 위한 허가를 갖는지를 확인하는 단계를 더 포함하는

방법.

청구항 5

제 1 항에 있어서,

상기 한번 이상의 보안 체크의 결과에 적어도 일부분 기초하여 액세스 토큰을 생성하는 단계는, 사용자 및 상기 요청된 서비스와 연관된 액세스 토큰을 생성하고 상기 액세스 토큰과 연관된 토큰 시크릿을 생성하는 단계를 포함하는

방법.

청구항 6

제 1 항에 있어서,

상기 한번 이상의 보안 체크의 결과에 적어도 일부분 기초하여 액세스 토큰을 생성하는 단계는, 정의된 액세스 승인을 가진 액세스 토큰을 생성하는 단계를 포함하고,

상기 정의된 액세스 승인은 상기 액세스 토큰이 액세스하는 데 사용될 수 있는 하나 이상의 연관된 서비스, 하나 이상의 연관된 사용자, 상기 액세스 토큰이 유효한 사용 기간, 및 상기 액세스 토큰이 유효한 사용 횟수 중 하나 이상을 포함하는

방법.

청구항 7

제 1 항에 있어서,

상기 원격 엔티티는 클라이언트 장치 또는 서비스 공급자 중 하나인

방법.

청구항 8

제 1 항에 있어서,

상기 원격 엔티티에 상기 액세스 토큰이 제공되도록 하는 단계에 후속하여,

서비스 공급자로부터 토큰 정보 요청 메시지를 수신하는 단계 - 상기 토큰 정보 요청 메시지는 상기 액세스 토큰을 포함하고, 상기 토큰 정보 요청 메시지는 서비스 키 및 서비스 시크릿을 사용하여 서명됨 - 와,

상기 액세스 토큰, 상기 서비스 키 및 상기 서비스 시크릿 사이의 연관성을 확인하는 단계와,

상기 액세스 토큰과 연관되는 사용자 식별정보, 토큰 시크릿 및 클라이언트 시크릿을 결정하는 단계와,

상기 결정된 사용자 식별정보, 클라이언트 키 및 토큰 시크릿을 포함하는 메시지가 상기 서비스로 전송되도록

하는 단계를 포함하는

방법.

청구항 9

컴퓨터 판독가능 프로그램 코드 부분이 저장된 컴퓨터 프로그램을 포함하는 적어도 하나의 컴퓨터 판독가능 저장 매체로서,

상기 컴퓨터 판독가능 프로그램 코드 부분은,

원격 엔티티로부터 액세스 토큰에 대한 요청을 수신하는 프로그램 코드 부분 - 상기 요청은 요청된 서비스의 표시를 포함함 - 과,

상기 수신된 요청의 요청 유형을 결정하는 프로그램 코드 부분 - 상기 결정된 요청 유형은 사용자 식별정보 및 암호 조합, 요청 토큰 교환, 또는 액세스 토큰 교환 중 하나임 - 과,

상기 결정된 요청 유형에 적어도 일부분 기초하여 상기 요청 내에 포함된 하나 이상의 파라미터를 추출하는 프로그램 코드 부분과,

상기 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 한번 이상의 보안 체크를 수행하는 프로그램 코드 부분과,

상기 한번 이상의 보안 체크의 결과에 적어도 일부분 기초하여 액세스 토큰을 생성하는 프로그램 코드 부분 - 상기 액세스 토큰은 적어도 상기 요청된 서비스 및 상기 원격 엔티티와 연관됨 - 과,

상기 원격 엔티티에 상기 액세스 토큰이 제공되도록 하는 프로그램 코드 부분을 포함하는

컴퓨터 판독가능 저장 매체.

청구항 10

제 9 항에 있어서,

상기 요청 내에 포함된 하나 이상의 파라미터를 추출하는 프로그램 코드 부분은,

상기 결정된 요청 유형이 사용자 식별정보 및 암호 조합인 경우, 사용자 식별정보, 암호의 해시, 및 클라이언트 키와 클라이언트 시크릿을 포함하는 시그니처를 추출하는 인스트럭션과,

상기 결정된 요청 유형이 요청 토큰 교환인 경우, 요청 토큰, 및 클라이언트 키와 클라이언트 시크릿을 포함하는 시그니처를 추출하는 인스트럭션, 또는

상기 결정된 요청 유형이 액세스 토큰 교환인 경우, 이전에 발행된 액세스 토큰, 및 클라이언트 시크릿과 토큰 시크릿을 포함하는 시그니처를 추출하는 인스트럭션을 포함하는

컴퓨터 판독가능 저장 매체.

청구항 11

제 10 항에 있어서,

상기 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 한번 이상의 보안 체크를 수행하는 프로그램 코드 부분은,

상기 사용자 식별정보 및 상기 암호의 해시가 알려져 있고 서로에 대응하는지를 확인하고, 상기 시그니처를 확인하며, 또한 상기 결정된 요청 유형이 사용자 식별정보 및 암호 조합인 경우 클라이언트 식별정보, 사용자 식별정보, 및 상기 요청된 서비스 사이의 연관성을 확인하는 인스트럭션과,

상기 시그니처를 확인하고, 상기 결정된 요청 유형이 요청 토큰 교환인 경우 상기 요청 토큰, 클라이언트 키,

및 클라이언트 시크릿 사이의 연관성을 확인하는 인스트럭션, 또는

상기 시그니처를 확인하고, 상기 결정된 요청 유형이 액세스 토큰 교환인 경우 상기 이전에 발행된 액세스 토큰, 토큰 시크릿, 및 클라이언트 시크릿 사이의 연관성을 확인하는 인스트럭션을 포함하는

컴퓨터 판독가능 저장 매체.

청구항 12

제 9 항에 있어서,

상기 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 한번 이상의 보안 체크를 수행하는 프로그램 코드 부분은, 상기 원격 엔티티가 상기 요청된 서비스에 액세스하기 위한 허가를 갖는지를 확인하는 인스트럭션을 포함하는

컴퓨터 판독가능 저장 매체.

청구항 13

제 9 항에 있어서,

상기 한번 이상의 보안 체크의 결과에 적어도 일부분 기초하여 액세스 토큰을 생성하는 프로그램 코드 부분은, 사용자 및 상기 요청된 서비스와 연관된 액세스 토큰을 생성하고 상기 액세스 토큰과 연관된 토큰 시크릿을 생성하는 인스트럭션을 포함하는

컴퓨터 판독가능 저장 매체.

청구항 14

제 9 항에 있어서,

상기 한번 이상의 보안 체크의 결과에 적어도 일부분 기초하여 액세스 토큰을 생성하는 프로그램 코드 부분은, 정의된 액세스 승인을 가진 액세스 토큰을 생성하는 인스트럭션을 포함하고,

상기 정의된 액세스 승인은 상기 액세스 토큰이 액세스하는 데 사용될 수 있는 하나 이상의 연관된 서비스, 하나 이상의 연관된 사용자, 상기 액세스 토큰이 유효한 사용 기간, 및 상기 액세스 토큰이 유효한 사용 횟수 중 하나 이상을 포함하는

컴퓨터 판독가능 저장 매체.

청구항 15

제 9 항에 있어서,

상기 원격 엔티티는 클라이언트 장치 또는 서비스 공급자 중 하나인

컴퓨터 판독가능 저장 매체.

청구항 16

제 9 항에 있어서,

서비스 공급자로부터 토큰 정보 요청 메시지를 수신하는 프로그램 코드 부분 - 상기 토큰 정보 요청 메시지는 상기 원격 엔티티에 제공되는 상기 액세스 토큰을 포함하고, 상기 토큰 정보 요청 메시지는 서비스 키 및 서비스 시크릿을 사용하여 서명됨 - 과,

상기 액세스 토큰, 상기 서비스 키 및 상기 서비스 시크릿 사이의 연관성을 확인하는 프로그램 코드 부분과,

상기 액세스 토큰과 연관되는 사용자 식별정보, 토큰 시크릿 및 클라이언트 시크릿을 결정하는 프로그램 코드 부분과,

상기 결정된 사용자 식별정보, 클라이언트 키 및 토큰 시크릿을 포함하는 메시지가 상기 서비스로 전송되도록 하는 프로그램 코드 부분을 더 포함하는

컴퓨터 판독가능 저장 매체.

청구항 17

적어도 하나의 프로세서, 및 컴퓨터 프로그램 코드를 저장하는 적어도 하나의 메모리를 포함하는 장치로서,

상기 적어도 하나의 메모리 및 저장된 컴퓨터 프로그램 코드는 상기 적어도 하나의 프로세서를 이용하여 상기 장치로 하여금

원격 엔티티로부터 액세스 토큰에 대한 요청을 수신 - 상기 요청은 요청된 서비스의 표시를 포함함 - 하고,

상기 수신된 요청의 요청 유형을 결정 - 상기 결정된 요청 유형은 사용자 식별정보 및 암호 조합, 요청 토큰 교환, 또는 액세스 토큰 교환 중 하나임 - 하고,

상기 결정된 요청 유형에 적어도 일부분 기초하여 상기 요청 내에 포함된 하나 이상의 파라미터를 추출하고,

상기 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 한번 이상의 보안 체크를 수행하고,

상기 한번 이상의 보안 체크의 결과에 적어도 일부분 기초하여 액세스 토큰을 생성 - 상기 액세스 토큰은 적어도 상기 요청된 서비스 및 상기 원격 엔티티와 연관됨 - 하고,

상기 원격 엔티티에 상기 액세스 토큰이 제공되도록 하게끔 구성되는

장치.

청구항 18

제 17 항에 있어서,

상기 적어도 하나의 메모리 및 저장된 컴퓨터 프로그램 코드는 상기 적어도 하나의 프로세서를 이용하여 상기 장치로 하여금

상기 결정된 요청 유형이 사용자 식별정보 및 암호 조합인 경우, 사용자 식별정보, 암호의 해시, 및 클라이언트 키와 클라이언트 시크릿을 포함하는 시그니처를 추출하고,

상기 결정된 요청 유형이 요청 토큰 교환인 경우, 요청 토큰, 및 클라이언트 키와 클라이언트 시크릿을 포함하는 시그니처를 추출하고, 또는

상기 결정된 요청 유형이 액세스 토큰 교환인 경우, 이전에 발행된 액세스 토큰, 및 클라이언트 시크릿과 토큰 시크릿을 포함하는 시그니처를 추출함으로써

상기 결정된 요청 유형에 기초하여 상기 요청 내에 포함된 하나 이상의 파라미터를 추출할 수 있도록 구성되는

장치.

청구항 19

제 18 항에 있어서,

상기 적어도 하나의 메모리 및 저장된 컴퓨터 프로그램 코드는 상기 적어도 하나의 프로세서를 이용하여 상기 장치로 하여금

상기 사용자 식별정보 및 상기 암호의 해시가 알려져 있고 서로에 대응하는지를 확인하고, 상기 시그니처를 확인하며, 또한 상기 결정된 요청 유형이 사용자 식별정보 및 암호 조합인 경우 클라이언트 식별정보, 사용자 식별정보, 및 상기 요청된 서비스 사이의 연관성을 확인하고,

상기 시그니처를 확인하고, 상기 결정된 요청 유형이 요청 토큰 교환인 경우 상기 요청 토큰, 클라이언트 키, 및 클라이언트 시크릿 사이의 연관성을 확인하며, 또는

상기 시그니처를 확인하고, 상기 결정된 요청 유형이 액세스 토큰 교환인 경우 상기 이전에 발행된 액세스 토큰, 토큰 시크릿, 및 클라이언트 시크릿 사이의 연관성을 확인함으로써

상기 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 한번 이상의 보안 체크를 수행할 수 있도록 구성되는

장치.

청구항 20

제 17 항에 있어서,

상기 적어도 하나의 메모리 및 저장된 컴퓨터 프로그램 코드는 상기 적어도 하나의 프로세서를 이용하여 상기 장치로 하여금, 상기 원격 엔티티가 상기 요청된 서비스에 액세스하기 위한 허가를 갖는지를 확인함으로써 상기 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 한번 이상의 보안 체크를 수행할 수 있도록 구성되는

장치.

청구항 21

제 17 항에 있어서,

상기 적어도 하나의 메모리 및 저장된 컴퓨터 프로그램 코드는 상기 적어도 하나의 프로세서를 이용하여 상기 장치로 하여금, 사용자 및 상기 요청된 서비스와 연관된 액세스 토큰을 생성하고 상기 액세스 토큰과 연관된 토큰 시크릿을 생성할 수 있도록 또한 구성되는

장치.

청구항 22

제 17 항에 있어서,

상기 적어도 하나의 메모리 및 저장된 컴퓨터 프로그램 코드는 상기 적어도 하나의 프로세서를 이용하여 상기 장치로 하여금, 정의된 액세스 승인을 가진 액세스 토큰을 생성할 수 있도록 또한 구성되고,

상기 정의된 액세스 승인은 상기 액세스 토큰이 액세스하는 데 사용될 수 있는 하나 이상의 연관된 서비스, 하나 이상의 연관된 사용자, 상기 액세스 토큰이 유효한 사용 기간, 및 상기 액세스 토큰이 유효한 사용 횟수 중 하나 이상을 포함하는

장치.

청구항 23

제 17 항에 있어서,

상기 원격 엔티티는 클라이언트 장치 또는 서비스 공급자 중 하나인

장치.

청구항 24

제 23 항에 있어서,

상기 적어도 하나의 메모리 및 저장된 컴퓨터 프로그램 코드는 상기 적어도 하나의 프로세서를 이용하여 상기 장치로 하여금,

상기 원격 엔티티에 상기 액세스 토큰이 제공되도록 한 후에,

서비스 공급자로부터 토큰 정보 요청 메시지를 수신 - 상기 토큰 정보 요청 메시지는 상기 액세스 토큰을 포함하고, 상기 토큰 정보 요청 메시지는 서비스 키 및 서비스 시크릿을 사용하여 서명됨 - 하고,

상기 액세스 토큰, 상기 서비스 키 및 상기 서비스 시크릿 사이의 연관성을 확인하며,

상기 액세스 토큰과 연관되는 사용자 식별정보, 토큰 시크릿 및 클라이언트 시크릿을 결정하고,

상기 결정된 사용자 식별정보, 클라이언트 키 및 토큰 시크릿을 포함하는 메시지가 상기 서비스로 전송되도록 하게끔 또한 구성되는

장치.

청구항 25

원격 엔티티로부터 액세스 토큰에 대한 요청을 수신하는 수단 - 상기 요청은 요청된 서비스의 표시를 포함함 - 과,

상기 수신된 요청의 요청 유형을 결정하는 수단 - 상기 결정된 요청 유형은 사용자 식별정보 및 암호 조합, 요청 토큰 교환, 또는 액세스 토큰 교환 중 하나임 - 과,

상기 결정된 요청 유형에 적어도 일부분 기초하여 상기 요청 내에 포함된 하나 이상의 파라미터를 추출하는 수단과,

상기 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 한번 이상의 보안 체크를 수행하는 수단과,

상기 한번 이상의 보안 체크의 결과에 적어도 일부분 기초하여 액세스 토큰을 생성하는 수단 - 상기 액세스 토큰은 적어도 상기 요청된 서비스 및 상기 원격 엔티티와 연관됨 - 과,

상기 원격 엔티티에 상기 액세스 토큰이 제공되도록 하는 수단을 포함하는

장치.

명 세 서

기 술 분 야

[0001] 본 발명의 실시예는 일반적으로 이동 통신 기술에 관한 것으로, 보다 구체적으로는, 웹 및 이동 장치 사용자에게 단일 서비스 사인 온을 제공하는 방법, 장치 및 컴퓨터 프로그램 제품에 관한 것이다.

배 경 기 술

[0002] 현대의 통신 시대는 유선 및 무선 네트워크의 거대한 확장을 야기한다. 컴퓨터 네트워크, 텔레비전 네트워크 및 전화 네트워크는 고객 요구에 의해 발생하는 선례 있는 기술 확장을 경험하고 있다. 무선 및 이동 네트워킹 기술은 정보 전송의 유연성과 즉시성을 더 많이 제공하면서, 관련된 고객 요구를 해결해 왔다.

[0003] 현재 및 미래의 네트워킹 기술은 정보 전송의 용이성 및 사용자에 대한 편의성을 계속 촉진한다. 정보 전송의 용이성 및 사용자에 대한 편의성을 더 향상시키기 위한 요구가 존재하는 일 영역은 네트워크를 통해 서비스에

액세스하는 사용자의 인증을 필요로 한다. 이들 서비스 중 몇몇은 일반적으로 얼마 동안 개인 컴퓨터 및 다른 컴퓨팅 장치의 사용자에게 이용가능하였지만, 최근에는 무선 및 이동 네트워킹 기술의 성장뿐만 아니라 이동 컴퓨팅 장치에서 사용되는 구성요소 및 고성능 프로세서의 소형화 및 전력 처리의 계속되는 개발 때문에 이동 단말기 사용자에게 이용가능하게 되었다. 이들 서비스의 예는 이메일, 인스턴트 메시징, 멀티 플레이어 게임, 피어 투 피어 파일 전송, 웹 브라우징, 소셜 네트워킹 및 사진 호스팅을 포함한다.

[0004] 이들 서비스는 이동 단말기 및 다른 컴퓨팅 장치의 사용자에게 사용자 계정을 수립하고 각각의 서비스 사용시에 고유한 사인 온을 사용하여 각각의 서비스에 대해 인증하라고 요청할 수 있다. 예컨대, 사용자는 사용자의 온라인 사진 앨범을 관리하기 위해 사진 호스팅 서비스에 대해 인증해야만 할 수도 있다. 사진 호스팅 서비스를 사용하는 동안, 사용자는 사진을 저장 서비스에 업로드하거나, 사진 호스팅 서비스와 함께 사용할 저장 서비스에 저장된 사진에 액세스하기를 원할 수 있다. 저장 서비스는 사용자에게 그 서비스를 사용하기 전에 저장 서비스에 별도로 사인 온(sign-on)하라고 요구할 수 있다. 이처럼, 사용자는 다수의 사용자 이름과 암호를 기억하고 각각의 서비스 사용시에 각각의 서비스에 개별적으로 사인 온하면서 실패를 경험할 수 있다.

