(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년10월23일
(11) 등록번호 10-1789113
(24) 등록일자 2017년10월17일

(51) 국제특허분류(Int. Cl.)
G06Q 20/04 (2012.01) *G06Q 20/20* (2012.01)
G07G 1/12 (2006.01) *H04B 5/02* (2006.01)
(21) 출원번호 10-2011-7029107
(22) 출원일자(국제) 2010년05월01일
심사청구일자 2015년04월30일
(85) 번역문제출일자 2011년12월05일
(65) 공개번호 10-2012-0030408
(43) 공개일자 2012년03월28일
(86) 국제출원번호 PCT/IB2010/051915
(87) 국제공개번호 WO 2010/128442
국제공개일자 2010년11월11일
(30) 우선권주장
PP 00032-2009 2009년05월03일 슬로바키아(SK)
(뒷면에 계속)
(56) 선행기술조사문헌
KR1020040049752 A*
WO2009036264 A1*
카탈로그, 'EMV Mobile Contactless Payment: Technical Issues and Position Paper', www.emvco.com, 2007.10.*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
에스에무케이 가부시키가이샤
일본국 도쿄토 시나가와쿠 도고시 6초메 5반 5고
(72) 발명자
플로렉, 미로슬라프
슬로바키아 821 01 브라티슬라바 세드모크라스코바 4
마사릭, 미할
슬로바키아 821 01 브라티슬라바 메드질라보레카 7
리펠매처, 데이비드 알랜
체코 120 00 프라하 2 호피노바 1472/ 14
(74) 대리인
특허법인(유)화우

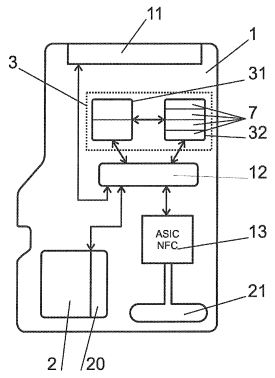
전체 청구항 수 : 총 33 항 심사관 : 이재근

(54) 발명의 명칭 **휴대폰과 같은 이동 통신 디바이스를 이용하는 지불 단말기 ; 자동 이체 지불 트랜잭션의 방법**

(57) 요 약

휴대폰과 같은 이동 통신 디바이스(4)를 이용한 지불 단말기가, 예를 들어 마이크로SD 카드 타입의 착탈식 메모리 카드(1)에 위치되며, 이는 추가 하드웨어 슬롯 예를 들어 메모리 슬롯으로 삽입될 수 있는 방식으로 조정된다. 지불 POS 단말기 어플리케이션은 적어도 하나의 지불 카드를 포함하는 착탈식 메모리 카드(1) 상에서 실행된다. 카드의 지불 어플리케이션을 갖는 지불 카드의 유닛(7)은 단말기의 구성 데이터 유닛(6)과 분리되어 메모리의 보안처리 부분에 위치된다. 단말기의 선택된 아이덴티티의 구성 데이터 및 지불 카드의 데이터는 보안 요소의 분리된 부분들에, 또는 완전히 독립적인 보안 요소들에 위치되거나, 또는 이들은 상인의 판매 디바이스에, 예를 들어 ICC 카드(29) 또는 SAM 카드(42) 내에서 로컬화될 수 있다.

대 표 도 - 도3



(30) 우선권주장
PP 50009-2010 2010년03월27일 슬로바키아(SK)
PP 50012-2010 2010년04월08일 슬로바키아(SK)
PP 50016-2010 2010년04월19일 슬로바키아(SK)

명 세 서

청구범위

청구항 1

이동 통신 디바이스를 이용한 지불 단말기에 있어서:

상기 지불 단말기는 메모리(2), 인터페이스(11), 및 마이크로제어기(12)를 포함하고, 상기 마이크로제어기(12)는 상기 메모리(2) 및 상기 인터페이스(11)와 연결되며, POS 단말기는 지불 POS 단말기 어플리케이션을 갖는 유닛(5) 및 지불 단말기의 구성 데이터를 갖는 유닛(6)을 포함하며,

상기 지불 단말기는 상기 지불 단말기의 대응하는 구성 데이터와 함께 착탈식 메모리 카드(removable memory card: 1)에 위치되고, 상기 착탈식 메모리 카드는 상기 이동 통신 디바이스(4)의 기본 기능들을 능가하는 기능성들을 추가하기 위해 사용되는 추가 하드웨어 슬롯으로 삽입될 수 있는 방식으로 조정되며, 상기 착탈식 메모리 카드(1)는 상기 POS 단말기의 구성 데이터 유닛(6)을 갖는 보안처리 메모리(3, 31) 및 지불 카드 유닛(7)을 갖는 보안처리 메모리(3, 32)를 포함하고, 상기 지불 카드 유닛(7)은 상기 POS 단말기의 구성 데이터와 분리되어 위치되며, 상기 보안처리 메모리들(3, 31, 32)은 상기 마이크로제어기(12)에 링크되고, 상기 마이크로제어기(12)는 상기 이동 통신 디바이스(4)의 회로들로의 연결을 위해 상기 인터페이스(11)에 링크되고,

상기 지불 단말기는 상기 착탈식 메모리 카드(1)상에서 상기 지불 POS 단말기 어플리케이션을 실행하여 상기 착탈식 메모리 카드(1)내에서 상기 POS 단말기를 구현하고,

상기 지불 POS 단말기 어플리케이션과 상기 지불 카드 유닛(7) 간의 통신은 상기 착탈식 메모리 카드(1)의 회로 내에서 실행되는 지불 단말기.

청구항 2

제 1 항에 있어서,

상기 지불 단말기의 구성 데이터의 저장을 위한 보안처리 메모리는 보안 요소(Secure Element: 31)에 의해 형성되고, 상기 보안 요소(31)는 상기 지불 카드 유닛(7)을 갖는 독립적인 보안 요소(32)와 분리된 하드웨어이거나, 또는

상기 지불 단말기의 구성 데이터 유닛(6) 및 상기 지불 카드 유닛(7)에 대한 보안처리 메모리들은 하나의 보안 요소(3)의 독립적인 도메인들로서 생성되는 지불 단말기.

청구항 3

제 1 항에 있어서,

상기 메모리 카드(1)는 SD 타입 또는 미니SD 또는 마이크로SD 카드 또는 M2로 구성되며, 상기 인터페이스(11)는 SD 타입 또는 M2 타입으로 구성되는 지불 단말기.

청구항 4

제 1 항에 있어서,

상기 메모리 카드(1)는 적어도 2-컨덕터(conductor) 또는 4-컨덕터 데이터 버스를 가지며, 상기 마이크로제어기(12)는 EEPROM 타입의 삭제할 수 없는 내부 메모리(10)를 포함하고, 상기 마이크로제어기(12)는 로딩된 지불 POS 단말기 어플리케이션에서의 승인되지 않은 간섭 제어(unauthorized interventions control)를 위한 부트-로더 유닛(boot-loader unit: 9)을 포함하는 지불 단말기.

청구항 5

제 1 항에 있어서,

상기 메모리 카드(1)에는, 보안 요소(31), 독립된 보안 요소(32) 및 상기 마이크로제어기(12)에 연결되거나 하

나의 보안 요소(3) 및 상기 마이크로제어기(12)에 연결되는 무접촉 통신 요소(13)가 장착되는 지불 단말기.

청구항 6

제 5 항에 있어서,

상기 메모리 카드(1) 상에, ISO14443 표준을 충족하는 NFC 타입의 무접촉 통신 요소(13)에 연결되는 안테나(21)가 존재하는 지불 단말기.

청구항 7

제 2 항에 있어서,

상기 보안 요소(31) 또는 상기 하나의 보안 요소(3)에, 상이한 독립적인 단말기들로부터의 구성 데이터를 갖는 적어도 2 개의 유닛(6)이 존재하는 지불 단말기.

청구항 8

제 2 항에 있어서,

상기 독립적인 보안 요소(32) 또는 상기 하나의 보안 요소(3)에, EMV 표준의 대응하는 지불 어플리케이션들을 갖는 독립적인 지불 카드들을 보유(hold)하는 적어도 2 개의 유닛(7)이 존재하는 지불 단말기.

청구항 9

제 1 항에 있어서,

상기 메모리(2)는 플래시 타입으로 구성되고, 상기 메모리(2)는 메모리 공간 중에 보안처리된 적어도 일부분을 가지며, 이 보안처리된 영역에 상기 지불 POS 단말기 어플리케이션(5)이 저장되는 지불 단말기.

청구항 10

제 1 항에 있어서,

상기 메모리(2)에, 메모리 제어기 유닛(17), 다운로드 관리 유닛(19), 및 웹 서버 유닛(18)이 존재하는 지불 단말기.

청구항 11

제 1 항에 있어서,

하나의 보안 요소(3)에, 비-금융 어플리케이션 유닛(16)이 존재하고, 상기 메모리(2)는 비보호 부분에 사용자에게 숨겨진 데이터에 대한 공간(20) 및 사용자의 자유 접근 데이터(free access data)에 대한 공간(15)을 갖는 지불 단말기.

청구항 12

제 1 항에 있어서,

가게에 위치되는 지불 POS 단말기 어플리케이션의 이니시에이터(initiator: 22)를 더 포함하고, 상기 이니시에이터는 지불 값을 생성하는 유닛을 포함하며, 상기 이니시에이터(22)에는 통신 요소(24)가 장착되고, 상기 통신 요소(24)는 상기 착탈식 메모리 카드(1)의 통신 요소(13) 또는 상기 이동 통신 디바이스(4)의 단거리 통신 요소와 호환가능한 지불 단말기.

청구항 13

이동 통신 디바이스(4)를 이용한 지불 단말기(27)에 있어서,

상기 지불 단말기(27)는 지불 POS 단말기 어플리케이션의 실행에 대한 유닛(5), 상인과 매칭하는 POS 단말기의 식별 데이터를 갖는 보안처리 메모리, 및 인터페이스(11)를 포함하고,

상기 지불 단말기(27)는 착탈식 메모리 카드(1)와 상인의 판매 디바이스(Sales Device: 28)의 임시 무접촉 연결(43)에 의해 형성되며, 상기 착탈식 메모리 카드(1)는 고객의 이동 통신 디바이스(4)의 슬롯으로 삽입되고, 상

기 판매 디바이스(28)는 지불 수령인에 의해 보유되고 상기 POS 단말기의 식별 데이터를 갖는 보안처리 유닛(6)을 포함하고, 상기 착탈식 메모리 카드(1)는 적어도 하나의 지불 카드 유닛(7)을 보유하고,

상기 지불 단말기(27)는 상기 착탈식 메모리 카드(1)상에서 상기 지불 POS 단말기 어플리케이션을 실행하여 상기 착탈식 메모리 카드(1)내에서 상기 POS 단말기를 구현하고,

상기 지불 POS 단말기 어플리케이션과 상기 지불 카드 유닛(7) 간의 통신은 상기 착탈식 메모리 카드(1)의 회로 내에서 실행되는 지불 단말기(27).

청구항 14

제 13 항에 있어서,

상기 착탈식 메모리 카드(1)는:

상기 지불 POS 단말기 어플리케이션의 실행을 위한 유닛(5),

적어도 하나의 지불 카드 유닛(7)을 갖는 보안처리 메모리(3, 32),

상기 판매 디바이스(28)와의 연결을 위한 안테나(21)를 갖는 통신 요소(13)를 포함하고,

상기 보안처리 메모리(3, 32)는 상기 지불 단말기(27)의 마이크로제어기(12)와 연결되며, 상기 마이크로제어기(12)는 상기 이동 통신 디바이스(4)의 회로들로의 연결을 위해 상기 지불 단말기(27)의 인터페이스(11)와 연결되고, 상기 판매 디바이스(28)는:

상기 POS 단말기의 식별 데이터를 갖는 상기 보안처리 유닛(6)을 형성하는 보안 요소,

암호화 키, 및

상기 착탈식 메모리 카드(1)와의 연결을 위한 안테나(41)를 갖는 통신 요소(35)를 포함하는 지불 단말기(27).

청구항 15

제 13 항에 있어서,

상기 POS 단말기의 식별 데이터를 갖는 상기 보안처리 유닛(6)은 상기 판매 디바이스(28) 내로 삽입되는 SAM 카드(42)에 위치되거나, 또는 상기 POS 단말기의 식별 데이터를 갖는 보안 유닛(6)은 상기 판매 디바이스(28)의 판독기 내로 삽입되는 ICC 카드(29)에 위치되는 지불 단말기(27).

청구항 16

제 13 항에 있어서,

상기 판매 디바이스(28)는 지불되는 총액의 삽입을 위한 키보드(36), 및 디스플레이(37)를 갖는 지불 단말기(27).

청구항 17

제 13 항에 있어서,

상기 착탈식 메모리 카드(1)는 2 개의 보안 요소들(31, 32)을 갖고, 상기 2 개의 보안 요소들(31, 32) 중 지불 카드 보안 요소(32)는 독립적인 지불 카드 유닛들(7)을 위한 수 개의 분리된 도메인들을 포함하며, 상기 착탈식 메모리 카드(1)는 사용자의 비보호 데이터를 위한 메모리(2)를 갖는 지불 단말기(27).

청구항 18

제 13 항에 있어서,

상기 판매 디바이스(28)는 외부 디바이스들의 연결을 위한 커넥터(39)를 갖는 지불 단말기(27).

청구항 19

제 13 항에 있어서,

상기 판매 디바이스(28)는 금전 등록기(26)와의 연결(38)을 갖는 지불 단말기(27).

청구항 20

제 1 항 또는 제 13 항에 있어서,

상기 착탈식 메모리 카드(1)는 접근 모드들을 가지고, 상기 접근 모드들은:

상기 착탈식 메모리 카드(1)의 무접촉 통신 요소(13)에 대한 보안 요소(3)로의 접근을 차단하는 상기 이동 통신 디바이스(4)의 메모리 용량 확장 기능을 위한 접근 모드(access mode), 및

상기 착탈식 메모리 카드(1)의 무접촉 통신 요소(13)가 활성화되고, 적어도 하나의 지불 카드 유닛(7)을 갖는 보안 요소(3)로의 접근이 허용되는 상기 착탈식 메모리 카드(1)의 지불 기능을 위한 접근 모드이며,

상기 착탈식 메모리 카드(1)의 지불 기능을 위한 접근 모드는 하드웨어 지불 버튼(44)의 물리적인 가압 후에만 활성화되고, 상기 지불 POS 단말기 어플리케이션을 갖는 유닛(5)은 오로지 상기 착탈식 메모리 카드(1)의 지불 기능을 위한 접근 모드에서만 접근가능한 지불 단말기(27).

청구항 21

제 20 항에 있어서,

상기 이동 통신 디바이스(4)의 소프트웨어는 다른 입력에 의한 상기 지불 버튼(44)으로부터의 신호의 에뮬레이션(emulation)의 가능성을 차단하는 지불 단말기(27).

청구항 22

이동 통신 디바이스를 이용하고, EMV 타입의 지불 POS 단말기 어플리케이션을 실행하는 자동 이체 지불 트랜잭션(direct debit payment transaction)의 방법에 있어서:

상기 지불 POS 단말기 어플리케이션은 추가 하드웨어를 위한 상기 이동 통신 디바이스(4)의 슬롯 내로 삽입되는 착탈식 메모리 카드(1) 상에서 실행되어 상기 착탈식 메모리 카드(1) 내에서 POS 단말기를 구현하고, 상기 지불 POS 단말기 어플리케이션과 지불 카드와의 통신은 상기 착탈식 메모리 카드(1)의 회로 내에서 실행되는 자동 이체 지불 트랜잭션 방법.

청구항 23

제 22 항에 있어서,

상기 지불 POS 단말기 어플리케이션은 상기 메모리 카드(1)에 위치된 마이크로제어기(12) 내로 로딩되고, 후속하여 선택된 단말기의 아이덴티티(identity)의 구성 데이터가 상기 선택된 단말기의 아이덴티티의 구성 데이터를 저장하고 있는 보안 요소(3, 31)로부터 로딩되는 자동 이체 지불 트랜잭션 방법.

청구항 24

제 22 항에 있어서,

선택된 지불 카드에 관한 데이터가 상기 선택된 지불 카드에 관한 데이터를 저장하고 있는 보안 요소(3, 32)로부터, 지불 단말기로서 작동하는, 상기 메모리 카드(1)에 위치된 마이크로제어기(12) 내로 로딩되는 자동 이체 지불 트랜잭션 방법.

청구항 25

제 22 항에 있어서,

상기 POS 단말기의 개시(initiation) 동안이나 그 이전에(during or before), 부트-로더 유닛(9)이 상기 지불 POS 단말기 어플리케이션의 변경 제어(change control)를 실행하는 자동 이체 지불 트랜잭션 방법.

청구항 26

제 22 항에 있어서,

상기 지불 POS 단말기 어플리케이션은 상기 이동 통신 디바이스(4)의 입력 디바이스를 통해 관리되는 자동 이체

지불 트랜잭션 방법.

청구항 27

제 22 항에 있어서,

요청된 지불 총액에 관한 데이터가 별도의 이니시에이터(22)로부터 상기 지불 POS 단말기 어플리케이션으로 삽입되고, 상기 별도의 이니시에이터(22)는 무접촉 통신 채널을 통해 개시 명령과 함께 요청된 지불에 관한 데이터를 송신하는 자동 이체 지불 트랜잭션 방법.

청구항 28

이동 통신 디바이스를 이용한 자동 이체 지불 트랜잭션의 방법에 있어서,

착탈식 메모리 카드(1)와 상인의 판매 디바이스(28)의 임시 연결에 의한 지불 프로세스 전이나 그 동안에(before or during) 지불 단말기(27)가 생성되고, 상기 착탈식 메모리 카드(1)는 고객에 의해 보유되는 한편, 상기 판매 디바이스(28)는 지불 수령인에 의해 보유되고,

상기 착탈식 메모리 카드(1)상에서 지불 POS 단말기 어플리케이션이 실행되어 상기 착탈식 메모리 카드(1)내에서 POS 단말기를 구현하고,

상기 지불 POS 단말기 어플리케이션과 상기 착탈식 메모리 카드(1)에 보유된 지불 카드 유닛(7) 간의 통신은 상기 착탈식 메모리 카드(1)의 회로 내에서 실행되는 자동 이체 지불 트랜잭션 방법.

