(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년12월22일
(11) 등록번호 10-0933387
(24) 등록일자 2009년12월14일

(51) Int. Cl.
G06Q 20/00 (2006.01)
(21) 출원번호 10-2002-7014247
(22) 출원일자 2001년04월24일
심사청구일자 2006년04월07일
(85) 번역문제출일자 2002년10월24일
(65) 공개번호 10-2003-0019361
(43) 공개일자 2003년03월06일
(86) 국제출원번호 PCT/US2001/013382
(87) 국제공개번호 WO 2001/82246
국제공개일자 2001년11월01일
(30) 우선권주장
60/199,727 2000년04월24일 미국(US)
(56) 선행기술조사문헌
KR1019960706141 A*
KR1020000012391 A*
WO9946881
US6016476
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
비자 인터내셔날 써비스 어쏘시에이션
미합중국 94404 캘리포니아주 포스터시티 메트로 센터 보우리바드 900
(72) 발명자
웰러,케빈디.
미국,캘리포니아94117, 샌프란시스코,콜레스트리트717
라이언,스티븐더블유.
미국,캘리포니아94019,해프문베이,이글트레이스드라이브376
(뒷면에 계속)
(74) 대리인
강명구, 강석용

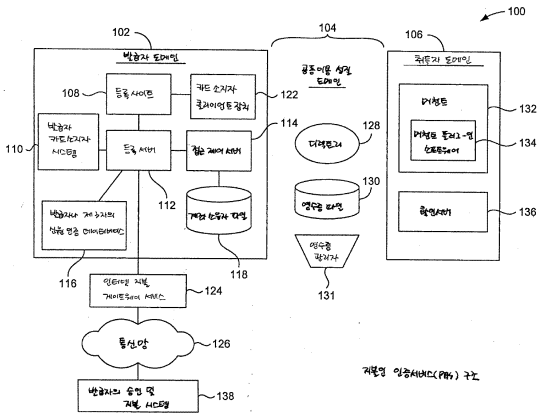
전체 청구항 수 : 총 29 항 심사관 : 이해평

(54) 온라인 지불인 인증 서비스

(57) 요 약

지불인증 서비스는 온라인 거래중 지불인의 신원을 인증한다. 본 발명의 인증 서비스에서는 비밀번호 이용처럼 다양한 인증 방법을 이용하여 카드소지자의 신원을 카드발급자가 확인할 수 있다. 또한, 인증서를 필요로하는 시스템 구성원은 오직 발급 금융회사이다. 온라인 거래 중 카드소지자의 신원을 인증하기 위한 발명의 한가지 실시예는 카드소지자가 지불 승인 서비스에 등록되어 있는 지 결정하기 위해 접근제어서버에 질의하는 과정을 포함하고, 카드소지자로부터 비밀번호를 요청하고, 비밀번호를 확인하며, 카드소지자 인증이 확인되었는지 여부를 머천트에게 알린다. 발명의 또다른 태양에서는 칩카드와 인증 서비스가 독립적으로 암호문을 발생시키며, 정확한 칩카드가 카드소지자에 의해 이용되고 있음을 상기 서비스가 확인하기 위해 이 두 암호문이 일치되어야 한다.

대 표 도



(72) 발명자

힐,피터알.

미국,캘리포니아93108,몬테시토,테이버레인678

매니시스,토마스제이.

미국,캘리포니아94044,퍼시피카,로시타로드1481

도밍게스,베네딕토에이치.

미국,캘리포니아94066,
산브루노,메리온드라이브2830

루이스,토니디.

미국,캘리포니아94552
카스트로밸리,데니슨플레이스7533

브레이,피터

미국,캘리포니아94552,카스트로밸리,에드윈마크햄
드라이브19701

(81) 지정국

국내특허 : 아랍에미리트, 안티구와바부다, 알바니아, 아르메니아, 오스트리아, 오스트레일리아, 아제르바이잔, 보스니아 헤르체고비나, 바베이도스, 불가리아, 브라질, 벨라루스, 벨리즈, 캐나다, 스위스, 중국, 쿠바, 체코, 독일, 덴마크, 도미니카, 알제리, 에스토니아, 스페인, 핀란드, 영국, 그루지야, 헝가리, 이스라엘, 아이슬랜드, 일본, 케냐, 키르키즈스탐, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 리베이라, 레소토, 리투아니아, 룩셈부르크, 라트비아, 모로코, 몰도바, 마다가스카르, 마케도니아공화국, 몽고, 말라위, 멕시코, 모잠비크, 노르웨이, 뉴질랜드, 폴란드, 포르투칼, 루마니아, 러시아, 수단, 스웨덴, 싱가포르, 슬로베니아, 슬로바키아, 타지키스탄, 투르크맨, 터어키, 트리니아드토바고, 탄자니아, 우크라이나, 우간다, 미국, 우즈베키스탄, 베트남, 남아프리카

AP ARIPO특허 : 가나, 감비아, 케냐, 레소토, 말라위, 수단, 시에라리온, 스와질랜드, 우간다, 짐바브웨

EA 유라시아특허 : 아르메니아, 아제르바이잔, 벨라루스, 키르키즈스탐, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크맨

EP 유럽특허 : 오스트리아, 벨기에, 스위스, 사이프러스, 독일, 덴마크, 스페인, 핀란드, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투칼, 스웨덴

OA OAPI특허 : 부르키나파소, 베닌, 중앙아프리카, 콩고, 코트디브와르, 카메룬, 가봉, 기니, 기니 비사우, 말리, 모리타니, 니제르, 세네갈, 차드, 토고

특허청구의 범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

제 3 자와의 온라인 거래 중 계좌를 이용하는 고객이 상기 계좌의 실제 권리자임을 제 3 자를 위하여 계좌 발급자가 인증하는 방법으로서, 이때, 상기 제 3 자는 상기 고객과의 상기 온라인 거래를 진행하기 이전에 상기 고객을 확인하고자 하며, 상기 방법은,

- 상기 고객이 등록 웹 사이트에서 입력한 등록 정보를 상기 발급자의 시스템이 수신하는 단계,

- 상기 등록 정보가 고객 정보의 기존 데이터베이스 내에 포함된 정보와 일치하는 지를 상기 발급자의 시스템이 확인하여, 상기 고객을 상기 계좌의 권리자로 확인하고, 그리고 상기 계좌에 한 지정 비밀번호를 연계시키는 단계,

