(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년01월03일
(11) 등록번호 10-1346734
(24) 등록일자 2013년12월24일

(51) 국제특허분류(Int. Cl.)
G06F 15/00 (2006.01)
(21) 출원번호 10-2007-0010277
(22) 출원일자 2007년01월31일
심사청구일자 2012년01월05일
(65) 공개번호 10-2007-0109797
(43) 공개일자 2007년11월15일
(30) 우선권주장
60/799,652 2006년05월12일 미국(US)
(56) 선행기술조사문헌
JP2005045641 A*
KR1020050094316 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
김여진
경기도 수원시 팔달구 인계로166번길 48-21, 샤르망 오피스텔 507호 (인계동)
오윤상
서울특별시 강남구 언주로 123, 개포한신아파트 8동 703호 (도곡동)
(뒷면에 계속)
(74) 대리인
특허법인가산

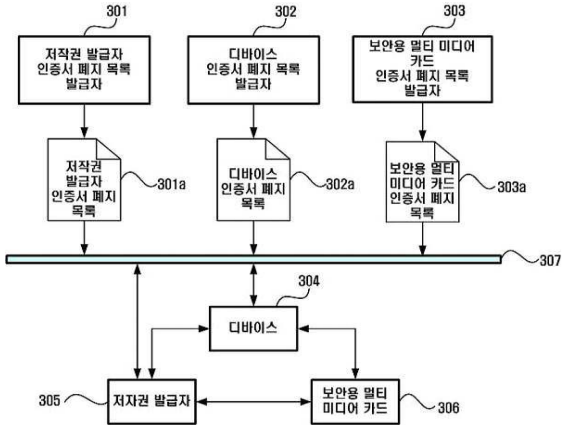
전체 청구항 수 : 총 8 항 심사관 : 이석형

(54) 발명의 명칭 **디지털 저작권 관리를 위한 다중 인증서 철회 목록 지원방법 및 장치**

(57) 요 약

디지털 저작권 관리(Digital Rights Management, 이하 DRM이라 칭함)를 위한 다중 인증서 철회 목록(Certificate Revocation List, 이하 CRL이라 칭함) 지원 방법 및 장치가 제공된다. DRM을 위한 다중 CRL 지원 방법은 제 1 CRL을 수신하고 상기 수신한 제 1 CRL의 발급자 식별 정보를 확인하는 확인 단계, 상기 확인된 발급자 식별 정보에 대응하는 제 2 CRL을 로딩하여 상기 제 1 CRL과 최신 여부를 비교하는 비교 단계 및 상기 비교 결과에 따라 상기 제 1 CRL 및 상기 제 2 CRL 중 어느 하나를 최신의 CRL로 갱신하는 갱신 단계를 포함한다.

대 표 도 - 도3



(72) 발명자

심상규

경기도 수원시 영통구 매영로247번길 15, 103동 202호 (원천동, 호산빌리지)

정경임

경기도 성남시 분당구 내정로 186, 롯데아파트 128동903호 (수내동, 파크타운)

김지수

경기도 용인시 수지구 수지로78번길 18 (상현동, 풍산아파트) 102동 701호

특허청구의 범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

인증서 철회 목록의 발급자 식별 정보를 포함한 제 1 인증서 철회 목록을 발신하는 발신 단계;

상기 발신된 제 1 인증서 철회 목록의 최신 여부에 따라 상기 제 1 인증서 철회 목록의 갱신 완료 및 갱신 요청 중 어느 하나에 대한 응답을 수신하는 수신 단계; 및

상기 수신한 응답에 따라 제 1 인증서 철회 목록의 갱신 여부를 결정하는 갱신 단계를 포함하고,

상기 갱신 요청에 대한 응답을 수신하는 경우 상기 제 1 인증서 철회 목록의 갱신 기준이 되는 최신의 인증서 철회 목록을 수신하는 디지털 저작권 관리를 위한 다중 인증서 철회 목록 지원 방법.

청구항 9

제 8항에 있어서,

상기 발신 단계는 장치간 상호 인증 수행 시 실행되는 디지털 저작권 관리를 위한 다중 인증서 철회 목록 지원 방법.

청구항 10

제 8항에 있어서,

상기 발신 단계는 상기 제 1 인증서 철회 목록의 갱신을 위한 임계값에 도달했을 때 실행되는 디지털 저작권 관리를 위한 다중 인증서 철회 목록 지원 방법.

청구항 11

제 10항에 있어서,

상기 임계값은 상기 식별 정보를 갖는 발급자 별로 설정 가능한 디지털 저작권 관리를 위한 다중 인증서 철회 목록 지원 방법.

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

인증서 철회 목록의 발급자 식별 정보를 포함한 제 1 인증서 철회 목록을 발신하는 발신부;

상기 발신된 제 1 인증서 철회 목록의 최신 여부에 따라 상기 제 1 인증서 철회 목록의 갱신 완료 및 갱신 요청 중 어느 하나에 대한 응답을 수신하는 수신부; 및

상기 수신한 응답에 따라 제 1 인증서 철회 목록의 갱신 여부를 결정하는 갱신 판단부를 포함하고,

상기 수신부는 상기 갱신 요청에 대한 응답을 수신하는 경우 상기 제 1 인증서 철회 목록의 갱신 기준이 되는 최신의 인증서 철회 목록을 수신하는 디지털 저작권 관리를 위한 다중 인증서 철회 목록 지원 장치.

청구항 21

제 20항에 있어서,

상기 발신부는 장치간 상호 인증 수행 시 상기 제 1 인증서 철회 목록을 발신하는 디지털 저작권 관리를 위한 다중 인증서 철회 목록 지원 장치.

청구항 22

제 20항에 있어서,

상기 발신부는 상기 제 1 인증서 철회 목록의 갱신을 위한 임계값에 도달했을 때 실행되는 디지털 저작권 관리를 위한 다중 인증서 철회 목록 지원 장치.

청구항 23

제 22항에 있어서,

상기 임계값은 상기 식별 정보를 갖는 발급자 별로 설정 가능한 디지털 저작권 관리를 위한 다중 인증서 철회 목록 지원 장치.

청구항 24

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0016] 본 발명은 DRM을 위한 다중 CRL 지원 방법 및 장치에 관한 것으로서, 더욱 상세하게는 서로 다른 CRL 발급자로부터 발급된 CRL을 구분하고 관리함으로써 여러 DRM 장치들 간의 신뢰를 보장하는 DRM을 위한 다중 CRL 지원 방법 및 장치에 관한 것이다.

[0017] 최근에 디지털 DRM에 관한 연구가 활발하며, DRM을 적용한 상용 서비스들이 도입되었거나 도입중에 있다.

[0018] 아날로그 데이터와는 달리 디지털 데이터는 손실이 없이 복제가 가능하며, 재사용 및 가공이 용이하고, 제3자에게 쉽게 배포될 수 있다는 특성을 가지고 있다.

[0019] 또한 이러한 디지털 데이터의 복제와 배포는 매우 적은 비용으로도 가능하다. 이에 비해 디지털 컨텐츠를 제작하기 위해서는 많은 비용, 노력 및 시간이 필요하므로, 각종 디지털 저작권의 보호를 위한 기술이 요구되고 있으며 이를 위해 DRM의 적용범위가 점차 확대되어가고 있다.

[0020] 디지털 컨텐츠를 보호하고자 하는 노력은 과거에도 있었으나, 이는 주로 디지털 컨텐츠에 대한 무단 접근 방지에 중점을 두고 있었다.

[0021] 따라서 디지털 컨텐츠에 대한 접근(access)은 대가를 지불한 일부 사람에게만 허용되도록 하였으며, 대가를 지불하지 않은 사람은 디지털 컨텐츠에 접근할 수 없었다.

[0022] 그러나 대가를 지불하여 디지털 컨텐츠에 접근한 사람이 이를 고의적으로 제3자에게 배포할 경우에 제3자는 대가를 지불하지 않고도 디지털 컨텐츠를 사용할 수 있게 되어 많은 문제점이 야기되었다.

[0023] 이에 비해 DRM은 디지털 컨텐츠에 대한 접근은 누구에게나 무제한으로 허용하고 있으나, 디지털 컨텐츠를 암호화하여 이를 실행시키려면 특정 라이센스를 필요하도록 하고 있다. 따라서, DRM을 적용하면 디지털 컨텐츠를 보다 효과적으로 보호할 수 있게 된다.

[0024] 도 1은 일반적인 DRM의 개념을 나타낸 도면이다.