[0005] 몇몇 기존의 서비스는 예컨대, 웹 브라우저를 통해 서비스에 액세스하는 사용자에게 다수의 서비스에 대한 액세스를 제공하는 인터넷 포털에서 단일 사인 온을 제공함으로써 이 서비스 사인 온 문제를 해결하려고 시도해 왔지만, 기존의 단일 사인 온 솔루션은 컴퓨팅 장치 사용자가 다양한 통신 프로토콜을 사용하는 다양한 컴퓨팅 장치 상의 다양한 애플리케이션 사용자 인터페이스를 통해 서비스에 액세스할 수 있다는 사실을 고려할 수 없다. 이들 서비스 중 몇몇은 사용자의 서비스 세션 동안에 사용자를 대신하여 다른 서비스에 액세스할 수 있다.

[0006] 단일 서비스 사인 온을 제공함으로써 사용자에게 적용될 수 있다는 이점 외에, 서비스 공급자는 인증 책임이 공통 서비스 인증 인터페이스를 통해 단일 관리 엔티티로 위임될 수 있다는 이점도 실현할 수 있다. 또한, 그러한 공통 서비스 인증 인터페이스는 서비스 개발 및 전개 비용을 간소화할 뿐만 아니라 강화된 보안도 제공할 수 있는 애플리케이션 및 서비스의 공통 라이브러리의 사용을 고려할 수 있다.

[0007] 따라서, 다수의 통신 프로토콜을 사용하는 다수의 장치 상에서 구현된 다수의 애플리케이션 인터페이스를 사용하여 다수의 서비스의 호출을 허용하는 단일 사인 온을 제공하는 시스템을 사용자에게 제공하는 것은 이로울 수 있다. 그러한 시스템은 이로써 전술한 단점 중 적어도 일부를 해결할 수 있다.

발명의 내용

과제의 해결 수단

[0008] 방법, 장치 및 컴퓨터 프로그램 제품은 컴퓨팅 장치의 사용자에게 단일 서비스 사인 온을 제공할 수 있게 하도록 제공된다. 특히, 방법, 장치 및 컴퓨터 프로그램 제품은 예컨대, 장치의 사용자가 한번 사인 온할 수 있게 하고 사용자에게 다른 서비스를 사용하기 위해 추가적인 사인 온 정보를 입력하기를 요구하지 않고도 사용자가 등록되거나 사용하도록 허가되는 다수의 서비스에 대한 액세스를 가지도록 제공된다. 제공된 단일 서비스 사인 온은 계정 관리 공급자가 몇몇 상이한 프로토콜에서 수신된 요청을 수신하고 이에 응답할 수 있는 것과 같이 독립적인 장치 및 애플리케이션이다.

[0009] 일 예시적인 실시예에서, 원격 엔티티로부터 액세스 토큰에 대한 요청을 수신하는 단계를 포함할 수 있는 방법이 제공되는데, 요청은 요청된 서비스의 표시를 포함한다. 방법은 요청 유형을 결정하는 단계를 더 포함할 수 있으며, 요청 유형은 사용자 식별정보 및 암호 조합, 요청 토큰 교환 또는 액세스 토큰 교환일 수 있다. 방법은 결정된 요청 유형에 기초하여 요청 내에 포함된 하나 이상의 파라미터를 추출하는 단계와, 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 하나 이상의 보안 체크를 수행하는 단계를 더 포함할 수 있다. 방법은 하나 이상의 보안 체크의 결과에 적어도 일부분 기초하여 액세스 토큰을 생성하는 단계와, 원격 엔티티에 액세스 토큰을 제공하는 단계를 추가적으로 포함할 수 있다.

[0010] 다른 예시적인 실시예에서, 컴퓨터 프로그램 제품이 제공된다. 컴퓨터 프로그램 제품은 컴퓨터 판독가능 프로그램 코드 부분이 저장된 적어도 하나의 컴퓨터 판독가능 저장 매체를 포함한다. 컴퓨터 판독가능 프로그램 코드 부분은 제 1, 제 2, 제 3, 제 4, 제 5 및 제 6 프로그램 코드 부분을 포함한다. 제 1 프로그램 코드 부분은 원격 엔티티로부터 액세스 토큰에 대한 요청을 수신하되, 요청은 요청된 서비스의 표시를 포함한다. 제 2 실행가능 부분은 요청 유형을 결정하되, 요청 유형은 사용자 식별정보 및 암호 조합, 요청 토큰 교환 또는 액세스 토큰 교환일 수 있다. 제 3 실행가능 부분은 결정된 요청 유형에 기초하여 요청 내에 포함된 하나 이상의 파라

미터를 추출한다. 제 4 실행가능 부분은 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 하나 이상의 보안 체크를 수행한다. 제 5 실행가능 부분은 하나 이상의 보안 체크의 결과에 적어도 일부분 기초하여 액세스 토큰을 생성한다. 제 6 실행가능 부분은 원격 엔티티에 액세스 토큰을 제공한다.

[0011] 다른 예시적인 실시예에서, 프로세서를 포함할 수 있는 장치가 제공된다. 프로세서는 원격 엔티티로부터 액세스 토큰에 대한 요청을 수신하도록 구성될 수 있되, 요청은 요청된 서비스의 표시를 포함한다. 프로세서는 요청 유형을 결정하도록 또한 구성될 수 있되, 요청 유형은 사용자 식별정보 및 암호 조합, 요청 토큰 교환 또는 액세스 토큰 교환일 수 있다. 프로세서는 결정된 요청 유형에 기초하여 요청 내에 포함된 하나 이상의 파라미터를 추출하고, 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 하나 이상의 보안 체크를 수행하도록 추가적으로 구성될 수 있다. 프로세서는 하나 이상의 보안 체크의 결과에 적어도 일부분 기초하여 액세스 토큰을 생성하고, 원격 엔티티에 액세스 토큰을 제공하도록 또한 구성될 수 있다.

[0012] 다른 예시적인 실시예에서, 장치가 제공된다. 장치는 원격 엔티티로부터 액세스 토큰에 대한 요청을 수신하는 수단을 포함할 수 있되, 요청은 요청된 서비스의 표시를 포함한다. 장치는 요청 유형을 결정하는 수단을 더 포함할 수 있되, 요청 유형은 사용자 식별정보 및 암호 조합, 요청 토큰 교환 또는 액세스 토큰 교환일 수 있다. 장치는 결정된 요청 유형에 기초하여 요청 내에 포함된 하나 이상의 파라미터를 추출하는 수단을 추가적으로 포함할 수 있다. 장치는 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 하나 이상의 보안 체크를 수행하는 수단을 더 포함할 수 있다. 장치는 하나 이상의 보안 체크의 결과에 적어도 일부분 기초하여 액세스 토큰을 생성하는 수단을 추가적으로 포함할 수 있다. 장치는 원격 엔티티에 액세스 토큰을 제공하는 수단을 더 포함할 수 있다.

[0013] 일반적인 용어로 본 발명의 실시예를 설명하므로, 반드시 실제 크기대로 도시된 것은 아닌 첨부 도면을 참조할 것이다.

도면의 간단한 설명

[0014] 도 1은 본 발명의 예시적인 실시예에 따른 이동 단말기의 개략적인 블록도이다.

도 2는 본 발명의 예시적인 실시예에 따른 무선 통신 시스템의 개략적인 블록도이다.

도 3은 본 발명의 예시적인 실시예에 따른 단일 서비스 사인 온을 제공하는 시스템의 블록도를 도시한다.

도 4는 본 발명의 다른 예시적인 실시예에 따른 단일 서비스 사인 온을 제공하는 시스템의 블록도를 도시한다.

도 5는 본 발명의 예시적인 실시예에 따른 단일 서비스 사인 온을 제공하는 예시적인 방법에 따른 순서도를 도시한다.

도 6은 본 발명의 예시적인 실시예에 따른 단일 서비스 사인 온을 제공하는 예시적인 방법에 따른 순서도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0015] 본 발명의 실시예는 이제 본 발명의 전부는 아니지만 몇몇 실시예가 도시되는 첨부 도면을 참조하여 보다 완전히 후술될 것이다. 실제로, 본 발명은 다수의 상이한 형태로 구현될 수 있고 전술한 실시예로 제한되는 것으로 구성되어서는 안 되며, 오히려, 이들 실시예는 이 개시물이 적용가능한 법적 요구조건을 충족하도록 제공된다. 동일한 참조 번호는 동일한 요소를 지칭한다.

[0016] 도 1은 본 발명으로부터 이득을 얻을 수 있는 이동 단말기(10)의 블록도를 도시한다. 그러나, 도시되고 이하 설명되는 이동 단말기가 본 발명으로부터 이득을 얻을 수 있는 일 유형의 전자 장치의 예시일 뿐이므로, 본 발명의 범위를 제한하는 것으로 간주되어서는 안 됨을 알아야 한다. 전자 장치의 몇몇 실시예가 예시를 위해 도시되고 이하 설명될 것이지만, PDA, 페이저, 랩탑 컴퓨터, 데스크탑 컴퓨터, 게임 장치, 텔레비전 및 다른 유형의 전자 시스템과 같은 다른 유형의 전자 장치가 본 발명을 이용할 수 있다.

[0017] 도시된 바와 같이, 이동 단말기(10)는 송신기(14) 및 수신기(16)와 통신하는 안테나(12)를 포함할 수 있다. 이동 단말기는 또한 각각 송신기 및 수신기로 신호를 공급하고 이로부터 신호를 수신하는 제어기(20) 또는 다른 프로세서를 포함할 수 있다. 이 신호는 적용가능한 셀룰러 시스템의 무선 인터페이스 표준 및/또는 Wi-Fi, WLAN 기술, 예컨대, IEEE 802.11 등을 포함하지만 이들로 제한되지 않는 임의의 수의 상이한 무선 네트워킹 기

술에 따라 시그널링 정보를 포함할 수 있다. 또한, 이 신호는 음성 데이터, 사용자가 생성한 데이터, 사용자가 요청한 데이터 등을 포함할 수 있다. 이와 관련하여, 이동 단말기는 하나 이상의 무선 인터페이스 표준, 통신 프로토콜, 변조 유형, 액세스 유형 등을 사용하여 작동할 수 있다. 보다 구체적으로, 이동 단말기는 다양한 1 세대(1G), 2 세대(2G), 2.5G, 3 세대(3G) 통신 프로토콜, 4 세대(4G) 통신 프로토콜 등에 따라 작동할 수 있다. 예컨대, 이동 단말기는 2G 무선 통신 프로토콜 IS-136 (TDMA), GSM 및 IS-95 (CDMA)에 따라 작동할 수 있다. 또한, 예컨대, 이동 단말기는 2.5G 무선 통신 프로토콜 GPRS, EDGE 등에 따라 작동할 수 있다. 또한, 예컨대, 이동 단말기는 UMTS, CDMA2000, WCDMA 및 TD-SCDMA와 같은 3G 무선 통신 프로토콜에 따라 작동할 수 있다. 이동 단말기는 추가적으로 LTE 또는 E-UTRAN과 같은 3.9G 무선 통신 프로토콜에 따라 작동할 수 있다. 부가적으로, 예컨대, 이동 단말기는 4G 무선 통신 프로토콜 등뿐만 아니라 앞으로 개발될 수 있는 유사한 무선 통신 프로토콜에 따라 작동할 수 있다.

[0018] 듀얼 또는 더 높은 모드의 전화기(예컨대, 디지털/아날로그 또는 TDMA/CDMA/아날로그 전화기)와 같이, 몇몇 NAMPS 및 TACS 이동 단말기는 또한 본 발명의 실시예로부터 이득을 얻을 수 있다. 추가적으로, 이동 단말기(10)는 무선 Wi-Fi 프로토콜에 따라 작동할 수 있다.

[0019] 제어기(20)가 이동 단말기(10)의 오디오 및 로직 기능을 구현하는 데 필요한 회로를 포함할 수 있음을 알아야한다. 예컨대, 제어기(20)는 디지털 신호 프로세서 장치, 마이크로프로세서 장치, 아날로그/디지털 변환기, 디지털/아날로그 변환기 등일 수 있다. 이동 단말기의 제어 및 신호 처리 기능은 이들 장치 각각의 능력에 따라 이들 장치 사이에 할당될 수 있다. 제어기는 내부 음성 코더(VC)(20a), 내부 데이터 모뎀(DM)(20b) 등을 추가적으로 포함할 수 있다. 또한, 제어기는 메모리 내에 저장될 수 있는 하나 이상의 소프트웨어 프로그램을 작동시키는 기능을 포함할 수 있다. 예컨대, 제어기(20)는 웹 브라우저와 같은 접속성 프로그램을 작동시킬 수 있다. 접속성 프로그램은 이동 단말기(10)가 무선 애플리케이션 프로토콜(WAP), 하이퍼텍스트 전송 프로토콜(HTTP) 등과 같은 프로토콜에 따라 위치 기반 콘텐츠와 같은 웹 콘텐츠를 송신하고 수신하게 할 수 있다. 이동 단말기(10)는 인터넷(50)을 통해 웹 콘텐츠를 송신하고 수신하도록 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP)을 사용할 수 있다.

[0020] 이동 단말기(10)는 또한 제어기(20)에 연결될 수 있는 통상적인 이어폰 또는 스피커(24), 신호기(ringer)(22), 마이크로폰(26), 디스플레이(28), 사용자 입력 인터페이스 등을 포함하는 사용자 인터페이스를 포함할 수 있다. 도시되지는 않았지만, 이동 단말기는 이동 단말기와 관련된 다양한 회로, 예컨대, 검출가능한 출력으로서 기계적 진동을 제공하는 회로에 전력을 공급하는 배터리를 포함할 수 있다. 사용자 입력 인터페이스는 이동 단말기가 데이터를 수신하게 하는 장치, 예컨대, 키패드(30), 터치 디스플레이(도시 생략), 조이스틱(도시 생략) 및/또는 다른 입력 장치를 포함할 수 있다. 키패드를 포함하는 실시예에서, 키패드는 통상적인 숫자(0-9) 및 관련 키(#, *) 및/또는 이동 단말기를 작동시키는 다른 키를 포함할 수 있다.

[0021] 도 1에 도시된 바와 같이, 이동 단말기(10)는 또한 데이터를 공유하고/공유하거나 획득하는 하나 이상의 수단을 포함할 수 있다. 예컨대, 이동 단말기는 단거리 무선 주파수(RF) 송수신기 및/또는 질문기(interrogator)(64)를 포함할 수 있으므로, 데이터가 RF 기술에 따라 전자 장치와 공유되고/공유되거나 이로부터 획득될 수 있다. 이동 단말기는 예컨대, 적외선(IR) 송수신기(66), 블루투스™ SIG(Special Interest Group)에 의해 개발된 블루투스™ 상표 무선 기술을 사용하여 동작하는 블루투스™(BT) 송수신기(68) 등과 같은 다른 단거리 송수신기를 포함할 수 있다. 블루투스 송수신기(68)는 Wibree™ 무선 표준에 따라 작동할 수 있다. 이에 관하여, 이동 단말기(10), 특히, 단거리 송수신기는 이동 단말기의 근접성 내의, 예컨대, 10 미터 내의 전자 장치로부터 데이터를 송신하고/송신하거나 데이터를 수신할 수 있다. 도시되지는 않았지만, 이동 단말기는 Wi-Fi, WLAN 기술, 예컨대, IEEE 802.11 기술 등을 포함하는 다양한 무선 네트워킹 기술에 따라 전자 장치로부터 데이터를 송신하고/송신하거나 수신할 수 있다.

[0022] 이동 단말기(10)는 이동 가입자와 관련된 정보 요소를 저장할 수 있는 가입자 식별 모듈(SIM)(38), 분리형 사용자 식별 모듈(R-UIM) 등과 같은 메모리를 포함할 수 있다. SIM 외에, 이동 단말기는 다른 분리형 및/또는 고정형 메모리를 포함할 수 있다. 이에 관하여, 이동 단말기는 데이터의 임시 저장을 위한 캐시 영역을 포함할 수 있는 휘발성 RAM과 같은 휘발성 메모리(40)를 포함할 수 있다. 이동 단말기는 내장되고/내장되거나 분리될 수 있는 다른 비휘발성 메모리(42)를 포함할 수 있다. 비휘발성 메모리는 EEPROM, 플래시 메모리 등을 포함할 수 있다. 메모리는 이동 단말기의 기능을 수행하기 위해 이동 단말기에 의해 사용될 수 있는 하나 이상의 소프트웨어 프로그램, 인스트럭션, 정보 단편, 데이터 등을 저장할 수 있다. 예컨대, 메모리는 이동 단말기(10)를 고유하게 식별할 수 있는 IMEI(international mobile equipment identification) 코드와 같은 식별자를 포함할

수 있다.

[0023] 이제 도 2를 참조하면, 도 1의 이동 단말기와 같은 전자 장치와의 통신을 지원할 수 있는 일 유형의 시스템의 도시가 예로써 그러나 제한하지 않는 것으로 제공된다. 도시된 바와 같이, 하나 이상이 이동 단말기(10)는 각각 기지국(BS)(44)으로 신호를 송신하고 기지국(BS)(44)으로부터 신호를 수신하는 안테나(12)를 포함할 수 있다. 기지국(44)은 하나 이상의 셀룰러 또는 이동 네트워크의 일부일 수 있으며, 각각은 네트워크를 작동시키는 데 필요한 요소, 예컨대, 이동 전화 교환국(MSC)(46)을 포함할 수 있다. 당업자에게 잘 알려져 있는 바와 같이, 이동 네트워크는 기지국/MSC/상호작용 기능(BMI)으로도 지칭될 수 있다. 동작시에, MSC(46)는 이동 단말기(10)가 호출을 하고 호출을 수신할 때 이동 단말기(10)로 및 이동 단말기(10)로부터 호출을 라우팅할 수 있다. MSC(46)는 또한 이동 단말기(10)가 호출에 수반될 때 유선 트렁크에 대한 접속을 제공할 수 있다. 또한, MSC(46)는 이동 단말기(10)로 및 이동 단말기(10)로부터 메시지의 포워딩을 제어할 수 있고, 또한 메시징 센터로 및 메시징 센터로부터 이동 단말기(10)에 대한 메시지의 포워딩을 제어할 수 있다. 도 2의 시스템에 MSC(46)가 도시되지만, MSC(46)는 단지 예시적인 네트워크 장치일 뿐이며 본 발명은 MSC를 이용하는 네트워크에서 사용하도록 제한되지 않음을 알아야 한다.