청구항 29

제 28 항에 있어서,

POS 단말기의 식별 데이터가 상기 판매 디바이스(28)로부터, 암호화된 전달을 통해 상기 착탈식 메모리 카드(1) 상으로 로딩되고, 후속하여 상기 착탈식 메모리 카드(1) 상의 제네릭(generic) POS 단말기가 대응하는 상인의 POS 단말기가 되며, 상기 지불 POS 단말기 어플리케이션이 상기 착탈식 메모리 카드(1) 상에서 실행되고, 고객의 선택에 따른 지불 카드의 유닛(7)으로부터의 데이터가 사용되는 자동 이체 지불 트랜잭션 방법.

청구항 30

제 28 항에 있어서,

지불 암호가 생성된 후, 상기 지불 암호는 상기 판매 디바이스(28)로 송신되고, 실현된 지불 기록의 메모리에 저장되는 자동 이체 지불 트랜잭션 방법.

청구항 31

제 28 항에 있어서,

지불 암호가 생성된 후, 상기 지불 암호는 상기 메모리 카드(1)의 인터페이스(11)를 통해 송신되며, 후속하여 상기 이동 통신 디바이스(4)를 통해 지불 프로세서 센터(25)로 송신되거나, 실현된 지불 기록들을 갖는 캐리어가 상기 판매 디바이스(28)로부터 빼내진 후 처리를 위해 은행 또는 지불 프로세서 센터(25)에 제공되는 자동 이체 지불 트랜잭션 방법.

청구항 32

제 28 항에 있어서,

지불 값에 관한 데이터는 키보드(36)를 통한 수동 삽입에 의해, 또는 금전 등록기(26)와의 연결(38)을 통해 상기 판매 디바이스(28)로부터 착탈식 메모리 카드(1)로 삽입되는 자동 이체 지불 트랜잭션 방법.

청구항 33

제 22 항 또는 제 28 항에 있어서,

상기 착탈식 메모리 카드(1)는 지불 프로세스가 실행되기 전에 메모리 용량 확장 기능을 위한 접근 모드에 있고, 지불 카드 유닛(7)은 상기 메모리 카드(1)의 인터페이스(11) 편으로부터 접근 불가능하며, 오로지 지불

하드웨어 버튼(44)의 물리적인 가압 후에만 상기 착탈식 메모리 카드(1)가 상기 지불 카드 유닛(7)으로의 접근이 허용되는 상기 착탈식 메모리 카드(1)의 지불 기능을 위한 접근 모드로 스위칭되고, 상기 착탈식 메모리 카드(1)가 상기 지불 기능을 위한 접근 모드로 스위칭된 후에 지불 단말기 유닛(5)을 갖는 보안 요소(3)가 접근가능하며, 상기 지불 프로세스가 종료 또는 중단된 후 상기 착탈식 메모리 카드(1)는 상기 이동 통신 디바이스(4)의 메모리 용량을 확장하는 기능을 위한 접근 모드로 스위칭되는 자동 이체 지불 트랜잭션 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 휴대폰과 같은 이동 통신 디바이스에 위치되는 지불 단말기와 관련된다. 지불 프로세스들을 실현하기 위해, 단말기는 주로 NFC 형태인 그 자체의 통신 요소를 통해서도 통신할 수 있다. 또한, 제시된 본 발명은 무접촉 전송 링크를 이용하는 자동 이체 지불(direct debit payment)의 방법을 설명하고, 특히 소규모 영업소를 위한 간소화된 구조를 갖는 임시 지불 단말기가 이동 통신 디바이스를 이용하여 생성될 수 있는 구성을 설명한다. 본 발명은, 예를 들어 마이크로SD 카드 형태의 착탈식(removable) 메모리 카드를 갖는 이동 통신 디바이스를 통한 지불에 있어서 보안 및 편안함을 증가시킨다.

배 경 기 술

[0002] 판매 영업소(commercial premises)에 영속적으로 위치되는 지불 단말기, POS(Point of Sale) 단말기가 알려져 있다. POS 단말기는, 구매자의 계좌로부터 가게 운영자의 계좌로의 돈의 전달이 합의된 시스템 내에서 안전하게 진행되는 방식으로 작용한다. 지금까지 POS 단말기를 통한 지불은, 지불의 수납자가 POS 단말기를 갖고 지불하는 고객이 지불 디바이스와 같은 대응하는 카드를 사용하는 지불로서 특징지어졌다. 제 1 단계에서, 카드 소지자의 체크, 검증(verification)이 실행된다 - 이 프로세스는 매우 안전하게 진행되어야 하며, 상인 및 지불하는 고객 모두의 편에서 불합리한 노력 없이도(without unreasonable effort) 실현되어야 한다. 후속하여, 가게 운영자의 계좌로 지불액이 자동 입금되는 프로세스가 실행된다. 원래는, 자기 띠(magnetic stripe)만이 장착된 카드들이 지불 단말기 어플리케이션의 실행에 사용되었다. 하지만, 기술적 제약들과 관련하여 로딩된 데이터를 갖는 자기 띠는 보안 위험을 보이는데, 이는 자기 띠가 단순한 기술적 디바이스들의 사용으로 복사되거나 변화될 수 있기 때문이다. 자기 띠로부터의 내부 데이터 판독은 저급 기술(low-tech)이다.

[0003] 그러므로, 90년대 후반에 카드 발행사들 Europay International, MasterCard 및 VISA 사이에 지불 카드에 위치된 마이크로칩을 이용한 EMV 표준의 생성에 관한 협정이 이루어졌다. EMV(Europay, MasterCard, VISA) 표준은 세계적인 상호운용성(worldwide interoperability)을 보장하기 위해 지불 카드 칩과 POS 단말기 간의 상호작용을 설명한다. 마이크로칩의 이용은, PIN 없이는 외부로부터 데이터에 접근할 수 없는 방식으로 상기 칩에 위치된 데이터를 보호할 수 있다. 또한, 카드 상의 칩의 이용은 카드소지자 검증(Cardholder Verification)이 프로세서 본부(processor headquarters)로의 온라인 연결 없이도 실현될 수 있게 한다. 자기 띠는 수동적인 데이터 캐리어(passive data carrier)를 나타내었지만, 카드의 칩은 기본적으로 그 자체의 연산 능력(computing capacity), 메모리의 보안처리 부분(secured part)들, 및 데이터 암호화 유닛을 갖는 소형 컴퓨터이다. 통상적인 POS 단말기들의 언급된 기술적 특성에도 불구하고, POS 단말기의 내부에서의 부정한 조정 및 조작의 경우나 리딩 디바이스(reading device)로의 중간 링크(intermediary link)를 삽입하는 경우에는 카드로부터의 데이터 및 PIN 코드가 드러날 수 있다는 것이 발견되었다. 일반적으로, 이는 담당자(attending personnel)에 의한 불충분한 제어의 경우 또는 다른 부정한 방식의 경우에 POS 단말기를 갖는 가게의 소유자에게 알려지지 않고 일어난다.

[0004] 하지만, 지금까지도 전체 상거래 관계의 개별적인 관계자(지불 카드 발행사, 처리 본부, 은행, 상인)에 의해 요청된 보안을 갖고, 지불하는 고객에 의해 소유될 수 있는 그러한 지불 단말기로 휴대폰을 전환할 수 있는 이러한 기술적 툴들이 알려져 있지 않다.

[0005] CN101351819 특허의 해결책은 POS 단말기로서 휴대폰을 이용할 가능성을 나타낸다; 하지만, 이는 시스템의 개별적인 필수 요소들의 특정한 조직(specific organization)을 다루지는 않는다. 특허들 CN101339685, CN101329801, US2008270246(A1), SI22595(A), US2008059375에서의 많은 해결책들은, 휴대폰에 직접 독립적인 POS 단말기 요소들이 존재하지 않음에도 불구하고 자동 이체 지불들에 대한 휴대폰의 관여를 설명한다. 또는, US20077241180(A1)에서와 같이 휴대폰 및 정적 POS 단말기가 상호작용하는 해결책들이 존재한다.

[0006] EMV 지불 어플리케이션의 보안 수준이 높고, EMV 표준의 형태로 제대로 최종 지불 암호들을 생성할, 기술적 해

결을 위한 요구가 존재하며, 이 모두는 인터넷 지불 또는 통상적인 상점들 외부에서 실현되는 다른 지불의 경우, 예를 들어 이동통신 사업자에 저장되는 프로그램들의 다운로드에 대해 지불하는 경우에도 해당된다. 이 종류의 해결책들은 현재는 알려져 있지 않거나, 아니면 이들은 예를 들어 NFC 또는 GPRS 통신의 경우 또는 인터넷을 통한 지불하는 고객의 지불 카드로부터 상인의 POS 단말기 또는 가상 POS 단말기로의 데이터 전달 시 통신의 공개 또는 악용에 이를 수 있다는 사실에 내재된 보안 위험들을 갖는다. 통상적인 상점에서의 POS 단말기와 지불 카드 간의 본래의 긴밀한 접촉이 인터넷 환경을 통한 통신으로 연장되는 경우에, 보안 위험들이 증가된다.

[0007] 기존 POS 단말기들은 안정된 구조에 의해 구별되며, 이는 무엇보다도 지불 처리 센터에 연결된 통신 채널, 프린터, 암호화 키, 카드 리더기, 주로 상이한 포맷 카드들의 리더기, 및 PIN(핀) 코드 입력을 위한 키보드를 포함한다. 이 종류의 기술적 구성은 소정 공간을 필요로 하며, 비교적 고가이다. 알려진 POS 단말기의 구현들은 스톤샵(stone shop)들의 안정된 판매 지점(stable sale location)들을 위한 것이며, 이때 POS 단말기의 고비용 구입, 설치 및 작동이 구입을 위한 지불의 합리적인 회전율(turnover)에 의해 균형을 이루게 된다.

[0008] 공개 특허 WO2008063990에 따른 해결책은, POS 단말기가 지불 처리 센터와의 통신 채널을 갖지 않고 이를 위해 고객의 휴대폰을 통한 중간매체 연결(mediated connection)을 사용하는 시스템을 설명한다. 이 해결책은, 지불 단말기 어플리케이션 자체가 원격 컴퓨터에서 실행되고 휴대폰은 단지 통신의 중간매체(mediator)이기 때문에 보안 수준이 더 낮다. 다른 공개 특허들은, 지불 장소에는 직접 그 관리 부분(managing part)만이 존재하고, 이것이 가게의 몇몇 다른 부분에 위치된 나머지 부분에 연결되는 방식으로 분리된 POS 단말기를 설명한다. 기존 해결책들 및 공개 특허들은 싸고, 복잡하지 않은, 그리고 결국 휴대할 수도 있는 POS 지불 단말기 -이는 현재 표준, 특히 EMV 표준에 따른 지불 암호를 생성할 수 있음- 를 생성하는 방식에 대한 간단한 설명도 제공하지는 않는다.

[0009] 현재 존재하는 모든 해결책들은 비교적 복잡한 설치를 필요로 하고, 비용을 증가시키는 많은 입력 및 출력 디바이스들을 포함한다. 지금까지, 간소함 및 수준 높은 보안을 특징으로 하고, 신문 키오스크(newspaper kiosk) 또는 패스트푸드를 파는 모바일 카운터(mobile counter)와 같은 소규모 가게들에서도 이용할 수 있고 휴대할 수 있는 이러한 디바이스들은 알려져 있지 않다.

[0010] 머지않아 비현금(cashless) 지불 어플리케이션에 대한 휴대폰과 같은 이동 통신 디바이스들의 이용이 증가하면, 지불 프로세스들의 편안함 및 보안의 증가에 대한 요구가 높아질 것이다. 이동 통신 디바이스들은 이동 데이터 네트워크와의 의도적이지만 관찰되지 않는 연결의 가능성을 갖고, 이로 인해 유해 프로그램들이 이동 통신 디바이스들의 환경으로 침투할 위험이 있다.

[0011] WO 2010/011670 A2로서 공개된 특허 파일에 따르면, 목적 지불-버튼(purpose Pay-button)이 알려져 있다. 이것에 의해, 무접촉 지불 어플리케이션의 실행에 필요한 NFC 통신 요소가 시작된다. 이 버튼은 지불 어플리케이션의 실행(launch)을 간소화하지만, 이동 통신 디바이스들의 디스플레이에 보여지는 메뉴의 가상 버튼에 의해 지불 어플리케이션이 시작되는 경우, NFC 통신 요소로의 그 연결이 이전 해결책들에 비해 증가된 보안을 제공하지는 않는다. 이동 통신 디바이스 내에 저장된 지불 카드에 대한 가능한 공격들의 분석은, 예를 들어 트로이 목마(troyan horse) 형태의 적절하지 않은 프로그램이 사용자 모르게 지불 어플리케이션을 초기화하는 경우의 위험을 지적하였다. 이동 통신 디바이스의 지불 카드가 지불 카드 리더기로 언제나 삽입되어 있기 때문에, 이 위치 자체가 카드로부터 데이터를 읽어들이려는 끊임없는 시도의 가능성도 포함한다. 이러한 이유로, 지금까지 지불 카드가 리더기 예를 들어 POS 단말기 또는 ATM에 장기간이면서 실제적으로 중단없이(without interruption) 삽입되어 있기 때문에 일어나지 않을 것으로 간주되었던 지불 카드의 보안 레벨의 실패, 예를 들어 심지어 EMV 표준의 실패에 도달할 위험이 존재한다. 이 이유로 이러한 해결책이 요구되며, 이는 편안함뿐만 아니라 지불 카드의 보안도 증가시킬 것이다. 예를 들어, 휴대폰의 포토 버튼(photo button)과 같은 기존 목적 버튼들은 상기 폰의 선택된 기능으로의 접근을 가속하고 간소화하는 목적만을 가졌으며, 이는 선택된 기능의 의식적 실행(conscious launch)의 보안 문제(security question)를 해결할 필요가 없었다.

[0012] 신규하고 더 안전한 해결책은 수행자의 편안함을 떨어뜨리지 않도록 충분히 편안하여야 하며, 이는 휴대폰을 통한 비현금 지불들의 연장(extension)에 있어서 중요한 가정이다.

발명의 내용

해결하려는 과제

[0013] 언급된 결점들이 휴대폰과 같은 이동 통신 디바이스를 이용한 지불 단말기에 의해 상당히 제거되어야 하며, 이

때 지불 단말기는 메모리, 인터페이스, 및 마이크로제어기를 포함한다. 마이크로제어기는 메모리에 링크되며, 인터페이스를 통해 이동 통신 디바이스들의 회로에도 링크된다. 지불 단말기는 지불 POS 단말기 어플리케이션을 갖는 하나의 유닛, 및 지불 단말기들의 구성 데이터 유닛을 가지며, 이는 메모리의 보안처리 부분에 저장된다. 본 발명의 본질은 관련 구성 데이터와 함께 지불 단말기가 착탈식 메모리 카드에 저장될 수 있고, 이것이 이동 통신 디바이스의 기본 기능들을 능가하고 있는(surpass) 기능성들을 추가하는데 사용되는 추가 하드웨어를 위해 이동 통신 디바이스들의 슬롯 안으로 삽입될 수 있는 방식으로 조정된다는 사실에 있다.

과제의 해결 수단

[0014] 해결책의 본질은 POS 단말기의 전체 프로세스 커널(kernel)이 이동 통신 디바이스 내로 삽입되는 착탈식 메모리 카드에 위치될 수 있는 한편, 대부분의 이용은 휴대폰의 통상적인 메모리 슬롯으로의 그 카드의 삽입에서 일어나는 구성이다. 모든 내부 지불 POS 단말기 어플리케이션의 실행은 이동 통신 디바이스 내로 삽입된 착탈실 메모리 카드에서 실현될 수 있다. 지불 프로세서 본부와의 통신 프로세스들에서는 예외일 수 있으며, 이때에는 이동 통신 디바이스 자체의 통신 채널들[SMS(short message service), GPRS(general packet radio service)]이 사용될 수 있다. 이동 통신 디바이스들의 디스플레이 툴들은 지불 어플리케이션의 실행을 보여주기 위해 사용될 수 있다.

[0015] 휴대폰 내의 보충 메모리 카드(supplementary memory card) 속으로만 POS 단말기의 처리 커널을 전달하는 것은 놀라운 기술적 이점들을 가져오지만, 이는 지불 카드로부터의 데이터의 로딩과 함께 복잡함을 야기할 수도 있는데, 이는 휴대폰들이 칩 카드 리더기들을 갖지 않기 때문이다. 이때, 제시된 해결책의 중요한 특성은 동일한 하드웨어 장비, 즉 착탈식 메모리 카드에 사용자의 지불 카드 또는 심지어 수 개의 지불 카드들이 배치될 수 있다는 사실에 있다. 기술적으로, 이는 착탈식 메모리 카드가 지불 단말기에 대한 데이터를 갖는 메모리의 보안처리 부분 이외에 지불 카드 데이터를 갖는 메모리의 별도의 보안처리 부분도 포함할 수 있는 방식으로 보장될 수 있다.

[0016] 지불 어플리케이션의 실행 시, 착탈식 메모리 카드는 이동 통신 디바이스의 기본 기능들을 능가하고 있는 기능성들을 추가하는데 사용되는 추가 하드웨어를 위한 이동 통신 디바이스의 슬롯으로 삽입된다. 슬롯은 주로(하지만, 전적인 것은 아님) 휴대폰과 같은 이동 통신 디바이스의 외부로부터 접근가능한 통상적으로 사용되는 슬롯(commonly used slot)일 것이다. 관련 슬롯은 이러한 기술적 장비를 위해 설계되며, 이 없이도 이동 통신 디바이스는 그것의 필수 기능을 충족시킬 수 있다. 그러므로, 해당 슬롯은 사업자의 네트워크에서 직접 음성 및/또는 데이터의 전송에 영향을 주지 않는다; 실제로, SIM(subscriber identity module) 카드에 대한 인터페이스와 상이하다. 본 발명의 중요한 요소인 메모리 카드는 SIM 카드의 기능성을 갖지 않는다. 본 발명의 해결책에서 설명된 착탈식 메모리 카드는 휴대폰의 SIM에 영향받지 않으며(not dependant), 상기 폰의 정규 기능들 중 어느 것도 중단시키지 않고 휴대폰으로 삽입되거나 제거될 수 있다.