[0025] DRM의 주된 내용은 암호화 또는 스크램블과 같은 방식으로 보호된 컨텐츠(이하에서는 암호화된 컨텐츠로 언급한다)와 암호화된 컨텐츠에 접근할 수 있도록 하는 라이센스의 취급에 관한 것이다.

[0026] 도 1에는 암호화된 컨텐츠에 접근하기를 원하는 디바이스들(110, 150)과, 컨텐츠를 공급하는 컨텐츠 공급자(Contents Issuer)(120)와, 컨텐츠를 실행시킬수 있는 라이센스를 포함하고 있는 권리객체(Rights Object; RO)를 발행하는 권리객체 발행기관(Rights Issuer; RI)(130), 및 인증서를 발행하는 인증기관(140)이 도시되어 있다.

[0027] 디바이스A(110)는 원하는 컨텐츠를 컨텐츠 공급자(120)로부터 얻을 수 있는데, 이 컨텐츠는 암호화된 컨텐츠다.

[0028] 디바이스A(110)는 암호화된 컨텐츠를 사용할 수 있는 라이센스가 포함된 권리객체를 권리객체 발행기관(130)으로부터 구입할 수 있으며, 권리객체를 구입한 디바이스A(110)는 암호화된 컨텐츠를 사용할 수 있게 된다.

[0029] 암호화된 컨텐츠는 자유롭게 유통되거나 배포될 수 있기 때문에, 디바이스A(110)는 디바이스B(150)에게 암호화된 컨텐츠를 자유롭게 전달할 수 있다.

[0030] 전달받은 암호화된 컨텐츠를 재생시키기 위해서는 디바이스B(150) 역시 권리객체가 필요하며, 이러한 권리객체는 권리객체 발행기관(130)으로부터 얻을 수 있다.

[0031] 한편, 인증기관(140)은 공개키가 확인된 디바이스의 이름, 인증서 일련번호, 인증서를 발행하는 인증기관의 명

칭, 해당 디바이스의 공개키 및 인증서 만료시기를 나타내는 메시지가 서명된 인증서(certificate)를 발행한다.

[0032] 각 디바이스들은 인증기관(140)에서 발행된 인증서를 통해 자신과 통신하는 디바이스가 정당한 디바이스인지 확인할 수 있다.

[0033] 각 인증서는 그 승인 여부를 확인하기 위하여 인증기관(140)의 비밀키에 의하여 서명되기 때문에, 디바이스는 인증기관(140)의 공개키를 사용하여 자신과 통신하는 다른 디바이스의 인증서를 확인할 수 있다.

[0034] 인증서는 디렉토리 서비스 시스템과 같이 각 디바이스들로부터 접근 용이한 장소에 저장되거나 각 디바이스 자체에 저장될 수도 있다.

[0035] 통신상의 보안성을 높이기 위하여, 모든 디바이스는 인증기관(140)으로부터 자신의 인증서를 발행 받을 필요가 있다.

[0036] 그러나, 인증기관(140)에서 발행된 인증서는 그 만료기간이 지나기 전에 폐지될 수도 있다.

[0037] 예를 들어, 특정 디바이스의 비밀키가 손상되거나 외부로 유출된 경우, 해당 디바이스의 인증서를 폐지함으로써 다른 디바이스가 이를 확인토록 할 수 있다.

[0038] 이처럼 유효기간이 만료되지 않은 인증서의 폐지 여부를 확인하기 위해서 다양한 방법이 제안되고 있는데, 그중 한가지 방법은 온라인 위치 상에 있는 모든 유효한 디바이스의 인증서를 접근이 용이한 디렉토리 서비스 시스템에 저장하고, 이를 일반적으로 이용할 수 있도록 하는 것이다.

[0039] 예컨대, 디바이스가 서버에 접속하고자 하는 경우에, 서버는 디렉토리 서비스 시스템에 접속하여 디바이스의 인증서가 있는지를 확인할 수 있다.

[0040] 만약 디바이스의 인증서가 디렉토리 서비스 시스템 내에 존재하지 않는 경우, 서버는 디바이스의 인증서가 폐지된 것으로 판단할 수 있다.

[0041] 인증서의 폐지 여부를 확인하는 다른 방법은, CRL, 즉 폐지된 인증서의 목록을 인증기관이 발행하는 것이다.

[0042] 이러한 CRL은 정기/비정기적으로 업데이트되어 새로이 발행되며 발행된 인증서 폐지 목록은 인증기관이 배포할 수 있다.

[0043] 각 디바이스는 자신과 통신하는 다른 디바이스의 인증서를 최근에 발행된 인증서 폐지 목록에서 검색하여, 해당 인증서가 인증서 폐지 목록에 포함되어 있지 않으면 해당 디바이스를 유효한 것으로 판단할 수 있다.

[0044] 만일, 상대 디바이스의 인증서가 인증서 폐지 목록에 포함되어 있는 경우에는, 상대 디바이스를 부당한 디바이스로 판단하여 상대 디바이스와의 통신을 중단시킬 수 있다.

[0045] 도 2는 종래 DRM 시스템 에서의 CRL 발급 및 갱신을 도시한 도면이다.

[0046] CRL 발급자(201)는 DRM 시스템을 구성하는 모든 장치(202~204)에 대한 인증서 철회 기록에 대해 CRL(201a)을 작성하여 네트워크(205)를 통해 배포하며, DRM 시스템의 구성 장치들(202~204)은 CRL 발급자(201) 또는 다른 장치(202~204)로부터 최신의 CRL을 받아 저장한다.

[0047] 각 장치들(202~204)은 다른 장치(202~204)와 통신할 때 상대 장치의 손상 여부를 파악하기 위해 CRL(201a)을 검사하며, 이때 두 장치에 저장된 CRL(201a)을 비교하여 발급시각이 동일하지 않다면 오래된 CRL을 최신의 CRL로 갱신한다.

[0048] 그러나 종래 기술의 경우, 두 개 이상의 다른 CRL 발급자가 발급한 CRL들이 하나의 장치에 저장될 경우 충돌이 발생할 수 있다.

[0049] 즉, CRL 검사 및 갱신 시 해당 장치는 어느 CRL을 로딩해야 하는지 알 수 없기 때문에 DRM의 종류, DRM 시스템 장치 및 CRL 발급자 등을 고려한 분산 CRL을 설계하기 어려운 문제점이 있다.

[0050] 또한, 하나의 CRL에 DRM 시스템을 구성하는 모든 장치에 대한 CRL을 기록하게 되므로 CRL의 크기가 증가하게 되어, 두 장치간 통신 시 상대 장치의 CRL을 검사할 때 다른 장치에 관한 불필요한 정보도 함께 교환해야 하는 등, CRL의 관리 효율이 낮아지는 문제점도 있다.

발명이 이루고자 하는 기술적 과제

[0051] 이에, 본 발명은 디지털 저작권 관리를 위한 다중 인증서 철회 목록 지원 방법 및 장치를 통해 서로 다른 CRL

발급자로부터 발급된 CRL을 구분하고 관리함으로써 여러 DRM 장치들 간의 신뢰를 보장하는 하는데 그 목적이 있다.

[0052] 본 발명의 목적들은 이상에서 언급한 목적들로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

발명의 구성 및 작용

[0053] 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 DRM을 위한 다중 CRL 지원 방법은 제 1 CRL을 수신하고 상기 수신한 제 1 CRL의 발급자 식별 정보를 확인하는 확인 단계, 상기 확인된 발급자 식별 정보에 대응하는 제 2 CRL을 로딩하여 상기 제 1 CRL과 최신 여부를 비교하는 비교 단계 및 상기 비교 결과에 따라 상기 제 1 CRL 및 상기 제 2 CRL 중 어느 하나를 최신의 CRL로 갱신하는 갱신 단계를 포함한다.

[0054] 상기 목적을 달성하기 위하여, 본 발명의 다른 실시예에 따른 DRM을 위한 다중 CRL 지원 방법은 인증서 철회 목록의 발급자 식별 정보를 포함한 제 1 인증서 철회 목록을 발신하는 발신 단계, 상기 발신된 제 1 인증서 철회 목록의 최신 여부에 따라 상기 제 1 인증서 철회 목록의 갱신 완료 및 갱신 요청 중 어느 하나에 대한 응답을 수신하는 수신 단계 및 상기 수신한 응답에 따라 제 1 인증서 철회 목록의 갱신 여부를 결정하는 갱신 단계를 포함한다.

