(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년12월26일
(11) 등록번호 10-1215343
(24) 등록일자 2012년12월18일

(51) 국제특허분류(Int. Cl.)
G06Q 50/00D0 (2008.03)
(21) 출원번호 10-2006-0028369
(22) 출원일자 2006년03월29일
심사청구일자 2011년01월20일
(65) 공개번호 10-2007-0097736
(43) 공개일자 2007년10월05일
(56) 선행기술조사문헌
KR1020040005922 A*
KR1020050032856 A*
JP2005150833 A
JP2006018682 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
티무르 고르키시코
경기도 수원시 영통구 청명북로 81, 청명마을4단지아파트 407동 501호 (영통동)
이경희
경기도 용인시 기흥구 사은로126번길 10, 쌍용아파트 113동 902호 (보라동)
(74) 대리인
특허법인무한

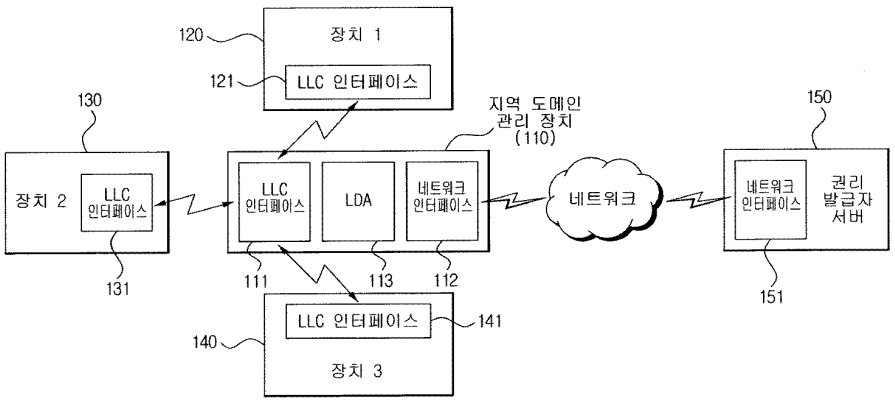
전체 청구항 수 : 총 34 항 심사관 : 이재근

(54) 발명의 명칭 **지역 도메인 관리 모듈을 가진 장치를 이용하여 도메인을 지역적으로 관리하는 장치 및 방법**

(57) 요 약

본 발명은 제한된 거리 내에 위치한 장치들의 정보를 수신하는 거리 제한 통신 채널 인터페이스, 및 상기 장치들 중 도메인의 구성원으로 선택된 장치를 인증(authenticate)하고, 상기 인증된 장치에게 상기 도메인에 대응한 장치 인증 정보(device authentication information)를 송신하고, 상기 인증된 장치를 상기 도메인의 구성원(member)으로 등록하는 지역 도메인 관리 모듈을 포함하는 도메인 관리 장치를 제공한다.

대 표 도



특허청구의 범위

청구항 1

제한된 거리 내에 위치한 장치들의 정보를 송수신하는 거리 제한 통신 채널 인터페이스; 및

상기 장치들 중 도메인의 구성원으로 선택된 장치를 인증(authenticate)하고, 상기 인증된 장치에게 상기 도메인에 대응한 장치 인증 정보(device authentication information)를 상기 거리 제한 통신 채널 인터페이스를 통하여 송신하고, 상기 인증된 장치를 상기 도메인의 구성원(member)으로 등록하는 지역 도메인 관리 모듈

을 포함하고,

상기 장치 인증 정보는 상기 인증된 장치에게 할당된(assigned) 도메인 내 장치 식별자(domain-based device ID), 권리 발급자 서버가 지역 도메인 관리 장치에게 할당한 LDA 식별자(LDA ID), 및 상기 인증된 장치의 장치 공용키 인증서(device public key certificate)의 해쉬값을 포함하는 것을 특징으로 하는 지역 도메인 관리 장치.

청구항 2

제한된 거리 내에 위치한 장치들의 정보를 송수신하는 거리 제한 통신 채널 인터페이스; 및

상기 장치들 중 도메인의 구성원으로 선택된 장치를 인증(authenticate)하고, 상기 인증된 장치에게 상기 도메인에 대응한 장치 인증 정보(device authentication information)를 상기 거리 제한 통신 채널 인터페이스를 통하여 송신하고, 상기 인증된 장치를 상기 도메인의 구성원(member)으로 등록하는 지역 도메인 관리 모듈

을 포함하고,

상기 장치 인증 정보는 지역 도메인 관리 장치의 LDA 공용키, 상기 인증된 장치에게 할당된(assigned) 도메인 내 장치 식별자(domain-based device ID), 및 권리 발급자 서버가 상기 지역 도메인 관리 장치에게 할당한 LDA 식별자(LDA ID)를 포함하는 것을 특징으로 하는 지역 도메인 관리 장치.

청구항 3

제한된 거리 내에 위치한 장치들의 정보를 송수신하는 거리 제한 통신 채널 인터페이스; 및

상기 장치들 중 도메인의 구성원으로 선택된 장치를 인증(authenticate)하고, 상기 인증된 장치에게 상기 도메인에 대응한 장치 인증 정보(device authentication information)를 상기 거리 제한 통신 채널 인터페이스를 통하여 송신하고, 상기 인증된 장치를 상기 도메인의 구성원(member)으로 등록하는 지역 도메인 관리 모듈

을 포함하고,

상기 장치 인증 정보는, 상기 도메인에 대한 도메인 정보; 상기 도메인의 도메인 개인키를 상기 인증된 장치의 공용키로 암호화한 암호화된 값(encrypted key); 및 상기 도메인의 도메인 공용키 인증서(domain public key certificate)를 포함하는 것을 특징으로 하는 지역 도메인 관리 장치.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 거리 제한 통신 채널 인터페이스는,

상기 제한된 거리 내에 위치한 장치들의 장치 식별자(device ID) 및 장치 공용키 인증서(device public key certificate)을 수신하는 것을 특징으로 하는 지역 도메인 관리 장치.

청구항 5

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 지역 도메인 관리 모듈은,

상기 제한된 거리 내에 위치한 상기 장치들의 정보를 사용자에게 제공하고, 상기 사용자로부터 상기 도메인의 구성원으로 등록할 장치에 대한 선택을 입력 받는 것을 특징으로 하는 지역 도메인 관리 장치.

청구항 6

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 지역 도메인 관리 모듈은,

상기 선택된 장치의 인증이 실패하면 상기 선택된 장치를 상기 지역 인증 폐기 목록(local revocation list)에 등록하는 것을 특징으로 하는 지역 도메인 관리 장치.

청구항 7

삭제

청구항 8

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 지역 도메인 관리 모듈은,

상기 인증된 장치를 상기 지역 도메인 관리 장치에 유지되는 도메인 구성원 리스트(domain member list)에 등록함으로써, 상기 인증된 장치를 상기 도메인의 구성원(member)으로 등록하는 것을 특징으로 하는 지역 도메인 관리 장치.

청구항 9

제8항에 있어서, 상기 도메인 구성원 리스트는 상기 도메인의 구성원의 장치 식별자 및 장치 인증 정보를 저장하는 것을 특징으로 하는 지역 도메인 관리 장치.

청구항 10

제9항에 있어서, 상기 지역 도메인 관리 모듈은,

제1 장치를 상기 도메인의 구성원으로부터 삭제하라는 요청에 응답하여, 상기 제1 장치를 상기 도메인 구성원 리스트로부터 삭제하고, 상기 제1 장치에게 상기 도메인에 대응한 장치 인증 정보의 삭제 요청을 송신하는 것을 특징으로 하는 지역 도메인 관리 장치.

청구항 11

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 지역 도메인 관리 모듈은,

상기 인증된 장치를 상기 도메인의 구성원으로 등록한 후, 상기 인증된 장치에게 할당된(assigned) 도메인 내 장치 식별자, 및 상기 인증된 장치의 장치 공용키 인증서를 권리 발급자 서버에게 송신하는 것을 특징으로 하는 지역 도메인 관리 장치.

청구항 12

제11항에 있어서, 상기 지역 도메인 관리 모듈은,

제1 장치를 상기 도메인의 구성원으로부터 삭제(delete)하는 경우, 상기 제1 장치의 장치 식별자를 상기 권리 발급자 서버에게 송신하는 것을 특징으로 하는 지역 도메인 관리 장치.

청구항 13

제1항에 있어서, 상기 지역 도메인 관리 모듈은,

사용자로부터 상기 도메인의 생성에 관한 도메인 정보(domain information)의 수신에 응답하여, 상기 지역 도메인 관리 장치의 장치 식별자(device ID), 상기 지역 도메인 관리 장치의 장치 공용키 인증서(device public key certificate) 및 상기 도메인 정보를 권리 발급자 서버(right issuer)에게 송신하는 것을 특징으로 하는 도메인 관리 장치.

청구항 14

제13항에 있어서, 상기 지역 도메인 관리 모듈은,

상기 권리 발급자 서버로부터 상기 도메인의 도메인 개인키(domain private key), LDA 공용키(LDA public key), LDA 개인키(LDA private key), LDA 공용키 인증서(LDA public key certificate), 및 도메인 크리덴셜(domain credential)을 수신하는 것을 특징으로 하는 지역 도메인 관리 장치.

청구항 15

제14항에 있어서, 상기 도메인 크리덴셜은,

도메인 공용키(domain public key), 상기 도메인 개인키(domain private key), 및 도메인 공용키 인증서(domain public key certificate)을 포함하는 것을 특징으로 하는 지역 도메인 관리 장치.

청구항 16

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 지역 도메인 관리 모듈은,

사용자로부터 상기 도메인의 제거 요청에 응답하여, 상기 도메인의 구성원으로 등록된 장치들을 상기 도메인에서 삭제하고, 상기 지역 도메인 관리 모듈에 저장된 상기 도메인의 도메인 정보를 삭제하는 것을 특징으로 하는 지역 도메인 관리 장치.