[0024] MSC(46)는 LAN(local area network), MAN(metropolitan area network) 및/또는 WAN(wide area network)과 같은 데이터 네트워크에 연결될 수 있다. MSC(46)는 데이터 네트워크에 직접 연결될 수 있다. 그러나, 전형적인 일 실시예에서, MSC(46)는 GTW(48)에 연결될 수 있고, GTW(48)는 인터넷(50)과 같은 WAN에 연결될 수 있다. 그 다음으로, 처리 요소(예컨대, 개인 컴퓨터, 서버 컴퓨터 등)와 같은 장치는 인터넷(50)을 통해 이동 단말기(10)에 연결될 수 있다. 예컨대, 후술되는 바와 같이, 처리 요소는 컴퓨팅 시스템(52)(도 2에 2 개가 도시됨), 원(origin) 서버(54)(도 2에 1 개가 도시됨) 등과 연관된 하나 이상의 처리 요소를 포함할 수 있으며, 이는 후술될 것이다.

[0025] 도 2에 도시된 바와 같이, BS(44)는 또한 시그널링 GPRS(General Packet Radio Service) 지원 노드(SGSN)(56)에 연결될 수 있다. 당업자에게 알려져 있는 바와 같이, SGSN(56)은 패킷 교환 서비스에 대해 MSC(46)와 유사한 기능을 수행할 수 있다. MSC(46)와 마찬가지로, SGSN(56)은 인터넷(50)과 같은 데이터 네트워크에 연결될 수 있다. SGSN(56)은 데이터 네트워크에 직접 연결될 수 있다. 이와 달리, SGSN(56)은 GPRS 코어 네트워크(58)와 같은 패킷 교환 코어 네트워크에 연결될 수 있다. 그 다음에 패킷 교환 코어 네트워크는 GTW GPRS 지원 노드(GGSN)(60)와 같은 다른 GTW(48)에 연결될 수 있고, GGSN(60)은 인터넷(50)에 연결될 수 있다. GGSN(60) 외에, 패킷 교환 코어 네트워크는 GTW(48)에도 연결될 수 있다. 또한, GGSN(60)은 메시징 센터에 연결될 수 있다. 이에 관하여, MSC(46)와 마찬가지로 GGSN(60) 및 SGSN(56)은 MMS 메시지와 같은 메시지의 포워딩을 제어할 수 있다. GGSN(60) 및 SGSN(56)은 또한 메시징 센터로 및 메시징 센터로부터 이동 단말기(10)에 대한 메시지의 포워딩을 제어할 수 있다.

[0026] 또한, SGSN(56)을 GPRS 코어 네트워크(58) 및 GGSN(60)에 연결함으로써, 컴퓨팅 시스템(52) 및/또는 원 서버(54)와 같은 장치는 인터넷(50), SGSN(56) 및 GGSN(60)을 통해 이동 단말기(10)에 연결될 수 있다. 이에 관하여, 컴퓨팅 시스템(52) 및/또는 원 서버(54)와 같은 장치는 SGSN(56), GPRS 코어 네트워크(58) 및 GGSN(60)을 통해 이동 단말기(10)와 통신할 수 있다. 이동 단말기(10)와 다른 장치(예컨대, 컴퓨팅 시스템(52), 원 서버(54) 등)을 인터넷(50)에 직접 또는 간접적으로 연결함으로써, 이동 단말기(10)는 예컨대, 하이퍼텍스트 전송 프로토콜(HTTP)에 따라 다른 장치 및 서로 통신하여 이동 단말기(10)의 다양한 기능을 수행할 수 있다.

[0027] 모든 가능한 이동 네트워크의 모든 요소가 도 2에 도시되는 것이 아니고 본 명세서에 설명되는 것도 아니지만, 이동 단말기(10)와 같은 전자 장치가 BS(44)를 통해 다수의 상이한 네트워크 중 하나 이상의 임의의 네트워크에 연결될 수 있음을 알아야 한다. 이에 관하여, 네트워크(들)는 다수의 1세대(1G), 2세대(2G), 2.5G, 3세대(3G), 4세대(4G) 및/또는 미래의 이동 통신 프로토콜 등 중 임의의 하나 이상에 따라 통신을 지원할 수 있다. 예컨대, 하나 이상의 네트워크(들)는 2G 무선 통신 프로토콜 IS-136(TDMA), GSM 및 IS-95(CDMA)에 따라 통신을 지원할 수 있다. 또한, 예컨대, 하나 이상의 네트워크(들)는 2.5G 무선 통신 프로토콜 GPRS, 강화 데이터 GSM 환경(EDGE) 등에 따라 통신을 지원할 수 있다. 또한, 예컨대, 하나 이상의 네트워크(들)는 E-UTRAN 또는 WCDMA 무선 액세스 기술을 이용하는 UMTS 네트워크와 같은 3G 무선 통신 프로토콜에 따라 통신을 지원할 수 있다. 듀얼 또는 더 높은 모드의 이동 단말기(예컨대, 디지털/아날로그 또는 TDMA/CDMA/아날로그 전화)와 같이, 몇몇 협대역 AMPS(NAMPS) 및 TACS 네트워크도 본 발명의 실시예로부터 이득을 얻을 수 있다.

[0028] 도 2에 도시된 바와 같이, 이동 단말기(10)는 또한 하나 이상의 무선 액세스 포인트(AP)(62)에 연결될 수 있다. AP(62)는 예컨대, 무선 주파수(RF), 블루투스™(BT), 적외선(IrDA)과 같은 기술 또는 IEEE 802.11(예컨대,

802.11a, 802.11b, 802.11g, 802.11n 등)과 같은 WLAN 기술, Wibree™ 기술, IEEE 802.16과 같은 WiMAX 기술, Wi-Fi 기술 및/또는 IEEE 802.15와 같은 초광대역(UWB) 기술 등을 포함하는 다수의 상이한 무선 네트워킹 기술 중 임의의 기술에 따라 이동 단말기(10)와 통신하도록 구성된 액세스 포인트를 포함할 수 있다. AP(62)는 인터넷(50)에 연결될 수 있다. MSC(46)와 마찬가지로, AP(62)는 인터넷(50)에 직접 연결될 수 있다. 그러나, 일 실시예에서, AP(62)는 GTW(48)를 통해 인터넷(50)에 간접적으로 연결될 수 있다. 또한, 일 실시예에서, BS(44)는 다른 AP(62)로서 간주할 수 있다. 알게 되듯이, 이동 단말기(10), 컴퓨팅 시스템(52), 원 서버(54) 및/또는 다수의 다른 장치 중 임의의 장치를 인터넷(50)에 직접 또는 간접적으로 접속시킴으로써, 이동 단말기(10)는 서로, 컴퓨팅 시스템 등과 통신하여 예컨대, 컴퓨팅 시스템(52)으로 데이터, 콘텐츠 등을 송신하고/송신하거나 컴퓨팅 시스템(52)으로부터 콘텐츠, 데이터 등을 수신하도록 이동 단말기(10)의 다양한 기능을 수행할 수 있다. 본 명세서에서 사용된 바와 같이, 용어 "데이터", "콘텐츠", "정보" 및 유사 용어는 본 발명의 실시예에 따라 송신, 수신 및/또는 저장될 수 있는 데이터를 지칭하는 데 상호교환적으로 사용될 수 있다. 따라서, 그러한 용어의 사용은 본 발명의 사상 및 범위를 제한하도록 의도되어서는 안 된다.

[0029] 도 2에 도시되지는 않았지만, 이동 단말기(10)를 인터넷(50)을 통해 컴퓨팅 시스템(52) 및/또는 원 서버(54)에 연결하는 것 외에 또는 대신으로 이동 단말기(10), 컴퓨팅 시스템(52) 및 원 서버(54)는 서로에 연결될 수 있고, 예컨대, RF, BT, IrDA 또는 LAN, WLAN, WiMAX, Wi-Fi, Wibree™ 및/또는 UWB 기술을 포함하는 다수의 상이한 유선 또는 무선 통신 기술 중 임의의 기술에 따라 통신할 수 있다. 하나 이상의 컴퓨팅 시스템(52)은 추가적으로 또는 대안적으로 콘텐츠를 저장할 수 있는 분리형 메모리를 포함할 수 있으며, 그 후 콘텐츠는 이동 단말기(10)로 전송될 수 있다. 또한, 이동 단말기(10)는 프린터, 디지털 프로젝터 및/또는 다른 멀티미디어 캡처, 생성 및/또는 저장 장치(예컨대, 다른 단말기)와 같은 하나 이상의 전자 장치에 연결될 수 있다. 컴퓨팅 시스템(52)과 마찬가지로, 이동 단말기(10)는 예컨대, RF, BT, IrDA과 같은 기술 또는 USB, LAN, Wibree™, Wi-Fi, WLAN, WiMAX 및/또는 UWB 기술을 포함하는 다수의 상이한 유선 또는 무선 통신 기술 중 임의의 기술에 따라 휴대용 전자 장치와 통신하도록 구성될 수 있다. 이에 관하여, 이동 단말기(10)는 근거리 통신 기술을 통해 다른 장치와 통신할 수 있다. 가령, 이동 단말기(10)는 근거리 통신 송수신기(80)를 구비하는 하나 이상의 장치(51)와 무선 근거리 통신할 수 있다. 전자 장치(51)는 블루투스™, RFID, IR, WLAN, IrDA 등을 포함하지만 이들로 제한되지 않는 다수의 상이한 근거리 통신 기술 중 임의의 기술에 따라 데이터를 송신 및/또는 수신할 수 있는 다수의 상이한 장치 및 트랜스폰더 중 임의의 것을 포함할 수 있다. 전자 장치(51)는 다른 이동 단말기, 무선 액세서리, 장치, PDA, 페이저, 랩탑 컴퓨터, 모션 센서, 광 스위치 및 다른 유형의 전자 장치를 포함하는 다수의 상이한 이동 또는 고정 장치 중 임의의 장치를 포함할 수 있다.

[0030] 도 3은 본 발명의 예시적인 실시예에 따라 단일 서비스 사인 온을 제공하는 시스템(300)의 블록도를 도시한다. 본 명세서에 도시된 바와 같이, "예시적인"은 단지 예를 의미하고 본 발명에 대한 일 예시적인 실시예를 나타내며 어떠한 방식으로도 본 발명의 범위 또는 사상을 축소하는 것으로 해석되어서는 안 된다. 본 발명의 범위가 본 명세서에 도시되고 설명된 것 외에 다수의 가능한 실시예를 포함함을 알아야 할 것이다. 도 1의 이동 단말기 및 도 2의 시스템(47)과 관련하여 예시를 위해 시스템(300)이 설명될 것이다. 그러나, 도 3의 시스템이 이동 및 고정인 다양한 다른 장치와 관련하여 이용될 수도 있으므로, 본 발명의 실시예는 도 1의 이동 단말기(10)와 같은 장치 상의 애플리케이션으로 제한되어서는 안 된다. 또한, 도 3의 시스템이 다양한 네트워크 구성 또는 프로토콜 중 임의의 것과 관련하여 사용될 수 있으며 도 2의 시스템(47)의 양상을 사용하는 실시예로 제한되지 않음을 알아야 한다. 도 3은 단일 서비스 사인 온을 제공하는 시스템의 구성의 일례를 도시하지만, 본 발명의 실시예를 구현하는 데 다수의 다른 구성이 사용될 수도 있음을 알아야 한다.

[0031] 이제 도 3을 참조하면, 시스템(300)은 서비스 공급자(302), 계정 관리 공급자(304) 및 클라이언트 장치(306)를 포함할 수 있다. 서비스 공급자(302) 및 계정 관리 공급자(304)는 각각 임의의 컴퓨팅 장치 또는 복수의 컴퓨팅 장치의 조합으로서 구현될 수 있다. 이에 관하여, 서비스 공급자(302) 및 계정 관리 공급자(304)는 각각 예컨대, 서버 또는 서버 클러스터로서 구현될 수 있다. 시스템(300)의 엔티티는 통신 링크(308)를 통해 서로 통신할 수 있다. 이들 통신 링크는 도 2의 시스템(47)의 구조와 같은 임의의 컴퓨터 네트워크 구조일 수 있고, 서비스 공급자(302), 계정 관리 공급자(304) 및 클라이언트 장치(306) 사이의 장치 간 통신을 용이하게 할 수 있는 임의의 통신 프로토콜 또는 통신 프로토콜의 조합을 이용할 수 있다. 추가적으로, 시스템(300)은 예시를 위해 하나의 서비스 공급자(302) 및 클라이언트 장치(306)만을 도시하지만, 시스템(300)은 복수의 서비스 공급자(302) 및 클라이언트 장치(306)를 포함할 수 있다.

[0032] 서비스 공급자(302)는 원격 사용자에게 서비스를 제공할 수 있다. 본 명세서에서 사용된 바와 같이, "서비스"는 데이터 또는 다른 콘텐츠뿐만 아니라 통신 링크(308)와 같은 네트워크 또는 통신 링크를 통해 원격 컴퓨팅

장치에 의해 액세스되고/액세스되거나 공급될 수 있는 예컨대, 이메일, 인스턴트 메시징, 멀티 플레이어 게임, 피어 투 피어 파일 전송, 웹 브라우징, 소셜 네트워킹, 사진 호스팅, 비디오 호스팅 및 다른 멀티미디어 호스팅 서비스와 같은 서비스도 포함할 수 있다. 이에 관하여, 서비스는 사용자에게 몇몇 기능을 제공한다. 예시적인 실시예에서, 서비스 공급자(302)는 프로세서(310), 서비스 사용자 인터페이스(312), 클라이언트 인증 유닛(314), 메모리(316) 및 통신 인터페이스(318)를 포함할 수 있다.

[0033] 프로세서(310)는 다수의 상이한 방법으로 구현될 수 있다. 예컨대, 프로세서(310)는 마이크로프로세서, 코프로세서, 제어기 또는 예컨대, ASIC(application specific integrated circuit) 또는 FPGA(field programmable gate array)와 같은 집적 회로를 포함하는 여러 다른 처리 수단 또는 요소로서 구현될 수 있다. 예시적인 실시예에서, 프로세서(310)는 메모리(316) 내에 저장된 인스트럭션을 실행하도록 구현되거나 프로세서(310)에 액세스가능할 수 있다.

[0034] 서비스 사용자 인터페이스(312)는 통신 인터페이스(318)에 의해 수신된 사용자 입력 또는 요청의 표시를 수신하고/수신하거나 통신 인터페이스(318)를 통해 사용자에게 청각, 시각, 기계적 또는 다른 출력을 제공하도록 프로세서(310)와 통신할 수 있다. 이들 출력은 서비스 공급자(302)에 의해 제공된 서비스의 사용자의 이용 및 그 서비스와의 상호작용을 용이하게 할 수 있다. 따라서, 서비스 사용자 인터페이스(312)는 통신 인터페이스(318)를 통해 사용자 장치로, 예컨대, 통신 링크(308)에 걸쳐 클라이언트 장치(306)로 전달될 수 있는 예컨대, 웹 페이지, GUI, 또는 다른 상호작용 수단을 제공할 수 있다. 이에 관하여, 서비스 사용자 인터페이스(312)는 클라이언트 장치(306)의 인증된 사용자뿐만 아니라 서비스 공급자(302)에 의해 제공된 서비스를 호출하는 중일 수 있는 다른 서비스 공급자에게 서비스 공급자(302)에 의해 제공된 서비스를 공급하는 것을 처리하도록 구성될 수 있다.

[0035] 클라이언트 인증 유닛(314)은 하드웨어, 소프트웨어, 펌웨어 또는 이들의 몇몇 조합으로 구현될 수 있고, 프로세서(310)로서 구현되거나 프로세서(310)에 의해 제어될 수 있다. 클라이언트 인증 유닛(314)이 프로세서(310)와 별도로 구현되는 실시예에서, 클라이언트 인증 유닛(314)은 프로세서(310)와 통신할 수 있다. 클라이언트 인증 유닛(314)은 클라이언트 장치(306) 또는 다른 서비스 공급자(집합적으로 "요청 클라이언트"로 지칭됨)로부터 서비스 액세스 요청 메시지를 수신하도록 구성될 수 있다. 클라이언트 인증 유닛(314)은 서비스 액세스 요청 메시지를 구성하고 다른 서비스 공급자로 전송하도록 또한 구성될 수 있다. 예시적인 실시예에서, 클라이언트 인증 유닛(314)은 요청 클라이언트의 유형뿐만 아니라 요청을 하는 데 사용된 클라이언트 애플리케이션의 유형을 결정하도록 구성될 수 있다. 클라이언트 인증 유닛(314)은 예컨대, 요청 클라이언트 또는 사용자가 만료되지 않은 사용 세션에 대해 이전에 클라이언트 인증 유닛(314)에 의해 인증된 경우에, 요청 클라이언트 및/또는 이 사용자에 대한 기존의 사인 온 세션이 존재하는지 여부를 판단하도록 추가적으로 구성될 수 있다.

