(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
G06F 17/60

(11) 공개번호 특2000-0076682
(43) 공개일자 2000년12월26일

(21) 출원번호 10-2000-0007502
(22) 출원일자 2000년02월17일
(30) 우선권주장 1999-39080 1999년02월17일 일본(JP)
1999-247457 1999년09월01일 일본(JP)
(71) 출원인 니폰 덴신 덴와 가부시끼가이샤 타카시 사와이
일본 도쿄 치요다쿠 오테마치 2쵸메 3-1 (우편번호:100-8116)
(72) 발명자 데라다,마사유키
일본도쿄신주쿠구니시-신주쿠3쵸우메20-2니폰덴신덴와가부시끼가이샤(내)
후지무라,고
일본도쿄신주쿠구니시-신주쿠3쵸우메20-2니폰덴신덴와가부시끼가이샤(내)
구노,히로시
일본도쿄신주쿠구니시-신주쿠3쵸우메20-2니폰덴신덴와가부시끼가이샤(내)
하나다테,마사유키
일본도쿄신주쿠구니시-신주쿠3쵸우메20-2니폰덴신덴와가부시끼가이샤(내)
(74) 대리인 남상선

심사청구 : 있음

(54) 원본 데이터 유통 방법, 시스템, 장치 및 컴퓨터 판독가능매체

요약

본 발명은 디지털 정보가 제공되는 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템에 관한 것이다. 원본 데이터 유통 시스템은 발행자 장치, 이용자 장치 및 개찰자 장치를 포함한다. 발행자 장치는 발행자 장치에 대응하는 제 1정보 및 데이터에 대응하는 제 2정보를 포함하는 원본성 정보를 발생시키며, 원본성 정보를 전송한다. 이용자 장치는 원본성 정보의 소스 장치의 유효성을 검증하고 유효성이 검증될 때 원본성 정보를 저장한다. 개찰자 장치는 원본성 정보의 소스 장치의 유효성을 검증하며 유효성이 검증될 때 제 2정보에 대응하는 데이터를 처리한다.

대표도

도1

명세서

도면의 간단한 설명

도 1은 본 발명의 제 1 실시예에 따른 원리를 설명하기 위한 블록도이다.

도 2는 본 발명의 제 1 실시예에 따른 데이터 저장 시스템의 블록도이다.

도 3은 본 발명의 제 1 실시예에 따른 데이터 저장 시스템의 발행자 장치에 대한 블록도이다.

도 4는 본 발명의 제 1 실시예에 따른 데이터 저장 시스템의 이용자 장치에 대한 블록도이다.

도 5는 본 발명의 제 1 실시예에 따른 데이터 저장 장치의 개찰자 장치에 대한 블록도이다.

도 6은 본 발명의 제 1 실시예에 따른 데이터 저장 장치의 접속 장치에 대한 블록도이다.

도 7은 본 발명의 제 1 실시예에 따른 데이터 저장 장치의 티켓 발행 처리를 도시한 시퀀스 챠트이다.

도 8은 본 발명의 제 1 실시예에 따른 데이터 저장 장치에서의 티켓 양도 처리를 도시한 시퀀스 챠트이다.

도 9는 본 발명의 제 1 실시예에 따른 데이터 저장 장치에서의 티켓 양도 처리를 도시한 시퀀스 챠트이다.

도 10은 본 발명의 제 1 실시예에 따른 데이터 저장 장치에서의 티켓 소비 처리를 도시한 시퀀스 챠트이

다.

도 11은 본 발명의 제 2 실시예에 따른 원리를 설명하기 위한 블록도이다.

도 12a 및 도 12b는 본 발명의 제 2 실시예에 따른 원본 데이터 유통 시스템의 데이터 저장 시스템에 대한 블록도이다.

도 13은 본 발명의 제 2 실시예에 따른 원본 데이터 유통 시스템의 발행자 장치에 대한 블록도이다.

도 14는 본 발명의 제 2 실시예에 따른 원본 데이터 유통 시스템의 이용자 장치에 대한 블록도이다.

도 15는 본 발명의 제 2 실시예에 따른 원본 데이터 유통 시스템의 개찰자 장치에 대한 블록도이다.

도 16은 본 발명의 제 2 실시예에 따른 원본 데이터 유통 시스템의 접속 장치에 대한 블록도이다.

도 17은 본 발명의 제 2 실시예에 따른 원본 데이터 유통 시스템에서의 티켓 발행 처리를 도시한 시퀀스 챠트이다.

도 18은 본 발명의 제 2 실시예에 따른 원본 데이터 유통 시스템에서의 티켓 양도 처리를 도시한 시퀀스 챠트이다.

도 19는 본 발명의 제 2 실시예에 따른 원본 데이터 유통 시스템에서의 티켓 양도 처리를 도시한 시퀀스 챠트이다.

도 20은 본 발명의 제 2 실시예에 따른 원본 데이터 유통 시스템에서의 티켓 소비 처리를 도시한 시퀀스 챠트이다.

도 21은 컴퓨터의 구조를 도시한 블록도이다.

도면의 주요부분에 대한 부호 설명

1: 발행자 장치 2: 이용자 장치

3: 개찰자 장치 4: 접속장치

11: 제어부 12: 서명부

13: 데이터 생성부 14: 매니페스트 생성부

15: 신임 정보 생성부 21: 제어부

22: 저장부 23: 제어부

24: 인증부 25: 서명부

26: 번호 생성부 27: 저장부

31: 제어부 32: 인증부

33: 번호 생성부 34: 저장부

41: 통신부 100: 발행자 장치

110: 제어부 120: 서명부

130: 데이터 생성부 140: 토큰 생성부

150: 신임 정보 생성부 200: 이용자 장치

210: 제어부 220: 저장부

230: 제어부 240: 인증부

250: 서명부 260: 번호 생성부

270: 저장부 280: 부정조작 방지 디바이스

300: 개찰자 장치 310: 제어부

320: 인증부 330: 번호 생성부

340: 저장부

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 원본 데이터 유통 방법, 시스템, 장치 및 컴퓨터 판독가능 매체에 관한 것이다. 특히, 본 발명은 디지털 권리, 디지털 콘텐츠 등을 나타내는 디지털 티켓과 같은 데이터를 저장하고 배포하는 기술을 제공하는 것에 관한 것이며, 여기서 상기와 같은 데이터의 유효한 복제 수가 한정된 수보다 적어야 한다.

디지털 권리를 나타내는 데이터 또는 디지털 티켓의 복제는 데이터 배포자가 의도한 수를 초과하는 것이 방지되어야 한다. 즉, 불법적인 이용자에 의하여 복제된 배포 데이터는 방지되어야 한다.

통성적으로, 상기와 같은 다중 사용은 다음에 설명된 기술에 의하여 방지된다.

첫 번째 방법은 원본 데이터의 양도 이력이 데이터에 부착되고 이들은 권리 행사를 요구할 때 데이터가 이미 사용되었는지를 판정하기 위하여 이용된다. 권리가 이미 사용되었다면, 데이터에 대한 서비스 제공자(또는 개찰자)는 데이터에 표시된 권리를 허용하는 것을 거부하도록 하는 것이다.

두 번째 방법은 부정조작 방지 디바이스에 데이터를 저장하여 부정조작 방지 디바이스를 통하는 것을 제외하고는 데이터에 액세스할 수 없도록 하는 것이다. 데이터가 사용될 때, 데이터는 부정조작 방지 디바이스로부터 삭제된다.

상기 첫 번째 방법에서는, 부정조작 방지 디바이스와 같은 특수 디바이스가 필요하지 않다. 그러나, 데이터가 유통될 때 문제가 발생한다. 특히, 데이터의 유효성은 권리가 상기 첫 번째 방법에 따라 행사될 때만 판정될 수 있다. 따라서, 데이터의 유효성은 데이터가 유통되는 동안에는 판단될 수 없다는 문제가 발생한다.

전술한 두 번째 방법에서, 데이터의 유일성(uniqueness)은 부정조작 방지 디바이스를 이용하여 보호될 수 있다. 또한, 일본 특허출원 6-503913 또는 일본 특허출원 9-511350에 개시된 방법은 상기 두 번째 방법에 함께 사용될 수 있으며, 여기서 다수의 부정조작 방지 디바이스는 암호화에 의하여 보호되는 보안 통신 경로를 통하여 접속된다. 데이터는 상기 통신 경로를 통하여 교환되어 데이터는 복제가 방지되면서 유통될 수 있도록 한다. 그러나, 상기 기술은 부정조작 방지 디바이스에 데이터가 저장되어야 하기 때문에 다음의 두가지 문제점을 가진다.

첫째, 데이터의 내용을 파악하는 것이 불가능하다. 따라서, 내용의 유효 기간의 판정과 같은 판정은 부정조작 방지 디바이스에게 맡겨야 한다는 제약이 따른다.

또한, 부정조작 방지 디바이스는 데이터를 저장할 뿐만 아니라 데이터 처리에 필요한 모든 처리를 수행하여야 하기 때문에, 많은 저장 용량 및 높은 처리 용량이 부정조작 방지 디바이스에 대하여 요구된다. 특히, 부정조작 방지 디바이스에 일반적으로 이용되는 IC 카드는 충분한 저장 용량 또는 처리 용량을 가지지 않는다.

발명이 이루고자하는 기술적 과제

본 발명의 목적은 데이터의 유효 복제 수가 특정 수 이하로 확실히 유지되도록 하는 원본 데이터 유통 방법, 시스템, 장치 및 컴퓨터 판독가능 매체를 제공하는 것이다. 또한, 부정조작 방지 디바이스는 복제에 대한 검증이외에 모든 검증을 수행하지 않아 처리 용량과 같은 처리 로딩 또는 메모리 용량이 감소될 수 있도록 한다.

발명의 구성 및 작용

상기 본 발명의 목적은 디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템에 의하여 달성되며, 상기 시스템은:

데이터를 발행하는 발행자 장치에 대응하는 제 1정보를 생성시키는 수단, 상기 제 1정보를 전송하는 수단, 및 상기 데이터에 대응하는 제 2정보를 전송하는 수단을 포함하는 장치; 및

수신된 상기 제 1정보의 유효성을 검증하는 수단, 유효한 제 1정보에 대한 발행자 장치가 유효한지를 검증하는 수단, 및 상기 발행자 장치가 유효할 때 상기 제 2정보에 대응하는 데이터가 유효한지를 결정하는 수단을 포함하는 장치를 포함한다.

상기 제 1정보는 예를 들어 아래의 H(PkI) 등일 수 있다. 제 2정보는 데이터의 해시값 또는 서명된 데이터의 해시값일 수 있다. 발행자 장치는 예를 들어 제 1정보의 소스 장치 및 제 1정보에 대응하는 장치가 동일할 때 유효성이 결정된다. 부정조작 방지 디바이스 등은 제 1정보를 이용하여 인증 프로세스를 수행하기 때문에, 상기 문제점이 해결되며 처리 로딩이 감소될 수 있다.

상기 본 발명의 목적은 또한 가치를 가지는 디지털 정보를 저장하는 데이터 저장 방법에 의하여 달성되는데, 상기 방법은:

상기 디지털 정보의 발행자 장치에 의하여 서명된 서명을 가진 디지털 정보인 제 3정보를 생성시키는 단계;

상기 발행자 장치에 의하여 상기 디지털 정보에 대응하는 매니페스트인 제 4정보를 생성시키는 단계;

상기 제 3정보 및 제 4정보를 이용하여 상기 발행자 장치의 동일성을 이용자 장치에 의하여 검증하는 단계; 및

상기 디지털 정보의 복제를 방지하는 단계를 포함한다.

제 4정보는 예를 들어, 서명된 데이터의 해시값일 수 있다. 해시값은 원본성 정보에 대응하는 매니페스트이다. 원본성 정보는 데이터의 권리의 진위를 나타내는 정보이다. 다시 말해, 원본성 정보는 데이터의 확실성 또는 원본성을 나타낸다.

전술한 발명에 따르면, 데이터 및 데이터의 서명은 저장되며 매니페스트는 데이터 및 서명에 일 대 일 대응하는 정보이다. 또한, 서명을 생성하는 서명자은 식별되며, 서명자이 매니페스트를 저장하고자 하는 당사자와 동일한지가 검증된다. 따라서, 서명자이 의도한 매니페스트의 수는 데이터 저장 시스템에

저장된다.

데이터 저장 방법은 다음 단계를 더 포함한다.

부정조작 방지 디바이스에 상기 제 4정보를 저장함으로써 상기 발행자 장치의 동일성을 검증하는 단계; 및

상기 디지털 정보의 복제를 방지하는 단계.

따라서, 부정조작 방지 디바이스가 이용되기 때문에 데이터는 데이터 저장 시스템이 아닌 장치에 저장될 수 있다.

상기 본 발명의 목적은 또한 가치를 가진 디지털 정보를 저장하는 데이터 저장 시스템에 의하여 달성되는데, 상기 데이터 저장 시스템은:

서명된 디지털 정보인 제 3정보를 생성시키고 상기 디지털 정보에 대응하는 매니페스트인 제 4정보를 생성시키는 발행자 장치; 및

상기 제 3정보 및 제 4정보를 이용하여 상기 발행자 장치의 동일성을 검증하고 상기 디지털 정보의 복제를 방지하는 이용자 장치를 포함한다.

상기 본 발명의 목적은 또한 가치를 가지는 디지털 정보를 저장하는 데이터 저장 시스템에서 디지털 정보를 이용하는 이용자 장치에 의하여 달성되는데, 상기 이용자 장치는:

서명된 디지털 정보를 저장하고 추출하는 제 1저장 수단;

디지털 정보에 대응하는 매니페스트를 저장하고 추출하는 제 2저장 수단;

상기 매니페스트가 유효한지를 검증하는 제 1인증 수단; 및

상기 제 1인증 수단이 상기 매니페스트가 유효한지를 검증할 때만 상기 제 2저장 수단에 상기 매니페스트를 저장하는 제 1제어 수단을 포함한다.

따라서, 데이터에 대응하는 매니페스트가 데이터 저장 시스템에 저장되어 있을 때만 데이터가 유효한지를 결정함으로써, 존재하는 매니페스트의 수를 초과하는 유효 데이터가 회피될 수 있다.

본 발명의 목적은 또한, 가치를 가지는 디지털 정보를 저장하는 데이터 저장 시스템에서 디지털 정보를 발행하는 발행자 장치에 의하여 달성되는데, 상기 발행자 장치는:

상기 디지털 정보의 서명자에 의하여 신뢰되는 신임 대상을 나타내는 정보 세트를 포함하는 신임 정보를 발생시키는 신임 정보 발생 수단;

상기 디지털 정보 및 상기 신임 정보에 서명을 제공하는 서명 수단;

상기 매니페스트를 생성하는 매니페스트 생성 수단;

상기 디지털 정보 및 상기 신임 정보를 이용자 장치에 전달하는 수단;

상기 이용자 장치의 검증 키이 및 일련 번호를 포함하는 세션 정보를 수신하는 수단; 및

상기 이용자 장치의 검증 키이 및 서명 기능을 이용하여 상기 매니페스트 및 세션 정보를 포함하는 정보를 전송하는 수단을 포함한다.

따라서, 신임 대상은 데이터의 서명자 발행자 장치에 의하여 서명된 서명에 의하여 신뢰된다. 매니페스트의 서명자이 신임 대상 또는 신임 대상에 의하여 신뢰되는 서명자에 포함되는 지가 검증된다. 또한, 신임 정보의 서명자과 데이터 서명자이 동일한지가 검증된다. 따라서, 매니페스트는 데이터 서명자에 의하여 신뢰되는 경로를 통하여만 전송될 수 있다. 동시에, 부정조작 방지 능력은 부정조작 방지 장치를 이용함으로써 보장된다.

본 발명의 목적은 또한 가치를 가지는 디지털 정보를 저장하는 데이터 저장 시스템에서 디지털 정보의 권리를 행사하는 개찰자 장치에 의하여 달성되는데, 상기 개찰자 장치는:

이용자 장치로부터 발행자의 서명이된 디지털 정보 및 상기 서명이된 신임 정보를 수신하는 수단;

상기 데이터 저장 시스템에 특정한 세션 정보를 생성하고 상기 세션 정보를 상기 이용자 장치에 전달하는 수단;

상기 이용자 장치로부터 상기 매니페스트 및 상기 세션 정보를 포함하는 정보를 수신하는 수단; 및

상기 세션 정보, 상기 매니페스트 및 상기 신임 정보가 유효한지를 검증하는 수단을 포함한다.

따라서, 세션 정보를 생성 및 저장함으로써, 암호화된 경로를 이용하지 않고 매니페스트가 다수의 저장부에 저장되는 것이 방지된다. 또한, 다수의 매니페스트를 저장부에 병렬로 전송하는 것이 가능하다.

상기 발명은 제 1실시예에서 상세히 설명될 것이다. 또한, 다음의 발명이 제 2실시예에 상세히 설명될 것이다.

본 발명의 상기 목적은 또한, 디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템의 원본 데이터 유통 방법에 의하여 달성되며, 상기 방법은:

장치에 대응하는 제 5정보 및 데이터 또는 상기 데이터에 대응하는 정보인 제 6정보를 포함하는 원본성 정보를 제 1장치에 의하여 전송하는 전송 단계;

상기 원본성 정보의 소스 장치를 제 2장치에 의하여 식별하는 식별 단계;

상기 소스 장치가 인증될 때 상기 원본성 정보가 유효한지를 결정하는 제 1인증 단계; 및

상기 소스 장치 및 상기 원본성 정보의 제 5정보에 대응하는 장치가 동일할 때만 상기 원본성 정보가 유효한지를 결정하는 제 2인증 단계를 포함한다.

본 발명의 상기 목적은 또한 디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템에 의하여 달성되며, 상기 원본 데이터 유통 시스템은:

장치에 대응하는 제 5정보 및 데이터 또는 상기 데이터에 대응하는 정보인 제 6정보를 포함하는 원본성 정보를 전송하는 전송 수단을 포함하는 제 1장치; 및

상기 원본성 정보의 소스 장치를 식별하는 식별 수단, 상기 소스 장치가 인증될 때 상기 원본성 정보가 유효한지를 결정하는 제 1인증 수단 및 상기 소스 장치 및 상기 원본성 정보의 제 5정보에 대응하는 장치가 동일할 때만 상기 원본성 정보가 유효한지를 결정하는 제 6인증 수단을 포함하는 제 2장치를 포함한다.

상기 원본성 정보는 제 2실시예에서 토큰이라고 한다. 제 5정보는 예를 들어 장치의 검증 키이(공개 키이)의 해시값일 수 있다. 제 6정보는 예를 들어 데이터의 해시값일 수 있다. 상기 발명에 따르면, 소스 장치 및 제 1정보에 대응하는 장치가 동일할 때만 원본성 정보가 유효한 것으로 제 2인증 수단이 결정하기 때문에, 종래의 문제점이 해결될 수 있다. 또한, 서명을 유통시킬 필요가 없기 때문에, 처리 로딩이 더 감소될 수 있다.

본 발명의 상기 목적은 또한 디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템의 발행자 장치에 의하여 달성되며, 상기 발행자 장치는:

상기 발행자 장치에 대응하는 제 5정보 및 데이터 또는 상기 데이터에 대응하는 정보에 상응하는 제 6정보를 포함하는 원본성 정보를 생성하는 원본성 정보 생성 수단; 및

상기 원본성 정보를 전송하기 위한 원본성 정보 전송 수단을 포함한다.

본 발명의 상기 목적은 또한 디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템의 이용자 장치에 의하여 달성되며, 상기 이용자 장치는:

장치에 대응하는 제 5정보 및 데이터 또는 상기 데이터에 상응하는 정보에 대응하는 제 6정보를 포함하는 원본성 정보를 전송하는 원본성 정보 전송 수단;

장치로부터 전송된 상기 원본성 정보의 소스 장치를 식별하는 식별 수단;

상기 소스 장치가 인증될 때 또는 상기 제 5정보에 대응하는 상기 장치 및 상기 소스 장치가 동일할 때 상기 원본성 정보가 유효한지를 결정하는 인증 수단; 및

상기 원본성 정보가 유효한지를 상기 인증 수단이 결정할 때 상기 원본성 정보를 저장하는 저장 수단을 포함한다.

본 발명의 목적은 또한 디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템의 개찰자 장치에 의하여 달성되며, 상기 개찰자 장치는:

원본성 정보의 소스 장치를 식별하는 식별 수단;

상기 소스 장치를 인증하는 인증 수단; 및

상기 개찰자 장치에 전송된 원본성 정보가 유효하다고 상기 인증 수단이 결정할 때, 상기 데이터 또는 상기 제 6정보에 상응하는 데이터에 대응하는 프로세스를 수행하는 데이터 처리 수단을 포함한다.