청구항 17

지역 도메인 관리 장치의 거리 제한 통신 채널 인터페이스를 통하여 상기 지역 도메인 관리 장치로부터 제한된 거리 내에 위치한 장치들의 정보를 수신하는 단계;

상기 지역 도메인 관리 장치의 지역 도메인 관리 모듈이 상기 장치들 중 도메인의 구성원으로 선택된 장치를 인증(authenticate)하는 단계; 및

상기 거리 제한 통신 채널 인터페이스가 상기 인증된 장치에게 상기 도메인에 대응한 장치 인증 정보(device authentication information)를 송신하는 단계; 및

상기 지역 도메인 관리 모듈이 상기 인증된 장치를 상기 도메인의 구성원(member)으로 등록하는 단계

를 포함하고,

상기 장치 인증 정보는 상기 인증된 장치에게 할당된(assigned) 도메인 내 장치 식별자(domain-based device ID), 권리 발급자 서버가 상기 지역 도메인 관리 장치에게 할당한 LDA 식별자(LDA ID), 및 상기 인증된 장치의 장치 공용키 인증서(device public key certificate)의 해쉬값을 포함하는 것을 특징으로 하는 도메인 관리 방법.

청구항 18

지역 도메인 관리 장치의 거리 제한 통신 채널 인터페이스를 통하여 상기 지역 도메인 관리 장치로부터 제한된 거리 내에 위치한 장치들의 정보를 수신하는 단계;

상기 지역 도메인 관리 장치의 지역 도메인 관리 모듈이 상기 장치들 중 도메인의 구성원으로 선택된 장치를 인증(authenticate)하는 단계; 및

상기 거리 제한 통신 채널 인터페이스가 상기 인증된 장치에게 상기 도메인에 대응한 장치 인증 정보(device authentication information)를 송신하는 단계; 및

상기 지역 도메인 관리 모듈이 상기 인증된 장치를 상기 도메인의 구성원(member)으로 등록하는 단계

를 포함하고,

상기 장치 인증 정보는 상기 지역 도메인 관리 장치의 LDA 공용키, 상기 인증된 장치에게 할당된(assigned) 도메인 내 장치 식별자(domain-based device ID),, 및 권리 발급자 서버가 상기 지역 도메인 관리 장치에게 할당한 LDA 식별자(LDA ID)를 포함하는 것을 특징으로 하는 도메인 관리 방법.

청구항 19

지역 도메인 관리 장치의 거리 제한 통신 채널 인터페이스를 통하여 상기 지역 도메인 관리 장치로부터 제한된 거리 내에 위치한 장치들의 정보를 수신하는 단계;

상기 지역 도메인 관리 장치의 지역 도메인 관리 모듈이 상기 장치들 중 도메인의 구성원으로 선택된 장치를 인증(authenticate)하는 단계; 및

상기 거리 제한 통신 채널 인터페이스가 상기 인증된 장치에게 상기 도메인에 대응한 장치 인증 정보(device

authentication information)를 송신하는 단계; 및

상기 지역 도메인 관리 모듈이 상기 인증된 장치를 상기 도메인의 구성원(member)으로 등록하는 단계

를 포함하고,

상기 장치 인증 정보는, 상기 도메인에 대한 도메인 정보; 상기 도메인의 도메인 개인키를 상기 인증된 장치의 공용키로 암호화한 암호화된 값(encrypted key); 및 상기 도메인의 도메인 공용키 인증서(domain public key certificate)를 포함하는 것을 특징으로 하는 도메인 관리 방법.

청구항 20

제17항 내지 제19항 중 어느 한 항에 있어서, 상기 제한된 거리 내에 위치한 장치들의 정보를 수신하는 상기 단계는,

상기 제한된 거리 내에 위치한 장치들의 정보를 거리 제한 통신 채널 인터페이스(LLC interface: location limited channel interface)를 통하여 수신하는 것을 특징으로 하는 도메인 관리 방법.

청구항 21

제17항 내지 제19항 중 어느 한 항에 있어서, 상기 제한된 거리 내에 위치한 장치들의 정보를 거리 제한 통신 채널 인터페이스를 통하여 수신하는 단계는,

상기 거리 제한 통신 채널 인터페이스가 상기 지역 도메인 관리 장치로부터 제한된 거리 내에 위치한 장치들의 장치 식별자(device ID) 및 장치 공용키 인증서(device public key certificate)를 수신하는 단계

를 포함하는 것을 특징으로 하는 도메인 관리 방법.

청구항 22

제17항 내지 제19항 중 어느 한 항에 있어서, 상기 장치들 중 도메인의 구성원으로 선택된 장치를 인증하는 단계는,

상기 지역 도메인 관리 모듈이 상기 제한된 거리 내에 위치한 상기 장치들의 정보를 사용자에게 제공하는 단계; 및

상기 사용자로부터 상기 도메인의 구성원으로 등록할 장치에 대한 선택을 입력 받는 단계

를 더 포함하는 것을 특징으로 하는 도메인 관리 방법.

청구항 23

제17항 내지 제19항 중 어느 한 항에 있어서, 상기 선택된 장치를 인증(authenticate)하는 단계는,

상기 지역 도메인 관리 모듈이 상기 선택된 장치의 장치 공용키 인증서를 체크하는 단계

를 더 포함하는 것을 특징으로 하는 도메인 관리 방법.

청구항 24

제17항 내지 제19항 중 어느 한 항에 있어서, 상기 선택된 장치를 인증(authenticate)하는 단계는,

상기 지역 도메인 관리 모듈이 상기 선택된 장치가 지역 인증 폐기 목록(local revocation list)에 등록되어 있는지 판단하는 단계; 및

상기 선택된 장치의 인증이 실패하면 상기 지역 도메인 관리 모듈이 상기 선택된 장치를 상기 지역 인증 폐기 목록에 등록하는 단계

를 더 포함하는 것을 특징으로 하는 도메인 관리 방법.

청구항 25

제17항 내지 제19항 중 어느 한 항에 있어서, 상기 선택된 장치를 인증(authenticate)하는 단계는,

상기 지역 도메인 관리 모듈이 권리 발급자 서버와 통신하여 상기 선택된 장치의 장치 공용키 인증서를 체크하

는 단계

를 더 포함하는 것을 특징으로 하는 도메인 관리 방법.

청구항 26

제17항 내지 제19항 중 어느 한 항에 있어서, 상기 선택된 장치를 인증(authenticate)하는 단계는,

상기 지역 도메인 관리 모듈이 권리 발급자 서버와 통신하여 상기 지역 도메인 관리 장치에서 상기 선택된 장치가 전역 인증 폐기 목록(global revocation list)에 등록되어 있는지 판단하는 단계;

상기 선택된 장치의 인증이 실패하면 상기 지역 도메인 관리 모듈이 권리 발급자 서버와 통신하여 상기 선택된 장치를 상기 전역 인증 폐기 목록에 등록하는 단계; 및

상기 지역 도메인 관리 모듈이 권리 발급자 서버와 통신하여 상기 지역 인증 폐기 목록의 갱신 요청을 수신하는 단계

를 더 포함하는 것을 특징으로 하는 도메인 관리 방법.

청구항 27

제17항 내지 제19항 중 어느 한 항에 있어서, 상기 장치 인증 정보는 도메인 크리덴셜(domain credential)을 더 포함하는 것을 특징으로 하는 도메인 관리 방법.

청구항 28

제27항에 있어서, 상기 도메인 크리덴셜은,

상기 도메인에 대한 도메인 정보;

상기 도메인의 도메인 개인키를 상기 인증된 장치의 공용키로 암호화한 암호화된 값(encrypted key); 및

상기 도메인의 도메인 공용키 인증서(domain public key certificate)

을 포함하는 것을 특징으로 하는 도메인 관리 방법

청구항 29

제28항에 있어서, 상기 도메인 정보는,

상기 도메인의 도메인 이름을 포함하는 것을 특징으로 하는 도메인 관리 방법.

청구항 30

제17항 내지 제19항 중 어느 한 항에 있어서, 상기 도메인의 구성원(member)으로 등록하는 단계는,

상기 인증된 장치를 상기 지역 도메인 관리 장치에 유지되는 도메인 구성원 리스트(domain member list)에 등록하는 것을 특징으로 하는 도메인 관리 방법.

청구항 31

제30항에 있어서, 상기 도메인 구성원 리스트는 상기 도메인의 구성원의 장치 식별자 및 장치 인증 정보를 저장하는 것을 특징으로 하는 도메인 관리 방법.

청구항 32

제30항에 있어서,

상기 지역 도메인 관리 장치가 제1 장치를 상기 도메인의 구성원으로부터 삭제하라는 요청을 수신하는 단계;

상기 지역 도메인 관리 장치가 상기 제1 장치를 상기 도메인 구성원 리스트로부터 삭제하는 단계; 및

상기 지역 도메인 관리 장치가 상기 제1 장치에게 상기 도메인에 대응한 장치 인증 정보의 삭제 요청을 송신하는 단계

를 더 포함하는 것을 특징으로 하는 도메인 관리 방법.

청구항 33

제17항에 있어서,

상기 지역 도메인 관리 장치가 상기 인증된 장치에게 할당된(assigned) 도메인 내 장치 식별자, 및 상기 인증된 장치의 장치 공용키 인증서를 권리 발급자 서버에게 송신하는 단계

를 더 포함하는 것을 특징으로 하는 도메인 관리 방법.

청구항 34

제33항에 있어서,

제1 장치를 상기 도메인의 구성원으로부터 삭제(delete)하는 경우, 상기 지역 도메인 관리 장치가 상기 제1 장치의 장치 식별자를 상기 권리 발급자 서버에게 송신하는 단계

를 더 포함하는 것을 특징으로 하는 도메인 관리 방법.

청구항 35

삭제

청구항 36

삭제

청구항 37

삭제

청구항 38

삭제

청구항 39

삭제

청구항 40

삭제

청구항 41

삭제

청구항 42

삭제

청구항 43

삭제

청구항 44

삭제

청구항 45

제17항 내지 제19항 중 어느 한 항의 방법을 수행하는 프로그램을 기록한 컴퓨터 판독 가능 기록매체.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0006] 본 발명은 디지털 콘텐츠의 보호(protection of digital contents)에 관한 것으로, 더욱 상세하게는 디지털 콘텐츠의 보호를 위하여 도메인을 생성 및 삭제하거나 상기 도메인에 장치를 추가하거나 삭제하는 도메인 관리 방법 및 장치에 관한 것이다.

