(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년05월31일
(11) 등록번호 10-1985029
(24) 등록일자 2019년05월27일

(51) 국제특허분류(Int. Cl.)
G06F 21/33 (2013.01) *G06F 16/00* (2019.01)
(21) 출원번호 10-2013-7024540
(22) 출원일자(국제) 2012년02월15일
심사청구일자 2017년01월31일
(85) 번역문제출일자 2013년09월16일
(65) 공개번호 10-2014-0043066
(43) 공개일자 2014년04월08일
(86) 국제출원번호 PCT/US2012/025172
(87) 국제공개번호 WO 2012/112640
국제공개일자 2012년08월23일
(30) 우선권주장
13/372,613 2012년02월14일 미국(US)
61/444,753 2011년02월20일 미국(US)
(56) 선행기술조사문헌
US20110010553 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
칸, 로버트, 에스.
미국, 뉴욕 10512, 카멜, 607 집시 트레일 로드, 집시 트레일 클럽
(72) 발명자
칸, 로버트, 에스.
미국, 뉴욕 10512, 카멜, 607 집시 트레일 로드, 집시 트레일 클럽
(74) 대리인
허용록

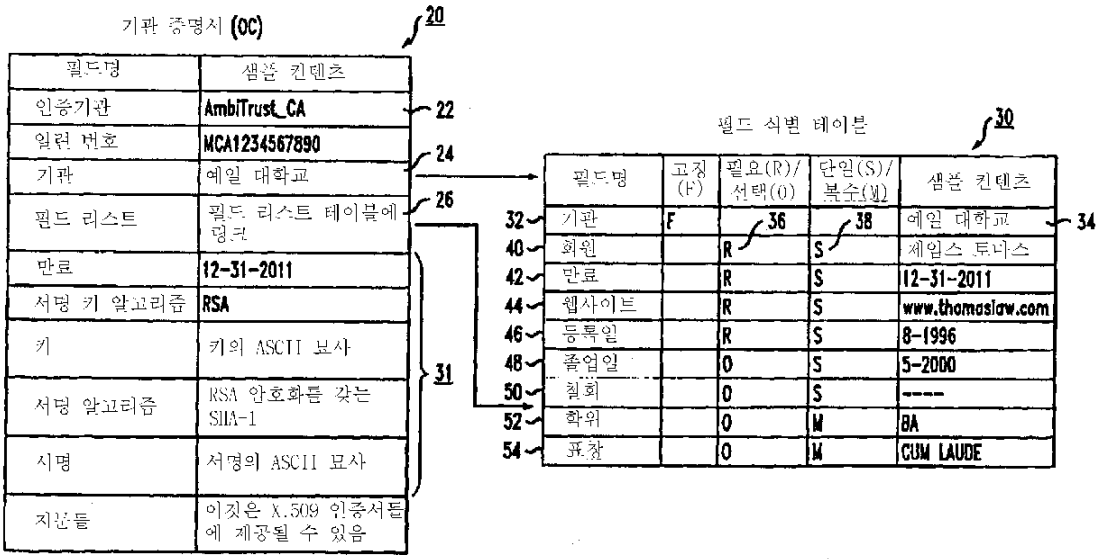
전체 청구항 수 : 총 18 항 심사관 : 문남두

(54) 발명의 명칭 **관련된 기관 증명서를 이용한 온 라인 회원 인증**

(57) 요 약

"회원 증명서"(membership certificate; MC)와 결합된 "기관 증명서(organization certificate; OC)"의 이용을 통해 독립적인 사람(제3자, 즉, 주장된 회원의 웹사이트의 사용자)에 특정된 자격 인증서의 인증을 제공하기 위한 시스템 및 방법이 제시되고, 상기 OC의 필드 구조는 발행 기관에 의해 증명될 수 있는 정보의 유형을 제한한다. 상기 OC에서의 일련의 필드들은 특정 유형의 기관과 관련되어 규정되며, 이때 임의의 관련 없는 정보는 적법한 회원 증명서(이후, "MC")의 일부를 형성하도록 허용되지 않는다. 그에 따라, 특정 필드 기술의 사용에 의해, OC에 있어서 대응하는 <필드> 태그를 갖지 않는 MC에 나타나는 임의의 필드는, 인증 절차 동안 사용자의 브라우저 확장에 의해 MC가 무효로 표시되도록 하는 것으로 가정한다.

대 표 도 - 도3



명 세 서

청구범위

청구항 1

주장된 회원의 웹사이트상에 제시된 회원 증명서를 인증하기 위한 컴퓨터 구현 방법으로서,

회원 증명서를 활성화시키는 단계로, 회원 증명서는 회원 증명서를 발행한 기관을 확인하는 필드와 페이로드부를 포함하고, 페이로드부는, 특정 분야 태그들로 구성되는, 발행 기관이 회원 증명서에 포함되도록 허용하는 주장된 회원에 대한 특정 정보를 포함하는, 단계;

회원 증명서를 생성한 기관과 관련된 기관 증명서를 검색하는 단계로서, 상기 기관 증명서는 특정 기관 유형에만 관련되고 회원을 규정하고 기관 증명서와 회원 증명서에서 확인되는 일련의 고정 필드들에 의해 통제되는 일련의 소정 정보 요소들을 포함하는, 단계;

상기 회원 증명서에서 제시된 요소들과 상기 기관 증명서를 비교하는 단계; 및

상기 회원 증명서에서 제시된 일련의 고정 필드들이 확인된 기관에 의해 규정된 기관 증명서 내에 구성된 일련의 고정 필드들과 일치하는 경우, 상기 회원 증명서를 인증하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 2

제1항에 있어서, 상기 기관 증명서는, 인증 기관(CA)에 의해 생성되고 또한 상기 방법은 상기 인증 기관에 관한 상기 기관 증명서를 유효화하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 3

제1항에 있어서, 상기 방법을 실행하는 로컬 컴퓨터는 유효 기관 증명서의 캐시를 포함하는, 컴퓨터 구현 방법.

청구항 4

제1항에 있어서, 상기 방법을 실행하는 로컬 컴퓨터는, 네트워크 데이터베이스로부터 현재의 유효 기관 증명서들의 리스트를 얻는, 컴퓨터 구현 방법.

청구항 5

제1항에 있어서, 회원 증명서 특정 필드들과 기관 증명서의 소정의 고정 필드들의 비교는, 각 특정 필드 내에 필요한 정보를 포함하기 위한 체크를 포함하는, 컴퓨터 구현 방법.

청구항 6

제1항에 있어서, 회원 증명서 특정 필드들과 기관 증명서의 소정의 고정 필드들의 비교는, 복수 엔트리들을 허용하지 않는 것으로서 규정되는 소정의 특정 필드에 대한 정보 요소의 단일 생성만을 위한 체크를 포함하는, 컴퓨터 구현 방법.

청구항 7

제1항에 있어서, 기관 증명서가 서명되고 만료되지 않은 것을 인증하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 8

제1항에 있어서, 회원 증명서가 만료되지 않은 것을 인증하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 9

제1항에 있어서, 상기 기관 증명서 및 회원 증명서는 결합 증명서로서 제공되고, 상기 기관 증명서는 회원 증명서를 인증하기 전에 먼저 인증되는, 컴퓨터 구현 방법.

청구항 10

주장된 회원의 웹사이트상에 제시된 회원 증명서를 인증하기 위한 시스템으로서,

회원 증명서를 활성화시키기 위한 제1 컴퓨터 사용가능한 프로그램 코드 하드웨어 요소로, 상기 회원 증명서는 상기 회원 증명서를 발행한 기관을 확인하는 필드와 페이로드부를 포함하고, 페이로드부는 특정 분야 태그들로 구성되는, 발행 기관이 회원 증명서에 포함되도록 허용하는 주장된 회원에 대한 특정 정보를 포함하고;

상기 회원 증명서를 생성한 기관과 관련된 기관 증명서를 검색하기 위한 제2 컴퓨터 사용가능한 프로그램 코드 하드웨어 요소로, 상기 기관 증명서는 특정 기관 유형에만 관련되고 회원을 규정하고 상기 기관 증명서 및 상기 회원 증명서에서 확인되는 일련의 고정 필드들에 의해 통제되는 일련의 소정 정보 요소들을 포함하고;

상기 회원 증명서에서 제시된 요소들과 상기 기관 증명서를 비교하기 위한 제3 컴퓨터 사용가능한 프로그램 코드 하드웨어 요소; 및

상기 회원 증명서에서 제시된 일련의 고정 필드들이 확인된 기관에 의해 규정된 기관 증명서 내에 구성된 일련의 고정 필드들과 일치하는 경우, 상기 회원 증명서를 인증하기 위한 제4 컴퓨터 사용가능한 프로그램 코드 하드웨어 요소를 포함하는 시스템.