[0036] "서비스 액세스 요청 메시지"는 서비스 공급자(302)에 의해 제공된 서비스의 사용을 또는 서비스에 대한 액세스를 나타내거나 요청하는 임의의 원격 장치로부터의 임의의 메시지 또는 다른 표시일 수 있다. 이에 관하여, 서비스 액세스 요청 메시지는 하나 이상의 파라미터를 포함할 수 있다. 본 명세서에서 사용된 바와 같이, "파라미터"는 1 비트 플래그 표시자, 복수의 비트로 구성된 값 또는 표시자뿐만 아니라 메시지의 바디에 추가되거나 그 안에 포함될 수 있는 파일 또는 객체를 포함할 수 있다. 이에 관하여, 파라미터는 메시지 바디, 시그니처 또는 메시지 헤더 내에 포함될 수 있다. 서비스 액세스 요청 메시지는 예컨대, 액세스 토큰, 요청 토큰, 사용자 식별정보, 암호, 암호의 해시, 클라이언트 키, 클라이언트 시크릿, 토큰 시크릿, 서비스 시크릿 및 서비스 키와 같은 파라미터들 중 하나 이상을 포함할 수 있다. 또한, 이 파라미터들 중 하나 이상은 메시지에 서명하는 데 사용될 수 있다. 몇몇 실시예에서, 서비스 요청 메시지에 포함된 파라미터는 OAuth 프로토콜에 따를 수 있다.

[0037] 본 명세서에서 사용된 바와 같이, 용어 "액세스 토큰"은 후술되는 방식으로 계정 관리 공급자(304)에 의해 생성될 수 있는 정보를 가진 투플(tuple)을 지칭한다. 이에 관하여, "액세스 토큰"은 서비스의 특정 사용자 또는 소비자와 연관되거나, 서비스 공급자(302)에 의해 제공된 서비스에 액세스하도록 예컨대, 계정 관리 공급자(304)에 의한 결정에 기초하여 사용자가 허가를 갖는다는 표시로서 기능할 수 있다. 액세스 토큰은 또한 사용자의 액세스 권한의 시간 또는 범주와 같은 범위를 나타내는 정보를 나타내거나 이와 연관될 수 있다. 따라서, 액세스 토큰은 사용 시간, 사용 범위 및/또는 서비스의 사용 개수에서 제한될 수 있다.

[0038] 본 명세서에서 사용된 바와 같이, 용어 "요청 토큰"은 인증된 사용자 세션으로 서비스를 바인딩하는 투플을 지칭한다. 요청 토큰은 예컨대, 서비스 액세스 요청 메시지로 서비스 공급자(302)에게 제공될 수 있다. 클라이언트 인증 유닛(314)은 메시지로부터 요청 토큰을 불러오고 그것을 액세스 토큰과 교환으로 계정 관리 공급자에

게 제공하도록 구성될 수 있다. 본 명세서에서 사용된 "시크릿"은 클라이언트, 서비스 또는 토큰과 연관되는 고유한 문자숫자 값과 같은 시크릿(즉, "클라이언트 시크릿", "서비스 시크릿", 또는 "토큰 시크릿")을 지칭한다. 설명을 위해 흔히 "클라이언트 키"와 "서비스 키"로서 개별적으로 지칭되지만, 용어는 상호교환적이고 집합적으로 "클라이언트 키"로서 지칭될 수 있다. 또한, 설명을 위해 흔히 "클라이언트 시크릿"과 "서비스 시크릿"으로서 개별적으로 지칭되지만, 용어는 상호교환적이고 집합적으로 "클라이언트 시크릿"으로서 지칭될 수 있다.

[0039] 클라이언트 인증 유닛(314)은 예컨대, 파싱(parsing)함으로써 서비스 액세스 요청 메시지로부터 파라미터를 불러오거나 추출하도록 또한 구성될 수 있다. 이에 관하여, 클라이언트 인증 유닛은 토큰 정보 요청 메시지 및/또는 생성 액세스 토큰 요청 메시지를 구성하고 전송하는 데 서비스 액세스 요청 메시지로부터 추출된 파라미터를 사용하도록 구성될 수 있다. 토큰 정보 요청 메시지는 액세스 토큰에 대한 정보를 요청하는 계정 관리 공급자(304)로 지시될 수 있는 메시지를 지칭하며, 예컨대, 서비스 액세스 요청 메시지로 서비스 공급자(302)에 의해 수신될 수 있다. 생성 액세스 토큰 요청 메시지는 예컨대, 이전에 발행된 액세스 토큰과 교환으로 또는 요청 토큰과 교환으로 액세스 토큰의 생성 및 발행을 요청하는 계정 관리 공급자(304)로 지시될 수 있는 메시지를 지칭한다. 따라서, 클라이언트 인증 유닛(314)은 계정 관리 공급자(304)로부터 액세스 토큰 및 토큰 정보 메시지를 수신하도록 또한 구성될 수 있다.

[0040] 클라이언트 인증 유닛(314)은 수신된 액세스 토큰을 인증하도록 또한 구성될 수 있다. 이에 관하여, 클라이언트 인증 유닛(314)은 수신된 액세스 토큰이 사용자, 클라이언트 장치(306) 및/또는 서비스 액세스 요청을 하는 서비스 공급자와 연관되는지 및 액세스 토큰이 여전히 유효한지를 확인하도록 구성될 수 있다. 액세스 토큰의 유효성을 확인하는 것은 예컨대, 허가된 수의 사용의 시간 한계 또는 소모의 만료 때문에, 액세스 토큰이 만료되지 않았는지를 확인하는 것을 포함할 수 있다. 클라이언트 인증 유닛(314)은 예컨대, 서비스 액세스 요청에서 수신된 파라미터를 토큰 정보 메시지에서 수신된 것과 비교하는 임의의 수의 수단을 통해 이 확인을 수행하도록 구성될 수 있다. 클라이언트 인증 유닛(314)은 보안 키 및/또는 해시를 계산함으로써 액세스 토큰을 인증하도록 추가적으로 또는 대안적으로 구성될 수 있다. 이 계산은 서비스 액세스 요청 및/또는 토큰 정보 메시지에서 수신된 파라미터에 기초할 수 있다. 또한, 계산된 값은 인증 목적을 위해 서비스 액세스 요청 및/또는 토큰 정보 메시지에서 수신된 파라미터에 비교될 수 있다. 클라이언트 인증 유닛(314)은 액세스 토큰 인증의 결과에 기초하여 사용자 액세스의 레벨을 결정하도록 또한 구성될 수 있다. 따라서 클라이언트 인증 유닛(314)은 요청된 서비스에 대한 사용자 액세스의 레벨을 나타내는 인스트럭션을 제공하도록 서비스 사용자 인터페이스(312)와 통신하도록 구성될 수 있다.

[0041] 몇몇 실시예에서, 클라이언트 인증 유닛(314)은 적합한 인증 프로토콜에 따라 클라이언트 장치(306) 상에서 실행되는 웹 브라우저 애플리케이션("클라이언트 웹 브라우저 애플리케이션"으로도 지칭됨)을 통해 서비스 공급자(302)에 의해 제공된 서비스에 액세스하는 사용자에게 사용자 인증을 제공할 수 있다. 몇몇 실시예에서, 사용된 인증 프로토콜은 보안 보장 마크업 언어(SAML) 표준에 따른 것일 수 있다. 그러나, 본 발명의 실시예는 SAML의 사용으로 제한되지 않고 SAML의 사용이 본 명세서에서 논의되는 경우에, 다른 적합한 웹 프로토콜, 언어 또는 표준이 사용될 수 있음을 알 것이다. 이에 관하여, 클라이언트 인증 유닛(314)은 예컨대, 웹 페이지 인터페이스를 통해 사용자 로그온(본 명세서에서 "사인 인" 또는 "사인 온"으로도 지칭됨) 정보를 수신하고, 파라미터로서 인코딩된 인증 요청을 사용하여 웹 브라우저 애플리케이션을 계정 관리 공급자(304)로 지시하도록 구성될 수 있다. 클라이언트 인증 유닛(314)은 SAML 아티팩트(artifact)를 포함할 수 있으며 계정 관리 공급자(304)로부터 지시된 웹 브라우저 애플리케이션을 수신하도록 또한 구성될 수 있다. 몇몇 실시예에서, 클라이언트 인증 유닛(314)은 계정 관리 공급자(304)로부터 SAML 어셜션(assertion)을 수신하라는 요청에 응답하여, 계정 관리 공급자(304)에게 아티팩트를 해결하라고 요청하는 SAML 아티팩트를 포함하는 메시지를 계정 관리 공급자(304)로 전송하도록 구성될 수 있다. SAML 어셜션은 서비스 공급자(302)에게 알려져 있는 클라이언트의 계정 식별정보 또는 그 표시 및 요청 토큰을 포함할 수 있다. 클라이언트 인증 유닛(314)은 클라이언트의 웹 브라우저 애플리케이션에 클라이언트 인증 유닛(314)에 의해 결정된 사용자의 액세스 허가에 따라 인증된 사용자의 서비스 홈 페이지를 제공하라고 서비스 사용자 인터페이스(312)에 지시하도록 또한 구성될 수 있다.

[0042] 메모리(316)는 예컨대, 휘발성 및/또는 비휘발성 메모리를 포함할 수 있다. 메모리(316)는 장치가 본 발명의 예시적인 실시예에 따라 다양한 기능을 수행할 수 있게 하는 정보, 데이터, 애플리케이션, 인스트럭션 등을 저장하도록 구성될 수 있다. 예컨대, 메모리(316)는 프로세서(310)에 의해 처리될 입력 데이터를 버퍼링하도록 구성될 수 있다. 추가적으로 또는 대안적으로, 메모리(316)는 프로세서(316)에 의해 실행될 인스트럭션을 저장하도록 구성될 수 있다. 또 다른 대안으로서, 메모리(316)는 예컨대, 이동 단말기 콘텍스트 정보, 인터넷 서비

스 콘텍스트 정보, 사용자 상태 표시자, 사용자 활동 등과 관련하여 정적 및/또는 동적 정보의 형태로 정보를 저장하는 복수의 데이터베이스 중 하나일 수 있다. 이에 관하여, 메모리(316)는 예컨대, 수신된 메시지, 수신된 메시지로부터 추출된 파라미터, 등록된 서비스 사용자에 대한 정보 및/또는 등록된 클라이언트 장치(304)에 대한 정보를 저장할 수 있다. 저장된 정보는 각각의 기능을 수행하는 서비스 사용자 인터페이스(312) 및/또는 클라이언트 인증 유닛(314)에 의해 사용될 수 있다.

[0043] 통신 인터페이스(318)는 네트워크 및/또는 서비스 공급자(302)와 통신하는 임의의 다른 장치 또는 모듈과 데이터를 주고 받도록 구성되는 하드웨어, 소프트웨어, 펌웨어 또는 이들의 조합으로 구현된 임의의 장치 또는 수단으로서 구현될 수 있다. 통신 인터페이스(318)는 프로세서(310)로서 구현되거나 프로세서(310)에 의해 제어될 수 있다. 이에 관하여, 통신 인터페이스(318)는 예컨대, 안테나, 송신기, 수신기, 송수신기 및/또는 통신 링크(308)를 통해 시스템(300)의 다른 엔티티와의 통신을 가능하게 하는 지원 하드웨어 또는 소프트웨어를 포함할 수 있다. 따라서, 통신 인터페이스(318) 및 통신 링크(308)를 통해, 서비스 공급자(302)는 계정 관리 공급자(304) 및/또는 클라이언트 장치(306)와 통신할 수 있다. 이에 관하여, 통신 인터페이스(318)는 서비스 사용자 인터페이스(312), 클라이언트 인증 유닛(314) 및 메모리(316)와 통신할 수 있다. 통신 인터페이스(318)는 임의의 네트워킹 프로토콜을 사용하여 시스템(300)의 원격 장치와 통신하도록 구성될 수 있다. 예시적인 실시예에서, 통신 인터페이스(318)는 전송 계층 보안(TLS) 또는 보안 소켓 계층(SSL)과 같은 하이퍼텍스트 전송 프로토콜(HTTP) 보안 확장을 사용하여 통신하도록 구성될 수 있다. 통신 인터페이스(318)는 하이퍼텍스트 마크업 언어(HTML), 확장성 마크업 언어(XML) 및/또는 이들의 보안 확장, 예컨대, 보안 보장 마크업 언어(SAML)와 같은 다양한 웹 프로토콜에 따라 포맷된 요청, 데이터 및 메시지를 전달하고 수신하도록 또한 구성될 수 있다.

[0044] 이제 도 3의 계정 관리 공급자(304)를 참조하면, 계정 관리 공급자(304)는 등록된 서비스 사용자에 대한 데이터의 저장부로서 기능할 수 있고, 예컨대, 메모리(326)에 저장될 수 있으며 등록된 서비스 사용자와 연관된 다수의 저장된 계정 식별정보 및 암호를 포함할 수 있다. 이에 관하여, 계정 관리 공급자(304)는 복수의 등록된 서비스 사용자에 대한 데이터를 저장할 수 있고, 각각의 등록된 서비스 사용자는 사용자 이름과 같은 복수의 계정 식별정보 및 암호 조합과 연관될 수 있으며, 각각의 조합은 상이한 서비스와 연관된다. 계정 관리 공급자는 단일 서비스 사인 온 및 집중 사용자 인증 관리자를 제공하도록 복수의 서비스 공급자(302)를 관리하거나 이와 통신할 수 있다. 예시적인 실시예에서, 계정 관리 공급자(304)는 프로세서(320), 요청 유형을 결정하는 수단, 결정된 요청 유형에 기초하여 요청 내에 포함된 하나 이상의 파라미터를 추출하는 수단, 하나 이상의 보안 체크를 수행하는 수단 및 액세스 토큰을 생성하는 수단, 예컨대, 토큰 생성 유닛(322), 토큰 확인 유닛(324), 메모리(326) 및 액세스 토큰에 대한 요청을 수신하는 수단 및 통신 인터페이스(328)와 같은 원격 엔티티에 액세스 토큰을 제공하는 수단을 포함할 수 있다.

[0045] 프로세서(320)는 다수의 상이한 방법으로 구현될 수 있다. 예컨대, 프로세서(320)는 마이크로프로세서, 코프로세서, 제어기, 또는 예컨대, ASIC 또는 FPGA와 같은 집적 회로를 포함하는 여러 다른 처리 수단 또는 요소로서 구현될 수 있다. 예시적인 실시예에서, 프로세서(320)는 메모리(326)에 저장되거나 프로세서(320)에 액세스 가능한 인스트럭션을 실행하도록 구성될 수 있다.

[0046] 토큰 생성 유닛은 소프트웨어, 하드웨어, 펌웨어 또는 이들의 임의의 조합으로 구현된 임의의 장치 또는 수단으로서 구현될 수 있고, 프로세서(320)로서 구현되거나 프로세서(320) 의해 제어될 수 있다. 토큰 생성 유닛(322)은 예컨대, 토큰에 대한 요청("생성 액세스 토큰 요청 메시지"로 지칭됨)에 응답하여 액세스 토큰 및/또는 요청 토큰을 생성하도록 구성될 수 있다. 이에 관하여, 토큰 생성 유닛(322)은 예컨대, 서비스 공급자(302) 또는 클라이언트 장치(306)로부터 생성 액세스 토큰 요청 메시지를 수신하도록 구성될 수 있다. 토큰 생성 유닛(322)은 예컨대, 생성 액세스 토큰 요청 내에 포함된 파라미터에 기초하여 생성 액세스 토큰 요청의 유형을 결정하도록 구성될 수 있다. 생성 액세스 토큰 요청 유형은 예컨대, 사용자 식별정보 및 암호 조합 -액세스 토큰은 수신된 사용자 식별정보 및/또는 암호에 기초하여 생성될 수 있음- 과, 요청 토큰 교환 -액세스 토큰은 수신된 요청 토큰에 기초하여 생성될 수 있음- 및 액세스 토큰 교환 -액세스 토큰이 토큰 생성 유닛(322)에 의해 이전에 생성되고 발행될 수 있는 수신된 액세스 토큰에 기초하여 생성될 수 있음- 을 포함할 수 있다. 따라서, 토큰 생성 유닛(322)은 결정된 요청 유형에 기초하여 생성 액세스 토큰 요청 메시지에 포함된 하나 이상의 파라미터를 추출하도록 구성될 수 있다. 이들 파라미터는 예컨대, 사용자 식별정보, 암호의 해시, 클라이언트 키, 클라이언트 시크릿, 이전에 발행된 액세스 토큰 및 요청 토큰 중 하나 이상을 포함할 수 있다.

[0047] 토큰 생성 유닛(322)은 요청 사용자 또는 클라이언트를 인증하도록 하나 이상의 보안 체크를 수행하는 데 추출된 파라미터를 사용하도록 구성될 수 있다. 예컨대, 토큰 생성 유닛(322)은 추출된 파라미터를 메모리(326)에 저장된 사용자 데이터와 비교할 수 있다. 이에 관하여, 토큰 생성 유닛(322)은 추출된 사용자 식별정보와 암호

가 알려져 있으며 서로 대응하는지 확인할 수 있다. 토큰 생성 유닛(322)은 요청 서비스 공급자(302) 또는 클라이언트 장치(30)의 식별정보와 같은 클라이언트 식별정보와 사용자 식별정보 및 요청된 서비스 사이의 연관을 확인하도록 추가적으로 또는 대안적으로 구성될 수 있다. 추가적으로 또는 대안적으로, 토큰 생성 유닛(322)은 생성 액세스 토큰 요청 메시지에 포함된 시그니처를 확인하도록 구성될 수 있다. 추가적으로 또는 대안적으로, 토큰 생성 유닛(322)은 추출된 요청 토큰, 클라이언트 키, 클라이언트 시크릿 및 요청된 서비스 사이의 연관을 확인하도록 또한 구성될 수 있다. 또한 추가적으로 또는 대안적으로, 토큰 생성 유닛(322)은 추출된 이전에 발행된 액세스 토큰, 연관된 토큰 시크릿, 클라이언트 시크릿 및 요청된 서비스 사이의 연관을 확인하도록 구성될 수 있다. 또한, 토큰 생성 유닛(322)은 요청 사용자 또는 클라이언트와 연관된 사전정의된 허가 레벨을 나타낼 수 있는 메모리(326)에 저장된 데이터에 기초하여 보안 체크를 수행하도록 구성될 수 있다.