[0007] 디지털 콘텐츠의 보호는 콘텐츠 소유자에게 매우 중요한 이슈이다. 만약 디지털 콘텐츠를 보호하는 메커니즘이 없다면, 누구나 아무런 대가 없이 디지털 콘텐츠를 소비할 수 있기 때문에, 콘텐츠 소유자는 콘텐츠를 배포하는 것으로부터 아무런 이익을 얻을 수 없다. 따라서, 일반적으로 콘텐츠 소유자는 자신의 콘텐츠를 권한 없이 소비하는 것을 방지하기 위한 메커니즘을 구현한다. 전형적으로, 이러한 디지털 콘텐츠의 보호에 디지털 저작권 관리 시스템(DRM system: digital rights management system)이 관여된다.

[0008] DRM 보호의 한 방법은 한 그룹의 장치들에게 콘텐츠 공유를 허용하는 것이다. 이러한 한 그룹을 통상 하나의 도메인(domain)으로 부른다. 즉, 하나의 도메인에 속한 장치들에게 콘텐츠 공유를 허용할 수 있다. 하나의 도메인에 속하는 장치들은, 예를 들어, 콘텐츠 제공 서버 상에 동일한 계정 정보를 가지고, 디지털 콘텐츠에 대한 접근을 공유할 수 있다. 사용자는 상기 도메인에 속하는 어떤 장치들을 이용해서도 상기 도메인에서 허용되는 콘텐츠를 접근할 수 있다.

[0009] 하나의 도메인에 속하는 콘텐츠를 접근하는 것에 대해 다양한 지불 방법이 사용될 수 있다. 예를 들어, 하나의 도메인에 속하는 장치들의 소유자는, 일단 자신이 구입한 콘텐츠에 대해 상기 도메인에 속하는 어떤 장치를 이용해서도 자유롭게 접근할 수 있다. 또 다른 지불 방법으로는 하나의 도메인에 속하는 장치들에 대하여 전체 접근 회수를 제한하는 방법이 있다. 하나의 도메인에 속하는 장치들 중 어떤 장치를 사용해서 접근하는지에 상관 없이 지불 금액에 따라 전체 접근 회수만 제한되는 것이다. 이러한 DRM 시스템은 콘텐츠 소유자 및 콘텐츠 소비자 모두에게 매우 편리하다.

[0010] 그러나, 콘텐츠의 소비자들이나 장치 제조업자들은 장치들의 도메인 관리에 몇 가지 문제점을 가지고 있다. 첫 번째 문제는 장치를 콘텐츠 제공자 또는 디지털 권리 발급자에 등록하기 위해서는 상기 장치가 인터넷 접속 능력을 가져야 한다는 것이다. 즉, 종래기술에 따르면, 권리 발급자 서버에 네트워크 통신을 통하여 접속하여 장치를 도메인에 추가하여야 하기 때문에, 상기 장치가 네트워크 통신 기능을 가지고 있어야 했다. 따라서, 장치 제조업자의 입장에서는 장치를 제조할 때 상기 장치에 네트워크 접속 능력을 포함시켜야 하고, 이는 추가적인 비용 부담이 되었다. 또한, 사용자의 입장에서는 네트워크 접속 능력이 없는 종래의 장치(legacy devices)를 도메인에 등록할 수 없었다. 통상적으로 MP3 플레이어, 디지털 카메라 등의 장치에는 네트워크 접속 능력이 포함되지 않으므로, 이러한 장치들은 종래기술에 따른 디지털 저작권 관리 시스템의 도메인 기능을 이용할 수 없었다. 두 번째 문제는 장치에 대한 도메인 멤버십 요청을 한 후 승인(authorization)을 받기까지 꽤 긴 시간을 기다려야 한다는 것이다. 종래기술에 따르면, 이러한 승인은 권리 발급자(right issuer)와 같이 외부의 권한 있는 객체(external trusted entity)에 의하여 수행되기 때문에, 이러한 외부의 권한 있는 객체와 통신하는 데 많은 시간이 소요되었다. 세 번째 문제는 도메인을 생성할 때 상기 도메인에 속하는 구성원 장치들을 모두 등록하여야 한다는 것이다. 따라서, 도메인에 속하는 구성원 장치들을 변경하는 작업이 매우 복잡해지고, 유연하지 못하게 된다. 또한, 도메인을 생성할 때 상기 도메인에 속하는 구성원 장치들을 모두 등록하여야 하지만, 콘텐츠를 구입할 때 상기 콘텐츠를 사용할 모든 장치를 파악하는 것이 용이하지 않아서 도메인 생성 시 구성원 장치들을 모두 등록하는 것은 현실적으로 어려움이 있었다. 이러한 이유들로 인하여 도메인 방식의 디지털 콘텐츠 관리 방법이 널리 사용되지 못하고 있다.

[0011] 따라서, 네트워크 접속 능력이 없는 장치들에 대해서도 도메인 멤버십을 허용하면서, 사용자에게 도메인 관리의 편리성을 제공하는 쉽고 안전한 도메인 관리 방법 및 장치가 요구되고 있다.

발명이 이루고자 하는 기술적 과제

[0012] 따라서, 본 발명은 상술한 본 발명의 문제점을 해결하기 위한 것으로서, 네트워크 접속 능력이 없는 장치들도

디지털 저작권 관리 시스템의 도메인 기능을 이용할 수 있도록 하는 도메인 관리 방법 및 장치를 제공하는 것을 목적으로 한다.

[0013] 또한 본 발명의 목적은 장치에 대한 도메인 멤버십 요청을 한 후 빠른 시간 내에 승인이 이루어질 수 있도록 하는 도메인 관리 방법 및 장치를 제공하는 것이다.

[0014] 또한 본 발명의 목적은 도메인의 생성 및 상기 도메인에의 새로운 장치의 추가를 쉽고 유연하게 수행할 수 있는 도메인 관리 방법 및 장치를 제공하는 것이다.

발명의 구성 및 작용

[0015] 상기와 같은 본 발명의 목적을 달성하기 위한 도메인 관리 장치는 제한된 거리 내에 위치한 장치들의 정보를 송수신하는 거리 제한 통신 채널 인터페이스, 및 상기 장치들 중 도메인의 구성원으로 선택된 장치를 인증(authenticate)하고, 상기 인증된 장치에게 상기 도메인에 대응한 장치 인증 정보(device authentication information)를 상기 거리 제한 통신 채널 인터페이스를 통하여 송신하고, 상기 인증된 장치를 상기 도메인의 구성원(member)으로 등록하는 지역 도메인 관리 모듈을 포함한다.

[0016] 본 발명의 일측에 따르면, 상기 장치 인증 정보는 상기 인증된 장치에게 할당된(assigned) 도메인 내 장치 식별자(domain-based device ID), 권리 발급자 서버가 상기 지역 도메인 관리 장치에게 할당한 LDA 식별자(LDA ID), 및 상기 인증된 장치의 장치 공용키 인증서(device public key certificate)의 해쉬 값을 상기 지역 도메인 관리 장치의 LDA 개인키(LDA public key)로 서명한 서명(signature)을 포함한다.

[0017] 본 발명의 또 다른 일측에 따르면, 지역 도메인 관리 장치에서 상기 지역 도메인 관리 장치로부터 제한된 거리 내에 위치한 장치들의 정보를 거리 제한 통신 채널 인터페이스(LLC interface: location limited channel interface)를 통하여 수신하는 단계, 상기 장치들 중 도메인의 구성원으로 선택된 장치를 인증(authenticate)하는 단계, 상기 인증된 장치에게 상기 도메인에 대응한 장치 인증 정보(device authentication information)를 송신하는 단계, 및 상기 인증된 장치를 상기 도메인의 구성원(member)으로 등록하는 단계를 포함하는 도메인 관리 방법이 제공된다.

[0018] 본 발명의 또 다른 일측에 따르면, 지역 도메인 관리 장치(LDA: local domain authority device)에서 도메인을 생성하는 단계, 및 상기 지역 도메인 관리 장치에서 상기 지역 도메인 관리 장치로부터 제한된 거리 내에 위치한 장치들의 정보를 거리 제한 통신 채널 인터페이스(LLC interface: location limited channel interface)를 통하여 수신하고, 상기 장치들 중 선택된 장치를 상기 도메인의 구성원(member)으로 등록하는 단계를 포함하는 도메인 관리 방법이 제공된다.

[0019] 본 발명의 또 다른 일측에 따르면, 지역 도메인 관리 장치로부터 상기 지역 도메인 관리 장치의 장치 공용키 인증서(device public key certificate), 상기 지역 도메인 관리 장치의 장치 식별자(device ID) 및 생성할 도메인에 대응한 도메인 정보를 수신하는 단계, 상기 장치 공용키 및 상기 장치 식별자를 체크하는 단계, 및 상기 도메인에 대응하는 도메인 개인키, 도메인 공용키 및 도메인 공용키 인증서를 상기 지역 도메인 관리 장치로 송신하는 단계를 포함하는 권리 발급자 서버에서의 도메인 관리 방법이 제공된다.

[0020] 이하 첨부 도면들 및 첨부 도면들에 기재된 내용들을 참조하여 본 발명의 바람직한 실시예를 상세하게 설명하지만, 본 발명이 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조부호는 동일한 부재를 나타낸다.

[0021] 도 1은 본 발명의 일례에 따라 지역 도메인 관리 장치로 선택된 사용자 장치 및 권리 발급자 서버의 연결을 도시한 도면이다.

