(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0084217
(43) 공개일자 2014년07월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 12/24* (2006.01)
(21) 출원번호 10-2014-7013401
(22) 출원일자(국제) 2012년10월19일
심사청구일자 2014년05월19일
(85) 번역문제출일자 2014년05월19일
(86) 국제출원번호 PCT/CN2012/083219
(87) 국제공개번호 WO 2013/056674
국제공개일자 2013년04월25일
(30) 우선권주장
201110319068.2 2011년10월20일 중국(CN)

(71) 출원인
알까텔 루슨트
프랑스 92100 불론뉴-비영꾸르 루뜨 들 라 렌느 148/152
(72) 발명자
후 지유안
중국 상하이 201206 푸동 진퀴아오 닝퀴아오 로드 388#
루오 지강
중국 상하이 201206 푸동 진퀴아오 닝퀴아오 로드 388#
완 용겐
중국 상하이 201206 푸동 진퀴아오 닝퀴아오 로드 388#
(74) 대리인
제일특허법인

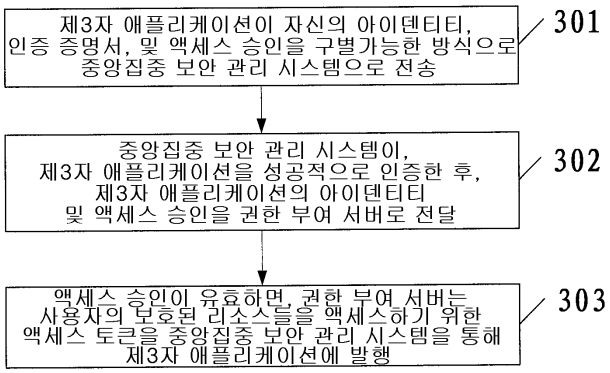
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **제3자 애플리케이션의 중앙집중 보안 관리 방법, 시스템 및 대응 통신 시스템**

(57) 요 약

본 발명은 제3자 애플리케이션에 대해 중앙집중 보안 관리를 수행하는 방법, 적어도 하나의 권한 부여 서버, 적어도 하나의 리소스 서버, 사용자 프록시, 제3자 애플리케이션 및 중앙집중 보안 관리 시스템을 포함하는 시스템 및 통신 시스템 제공하는 것으로, 제3자 애플리케이션의 중앙집중 보안 관리 시스템은 제3자 애플리케이션의 보안을 유효화하고 그것을 디지털식으로 서명하는 것을 담당하고, 중앙집중 보안 관리 시스템이 제3자 애플리케이션을 인증할 수 있는 인증 증명서를 발행한다. 상기 방법은, 제3자 애플리케이션에 의해, 자신의 아이덴티티, 인증 증명서 및 액세스 승인을 중앙집중 보안 관리 시스템에 구별가능한 방식으로 전송하는 단계; 중앙집중 보안 관리 시스템에 의해, 제3자 애플리케이션을 성공적으로 인증한 후, 아이덴티티 및 액세스 승인을 권한 부여 서버로 전달하는 단계; 및 권한 부여 서버에 의해, 액세스 승인이 유효하면, 중앙집중 보안 관리 시스템을 통해 보호된 리소스들을 액세스하기 위한 액세스 토큰을 제3자 애플리케이션에 발행하는 단계를 포함한다.

대 표 도 - 도3



특허청구의 범위

청구항 1

리소스 서버에 저장된 사용자 보호된 리소스들에 액세스하기 위한 제3자 애플리케이션에 대해 중앙집중 보안 관리를 수행하는 방법으로서,

중앙집중 보안 관리를 위한 상기 제3자 애플리케이션의 중앙집중 보안 관리 시스템은 상기 제3자 애플리케이션의 보안을 유효화하고 상기 제3자 애플리케이션을 디지털식으로 서명하는 것을 담당하고, 상기 중앙집중 보안 관리 시스템이 상기 제3자 애플리케이션을 인증할 수 있는 인증 증명서(authentication credential)를 발행하며,

상기 방법은,

상기 제3자 애플리케이션에 의해, 자신의 아이덴티티, 인증 증명서 및 액세스 승인을 상기 중앙집중 보안 관리 시스템에 구별가능한 방식으로 전송하는 단계와,

상기 중앙집중 보안 관리 시스템에 의해, 상기 제3자 애플리케이션을 성공적으로 인증한 후, 상기 아이덴티티 및 상기 액세스 승인을 권한 부여 서버(Authorization Server)로 전달하는 단계와,

상기 권한 부여 서버에 의해, 상기 액세스 승인이 유효하면, 상기 중앙집중 보안 관리 시스템을 통해 상기 사용자의 보호된 리소스들을 액세스하기 위한 액세스 토큰을 상기 제3자 애플리케이션에 발행하는 단계를 포함하는

중앙집중 보안 관리 수행 방법.

청구항 2

제1항에 있어서,

상기 액세스 승인 및 상기 액세스 토큰은 IETF 정의 인증 프로토콜 OAuth2.0에 부합하고, 및/또는 상기 인증 증명서는 디지털 인증서, 키 또는 패스워드 중 하나인

중앙집중 보안 관리 수행 방법.

청구항 3

제1항 또는 제2항에 있어서,

상기 제3자 애플리케이션이 액세스를 위해 인증받기 전에, 상기 제3자 애플리케이션이 상기 액세스 승인을 이용하여 액세스 토큰을 획득하기 위해 상기 액세스 승인을 얻도록 사용자는 상기 권한 부여 서버에 의해 인증을 받아야 하고, 및/또는

상기 권한 부여 서버가 상기 제3자 애플리케이션에 상기 액세스 승인을 전송한 후, 상기 제3자 애플리케이션은 상기 제3자 애플리케이션의 아이덴티티, 인증 증명서, 및 액세스 승인을 상기 중앙집중 보안 관리 시스템에 전송하는

중앙집중 보안 관리 수행 방법.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 제3자 애플리케이션이 상기 리소스 서버에 저장된 상기 사용자의 보호된 리소스들을 액세스하기를 요청할 때, 상기 제3자 애플리케이션이 유효 액세스 토큰을 갖고 있지 않으면, 상기 리소스 서버는 상기 제3자 애플리케이션의 액세스 요청을 사용자 에이전트로 리다이렉트(redirect)하고, 및/또는

상기 권한 부여 서버가 상기 중앙집중 보안 관리 시스템을 통해 상기 제3자 애플리케이션에 상기 액세스 토큰을 발행한 후, 상기 제3자 애플리케이션은 상기 사용자의 보호된 리소스들을 액세스하기 위해 상기 액세스 토큰을 상기 리소스 서버에 제출하는

중앙집중 보안 관리 수행 방법.

