(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) Int. Cl.[6]
G07F 7/08

(45) 공고일자 2003년08월19일
(11) 등록번호 10-0374071
(24) 등록일자 2003년02월17일

(21) 출원번호	10-1997-0702002	(65) 공개번호	특1997-0706557
(22) 출원일자	1997년03월27일	(43) 공개일자	1997년11월03일
번역문제출일자	1997년03월27일		
(86) 국제출원번호	PCT/DE1995/01286	(87) 국제공개번호	WO 1996/10810
(86) 국제출원일자	1995년09월19일	(87) 국제공개일자	1996년04월11일
(81) 지정국	국내특허 : 아일랜드 중국 일본 대한민국 우크라이나 미국 EA 유라시아특허 : 러시아 EP 유럽특허 : 오스트리아 벨기에 스위스 리히텐슈타인 독일 덴마크 스페인 프랑스 영국 그리스 이탈리아 룩셈부르크 모나코 네덜란드 포르투칼 스웨덴 핀랜드		

(30) 우선권주장 P 44 35 137.2 1994년09월30일 독일(DE)
P 44 39 266.4 1994년11월03일 독일(DE)

(73) 특허권자 지멘스 악티엔게젤샤프트
독일 뮌헨 80333 비텔스파허프라쯔 2
(72) 발명자 쉬렝크, 하르트무트
독일 데-85540 하르 파자넨베크 22
(74) 대리인 남상선

심사관 : 김기영

(54) 터미널과휴대용데이터캐리어장치를갖고있는데이터전송시스템및이터미널에의하여상기휴대용데이터캐리어장치를재충전하는방법

명세서

기술분야

<1> 본 발명은 적어도 하나의 터미널을 갖고 있으며, 카운터로서 역할을 하며 청구할 수 있는 금액을 나타내는 적어도 하나의 제 1 값 영역이 존재하는 비휘발성 반도체 메모리가 갖추어진 적어도 하나의 휴대용 데이터 캐리어 장치를 갖고 있는 데이터 전송 시스템에 관한 것이고, 또한 휴대용 데이터 캐리어 장치의 값 영역을 재충전하는 방법에 관한 것이다.

배경기술

<2> 그런 휴대용 데이터 캐리어 장치는 예컨대 전화카드로서 사용되는 현재의 관용 칩카드이다. 이 경우 고정 터미널은 카드를 사용할 수 있는 전화기 세트이다. 단순한 메모리 카드로 설계된 그런 칩 카드들은 EEPROM과 같은 비휘발성 반도체 메모리를 포함하는데, 그것은 필연적으로 청구될 선납된 전화 유니트를 위한 카운터로서의 역할을 한다. 상기 EEPROM 은 이 경우 예를들어 EP-B 0 321 727 또는 US-A 5,001,332 에 따라서 와이어드(wired)될 수 있고, 그에 따라 다단계의 주판과 같은 카운터로서의 역할을 한다. 카드의 값과 그에 따른 카운터의 카운팅 범위는 카드에 대한 기록 및 더 이상 인정되지 않는 카운터의 범위를 막는것으로 설정된다. 이와 같은 설정 동작 이전의 카운터는 언제나 최대 카운팅 범위를 갖고 있다. 현행의 관용 전화카드는 오직 한번 사용될 수 있고 사용후에는 폐기된다. 그러나, 전자지갑으로서의 그런 칩 카드들의 사용에 관하여도 역시 현재 논의 중이다. 이 목적을 위해 사용될 수 있는 칩 카드들은 재충전 가능할 때, 즉 카운터의 상태가 어떤 양만큼 청구된 이후에 다시 증가될 수 있을 때에만 그 가치가 있다. 이러한 카운터 상태의 증가는 특별한 충전 터미널들에서 이루어지며, 거기에서 사용자들은 현금지불로, 신용카드 수단으로 또는 계좌번호를 알려줌으로써 어떤 양만큼 자신의 카드를 채울 수 있다.

<3> 칩 카드의 카운터를 재충전할 때, EEPROM 의 구조상 더 큰 카운팅 범위 또는 전체의 카운터를 처음상태로 지우는 것, 즉 너무 많은 카운팅 범위가 일시적으로 세트되는 것이 필수적일 것이다. 오로지 그 이후에만 새로운 카운터 상태가 프로그래밍 동작들에 의하여 카운팅 범위의 새로운 제한값으로 세트된다. 만약 사용자가 카운터를 지우는 것과 새로운 프로그래밍을 하는 시간사이에 카드를 터미널로부터 빼내다면, 그런 부적법한 조작의 결과로서 그가 너무 많은 양을 채우게 되는 것이 가능하다. 또한, 사용자가 터미널과 카드사이의 데이터 트래픽을 조작하여 너무 많은 양을 채울 수 있게 되는 것도 생각할 수 있다.