[0017] 지불 카드와 POS 단말기 간의 통신이 어플리케이션의 실행 동안에 휴대폰에 삽입되는 하나의 하드웨어 디바이스 내에서의 데이터 전송으로 좁혀지는 경우에는, 통상적인 수단에 의해 이 통신을 모니터링하고 악용하는 것이 불가능하다. 지불이 실현된 후, 실현된 지불에 관한 암호화된 정보가 착탈식 메모리 카드로부터 송신된다. 이 정보는 EMV 표준의 형태로 충분한 보안에 의해 구별된다. 통상적인 구성에서, 이동 통신 디바이스는 휴대폰일 수 있으며, 이는 착탈식 메모리 카드 상에서의 지불 어플리케이션의 실행을 위해 지불 처리 본부와의 통신으로서 외부 기능들(outside functions)을 보장할 것이다. 또한, 휴대폰은 착탈식 메모리 카드의 전력공급(powering)을 보장할 것이다.

[0018] 착탈식 메모리 카드는 주로 EMV 형태의 지불 어플리케이션을 갖는 지불 카드 유닛도 포함할 수 있다. 이 종류의 지불 카드 유닛은 EMV 표준에 따라 칩이 갖는 것과 유사한 기능들의 보증을 위한 하드웨어 및 소프트웨어 툴들을 포함할 것이다. 이 유닛의 인터페이스들은 이것이 통상적인 형태의 리더기들에서 읽어들이도록 설계되는 것이 아니라, 착탈식 메모리 카드 캐리어(removable memory card carrier)와 단단히 분리할 수 없게(firmly, undetachably) 연결될 것이기 때문에 상이할 수 있다.

[0019] POS 지불 단말기 및 지불 카드를 하나의 심지어는 불가분의(indivisible) 하드웨어 장비 내에 배치하는 것은 지금까지 이해할 수 없었는데, 이는 단말기들이 물리적으로는 상인들 편에 배치되는 한편, 이들이 일반적으로 은행, 지불 프로세서 등에 의해 소유되었기 때문이다. 제시된 해결책을 통해, 사용자가 지불 단말기를 임차(leasehold)하는 것이 달성될 수 있고, 이러한 경우 하나의 하드웨어 장비 내로 지불 단말기 및 지불 카드를 배치하는 것이 가능하다. 구성 아이덴티티(configuration identity)의 관점으로부터, 단말기는 지금까지 상인 편에 배치되었던 단말기를 이용했던 바와 같이 특정한 은행 또는 처리 기관의 소유물로 보유될 것이다. 지불 카

드와 POS 단말기 간의 통신이 제어기, 착탈식 메모리 카드의 하드웨어 내의 마이크로제어기를 통해 실행되고, 지불 디바이스의 아주 작은 크기를 고려할 때, 본질적으로는 외부로부터 불법적으로 이 통신을 읽어들이는 것이 기술적으로 실행가능하지 않을 것이다(unfeasible).

[0020] 암호화 키 및 식별 데이터와 같은 POS 지불 단말기의 정교한 데이터(delicate data)가 메모리의 보안처리 부분, 바람직하게는 소위 보안 요소(Secure Element)에 저장되어야 한다. 보안 요소는 특정한 하드웨어 특성들에 의해 특징지어지고, 대응하는 증명(certification)을 받게 되며, 그 덕분에 가담하는 구성원들(participating members)이 이러한 메모리 디바이스 내의 그 정교한 데이터를 기꺼이 신뢰하려고 한다. 이 POS 지불 단말기의 데이터는 지불 카드 데이터로의 접근으로부터 철저히 분리되고, 그 반대의 경우도 마찬가지이다. 이러한 이유로, 적어도 2 이상의 독립적인 별도의 보안 메모리 도메인들이 착탈식 메모리 카드에 있을 수 있다. 이들은, 예를 들어 하나의 보안 요소의 분리된 파티션(partition)들의 형태일 수 있다.

[0021] 지불 단말기 어플리케이션 내의 프로세스들을 최적화하는 관점으로부터, 이는 착탈식 메모리 카드가 2 개의 독립적인 하드웨어 보안 요소를 갖는 것이 유리하지만 필수적인 것은 아니다. 이들은 2 개의 동일 형태의 칩(uniform chip)들의 형태일 수 있으며, 이는 착탈식 메모리 카드의 인쇄 회로에 독립적으로 배치될 수 있다. 이때 제 1 보안 요소는 POS 단말기 데이터의 저장 또는 상이한 POS 단말기들의 데이터 각각의 저장을 위한 것일 수 있다. 제 2 보안 요소는 지불 카드의 데이터 또는 다양한 지불 카드들의 데이터의 저장을 위해 의도될 것이다. 그러므로, 제시된 해결책은 하나의 하드웨어 디바이스에 여러 사업자들의 POS 단말기들, 및 한 사용자의 여러 지불 카드들(즉, 한 사람의 명의로 발행된 다양한 은행들의 지불 카드들)을 배치할 수 있게 한다. 접근(access)의 관점으로부터, 상이한 회사들에 속한 이들 구성 및 지불 데이터는 분리되어 위치되어야 하기 때문에, 보안 요소들이 수 개의 독립적인 도메인, 파티션들로 나누어질 것이다. 2 개의 보안 요소들이 사용되는 경우, 그들의 상호 통신 및 두 어플리케이션들의 실행은 보안 요소가 멀티태스킹(multitasking)을 갖지 않을 경우에도 가능해질 것이다. 2 개, 또는 수 개의 보안 요소들의 이용은 지불 POS 단말기 어플리케이션이 보안 요소들 상에서 직접 실행될 수 있는 방식으로 이용가능한 총 메모리 용량을 증가시킨다. 하나의 보안 요소를 갖는 구성에서는, 또 다른, 주로 싸고 보안처리되지 않은 메모리를 사용하는 것이 더 적절할 것이며, 그 메모리에 지불 POS 단말기 어플리케이션이 로딩되고 지불 프로세스 동안 그 어플리케이션이 실행될 것이다.

[0022] 통상적인 메모리 자체를 포함하는 것 외에, 메모리 카드는 단말기의 구성 데이터를 갖는 유닛이 저장되는 보안 메모리를 갖는 칩의 형태로 보안 요소를 보유(hold)할 수 있다. 이 유닛은 단말기가 그 자신의 아이덴티티를 할당하기 위해 필요로 하는 데이터의 안전한 저장을 위해 사용된다. 원칙적으로, 이들은 대부분 관련 데이터를 갖는 단말기가 어디에 속하는지를 결정하는 데이터이다.

[0023] 보안 요소는 마이크로제어기와 연결된다. 마이크로제어기라는 용어는 제어기 또는 제어기 형태의 몇몇 좁은 의미의 하드웨어(narrowed hardware)도 의미할 수 있다. 또한, 마이크로제어기는 그 기능들이 나누어지는 방식으로 위치될 수 있으며, 예를 들어 제어기 부분이 또 다른 칩에서의 연산 부분(computing part)으로부터 나누어진다. 지불 POS 단말기 어플리케이션을 실행할 수 있기 위해, 마이크로제어기는 메모리 카드의 메모리에도 연결될 수 있으며, 그 메모리에 지불 POS 단말기 어플리케이션을 갖는 유닛이 저장된다. 이 어플리케이션은 특히 EMV 어플리케이션의 형태일 수 있다. 마이크로제어기는 각각의 유닛으로부터 지불 POS 단말기 어플리케이션을 읽어들이며, 이로 인해 각 유닛이 소위 제네릭 POS 단말기(Generic POS Terminal)가 된다. 이는 일반적인 POS 지불 단말기이지만, 이 순간에는 여전히 평범한 상태이다(indifferent). POS 지불 단말기가 몇몇 특정한 은행, 특정한 기관과 연계되기 위해서는, 스마트 카드 칩 내의 선택된 유닛으로부터 단말기 구성 데이터를 다운로드해야 한다.

[0024] 이 구성은 지불 POS 단말기 작동들을 실현할 수 있도록 구성되고 적합하게 된 메모리 카드를, 메모리 연장을 위한 슬롯을 갖는 통상적인 휴대폰으로 삽입하게 할 수 있다.

[0025] 지불 카드 유닛은 단말기 구성 데이터를 갖는 유닛으로부터 분리되어, 바람직하게는 특수화된 칩 내의 보안 요소의 독립적인 도메인 상에서 메모리의 보안처리 부분에 위치될 것이다. 메모리 카드의 적절한 구조와 관련해서, 그리고 SD 슬롯을 갖는 이동 통신 디바이스들의 높은 침투(high penetration)와 관련하여, 상기 카드는 SD 타입, 또는 미니SD, 또는 마이크로SD 카드, 또는 심지어 M2(Memory Stick Micro)로 구성되는 것이 적절하다. 이때, 이동 통신 디바이스의 회로를 향하는 메모리 카드의 인터페이스는 SD 또는 M2 타입의 인터페이스로 구성될 것이다. 마이크로제어기는 SD 카드 연합(Technical Committee SD Card Association)에 의해 정의된 사양에 의해 언급된 바와 같이 카드의 인터페이스에 연결될 수 있다.

[0026] 충분한 데이터 투과성(data permeability)에 도달하기 위해, 지불 카드가 적어도 2-컨덕터(conductor) 또는 더

우수하게는 4-컨덕터 데이터 버스를 갖는 경우가 적절할 수 있다. 상기 카드는 24 ㎜보다 작은 최대 파라미터(largest parameter), 및 14 ㎜보다 작은 두번째로 큰 파라미터를 갖는 것이 바람직하다.

[0027] 마이크로제어기에, 바람직하게는 EEPROM 타입의 삭제할 수 없는 내부 메모리가 장착될 수 있다. 또한, 충분한 레벨의 보안을 달성하기 위해, 마이크로제어기는 로딩된 POS 지불 어플리케이션 내에 승인되지 않은 간섭(unauthorized intervention)들의 제어를 위한 부트-로더 유닛(boot-loader unit)을 포함할 수 있다. 부트-로더는 마이크로제어기 프로세서 메모리의 읽기-전용 부분(read-only part)에 위치될 수 있으며, 이는 단말기의 각 리셋 이후에 실행된다. 부트-로더 기능은 거기에서 여하한의 승인되지 않은 간섭에 의해 운영 체제(operating system) 또는 어플리케이션 프로그램들이 변경되지 않았는지를 제어하는 것이다. 각각의 리셋 이후, 부트-로더는 운영 체제 및 어플리케이션들이 저장되는 프로그램의 외부 플래시 메모리의 컨텐츠로부터 Hash(해시) 값(디지털 서명)을 계산한다. 그 후, 이는 EEPROM 내부 메모리에 저장된 값과 결과를 비교한다. 데이터가 동일한 경우, 부트-로더는 운영 체제에 관리(management)를 넘긴다(leave). 그렇지 않은 경우에는, 부트-로더가 실패한 시도들의 카운터를 감소시킨(decrement) 후, 중단된다. 카운터가 0에 도달한 경우, 마이크로제어기를 더 이상 시동(start-up)시킬 수 없다. 메모리에는, [주소지정된 영역(addressed area)의 시작과 끝으로서] 저장된 운영 체제가 존재할 수 있는 한편, 메모리의 용량의 Hash 값(디지털 서명)은 제 1 운영 체제 및 어플리케이션 저장 시 마이크로제어기 내로 저장된다. 추후, 이 데이터를 더 이상 변경할 수 없다.

[0028] 통상적인 버전에서, 마이크로제어기는 32-비트 마이크로프로세서 구조를 가질 수 있다.

[0029] 단말기의 유용성은 지불 단말기가 그 자신의 통신 채널 -즉, 이는 기본적으로 이동 통신 디바이스의 통신 경로들에 독립적임- 을 가질 수 있는 구성에 의해 상당히 증가될 수 있다. 이 구성 버전은 보안 요소들 및/또는 마이크로제어기에 연결되는 무접촉 통신 요소를 포함한 메모리 카드에 의해 특징지어진다. 이는 메모리 카드에 직접 안테나가 위치되는 경우, 및 안테나가 무접촉 통신 요소에 연결되는 경우에 바람직하다. 이러한 방식으로, 단말기의 기능적 독립(functional independence)이 달성될 것이다. 무접촉 통신 요소에는 주변 전자기장의 검출부가 장착될 수 있으며, 이로 인해 그 회로들이 요청된 연결에서만 활성화될 것이고, 이는 단말기의 에너지 요구를 낮추게 할 것이다. 단말기는 전자기장에 의해, 그리고 관련 메모리 카드의 인터페이스를 통한 휴대폰의 전력 공급기에 의해 전력공급될 수 있다. 무접촉 통신 디바이스는 암호화 유닛을 제외한 보안 요소 상의 모든 유닛들에 링크될 수 있으며, 암호화 유닛은 코드의 승인되지 않은 침입(unauthorized breach)의 위험을 낮추기 위해 마이크로제어기를 통해서만 접근가능할 것이다. 통신 타입들의 기존 분포(distribution)에 대하여, 통신 요소는 ISO14443 표준에 따른 NFC 타입으로 구성되는 것이 바람직하다.

[0030] 지불 단말기는 보안 요소에 상이한 독립적인 단말기들로부터의 구성 데이터를 갖는 더 많은 개별적인 유닛들을 가질 수 있다. 이들은 보안 요소의 분리된 도메인들에 저장될 것이다. 이 기술적 해결책은 지불 단말기가 상이한 지불 프로세서들에 속하는 단말기로 활성화하게 할 것이다. 이 능력은 사용자의 선택 또는 다른 명령에 의존할 것이다. 이 방식으로, 하나의 메모리 카드가 수 개의 독립적인 지불 단말기들의 시퀀스 기능(sequence function)들을 포괄하고 실행할 수 있다. 이 구성은 특히 설명된 지불 단말기의 이동성(mobility) 및 특정 상인의 그 독립성이 고려되는 경우에, 또는 지불 단말기의 아이덴티티 및 소유권(ownership)을 선택할 가능성을 갖는 것이 바람직한 경우에 유리할 것이다.

[0031] 또한, 지불 단말기는 보안 요소에 각각의 지불 어플리케이션들을 갖는 독립적인 지불 카드들을 보유한 수 개의 독립적인 유닛들을 가짐으로써 수 개의 지불 카드들을 포함할 수 있다. 그러므로, 지불 단말기는 다중지불(multipayment) 단말기일 뿐만 아니라, 다중 카드(multiple card)일 수 있다. 한 사용자에 의해 소유된 카드들의 증가된 수와 함께, 이 해결책은 휴대폰으로 삽입되는 하나의 메모리 카드로의 이 지불 수단의 편안하고 안전한 결합을 위한 공간을 생성할 것이다.

[0032] 바람직하게는 플래시 메모리의 형태인 메모리 카드의 메모리는 메모리 공간의 적어도 일부를 보호할 수 있다. 이러한 경우, 지불 POS 단말기 어플리케이션 유닛이 이 메모리 내로 저장될 수 있다. 이 유닛은 심지어 직접 마이크로프로세서 또는 보안 요소에 위치될 수 있지만, 몇몇 회로 기판 아키텍처에서는 메모리 영역의 필요한 크기가 고려되는 경우 이 종류의 해결책이 충분히 유연하지 않을 수 있다. 또한, 지불 POS 단말기 어플리케이션이 점차 업데이트될 필요가 있을 것이며, 이 활동은 메모리에 저장되는 다운로드 관리 유닛에 의해 수행될 수 있다. 메모리 카드에는 데이터 흐름 관리에 사용되는 메모리 제어기 프로세스 유닛이 장착될 수 있다. 웹 인터페이스를 통한 메모리 카드와 휴대폰 간의 통신에 대한 여하한의 필요성이 존재하는 경우, 웹 서버 유닛이 메모리 카드 내로 포함될 수 있다.

[0033] 제시된 설명에 따르면, 단말기의 유용성은 비-금융 성격(non-financial character)의 기능들에 대해 이를 연장

시킴으로써 증가될 것이다. 외부 디바이스, 예를 들어 원격 제어, 게이트에 대한 전자 키 등을 제어하기 위해, 메모리 카드의 기존 요소들, 독립적인 보안 요소 도메인, 무접촉 통신 요소, 및 암호화 유닛이 사용될 수 있다. 그 경우, 마이크로제어기를 통해 초기화되는 비-금융 어플리케이션 유닛이 보안 요소 또는 통제 스마트 카드 칩(governing smart card chip) 내에 있을 수 있다.

[0034] 이 해결책에 따른 구성에서, 지불 단말기 기능을 갖는 메모리 카드는 이동 통신 디바이스의 연장된 메모리의 기능도 더 충족시킬 수 있다. 보호되지 않은 부분에, 메모리는 그림, 음악 파일 및 유사한 것들과 같이 사용자의 자유롭게 접근가능한 데이터를 위한 영역을 가질 수 있다. 이 부분은 이동 통신 디바이스를 보는 경우에 직접 보일 수 있다. 사용자로부터 숨겨지는 데이터를 위한 메모리에는, 지불 트랜잭션 결과들 및 유사한 것들의 기록들로서 시스템 데이터가 존재할 수 있다.

[0035] 상기 시스템은 표준 가게(standard shop)에서 지불하기 위하여 지불 POS 단말기 어플리케이션 이니시에이터(initiator)로 보충될 수 있다; 이니시에이터는 간단한 하드웨어 요소의 형태이거나, 금전 등록기의 일부분일 수 있다. 이니시에이터는 지불 값 생성 유닛을 가질 수 있다. 상인은 이니시에이터를 통해 필요한 지불의 총액을 입력한다. 또한, 이 총액은 금전 등록기로부터 산출된 최종 구매 총액으로서 생성될 수 있다. 이니시에이터가 통신 요소에 부착되거나, 여기에 통신 요소가 완전히(downright) 장착되며, 이는 착탈식 메모리 카드 상의 통신 요소와, 또는 이동 통신 디바이스의 단거리 통신 요소와 호환가능하다.

[0036] 본 발명에 따르면, 이동 통신 디바이스를 이용한 지불의 자동 이체 방식은 지불 POS 단말기 어플리케이션이 추가 하드웨어를 위한 휴대폰의 슬롯 내로 삽입되는 착탈식 메모리 카드 상에서 실행될 수 있고, 또한 지불 카드 어플리케이션이 동일한 하드웨어 디바이스 상에서 실행될 수 있다는 사실에 기초한다. 지금까지 알려졌던 지불 POS 단말기 어플리케이션의 실행은, 지불 카드가 지불의 실현 동안 임시로 POS 단말기에 연결된다는 사실을 특징으로 하였다. 제시된 해결책에 따르면, 지불 카드는 지불 단말기에 고정적으로(firmly) 연결되고, 이에 따라 POS 단말기와 지불 카드 간의 통신이 지불 카드의 회로들을 통해 직접 실행될 수 있다. 다양한 신규한 지불 어플리케이션 절차들의 가능성이 이 기술적 해결책으로부터 급등하고, 기본적으로 지불 POS 단말기 어플리케이션들의 결과가 오늘날 사용되는 포맷 - EMV 지불 암호로 이루어질 수 있다.