청구항 11

제10항에 있어서, 상기 기관 증명서는, 인증 기관(CA)에 의해 생성되고, 상기 제3 컴퓨터 사용가능한 프로그램 코드 하드웨어 요소는 상기 인증 기관에 관한 상기 기관 증명서를 유효화하기 위한 것인, 시스템.

청구항 12

제10항에 있어서, 상기 제2 컴퓨터 사용가능한 프로그램 코드 하드웨어 요소는 유효 기관 증명서의 로컬 캐시를 검색하는 단계를 실행하는, 시스템.

청구항 13

제10항에 있어서, 상기 제2 컴퓨터 사용가능한 프로그램 코드 하드웨어 요소는 네트워크 데이터베이스부터 유효 기관 증명서들을 검색하는 단계를 실행하는, 시스템.

청구항 14

제10항에 있어서, 상기 제4 컴퓨터 사용가능한 프로그램 코드 하드웨어 요소는 각 특정 필드 내에 필요한 정보를 포함하기 위해 회원 증명서 특정 필드들을 체크하는 단계를 실행하는, 시스템.

청구항 15

제10항에 있어서, 상기 제4 컴퓨터 사용가능한 프로그램 코드 하드웨어 요소는, 복수 엔트리들을 허용하지 않는 것으로서 규정되는 소정 특정 필드에 대한 정보 요소의 단일 생성만을 위해 체크하는 단계를 실행하는, 시스템.

청구항 16

제10항에 있어서, 상기 제4 컴퓨터 사용가능한 프로그램 코드 하드웨어 요소는, 기관 증명서가 서명되고 만료되지 않은 것을 인증하는 단계를 실행하는, 시스템.

청구항 17

제10항에 있어서, 상기 기관 증명서 및 회원 증명서는 결합 증명서로서 제시되며, 이때 상기 제4 컴퓨터 사용가능한 프로그램 코드 하드웨어 요소는 먼저 상기 기관 증명서 부분의 인증을 실행한 다음 회원 증명서 부분의 인증을 실행하는, 시스템.

청구항 18

제10항에 있어서, 상기 제4 컴퓨터 사용가능한 프로그램 코드 하드웨어 요소는, 회원 증명서가 만료되지 않은 것을 인증하는 단계를 실행하는, 시스템.

발명의 설명

기 술 분 야

[0001] 관련 출원에 대한 상호 참조

[0002] 본 출원은 2011년 2월 20일자로 출원된 미국 가출원 제61/444,753호의 우선권을 주장하며 상기 가출원은 본 명세서에 참고로 통합된다.

[0003] 기술분야

[0004] 본 발명은, 제2 사이트 인증을 요구하지 않고 인증 기관으로부터의 특정되고, 제한된 자격 인증서의 온 라인 인증을 제공하는 시스템 및 방법에 관한 것이다.

배 경 기 술

[0005] 온 라인 인증 문제는 여러 해 동안 적극적인 연구의 영역으로 되어 왔다. 개인 또는 기관이 자신이 주장하는 사람이 맞는지 여부에 대한 문제는 다수의 웹 기반 기술혁신들을 가져왔다. 종종 온 라인 업자들과 관련하여, 웹 사이트는 그 온 라인 업자의 확인을 "인증"하도록 주장하는 다른 사이트에 대한 링크를 포함할 수 있다. 그 링크를 클릭함으로써, (잠재적 고객과 같은) 사용자는 그 온 라인 업자의 "인증서"를 표시하는 다른 웹사이트 페이지로 다시 향하게 된다. 일반적으로, 이들 시스템은 "제2 사이트 인증"으로 지칭되고 (유감스럽게도) 비교적 위조하기가 쉬운 것으로 알려져 있다. 신용할 수 있는 "인증 서비스들"과 비교적 유사한 도메인 명칭들이 부도덕한 사람들에 의해 판매되고 있고 이들 부도덕한 사람들은 '가짜' 인증서를 만들고 그것들을 특정 제품 또는 서비스의 인증을 구하는 부주의한 제3자에게 제공한다. 간단히 말해, 좋은 사이트들은 확인을 위해 다른 좋은 사이트들을 사용자에 보내고, 불량 사이트들은 다른 불량 사이트들을 사용자에 보낸다. 더욱이, 제2 사이트 인증 서비스들의 시장에 있어서의 불량 사이트의 확산이 문제로 된다. 일부 브라우저 애드-온(add-on)들은 사용자가 "불량 사이트들"에 대해 경계할 수 있으나, 이 해법은 새로운 불량 사이트들을 생성하는 부도덕한 자들 간의 경쟁으로 귀결되고, 이러한 사람들은 애드-온(add-on)들을 관리하게 되고 불량 사이트들의 확인을 계속 갱신하는 일을 한다. 실제로, 이 접근법은 인터넷 기반 음란물의 경고에 대한 시청 규제에 의해 사용되는 것과 동일하다. 경험상 상기 경쟁이 결코 끝나지 않는 것을 보여주며, 뜻밖의 정보에 액세스하기 위한 방법이 항상 존재할 것이다.

[0006] 이러한 문제를 다루려고 한 하나의 종래 기술은, 폴 엘. 올슨(Paul L. Olson)에 의해 2009년 7월 9일자로 발행된, 미국 특허 출원 공개 공보 2009/0177694호에 개시되어 있다. 이 개시내용에 있어서는, 모든 확인된 자격 인증서(credential)들을 저장하기 위한 중앙 저장소가 생성되고, 이때 각각의 자격 인증서는 검사합(checksum)을 포함하도록 형성된다. 특별한 자격 인증서를 살펴 보는 것에 관심 있는 개인은 상기 저장소에 액세스하고, 원하는 자격 인증서를 검색하며 인증을 위해 검사합이 계산되고 제시된다. 일치하면 그에 따라 그 개인에 대한 자격 인증서를 인증하는 것이 고려된다.

[0007] 더욱 일반적인 제2 사이트 인증에 대한 개선이 진행되고 있으나, 누군가가 유사한 방식으로 가짜의 자격 인증서들을 유지하기 위한 "가짜 사이트(faux site)"를 설정하고 유지하기 위해 상기 올슨의 시스템을 구현할 가능성이 잔존한다. 이것이 가능한 하나의 이유는, 원천 기관(originating organization)들(예컨대, 전문적인 협회들, 대학들, 인허가 기구들 등)이 그 인증서의 통제권을 보유하지 않고 상기 저장소로부터 벗어나 있기 때문이다. 또한, 임의 종류의 자격 인증서의 만료가 상기 저장소에 저장된 데이터에 포함되었는지를 나타내지 못한다.

[0008] 2010년 7월 2일자로 출원된 미국 특허 출원 제12/829,550호에서 구현되고 본 명세서에 참고로 통합되는, 상기 발명자에 의한 기술은, 상기 종래 기술의 많은 단점들을 극복한다. 그러나, 후에 상세히 기술되는 바와 같이, 상기 종래 시스템은 자격 인증서에 포함될 수 있는 것으로 생각되는 정보의 "유형(type)"를 제한하지 못하며, 이는 잘못된 이해를 야기할 수 있다.

[0009] 예컨대, 자격인정 기구가 예일 대학교(Yale University)인 경우, 예일이 그 등급(들)을 증명하고 개인에 부여하면 그만이다. 그러나, 예일은 직업 경력, 군대 복무 또는 시민권에 대한 바람직한 정보원으로 고려되지 않는다. 이에 따라, 자격인정 기관에 의해 인증된 정보의 유형도 통제하는 구성의 필요성이 남아있다.

발명의 내용

해결하려는 과제

[0010] 상기 종래 기술의 이들 및 다른 한계점들은 본 발명에 의해 다루어지며, 본 발명은 제2 사이트의 인증을 필요로 하지 않고 자격인정 기관으로부터의 특정되고 한정된 자격 인증서의 온 라인 인증을 제공하는 시스템 및 방법에 관한 것이다

과제의 해결 수단

[0011] 특히, 본 발명은, "회원 증명서"(MC)와 결합하여 "기관 증명서"(OC)의 이용을 통해 독립적인 사람(제3자, 즉, 주장된 회원의 사용자)에 대해 특정한 자격 인증서의 인증을 제공하기 위한 시스템 및 방법을 기술하며, OC의 필드 구조는 발행 기관에 의해 증명될 수 있는 정보의 유형을 제한한다.