- 상기 온라인 거래 중 상기 제 3 자로부터 고객 컴퓨터를 통하여, 상기 발급자의 시스템에 의해 동작하는 접근 제어서버에서 인증 요청 메시지를 수신하는 단계로서, 이때, 상기 인증 요청 메시지는 상기 고객의 확인을 요청하는 메시지인 것을 특징으로 하는 단계,

- 상기 온라인 거래 중 상기 발급자의 시스템이 네트워크를 통해, 상기 고객으로부터 고객 인증 비밀번호를 요청하는 단계,

- 상기 고객으로부터의 상기 고객 인증 비밀번호가 상기 계좌에 대해 앞서 지정된 비밀번호와 일치하는 지를 상기 발급자의 시스템이 확인하는 단계, 그리고

- 상기 고객에 의해 입력된 고객 인증 비밀번호가 상기 계좌에 대해 앞서 지정된 비밀번호와 일치할 때, 상기 고객이 상기 계좌의 실제 권리자임을, 상기 온라인 거래 중 상기 네트워크를 통해 상기 발급자의 시스템이 고객 컴퓨터를 통하여 상기 제 3 자에게 알리는 단계로서, 이에 따라, 상기 온라인 거래 중 상기 발급자의 시스템이 상기 제 3 자를 위해 상기 고객을 인증하는 단계를 포함하는 것을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 8

제 7 항에 있어서, 상기 발급자는 계좌 발급 금융회사이고, 상기 제 3 자는 온라인 머천트(online merchant)이며, 상기 온라인 머천트는 상기 고객과 온라인 금융 거래를 실행하고, 상기 고객의 상기 계좌가 상기 발급 금융회사의 시스템에 의해 관리되는 것을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 9

제 7 항에 있어서, 상기 접근제어서버에서 제 3자로부터 인증 요청 메시지를 수신하기 전에, 상기 고객의 계좌가 인증 서비스에 등록되어있는 지를 결정하기 위해 상기 접근제어서버(access control server)에 질의하는 단계를 추가로 포함하는 것을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 10

제 9 항에 있어서, 상기 접근제어서버가 인증 요청 메시지를 상기 제 3 자로부터 수신하기 전에, 상기 고객 계좌가 등록 고객 계좌들의 데이터베이스에 포함되어 있음을 확인함으로서 상기 고객 계좌가 등록되어 있는 지를 상기 접근제어서버가 결정하는 것을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 11

제 9 항에 있어서, 상기 고객 계좌가 상기 인증 서비스에 참여하고 있는 발급 금융회사의 시스템에 연계되어 있음을 확인하기 위해 디렉토리 서버에 질의하는 단계를 추가로 포함하고, 이에 따라, 상기 고객 계좌가 발급 금융회사의 시스템과 연계되지 않은 경우 상기 고객 계좌가 상기 인증 서비스에 등록되어 있지 않은 것임을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 12

제 11 항에 있어서, 상기 접근제어서버에 대한 인터넷 주소를 상기 제 3 자의 컴퓨터 시스템에 전송하는 단계를 추가로 포함하며, 이때, 상기 인터넷 주소는 상기 제 3 자의 컴퓨터 시스템에 도달하기 전에 상기 디렉토리 서버를 통과하며, 이에 따라, 상기 접근제어서버에 대한 상기 인터넷 주소는 상기 제 3 자를 상기 접근제어서버와 직접 통신하게 하는 것을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 13

제 9 항에 있어서, 상기 고객 계좌가 상기 인증 서비스에 참여중인 발급 금융회사의 시스템과 연계되어 있음을 확인하기 위해 상기 제 3 자에 의해 제어되는 메모리 장치를 리뷰(review)하는 단계를 추가로 포함하고, 이에 따라, 상기 고객 계좌가 발급 금융회사의 시스템과 연계되어 있지 않을 경우, 상기 고객 계좌가 상기 인증 서비스에 등록되지 않은 것임을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 14

제 7항에 있어서, 상기 발급자 시스템의 서명 키(signature key)를 이용하여 디지털 방식으로 서명한 거래 영수증을 상기 발급자의 시스템이 발생시키는 단계, 그리고

- 상기 디지털 방식으로 서명한 거래 영수증을 상기 발급자의 시스템이 상기 제 3 자에게 전송하는 단계

를 추가로 포함하고, 이에 따라, 상기 디지털 방식으로 서명한 거래 영수증이 상기 제 3 자에게 상기 고객이 인증되었음을 확인해주는 것임을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 15

제 14 항에 있어서, 상기 거래 영수증은 거래 지불 일자, 거래 지불 금액, 그리고 상기 고객 계좌에 연계된 숫자를 포함하는 것을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 16

제 7항에 있어서, 카드 인증 확인값을 상기 계좌 발급자가 상기 제 3 자에게 전송하는 단계로서, 상기 카드 인증 확인값은 상기 고객 계좌와 특정 거래에 대한 고유 값을 포함하며, 이에 따라, 상기 카드 인증 확인 값은 인증된 특정 거래를 고유하게 식별하는 것임을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 17

제 14 항에 있어서, 상기 거래 영수증이 특정 발급자로부터 전송된 것임을 상기 제 3 자에게 보장하도록 상기 디지털방식으로 서명한 거래 영수증을 상기 제 3 자가 확인하는 단계를 추가로 포함하는 것을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 18

제 7 항에 있어서, 상기 방법은, 상기 고객 계좌가 요청 구매에 대해 충분한 신용을 가지고 있음을 확인하기 위해 상기 제 3 자가 발급 금융 회사의 시스템에 승인 메시지(authorization meassage)를 전송하는 단계를 추가로 포함하는 것을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 19

삭제

청구항 20

제 3 자와의 온라인 거래 중 계좌를 이용하는 고객이 상기 계좌의 실제 권리자임을 제 3 자를 위해 계좌 발급자가 인증하는, 인증 서비스에 의해 실행되는 방법으로서, 상기 방법은,

- 상기 고객이 등록 웹 사이트에서 입력한 등록 정보를 상기 발급자의 시스템이 수신하는 단계,

- 상기 등록 정보가 고객 정보의 기존 데이터베이스 내에 포함된 정보와 일치하는 지를 상기 발급자의 시스템이 확인하여, 상기 고객을 상기 계좌의 권리자로 확인하고, 그리고 상기 계좌에 한 지정 비밀번호를 연계시키는 단계,