[0037] 가능한 절차의 버전들 중 하나에서, 지불 POS 단말기 어플리케이션은 메모리 카드의 마이크로제어기 내로 로딩되고, 후속하여 선택된 단말기의 아이덴티티의 구성 데이터가 대응하는 보안 요소로부터 로딩된다. 또한, 중요한 특징은 보안 요소로부터 지불 단말기로서 작동하는 마이크로제어기로 지불 카드 데이터를 로딩할 가능성이며, 따라서 상기 데이터는 지불 POS 단말기 어플리케이션에 의해 그 실행을 위해 사용되는 동일한 종류의 하드웨어 장비로부터 로딩된다. 보안 요소가 충분한 연산 능력을 갖는 경우, 지불 POS 단말기 어플리케이션은 보안 요소에서 직접 실행될 수 있다. 이는, 예를 들어 하나는 지불 단말기들를 위해, 다른 하나는 지불 카드를 위해 2 개의 보안 요소들이 사용되는 경우에 일어날 것이다. 이 구성에서도, 지불 POS 단말기 어플리케이션은 평범한 상태의, 모든 지불 단말기의 아이덴티티에 대해 공통인 것으로서 생성될 수 있으며; 지불 단말기가 선택된 이후에만 지불 POS 단말기 어플리케이션에서 보안 요소의 대응하는 독립적인 도메인으로부터 식별 데이터가 로딩된다. 또한, 이미 삽입된 구성 데이터를 갖는 독립적인 지불 POS 단말기 어플리케이션을 이용하는 버전은 제거되지 않는다.

[0038] 보안의 레벨을 증가시키기 위해, 부트-로더는 지불 POS 단말기 어플리케이션 자체를 실행시키기 전에 지불 POS 단말기 어플리케이션에서의 변경 제어(changes control)를 실행하는 것이 바람직하다. 지불 POS 단말기 어플리케이션은 이동 통신 디바이스의 입력 디바이스, 주로 키보드를 통해 관리될 것이다.

[0039] 지불 카드들 또는 적어도 하나의 지불 카드가 착탈식 메모리 카드에 위치되는 경우, 및 지불 단말기 어플리케이션이 동일한 착탈식 메모리 카드에서 실행되는 경우와 같이, 동일한 기술을 기반으로 상인의 기술적 장비에 대한 요건들을 간소화하는 구조의 "라이트 POS(light POS)"도 생성할 수 있다. 이 버전의 구성의 주제(subject matter)는, POS 지불 단말기가 착탈식 메모리 카드와 판매 디바이스(Sales Device)의 임시 연결 동안 착탈식 메모리 카드에 생성된다는 사실에 있다. 판매 디바이스는 상인에게 속하거나, 또는 이는 상인에 의해 보유되고 식별 데이터를 갖는 보안처리 유닛을 포함하며, 이는 특히 POS 지불 단말기를 대응하는 상인의 은행 계좌에 매칭하는데 필요한 데이터를 포함한다. 기본적으로, 판매 디바이스는 하드웨어에 의해 형성되며, 이는 임시로 생성된 POS 지불 단말기의 올바른 아이덴티티를 보장한다.

[0040] 통상의 기본적인 기술적 개념의 이러한 이용의 중요한 특성은, 앞서 정의된 구조들을 갖는 POS 단말기가 두 부분들의 임시 연결로부터 생성된다는 사실에 있다. 상기 연결은 임시적인 것으로 분류되는데, 이는 지불 프로세스가 종료된 후 부분들의 연결이 끊어지고, 통신 채널이 중단되며, 판매 디바이스와 또 다른 착탈식 메모리 카

드 간의 또 다른 새로운 연결이 생성될 수 있기 때문이다. 당연히, 앞서 상호작용한 착탈식 메모리 카드와 판매 디바이스의 반복된 연결도 배제되지 않는다. 연결의 일시성은 현실적으로 하나의 지불 프로세스에 의해 제한된 시간상 단계(time phase)로서 이해되는 한편, 이는 지불 프로세스의 시작 전과 종료 후 약간의 연결 시간도 요구될 수 있다. 상인과 지불하는 고객의 편에서 항상 새로운 쌍의 요소들을 짝지을 가능성은, 지불하는 고객의 이동 통신 디바이스에서 대응하는 상인의 아이덴티티를 갖는 POS 단말기를 항상 생성할 수 있는 해결책이다.

[0041] 판매 디바이스 단어 배열(collocation of words)은 POS 지불 단말기 분야에서 통상적으로 사용되는 용어가 아니며, 이 배열에서 이 설명에 따른 기능들의 실현을 위해 대응하는 소프트웨어가 장착된 여하한 타입의 하드웨어 요소를 떠올려야 한다. 판매 디바이스는 외부로부터의 POS 지불 단말기로서 동작하고, 실제로 상인들은 보통 그것을 그러한 방식으로 부를 것이지만, 어플리케이션의 구조 및 실행 관점으로부터 판매 디바이스는 전체 POS 지불 단말기의 단지 중요한 부분일 뿐 충분한 부분(sufficient part)은 아니다. 그러므로, 기본적으로 상인이나 구매 위치에 연결되고, 직불(debit payment)들의 올바른 경로를 보장하는 단말기의 일부분으로서 일반적인 의미에서 판매 디바이스라는 용어를 이해할 필요가 있다.

[0042] 전체 POS 지불 단말기에서, 판매 디바이스는 POS 단말기의 아이덴티티를 전달하고 지불의 값을 입력하는 2 개의 기본 기능들을 가질 수 있다. 기본적으로, 더 좁은 하드웨어 버전도 가능하며, 여기에 이동 통신 디바이스의 키보드를 통해 지불 값이 입력된다. 하지만, 이 종류의 버전은 상인에게는 불편한데, 이는 상인이 고객의 이동 통신 디바이스를 제어하거나, 고객이 지불 단말기 어플리케이션에 올바른 지불 총액을 입력할 것을 신뢰해야 하기 때문이다. 삽입된 값은 판매 디바이스 디스플레이 상에서도 보여질 수 있어서, 상인이 이를 체크할 수 있더라도, 지불된 총액이 상인 편의 요소들을 통해 입력되는 것이 훨씬 더 편할 것이다. 이동 통신 디바이스의 키보드를 통해 지불 값을 입력하는 것으로 이 부분에서 설명된 버전은 직불 실현 시 상인의 행동 및 동작들에 대한 표준(예를 들어, EMV)을 충족시킬 필요가 없을 것이지만, 이는 기본적으로 제시된 해결책의 원리를 이용하여 실현될 수 있다.

[0043] 판매 디바이스는 지불 단말기 어플리케이션을 독립적으로 수행할 수 없고, 이는 처리 센터와의 연결 생성을 위해 통신 채널들을 갖지 않아도 된다. 하드웨어 세트는 고객의 이동 통신 디바이스 내로 삽입된 착탈식 메모리 카드와 상인의 판매 디바이스의 연결에 의해서만 통상적인 POS 지불 단말기의 기본 기능들을 모두 충족시킬 수 있다. 임시 연결은 기본적으로 각각의 개별적인 지불의 실현을 위해 생성될 수 있는 한편, 이는 항상 상이한 고객들 편의 상이한 통신 디바이스일 수 있다. 정확하게는, 이동 통신 디바이스는 기존 GSM/GPRS(Global System for Mobile Communications/General Packet Radio Service)로 인해 지불 센터와의 필요한 연결을 생성할 수 있다. 하지만, 본 기재내용에 따른 해결책이 오프라인 및 온라인 지불을 처리할 수 있기 때문에, 이 연결은 각각의 지불 시 생성되지 않아도 된다.

[0044] 판매 디바이스와의 연결을 위한 착탈식 메모리 카드 구조는 앞서 언급된 변형예들과 유사하다. 또한, 이는 판매 디바이스 및 이동 통신 디바이스로 구성된 세트가 지불 단말기 어플리케이션을 실행하고 수행할 수 있도록 하드웨어 및 소프트웨어 요소들을 포함하며, 이는 프로세스 관점에서 착탈식 메모리 카드 상에 직접 직불 작동의 커널을 형성한다. 판매 디바이스 및 이동 통신 디바이스로 구성된 세트에는 외부 지불 카드 리더기가 장착될 필요가 없기 때문에, 이는 지불 카드 유닛을 갖는 보안처리 메모리도 착탈식 메모리 카드 상에 직접 있는 경우에 적절할 것이다. 또한, 판매 디바이스와의 연결을 위한 통신 요소 및 지불 단말기 어플리케이션의 실행을 위한 유닛이 착탈식 메모리 카드 상에 있을 것이다. POS 지불 단말기의 식별 데이터를 갖는 보안처리 메모리 이외에, 판매 디바이스는 착탈식 메모리 카드와의 연결을 위한 통신 요소도 포함한다. 이 요소들로 인해, 메모리를 연장하는 카드에 대한 슬롯을 갖는 통상적인 휴대폰의 도움으로 POS 지불 단말기가 생성된다. 이에 따라, 착탈식 메모리 카드가 일반적인 지불 단말기를 포함할 수 있으며, 이는 판매 디바이스와 연결된 후에만 유일한 아이덴티티를 갖는 특정한 지불 단말기가 될 것이다. 판매 디바이스는 지불이 수행되어야 하는 누군가를 위해 이 임시 연결에 대해 명백한 식별을 제공할 것이다. NFC(Near Field Communication) 통신 요소가 없는 휴대폰들에서도 이 기능의 관심이 존재하기 때문에, 이러한 NFC 통신 요소가 착탈식 메모리 카드에 직접 포함될 수 있다. 기본적으로, 이동 통신 디바이스와 판매 디바이스 간의 연결은 접촉 인터페이스의 형태일 수 있지만, 이는 커넥터들의 복잡한 통합 및 호환성의 문제들을 필요로 할 것이다. 그러므로, 유일한 해결책이 아니라면, 판매 디바이스와 착탈식 메모리 카드 간의 연결이 널리 표준화되는 NFC 통신 채널의 형태인 것이 적절할 것이다.

[0045] 설명된 구성으로 인해, 상인이 매우 간단한 판매 디바이스만을 가질 수 있을 것이며, 이는 아이덴티티, 단말기의 번호, 및 지불 프로세서 센터에서 대응하는 상인의 계좌 번호에 할당될 수 있는 정보를 전달할 것이다. 이 종류의 판매 디바이스는 매우 작고 단순할 것이다. 이는 상인이 요청된 지불 총액을 입력하기 위한 키보드 및

디스플레이를 갖는 작은 박스의 형태일 수 있다. 식별 데이터는 판매 디바이스의 인쇄 회로 상의 대응하는 요소에 직접 저장될 수 있으며, 또는 ICC(integrated circuit card) 카드, 또는 예를 들어 지금까지 암호 키를 갖는 SAM(Security Authentication Module) 카드들로 알려진 다른 캐리어들에 저장될 수 있다. 이 버전에서는, 판매 디바이스의 커버를 벗긴 후에 통상적인 SIM(Subscriber Identity Module) 카드 크기의 SAM 카드가 이용가능하다. SAM 카드는 제 1 활성화 전에 판매 디바이스 내로 삽입된다.

[0046] 고객은 그의 이동 통신 디바이스를 판매 디바이스에 가볍게 접촉시킬 것이다(tap). 이를 가볍게 접촉시킴으로써, NFC 통신 채널이 생성될 것이며, 이 임시로 생성된 POS 지불 단말기의 아이덴티티에 대한 정보가 판매 디바이스로부터 착탈식 메모리 카드로 송신될 것이다. 그 후, 식별 데이터는 판매 디바이스 내의 보안 요소 내에 저장되는 Master Key(마스터 키)에 의해 암호화될 수 있다. 판매 디바이스로부터의 입력 데이터는 지불 단말기 어플리케이션이 착탈식 메모리 카드 상에서 읽힌 후, 지불 단말기 어플리케이션의 실행을 위한 기초가 될 것이다. 지불 단말기 어플리케이션은 그 자신의 아이덴티티 없이 평범한 형태로 착탈식 메모리 카드에 로딩될 수 있다. 기본적으로, 판매 디바이스와 착탈식 메모리 카드 간의 임시 연결의 생성 이후, 일반적이고 포괄적인(general, generic) 평범한 단말기가 시스템에서 대응하는 상인에게 할당되는 특정 POS 단말기로 전환될 것이다. 이 단계는 새로운 1-회용 POS 단말기의 시작을 위한 어떠한 준비를 형성한다. 후속하여, 예를 들어 EMV 타입의 지불 단말기 어플리케이션이 연결 동안에 지금까지처럼 표준 POS 단말기들과 유사한 방식으로 실행될 수 있다.

[0047] POS 단말기의 식별 데이터의 암호화는 Master Key로 행해지며, 이는 추후에 지불 암호의 생성을 위해 지불 단말기 어플리케이션에 의해 사용되는 암호 키들과 일반적으로 상이할 수 있으며, 대부분 상이할 것이다. Master Key는, 예를 들어 판매 디바이스 하드웨어의 공급자로부터의 것일 수 있으며, 지불 단말기 어플리케이션의 암호 키들은 은행 또는 지불 프로세서에 의해 발행될 수 있다. 실제로, 암호화 키들의 차이는 지불 결제 시스템(payment clearing system)에서 작동하는 개별적인 개체들의 상이한 요청들에 따를 것이다.

[0048] 보안 증가의 관점으로부터, 지불 총액에 관한 입력도 판매 디바이스로부터 이동 통신 디바이스까지의 전달 동안 암호화될 수 있다. 이로 인해, 지불 단말기 어플리케이션 커널이 실행되기도 전에 지불하는 사용자가 지불 값을 낮출 수 있는 위험이 낮아진다. 이러한 종류의 변경은 지불되는 총액을 보여주는 형태로 상인 편의 지불의 최종 확정에서 나타날 것이지만, 부주의(inobservance) 및 루틴 접근의 경우 상인은 총액의 변경을 알아채지 못할 수 있다.

[0049] 선택된 지불 카드의 유닛과의 통신이 지불 단말기 어플리케이션의 실행 시 착탈식 메모리 카드에서 직접 행해지는 구성이 적절하다. 독립적인 지불 카드들의 수 개의 유닛들은 물리적인 별도 보안 요소들이나 하나의 보안 요소의 독립적인 도메인들 상에서 착탈식 메모리 카드에 저장될 수 있다. 이 구성에서, 지불 단말기 어플리케이션은 착탈식 메모리 카드 상에서 직접 실행될 수 있고, 고객의 지불 카드의 데이터는 외부 리더기를 통해, 그리고 인터넷 영역으로도 송신되지 않으며, 이 사실은 지불 작동의 보안에 긍정적인 영향을 준다.

[0050] 판매 디바이스는 상이한 형태일 수 있다; 식별 데이터를 갖는 보안 요소를 직접 포함하는 키보드를 갖는 작은 박스 이외에, 이는 그 안에서 바람직하게는 전형적인 표준 ICC(integrated circuit card) 카드 포맷의 외부 카드들의 생성된 리더기인 방식으로도 생성될 수 있다. 그 후, 중요 데이터(sensitive data)가 이러한 종류의 카드 칩으로 로딩될 수 있다. 또한, 카드의 칩은 적절하게는 실현된 지불 트랜잭션들에 대한 데이터의 입력을 위해 사용될 수 있는 소정 메모리 용량을 포함한다. 그날이 지난 후, 상인은 가게에서, 예를 들어 신문 가판대에서 판매 디바이스의 기초 부분을 남길 수 있으며, ICC 카드만을 휴대할 수 있다(take). 판매 디바이스로부터 ICC 카드를 휴대하는 경우, 그는 처리를 위해 이를 은행으로 가져가거나 리더기를 이용함으로써 집 컴퓨터에서 이로부터의 데이터를 백업(back up)할 수 있다. 상인이 수 개의 모바일 스탠드(mobile stand)들을 갖는 경우, 하나의 단말기 및 하나의 은행 계좌의 식별 데이터를 갖는 하나의 ICC와 조합된 수 개의 판매 디바이스들이 존재할 수 있으며, 반면 하나의 판매 디바이스가 하나의 가게의 복수 작업 영업소(multiple shift business premises) 내의 상이한 상인들에 속하는 수 개의 ICC 카드들과 연속적으로 사용될 수 있다.

[0051] 필요에 따라, 판매 디바이스가 연장된 부속품들과의 연결을 위해, 예를 들어 USB 포맷의 그 자신의 인터페이스를 갖는 경우에 적절하며, 이는 지불 데이터가 판매 디바이스로부터 직접 프린트될 수 있게 하며, 또는 각각 이 커넥터를 통해 지불 카드 리더기, GPRS 모뎀 및 유사한 것들을 연결하는 것이 가능하다.

[0052] 본 명세서에서 설명된 시스템들의 구현 후, 이동 통신 디바이스가 지불 카드의 데이터를 훔칠 목적으로 공격 타겟이 될 수 있는 것으로 여겨질 수 있으며, 이는 이동 통신 디바이스의 회로들과의 상호작용을 위해 끊임없이 준비되고 있다. 이 순간에, 이 관련 해커들의 전략이 진행할 방향을 나타내는 것은 불가능한데, 이는 제시된

해결책이 신규하고, 지금까지 널리 보급되지 않았었기 때문이다. 하지만, 이는 일정한 기미(constant promptness), 용이함(readiness), 및 지불 카드 또는 착탈식 메모리 카드의 지불 단말기 각각의 접속가능성(connectivity)을 악용하는 경향들이 존재할 것으로 여겨질 수 있다. 이상적인 구성에서는, 착탈식 카드가 2개의 독립적인 접근 모드를 갖는 경우에 이 위험을 낮추는 것이 가능할 것이다. 하나의 접근 모드는 휴대폰과 같은 이동 통신 디바이스의 메모리 용량의 연장에 놓인 착탈식 메모리 카드의 통상적인 기능을 위해 설계되고 설정된다. 이 접근 모드는 지불 카드를 갖는 유닛으로의 접근, 및 착탈식 메모리 카드 상의 무접촉 통신 요소로의 접근을 방지한다. 기본적으로, 착탈식 메모리 카드의 인터페이스의 이 접근 모드에서 이 카드는 착탈식 메모리 카드의 통신 요소가 없는, 그리고 보안 요소가 없는 통상적인 착탈식 카드로 보인다.