[0055] 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 DRM을 위한 다중 CRL 지원 장치는 제 1 인증서 철회 목록을 수신하고 상기 수신한 제 1 인증서 철회 목록의 발급자 식별 정보를 확인하는 식별 정보 확인부, 상기 확인된 발급자 식별 정보에 대응하는 제 2 인증서 철회 목록을 로딩하여 상기 제 1 인증서 철회 목록과 최신 여부를 비교하는 갱신 판단부 및 상기 비교 결과에 따라 상기 제 1 인증서 철회 목록 및 상기 제 2 인증서 철회 목록 중 어느 하나를 최신의 인증서 철회 목록으로 갱신하는 갱신부를 포함한다.

[0056] 목적을 달성하기 위하여, 본 발명의 다른 실시예에 따른 DRM을 위한 다중 CRL 지원 장치는 인증서 철회 목록의 발급자 식별 정보를 포함한 제 1 인증서 철회 목록을 발신하는 발신부, 상기 발신된 제 1 인증서 철회 목록의 최신 여부에 따라 상기 제 1 인증서 철회 목록의 갱신 완료 및 갱신 요청 중 어느 하나에 대한 응답을 수신하는 수신부 및 상기 수신한 응답에 따라 제 1 인증서 철회 목록의 갱신 여부를 결정하는 갱신 판단부를 포함한다.

[0057] 기타 실시예들의 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

[0058] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는

[0059] 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다.

[0060] 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.

[0061] 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0062] 이하, 본 발명의 실시예들에 의한 디지털 저작권 관리를 위한 다중 인증서 철회 목록 지원 방법 및 장치를 설명하기 위한 구성도 또는 처리 흐름도에 대한 도면들을 참고하여 본 발명에 대해 설명하도록 한다.

[0063] 이때, 처리 흐름도 도면들의 각 구성과 흐름도 도면들의 조합들은 컴퓨터 프로그램 인스트럭션들에 의해 수행될 수 있음을 이해할 수 있을 것이다.

[0064] 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 흐름도 구성(들)에서 설명된 기능들을 수행하는 수단을 생성하게 된다.

[0065] 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용 가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 흐름도 구성(들)에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다.

[0066] 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어

컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 흐름도 구성(들)에서 설명된 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

[0067] 또한, 각 구성은 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다.

[0068] 또, 몇 가지 대체 실행예들에서는 구성들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다.

[0069] 예컨대, 잇달아 도시되어 있는 두 개의 구성들은 사실 실질적으로 동시에 수행되는 것도 가능하고 또는 그 구성들이 때때로 해당하는 기능에 따라 역순으로 수행되는 것도 가능하다.

[0070] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명하기로 한다.

[0071] 도 3은 본 발명의 실시예에 따른 다중 CRL의 관리를 도시한 도면으로서, DRM 시스템을 구성하는 다양한 장치들(304~306) 및 복수개의 CRL 발급자(301~303)가 존재하며, 각 CRL 발급자(301~303)는 CRL을 효율적으로 관리하기 위해 각 장치를 위한 CRL(301a~303a)을 작성하여 네트워크(307)를 통해 배포한다.

[0072] 이때, 각 CRL(301a~303a) 내부에는 해당 CRL(301a~303a)을 발급한 CRL 발급자(301~303)를 구분할 수 있는 정보(예를 들어, 발급자 ID)를 포함하므로, DRM 시스템을 구성하는 장치들(304~306)은 서로 다른 CRL 발급자(301~303)가 발급한 CRL들(301a~303a)을 저장, 교환 및 갱신할 수 있다.

[0073] 이하, 도 4 내지 도 6를 통하여 도 3에 도시된 다중 CRL 지원 방법 및 장치를 상세히 설명하도록 한다.

[0074] 이때, DRM 시스템을 구성하는 장치는 클라이언트 및 서버를 포함하고, 두 장치(클라이언트, 서버)는 두 개 이상 다수의 CRL 발급자가 발급한 CRL을 저장하고 있으며, CRL에는 해당 CRL을 발급한 CRL 발급자를 구분할 수 있는 식별 정보, 즉 CRL 발급자 ID를 포함하고 있다고 가정한다.

[0075] 또한 소정의 프로토콜을 통하여 두 장치간 통신이 가능하며, 두 장치 중 하나가 CRL 검사 조건에 해당되어 CRL 갱신이 수행된다고 가정하도록 한다.

[0076] 여기에서 CRL 검사 조건은, 장치간 검증이 요구되는 상호 인증 수행 시, 그리고 CRL이 특정 임계값에 도달했을 때를 의미하는 것으로, 특정 임계값은 CRL 발급자 ID별로 하나 이상 설정 가능하며, 설정된 특정 임계값에 도달하면 장치의 기능 중 일부가 제한될 수 있다.

[0077] 예를 들어, 멀티 미디어 보안 카드 CRL 발급자는 해당 보안 카드에 저장된 자료의 교환 횟수에 대한 특정 임계값을 설정할 수 있으며, 장치 CRL 발급자는 특정 기간을 임계값으로 설정하여 해당 횟수나 해당 기간에 도달하면 저작권 객체에 대한 접근을 제한하는 것이다.

[0078] 물론, 새로운 CRL로 갱신된 후에는 특정 임계값은 초기화되고 임계값 도달로 인해 제한되었던 기능은 해제된다.

[0079] 도 4는 본 발명의 실시예에 따른 CRL 지원 방법을 도시한 흐름도이다.

[0080] 먼저, 클라이언트는 자신이 소유한 서버의 CRL을 갱신 요청 메시지와 함께 서버에 전송한다(S401).

[0081] 이때, S401의 전송 시점은 상술한 CRL의 검사 조건에 해당될 때이다.

[0082] S401 후, 서버는 클라이언트에서 전송한 갱신 요청 메시지 및 자신의 CRL을 수신하고, 수신한 CRL에 포함된 CRL 발급자 ID를 확인한다(S402).

[0083] S402 후, 서버는 S402에서 확인한 CRL 발급자 ID에 대응하는, 즉 해당 발급자가 발급한 자신(서버)의 CRL을 로딩하고, 클라이언트로부터 수신한 CRL과 최신 여부를 비교한다(S403).

[0084] 비교 결과, 클라이언트로부터 수신한 CRL이 최신일 경우, 서버는 자신의 CRL을 클라이언트로부터 수신한 CRL로 갱신하고(S404), 갱신이 완료 되었음을 알리는 응답 메시지를 클라이언트에게 전송한다(S405).

[0085] 참고로, S404에서의 갱신은 서버에서 자신(서버)의 CRL을 폐기하고 수신한 클라이언트의 최신 CRL을 자신(서버)의 새로운 CRL로 사용하거나, 서버에서 자신(서버)의 CRL을 폐기하지 않고 수신한 클라이언트의 최신 CRL을 참조하여 자신(서버)의 CRL을 클라이언트의 CRL과 같도록 하는 것일 수 있다.

[0086] 만일 S403 결과, 클라이언트로부터 수신한 CRL보다 서버 자신의 CRL이 최신일 경우, 서버는 자신의 CRL을 보존하고(S406) 클라이언트로부터 수신한 CRL이 갱신할 필요가 있음을 알리는 응답 메시지를 클라이언트에게 전송한

다(S407).

[0087] 이때, 서버는 자신의 최신 CRL을 응답 메시지와 함께 전송할 수 있다.

[0088] S407 후, 클라이언트는 서버로부터 응답 메시지와 최신 CRL을 수신하고, 수신한 최신 CRL로 자신의 CRL을 갱신한다(S408).

[0089] 참고로, S408에서의 갱신은 클라이언트에서 자신(클라이언트)의 CRL을 폐기하고 수신한 서버의 최신 CRL을 자신(클라이언트)의 새로운 CRL로 사용하거나, 클라이언트에서 자신(클라이언트)의 CRL을 폐기하지 않고 수신한 서버의 최신 CRL을 참조하여 자신(클라이언트)의 CRL을 서버의 CRL과 같도록 하는 것일 수 있다.

[0090] 도 5는 본 발명의 다른 실시예에 따른 CRL 지원 방법을 도시한 흐름도이다.

[0091] 클라이언트가 확인하기 원하는 CRL 발급자 ID를 포함한 클라이언트 자신의 CRL을 송신 요청 메시지와 함께 서버에 전송한다(S501).

[0092] 이때, S501의 전송 시점은 상술한 CRL의 검사 조건에 해당될 때이다.

[0093] S501 후, 서버는 클라이언트의 CRL 및 송신 요청 메시지를 수신하고, 수신한 클라이언트의 CRL에 포함된 CRL 발급자 ID를 확인한다(S502).

[0094] S502 후, 서버는 S502에서 확인한 CRL 발급자 ID에 대응하는, 즉 해당 발급자가 발급한 자신(서버)의 CRL을 로딩하여(S503) 로딩한 CRL을 클라이언트에게 전송한다(S504).