청구항 5

제3항에 있어서,

상기 사용자를 인증하는 상기 권한 부여 서버는 상기 권한 부여 서버에 대하여 직접적으로 인증하는 것을 통해 사용자 에이전트에 의해 행해지고,

상기 액세스 승인은 상기 사용자 에이전트를 통해 상기 권한 부여 서버에 의해 상기 제3자 애플리케이션으로 전송되는

중앙집중 보안 관리 수행 방법.

청구항 6

제3항에 있어서,

상기 사용자를 인증하는 상기 권한 부여 서버는 인증을 위해 상기 중앙집중 보안 관리 시스템을 통해 상기 권한 부여 서버로 리다이렉트하는 것을 통해 사용자 에이전트에 의해 행해지고,

상기 액세스 승인이 상기 중앙집중 보안 관리 시스템 및 상기 사용자 에이전트를 통해 상기 권한 부여 서버에 의해 상기 제3자 애플리케이션으로 전송되는 단계, 또는 상기 액세스 승인이 상기 사용자 에이전트를 통해 상기 권한 부여 서버에 의해 상기 제3자 애플리케이션으로 전송되는 단계 중 적어도 하나의 단계가 수행되는

중앙집중 보안 관리 수행 방법.

청구항 7

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 구별가능한 방식은, 상기 제3자 애플리케이션이 상기 아이덴티티, 상기 인증 증명서, 및 상기 액세스 승인을 개별적으로 패키징하는 방식, 또는 상기 제3자 애플리케이션이 상기 아이덴티티, 상기 인증 증명서, 및 상기 액세스 승인을 개별적으로 마킹(mark)하는 방식 중 하나를 포함하는

중앙집중 보안 관리 수행 방법.

청구항 8

리소스 서버에 저장된 사용자의 보호된 리소스들에 액세스하기 위한 제3자 애플리케이션에 대해 중앙집중 보안 관리를 수행하는 시스템으로서,

상기 시스템은 상기 제3자 애플리케이션의 보안을 유효화하고 상기 제3자 애플리케이션을 디지털식으로 서명하는 것을 담당하고, 상기 시스템이 상기 제3자 애플리케이션을 인증할 수 있는 인증 증명서를 발행하며,

상기 시스템은,

상기 제3자 애플리케이션에 의해 구별가능한 방식으로 전송된 상기 제3자 애플리케이션의 아이덴티티, 인증 증명서 및 액세스 승인을 수신하기 위한 제1 수신 디바이스와,

상기 아이덴티티, 상기 인증 증명서, 및 상기 액세스 승인을 수신한 후, 상기 아이덴티티, 상기 인증 증명서를 이용하여 상기 제3자 애플리케이션을 인증하기 위한 제1 인증 디바이스와,

상기 제3자 애플리케이션을 성공적으로 인증한 후, 상기 제3자 애플리케이션의 상기 아이덴티티 및 상기 액세스 승인을 권한 부여 서버로 전달하기 위한 제1 전달 디바이스와,

상기 권한 부여 서버에 의해 발행된 액세스 토큰을 상기 제3자 애플리케이션으로 전달하기 위한 제2 전달 디바이스를 포함하는

중앙집중 보안 관리 수행 시스템.

청구항 9

제8항에 있어서,

개인 개발자 또는 서비스 제공자에 의해 개발되고 디지털 서명을 위해 상기 개인 개발자 또는 상기 서비스 제공자의 개인 키들을 이용하는 제3자 애플리케이션을 수신하기 위한 제2 수신 디바이스와,

상기 개인 개발자 또는 상기 서비스 제공자에 의해 개발된 디지털 인증서를 이용하여 상기 제2 수신 디바이스에 의해 수신된 상기 제3자 애플리케이션의 디지털 서명을 인증하기 위한 제2 인증 디바이스와,

상기 제2 인증 디바이스의 성공적인 인증 후 상기 제3자 애플리케이션이 악성 코드 또는 바이러스를 포함하는지 여부를 검출하기 위한 안전 체크 디바이스와,

상기 제3자 애플리케이션을 성공적으로 안전 체크한 후 상기 시스템의 개인 키들을 이용하여 상기 제3자 애플리케이션을 디지털식으로 서명하기 위한 디지털 서명 디바이스와,

상기 제3자 애플리케이션에 대한 아이덴티티, 인증 증명서 및 관련 속성들의 균일한 배포의 관리를 위한 제3자 애플리케이션 레지스트리 및 관리 디바이스와,

모든 관련 디지털 인증서들의 균일한 관리를 위한 인증서 관리 디바이스를 더 포함하는

중앙집중 보안 관리 수행 시스템.

청구항 10

제8항 또는 제9항에 있어서,

상기 액세스 승인 및 상기 액세스 토큰은 IETF 정의 인증 프로토콜 OAuth2.0에 부합하고, 및/또는

상기 인증 증명서는 디지털 인증서, 키 또는 패스워드 중 하나이며, 및/또는

상기 디지털 인증서에 대한 인증 관리 디바이스의 관리는 생성하는 것, 발행하는 것 및 취소(withdrawing)하는 것을 포함하는

중앙집중 보안 관리 수행 시스템.

청구항 11

제8항 내지 제10항 중 어느 한 항에 있어서,

모든 관련 디지털 인증서들에 대한 균일한 관리는 생성하는 것, 발행하는 것 및 취소하는 것을 포함하고, 및/또는

상기 권한 부여 서버가 상기 액세스 승인을 상기 제3자 애플리케이션에 전송한 후, 상기 제3자 애플리케이션은 상기 제3자 애플리케이션의 아이덴티티, 인증 증명서, 및 액세스 승인을 상기 시스템에 전송하며, 및/또는

상기 제3자 애플리케이션이 상기 액세스 승인에 의해 액세스 토큰을 획득하기 위해 상기 액세스 승인을 얻도록, 상기 제3자 애플리케이션이 액세스를 위해 인증되기 전에, 사용자는 사용자 에이전트를 통해 상기 권한 부여 서버에 의해 인증되어야 하고, 및/또는

상기 제3자 애플리케이션이 상기 리소스 서버의 상기 사용자의 보호된 리소스들을 액세스하는 것을 요청할 때,

상기 제3자 애플리케이션이 유효한 액세스 토큰을 갖고 있지 않으면, 상기 리소스 서버는 상기 제3자 애플리케이션의 액세스 요청을 상기 사용자 에이전트에 리다이렉트하고, 및/또는

상기 권한 부여 서버가 상기 시스템을 통해 상기 제3자 애플리케이션에 상기 액세스 토큰을 발행한 후, 상기 제3자 애플리케이션은 상기 사용자의 보호된 리소스들을 액세스하기 위해 상기 액세스 토큰을 상기 리소스 서버에 제출하는

중앙집중 보안 관리 수행 시스템.

청구항 12

제11항에 있어서,

상기 사용자를 인증하는 상기 권한 부여 서버는 상기 권한 부여 서버에 대하여 직접적으로 인증하는 것을 통해 상기 사용자 에이전트에 의해 행해지고,

상기 액세스 승인은 상기 사용자 에이전트를 통해 상기 권한 부여 서버에 의해 상기 제3자 애플리케이션으로 전송되는

중앙집중 보안 관리 수행 시스템.