[0053] 제 2 접근 모드는 착탈식 메모리 카드의 지불 기능을 위해 설계되고 설정되며, 이때 지불 카드를 갖는 유닛 및 착탈식 메모리 카드 상의 무접촉 통신 요소로의 접근이 인터페이스를 통해 이동 통신 디바이스의 회로들로부터 허용된다. 착탈식 메모리 카드에 위치된 지불 단말기를 갖는 유닛도 존재하는 경우, 이 유닛도 지불 기능을 위한 접근 모드에서만 접근가능하다.

[0054] 두 모드들은 번갈아 선택가능하고, 착탈식 메모리 카드의 지불 기능을 위한 접근 모드는 하드웨어 지불 버튼의 물리적인 가압 후에만 활성화될 수 있다는 것이 중요하다.

[0055] 적어도 하나의 지불 카드 유닛이 위치되는 착탈식 메모리 카드는, 목적 지불 버튼이 물리적으로 눌러지는 순간까지 인터페이스에서 이동 통신 디바이스의 메모리 용량의 연장을 위한 착탈식 메모리 카드로 보인다. 그 후, 착탈식 메모리 카드는 보안 요소 및 적어도 하나의 지불 카드 유닛을 갖는 카드로서 인터페이스 상에서 접근가능하게 된다.

[0056] 이 버전의 적절한 해결책에 따른 착탈식 메모리 카드는, 통상적으로 접근가능한 플래시 메모리를 포함하고, 지불 카드의 하드웨어 및 소프트웨어 요소들 또는 지불 단말기의 하드웨어 및 소프트웨어 요소들을 갖는 아키텍처를 갖는다. 이동 통신 디바이스의 통상적인 이용 시, 착탈식 메모리 카드는 대응하는 마이크로제어기를 갖는 메모리 용량의 연장을 위한 플래시 메모리만을 포함하는 것처럼 동작한다. 이 상태에서는, 착탈식 메모리 카드의 메모리에서 파일들의 리딩 및 기록이 가능해지지만, 다른 요소들 예를 들어 보안 요소, NFC 통신 요소는 숨겨지고 이 모드에서 관리되거나 실행될 수 없다.

[0057] 목적 하드웨어 지불 버튼의 존재는, 그 인터페이스 레벨에서의 착탈식 지불 카드의 성격의 변경이 오로지 지불 버튼의 물리적 가압에 따르게 할 수 있다. 버튼의 물리적 가압의 필요성은 사용자의 의지를 가장한 스크립트 또는 몇몇 바람직하지 않은 소프트웨어에 의해 지불 어플리케이션을 실행할 가능성을 배제한다.

[0058] 이 구성에 의해, 사용자 모르게 보안 요소들을 극복하려는 시도에 대해 착탈식 메모리 카드의 인터페이스가 악용될 위험이 배제될 것이다. 버튼의 물리적 가압과 대응하는 펌웨어의 실행 간의 연결은, 결코 이를 다시 기록하거나, 변경시키거나, 업데이트할 수 없는, 또는 대응하는 패스워드 없이 이를 행할 수 없는 방식으로 메모리에 저장될 수 있다. 이때, 승인되지 않은 프로그램은 신호가 어플리케이션의 실행의 다른 단계들로의 버튼의 실제 물리적 가압으로서 보일 수 있는 방식으로 물리적인 지불 버튼으로부터 그 신호를 에뮬레이트(emulate)하는 것이 불가능하다. 침입자는 원격 이동 통신 디바이스의 설명된 버튼을 물리적으로 가압할 가능성을 갖지 않을 것이기 때문에, 침입자가 지불 카드의 유닛 또는 착탈식 메모리 카드 상의 지불 단말기의 유닛으로의 제어하기 힘든 접근(uncontrollable access)을 얻을 수 있는 것이 배제된다. 착탈식 메모리 카드는 표준 메모리 카드로서 동작할 것이며, 지불 버튼의 물리적 가압 후에만 지불 카드 모드로 스위칭할 것이다. 지불 어플리케이션의 종료는 자동으로 카드의 모드를 메모리 용량을 연장한 통상적인 카드 모드로 스위칭할 것이다.

[0059] 이동 통신 디바이스 내의 지불 프로세스의 앞서 설명된 실행의 오프셋은 두 접근 모드의 동일한 원리에 기초한다. 이 절차의 변형예는, 착탈식 메모리 카드가 지불 프로세스의 실행 전에 메모리 용량을 연장한 통상적인 기능을 위한 접근 모드에 있다는 사실에 기초한다. 이때, 지불 카드 및 적절하게는 심지어 무접촉 통신 요소를 갖는 유닛, 및 지불 단말기를 갖는 유닛은, 착탈식 메모리 카드에 위치되는 경우, 인터페이스 편으로부터 접근할 수 없다. 오로지 하드웨어 지불 버튼의 물리적 가압 후에만, 착탈식 메모리 카드가 지불 카드를 갖는 유닛에 대해 허용된 접근을 갖는 착탈식 메모리 카드의 지불 기능을 위한 접근 모드로 스위칭한다.

도면의 간단한 설명

[0060] 도 1 내지 도 14를 참조하여, 본 발명을 더 상세히 설명한다.

도 1에서, 하나의 분리된 보안 요소를 갖는 메모리 카드 상의 개별적인 요소들 간의 연결을 보이는 메모리 카드

의 개별적인 요소들의 블록도가 존재하며, 상기 보안 요소 상에서 지불 POS 단말기 및 수 개의 지불 카드들로부터의 데이터가 보호된다.

도 2는 모바일 네트워크로부터 다운로드된 파일들에 대한 지불 시, 또는 인터넷 가게에서의 지불 시 메모리 카드를 갖는 휴대폰이 존재하는 해결책을 나타낸다.

도 3에서, 2 개의 독립적인 보안 요소들, 및 메모리 카드에 직접 위치되는 안테나와 같은 통신 요소를 갖는 마이크로SD 타입의 착탈식 메모리 카드가 존재한다. 또한, 이 도면은 평범한 상태의 POS 지불 단말기의 유닛, 및 다양한 은행으로부터의 4 개의 독립적인 지불 카드의 유닛들을 갖는 구성을 도시할 수 있다.

도 4에서, 2 개의 보안 요소를 갖는 옵션에서 간소화된 아키텍처를 갖는 선불(pre-paid) 착탈식 메모리 카드가 존재한다.

도 5에서, 모바일 네트워크에서 제공된 파일에 대해 지불하는 동안 착탈식 메모리 카드에서 실행되는 지불 어플리케이션 내의 연속한 작업들이 존재한다.

도 6에서, 지불 이니시에이터를 갖는 해결책이 존재하며, 상기 이니시에이터는 물리적인 가게에서 실제로 영속하여(permanently) 금전 등록기 옆에 위치된다.

도 7에서, 판매 디바이스 부근에 배치되는 통상적인 휴대폰의 형태인 이동 통신 디바이스에 대한 외부 관점의 개략적인 설명이 존재한다. 판매 디바이스에 대한 이동 통신 디바이스의 부분 비(proportion ratio), 치수, 및 형상은 정해진 것이 아니며, 단지 도면의 더 우수한 명료성을 위해 선택된 것이다. 도면에서, 휴대폰 및 판매 디바이스는 도면의 명확함을 증가시키기 위해 겹쳐지지 않지만, 실제로는 휴대폰이 판매 디바이스의 표면에 직접 배치될 수 있다.

도 8에서, 판매 디바이스의 기초 구조에 대한 사시도가 존재하며, 이때 휴대폰 편의 통신 요소가 착탈식 메모리 카드에 위치되는 것을 볼 수 있다. POS 단말기의 식별 데이터를 갖는 메모리는 착탈식 메모리 카드에 위치된다. POS 단말기의 식별 데이터를 갖는 메모리는 SAM 카드에 위치된다. 또한, 도 8에서 착탈식 메모리 카드와 판매 디바이스 간의 NFC 통신 채널이 존재한다.

도 9에서, 상인의 ICC 카드가 리더기의 몸체로 삽입되는 구성의 판매 디바이스 구조의 개략도가 존재한다.

도 10에서, 금전 등록기에 연결되는 구성이 존재한다. 또한, 판매 디바이스는 ICC 카드의 리더기를 포함하고, 또한 이는 미니 USB 커넥터를 갖는다.

도 11에서, 하드웨어 지불 버튼의 가압과 함께 지불 어플리케이션의 실행의 연속을 나타내는 개략적인 다이어그램이 존재하며, 이때 레벨 폰 하드웨어/폰 펌웨어/착탈식 메모리 카드에서 어플리케이션의 실행 동안 개별적인 작업들 및 프로세스들의 로컬리제이션(localization)을 볼 수 있다.

도 12에서, 휴대폰의 메모리 접근 모드의 통상적인 연장의 경우, 착탈식 메모리 카드가 외관상 나타나는 구조를 알 수 있다.

도 13에서, 지불 카드 접근 모드의 경우 착탈식 메모리 카드가 외관상 나타나는 구조가 존재한다. 이 구성에서는, 착탈식 메모리 카드에 위치된 지불 단말기를 갖는 유닛도 존재한다.

도 14에서, 지불 버튼을 갖는 휴대폰의 일 예시가 존재한다.

발명을 실시하기 위한 구체적인 내용

[0061] 제 1 예시

[0062] 이 예시에서, 도 3에 따른 2 개의 독립적인 보안 요소(31, 32)를 갖는 해결책이 설명된다. 분리된 하드웨어 보안 요소들(31, 32)의 이용은 증명 요건들을 간소화하고, 이들은 보안 요소(3, 31, 32)들 상의 중요 데이터의 저장에 대해 지불 시스템의 개별적인 관계자들(카드 발행사, 결제 센터 운영자)에 의해 설정된다. 또한, 이 예시에서 보안 요소들(31, 32) 각각은 독립적인 도메인들로 나누어지며, 이는 상이한 카드 발행사 및 POS 단말기 구성 데이터의 상이한 소유자들에게 제공될 수 있다. 보안 요소들(31, 32)은 회로 기판 상의 독립적인 칩들의 형태이며, 이때 이들은 마이크로제어기(12)의 역할을 충족시키는 제어기와 연결된다. 제어기(12)를 향한 이들의 인터페이스는 ISO 7816이다. 착탈식 메모리 카드(1)는 마이크로SD 카드의 형태이다. NFC 플랫폼 통신 프로세스들을 수행하도록 설정되고 이러함으로써 통신 요소(13)의 기능을 충족시키는 ASIC(application-specific integrated circuit) 칩이 마이크로제어기(12)와 연결된다. 착탈식 메모리 카드의 몸체(1)에 직접 위치되는 안

테나(21)는 본 특허권자의 상이한 특허 출원들에 따라 설계되고, NFC 통신을 가능하게 하는 방식으로 ASIC 칩에 연결되며, 이는 휴대폰(4)의 다른 하드웨어에 독립적이다. 또한, 착탈식 메모리 카드(1)는 예를 들어 2GB의 용량을 갖는 통상적인 플래시 메모리(2)를 포함한다. 사용자는 휴대폰 인터페이스(4)로부터 상기 메모리(2)의 일부분(20)에 접근할 수 없다; 상기 메모리의 이 부분은 실현된 지불 기록들의 파일보관(archiving)에 사용된다. 메모리(2)의 나머지 부분은 음악, 그림 및 유사한 것의 통상적인 저장을 위해 사용되며, 이로 인해 전체 메모리 카드(1)가 사용자에게 통상적인 메모리 매체로 보인다. 착탈식 메모리 카드(1) 상에 POS 단말기 및 지불 카드를 배치함으로써, 메모리 용량을 확장하도록 설계된 휴대폰(4)의 슬롯의 초기 기능이 사라지지는 않았다.

[0063] 지불은 2 개의 상이한 형태로 실행될 수 있다. 예를 들어 도 6에 나타낸 바와 같이, 휴대폰(4)의 사용자는 인터넷 가게에서 전자 형식의 맵을 사려고 결심한다. 이 경우, 인터넷 가게의 운영자(operator)는 휴대폰(4) 프로듀서(producer)일 수 있다. 설명된 기술적 해결책에 따라 생성된 마이크로SD 메모리 카드(1)는 휴대폰(4)의 외부로부터 접근가능한 측면 슬롯(lateral slot)으로 삽입된다. 보안 요소(31) 상에, 인터넷 가게의 운영자를 포함한 여러 사람에게 속하는 POS 단말기 구성 데이터(6)가 저장된다. 구매되는 아이템의 선택 후, 대응하는 총액의 지불에 대한 요청이 인터넷 가게로부터 휴대폰(4)으로 송신된다. 사용자는 휴대폰에 장착되어 있는 지불 버튼을 누른다. 또 다른 지불 예시에서는, 지불 선택이 휴대폰(4) 디스플레이 상에 보여지는 소프트웨어 버튼에 의해 초기화될 수 있다. 지불 POS 어플리케이션의 개시에 대한 요청이 인터페이스(11)로 송신된다. 지불 POS 단말기 어플리케이션은, 표준 POS 지불 단말기와 POS 단말기의 리더기에 삽입되는 지불 카드 간의 관계의 경우와 동일한 방식으로 메모리 카드(1) 상에서 실행된다. 휴대폰(4)의 디스플레이는 지불의 실행을 관리하기 위해 사용된다. 사용자는 요청된 총액을 지불하고자 하는 지불 카드를 선택한다. 선택된 지불 카드의 대응하는 유닛(7)에서 어플리케이션을 활성화한 후, 대응하는 카드 발행사의 위험 관리의 사전설정된 규칙(preset rule)들에 의해 지불의 실행이 관리될 수 있다. 이에 따라, 지불 카드 패스워드를 입력해야 할 수도 있고 없을 수도 있다.

[0064] 지불 POS 단말기 어플리케이션을 종료시킨 후, 소프트웨어에 의해 POS 지불 단말기와 지불 카드 간의 연결이 끊어지고, 결과적인 지불 암호가 인터넷 가게에서 처리되도록 GPRS 채널을 통해 송신된다. 인터넷 가게가 지불 파일을 수신하고 암호 해독한 후, 지불이 평가되며, 승인되는 결과(affirmative result)의 경우 비용을 지불한 아이템, 이 예시에서는 맵이 휴대폰(4)으로 송신된다.

[0065] 제 2 예시

[0066] 표준 마이크로SD 카드와 형상 및 파라미터들이 대비될 수 있는 마이크로SD 타입의 착탈식 지불 카드(1) 플랫폼에서의 지불 단말기가 이 예시에서 설명된다. 도 1에서와 같은 지불 카드(1)는 멀티-태스크 운영 체제(8)[이 예시에서는, Linux(리눅스)]에서 작동하는 32-비트 마이크로프로세서의 형태인 마이크로제어기(12)를 갖는다. 플래시 메모리(2), 보안 요소(3) 및 SD 인터페이스(11)가 마이크로제어기(12)에 연결된다. 마이크로프로세서(12)는 내부 EEPROM 메모리(10), 및 로딩된 지불 POS 단말기 어플리케이션에서 비-승인된 간섭들을 제어하는 부트-로더 유닛(9)을 포함한다.

[0067] 플래시 메모리(2)는 보안처리 부분 및 비보호 부분으로 나누어진다. 비보호 부분에, 사용자의 자유롭게 접근가능하고 볼 수 있는 데이터를 위한 공간(15) 및 숨겨진 시스템 파일들, 특히 지불 단말기에 의해 처리되는 지불 트랜잭션들의 기록들을 위한 공간(20)이 존재한다. 메모리 카드의 보안처리 부분에는, 운영 체제(이 예시에서는 Linux)를 보유한 유닛(8), 및 특히 EMV 타입의 어플리케이션인 경우의 지불 POS 단말기 어플리케이션이 저장되는 지불 POS 단말기 어플리케이션 유닛(5)이 존재한다. 이 예시에서, 메모리(2)의 보안처리 부분에는 메모리 카드(1)에 소프트웨어 업데이트 관리 및 저장을 위해 사용되는 다운로드 관리 유닛(19)도 존재한다. 스마트 카드 칩(3)에 어플리케이션들을 로드/업그레이드할 필요가 있는 경우, 어플리케이션의 이진 데이터가 플래시 메모리(2)의 비보호 부분에, 예를 들어 사용자에게 숨겨진 데이터가 저장되는 공간(20)의 시스템 데이터 유닛에 로딩된다. 다운로드 관리 유닛(19)은 보안 요소(3)에 로딩되어야 하는 어떠한 새로운 파일도 시스템 데이터 유닛에 존재하지 않는지를 주기적으로 체크한다. 존재하는 경우, 각각의 설치가 실행된다.

[0068] 또한, 메모리(2)의 보안처리 부분에는, EMV 지불 어플리케이션을 제외한, 보안 요소(3)에 저장되는 어플리케이션들을 관리하는데 사용되는 SCWS 웹 서버 유닛이 존재한다. 마이크로제어기(12)에, (주소지정된 영역의 시작 및 끝으로서) 운영 체제가 저장되는 메모리 공간이 존재한다. 제 1 운영 체제 및 어플리케이션 저장 동안, 메모리의 용량의 Hash 값(디지털 서명)이 마이크로제어기(12) 내로 저장된다. 추후에, 이 데이터를 더 이상 변경시킬 수 없으며, 이는 금지된 소프트웨어 변경으로부터의 보호를 보장한다.

[0069] 수 개의 개별적인 도메인들이 스마트 카드 칩(3)의 보안 요소에 생성된다. 본 명세서에서는, 이들 중 세 개가 3 개의 상이한 지불 프로세서들에 속하는 3 개의 독립적인 단말기들의 구성 데이터 유닛들(6)을 보유하는데 사용된다. 보안 요소의 두 부분들은 EMV 타입의 각각의 지불 어플리케이션들을 갖는 2 개의 독립적인 지불 카드들(7)을 포함한다. 그러므로, 본 명세서에 주어진 예시는 3 개의 단말기들에서 2 개의 상이한 지불 카드들에 의해 사용자가 지불할 수 있는 해결책을 설명하고, 단말기들 각각은 상이한 지불 프로세서에 속한다. 예를 들어, 이러한 지불 프로세서들 중 하나는 자동 이체 지불 트랙잭션 처리 서비스들에 통신 서비스(telecommunication service)들을 연결하는 휴대폰 네트워크 사업자일 수 있다. 또한, 보안 요소에는 RSA 암호화 유닛(14)이 존재한다.