[0022] 본 발명에 따르면, 지역 도메인(local domain)의 구성원(member)이 되려는 모든 장치들(110, 120, 130, 140)은 거리 제한 통신 채널 인터페이스(LLC interface: location limited channel interface)(111, 121, 131, 141)를 포함한다. 거리 제한 통신 채널 인터페이스(LLC interface)는 제한된 거리 내에 있는 상대방 장치와만 통신할 수 있는 통신 채널 인터페이스(communication channel interface)로, 거리의 제한 없이 통신할 수 있는 네트워크 인터페이스(network interface)와 구별된다. 거리 제한 통신 채널의 예로는 적외선 통신 채널(infra red communication channel), 블루투수(Bluetooth)와 같은 단거리 무선 통신 채널(short range wireless communication channel), 제한된 거리의 케이블을 갖는 유선 통신 채널(wire communication channel with limited length of cable), 초음파 통신 채널(ultrasonic channel) 등이 있다. 거리의 제한 없이 통신할 수 있는 네트워크 인터페이스는 인터넷 통신 기능을 지원하는 이더넷 인터페이스(Ethernet interface) 등이 있다.

[0023] 본 발명에 따르면, 인증(authentication)의 목적을 위하여, 모든 장치들(110, 120, 130, 140)은 장치 공용키/개인키 쌍(device public/private key pair) 및 장치 공용키 인증서(device public key certificate)을 가지고 있다. 상기 장치 공용키/개인키 쌍 및 장치 공용키 인증서는 상기 장치의 생산 시 장치 제조업자에 의하여 상기 장치들에 저장될 수 있다. 또한, 상기 장치들(110, 120, 130, 140)은 고유의 장치 식별자(device identifier)를 가지고 있다. 상기 장치 식별자(device ID)는 상기 장치를 식별하기 위한 것으로, 예를 들어, 상기 장치의 고유한 시리얼 번호, 장치의 이름, 제조업자 식별 데이터 등을 포함할 수 있다. 장치 식별자도 제조업자에 의하여 장치의 생산 시 상기 장치에 저장될 수 있다.

[0024] 사용자는 자신이 사용하는 장치들 중 지역 도메인 관리 모듈(local domain authority module: LDA module)(113)이 장착된 장치(110)를 선택하여 지역 도메인 관리 장치(local domain authority device)로 사용한다. 지역 도메인 관리 모듈(113)은 지역 도메인 관리를 책임진다. 예를 들어, 지역 도메인 관리 모듈(113)은 사용자의 장치들 중 도메인의 구성원으로 선택된 장치를 인증(authenticate)하고, 상기 인증된 장치에게 상기 도메인에 대응한 장치 인증 정보(device authentication information)를 상기 거리 제한 통신 채널 인터페이스를 통하여 송신하고, 상기 인증된 장치를 상기 도메인의 구성원(member)으로 등록한다. 도메인에 조인(join)하는 장치들 모두가 LDA 모듈을 포함하고 있을 필요는 없다. 단지 지역 도메인 관리 장치로 사용될 장치만 LDA 모듈을 포함하고 있으면 된다. 한 사용자가 사용하는 장치들 중 지역 도메인 관리 모듈이 장착된 장치가 복수 개 있는 경우에는, 사용자는 하나의 도메인에 대하여 하나의 장치를 선택하고, 상기 선택된 장치를 지역 도메인 관리 장치로 사용할 수 있다. 따라서, 이 경우에는 지역 도메인 관리 모듈이 있는 장치라 하더라도 지역 도메인을 관리하지 않고 단지 구성원 장치(member device)로만 동작할 수 있다.

[0025] 지역 도메인 관리 장치(LDA device)(110)는 또한 다른 장치들과 거리 제한 통신을 수행하기 위한 거리 제한 통신 채널 인터페이스(LLC interface)(111)를 포함한다. 거리 제한 통신 채널 인터페이스(111)는 다른 장치들과 도메인 관리에 관한 정보를 통신하는 데 사용된다.

[0026] 지역 도메인 관리 장치(110)는 또한 권리 발급자 서버(right issuer)(150)와 통신하기 위한 네트워크 인터페이스(112)를 포함한다. 본 발명에 따르면, 지역 도메인 관리 장치(110)에 대해서만 네트워크 인터페이스가 필수적으로 요청되고, 다른 장치들에 대해서는 네트워크 인터페이스가 필수적으로 요청되지 않는다. 따라서, 본 발명에 따르면, 다른 장치들은 네트워크 인터페이스를 포함하지 않더라도 도메인에 조인하여 디지털 콘텐츠에 접근할 수 있다.

[0027] 네트워크 인터페이스 및 거리 제한 통신 채널 인터페이스를 포함한 이동 전화에 LDA 모듈을 탑재한 경우, 상기 이동 전화가 지역 도메인 관리 장치로 이용될 수 있다. 사용자는 상기 이동 전화를 지역 도메인 관리 장치로 선택하고, 사용자의 다른 장치들(MP3 플레이어, 디지털 카메라, 기타 홈 네트워킹 장비들 등)을 상기 이동 전화를 이용하여 도메인에 조인시킬 수 있다. 그러면, 상기 사용자의 다른 장치들은 네트워크 통신 기능이 없어도, 디지털 저작권 관리를 위한 도메인 기능을 이용할 수 있게 된다.

[0028] 지역 도메인 관리 장치(110)도 다른 장치들과 같이 장치 공용키/개인키 쌍(device public/private key pair), 장치 공용키 인증서(device public key certificate) 또는 장치 식별자(device ID)를 포함할 수 있다.

[0029] 권리 발급자 서버(right issuer)(150)는 네트워크 인터페이스(151)를 통하여 지역 도메인 관리 장치(110)와 통신한다. 본 발명에서는, 권리 발급자 서버(150)는 도메인에 조인한 모든 장치들과 통신할 필요가 없다. 권리 발급자 서버(150)는 단지 도메인에 대응하는 지역 도메인 관리 장치(110)와만 통신하면 된다.

[0030] 본 발명의 도메인 관리 절차는 권리 발급 서버(150)가 지역 도메인 관리 장치(110)에게 얼마나 많은 도메인 관리 권한을 위임했는지에 따라 다르게 된다. 위임되는 도메인 관리 권한은 모든 권한으로부터 아무런 권한이 없는 것까지 다양하다. 모든 권한을 위임한 경우에는, 지역 도메인 관리 장치(110)는 자신의 자원을 사용하여 도메인을 관리하고, 장치들을 인증한다. 권리 발급 서버(150)는 단지 선택적으로 지역 도메인 관리 장치(110)가 수행한 도메인 관리 액션들에 대하여 통지 받을 뿐이다. 아무런 권한도 위임하지 않은 경우에는, 지역 도메인 관리 장치(110)는 "관리 프록시(management proxy)"와 같이 동작하고, 모든 정보를 권리 발급자 서버(150)에 전달한다. 권리 발급자 서버(150)는 도메인 관리에 필요한 모든 액션들을 수행하고, 지역 도메인 관리 장치(110)에게 액션의 결과들에 관하여 통지한다. 이 경우에도, 도메인에 조인하는 장치들은 네트워크 인터페이스가 필요하지 않다. 권리 발급 서버(150)가 지역 도메인 관리 장치(110)에게 일부의 권리를 위임한 경우, 도메인 관리 절차는 지역 도메인 관리 장치(110) 및 권리 발급 서버(150)에 의하여 나누어 수행된다.

[0031] 지역 도메인(local domain)을 생성하기 위해, 사용자는 LDA를 가진 자신의 장치(110)를 권리 발급 서버(150)에

등록한다. 이에 대한 응답으로 권리 발급 서버(150)는 LDA 공용키/개인키 쌍(LAD public/private key pair), LDA 공용키 인증서(LDA public key certificate), LDA 식별자(LDA ID) 및 도메인 크리덴셜(domain credential)을 LDA를 가진 장치(110)에게 송신한다. 뒤에 LDA 모듈(113)은 상기 정보들을 권리 발급 서버(150)와 통신하거나 다른 장치들(120, 130, 140)을 위한 인증 정보(authentication information)를 서명(sign)하는 데 사용할 수 있다. 또한, 도메인에 속한 장치들은 해당 도메인의 콘텐츠를 접근하기 위하여 도메인 크리덴셜을 사용한다. 즉, 해당 콘텐츠를 접근할 때 도메인 크리덴셜에 따라 접근이 허용되는 것이다.

[0032] 본 발명에서 LDA를 가진 장치(110)는 다른 장치들(120, 130, 140)과 접촉하고 정보를 교환하기 위하여 거리 제한 통신 채널(LLC: location limited channel)(111)을 사용한다. 사용자는 LDA를 가진 장치(110)를 사용하여 지역 도메인을 구성(form)할 장치들을 탐색(discover)한다. 상기 LDA를 가진 장치(110)로는 LDA 모듈이 탐재된 이동 전화가 사용될 수 있다. 사용자는 이렇게 탐색된 장치들 중 지역 도메인에 추가할 장치들을 선택할 수 있다. 이러한 접근은 사용자에게 매우 자연스럽다. 예를 들어, 적외선 거리 제한 통신 채널(infra-red location limited channel)을 사용하여 지역 도메인 관리 장치(110)로부터 일정한 거리 내에 위치한 장치들(120, 130, 140)을 탐색한다. 상기 탐색된 장치들(120, 130, 140)과 지역 도메인 관리 장치(110)는 거리 제한 통신 채널(LLC)을 통하여 정보를 교환한다. 더 구체적으로 상기 탐색된 장치들(120, 130, 140)은 상기 지역 도메인 관리 장치(110)로 장치 식별자(device ID) 및 장치 공용키 인증서(device public key certificate)을 송신한다. 지역 도메인 관리 장치(110)는 상기 탐색된 장치들(120, 130, 140)로부터 수신된 장치 공용키 인증서를 검증(verify)한다. 탐색되거나 검증된 장치들의 정보는 상기 지역 도메인 관리 장치(110)의 디스플레이에 표시된다. 그러면, 사용자는 상기 디스플레이에 표시된 장치들 중 지역 도메인에 추가할 장치들을 포인팅하여 선택할 수 있다. 지역 도메인 관리 장치(110)는 상기 선택된 장치들에게 도메인 크리덴셜 및 장치 인증 정보(device authentication information)를 송신한다. 후에, 상기 장치들은 지역 도메인 관리 장치, 다른 장치들 또는 권리 발급 서버에게 상기 장치 인증 정보를 제시함으로써, 자신이 해당 도메인의 구성원임을 증명할 수 있다.

