(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) Int. Cl.[6]
G06F 17/25

(45) 공고일자 1999년01월15일
(11) 등록번호 특0168481
(24) 등록일자 1998년10월02일

(21) 출원번호 특1995-005175
(22) 출원일자 1995년03월09일
(65) 공개번호 특1995-033921
(43) 공개일자 1995년12월26일
(30) 우선권주장 94-02717 1994년03월09일 프랑스(FR)

(73) 특허권자 뷜 쎄베8 미쉘 꼴롱브
프랑스공화국 78430 루브시엔느 베.베.45 루트 드 베르사이유 68
(72) 발명자 파타렝 쟈끄
프랑스공화국 비로플레 78220 뤼 아메디 데일리 1
(74) 대리인 이태희

심사관 : 이은철

(54) 한 서비스 또는 한 장소로의 접근 또는 거래를 가능하게 하는 데이터 캐리어를 확증하는 방법과 장치 및 그에 상응하는 캐리어

요약

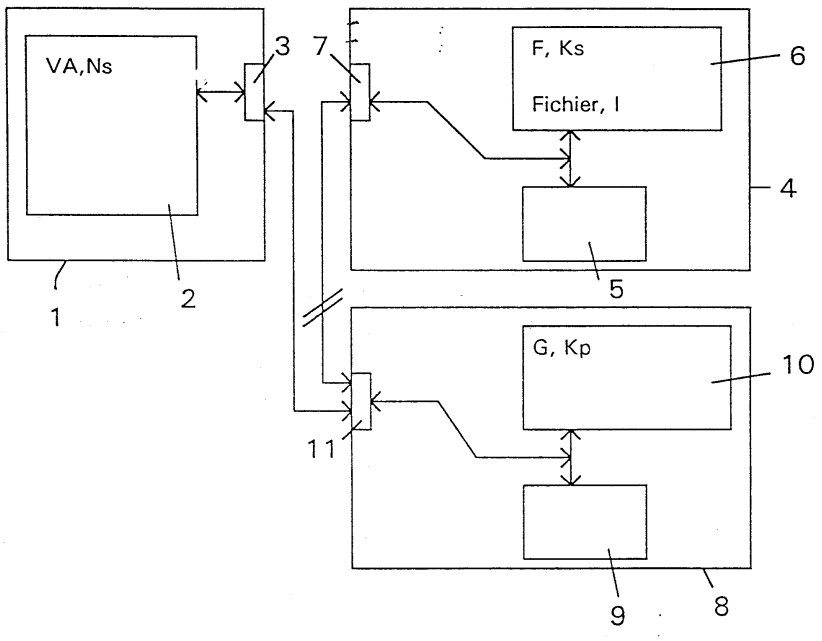
본 발명은 어떤 서비스 또는 어떤 장소로의 접근 또는 거래를 가능하게 하는 데이터 캐리어를 확증하는 방법 및 장치에 관한 것이다.

본 발명에서, 상기 캐리어(1)는, 이 캐리어에 귀속하는 권리를 한정하는 특정 번호 및 정보(I)로부터, 비대칭 알고리즘(F) 및 비밀 키(Ks)에 의해 계산된 확증값 및 특정 번호(Ns)를 갖는다.

2종류의 확증이 제공되고, 하나는 공인하는 기관과 단절된 모드로 제공되는 현재값이고, 다른 하나는 연결된 모드로 제공되는 주기적인 값이다. 단절된 모드에 있어서, 비대칭 알고리즘(F)과 관련되고 비밀 키(Kp)를 이용하는 알고리즘(G), 한편으로 확증값(VA)이 특정 번호(Ns) 및 정보(I)와 양립가능함을 그리고 다른 한 편으로는 요구되는 거래나 서비스가 정보(I)와 양립가능함을 확인하기 위해, 캐리어로부터 판독된 확증값(VA)에 적용된다.

연결 모드에 있어서, 캐리어의 확증값을 수정할 수도 있다.