[0070] 또한, 메모리 카드(1)는 메모리 카드(1) 내에 그 자신의 NFC 무접촉 통신 요소(13) 및 그 위에 배치된 안테나(21)를 각각 갖는다. 이 구성은 NFC 칩을 갖지 않는 통상적인 폰과 ISO14443 표준을 충족하는 관련 리더기 간의 NFC 통신 연결의 생성을 가능하게 한다.

[0071] 또한, 보안 요소(3)에는 비-금융 어플리케이션 유닛(16)이 존재하며, 이는 이 예시에서 도어 개방(door opening)을 위한 전자 무접촉 키로서 작동하도록 구성된다.

[0072] 플래시 메모리(2) 제어기(17)는 메모리(2)의 보안처리 부분에 존재하며, 이는 휴대폰과 메모리 카드(1)의 플래시 메모리(2) 간의 데이터 전달을 관리한다. 플래시 메모리(2) 제어기(17)는 데이터를 보거나 메모리(2)의 보안처리 부분에 기록할 가능성을 유닛화하고(unit the possibility), 또한 시스템 데이터 유닛(판독 및 기록이 허용됨)이 위치되는 메모리(2)의 비보호 부분을 볼 가능성을 유닛화한다.

[0073] 지불 POS 단말기 어플리케이션은 추가 하드웨어를 위한 이동 통신 디바이스의 슬롯(4)으로 삽입되는 착탈식 메모리 카드(1)에서 실행된다. 지불 POS 단말기 어플리케이션은 메모리 카드(1)의 마이크로제어기(12)로 로딩되며, 후속하여 선택된 단말기의 아이덴티티의 구성 데이터가 보안 요소(3)로부터 로딩된다. 선택된 지불 카드 데이터는 보안 요소(3)로부터 지불 단말기로서 작동하는 마이크로제어기(12) 내로 로딩된다. 어떤 지불 카드 데이터가 로딩되는지는 사용자의 선택에 달려 있다.

[0074] 지불 POS 단말기 어플리케이션이 자체적으로 시작되기 전에, 부트-로더(9)는 지불 POS 단말기 어플리케이션의 변경 제어(change control)를 실행한다. 키보드 및 이동 통신 디바이스(4)의 디스플레이를 이용하여, 지불 POS 단말기 어플리케이션이 관리된다. 휴대폰은 사용자, 메모리 카드(1) 및 HOST 프로세서 간의 통신을 가능하게 하는 그래픽 GUI(Graphic User Interface) 인터페이스를 갖는다. 또한, 상기 폰에 SMS 푸시(push) 기술이 존재한다. 지불 POS 단말기 어플리케이션은 마이크로SD 메모리 카드(1) 상에서 지불 어플리케이션을 이용하여 온라인 및 오프라인 지불들을 가능하게 하는 SD 마이크로제어기 어플리케이션(12)이다. 지불은 "카드는 존재한다(Card is present)"는 것으로서 실현되며, 이는 보안을 매우 증가시킨다 - 트랜잭션은 암호로 서명되고, 각각의 트랜잭션 동안 ATC 카운터가 하나씩 증가하며, 이는 몇몇 키들을 얻기 위해 무제한 횟수의 트랜잭션들을 생성하는 것이 불가능함을 의미한다. 클라이언트는 자신의 폰에 설치되는 GUI 어플리케이션을 통해 지불 POS 단말기 어플리케이션을 관리한다. 이 예시에서, 지불 POS 단말기 어플리케이션은 마이크로제어기(12)와 함께 제네릭 POS 단말기를 형성한다. 상이한 구성에서, 제네릭 POS 단말기는 보안 요소를 갖는 칩에 직접 존재하는 연산 요소와 함께 지불 POS 단말기 어플리케이션으로 형성될 수 있다. 후속하여, 구성 파라미터들과 함께, 이들은 EMBEDDED POS TERMINAL(임베디드 POS 단말기): Terminal_type(단말기_타입) 1x = 금융 기관에 속하는 단말기, 2x = 상인에 속하는 단말기, 3x = 카드 소지자에 속하는 단말기 - 카드 소지자 단말기를 형성한다. 단말기의 구성 데이터 유닛(6)은 단말기의 ID 번호, PDOL(Processing Option Data Object List) 데이터, Terminal Risk Management(단말기 위험 관리), 오프라인 뱃치 파일 포맷(off-line batch file format), HOST의 SMS 게이트, HOST의 IP 어드레스, 오프라인 트랜잭션에 서명하는 코드를 포함한다. 지불들은 오프라인 또는 온라인일 수 있다. SMS 메시지들 또는 GPRS를 통해 지불 프로세서와의 통신이 실현될 수 있다.

[0075] 제 3 예시

[0076] 지불의 실현에 필요한 최소 세트만을 포함하는 착탈식 메모리 카드(1)가 이 예시에 설명된다. 그 구조는 도 4에 도시되어 있다. 이러한 종류의 착탈식 메모리 카드는 사전-입력된 금액을 갖는 선불 카드로서만 판매되도록 설계되며, 예를 들어 상이한 화폐를 갖는 국가로부터 온 관광객에게 판매되도록 의도된다. 착탈식 메모리 카드(1)는 마이크로SD 사양에 따른 접촉부를 갖는 인터페이스(11)를 포함한다. 착탈식 메모리 카드(1)의 플라스틱 몸체에 2 개의 보안 요소들(31, 32)이 존재한다. 제 1 보안 요소(31)에는 선불 카드 시스템의 운영자에 의해

생성된 POS 단말기의 구성 데이터가 존재한다. 제 2 보안 요소(32)에는 일회용 지불 카드의 데이터가 존재한다. 착탈식 메모리 카드(1)와 함께, 상업용 패키지는 지불 카드로의 접근의 관리를 위한 대응하는 PIN 코드가 존재하는 스크랩 필드(scrap field)를 갖는 페이퍼 캐리어(paper carrier)도 포함한다. 메모리 카드(1)는 지불하는 고객의 지불 카드에 연결될 때, 상인이 보유한 통상적인 POS 단말기로서 모든 작동들을 수행한다. 휴대폰(4)의 설비는 디스플레이 및 통신을 위해 사용된다.

[0077] 제 4 예시

[0078] 이 예시에서, 시스템은 지불 POS 단말기의 어플리케이션 이니시에이터(22)로 보충된다. 이는 NFC 통신 요소를 갖는 단일 목적 디바이스의 형태일 수 있다. 이 예시에서, 이니시에이터는 금전 등록기의 출력부에 연결되며, 이는 요청된 총 지불에 관한 정보를 출력부로 송신할 것이다. 이니시에이터(22)는 지불 값, 상인의 계좌에 관한 정보 및 요청 명령을 포함하는 파일을 생성한다. 이니시에이터(22)는 이 파일을 통신 요소(24)를 통해 이에 적용되는 휴대폰(4)으로 송신한다. 메모리 카드(1)의 이 파일의 수신은 지불 POS 단말기 어플리케이션의 개시를 유도한다. 이 해결책은 자신의 POS 단말기를 갖지 않는 보통의 상점들에서 자동 이체 지불을 위해 사용자의 휴대폰(4)에서 지불 단말기를 사용하게 할 수 있다.

[0079] 제 5 예시

[0080] 이 예시에서는 도 3, 도 7 및 도 8에 도시된 바와 같은 시스템이 설명되고, 상인 편에 단일 목적 박스(one-purpose box)의 형태로 판매 디바이스(28)가 위치되며, 이는 숫자 키보드(36), 디스플레이(37), 및 재충전가능한 어큐뮬레이터(accumulator)의 형태인 자체 전력원을 갖는다. 판매 디바이스(28)는 상부 커버의 표면 아래에 안테나(21)를 갖는 NFC 통신 요소(35)를 가지며, 안테나(21)의 중심은 타겟의 안내 심볼(40)로 그래픽적으로 도시된 커버 외부에 존재한다. SAM 카드(42)의 하드웨어에서, 판매 디바이스(28)는 보안 요소(6)를 포함하며, 이 안으로 POS 지불 단말기(27) 식별 및 통신된 데이터의 암호화를 위한 마스터 키가 로딩된다. 다른 버전에서, 데이터는 판매 디바이스(28)의 인쇄 회로의 보호된 메모리에 직접 로딩될 수 있다.

[0081] 상인은, 팔 때에 키보드(36)를 통해 디스플레이(37)로 상품에 대해 원하는 총액을 입력하는 방식으로 판매 디바이스(28)를 사용한다. 디스플레이(37) 상의 총액을 체크한 후, 상인은 확인 버튼을 누른다. 이 행동 후, 마스터 키를 이용하여 POS 지불 단말기(27)의 식별 데이터가 암호화되고, 이 암호화 데이터는 지불 총액과 함께 NFC 통신 요소(35)로 송신되며, 이는 안테나(41)를 통해 암호화된 메시지를 송신하고, 이동 통신 디바이스(4)가 판매 디바이스(28)에 배치될 것을 기대한다. 그의 이동 통신 디바이스(4)에서, 고객은 특정한 하드웨어 키보드 또는 소프트웨어 버튼을 통해 지불 어플리케이션의 실행을 활성화한다. NFC 통신 채널의 생성 후, 판매 디바이스(28)로부터 암호화된 데이터가 판독되고 암호 해독되며, 이 결과는 POS 단말기(27) 식별 데이터 및 요청된 지불 총액이다.

[0082] 또한, 이 전달의 부분은

[0083] $3DES[Mk\{Cfg\}] \xrightarrow{NFC} 3DES^{-1}[Mk\{Cfg\}]=Cfg$ 로서 표현될 수 있으며,

[0084] 여기서, 3DES는 TDEA(Triple Data Encryption Algorithm: 트리플 데이터 암호화 알고리즘)를 통한 암호화를 의미하고, Mk는 지불 프로세서에 의해 공급된 마스터 키이며, Cfg는 구성 데이터를 의미하고, NFC는 판매 디바이스와 착탈식 메모리 카드 간의 전달 경로를 나타낸다.

[0085] 지불된 총액은 고객에 의해 그의 이동 통신 디바이스(4)의 디스플레이 상에서 검증될 수 있다. 판매 디바이스(28)로부터의 식별 데이터가 착탈식 메모리 카드(1)의 평범한 상태의 POS 단말기(27)에 제공되어, 주어진 상인을 위한 특정한 POS 지불 단말기(27)가 되게 한다.

[0086] 이 프로세스는

[0087] $Cfg + Generic\ POS = ACg\ POS$ 으로 표현될 수 있으며,

[0088] 여기서, Generic POS는 평범한 상태의 포괄적인 POS의 식별을 나타내고, ACg POS는 해당 상인의 POS이다.

[0089] 후속하여, 지불 단말기 어플리케이션은 예를 들어 EMV 표준을 따라 정상적인 방식으로 실행된다. 지불 카드(7)의 사전설정된 위험 관리에 따라, 그리고 지불되는 총액의 정도(the height of the amount)와 관련하여, 패

스워드, PIN 코드를 입력하는 것이 요청될 수 있으며, 이는 이동 통신 디바이스(4)의 키보드로 고객에 의해 입력된다. 이러한 방식으로, 지불 단말기 어플리케이션이 착탈식 메모리 카드(1)에서 직접 실행되기 때문에 높은 수준의 보안에 도달하고, 여기에 지불 카드(7) 유닛들도 저장되며, 중요 데이터는 판매 디바이스(28)와 착탈식 메모리 카드(1) 간의 연결의 하드웨어를 떠나지 않는다. 지불 어플리케이션의 결과는 지불 암호의 생성이며, 이는 판매 디바이스(28)로 송신되고, 온라인 지불의 경우에는 인터페이스(11)를 통해 이동 통신 디바이스(4)로 송신되며, 후속하여 모바일 네트워크를 통해 지불 프로세서로 송신된다. 또한, 지불 암호가 생성될 수 있으며, 다음의 관계:

[0090] $3DES[Mk\{Transaction\}] \xrightarrow{NFC}$ 에 따라 송신되며, 적절하게는

[0091] $3DES[Mk\{\ Transaction\ \}] \xrightarrow{GPRS}$ 로서 지불 프로세서 편으로 송신된다.

[0092] 이 경우, 착탈식 메모리 카드는 마이크로SD 카드의 형태이다.

[0093] 제 6 예시

[0094] 이 예시에서, 도 4에 따르면 판매 디바이스(28)는 대응하는 포맷의 리더기를 갖는 ICC 카드(29)의 삽입을 위한 슬롯을 갖는 디바이스의 형태이다. 상인은 판매 디바이스(28)를 어디에서도 살 수 있으며, 이 판매 디바이스(28)는 자신의 아이덴티티를 갖지 않는다. 상인은 은행 또는 지불 프로세서로부터 ISO 7810 85.60 × 53.98 mm에 따라 공통 파라미터들의 ICC 카드(29)를 받는다. 해당 상인에게 할당하기 위한 POS 단말기의 식별 데이터 및 지불 프로세서의 마스터 키가 ICC 카드 칩의 보안 요소에 로딩된다. ICC 카드(29)를 리더기에 삽입함으로써, 앞선 설명에 따른 판매 디바이스(28)가 생성된다. 또한, 판매 디바이스(28)는 미니-B USB 커넥터(39)를 포함하며, 이를 통해 확장된 구성으로 프린터, 컴퓨터 및 다른 출력 또는 입력 유닛들을 연결시킬 수 있다. 판매 디바이스(28)를 포함하고 작동하는 것(attendance and operation)은 첫 번째 경우와 유사하지만, 그 변화를 실현한 후, 상인이 그의 ICC 카드(29)를 꺼내고, 예를 들어 오프라인 지불들의 처리를 위해 은행에 이를 가져갈 수 있다는 점에서 상이하다. 또한, 이는 ATM 기계들에서의 이러한 종류의 ICC 카드(29)의 직접적인 처리를 배제하지 않는다. 또한, 이 해결책은 ICC 카드가 작동이 쉽고, 실제 파라미터(practical parameter)들로 되어 있으며, 판매 디바이스(28)로부터 이를 빼냄으로써 예를 들어 한밤중 등에 영업소들로부터 그 카드의 절도가 방지된다는 사실에서 장점을 갖는다. 또한, ICC 카드(29)는 단순한 리더기를 갖는 컴퓨터에 데이터의 백업 및 후속 작업을 위한 영역을 제공한다.

[0095] 또한, 이 예시에 따른 구성의 장점은 리더기, 디스플레이(37) 및 키보드(36)를 갖는 하나의 디바이스가 하나의 영업소에서 교대로 일하는 여러 상인들에 의해 사용될 수 있는 한편, 그 순간에 ICC 카드(29)를 리더기에 삽입한 해당 상인을 위해 지불이 처리되는 가능성이다.

[0096] 제 7 예시

[0097] 이전의 예시들에 언급된 요소들 이외에도, 도 5에 따른 판매 디바이스(28)는 RS232(Recommended Standard 232) 인터페이스를 포함하며, 이를 통해 금전 등록기(26)에 연결될 수 있다. 이 예시에서, 판매 디바이스(28)는 기본적으로 POS 단말기(27)에 대한 상인의 기존 금전 등록기(26)의 연장인 한편, 지불 단말기 어플리케이션은 다시 착탈식 메모리 카드(1)에서 실행되며, 이는 이동 통신 디바이스(4)와 함께 고객에 의해 보유된다.

[0098] 케이블 연결(38)을 통해, 금전 등록기(26)로부터의 결과는 판매 디바이스(28)로 전달되고, 이는 디스플레이(37)에 나타나며, 상인이 확인 버튼에 의해 이를 확인한다. 후속하여, 프로세스는 지불된 총액이 판매 디바이스(28)의 키보드(36)를 통해 입력되었던 경우와 동일한 방식으로 실행된다. 이 연결에서, 판매 디바이스(28)는 지불된 총액의 입력를 위해 키보드(36)를 포함하지 않아도 되지만, 다양한 시스템에서의 판매 디바이스(28)의 유용성으로부터, 키보드(36)는 이 예시에서 판매 디바이스(28)의 일부분이다.

[0099] 제 8 예시

[0100] 도 11 내지 도 14에 따른 이 예시에서는, 착탈식 메모리 카드(1)가 마이크로SD 카드의 형태인 시스템이 설명된다. 이 예시에서는 그 위에 2 개의 보안 요소들(3)이 위치되며, 이때 하나의 보안 요소(3)는 지불 카드 유닛

(7)에 대해, 또는 상이한 발행사들로부터의 여러 지불 카드 유닛들(7) 각각에 대해 설계되며, 제 2 보안 요소(3)는 지불 단말기 유닛(5)을 포함한다. 다른 예시에서, 착탈식 메모리 카드(1)는 로컬화되는 지불 단말기 유닛(5) 없이 단 하나의 지불 카드 유닛(7)만을 포함할 수 있다.

[0101] 통상적인 플래시 메모리(2)를 갖는 착탈식 메모리 카드(1)는 통상적인 마이크로SD 표준의 인터페이스(11)를 가지며, 이동 통신 디바이스(4)의 슬롯으로 삽입된다. 이는 확장 메모리들의 삽입을 위해 설계된 통상적인 슬롯이다.

[0102] 이 예시에서, 안테나(21)를 갖는 NFC 통신 요소(13)가 착탈식 메모리 카드(1)에 위치된다. 이동 통신 디바이스(4)는 키보드(45) 옆에 위치된 지불 버튼(44)을 갖는다. 지불 버튼(44)은 이동 통신 디바이스(4) 상의 마이크로스위치와 연결된다. 마이크로스위치의 특정한 실현(specific realization)은 중요하지 않으며, 예를 들어 멤브레인 스위치(membrane switch), 커패시티 스위치(capacity switch) 및 유사한 것과 같이 상이한 형태일 수 있다.

[0103] 지불 버튼(44)은, 적어도 이동 통신 디바이스(4)에 이 종류의 지불 버튼(44)이 장착되는 경우, 착탈식 메모리 카드(1)의 접근 모드의 변경에 대해 유일하게 허용가능한 명령은 지불 버튼(44)의 접촉으로부터 이루어지는 방식으로 펌웨어에 연결된다. 동일한 착탈식 메모리 카드(1)가 목적 하드웨어 지불 버튼(44)을 갖지 않는 이동 통신 디바이스(4)의 슬롯으로 삽입될 경우, 접근 모드의 변경은 이동 통신 디바이스(4)의 디스플레이(46) 상의 메뉴를 통해 실현될 것이다. 이러한 경우, 착탈식 메모리 카드(1)는 두 접근 모드에서 기능하는(functional) 것이지만, 이동 통신 디바이스(4)와의 전체 연결은 지불에 있어서 더 낮은 수준의 보안을 가질 것이다.