[0012] 인증 기관(Certificate Authority; CA)에 의해 발행되는 표준 X.509 인증서들과 유사하게, 본 발명의 방법에 의해 사용되는 OC는 먼저 한 기관을 조사하고 그의 공개 키(public key)을 인증하는 CA에 의해 상기 기관에 대해 발행된다.

[0013] 본 발명에 따르면, 기관 증명서(이후, "OC")는, MC에 내포된 정보가 신뢰할 수 있는 것을 보장하도록 CA에 의해 통제되는 일련의 소정 필드들을 이용하는 것이 제안된다. 상기 OC의 일련의 필드들은 기관의 특정 유형과 관련하여 규정되며, 이때 임의의 관련 없는 정보는 적법한 회원 증명서(이후, "MC")의 일부를 형성하도록 허용되지 않는다. 그에 따라, 특정 필드 기술의 사용에 의해, OC에 있어서 대응하는 <필드(field)> 태그를 갖지 않는 MC에 나타나는 임의의 필드는, 인증 절차 동안 사용자의 브라우저 확장에 의해 MC가 무효로 표시되도록 하는 것으로 가정한다.

[0014] 본 발명의 다른 실시예에 있어서, 각 필드와 관련된 체크들의 수는 하나 이상의 특정 필드들의 속성(attribute)들을 인증하기 위해 확장될 수 있다. 또한, 본 발명에 따라 MC를 인증하는 절차에서 검토되는 "취소된(revoked)" OC의 리스트를 포함할 수 있다.

[0015] 본 발명에 따르면, 고객들이 그들의 웹사이트와 관련하여 그들의 식별의 신뢰할만한 증명을 제시할 수 있는 사람(또는 기관)과 거래하는 것을 고객들(이후 일반적으로 "사용자들"로 지칭)에 보장하도록 프로토콜 및 암호작성법을 이용하는 시스템 및 방법이 제공된다. 상기 시스템은, 인증서의 인증 절차가 굳이 다른(아마도 부도덕한) 웹사이트로부터 정보를 얻을 필요 없이, "현지에서" 수행되도록, 사용자의 브라우저로부터 직접 착수된다. 바람직하게, 인증서가 만료되는 고정 날짜를 생성할 뿐만 아니라, 인증서가 "시효경과(stale)" 되지 않도록 보장하기 위해 OC 및 MC 모두에 만료일이 포함된다.

[0016] 본 발명의 한 양태는, 상기 시스템 및 방법에 의해 제공된 기관 및 회원 증명서들이 위조 또는 도난 당하기 어렵게 하는 것이다. 박식한(즉, 컴퓨터에 정통한) 사용자는 인증서들의 확인을 수동으로 인증하는 것이 가능하겠지만, 본 시스템의 바람직한 실시예는, 사용자의 브라우저에 의해 채용되고 또한 원천 인증 기관(CA)의 공개 키와 결합하여 자격인정 기관과 관련된 공개 키들을 이용하는 새로운 MIME(Multipurpose Internet Mail Extensions) 유형의 생성에 기초한다. 종래 기술과 달리, 상기 자격인정 기관은 회원 증명서의 통제를 유지한다.

[0017] 일 실시예에서, 본 발명은, 주장된 회원의 웹사이트상에 아이콘 또는 하이퍼링크로서 제시된 회원 증명서를 인증하기 위한 컴퓨터 구현 방법을 포함하며, 상기 방법은, 회원 증명서 아이콘을 활성화시키는 단계, 회원 증명서를 생성한 기관과 관련된 기관 증명서(회원을 규정하는 일련의 소정 정보 요소들을 포함하는 기관 증명서)를 검색하는 단계, 상기 회원 증명서에서 제시된 요소들과 상기 기관 증명서를 비교하는 단계, 및 상기 회원 증명서에서 제시된 요소들이 상기 기관 증명서 내의 상기 일련의 소정 정보 요소들과 일치하는 경우 및 경우에만 상기 회원 증명서를 인증한 다음, 상기 기관 증명서에 공개된 공개 키에 대해 회원 증명서의 서명을 인증하기 위한 단계를 포함한다.

[0018] 다른 실시예에서, 본 발명은, 주장된 회원의 웹사이트 상에 아이콘으로서 제시된 회원 증명서를 인증하기 위한 컴퓨터 사용가능 코드를 포함하는 컴퓨터 사용가능 매체를 구비하는 컴퓨터 사용가능 프로그램 제품을 규정하며, 이는, 회원 증명서 아이콘을 활성화시키기 위한 컴퓨터 사용가능한 코드, 회원 증명서를 생성한 기관과 관련된 기관 증명서(회원을 규정하는 일련의 소정 정보 요소들을 포함하는 기관 증명서)를 검색하기 위한 컴퓨터 사용가능한 코드, 상기 회원 증명서에서 제시된 요소들과 상기 기관 증명서를 비교하기 위한 컴퓨터 사용가능한 코드, 및 상기 회원 증명서에서 제시된 요소들이 상기 기관 증명서 내의 상기 일련의 소정 정보 요소들과 일치하는 경우 및 경우에만 상기 회원 증명서를 인증하고, 다음, 상기 기관 증명서에 공개된 공개 키에 대해

회원 증명서의 서명을 인증하기 위한 컴퓨터 사용가능한 코드를 포함한다.

[0019] 또 다른 실시예에서, 본 발명은, 주장된 회원의 웹사이트상에 아이콘으로서 제시된 회원 증명서를 인증하기 위한 시스템을 기술하며, 상기 시스템은, 회원 증명서 아이콘을 활성화시키기 위한 컴퓨터 사용가능한 코드 수단, 회원 증명서를 생성한 기관과 관련된 기관 증명서(회원을 규정하는 일련의 소정 정보 요소들을 포함하는 기관 증명서)를 검색하기 위한 컴퓨터 사용가능한 코드 수단, 상기 회원 증명서에서 제시된 요소들과 상기 기관 증명서를 비교하기 위한 컴퓨터 사용가능한 코드 수단, 및 상기 회원 증명서에서 제시된 요소들이 상기 기관 증명서 내의 상기 일련의 소정 정보 요소들과 일치하는 경우 및 경우에만 상기 회원 증명서를 인증하기 위한 컴퓨터 사용가능한 코드 수단을 포함한다.

[0020] 본 발명의 다른 추가적 양태들 및 실시예들은 첨부 도면을 참조한 이하의 설명으로부터 명백해질 것이다.

도면의 간단한 설명

[0021] 도 1은 본 발명에 따라 형성된 회원 증명서(MC)의 기본 도면이다.

도 2는 예시적 MC의 리스트를 포함한다.

도 3은 본 발명에 따라 형성된 기관 증명서(OC) 및 관련 분야 식별 테이블의 기본 도면이다.

도 4는 예시적 OC의 인증 기관 부분의 리스트를 포함한다.

도 5는 예시적 OC의 기관 식별 부분의 리스트를 포함한다.

도 6은 본 발명의 절차에 사용될 수 있는 분야 식별 테이블의 확장된 유형을 도시한다.

도 7은 OC 및 MC 모두를 구현하는 결합 증명서(CC)의 기본 도면이다.

도 8은 본 발명에 따라, 제시된 MC를 인증하기 위한 예시적 절차의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0022] 이하에 상세히 기술되는 바와 같이, 본 발명은, 회원 증명서(MC)를 생성하기 위한 기관 증명서(OC)를 이용하며 회원 증명서(MC)는, 후에 (개인, 업체, 기업, 등과 같은) "회원"이 참여(자격증 수여) 기관(예컨대, 대학교, 인허가 기관, 전문분야의 기구)과 합법적으로 관련된 것을 인증하기 위해 제3자에 의해 접근될 수 있다. 특히, OC는, 발행 기관에 적절한 정보만 MC 내에 포함될 수 있도록 정보의 유형을 제한하도록 구성된다.

[0023] 본 발명은 특정한 개인 또는 업체(또는 임의의 다른 유형의 개체)가 그들의 웹사이트를 방문할 때 이들의 확인을 인증하도록 일반 사람들에 의해 이용될 것으로 생각된다. 웹사이트는, 실시간으로 인증 절차를 개시하도록 활성화 및 사용될 수 있는 MC 아이콘(또는 하이퍼링크)을 포함한다. 이에 따라, 웹사이트를 방문하는 개인(이후, "사용자"로서 규정)은 "membership"(회원) 아이콘/하이퍼링크를 보고 인증 절차를 행하도록 그 위치상에서 클릭할 것이다. 만약 클릭이 성공적인 경우, 그 절차는 다음, 사용자에 의한 시각적 검사를 위해 인증된 증명서를 표시하고, 만약 그 절차가 어떤 이유로 실패인 경우, "error/failure" (에러/실패) 메시지가 사용자에 표시될 것이다. 사용자의 브라우저는 아마도, 모든 유효한 OC들의 식별을 포함한 인증 절차를 행하기 위해 필요한 애드-온(add-on)을 포함하도록 구성되며, 이때 사용자에 의해 채용되는 시스템의 상세 내용은 본 출원인의 공동 계류중인 출원번호 제12/829,550호에 상세히 기술되어 있고 이 출원은 본 명세서에 참고로 통합된다.