[0033] 사용자는 지역 도메인 관리 모듈(LDA: local domain authority)을 가진 장치(110)를 사용하여 장치들(120, 130, 140)의 지역 도메인(local domain)을 관리한다. 지역 도메인 관리 모듈(LDA)을 가진 장치(110)는 다른 장치들(120, 130, 140)과 접촉하고, 상기 다른 장치들과 정보를 교환하고, 상기 다른 장치들을 지역 도메인에 등록(register)한다. LDA를 가진 장치(110)는 도메인 관리에 관한 권한(authorization)을 권리 발급 서버(right issuer)(150)로부터 부여 받을(delegated) 수 있다. 상기 도메인 관리(domain management)에는 새로운 도메인을 생성하는 것, 도메인에 새로운 장치를 추가하는 것, 도메인으로부터 장치를 삭제하는 것, 및 도메인을 삭제하는 것 등의 일부 혹은 전부를 포함한다. 본 발명의 일 실시예에 따르면, LDA를 가진 장치(110)는 권리 발급 서버(150)에 접촉하여 지역 도메인 관리에 대한 권한(authorization)을 수신할 수 있다.

[0034] 본 발명에서 도메인 관리를 수행하는 장치는 LDA 모듈을 포함한 지역 도메인 관리 장치이다. 지역 도메인 관리 장치는 인증을 위하여 LDA 공용키/개인키 쌍(LDA public/private key pair)를 가진다. 지역 도메인 관리 장치는 상기 LDA 공용키/개인키 쌍을 다양한 방법으로 얻을 수 있다. 한 방법은 지역 도메인 관리 장치가 도메인을 생성하기 전에 권리 발급 서버로부터 상기 키 정보를 수신하는 것이다. 또 다른 방법으로는 LDA 모듈이 스스로 상기 키 정보를 생성할 수도 있다.

[0035] 도메인의 보안은 매우 중요한 이슈이기 때문에, 지역 도메인 관리 장치(110) 또는 권리 발급 서버(150)는 인증 폐기 목록(device revocation list)을 유지할 수 있다. 인증 폐기 목록은 어떠한 이유로든 지역 도메인 관리 장치(110) 또는 권리 발급 서버(150)에게 인증이 실패한 것으로 알려진 장치들에 대한 정보를 유지한다. 인증 폐기 목록에 등록된 장치는 보안상 문제가 있는 장치로 볼 수 있다. 몇몇 제3의 기관(예를 들어, 콘텐츠 관리자, 장치 제조업자 등)이 주기적으로 지역 도메인 관리 장치(110) 또는 권리 발급 서버(150)에게 인증 폐기 목록(device revocation list)의 갱신 정보를 제공할 수도 있다. 권리 발급 서버(150)가 지역 도메인 관리 장치(110)에 얼마나 많은 권한을 위임했는지에 따라, 지역 인증 폐기 목록(local device revocation list) 및 전역 인증 폐기 목록(global device revocation list)이 사용될 수 있다. 지역 인증 폐기 목록은 지역 도메인 관리 장치(110)에 유지되는 인증 폐기 목록으로, 인증 폐기 목록에 대한 체크가 지역 도메인 관리 장치(110)에서 처리되는 경우에 사용된다. 전역 인증 폐기 목록은 권리 발급 서버(150)에 유지되는 인증 폐기 목록으로, 인증 폐기 목록에 대한 체크가 권리 발급 서버(150)에서 처리되는 경우에 사용된다. 상기 인증 폐기 목록 중 하나만 가지거나 또는 둘 모두를 유지할 수도 있다. 둘 모두를 유지하는 경우, 권리 발급 서버(150)는 자신의 전역 인증 폐기 목록을 갱신한 후, 지역 도메인 관리 장치(110)에게 인증 폐기 목록의 갱신 정보를 전송하여, 지역 도메인 관리 장치(110)가 지역 인증 폐기 목록을 갱신하도록 할 수 있다.

[0036] 이하에서, 지역 도메인 관리 장치는 지역 도메인 관리 모듈을 포함하고 있는 장치이며, 이하에서 설명되는 지역 도메인 관리 장치의 도메인 관리 동작들은 지역 도메인 관리 모듈에서 수행된다.

[0037] 도 2는 본 발명의 일례에 따라 도메인을 생성(domain creation)하는 방법을 도시한 흐름도이다.

[0038] 사용자는 LDA 모듈을 가진 지역 도메인 관리 장치(201)를 사용하여 새로운 도메인을 생성할 수 있다. 새로운 도메인의 생성을 위하여 지역 도메인 관리 장치(201)는 사용자로부터 생성할 도메인의 도메인 정보(domain information)을 수신한다(단계 211). 상기 도메인 정보는 도메인 이름(domain name)을 포함한다. 또한, 상기 도메인 정보는 도메인 설명(domain description)과 상기 도메인과 관련한 다른 정보들을 포함할 수 있다. 사용자는 자신의 지역 도메인 관리 장치(201)의 입력 수단을 이용하여 도메인 정보를 지역 도메인 관리 장치(201)에 입력한다.

[0039] 단계 212에서, 지역 도메인 관리 장치(201)는 자신의 장치 식별자(device ID) 및 상기 도메인 정보를 권리 발급자 서버(202)에게 송신한다. 본 발명의 일 실시예에 따르면, 지역 도메인 관리 장치(201)는 자신의 장치 공용키 인증서(device public key certificate) 및 도메인 정책(domain policy)을 상기 권리 발급자 서버(202)에게 송신한다(단계 202). 상기 도메인 정책은 사용자에 의하여 입력될 수 있다. 상기 도메인 정책은 상기 도메인에 포함될 수 있는 장치의 최대수에 관한 사용자의 의도를 반영할 수 있다. 예를 들어, 사용자는 하나의 도메인에 대한 장치의 수를 10개로 할 수 있다. 지역 도메인 관리 장치(201)는 후에 도메인을 관리할 때 상기 도메인 정책을 참고(consult)한다. 지역 도메인 관리 장치(201)의 장치 식별자 및 장치 공용키 인증서는 제조업자에 의하여 지역 도메인 관리 장치(201)의 생산 시 지역 도메인 관리 장치(201)에 저장될 수 있다.

[0040] 단계 213에서 권리 발급자 서버(202)는 지역 도메인 관리 장치(201)로부터 수신한 정보를 기초로 지역 도메인 관리 장치(201)를 인증(authenticate)한다. 권리 발급자 서버(202)는 도메인 관리 장치(201)로부터 수신한 상기 도메인 관리 장치(201)의 장치 식별자 및 상기 도메인 관리 장치의 상기 장치 공용키 인증서를 체크함으로써, 지역 도메인 관리 장치(201)를 인증할 수 있다.

[0041] 지역 도메인 관리 장치(201)에 대한 인증이 성공하였으면, 권리 발급자 서버(202)는 지역 도메인 관리 장치(201)에 대하여 LDA 식별자(LDA ID)를 부여(assign)한다(단계 214).

[0042] 단계 215에서 권리 발급자 서버(202)는 지역 도메인 관리 장치(201)에게 상기 도메인의 도메인 개인키(domain private key), LDA 공용키/개인키 쌍(LDA public/private key pair), LDA 공용키 인증서(LDA public key certificate), 및 도메인 크리덴셜(domain credential)을 송신한다. 상기 도메인 개인키는 후에 도메인 관련 인증에 사용된다. 상기 LDA 공용키 인증서는 권리 발급 서버(202)에 의하여 서명되거나(signed) 또는 상기 권리 발급 서버(202)에 의하여 인증된(trusted) 제3의 장치에 의하여 서명된 것일 수 있다. 상기 도메인 크리덴셜은 도메인 공용키(domain public key), 상기 도메인 개인키(domain private key), 및 도메인 공용키 인증서(domain public key certificate)을 포함한다. 본 발명의 일 실시예에 따르면, 권리 발급자 서버(202)는 상기의 정보들 모두를 송신하는 대신 상기의 정보들 중 일부만 지역 도메인 관리 장치(201)에 송신할 수 있다. 상기 도메인 크리덴셜을 안전하게 전송하기 위하여, 권리 발급 서버(202)는 지역 도메인 관리 장치(201)의 장치 공용키(device public key)를 사용하여 도메인 개인키(domain private key)를 암호화(encrypt)할 수 있다. 도메인 크리덴셜의 안전한 전송을 위하여 다른 방법들이 사용될 수도 있다. 예를 들어, 권리 발급 서버(202)와 지역 도메인 관리 장치(201)는 키 설정 프로토콜(key establishing protocol)을 수행하고, 공통키(common key)를 설정할 수 있다. 그리고, 상기 공통키를 이용하여 도메인 크리덴셜의 암호화(encryption) 및 해독(decryption)을 수행할 수 있다. 지역 도메인 관리 장치(201)는 도메인 크리덴셜을 수신하고, 도메인 크리덴셜을 해독한다. 그리고, 지역 도메인 관리 장치(201)는 안전한 방법으로 도메인 개인키(domain private key)를 저장한다. 예를 들어, EEPROM에 저장할 수 있다.

[0043] 지역 도메인 관리 모듈을 가지고 있는 장치가 도메인 크리덴셜을 수신하게 되면, 상기 장치는 생성된 도메인을 관리할 수 있게 된다. 즉, 상기 장치는 도메인에 장치를 추가하거나 삭제할 수 있다.

[0044] 도 3은 본 발명의 일례에 따라 장치를 도메인에 추가(addition)하는 방법을 도시한 흐름도이다.