- 상기 온라인 거래 중 네트워크를 이용하여 제 3 자 소프트웨어 모듈로부터 고객 컴퓨터를 통해 인증 요청 메시지를 전송하는 단계로서, 이때, 상기 소프트웨어 모듈은 상기 제 3 자의 통제 하에 있는 제 3 자 컴퓨터에 위치하는 것을 특징으로 하는 단계,

- 상기 발급자의 시스템에 의해 운영되는 접근제어서버(access control server)에서 상기 인증 요청 메시지를 수신하는 단계,

- 상기 발급자의 시스템이 네트워크를 통해, 상기 고객으로부터 비밀번호를 요청하는 단계,

- 상기 고객에 의해 입력되는 상기 비밀번호가 상기 계좌에 대해 앞서 지정된 비밀번호와 일치하는 지를 상기 발급자의 시스템이 확인하는 단계, 그리고

- 상기 발급자의 시스템이 상기 네트워크를 통해, 제 3 자 소프트웨어 모듈로 고객 컴퓨터를 통하여 인증 응답 메시지를 전송하는 단계로서, 이때, 상기 인증 응답 메시지는 인증 상태 인디케이터를 포함하고, 이에 따라, 상기 발급자의 시스템이 상기 제 3 자를 위해 상기 고객을 인증하는 단계를 포함하는 것을 특징으로 하는 인증 서비스에 의해 실행되는 방법.

청구항 21

제 3 자와의 온라인 거래 중 계좌를 이용하는 고객이 상기 계좌의 실제 권리자임을 상기 계좌 발급 금융 회사가 제 3 자를 위해 인증하는 인증 서비스에 사용되는 고객 컴퓨터에 의해 실행되는 방법에 있어서, 상기 방법은,

- 상기 계좌 발급 금융 회사가 상기 고객을 상기 계좌의 실제 소유자로 확인할 수 있도록, 등록 과정 중 상기 고객이 등록 정보를 등록 웹사이트에 전송하는 단계,

- 상기 등록 과정 중 상기 계좌에 대해 지정되는 비밀번호를 제공하는 단계,

- 온라인 거래 중에 제 3자로부터 인증 서비스의 개시를 요청하는 인증 요청 메시지를 고객 컴퓨터에서 수신하는 단계로서, 이에 의해 상기 고객이 인증될 수 있는 단계,

- 상기 고객 컴퓨터로부터 상기 계좌 발급 금융 회사에 의해 동작되는 접근제어서버로 상기 인증 요청 메시지를 전송하는 단계로서, 이때, 상기 고객이 상기 계좌 발급 금융 회사의 한 계좌를 가지는 단계,

- 상기 온라인 거래 중 상기 고객을 확인하는 데 사용되는 비밀번호를 상기 고객이 입력하도록 하는 요청을 상기 접근제어서버로부터 수신하는 단계,

- 고객 확인에 사용되는 상기 비밀번호를 제공하는 단계, 그리고

- 상기 고객의 확인에 관해 상기 접근제어서버로부터 상기 고객 컴퓨터를 통해 상기 제 3 자에게 인증 응답 메시지를 전송시키는 단계로서, 이에 따라, 상기 접근제어서버가 상기 제 3 자를 위해 상기 고객을 확인하는 단계

를 포함하는 것을 특징으로 하는 인증 서비스에 사용되는 고객 컴퓨터에 의해 실행되는 방법.

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

계좌 발급자가 제 3 자를 위해 고객을 인증하는 인증 서비스에 의해 실행되는 방법으로서, 상기 방법은,

- 상기 고객으로부터 입력 받은 등록 정보를 고객 정보 데이터베이스와 비교함으로서, 등록 과정 중 상기 계좌 발급자가, 상기 계좌의 실제 권리자로서 상기 고객을 확인하는 단계,

- 상기 등록 과정 중 상기 계좌 발급자가, 상기 계좌에 지정 비밀번호를 연계시키는 단계,

- 상기 제 3 자와의 온라인 거래를 실행하기 위한 요청을 고객 컴퓨터로부터 네트워크를 통해 수신하는 단계,

- 상기 고객이 상기 인증 서비스에 등록되어 있음을 결정하는 단계,

- 상기 온라인 거래 중 네트워크를 이용하여 상기 제 3 자로부터 상기 고객 컴퓨터를 통해 인증 요청 메시지를 전송하는 단계로서, 이때, 상기 인증 요청 메시지는 상기 계좌 발급자의 컴퓨터로 향하는 단계,

- 상기 온라인 거래 중 상기 계좌 발급자의 컴퓨터로부터 상기 고객 컴퓨터를 통해 인증 응답 메시지를 수신하는 단계로서, 이때, 상기 인증 응답 메시지는 상기 고객의 인증을 표시하고, 상기 인증은 상기 온라인 거래 중 상기 고객에 의해 상기 계좌 발급자의 컴퓨터로 제공된 비밀번호와, 상기 계좌에 대해 앞서 지정된 비밀번호에 기초하여 이루어지며, 이에 따라, 상기 계좌 발급자가 상기 제 3자를 위해 상기 고객을 인증하는 단계를 포함하는 것을 특징으로 하는 인증 서비스에 의해 실행되는 방법.

청구항 33

제 7 항에 있어서, 상기 온라인 거래가 지불 거래인 것을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 34

제 20 항에 있어서, 상기 온라인 거래가 지불 거래인 것을 특징으로 하는 인증 서비스에 의해 실행되는 방법.

청구항 35

제 21 항에 있어서, 상기 온라인 거래가 지불 거래인 것을 특징으로 하는 인증 서비스에 사용되는 고객 컴퓨터에 의해 실행되는 방법.

청구항 36

제 32 항에 있어서, 상기 온라인 거래가 지불 거래인 것을 특징으로 하는 인증 서비스에 의해 실행되는 방법.

청구항 37

제 20 항에 있어서, 상기 인증 서비스는 중앙 집중형 구조(700, 도7 및 도 8)를 이용하며, 상기 중앙 집중형 구조는 카드소지자 클라이언트 장치와 인증 서비스로 구성되고, 상기 인증 서비스는 등록 서버와 디렉토리 서버를 포함하는 것이며, 상기 제 3 자 소프트웨어 모듈은 상기 인증 요청 메시지를 상기 고객 컴퓨터의 브라우저를 통해 상기 접근제어서버로 전송하는 것을 특징으로 하는 인증 서비스에 의해 실행되는 방법.