청구항 13

제11항에 있어서,

상기 사용자를 인증하는 상기 권한 부여 서버는 인증을 위해 상기 시스템을 통해 상기 권한 부여 서버로 리다이렉트하는 것을 통해 상기 사용자 에이전트에 의해 행해지고,

상기 액세스 승인이 상기 시스템 및 상기 사용자 에이전트를 통해 상기 권한 부여 서버에 의해 상기 제3자 애플리케이션으로 전송되는 단계, 또는 상기 액세스 승인이 상기 사용자 에이전트를 통해 상기 권한 부여 서버에 의해 상기 제3자 애플리케이션으로 전송되는 단계 중 적어도 하나의 단계가 수행되는

중앙집중 보안 관리 수행 시스템.

청구항 14

제8항 내지 제10항 중 어느 한 항에 있어서,

상기 구별가능한 방식은, 상기 제3자 애플리케이션이 상기 아이덴티티, 상기 인증 증명서, 및 상기 액세스 승인을 개별적으로 패키징하는 방식, 또는 상기 제3자 애플리케이션이 상기 아이덴티티, 상기 인증 증명서, 및 상기 액세스 승인을 개별적으로 마킹하는 방식 중 하나를 포함하는

중앙집중 보안 관리 수행 시스템.

청구항 15

통신 시스템으로서,

적어도 하나의 권한 부여 서버와,

적어도 하나의 리소스 서버와,

사용자 에이전트와,

제3자 애플리케이션과,

제7항 내지 제14항 중 어느 한 항에 따른, 리소스 서버에 저장된 사용자의 보호된 리소스들에 액세스하기 위한

제3자 애플리케이션에 대해 중앙집중 보안 관리를 수행하는 시스템을 포함하는

통신 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 통신에 관한 것으로, 특히, 사용자의 보호된 리소스들을 액세스하기 위해 제3자 애플리케이션/클라이언트에 대한 중앙집중 보안 관리를 수행하기 위한 기술에 관한 것이다.

배 경 기 술

[0002] 현재 인터넷 서비스들의 통합은 불가피한 동향이 되었다. 사용자들에게 보다 나은 서비스를 제공하기 위해, 많은 서비스 제공자들은 제3자 애플리케이션/클라이언트들이 "오픈 네트워크 API(Application Programming Interface)"를 유발함으로써 사용자들에게 더 많은 애플리케이션을 제공하게 할 수 있다. 오픈 플랫폼의 핵심 문제는 사용자 인증, 권한 부여 및 제3 자 애플리케이션/클라이언트가 오픈 네트워크 API를 안전하게 사용해야 한다는 점이다. 사용자에 대해, 그는 제3자가, 당사자 간에 강한 신뢰관계가 있지 않은 한, 자신의 사용자 이름 및 패스워드를 직접 사용하여 사용자 보호 네트워크 리소스들을 액세스할 수 있는 것을 일반적으로 원하지 않는다. OAuth(Oepn Authorization; 오픈 승인) 프로토콜은 서비스들의 통합동안 "인증 및 권한 부여"의 근본적인 문제를 해결할 목적으로 제시되어 있다.

[0003] IETF(즉, Internet Engineering Task Force)에 의해 개발된 OAuth 프로토콜은, 제3자 애플리케이션/클라이언트에게 리소스들의 소유자를 나타냄으로써 보호된 리소스들에 액세스하는 방법을 제공하는 현재 국제적으로 일반적인 권한 부여 방식이다. 보호된 리소스들을 액세스하기 전에, 제3자 애플리케이션/클라이언트는 리소스들의 소유자로부터 권한 부여, 즉, 액세스 승인(액세스 승인은 리소스들의 소유자에 의해 제공되는 권한 부여를 나타내고, 그의 유형은 제3자 애플리케이션/클라이언트에 의해 사용되는 획득 방식 및 권한 부여 서버에 의해 지원되는 방식에 의존함)을 우선적으로 획득하고, 다음에 액세스 에이전트와 (액세스 승인의 액션 범위, 지속 기간 및 다른 속성들을 나타내는) 액세스 토큰을 교환해야 한다. 제3자 애플리케이션/클라이언트는 리소스 서버에 액세스 토큰을 보여줌으로써 보호된 리소스들을 액세스한다.

[0004] OAuth 프로토콜의 새로운 버전인 OAuth2.0은 구현을 원리적으로 간소화시키고, 더 많은 액세스 형태를 지원한다; 예를 들면, "웹 애플리케이션, 데스크톱 애플리케이션, 모바일 단말기, 홈 디바이스" 등을 동시에 지원한다. OAuth2.0은 사용자로 하여금, 자신들의 장기간 인증 또는 심지어 자신들의 아이덴티티를 드러낼 필요없이, 제3자 애플리케이션/클라이언트가 사용자의 보호된 리소스들에 액세스하는 것을 승인하게 할 수 있다. 이 방식에서, 사용자 민감 정보의 프라이버시가 보호될 수 있다.

[0005] 이러한 목적을 위해, 서비스 제공자들은 사용자들의 리소스들을 관리하고,

[0006] - 사용자들의 관리;

[0007] - 제3자 애플리케이션/클라이언트의 관리;

[0008] - 제3자 애플리케이션/클라이언트가 액세스 토큰을 적용하는 액세스 승인을 발행(IETF OAuth2.0의 정의 참조);

[0009] - 권한 부여 서버와 사용자 간의 상호 인증;

[0010] - 권한 부여 서버와 제3자 애플리케이션/클라이언트 간의 상호 인증;

[0011] - 액세스 승인의 유효화; 및

[0012] - 제3자 애플리케이션/클라이언트가 사용자들의 보호된 리소스들을 액세스할 수 있는 액세스 토큰을 발행

[0013] 하는 것을 담당하는 IETF OAuth2.0에 정의된 권한 부여 서버를 구축해야한다.

[0014] 도 1은 IETF OAuth2.0에 따른 시스템 및 워크플로우를 개략적으로 도시한다.

[0015] 도 1에 도시된 워크플로우는 다음과 같다:

[0016] 1. 제3자 애플리케이션/클라이언트가 리소스 서버에 저장된 사용자의 보호된 리소스들을 액세스할 예정이다;

[0017] 2. 리소스 서버는, 제3자 애플리케이션/클라이언트가 유효한 액세스 토큰을 갖지 않은 것을 발견한 다음, 사용자의 권한 부여를 얻기 위해 제3자 애플리케이션/클라이언트를 사용자 에이전트에게 리다이렉트한다;

[0018] 3. 사용자가 승인 액세스로 제3자 애플리케이션/클라이언트에게 권한을 부여하기 전에, 사용자는 권한 부여 서버에 의해 권한을 부여받아야하고, 사용자는 권한 부여 서버에게 동시에 권한을 부여할 필요가 있을 수 있다;

[0019] 4. 권한 부여 서버는 사용자 에이전트를 통해 승인 액세스를 제3자 애플리케이션/클라이언트에게 전송한다;

[0020] 5. 제3자 애플리케이션/클라이언트는 액세스 토큰을 적용하기 위해 아이덴티티, 승인 액세스 및 자신의 인증 증명서를 권한 부여 서버에 제출한다;

[0021] 6. 권한 부여 서버와 제3자 애플리케이션/클라이언트 간의 상호 인증 후, 그리고, 승인 액세스를 유효화한 후, 권한 부여 서버는 액세스 토큰을 제3자 애플리케이션/클라이언트에게 발행한다.