[0024] 도 1은, 본 명세서에서 MC(10)로서 규정되는 예시적 회원 증명서 (Membership Certificate)에 포함되는 정보의 유형을 포함하며, 이는 하이 레벨 다이어그램 포맷으로 나타냈다. MC(10)의 요소들의 순서는 중요하지 않으며 본 발명의 범주를 제한하도록 고려되지 않아야 한다. 도시된 바와 같이, MC(10)는 웹사이트 식별 요소(Website Identification Element; 12)를 포함하며, 이는 이 특정한 MC와 관련된 웹사이트를 규정한다. 웹사이트 정보의 포함에 따라, 부도덕한 자에 의한 MC의 "도난" 및 다른 웹사이트상에 그를 공개하는 것을 방지한다. MC(10)는 또한, 기관 식별 요소(Organization Identification Element; 14)를 포함하며, 이는, 처음에 기관 증명서(OC)를 승인한 인증 기관(CA)에 의해 제공된 "인증(certifying)" 일련 번호를 포함하는 MC를 발행하는 기관을 규정하는 정보를 포함한다. 이하에 간단히 설명되고, 본 출원인의 공동 계류중인 출원에 상세히 기술된 바와 같이, CA는, "요구 기관(requesting organization)"이 진짜로 주장된 자인 지를 확인하는 서류를 제시한다. 다음, 정보는 (상황에 따라, 더 높거나 더 낮은 등급으로) 조사되고, 확인에 따라, CA는 그 요구 기관에 대한 특정한 일련 번호를 OC에 교부하며, 이때 번호는 그의 OC 및 교부된 모든 MC에 포함된다. MC(10)(웹사이트의 개인/업체는 사용자에 의해 방문된다)와 관련된 특정 "회원"의 확인은, MC(10)에 회원 식별 요소(Member Identification

Element; 16)로서 포함된다. 도 1에 도시된 바와 같이, MC(10)의 페이로드부(18)는, 발행 기관이, 특정 분야 태그들로 구성되는, MC(10)에 포함되도록 허용하는 개인에 대해 적절한 특정 정보를 포함한다.

[0025] 도 2는 웹사이트 식별 요소(12)에 대응하는 라인 1을 갖는 MC(10)의 예시적 리스트를 포함한다. 중요한 것은, 리스트의 라인 2가 이와 같은 특정 MC의 만료 날짜를 포함하는 것으로, 이는 상기한 바와 같이, MC의 정보가 "도난"되지 않는 것이 중요하고, 인증된 정보의 확인을 더욱 확실히 하기 위해 만료 날짜가 포함된다. 그 다음의 두 개의 라인들은 기관 식별 요소(14)를 구현하며, 기관 식별 요소는 발행 기관(본 발명에서는 예일 대학교)의 명칭 및 해외 CA에 의해 예일 대학교에 발행된 특정한, 고유의 일련 번호 둘 다를 포함한다. 리스트의 라인 5는, 도 1의 도면에서 요소(16)로서 포함된, MC(10)와 관련된 특정 "회원"의 확인을 포함한다.

[0026] 본 발명에 따르면, 도 2의 리스트의 나머지 필드들은 확실하게 태그를 붙이고 (예컨대, MC(10)의 "페이로드"부(18)과 같은) 발행 기관에 의해 공급되도록 허용되는 상세한 정보를 포함한다. 후에 상세히 기술되는 바와 같이, 필드들의 다른 것들은 다른 특성들을 가지며, 이때 어떤 것들은 일련의 "단일(single)" 정보만 포함할 수 있고, 어떤 것들은 "복수(multiple)" 정보들을 포함할 수 있다. 또한, 어떤 필드들은 "의무적(mandatory)"일 수 있는 반면 다른 어떤 것들은 "선택적 (optional)"일 수 있다. 명백하게, 이들 특성들은 교부되는 MC의 유형에 대해 특정적이며, 이때 대학교는 일련의 필드들 및 특성들을 갖고 AMA와 같은 인허가 기관은 또 하나를 가질 것이다. 실제로, 본 발명의 중요한 양태에서는, 발행 기관에 의해 MC에 공급되는 정보의 유형이 OC 및 MC에서 확인되는 일련의 고정 필드들에 의해 통제된다.

[0027] 상기 공동 계류 출원인 일련 번호 12/829,550호에 기술된 이전의 구성과 비교하여, 기관을 인증하는 것과 관련된 서명된 GPS 키들 및 서명된 X.509 인증서 대신 OC가 사용된다. 일반적으로, OC는 대략적으로는 X.509 인증서에 기초하지만, 몇몇 키의 차이들이 있다. OC는, 표준 X.509 인증서에 포함된 것보다 하나의 기관에 관해 더 많은 정보를 포함한다. 또한, 후에 설명되는 바와 같이, 하나의 OC는, X.509 인증서들에 의해 허용되는 방식에 있어서의 인증 기관 (CA)에 대해 CA을 "연계(chain)"시킬 수 없지만, "루트(root)" CA로 돌아가는 모든 기관에 의해 서명될 필요가 있다.

[0028] 보다 상세히 설명하면, 본 발명의 OC는, (1) 인증 기관(certifying authority)의 확인; (2) 기관(organization; 단체)의 확인; (3) 기관에 의해 제공된 특정 정보를 규정하는 필드 식별; (4) 기관의 공개 키; (5) OC의 유효 기간(예컨대, 만료일)을 포함하는, (상이하게 구현될 수 있는) 일련의 선택된 요소들을 필요로 한다. 도 3은 이들 요소들을 포함하는 예시적 OC(20)를 도시하며, OC(20)는, 주장된 "회원"들의 웹사이트를 보고 있는 사용자에 의한 인증을 위해 제시된 MC를 유효화(또는, 경우에 따라서는 무효화)하도록 사용된다.

[0029] 도 3에 도시된 바와 같이, OC(20)는 상기한 요소들을 특정하는 다수의 별도의 필드들을 포함한다. 특히, OC(20)는, OC를 발행하고 기관에 특유한 일련 번호를 할당하는 "인증 기관"(CA)을 규정하는 제1 필드(22)를 포함한다. OC(20) 내의 다음 필드(24)는 이 인증서가 생성되는 특정 기관을 확인한다. 도 3에 도시된 바와 같이, 필드 식별 포인터(26)가 OC(20)에 포함되고 또한 별도의 필드 식별 테이블(30)에 대한 절차로 진행하는 데에 사용된다. 후에 상세히 기술되는 바와 같이, 필드 식별 테이블(30)은, MC를 생성할 때 한 기관에 의해 채워지는 태그가 붙은 특정 필드를 포함한다. 끝으로, OC(20)는 유효 필드(28)를 포함하며, 이는 발행 기관의 공개 키 및 바람직하게는 OC(20)에 대한 만료 일을 포함한다.

[0030] MC들에 의해 발생된 인허가 및 수입을 적절히 관리하기 위해, OC는 다시 루트 CA로 가는 체인에 있어서 모든 발행인들에 의해 서명될 필요가 있다. 대안적으로, OC는 원천 CA(즉, 체인에 있어서 OC에 "가장 근접한" CA) 및 루트 CA에 의해 서명될 수 있다. 이 양태는 시행될 여러 CA들 간의 상업적 관계를 허용하는 데에 이용된다.

[0031] 이는 예시적으로 도시될 수 있다. CA1은 루트 CA이고, 전 세계적으로 생성된 모든 OC들을 서명하는 것으로 가정한다. CA1은 캐나다의 지역(country)에 대한 기관 증명서를 발행하기 위해 CA2와의 상업적 관계로 진입한다. 또한, CA2는, 온타리오(Ontario)의 지방에 대한 인증서들을 발행하기 위해 CA3와의 관계로 진입한다.

[0032] 만약 토론토 대학교(University of Toronto)가 그의 졸업생들에 대해 MC들을 발행하기 위해 OC를 얻는 것을 원할 경우, CA3과 접촉하도록 진행될 것이다. 후에, CA3은 토론토 대학교를 인증하기 위해 요구되는 실사(due diligence)를 행하고 그 대학교에 대한 OC에 서명한다. 다음, 서명된 OC 및 지원 서류를 그의 서명을 위해 CA에 보내며, 이때 최종 서명을 위해 패키지가 CA1에 보내진다. 이 절차는, 기관 및 상업적 관계들에 대한 질서정연한 회계업무를 조사하기 위한 꾸준한 절차가 존재하도록 한다.