[0095] S504 후, 클라이언트는 서버로부터 서버의 CRL을 수신하고, 자신의 CRL과 최신 여부를 비교한다(S505).

[0096] 비교 결과, 수신한 서버의 CRL이 최신일 경우, 클라이언트는 자신의 CRL을 서버의 CRL로 갱신하고(S506), 갱신이 완료 되었음을 알리는 응답 메시지를 서버에게 전송한다(S507).

[0097] 참고로, S506에서의 갱신은 클라이언트에서 자신(클라이언트)의 CRL을 폐기하고 수신한 서버의 최신 CRL을 자신(클라이언트)의 새로운 CRL로 사용하거나, 클라이언트에서 자신(클라이언트)의 CRL을 폐기하지 않고 수신한 서버의 최신 CRL을 참조하여 자신(클라이언트)의 CRL을 서버의 CRL과 같도록 하는 것일 수 있다.

[0098] 만일 S505 결과, 수신한 서버의 CRL보다 클라이언트 자신의 CRL이 최신일 경우, 클라이언트는 자신의 CRL을 보존하고(S508) 서버의 CRL이 갱신할 필요가 있음을 알리는 응답 메시지를 서버에게 전송한다(S509).

[0099] 이때, 클라이언트는 자신의 최신 CRL을 응답 메시지와 함께 전송할 수 있다.

[0100] S509후, 서버는 클라이언트로부터 응답 메시지와 최신 CRL을 수신하고, 수신한 최신 CRL로 자신의 CRL을 갱신하고(S510), 갱신이 완료 되었음을 알리는 응답 메시지를 클라이언트에게 전송한다(S511).

[0101] 참고로, S510에서의 갱신은 서버에서 자신(서버)의 CRL을 폐기하고 수신한 클라이언트의 최신 CRL을 자신(서버)의 새로운 CRL로 사용하거나, 서버에서 자신(서버)의 CRL을 폐기하지 않고 수신한 클라이언트의 최신 CRL을 참조하여 자신(서버)의 CRL을 클라이언트의 CRL과 같도록 하는 것일 수 있다.

[0102] 도 6은 본 발명의 또 다른 실시예에 따른 CRL 지원 방법을 도시한 흐름도이다.

[0103] 클라이언트가 확인하기 원하는 CRL 발급자 ID를 포함한 클라이언트 자신의 CRL을 갱신 요청 메시지와 함께 서버에 전송한다(S601).

[0104] 이때, S601의 전송 시점은 상술한 CRL의 검사 조건에 해당될 때이다.

[0105] S601 후, 서버는 클라이언트의 CRL 및 갱신 요청 메시지를 수신하고, 수신한 클라이언트의 CRL에 포함된 CRL 발급자 ID를 확인한다(S602).

[0106] S602 후, 서버는 S602에서 확인한 CRL 발급자 ID에 대응하는, 즉 해당 발급자가 발급한 자신(서버)의 CRL을 로딩하고, 수신한 클라이언트의 CRL과 최신 여부를 비교한다(S603).

[0107] 비교 결과, 수신한 클라이언트의 CRL이 최신일 경우, 서버는 자신의 CRL을 클라이언트로부터 수신한 CRL로 갱신하고(S604), 갱신이 완료 되었음을 알리는 응답 메시지를 클라이언트에게 전송한다(S605).

[0108] 참고로, S604에서의 갱신은 서버에서 자신(서버)의 CRL을 폐기하고 수신한 클라이언트의 최신 CRL을 자신(서버)의 새로운 CRL로 사용하거나, 서버에서 자신(서버)의 CRL을 폐기하지 않고 수신한 클라이언트의 최신 CRL을

참조하여 자신(서버)의 CRL을 클라이언트의 CRL과 같도록 하는 것일 수 있다.

[0109] 만일 S603 결과, 수신한 클라이언트의 CRL보다 서버 자신의 CRL이 최신일 경우, 서버는 자신의 CRL을 보존하고(S606), 수신한 클라이언트의 CRL을 갱신하여(S607) 클라이언트의 CRL이 갱신되었음을 알리는 응답 메시지와 함께 갱신된 클라이언트의 CRL을 클라이언트에게 전송한다(S608).

[0110] 참고로, S606 이후, 서버는 클라이언트의 CRL을 폐기하고 자신(서버)의 최신 CRL을 응답 메시지와 함께 클라이언트에게 전송하여 클라이언트에서 서버의 최신 CRL을 사용할 수 있도록 하거나, 수신한 클라이언트의 CRL을 자신(서버)의 최신 CRL과 같도록 갱신하여 클라이언트의 CRL이 갱신되었음을 알리는 응답 메시지와 함께 갱신된 클라이언트의 CRL을 클라이언트에게 전송할 수도 있으며, 도 6에서는 설명의 편의상 후자의 경우를 예로 들어 설명하였다.

[0111] 도 7은 본 발명의 실시예에 따른 DRM을 위한 다중 CRL 지원 장치의 구성을 도시한 블록도이다.

[0112] 본 발명의 실시예에 따른 DRM을 위한 다중 CRL 지원 장치(700)는 제 1 인증서 철회 목록을 수신하고 수신한 제 1 인증서 철회 목록의 발급자 식별 정보를 확인하는 식별 정보 확인부(701), 식별 정보 확인부(701)에서 확인된 발급자 식별 정보에 대응하는 제 2 인증서 철회 목록을 로딩하여 제 1 인증서 철회 목록과 최신 여부를 비교하는 갱신 판단부(702) 및 갱신 판단부(702)의 비교 결과에 따라 제 1 인증서 철회 목록 및 제 2 인증서 철회 목록 중 어느 하나를 최신의 인증서 철회 목록으로 갱신하는 갱신부(703)를 포함한다.

[0113] 도 8은 본 발명의 다른 실시예에 따른 DRM을 위한 다중 CRL 지원 장치의 구성을 도시한 블록도이다.

[0114] 본 발명의 다른 실시예에 따른 DRM을 위한 다중 CRL 지원 장치(800)는 인증서 철회 목록의 발급자 식별 정보를 포함한 제 1 인증서 철회 목록을 발신하는 발신부(801), 발신부(801)에서 발신된 제 1 인증서 철회 목록의 최신 여부에 따라 제 1 인증서 철회 목록의 갱신 완료 및 갱신 요청 중 어느 하나에 대한 응답을 수신하는 수신부(802) 및 수신부(802)에서 수신한 응답에 따라 제 1 인증서 철회 목록의 갱신 여부를 결정하는 갱신부(803)를 포함한다.

[0115] 본 발명의 실시예에 따른 도 7 내지 도 8에서 도시된 구성요소들은 소프트웨어 또는 FPGA(Field Programmable Gate Array) 또는 ASIC(Application Specific Integrated Circuit)와 같은 하드웨어 구성요소를 의미하며, 소정의 역할들을 수행한다.

[0116] 그렇지만 구성요소들은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니며, 각 구성요소는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다.

[0117] 따라서, 일 예로서 구성요소는 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들, 및 변수들을 포함한다.

[0118] 구성요소들과 해당 구성요소들 안에서 제공되는 기능은 더 작은 수의 구성요소들로 결합되거나 추가적인 구성요소들로 더 분리될 수 있다.

[0119] 참고로, DRM 시스템을 구성하는 장치는 클라이언트 및 서버를 포함하고, 두 장치(클라이언트, 서버)는 두 개 이상 다수의 CRL 발급자가 발급한 CRL을 각각 저장하고 있으며, CRL에는 해당 CRL을 발급한 CRL 발급자를 구분할 수 있는 식별 정보, 즉 CRL 발급자 ID를 포함하고 있다고 가정한다.

[0120] 이때, 도 7에 도시된 장치(700)는 서버에 포함되고, 도 8에 도시된 장치(800)는 클라이언트에 포함될 수 있으며, 반대로 도 8에 도시된 장치(800)가 서버에 포함되고, 도 7에 도시된 장치(700)가 클라이언트에 포함될 수 있다. 또한 CRL 갱신 판단의 신뢰성을 높이기 위해 서버와 클라이언트 모두 갱신 판단부(702)를 포함할 수 있다.

[0121] 설명의 편의상, 본 발명의 실시예에서는 도 7에 도시된 장치(700)는 서버에 포함되고, 도 8에 도시된 장치(800)는 클라이언트에 포함되는 경우를 설명하도록 한다.

[0122] 먼저, 도 8에 도시된 장치(800), 즉 클라이언트의 발신부(801)는 CRL 발급자 ID를 포함한 CRL을 도 7에 도시된 장치(700), 즉 서버에게 전송한다.