<4> 전송 경로상에서의 데이터의 조작은 소위 전자서명에 의하여 막을수는 있다. 전송되는 데이터가 비밀 키의 수단에 의하여 인코딩될 수 있고 데이터의 전송자에게 유일하게 할당된 특별한 키에 의하여만 디코딩될 수 있는데, 그 결과로서 전송자는 결정적으로 자기임을 나타낼 수 있고 데이터는 조작될 수 없

는데 그것은 인코딩 키가 비밀이기 때문이다. 그러나 그런 인코딩과 디코딩은 복잡하고 매우 빠른 수학적 장치를 요하는데, 이미 알려진 암호카드의 예에서 사용되는 것과 같은 고가의 마이크로프로세서들에 의해서만 가능하다.

<5> 유럽특허공개공보 0 398 545 호는 적어도 두 개의 영역을 가지는 비휘발성 메모리에 데이터를 저장하기 위한 방법 및 장치를 기술하고, 상기 메모리에 연속적인 데이터가 선택적으로 기입된다. 이런 경우, 각 메모리 영역은 비휘발성 상태로 설정될 수 있는 플래그에 의해 특정 시간에 예를들어 스위칭 온 시간에 유효 메모리로 식별될 수 있다. 각각의 메모리가 두 개의 상태를 가정할 수 있는 자신의 플래그를 할당하기 때문에 동일 상태를 양쪽 플래그가 가정할 수 있다. 그러므로, 공지된 방법/공지된 장치의 경우에 "조정" 로직에 의해 실제적으로 유효한 상태를 결정하는 것이 필요하다.

<6> 공지된 장치의 경우, 메모리 동작의 "일반적인 경우"에서 양쪽 플래그는 항상 시간내 특정 포인트에서 동일 설정 상태를 가정하지만, 마지막 설정하지 않은 플래그는 리셋된다. 그러나 이것은 기입 동작 및 제거 동작이 항상 필요하고, 부가적인 시간을 가진다.

발명의 상세한 설명

<7> 따라서 본 발명의 목적은 이런 일반적인 형태의 데이터 전송 시스템 및 휴대용 데이터 캐리어 장치 카운터의 조정을 막는 재충전이 가능한 빠르며 간단한 회로를 가질 수 있는 방법을 제시하는 것이다.

<8> 상기의 목적은 비휘발성 반도체 메모리에 두 번째 값 영역을 둠으로써 달성되는데, 각 경우에 두 값 영역중에서 오직 하나만이 비휘발성 상태에서 활성화될 수 있고 각 경우에 다른 값 영역은 단지 일시적으로 활성화될 수 있다.

<9> 여기에서 비휘발성 상태로의 활성화가 가능하다는 것은 상기 두 값 영역중에서 청구가 행해질 수 있는 값 영역인 것으로 마지막으로 정의된 정보가 작동 전압을 스위칭 오프한 후에도 또는 충전 동작의 중단시에도 그대로 유지된다는 것을 의미한다. 이것은 단지 일시적으로 활성화된 값 영역은 작동전압을 스위칭 오프 또는 충전 동작의 중단 그리고 그 작동 전압이 다시 스위칭온 또는 충전 동작의 재개후에 다시 비활성화되고 일시적으로 다시 한번 활성화되어야 한다는 것을 의미한다. 오로지 성공적이고 올바른 칩 카드의 재충전 이후에만, 즉 오로지 잔여액과 터미널에 입력된 채워질 수 있는 값의 합계에 따라서 단지 일시적으로 활성화된 값 영역의 카운팅 범위의 정확한 제한을 가한 후에만 단지 일시적으로 활성화된 값 영역은 전환되어 비휘발성 상태로의 활성화가 가능하고, 그 결과로서 그전에 비휘발성 상태로의 활성화가 된 값 영역은 비활성화되고 처음상태로 새로운 차징 동작을 위하여 오직 일시적으로 활성화될수 있다.

<10> 그러므로, 만약 단지 일시적으로 활성화된 값 영역의 차징 동작 동안에 악의를 가진 사람이 카운터를 지운후 입력할 값에 따른 그 카운팅 범위의 새로운 제한을 하기 전에 카드를 터미널로부터 제거시키려고 한다면, 다음번 사용할 때, 즉 동작전압이 다음번에 가해질 때 비휘발성 상태로의 활성화가 가능한 값 영역은 계속 활성화될 것이고 이전에 오직 일시적으로 활성화된 값 영역은 비활성화될 것이다.

<11> 본 발명의 유리한 개선점에 있어서, 제 2 청구항과 관련한 비휘발성 메모리의 값 영역들은 선택 논리회로를 통하여 비휘발성 플래그 메모리와 연결되어 있고, 그 상태는 비휘발성 상태로의 활성화된 값 영역을 결정한다. 동작 전압이 스위칭 오프될 때 그 비휘발성 플래그 메모리는 유지되고 특별한 상태가 언제나 동일한값 영역에 할당된다.

<12> 각 경우에 다른 값 영역을 일시적으로 활성화하기 위하여, 본 발명에 따라 선택 논리회로는 충전 제어신호의 지배를 받는다. 이 충전 제어신호는 그 중성 상태, 즉 동작전압을 가한후의 상태 예를들면 논리적인 “0” 레벨을 갖고, 또 새롭게 충전될 값 영역을 일시적으로 활성화하기 위하여 그에 상응하게 “1” 레벨로 전환된다.