[0033] OC를 처리하는 브라우저 확장은, CA1에 의한 "외측" 서명만 인증할 필요가 있고 - CA2 및 CA3에 의한 "내측" 서명들은 무시될 수 있음을 이해해야 할 것이다(CA1은 이전의 기관들이 조사되고 OC를 승인한 경우에만 발견되는

것으로 가정함). 대안적으로, 브라우저 확장은 모든 CA 공개 키들의 데이터베이스를 유지하고 CA에 포함된 서명의 각 하나를 인증할 수 있다.

[0034] 도 4는 OC(20) 내에 포함된 예시적 CA 필드(22)의 리스트이고, OC(20)의 부분이 X.509 인증서에 있어서의 필드와 유사한 것으로 나타냈다. 이 경우에, 인증 기관으로서 리스트의 라인 5에 "Verify Membership, Inc"가 도시된다. 도 4의 라인 2에 나타낸 일련 번호는 CA의 식별 번호로 시작한다. 이 특정 실시예에서, 번호 00:00이 도시되고 "root"로서 규정되어 있는데, 그 이유는 "issuer_parent"와 동일하기 때문이다. 본 발명의 인증 시스템은 단일 루트 기관, 또는 사업 결정 및 효율적인 운영에 의해 관리되는 다수의 루트들을 이용할 수 있다. 도 4에 도시된 바와 같이, CA는, 특정 MC를 인증할 때 관련되는 사용자가 모든 필요한 정보에 대해 액세스할 수 있도록 하기 위해, OC(20)의 이 부분에 광범위한 접촉 정보를 포함한다. 도 4에 도시된 특정 실시예에서, "인증 레벨(verification level)"의 표시는 OC(20)의 부분에 있어서 라인 10에 포함되고 그 기관의 신원 및 그의 경력을 결정하기 위한 CA에 의해 수행되는 조사의 범위를 나타낸다. 이러한 "레벨(level)" 정보의 포함에 의해, 그들의 MC에 있어서의 기관에 의해 궁극적으로 공급되는 정보에 있어서 고위 및 하위 레벨들의 진실을 허용한다.

[0035] 도 5는 "기관(organization)" 예일 대학교(단지 설명의 편의를 위한 것임)에 대한 경우에, OC(20)의 기관 식별 필드(Organization ID filed; 24)에 대한 예시적 리스트를 포함한다. 이 리스트는, 주소, 전화 및 웹사이트 정보와 같은 예일 대학교에 대한 각종 상세 내역들을 포함하는 것으로 나타난다. 상기한 바와 같이, 본 발명에 따라 구성되는 특정 OC는 표준 X.509 인증서보다 더욱 상세하게 발행 기관을 확인한다. 그 결과, 특정 MC를 보는 사용자 역시, 우선 먼저 MC를 발행한 기관과 관련된 임의의 필요한 배경 정보에 대한 공유가 허용된다.

[0036] 본 발명의 중요한 양태는 특정 기관에 의해 "인증"될 수 있는 정보의 유형의 통제이다. 교육 기관의 경우에, 정보 유형은 대학 입학 허가 및 졸업일자, 수여된 학위, 표창 등에 제한된다. 한 기관이 MC에 대해 "인증"하도록 허용되는 정보의 유형에 대한 이와 같은 통제를 제공하기 위해, OC는 도 3에 도시된 바와 같이 필드 식별 테이블(30)을 이용하며, 이는, 기관에 의해 발행되는 MC에 포함될 수 있는 특정된 일련의 제한된 기술자(descriptor)들을 포함한다. 명백하게, 제시된 MC를 인증하는 절차 동안 조사되는 특정 테이블이 명명되지 않은 임의의 필드들을 포함하는 경우, OC(20)는 무효로서 거절된다.

[0037] 도 3을 참조하면, 필드 식별 테이블(field identification table)(30)이 대학교(또는 임의의 유형의 교육 기관)와 관련된 정보를 포함하는 것이 명백하다. 본 발명에 따르면, 다른 유형의 기관들이, 그 기관에 있어서의 회원을 확인하기 위해 적절한 정보를 규정하는 테이블에 있어서 상이한, 일련의 특정 필드들을 이용하는 것을 이해해야 한다. 예컨대, 미국 적십자 사(American Red Cross)와 관련된 OC는, "회원"의 혈액 유형만 확인하고 아마도, 그 회원이 마지막으로 헌혈한 때를 확인하는 필드 리스트 식별 테이블을 이용할 수도 있다.

[0038] 상기 테이블(30)을 참조하면, 다수의 특정 필드들이 도시되어 있고, 각각의 필드 역시 그 필드를 규정하는 일련의 특정한 특성들을 포함한다. 도시된 바와 같이, 제1 필드(32)는 이 테이블에 대한 질의가 유래하는 특정 OC와 관련된 특정 "기관"을 규정한다. 이 경우에, "컨텐츠 특성(contents property)"(34)은 "예일 대학교"로서 도시된다(이때, 명백히, 이것이 원천 OC에 있어서의 기관 정의와 일치하지 않은 경우, 절차는 중단되고 OC는 무효로 간주된다). 이 필드는 바람직하게는, "고정된(fixed)" 엔트리로서 테이블에 규정되고, 이는 항상 요구되는 필드이고 테이블에 한 번만 나타날 수 있다. 명백히, 인증 기관의 확인이 이 정보의 유형이다.

[0039] 계속해서, 필드 식별 테이블(30)의 회원(member) 필드(40)는 MC를 요구하는 특정 "회원"을 확인한다. 회원 필드(40)는, "required/optional" 인디케이터(indicator)(36) 및 "single/multiple" 인디케이터(38)를 포함하여 규정되는 두 개의 특성들을 포함한다. 인디케이터(36) 내의 "required/optional"표시는, 발행된 MC에 포함되어야 하는 정보를 규정하며, MC의 인증 시 "누락(missing)"이 있으면, 사용자의 브라우저는 에러 메시지를 생성할 것이다(또한 사용자는 요청된 MC가 위조 또는 잘못 생성된 것으로 추정할 수 있다). 이와 유사하게, 인디케이터(38) 내의 "single" 표시는, 이 특정 필드의 단 하나의 예만 MC에 포함될 수 있음을 의미한다(상기에서 "single" 역시 "required"로 규정되지 않은 경우 이 필드가 "누락"되도록 한다). 만약 복수의 엔트리들을 포함할 경우, 인증 절차를 실행하는 사용자의 브라우저는 재차 에러 메시지를 발할 것이다. 명백히, MC와 관련된 "회원"의 확인은 *required*(필수)이면서 또한 *single*(단일)이어야 한다. (이 실시예에서 "제임스 토마스(James Thomas)"로 나타낸) 회원의 이름은 필드들의 컨텐츠 부에 포함된다.

[0040] 인증서의 만료는 필드(42)에 포함되고(다시, "required", "single") 또한 MC가 나타날 때 웹사이트는 필드(44)에 포함된다("required", "single"). 기관의 유형에 관계없이, 이들 제1의 4개의 필드들은 (아마도, 테이블 내에 다른 위치들 및 다른 순서로) 대부분의 발행 인증서에 포함될 것이다.

[0041] 테이블(30)에 나타낸 다음 필드들은 OC로서 대학교를 갖는 특정 항목들에 적절하다. 도시된 바와 같이, 필드(46)은 개인이 등록한 날짜를 특정하고("required", "single") 이어서 필드(48)에서 개인의 졸업 일자를 특정한다. 한 교육 기관에 등록하는 모든 사람들이 졸업하는 것은 아니기 때문에, 이 필드는 식별자(identifier)(46)으로 나타낸 바와 같이 "선택적(optional)"이다(반면에 이는 식별자(48)에 "single" 표시를 유지한다). 이 특정 테이블에서 별도의 필드(50)는 표시 "withdrew(철회)"를 수반하며, 이 정보가 인증서에 포함되도록 한다. 필드(52)는 수여된 학위(들)(("optional(선택적)" 및 "multiple(복수)")), 및 인디케이터(56 및 58)에 의해 "optional(선택적)" 및 "multiple(복수)"로 각각 규정된 ("표창들(honors)"을 갖는) 필드(54)에 나타낸 바와 같이 임의의 특정 표창들을 규정한다.