[0045] 도메인에 장치를 추가하기 위하여, 사용자는 지역 도메인 관리 장치(301)를 사용하여 지역 도메인 관리 장치(301)와 제한된 거리 내에 위치한 장치들을 탐색(discover)한다. 사용자가 지역 도메인 관리 장치(301)에서 탐색을 명령하면, 지역 도메인 관리 장치(301)는 자신의 LLC 인터페이스를 이용하여 거리 제한 통신으로 자신으로부터 제한된 거리에 있는 장치들에게 장치 식별자(device ID) 및 장치 공용키 인증서(device public key certificate)을 송신할 것을 요청한다. 상기 요청을 수신한 장치들은 지역 도메인 관리 장치(301)에게 자신의

장치 식별자 및 장치 공용키 인증서를 거리 제한 통신 채널 인터페이스(location limited channel interface)을 이용하여 송신한다. 즉, 단계(310)에서 지역 도메인 관리 장치(301)는 상기 지역 도메인 관리 장치로부터 제한된 거리 내에 위치한 장치들(302)의 정보를 거리 제한 통신 채널 인터페이스(LLC interface: location limited channel interface)를 통하여 수신한다.

[0046] 지역 도메인 관리 장치(301)는 이렇게 탐색된 장치들에 대한 정보를 사용자에게 제공하고, 사용자로부터 상기 도메인의 구성원으로 등록할 장치에 대한 선택을 입력 받는다(단계 311). 예를 들어, 지역 도메인 관리 장치(301)가 탐색된 장치들의 정보를 자신의 디스플레이에 표시하면, 사용자는 표시된 장치들 중 하나의 장치를 선택하여 클릭함으로써 상기 장치를 도메인에 추가할 것을 명령할 수 있다. 이러한 "포인트 앤 클릭(point and click)" 방식은 사용자에게 매우 친숙한 환경을 제공하게 된다. 그러면, 지역 도메인 관리 장치(301)는 단계(312) 내지 단계(319)에서 상기 탐색된 장치들 중 도메인의 구성원으로 선택된 장치를 인증(authenticate)한다. 인증의 방법은 권리 발급 서버(303)로부터 지역 도메인 관리 장치(301)에게 얼마나 많은 권한이 위임(delegate)되었는지에 따라 다르게 된다.

[0047] 만약 권리 발급 서버(303)가 지역 도메인 관리 장치(301)에게 새로운 장치의 인증에 대하여 모든 권리를 위임하였다면, 지역 도메인 관리 장치(301)는 선택된 장치의 장치 공용키 인증서(device public key certificate)을 체크한다(단계 312). 상기 장치 공용키 인증서가 유효하지 않으면, 인증은 실패한다. 또한, 지역 도메인 관리 장치(301)는 지역 인증 폐기 목록(local device revocation list)를 체크한다(단계 313). 만약 선택된 장치가 지역 인증 폐기 목록에 등록되어 있으면, 인증은 실패한다. 지역 도메인 관리 장치(301)는 추가적으로 선택된 장치의 장치 식별자를 체크할 수도 있다. 인증이 실패하면, 지역 도메인 관리 장치(301)는 이 장치가 도메인에 추가될 수 없음을 사용자에게 통지한다. 또한, 상기 선택된 장치의 인증이 실패하면 상기 선택된 장치를 상기 지역 인증 폐기 목록에 등록한다.

[0048] 만약 권리 발급 서버(303)가 지역 도메인 관리 장치(301)에게 새로운 장치의 인증에 대하여 부분적 권리(partial rights)를 위임하였다면, 지역 도메인 관리 장치(301)는 권리 발급자 서버(303)에게 사용자에 의해 선택된 장치의 장치 공용키 인증서(device public key certificate)을 송신한다(단계 316). 권리 발급 서버(303)는 수신한 장치 공용키 인증서를 체크하고(단계 317), 상기 선택된 장치가 전역 인증 폐기 목록(global device revocation list)에 등록되어 있는지 체크한다(단계 318). 권리 발급 서버(303)는 추가적으로 선택된 장치의 장치 식별자를 체크할 수도 있다.

[0049] 인증이 성공하면, 권리 발급자 서버(303)는 상기 선택된 장치에 대하여 도메인 내 장치 식별자(domain-based device ID)를 부여(assign)한다. 그리고, 권리 발급자 서버(303)는 상기 도메인 내 장치 식별자와 함께 지역 도메인 관리 장치(301)에 송신한다(단계 319).

[0050] 인증이 실패하면, 권리 발급자 서버(303)는 상기 선택된 장치를 도메인에 추가하는 것에 관하여 거부 결정(negative decision)을 내렸음을 지역 도메인 관리 장치(301)에게 전달한다(단계 319). 또한, 상기 선택된 장치의 인증이 실패하면, 권리 발급자 서버(303)는 상기 선택된 장치를 상기 전역 인증 폐기 목록에 등록하고, 지역 도메인 관리 장치(301)에게 지역 인증 폐기 목록의 갱신을 요청한다. 그러면, 지역 도메인 관리 장치(301)는 자신의 지역 인증 폐기 목록을 갱신한다(단계 314).

[0051] 도메인에 추가될 장치에 대한 인증이 성공하면, 지역 도메인 관리 장치(301)는 상기 장치에 대해 도메인 내 장치 식별자(domain-based device ID)를 할당한다(단계 315). 대안적으로, 도메인 내 장치 식별자는 권리 발급자 서버(303)에서 생성될 수 있다. 이 경우 지역 도메인 관리 장치(301)는 권리 발급자 서버(303)로부터 도메인 내 장치 식별자를 수신(단계 319 참조)하기 때문에, 지역 도메인 관리 장치(301)가 별도로 도메인 내 장치 식별자(domain-based device ID)를 할당할 필요는 없다. 도메인 내 장치 식별자는 해당 도메인 내에서 도메인에 속한 장치들을 열거(enumeration)하는데 사용된다.

[0052] 단계(315)에서 지역 도메인 관리 장치(301)는 도메인 정책을 체크한다. 예를 들어, 도메인 정책에 따르면, 해당 도메인에 조인 가능한 장치의 최대수가 10개인데, 이미 10개의 장치가 조인되어 있는 경우에는, 새로운 장치의 추가는 거부된다.

[0053] 도메인 정책의 체크가 성공하면, 지역 도메인 관리 장치(301)는 도메인에 추가할 장치(302)의 장치 공용키를 이용하여 도메인 개인키를 암호화한다(단계 321).

[0054] 또한, 지역 도메인 관리 장치(301)는 (1) 장치(302)에게 할당된(assigned) 도메인 내 장치 식별자(domain-based device ID), (2) 권리 발급자 서버가 상기 지역 도메인 관리 장치에게 할당한 LDA 식별자(LDA ID), 및

(3) 상기 인증된 장치의 장치 공용키 인증서(device public key certificate)의 해쉬값의 3개 값((1)-(3))을 상기 지역 도메인 관리 장치의 LDA 개인키(LDA public key)로 서명(sign)한다. 상기 도메인 내 장치 식별자(domain-based device ID)는 지역 도메인 관리 장치(301) 또는 권리 발급자 서버(303)에 의하여 할당(assign)된다.

[0055] 단계(322)에서 지역 도메인 관리 장치(301)는 상기 인증된 장치(302)에게 상기 도메인에 대응한 장치 인증 정보(device authentication information)를 송신한다. 장치 인증 정보는 해당 도메인과 관련하여 장치(302)가 이미 인증되었음을 증명하는 정보가 된다. 상기 장치 인증 정보는 다음과 같은 정보를 포함할 수 있다.

[0056] (1) 상기 지역 도메인 관리 장치(301)의 LDA 공용키(LDA public key)

[0057] (2) 상기 장치(302)에 대한 도메인 내 장치 식별자(domain-based device ID);

[0058] (3) 상기 지역 도메인 관리 장치(301)의 LDA 식별자(LDA ID) - LDA ID는 권리 발급자 서버(303)에 의하여 부여(assign)됨

[0059] (4) 아래의 3 값을 지역 도메인 관리 장치(301)의 LDA 개인키(LDA public key)로 서명한 서명(signature)

[0060] 1) 상기 장치(302)에게 할당된(assigned) 도메인 내 장치 식별자(domain-based device ID)

[0061] 2) 권리 발급자 서버(303)가 상기 지역 도메인 관리 장치(301)에게 할당한 LDA 식별자(LDA ID), 및

[0062] 3) 상기 인증된 장치(302)의 장치 공용키 인증서(device public key certificate)의 해쉬값

[0063] 또한, 지역 도메인 관리 장치(301)는 상기 인증된 장치(302)에게 상기 도메인에 대응한 도메인 크리덴셜(domain credential)을 송신한다. 상기 도메인 크리덴셜은 (1) 상기 도메인에 대한 도메인 정보(domain credential), (2) 상기 도메인의 도메인 개인키를 상기 인증된 장치의 공용키로 암호화한 암호화된 값(encrypted key), 및 (3) 상기 도메인의 도메인 공용키 인증서(domain public key certificate) 중 일부 또는 전부를 포함할 수 있다. 상기 도메인 정보는 도메인 이름, 도메인 식별자 등과 같은 도메인에 관한 정보를 포함한다. 도메인 크리덴셜은, 상기 장치가 해당 도메인에 속한 콘텐츠를 접근할 때, 상기 장치가 접근 권한이 있는지를 나타내게 된다. 예를 들어, 상기 장치가 해당 도메인에 속한 콘텐츠를 접근할 때 상기 도메인 크리덴셜을 상기 콘텐츠를 관리하고 있는 장치에게 제시함으로써, 상기 콘텐츠를 접근할 수 있게 된다.

[0064] 모든 정보를 장치(302)에 송신한 후, 단계(323)에서 지역 도메인 관리 장치(301)는 상기 인증된 장치(302)를 상기 도메인의 구성원(member)으로 등록한다. 보다 구체적으로, 지역 도메인 관리 장치(301)는 상기 장치(302)를 상기 지역 도메인 관리 장치(301)에 유지되는 도메인 구성원 리스트(domain member list)에 등록한다. 도메인 구성원 리스트는 상기 도메인의 구성원의 장치 식별자 및 장치 인증 정보(device authentication information)를 저장한다.

[0065] 장치(302)를 도메인의 구성원으로 등록한 후, 선택적으로, 지역 도메인 관리 장치(301)는 상기 장치(301)에게 할당된(assigned) 도메인 내 장치 식별자, 및 상기 장치(301)의 장치 공용키 인증서를 권리 발급자 서버(303)에게 통지할 수 있다.