대표도



명세서

도면의 간단한 설명

제1도는 공인하는 기관의 단말기 및 판매 지점에 설치된 단말기와 상호 협력하는 휴대물(portable object)을 도시하는 도면이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 데이터 캐리어(data carrier) 또는 장치가 공인 기관 (authorized organization) 에 의해 진정으로 발행된 것임을 확인하는 방법에 관한 것으로, 상기 캐리어 또는 장치는 거래 (transaction)를 행하거나 또는 상기 기관의 관련 판매업자 (distributor)의 건물에서 어떤 서비스 또는 어떤 장소로의 접근을 허용하기 위한 것이고, 상기 기관은 각각의 캐리어에 귀속하는 현재 권리의 내용을 하나의 파일 속에 간직하며, 상기 방법은 상기 기관에서 만들어진 한 세트의 캐리어들 사이에서 구별되도록 특정번호 (Ns)를 각각의 캐리어에 할당하고, 이 번호를 해당 캐리어에 입력하는 과정을 포함한다.

발명이 이루고자 하는 기술적 과제

본 발명의 목적은, 상기 캐리어 자체 및 상기 캐리어와 상호 작용하도록 한 판매업자의 선택적 단말기(optional terminal)내에서 가장 단순하고 가능한 수단을 이용하는 전술한 종류의 방법을 제안하는 데 있다. 상기 캐리어가 예컨대 전자식이라면, 어떠한 관련된 연산 회로 없이, 최소의 가능한 크기를 갖는 각각의 메모리에 대해, 그것이 단 하나의 메모리로 이루어지는 것이 바람직하다. 또한, 비밀 키(key)를 포함하는 것은 관련 단말기는 물론 캐리어에도 바람직하지 않으며, 이는 이러한 키가 남을 속이려는 의도를 가진 사람에 의해 발견되기 용이하기 때문이다.

발명의 구성 및 작용

본 발명에 따르면, 상기 목적은 위에서 언급한 일반적인 형태의 방법에 의해 달성되며, 또한 다음을 더 포함한다; 상기 캐리어 또는 장치에 정보(I)를 할당하여 이 캐리어 또는 장치를 초기화하며, 상기 정보는 상기 파일의 내용의 한 기능으로서, 특정 번호 (Ns) 및 정보(I) 로부터, 비대칭형 알고리즘(F)과 비밀 키(Ks)를 이용해 확증값 (authentication value)(VA)을 계산하고, 상기 확증값을 캐리어에 입력하여, 이 캐리어에 귀속되는 권리를 한정하며 ; 상기 캐리어를 사용할 때마다, 상기 캐리어로부터 판독된 확증값(VA) 및 상기 비밀 키와 관련된 공공 키 (public key) (KP)에 대해 상기 비대칭 알고리즘 (F)과 관련된 알고리즘 (G)을 적용하여 계산을 행하여, 공인된 엔티티 (entity)에 접속되지 않은 모드로 그의 분류를 행하여, 한편으로는 상기 확증값(VA)이 특정 번호(Ns) 및 정보(I)와 양립하도록 확인하고, 다른 한편으로는 요구되는 거래 또는 서비스가 정보(I)와 양립하도록 확인하며 ; 주기적으로 또는 이와 같은 종류의 거래 또는 서비스의 한 기능으로서, 우선 공인 기관 또는 판매업자에 의한 캐리어의 확증을 행하여, 캐리어로부터 판독된 확증값(VA)이 특정 번호(Ns) 및 정보(I)와 양립할 수 있음을 확인함으로써, 공인 기관에 연결된 모드에서 판매업자로부터의 캐리어에 대한 확증 작업을 실시하고, 이 확증이 긍정적이면, 이 캐리어가 상기 파일의 현재 상태의 한 기능으로서 그 권리들을 여전히 가지고 있음이 공인 기관에 의해 확인되고, 그 후 그 응답이 긍정적이고 정보(I)의 변경이 권리의 현재 상태를 해석하기 위해 필요하면, 비대칭 알고리즘(F) 및 비밀 키(Ks)에 의해, 특정 번호(Ns) 및 새로운 정보(I)로부터 새로운 확증값(VA')을 계산하여, 이 새로운 값을 캐리어에 입력한다. 비대칭 알고리즘이 이용되므로, 확증값(VA)을 기록하는 동작만이 비밀 키의 사용을 필요로 하는 반면, 이 값의 전형적인 확인은 공공 키만을 필요로 한다.