<13> 그 출력신호 또는 신호들은 그 값 영역들을 연결하는 스위칭 장치를 프로그래밍 논리회로 및 확인 논리회로를 구동한다. 그러므로 값 영역은 프로그래밍 논리회로와 확인 논리회로로 연결됨으로써 활성화된다.

<14> 휴대용 데이터 캐리어 장치 또는 본 발명에 따른 데이터 전송 시스템의 칩 카드 및 이 시스템의 유리한 개선점은 제 5 청구항에 따른 방법에 의하여 재충전된다. 그 방법의 유리한 개선점은 종속항에 상세히 나타나있다.

<15> 이하에서 본 발명은 도면을 참조로 상세히 설명된다.

도면의 간단한 설명

<16> 도 1은 다음에서 소개되는 충전 터미널과 휴대용 데이터 캐리어 장치를 도식적으로 도시한 도.

실시예

<17> 데이터 전송 시스템의 두부분인 본 발명에 필수적인 회로 장치들은 블록도의 형태로 표현되어 있다.

<18> 본 도에서 휴대용 데이터 캐리어 장치는 예컨대 키와 같은 다른 구조도 생각할 수 있으나 이하에서는 카드로 참조되며, 데이터 전송 시스템의 충전 터미널내에 삽입되어 있다. 카드는 EEPROM에 의하여 유리한 방식으로 구현될 수 있는 비휘발성 메모리(NVM;Non-Volatile Memory)를 포함한다. 이 경우, 메모리 NVM 은 여러 영역으로 나뉘어지는데, 그들중 둘은 값 영역 WBA, WBB로 동작한다. 이들 값 영역 WBA,WBB는 다단계 카운터로서 유리한 방식으로 설계되고, 예를 들면 EP-B 0 321 727 또는 US-A 5,001,332 에 따라서 와이어드된다. 클리어 또는 충전된 상태에서 논리 상태 “1” 을 가지며, 그 결과 카운팅 단계의 개수 및 단계별 비트에 의하여 결정되는 최대 카운팅 범위를 가지고 있다면, 그런 카운터들은 하향식

카운터이다. 적절한 개수의 상위 단계 또는 상기 상위 단계의 최하위 비트에 기록함으로써, 카운팅 범위는 제한되며 카운팅 다운은 이 요구되는 값으로부터 최종 값 "0"으로 수행된다.

<19> 상기 값 영역 WBA,WBB들은 스위칭 장치(SV)를 통하여 프로그래밍 논리회로(PL)에 접속되고 확인 논리회로(VL)에 접속된다. 상기 프로그래밍 논리회로(PL)와 확인 논리회로(VL)는 이 경우에 제어장치(ST)의 부품을 이루는 부분들이다. 상기 제어 장치(ST)의 내부에서 스위칭 부품들의 연결 라인들은 점선으로 표현되어 있고, 그 의도는 제어장치(ST)로의 각 연결라인은 제어장치(ST) 내에서 (그림에 나타내지는 않았지만) 제어장치(ST)의 다른 부품들과 연결될 수 있다는 것을 나타내기 위한 것이다.

<20> 프로그래밍 논리회로(PL)은 값 영역인 WBA,WBB 로의 기입과 프로그래밍을 하기 위한 역할을 하고, 확인 논리회로(VL)은 쓰여진 영역들이 정확히 쓰여졌는지의 여부에 관하여 확인하거나 체크하기 위한 역할을 한다. 유리한 방식으로 확인 논리회로(VL)은 값 상태의 전자서명을 생성해내는 역할도 한다.

<21> 스위칭 장치(SV)는 선택 논리 회로(AL)에 의하여 구동되며 그런 방법으로 각 경우에 값 영역 WBA,WBB 중의 오직 하나만이 프로그래밍 논리회로(PL) 및 확인 논리회로(VL)과 연결되며 그 결과로서 활성화된다. 선택 논리 회로(AL)는 플래그 메모리(FS)에 의하여 그리고 제어 장치(ST)로부터의 충전 제어 신호(LAD)의 수단에 의하여 구동되는 그 부품을 위한 것이다. 선택 논리회로(AL)는 예컨대 비반전 출력과 반전 출력을 가지는 EXOR 게이트에 의하여 구성될 수 있다. 플래그 메모리(FS)는 비휘발성 메모리이고 제어장치(ST)로부터의 신호(PROG)에 의하여 구동된다. 플래그 메모리(FS)는 두 상태를 가진 것으로 볼 수 있는데, 이들 상태들 각각은 값 영역 WBA,WBB 중의 하나에 할당된다. 플래그 메모리(FS)의 상태는 비휘발성 상태로 저장되므로, 각각의 저장된 상태에 해당하는 값 영역 WBA 또는 WBB는 동작전압이 카드에 가해졌을 때, 즉 예를들면 카드를 충전 터미널에 접촉시켰을 때 활성화된다. 이 목적을 위하여 충전 제어 신호(LAD)는 동작전압이 가해졌을 때 정해진 상태를 가진다. 오직 충전 제어신호(LAD)의 상태를 변경시킨 후에만 다른 값 영역 WBB 또는 WBA는 각 경우에 일시적으로 활성화되고, 이전에 활성화된 값 영역 WBA 또는 WBB는 선택 논리회로(AL)에 의하여 상응하게 구동되는 스위칭 장치(SV)에 의하여 비활성화된다. 이것은 일시적인데 그것은 충전 제어 신호의 상태가 휘발성이고 동작전압이 스위치 오프되었을 때 그의 정의된 비활성화 상태를 다시 갖기 때문인바, 그것은 예를들면 충전 터미널로부터 카드를 제거시킴으로써 일어나게 되며, 그렇게 함으로써, 동작전압의 모두를 스위칭 오프한후 또는, 본 발명에 의한 바대로, 충전 동작의 모든 중단후에 상기 플래그 메모리(FS)에 의하여 정해진 값 영역은 다시 활성화가 가능해지거나 또는 활성화된다.