[0042] 상기 필드 식별 테이블(30)에 나타낸 바와 같은 필드들의 리스트는 단지 예시적일 뿐이고, 다른 것들도 포함될 수 있다. 그러나, 어떤 경우에도 교육 기관은 "고용 상태", "시민권", "군대 복무 기록"들과 같은 임의 유형의 정보들을 인증하도록 허용되지 않으며, 항목들은 모두 다른 기관에 의해 더욱 양호하게 인증된다. 이에 따라, 본 발명에 의하면, 예일 대학교와 같은 OC에 의해 발행되는 MC는 개개인의 교육적 인증서와 관련된 정보만을 포함하도록 한정될 것이다. 이와 유사하게, 기업과 같은 OC에 의해 발행된 MC는 근무 경력에만 한정되고, 미국 공군과 같은 OC에 의해 발행된 MC는 군대 복무 등에만 한정된다. 고려된 CA의 조사 절차의 일부는, MC에 포함될 특정 필드에 대해 결정하도록 그 기관과 함께 작업하는 것을 포함한다. 이 절차의 채용이 광범위하게 될 경우, 단과대학 또는 대학교는 학위의 수여를 확인하도록 발행된 MC에 있어서 필드들의 표준 리스트를 승인하며, 이에 따라 다른 자동적인 절차가 실시될 수 있게 된다.

[0043] 본 발명에 의하면, 컨텐츠를 인증하기 위해 테이블(30)에 부가적인 체크사항들을 생성할 수도 있다. 예를 들면, 테이블(30)의 특정 배치에 있어서, "graduated(졸업)" 필드(48) 및 "withdrew(철회)" 필드(50) 모두 "true (진실)"이어서는 안되며, 이들은 오직 하나만 존재하는 선택사항으로 되도록 예정된다. 이 유형의 에러가 테이블에 진입하지 않도록 하기 위해 권한 체크(semantic check)가 적용될 수 있다. 부가적 또는 대안적으로, 다른 필드들이 포함될 수 있으며("최종 상태"로 규정됨) *withdrew, transferred, graduated, expelled, current_student* 값들의 드롭 메뉴로부터 선택된 값을 갖는다.

[0044] 다시 도 2에 도시된 바와 같이 MC(10)와 관련된 특정 리스트를 참조하면, MC(10)는, <matriculated(대학입학 허가)2> 및 <graduated(졸업)2>에 부가하여, 선택적 필드로서 <degree(학위)2>을 포함한다. 명백히, 이는 MC가, 임의의 사항이 <degree(학위)2> 필드에 들어가지 않고 <matriculated(대학입학 허가)2>에 정보를 포함하도록 생성되게 하는데, 이는 무의미한 유형의 증명서이다. 이 문제를 피하기 위해, 필드 식별 테이블은 두 개의 부가적인 인디케이터들, 즉 "requires" 및 "produces"을 포함하도록 보강된다. 도 6은, 공급된 정보가 유효한 것을 보장하도록 이들 인디케이터들을 이용하는 예시적인 필드 식별 테이블(50)의 일부를 포함한다.

[0045] 적시된 바와 같이, 테이블(50)은 예비적이다. 이는, <degree2>가 <matriculated2> 및 <graduated2> 모두에 대해 정보를 발하는 것을 보여주며, 이는 <matriculated2>가 <degree2>를 *필요로 하는(requires)* 것과 같다. 설명의 편의를 위해, 테이블은, 제2 테이블이 "required/optional, "single/multiple"인지 다른 필드를 *필요로 하는(requires)* 필드가 허용가능하게 되도록 구성될 수 있다. MC를 인증하는 브라우저 확장에 의해, 제2 필드와 당면했을 때 제1 필드의 일례가 증명서에 있는 것을 간단히 체크한다. 이는 증명서의 두 개의 판독을 필요로 한다. 재1 패스는 그 인증서에 있는 필드들을 확인하고, 제2 패스는 *requires* 및 *produces* 인디케이터들에 의해 특정된 조건들이 충족되는 것을 인증한다.

[0046] 각각의 OC는 발행 기관 및 CA 모두에 대한 접촉 정보를 포함하기 때문에, 임의의 오류에 대한 디폴트 액션은 대응하는 MC를 인증할 때 사용하기 위한 OC를 거절하는 것이다(또한 그 OC에 의해 서명된 모든 MC들이 거절되도록 한다). 처리 소프트웨어는 브라우저 확장과 매우 유사하고, OC의 사용자가 이들 개체의 하나 이상과 접하는 것을 제시할 수 있다. 전형적인 에러들은, 이들에 한정되지 않지만, 만료된 서명 키, 불량한 서명, 일치되지 않은 시작 및 끝의 태그들, 의무적 태그들의 누락, 제공된 태그가 필드 기술자에 포함되지 않은 것, 및 "single(단일)"로서 규정된 필드에 "multi(복수)" 유형의 데이터의 포함을 들 수 있다.

[0047] 만약 웹사이트가 MC를 포함하는 경우, MC를 인증하려고 시도하는 개인 역시 대응하는 OC를 얻을 필요가 있다. 이에 대한 하나의 해법은 모든 현재의 OC들을 저장하는 웹사이트를 유지하는 것이다. 사용자의 기계에 있어서의 브라우저 확장 또는 플러그-인은, 안티-바이러스 프로그램이 주기적으로, 정기적으로 바이러스 서명을 다운로드하는 것과 거의 동일한 방식으로 OC 웹사이트에 액세스할 수 있다.

[0048] 대안적으로, OC 및 MC는, 회원의 웹사이트에 위치되는, 결합 증명서(Combined Certificate: CC)로 불리는 단일 패키지로 결합될 수 있다. 도 7은 예시적 CC(60)를 도시하며, 이는 OC(20)와 MC(10) 사이의 구분을 나타내기 위

해 사용되는 특정한 구분기호를 포함한다. 도시된 바와 같이, CC(60)는, 기관의 개인 키(private key)로 서명되고 OC(20)는 CA의 개인 키로 서명된다.

[0049] 도 7에 도시된 바와 같이 특정한 CC를 사용하여 MC에 액세스하고 인증하는 것과 관련된 특정 절차 흐름이 도 8의 흐름도에 포함된다. 일반적으로, 상기 절차는 먼저 CC(60) 내의 OC(20)를 분리하도록 진행하고, 다음 MC(10)를 추출하고 OC(20)에 대해 그의 컨텐츠를 인증한다.

[0050] 도 8의 흐름도를 참조하면, 그 절차는 OC(20)의 서명 인증에 따라 시작된다(단계 100). 브라우저 확장은, OC(20)의 서명을 인증하기 위해 사용될 수 있는 초기의 일련의 CA 공개 키들을 포함한다. 만약 CA 서명이 이들 키 중 하나에 대해 올바르면, OC(20)는 유효(정당)한 것으로 고려되고, 기관 공개 키가 OC(20)로부터 추출된다(단계 110). 그렇지 않은 경우, 절차는 사용자의 브라우저에 의해 정지되고 "error(에러)"가 기록된다(단계 120). 일단 에러가 기록되면, OC(20) 및 MC(10) 모두에 포함된 정보는 무효인 것으로 고려되고 웹 브라우저에 의해 사용자에 표시되지 않는다. 대신에, 사용자에게, CA 키들과 함께 문제들의 결과로서 CC(60)가 유효하지 않다는 것이 통지된다. 정확한 CA 공개 키를 발견하는 것에 대한 실패에 따라, CA 공개 키들의 캐시에 대한 갱신을 위한 원격 조사를 개시하는 것을 가능하게 하며(단계 130), 만약 키가 발견된 경우에는, 절차는 단계 140으로 이동한다.

[0051] 어떤 경우에도, 일단 OC 공개 키가 추출되면, OC(20)의 만료 일자가 현재 시간 및 날짜에 대해 체크된다(단계 140). 만약 기간이 경과된 경우(또는 아직 시작되지 않은 경우), 에러가 기록되고(단계 150) 처리가 중단되며, 이때 에러 메시지 외에 사용자에 대해 표시되는 정보는 없다. 공개 키가 유효한 것으로 추정되면, 그는 CC(60)의 서명을 인증하도록 사용된다(단계 160). 다시, 인증되지 않은 경우, 절차는 에러 메시지와 함께 중단된다(단계 170). CC(60)의 서명이 유효한 것으로 추정되면, 그 절차의 다음 단계(단계 180)가 CC(60)로부터 MC(10)를 추출하도록 진행하고 <website>가 CC(60)에 나타낸 위치(URL)에 대해 체크된다(단계 190). 만약 일치되지 않으면, 절차는 종료된다(단계 200). 기관에는, 이 포인트에서 부도덕한 개인이 다른 개인을 위해 생성된 회원 증명서를 사용하는 것을 시도하고 있음을 통지될 수 있다.