그러나, 공인하는 기관과의 주기적인 접속이 예상된다는 사실을 통해, 각각의 캐리어에 귀속하는 권리의 보다 완전한 확인 및 필요한 경우 이 캐리어의 갱신을 행할 수 있다.

또한 본 발명은 상기 방법과 관련된 여러 가지 장치에 관한 것이다.

본 발명의 세부 사항 및 장점은, 단일 첨부 도면을 참고로, 바람직하나 비제한적인 실시예의 상세한 설명을 통해 더욱 명확해질 것이다. 상기 도면에는, 공인하는 기관의 단말기 및 판매 지점에 설치된 단말기와 상호 협력하는 휴대물(portable object)이 개략적으로 도시되어 있다.

상기 도면에는, 휴대물(1) 특히, 인터페이스(3)를 통해 외부와 연결되는 EEPROM 메모리를 구비하고 있는 전자 카드가 도시되어 있다. 이 카드는 마이크로프로세서 타입의 어떠한 처리 회로도 포함하고 있지 않다. 특히 메모리(2)에는 2개의 정보 특히, 카드가 제작될 때 할당되는 카드의 일련 번호(Ns) 및 카드가 실제로 공인 기관에 의해 발행되었음을 확인하는 확증값(VA)이 위치한다. 이 값(VA)의 계산은 하기에 설명한다.

부호 4는 카드(1)를 발행하거나 갱신하는 권한을 가진 기관의 중앙 컴퓨터를 나타낸다. 특히 이 컴퓨터는 처리 회로(5)와 메모리(6)를 포함하며, 이것들은 서로 통신하며 인터페이스(7)와 통신한다. 메모리(6)에는 데이터를 암호화하기 위해 메모리에서도 비밀 키(Ks)를 이용해야 하는 비대칭 암호 알고리즘(F)의 프로그램이 입력되어 있는 반면, 그 데이터를 해독하는데는 상응하는 공공 키(Kp)만의 사용을 필요로 한다. 또한 메모리(6)에는 공인 기관에 의해 발행된 각각의 캐리어에 귀속하는 현재의 권리를 포함하고 있는 파일이 위치한다.

상기 목적은, 2개의 데이터 특히, 이 카드에 첨부된 권리를 한정하는 정보(I)의 항목 및 카드의 일련 번호(Ns)를 이용하여, 카드(1)로 전달하기 위한 확증값(VA)을 계산하는데 있다. 상기 정보(I)는 파일의 내용으로서의 기능을 행하며, 다음 형태 중 하나를 취할 수 있다. 예컨대 :

1. 권리에 대한 기한의 계산을 가능하게 하는 관련 데이터 : 이는 카드의 소유주가 소정의 기간 동안의 소정의 서비스에 대해 서명한 날짜, 또는 직접적으로 이 서비스로의 접근 기한을 포함한다 ;

2. 다음의 메시지 : 100 F 보다 더 큰 양의 어떤 거래도 받아들이지 말 것 ;

3. 메시지 : 오늘부터, X 씨의 권리는 유효함

4. 1과 10 사이의 숫자, 이것은 기관이 카드의 소유자에 대해 가지는 신용의 정도를 한정함.

바람직하게는, 비밀이 아닌 정보(I)라도, 확실한 신용도를 유지하기 위해, 암호화된 형태로 표현된다. 따라서, 다음과 같이 기록될 수 있다:

VA = F(Ns, I, Ks)

VA는 일련번호 (Ns) 및 정보(I)로 구성된 메시지의 비대칭 서명으로 생각할 수 있다.

변형예에 있어서, 상기 번호(Ns)는 카드(1)를 개별적으로 확인할 수 있는 어떤 다른 번호로 이루어질 수 있다.