본 발명에서, 신뢰된 제삼자를 나타내는 신임 정보가 이용되기 때문에, 원본성 정보는 신뢰된 당사자사이에 유통될 수 있다.

본 발명의 상기 목적은 또한 디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템에 의하여 달성되며, 상기 원본 데이터 유통 시스템은 발행자 장치, 이용자 장치 및 개찰자 장치를 포함하며,

상기 발행자 장치는: 상기 발행자 장치에 대응하는 제 5정보 및 데이터 또는 상기 데이터에 대응하는 정보에 상응하는 제 6정보를 포함하는 원본성 정보를 생성하는 제 1원본성 정보 생성 수단 및 상기 원본성 정보를 전송하기 위한 제 1원본성 정보 전송 수단을 포함하며,

상기 이용자 장치는: 장치에 대응하는 제 5정보 및 데이터 또는 상기 데이터에 상응하는 정보에 대응하는 제 6정보를 포함하는 원본성 정보를 전송하는 제 1원본성 정보 전송 수단, 장치로부터 전송된 상기 원본성 정보의 소스 장치를 식별하는 제 1식별 수단, 상기 소스 장치가 인증될 때 또는 상기 제 5정보에 대응하는 상기 장치 및 상기 소스 장치가 동일할 때 상기 원본성 정보가 유효한지를 결정하는 제 1인증 수단 및 상기 원본성 정보가 유효한지를 상기 인증 수단이 결정할 때 상기 원본성 정보를 저장하는 저장 수단을 포함하며,

상기 개찰자 장치는: 원본성 정보의 소스 장치를 식별하는 제 2식별 수단, 상기 소스 장치를 인증하는 제 2인증 수단 및 상기 개찰자 장치에 전송된 원본성 정보가 유효하다고 상기 인증 수단이 결정할 때 상기 데이터 또는 상기 제 6정보에 상응하는 데이터에 대응하는 프로세스를 수행하는 데이터 처리 수단을 포함한다.

따라서, 상기 장치에서 티켓을 발행하고, 티켓을 양도하고 티켓을 사용하고 증정하는 것이 가능하다.

이하 첨부된 도면을 참조로 본 발명을 설명한다.

(제 1 실시예)

우선, 본 발명의 원본 데이터 유통 시스템으로서 데이터 저장 시스템을 설명하도록 한다.

도 1은 본 발명의 원리를 설명하기 위한 블록도이다. 본 발명이 데이터 저장 시스템에 있어서, 디지털 정보 발행 장치는 단계 1에서 디지털 정보에 디지털 서명을 추가함으로써 제 1 정보를 생성한다. 상기 발행 장치는 단계 2에서 디지털 정보에 해당하는 매니페스트가 되는 제2 정보를 생성하고, 상기 제 1 정보에 제 2 정보를 추가한다. 이용자 장치는 단계 3에서 디지털 정보의 인증되지 않은 복제가 방지될 수 있도록 제2 디지털 정보와 제 1 디지털 정보를 사용하여 발행자 장치의 동일성을 판정한다.

제1 실시예에 있어서, 서비스 또는 상품을 주문하기 위한 권리의 표현인 디지털 티켓은 유통되는 디지털 정보의 예이다.

도 2는 데이터 저장 시스템의 블록도를 도시한다. 도 2에 도시된 바와 같이, 발행자는 디지털 티켓을 발행한다. 이어, 이용자는 디지털 티켓을 다른 이용자에게 양도한다. 디지털 티켓을 수신하는 이용자가 디지털 티켓을 사용할 때, 검증기는 디지털 티켓의 유효성을 검증한다.

도 2에 있어서, 디지털 티켓의 발행자는 발행 장치(1)를 포함하며, 디지털 티켓을 수신하는 이용자는 이용자 장치(2)를 가진다. 디지털 티켓을 발행할 때, 발행 장치(1)와 이용자 장치(2) 사이의 통신 채널은 접속 장치(4)를 통해 성립된다. 통신 채널은 발행 시작 시간에서 발행 종료 시간까지의 구간 동안에만 존재할 수도 있다.

디지털 티켓을 양도할 때, 통신 채널은 디지털 티켓을 발행할 때와 동일한 방식으로 이용자 장치들(2) 사이에서 성립된다. 이어, 디지털 티켓이 이용자 장치들(2) 사이에서 양도된다. 디지털 티켓의 개찰자는 개찰자 장치(3)를 가진다. 디지털 티켓을 개찰할 때, 통신 채널은 디지털 티켓을 발행할 때와 동일한 방식으로 통신 장치(4)를 통해 이용자 장치(2)와 개찰자 장치(3) 사이에서 성립된다. 이어, 디지털 티켓은 개찰자 장치(3)로 전송된다.

상술한 바와 같이, 본 발명의 데이터 저장 시스템은 하나 또는 다수의 발행 장치, 하나 또는 다수의 이용자 장치(2) 및 하나 또는 다수의 개찰자 장치(3)를 포함하며, 상기 장치들은 일시적인 통신 채널을 제공하는 접속 장치(4)에 의해 접속된다.

데이터 저장 시스템에 포함된 각각의 장치들을 설명하도록 한다. 설명에 앞서, 설명을 위해 사용되는 상투적인 어구에 대한 의미를 설명하도록 한다.

x‖y는 x와 y의 연속된 연결을 의미한다. H는 단방향 해시 함수를 의미한다. 상기 해시 함수는 y=H(x)를 만족하는 y로부터 x를 결정하는 것이 어렵다는 특성을 가진다. RSA의 MD5가 해시 함수로서 공지되었다.

S_{Pk}는 검증 함수(V_{Pk})에 의해 검증될 수 있는 디지털 서명을 발생시키는 서명 함수이다. 상기 검증 함수(V_{Pk})는 $V_{Pk}(x‖S_{Pk}(x))=1$, $V_{Pk}(x‖나머지)=0$(여기에서 나머지는 $S_{Pk}(x)$가 아닌 것)의 특성을 가진다. 즉, 검증 함수V_{Pk}는 정보x가 서명 함수S_{Pk}에 의해 서명된 서명을 가지는 지를 검증할 수 있다. 게다가 검증 함수V_{Pk}는 디지털 서명$S_{Pk}(x)$이 x에 대하여 S_{Pk}로 서명된 서명을 정정할 수 있다.

Pk는 검증키이며, 검증 키Pk를 검증기v에 제공하므로써 V_{Pk}가 형성될 수 있다는 특성을 가진다. 특히, 검증키$Pk2‖S_{Pk1}(Pk2)$은 Pk1에 따른 Pk2의 키 증명서로 불린다.

일본 전신 전화국의 ESIGN은 상술한 S_{Pk} 및 V_{Pk}를 실현한 디지털 서명 방식으로 공지되어 있다.

도 3은 본 발명의 실시예에 따른 발행자 장치를 도시한다.

도 3에 도시된 발행자 장치(1)는 제어부(11), 서명부(12), 데이터 생성부(13), 매니페스트 생성부(14) 및 신임 정보 생성부(15)를 포함한다.

상기 제어부(11)는 검증키PkI를 가지며, 디지털 티켓을 안전하게 유통하도록 발행자 장치(1)를 제어한다. PkI은 서명부(12)에서 제공된 서명 함수S_{PkI}에 대응하는 검증키이다. 제어부(11)에 대한 상세한 설명은 이후에 하도록 한다.

서명부(12)는 서명 함수S_{PkI}을 포함한다. 각각의 발행자 장치는 상이한 서명함수S_{PkI}을 가진다. 상기 함수S_{PkI}는 서명부(12)에 의해 은닉된다.

데이터 생성부(13)는 발행자 장치(1)에서 발생된 정보 또는 외부로부터 주어진 정보에 기초하여 데이터(m)를 생성한다. 본 발명의 데이터 저장 시스템에 따르면, 데이터m의 내용에 대한 어떠한 제한도 없다. 따라서, 콘서트 티켓과 같은 일반 티켓에 대한 권리를 나타내는 디지털 정보, 프로그램 데이터, 음악 데이터 및 이미지 데이터가 데이터m으로 사용될 수 있다.

게다가, m은 $H(m_0)$를 취득함으로써 다른 데이터와의 관계 또는 다른 데이터와의 관계를 포함하는 데이터로서 형성될 수 있으며, 여기에서 m_0은 외부로부터 제공된다. 적절하게, 이후에 설명되는 부정 조작 방지 디바이스(28)로 전송되는 데이터 량은 디지털 티켓을 발행할 때 감소될 수도 있다.

매니페스트 생성부(14)는 단방향 해시 함수H를 가지며, 서명$m‖S_{PkI}(m)$을 가지는 데이터(즉, 서명된 데이터)의 매니페스트$c_{(m,PkI)}=H(m‖S_{PkI}(m))$를 생성시킨다.

신임 정보 생성부(15)는 신임정보t=(t_I,t_C)를 발생시킨다. 신임 정보 t=(t_I,t_C)에서 t_I= PkI, t_C=(H(PkC$_1$), H(PkC$_2$), ..., H(PkC$_n$))이다. 여기에서 PkI는 제어부(11)에 의해 유지되는 검증키이며, PkC$_1$은 발행자에 의해 "신뢰받는", 후술될 제 3자에 의해 서명된 서명을 검증하기 위한 검증키이다.

도 4는 본 발명의 실시예에 따른 이용자 장치(2)이다. 상기 이용자 장치(2)는 제어부(21), 저장부(22) 및 부정 조작 방지 디바이스(28)를 포함하며, 상기 부정 조작 방지 디바이스(28)는 제어부(23), 인증부(24), 서명부(25), 번호 발생부(26) 및 저장부(27)를 포함한다. 부정 조작 방지 디바이스(28)는 함수 및 상기 부분들의 내용물들이 부당하게 사용되는 것을 방지한다. 부정 조작 방지 디바이스(28)의 이용자조차도 부정 조작 방지 디바이스(28)를 부당하게 사용할 수 없다. 네트워크에 의해 엄격하게 관리되는 IC 카드 또는 서버가 부정 조작 방지 디바이스(28)로 사용될 수 있다.

상기 제어부(21) 및 부정 조작 방지 디바이스(28)내의 제어부(23)는 디지털 티켓을 안전하게 유통하도록 이용자 장치(2)를 제어한다. 제어부(21)에 대한 상세한 설명은 다음에 하기로 한다.

저장부(22)는 이용자에 의해 유지되는 서명된 데이터 세트M_u 및 발행자에 의해 서명된 서명을 가지는 신임 정보 세트T_u를 저장한다. 상기 데이터 세트들은 제어부(21)에 의해 업데이트될 수 있다.

제어부(23)는 검증키 PkU 와 PkC 및 키 증명서PkU‖S_{PkC}(PkU)를 가진다. 여기에서 검증키PkU는 서명부(25)내의 S_{PkU}에 대응한다. S_{PkC}는 부정 조작 방지 디바이스(28)의 안전성을 보증하는 제 3자에 의해 은닉되는 서명 함수이다. 상기 제 3자는 IC 카드 조작자, 부정 조작 방지 서버 관리자 등이다. 즉, 서명 함수(S_{PkU})를 포함하는 부정 조작 방지 디바이스(28)의 부정조작 방지 능력은 서명 함수S_{PkC}를 가지는 제 3자에 의해 보증된다.

다른 이용자 장치의 저장부(22) 및/또는 후술할 개찰자 장치(3)의 저장부(34)는 저장부(22)를 사용하여 또는 저장부(22)를 대신하여 사용될 수 있다. 이러한 경우에 있어서, 데이터m 및 후술할 신임 데이터(t_1, t_2, t_3)가 이용자 장치 및 개찰자 장치에 의해 공유되기 때문에, 데이터 m 및 신임 데이터(t_1, t_2, t_3)는 상기 장치들 사이에서 반드시 전송될 필요는 없다.

인증부(24)는 검증기(V)를 포함한다. 상기 서명부(25)는 서명 함수S_{PkU}를 가진다. 각각의 이용자 장치는 상이한 서명함수S_{PkU}을 가진다. 상기 함수S_{PkU}는 서명부(25)에 의해 은닉된다.

번호 발생부(26)는 다음 번호r_U를 저장한다. 번호 발생부(26)가 번호를 발생시키도록 요구될 때, 번호 발생부(26)는 현재 번호(r_U)를 발생하고 r_U를 증가시킨다.

저장부(27)는 매니페스트 세트C_U = {c_1, c_2, ... ,c_n} 및 번호 세트 R_U = {r_1, r_2, ... ,r_m}을 저장한다. 이러한 세트들은 제어부(21)에 의해 업데이트될 수 있다.

도 5는 본 발명의 실시예에 따른 개찰자 장치(3)의 블록도이다. 개찰자 장치(3)는 제어부(31), 인증부(32), 번호 발생부(33) 및 저장부(34)를 포함한다.

제어부(31)는 검증키PkV를 가지며, 디지털 티켓을 안전하게 유통하도록 개찰자 장치(3)를 제어한다. 제어부(31)의 동작에 대한 상세한 설명은 이후에 하도록 한다.

인증부(32)는 검증기(V)를 포함한다.

번호발생부(33)는 다음 번호T_V를 저장한다. 번호 발생부(26)가 번호를 발생시키도록 요구될 때, 번호 발생부(33)는 현재 번호(r_V)를 발생시켜 r_V를 증가시킨다.

저장부(34)는 번호 세트 R_V = {r_1, r_2, ... ,r_m}을 저장한다. 상기 세트는 제어부(31)에 의해 업데이트될 수 있다.

도 6은 본 발명의 실시예에 따른 접속 장치(4)의 블록도이다.

접속 장치(4)는 통신부(41)를 포함한다. 상기 통신부(41)는 발행자 장치(1), 이용자 장치(2)와 개찰자 장치(3) 사이에 또는 이용자 장치들 사이에 일시적 또는 영구적인 통신 채널을 제공한다. 키오스크(kiosk)에 IC 카드 슬롯을 가지는 단말기 , 네트워크를 통해 접속된 다수의 PC 또는 이와 유사한 것들이 접속 장치(4)로서 사용될 수 있다.

상술한 장치를 사용하여 디지털 티켓을 안전하게 유통하기 위한 방법을 설명하도록 한다.

유통 방법의 기본 개념은 다음과 같다.

- 디지털 티켓은 발행자에 의해 서명된 데이터m‖S_{PkI}(m)로 표현된다. 발행자에 의해 디지털 티켓의 주인에게 주어지는 권리의 내용은 m내에서 설명된다. 그렇지 않으면, m은 권리의 내용이 설명되어지는 데이터에 대한 관계를 포함한다.

- 디지털 티켓의 부당한 사용은 디지털 티켓 발행자의 서명 함수S_{PkI}를 사용함으로써 방지된다.

- 디지털 티켓의 복제는 금지된다.

- 매니페스트$c_{(m,PkI)}$는 디지털 티켓으로부터 생성될 수 있다. 매니페스트는 실지적으로 디지털 티켓과 1대 1 대응 방식이다.

- 매니페스트는 발행자에 의해 신뢰받는 부정 조작 방지 디바이스(28)의 저장부(27)에 저장됨으로써 유효하게 된다.

- 발행자에 의해 신뢰받는 부정 조작 방지 디바이스는, 부정 조작 방지 능력이 발행자에 의해 신뢰받는 제 3자에 의해 보증되는 디바이스이다. 상기 발행자에 의해 신뢰받는 제 3자는 신임 정보t_I에 의해 정의된다.

- 유효한 매니페스트는 해당 디지털 티켓의 발행자에 의해서만 새롭게 발생된다.

- 하나의 유효한 매니페스트로부터 하나 또는 다수의 유효한 매니페스트를 발생시키는 것은 금지된다. 즉, 이용자가 나머지 이용자들에 의해 서명되는 디지털 티켓의 매니페스트를 발생시키는 것이 금지된다.

이하, 디지털 티켓의 유통 방법을 (1) 디지털 티켓 발행, (2) 디지털 티켓의 양도 및 (3) 디지털 티켓의 소비의 각각의 경우에 대하여 설명하도록 한다. 다음의 설명에서, 장치들 간의 통신은 접속 장치(4)의 통신부(41)를 통해 행하여진다.

(1) 디지털 티켓의 발행

접속 장치(4)를 통해 디지털 장치(1)로부터 이용자 장치(2)로의 디지털 티켓 발행 처리를 설명하도록 한다. 도 7은 본 발명의 실시예에 따른 처리에 대한 시퀀스 챠트이다.

단계 101) 제어부(11)는 서명된 데이터인 디지털 티켓 $m \| S_{PkI}(m)$을 생성하기 위한 다음의 절차에 따라 m 및 $S_{PkI}(m)$을 취득한다.

(a) 데이터 생성부(13)는 데이터m을 발생시킨다.

(b) m은 서명부(12)가 $S_{PKI}(m)$을 생성하도록 서명부(12)에 제공된다.

단계 102) 제어부(1)는 매니페스트 생성부(14)가 매니페스트$c_{(m,PKI)}$를 발생시키도록 디지털 티켓 $m \| S_{PkI}(m)$을 매니페스트 생성부(14)에 제공한다.

단계 103) 제어부(11)는 다음의 절차에 따라 신임 정보t 및 서명 함수 $S_{PkI}(t)$를 취득하여, 서명된 신임 정보$t \| S_{PkI}(t)$를 생성시킨다.

(a) 상기 신임 정보 생성부(15)는 신임 정보t를 생성한다. t의 구조는 앞서 설명하였다.

(b) 상기 신임 정보t는 서명부(12)가 서명$S_{PkI}(t)$를 생성하도록 서명부(12)로 제공된다.

단계 104) 제어부(11)는 디지털 티켓$m \| S_{PkI}(t)$ 및 서명된 신임 정보$t \| S_{PkI}(t)$를 제어부(21)로 전송한다.

단계 101에서 데이터 생성부(13)에 의해 생성된 m은 다른 데이터와의 관계, 예를 들어 $m=H(m_o)$가 될 때 또는 m이 관계를 포함할 때, 관련 데이터(m_o)는 필수적인 것으로 전송되며, 이것은 후술할 양도 및 소비의 경우에서와 동일하다.

단계 105) 이용자 장치(2)의 제어부(21)는 상기 세트M_U에 디지털 티켓$m \| S_{PkI}(m)$을 추가하고, 상기 세트T_U에 상기 서명된 신임 정보$t \| S_{PkI}(t)$를 추가하여 그들을 저장부(22)에 저장한다.

m에 관련된 데이터가 전송될 때, 관계가 검증된다. 상기 검증이 실패하면, 처리는 인터럽트되며, 발행자 장치는 이를 인지한다. 이는 후술할 양도 및 소비의 경우에서도 동일하다.

단계 106) 제어부(21)는 제어부(23)에 세션 정보(s_1,s_2)를 발생할 것을 요구한다.

제어부(23)는 다음의 절차에 따라 세션 정보(s_1,s_2)를 생성하여, 제어부(21)로 전송한다.

(a) 제어부(23)는 번호 발생부(26)에 의해 생성된 번호r_U를 취득한다.

(b) 번호r_U는 저장부(27)내의 번호 세트R_U에 추가된다.

(c) 세션 정보(s_1,s_2)=(H(PkU), r_U)가 생성된다. 여기에서 PkU는 제어부(21)에 의해 유지되는 검증키이다.

단계 107) 제어부(21)는 세션정보(s_1,s_2)를 제어부(11)로 전송한다.

단계 108) 제어부(11)는 서명부(12)의 S_{PkI}를 사용하여 매니페스트 발행 포맷 $e_I = (e_1, e_2, e_3, e_4, e_5)$를 취득하고, 제어부(11)에 의해 유지되는 검증키PkI를 취득한다. e_I의 각 요소는 다음과 같다.

$e_1 = c_{(m,PkI)}$

$e_2 = s_1$

$e_3 = s_2$

$e_4 = S_{PkI}(c_{(m,PkI)} \| s_1 \| s_2)$

e_5 = PkI

단계 109) 제어부(11)는 매니페스트 발행 포맷e_I을 제어부(21)로 전송한다.

단계 110) 제어부(21)는 디지털 티켓$m \| S_{PkI}(m)$ 및 매니페스트 발행 포맷을 제어부(23)로 전송하고, 매니페스트를 e_I내에 저장할 것을 요구한다.