[0123] 참고로, 본 발명의 실시예에 따라 DRM 시스템에서 CRL 발급자 ID를 포함한 CRL을 전송하여 CRL을 검사하는 경우는, 장치간 검증이 요구되는 상호 인증 수행 시, 그리고 CRL이 특정 임계값에 도달했을 때이다.

[0124] 여기에서 특정 임계값은 CRL 발급자 ID별로 하나 이상 설정 가능하며, 설정된 특정 임계값에 도달하면 장치의 기능 중 일부가 제한될 수 있다.

[0125] 예를 들어, 멀티 미디어 보안 카드 CRL 발급자는 해당 보안 카드에 저장된 자료의 교환 횟수에 대한 특정 임계값을 설정할 수 있으며, 장치 CRL 발급자는 특정 기간을 임계값으로 설정하여 해당 횟수나 해당 기간에 도달하면 저작권 객체에 대한 접근을 제한하는 것이다.

[0126] 물론, 새로운 CRL로 갱신된 후에는 특정 임계값은 초기화되고 임계값 도달로 인해 제한되었던 기능은 해제된다.

[0127] 서버의 식별 정보 확인부(701)는 클라이언트의 발신부(801)에서 발신한 CRL(이하, 제 1 CRL이라 칭함)을 수신하고, 수신한 제 1 CRL의 발급자 식별 정보인 CRL 발급자 ID를 확인한다.

[0128] 여기에서 CRL 발급자 ID는 CRL 내 CRL 발급자를 구분하기 위한 식별 정보이며, 본 발명의 실시예에 따른 CRL 발급자의 구성은 저작권으로 보호된 컨텐츠의 재생을 지원하는 장치인 호스트, 저작권으로 보호된 컨텐츠를 재생할 수 있도록 관련 정보를 안전하게 저장하고 관리하는 멀티미디어카드(Secure Removable Media)를 포함하는 디바이스의 종류에 따른 CRL 발급자, 저작권 발급자(Rights Issuer)나 인증기관(Certificate Authority)과 같은 DRM 시스템 구성에 따른 CRL 발급자, 컨텐츠 서비스 사업자와 DRM 장치 제조업체와 같은 DRM 시스템을 운영하는 기관에 따른 CRL 발급자, OMA(Open Mobile Alliance) DRM이나 MSW(Micosoft Window Media) DRM과 같은 DRM 종류에 따른 CRL 발급자 등으로 분류될 수 있다.

[0129] 참고로, 상술한 CRL 발급자의 분류 외에도 필요에 따라 여러 CRL 발급자로 분류될 수 있으며 이는 본 발명의 실시예로 한정하지 않는다.

[0130] 따라서, 상술한 CRL 발급자 ID를 통해서, 서버의 식별 정보 확인부(701)는 수신한 제 1 CRL의 CRL 발급자 ID를 확인하고 상대 장치에서 어떤 CRL을 검증하기 원하는 지를 판단하게 되는 것이다.

[0131] 서버의 갱신 판단부(702)는 식별 정보 확인부(701)에서 확인한 제 1 CRL 발급자 ID를 통해 해당 ID와 대응되는 CRL, 즉 동일한 CRL 발급자 ID를 갖는 CRL(이하, 제 2 CRL이라 칭함)을 서버의 저장소에서 로딩한다.

[0132] 참고로, 서버의 저정소에는 암호화된 컨텐츠들과 권리 객체들 그리고 서버의 인증서와 CRL이 저장될 수 있다.

[0133] 서버의 갱신 판단부(702)는 제 2 CRL을 로딩하고, 수신한 제 1 CRL과 최신 여부를 비교하여 비교 결과를 갱신부(703)에 전달한다.

[0134] 여기에서 최신 여부의 비교는 CRL 발급일자를 기준으로 하며, 갱신 판단부(702)는 CRL 발급 일자가 최근 일자일수록 최신의 CRL로 판단한다.

[0135] 서버의 갱신부(703)는 갱신 판단부(702)로부터 전달받은 제 1 CRL과 제 2 CRL의 비교 결과를 통해 제 1 CRL 및 제 2 CRL 중 어느 CRL을 갱신할 것인지를 결정하고, 갱신 대상이 되는 CRL을 최신의 CRL로 갱신한다.

[0136] 예를 들어, 만일 클라이언트의 제 1 CRL이 서버의 제 2 CRL보다 최신의 CRL이면, 서버의 갱신부(703)는 제 2 CRL을 제 1 CRL로 갱신하게 되는데, 이러한 갱신은 서버의 저장소에 저장되어있던 기존의 제 2 CRL을 폐기하고 클라이언트의 제 1 CRL을 새로운 CRL로서 서버의 저장소에 저장한 후, 서버의 제 2 CRL을 클라이언트의 제 1 CRL로 갱신했음을 알리는 응답 메시지를 클라이언트에게 전송하는 갱신일 수 있다.

[0137] 또한, 서버의 제 2 CRL이 클라이언트의 제 1 CRL보다 최신이면, 서버의 갱신부(703)는 제 1 CRL을 제 2 CRL로 갱신하게 되는데, 이러한 갱신은 서버의 갱신부(703)에서 클라이언트의 제 1 CRL을 폐기하고, 이를 알리는 응답 메시지와 함께 서버의 CRL을 전송하여 클라이언트에서 서버의 최신 CRL로 갱신할 수 있도록 하거나, 서버의 갱신부(703)에서 클라이언트의 제 1 CRL을 폐기하지 않고 서버의 제 2 CRL로 클라이언트의 제 1 CRL을 갱신한 후, 이를 알리는 응답 메시지와 함께 갱신된 클라이언트의 CRL을 클라이언트에게 전송하는 갱신일 수 있으며, 서버의 갱신부(703)에서 클라이언트의 제 1 CRL을 갱신하지 않고, CRL의 갱신이 필요함을 알리는 응답 메시지와 함께 서버의 제 2 CRL을 클라이언트에게 전송하여 클라이언트에서 서버의 최신 CRL을 수신하고, 수신한 서버의 최신 CRL로 클라이언트의 CRL을 갱신하도록 하는 것일 수 있다.

[0138] 만일, 클라이언트의 제 1 CRL 및 서버의 제 2 CRL의 발급일자가 동일할 경우, CRL의 갱신 없이 서버와 클라이언트의 통신은 계속 유지된다

[0139] 한편, 클라이언트의 수신부(802)는 클라이언트의 발신부(801)에서 발신한 제 1 CRL의 최신 여부에 따라 서버의 갱신부(703)로부터 제 1 CRL의 갱신 완료 및 갱신 요청 중 어느 하나에 대한 응답 메시지를 수신한다.

[0140] 예를 들어, 클라이언트에서 발신한 제 1 CRL이 서버의 제 2 CRL보다 최신일 경우, 서버의 갱신부(703)에서는 서버의 제 2 CRL을 클라이언트의 제 1 CRL로 갱신하고, 갱신이 완료되었음을 알리는 응답 메시지를 전송하면 클라이언트의 수신부(802)는 해당 응답 메시지를 수신한다.

[0141] 이후, 클라이언트의 갱신부(803)는 수신부(802)에서 수신한 응답 메시지를 참조하여 CRL 갱신을 종료한 후 서버와의 통신을 유지한다.

[0142] 만일, 클라이언트에서 발신한 제 1 CRL보다 서버의 제 2 CRL이 최신일 경우, 서버의 갱신부(703)에서 클라이언트의 제 1 CRL이 갱신되어야 함을 알리는 응답 메시지와 함께 서버의 제 2 CRL을 송신하면, 클라이언트의 수신부(802)는 해당 응답 메시지와 함께 서버의 제 2 CRL을 수신한다.

[0143] 이후, 클라이언트의 갱신부(803)는 수신부(802)에서 수신한 응답 메시지를 참조하여 클라이언트의 저장소에 저장되어있던 기존의 제 1 CRL을 폐기하고 수신부(802)를 통해 수신한 서버의 제 2 CRL을 새로운 CRL로서 클라이언트의 저장소에 저장한 후 서버와의 통신을 유지한다.

[0144] 클라이언트에서 발신한 제 1 CRL보다 서버의 제 2 CRL이 최신일 경우, 상술한 방법 외에도, 서버의 갱신부(703)에서 서버의 제 2 CRL로 클라이언트의 제 1 CRL을 갱신하고, 이를 알리는 응답 메시지와 함께 갱신된 클라이언트의 CRL을 전송하면, 클라이언트의 수신부(802)는 해당 응답 메시지와 갱신된 CRL을 수신한 후 CRL 갱신을 종료하고 서버와의 통신을 유지할 수 있다.