판매 단말기(8)의 한 지점이, 상품 또는 서비스의 배달 또는 그들에 대한 지불을 위해 도시되어 있다. 이것은 서로 협력하여 동작하며 적절한 링크에 의해 인터페이스(11)와 함께 동작하는 처리 회로(9) 및 메모리(10)를 포함한다. 상기 메모리는 전술한 알고리즘(F)과 관련된 알고리즘(G)의 프로그램을 포함하고, 또한 비밀 키(Ks)와 관련된 공공 키(Kp)도 포함한다. 제 1 실시예에 있어서, 메시지 회복으로 형태의 과정이 이용된다(즉, 메시지의 내용을 회복시키는 과정). 이 경우, 상기 알고리즘(F)은 인수 분해(factoring)의 문제에 근거하고 있고, 단말기에 포함되어 있는 알고리즘(G)은 알고리즘(F)의 역인 알고리즘 F^{-1}으로 이루어진다. VA의 계산의 안전성 지향의 특성을 보장하기 위해, 카드(1)의 메모리(2)에서 VA의 크기가 적어도 512 비트와 동일한 것이 바람직하다.

따라서, 상기 단말기는, 다음과 같이 값들(Ns, I)의 쌍을 회복할 수 있다;

$(Ns, I) = F^{-1} (VA, Kp)$

상기 알고리즘(F)으로서, 특히 RFA (Rivest, Shamir, Adleman) 형의 알고리즘이, 예컨대 다음의 형태로 이용될 수 있다 :

VA = [(Ns, I)의 세제곱근] modulo n

이 식에서 :

- (Ns, I)는 Ns와 I의 연접을 의미한다 ;

- n은 공공 키 Kp ; n = p × q를 의미하며, 여기서 p 와 q 는 비밀 키 (Ks)를 구성하는 첫 번째 두 개의 비밀 번호이다.

이 경우, F^{-1}는 다음과 같이 표현된다.

$(Ns, I) = VA^3$ modulo n

카드를 확증하는 방법은, 먼저, 공인 기관에서의 초기화 단계를 포함하며 그것의 중앙 컴퓨터는 소정의 카드에 대한 첫 번째 값(VA)을 계산하여 이것을 카드의 메모리(2)에 입력한다.

공인 기관과 관련된 판매의 각 지점에서의 단말기(8)은, 필요한 많은 거래에 상응하여 동일 카드(1)의 임의의 수만큼의 연속적인 확인을 실행하는 기관의 중앙 컴퓨터(4)와 관련된 불연속 모드에서 진행할 수 있다.

각 확인시, 이것은 카드의 메모리에서 판독하는 값(VA)에 적용된 알고리즘(F^{-1})으로부터 Ns, I쌍을 재계산한다. 그 후, 이것은 한 편으로, 카드의 메모리로부터 실제로 판독되는 일련 번호(Ns)가 계산된 번호에 상응함을 확인하고, 다른 한편으로, 계산된 정보(I)가 원래 일관된(coherent) 정보이거나, 또는 다시 말해, 요구되는 거래와 양립할 수 있는 이해 가능한 메시지를 구성함을 확인한다. 이의 결과가 긍정적이면, 판매 단말기의 지점은 거래를 허가할 수 있다.

상기 정보 (I)에 대한 예와 관련하여, 상기 양립성의 확인은 예컨대 다음을 보장하는 것을 포함할 수 있다 :

1. 권리의 기한이 거래일에 만료되지 않았음 ;

2. 거래량이 100 F 이하임 ;

3. X 씨의 권리는, 마지막 승인이 얼마나 오래 전에 이루어졌는지에 근거하여, 공인 기관측에서 재승인을 필요로 하지 않음 ;

4. 거래의 특성이 할당된 번호에 근거하여 인정됨.

다른 한편, 판독되는 Ns와 계산되는 Ns간의 차, 또는 계산된 정보(I)의 모순은 카드가 공인 기관에 의해 발행되지 않았음을 나타내며, 따라서, 판매 단말기의 지점이 이 거래를 거부한다.