청구항 38

제 20 항에 있어서, 상기 인증 서비스는 분산형 구조(900, 도 9 및 도 10)를 이용하며, 상기 분산형 구조는 카드소지자 클라이언트 장치와 인증 서비스로 구성되고, 상기 인증 서비스는 등록 서버를 포함하는 것으로서, 상기 제 3 자 소프트웨어 모듈은 상기 인증 요청 메시지를 상기 고객 컴퓨터의 소프트웨어 모듈로 전송하고, 그후 상기 고객 컴퓨터는 상기 인증 요청 메시지를 상기 접근제어서버로 전송함을 특징으로 하는 인증 서비스에 의해 실행되는 방법.

청구항 39

제 32 항에 있어서, 상기 인증 서비스는 중앙 집중형 구조(700, 도 7 및 도 8)를 이용하며, 상기 제 3 자는 상기 인증 요청 메시지를 상기 고객 컴퓨터의 브라우저를 통해 상기 계좌 발급자의 컴퓨터로 전송함을 특징으로 하는 인증 서비스에 의해 실행되는 방법.

청구항 40

제 32 항에 있어서, 상기 인증 서비스는 분산형 구조(900, 도 9 및 도 10)를 이용하며, 상기 제 3 자는 상기 인증 요청 메시지를 상기 고객 컴퓨터의 소프트웨어 모듈로 전송하며, 그후 상기 고객 컴퓨터는 상기 인증 요청 메시지를 상기 계좌 발급자의 컴퓨터로 전송함을 특징으로 하는 인증 서비스에 의해 실행되는 방법.

청구항 41

제 7 항에 있어서, 상기 제 3 자로부터 상기 고객의 컴퓨터 내 인터넷 브라우저를 통해 상기 계좌 발급자에게 인증 요청 메시지를 전달하는 단계, 그리고, 상기 계좌 발급자로부터 상기 고객의 컴퓨터 내 인터넷 브라우저를 통해 상기 제 3 자에게로 인증 응답 메시지를 전달하는 단계를 추가로 포함하는 것을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 42

제 7 항에 있어서, 상기 고객이 고객 컴퓨터의 인터넷 브라우저를 이용하여 제 3 자의 웹사이트에 액세스하는 단계, 상기 컴퓨터의 상기 인터넷 웹브라우저를 상기 웹사이트로부터 상기 계좌 발급자의 접근제어서버로 리디렉션시키는 단계로서, 이에 따라, 상기 계좌 발급자가 고객 -인증 비밀번호를 수신하는 단계, 그리고 상기 컴퓨터의 상기 인터넷 웹브라우저를 상기 접근 제어서버로부터 상기 제 3자 웹 사이트로 다시 리디렉션시킴을 포함함을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 43

제 7 항에 있어서, 상기 고객의 컴퓨터 상에서 인증 소프트웨어를 이용하지 않으면서 고객 인증 요청 단계를 수행하는 것을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 44

제 7 항에 있어서, 상기 등록 과정 중 상기 고객에 관한 인증 정보를 상기 접근제어서버에서 수신하는 단계를 추가로 포함하는 것을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 45

제 44 항에 있어서, 상기 접근제어서버는 상기 등록 과정 중 상기 계좌 발급자로부터 상기 고객 인증 정보와 지정 비밀번호를 수신하는 것임을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

청구항 46

제 44 항에 있어서, 상기 접근제어서버는 상기 등록과정 중 상기 고객으로부터 상기 고객 인증 정보와 지정된 비밀번호를 수신하는 것임을 특징으로 하는 계좌 발급자에 의한 온라인 고객 인증 방법.

명 세 서

기 술 분 야

<1> 본 출원은 2000년 4월 24일자 미국특허출원 60/199,727 호 -"비자 지불인 인증 서비스 설명(Visa Payer Authentication Service Description)"에 기반하여 우선권을 주장한다.

<2> 본 발명은 금융거래에 관한 것으로서, 특히, 온라인 거래중 지불인 신원 인증에 관한 것이다.

배 경 기 술

<3> 지불식 카드(가령, 신용카드, 데빗카드 등)을 이용한 지불 거래 중, 승인되지 않은 이용처럼 여러 가지 문제점들을 피하기 위해 카드소지자가 계좌의 소유자인 지를 확인하는 것이 중요하다. 지불인 인증은 카드소지자가 계좌의 소유자임을 확인하는 과정이다. 카드소지자가 계좌의 소유자임을 확인하는 가장 흔한 방법은 "카드 제시" 거래라 불리는 행위중에 판매 시점에서 흔히 발생한다. 카드 제시 거래는 머천트(merchant)가 카드소지자의 카드를 받아, 지불 카드 단자를 통해 카드를 긁어서 계좌 상태 및 신용 라인을 확인하고, 그후, 카드 후면 서명과 구매자 서명이 일치하는 지 여부를 확인하는 과정을 포함한다. 머천트가 이 종류의 거래에 대한 특정 가이드라인을 따를 경우, 머천트는 승인된 요금보다 조금 적은 요금을 보증받을 것이다. "비자 인터내셔널 서비스 조직"같은 서비스 제공자가 이런 특정 가이드라인을 제공할 수 있다.

<4> 이와는 달리, 메일이나 전화를 통해 온라인 상으로 이루어지는 "카드 비제시" 거래는 머천트에게서 보증받지 못하는 지불을 포함한다. 지불인이 비대면 거래에서 인증되지 않기 때문에 원칙적으로 어떠한 보증도 제공되지 않으며, 따라서, "카드비제시" 거래를 행하는 데는 여러 위험이 따른다. 이러한 위험으로 인해, 온라인 머천트에 대해 지불 거래를 환불하거나, 머천트 및 카드소지자에 대한 사기행위 문제가 생기고, 은행 비용을 다루는 이의(항의) 아이템이 증가하고, 그리고 상품 및 서비스를 온라인으로 구매하는 것이 안전하지 않다는 관념이 커지게 된다. 따라서 일부 소비자들이 온라인 구매를 꺼리게 된다. 구체적인 예를 들자면, 상품 및 서비스의 온라인 구매를 위해 훔친 계좌 정보를 승인없이 이용하거나, 부정한 온라인 구매를 위해 카드 계좌 번호를 제작하거나, 네트워크트래픽으로부터 텍스트 계좌 정보를 빼내는 등의 행위를 들 수 있다.