[0104] 지불 버튼(44)이 장착되는 휴대폰에서, 지불 버튼(44)과 연결된 사전정의된 펌웨어를 통하는 것과 다른 어떠한 방식에 의해 착탈식 메모리 카드의 보안 요소(3)에 접근하는 것은 불가능할 것이다. 이 예시에서, 이는 LGM 어플리케이션일 것이다.

[0105] 두 접근 모드들은 다음의 특성을 가질 수 있다:

표 1

[0106]

기능	메모리 확장 접근 모드	지불 기능용 접근 모드
파일들의 판독/기록	YES	YES
NFC 통신	NO	NO
확장된 접근(SDIO...)	휴대폰에 따라 YES/NO	YES
휴대폰의 어플리케이션으로부터 SE로의 접근	NO	YES
플래시 내의 파일 캐시 메모리	휴대폰에 따라 YES/NO	NO
카드의 영구적인 전력공급	휴대폰에 따라 YES/NO	YES

[0107] 지불 기능의 접근 모드에서, 착탈식 메모리 카드(1)의 파일들의 캐싱(caching)은 꺼질 것이며, 플래시 메모리(2)로의 접근 및 파일 시스템으로의 접근은 지원될 것이다.

[0108] 이동 통신 디바이스(4)가 더 높은 통신 인터페이스, 예를 들어 SDIO(Secure Digital Input Output) 표준, McEX를 지원할 수 있을 경우, 대응하는 인터페이스는 지불 기능의 접근 모드에도 접근가능할 것이다.

[0109] 산업적 이용가능성

[0110] 산업적 이용가능성은 명백하다. 본 발명에 따르면, 메모리 카드에 구현된 지불 단말기들을 산업적으로 및 반복적으로 제조하고 사용할 수 있으며, 이는 하나의 메모리 카드에 하나 또는 그 이상의 지불 카드들을 갖는다. 또한, POS 지불 단말기를 생성하고 사용할 수 있으며, 이는 판매 디바이스와 이동 통신 디바이스의 연결에 의하여 특정한 지불을 위해 임시로 생성된다. 그 후, 상인의 POS 단말기의 필수 구조들은 지불하는 사용자의 이동 통신 디바이스 내의 착탈식 메모리 카드와의 연결이 실현된 후에만 생성된다.

[0111] 이 해결책에 따르면, 이동 통신 디바이스의 하드웨어 지불 버튼의 도입도 산업적으로 및 반복적으로 제조할 수 있으며, 이때 이 버튼은 착탈식 메모리 카드의 현재 접근 모드의 선택자(selector)를 나타낸다.

부호의 설명

[0112] 1- 메모리 카드

2- 메모리

3- 보안 요소

31- POS 단말기의 보안 요소(Secure Element)

32- 지불 카드의 보안 요소

4- 이동 통신 디바이스

5- 지불 POS 단말기 어플리케이션

6- 단말기의 구성 데이터 유닛

7- 지불 카드 유닛

8- 운영 체제 유닛

9- 부트-로더 유닛

10- 내부 마이크로제어기 메모리

11- 인터페이스

12- 마이크로제어기

13- 통신 요소

14- 암호화 유닛

15- 자유롭게 접근가능한 사용자의 데이터 공간

16- 비-금융 어플리케이션 유닛

17- 플래시 메모리 제어기

18- 웹 서버 유닛

19- 다운로드 관리 유닛

20- 숨겨진 데이터 공간

21- 안테나

22- 이니시에이터

23- 지불 수신인의 컴퓨터

24- 이니시에이터의 통신 요소

25- 지불 처리 본부

26- 금전 등록기

27- POS 지불 단말기

28- 판매 디바이스(Sales Device)