예컨대, 한 달에 한 번 또는 주요 거래가 이루어진 때, 판매 단말기의 지점이 연속 모드, 즉 공인 기관의 중앙 컴퓨터(4)에 접속된 상태로 확인 작업을 행한다. 제1단계에 있어서, 이 카드가 실제로 진찌임을 보장하는 과정이 포함된다. 이것은 2가지 방법으로 행해질 수 있다. 전술한 바와 같이 판매 단말기의 지점이 불연속 모드로 값(VA)을 확인하거나, 또는 공인 기관이 이를 떠맡게 된다. 이 기관은 카드에 확증값(VA)의 할당을 허용하는 모든 요소를 갖고 있고, 따라서 이 기관이, 예컨대 확증값(VA), 일련 번호 (Ns) 및 정보(I)가 놓인 파일의 내용과의 직접적인 비교에 의해, 또는 전술한 방식으로 특정 상황에 대해 재계산된 값(VA)과의 비교에 의해, 카드로부터 판독된 값(VA)을 용이하게 확인할 수 있다.

모든 경우의 기능이 연속 모드로 되는 제2단계에 있어서, 기관의 중앙 컴퓨터가, 파일을 조사하여, 재계산된 숫자(Ns)를 지니고 있는 카드는 그 권리를 여전히 갖고 있음을 확인한다. 예컨대, 이것은 다음을 확인한다:

-카드가 도난되었다는 신고 서류가 제출되지 않았음;

-카드는 권리를 갖고 있는 은행 계좌(bank account)가 초과 인출되지 않았음; 등.

제3단계에 있어서, 필요에 따라, 기관은 유효 기간을 연장하기 위해, 카드의 현존하는 권리의 한 기능으로서, 또는 이전의 연결이래 허용된 새로운 권리의 한 기능으로서 확증값(VA)을 갱신한다. 그를 위해, 기관의 중앙 컴퓨터가, 새로운 정보(I')의 한 기능오로서, 권리의 수정안을 다음과 같이 고려한다:

VA' = F(Ns, I' , Ks)

그 후, 이것은 상기 과정을 종료시키는 현재의 값(VA)을 대신하여, 카드의 메모리(2)에 이 값(VA')을 기록한다.

본 발명의 제2실시예에 있어서, 메시지 회복이 없는 형태(즉, 메시지의 내용을 회복할 수 없는)의 과정이 이용된다. 이 경우, 알고리즘(F)은 예컨대 불연속 대수(discrete logarithm)의 문제에 근거하며, 단말기에 포함된 알고리즘(G)은 F의 역인 알고리즘(F^{-1})으로 이루어지는 것이 아니라, 오히려 확증값(VA)이 일련번호(Ns) 및 정보(I)로부터 실제로 계산될 수 있다는 확신을 가능하게 하는 방식으로후자와만 관련된다. 예로서, 상기 알고리즘(G)은 공지의 DSS(Digital Signal Standard) 알고리즘이며, 이것은 확증값(VA) 및 공공 키(Kp) 뿐만 아니라, 일련 번호(Ns)및 정보(I)에 근거하여, 한 편으로 Ns, 일련번호(Ns)및 정보(I)에 근거하여, 한 편으로 VA와 다른 한편으로 Ns, I 간의 양립성을 확인할 수 있도록 한다. 여기서, 단말기에 의한 Ns, I간의 양립성을 확인할 수 있도록 한다. 한편, VA의 안전성 지향 특성을 보장하기 위해, 카드(I)의 메모리(2)에서의 그 크기가 적어도 320비트가 되는 것이 바람직하다.

단말기에 의한 양립성의 계산은, 이 제2실시예에 있어서, 단말기이 일련 번호(Ns) 및 정보(I)에 관한 지식을 갖고 있는 것이 필요하다.

일련 번호와 관련하여, 이것은 카드(1)로부터 단말기에 의해 판독된다.

정보(I)에 관해서는, 2개의 상황이 고려될 수 있다 :

- 이 정보가 카드의 메모리(2)에 저장되고 단말기에 그것을 거기에서 판독함;

- 이 정보가 고객의 전체 카테고리에 대해 유일하므로, 단말기에 의해 은연중에 공지됨; 이것은 예컨대 다음과 같은 형태의 정보일 것이다:

1000 F까지 허용된 거래.

각 판매 지점의 단말기(8)은 동일 카드(1)의 연속적인 확인을 행하는 불연속 모드로 진행될 수 있다. 매번, 이것은 알고리즘(G)을 이용하여 값(Ns)과 값(VA)의 양립성을 확인하며, 이들 3개의 값은 카드로부터 판독되거나 또는 - 정보(I)와 관련하여 - 단말기에 의해 은연중에 공지된다.