<5> 전자상거래가 계속해서 크게 성장함에 따라, 지불인 인증 방법을 제공하는 것이 중요하다. 이는 카드소지자, 머천트, 그리고 금융회사를 포함한 모든 지불 시스템 구성원에게 이익을 부여할 것이다. 온라인 구매 거래중 지불인의 인증은 사기, 분쟁, 보상, 그리고 환불 수준을 크게 감소시킬 것이고, 이는 결과적으로 이 행위들 에 관련된 비용을 감소시킬 것이다. 지불인 인증은 소비자의 보안에 대한 우려를 불식시킬 것이고 따라서 온라인 판매량을 증가시킬 것이다. 온라인 거래중 소비자를 인증하는 데 사용되었던 종래 시스템은 폭넓게 채택되지 않고 있다. 왜냐하면 이 시스템들이 사용하기 어렵고 복잡한 설계방식을 취하고 있으며 상당한 초기 투자를 필요로하며 공동이용성질(interoperability)이 결여되어 있기 때문이다. 일부 종래 시스템들은 이외에도, 머천트, 카드소지자, 발급자, 그리고 취득자에 의한 인증서의 생성, 분배, 이용을 필요로한다. 이러한 인증서 이용은 상당한

부담이 되는 것으로 알려져 있다.

<6> 앞서 내용으로부터, 온라인 거래 중 지불인 신원 인증을 위한 시스템이 요구된다. 이러한 인증 시스템은 구현 및 이용이 용이하여야 하고, 리소스 투자가 최소한으로 되어야 하며, 시스템 구성자간에 상당한 공동이용성질(interoperability)이 제공되어야 한다.

발명의 상세한 설명

<7> 본 발명은 온라인 거래중 지불인의 신원을 인증하는 온라인 서비스를 지향한다. 본 발명은 구현 및 이용이 용이하고, 구현을 위해 최소한의 자원 투자만을 요하며, 시스템 구성원간에 높은 공동기능성질을 제공한다. 본 발명의 인증 서비스로 인해, 카드 발급자는 비밀번호 이용같은 다양한 인증 방법을 이용하여 카드소지자의 신원을 확인할 수 있다. 또한, 인증서를 필요로하는 시스템 구성원은 발급 금융회사뿐이다. 또한 인증 서비스는 계산처리 중 실시간으로 머천트에게 인증 결과를 제공할 수 있다.

<8> 제 1 실시예에서, 발명은 신용카드, 데빗카드, 신원 카드 등같은 종래 카드의 이용을 지향한다. 제 1 실시예의 한가지 태양은 온라인 거래 중 카드소지자의 신원 식별 방법에 관한 것이다. 이 방법은 카드소지자가 지불 인증 서비스에 등록되어있는 지를 결정하기 위해 카드 발급자가 관리하는 접근제어서버에 머천트가 질의하고, 카드소지자로부터 비밀번호를 요청하며, 상기 비밀번호를 확인하고, 그리고 상기 카드소지자가 입력한 비밀번호가 인증될 경우 카드소지자가 인증되었음을 머천트에게 알리는, 이상의 과정을 포함한다.

<9> 제 2 실시예에서, 발명은 (스마트카드나 칩카드라고도 알려진) 집적 회로 카드 이용에 관한 것이다. 제 2 실시예의 한가지 태양은 칩카드를 이용하는 카드소지자의 신원을 인증하는 방법에 관한 것이다. 이 방법은 상기 카드소지자 클라이언트 장치가 칩카드 판독기를 포함하는 지를 확인하고, 그후, 상기 칩카드를 칩카드 판독기 내로 밀어넣는다. 칩카드 판독기가 칩카드를 받아들인 후, 칩카드는 암호문을 생성하고 이 암호문은 접근제어서버로 전달된다. 접근제어서버는 그후 칩카드의 정보를 바탕으로 제 2 암호문을 독립적으로 발생시키고, 칩카드 암호문을 제 2 암호문과 비교한다. 독립적으로 발생된 두 암호문이 일치하면, 카드가 인증된다.

<10> 본 발명의 서비스는 여러 장점을 제공한다. 예를 들자면, 인증 서비스는 "카드 비제시" 거래와 연계된 머천트에 대한 지불 보증을 성립시키기 위한 기반을 바탕에 깔고 있다. 게다가, 인증 서비스는 환불, 사기행위, 항의건 처리를 감소시킬 것이다. 본 발명의 이러한 여러 장점들이 아래에서 더욱 상세하게 설명될 것이다.

실 시 예

<30> 지불인 인증 서비스(PAS)에 의해 이용되는 인증 서비스에 대한 설명이 제공될 것이다. 시스템 설정 및 고객 등록, 그리고 구체적 메시지 흐름 등의 인증 서비스 및 그 외 다른 과정에 대한 보다 상세한 설명이 제공될 것이다. 앞 문단에서 설명한 바와 같이, PAS는 온라인 거래중 카드소지자의 계좌소유를 인증하도록 설계된다. 예를 들어 카드소지자가 온라인 쇼핑을 할 때, 쇼핑카트에 품목을 담을 때, 온라인 머천트의 대금계산 페이지로 진행할 때, 그리고 온라인 머천트 계산 폼을 완성할 때, PAS가 사용될 것이다. 보증자(Trusted Party)가 제 3 자의 이익을 위해 개인이나 법인의 신원을 인증할 때 여러 거래에 PAS가 사용될 수도 있다. 통상적으로 알려진 바와 같이, 보증자(Trusted Party)는 제 3 자에게 개인이나 법인의 법적 인증 책임을 얻는다. 예를 들어, 온라인 폼을 완성시키기 위해 인터넷 웹사이트에 접근할 때 금융기관의 고객을 인증하는 데 PAS가 사용될 수 있다. PAS는 데빗 카드, 구매카드(purchase cards), 가치 저장 카드(stored value cards)같은 소매 뱅킹뿐만 아니라, 도매 뱅킹, 의료 사업, 보험 사업, 증권 중개업같은 분야에도 사용될 수 있다. ID 카드가 PAS와 함께 사용될 수도 있다. 예를 들어, AAA는 PAS를 이용하여 고객의 신원을 인증할 수 있고, 또는 전화카드사가 PAS를 이용하여 전용 카드 이용자의 신원을 인증할 수 있다.