단계 111) 제어부(23)는 인증부(24)를 사용하여 다음의 조건들이 만족되는지를 검증한다. 검증이 실패한 경우, 이후의 처리는 인터럽트되며, 제어부(23)는 제어부(11)의 처리 인터럽트를 제어부(21)를 통해 인지한다.

$$e_2 = H(PkI) \quad (1)$$

$$e_3 \in R_U \quad (2)$$

$$V_{e5}(m \| S_{PkI}(m)) = 1 \quad (3)$$

$$V_{e5}(e_1 \| e_2 \| e_3 \| e_4) = 1 \quad (4)$$

$$e_1 = H(m \| S_{PkI}(m)) \quad (5)$$

상술한 식(1)과 식(2)은 세션 정보의 유효성 검증을 의미한다. 검증에 따라 부정 행위가 방지된다. 예를 들어 이러한 부정 행위는 다른 이용자 장치(2)를 수신지로 하는 매니페스트 발행 포맷의 저장 또는 매니페스트 발행 포맷을 재이용한 매니페스트의 복제가 될 수 있다. 식(3) 및 식(4)은 매니페스트 발행 포맷의 서명에 대한 유효성 검증을 의미한다. 검증에 따라, 매니페스트 발행 포맷 내에 포함되고 발행자에 의해 서명된 서명을 가지는 하나 이상의 다른 매니페스트의 발생이 저장되는 것이 방지될 수 있다. 식(5)은 매니페스트와 디지털 티켓 사이의 대응 관계에 대한 검증을 의미한다. 검증에 따라, 다른 디지털 티켓에 대응하는 것과 같은 디지털 티켓에 대응하지 않은 매니페스트의 발생이 방지된다.

단계 112) 제어부(23)는 저장부(27)내의 번호 세트R_U에서 $e_3(=r_U)$을 삭제한다.

단계 113) 제어부(23)는 저장부(27)내의 매니페스트 세트C_U에 $e_1(=c_{(m,PkI)})$를 추가한다.

단계 114) 제어부(23)는 c_1을 제어부(21)로 전송하여 정상적인 종료를 인지하도록 한다.

(2) 디지털 티켓의 양도

접속 장치(4)를 통한 이용자 장치(2a)로부터 이용자 장치(2b)로의 디지털 티켓 양도 처리는 다음과 같이 설명된다.

도 8 및 도 9는 본 발명의 실시예에 따른 디지털 티켓 양도 처리를 설명하는 시퀀스 챠트이다.

단계 201) 제어부(21a)는 저장부(22a)에 의해 유지된 서명된 데이터 세트m_{Ua}에서 전송될 대상이 되는 디지털 티켓$m \| S_{PkI}(m)$을 추출한다.

단계 202) 제어부(21a)는 저장부(22a)내의 T_{Ua}에서 $m \| S_{PkI}(m)$의 발행자에 의해 서명된 신임 정보 $t \| S_{PkI}(t)$를 추출한다.

단계 203) 제어부(21a)는 $m \| S_{PkI}(m)$ 및 $t \| S_{PkI}(t)$를 제어부(21b)로 전송한다.

단계 204) 제어부(21b)는 저장부(22b)내의 서명된 데이터 세트M_{Ub}내에 $m \| S_{PkI}(m)$을 저장하고 저장부(22b)내의 신임 정보 세트T_{Ub}내에 $t \| S_{PkI}(t)$를 저장한다.

단계 205) 제어부(21b)는 제어부(23b)로 세션 정보(s_1,s_2)를 생성할 것을 요구한다.

제어부(23b)는 다음의 절차에 따라 세션 정보(s_1,s_2)를 생성하고, 그것을 제어부(21b)로 전송한다.

(a) 제어부(23b)는 번호 발생부(26b)에 의해 생성된 번호r_{Ub}를 취득한다.

(b) 번호 r_{Ub}는 저장부(27b)내의 번호 세트R_{Ub}에 추가된다.

(c) 세션 정보(s_1,s_2) = (H(PKUb),r_{Ub})가 발생된다. 여기에서 PkUb는 제어부(21b)에 의해 유지되는 검증키이다.

단계 206) 제어부(21b)는 세션 정보(s_1,s_2)를 제어부(21a)로 전송한다.

단계 207) 제어부(21a)는 (s_1,s_2) 및 전송될 디지털 티켓의 해시값 $H(m \| S_{PkI}(m))$를 제어부(23a)로 전송한다.

단계 208) 제어부(23a)는 다음의 식이 저장부(27a)에 저장된 매니페스트들의 매니페스트 세트C_{Ua}에 대하여 만족되는 지를 검증한다.

$$H(m \| S_{PkI}(m)) \in C_{Ua} \quad (6)$$

검증이 실패할 때, 이후의 처리는 인터럽트되고 제어부(21a)는 이러한 실패를 인지한다.

상기 식(6)은 전송될 디지털 티켓에 대응하는 매니페스트$c_{(m,Pkl)} = H(m \| S_{Pkl}(m))$가 저장부(27a)내에 저장되었는 지에 대한 검증을 의미한다.

단계 209) 제어부(23a)는 서명부(25a)내에 포함된 S_{Pkl}와 제어부(11)에 포함된 증명키 PkUa, PkCa 및 키 증명서$PkUa \| S_{PkCa}(PkUa)$를 사용하여 매니페스트 전송 포맷 $e_c = (e_1, e_2, e_3, e_4, e_5, e_6, e_7)$을 취득한다. e_c의 각 요소는 다음과 같다.

$e_1 = c_{(m,Pkl)}$

$e_2 = s_1$

$e_3 = s_2$

$e_4 = S_{PkUa}(c_{(m,Pkl)} \| s_1 \| s_2)$

$e_5 = PkUa$

$e_6 = S_{PkCa}(PkUa)$

$e_7 = PkCa$

단계 210) 제어부(23a)는 매니페스트 세트C_{Ua}에서 $c_{(m,Pkl)}$를 삭제한다.

단계 211) 제어부(23a)는 e_c를 제어부(21a)로 전송한다.

단계 212) 제어부(21a)는 e_c를 제어부(21b)로 전송한다. 제어부(21b)는 $e_1 = H(m \| S_{Pkl}(m))$가 만족되는 지의 여부에 대하여 전송된 e_c내의 e_1을 검증한다.

단계 213) 제어부(21b)는 e_c, $t \| S_{Pkl}(t)$ 및 $m \| S_{Pkl}(m)$를 제어부(23b)로 전송하고 e_c내에 매니페스트를 저장할 것을 요구한다.

단계 214) 제어부(23b)는 인증부(24b)를 사용하여 아래의 모든 식이 만족되어지는 지를 검증한다. 검증이 실패한 경우, 처리는 인터럽트되며, 제어부(21b)는 인터럽트를 인지한다.

$e_2 = H(PkUb)$ (7)

$e_3 \in R_{Ub}$ (8)

$V_{e5}(e_1 \| e_2 \| e_3 \| e_4, e_5) = 1$ (9)

$V_{e7}(e_5 \| e_6) = 1$ (10)

$H(e_7) \in t_c$ (11)

$V_{tl}(m \| S_{Pkl}(m)) = 1$ (12)

$V_{tl}(t \| S_{Pkl}(t)) = 1$ (13)

상기 식(7) 및 식(8)은 세션 정보의 유효성에 대한 검증을 의미한다. 검증을 사용하여, 다른 이용자 장치상에서 매니페스트 전송 포맷의 저장, 매니페스트 전송 포맷을 재사용한 매니페스트 복제 또는 유사한 동작과 같은 부정 행위가 방지된다.

식(9)은 매니페스트 전송 포맷의 서명자를 식별하기 위한 검증을 의미한다. 식(10)은 서명자의 키 증명서에 대한 검증을 의미한다. 식(11)은 발행자가 키 증명서의 서명자를 신임 정보내의 신임 대상으로서 신뢰하는 지에 대한 검증을 의미한다. 상기 검증에 따라, 매니페스트 전송 포맷의 소스에 대한 부정 조작 방지 능력이 발행자에 의해 신뢰받는 제 3자에 의해 보증되는 지가 검증된다.

식(12) 및 식(13)은 신임 정보 상에 서명된 서명의 유효성 검증을 의미한다. 검증에 따라, 신임 정보가 디지털 티켓의 서명자에 의해 적절하게 서명되었는 지가 검증된다.

단계 215) 제어부(23b)는 저장부(27b)내의 번호세트R_{Ub}에서 $e_3(=r_{Ub})$을 삭제한다.

단계 216) 제어부(23b)는 저장부(27b)내의 매니페스트 세트C_{Ub}에 $e_1(=c_{(m,Pkl)})$을 추가한다.

단계 217) 제어부(23b)는 제어부(21b)가 처리를 정상적 완료한 것을 인지한다.

(3) 디지털 티켓의 소비

접속 장치(4)를 통한 이용자 장치(2)로부터 개찰자 장치(3)로의 디지털 티켓 소비 처리를 설명하도록 한다.

도 10은 본 발명의 실시예에 따른 티켓 소비 처리의 시퀀스 챠트이다.

단계 301) 제어부(21)는 소비될 디지털 티켓 $m \| S_{Pkl}(m)$을 저장부(22)에 포함된 서명된 데이터 세트에서

추출한다.

단계 302) 제어부(21)는 $m \| S_{PkI}(m)$의 발행자에 의해 서명된 신임 정보$t \| S_{PkI}(t)$를 저장부(22)내에 포함된 서명된 신임 정보 세트T_U에서 추출한다.

단계 303) 제어부(21)는 $m \| S_{PkI}(m)$ 및 $t \| S_{PkI}(t)$를 제어부(31)로 전송한다.

단계 304) 제어부(31)는 다음의 절차에 따라 세션 정보(s_1,s_2)를 생성한다.

(a) 제어부(23)는 번호 발생부(33)로부터 번호r_V를 취득한다.

(b) 번호r_V는 저장부(34)내의 번호 세트R_V에 추가된다.

(c) 세션 정보(s_1,s_2)=(H(PkV),r_V)가 생성된다. 여기에서 PkV는 제어부(31)에 의해 유지되는 검증키이다.

단계 305) 제어부(31)는 세션 정보를 제어부(21)로 전송한다.

단계 306) 제어부(21)는 (s_1,s_2) 및 소비될 디지털 티켓의 해시값 $H(m \| S_{PkI}(m))$를 제어부(23)로 전송한다.

단계 307) 제어부(23)는 저장부(27)에 저장된 매니페스트 세트C_U에 대하여 다음의 식이 만족되는 지를 검증한다.

$$H(m \| S_{PkI}(m)) \in C_U \quad (15)$$

검증이 실패할 때, 이후의 처리는 인터럽트되며, 제어부(21)는 이러한 실패를 인지한다.

상기 식(15)은 소비될 디지털 티켓에 대응하는 매니페스트$c_{(m,PkI)} = H(m \| S_{PkI}(m))$가 저장부(27)에 저장되는 지를 검증한다.

단계 308) 제어부(23)는 서명부(25)내에 포함된 S_{PkU}와 제어부(21)에 포함된 증명키 PkU, PkC 및 키 증명서$PkU \| S_{PkC}(PkU)$를 사용하여 매니페스트 전송 포맷 $e_c = (e_1, e_2, e_3, e_4, e_5, e_6, e_7)$을 취득한다. e_c의 각 요소는 다음과 같다.

$e_1 = c_{(m,PkI)}$

$e_2 = s_1$

$e_3 = s_2$

$e_4 = S_{PkU}(c_{(m,PkI)} \| s_1 \| s_2)$

$e_5 = PkU$

$e_6 = S_{PkC}(PkU)$

$e_7 = PkC$

단계 309) 제어부(23)는 매니페스트 세트C_U에서 $c_{(m,PkI)}$를 삭제한다.

단계 310) 제어부(23)는 e_c를 제어부(21)로 전송한다.

단계 311) 제어부(21)는 e_c를 제어부(31)로 전송한다.

단계 312) 제어부(31)는 인증부(32)를 사용하여 아래의 모든 식이 만족되는 지를 검증한다. 검증이 실패한 경우, 처리는 인터럽트되며, 제어부(21)는 인터럽트를 인지한다.

$$e_2 = H(PkV) \quad (16)$$

$$e_3 \in R_V \quad (17)$$

$$V_{e5}(e_1 \| e_2 \| e_3 \| e_4, e_5) = 1 \quad (18)$$

$$V_{e7}(e_5 \| e_6) = 1 \quad (19)$$

$$H(e_7) \in t_c \quad (20)$$

$$V_{tI}(m \| S_{PkI}(m)) = 1 \quad (21)$$

$$V_{tI}(t \| S_{PkI}(t)) = 1 \quad (22)$$

상기 식(16) 및 식(17)은 세션 정보의 유효성에 대한 검증을 의미한다. 검증을 사용하여, 다른 개찰자 장치상에 매니페스트 전송 포맷의 저장, 매니페스트 전송 포맷을 재사용한 매니페스트 복제 또는 유사한 동작과 같은 부정 행위가 방지된다.

식(18)은 매니페스트 전송 포맷의 서명자를 식별하기 위한 검증을 의미한다. 식(19)은 서명자의 키 증명서에 대한 검증을 의미한다. 식(20)은 신임 정보내의 신임된 대상으로서 키 증명서의 서명자를 발행자가 신뢰하는 지에 대한 검증을 의미한다. 상기 검증에 따라, 발행자가 신뢰하는 제 3 자에 의해 매니페스트 전송 포맷의 소스에 대한 부정 조작 방지 능력이 보증되는 지가 검증된다.

식(21) 및 식(22)은 신임 정보에 대한 서명의 유효성 검증을 의미한다. 검증에 따라, 신임 정보가 디지털 티켓의 서명자에 의해 적절하게 서명되었는 지가 검증된다.

단계 313) 제어부(31)는 저장부(34)내의 번호세트R_V에서 $e_3(=r_V)$을 삭제한다.

단계 314) 제어부(31)는 아래의 모든 식이 만족되는 지를 검증한다. 검증이 실패한 경우, 제어부(21)는 처리 인터럽트를 인지한다. 검증이 성공적인 경우, m에 대응하는 서비스가 소비자에게 제공된다.

$$e_1 = H(m \| S_{PKI}(m)) \qquad (23)$$

상기 식(23)은 소비될 디지털 티켓에 대응하는 매니페스트가 전송되었는 지에 대한 검증을 의미한다. 검증에 따라 유효한 디지털 티켓이 소비되었는 지가 검증된다.

발행자 장치(1), 이용자장치(2) 또는 개찰자 장치(3)의 각 요소들은 프로그램에 의해 구성될 수도 있다. 프로그램은 발행자 장치, 이용자 장치 또는 개찰자 장치로서 사용될 수 있는 컴퓨터에 접속된 디스크 유니트 내에 저장될 수 있다. 프로그램은 플로피 디스크, CD-ROM 등과 같은 운송 가능한 컴퓨터 판독가능 매체 내에 저장될 수도 있다. 프로그램은 본 발명이 컴퓨터에 의해 구현되도록 컴퓨터 판독가능 매체로부터 컴퓨터로 설치된다.

상술한 바와 같이, 본 발명이 제 1 실시예에 따라, 서명자가 저장하기를 의도하는 번호의 매니페스트만이 데이터 저장 시스템의 매니페스트 저장부내에 저장되기 때문에, 서명자 이외의 다른 사람에 의해 새롭게 저장된 매니페스트의 발생이 방지된다. 게다가, 매니페스트의 개수를 초과하는 유효한 데이터가 존재하는 것이 방지된다. 더욱이, 매니페스트가 서명자에 의해 신뢰되는 경로를 통해서만 전송될 수 있다는 것이 가능하여 진다.

본 발명의 데이터 저장 시스템내의 데이터와 같은 디지털 티켓을 사용함으로써, 부정 조작 방지 디바이스 내에 디지털 티켓을 저장하지 않고, 디지털 티켓의 유용한 복제의 수를 일정한 개수 보다 작게 유지할 수 있다.

게다가, 본 발명의 데이터와 같은 프로그램을 사용하고 프로그램의 라이선스와 같은 매니페스트를 사용함으로써, 프로그램의 불법 복사 및 사용이 방지될 수 있다.

더욱이, 본 발명의 데이터와 같은 음악 데이터, 이미지 데이터를 사용함으로써, 음악 데이터 또는 이미지 데이터의 불법 복사 및 사용이 방지될 수 있다. 또한 데이터가 사용되는 매 시간마다 데이터를 "소비"((3)실시예에서)함으로써, 청구 시스템(billing system)(예를 들어 유료 요금 청구 시스템)에서 이용될 때마다의 청구서를 작성하는 데에 본 발명의 시스템이 사용될 수 있다.

(제 2 실시예)

이어, 본 발명의 제 2 실시예를 설명하도록 한다.

상술한 제 1 실시에 따라, 원본성을 표현하는 데이터(매니페스트)만이 부정 조작 방지 장치 내에 저장되고 데이터의 유효한 복제의 개수가 미리 설정된 일정한 개수 이하로 유지된다는 점이 보증된다. 이에 따라, 부정 조작 방지 디바이스가 복제에 대한 검증 이외의 검증을 반드시 수행할 필요는 없다. 검증은 표현의 유효성에 대한 검증을 포함한다. 따라서, 처리속도 및 메모리 용량과 같은 처리 부하는 감소될 수 있다. 상술한 본 발명은 종래의 기술과 비교하여 현저한 효과를 가진다. 그러나, 실제 상태에 대해 아래와 같은 두 가지 문제점이 존재한다.

첫째, 원본성 또는 신뢰성 또는 진실성을 나타내는 데이터를 생성할 때, 데이터 및 서명을 검증하기 위하여 부정 조작 방지 디바이스로 데이터와 서명을 반드시 전송하여야 한다. 반면에, IC 카드의 전송 속도는 약 9600bps(ISO-7816)이며, 이것은 상당히 느리다. 그러므로, 데이터의 크기가 클 때, 원본성을 나타내는 데이터를 생성하기 위한 시간은 현저하게 증가될 수 있다.

또한, 상술한 제 1 실시예에 따라, 원본성을 나타내는 데이터는 데이터 및 서명으로부터 생성되며, 데이터를 소비할 때 데이터와 서명을 사용하여 원본성을 나타내는 데이터를 반드시 검증하여야 한다. 이에 따라, 데이터뿐만 아니라 서명도 반드시 유통시키는 것이 필연적이다. 따라서, 시스템에 대하여 요구되는 메모리 요구 용량 및 유통을 위한 처리 시간이 증가될 수 있다.

제 2 실시예에 있어서, 원본 데이터 유통 시스템을 설명하도록 한다. 시스템에 따라, 원본성을 나타내는 데이터를 생성하고 데이터를 유통시키기 위한 처리 부하가 감소된다.

도 11은 본 발명의 제 2 실시예의 원리를 설명하기 위한 블록도이다.

디지털 정보가 되는 원본 데이터를 저장 및 유통하기 위한 원본 데이터 유통시스템은 발행자 장치(50), 이용자 장치(60) 및 개찰자 장치(70)를 포함한다.

발행자 장치는 제 1 원본성 정보 생성부(51) 및 제 1 원본성 정보 전송부(52)를 포함한다. 제 1 원본성 정보 생성부(51)는 원본성 정보를 생성한다. 제1 원본성 정보 전송부(52)는 원본성 정보를 전송한다. 여기에서, 원본성 정보는 발행된 데이터의 권리에 대한 진실성을 나타내는 데이터이다. 다시 말하면, 원본성 정보는 발행된 데이터의 신뢰성 또는 원본성을 나타낸다.

이용자 장치(60)는 제 2 원본성 정보 전송부(61), 제 1 식별부(62), 제 1 인증부(63) 및 저장부(64)를

포함한다.

제 2 원본성 정보 전송부(61)는 장치에 대응하는 5번째 정보와 데이터가 되는 또는 데이터에 대응하는 6번째 정보에 의해 형성된 원본성 정보를 수신한다. 원본성 정보가 다른 장치로부터 수신될 때, 제 1 식별부(62)는 원본성 정보의 소스 장치를 식별한다. 소스 장치가 인증될 때, 제 1 인증부(63)는 소스 장치 및 원본성 정보의 제 1 정보에 대응하는 정보가 동일할 때에만 원본성 데이터가 유효한 지를 결정한다. 저장부(64)는 원본성 정보가 제 1 인증부(63)에 의해 유효한 것으로 결정될 때, 원본성 정보를 저장한다.

개찰자 장치(70)는 제 2 식별부(71), 제 2 인증부(72) 및 데이터 처리부(73)를 포함한다.

제 2 인증부(71)는 원본성 정보를 전송하는 소스 장치를 식별한다. 제 2 인증부(72)는 소스 장치를 인증한다. 데이터 처리부(73)는 원본성 정보 데이터 또는 제 2 정보에 대응하는 데이터에 대한 처리를 수행한다.

도 12a 및 도 12b는 원본 데이터 유통 시스템내의 데이터 저장 시스템에 대한 구성을 도시한다.