[0022] 7. 제3자 애플리케이션/클라이언트는 사용자들의 리소스들을 액세스하기 위해 액세스 토큰을 리소스 서버에 제출한다.

[0023] 8. 액세스 토큰이 유효하면, 리소스 서버는 제3자 애플리케이션/클라이언트에 대한 데이터 응답한다.

발명의 내용

해결하려는 과제

[0024] 그러나, IETF OAuth2.0은 일부 대규모 서비스 제공자들이 (아이덴티티, 인증, 인증 증명서 관리 등과 같은) 자신들에 의한 제3자 애플리케이션/클라이언트의 관리를 제공할 수 있기 때문에 그들에게만 매우 유익하다. 그러나, 제3자 애플리케이션/클라이언트를 관리하기에 너무 많은 비용이 들기 때문에 소규모 또는 중간 서비스 제공자들이 이것을 행하기에는 쉽지 않다. 더욱이, 대규모 서비스 제공자들은 그들이 개별 리소스 서버들을 내부적으로 갖는다면 제3자 웹 사이트 및 애플리케이션/클라이언트를 관리하기 위해 중첩된 컴포넌트들을 개발하고 배치해야 한다.

[0025] 더욱이, 제3자 애플리케이션/클라이언트가 많아짐에 따라 - 그들 중 일부는 개인들에 의해 개발되고 제공될 수 있음 -, 공격자들이 악성 네트워크 API를 개발하여 네트워크 API를 오용함으로써 불법적으로 사용자의 리소스들을 액세스할 가능성이 있다. 따라서, 모든 제3자 애플리케이션/클라이언트가 사용자들의 보호된 리소스들을 액세스할 수 있기 전에 그들이 보안성이 있고 신뢰를 갖게 되는 것을 보장하는 것은 용이하지 않다.

과제의 해결 수단

[0026] 종래 기술의 상기 결점들을 해결하기 위해, 본 발명의 제1 양상에 따라, 본 발명은 리소스 서버에 저장된 사용자 보호된 리소스들에 액세스하기 위한 제3자 애플리케이션에 대해 중앙집중 보안 관리를 수행하는 방법을 제공한다. 상기 방법에 따라, 중앙집중 관리를 위한 제3자 애플리케이션의 중앙집중 보안 관리 시스템은 제3자 애플리케이션의 보안을 유효화하고 제3자 애플리케이션을 발행하기 전에 제3자 애플리케이션을 디지털식으로 서명하는 것을 담당하고, 중앙집중 보안 관리 시스템이 제3자 애플리케이션을 인증할 수 있는 인증 증명서(authentication credential)를 발행한다. 상기 방법은, 제3자 애플리케이션에 의해, 자신의 아이덴티티, 인증 증명서 및 액세스 승인을 상기 중앙집중 보안 관리 시스템에 구별가능한 방식으로 전송하는 단계; 중앙집중 보안 관리 시스템에 의해, 제3자 애플리케이션을 성공적으로 인증한 후, 액세스 승인을 권한 부여 서버로 전달하는 단계; 및 권한 부여 서버가 액세스 승인을 유효한 것으로 성공적으로 인증하면, 중앙집중 보안 관리 시스템을 통해 사용자의 보호된 리소스들을 액세스하기 위한 액세스 토큰을 권한 부여 서버에 의해 제3자 애플리케이션에 발행하는 단계를 포함한다.

[0027] 본 발명의 또 다른 양상에 따라, 리소스 서버에 저장된 사용자의 보호된 리소스들에 액세스하기 위한 제3자 애플리케이션에 대해 중앙집중 보안 관리를 수행하는 시스템으로서, 상기 시스템은, 제3자 애플리케이션에 의해 구별가능한 방식으로 전송된 제3자 애플리케이션의 아이덴티티, 인증 증명서 및 액세스 승인을 수신하기 위한 제1 수신 디바이스; 아이덴티티, 인증 증명서 및 액세스 승인을 수신한 후, 아이덴티티 및 인증 증명서를 이용하여 제3자 애플리케이션을 인증하기 위한 제1 인증 디바이스; 제3자 애플리케이션을 성공적으로 인증한 후, 상

기 제3자 애플리케이션의 액세스 승인을 권한 부여 서버로 전달하기 위한 제1 전달 디바이스; 및 권한 부여 서버에 의해 발행된 액세스 토큰을 제3자 애플리케이션으로 전달하기 위한 제2 전달 디바이스를 포함한다.

[0028] 바람직하게, 본 발명에 따른 시스템은, 개인 개발자 또는 서비스 제공자에 의해 개발되고 디지털 서명을 위해 개인 개발자 또는 서비스 제공자의 개인 키들을 이용하는 제3자 애플리케이션을 수신하기 위한 제2 수신 디바이스; 개인 개발자 또는 서비스 제공자에 의해 개발된 디지털 인증서를 이용하여 제2 수신 디바이스에 의해 수신된 제3자 애플리케이션의 디지털 서명을 인증하기 위한 제2 인증 디바이스; 제2 인증 디바이스의 성공적인 인증 후 제3자 애플리케이션이 악성 코드 또는 바이러스를 포함하는지 여부를 검출하기 위한 안전 체크 디바이스; 제3자 애플리케이션을 성공적으로 안전 체크한 후 시스템의 개인 키들을 이용하여 제3자 애플리케이션을 디지털식으로 서명하기 위한 디지털 서명 디바이스; 제3자 애플리케이션에 대한 아이덴티티, 인증 증명서 및 관련 속성들의 균일한 배포의 관리를 위한 제3자 애플리케이션 레지스트리 및 관리 디바이스; 및 모든 관련 디지털 인증서들의 생성, 발행 및 취소와 같은 균일한 관리를 위한 인증서 관리 디바이스를 더 포함한다.

[0029] 본 발명의 또 다른 양상에 따라, 적어도 하나의 권한 부여 서버; 적어도 하나의 리소스 서버; 사용자 에이전트; 제3자 애플리케이션; 및 본 발명에 따라 리소스 서버에 저장된 사용자의 보호된 리소스들에 액세스하기 위한 제3자 애플리케이션에 대해 중앙집중 보안 관리를 수행하는 시스템을 포함하는 통신 시스템이 제공된다.