[0052] <website>가 CC와 일치하는 것으로 추정되면, OC(20)에서의 포인터(26)가 MC(10) 내의 필드들에 액세스하기 위해 사용되고(단계 210), MC(10) 내의 필드들이 필드 식별 테이블(30)에 대해 체크되고(단계 220), 단계 230에서 비교 동작을 행한다. 만약 필드들이 적절히 덧붙여지지 않으면(예컨대, "required" 필드들이 누락되고, "single" 필드들이 "multiple" 표시를 갖는 경우), 또는 권한 체크들이 "true"가 아니거나 MC가 테이블(30)에 있어서 특정되지 않은 정보의 포함을 시도하는 경우, 절차는 종료되고(단계 240) 사용자에 대해 리뷰에 의한 MC가 유효하지 않은 것이 "경고된다(warmed)". 그렇지 않은 경우, 절차는 CC(60) 그 자체의 만료 날짜를 체크함으로써 계속 진행한다(단계 250).

[0053] 하기에 기술한 바와 같이, MC(10)의 유효성을 더 보장하기 위해 다른 체크들(단계 260)이 상기 절차에 부가될 수 있다. 일단 모든 테스트들이 완료되면, MC(10)의 컨텐츠는 사용자가 보는 동안 표시되고(단계 270), 인증서의 특정 특성들의 시각적 확인을 제공한다(웹사이트 소유자가 예일 대학교의 졸업생이라는 것의 확인).

[0054] 특히, 사용자의 브라우저가 "history"를 질의하는 것을 지원할 경우, "previous page"가 MC에 포함된 <website>에 대응한다는 것이 체크될 수 있다. MC의 인증을 더 제어하기 위해, "playback attacks"를 피하도록 사용되고 사용자의 브라우저에 대해 국부적인, 국부적으로 선택되는(즉, "secret") 컬러에 있어서 국부적으로 알려진(즉, "secret") 비밀 문장을 포함하도록 구성될 수도 있다. 이 문장 없이, 불량 웹사이트는 단순히, 제공된 MC의 인증과 유사한 것 같이 보이는 웹 페이지를 제공할 수 있다. 따라서, "secret color"로 인쇄된 "secret phrase"가 인증서를 체크하는 절차에서 나타나지 않는 한, 사용자는 어떤 사람이 그에게 가짜 인증의 제공을 시도하고 있다는 것을 알 것이다.

[0055] 또한, 인증 절차 시 취소된 OC의 "check(체크)"를 포함하도록 할 수도 있다. 예를 들면, CA는, 특정 기관의 OC를 취소하도록 원할 수 있다. 그 경우에, CA는 "불량" 기관에 의해 발생된 모든 MC들이 무효로 되도록 보장되는 것을 원한다. 이 경우에, 사용자 브라우저 확장은 그의 인증 취소 리스트(CRL)에 대해 CA에 질의한다. OC는 초기/발행 CA로부터 루트(root)로 (복수의 CA들이 존재하는 경우) CA들의 체인을 리커싱(recursing up)함으로써 체크될 수도 있다. 이는, "불량" CA에 의해 발행된 모든 OC들이 즉시 취소될 수 있도록 한다.

[0056] 현재의 절차와 관련된 특정 OC가 리스트 상에 없는 경우, 확장은 특정 MC가 취소되었는지를 판단하도록 기관 그 자체를 질의할 수 있다. 이는, X.509 인증서와 같은 MC들이 특정 ID로 발행되는 것을 요구한다. 어떤 경우에도, 브라우저 확장은 에러 기록 기구를 사용하여 발행 기관에 대해 (MC에 기초하여) 취소된 CC의 사용을 기록할 수

있다. 이는, 발행 기관이, 웹사이트의 소유자를 추적하여 CC가 제거된 것을 주장할 수 있도록 한다.

[0057] 상술한 블록도의 구성요소들 및 흐름도의 단계들은 단지 예시적일 뿐이다. 이 구성요소들 및 단계들은 본 발명을 명확히 하기 위해 선택된 것으로 도시된 실시예들에 한정되지 않는다. 예컨대, 상기 도시된 실시예들의 범주로부터 벗어남이 없이, 특정 구현 예는, 상기 구성요소들 및 단계들을, 결합, 생략, 더 세분, 변경, 증가, 감소시키거나 또는 다른 유형으로 실시할 수도 있다. 더욱이, 상술한 절차들의 단계들은 상기 도시된 실시예들의 범주 내에서 다른 순서로 행해질 수도 있다.

[0058] 이에 따라, 본 발명에 따른 기관 증명서 및 회원 증명서들의 사용을 인증 및 시행하기 위해 컴퓨터 구현 방법, 장치 및 컴퓨터 프로그램 제품이 도시된 실시예들에 제공된다. 본 발명은 전체적인 하드웨어 실시예, 전체적인 소프트웨어 실시예, 또는 하드웨어 및 소프트웨어 요소들을 포함하는 실시예의 유형을 취할 수 있다. 바람직한 실시예들에 있어서, 본 발명은, 이에 한정되지 않으나, 펌웨어, 레지던트 소프트웨어 또는 마이크로코드를 포함하는 소프트웨어로 구현된다.

[0059] 또한, 본 발명은, 컴퓨터 또는 임의의 명령 실행 시스템에 의해 또는 그와 관련하여 사용하기 위한 프로그램 코드를 제공하는 컴퓨터 사용가능 또는 컴퓨터 판독가능 매체로부터 액세스 가능한 컴퓨터 프로그램 제품의 유형을 취할 수 있다. 본 발명의 목적을 위해, 컴퓨터 사용가능 또는 컴퓨터 판독가능 매체는 명령 실행 시스템, 장치 또는 디바이스에 의해 또는 그와 관련하여 사용하기 위한 프로그램을 내장, 저장, 통신, 확산 또는 전송할 수 있는 임의의 탠저블 장치로 될 수 있다.

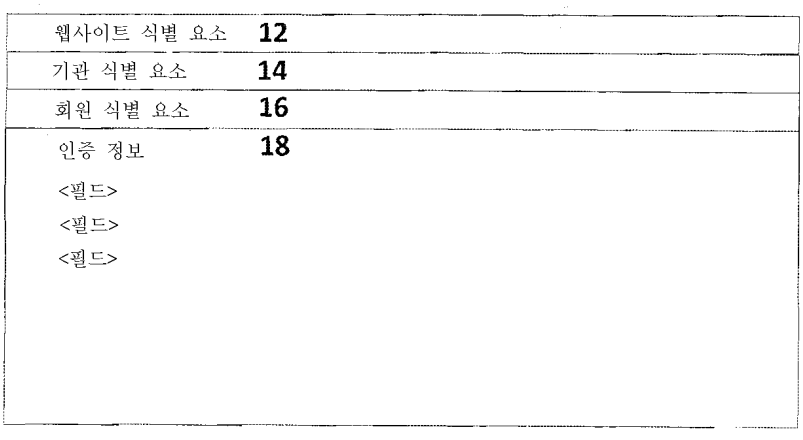
[0060] 상기 매체는, 전자(electronic), 자기(magnetic), 광학, 전자기(electro-magnetic), 적외선, 또는 반도체 시스템(또는 장치 또는 디바이스)일 수 있다. 컴퓨터 판독가능 매체의 예를 들면, 반도체 또는 솔리드 스테이트 구성요소, 자기 테이프, RAM(random access memory), ROM(read-only memory), 강체 자기 디스크 및 광학 디스크를 포함한다. 광학 디스크들의 예를 들면, CD-ROM(compact disk-read only memory), CD-R/W(compact disk-read/write) 및 DVD를 포함한다.

[0061] 또한, 컴퓨터 저장 매체는 컴퓨터 판독가능 프로그램 코드를 내장 또는 저장하여, 컴퓨터 판독가능 프로그램 코드가 컴퓨터 상에서 실행될 때 이 컴퓨터 판독가능 프로그램 코드의 실행에 의해 컴퓨터가 통신 링크를 통해 다른 컴퓨터 판독가능 프로그램 코드를 전송하도록 한다. 통신 링크는, 예컨대, 제한 없이, 물리적 또는 무선으로 이루어지는 매체를 사용할 수도 있다.