[0066] 도 4는 본 발명의 일례에 따라 장치를 도메인으로부터 삭제(delete)하는 방법을 도시한 흐름도이다.

[0067] 만약 사용자가 도메인으로부터 하나의 장치(402)를 삭제하기를 원하는 경우, 사용자는 상기 도메인을 관리하고 있는 지역 도메인 관리 장치(401)를 사용하여 삭제할 도메인 구성원을 선택한다(단계 411).

[0068] 상기 장치(402)를 상기 도메인의 구성원으로부터 삭제하라는 요청을 수신하면, 지역 도메인 관리 장치(401)는 상기 선택된 장치(402)를 상기 도메인의 도메인 구성원으로부터 제거한다(단계 412). 보다 구체적으로, 지역 도메인 관리 장치(401)는 도메인 구성원 리스트에 저장된 상기 장치(402)의 장치 식별자 및 장치 인증 정보를 삭제한다.

[0069] 단계(413)에서, 지역 도메인 관리 장치(401)는 장치(402)에게 상기 도메인에 대응한 장치 인증 정보의 삭제 요청을 송신한다. 추가로 지역 도메인 관리 장치(401)는 장치(402)에게 해당 도메인에 관한 정보들의 삭제를 요청할 수 있다. 예를 들어, 지역 도메인 관리 장치(401)는 도메인 정보, 도메인 공용키/개인키 쌍, 및 도메인

공용키 인증서의 삭제를 장치(402)에게 요청할 수 있다.

[0070] 선택적으로, 지역 도메인 관리 장치(401)는 권리 발급 서버(403)에게 특정한 장치 식별자를 가진 장치(402)가 특정 도메인에서 삭제되었음을 통지할 수 있다(단계 415).

[0071] 도 5는 본 발명의 일례에 따라 도메인을 삭제(delete)하는 방법을 도시한 흐름도이다.

[0072] 도메인을 삭제하기 위하여, 사용자는 지역 도메인 관리 장치(501)에 의하여 유지되고 있는 도메인의 리스트로부터 삭제할 도메인을 선택한다(단계 511). 그러면, 지역 도메인 관리 장치(501)는 선택된 도메인의 구성원 장치들을 모두 삭제한다(단계 512). 상기 선택된 도메인의 구성원 장치들을 삭제하는 것은 도 4에 설명된 방법을 사용한다. 이 과정에는 지역 도메인 관리 장치(501), 사용자 장치(502) 또는 권리 발급자 서버(503)가 관여될 수 있다. 도메인으로부터 모든 장치를 삭제한 후, 지역 도메인 관리 장치(501)는 자신에게 저장되어 있는 도메인 정보 및 도메인 크리덴셜을 삭제한다(단계 513). 선택적으로, 지역 도메인 관리 장치(501)는 권리 발급 서버(503)에게 삭제된 장치들의 리스트 및 삭제된 도메인에 관한 정보를 통지할 수 있다(단계 514). 삭제된 장치들의 리스트로는 삭제된 장치들의 장치 식별자의 리스트가 사용될 수 있다. 삭제된 도메인에 관한 정보로는 도메인 이름 또는 도메인 식별자가 사용될 수 있다.

[0073] 또한 본 발명의 실시예들은 다양한 컴퓨터로 구현되는 동작을 수행하기 위한 프로그램 명령을 포함하는 컴퓨터 판독 가능 매체를 포함한다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 매체는 프로그램 명령, 데이터 구조 등을 지정하는 신호를 전송하는 반송파를 포함하는 광 또는 금속선, 도파관 등의 전송 매체일 수도 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0074] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다. 예를 들어, 본 발명에서 지역 도메인 관리 장치와 사용자 장치는 거리 제한 통신 채널을 이용하여 통신하는 것으로 설명되었으나, 본 발명의 특징을 포함하면서 다른 사용 가능한 통신 채널을 이용하는 것도 가능하다.

발명의 효과

[0075] 본 발명의 도메인 관리 방법 및 장치에 따르면, 장치들은 디지털 저작권 관리 시스템의 도메인 기능을 이용하기 위하여 네트워크 접속 능력을 포함하지 않아도 된다. 장치들은 단지 거리 제한 통신 채널만 구비하고 있으면, 본 발명에 따른 디지털 저작권 관리 시스템의 도메인 기능을 이용할 수 있게 된다. 따라서, 디지털 콘텐츠에 대한 접근이 필요한 많은 장치들에 대하여 비용이 비싼 네트워크 인터페이스 대신 저렴한 거리 제한 통신 채널만 구현하면 되므로, 장치의 생산 비용이 절감된다.

[0076] 본 발명은 제한된 자원을 가진 장치에게 유용하다. 본 발명은 장치들에 대하여 도메인에 등록하기 위하여 인터넷 접속 기능을 사용할 것을 요구하지 않는다. 단지 거리 제한 통신 채널 인터페이스만을 요구할 뿐이다.

[0077] 또한, 본 발명에 따르면, 장치를 도메인에 등록할 때 매우 빠르게 처리된다. 지역 도메인 관리 장치가 장치의 인증에 관한 모든 권리를 가지고 있다면, 장치 인증에 관한 모든 절차는 지역적으로 수행되므로, 빠르게 처리된다. 상기 인증된 장치들에게는 인증 정보가 제공되므로, 후에 상기 장치들과 도메인의 다른 구성원들 간의 통신도 쉽게 인증된다.

[0078] 특히, 사용자들은 지역 도메인 관리 장치에 표시되는 탐색된 장치들 중 도메인에 추가할 장치를 "포인트 앤 클릭(point and click)" 방식으로 선택할 수 있기 때문에, 장치를 도메인에 추가하는 방법이 매우 사용자에게 친숙하게 된다.

[0079] 또한, 종래에는 도메인의 생성 시에 상기 도메인에 추가될 장치들이 결정되어야 했지만, 본 발명에 따르면 구성

원 장치가 하나도 없는 상태에서도 도메인의 생성이 가능하며, 도메인의 추가 및 삭제가 지역적으로 수행됨으로써, 도메인 관리가 매우 유연하게 수행된다.

도면의 간단한 설명

[0001] 도 1은 본 발명의 일례에 따라 지역 도메인 관리 장치로 선택된 사용자 장치 및 권리 발급자 서버의 연결을 도시한 도면이다.

[0002] 도 2는 본 발명의 일례에 따라 도메인을 생성(domain creation)하는 방법을 도시한 흐름도이다.

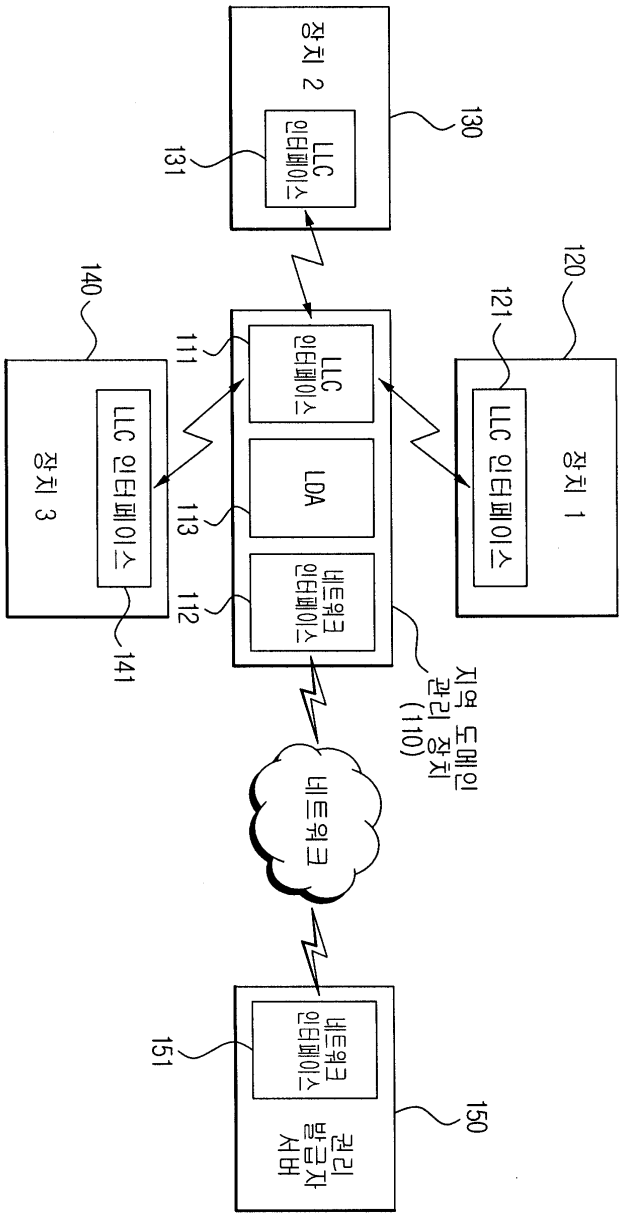
[0003] 도 3은 본 발명의 일례에 따라 장치를 도메인에 추가(addition)하는 방법을 도시한 흐름도이다.

[0004] 도 4는 본 발명의 일례에 따라 장치를 도메인으로부터 삭제(delete)하는 방법을 도시한 흐름도이다.