<22> 플래그 메모리 상태의 변경, 그리고 그에 따라서 활성화된 또는 활성화 가능한 값 영역의 비휘발성 상태로의 교체는 제어 장치(ST)로부터 플래그 메모리(FS)로의 신호(PROG)에 의하여 수행된다. 비휘발성 메모리(NVM)은 뒤에서 설명되는 서명 메모리(SIGSP) 영역, 충전 동작의 카운트가 가능하도록 하는 충전 카운터(LZ), 카드에 특수한 데이터를 저장하는 영역(KSD), 비밀코드가 저장되는 영역(GC) 등의 영역을 더 포함한다.

<23> 제어장치(ST)에는 유사-랜덤 생성기(pseudo-random generator;PZG)도 역시 포함되는데, 그것은 확인 논리회로(VL)과 동작가능하도록 연결되어 있고 비휘발성 메모리(NVM)의 서명 메모리(SIGSP), 충전 카운터(LZ), 영역(KSD) 그리고 비밀코드영역(GC)와 연결되어 있다. 이 유사-랜덤 생성기(PZG)는 EP-A 0 616 429 에 따라서 유리한 방법으로 만들어진다.

<24> 충전 터미널에는 제어장치(STT)도 역시 포함되는데, 그것은 마찬가지로 확인 논리회로(VLT) 그리고 유사-랜덤 생성기(PZGT)를 포함하며, 두 유사-랜덤 생성기 (PZG 및 PZGT)는 카드와 터미널이 실재한다면 똑같아야 한다. 카드의 제어장치(ST)와 터미널의 제어장치(STT)는 데이터를 교환하기 위하여 라인 LT1,LT2를 통하여 서로 연결되어 있다. 충전 동작의 처음단계에서, 터미널은 카드에 특수한 데이터, 활성화된 그리고 그에 따라서 청구가능한 값 영역 WBA 또는 WBB의 현재 상태, 그리고 충전 카운터(LZ)와 서명 메모리(SIGSP)의 상태를 판독한다. 카드에 특별한 데이터로부터, 진정한 터미널은 예컨대 테이블에 의하여 카드의 비밀코드를 결정할 수 있다.

<25> 이들 데이터와 소위 챌린지라고 불리우는 랜덤 숫자 역시도 터미널에서 유사-랜덤 생성기(PZGT)로의 입력이 되는데, 그것이 응답을 계산한다. 챌린지와 응답 모두는 그다음에 카드에 보내진다. 응답은 마찬가지로 그 데이터에 기초하여 거기에서 계산되고, 또 터미널로부터 전송된 응답을 가지고 마찬가지로 제어장치(ST)에 포함된 비교기의 수단에 의하여 비교된다. 만약 그들이 일치하면, 터미널은 진정한 것이라는 것이 입증되는데, 한 측면에서는 그것이 정확한 비밀코드를 결정할 수 있고 또한 정확한 유사-랜덤 생성기(PZGT)를 갖고 있기 때문이다. 유사-랜덤 생성기(PZG 또는 PZGT)는 값 영역 WBA,WBB의 내용, 즉 다시말하면 그들의 카운터 상태들의 전자서명을 생성해낼 목적으로 이용된다. 유사-랜덤 생성기의 출력신호가 카드의 비밀번호에 의존하고 오직 이 비밀코드에 의하여 재계산되므로, 만약 유사-랜덤 생성기(PZG 또는 PZGT)의 출력신호들이 일치한다면 동일한 비밀코드가 사용된 것이 틀림없는 것이다. 따라서 유사-랜덤 생성기의 출력신호가 특정의 카드에 유일하게 할당될 수 있고, 그것은 카운터 상태하의 카드의 서명을 말하는 것이 된다.