[0062] 본 발명의 상기 설명은 예시 및 기술의 목적으로 제시되었으며, 기재된 형태로 본 발명을 완벽하게 하고자 하거나 또는 제한하고자 의도하지 않는다. 당업자들에 의해서는 수많은 변경 또는 변형 예들이 명백히 가능할 것이다. 상기 실시예들은, 본 발명의 원리 및 실제 응용을 설명하기 위해, 또한 고려되는 특정 용도에 적합한 많은 변형 예들을 갖는 각종 실시예들에 대해 다른 당업자들이 본 발명을 이해할 수 있도록 하기 위해 선택되고 기술된 것이다.

도면

도면1



회원 증명서 (MC) 10

도면2

```
<website>www.james_taylor.com</website>                    12
<expires>12-31-2012</expires>
<organization>Yale University</organization>
<OC>00:00:A3:DA:42:7E:A4:B1:AE:DA</OC>                     } 14
<member>James Taylor</member>                              16
<degree>Bachelor of Arts</degree>
<matriculated1>9-2000</matriculated1>
<graduated>6-2004</graduated>
<honors>Undergraduate Leadership Medal</honors>
<honors>Cum Laude</honors>
<honors>Lacrosse Letter 2003, 2004</honors>                } 18
<major>English</major>
<major>Visual Arts</major>
<degree2>Master of Fine Arts</degree2>
<matriculated2>9-2000</matriculated2>
<graduated2>6-2004</graduated2>
<major2>Sculpture</major2>
<minor2>Web Design</minor2>
<comment>You may contact the registrar at 203-234-5678 for any additional information about the
student. Our offices are open 9 AM to 4 PM Eastern time</comment>
```

도면3

기관 증명서 (OC) 20

필드명	샘플 컨텐츠
인증기관	AmbiTrust_CA (22)
일련 번호	MCA1234567890
기관	예일 대학교 (24)
필드 리스트	필드 리스트 테이블에 링크 (26)
만료	12-31-2011
서명 키 알고리즘	RSA
키	키의 ASCII 표시
서명 알고리즘	RSA 암호화를 갖는 SHA-1
서명	서명의 ASCII 표시
지문들	이것은 X.509 인증서들에 제공될 수 있음

(31)

필드 식별 테이블 30

	필드명	고정(F)	필요(R)/선택(O)	단일(S)/복수(M)	샘플 컨텐츠
32	기관	F	36	38	예일 대학교 (34)
40	회원		R	S	제임스 테일스
42	만료		R	S	12-31-2011
44	웹사이트		R	S	www.thomaslaw.com
46	등록일		R	S	8-1996
48	졸업일		O	S	5-2000
50	회회		O	S	----
52	학위		O	M	BA
54	표창		O	M	CUM LAUDE

도면4

CA 필드 22

```
<OC_version>1</OC_version>
<OC_serial_number>00:00:A3:DA:42:7E:A4:B1:AE:DA</OC_serial_number>
<issuer_number>00:00</issuer_number>
<issuer_parent>00:00</issuer_parent>
<issuer>Verify Membership Inc.</issuer>
<issuer_URL>verify-membership.com</issuer_URL>
<issuer_phone_number>1-845-555-1212</issuer_phone_number>
<issuer_email>OC_information@verify-membership.com</issuer_email>
<issuer_signature_algorithm>PGP</issuer_signature_algorithm>
<certificate_verification_level>1</certificate_verification_level>
<issuer_CRL_URL>www.verify-membership.com/CRL</issuer_CRL_URL>
```

도면5

기관 ID 필드 24

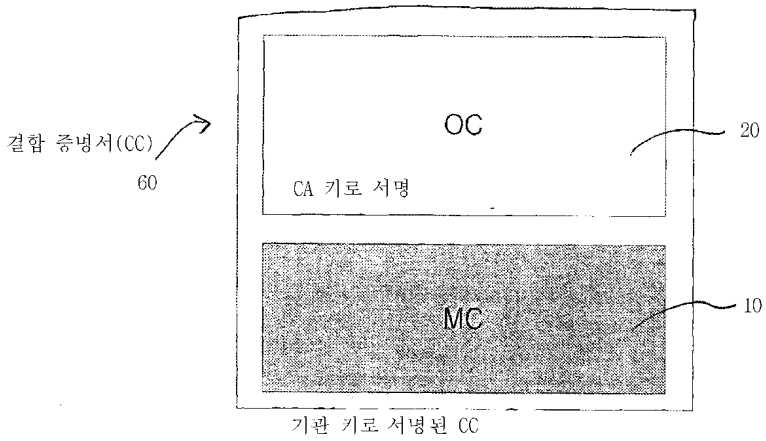
<organization>Yale University</organization>
<Sub_organization>Yale College</Sub_organization>
<organization_common_name>Yale</organization_common_name>
<organization_street_address>123 Elm Street, New Haven, Ct</organization_street_address>
<organization_country>USA</organization_country>
<organization_telephone>1-203-555-1212</organization_telephone>
<organization_website>www.yale.edu</organization_website>
<organization_industry>Higher Education</organization_industry>
<organization_CRL_URL>www.yale.edu/registrar/CRL</organization_CRL_URL>

도면6

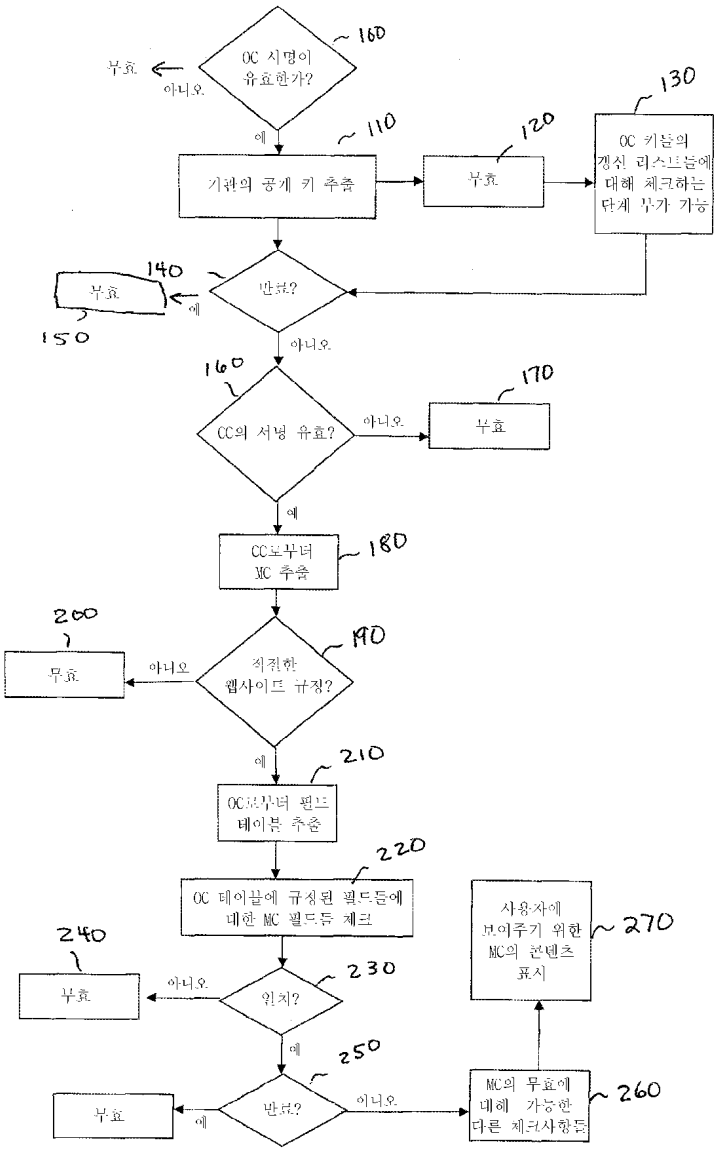
50

이름	필요(R)/선택(O)	단일(S)/복수(M)	요구를	생산물를
학위2	O	S	학위	대학입학허가2, 졸업2
대학입학허가2	O	S	학위2	
졸업2	O	S	학위2	

도면7



도면8


OC 서명이 유효한가?
160
부효
아니오
예
기관의 공개 키 추출
110
부효
120
OC 키들의 갱신 리스트들에 대해 체크하는 단계 부가 가능
130
만료?
140
부효
150
예
아니오
CC의 서명 유효?
160
아니오
부효
170
예
CC로부터 MC 추출
180
적절한 웹사이트 규정?
190
부효
200
아니오
예
OC로부터 펀드 테이블 추출
210
OC 테이블에 규정된 필드들에 대한 MC 필드들 체크
220
위치?
230
부효
240
아니오
예
만료?
250
부효
예
아니오
MC의 무효에 대해 가능한 다른 제어사항들
260
사용자에 보이주기 위한 MC의 콘텐츠 표시
270