[0145] 이상과 첨부된 도면을 참조하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다.

발명의 효과

[0146] 상기한 바와 같은 본 발명의 디지털 저작권 관리를 위한 다중 인증서 철회 목록 지원 방법 및 장치에 따르면 다음과 같은 효과가 하나 혹은 그 이상 있다.

[0147] 기관별, 장치별 CRL 발급자에 따라 개별적으로 그리고 목적에 맞게 CRL 관리가 가능하므로, 불필요한 CRL을 유지 및 관리할 필요가 없어 하나의 장치 내에서 관리되는 CRL의 크기를 감소시키고 관리의 효율을 높이는 장점이 있다.

[0148] 또한, CRL 발급자에 따라 필요한 CRL을 직접 관리할 수 있기 때문에, 여러 기관에서 발급한 CRL이 하나의 장치에 저장되어 사용되는 경우, 서로 다른 CRL 발급자로 인해 발생되는 충돌을 방지하는 장점도 있다.

[0149] 또한, 멀티 DRM을 지원하는 장치의 경우, 특정 DRM이 동작하고 있을 때, DRM 종류별 CRL 발급자에 따라 필요한 CRL 관리가 가능하므로, 해당 종류의 DRM에 관한 CRL만 별도로 관리하는 장점도 있다.

도면의 간단한 설명

[0001] 도 1은 일반적인 DRM의 개념을 나타낸 도면이다.

[0002] 도 2는 종래 DRM 시스템 에서의 CRL 발급 및 갱신을 도시한 도면이다.

[0003] 도 3은 본 발명의 실시예에 따른 다중 CRL의 관리를 도시한 도면이다.

[0004] 도 4는 본 발명의 실시예에 따른 CRL 지원 방법을 도시한 흐름도이다.

[0005] 도 5는 본 발명의 다른 실시예에 따른 CRL 지원 방법을 도시한 흐름도이다.

[0006] 도 6은 본 발명의 또 다른 실시예에 따른 CRL 지원 방법을 도시한 흐름도이다.

[0007] 도 7은 본 발명의 실시예에 따른 DRM을 위한 다중 CRL 지원 장치의 구성을 도시한 블록도이다.

[0008] 도 8은 본 발명의 다른 실시예에 따른 DRM을 위한 다중 CRL 지원 장치의 구성을 도시한 블록도이다.