<26> 입력 데이터와 유사-랜덤 생성기의 구축이 많은 계산 동작들의 분석에 의하여 결정될 수 없게 하기 위하여, 하나 또는 그 이상의 입력 데이터는 변경가능하고 또한 모든 계산동작과 변경된다. 이들 데이터중의 하나는 충전 카운터(LZ)의 상태이고, 모든 새로운 충전 동작마다, 따라서 모든 새로운 북킹(booking) 동작마다, 1씩 증가되며 카운팅 범위가 고갈되었을 때마다 리셋된다.

<27> 또다른 데이터는 서명 메모리(SIGSP)의 내용이다. 유사-랜덤 생성기의 이전 계산의 결과 이전 카운터 상태의 서명은 각 경우에 상기 메모리에 쓰여진다. 따라서 유사-랜덤 생성기(PZG)의 출력신호가 반복되고 또 그러므로써 분석되지 못하게 하는 오직 미소한 가능성만이 있다는 것이 확실하다.

<28> 본 발명의 변형예에서, 새로운 값은 충전 동작의 서명으로써 모든 충전 동작시마다 충전 터미널을 경유하여 서명 메모리(SIGSP)로 직접 쓰여질 수 있다.

<29> 본 발명에 따라서 충전 동작은, 카드를 충전 터미널에 접촉시킨후 그리고 그에 따라서 동작 전압을 가한후, 플래그 메모리(FS)의 상태에 의하여 정해진 값 영역 WBA 또는 WBB가 활성화되고 터미널로부터

판독되는 것과 같은 단순한 방법으로 진행된다. 충전 제어신호(LKD)의 상태를 변경함으로써, 다른 값 영역 WBA 또는 WBB가 일시적으로 활성화되고 이전에 활성화된 영역은 일시적으로 비활성화된다.

<30> 그러면 그때 활성화된 값 영역 WBB 또는 WBA는 클리어되고, 그 카운터는 너무 큰 카운팅 범위를 갖는다. 이 이후에, 새로운 카운터 상태가 그의 옛 카운터 상태로부터 그리고 사용자에 의해 터미널로 입력된 청구될 양으로부터 터미널내에서 결정되며 카드로 전송된다. 사용자가 만약 미리 터미널로부터 카드를 제거할 때, 만약 값 영역의 프로그래밍이 이미 결정적으로 발생했고 비휘발성 상태이라면 그는 너무 많은 청구할 양을 얻게될 것이다. 그러나 본 발명에 의한 방법에서는, 카드를 새로이 터미널에 접촉시켰을 때, 플래그 메모리(FS)의 상태는 아직 변경되지 아니했으므로, 이전의 값영역 WBA 또는 WBB가 옛 카운터 상태를 가지고 다시활성화된다. 오직 새로운 카운터 상태가 일시적으로 활성화된 값 영역 WBB 또는 WBA 로 프로그램되었을때에만, 플래그 메모리(FS)의 상태는 제어장치(ST)로부터의 신호(PROG)에 의하여 변경되며, 그 결과로서 새로운 값 영역은 비휘발성 상태에서 활성화될 수 있고 동작전압이 새롭게 가해졌을때마다 즉, 예를들면 돈을 청구하기 위하여, 카드를 터미널에 접촉시켰을 때마다 활성화된다.

<31> 터미널에서 카드로 전송하는 동안 새로운 카운터 상태의 조작을 방지하기 위하여, 본 발명에 따른 발전된 방법에서는, 새로운 카운터 상태를 카드로 전송한후 카운터 상태는 위에서 기술된 방법에 따라 거기에서 서명된다. 그 서명은 계속해서 터미널로 보내지고 거기에서 마찬가지로 결정된 서명과 비교된다. 만약 그들이 일치하면 정확한 카운터 상태가 카드로 전송되었다는 것이 확실한 것이 된다. 만약 그들이 일치하지 않으면, 충전 동작은 비정상적으로 종료되고, 그 결과로서 부정확한 카운터 상태는 다음의 청구 동작들에게 영향을 미치지 아니하는데, 이는 플래그 메모리(FS)의 상태가 아직 변경되지 아니했기 때문이다. 후자는 서명이 일치하고 그에 따른 신호가 터미널에서 카드로 전송된 후에야 비로소 변경이 된다.

<32> 본 발명에 따른 발전된 방법에서는, 터미널은 충전동작이 시작되기 전에 카드에 관하여 그 자신이 인가되는 것이 가능해야만 한다.

<33> 이것은 어떠한 부정확한 체인저(changer)도 카드를 크레디팅(crediting)하기 위하여 사용될 수 없다는 것을 보장한다. 이 인가를 위하여 응답은 챌린지로부터 그리고 터미널에 의해 카드로부터 판독된 데이터로부터 계산되고 또 이 응답은 챌린지와 함께 카드로 전송되고 거기에서 마찬가지로 챌린지와 카드 데이터의 수단에 의하여 계산된 응답과 비교된다. 오직 응답이 일치할 때에만 충전 제어 시스템(LAD)와 프로그래밍 신호(PROG)가 생성될 수 있고, 따라서 충전 동작이 시작된다. 이 목적을 위하여, 제어 장치(ST)에 의하여 적합하게 구동된 인에이블링 장치 FGV1, FGV2가 휴대용 데이터 캐리어 장비에 제공된다. 그런 충전 동작은 이 경우에, 예를들면 충전 카운터(LZ)의 상태의 증가에 의하여 또는 더미(dummy) 프로그래밍 펄스에 의하여 시작된다. 더미 프로그래밍 펄스는 이 경우에 카드의 제어 장치(ST)에 의하여 제어신호로서 감지된 비휘발성 메모리(NVM)의 유효하지 아니한 주소에 대한 프로그래밍 펄스이다.