그 응답이 긍정적이면, 거래를 인가할 수 있다. 제 1 실시예에서와 같이, 단말기는 필요한 거래와 정보(I)의 양립성을 확인할 수 있다.

접속 모드에서의 기능은 제 1 실시예에 대해 설명한 것과 유사하며, 유일한 차이점은, 카드의 확증이 확인되는 상기 제 1 단계가 판매 단말기의 지점에 의해 행해지는 경우, 문제의 값(Ns, I)이 재계산된 값이 아니라 카드로부터 판독된 값이라는 점이다. 카드에 첨부된 권리가 수정되어야 하는 경우, 공인 기관의 중앙 컴퓨터는, 적용가능한 새로운 정보(I')로서, 새로운 확증값(VA')을 현재의 데이터를 대신하여 기록한다.

발명의 효과

본 발명은, 메모리 카드의 확증뿐만 아니라, 일반적으로, 전자식인지의 여부에 관계없이, 예컨대 종이 형태(일련 번호(Ns) 및 확증값(VA)이 기록된 신분 증명서 또는 수권 카드) 등의 어떠한 데이터 캐리어의 확증에도 적용될 수 있다.

상기 데이터 캐리어는, 일련 번호(Ns) 및 확증값(VA)을 결합하는 휴대용 컴퓨터(PC)와 같은 장치에 의해서도 구현될 수 있다.

(57) 청구의 범위

청구항 1

데이터 캐리어가 거래(transaction)를 행하거나 또는 공인 기관의 관련 판매업자 (distributor)의 구내에서 어떤 서비스 또는 어떤 장소로의 접근을 허용하도록 기능하며, 공인 기관은 상기 캐리어에 첨부된 현재 권리를 정의하는 파일을 구비하고, 상기 데이터캐리어 (data carrier)가 공인 기관 (authorized organization)에 의해 진정으로 발행된 것임을 확인하는 방법에 있어서, 상기 방법은, 상기 기관에 의해 제조된 한 세트의 캐리어들중 상기 캐리어가 구별되도록 특정 번호(Ns)를 상기 캐리어에 할당하는 단계 ; 상기 특정 번호를 캐리어에 입력하는 단계 ; 상기 파일의 내용의 한 기능이고, 상기 캐리어에 첨부된 현재 권리를 정의하는 정보(I)를 상기 캐리어에 할당하고, 상기 특정 번호(Ns) 및 상기 정보(I)로부터, 비대칭형 알고리즘(F)과 비밀 키(Ks)를 사용하여 현재 확증값(authentication value)(VA)을 계산하여 공인 기관에서 상기 캐리어를 초기화시키고, 상기 캐리어에 상기 현재 확증값을 입력하는 단계 ; 상기 캐이어를 사용할 때마다, 상기 캐리어로부터 판독된 현재 확증값(VA) 및 상기 비밀 키와 조합된 공공 키(public key) (Kp)에 대해 상기 비대칭 알고리즘(F)과 관련된 알고리즘(G)을 적용하여 계산을 행하여, 공인 기관

에 결합되지 않은 모드로 상기 관련된 판매업자에 의해 그의 분류를 행하여, 상기 확증값(VA)이 특정 번호(Ns) 및 정보(I)와 양립하는 것을 확인하고, 또한 요구되는 거래 또는 서비스가 정보(I)와 양립하는 것을 인하는 단계 ; 및 단말기가 상기 공인 기관에 결합된 모드에서 상기 데이터캐리어의 확증이 행해져야 할 때를 정의하는 소정 조건에 기초하여, 상기 판매업자 또는 상기 공인 기관에 의해 상기 캐리어의 확증을 우선적으로 행하며, 상기 공인 기관에 결합된 모드로 상기 데이터캐리어의 확증을 선택적으로 행하고, 상기 캐리어로부터 판독된 현재 확증값(VA)이 상기 특정 번호(Ns) 및 정보(I)와 양립할 수 있음을 확인하며, 상기 확증이 포지티브이면, 상기 캐리어가 상기 파일의 현재 상태의 한 기능으로서 권리들을 계속 소유하는 것을 공인 기관에 의해 확인을 행하고, 상기 확인이 긍정적이고 상기 정보(I)의 변경이 권리의 현재 상태를 해석하기 위해 필요한 경우, 비대칭 알고리즘(F) 및 비밀 키(Ks)에 의해, 특정 번호(Ns) 및 갱신된 정보(I')로부터 갱신된 확증값(VA')을 계산하여, 이 갱신된 값을 캐리어에 입력하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 2