[0048] 수행된 보안 체크의 결과에 기초하여, 토큰 생성 유닛(322)은 특정 콘텐츠에 대한 액세스 또는 서비스 제공의 범위, 사용 권한 또는 한계, 만료 시간, 허용가능한 사용의 수, 허가가능한 사용자의 수 및/또는 연관된 허가가능한 사용자(들)의 표시, 액세스 토큰이 사용될 수 있는 하나 이상의 연관된 서비스의 표시와 같은 한정된 서비스 액세스 권한 및/또는 요청과 연관된 사용자, 생성 액세스 토큰 요청과 연관된 요청된 서비스, 및/또는 요청 클라이언트 장치(306)에 기초하여 다른 유사한 권한 또는 제약을 가진 액세스 토큰을 생성하도록 구성될 수 있다. 이에 관하여, 몇몇 요청 사용자 또는 클라이언트는, 신뢰받는 사용자 또는 신뢰받는 클라이언트가 일반 사용자 또는 클라이언트보다 더 많은 서비스 사용 또는 액세스 권한을 가질 수 있다는 점에서 다른 것보다 더 "신뢰받을 수 있다". 예컨대, 만일 사진 호스팅 서비스 및 음악 호스팅 서비스가 각각 저장 서비스를 사용하려고 시도하는 클라이언트로서 작용하면, 사진 호스팅 서비스는 예컨대, 각각의 요청 서비스에 의해 요구되거나 요청되는 저장 공간 또는 저장 서비스 상의 음악 파일을 잠재적으로 침해하는 음악 호스팅 서비스 저장에 의해 발생할 수 있는 지적재산권 염려에 기초하여, 음악 호스팅 서비스보다 더 신뢰받을 수 있고 저장 서비스에 대한 더 큰 사용 권한을 받을 수 있다.

[0049] 토큰 생성 유닛(322)은 SAML 아티팩트를 해결하라는 요청을 수신하는 것에 응답하여 요청 토큰을 생성하도록 또한 구성될 수 있다. 추가적으로, 토큰 생성 유닛(322)은 생성된 액세스 토큰 또는 요청 토큰을 요청하는 서비스 공급자(302) 또는 클라이언트 장치(306)로 제공하도록 구성될 수 있다. 따라서, 토큰 생성 유닛(322)은 예컨대, 메시지 내의 파라미터로서 생성된 액세스 토큰 또는 요청 토큰을 요청 엔티티로 전송하거나 예컨대, 메모리(326) 내의 계정 관리 공급자(304) 상에 저장된 생성된 토큰에 액세스하거나 다운로드하는 수단을 원격 엔티티에 제공할 수 있다. 토큰 확인 유닛(324)은 하드웨어, 소프트웨어, 펌웨어 또는 이들의 조합으로 구현된 임의의 장치 또는 수단으로서 구현될 수 있고, 프로세서(320)로서 구현되거나 프로세서(320)에 의해 제어될 수 있다. 토큰 확인 유닛(324)은 서비스 공급자(302)로부터 토큰 정보 요청 메시지를 수신하도록 구성될 수 있다. 토큰 정보 요청 메시지는 액세스 토큰을 포함할 수 있고 몇몇 실시예에서, 토큰 정보 요청 메시지는 토큰 정보 요청 메시지가 수신되었던 서비스 공급자와 연관된 서비스 키 및 서비스 시크릿을 더 포함할 수 있다. 토큰 정보 요청 메시지가 서비스 키 및 서비스 시크릿을 포함하는 몇몇 실시예에서, 서비스 키 및 서비스 시크릿은 토큰 정보 요청 메시지가 서명되는 시그니처에 포함될 수 있다. 따라서 토큰 확인 유닛(324)은 액세스 토큰, 서비스 키 및 서비스 시크릿 사이의 연관을 확인하도록 구성될 수 있다. 이 확인은 예컨대, 메모리(326)에 저장될 수 있는 발행된 액세스 토큰 또는 다른 액세스 토큰의 데이터베이스에 기초할 수 있다.

[0050] 추가적으로, 토큰 확인 유닛(324)은 액세스 토큰과 연관되는 사용자 식별정보, 토큰 시크릿 및 클라이언트 시크릿 중 하나 이상을 결정하도록 구성될 수 있다. 사용자 식별정보, 토큰 시크릿 및 클라이언트 시크릿은 예컨대, 메모리(326) 내의 액세스 토큰의 표시와 관련하여 저장될 수 있다. 이에 관하여, 토큰 확인 유닛(324)에 의해 결정된 사용자 식별정보는 토큰 정보 요청이 수신되었던 서비스 공급자(302)에게 알려져 있는 사용자 또는 클라이언트의 사용자 식별정보이다. 이 사용자 식별정보는 사용자 또는 클라이언트가 계정 관리 공급자(304)에게 알려져 있는 계정 식별정보와 동일하지 않을 수 있고, 요청 서비스 공급자(302)와 다른 서비스 공급자에게 알려져 있는 사용자 식별정보와 다를 수도 있다. 따라서, 토큰 확인 유닛(324)은 토큰 정보 요청 메시지에 응답하여 서비스 공급자(302)로 결정된 사용자 식별정보, 클라이언트 키 및 토큰 시크릿 중 하나 이상을 포함하는 메시지를 전송하도록 또한 구성될 수 있다.

[0051] 메모리(326)는 예컨대, 휘발성 및/또는 비휘발성 메모리를 포함할 수 있다. 메모리(326)는 장치가 본 발명의 예시적인 실시예에 따라 다양한 기능을 수행할 수 있게 하는 정보, 데이터, 애플리케이션, 인스트럭션 등을 저장하도록 구성될 수 있다. 예컨대, 메모리(326)는 프로세서(320)에 의해 처리될 입력 데이터를 버퍼링하도록 구성될 수 있다. 추가적으로 또는 대안적으로, 메모리(326)는 프로세서(326)에 의해 실행될 인스트럭션을 저장하도록 구성될 수 있다. 이에 관하여, 메모리(326)는 예컨대, 수신된 메시지, 수신된 메시지로부터 추출된 파

라미터, 등록된 계정 사용자, 등록된 서비스 공급자에 대한 정보 및/또는 등록된 클라이언트 장치(304)에 대한 정보를 저장할 수 있다. 이 저장된 정보는 각각의 기능을 수행하는 토큰 생성 유닛(322) 및/또는 토큰 확인 유닛(324)에 의해 사용될 수 있다.

[0052] 통신 인터페이스(328)는 네트워크 및/또는 계정 관리 공급자(304)와 통신하는 임의의 다른 장치 또는 모듈과 데이터를 주고 받도록 구성되는 하드웨어, 소프트웨어, 펌웨어 또는 이들의 조합으로 구현된 임의의 장치 또는 수단으로서 구현될 수 있다. 통신 인터페이스(328)는 프로세서(320)로서 구현되거나 프로세서(320)에 의해 제어될 수 있다. 이에 관하여, 통신 인터페이스(328)는 예컨대, 안테나, 송신기, 수신기, 송수신기 및/또는 통신 링크(308)를 통해 시스템(300)의 다른 엔티티와의 통신을 가능하게 하는 지원 하드웨어 또는 소프트웨어를 포함할 수 있다. 따라서, 통신 인터페이스(328) 및 통신 링크(308)를 통해, 계정 관리 공급자(304)는 서비스 공급자(302) 및/또는 클라이언트 장치(306)와 통신할 수 있다. 이에 관하여, 통신 인터페이스(328)는 토큰 생성 유닛(322), 토큰 확인 유닛(324) 및 메모리(326)와 통신할 수 있다. 통신 인터페이스(328)는 임의의 네트워킹 프로토콜을 사용하여 시스템(300)의 원격 장치와 통신하도록 구성될 수 있다. 예시적인 실시예에서, 통신 인터페이스(328)는 전송 계층 보안(TLS) 또는 보안 소켓 계층(SSL)과 같은 하이퍼텍스트 전송 프로토콜(HTTP) 보안 확장을 사용하여 통신하도록 구성될 수 있다. 통신 인터페이스(328)는 하이퍼텍스트 마크업 언어(HTML), 확장성 마크업 언어(XML) 및/또는 이들의 보안 확장, 예컨대, 보안 보장 마크업 언어(SAML)와 같은 다양한 웹 프로토콜에 따라 포맷된 요청, 데이터 및 메시지를 전달하고 수신하도록 또한 구성될 수 있다.

[0053] 이제 도 3의 클라이언트 장치(306)를 참조하면, 클라이언트 장치(306)는 사용자가 서비스 공급자(302)에 의해 제공된 서비스에 액세스하거나 그 서비스를 사용할 수 있는 임의의 컴퓨팅 장치일 수 있다. 몇몇 실시예에서, 클라이언트 장치(306)는 도 1의 이동 단말기(10)일 수 있다. 그러나, 클라이언트 장치(306)는 좁게 한정되지 않으며, 예컨대, 데스크탑 컴퓨팅 장치, 랩탑 컴퓨팅 장치 및 PDA로서 또한 구현될 수 있다. 또한, 도 3에는 단일 클라이언트 장치(306)만 도시되지만, 복수의 클라이언트 장치(306)가 시스템(300)에 포함될 수 있음을 알 것이다. 예시적인 실시예에서, 클라이언트 장치(306)는 프로세서(330), 애플리케이션 사용자 인터페이스(332), 통신 인터페이스(334) 및 메모리(336)를 포함할 수 있다.

[0054] 프로세서(330)는 다수의 상이한 방법으로 구현될 수 있다. 예컨대, 프로세서(330)는 마이크로프로세서, 코프로세서, 제어기 또는 예컨대, ASIC 또는 FPGA와 같은 집적 회로를 포함하는 여러 다른 처리 수단 또는 요소로서 구현될 수 있다. 예시적인 실시예에서, 프로세서(330)는 메모리(336)에 저장되고 프로세서(330)에 액세스 가능한 인스트럭션을 실행하도록 구성될 수 있다. 클라이언트 장치(306)가 이동 단말기(10)인 실시예에서, 프로세서(330)는 제어기(20)로서 구현될 수 있다.

[0055] 애플리케이션 사용자 인터페이스(332)는 소프트웨어, 하드웨어, 펌웨어 또는 이들의 조합으로서 구현될 수 있고 프로세서(330)로서 구현되거나 프로세서(330)에 의해 제어될 수 있다. 애플리케이션 사용자 인터페이스(332)는 서비스 공급자(302)에 의해 제공된 서비스에 대한 액세스 및/또는 서비스의 사용을 용이하게 하는 임의의 애플리케이션으로서 구현되거나 이를 포함할 수 있다. 이에 관하여, 애플리케이션 사용자 인터페이스(332)는 예컨대, 사진 클라이언트 업로더, 이메일 애플리케이션, 게임 애플리케이션, 멀티미디어 플레이어 애플리케이션 등과 같은 전용 애플리케이션일 수 있다. 추가적으로 또는 대안적으로, 애플리케이션 사용자 인터페이스(332)는 네트워크를 통해 서비스 공급자(302)에 의해 제공된 서비스에 대한 액세스 및/또는 서비스의 이용을 가능하게 하는 웹 브라우저 애플리케이션과 같은 범용 애플리케이션으로서 구현되거나 이를 포함할 수 있다. 애플리케이션 사용자 인터페이스(332)는 또한 웹 브라우저 애플리케이션 플러그 인, 스크립트 및/또는 네트워크를 통해 분산 방식으로 배치될 수 있는 애플리케이션으로서 구현되거나 이들을 포함할 수 있다. 애플리케이션 사용자 인터페이스(332)는 키보드, 마우스, 조이스틱, 터치 스크린 디스플레이, 통상적인 디스플레이, 마이크로폰, 스피커 또는 다른 입력/출력 메커니즘과 같은 애플리케이션 사용자 인터페이스(332)에 대한 사용자 입력의 표시를 수신하도록 또한 구성될 수 있다. 예컨대, 애플리케이션 사용자 인터페이스(332)는 서비스를 사용하기 위한 요청, 서비스와의 상호작용뿐만 아니라 사용자 이름 및 암호와 같은 사인 온 정보의 입력을 수신하도록 구성될 수 있다. 추가적으로, 애플리케이션 사용자 인터페이스(332)는 클라이언트 장치(306)의 사용자에게 오디오/시각 출력을 제공하도록 구성될 수 있다. 이에 관하여, 출력은 서비스 공급자(302) 및 계정 관리 공급자(304)로부터 수신된 데이터, 서비스, 콘텐츠, 메시지 및/또는 요청을 포함할 수 있다.

[0056] 통신 인터페이스(334)는 네트워크 및/또는 클라이언트 장치(306)와 통신하는 임의의 다른 장치 또는 모듈과 데이터를 주고 받도록 구성되는 하드웨어, 소프트웨어, 펌웨어 또는 이들의 조합으로 구현된 임의의 장치 또는 수단으로서 구현될 수 있다. 통신 인터페이스(334)는 프로세서(330)로서 구현되거나 프로세서(330)에 의해 제어될 수 있다. 이에 관하여, 통신 인터페이스(334)는 예컨대, 안테나, 송신기, 수신기, 송수신기 및/또는 통신

링크(308)를 통해 시스템(300)의 다른 엔티티와의 통신을 가능하게 하는 지원 하드웨어 또는 소프트웨어를 포함할 수 있다. 따라서, 통신 인터페이스(334) 및 통신 링크(308)를 통해, 클라이언트 장치(306)는 서비스 공급자(302) 및/또는 계정 관리 공급자(304)와 통신할 수 있다. 이에 관하여, 통신 인터페이스(334)는 애플리케이션 사용자 인터페이스(332) 및 메모리(336)와 통신할 수 있다. 통신 인터페이스(334)는 임의의 네트워킹 프로토콜을 사용하여 시스템(300)의 원격 장치와 통신하도록 구성될 수 있다. 예시적인 실시예에서, 통신 인터페이스(334)는 전송 계층 보안(TLS) 또는 보안 소켓 계층(SSL)과 같은 하이퍼텍스트 전송 프로토콜(HTTP) 보안 확장을 사용하여 통신하도록 구성될 수 있다. 통신 인터페이스(334)는 하이퍼텍스트 마크업 언어(HTML), 확장성 마크업 언어(XML) 및/또는 이들의 보안 확장, 예컨대, 보안 보장 마크업 언어(SAML)와 같은 다양한 웹 프로토콜에 따라 포맷된 요청, 데이터 및 메시지를 전달하고 수신하도록 또한 구성될 수 있다.

[0057] 메모리(336)는 예컨대, 휘발성 및/또는 비휘발성 메모리(예컨대, 클라이언트 장치(306)가 이동 단말기(10)인 실시예에서 휘발성 메모리(40) 및 비휘발성 메모리(42))를 포함할 수 있다. 메모리(336)는 장치가 본 발명의 예시적인 실시예에 따라 다양한 기능을 수행할 수 있게 하는 정보, 데이터, 애플리케이션, 인스트럭션 등을 저장하도록 구성될 수 있다. 예컨대, 메모리(336)는 프로세서(330)에 의해 처리될 입력 데이터를 버퍼링하도록 구성될 수 있다. 추가적으로 또는 대안적으로, 메모리(336)는 프로세서(336)에 의해 실행될 인스트럭션을 저장하도록 구성될 수 있다. 이에 관하여, 메모리(336)는 예컨대, 계정 관리 공급자(304) 및/또는 복수의 서비스 공급자(302)에 대해 사용된 사용자 식별정보 및 임의의 연관된 암호와 같은 사용자 계정 정보를 저장할 수 있다. 몇몇 실시예에서, 이 계정 관리 정보의 일부 또는 전부는 애플리케이션 사용자 인터페이스(332) 내에 포함된 웹 브라우저 애플리케이션에 의해 액세스되고 사용될 수 있는 쿠키의 형태로 저장될 수 있다. 메모리는 계정 관리 공급자(304)로부터 수신될 수 있는 액세스 토큰을 또한 저장할 수 있다. 이 저장된 정보는 애플리케이션 사용자 인터페이스(332)에 의해 사용될 수 있다.

[0058] 이제 도 4를 참조하면, 시스템(300)의 보다 특정한 실시예가 도시된다. 도 4의 시스템은 도시된 네트워크를 통해 상호접속되는, 클라이언트 웹 브라우저 애플리케이션(400), 사진 서비스(402), 계정 관리 공급자(304), 저장 장치(406) 및 사진 클라이언트 애플리케이션(408)을 포함한다. 이에 관하여, 사진 서비스(402) 및 저장 서비스(406)는 사진 호스팅 및 액세스 서비스 및 파일 저장 서비스를 각각 제공하는 서비스 공급자(302)의 특정 실시예를 나타낸다. 클라이언트 웹 브라우저 애플리케이션(400) 및 사진 클라이언트 애플리케이션(408)은 애플리케이션 사용자 인터페이스(332)의 예시적인 실시예이고 동일한 클라이언트 장치(306) 또는 개별 클라이언트 장치(306) 내에 구현될 수 있다. 예시적인 사용 경우 시나리오는 이제 도 4의 시스템 및 시스템(300)의 엔티티와 관련하여 설명될 것이다. 이 사용 경우 시나리오는 단지 예시용으로만 제공되며, 본 발명을 사용 경우 시나리오에 설명된 엔티티, 서비스, 통신 프로토콜 또는 동작 순서에 관하여 임의의 방식으로 제한하는 것으로 해석되어서는 안 된다.