<31> PAS는 자신이 원하는 상품이나 서비스를 구매하고자 결정한 후, 가령, 소비자가 "구매" 버튼을 클릭한 후, 인증 과정을 실행할 수 있다. PAS는 "구매" 버튼을 클릭한 후뿐만 아니라, 소비자의 구매 거래 중 여러 다른 순간에서 그 인증 과정을 시작할 수도 있다. 인증 과정은 지불 통신망의 여러 지점에서 통합된 소프트웨어를 이용함으로서 소비자에게 투명한 모드로 주로 실행된다. PAS는 카드소지자와 카드소지자의 금융회사에 의해 참가를 확인하고, 카드소지자로부터 이전에 등록된 비밀번호를 요청함으로서 소비자의 신원을 확인할 수 있는 윈도를 생성한다. 소비자 신원이 확인되면, 지불 정보 및 소비자 인증 통지가 머천트에게 다시 전달된다. 그후, 통상적으로 이루어지는 바와 같이, 지불 거래가 머천트에 의해 처리된다. 예를 들어, 머천트가 카드소지자의 브라우저에 주문 확인 메시지를 전송할 수 있다.

<32> 도 1은 PAS를 지원할 수 있는 조직구조(100)의 한 실시예를 도식적으로 나타낸다. 이 조직구조는 세 개의 도메

인으로 나누어진다. 즉, 발급자 도메인(102), 공동이용성질 도메인(104), 그리고 취득자 도메인(106)으로 나누어진다. 발급자 도메인(102)은 발급자에 의해 주로 제어되는 구성성분들을 포함한다. 예를 들어 발급자는 소비자에게 지불 카드를 발급하는 금융회사일 수 있다. 구체적으로, 발급자나 카드 발급자는 카드 공급자로부터 받은 새 카드를 개인별로 특성화하여 이 카드들을 고객에게 발급한다. 개인별 특성화는 카드 공급자에 의해 수행될 수도 있고 개별특성화 사무소에 의해 이루어질 수도 있다. 금융회사에 추가하여, 발급자는 전화망 운영자, 서비스 기구, 머천트나 그 외 다른 조직, 심지어는 발급자의 대리자같은 어떤 적절한 발급 실체일 수 있다. 취득자 도메인(106)은 취득자(acquirer)에 의해 제어되는 구성성분들을 포함한다. 예를 들어, 취득자는 머천트를 지불 기법에 등록시키고 머천트 계좌를 관리하는 금융회사일 수 있다. 취득자는 온라인 머천트로부터 통신망까지 정보를 이동시키기도 한다. 공동이용성질 도메인(104)은 인터넷에 의해 지원되며, 발급자와 취득자에 의해 이용되는 구성성분들을 이용한다. 통상적으로 비자같은 카드 관리자에 의해 공동이용성질 도메인(104)이 관리된다. 공동이용성질 도메인(104)은 인터넷이 아닌 다른 통신망에 의해 지원될 수도 있다.

<33> 발급자 도메인(102)은 등록 사이트(108), 발급자 카드소지자 시스템(110), 카드소지자 클라이언트 장치(122), 등록 서버(112), 접근제어서버(114), 발급자나 제 3 자의 신원 식별 성분(116), 그리고 계좌 소유자 파일(118)을 포함한다. 부가적으로, 발급자 도메인(102)은 승인된 카드소지자(120)의 발급자 파일을 포함할 수 있다. 등록 서버(112)는 카드소지자가 답변하고 발급자가 확인할 웹 인터페이스를 통해 일련의 질문을 제시함으로서 PAS 서비스 내에서 카드소지자 등록을 관리하는 컴퓨터이다. 도 1에 도시되는 바와 같이, 카드 발급자가 등록 서버(12)를 운영한다. 그러나, 비자같은 서비스 기구가 발급자를 대신하여 등록 서버(112)를 운영할 수 있다. 발급자는 카드소지자의 실체 확인을 돕기 위해 등록 과정 중 제 3 자에 의해 제공되는, 웹에 의해 동작하는 대화형 "실체 인증 서비스"를 이용할 수 있다. 등록 서버(112)는 인터넷 지불 게이트웨이 서비스(124)에 인터넷을 통해 연결되어, 다시 비자넷같은 통신망(126)에 연결된다. 인터넷 지불 게이트웨이 서비스(124)에 의해, 등록 서버(112)가 통신망(126)과 대화할 수 있다. 지불 게이트웨이 서비스(124)를 통한 연결로 인해, 등록된 카드소지자가 유효한 카드 계좌를 가지고 있는 지를 결정하기 위해 등록 서버(112)가 발급자 승인 시스템(127)에게 질의할 수 있다. 등록 사이트(108)는 카드소지자가 PAS에 참가하기 위해 등록할 수 있는 인터넷 웹사이트이다.

<34> 접근제어서버(ACS)(114)는 카드소지자 계좌와 비밀번호 정보를 내장한 PAS용으로 등록된 카드소지자의 데이터베이스를 가진 컴퓨터이다. 온라인 지불 거래 중, 접근제어서버(114)는 머천트에게 디지털 방식으로 서명한 영수증을 제공하고, PAS에 대한 접근을 제어하며, 카드소지자의 서비스 참여를 확인한다. 카드 발급자나 비자같은 서비스 기구는 접근제어서버(114)를 운영할 수 있다. PAS가 추가 카드소지자 소프트웨어의 이용을 필요로하지 않기 때문에, 추가적인 카드소지자 소프트웨어와 하드웨어가 전개될 수 있다. 카드소지자 소프트웨어는 디지털 인증서, 집적회로 카드(칩카드), 그리고 칩카드 판독기같은 추가 인증 기술을 지원하는 데 사용될 수 있고, 접근제어서버가 적절한 카드소지자 클라이언트 장치에 적절히 관련되는 지를 확인하는 데 사용될 수 있다. 계좌 소유자 파일(118)은 PAS에 성공적으로 등록된 카드소지자에 관한 정보를 저장하기 위한, 발급자에 의해 관리되는 데이터베이스이다.

<35> 카드소지자 클라이언트 장치(122)는 PAS에 참가하기 위해 카드소지자에 의해 이용된다. 구체적으로, 카드소지자 클라이언트 장치(122)는 개인용 컴퓨터, 이동전화, PDA, 또는 대화형 케이블 TV처럼 인터넷에 접근할 수 있는 장치일 수 있다.