도 12에 있어서, 디지털 티켓의 발행자는 발행자 장치(100)를 가지고, 디지털 티켓을 수신하는 이용자는 이용자 장치(200)를 가진다. 디지털 티켓을 발행할 때, 발행자 장치(100)와 이용자 장치(200) 사이에 통신 채널이 접속 장치(400)를 통해 형성된다. 발행자 장치(100)는 발행자 장치(100)에서 유효하게 되는 디지털 티켓을 이용자 장치(200)로 전송한다.

상술한 장치는 도 12a 및 도 12b에 도시된 것과 같이 구성될 수 있다. 도 12a는 IC 카드가 이용자 장치(200)로 사용되고 IC 카드 리더가 접속 장치(400)로 사용될 때의 구성을 도시한다. 도 12b는 IC 카드 또는 안전한 장소에 보유된 PC와 같은 부정 조작 방지 디바이스 이용자 장치로 사용되고 네트워크가 접속 장치(400)로 사용될 때의 구성을 도시한다. 도 12a 및 도 12b에 도시된 구성은 혼합될 수도 있다.

상술한 통신 채널은 발행 시작 시간에서 발행 종료 시간까지의 구간 동안에만 존재할 수도 있으며, 이것은 "양도", "소비" 및 "증정"의 경우에 적용된다.

디지털 티켓을 양도할 때, 통신 채널은 디지털 티켓을 발행할 때와 동일한 방식으로 통신 장치(400)를 통해 이용자 장치(200)들 사이에서 성립된다. 이어 디지털 티켓이 이용자 장치(200)들 사이에서 양도된다.

디지털 티켓의 개찰자는 개찰자 장치(300)를 가진다. 디지털 티켓을 소비할 때, 통신 채널은 디지털 티켓을 발행할 때와 동일한 방식으로 이용자 장치(200)와 개찰자 장치(300) 사이에서 통신 장치(400)를 통하여 성립된다. 이어, 유효한 디지털 티켓이 개찰자 장치(300)로 양도된다.

디지털 티켓을 증정할 때, 이용자 장치(200)가 유효한 디지털 티켓을 가진다는 증명서를 다른 이용자 장치 또는 개찰자 장치(300)로 제시하도록, 통신 채널은 이용자 장치들(200) 사이 또는 이용자 장치(200)와 개찰자 장치(300) 사이에서 통신 장치(400)를 통해 성립된다.

상술한 바와 같이, 본 발명의 데이터 저장 시스템은 하나 또는 다수의 발행자 장치(100), 하나 또는 다수의 이용자 장치(200) 및 하나 또는 다수의 개찰자 장치(300)를 포함하며, 이들은 일시적인 통신 채널을 제공하는 접속 장치(400)에 의해 접속된다.

이어서, 본 발명의 실시예를 도면을 참조하여 설명하도록 한다.

상술한 데이터 저장 시스템을 형성하는 각각의 장치는 도 13 내지 도16을 사용하여 설명하도록 한다. 아래에서의 표현을 위해 사용된 식의 의미는 제 1 실시예에서 사용된 것과 동일하다. 특히, 검증키 Pk2 및 S_{Pk1}에 의한 Pk2의 디지털 서명S_{Pk1}(Pk2)의 조합(Pk2, S_{Pk1}(Pk2))은 Pk1에 따른 Pk2의 키 증명서로 불린다. H(Pk)는 Pk의 해시값으로 불린다.

도 13은 본 발명의 실시예에 따른 발행자 장치를 도시한다.

도 13에 도시된 발행자 장치(100)는 제어부(110), 서명부(120), 데이터 생성부(130), 토큰 생성부(140) 및 신임 정보 생성부(150)를 포함한다.

제어부(110)는 검증키(PkI)를 가지며, 발행자 장치(100)가 디지털 티켓을 안전하게 유통시키도록 한다. PkI는 서명부(120)에서 제공된 서명 함수S_{PkI}에 대응하는 검증키이다. H(PkI)의 해시값은 발행자를 식별하는 식별자로서 사용된다. 제어부(110)에 대한 상세한 설명은 다음에 하도록 한다.

서명부(120)는 서명 함수S_{PkI}를 포함한다. S_{PkI}는 각각의 발행자 장치(100)에 대하여 상이하며, 서명부(120)에 의해 은닉된다.

데이터 생성부(130)는 발행자 장치(100)에서 생성된 정보 또는 외부에서 주어진 정보에 기초하여 데이터(m)를 생성한다. 본 발명의 데이터 저장 시스템에 따라, 데이터m의 내용에 대하여는 어떠한 제약도 없다. 이에 따라, 콘서트 티켓과 같은 일반적인 티켓의 권리를 표현하는 디지털 정보, 프로그램 데이터, 음악 데이터 이미지 데이터가 데이터 m으로 사용될 수 있다.

토큰 생성부(140)는 단방향 해시 함수 H를 가지며, 데이터 m과 검증키 PkI로부터 토큰(c_1,c_2)=(H(m),H(PkI))를 생성한다. c_2는 토큰의 발행자를 식별하는 해시값이 되는 토큰 발행자 정보이다. 여기에서 데이터 m의 해시는 c_1로 사용되며; 그러나, m을 식별하기 위한 식별자는 c_1로 사용될 수 있다.

신임 정보 생성부(150)는 신임 정보(t_1, t_2, t_3)를 생성한다. (t_1, t_2, t_3)는 서명부(120)를 사용하여

아래에 설명된 것과 같이 형성될 수 있다.

$t_1 = \{H(PkA_1), H(PkA_2),.....,H(PkA_n)\}$

$t_2 = S_{PkI}\{H(PkA_1) \| H(PkA_2) \| .... \| H(PkA_n)\}$

$t_3 = PkI$

여기에서 $H(PkA_1)$는 발행자에 의해 "신뢰받는" 후술할 제 3자를 식별하기 위한 해시값이다.

신임 정보는 또한 다음(t'_1, t'_2, t'_3, t'_4)과 같이 형성될 수도 있다.

$t'_1 = \{H(PkA_1), H(PkA_2),.....,H(PkA_n)\}$

$t'_2 = H(m)$

$t_3 = S_{PkI}(H(PkA_1) \| H(PkA_2) \| .... \| H(PkA_n) \| H(m))$

$t_4 = PkI$

이러한 경우, $H(PkA_1)$는 데이터m을 유통시키기 위하여 발행자가 신뢰하는 제 3자를 식별하기 위한 해시값이다.

게다가, 제 3자는 상술한 신임 정보가 반복적으로 구성될 수 있도록 신임 정보를 발행한다.

더욱이, 신임 정보는 각각의 발행자에 의해 생성되는 대신에 이용자 장치의 부정 조작 방지 디바이스의 제어부에 또는 개찰자 장치의 제어부에 미리 저장될 수 있다. 이러한 경우, 서명은 필수적인 것은 아니며, 신임 정보는 아래와 같이 ($t"_1$,$t"_2$) 또는 단지 $t"_1$로 구성될 수 있다.

$t"_1 = \{H(PkA_1), H(PkA_2),.....,H(PkA_n)\}$

$t"_3 = H(m)$

이러한 경우, $H(PkA_1)$는 데이터m을 유통시키기 위해 제어부를 형성하는 제 3자에 의해 신뢰받는 제 3자를 식별하기 위한 해시값이다.

이하, 신임 정보는 (t_1, t_2, t_3)로서 가정된다. 그러나, 상술한 임의의 신임 정보가 사용될 수도 있다.

도 14는 본 발명의 실시예에 따른 이용자 장치(200)이다.

이용자 장치(200)는 제어부(210), 저장부(220) 및 부정 조작 방지 디바이스(280)를 포함하며, 상기 부정 조작 방지 디바이스(280)는 제어부(230), 인증부(240), 서명부(250), 번호 발생부(260) 및 저장부(270)를 포함한다. 부정 조작 방지 디바이스(280)는 함수 및 상기 부분들의 내용물들이 부당하게 사용되는 것을 방지한다. 부정 조작 방지 디바이스(280)의 이용자조차도 부정 조작 방지 디바이스(280)를 부당하게 사용할 수 없다. 네트워크를 통해 제 3자에 의해 엄격하게 관리되는 서버 또는 IC 카드가 부정 조작 방지 디바이스(280)로 사용될 수 있다.

상기 제어부(210)는 발행자 정보$I_U = \{H(PkI_1), H(PkI_2),.....,H(PkI_n)\}$를 포함한다. 상기 제어부(210) 및 부정 조작 방지 디바이스(280)내의 제어부(23)는 디지털 티켓을 안전하게 유통하도록 이용자 장치(200)를 제어한다. I_U는 이용자가 신뢰하는 발행자를 나타내는 세트이고 임의의 시간에 이용자에 의해 업데이트될 수 있다. 상기 제어부(210)는 I_U내에 포함된 발행자에 의해 발행된 토큰이 유효한 지를 결정한다. 제어부(210)에 대한 상세한 설명은 다음에 하기로 한다.

추가로, I_U는 $I_U(m_i)=\{H(PkI_{i1}), H(PkI_{i2}),.....,H(PkI_{in})\}$으로 실현될 수도 있다. 즉, 발행자 정보 세트는 하나의 데이터에서 다른 데이터까지 다루어질 수 있다.

저장부(220)는 이용자에 의해 유지되는 서명된 데이터 세트M_u 및 발행자에 의해 서명된 서명을 가지는 신임 정보 세트T_u를 저장한다. 상기 데이터 세트들은 제어부(210)에 의해 업데이트될 수 있다.

제어부(230)는 검증키 PkU와 PkA 및 키 증명서(PkU,S_{PkA}(PkU)를 가진다. 제어부(230)는 디지털 티켓을 안전하게 유통하도록 이용자 장치를 제어한다. 여기에서 검증키PkU는 서명부내의 S_{PkU}에 대응한다. 그것의 해시 데이터H(PkU)는 이용자 장치를 식별하기 위한 식별자로서 사용된다. S_{PkA}는 부정 조작 방지 디바이스(280)에 의해 은닉되는 서명 함수이다. 제 3자는 IC 카드 제조업자, 부정 조작 방지 서버 관리자 등일 수 있다. 즉, 서명 함수(S_{PkU})를 포함하는 부정 조작 방지 디바이스(280)의 부정 조작 방지 능력은 서명 함수S_{PkA}를 가지는 제 3 자에 의해 보증된다. 제어부(230)에 대한 상세한 설명은 다음에 하기로 한다. PkA는 S_{PkA}의 검증키이다.

인증부(240)는 검증기(V)를 포함한다.

상기 서명부(250)는 서명 함수S_{PkU}를 가진다. 각각의 이용자 장치는 상이한 서명 함수S_{PkU}를 가진다. 상기 함수S_{PkU}는 서명부(250)에 의해 은닉된다.

번호 발생부(260)는 다음 번호r_U를 저장한다. 번호 발생부(260)가 번호를 발생시키도록 요구될 때, 번호 발생부(260)는 현재 번호(r_U)를 발생하고 r_U를 증가시킨다.

저장부(270)는 토큰 세트C_U 및 번호 세트 R_U를 저장한다. 이러한 세트들은 제어부(230)에 의해 업데이트될 수 있다.

도 15는 본 발명의 실시예에 따른 개찰자 장치(300)의 블록도이다. 개찰자 장치(300)는 제어부(310), 인증부(320), 번호 발생부(330) 및 저장부(340)를 포함한다.

제어부(310)는 검증키PkE 및 발행자 정보I_E = {H(PkI_1), H(PkI_2), ..., H(PkI_n)}를 가지며, 디지털 티켓을 안전하게 유통하도록 개찰자 장치(300)를 제어한다. I_E는 개찰자에 의해 신뢰받는 발행자를 나타내는 세트이고 임의의 시간에 발행자에 의해 업데이트될 수 있다. 제어부(310)는 I_E내에 포함된 발행자에 의해 발행된 토큰이 유효한지를 결정하여 단지 유효한 토큰을 가지는 디지털 티켓을 소비하는 서비스를 제공한다. 제어부(310)의 동작에 대한 상세한 설명은 이후에 하도록 한다.

게다가, 제어부(210)의 I_U와 동일한 방식으로 I_E는 $I_E(m_I)$ = {H(PkI_{i1}), H(PkI_{i2}), ..., H(PkI_{in})}로서 실현될 수 있다. 즉, 발행자정보는 하나의 데이터에서 다른 데이터까지 다루어진다.

인증부(320)는 검증기(V)를 포함한다.

번호 발생부(330)는 다음 번호r_E를 저장한다. 번호 발생부(330)가 번호를 발생시키도록 요구될 때, 번호 발생부(330)는 현재 번호(r_E)를 발생시키고 r_E를 증가시킨다. 상기 r_E는 양수이다.

저장부(340)는 번호 세트 R_E를 저장한다. 상기 세트는 제어부(310)에 의해 업데이트될 수 있다.

도 16은 본 발명의 실시예에 따른 접속 장치(400)의 블록도이다.

접속 장치(400)는 통신부(410)를 포함한다. 상기 통신부(410)는 발행자 장치(100), 이용자 장치(200) 및 개찰자 장치(300) 사이에 또는 이용자 장치들 사이에 일시적 또는 영구적인 통신 채널을 제공한다. 키오스크에 IC 카드 슬롯을 가지는 단말기, 네트워크를 통해 접속된 다수의 PC 또는 이와 유사한 것들이 접속 장치(400)로서 사용될 수 있다.

상술한 장치를 사용하여 디지털 티켓을 안전하게 유통시키는 방법은 다음과 같다.

이하, 디지털 티켓의 유통 방법은 ; (1) 디지털 티켓 발행, (2) 디지털 티켓의 양도 및 (3) 디지털티켓의 소비의 각각의 경우에 대하여 설명하도록 한다. 다음의 설명에서, 장치들 간의 통신은 접속 장치(400)의 통신부(410)를 통해 행하여진다.

(1) 디지털 티켓의 발행

도 17은 본 발명의 실시예에 따른 처리에 대한 시퀀스 챠트이다. 도 17에서, 발행자 장치(100)와 이용자 장치(200) 사이에 존재하는 접속 장치(400)는 도시되지 않았다.

단계 1101) 발행자 장치(100)의 제어부(110)는 데이터 생성부(130)에서 데이터m을 취득한다. 상기 데이터m은 권리 정보를 나타내는 디지털 티켓이다.

단계 1102) 발행자 장치(100)의 제어부(110)는 토큰 생성부(410)가 토큰(c_1,c_2) = (H(m), H(PkI))를 생성하도록 토큰 생성부(410)로 데이터m을 제공한다.

단계 1103) 제어부(10)는 신임 정보 생성부(150)로부터 신임 정보(t_1,t_2,t_3)를 취득한다. 상기 신임 정보의 구성은 앞서 설명되었다.

단계 1104) 제어부(110)는 m 및 신임 정보(t_1,t_2,t_3)를 이용자 장치(200)내의 제어부(210)로 전송한다.

단계 1105) 이용자 장치(200)의 제어부(210)는 m을 저장부(220)의 M_U내에 추가하고 저장부(220)의 t_U내에 (t_1,t_2,t_3)를 추가하여 상기 저장부(220)내에 그들을 저장한다.

단계 1106) 제어부(210)는 제어부(230)가 세션 정보(s_1,s_2)를 생성하도록 요구한다.

제어부(230)는 다음의 절차에 따라 세션 정보(s_1,s_2)를 생성하여 제어부(210)로 전송한다.

(a) 제어부(230)는 부정 조작 방지 디바이스(280)내의 번호 발생부(260)에 의해 생성된 번호r_U를 취득한다.

(b) 번호r_U는 저장부(270)내에서 번호 세트R_U에 추가된다.

(c) 세션 정보(s_1,s_2)=(H(PkU), r_U)가 생성된다. 여기에서 PkU는 제어부(210)에 의해 유지되는 검증키이다.

단계 1107) 제어부(210)는 세션 정보(s_1,s_2)를 발행자 장치(100)의 제어부(110)로 전송한다.

단계 1108) 발행자 장치의 제어부(110)는 서명부(120)의 S_{PkI}를 사용하여 토큰 교환 포맷 e = (e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8)를 취득하고, 제어부(110)에 의해 유지되는 검증키PkI를 취득한다. e의 각 요소는 다음과 같다. 디지털 티켓을 발행할 때, e_7 및 e_8이 더미 데이터이기 때문에 e_7 및 e_8은 소정의 값을

취한다.

$e_1 = c_1$

$e_2 = c_2$

$e_3 = s_1$

$e_4 = s_2$

$e_5 = S_{Pkl}(c_1 \parallel c_2 \parallel c_3 \parallel c_4)$

$e_6 = Pkl$

e_7 = 임의의 값

e_8 = 임의의 값

단계 1109) 제어부(110)는 e를 이용자 장치(200)의 제어부(210)로 전송한다.

단계 1110) 제어부(210)는 e를 제어부(230)로 전송하여 제어부(230)가 e를 저장하도록 요구한다.

단계 1111) 부정 조작 방지 디바이스(280)의 제어부(230)는 인증부(240)를 사용하여 다음의 식들이 만족되는 지를 검증한다. 검증이 실패한 경우, 이후의 처리는 인터럽트되며, 제어부(230)는 발행자 장치(100)내 제어부(110)의 처리 인터럽트를 제어부(210)를 통해 인지한다.

$e_3 = H(PkU)$ (1)

$e_4 \in R_U$ (2)

$V_{e6}(e_1 \parallel e_2 \parallel e_3 \parallel e_4, e_5) = 1$ (3)

$e_2 = H(e_6)$ (4)

상술한 식(1)과 식(2)은 세션 정보의 유효성 검증을 의미한다. 검증을 사용하여 부정 행위가 방지된다. 예를 들어 이러한 부정 행위는 다른 이용자 장치에 토큰 교환 포맷을 저장 또는 토큰 교환 포맷을 재이용한 토큰 복제 등이 될 수 있다.

식(3)은 토큰 교환 포맷의 서명에 대한 유효성 검증을 의미한다. 검증에 따라, 토큰 교환 포맷에 대한 부당한 사용이 방지될 수 있다.

식(4)은 토큰의 서명자 이외의 다른 발행자에 의해 발행된 토큰을 저장하는 것이 방지된다.

단계 1112) 이용자 장치(200)내의 부정 조작 방지 디바이스(280)의 제어부(230)는 저장부(270)내의 번호 세트R_U에서 $e_4(=r_U)$를 삭제한다.

단계 1113) 제어부(230)는 저장부(270)내의 C_U에 (e_1, e_2)를 추가한다.

단계 1114) 제어부(230)는 (e_1, e_2)을 제어부(210)로 전송하여 정상적인 종료를 인지하도록 한다.

단계 1115) 제어부(210)는 다음의 식이 만족되는 지를 검증한다. 검증이 실패한 경우, 처리는 인터럽트되고, 제어부(230)는 발행자 장치(100)내의 제어부(110)에 대한 처리 인터럽트를 인지한다.

$e_1 = H(m)$ (5)

$e_2 \in I_U$ (6)

식(5) 및 식(6)은 전송된 토큰이 실제 디지털 티켓에 대응하는 지와 적합한 발행자에 의해서 발행되었는지에 대한 검증을 의미한다. 상기 검증에 따라, 발행된 티켓이 유효한지가 검증된다.

(2) 디지털 티켓의 양도

접속 장치(400)를 통한 이용자 장치(200a)에서 이용자 장치(200b)로의 디지털 티켓 양도 처리를 설명하도록 한다.

도 18 및 도 19는 본 발명의 실시예에 따른 디지털 티켓 양도 처리를 도시한 시퀀스 챠트이다. 도 18 및 도 19에서, 두 개의 이용자 장치(200a, 200b) 사이에 존재하는 접속 장치(400)는 도시되지 않았다. 여기에서 "a"는 이용자 장치(200a)의 각 요소의 명칭에 부가되었고 "b"는 이용자 장치(b)의 각 요소의 명칭에 부가된다.

단계 2201) 제어부(210a)는 저장부(220a)에 의해 유지되는 세트M_{Ua}에서 전송될 대상이 되는 디지털 티켓을 추출한다.

단계 2202) 이용자 장치(200a)의 제어부(210a)는 저장부(220a)내에 포함된 m 발행자에 의해 생성된 신임 정보(t_1, t_2,t_3)를 T_{Ua}에서 추출한다.

단계 2203) 제어부(210a)는 m 및 (t_1, t_2,t_3)을 이용자 장치(220b)의 제어부(210b)로 전송한다.

단계 2204) 제어부(210b)는 저장부(220b)내의 세트M_{Ub}내에 m을 저장하고 저장부(220b)내의 세트T_{Ub}내에 (t_1, t_2,t_3)를 저장한다.

단계 2205) 제어부(210b)는 부정 조작 방지 디바이스(280b)내의 제어부(230b)로 세션 정보(s_1,s_2)를 생성할 것을 요구한다.