[0059] 사진 클라이언트 애플리케이션(408)을 사용하는 사용자는 사진 서비스(402)에서 사진 앨범에 액세스하기를 원할 수 있다. 사진 클라이언트 애플리케이션(408)은 사진 서비스(402)에 액세스하도록 액세스 토큰을 필요로 할 수 있고, 계정 관리 공급자(304)로부터 액세스 토큰을 획득할 수 있다. 따라서 사진 클라이언트 애플리케이션(408)은 생성 액세스 토큰 요청 메시지를 구성할 수 있다. 이 메시지는 XML로 포맷될 수 있고 계정 관리 공급자(304)에게 알려져 있는 사용자 식별정보 및 사용자의 암호를 포함할 수 있다. 사진 클라이언트 애플리케이션(408)은 메모리(336)와 같은 메모리로부터 사용자 식별정보 및 암호를 불러올 수 있고 또는 사용자에게 사용자 식별정보 및 암호를 입력하라고 프롬프트할 수 있다. 그 다음에 사진 클라이언트 애플리케이션은 클라이언트 키 및 클라이언트 시크릿을 사용하여 생성 액세스 토큰 요청 메시지에 서명할 수 있다. 키 및 시그니처는 HTTP 헤더 내에 전달될 수 있다. 생성 액세스 토큰 요청 메시지는 TLS HTTP 접속(http)을 통해 계정 관리 공급자(304)로 전송될 수 있다.

[0060] 계정 관리 공급자(304)의 토큰 생성 유닛(322)은 수신된 생성 액세스 토큰 요청 메시지의 요청 유형이 사용자 식별정보 및 암호 조합이라고 결정하고, 생성 액세스 토큰 요청 메시지로부터 사용자 식별정보, 암호, 클라이언트 키 및 클라이언트 시크릿을 추출할 수 있다. 토큰 생성 유닛(322)은 추출된 파라미터에 기초하여 보안 체크를 수행하는 동안에 사용자 식별정보 및 암호뿐만 아니라 클라이언트 키, 생성 액세스 토큰 요청 메시지의 시그니처, 및 클라이언트 식별정보, 사용자 식별정보 및 사진 서비스 사이의 연관을 확인할 수 있다. 토큰 생성 유닛(322)이 생성 액세스 토큰 요청 메시지를 정확히 확인한다고 가정하면, 토큰 생성 유닛(322)은 액세스 토큰을 생성할 수 있고 그것을 요청 사용자에 대한 인증 세션, 사진 서비스(402) 및 토큰 시크릿과 연관시킬 수 있다. 토큰 생성 유닛(322)은 사진 클라이언트 애플리케이션(408)으로 액세스 토큰 및 토큰 시크릿을 포함하는 메시지를 전송할 수 있다. 사진 클라이언트 애플리케이션(408)은 이제 수신된 액세스 토큰을 사용하여 사진 서비스

(402)에 액세스할 수 있다.

[0061] 사용자로부터의 요청에 응답하여, 사진 클라이언트 애플리케이션(408)은 사진 서비스(402)로 사진을 업로드하기 위한 메시지를 구성할 수 있다. 사진 서비스(402)와 상호작용하도록 사진 클라이언트 애플리케이션(408)에 의해 사용된 인터페이스 및 통신 프로토콜은 사진 서비스(402) 및 사진 클라이언트 애플리케이션(408)이 사용하도록 구성되고 따라서 본 발명의 실시예에 의해 임의의 방식으로 제한되지 않는 임의의 인터페이스 및 통신 프로토콜에 따른 것일 수 있다. 그러나, 일반적으로, 사진 클라이언트 애플리케이션(408)은 예컨대, 액세스 토큰, 하나 이상의 사진 파일, 사진 앨범 식별자 및 사진 파일과 연관된 캡션(caption)과 같은 임의의 연관 데이터를 포함하는 메시지를 구성할 수 있다. 사진 클라이언트 애플리케이션(408)은 클라이언트 시크릿과 토큰 시크릿의 접합(concatenation)으로 메시지에 서명할 수 있고, 시그니처, 액세스 토큰 및 클라이언트 키를 메시지 헤더 내에 배치할 수 있다. 이에 관하여, 액세스 토큰은 메시지 내의 토큰으로서 및 발신자 키의 일부로서 사용되어 메시지에 서명할 수 있다. 따라서 장명(long-lived) 클라이언트 키와 클라이언트 시크릿이 클라이언트 장치(306)로부터 해킹될 수 있는 동안, 토큰 키 및 토큰 시크릿이 계정 관리 공급자(304)에 의해 임의로 생성되고 발행되며 비교적 단명(short-lived)이므로, 액세스 토큰은 클라이언트 애플리케이션 키와 연관된 보안 취약성을 극복하는 데 사용될 수 있다. 사진 클라이언트 애플리케이션은 예컨대, HTTP를 사용함으로써 사진 서비스(402)로 사진 업로드 메시지를 전송할 수 있다.

[0062] 사진 서비스(402)는 사진 클라이언트 애플리케이션으로부터 사진 업로드 메시지를 수신할 수 있고, 메시지 내에 포함된 액세스 토큰을 불러올 수 있다. 현재, 사진 서비스(402)는 액세스 토큰이 연관되는 사진 서비스의 사용자가 무엇인지 알지 못할 수 있으므로 토큰 정보 요청 메시지를 구성하고 이를 계정 관리 공급자(304)로 전송할 수 있다. 사진 서비스(402)는 그 자신의 서비스 키 및 서비스 시크릿을 사용하여 메시지에 서명할 수 있다. 메시지는 TLS에 따라 전송될 수 있다. 토큰 정보 요청 메시지의 수신시에, 계정 관리 공급자(304)는 토큰 정보 요청 메시지에 포함된 액세스 토큰, 서비스 키 및 서비스 시크릿 사이의 연관을 확인하는 단계와 같은 다수의 확인 단계를 수행할 수 있다. 이어서 계정 관리 공급자(304)의 토큰 확인 유닛(324)은 액세스 토큰, 토큰 시크릿 및 액세스 토큰을 획득하고 사용자 식별정보, 토큰 시크릿 및 클라이언트 키를 포함하는 토큰 정보 메시지를 구성하는 데 사용되었던 클라이언트 키와 연관되는 사진 서비스(402)에 알려져 있는 바와 같이 사용자 식별정보를 결정할 수 있고, 사진 서비스(402)로 토큰 정보 메시지를 전송할 수 있다.

[0063] 토큰 정보 메시지의 수신시에, 사진 서비스(402)의 클라이언트 인증 유닛(314)은 토큰 정보 메시지에 포함된 파라미터를 추출하고, 토큰 정보 메시지 내에 수신된 클라이언트 키가 사진 클라이언트 애플리케이션(408)으로부터 사진 업로드 메시지 내에 수신된 클라이언트 키와 일치하는지 확인할 수 있다. 이어서 사진 서비스(402)는 사진 업로드 메시지 상의 시그니처를 확인할 수 있고 또한 액세스 토큰이 연관되는 사용자가 여전히 업로드 사진에 대한 액세스 허가를 가지는지 확인할 수 있다. 사진 서비스(402)는 업로드된 사진의 저장을 위해 저장 서비스(406)를 사용할 수 있다. 사진 서비스(402)가 저장 서비스(406)를 호출하게 하기 위해, 사진 서비스(402)는 적합한 액세스 토큰을 필요로 한다. 따라서, 사진 서비스(402)는 사진 클라이언트 애플리케이션(408)으로부터 수신된 액세스 토큰 및 예컨대, 저장 서비스(406)의 DNS 이름과 같은 저장 서비스(406)의 표시를 포함하는 생성 액세스 토큰 요청 메시지를 구성할 수 있다. 사진 서비스(402)는 서비스 시크릿 및 액세스 토큰 시크릿을 사용하여 생성 액세스 토큰 요청 메시지에 서명할 수 있고, 생성 액세스 토큰 요청 메시지를 계정 관리 공급자로 전송할 수 있다. 메시지는 예컨대, TLS 프로토콜에 따라 전송될 수 있다.

[0064] 생성 액세스 토큰 요청 메시지를 수신하면, 계정 관리 공급자(304)의 토큰 생성 유닛(322)은 요청 유형이 액세스 토큰 교환이라고 결정하고, 메시지로부터 이전에 발행된 액세스 토큰, 서비스 시크릿 및 토큰 시크릿을 추출할 수 있다. 이어서 토큰 생성 유닛(322)은 액세스 토큰, 토큰 시크릿 및 서비스 시크릿 사이의 연관을 확인할 수 있다. 토큰 생성 유닛(322)은 수신된 액세스 토큰이 연관되는 사용자 또는 클라이언트 및/또는 사진 서비스(402)가 저장 서비스(406)에 액세스하기 위한 허가를 가지는지 또한 확인할 수 있다. 토큰 생성 유닛(322)이 생성 액세스 토큰 요청 메시지 및 저장 서비스(406)에 액세스하기 위한 허가를 정확히 확인한다고 가정하면, 이전과 같이, 토큰 생성 유닛(322)은 액세스 토큰을 생성하고 그것을 요청 사용자에 대한 인증 세션, 저장 서비스(406) 및 토큰 시크릿과 연관시킬 수 있다. 이어서 토큰 생성 유닛(322)은 새롭게 생성된 액세스 토큰 및 토큰 시크릿을 포함하는 메시지를 사진 서비스(402)로 전송할 수 있다.

[0065] 새롭게 생성된 액세스 토큰을 포함하는 메시지의 계정 관리 공급자(304)로부터 메시지를 수신할 때, 사진 서비스(402)는 새로운 액세스 토큰 및 사진 파일을 포함하는 저장 파일 메시지를 생성할 수 있다. 사진 서비스(402)는 자신의 서비스 시크릿과 새로운 토큰 시크릿의 접합을 사용하여 저장 파일 메시지에 서명할 수 있다. 사진 서비스(402)는 예컨대, 서비스 키, 새로운 액세스 토큰 및 시그니처를 HTTP 허가 헤더 내에 배치할 수 있

고, 저장 파일 메시지를 저장 서비스(406)로 전송할 수 있다. 이어서 저장 서비스(406)의 클라이언트 인증 유닛(314)은 수신된 저장 파일 메시지로부터 액세스 토큰을 파싱할 수 있고, 파싱된 액세스 토큰을 포함하는 토큰 정보 요청 메시지를 구성할 수 있다. 그 다음에 저장 서비스(406)의 클라이언트 인증 유닛(314)은 저장 서비스 키 및 저장 서비스 시크릿을 사용하여 토큰 정보 요청 메시지에 서명할 수 있고, 예컨대, TLS를 사용하여 토큰 정보 요청 메시지를 계정 관리 공급자(304)로 전송할 수 있다.

[0066] 토큰 정보 요청 메시지의 수신시에, 계정 관리 공급자(304)는 이전과 같이 토큰 정보 요청 메시지 내에 포함된 액세스 토큰, 서비스 키 및 서비스 시크릿 사이의 연관을 확인하는 단계와 같은 다수의 확인 단계를 수행할 수 있다. 이어서 계정 관리 공급자(304)의 토큰 확인 유닛(324)은 액세스 토큰, 토큰 시크릿 및 액세스 토큰을 획득하고 사용자 식별정보, 토큰 시크릿 및 사진 서비스 키를 포함하는 토큰 정보 메시지를 구성하는 데 사용되었던 사진 서비스 키(하나의 서비스 공급자가 제 2 서비스 공급자를 호출하고 있는 이 경우에, 제 1 서비스 공급자, 예컨대, 사진 서비스는 클라이언트로서 작용하고 있고, 본질적으로 사진 서비스 키는 클라이언트 키와 동일함을 알아야 한다)와 연관되는 저장 서비스(406)에 알려져 있는 바와 같이 사용자 식별정보를 결정할 수 있고, 저장 서비스(406)로 토큰 정보 메시지를 전송할 수 있다.

[0067] 이어서 저장 서비스(406)의 클라이언트 인증 유닛(314)은 저장 파일 메시지에 포함된 사진 서비스 키를 계정 관리 공급자(304)로부터 토큰 정보 메시지 내에 수신된 사진 서비스 키와 비교함으로써 그 사진 서비스 키를 확인할 수 있다. 저장 서비스(406)의 클라이언트 인증 유닛(314)은 토큰 시크릿 및 사진 서비스 시크릿을 사용하여 저장 파일 메시지 상의 시그니처를 추가적으로 확인할 수 있다. 만일 저장 서비스가 저장 파일 메시지를 정확히 확인하면, 저장 서비스(406)는 사용자 식별정보를 사용하여, 저장 파일 메시지에 포함된 사진 데이터를 어떤 계정 저장 공간 내에 저장할지를 결정할 수 있다.

[0068] 얼마 후에, 사용자는 자신의 온라인 사진 앨범을 구성하기를 원할 수 있으므로 클라이언트 웹 브라우저 애플리케이션(400)을 사용하여 예컨대, 사진 서비스(402)의 서비스 사용자 인터페이스(312)에 의해 제공될 수 있는 사진 서비스(402)의 웹 사용자 인터페이스를 브라우징할 수 있다. 사진 서비스(402)의 서비스 사용자 인터페이스(312)는 예컨대, 클라이언트 웹 브라우저 애플리케이션(400)이 사진 클라이언트 애플리케이션(408)과 다른 클라이언트 장치 상에 구현되거나 이전 로그인 세션이 만료된 경우에, 사용자에 대한 기존의 세션이 존재하지 않으면, 클라이언트 웹 브라우저 애플리케이션(400)에 로그인 폼을 제공할 수 있다. 이어서 사용자는 적합한 로그인 정보를 입력할 수 있고 사진 서비스(420)의 클라이언트 인증 유닛(314)은 클라이언트 웹 브라우저 애플리케이션(400)을 URL 파라미터로서 인코딩된 인증 요청을 가진 계정 관리 공급자(304)의 인증 요청 엔드포인트로 재지시할 수 있다. 이어서 계정 관리 공급자(304)는 사용자 로그인 정보를 확인할 수 있고 클라이언트 웹 브라우저 애플리케이션을 파라미터로서 SAML 아티팩트를 가진 사진 서비스(402)로 재지시할 수 있다. 그 다음에 클라이언트 인증 유닛(314)은 SAML 아티팩트가 해결되기를 요청하는 메시지를 계정 관리 공급자(304)로 전송할 수 있다. 계정 관리 공급자(304)는 사진 서비스(402) 및 요청 토큰에 알려져 있는 사용자의 계정 식별정보로 구성된 SAML 어설션으로 응답할 수 있다. 사진 서비스(402)의 서비스 사용자 인터페이스(312)는 이제 클라이언트 웹 브라우저 애플리케이션(400)에 예컨대, 사용자의 사진 앨범으로의 링크를 포함할 수 있는 사용자의 홈 페이지를 제공할 수 있다.

[0069] 이어서 사용자는 자신의 사진 앨범 중 하나에 액세스하도록 링크를 클릭할 수 있다. 사진 서비스(402)는 이제 저장 서비스(406)로부터 몇몇 사진 파일을 불러오는 것을 필요로 할 수 있다. 따라서 사진 서비스(402)는 액세스 토큰을 필요로 하며, SAML 어설션 내에 수신된 요청 토큰 및 저장 서비스(406)의 표시, 예컨대, 저장 서비스(406)의 DNS 네임을 포함하는 생성 액세스 토큰 요청 메시지를 구성한다. 사진 서비스(402)는 사진 서비스 키 및 사진 서비스 시크릿을 사용하여 생성 액세스 토큰 요청 메시지에 서명할 수 있고, TLS를 통해 계정 관리 공급자(304)로 메시지를 전송할 수 있다.

[0070] 이어서 계정 관리 공급자(304)의 토큰 생성 유닛(322)은 생성 액세스 토큰 요청 메시지의 요청 유형이 요청 토큰 교환이라고 결정하고 요청 토큰, 사진 서비스 키(저장 서비스를 호출하기 위해 클라이언트 키와 동일함) 및 사진 서비스 시크릿(저장 서비스를 호출하기 위해 클라이언트 서비스와 동일함)을 추출할 수 있다. 그 다음에 토큰 생성 유닛(322)은 생성 액세스 토큰 요청 메시지의 시그니처를 확인할 수 있고 추출된 파라미터에 기초하여 요청 토큰 사진 서비스 키와 사진 서비스 시크릿 사이의 연관을 확인할 수 있다. 토큰 생성 유닛(322)이 생성 액세스 토큰 요청 메시지를 정확히 확인한다고 가정하면, 토큰 생성 유닛(322)은 액세스 토큰을 생성할 수 있고 그 액세스 토큰을 요청 사용자에 대한 인증 세션, 저장 서비스(406) 및 토큰 시크릿과 연관시킬 수 있다. 이어서 토큰 생성 유닛(322)은 액세스 토큰 및 토큰 시크릿을 포함하는 메시지를 사진 서비스(402)로 전송할 수

있다.

[0071] 그 다음에 사진 서비스(402)는 수신된 액세스 토큰, 요청된 파일 이름(들) 및 사진 서비스 키를 포함하는 획득 파일 메시지를 구성할 수 있다. 사진 서비스(402)는 사진 서비스 시크릿 및 토큰 시크릿을 사용하여 획득 파일 메시지에 서명할 수 있고, 그 메시지를 저장 서비스(406)로 전송할 수 있다. 이전과 같이, 저장 서비스(406)는 메시지로부터 파라미터를 추출할 수 있고, 토큰 정보 요청 메시지를 구성할 수 있으며, 토큰 정보 요청 메시지를 계정 관리 공급자(304)로 전송할 수 있다. 다시, 이전과 같이, 계정 관리 공급자(304)는 액세스 토큰을 확인할 수 있고 토큰 정보 메시지로 저장 서비스(406)에 응답할 수 있다. 저장 서비스(406)는 획득 파일 메시지를 확인하고 토큰 정보 메시지 내에 수신된 사용자 식별정보를 사용하여 사용자 파일에 적절히 액세스하는 방법을 결정하도록 이전과 같이 토큰 정보 메시지에 포함된 파라미터를 사용할 수 있다.