<34> 충전 동작의 시작이후에 조차도, 터미널이 그의 인가를 확인하고 충전 신호(LAD)가 생성된 이후에, 악의를 가진 자는 카운터 상태의 값에 영향을 미치는 것 그리고 터미널과 관계없이 카운터 상태의 비휘발성 활성화를 위한 프로그래밍 신호 (PROG)를 개시하는 것을 성공할 수도 있다. 본 발명에 따른 유리한 방법에서, 터미널은 프로그래밍 신호(PROG)의 생성이전에 다시한번 그의 인가를 확인해야만 하는데, 그것은 다시한번 그 스스로를 인가해야만 한다. 이 경우 응답의 생성은 충전 동작의 시작에서 점검한 첫번째 인가의 경우의 것과 일치한다.

<35> 프로그래밍 신호(PROG)를 생성하기 위하여 사용될 수 있고 또 인가 계산 동안에 데이터 캐리어 장치에 의한 출력인 응답의 반복을 방지하기 위하여, 본 발명에 따른 방법에서는 모든 응답 계산과 변경된 데이터가 응답의 생성을 위하여 사용된다. 이 데이터는 응답 카운터(RZ)에 의하여 공급되는데, 그것은 모든 응답 계산 이전에 비휘발성 상태로 변경되고 그것의 카운터 상태는 응답 계산에 영향을 미친다. 응답 카운터(RZ)은 유리한 방법에 있어서는 비휘발성 메모리의 한 영역으로 인식된다.

<36> 본 발명에 따른 데이터 전송 시스템과 본 발명에 따른 방법에 의하여, 휴대용 데이터 캐리어 장치 예를들면 칩카드의 신뢰성있는 재충전을 얻을 수 있다.

(57) 청구의 범위

청구항 1

적어도 하나의 터미널 및 적어도 하나의 휴대용 데이터 캐리어 장치를 가지며, 상기 휴대용 데이터 캐리어 장치는 카운터로서의 역할을 하면서 청구가능 금액을 나타내는 적어도 하나의 제 1값 영역(WBA)을 갖는 비휘발성 반도체 메모리(NVM)를 가지는 데이터 전송시스템에 있어서,

상기 비휘발성 반도체 메모리(NVM)는 제 2값 영역(WBB)를 가지며,

상기 비휘발성 메모리(NVM)의 값 영역(WBA, WBB)은 선택 논리 회로(AL)를 통하여 비휘발성 플래그 메모리(FS)에 접속되고, 단지 두 개의 상태만을 가정할 수 있으며,

상기 플래그 메모리(FS)의 각각의 상태는 판독 및 카운팅을 위하여 비휘발성 상태로 인에이블될 수 있지만 충전이 금지된 두 개의 값 영역(WBA 또는 WBB)중 하나를 결정하며,

상기 각각의 다른 값 영역(WBB 또는 WBA)은 충전을 위하여 일시적으로 휘발성 상태로만 인에이블될 수 있으며, 그리고

특정 시간에는 단지 하나의 값 영역(WBA, WBB)만이 각각 인에이블될 수 있는 것을 특징으로 하는 데이터 전송 시스템.

청구항 2

제 1항에 있어서, 상기 선택 논리 회로(AL)는 충전 제어 신호(LAD)에 의하여 동작하며, 상기 충

전 제어 신호(LAD)는 비휘발성 상태로 인에이블될 수 없는 값 영역(WBB 또는 WBA)의 일시적인 활성화 및 비휘발성 상태로 인에이블될 수 있는 값 영역(WBA 또는 WBB)의 일시적인 불활성화에 영향을 미치는 것을 특징으로 하는 데이터 전송 시스템.

청구항 3

제 1항 또는 제 2항에 있어서, 상기 선택 논리회로(AL)와 상기 비휘발성 메모리(NVM) 사이에는 스위칭 장치(SV)가 제공되며, 상기 스위칭 장치(SV)는 상기 선택 논리회로(AL)의 출력신호 또는 신호들의 함수로서, 프로그래밍 논리회로(PL)와 확인 논리회로(VL)를 각각의 상기 활성 값 영역(WBA 또는 WBB)에 접속시키는 것을 특징으로 하는 데이터 전송 시스템.

청구항 4

제 2항에 있어서, 오직 상기 터미널의 긍정적인 인증후에만 충전 신호(LAD)의 생성을 허용하는 제 1인에이블링 장치(FGV1)가 상기 데이터 캐리어 장치에 구비되어 있는 것을 특징으로 하는 데이터 전송 시스템.