도면의 간단한 설명

[0030] 본 발명의 다른 특징, 목적 및 이점은 첨부 도면을 참조하여 다음에 이어지는 비제한적인 실시예의 상세한 설명을 읽음으로써 더 자명해 질 것이다.

도 1은 종래 기술의 IETF OAuth2.0에 따른 시스템 및 워크플로우를 개략적으로 도시한다.

도 2는 본 발명에 따라 제3자 애플리케이션에 대해 중앙집중 보안 관리를 수행하기 위한 시스템 및 워크플로우를 개략적으로 도시한다.

도 3은 본 발명의 실시예에 따른 제3자 애플리케이션에 대한 중앙집중 보안 관리의 플로우차트이다.

도 4는 본 발명의 실시예에 따라 제3자 애플리케이션에 대해 중앙집중 보안 관리를 수행하기 위한 시스템의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0031] 본 발명의 기본적인 생각은 리소스 서버에 저장된 사용자들의 보호된 리소스들에 액세스하기 위한 제3자 애플리케이션/클라이언트에 대해 중앙집중 보안 관리를 수행하기 위한 것이다. 간소화를 위해, 다음의 텍스트에 있는 "제3자 애플리케이션/클라이언트"는 "제3자 애플리케이션"으로 지정될 것이다. 도 2는 제3자 애플리케이션에 대해 중앙집중 보안 관리를 수행하기 위한 시스템 및 워크플로우를 개략적으로 도시한다. 도 2에 도시된 바와 같이, 도 1의 기존의 솔루션에 비해, 중앙집중 보안 관리 시스템이 부가되어 있다. 시스템은 다음의 기능들을 구비한다:

[0032] - 제3자 애플리케이션을 공식적으로 배포하기 전에,

[0033] ◆ 개인 개발자 또는 서비스 제공자의 디지털 인증서를 이용하여 개인 개발자 또는 서비스 제공자의 키들을 통한 서명을 위해 제3자 애플리케이션을 인증함으로써 제3자 애플리케이션의 추적가능성을 보장;

[0034] ◆ 제3자 애플리케이션이 (예를 들면, 안티-바이러스/안티-악성웨어를 체크하여) 보안성이 있는지 여부를 유효화;

[0035] ◆ 서비스 제공자 또는 최종 사용자가 제3자 애플리케이션의 설치 전에 제3자 애플리케이션의 보안성, 인증 및 신뢰성을 검증할 수 있도록 제3자 애플리케이션을 자신의 키들로 서명;

[0036] ◆ 인증을 위해 사용되는 제3자 애플리케이션에 대한 증명서(예를 들면, 인증서 또는 키)를 발행;

[0037] - 제3자 애플리케이션을 공식적으로 배포

[0038] - 제3자 애플리케이션이 사용자의 보호된 리소스들에 액세스하기 전에, 시스템은 다음의 기능을 갖는다:

[0039] ◆ 중앙집중 보안 관리 시스템과 제3자 애플리케이션 간 상호 인증;

[0040] ◆ 제3자 애플리케이션에 대한 아이덴티티 및 그의 인증 증명서의 관리.

[0041] 도 1의 기존의 솔루션에 비해, 도 2의 제3자 애플리케이션은 그들의 아이덴티티, 인증 증명서 및 액세스 승인을 개별적으로 패킹(pack)하거나, 또는 아이덴티티, 인증 증명서 및 액세스 승인을 개별적으로 마킹(mark)하여, 본 출원에 따른 중앙집중 보안 관리 서버가 그들을 개별적으로 구별할 수 있도록 할 필요가 있을 수 있다.

[0042] 도 2에서, 권한 부여 서버_1/리소스 서버_1, 권한 부여 서버_2/리소스 서버_2 및 권한 부여 서버_n/리소스 서버_n은:

[0043] ◆ 상이한 소규모 및 중간 규모의 서비스 제공자, 또는

[0044] ◆ 몇몇 리소스 서버를 개별적을 배치한 동일한 대규모 서비스 제공자에 속할 수 있다.

[0045] 도 1의 기존 솔루션에 비해, 권한 부여 서버_i는 단계 5의 메시지가 제3자 애플리케이션으로부터 직접 오는 것인지 또는 단계 5에 도시된 바와 같이 중앙집중 보안 관리 시스템으로부터 오는 것인지를 구별해야 한다. 이러한 구별은, 예를 들면, 플래그를 통해 구현될 수 있다. 단계 5의 메시지가 제3자 애플리케이션으로부터 직접 오는 것이라면, 권한 부여 서버_i는 제3자 애플리케이션을 인증하고 액세스 승인을 유효화해야 한다; 단계 5의 메시지가 중앙집중 보안 관리 시스템에서 오는 것이라면, 권한 부여 서버_i는 액세스 승인을 단지 유효화해야 한다.

[0046] 도 1의 기존 솔루션에 비해, 도 5의 워크플로우의 변화는 다음과 같이 존재한다:

[0047] - 단계 5에서, 제3자 애플리케이션의 아이덴티티, 인증 증명서 및 액세스 승인은 구별가능한 방식으로 중앙집중 보안 관리 시스템으로 전송될 수 있고, 여기서, 구별가능한 방식은 중앙집중 보안 관리 시스템이 아이덴티티, 인증 증명서 및 액세스 승인을 구별할 수 있도록 그들을 개별적으로 패키징하거나 개별적으로 마킹할 수 있다는 것을 의미한다.

[0048] - 단계 6에서, 다음과 같은 두 개의 서브 단계를 포함한다:

[0049] ◆ 6-1: 제3자 애플리케이션을 성공적으로 인증한 후, 중앙집중 보안 관리 시스템은 액세스 승인을 권한 부여 서버_n으로 전달한다. 액세스 승인이 유효하면, 권한 부여 서버_n는 제3자 애플리케이션에 대해 발행된 액세스 토큰을 중앙집중 보안 관리 시스템으로 전송할 것이다. 본 발명에서, 액세스 승인 및 액세스 토큰은, 예를 들면, IETF 정의 인증 프로토콜에 부합한다.

[0050] ◆ 6-2: 중앙집중 보안 관리 시스템은 액세스 토큰을 제3자 애플리케이션으로 전달한다.

[0051] 더욱이, 본 발명의 솔루션에 따라, 제3자 애플리케이션이 유효한 액세스 토큰을 갖지 않으면, 리소스 서버는 제3자 애플리케이션의 액세스 요청을 사용자 에이전트로 리다이렉트한다.

[0052] 본 발명에 따른 중앙집중 보안 관리 시스템은, 예를 들면, 인증서를 발행하는 관리 서버, 제3자 애플리케이션의 보안 체크 서버, 제3자 애플리케이션의 레지스트리 관리 서버, 제3자 애플리케이션의 인증 서버, 제3자 애플리케이션의 저장 및 배포 서버 등을 포함할 수 있는 서버 그룹을 포함한다는 것을 유의해야 한다.