[0072] 도 5 및 도 6은 본 발명의 예시적인 실시예에 따른 시스템, 방법 및 컴퓨터 프로그램 제품의 순서도이다. 순서도의 각각의 블록 또는 단계 및 순서도 내의 블록들의 조합은 하드웨어, 펌웨어 및/또는 하나 이상의 컴퓨터 프로그램 인스트럭션을 포함하는 소프트웨어와 같은 다양한 수단에 의해 구현될 수 있다. 예컨대, 하나 이상의 전술된 절차는 컴퓨터 프로그램 인스트럭션에 의해 구현될 수 있다. 이에 관하여, 전술된 절차를 구현하는 컴퓨터 프로그램 인스트럭션은 이동 단말기, 서버 또는 다른 컴퓨팅 장치의 메모리 장치에 의해 저장될 수 있고, 컴퓨팅 장치 내의 내장형 프로세서에 의해 실행될 수 있다. 알게 되듯이, 임의의 그러한 컴퓨터 프로그램 인스트럭션은 컴퓨터 또는 다른 프로그램가능 장치 상에서 실행되는 인스트럭션이 순서도 블록(들) 또는 단계(들)에 지정된 기능을 구현하는 수단을 생성하도록, 컴퓨터 또는 다른 프로그램가능 장치(즉, 하드웨어)로 로딩되어 기계를 생성한다. 이들 컴퓨터 프로그램 인스트럭션은 또한 컴퓨터 판독가능 메모리에 저장된 인스트럭션이 순서도 블록(들) 또는 단계(들)에 지정된 기능을 구현하는 인스트럭션 수단을 포함하는 제조물을 생성하도록, 컴퓨터 또는 다른 프로그램가능 장치를 특정 방식으로 기능하도록 지시할 수 있는 컴퓨터 판독가능 메모리에 저장될 수 있다. 컴퓨터 프로그램 인스트럭션은 또한 컴퓨터 또는 다른 프로그램가능 장치 상에서 실행되는 인스트럭션이 순서도 블록(들) 또는 단계(들)에 지정된 기능을 구현하는 단계를 제공하도록, 일련의 동작 단계가 컴퓨터 구현 프로세스를 생성하도록 컴퓨터 또는 다른 프로그램가능 장치에서 수행되게 하도록 컴퓨터 또는 다른 프로그램가능 장치로 로딩될 수 있다.

[0073] 따라서, 순서도의 블록 또는 단계는 지정된 기능을 수행하는 수단의 조합, 지정된 기능을 수행하는 단계와 지정된 기능을 수행하는 프로그램 인스트럭션 수단의 조합을 지원한다. 순서도의 하나 이상의 블록 또는 단계 및 순서도의 블록 또는 단계의 조합이 지정된 기능 또는 단계, 또는 특별 용도의 하드웨어와 컴퓨터 인스트럭션의 조합을 수행하는 특별 용도의 하드웨어 기반 컴퓨터 시스템에 의해 구현될 수 있음을 또한 알 것이다.

[0074] 이에 관하여, 본 발명의 예시적인 실시예에 따라 계정 관리 공급자의 관점에서 단일 서비스 사인 온을 제공하는 일 예시적인 방법이 도 5에 도시된다. 그 방법은 동작(500)에서, 원격 엔티티로부터 요청된 서비스의 표시를 갖는 생성 액세스 토큰 요청 메시지를 수신하는 단계를 포함할 수 있다. 동작(510)은 계정 관리 공급자가 요청 유형을 결정하는 단계를 포함할 수 있다. 이에 관하여, 요청 유형은 사용자 식별정보 및 암호 조합, 요청 토큰 교환, 또는 액세스 토큰 교환일 수 있다. 그 다음, 동작(520)에서, 계정 관리 공급자는 결정된 요청 유형에 기초하여, 생성 액세스 토큰 요청 메시지로부터 하나 이상의 파라미터를 추출할 수 있다. 동작(530)은 계정 관리 공급자가 하나 이상의 추출된 파라미터에 적어도 일부분 기초하여 하나 이상의 보안 체크를 수행하는 단계를 포함할 수 있다. 그 다음, 동작(540)에서, 계정 관리 공급자는 하나 이상의 보안 체크의 결과에 기초하여 액세스 토큰을 생성할 수 있다. 동작(550)은 계정 관리 공급자가 요청 원격 엔티티에 액세스 토큰을 제공하는 단계를 포함할 수 있다.

[0075] 도 6은 본 발명의 예시적인 실시예에 따라 서비스 공급자의 관점에서 단일 서비스 사인 온을 제공하는 예시적인 방법을 도시한다. 도 6a를 참조하면, 동작(600)은 예컨대, 사용자 장치 또는 다른 서비스 공급자로부터 서비스 액세스 요청을 수신하는 단계를 포함할 수 있다. 동작(605)은 웹 브라우저 애플리케이션으로부터 서비스 액세스 요청이 수신되는지를 판정하는 단계를 포함할 수 있다. 웹 브라우저 애플리케이션으로부터 요청이 수신되지 않았으면, 방법은 도 6b의 동작(620)으로 진행될 수 있다. 동작(620)은 서비스 액세스 요청 메시지로부터 액세스 토큰을 불러오는 과정을 포함할 수 있다. 그 다음, 서비스 공급자는, 동작(625)에서 토큰 정보 요청 메시지를 구성하여, 동작(630)에서 계정 관리 공급자로 토큰 정보 요청 메시지를 전송할 수 있다. 동작(635)은 서비스 공급자가 계정 관리 공급자로부터 토큰 정보 메시지를 수신하는 단계를 포함할 수 있다. 그 다음 동작(640)에서, 서비스 공급자는 토큰 정보 메시지에서 획득된 정보에 기초하여 서비스 액세스 요청 메시지의 클라이언트 키 및 시그니처를 확인할 수 있다. 서비스 공급자가 서비스 액세스 요청 메시지를 정확히 확인하면, 이 방법은 도 6a의 동작(615)으로 진행할 수 있으며, 서비스 공급자는 요청 클라이언트의 허가 레벨과 액세스 프로토

콜 능력에 기초하여 요청된 서비스를 제공할 수 있다.

[0076] 다시 도 6a를 참조하면, 동작(605)에서, 서비스 공급자가 웹 브라우저 애플리케이션으로부터 서비스 액세스 요청 메시지가 수신되었다고 판정하면, 동작(610)에서, 서비스 공급자는 요청 클라이언트에 대한 기존의 사인 온 세션이 존재하는지를 판정할 수 있다. 기존의 사인 온 세션이 존재하면, 동작(615)에서, 서비스 공급자는 클라이언트의 허가 레벨과 액세스 프로토콜 능력에 기초하여 요청된 서비스를 제공할 수 있다. 기존의 사인 온 세션이 존재하지 않으면, 이 방법은 도 6c의 동작(645)으로 진행될 수 있다. 이와 관련하여, 동작(645)은 사용자 로그인 정보를 수신하고, 파라미터로서 인코딩된 인증 요청을 갖는 계정 관리 공급자에게 클라이언트 웹 브라우저 애플리케이션을 재지시하는 단계를 포함할 수 있다. 그 다음, 동작(650)에서, 서비스 공급자는 계정 관리 공급자로부터 재지시된 클라이언트 웹 브라우저 애플리케이션을 수신할 수 있으며, 여기서 재지시된 클라이언트 웹 브라우저 애플리케이션 내에 SAML 아티팩트가 포함된다. 동작(655)은 서비스 공급자가 계정 관리 공급자에게, 계정 관리 공급자가 SAML 아티팩트를 해결할 것을 요청하는 메시지를 전송하는 단계를 포함할 수 있다. 그 다음, 동작(660)에서, 서비스 공급자는 계정 관리 공급자로부터 요청 클라이언트의 계정 식별정보와 요청 토큰을 포함하는 SAML 어설션을 수신할 수 있다. 그 다음, 동작(665)에서, 서비스 공급자는 클라이언트 웹 브라우저 애플리케이션에 사용자의 서비스 홈 페이지를 제공할 수 있다.

[0077] 이제 도 6d를 참조하면, 동작(670)에서, 사용자의 서비스와의 상호작용 동안에, 서비스 공급자는 클라이언트 웹 브라우저 애플리케이션으로부터 제 2 서비스의 호출을 요청하는 요청을 수신할 수 있다. 그 다음, 동작(675)에서 서비스 공급자는 요청 토큰을 포함하는 생성 액세스 토큰 요청 메시지를 구성할 수 있고, 동작(680)에서 계정 관리 공급자로 생성 액세스 토큰 요청 메시지를 전송할 수 있다. 그 다음, 서비스 공급자는 동작(685)에서 계정 관리 공급자로부터 액세스 토큰을 수신할 수 있고, 그 후 동작(690)에서 제 2 서비스 공급자에게 액세스 토큰을 포함하는 서비스 액세스 요청 메시지를 전송할 수 있다. 이어서 제 2 서비스 공급자는 제 1 서비스 공급자가 요청 클라이언트인 전술한 내용과 같이 도 6a의 동작(600)으로부터 계속될 수 있다.

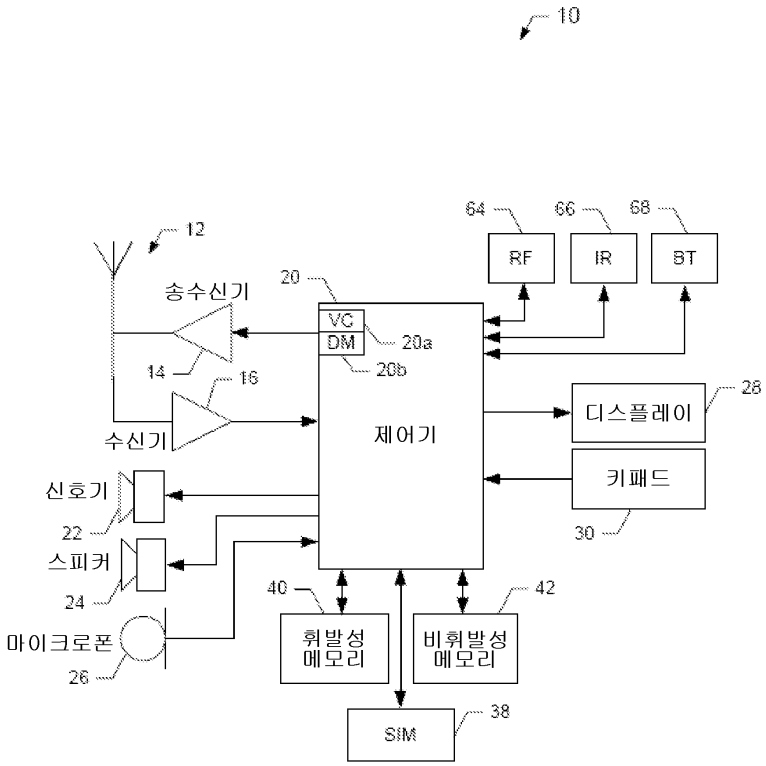
[0078] 전술한 기능은 다수의 방법으로 수행될 수 있다. 예컨대, 전술된 기능의 각각을 수행하는 임의의 적합한 수단은 본 발명의 실시예를 수행하는 데 이용될 수 있다. 일 실시예에서, 요소들의 전부 또는 일부는 일반적으로 컴퓨터 프로그램 제품의 제어 하에서 작동할 수 있다. 본 발명의 실시예의 방법을 수행하는 컴퓨터 프로그램 제품은 비휘발성 저장 매체와 같은 컴퓨터 판독가능 저장 매체 및 컴퓨터 판독가능 저장 매체에 내장된 일련의 컴퓨터 인스트럭션과 같은 컴퓨터 판독가능 프로그램 코드 부분을 포함한다.

[0079] 이처럼, 본 발명의 몇몇 실시예는 이동 단말기(10)와 같은 컴퓨팅 장치의 사용자에게 몇몇 이점을 제공할 수 있다. 예컨대, 사용자 장치의 사용자는 단일 서비스에 사인 온하라고 요청되는 동안에만 사용자가 다양한 서비스를 사용하게 하는 단일 서비스 사인 온을 구비할 수 있다. 이에 관하여, 계정 관리 공급자는 사용자와 다수의 서비스 사이의 상호작용을 관리하고 용이하게 할 수 있다. 본 발명의 실시예는 다수의 서비스 공급자에 대한 인증이 집중 계정 관리 공급자에 의해 처리될 수 있을 때 공통 애플리케이션 라이브러리 및 인터페이스가 인증 목적을 위해 사용될 수 있으므로 서비스 공급자에게 이점을 더 제공할 수 있다. 또한, 본 발명의 실시예는 사용자가 후속 서비스 요청을 하는 데 다른 애플리케이션 또는 컴퓨팅 장치를 사용하는 경우에도 사인 온 세션이 사용자에 대해 유지되거나 상관될 수 있도록, 계정 관리 공급자가 몇몇 상이한 프로토콜에서 수신된 요청을 수신하고 이에 응답하며 요청 사용자와 모든 사인 온을 연관시킬 때 독립적인 장치 및 애플리케이션인 단일 서비스 사인 온을 제공할 수 있다. 추가적으로, 본 발명의 실시예는 단명 액세스 토큰의 사용을 통해 사용자 계정 및 서비스 공급자에 의해 제공된 데이터 및 콘텐츠를 보호하도록 강화된 보안을 제공할 수 있다.

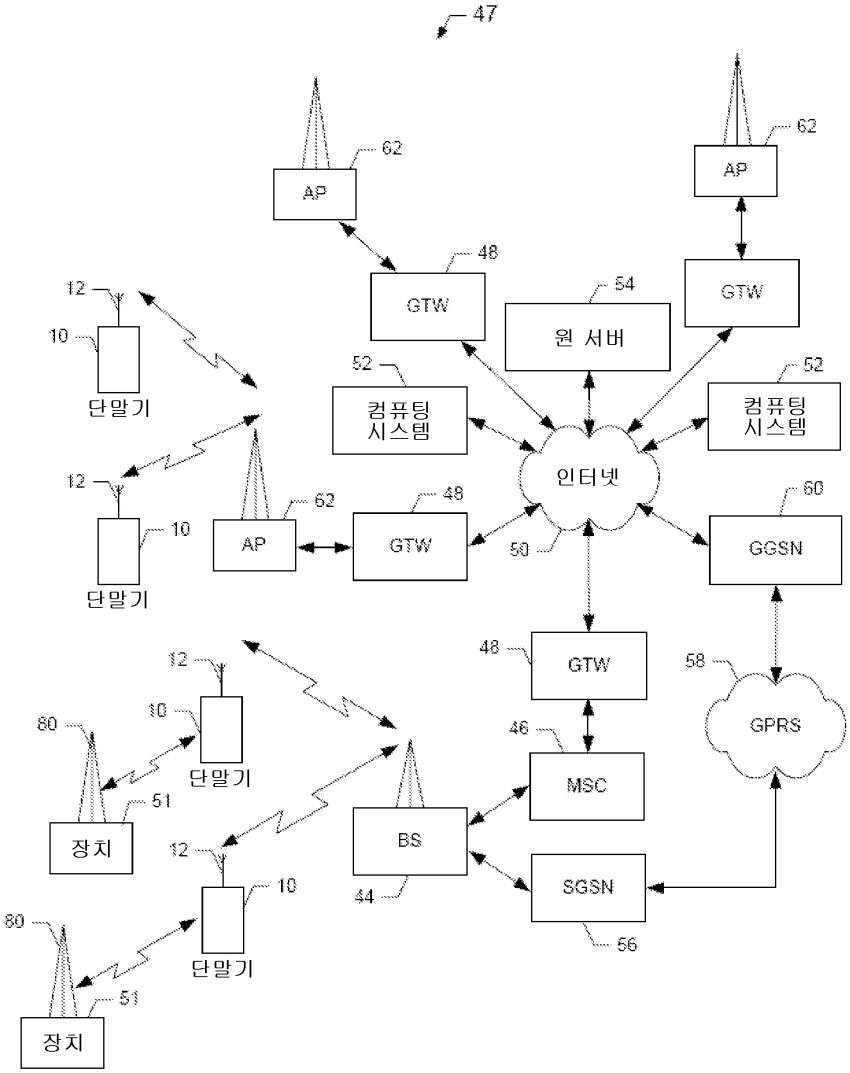
[0080] 당업자는 본 명세서에 설명된 본 발명의 다수의 변경 및 다른 실시예에 전술한 설명 및 관련 도면에 제공된 교시의 이점을 가지는 이들 발명이 속하는 것을 기억할 것이다. 그러므로, 본 발명의 실시예가 개시된 특정 실시예로 제한되지 않으며, 변경 및 다른 실시예가 첨부된 특허청구범위의 범주 내에 포함되도록 의도됨을 알아야 한다. 또한, 전술한 설명 및 관련 도면은 요소 및/또는 기능의 특정 예시적인 조합의 관점에서 예시적인 실시예를 설명하지만, 요소 및/또는 기능의 상이한 조합이 첨부된 특허청구범위의 범주로부터 벗어나지 않으면서 다른 실시예에 의해 제공될 수 있음을 알아야 한다. 이에 관하여, 예컨대, 명백히 전술된 것과 상이한 요소 및/또는 기능의 조합도 첨부된 특허청구범위 중 몇몇에서 설명될 수 있는 바와 같이 고려된다. 본 명세서에서 특정 용어가 이용되지만, 그 용어들은 일반적이고 기술적인 의미로만 사용되며 제한하기 위해 사용되는 것은 아니다.