[0009] <도면의 주요 부분에 관한 부호의 설명>

[0010] 701 : 식별 정보 확인부

[0011] 702 : 갱신 판단부

[0012] 703 : 갱신부

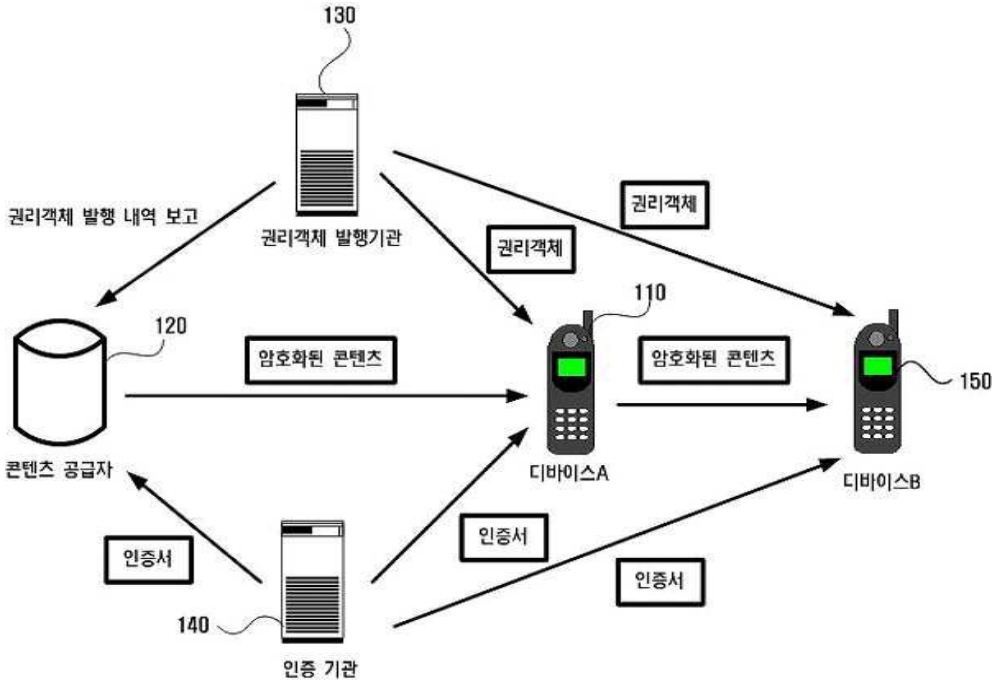
[0013] 801 : 발신부

[0014] 802 : 수신부

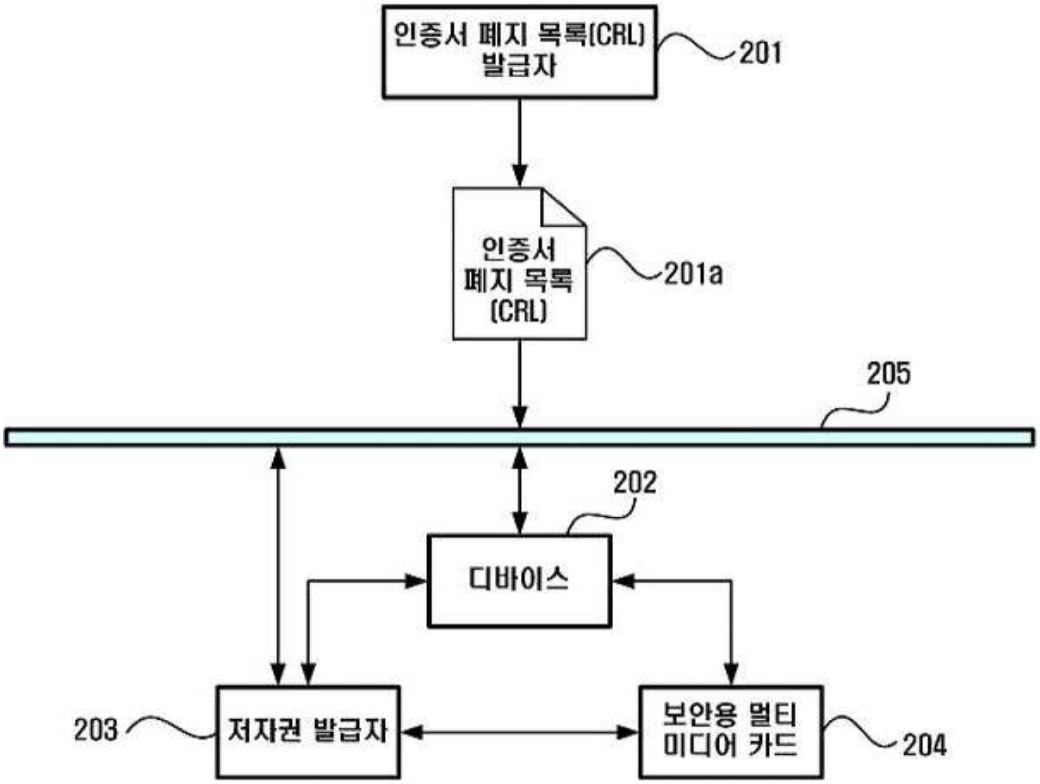
[0015] 803 : 갱신부

도면

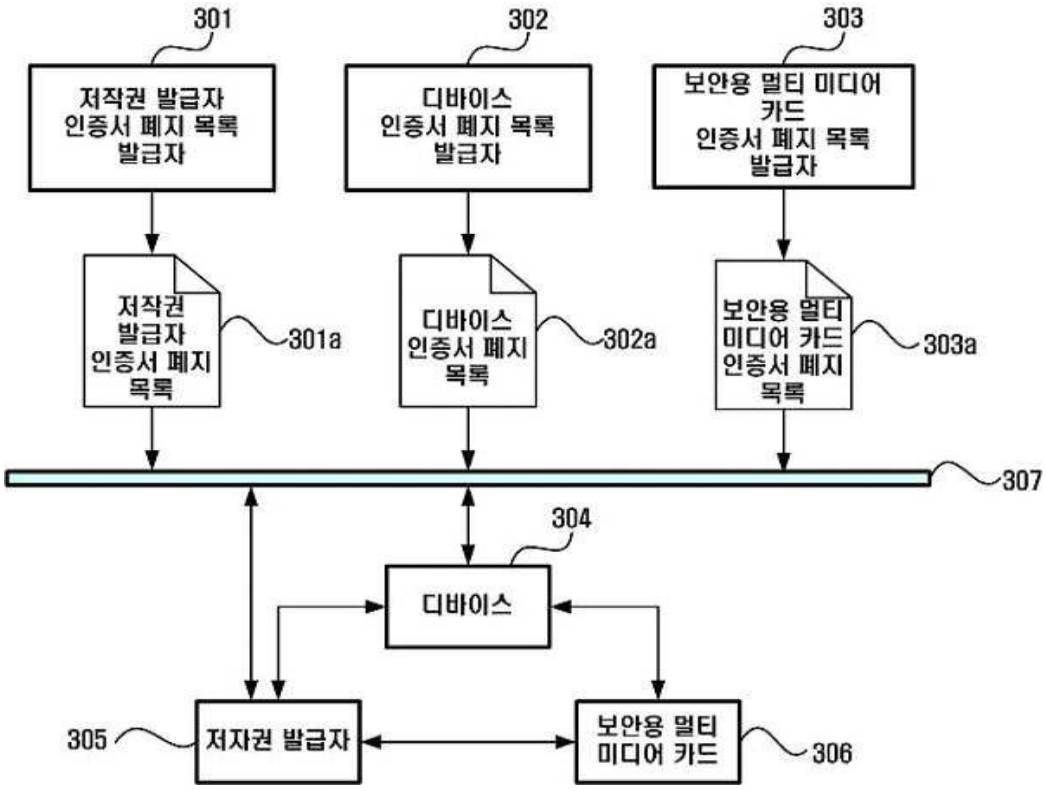
도면1



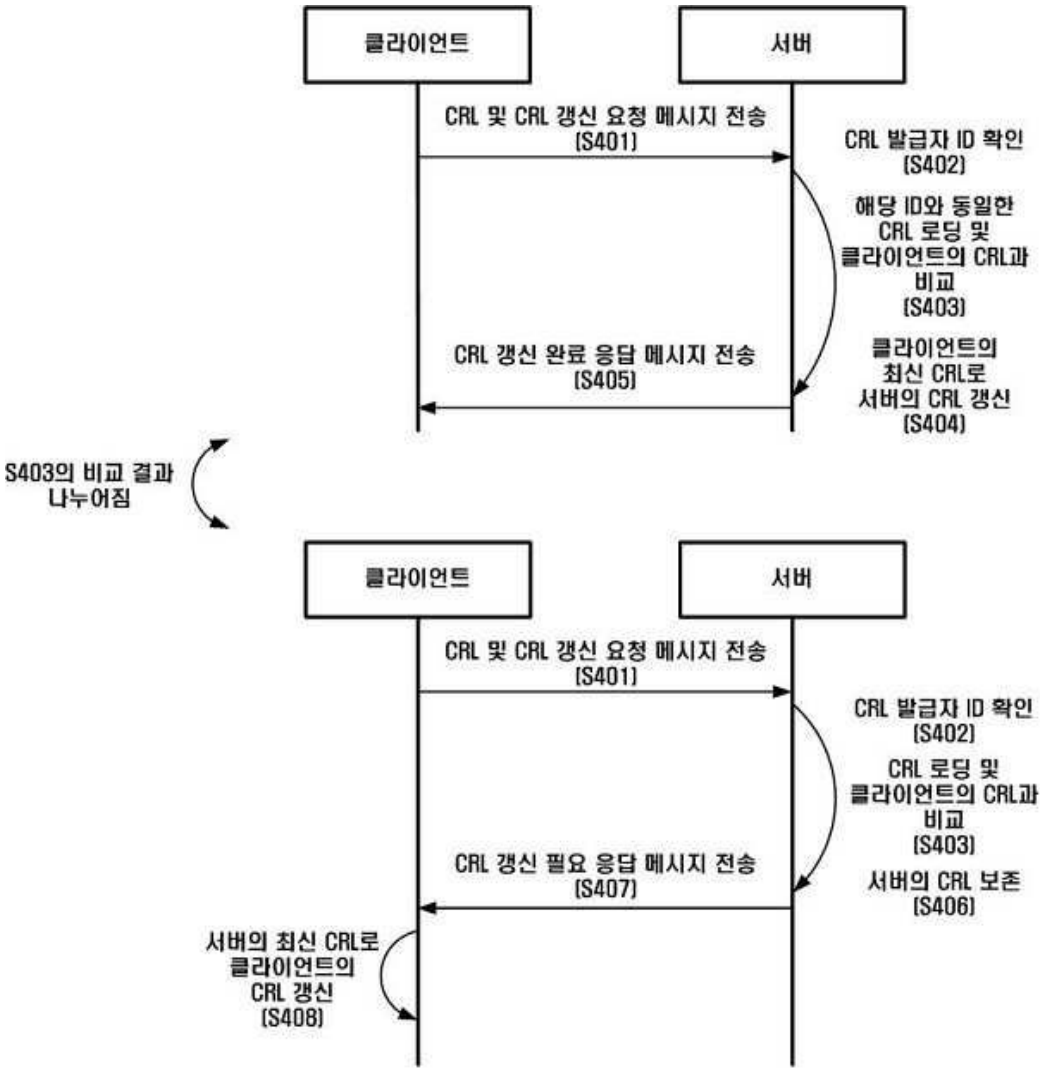
도면2


인증서 폐지 목록(CRL) 발급자
201
인증서 폐지 목록 (CRL)
201a
205
202
디바이스
203
저자권 발급자
보안용 멀티 미디어 카드
204

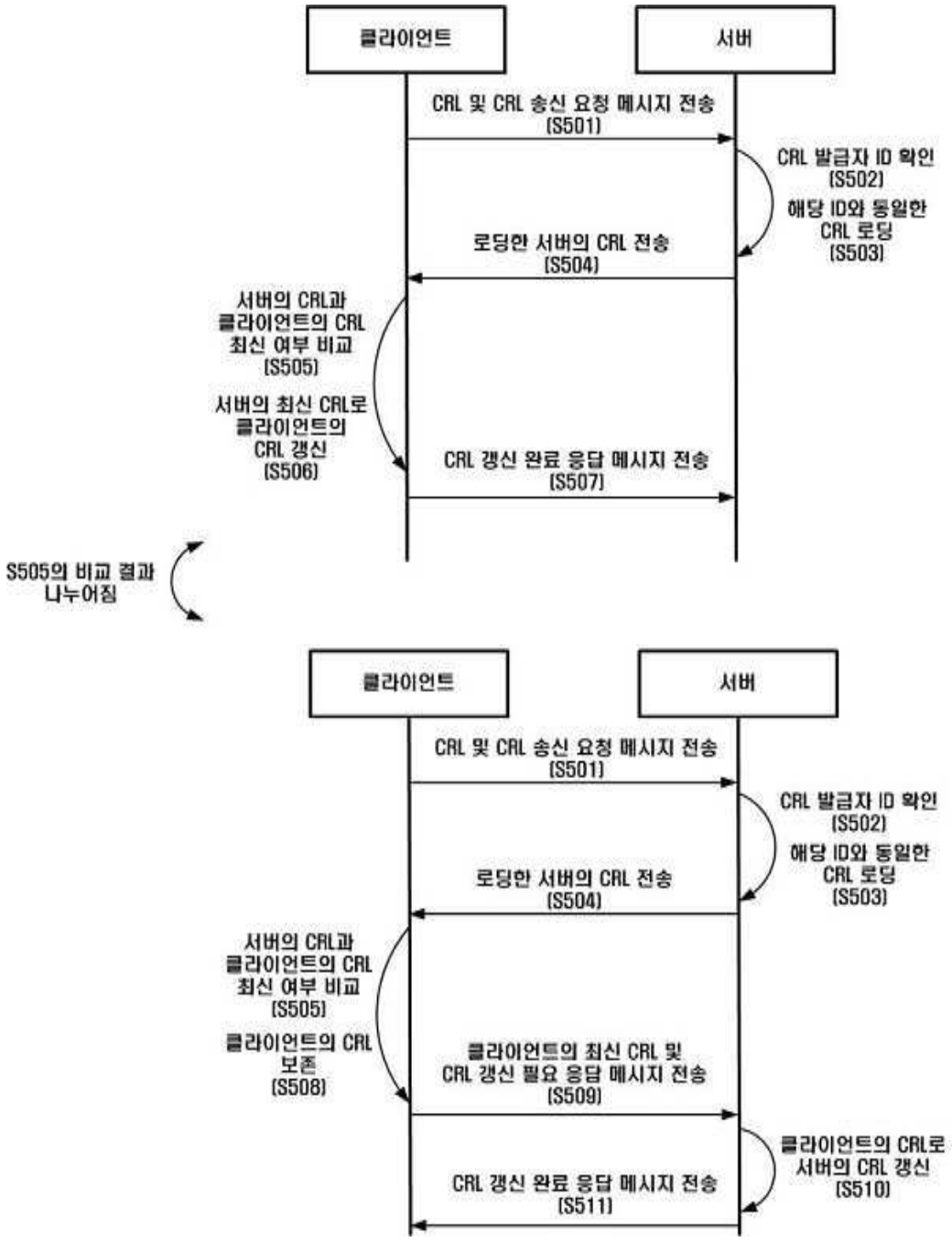
도면3


301
저작권 발급자 인증서 폐지 목록 발급자
302
디바이스 인증서 폐지 목록 발급자
303
보안용 멀티 미디어 카드 인증서 폐지 목록 발급자
저작권 발급자 인증서 폐지 목록
301a
디바이스 인증서 폐지 목록
302a
보안용 멀티 미디어 카드 인증서 폐지 목록
303a
307
304
디바이스
305
저자권 발급자
보안용 멀티 미디어 카드
306