[0053] 본 발명에서, 사용자는 제3자 애플리케이션이 자신의 보호된 리소스들을 액세스하는 것을 가능하게 할 수 있다고 가정된다는 것을 또한 유의해야 한다. 자신의 보호된 리소스들 액세스하기 위해 제3자 애플리케이션에 권한 부여를 하기 전에, 사용자는 사용자의 아이덴티티가 인증되고 자신의 보호된 리소스들에 액세스하기 위한 제3자 애플리케이션을 승인할 권한을 가져, 제3자 애플리케이션이 액세스 토큰을 얻기 위한 액세스 승인을 얻는 것을 보장하도록 권한 부여 서버에 의해 인증되어야 한다. 본 발명의 솔루션에 따라, 사용자 인증은 사용자 에이전트와 권한 부여 서버 간의 직접적인 통신에 의해 또는 중앙집중 보안 관리 시스템을 통해 사용자 에이전트에 의한 권한 부여 서버로의 리디렉션(redirection)에 의해 구현될 수 있다.

[0054] 유사하게, 액세스 승인은 권한 부여 서버에 의해 사용자 에이전트를 통해 제3자 애플리케이션으로 전송되거나, 권한 부여 서버에 의해 중앙집중 보안 관리 시스템과 사용자 에이전트를 통해 제3자 애플리케이션으로 전송될 수 있다.

[0055] 더욱이, 본 발명에 따른 중앙집중 보안 관리 시스템은 다음의 기능들을 구현할 수 있다:

[0056] - 개인 개발자 또는 서비스 제공자에 의해 개발되고 개인 개발자 또는 서비스 제공자의 키들을 이용하여 서명하고 싸인하는 제3자 애플리케이션이 수신되는 경우, 개인 개발자 또는 서비스 제공자의 디지털 인증서를 이용하여 제3자 애플리케이션의 디지털 서명을 인증함으로써 제3자 애플리케이션의 추적가능성을 보장;

[0057] - 인증이 성공적으로 구현된 후, 제3자 애플리케이션이 악성 코드 또는 바이러스를 포함하고 있는지를 검출;

[0058] - 제3자 애플리케이션에 대한 안전 검출이 성공적으로 구현된 후, 중앙집중 보안 관리 시스템의 키들을 이용하여 제3자 애플리케이션을 디지털식으로 서명함으로써, 제3자 애플리케이션이 설치될 때, 보안성, 인증 및 신뢰성을 보장;

[0059] - 제3자 애플리케이션에 대한 아이덴티티, 인증 증명서 및 관련 속성의 균일한 배포의 관리를 수행;

[0060] - 생성, 발행 및 취소와 같은 모든 연관된 디지털 인증서에 대해 균일한 관리를 수행.

[0061] 본 발명에 따른 중앙집중 보안 관리 시스템을 이용함으로써, (사용자 및 보호된 리소스들의 관리만을 담당하는 것을 의미하는) 소규모 및 중간 규모의 서비스 제공자들의 부담을 줄이고 대량의 비용을 절감할 수 있으며, 또한 대규모 서비스 제공자가 그에 의해 배치된 복수의 내부 리소스 서버들에게 제3자 애플리케이션에 대한 중앙집중 관리를 제공하게 할 수 있다. 또한, 본 발명의 솔루션을 이용함으로써, 제3자 애플리케이션이 신뢰성있는 제3자 메커니즘(즉, 본 발명의 중앙집중 보안 관리 시스템)에 의해 안전하게 관리되기 때문에 제3자 애플리케이션이 더 보안적이고 신뢰성을 갖게 될 수 있다.

[0062] 이하, 본 발명의 실시예에 따른 제3자 애플리케이션에 대한 중앙집중 보안 관리를 수행하기 위한 방법이 도 3을 참조하여 설명된다. 이 실시예의 방법은 상기 도 2에 도시된 시스템에 적용될 수 있고, 우리는 전술한 시스템의 설명에 추가로 나아가지는 않을 것이다.

[0063] 도 3에 도시된 바와 같이, 첫 번째로, 단계 301에서, 제3자 애플리케이션은 자신의 아이덴티티, 인증 증명서 및 액세스 승인을 구별가능한 방식으로 중앙집중 보안 관리 시스템으로 전송한다. 인증 증명서는 여기서, 예를 들면, 디지털 인증서, 암호 또는 패스워드일 수 있고, 액세스 승인은, 예를 들면, IETF 정의 인증 프로토콜 OAuth2.0에 부합할 수 있다. 구별가능한 방식은, 아이덴티티, 인증 증명서 및 액세스 승인이 개별적으로 패키징되거나 개별적으로 마킹되어 중앙집중 보안 관리 시스템이 그들을 구별할 수 있도록 하는 것을 의미한다. 전술한 바와 같이, 실시예에서, 사용자는 제3자 애플리케이션이 자신의 보호된 리소스들에 액세스하는 것을 가능하게 한다고 가정된다. 제3자 애플리케이션이 리소스 서버에서 사용자의 보호된 리소스들에 액세스하는 것을 요청하는 경우, 제3자 애플리케이션인 유효한 액세스 토큰을 갖지 않는 경우, 리소스 서버는 제3자 애플리케이션의 액세스 요청을 사용자 에이전트로 리다이렉트(redirect)한다.

[0064] 액세스하기 위해 제3자 애플리케이션에 권한을 부여하기 전에, 제3자 애플리케이션이 액세스 승인을 이용하여 액세스 토큰을 얻기 위해 액세스 승인을 얻도록 사용자는 권한 부여 서버에 의해 인증되어야 하고, 권한 부여 서버에 의한 사용자의 인증은 권한 부여 서버에 대해 직접적으로 인증하는 사용자 에이전트에 의해 또는 인증을 위해 중앙집중 보안 관리 시스템을 통해 사용자 에이전트에 의한 권한 부여 서버로의 리디렉션에 의해 구현될 수 있다는 것을 유의해야 한다.

[0065] 권한 부여 서버가 액세스 승인을 제3자 애플리케이션에 전송한 후, 제3자 애플리케이션은 제3자 애플리케이션의 아이덴티티, 인증 증명서 및 액세스 승인을 중앙집중 보안 관리 시스템으로 전송하고, 액세스 승인은 권한 부여 서버에 의해 사용자 에이전트를 통해 제3자 애플리케이션으로 전송되거나 권한 부여 서버에 의해 중앙집중 보안 관리 시스템 및 사용자 에이전트를 통해 제3자 애플리케이션으로 전송될 수 있다는 것을 유의하자.

[0066] 다음에, 단계 302에서, 제3자 애플리케이션을 성공적으로 인증한 후 중앙집중 보안 관리 시스템은 액세스 승인을 권한 부여 서버로 전달한다. 액세스 승인은, 예를 들면, IETF 정의 인증 프로토콜 OAuth2.0에 부합한다.