제어부(230b)는 다음의 절차에 따라 세션 정보(s_1,s_2)를 생성하고, 그것을 제어부(210b)로 전송한다.

(a) 제어부(230b)는 부정 조작 방지 디바이스(280b)내의 번호 발생부(260b)에 의해 생성된 번호r_{Ub}를 취득한다.

(b) 번호 r_{Ub}는 부정 조작 방지 디바이스(280b)내의 저장부(270b)내의 번호 세트R_{Ub}에 추가된다.

(c) 세션 정보(s_1,s_2) = (H(PKUb),r_{Ub})가 생성된다. 여기에서 PkUb는 제어부(210b)에 의해 유지되는 검증키이다.

단계 2206) 제어부(210b)는 세션 정보(s_1,s_2)를 이용자 장치(200)의 제어부(210a)로 전송한다. 추가로, 발행자 정보I_{Ub}는 세션 정보(s_1,s_2)와 함께 전송된다. 발행자 정보에 대한 통고를 미리 제공함으로써, 식(16) 또는 식(26)을 만족시키지 않는 토큰 교환 포맷의 발생 및 전송은 방지될 수 있다.

단계 2207) 제어부(210a)는 (s_1,s_2) 및 전송될 디지털 티켓의 해시값 H(m)를 제어부(230a)로 전송한다.

단계 2208) 부정 조작 방지 디바이스(280a)의 제어부(230a)는 다음의 식이 저장부(270a)에 저장된 C_{Ua}에 대하여 만족되는 지를 검증한다.

$$\exists c_2((H(m),c_2)\in C_{Ua}),\ c_2 \in I_{Ub} \qquad (7)$$

검증이 실패할 때, 이후의 처리는 인터럽트되고 제어부(210a)는 이러한 실패를 인지한다.

상기 식(7)은 전송될 디지털 티켓m에 대응하는 토큰(H(m), c_2))이 저장부(270a)내에 저장되었는 지에 대한 검증을 의미한다.

단계 2209) 부정 조작 방지 디바이스(280a)의 제어부(230a)는 서명부(250a)내에 포함된 S_{PkUa}와 이용자 장치(200a)의 제어부(210a)에 포함된 증명키 PkUa, PkAa 및 키 증명서(PkUa‖S_{PkAa}(PkUa))를 사용하여 토큰 교환 포맷 e = (e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8)를 취득한다. e의 각 요소는 다음과 같다.

e_1 = H(m)

e_2 = c_2

e_3 = s_1

e_4 = s_2

e_5 = S_{PkUa}(H(m) ‖ c_2 ‖ s_1 ‖ s_2)

e_6 = PkUa

e_7 = S_{PkAa}(PkUa)

e_8 = PkAa

단계 2210) 제어부(230a)는 s_2가 양이 될 경우 C_{Ua}에서 (H(m), c_2)를 삭제한다.

단계 2211) 제어부(230a)는 e를 제어부(210a)로 전송한다.

단계 2212) 제어부(210a)는 e를 이용자 장치(200b)의 제어부(21b)로 전송한다.

단계 2213) 제어부(210b)는 e 및 신임 정보 t를 부정 조작 방지 디바이스(280b)의 제어부(230b)로 전송한다. 제어부(210b)는 e내에 토큰을 저장할 것을 요구한다.

단계 2214) 제어부(230b)는 인증부(240b)를 사용하여 아래의 모든 식이 만족되어지는 지를 검증한다. 검증이 실패한 경우, 처리는 인터럽트되며, 제어부(210b)는 인터럽트를 인지한다.

$$e_3 = H(PkUb) \qquad (8)$$

$$e_4 \in R_{Ub} \qquad (9)$$

$$V_{e6}(e_1 ‖ e_2 ‖ e_3 ‖ e_4,\ e_5) = 1 \qquad (10)$$

$$V_{e8}(e_6,\ e_7) = 1 \qquad (11)$$

$$H(e_8) \in t_1 \qquad (12)$$

$$V_{t3}(t_1, t_2) = 1 \quad (13)$$

$$e_2 = H(t_3) \quad (14)$$

상기 식(8) 및 식(9)은 세션 정보의 유효성에 대한 검증을 의미한다. 검증에 따라, 이용자 장치(200b) 이외의 다른 이용자 장치에 토큰 교환 포맷을 저장, 토큰 교환 포맷을 재사용한 토큰 복제 등과 같은 부정 행위가 방지된다.

식(10)은 토큰 교환 포맷의 서명자에 대한 유효성에 대한 검증을 의미한다. 상기 검증에 따라, 토큰 교환 포맷에 대한 부당한 사용이 방지될 수 있다.

식(11)은 서명자의 키 증명서에 대한 검증을 의미한다. 식(12)은 신임 정보내의 신임 대상에 키 증명서의 서명자가 포함되는 지에 대한 검증을 의미한다. 식(13) 및 식(14)은 신임 정보의 서명자가 토큰 발행자와 동일한 지에 대한 검증을 의미한다. 검증에 따라, 토큰 교환 포맷의 소스에 대한 부정 조작 방지 능력이 발행자가 신뢰하는 제 3자에 의해 보증된다는 것이 검증된다.

단계 2215) 제어부(230b)는 저장부(270b)내의 번호세트R_{Ub}에서 $e_4(=r_{Ub})$를 삭제한다.

단계 2216) 제어부(230b)는 저장부(270b)내의 세트C_{Ub}에 (e_1,e_2)를 추가한다.

단계 2217) 제어부(230b)는 제어부(210b)가 처리를 정상적 완료한 것을 인지한다.

단계 2218) 제어부(210b)는 아래의 모든 식이 만족되는 지를 검증한다. 검증이 실패하면, 처리는 인터럽트되고 제어부(210a)는 상기 인터럽트를 인지한다. 검증이 성공적이면, 제어부(210a)는 처리의 정상적인 완료를 인지한다.

$$e_1 = H(m) \quad (15)$$

$$e_2 \in I_{Ub} \quad (16)$$

식(15) 및 식(16)은 전송된 토큰이 실제 디지털 티켓에 대응하는 지와 적합한 발행자에 의해서 발행되었는지에 대한 검증을 의미한다. 상기 검증에 따라, 양도된 티켓이 유효한 지가 검증된다.

발행자 정보가 제어부(210b)에서 데이터 단위로 다루어질 때, $e_2 \in I_{Ub}(m)$이 식(16)을 대신한다.

(3) 디지털 티켓의 소비

접속 장치(400)를 통한 이용자 장치(200)로부터 개찰자 장치(300)로의 디지털 티켓 소비 처리를 설명하도록 한다.

도 20은 본 발명의 실시예에 따른 티켓 소비 처리의 시퀀스 챠트이다. 도 20에서 이용자 장치(200)와 개찰자 장치(300) 사이에 존재하는 접속 장치(400)는 도시되지 않았다

단계 3301) 제어부(210)는 소비될 디지털 티켓 m을 저장부(220)에 포함된 세트M_U에서 추출한다.

단계 3302) 제어부(210)는 m의 발행자(m)에 의해 서명된 신임 정보(t_1, t_2, t_3)를 저장부(220)내에 포함된 세트T_U에서 추출한다.

단계 3303) 제어부(210)는 m 및 (t_1, t_2, t_3)을 발행자 장치(300)의 제어부(310)로 전송한다.

단계 3304) 제어부(310)는 다음의 절차에 따라 세션 정보(s_1,s_2)를 생성한다.

(a) 제어부(310)는 번호 발생부(330)로부터 번호r_E를 취득한다.

(b) 번호r_E는 저장부(340)내의 번호 세트R_E에 추가된다.

(c) 세션 정보$(s_1,s_2)=(H(PkE),r_E)$가 생성된다. 여기에서 PkE는 제어부(310)에 의해 유지되는 검증키이다.

단계 3305) 제어부(310)는 세션 정보(s_1,s_2)를 이용자 장치(200)의 제어부(21)로 전송한다.

단계 3306) 제어부(210)는 (s_1,s_2) 및 소비될 디지털 티켓의 해시값 H(m)를 부정 조작 방지 디바이스(280)의 제어부(230)로 전송한다.

단계 3307) 제어부(230)는 저장부(270)에 저장된 세트C_U에 대하여 다음의 식이 만족되는 지를 검증한다.

$$\exists c_2((H(m),c_2) \in C_U) \quad (17)$$

검증이 실패할 때, 이후의 처리는 인터럽트되고 제어부(210)는 이러한 실패를 인지한다.

상기 식(17)은 소비될 디지털 티켓m에 대응하는 토큰$(H(m), c_2))$이 부정 조작 방지 디바이스(280)의 저장부(270)내에 저장되었는 지에 대한 검증을 의미한다.

단계 3308) 제어부(230)는 서명부(250)내에 포함된 S_{PkU}와 제어부(210)에 포함된 증명키 PkU, PkA 및 키 증명서$PkU \| S_{PkA}(PkU)$를 사용하여 토큰 교환 포맷 $e = (e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8)$를 취득한다. e의 각 요소는 다음과 같다.

$e_1 = H(m)$

$e_2 = c_2$

$e_3 = s_1$

$e_4 = s_2$

$e_5 = S_{PkU}(H(m) \| c_2 \| s_1 \| s_2)$

$e_6 = PkU$

$e_7 = S_{PkA}(PkU)$

$e_8 = PkA$

단계 3309) 부정 조작 방지 디바이스(280)의 제어부(230)는 s_2가 양이 될 때, C_U에서 $(H(m), c_2)$를 삭제한다.

단계 3310) 제어부(230)는 e를 제어부(210)로 전송한다.

단계 3311) 제어부(210)는 e를 개찰자 장치(300)의 제어부(310)로 전송한다.

단계 3312) 제어부(310)는 인증부(320)를 사용하여 아래의 모든 식이 만족되어지는 지를 검증한다. 검증이 실패한 경우, 처리는 인터럽트되며, 이용자 장치(200)의 제어부(210)는 인터럽트를 인지한다.

$e_3 = H(PkE)$ (18)

$e_4 \in R_E$ (19)

$V_{e6}(e_1 \| e_2 \| e_3 \| e_4, e_5) = 1$ (20)

$V_{e8}(e_6, e_7) = 1$ (21)

$H(e_8) \in t_1$ (22)

$V_{t3}(t_1, t_2) = 1$ (23)

$e_2 = H(t_3)$ (24)

상기 식(18, 19)은 세션 정보의 유효성 검증을 의미한다. 검증에 따라, 개찰자 장치(300)이외의 다른 개찰자 장치에 토큰 교환 포맷을 저장하고 토큰 교환 포맷을 재사용하기 위하여 토큰을 복제하는 것과 같은 부정 수단이 방지된다.

식(20)은 토큰 교환 포맷의 서명자의 유효성 검증을 의미한다. 이러한 검증에 따라, 토큰 교환 포맷의 부정사용이 방지될 수 있다.

식(21)은 서명자의 키이 증명서의 검증을 의미한다. 식(22)은 키이 증명서의 서명자은 신임 정보의 신임 대상에 포함되었는지를 검증한다. 식(23)은 신임 정보의 유효성의 검증을 의미한다. 식(24)은 신임 정보의 서명자이 토큰 발행자와 동일한지를 검증한다. 상기 검증에 따라, 토큰 교환 포맷의 소스의 부정조작 방지 능력이 발행자에 의하여 신뢰되는 당사자에 의해 보증되는 지가 검증된다.

단계 3313) 개찰자 장치(300)의 제어부(310)는 저장부(340)의 R_E로부터 $e_4(=r_E)$를 삭제한다.

단계 3314) 제어부(310)는 이하의 모든 식이 만족되는 지를 검증한다. 검증이 실패하면, 이용자 장치(200)의 제어부(210)에는 프로세스 간섭이 통지된다. 검증이 성공하면, m에 대응하는 서비스가 소비자에게 제공된다.

$e_1 = H(m)$ (25)

$e_2 \in I_E$ (26)

식(25, 26)은 전송된 토큰이 해당 디지털 정보에 대응하는지 그리고 적당한 발행자에 의하여 발행되었는지를 검증함을 의미한다. 상기 검증에 따라, 소비된 티켓이 유효한지를 검증한다.

이용자 정보가 제어부(310)의 데이터 단위로 관리될 때, $e_2 \in I_E(m)$은 식(26)대신 대체된다.

(4) 디지털 티켓 증정

디지털 티켓의 증정은 다음과 같이 티켓 소비 프로세스를 변형함으로써 구현될 수 있다.

- 제어부(310)는 단계(3304)의 (c)에서 $(s_1, s_2)=(H(PkE), -r_E)$를 생성한다.

식 $-e_4 \in R_E$는 단계(3312)에서 식(19)으로 대체된다.

상기 변형예에 따르면, s_2는 음이 되기 때문에, $(H(m), c_2)$는 단계(3309)의 C_u로부터 삭제되지 않는다. 즉, 유효 디지털 티켓이 이용자 장치에 남아 있는 동안 이용자 장치가 증정시에 유효 디지털 티

켓을 가지고 있는 지를 검증하는 것이 가능하다. 따라서, 디지털 티켓의 검사가 가능하다.

상기 설명(1-4)에서, 전송된 토큰 교환 포맷은 명확하게 저장되지 않는다. 한편, 저장부(220)에 토큰 교환 포맷의 저장이 이루어진다. 즉, 이용자 장치는 m을 전송할 때 토큰 교환 포맷의 이력을 전송할 수 있다. 그 결과, 부정 수단(이중 사용)이 발견될 때 부정사용하는 장치를 식별하는 것이 가능하다. 상기와 같은 부정 수단은 예를 들어 부정조작 방지 디바이스(28)를 고장나게 하는 것일 수 있다.

(5) 디지털 티켓 반환

개찰자는 소비되거나 증정된 디지털 티켓을 발행자에게 반환할 수 있다. 다음에, 발행자는 개찰자에게 가치를 지불할 수 있다. 따라서, 요금과 같은 가치는 이중 청구를 방지하면서 디지털 티켓을 개찰 또는 검사한 발행자에게 지불될 수 있다.

다음에 반환 프로세스가 설명된다.

발행자 장치(100)는 토큰 교환 포맷(e)을 저장하는 부분(저장부(160)) 및 반환된 토큰 및 신임 정보(t_1, t_2, t_3)에 대응하는 데이터(m)를 저장 또는 취득하는 부분을 더 포함한다.

소비되거나 증정된 디지털 티켓을 발행자 장치(300)에 반환하는 프로세스가 이하에 설명된다.

단계 5501) 발행자 장치(300)는 소비되거나 증정된 토큰 교환 포맷(e)을 발행자 장치(100)에게 전송한다.

단계 5502) 발행자 장치(100)의 제어부(100)는 식 e_2 =H(PkI)를 만족하는지를 검증하는데, 여기서 e_2는 e에 포함되어 있다. 검증에 실패하면, 발행자 장치는 실패를 표시하고 프로세스는 인터럽트된다. 상기 검증에 의하여, 발행자 장치(100) 자신에 의하여 발행된 디지털 티켓이 e와 대응하는지가 검증된다.

단계 5503) 제어부(110)는 e에 대하여 식(20-22)을 만족하는지를 검증한다. 신임 정보(t_1, t_2, t_3)가 신뢰할 수 없는 경로를 경유하여 (예를 들어, 발행자를 경

유하여) 취득될 때, 식(23, 24)이 또한 검증된다. 이 경우, 식(24)을 검증할 때, PkI는 t_3대신 대체된다. 검증이 실패하면, 발행자 장치(300)는 실패를 표시하고 프로세스는 인터럽트된다. 이러한 검증에 의하여, e가 유효한 유통 경로를 통하여 유통되는지가 검증된다.

단계 5504) 제어부(110)는 e_3의 부정조작 방지 능력이 t_1에 의하여 신뢰되는 어느 제삼자에 의하여 보증되지 않음을 검증하는데, e_3은 e_4가 양일 때 e에 포함된다. 따라서, 유효 토큰이 저장되지 않았는지, 즉 토큰의 권리가 소비에 의하여 종료되었는지가 검증된다.

단계 5505) 제어부(110)는 저장부(160)에 e를 저장한다. e가 이미 저장부(160)에 저장되어 있다면, 발행자 장치(300)는 실패를 표시하며 프로세스는 인터럽트된다.

단계 5506) 발행자는 반환된 디지털 티켓에 따른 가치를 발행자에게 제공한다.

(6) 티켓 북

티켓 북은 토큰 교환 포맷의 토큰에 번호 정보 또는 시간 정보를 추가함으로써 구현될 수 있다. 번호 정보는 티켓 번호일 수 있다.

따라서, 동일 발행자에 의하여 발행되고 동일한 콘텐츠를 가진 다수의 디지털 티켓이 발행될 때, 디지털 티켓은 적합하게 처리될 수 있고 다수의 동일한 토큰은 효율적으로 전송될 수 있다.

특히, 상기 실시예를 변형함으로써, 티켓 북이 구현될 수 있다.

- 번호 정보(C_3)는 토큰에 추가된다.

- 번호 정보(e_n)는 토큰 교환 포맷에 추가된다.

- 디지털 티켓 발행 프로세스에서, 티켓 번호는 토큰이 발생될 때 N으로서 특정된다(단계 1102).

- 디지털 티켓 양도/소비 프로세스에서, 단계(2207) 또는 단계(3306)가 수행될 때, 양도/소비될 디지털 티켓의 번호는 n으로서 특정된다.

- 디지털 티켓 양도/소비 프로세스에서, 토큰이 단계(2208) 또는 단계(3307)에 저장되었음이 검증될 때, 티켓 번호가 적당하다는 것이 검증된다. 즉, C_u는 (c_1, c_2, c_3)을 포함하며, 여기서 c_1 =H(m)∩c_3≥n을 만족한다.

- 토큰 교환 포맷이 단계(1108), 단계(2209) 또는 단계(3308)에서 생성될 때, e_n = n이 추가되고 n이 추가되고 e_5에 서명될 대상에 연결되어 c_1 ‖ c_2 ‖ s_1 ‖ s_2 ‖ n이 얻어지도록 한다.

- 양도/소비 프로세스에서, 토큰을 삭제할 때(s_2가 단계(2201) 또는 단계(3309)에서 양일 때), (H(m), c_2, c_3)는 c_3 = n을 만족할 때만 c_u로부터 삭제된다. c_3 〈n일 때, c_u에서 (H(m), c_2, c_3)는 (H(m), c_2, c_3-n)으로 갱신된다.

- 단계(1111), 단계(2214) 또는 단계(3312)에서 토큰 교환 포맷을 검증할 때, e_n은 추가되고 e_5(

식(3), (10) 및 (20))에 의하여 서명 검증이 검증될 대상과 연결되어 $e_1 \| e_2 \| e_3 \| e_4 \| e_n$이 얻어진다.

- 디지털 티켓 발행/양도 프로세스에서, 단계(1113) 또는 단계(2216)에서 토큰을 저장할 때, c_u가 이미 토큰(c_1, c_2, c_3)을 포함하고 $e_1=c_1$ 및 $e_2=c_2$가 만족될 때, c_u의 토큰(c_1, c_2, c_3)은 (c_1, c_2, c_3+e_n)으로 갱신된다.

- 디지털 티켓의 소비/반환 프로세스에서, 서비스 또는 가치는 e_n에 따라 여러 번 제공된다.

(7) 재전송 제어

토큰은 경로의 의도치 않은 중단과 같은 비정상 상태가 발생한 후에 복제를 방지하면서 재전송될 수 있다. 다음에 재전송 프로세스가 설명된다. 특히, 다음 프로세스는 전술한 실시예들에 일부 단계가 부가되었다.

- 제어부(110) 또는 (230)은 단계(1108), 단계(2209) 또는 단계(3308)에서 생성된 토큰 교환 포맷(e)을 유지한다.

- 제어부(210) 또는 (310)은 수신 응답이 단계(1115), 단계(2218)의 완료 또는 단계(3314)에서 서비스 제공시 전송되었을 때 (s_1, s_2)의 디지털 티켓을 전송한 제어부(110) 또는 (210)을 통지한다.

- 제어부(110, 210)는 수신 응답이 수신된 후에 (s_1, s_2)에 대응하는 토큰 교환 포맷을 삭제한다.

재전송을 수행할 때, 상기 실시예의 일부 단계는 다음과 같이 변형된다.

- 세션 정보가 단계(1106), (2205) 또는 (3304)에서 취득될 때, 세션 정보는 새롭게 생성되지 않는다. 대신, 저장부(220) 또는 9340)에 저장된 세션 정보(s_1, s_2)가 이용된다.