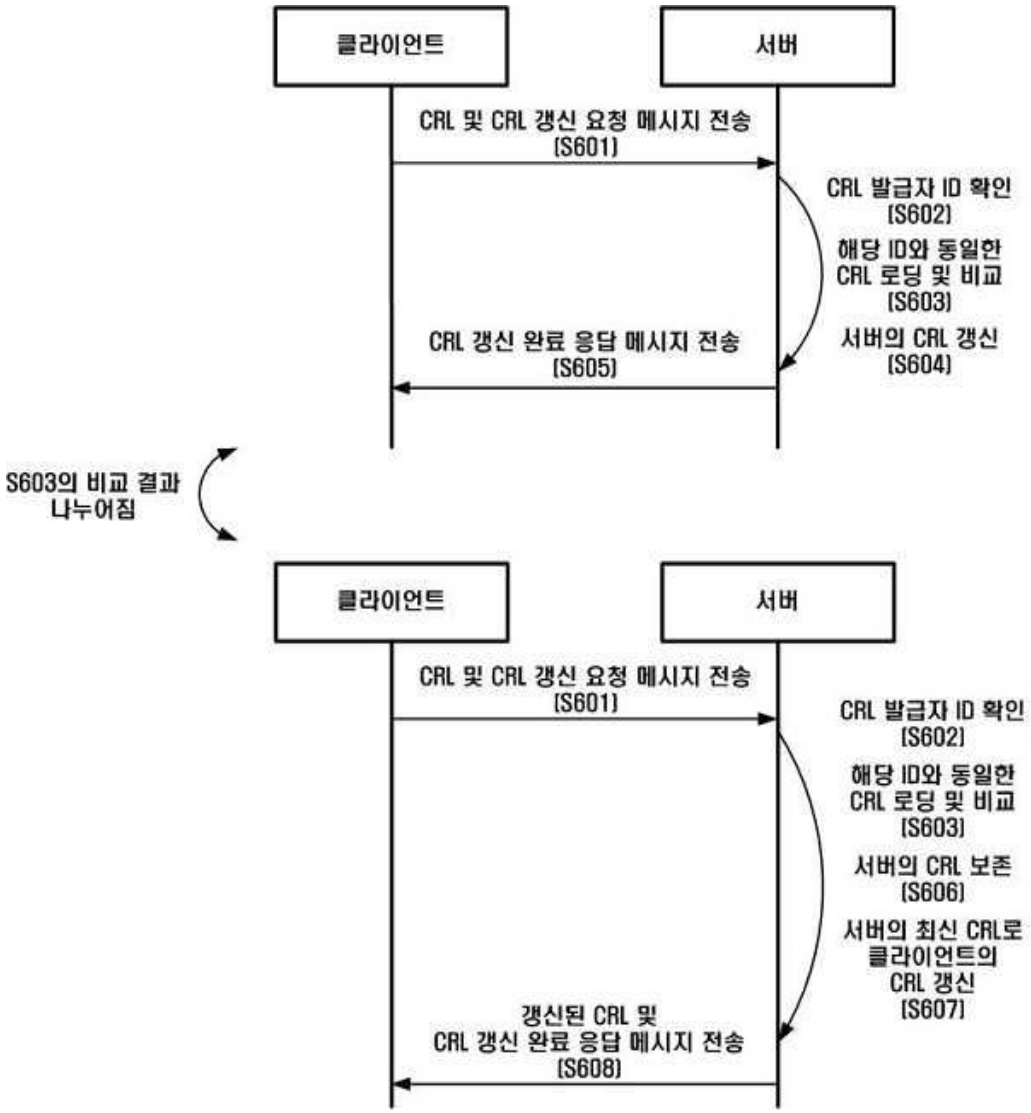
도면4


클라이언트
서버
CRL 및 CRL 갱신 요청 메시지 전송
(S401)
CRL 발급자 ID 확인
(S402)
해당 ID와 동일한
CRL 로딩 및
클라이언트의 CRL과
비교
(S403)
CRL 갱신 완료 응답 메시지 전송
(S405)
클라이언트의
최신 CRL로
서버의 CRL 갱신
(S404)
S403의 비교 결과
나누어짐
클라이언트
서버
CRL 및 CRL 갱신 요청 메시지 전송
(S401)
CRL 발급자 ID 확인
(S402)
CRL 로딩 및
클라이언트의 CRL과
비교
(S403)
CRL 갱신 필요 응답 메시지 전송
(S407)
서버의 CRL 보존
(S406)
서버의 최신 CRL로
클라이언트의
CRL 갱신
(S408)

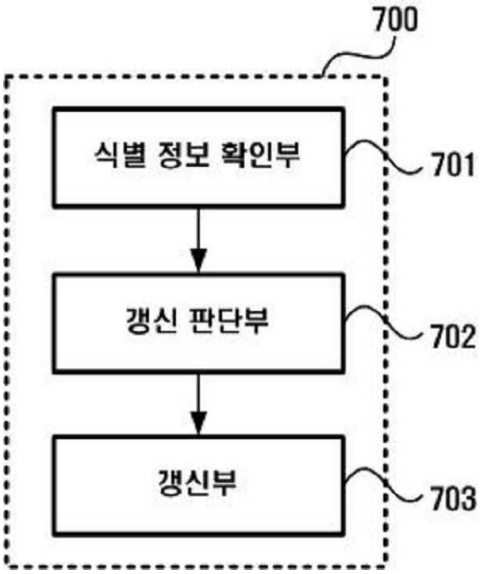
도면5


클라이언트
서버
CRL 및 CRL 송신 요청 메시지 전송
(S501)
CRL 발급자 ID 확인
(S502)
해당 ID와 동일한
CRL 로딩
(S503)
로딩한 서버의 CRL 전송
(S504)
서버의 CRL과
클라이언트의 CRL
최신 여부 비교
(S505)
서버의 최신 CRL로
클라이언트의
CRL 갱신
(S506)
CRL 갱신 완료 응답 메시지 전송
(S507)
S505의 비교 결과
나누어짐
클라이언트
서버
CRL 및 CRL 송신 요청 메시지 전송
(S501)
CRL 발급자 ID 확인
(S502)
해당 ID와 동일한
CRL 로딩
(S503)
로딩한 서버의 CRL 전송
(S504)
서버의 CRL과
클라이언트의 CRL
최신 여부 비교
(S505)
클라이언트의 CRL
보존
(S508)
클라이언트의 최신 CRL 및
CRL 갱신 필요 응답 메시지 전송
(S509)
클라이언트의 CRL로
서버의 CRL 갱신
(S510)
CRL 갱신 완료 응답 메시지 전송
(S511)

도면6


클라이언트
서버
CRL 및 CRL 갱신 요청 메시지 전송
(S601)
CRL 발급자 ID 확인
(S602)
해당 ID와 동일한
CRL 로딩 및 비교
(S603)
서버의 CRL 갱신
(S604)
CRL 갱신 완료 응답 메시지 전송
(S605)
S603의 비교 결과
나누어짐
클라이언트
서버
CRL 및 CRL 갱신 요청 메시지 전송
(S601)
CRL 발급자 ID 확인
(S602)
해당 ID와 동일한
CRL 로딩 및 비교
(S603)
서버의 CRL 보존
(S606)
서버의 최신 CRL로
클라이언트의
CRL 갱신
(S607)
갱신된 CRL 및
CRL 갱신 완료 응답 메시지 전송
(S608)

도면7



도면8