제1항에 있어서, 상기 비대칭 알고리즘(F)과 관련된 알고리즘(G)이 상기 비대칭 알고리즘의 역인 알고리즘(F^{-1})을 포함하며, 캐리어가 이용될 때마다, 상기 캐리어로부터 판독된 현재 확증값을 사용하여, 상기 알고리즘에 의해, 상기 캐리어에 관련된 특정 번호(Ns) 및 정보(I)를 계산함으로써 상기 확증이 계산에 의해 행해지고, 다음, 판독된 특정 번호(Ns)가, 계산된 것과 동일하고 또한 이 계산된 정보(I)가 포괄적 메시지를 구성하며 또한 요구되는 거래 또는 서비스와 양립할 수 있음을 확인하는 것을 특징으로 하는 방법.

청구항 3

제1항에 있어서, 상기 비대칭 알고리즘(F)과 관련된 상기 알고리즘(G)은, 상기 확증이 정보(I) 및 특정 번호(Ns)에 대한 지식을 필요로 하고, 정보(I)는 캐리어에 입력되어 있거나 또는 판매업자에 의해 공지되어 있으며, 캐리어가 사용될 때마다, 캐리어로부터 판독된 특정 번호(Ns) 및 상기 정보(I)를 관련 알고리즘(G)에 추가로 적용함으로써 상기 계산이 행해지는 것을 특징으로 하는 방법.

청구항 4

제1항에 있어서, 상기 정보(I)는 캐리어에 첨부된 권리의 기한의 계산을 가능하게 하고, 각 확증시, 요구되는 거래 또는 서비스 일자에, 권리의 기한이 만료되었는지의 여부를 확인하는 기준일을 포함하는 것을 특징으로 하는 방법.

청구항 5

제1항에 있어서, 상기 소정 조건은, 상기 단말기가 상기 공인 기관에 결합된 모드로 상기 데이터캐리어의 확증이 주기적으로 행해져야 하는 것을 정의하는 것을 특징으로 하는 방법.

청구항 6

제1항에 있어서, 상기 소정 조건은, 상기 단말기가 상기 공인 기관에 결합된 모드로 상기 데이터캐리어의 확증이 거래 또는 서비스 형태의 기능으로 행해져야 하는 것을 정의하는 것을 특징으로 하는 방법.

청구항 7

공인 기관에 의해 제조된 한 세트의 캐리어들중 데이터 캐리어가 구별되도록 그안에 기억된 특정 번호(Ns); 및 비밀키(Ks), 상기 특정 번호(Ns), 및 공인 기관의 소유이고 상기 데이터 캐리어에 첨부된 현재 권리를 정의하는 파일의 내용의 기능인 정보(I)로부터 비대칭 알고리즘(F)에 의해 계산되어 기억되고, 상기 데이터 캐리어에 첨부된 상기 현재 권리의 수정에 따라 공인 기관에 의해 갱신되는 현재 확증값(VA)을 포함하는 것을 특징으로 하는 데이터 캐리어.

청구항 8

제7항에 있어서, 비대칭 알고리즘(F)은, 캐리어의 확증이 정보(I) 및 특정 번호(Ns)에 관한 지식을 필요로 하며, 이 정보(I)는 각각의 캐리어에 대해 특유하며 상기 캐리어에 입력되는 것을 특징으로 하는 데이터 캐리어.

청구항 9

제7항에 있어서, 상기 캐리어는, 상기 현재 확증값(VA)이 저장되어 있는 전자 EEPROM 메모리를 구비하는 휴대물인 것을 특징으로 하는 데이터 캐리어.