- 단계(1108), 단계(2208-2210) 및 단계(3307-3309)에서, 제어부(110) 또는 (210)이 e를 가지며, $(e_3=s_1) \cap (e_4=s_2)$이 만족될 때, e는 새롭게 생성되지 않으며 보유된 e가 사용된다.

(8) 발행 변경

디지털 티켓의 발행은 티켓(토큰) 생성 및 티켓의 논리적 양도로 생각할 수 있기 때문에, 디지털 티켓은 예를 들어 이하에 설명된 티켓 양도 프로세스를 이용하여 발행될 수 있다. 프로세스에 필요한 처리량은 전술한 티켓 발행 프로세스와 비교해서 증가하는데, 이는 티켓 양도의 검증 프로세스가 티켓 발행의 검증 프로세스보다 복잡하기 때문이다.

(8-1) 자기-증명서 이용

전술한 프로세스에 따르면, 제어부(230)에 의한 토큰 교환 포맷의 검증 프로세스는 티켓 발행(단계 1111) 및 티켓 양도(단계 2214)사이에서 상이하다. 구현 비용은 검증 프로세스를 단계(2214)에서 하나로 단일화시킴으로써 감소될 수 있다.

제어부(110)는 자체적으로 키이 증명서(PkI, S_{PkI}(PkI))를 포함한다. 이하에 설명하는 바와 같이, 티켓 발행 프로세스를 변형함으로써, 수신측에 있는 제어부(230)의 프로세스가 통일될 수 있다.

- 신임 정보 생성부(150)가 단계(1103)에서 신임 정보를 생성할 때 발행자 장치는 발행자에 의하여 신임 대상(t_1)에 자체 해시값H(PkI)를 포함한다.

- $e_7=S_{PkI}$(PkI) 및 e_8=PkI는 토큰 교환 포맷 e가 단계(1108)에서 생성될 때 이용된다.

-식(8)-(14)은 토큰 교환 포맷 e가 단계(1111)에서 검증될 때 식(1-4)대신 이용된다. U는 Ub 대신 대체된다.

(8-2) 이용자 장치에 의한 디지털 티켓 발행

이하에 설명되는 바와 같이, 이용자 장치는 이용자 장치에 의하여 발행된 토큰을 생성할 수 있는 능력을 가지도록 함으로써 디지털 티켓을 발행할 수 있다.

프로세스는 이하에 설명된다. 설명에서, 데이터m은 이미 생성된 것으로 생각한다.

- 제어부(210)는 디지털 티켓 및 신임 대상 t_1=[H(PkA_1), H(PkA_2),..., H(PkA_i)]에 대응하는 데이터m의 해시값H(m)를 제어부(230)에 제공한다.

- 제어부(230)는 검증 키이(PkU)를 이용하여 저장부(270)에 (H(m), H(PkU))를 저장한다.

제어부(230)는 서명부(250)를 이용하여 $t_2=S_{PkU}$(H(PkA_1) $\|$ H(PkA_2) $\|$ ... $\|$ H(PkA_i))를 생성한다.

- 제어부(230)는 (t_1, t_2, t_3)을 제어부(210)로 반환한다. 제어부(210)는 저장부(220)에 (t_1, t_2, t_3)를 저장한다. 다음에, 디지털 티켓이 전송된다.

상기 티켓 반환, 티켓 북, 재전송 제어 및 발행 검증의 예는 제 1실시예에 적용될 수 있다.

발행자 장치(100), 이용자 장치(200) 또는 개찰자 장치(300)의 각 엘리먼트는 프로그램에 의하여 구성될 수 있다. 프로그램은 발행자 장치, 이용자 장치 또는 개찰자 장치로서 사용될 수 있는 컴퓨터에 연결된 디스크 유니트에 저장될 수 있다. 프로그램은 또한 플로피 디스크, CD-롬 등과 같은 휴대용 컴퓨터 판독가능 매체에 저장될 수 있다. 프로그램은 컴퓨터 판독가능 매체로부터 컴퓨터에 설치될 수 있

어 본 발명은 컴퓨터에 의하여 구현되도록 한다.

도 21은 상기와 같은 컴퓨터의 하드웨어 구성을 도시하는 블록도이다. 도 21에 도시된 바와 같이, 컴퓨터 시스템은 프로그램의 프로세스가 수행되는 CPU(500), 데이터와 프로그램을 임시로 저장하는 메모리(501), 메모리(501)에 로딩될 데이터와 프로그램을 저장하는 외부 저장 유니트(502), 데이터를 디스플레이하기 위한 디스플레이(503), 데이터 또는 명령을 입력하는 키보드(504) 및 네트워크를 통하여 컴퓨터 시스템이 다른 컴퓨터와 통신하도록 하는 통신 처리 유니트(505)를 포함한다. 프로그램은 외부 저장 유니트(502)에 설치되고 메모리(501)에 로딩되고 CPU(500)에 의하여 수행된다.

발명의 효과

전술한 바와 같이, 본 발명의 제 2실시예에 따르면, 토큰은 발행자 및 이용자 또는 발행자에 의하여 식별된 개찰자 장치에 의하여 신뢰되는 경로를 통해서만 전송될 수 있다. 따라서, 토큰의 토큰 발행자 정보에 의하여 표시된 발행자 이외의 사람이 토큰 저장부에 새롭게 저장하는 데이터에 상응하는 토큰의 발생이 방지될 수 있다. 또한, 토큰이 양도되는 동안 다수의 토큰 저장부에 토큰이 복제되는 것이 방지될 수 있다.

또한, 원본과 같은 특정 발행자에 의하여 발행된 토큰을 데이터와 연관시킴으로써, 발행자에 의하여 원본 데이터의 번호 발행을 제한하는 것이 가능하다.

또한, 네트워크에서 데이터로서 존재하는 URL과 같은 정보 식별자를 이용함으로써, 복제될 수 없고 양도될 수 있는 정보의 엑세스 권리가 제공될 수 있다.

또한, 정확한 콘텐츠를 가진 티켓을 이용하거나 티켓 식별자를 이용함으로써 유효한 토큰을 가진 티켓만이 유효한 티켓으로 간주되며 이용자 또는 개찰자는 유효한 티켓이외의 티켓을 거절할 수 있다. 따라서, 티켓의 부정사용(예를 들어, 이중 사용 및 불법적 복제)이 방지될 수 있다.

또한, 본 발명의 데이터로서 프로그램을 이용하고 프로그램 라이센스로서 특정 발행자에 의하여 발행된 토큰을 사용함으로써 프로그램의 불법적 복제 및 사용이 방지될 수 있다. 이 경우, 프로그램 수행 장치는 토큰을 가진 프로그램이외의 프로그램 수행을 거절할 수 있다.

또한, 본 발명의 데이터로서 뮤직 데이터 또는 이미지 데이터를 이용함으로써, 특정 발행자에 의하여 발행된 토큰이 적당한 권리로서 이용되는 뮤직 데이터 또는 이미지 데이터의 불법적인 복제 및 사용이 방지될 수 있다. 데이터의 디스플레이 장치 또는 재생 장치는 토큰을 가진 데이터 이외의 데이터에 대한 디스플레이 또는 재생을 거절할 수 있다.

본 발명은 특정 실시예에 제한되지 않으며 여러 가지 변형 및 변경이 본 발명의 권리 범위에서 벗어나지 않고 이루어질 수 있다.

(57) 청구의 범위

청구항 1

디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템에 있어서,

데이터를 발행하는 발행자 장치에 대응하는 제 1정보를 생성시키는 수단, 상기 제 1정보를 전송하는 수단, 및 상기 데이터에 대응하는 제 2정보를 전송하는 수단을 포함하는 장치; 및

수신된 상기 제 1정보의 유효성을 검증하는 수단, 유효한 제 1정보에 대한 발행자 장치가 유효한지를 검증하는 수단, 및 상기 발행자 장치가 유효할 때 상기 제 2정보에 대응하는 데이터가 유효한지를 결정하는 수단을 포함하는 장치를 포함하는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 2

디지털 정보인 원본 데이터를 저장 또는 유통시키기 위한 원본 데이터 유통 시스템에서의 원본 데이터 유통 방법에 있어서,

데이터를 발행하는 발행자 장치에 대응하는 제 1정보를 생성시키는 단계;

상기 제 1정보를 전송하는 단계;

상기 데이터에 대응하는 제 2정보를 전송하는 단계;

수신된 상기 제 1정보의 유효성을 검증하는 단계;

유효한 제 1정보에 대한 발행자 장치가 유효한지를 검증하는 단계; 및

상기 발행자 장치가 유효할 때 상기 제 2정보에 대응하는 데이터가 유효한지를 결정하는 단계를 포함하는 것을 특징으로 하는 원본 데이터 유통 방법.

청구항 3

가치를 가지는 디지털 정보를 저장하는 데이터 저장 방법에 있어서,

상기 디지털 정보의 발행자 장치에 의하여 서명된 서명을 가진 디지털 정보인 제 1정보를 생성시키는 단계;

상기 발행자 장치에 의하여 상기 디지털 정보에 대응하는 매니페스트인 제 2정보를 생성시키는

단계;

상기 제 1정보 및 제 2정보를 이용하여 상기 발행자 장치의 동일성을 이용자 장치에 의하여 검증하는 단계; 및

상기 디지털 정보의 복제를 방지하는 단계를 포함하는 것을 특징으로 하는 데이터 저장 방법.

청구항 4

제 3항에 있어서, 관련된 디지털 정보의 발행이 엄격하게 관리되는 서버에 의하여 발행된 검증 키이를 얻는 단계;

상기 이용자 장치에 의하여 상기 검증 키이로부터의 세션 정보를 생성시키는 단계; 및

상기 세션 정보의 유효성을 검증하는 단계를 더 포함하는 것을 특징으로 하는 데이터 저장 방법.

청구항 5

제 3항에 있어서,

부정조작 방지 디바이스에 상기 제 2정보를 저장함으로써 상기 발행자 장치의 동일성을 검증하는 단계; 및

상기 디지털 정보의 복제를 방지하는 단계를 더 포함하는 것을 특징으로 하는 데이터 저장 방법.

청구항 6

가치를 가진 디지털 정보를 저장하는 데이터 저장 시스템에 있어서,

서명된 디지털 정보인 제 1정보를 생성시키고 상기 디지털 정보에 대응하는 매니페스트인 제 2정보를 생성시키는 발행자 장치; 및

상기 제 1정보 및 제 2정보를 이용하여 상기 발행자 장치의 동일성을 검증하고 상기 디지털 정보의 복제를 방지하는 이용자 장치를 포함하는 것을 특징으로 하는 데이터 저장 시스템.

청구항 7

제 6항에 있어서, 상기 이용자 장치는 관련된 디지털 정보의 발행이 엄격하게 관리되는 서버에 의하여 발행된 검증 키이를 얻는 수단을 더 포함하며,

상기 데이터 저장 시스템은: 검증 키이로부터 세션 정보를 생성시키는 수단 및 상기 세션 정보의 유효성을 검증하는 수단을 포함하는 수집 장치를 더 포함하는 것을 특징으로 하는 데이터 저장 시스템.

청구항 8

제 6항에 있어서, 상기 이용자 장치는:

부정조작 방지 디바이스에 상기 제 2정보를 저장함으로써 상기 발행자 장치의 동일성을 검증하고 상기 디지털 정보의 복제를 방지하는 수단을 더 포함하는 것을 특징으로 하는 데이터 저장 시스템.

청구항 9

가치를 가지는 디지털 정보를 저장하는 데이터 저장 시스템에서 디지털 정보를 이용하는 이용자 장치에 있어서,

서명된 디지털 정보를 저장하고 추출하는 제 1저장 수단;

디지털 정보에 대응하는 매니페스트를 저장하고 추출하는 제 2저장 수단;

상기 매니페스트가 유효한지를 검증하는 제 1인증 수단; 및

상기 제 1인증 수단이 상기 매니페스트가 유효한지를 검증할 때만 상기 제 2저장 수단에 상기 매니페스트를 저장하는 제 1제어 수단을 포함하는 것을 특징으로 하는 이용자 장치.

청구항 10

제 9항에 있어서, 상기 제 2저장 수단 및 제 1인증 수단은 부정조작 방지 능력을 가지는 것을 특징으로 하는 이용자 장치.

청구항 11

제 9항에 있어서, 상기 제 1인증 수단은:

상기 정보에 대응하는 매니페스트가 상기 제 2저장 수단에 저장되었음을 검증함으로써 상기 제 1저장 수단에 저장된 상기 디지털 정보가 유효한지를 결정하는 수단; 및

상기 매니페스트가 상기 제 2저장 수단에 저장될 때만 상기 디지털 정보가 유효한지를 결정하고 상기 매니페스트가 상기 제 2저장 수단에 저장되지 않았을 때 상기 디지털 정보가 무효인지를 결정하는 수단을 포함하는 것을 특징으로 하는 이용자 장치.

청구항 12

제 9항에 있어서,

디지털 정보에 서명을 제공하는 서명 수단;

상기 매니페스트의 서명자이 신임(accredited) 대상에 포함되는 지를 검증하고 상기 신임 정보의 서명자 및 상기 디지털 정보의 서명자이 동일인인지를 검증하는 제 2인증 수단; 및

상기 이용자 장치가 상기 제 2저장 수단에서 다른 저장 수단으로 상기 매니페스트를 이동시킬 때 상기 제 2저장 수단으로부터 상기 매니페스트를 추출하는 수단, 상기 서명 수단을 이용하여 상기 매니페스트에 서명을 제공하는 수단, 상기 제 2저장 수단으로부터 상기 매니페스트를 삭제하는 수단, 상기 제 2인증 수단을 이용하여 상기 매니페스트의 서명자이 상기 디지털 정보의 서명자에 의하여 신뢰되는 지를 검증하는 수단 및 상기 검증이 성공적일 경우에만 상기 다른 저장 수단에 상기 매니페스트를 저장하는 수단을 포함하는 제 2제어 수단을 더 포함하는 것을 특징으로 하는 이용자 장치.

청구항 13

제 9항에 있어서, 상기 데이터 저장 시스템에서 유일성을 가진 세션 정보를 생성시키는 세션 정보 생성 수단을 더 포함하며,

상기 세션 정보는 상기 이용자 장치의 검증 키이 및 일련 번호를 포함하며, 상기 이용자 장치에 저장되며, 상기 매니페스트의 전송 당사자에게 전송되며,

상기 이용자 장치는 상기 전송 당사자로부터 상기 매니페스트 및 상기 세션 정보를 수신하고 상기 저장된 세션 정보를 이용하여 수신된 세션 정보의 유효성을 검증하여 상기 이용자 장치가 상기 매니페스트의 복제를 방지하는 것을 특징으로 하는 이용자 장치.

청구항 14

가치를 가지는 디지털 정보를 저장하는 데이터 저장 시스템에 디지털 정보를 발행하는 발행자 장치에 있어서,

상기 디지털 정보의 서명자에 의하여 신뢰되는 신임 대상을 나타내는 정보 세트를 포함하는 신임 정보를 발생시키는 신임 정보 발생 수단;

상기 디지털 정보 및 상기 신임 정보에 서명을 제공하는 서명 수단;

상기 매니페스트를 생성하는 매니페스트 생성 수단;

상기 디지털 정보 및 상기 신임 정보를 이용자 장치에 전달하는 수단;

상기 이용자 장치의 검증 키이 및 일련 번호를 포함하는 세션 정보를 수신하는 수단; 및

상기 이용자 장치의 검증 키이 및 서명 기능을 이용하여 상기 매니페스트 및 세션 정보를 포함하는 정보를 전송하는 수단을 포함하는 것을 특징으로 하는 발행자 장치.

청구항 15

가치를 가지는 디지털 정보를 저장하는 데이터 저장 시스템에서 디지털 정보의 권리를 행사하는 개찰자 장치에 있어서,

이용자 장치로부터 발행자의 서명이된 디지털 정보 및 상기 서명이된 신임 정보를 수신하는 수단;

상기 데이터 저장 시스템에서 유일성을 가진 세션 정보를 생성하고 상기 세션 정보를 상기 이용자 장치에 전달하는 수단;

상기 이용자 장치로부터 상기 매니페스트 및 상기 세션 정보를 포함하는 정보를 수신하는 수단; 및

상기 세션 정보, 상기 매니페스트 및 상기 신임 정보가 유효한지를 검증하는 수단을 포함하는 것을 특징으로 하는 개찰자 장치.

청구항 16

가치를 가지는 디지털 정보를 저장하는 데이터 저장 시스템에 있어서,

디지털 정보를 사용하는 이용자 장치;

디지털 정보를 발행하는 발행자 장치; 및

디지털 정보의 권리를 행사하는 개찰자 장치를 포함하며,

상기 이용자 장치는: 서명된 디지털 정보를 저장하고 추출하는 제 1저장 수단; 디지털 정보에 대응하는 매니페스트를 저장하고 추출하는 제 2저장 수단; 상기 매니페스트가 유효한지를 검증하는 제 1인증 수단; 및 상기 제 1인증 수단이 상기 매니페스트가 유효한지를 검증할 때만 상기 제 2저장 수단에 상기 매니페스트를 저장하는 제 1제어 수단을 포함하며,

상기 발행자 장치는: 상기 디지털 정보의 서명자에 의하여 신뢰되는 신임 대상을 나타내는 정보 세트를 포함하는 신임 정보를 발생시키는 신임 정보 발생 수단;

상기 디지털 정보 및 상기 신임 정보에 서명을 제공하는 서명 수단;

상기 매니페스트를 생성하는 매니페스트 생성 수단;

상기 디지털 정보 및 상기 신임 정보를 이용자 장치에 전달하는 수단;

상기 이용자 장치의 검증 키이 및 일련 번호를 포함하는 세션 정보를 수신하는 수단; 및

상기 이용자 장치의 검증 키이 및 서명 기능을 이용하여 상기 매니페스트 및 세션 정보를 포함하는 정보를 전송하는 수단을 포함하며,

상기 개찰자 장치는: 이용자 장치로부터 발행자의 서명이된 디지털 정보 및 상기 서명이된 신임 정보를 수신하는 수단;

상기 데이터 저장 시스템에서 유일성을 가진 세션 정보를 생성하고 상기 세션 정보를 상기 이용자 장치에 전달하는 수단;

상기 이용자 장치로부터 상기 매니페스트 및 상기 세션 정보를 포함하는 정보를 수신하는 수단; 및

상기 세션 정보, 상기 매니페스트 및 상기 신임 정보가 유효한지를 검증하는 수단을 포함하는 것을 특징으로 하는 데이터 저장 시스템.