[0067] 다음에, 단계 303에서, 액세스 승인이 유효하면, 권한 부여 서버는 사용자의 보호된 리소스들을 액세스하기 위한 액세스 토큰을 중앙집중 보안 관리 시스템을 통해 제3자 애플리케이션으로 발행한다. 액세스 토큰은, 예를 들면, IETF 정의 인증 프로토콜 OAuth2.0에 부합한다. 따라서, 제3자 애플리케이션은 사용자의 보호된 리소스들을 액세스하기 위해 액세스 토큰을 리소스 서버에 제출할 수 있다.

[0068] 실시예에서, 중앙집중 보안 관리 시스템, 사용자 에이전트, 제3자 애플리케이션, 권한 부여 서버 및 리소스 서버 간의 상호작용 프로세스는 임의의 기존 및 미래의 솔루션, 표준 및 기준의 방식에 부합할 수 있고, 전술한 OAuth2.0에 제한되지는 않는다.

[0069] 전술한 설명에서, 기존 시스템에 새로운 중앙집중 보안 관리 시스템을 부가함으로써 실시예에 따른 제3자 애플리케이션에 대한 중앙집중 보안 관리를 수행하는 방법을 이용함으로써, (사용자 및 보호된 리소스들의 관리만을 담당하는 것을 의미하는) 소규모 및 중간 규모의 서비스 제공자들의 부담을 줄이고 대량의 비용을 절감할 수 있으며, 또한 대규모 서비스 제공자가 그에 의해 배치된 복수의 내부 리소스 서버들에게 제3자 애플리케이션에 대

한 중앙집중 관리를 제공하게 할 수 있다는 것을 알 수 있다. 또한, 본 발명의 솔루션을 이용함으로써, 제3자 애플리케이션이 신뢰성있는 제3자 메커니즘(즉, 본 발명의 중앙집중 보안 관리 시스템)에 의해 안전하게 관리되기 때문에 제3자 애플리케이션이 더 보안적이고 신뢰성을 갖게 될 수 있다.

[0070] 동일한 개념 하에서, 본 발명의 또 다른 양상에 따라, 리소스 서버에 저장된 사용자의 보호된 리소스들에 액세스하기 위해 제3자 애플리케이션에 대한 중앙집중 보안 관리를 수행하기 위한 시스템이 제공된다. 이하, 도면을 참조하여 그러한 시스템을 설명할 것이다.

[0071] 도 4는 본 발명의 실시예에 따른 중앙집중 보안 관리 시스템(400)을 도시한다. 시스템(400)은 수신 디바이스(401), 인증 디바이스(402), 제1 전달 디바이스(403), 및 제2 전달 디바이스(404)를 포함한다. 유사하게, 사용자는 제3자 애플리케이션이 자신의 보호된 리소스들에 액세스하는 것을 가능하게 할 수 있다고 가정된다. 특히, 제3자 애플리케이션이 보호된 리소스들에 액세스하기 위해 요청할 때, 권한 부여 서버가 사용자를 성공적으로 인증하고 액세스 승인을 제3자 애플리케이션에 발행한 후, 수신 디바이스(401)는 제3자 애플리케이션에 의해 구별가능한 방식으로 전송된 제3자 애플리케이션의 아이덴티티, 인증 증명서 및 액세스 승인을 수신한다. 구별가능한 방식은 아이덴티티, 인증 증명서 및 액세스 승인이 개별적으로 패키징되거나 개별적으로 마킹되어, 중앙집중 보안 관리 시스템이 그들을 구별할 수 있도록 하는 것을 의미한다. 아이덴티티, 인증 증명서 및 액세스 승인을 수신한 후, 인증 디바이스(402)는 아이덴티티, 인증 증명서를 이용하여 제3자 애플리케이션을 인증한다. 제1 전달 디바이스(403)는 제3자 애플리케이션을 성공적으로 인증한 후 제3자 애플리케이션의 액세스 승인을 권한 부여 서버로 전달하고, 제2 전달 디바이스(404)는 권한 부여 서버에 의해 발행된 액세스 토큰을 제3자 애플리케이션에 전달한다. 따라서, 제3자 애플리케이션은 액세스 토큰을 리소스 서버에 제출함으로써 사용자의 보호된 리소스들에 액세스할 수 있다.

[0072] 전술한 바와 같이, 중앙집중 보안 관리 시스템(400)은 다음의 기능들을 추가로 구현한다:

[0073] - 개인 개발자 또는 서비스 제공자에 의해 개발되고 개인 개발자 또는 서비스 제공자의 키들을 이용하여 서명하고 싸인하는 제3자 애플리케이션이 수신되는 경우, 개인 개발자 또는 서비스 제공자의 디지털 인증서를 이용하여 제3자 애플리케이션의 디지털 서명을 인증함으로써 제3자 애플리케이션의 추적가능성을 보장;

[0074] - 인증이 성공적으로 구현된 후, 제3자 애플리케이션이 악성 코드 또는 바이러스를 포함하고 있는지를 검출;

[0075] - 제3자 애플리케이션에 대한 안전 검출이 성공적으로 구현된 후, 중앙집중 보안 관리 시스템의 키들을 이용하여 제3자 애플리케이션을 디지털식으로 서명함으로써, 제3자 애플리케이션이 설치될 때 보안성, 인증 및 신뢰성을 보장;

[0076] - 제3자 애플리케이션에 대한 아이덴티티, 인증 증명서 및 관련 속성의 균일한 배포의 관리를 수행;

[0077] - 생성, 발행 및 취소와 같은 모든 연관된 디지털 인증서에 대해 균일한 관리를 수행.

[0078] 제3자 애플리케이션에 대한 중앙집중 보안 관리 시스템의 보안 체크는 임의의 기존 및 미래의 솔루션, 표준 및 기준의 방식에 부합할 수 있다.

[0079] 구현예에서, 중앙집중 보안 관리 시스템(400) 및 수신 디바이스(401), 인증 디바이스(402), 제1 전달 디바이스(403) 및 제2 전달 시스템(404)은 소프트웨어, 하드웨어, 및 소프트웨어와 하드웨어의 조합의 형태로 구현될 수 있다. 예를 들면, 당업자는, 마이크로프로세서, 마이크로컨트롤러, ASIC(Application Specific Integrated Circuit), PLD(Programmable Logic Device) 및/또는 FPGA(Field Programmable Gate Array) 등과 같은 수단을 구현하기 위한 다양한 종류의 디바이스를 안다. 실시예에 따른 중앙집중 보안 관리 시스템의 각각의 컴포넌트들은 물리적으로 개별적으로 그리고 서로 동작가능하게 접속되어 실현될 수 있다.