도면

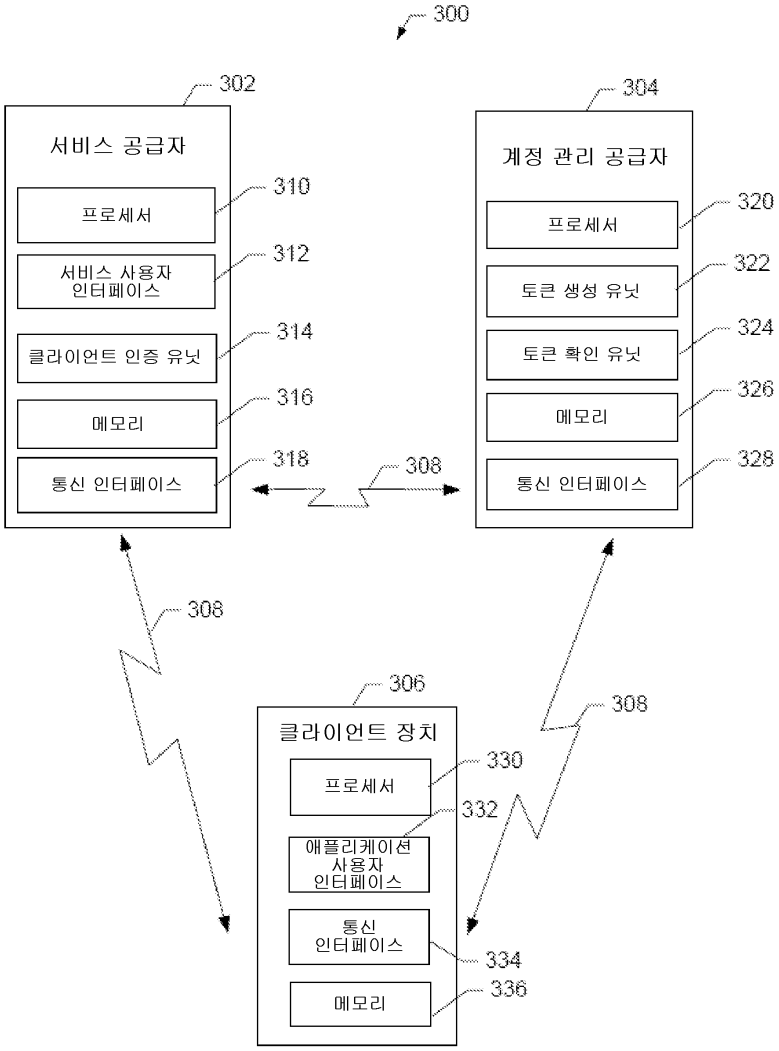
도면1


10
12
송수신기
14
16
수신기
20
VC
DM
20a
20b
제어기
64
RF
66
IR
68
BT
디스플레이
28
키패드
30
신호기
22
스피커
24
마이크로폰
26
40
휘발성 메모리
42
비휘발성 메모리
SIM
38

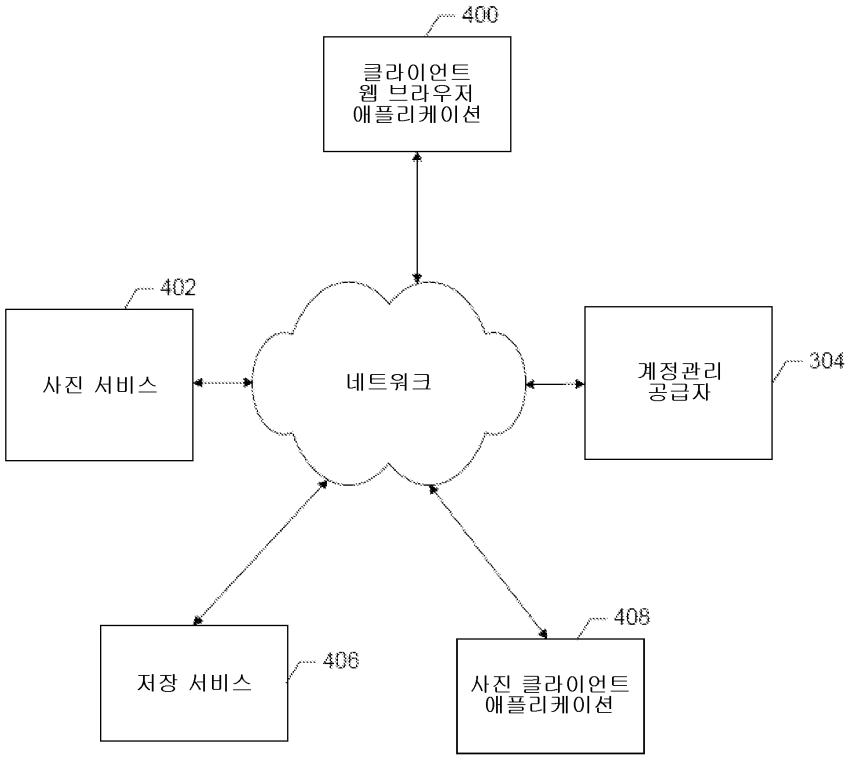
도면2


47
AP
62
AP
62
48
GTW
54
원 서버
GTW
12
10
단말기
52
컴퓨팅 시스템
52
컴퓨팅 시스템
인터넷
12
10
단말기
AP
62
48
GTW
50
60
GGSN
48
GTW
58
GPRS
12
10
단말기
80
51
장치
46
MSC
BS
12
10
단말기
44
SGSN
56
80
51
장치

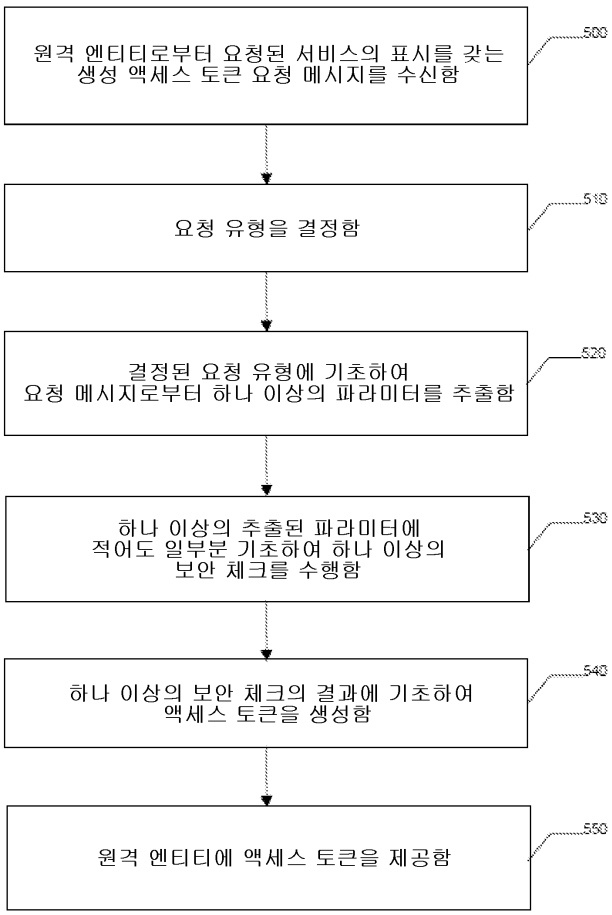
도면3


300
302
서비스 공급자
310
프로세서
312
서비스 사용자 인터페이스
314
클라이언트 인증 유닛
316
메모리
318
통신 인터페이스
308
304
계정 관리 공급자
320
프로세서
322
토큰 생성 유닛
324
토큰 확인 유닛
326
메모리
328
통신 인터페이스
308
306
클라이언트 장치
330
프로세서
332
애플리케이션 사용자 인터페이스
334
통신 인터페이스
336
메모리
308

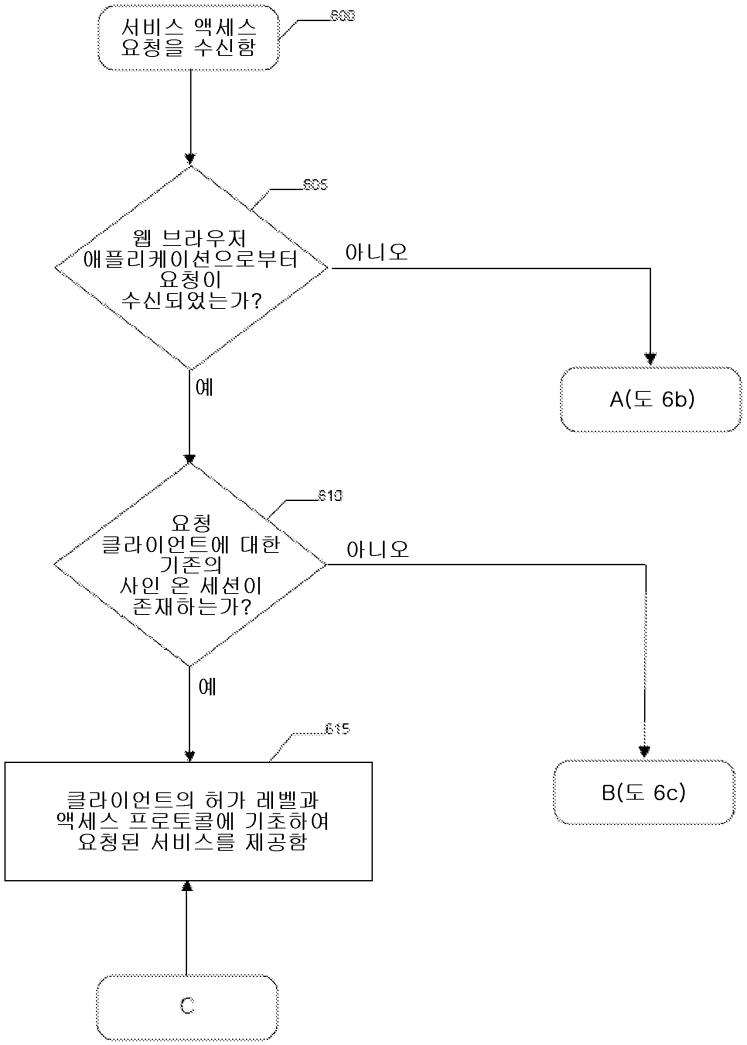
도면4


400
클라이언트
웹 브라우저
애플리케이션
402
사진 서비스
네트워크
계정관리
공급자
304
406
저장 서비스
408
사진 클라이언트
애플리케이션

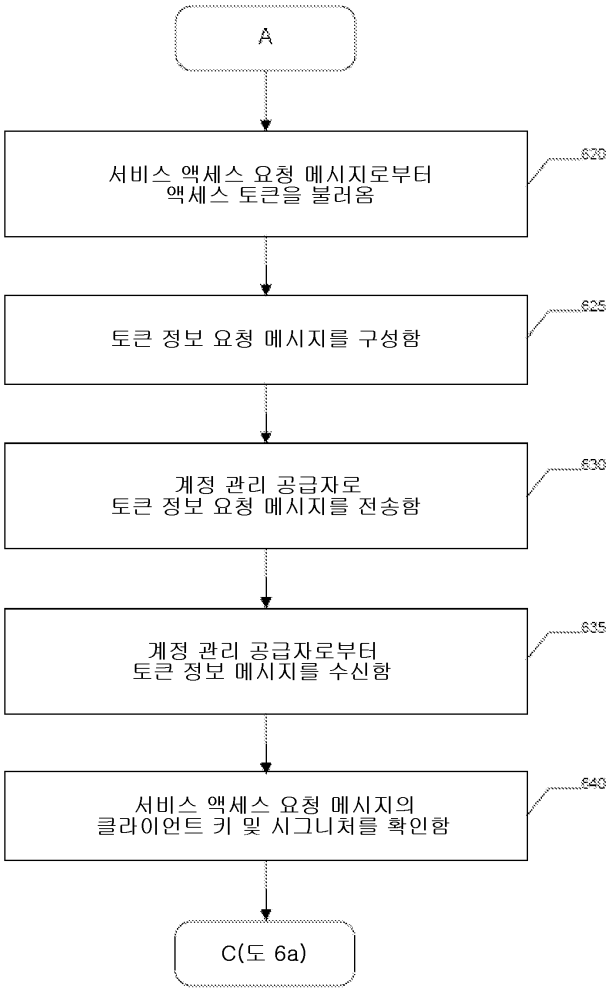
도면5


원격 엔티티로부터 요청된 서비스의 표시를 갖는
생성 액세스 토큰 요청 메시지를 수신함
500
요청 유형을 결정함
510
결정된 요청 유형에 기초하여
요청 메시지로부터 하나 이상의 파라미터를 추출함
520
하나 이상의 추출된 파라미터에
적어도 일부분 기초하여 하나 이상의
보안 체크를 수행함
530
하나 이상의 보안 체크의 결과에 기초하여
액세스 토큰을 생성함
540
원격 엔티티에 액세스 토큰을 제공함
550

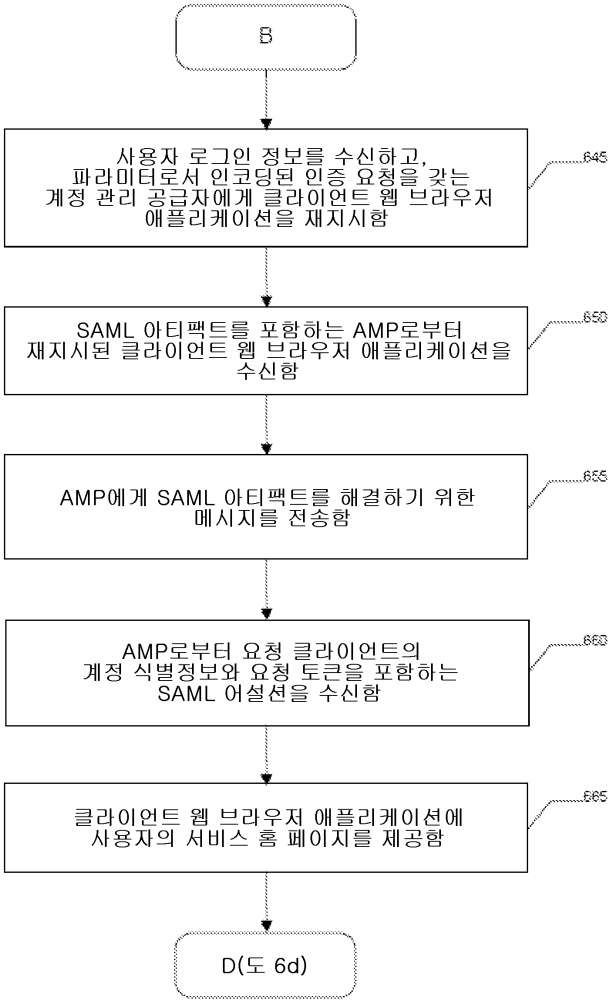
도면6a


서비스 액세스 요청을 수신함
600
웹 브라우저 애플리케이션으로부터 요청이 수신되었는가?
605
아니오
예
A(도 6b)
요청 클라이언트에 대한 기존의 사인 온 세션이 존재하는가?
610
아니오
예
B(도 6c)
클라이언트의 허가 레벨과 액세스 프로토콜에 기초하여 요청된 서비스를 제공함
615
C

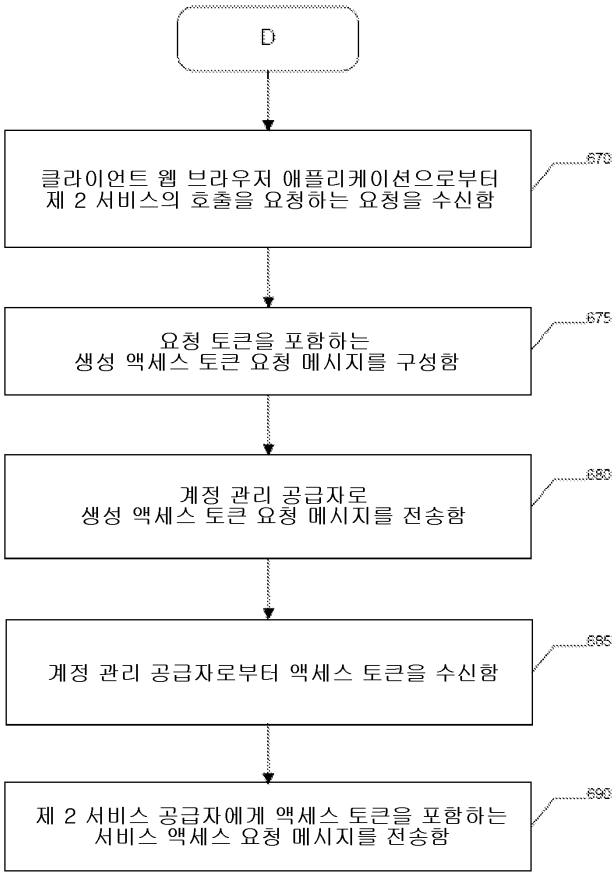
도면6b


A
서비스 액세스 요청 메시지로부터
액세스 토큰을 불러옴
620
토큰 정보 요청 메시지를 구성함
625
계정 관리 공급자로
토큰 정보 요청 메시지를 전송함
630
계정 관리 공급자로부터
토큰 정보 메시지를 수신함
635
서비스 액세스 요청 메시지의
클라이언트 키 및 시그니처를 확인함
640
C(도 6a)

도면6c


B
사용자 로그인 정보를 수신하고,
파라미터로서 인코딩된 인증 요청을 갖는
계정 관리 공급자에게 클라이언트 웹 브라우저
애플리케이션을 재지시함
645
SAML 아티팩트를 포함하는 AMP로부터
재지시된 클라이언트 웹 브라우저 애플리케이션을
수신함
650
AMP에게 SAML 아티팩트를 해결하기 위한
메시지를 전송함
655
AMP로부터 요청 클라이언트의
계정 식별정보와 요청 토큰을 포함하는
SAML 어설션을 수신함
660
클라이언트 웹 브라우저 애플리케이션에
사용자의 서비스 홈 페이지를 제공함
665
D(도 6d)

도면6d


D
클라이언트 웹 브라우저 애플리케이션으로부터
제 2 서비스의 호출을 요청하는 요청을 수신함
670
요청 토큰을 포함하는
생성 액세스 토큰 요청 메시지를 구성함
675
계정 관리 공급자로
생성 액세스 토큰 요청 메시지를 전송함
680
계정 관리 공급자로부터 액세스 토큰을 수신함
685
제 2 서비스 공급자에게 액세스 토큰을 포함하는
서비스 액세스 요청 메시지를 전송함
690