청구항 17

가치를 가지는 디지털 정보를 컴퓨터가 저장하도록 하는 프로그램 코드를 저장하는 컴퓨터 판독가능 매체에 있어서,

상기 컴퓨터는 데이터 저장 시스템의 발행자 장치로서 이용되며,

상기 컴퓨터 판독가능 매체는:

서명된 디지털 정보인 제 1정보를 생성하는 프로그램 코드 수단; 및

상기 디지털 정보에 대응하는 매니페스트인 제 2정보를 생성하는 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 18

가치를 가지는 디지털 정보를 컴퓨터가 저장하도록 하는 프로그램 코드를 저장하는 컴퓨터 판독가능 매체에 있어서,

상기 컴퓨터는 데이터 저장 시스템의 이용자 장치로서 이용되며,

상기 컴퓨터 판독가능 매체는:

제 1정보 및 제 2정보를 이용하여 발행자 장치의 동일성을 검증하고 상기 디지털 정보의 복제를 방지하는 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 19

제 18항에 있어서,

관련된 디지털 정보의 발행이 엄격하게 관리되는 서버에 의하여 발행된 검증 키이를 취득하는 프로그램 코드 수단;

상기 검증 키이로부터 세션 정보를 생성하는 프로그램 코드 수단; 및

상기 세션 정보의 유효성을 검증하는 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 20

가치를 가지는 디지털 정보를 컴퓨터가 저장하도록 하는 프로그램 코드를 저장하는 컴퓨터 판독가능 매체에 있어서,

상기 컴퓨터는 데이터 저장 시스템의 이용자 장치로서 이용되며,

상기 컴퓨터 판독가능 매체는:

제 1저장 수단에 서명된 디지털 정보를 저장하고 서명된 상기 디지털 정보를 추출하는 제 1저장 프로그램 코드 수단;

상기 디지털 정보에 대응하는 매니페스트를 제 2저장 수단에 저장하고 상기 디지털 정보에 대응하는 상기 매니페스트를 추출하는 제 2저장 프로그램 코드 수단;

상기 매니페스트가 유효한지를 검증하는 제 1인증 프로그램 코드 수단; 및

상기 매니페스트가 유효한지를 검증하는 제 1인증 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 21

제 20항에 있어서, 상기 제 1인증 프로그램 코드 수단은:

상기 정보에 대응하는 상기 매니페스트가 상기 제 2저장 수단에 저장되었는지를 검증함으로써 상기 제 1저장 수단에 저장된 상기 디지털 정보가 유효한지를 결정하는 프로그램 코드 수단; 및

상기 매니페스트가 제 2저장 수단에 저장되었을 때만 상기 디지털 정보가 유효한지를 결정하고 상기 매니페스트가 상기 제 2저장 수단에 저장되지 않았을 때 상기 디지털 정보가 유효한지를 결정하는 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 22

제 20항에 있어서,

디지털 정보에 서명을 제공하는 서명 프로그램 코드 수단;

상기 매니페스트의 서명자이 신임 대상에 포함되는 지를 검증하고 상기 신임 정보의 서명자 및 상기 디지털 정보의 서명자이 동일인인지를 검증하는 제 2인증 프로그램 코드 수단; 및

상기 이용자 장치가 상기 매니페스트를 이동시킬 때 상기 매니페스트를 추출하는 프로그램 코드 수단;

상기 서명 프로그램 코드 수단을 이용하여 상기 매니페스트에 서명을 제공하는 프로그램 코드 수단;

상기 제 2저장 수단으로부터 상기 매니페스트를 삭제하는 프로그램 코드 수단;

상기 제 2인증 프로그램 코드 수단을 이용하여 상기 매니페스트의 서명자이 상기 디지털 정보의 서명자에 의하여 신뢰되는 지를 검증하는 프로그램 코드 수단; 및

상기 검증이 성공적일 경우에만 상기 매니페스트를 이동시키는 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 23

가치를 가지는 디지털 정보를 컴퓨터가 저장하도록 하는 프로그램 코드를 저장하는 컴퓨터 판독가능 매체에 있어서,

상기 컴퓨터는 데이터 저장 시스템의 발행자 장치로서 이용되며,

상기 컴퓨터 판독가능 매체는:

상기 디지털 정보의 서명자에 의하여 신뢰되는 신임 대상을 나타내는 정보 세트를 포함하는 신임 정보를 발생시키는 신임 정보 발생 프로그램 코드 수단;

상기 디지털 정보 및 상기 신임 정보에 서명을 제공하는 서명 프로그램 코드 수단;

상기 매니페스트를 생성하는 매니페스트 생성 프로그램 코드 수단;

상기 디지털 정보 및 상기 신임 정보를 이용자 장치에 전달하는 프로그램 코드 수단;

상기 이용자 장치의 검증 키이 및 일련 번호를 포함하는 세션 정보를 수신하는 프로그램 코드 수단; 및

상기 이용자 장치의 검증 키이 및 서명 기능을 이용하여 상기 매니페스트 및 세션 정보를 포함하는 정보를 전송하는 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 24

가치를 가지는 디지털 정보를 컴퓨터가 저장하도록 하는 프로그램 코드를 저장하는 컴퓨터 판독가능 매체에 있어서,

상기 컴퓨터는 데이터 저장 시스템의 개찰자 장치로서 이용되며,

상기 컴퓨터 판독가능 매체는:

이용자 장치로부터 발행자의 서명이된 디지털 정보 및 상기 서명이된 신임 정보를 수신하는 프로그램 코드 수단;

상기 데이터 저장 시스템에서 유일성을 가진 세션 정보를 생성하고 상기 세션 정보를 상기 이용자 장치에 전달하는 프로그램 코드 수단;

상기 이용자 장치로부터 상기 매니페스트 및 상기 세션 정보를 포함하는 정보를 수신하는 프로그램 코드 수단; 및

상기 세션 정보, 상기 매니페스트 및 상기 신임 정보가 유효한지를 검증하는 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 25

디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템의 원본 데이터 유통 방법에 있어서,

장치에 대응하는 제 1정보 및 데이터 또는 상기 데이터에 대응하는 정보인 제 2정보를 포함하는 원본성 정보를 제 1장치에 의하여 전송하는 전송 단계;

상기 원본성 정보의 소스 장치를 제 2장치에 의하여 식별하는 식별 단계;

상기 소스 장치가 인증될 때 상기 원본성 정보가 유효한지를 결정하는 제 1인증 단계; 및

상기 소스 장치 및 상기 원본성 정보의 제 1정보에 대응하는 장치가 동일할 때만 상기 원본성 정보가 유효한지를 결정하는 제 2인증 단계를 포함하는 것을 특징으로 하는 원본 데이터 유통 방법.

청구항 26

제 25항에 있어서,

상기 제 1장치에 의하여 비밀 키이를 감추는 단계; 및

하나 또는 다수의 비밀 키이에 대응하는 공개 키이에 단방향성 기능을 부여함으로써 해시값이 발생되는 제 2장치의 해시값을 상기 제 2장치에 의하여 저장 또는 취득하는 단계를 더 포함하며,

상기 제 1인증 단계는 상기 제 1장치가 상기 해시값에 대응하는 비밀 키이를 가졌는지를 검증함으로써 상기 제 1장치를 인증하는 단계를 포함하는 것을 특징으로 하는 원본 데이터 유통 방법.

청구항 27

제 25항에 있어서, 상기 전송 단계는 상기 제 2장치에 제삼자 증명서를 전송하는 단계를 포함하며, 상기 제삼자 증명서는 상기 제 1장치가 하나 또는 다수의 제삼자에 의하여 인증되었음을 나타내는 증명서이며, 상기 제삼자 증명서는 제삼자의 인증자에 상응하며,

상기 방법은 하나 또는 다수의 제삼자에 대응하는 제삼자 정보를 상기 제 2장치에 의하여 저장 또는 취득하는 단계를 포함하며,

상기 제 1인증 단계는 상기 제 1장치가 상기 제삼자 증명서에서 인증될 대상인지를 검증하고 상기 제삼자 증명서의 인증자가 상기 제삼자 정보의 제삼자에 포함되어 있는지를 검증함으로써 상기 제 1장치를 인증하는 단계를 포함하는 것을 특징으로 하는 원본 데이터 유통 방법.

청구항 28

제 27항에 있어서, 상기 방법은 상기 제 1정보 및 하나 또는 다수의 제삼자에 대응하는 제삼자 신임 정보를 상기 제 2장치에 의하여 저장 또는 취득하는 단계를 포함하며,

상기 제 1인증 단계는 상기 제 1장치가 상기 제삼자 증명서에서 인증될 대상인지를 검증하고 상기 제삼자 증명서의 인증자가 상기 제삼자 신임 정보의 제삼자에 포함되어 있는지를 검증함으로써 상기 제 1장치를 인증하는 단계를 포함하며, 상기 제삼자는 상기 제 1정보에 대응하며 상기 제삼자 신임 정보로부터 추출되는 것을 특징으로 하는 원본 데이터 유통 방법.

청구항 29

제 27항에 있어서, 상기 방법은 상기 제 1정보 및 하나 또는 다수의 제삼자에 대응하는 제삼자 신임 정보를 상기 제 2장치에 의하여 저장 또는 취득하는 단계를 포함하며,

상기 제 1인증 단계는 상기 제삼자 증명서의 인증자가 상기 제삼자 신임 정보로부터 추출된 제삼자에 포함되어 있는지를 검증함으로써 상기 제 1장치를 인증하는 단계를 포함하며, 상기 제삼자는 상기 제 1정보 및 제 2정보에 대응하는 것을 특징으로 하는 원본 데이터 유통 방법.

청구항 30

제 25항에 있어서,

상기 제 1장치에 의하여 비밀 키이를 감추는 단계;

상기 제 1장치를 신뢰하는 제삼자에 의한 서명이 제공되는 상기 비밀 키이의 공개 키이인 공개 키이 증명서 및 서명을 비밀 키이에 의하여 전송하는 단계;

상기 공개 키이 증명서를 검증함으로써 상기 제삼자의 공개 키이를 상기 제 2장치에 의하여 식별하는 단계; 및

하나 또는 다수의 해시값을 저장 또는 취득하는 단계를 포함하며,

상기 제 1인증 단계는 공개 키이를 이용하여 상기 서명이 상기 공개 키이 증명서에 포함되었는지를 검증하고 상기 제삼자의 상기 공개 키이에 단방향성 기능을 부여함으로써 생성된 정보가 상기 해시값에 포함되어 있는지를 검증함으로써 상기 제 1장치를 인증하는 단계를 포함하는 것을 특징으로 하는 원본 데이터 유통 방법.

청구항 31

제 25항에 있어서, 상기 방법은 상기 제 1정보 및 하나 또는 다수의 제삼자에 대응하는 이용자 신임 정보를 상기 제 2장치에 의하여 저장 또는 취득하는 단계를 포함하며,

상기 제 1인증 단계는 상기 이용자 신임 정보를 이용하여 상기 제 1정보로부터 추출된 상기 제 1장치에 대응하는 정보에 상기 소스 장치가 포함되었는 지를 검증함으로써 상기 제 1장치를 인증하는 단계를 포함하는 것을 특징으로 하는 원본 데이터 유통 방법.

청구항 32

제 25항에 있어서, 상기 방법은 상기 제 1정보 및 제 2정보로부터 하나 또는 다수의 제 1장치에 대응하는 이용자 신임 정보를 상기 제 2장치에 의하여 저장 또는 취득하는 단계를 포함하며,

상기 제 1인증 단계는 상기 이용자 신임 정보로부터 추출된 상기 제 1장치 상의 정보에 상기 소스 장치가 포함되었는 지를 검증함으로써 상기 제 1장치를 인증하는 단계를 포함하며, 상기 정보는 제 1정보 및 제 2정보에 대응하는 것을 특징으로 하는 원본 데이터 유통 방법.

청구항 33

디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템에 있어서,

장치에 대응하는 제 1정보 및 데이터 또는 상기 데이터에 대응하는 정보인 제 2정보를 포함하는 원본성 정보를 전송하는 전송 수단을 포함하는 제 1장치; 및

상기 원본성 정보의 소스 장치를 식별하는 식별 수단, 상기 소스 장치가 인증될 때 상기 원본성 정보가 유효한지를 결정하는 제 1인증 수단 및 상기 소스 장치 및 상기 원본성 정보의 제 1정보에 대응하는 장치가 동일할 때만 상기 원본성 정보가 유효한지를 결정하는 제 2인증 수단을 포함하는 제 2장치를 포함하는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 34

제 33항에 있어서, 상기 제 1장치는 비밀 키이를 감추는 수단을 더 포함하며,

상기 제 2장치는 하나 또는 다수의 비밀 키이에 대응하는 공개 키이에 단방향성 기능을 부여함으로써 해시값이 발생되는 제 2장치의 해시값을 저장 또는 취득하는 수단을 더 포함하며,

상기 제 2장치의 상기 제 1인증 수단은 상기 제 1장치가 상기 해시값에 대응하는 비밀 키이를 가졌는지를 검증함으로써 상기 제 1장치를 인증하는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 35

제 33항에 있어서, 상기 전송 수단은 상기 제 2장치에 제삼자 증명서를 전송하는 수단을 포함하며, 상기 제삼자 증명서는 상기 제 1장치가 하나 또는 다수의 제삼자에 의하여 인증되었음을 나타내는 증명서이며, 상기 제삼자 증명서는 제삼자의 인증자에 상응하며,

상기 제 2장치는 하나 또는 다수의 제삼자에 대응하는 제삼자 정보를 저장 또는 취득하는 수단을 포함하며,

상기 제 1인증 수단은 상기 제 1장치가 상기 제삼자 증명서에서 인증될 대상인지를 검증하고 상기 제삼자 증명서의 인증자가 상기 제삼자 정보의 제삼자에 포함되어 있는지를 검증함으로써 상기 제 1장치를 인증하는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 36

제 35항에 있어서, 상기 제 2장치는 상기 제 1정보 및 하나 또는 다수의 제삼자에 대응하는 제삼자 신임 정보를 저장 또는 취득하는 수단을 포함하며,

상기 제 1인증 수단은 상기 제 1장치가 상기 제삼자 증명서에서 인증될 대상인지를 검증하고 상기 제삼자 증명서의 인증자가 상기 제삼자 신임 정보의 제삼자에 포함되어 있는지를 검증함으로써 상기 제 1장치를 인증하며, 상기 제삼자는 상기 제 1정보에 대응하며 상기 제삼자 신임 정보로부터 추출되는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 37

제 35항에 있어서, 상기 제 2장치는 상기 제 1정보 및 하나 또는 다수의 제삼자에 대응하는 제삼자 신임 정보를 저장 또는 취득하는 수단을 포함하며,

상기 제 1인증 수단은 상기 제삼자 증명서의 인증자가 상기 제삼자 신임 정보로부터 추출된 제삼자에 포함되어 있는지를 검증함으로써 상기 제 1장치를 인증하며, 상기 제삼자는 상기 제 1정보 및 제 2정보에 대응하는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 38

제 33항에 있어서,

상기 제 1장치는 비밀 키이를 감추는 수단 및 상기 제 1장치를 신뢰하는 제삼자에 의한 서명이 제공되는 상기 비밀 키이의 공개 키이인 공개 키이 증명서 및 서명을 비밀 키에 의하여 전송하는 수단을 포함하며,

상기 제 2장치는 상기 공개 키이 증명서를 검증함으로써 상기 제삼자의 공개 키이를 식별하는 수단 및 하나 또는 다수의 해시값을 저장 또는 취득하는 수단을 포함하며,

상기 제 1인증 수단은 상기 공개 키이를 이용하여 상기 서명이 상기 공개 키이 증명서에 포함되었는 지를 검증하고 상기 제삼자의 상기 공개 키이에 단방향성 기능을 부여함으로써 생성된 정보가 상기 해시값에 포함되어 있는지를 검증함으로써 상기 제 1장치를 인증하는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 39

제 33항에 있어서, 상기 제 2장치는 상기 제 1정보 및 하나 또는 다수의 제삼자에 대응하는 이용자 신임 정보를 저장 또는 취득하는 수단을 포함하며,

상기 제 1인증 수단은 상기 이용자 신임 정보를 이용하여 상기 제 1정보로부터 추출된 상기 제 1장치에 대응하는 정보에 상기 소스 장치가 포함되었는 지를 검증함으로써 상기 제 1장치를 인증하는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 40

제 33항에 있어서, 상기 제 2장치는 상기 제 1정보 및 제 2정보로부터 하나 또는 다수의 제 1장치에 대응하는 이용자 신임 정보를 저장 또는 취득하는 수단을 포함하며,

상기 제 1인증 수단은 상기 이용자 신임 정보로부터 추출된 상기 제 1장치 상의 정보에 상기 소스 장치가 포함되었는 지를 검증함으로써 상기 제 1장치를 인증하며, 상기 정보는 제 1정보 및 제 2정보에 대응하는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 41

디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템의 발행자 장치에 있어서,

상기 발행자 장치에 대응하는 제 1정보 및 데이터 또는 상기 데이터에 대응하는 정보에 상응하는 제 2정보를 포함하는 원본성 정보를 생성하는 원본성 정보 생성 수단; 및

상기 원본성 정보를 전송하기 위한 원본성 정보 전송 수단을 포함하는 것을 특징으로 하는 발행자 장치.

청구항 42

제 41항에 있어서,

비밀 키이를 감추는 수단; 및

제 1정보로서 상기 발행자 장치의 해시값을 생성하는 수단을 포함하며, 상기 해시값은 단방향성 기능을 부여함으로써 상기 비밀 키이의 공개 키이로부터 생성되는 것을 특징으로 하는 발행자 장치.

청구항 43

제 41항에 있어서, 상기 데이터에 단방향성 기능을 부여함으로써 상기 제 2정보를 생성하는 수단을 포함하는 것을 특징으로 하는 발행자 장치.

청구항 44

제 43항에 있어서, 상기 제 2정보는 네트워크의 콘텐츠를 식별하는 식별자인 것을 특징으로 하는 발행자 장치.

청구항 45

디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템의 이용자 장치에 있어서,

장치에 대응하는 제 1정보 및 데이터 또는 상기 데이터에 상응하는 정보에 대응하는 제 2정보를 포함하는 원본성 정보를 전송하는 원본성 정보 전송 수단;

장치로부터 전송된 상기 원본성 정보의 소스 장치를 식별하는 식별 수단;

상기 소스 장치가 인증될 때 또는 상기 제 1정보에 대응하는 상기 장치 및 상기 소스 장치가 동일할 때 상기 원본성 정보가 유효한지를 결정하는 인증 수단; 및

상기 원본성 정보가 유효한지를 상기 인증 수단이 결정할 때 상기 원본성 정보를 저장하는 저장 수단을 포함하는 것을 특징으로 하는 이용자 장치.

청구항 46

제 45항에 있어서, 상기 이용자 장치가 상기 원본성 정보를 전송할 때 상기 원본성 정보를 삭제하는 수단을 포함하는 것을 특징으로 하는 이용자 장치.

청구항 47

디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템의 개찰자 장치에 있어서,

원본성 정보의 소스 장치를 식별하는 식별 수단;

상기 소스 장치를 인증하는 인증 수단; 및

상기 개찰자 장치에 전송된 원본성 정보가 유효하다고 상기 인증 수단이 결정할 때, 상기 데이터 또는 상기 제 2정보에 상응하는 데이터에 대응하는 프로세스를 수행하는 데이터 처리 수단을 포함하는 것을 특징으로 하는 개찰자 장치.

청구항 48

제 47항에 있어서, 상기 개찰자 장치는 발행자 정보를 저장 또는 취득하는 수단을 더 포함하며,

상기 데이터 처리 수단은 상기 개찰자 장치에 전송된 원본성 정보가 유효하다고 상기 인증 수단이 결정하고 상기 제 1정보에 대응하는 발행자 장치가 상기 발행자 정보에 포함되어 있을 때 상기 데이터 또는 제 2정보에 상응하는 데이터에 대응하는 프로세스를 수행하는 것을 특징으로 하는 개찰자 장치.

청구항 49

디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템에 있어서,

상기 발행자 장치에 대응하는 제 1정보 및 데이터에 대응하는 제 2정보를 포함하는 원본성 정보를 생성하고 전송하는 수단을 포함하는 발행자 장치;

상기 원본성 정보의 소스 장치의 유효성을 검증하는 수단 및 상기 유효성이 검증될 때 상기 원본성 정보를 저장하는 수단을 포함하는 이용자 장치; 및

상기 원본성 정보의 소스 장치의 유효성을 검증하는 수단 및 상기 유효성이 검증될 때 상기 제 2정보에 대응하는 데이터를 처리하는 데이터 처리 수단을 포함하는 개찰자 장치를 포함하는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 50

디지털 정보인 원본 데이터를 저장 또는 유통시키는 원본 데이터 유통 시스템에 있어서,

상기 원본 데이터 유통 시스템은 발행자 장치, 이용자 장치 및 개찰자 장치를 포함하며,

상기 발행자 장치는: 상기 발행자 장치에 대응하는 제 1정보 및 데이터 또는 상기 데이터에 대응하는 정보에 상응하는 제 2정보를 포함하는 원본성 정보를 생성하는 제 1원본성 정보 생성 수단 및 상기 원본성 정보를 전송하기 위한 제 1원본성 정보 전송 수단을 포함하며,

상기 이용자 장치는: 장치에 대응하는 제 1정보 및 데이터 또는 상기 데이터에 상응하는 정보에 대응하는 제 2정보를 포함하는 원본성 정보를 전송하는 제 1원본성 정보 전송 수단, 장치로부터 전송된 상기 원본성 정보의 소스 장치를 식별하는 제 1식별 수단, 상기 소스 장치가 인증될 때 또는 상기 제 1정보에 대응하는 상기 장치 및 상기 소스 장치가 동일할 때 상기 원본성 정보가 유효한지를 결정하는 제 1인증 수단 및 상기 원본성 정보가 유효한지를 상기 인증 수단이 결정할 때 상기 원본성 정보를 저장하는 저장 수단을 포함하며,

상기 개찰자 장치는: 원본성 정보의 소스 장치를 식별하는 제 2식별 수단, 상기 소스 장치를 인증하는 제 2인증 수단 및 상기 개찰자 장치에 전송된 원본성 정보가 유효하다고 상기 인증 수단이 결정할 때 상기 데이터 또는 상기 제 2정보에 상응하는 데이터에 대응하는 프로세스를 수행하는 데이터 처리 수단을 포함하는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 51

제 49항에 있어서,

상기 개찰자 장치는 상기 이용자 장치로부터 전송된 원본성 정보를 상기 발행자 장치에 전송하는 수단을 더 포함하며,

상기 발행자 장치는:

상기 원본성 정보가 상기 발행자 장치에 의하여 생성되었는지를 검증하는 수단;

상기 원본성 정보가 유효한 경로를 통하여 전송되었는 지를 검증하는 수단;

상기 제 2정보에 대응하는 상기 데이터가 상기 데이터 처리 수단에 의하여 처리되었는 지를 검증하는 수단: 및

상기 데이터에 상응하는 가치를 상기 개찰자 장치에 제공하는 수단을 포함하는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 52

제 49항에 있어서, 상기 발행자 장치는 카운트 정보로서 이용가능한 수의 상기 데이터를 상기 원본성 정보에 가산하는 수단을 더 포함하며,

상기 이용자 장치는 상기 카운트 정보를 검증하는 수단을 더 포함하며,

상기 개찰자 장치는 상기 카운트 정보를 검증하는 수단을 더 포함하며,

상기 이용자 장치는 상기 데이터를 이용가능한 횟수동안 사용할 수 있는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 53

제 49항에 있어서, 상기 데이터 유통 시스템의 장치는 상기 장치가 상기 원본성 정보를 전송할 때 상기 데이터 유통 시스템에서 유일성을 가진 세션 정보를 전송하며,

상기 원본성 정보를 전송하는 전송측 장치는 상기 전송측 장치에 상기 원본성 정보 및 세션 정보

를 전송하며,

수신측 장치는 상기 원본성 정보를 수신할 때 상기 수신측 장치에 상기 세션 정보를 전송하며,

상기 전송측 장치는 상기 전송측 장치에 저장된 상기 원본성 정보 및 세션 정보를 삭제하는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 54

제 49항에 있어서, 상기 이용자 장치는 상기 원본성 정보를 생성하는 수단을 더 포함하는 것을 특징으로 하는 원본 데이터 유통 시스템.