청구항 5

제 1, 2 또는 4항에 있어서, 상기 비휘발성 플래그 메모리(FS)는 프로그래밍 신호(PROG)에 의하여 종속될 수 있으며, 상기 프로그래밍 신호(PROG)는 일시적으로 인에이블 값 영역(WBB 또는 WBA)을 비휘발성 상태로 인에이블될 수 있는 값 영역(WBA 또는 WBB)으로 변경하는 것을 개시하는 것을 특징으로 하는 데이터 전송 시스템.

청구항 6

제 5항에 있어서, 오직 상기 터미널의 긍정적인 인가후에만 상기 프로그래밍 신호(PROG)의 생성을 허용하는 제 2인에이블링 장치(FGV2)가 상기 데이터 캐리어 장치에 구비되어 있는 것을 특징으로 하는 데이터 전송 시스템.

청구항 7

제 4항에 있어서, 상기 비휘발성 반도체 메모리(NVM)는 비휘발성 카운팅 장치로서의 역할을 하는 인에이블링 영역(FGB)을 가지며, 인에블링을 이루려는 시도가 비휘발성 상태로 등록될 수 있어 후속 인에블링 절차들과 구별될 수 있도록 하는 것을 특징으로 하는 데이터 전송 시스템.

청구항 8

제 1, 2 또는 4항에 따른 데이터 전송 시스템 터미널에 의하여 금액을 표시하는 휴대용 데이터 캐리어 장치를 재충전하는 방법에 있어서 ;

a) 터미널 수단에 의하여 상기 휴대용 데이터 캐리어 장치로부터 비휘발성 상태로 인에이블링된 값 영역(WBA 또는 WBB)의 예전 카운터 상태를 판독하는 단계;

b) 상기 터미널에 입력된 청구될 데이터 및 예전 카운터 상태로부터 새로운 카운터 상태를 상기 터미널에서 계산하는 단계;

c) 상기 새로운 카운터 상태를 상기 티미널에서 상기 휴대용 데이터 캐리어 장치로 전송하는 단계;

d) 충전 제어 신호(LAD)의 수단에 의하여 오직 휘발성 상태로만 활성화되었던 상기 비휘발성 메모리(NVM)의 상기 값 영역(WBA 또는 WBB)에 상기 새로운 카운터 상태를 기록하는 단계; 그리고

e) 플래그 메모리(FS)의 상태를 변경하여 새로운 카운터 상태를 가지는 값 영역(WBB 또는 WBA)이 비휘발성 상태로 인에이블되는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 9

제 8항에 있어서, 상기 단계(d) 이후에

d1) 상기 휴대용 데이터 캐리어 장치에서 상기 새로운 카운터 상태를 서명하고 상기 서명을 상기 터미널로 전송하는 단계; 그리고

d2) 상기 터미널에서 상기 새로운 카운터의 상기 서명을 결정하고 상기 두 서명들을 비교하는 단계를 더 수행하며,

상기 단계 e)는 두 서명들이 일치할때에만 수행되고, 만약 상기 두 서명들이 일치하지 아니하면 상기 방법은 비정상적으로 종료되는 것을 특징으로 하는 방법.

청구항 10

제 8항에 있어서, 상기 단계 a) 이후에

a1) 상기 터미널에 의하여 상기 휴대용 데이터 캐리어 장치에 고유한 데이터를 상기 휴대용 데이터 캐리어 장치로부터 판독하는 단계;

a2) 챌린지(challenge)를 생성하고, 상기 터미널에서 상기 챌린지 및 상기 고유 데이터의 적어도 몇몇과 상기 예전 카운터 상태로부터 응답을 결정하는 단계;

a3) 상기 챌린지와 상기 응답을 상기 터미널로부터 상기 휴대용 데이터 캐리어 장치로 전송하는 단계; 그리고

a4) 상기 휴대용 데이터 캐리어 장치에서 상기 챌린지로부터 응답을 결정하고 상기 두 응답들을 비교하는 단계를 더 수행하는 것을 특징으로 하는 방법.

청구항 11

제 9항에 있어서, 상기 단계 d) 또는 상기 단계 d2) 이후에

d3) 상기 휴대용 데이터 캐리어 장치에 고유한 데이터를 상기 터미널에 의하여 상기 휴대용 데이터 캐리어 장치로부터 판독하는 단계 ;

d4) 챌린지를 생성하고, 상기 터미널에서 상기 챌린지 및 상기 고유 데이터의 적어도 몇몇과 상기 예전 카운터 상태로부터 응답을 결정하는 단계 ;

d5) 상기 챌린지와 상기 응답을 상기 터미널로부터 상기 휴대용 데이터 캐리어 장치로 전송하는 단계 ; 그리고

d6) 상기 휴대용 캐리어 장치에서 상기 챌린지로부터 응답을 결정하고 상기 두 응답들을 비교하는 단계를 포함하고,

상기 단계 e)는 두 응답들이 일치할때에만 일어나고, 만약 그들이 일치하지 아니하면 상기 방법은 비정상적으로 종료되는 것을 특징으로 하는 방법.