<36> 발급자 카드소지자 시스템(110)은 카드소지자에 관한 정보를 내장한, 발급자에 의해 제어되는 시스템이다. 이 시스템 정보는 계좌 정보, 카드소지자에 의해 이용된 서비스 등에 관한 정보를 포함한다. 발급자 카드소지자 시스템 내 일부 정보는 PAS에 카드소지자를 등록하는 과정에서 사용될 수 있다.

<37> 발급자나 제 3 자의 신원 인증 데이터베이스(116)는 발급자나 제 3 자가 카드소지자에 관한 파일에 이미 가지고 있는 정보를 내장한다. 데이터베이스(116)는 카드소지자의 신원을 확인하기 위해 카드소지자를 등록하는 과정에서 발급자에 의해 이용된다. 예를 들어, PAS 등록 과정 중 카드소지자에 의해 입력되는 정보는 카드소지자가 PAS에 성공적으로 등록하기 위해 인증 데이터베이스(116) 내 파일 상의 정보와 부합하여야 한다. 제 3 자는 이퀴팩스(Equifax)와 같은 회사일 수 있다.

<38> 공동이용성질 도메인(104)은 디렉토리서버(128), 영수증 파일(130), 그리고 영수증 관리자(131)를 포함한다. 디렉토리서버(128)는 머천트로부터 특정 접근제어서버까지 인증 요청을 전달한다. 디렉토리서버(128)는 비자처럼 서비스 기구에 의해 운영된다. 영수증 파일(130)과 영수증 관리자(131)는 각각의 인증된 구매 거래에 대해 서명된 영수증을 저장한다. 영수증 파일(130)은 어느 거래가 인증되었는 지를 확인하는 정보를 내장하고, 분쟁 해결 과정 중 추가 정보를 제공한다. 영수증 파일(130)과 영수증 관리자(131)는 서비스 기구에 의해 운영된다. 발급

자, 취득자, 또는 머천트가 디지털방식으로 서명한 영수증의 사본을 관리할 수도 있다.

<39> 취득자 도메인(106)은 머천트(132)와 확인 서버(136)를 포함한다. 머천트 플러그-인 소프트웨어 모듈(134)은 머천트(132) 위치에 놓인다. 머천트 플러그-인 소프트웨어 모듈(134)은 머천트(132)의 전자 상거래 웹사이트에 통합되는 PAS 소프트웨어 모듈이다. 플러그-인 소프트웨어 모듈(134)은 PAS와 머천트의 지불 처리 소프트웨어 사이에 인터페이스를 제공한다. 확인 서버(136)는 지불 거래중 PAS에 의해 머천트에게 돌아온 영수증에 서명하는데 사용되는 카드 발급자의 디지털 서명을 확인한다. 발명의 대안의 실시예에서, 확인 서버(136)의 기능은 머천트 플러그-인 소프트웨어 모듈(134) 내에 포함될 수 있어서, 별도의 확인 서버(136)에 대한 필요성을 제거한다. 확인 서버(136)는 머천트, 취득자, 또는 서비스 기구에 의해 운영된다.

<40> PAS의 조직구조는 두가지 별개의 구조적 접근으로 구현될 수 있다. 한가지 접근법은 중앙집중식 구조이고 다른 하나는 분산형 구조이다. 중앙집중식 접근법은 카드소지자의 클라이언트 장치에 어떤 소프트웨어나 데이터도 저장될 필요가 없다. 분산형 구조에서는, PAS 소프트웨어가 카드소지자의 클라이언트 장치 상에 존재한다. 이 소프트웨어는 등록 과정 중 등록 서버에 의해 카드소지자 클라이언트 장치로 다운로드된다. 분산형 접근법에서, 머천트는 카드소지자의 시스템 클라이언트 장치에 의해 제공되는 메카니즘을 통해 PAS에 대한 카드소지자의 참가를 결정한다. 판매자(vendor)인 PAS 소프트웨어 공급자의 구체적 사업 요구사항이나 그 고객의 구체적 사업 요구사항에 따라 중앙집중식, 또는 분산형, 또는 이들의 조합을 생성하는 것을 pas 소프트웨어 공급자가 선택할 수 있다는 점에 주목하여야 한다. 도 7-10은 중앙 집중식 및 분산형 구조에 관해 보다 상세한 설명을 제공할 것이다.

<41> 앞서 언급한 바와 같이, 분산형 구조는 카드소지자 클라이언트 장치 상에 저장될 소프트웨어를 필요로한다. 분산형 PAS는 카드소지자가 지불 응용프로그램 및 계속적 데이터를 한 카드소지자 클라이언트 장치로부터 또다른 카드소지자 클라이언트 장치로 전달하기 위한 메카니즘을 제공한다. 이 메카니즘은, 카드소지자 클라이언트 장치가 등록 과정 중 카드소지자가 접근한 클라이언트 장치와는 다른 클라이언트 장치일 때, 카드소지자의 신원을 인증하는 능력을 PAS에 제공한다. 현 카드소지자의 클라이언트 장치가 카드소지자가 이전에 사용하지 않은 카드소지자 클라이언트 장치일 때 PAS 시스템이 카드소지자 신원을 인증할 수도 있다. 다시말해서, 카드소지자가 한 개보다 많은 클라이언트 장치 상에서 PAS를 이용할 수 있다. 카드소지자 클라이언트 장치간에 PAS 소프트웨어를 전달하기 위해서는 두가지 이상의 방법이 존재한다. 첫 번째 방법은 플라피디스크처럼 휴대용 기억매체를 이용하여 카드소지자가 소프트웨어를 전달한다. 두 번째 방법은 카드소지자에 의해 이용될 추가적인 클라이언트 장치에게로 접근 제어 장치가 소프트웨어를 동적으로 다운로드하는 것이다.

<42> 일부 실시예에서, PAS는 전자 지갑같은 다른 카드소지자 응용프로그램과 공동이용할 수 있고, PAS는 전자상거래 마크-업 랭기지(ECML 소프트웨어)와 호환되어 작용할 수 있다. PAS는 분쟁 해결 및 환불용으로 카드소지자 인증 증거를 제공하기 위해 충분한 정보를 머천트가 유지하게 한다.