청구항 55

원본 데이터 유통 시스템이 디지털 정보인 원본 데이터를 저장 또는 유통시키도록 하는 프로그램 코드를 저장하는 컴퓨터 판독가능 매체에 있어서,

장치에 대응하는 제 1정보 및 데이터 또는 데이터에 상응하는 정보에 대응하는 제 2정보를 포함하는 상기 원본성 정보를 전송하는 전송 프로그램 코드 수단을 포함하고 제 1장치에 로딩되는 제 1프로그램 코드 수단;

제 2장치에 로딩되는 제 2프로그램 코드 수단을 포함하는데,

상기 제 2프로그램 코드 수단은:

상기 원본성 정보의 소스 장치를 식별하는 식별 프로그램 코드 수단;

상기 소스 장치가 인증될 때 상기 원본성 정보가 유효한지를 결정하는 제 1인증 프로그램 코드 수단; 및

상기 소스 장치 및 상기 원본성 정보의 제 1정보에 대응하는 장치가 동일할 때만 상기 원본성 정보가 유효한지를 결정하는 제 2인증 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 56

제 55항에 있어서, 상기 제 1프로그램 코드 수단은 비밀 키이를 감추는 프로그램 코드 수단을 더 포함하며,

상기 제 2프로그램 코드 수단은 하나 또는 다수의 비밀 키이에 대응하는 공개 키이에 단방향성 기능을 부여함으로써 해시값이 발생되는 제 2장치의 해시값을 저장 또는 취득하는 프로그램 코드 수단을 더 포함하며,

상기 제 1인증 프로그램 코드 수단은 상기 제 1장치가 상기 해시값에 대응하는 비밀 키이를 가졌는지를 검증함으로써 상기 제 1장치를 인증하는 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 57

제 55항에 있어서,

상기 전송 프로그램 코드 수단은 상기 제 2장치에 제삼자 증명서를 전송하는 프로그램 코드 수단을 포함하며, 상기 제삼자 증명서는 상기 제 1장치가 하나 또는 다수의 제삼자에 의하여 인증되었음을 나타내는 증명서이며, 상기 제삼자 증명서는 제삼자의 인증자에 상응하며,

상기 제 2프로그램 코드 수단은 하나 또는 다수의 제삼자에 대응하는 제삼자 정보를 저장 또는 취득하는 프로그램 코드 수단을 포함하며,

상기 제 1인증 프로그램 코드 수단은 상기 제 1장치가 상기 제삼자 증명서에서 인증될 대상인지를 검증하고 상기 제삼자 증명서의 인증자가 상기 제삼자 정보의 제삼자에 포함되어 있는지를 검증함으로써 상기 제 1장치를 인증하는 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 58

제 57항에 있어서, 상기 제 2프로그램 코드 수단은 상기 제 1정보 및 하나 또는 다수의 제삼자에 대응하는 제삼자 신임 정보를 저장 또는 취득하는 프로그램 코드 수단을 포함하며,

상기 제 1인증 프로그램 코드 수단은 상기 제 1장치가 상기 제삼자 증명서에서 인증될 대상인지를 검증하고 상기 제삼자 증명서의 인증자가 상기 제삼자 신임 정보의 제삼자에 포함되어 있는지를 검증함으로써 상기 제 1장치를 인증하는 프로그램 코드 수단을 포함하며, 상기 제삼자는 상기 제 1정보에 대응하며 상기 제삼자 신임 정보로부터 추출되는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 59

제 57항에 있어서, 상기 제 2프로그램 코드 수단은 상기 제 1정보 및 하나 또는 다수의 제삼자에 대응하는 제삼자 신임 정보를 저장 또는 취득하는 프로그램 코드 수단을 포함하며,

상기 제 1인증 프로그램 코드 수단은 상기 제삼자 증명서의 인증자가 상기 제삼자 신임 정보로부터 추출된 제삼자에 포함되어 있는지를 검증함으로써 상기 제 1장치를 인증하는 프로그램 코드 수단을

포함하며, 상기 제삼자는 상기 제 1정보 및 제 2정보에 대응하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 60

제 55항에 있어서, 상기 제 1프로그램 코드 수단은 비밀 키이를 감추는 프로그램 코드 수단 및 상기 제 1장치를 신뢰하는 제삼자에 의한 서명이 제공되는 상기 비밀 키이의 공개 키이인 공개 키이 증명서 및 서명을 비밀 키에 의하여 전송하는 프로그램 코드 수단을 포함하며,

상기 제 2프로그램 코드 수단은 상기 공개 키이 증명서를 검증함으로써 상기 제삼자의 공개 키이를 식별하는 프로그램 코드 수단 및 하나 또는 다수의 해시값을 저장 또는 취득하는 프로그램 코드 수단을 포함하며,

상기 제 1인증 프로그램 코드 수단은 상기 공개 키이를 이용하여 상기 서명이 상기 공개 키이 증명서에 포함되었는 지를 검증하고 상기 제삼자의 상기 공개 키이에 단방향성 기능을 부여함으로써 생성된 정보가 상기 해시값에 포함되어 있는지를 검증함으로써 상기 제 1장치를 인증하는 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 61

제 55항에 있어서, 상기 제 2프로그램 코드 수단은 상기 제 1정보 및 하나 또는 다수의 제삼자에 대응하는 이용자 신임 정보를 저장 또는 취득하는 프로그램 코드 수단을 포함하며,

상기 제 1인증 프로그램 코드 수단은 상기 이용자 신임 정보를 이용하여 상기 제 1정보로부터 추출된 상기 제 1장치에 대응하는 정보에 상기 소스 장치가 포함되었는 지를 검증함으로써 상기 제 1장치를 인증하는 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 62

제 55항에 있어서, 상기 제 2프로그램 코드 수단은 상기 제 1정보 및 제 2정보로부터 하나 또는 다수의 제 1장치에 대응하는 이용자 신임 정보를 저장 또는 취득하는 프로그램 코드 수단을 포함하며,

상기 제 1인증 프로그램 코드 수단은 상기 이용자 신임 정보로부터 추출된 상기 제 1장치 상의 정보에 상기 소스 장치가 포함되었는 지를 검증함으로써 상기 제 1장치를 인증하는 프로그램 코드 수단을 포함하며, 상기 정보는 제 1정보 및 제 2정보에 대응하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 63

원본 데이터 유통 시스템의 컴퓨터가 디지털 정보인 원본 데이터를 저장 또는 유통시키도록 하는 프로그램 코드를 저장하는 컴퓨터 판독가능 매체에 있어서,

상기 컴퓨터는 발행자 장치로 이용되며,

상기 컴퓨터 판독가능 매체는:

상기 발행자 장치에 대응하는 제 1정보 및 데이터 또는 상기 데이터에 대응하는 정보에 상응하는 제 2정보를 포함하는 원본성 정보를 생성하는 원본성 정보 생성 프로그램 코드 수단; 및

상기 원본성 정보를 전송하기 위한 원본성 정보 전송 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 64

제 63항에 있어서,

비밀 키이를 감추는 프로그램 코드 수단; 및

제 1정보로서 상기 발행자 장치의 해시값을 생성하는 프로그램 코드 수단을 포함하며, 상기 해시값은 단방향성 기능을 부여함으로써 상기 비밀 키이의 공개 키이로부터 생성되는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 65

제 63항에 있어서, 상기 데이터에 단방향성 기능을 부여함으로써 상기 제 2정보를 생성하는 프로그램 코드 수단을 더 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 66

제 65항에 있어서, 네트워크의 콘텐츠를 식별하는 식별자를 상기 제 2정보로서 이용하는 프로그램 코드 수단을 더 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 67

원본 데이터 유통 시스템의 컴퓨터가 디지털 정보인 원본 데이터를 저장 또는 유통시키도록 하는 프로그램 코드를 저장하는 컴퓨터 판독가능 매체에 있어서,

상기 컴퓨터는 이용자 장치로서 이용되며,

상기 컴퓨터 판독가능 매체는:

장치에 대응하는 제 1정보 및 데이터 또는 상기 데이터에 상응하는 정보에 대응하는 제 2정보를

포함하는 원본성 정보를 전송하는 원본성 정보 전송 프로그램 코드 수단;

장치로부터 전송된 상기 원본성 정보의 소스 장치를 식별하는 식별 프로그램 코드 수단;

상기 소스 장치가 인증될 때 또는 상기 제 1정보에 대응하는 상기 장치 및 상기 소스 장치가 동일할 때 상기 원본성 정보가 유효한지를 결정하는 인증 프로그램 코드 수단; 및

상기 원본성 정보가 유효한지를 상기 인증 수단이 결정할 때 상기 원본성 정보를 저장하는 저장 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 68

제 67항에 있어서, 상기 이용자 장치가 상기 원본성 정보를 전송할 때 상기 원본성 정보를 삭제하는 프로그램 코드 수단을 더 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 69

원본 데이터 유통 시스템의 컴퓨터가 디지털 정보인 원본 데이터를 저장 또는 유통시키도록 하는 프로그램 코드를 저장하는 컴퓨터 판독가능 매체에 있어서,

상기 컴퓨터는 개찰자 장치로서 이용되며,

상기 컴퓨터 판독가능 매체는:

원본성 정보의 소스 장치를 식별하는 식별 프로그램 코드 수단;

상기 소스 장치를 인증하는 인증 프로그램 코드 수단; 및

상기 개찰자 장치에 전송된 원본성 정보가 유효하다고 상기 인증 수단이 결정할 때, 상기 데이터 또는 상기 제 2정보에 상응하는 데이터에 대응하는 프로세스를 수행하는 데이터 처리 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 70

제 69항에 있어서,

발행자 정보를 저장 또는 취득하는 프로그램 코드 수단을 더 포함하며,

상기 데이터 처리 프로그램 코드 수단은 상기 개찰자 장치에 전송된 원본성 정보가 유효하다고 상기 인증 수단이 결정하고 상기 제 1정보에 대응하는 발행자 장치가 상기 발행자 정보에 포함되어 있을 때 상기 데이터 또는 제 2정보에 상응하는 데이터에 대응하는 프로세스를 수행하는 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 71

원본 데이터 유통 시스템의 컴퓨터가 디지털 정보인 원본 데이터를 저장 또는 유통시키도록 하는 프로그램 코드를 저장하는 컴퓨터 판독가능 매체에 있어서,

상기 컴퓨터 판독가능 매체는:

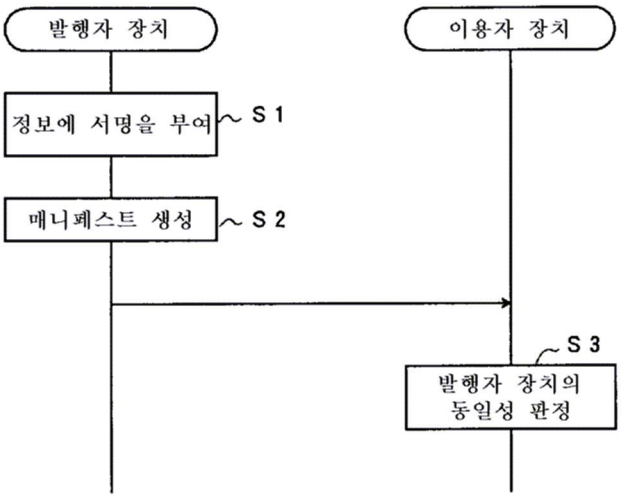
발행자 장치에 로딩되어, 상기 발행자 장치에 대응하는 제 1정보 및 데이터 또는 상기 데이터에 대응하는 정보에 상응하는 제 2정보를 포함하는 원본성 정보를 생성하는 제 1원본성 정보 생성 프로그램 코드 수단 및 상기 원본성 정보를 전송하는 제 1원본성 정보 전송 프로그램 코드 수단을 포함하는 발행자 프로그램 코드 수단;

이용자 장치에 로딩되어, 장치에 대응하는 제 1정보 및 데이터 또는 상기 데이터에 상응하는 정보에 대응하는 제 2정보를 포함하는 원본성 정보를 전송하는 제 1원본성 정보 전송 프로그램 코드 수단, 장치로부터 전송된 상기 원본성 정보의 소스 장치를 식별하는 제 1식별 프로그램 코드 수단, 상기 소스 장치가 인증될 때 또는 상기 제 1정보에 대응하는 상기 장치 및 상기 소스 장치가 동일할 때 상기 원본성 정보가 유효한지를 결정하는 제 1인증 프로그램 코드 수단 및 상기 원본성 정보가 유효한지를 상기 인증 수단이 결정할 때 상기 원본성 정보를 저장하는 저장 프로그램 코드 수단을 포함하는 이용자 프로그램 코드 수단; 및

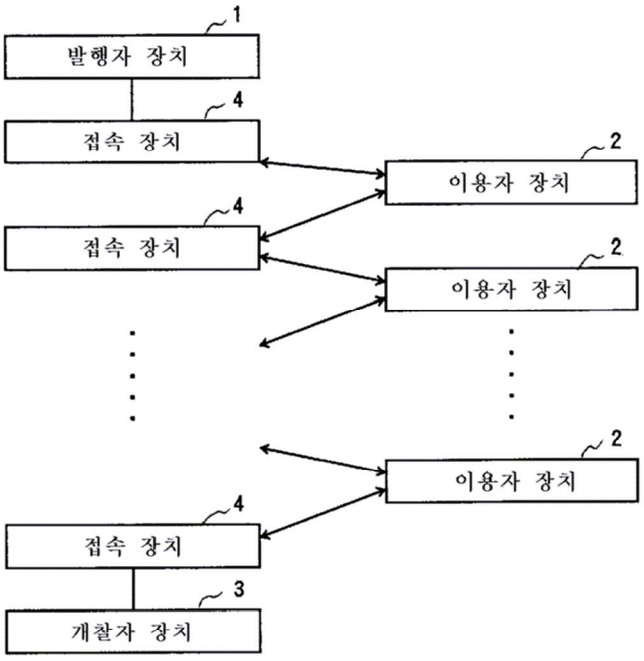
개찰자 장치에 로딩되어, 원본성 정보의 소스 장치를 식별하는 제 2식별 프로그램 코드 수단, 상기 소스 장치를 인증하는 제 2인증 프로그램 코드 수단 및 상기 개찰자 장치에 전송된 원본성 정보가 유효하다고 상기 인증 수단이 결정할 때 상기 데이터 또는 상기 제 2정보에 상응하는 데이터에 대응하는 프로세스를 수행하는 데이터 처리 프로그램 코드 수단을 포함하는 는 개찰자 프로그램 코드 수단을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

도면

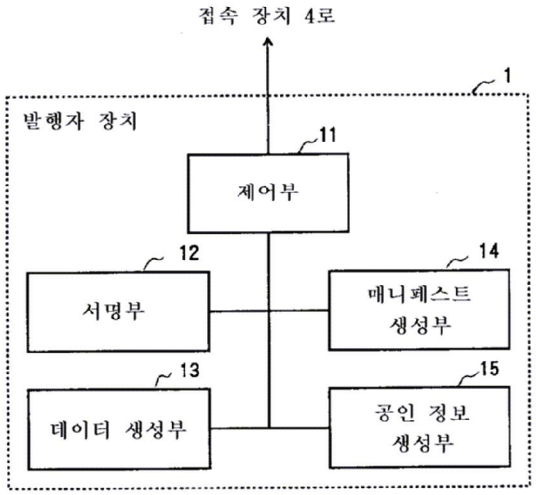
도면1


발행자 장치
이용자 장치
정보에 서명을 부여
S 1
매니페스트 생성
S 2
S 3
발행자 장치의
동일성 판정

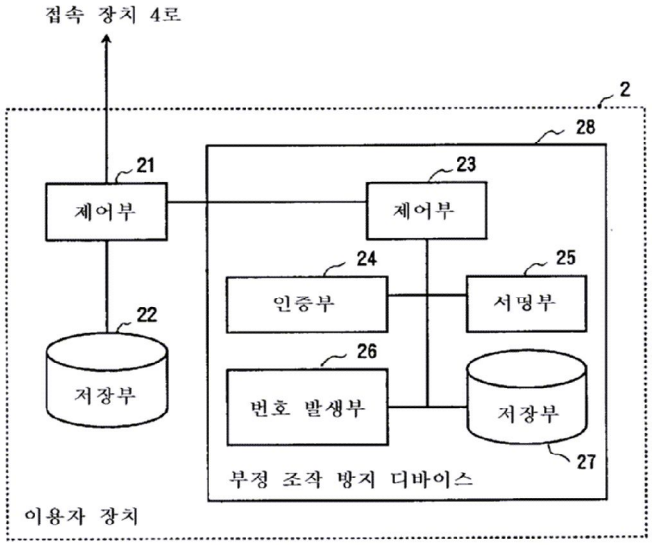
도면2


1
발행자 장치
4
접속 장치
2
이용자 장치
4
접속 장치
2
이용자 장치
2
이용자 장치
4
접속 장치
3
개찰자 장치

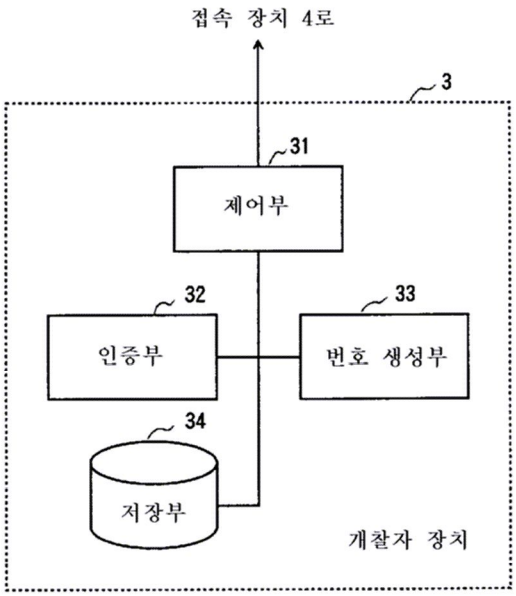
도면3


접속 장치 4로
1
발행자 장치
11
제어부
12
서명부
14
매니페스트 생성부
13
데이터 생성부
15
공인 정보 생성부

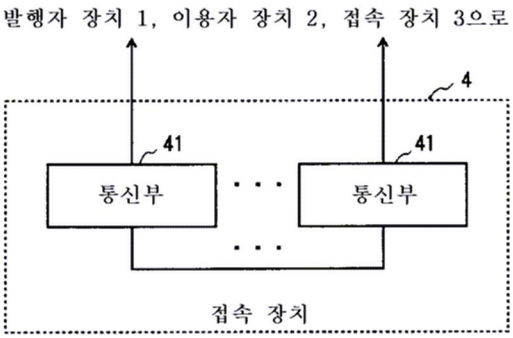
도면4


접속 장치 4로
2
28
21
제어부
23
제어부
24
인증부
25
서명부
22
저장부
26
번호 발생부
저장부
27
부정 조작 방지 디바이스
이용자 장치

도면5


접속 장치 4로
3
31
제어부
32
인증부
33
번호 생성부
34
저장부
개찰자 장치

도면6


발행자 장치 1, 이용자 장치 2, 접속 장치 3으로
4
41
통신부
41
통신부
접속 장치