청구항 12

제 9항에 있어서, 카운터 상태를 서명하거나 응답을 생성하기 위하여 각각의 충전과정에서 변동된 데이터가 사용되며, 상기 서명 또는 응답의 생성은 유사-랜덤 생성기(PZG)에 의하여 이루어지는 것을 특징으로 하는 방법.

청구항 13

제 12항에 있어서, 상기 데이터는 모든 충전 동작을 카운트하는 충전 카운터(LZ)의 값인 것을 특징으로 하는 방법.

청구항 14

제 12항에 있어서, 상기 데이터는 비휘발성 상태로 각각 인에이블될 수 있는 상기 값 영역(WBA 또는 WBB)의 예전 값 서명이 기록된 서명 메모리(SIGSP)의 값인 것을 특징으로 하는 방법.

청구항 15

제 12항에 있어서, 상기 데이터는 새로운 충전 동작마다 상기 충전 동작의 서명으로서 새로운 값이 상기 충전 터미널을 경유하여 기록된 서명 메모리(SIGSP)의 값인 것을 특징으로 하는 방법.

청구항 16

제 12항에 있어서, 모든 응답 계산전마다, 응답 카운터(RZ)는 비휘발성 상태로 변경되며 변경하는 데이터로서 사용되는 것을 특징으로 하는 방법.

요약

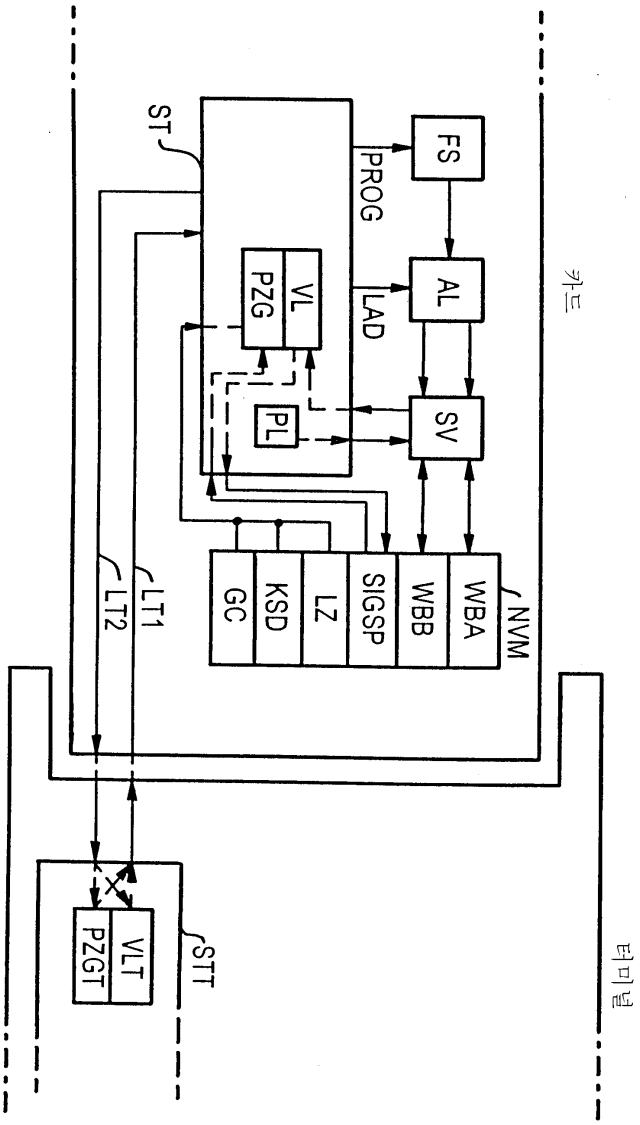
본 발명은 터미널과 휴대용 데이터 캐리어 장치를 갖고 있는 데이터 전송 시스템과 그 터미널에 의하여 그 휴대용 데이터 캐리어 장치를 리차징하는 방법에 관한 것이다. 적어도 하나의 터미널과 적어도 하나의 휴대용 데이터 캐리어 장치, 예컨대 칩카드에 의하여 이루어진 데이터 전송 시스템의 경우에, 금액을 나타내는 카드의 비휘발성 메모리(NVM)의 영역은 두 값 영역(WBA,WBB)으로 나뉘어지는데, 그들중의 오직 하나(WBA 또는 WBB)만이 각 경우에 비휘발성 상태로 활성화될 수 있고 다른 것(WBB 또는 WBA)은 단지 임시적으로만 활성화된다. 카드가 리차지되었을 때, 새로운 카운터 상태가 단지 임시적으로만 처음부터 활성화되어 있었던 값 영역(WBB)으로 쓰여지고, 정확한 쓰기였는지를 체크한 후에만 이 값 영역(WBB)은 비휘발성 상태로 활성화될 수 있도록 전환된다.

대표도

도1

도면

도면1


ST
FS
PROG
AL
LAD
VL
PZG
PL
SV
카드
LT1
LT2
GC
KSD
LZ
SIGSP
WBB
WBA
NVM
STT
VLT
PZGT
터미널