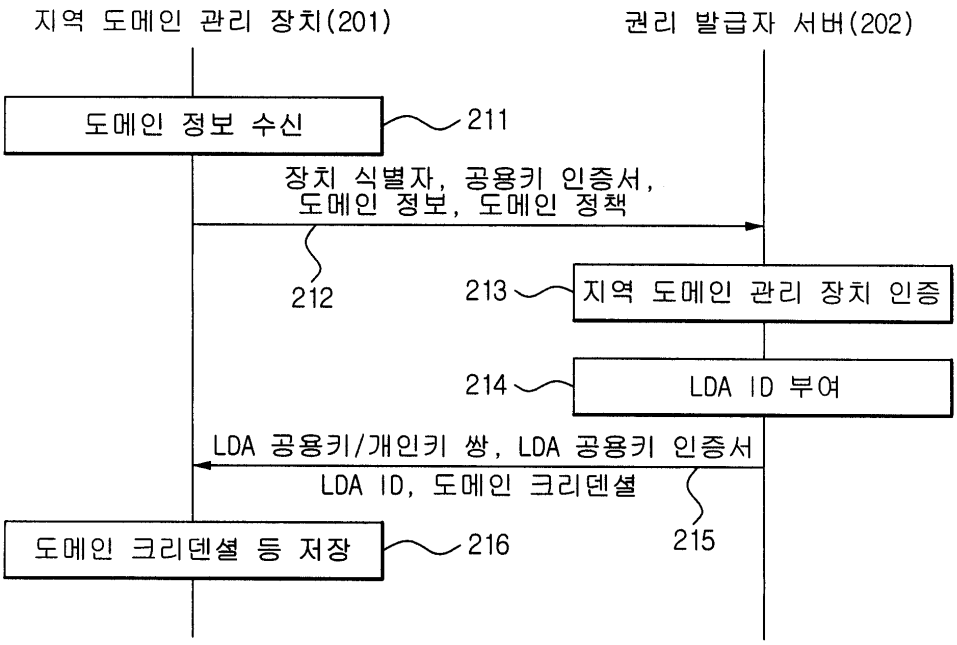
[0005] 도 5는 본 발명의 일례에 따라 도메인을 삭제(delete)하는 방법을 도시한 흐름도이다.

도면

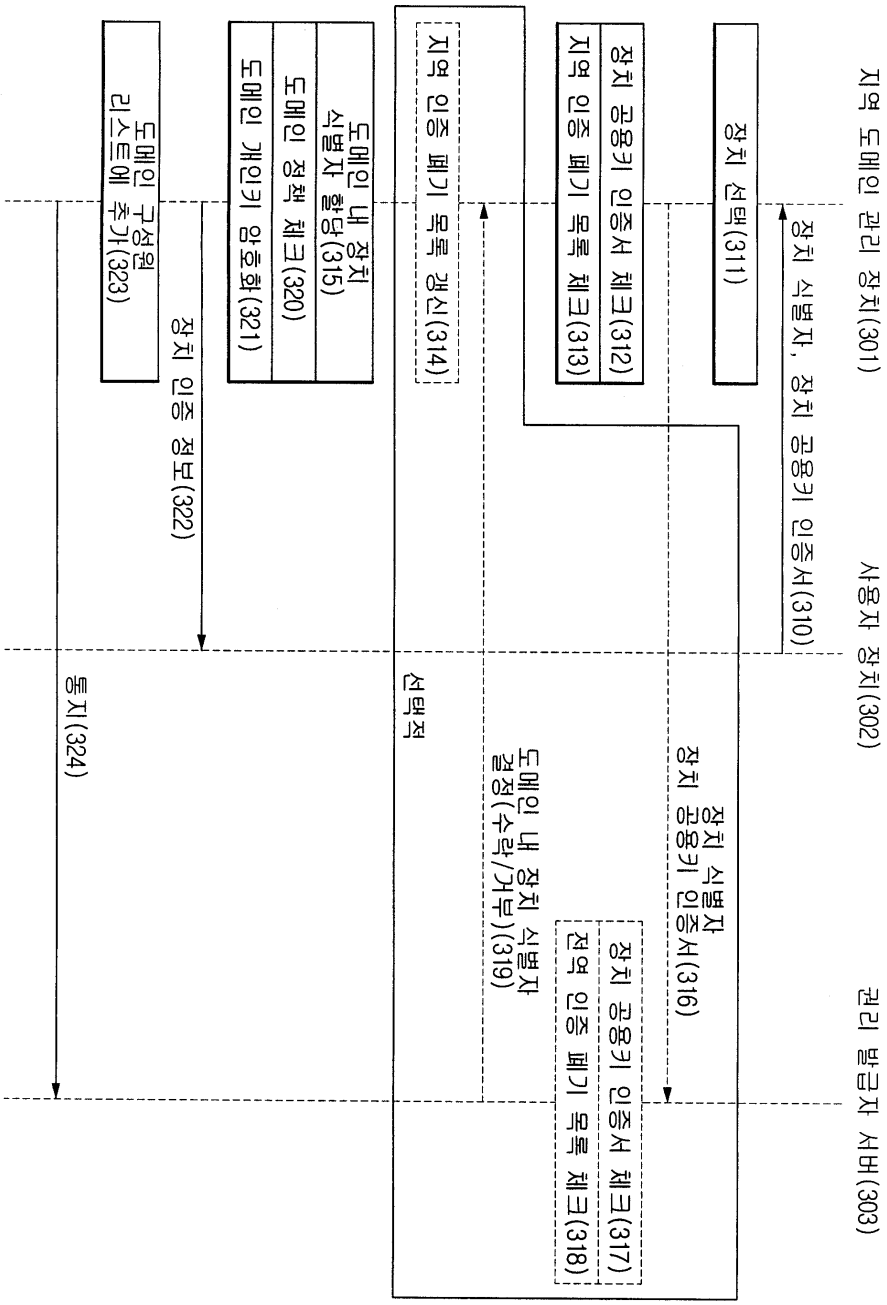
도면1



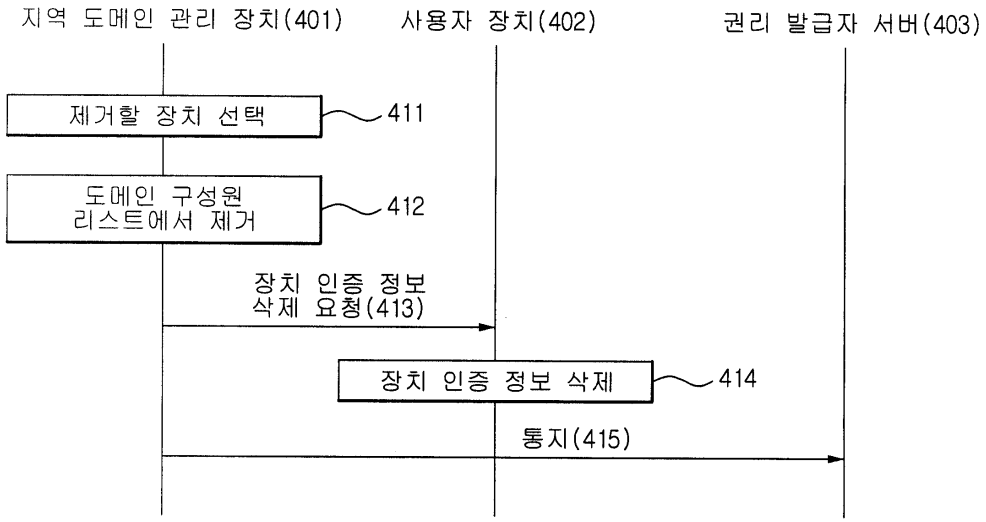
도면2


지역 도메인 관리 장치(201)
권리 발급자 서버(202)
도메인 정보 수신
211
장치 식별자, 공용키 인증서,
도메인 정보, 도메인 정책
212
213
지역 도메인 관리 장치 인증
214
LDA ID 부여
LDA 공용키/개인키 쌍, LDA 공용키 인증서
LDA ID, 도메인 크리덴셜
215
도메인 크리덴셜 등 저장
216

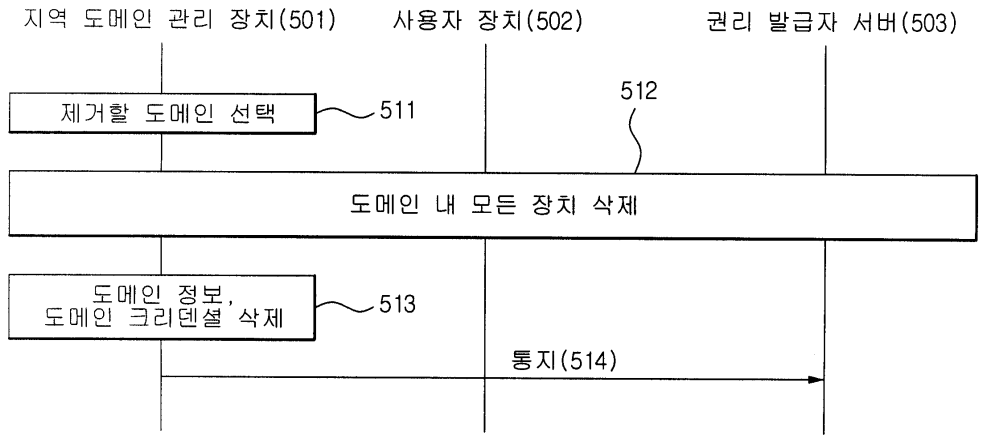
도면3


지역 도메인 관리 장치(301)
사용자 장치(302)
권리 발급자 서버(303)
장치 선택(311)
장치 식별자, 장치 공용키 인증서(310)
장치 공용키 인증서 체크(312)
지역 인증 폐기 목록 체크(313)
지역 인증 폐기 목록 갱신(314)
도메인 내 장치 식별자 할당(315)
도메인 정책 체크(320)
도메인 개인키 암호화(321)
장치 인증 정보(322)
도메인 구성원 리스트에 추가(323)
통지(324)
장치 식별자 장치 공용키 인증서(316)
장치 공용키 인증서 체크(317)
전역 인증 폐기 목록 체크(318)
도메인 내 장치 식별자 결정(수락/거부)(319)
선택적

도면4


지역 도메인 관리 장치(401)
사용자 장치(402)
권리 발급자 서버(403)
제거할 장치 선택
411
도메인 구성원 리스트에서 제거
412
장치 인증 정보 삭제 요청(413)
장치 인증 정보 삭제
414
통지(415)

도면5


지역 도메인 관리 장치(501)
사용자 장치(502)
권리 발급자 서버(503)
제거할 도메인 선택
511
512
도메인 내 모든 장치 삭제
도메인 정보, 도메인 크리덴셜 삭제
513
통지(514)