청구항 10

제8항에 있어서, 상기 캐리어는, 상기 현재 확증값(VA)이 저장되어 있는 전자 EEPROM 메모리를 구비하는 휴대물인 것을 특징으로 하는 데이터 캐리어.

청구항 11

데이터 캐리어와 협동하여 거래 또는 서비스를 제공하기 위한 단말기로서, 상기 데이터 캐리어는, 비밀키(Ks), 특정 번호(Ns), 및 공인 기관의 소유이고 상기 데이터 캐리어에 첨부된 현재 권리를 정의하는 파일의 내용의 기능인 정보(I)로부터 비대칭 알고리즘(F)에 의해 계산된 현재 확증값(authenttication value)(VA) 및 공인 기관에 의해 제조된 한 세트의 캐리어들중 데이터 캐리어가 구별되도록 특정 번호(Ns)를 기억하는, 단말기에 있어서, 상기 비대칭 알고리즘(F)과 관련된 알고리즘(G), 비밀 키(Ks)와 조합된 공공 키(Kp), 및 단말기가 공인 기관에 결합된 모드로 데이터캐리어의 확증이 행해져야 할 때를 정의하는 소정 조건을 기억하기 위한 수단; 상기 알고리즘(F), 공공 키(Kp), 및 상기 데이터 캐리어로부터 판

독된 현재 확증값(VA)을 이용하여 계산을 행하여, 상기 현재 확증값(VA)이 특정 번호(Nf) 및 정보(I)와 양립하고, 또한 요구되는 거래 또는 서비스가 정보(I)와 양립하는 것을 확인하는 수단; 상기 소정 조건에 기초하여, 상기 단말기가 상기 공인 기관에 결합된 모드로 상기 데이터캐리어의 확증이 행해지는지의 여부를 결정하기 위한 수단; 및 상기 확증이 상기 모드에서 행해져야 하는 경우 상기 현재 확증값(VA)을 검사하도록 공인 기관에 요구하기 위한 수단을 포함하는 것을 특징으로 하는 단말기.

청구항 12

제11항에 있어서, 상기 소정 조건은, 상기 단말기가 상기 공인 기관에 결합된 모드로 상기 데이터캐리어의 확증이 주기적으로 행해져야 하는 것을 정의하는 것을 특징으로 하는 단말기.

청구항 13

제11항에 있어서, 상기 소정 조건은, 상기 단말기가 상기 공인 기관에 결합된 모드로 상기 데이터캐리어의 확증이 거래 또는 서비스 형태의 기능으로서 행해져야 하는 것을 정의하는 것을 특징으로 하는 단말기.

청구항 14

비밀키(Ks), 특정 번호(Ns), 및 공인 기관의 소유이고 상기 데이터 캐리어에 첨부된 현재 권리를 정의하는 파일의 내용의 기능인 정보(I)로부터 비대칭 알고리즘(F)에 의해 계산된 현재 확증값 (authentication value) (VA) 및 공인 기관에 의해 제조된 한 세트의 캐리어들중 데이터 캐리어가 구별되도록 특정 번호(Ns)를 기억하는 수단을 갖는 데이터 캐리어와 협동하기 위한 공인기관의 중앙장치로서, 상기 중앙 장치는, 상기 파일, 상기 비대칭 알고리즘(F), 및 상기 비밀 키(Ks)를 기억하기 위한 수단 ; 상기 데이터 캐리어가 상기 파일의 현재 상태의 한 기능으로서, 권리를 계속 소유하고 있는 지 및 상기 데이터 캐리어에 대한 상기 현재 확증값(VA)의 갱신되어야 하는지의 여부를 체크하기 위한 수단 ; 상기 파일 및 특정 번호(Ns)에서 판독된 갱신 정보(I')로부터, 비대칭 알고리즘(F) 및 비밀 키 (Ks)를 사용하여 갱신된 확증값(VA')을 계산하기 위한 수단 ; 및 상기 갱신된 값을 상기 데이터 캐리어에 입력하기 위한 수단을 포함하는 것을 특징으로 하는 중앙 장치.

도면

도면1