[0080] 동작시에, 상기 도 4와 결합하여 설명된 실시예의 리소스 서버에 저장된 사용자의 보호된 리소스들에 액세스하기 위한 제3자 애플리케이션에 대한 중앙집중 보안 관리를 수행하기 위한 시스템은 전술한 제3자 애플리케이션에 대한 중앙집중 관리를 수행하기 위한 방법을 구현할 수 있다. 이 시스템을 이용함으로써, (사용자 및 보호된 리소스들의 관리만을 담당하는 것을 의미하는) 소규모 및 중간 규모의 서비스 제공자들의 부담을 줄이고 대량의 비용을 절감할 수 있으며, 또한 대규모 서비스 제공자가 그에 의해 배치된 복수의 내부 리소스 서버들에게 제3자 애플리케이션에 대한 중앙집중 관리를 제공하게 할 수 있다는 것을 알 수 있다. 또한, 본 발명의 솔루션을 이용함으로써, 제3자 애플리케이션이 신뢰성있는 제3자 메커니즘(즉, 본 발명의 중앙집중 보안 관리 시스템)에 의해 안전하게 관리되기 때문에 제3자 애플리케이션이 더 보안적이고 신뢰성을 갖게 될 수 있다.

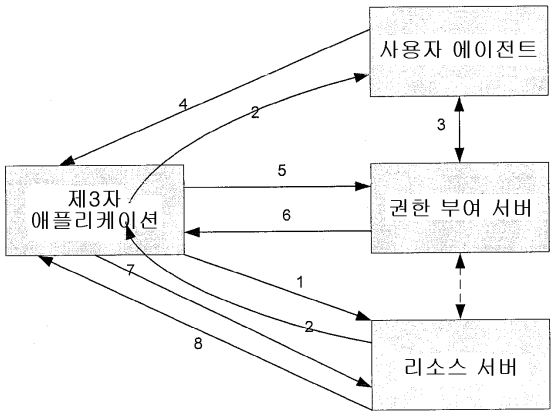
[0081] 동일한 진보적인 개념 하에서, 본 발명의 또 다른 양상에 따라, 적어도 하나의 권한 부여 서버, 적어도 하나의

리소스 서버, 사용자 에이전트, 제3자 애플리케이션, 및 본 발명에 따라 리소스 서버에 저장된 사용자의 보호된 리소스들에 액세스하기 위한 제3자 애플리케이션에 대해 중앙집중 보안 관리를 수행하는 시스템을 포함하는 통신 시스템이 제공된다. 더욱이, 통신 시스템은 라우터 등과 같은 다른 네트워크 구성요소들을 포함할 수 있다.

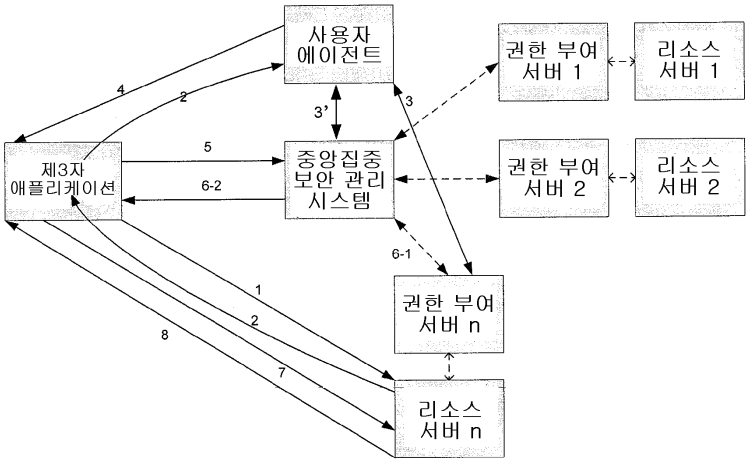
[0082] 제3자 애플리케이션에 대한 중앙집중 보안 관리를 수행하기 위한 방법, 리소스 서버에 저장된 사용자의 보호된 리소스들에 액세스하기 위한 제3자 애플리케이션에 대한 중앙집중 보안 관리를 수행하기 위한 시스템, 및 적어도 하나의 권한 부여 서버, 적어도 하나의 리소스 서버, 사용자 에이전트, 제3자 애플리케이션, 및 본 발명에 따라 리소스 서버에 저장된 사용자의 보호된 리소스들에 액세스하기 위한 제3자 애플리케이션에 대해 중앙집중 보안 관리를 수행하는 시스템을 포함하는 통신 시스템이 일부 예시적인 실시예에 의해 특별히 설명되어 있지만, 실시예들은 제한적이기보다는 예시적인 것으로 고려되어야 하고, 당업자는 본 발명의 사상 및 범위 내에서 다양한 종류의 변경예 및 수정예를 구현할 수 있다. 따라서, 본 발명은 실시예에 제한되지 않고, 본 발명의 범위는 첨부된 청구범위에 의해서만 정의된다.

도면

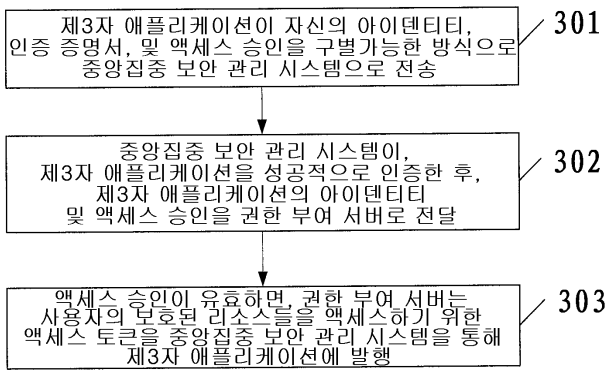
도면1



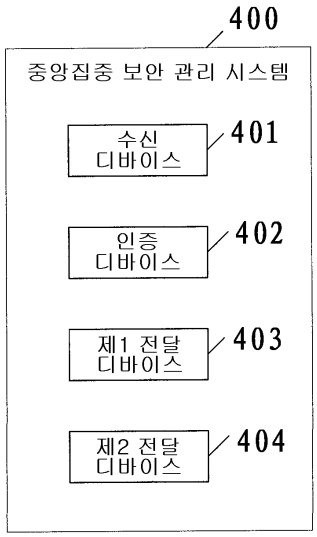
도면2



도면3


제3자 애플리케이션이 자신의 아이덴티티, 인증 증명서, 및 액세스 승인을 구별가능한 방식으로 중앙집중 보안 관리 시스템으로 전송
301
중앙집중 보안 관리 시스템이, 제3자 애플리케이션을 성공적으로 인증한 후, 제3자 애플리케이션의 아이덴티티 및 액세스 승인을 권한 부여 서버로 전달
302
액세스 승인이 유효하면, 권한 부여 서버는 사용자의 보호된 리소스들을 액세스하기 위한 액세스 토큰을 중앙집중 보안 관리 시스템을 통해 제3자 애플리케이션에 발행
303

도면4


400
중앙집중 보안 관리 시스템
수신 디바이스
401
인증 디바이스
402
제1 전달 디바이스
403
제2 전달 디바이스
404