29- ICC 카드

35- 판매 디바이스 통신 요소

36- 키보드

37- 디스플레이

38- 금전 등록기에 대한 연결

39- 외부 커넥터

40- 타겟 심볼

41- 판매 디바이스 안테나

42- SAM 카드

43- 임시 무접촉 연결

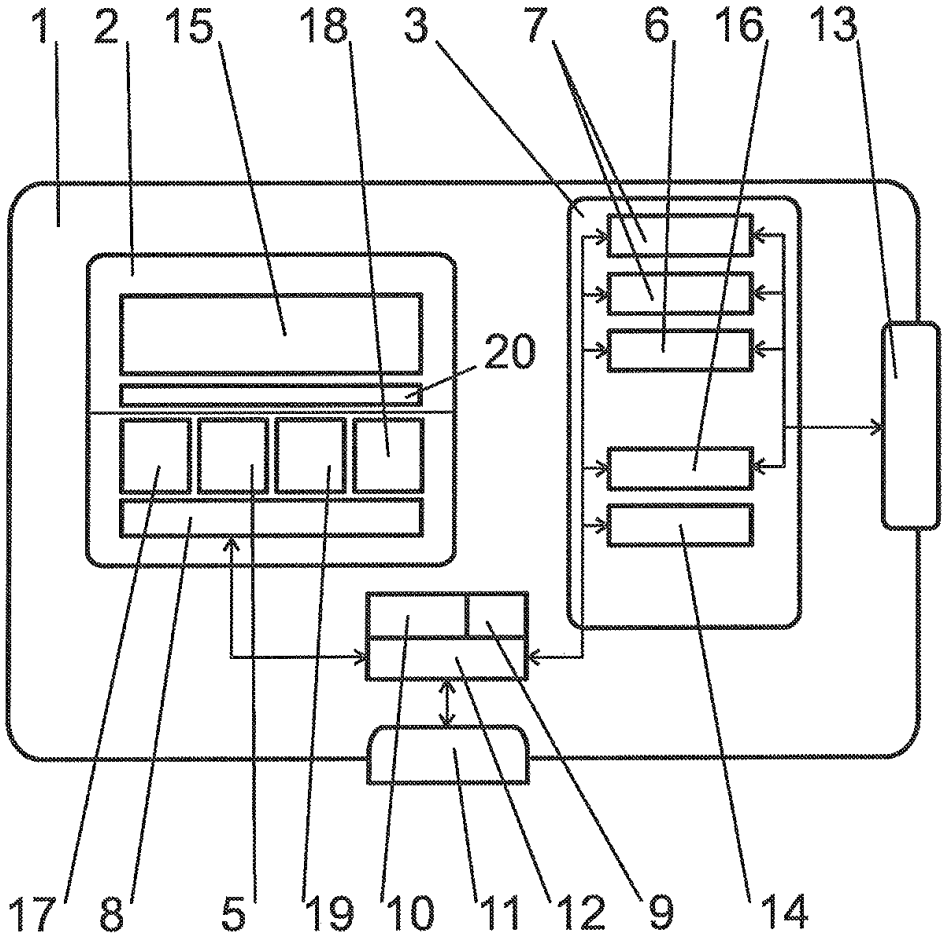
44- 지불 버튼

45- 이동 통신 디바이스의 키보드

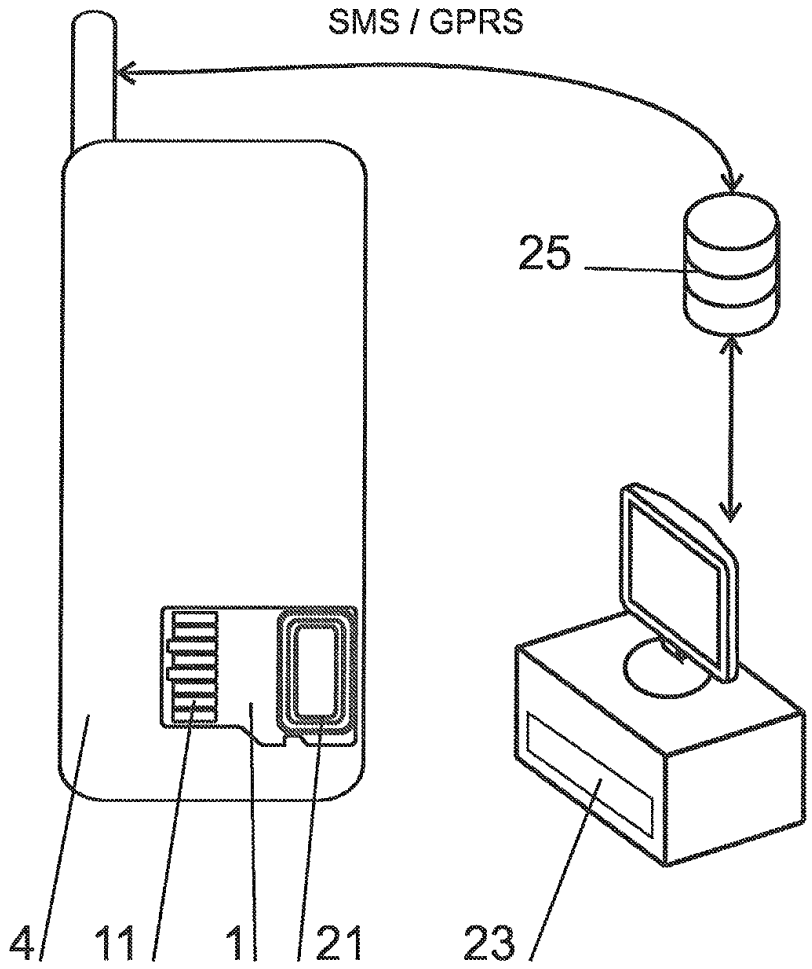
46- 디스플레이

도면

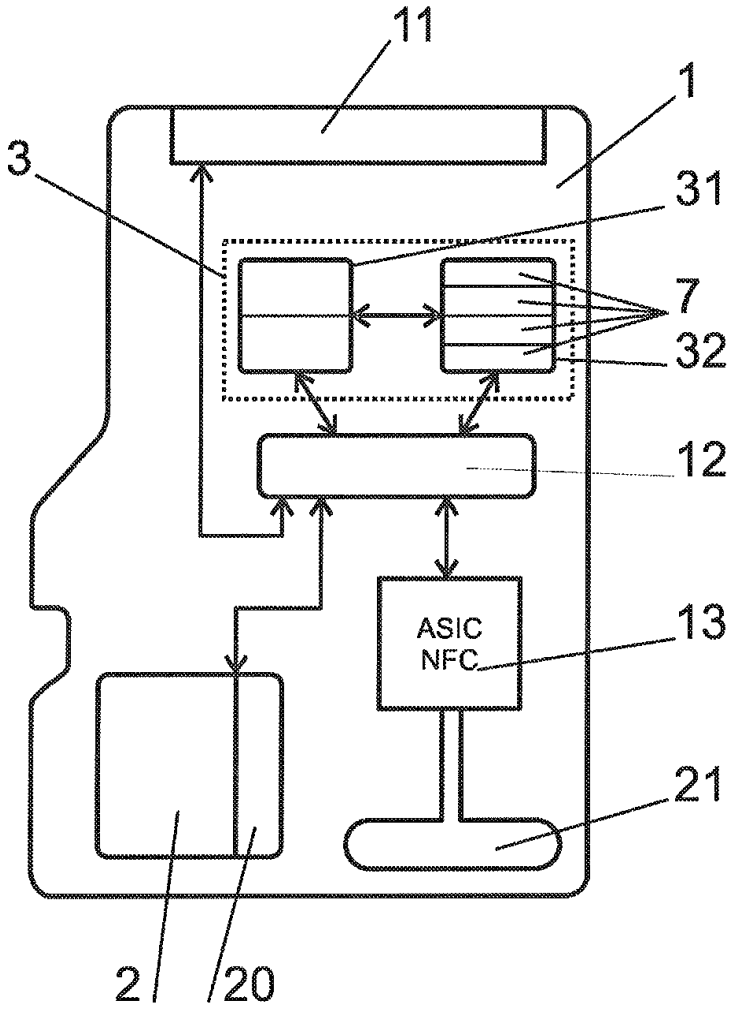
도면1



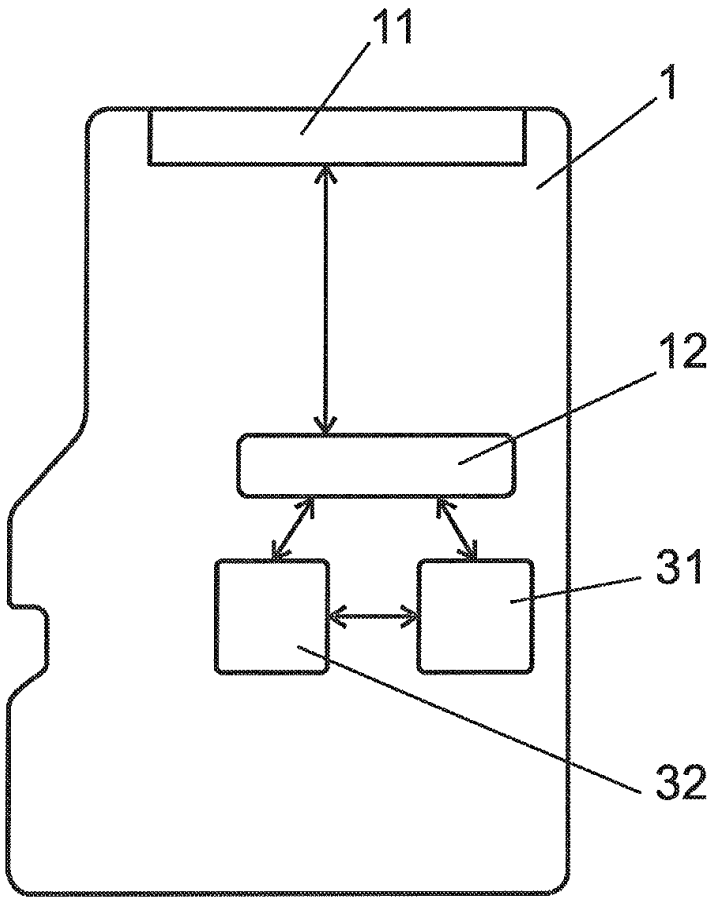
도면2



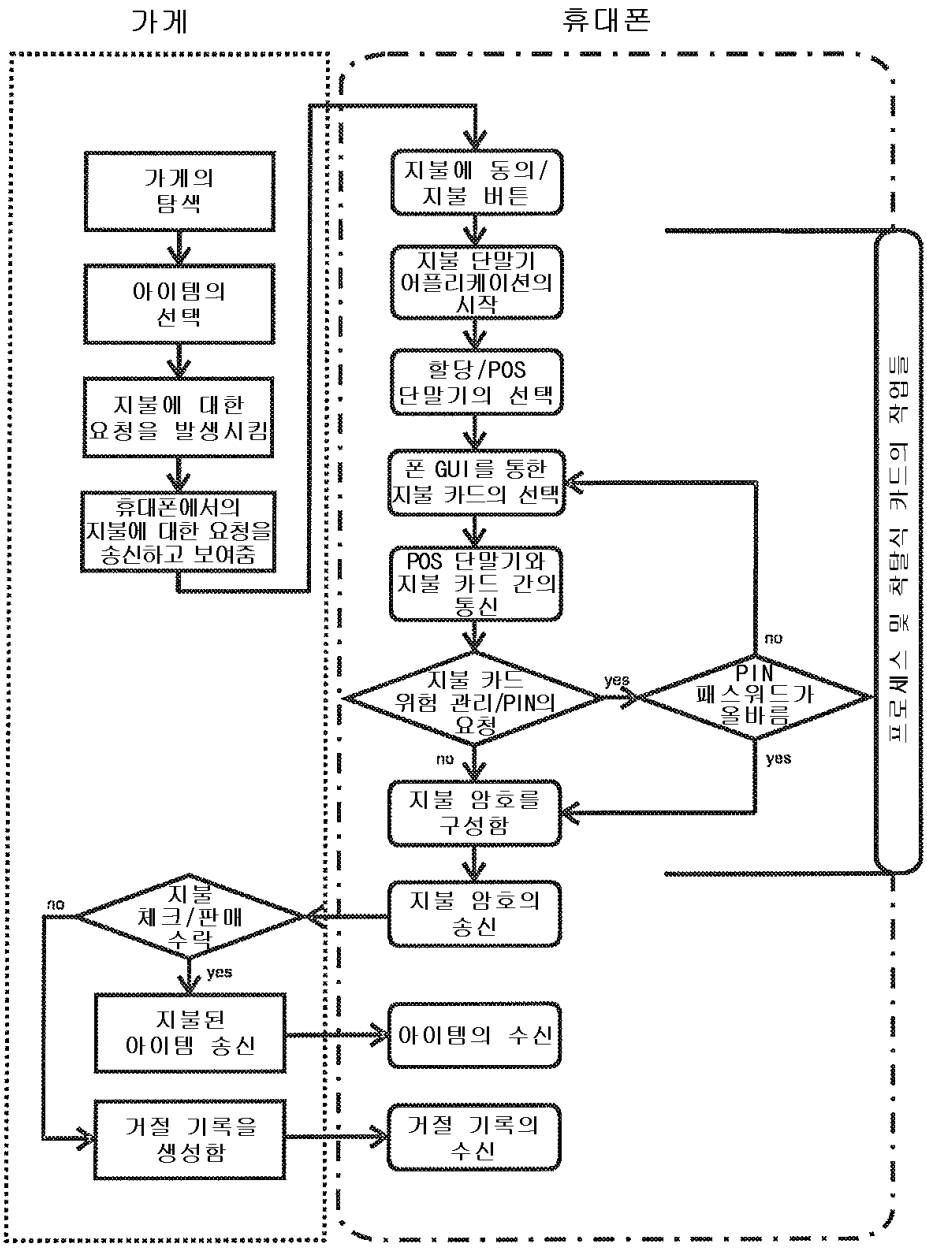
도면3



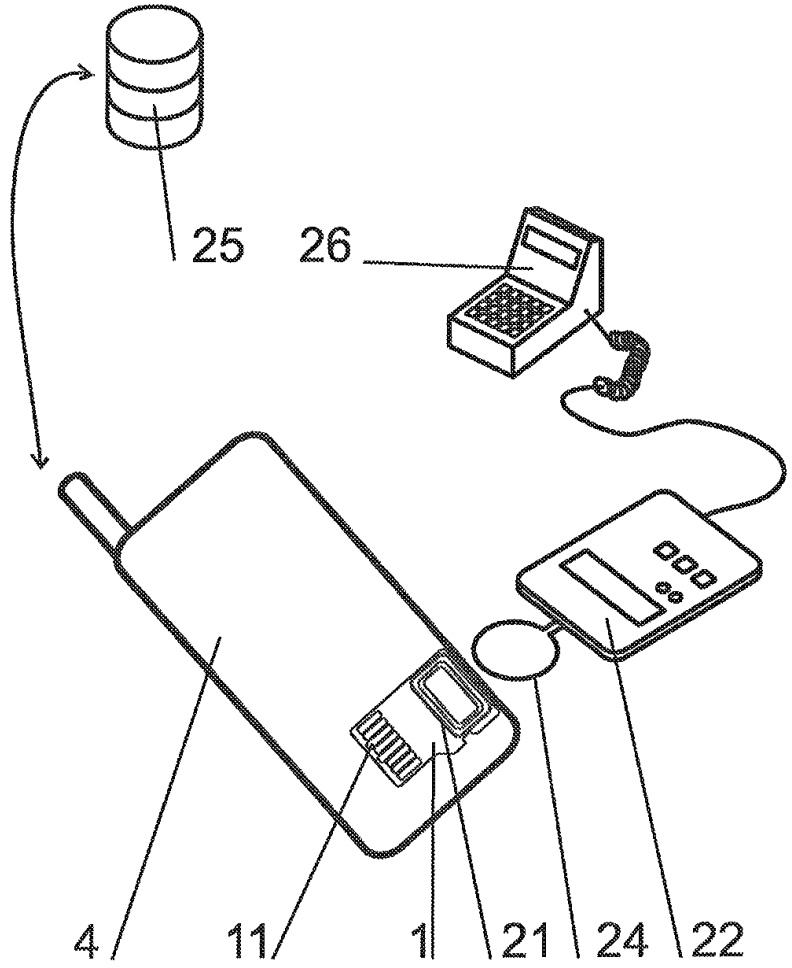
도면4



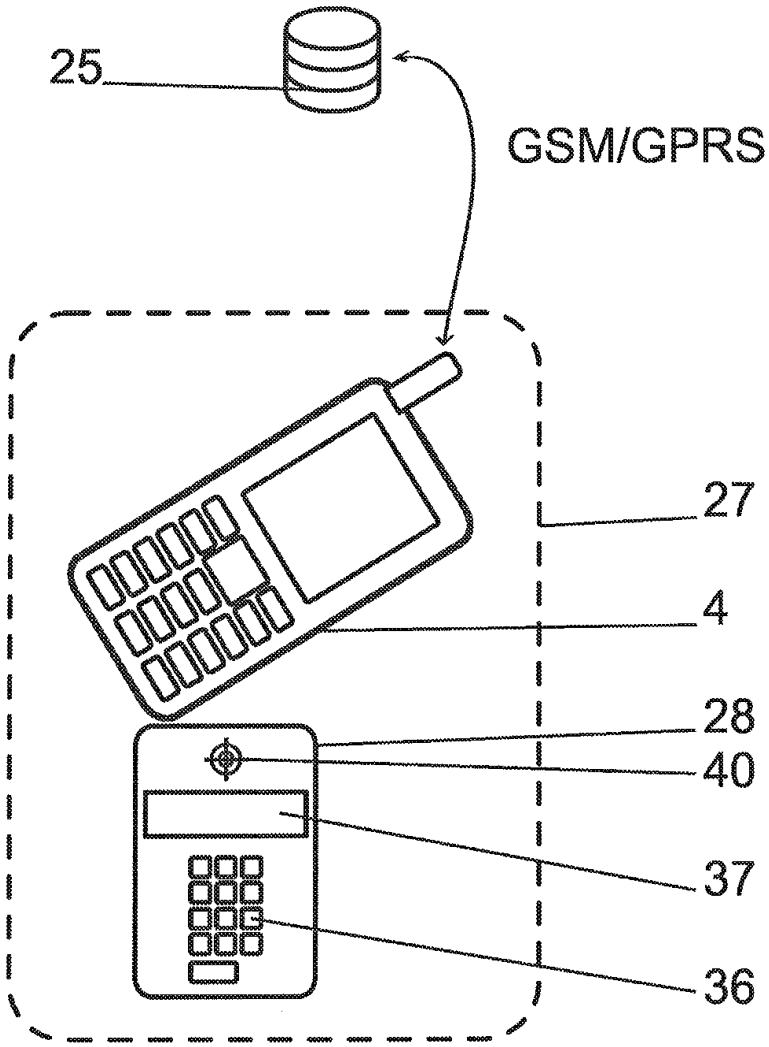
도면5


가게
휴대폰
가게의 탐색
아이템의 선택
지불에 대한 요청을 발생시킴
휴대폰에서의 지불에 대한 요청을 송신하고 보여줌
지불에 동의/지불 버튼
지불 단말기 어플리케이션의 시작
할당/POS 단말기의 선택
폰 GUI를 통한 지불 카드의 선택
POS 단말기와 지불 카드 간의 통신
지불 카드 위험 관리/PIN의 요청
yes
PIN 패스워드가 올바름
no
yes
no
지불 암호를 구성함
지불 암호의 송신
지불 체크/판매 수락
no
yes
지불된 아이템 송신
아이템의 수신
거절 기록을 생성함
거절 기록의 수신
프로세스 및 착탈식 카드의 작업들

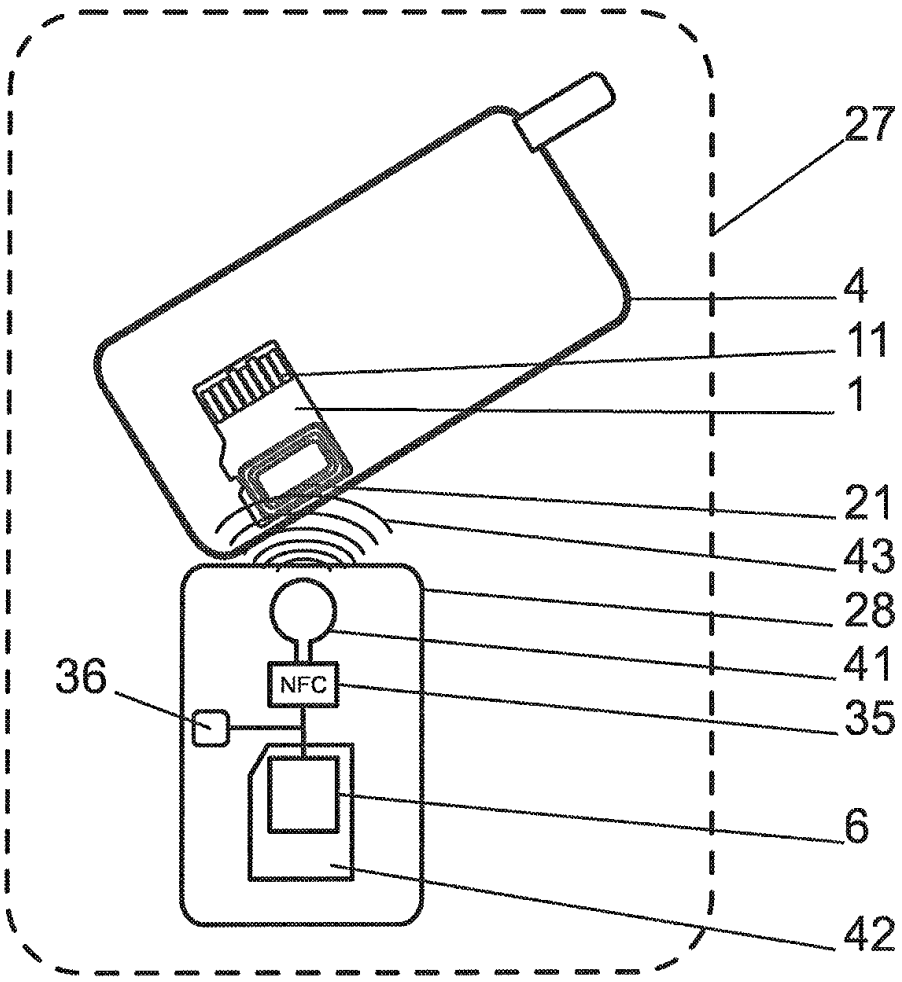
도면6



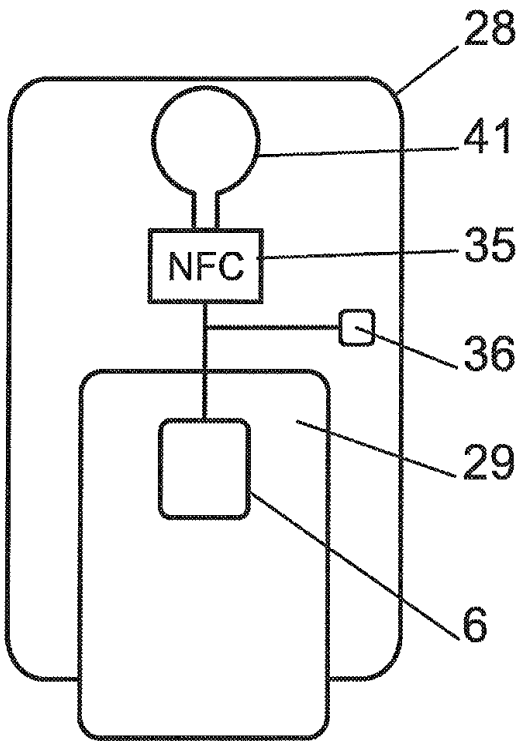
도면7



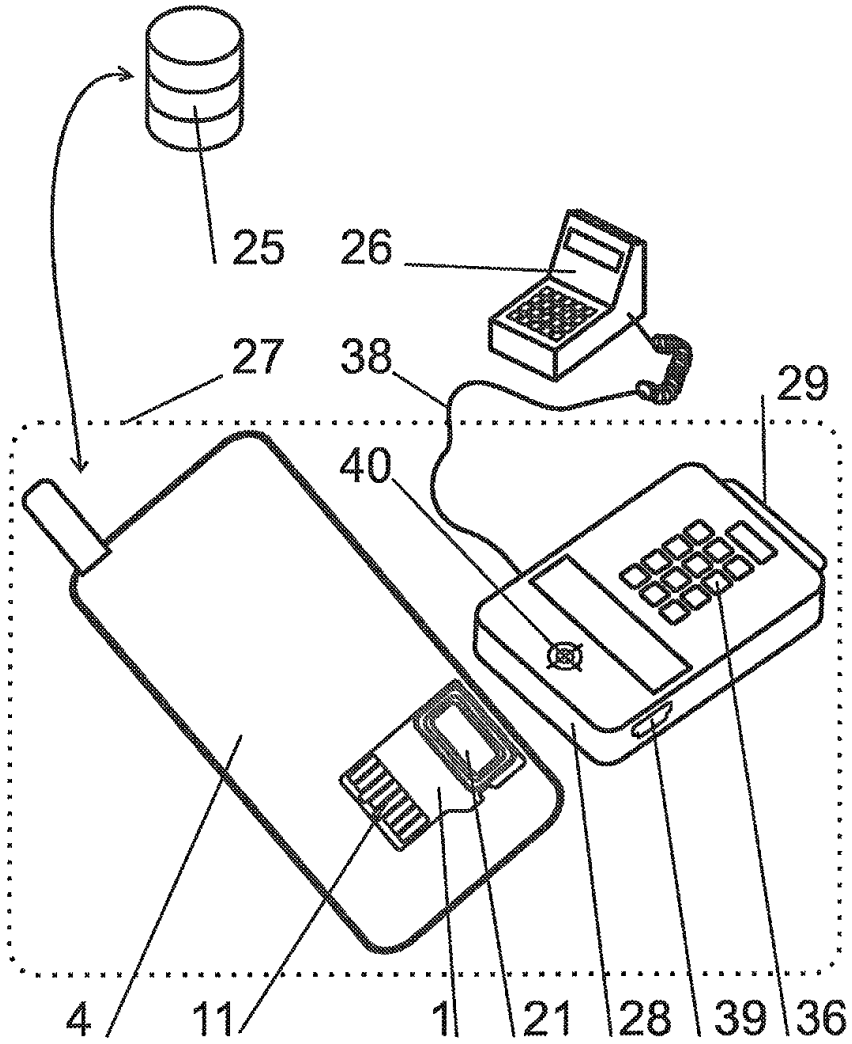
도면8



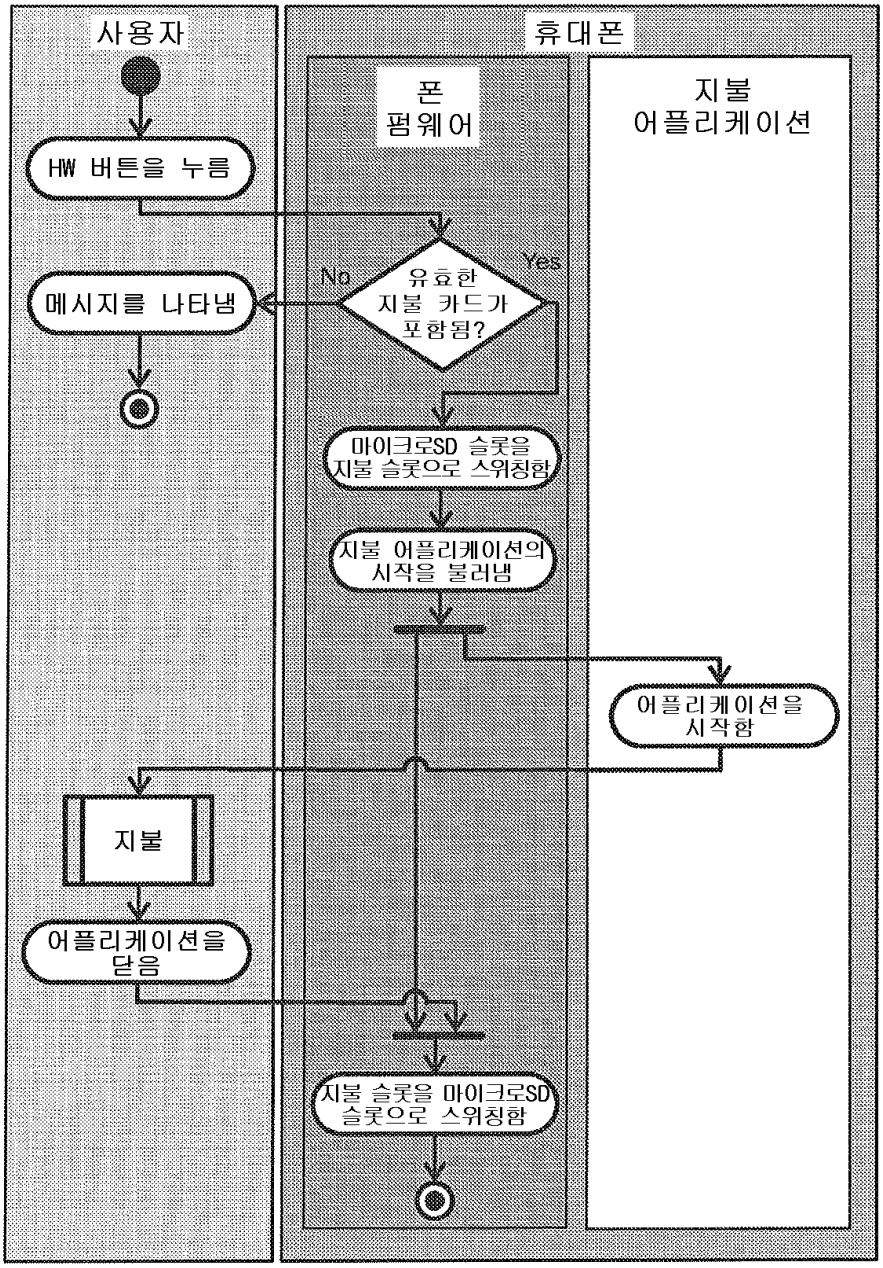
도면9



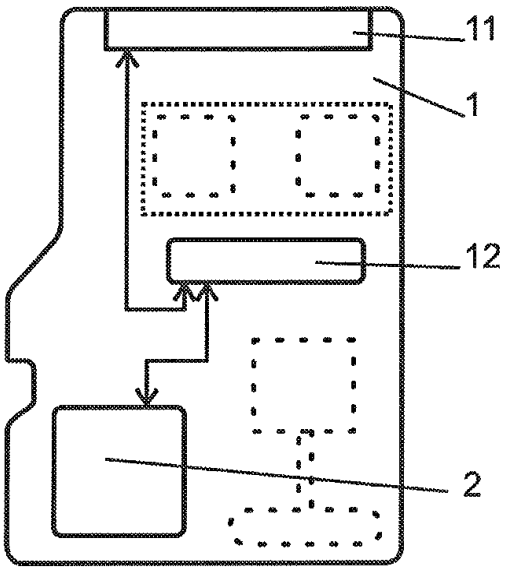
도면10



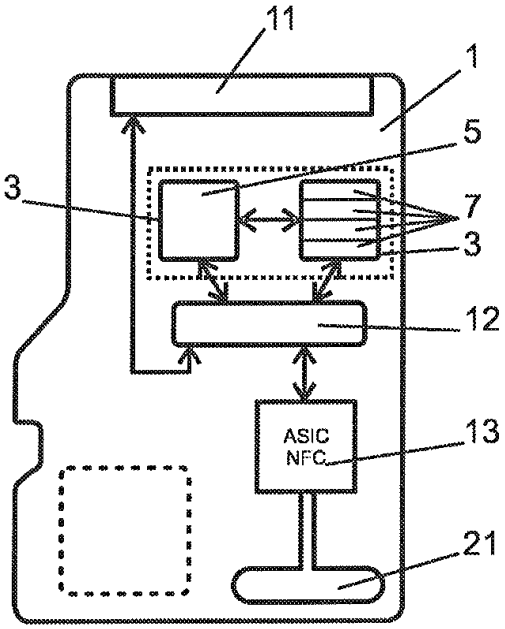
도면11


사용자
휴대폰
폰 펌웨어
지불 어플리케이션
HW 버튼을 누름
No
유효한 지불 카드가 포함됨?
Yes
메시지를 나타냄
마이크로SD 슬롯을 지불 슬롯으로 스위칭함
지불 어플리케이션의 시작을 불러냄
어플리케이션을 시작함
지불
어플리케이션을 닫음
지불 슬롯을 마이크로SD 슬롯으로 스위칭함

도면12



도면13



도면14