<43> **설정, 등록, 그리고 승인에 대한 상세한 설명**

<44> 아래의 내용은 PAS 설정으로부터 온라인 거래의 실제 승인까지 여러 단계에 관하여 상세하게 설명한다. 먼저, 여러 시스템 구성원들을 설정하는 데 필요한 과정들이 설명될 것이다. 그후 PAS에 등록하기 위한 카드소지자 과정이 설명될 것이다. 이 과정들이 설명된 후, 지불 거래의 실제 승인에 관한 설명이 제공될 것이다.

<45> PAS를 설정하는 것은 시스템 내 모든 구성원에 대한 설정 과정을 포함한다. 이 구성원들은 머천트, 금융회사, 카드소지자같은 실체들을 포함한다. 먼저, 온라인 머천트 및 금융회사의 설정 과정이 설명될 것이고, 이어서 카드소지자에 대한 설정 과정이 설명될 것이다.

<46> PAS에 서명한 온라인 머천트들은 도 1의 플러그-인 소프트웨어 모듈(134)처럼 머천트 플러그-인 소프트웨어 모듈을 수령한다. 플러그-인 소프트웨어 모듈은 머천트가 사용하는 연산 플랫폼 및 상거래 서버 소프트웨어 전용이어야 한다. PAS에 참가하고 있는 금융회사들은 주문제작된 PAS 등록 사이트 템플릿에 통합될 은행 로고 및 마케팅 디자인을 제공한다. 취득자 역시 머천트에게 서비스 기구 인증 당국(CA) 루트 인증서, 클라이언트 인증용 서비스 기구 인증 당국 SSL 인증서, 그리고 통합 지원체를 제공하여야 한다.

<47> 발급자가 PAS를 이용하도록 설정되기 전에, 이들은 발급자 도메인에 명시된 모든 PAS 소프트웨어의 사본을 취득하여야 하고, 하드웨어 시스템과 PAS 소프트웨어를 설치해야 한다. 그후 발급자 금융회사는 카드소지자 신원 확인 과정에 사용될 신원 인증 정책 및 참가 BIN 정보를 PAS에 제공할 것이다. 부가적으로, 발급자는 계좌 소유자 파일(118) 내로 프리-로딩(pre-loading)하기 위해 카드소지자 인증 정보를 PAS에 제공할 수 있다. 프리로딩은 카드소지자의 대용량 지원을 촉진시킨다. 예를 들어, 발급자가 모든(또는 대부분의) PAS 카드소지자를 활성화시

키고자 할 경우, 발급자는 모든 카드소지2자에게 PIN 번호를 전송할 수 있다. 그후 PIN 번호는 프리로딩된 비밀번호에 접근하기 위해 각각의 카드소지자에 의해 이용될 수 있다. 이 방식으로, 등록 과정이 촉진된다. 왜냐하면 각각의 카드소지자들이 공식적인 PAS 등록 과정을 거칠 필요가 없기 때문이다. 카드소지자가 처음으로 프리로딩된 비밀번호를 이용한 후, 카드소지자는 비밀번호를 기억하기 위해 새롭고 더 쉬운 지정 옵션을 가진다.

<48> 카드소지자 인증 정보는 회사 신원, 국가 코드, 카드 계좌 번호, 카드 유효기간, 카드소지자명, "BIN에 참여하는" 데이터에 명시된 발급자 전용 인증 데이터뿐 아니라, 청구지 주소, 배송 주소, 사회보장번호, 전화번호, 계좌잔고, 거래 내역, 그리고 운전면허번호같은 다른 정보도 포함한다. 발급자는 디렉토리서버에 접근제어서버 IP 주소(URL)와 신용카드 계좌 포트폴리오에 대한 계좌번호 범위를 제공하여야 한다. PAS는 은행 브랜드의 웹사이트를 통해 제공될 것이고, 이로 인해 카드소지자가 PAS에 등록할 수 있을 것이다.

<49> 도 2는 발명의 한 실시예에 따라 카드소지자가 PAS에 등록하는 과정을 도시한다. 단계 1에 도시되는 바와 같이, 발급자처럼 금융회사에 의해 관리되는 등록서버 인터넷 웹사이트를 카드소지자가 방문한다. 카드소지자들은 신용카드 계좌번호를 등록함으로서 PAS에 등록한다. 대안으로, 체크와 데빗카드같은 카드로 등록할 수도 있다. 또한, 카드소지자들은 한개 이상의 카드를 PAS에 등록할 수도 있다. 단계 2에 도시되는 바와 같이, 카드소지자는 주계좌번호(PAN), 이름 및 카드유효기간같은 정보를 입력한다. 이 시점에서 고객이 추가 정보를 입력할 수도 있다. 예를 들어, 주소, 이메일 주소, 쇼핑자 신원인증, 계좌 확인 값, 카드소지자전용 비밀번호, 발급자전용 인증 정보 등을 카드소지자가 입력할 수도 있다. 이 정보는 도 3에 도시되는 페이지(300)같은 등록 웹사이트의 페이지에 입력될 수 있다.

<50> 등록 사이트(108)에서 요청한 정보를 카드소지자가 입력한 후, 공동이용성질 도메인(104)의 디렉토리서버(128)에 발급자에 의해 등록되는 카드 범위 내에 카드소지자 PAN이 있는 지를 PAS가 확인한다. PAS는 여러 방법을 이용하여 카드소지자 신원을 확인할 수 있다. 먼저, 앞서 언급한 바와 같이, PAS는 발급자 고유의 인증 데이터베이스를 통해, 또는 제 3 자의 인증 데이터베이스를 통해 카드소지자 신원을 확인할 수 있다. 추가적으로, 승인된 카드소지자(120)의 발급자 제공 파일을 이용함으로서, 상태 확인 승인을 발급자에게 전송함으로서, 그리고 응답들을 금융회사에 의해 제공되는 프리로딩된 정보와 비교함으로서, 확인이 실행될 수 있다.

<51> PAN이 발급자가 등록한 카드 범위 내에 있지 않을 경우, 등록이 거절되고 등록 과정이 종료된다. PAN이 등록된 카드 범위 내에 있을 때, 비자넷처럼 서비스 기구 지불통신망을 통해 발급자 금융회사에 1달러에 대한 승인이 제출될 것이다. 1달러 거래 승인으로 인해, 발급자는 카드 계좌 상태를 확인할 수 있고 주소 확인 서비스를 이용하여 주소를 확인할 수 있으며, 그리고 카드소지자 확인값2(CVV2)을 확인할 수 있다. CVV2는 지불 카드의 후면의 서명 띠에 인쇄된 세자리 번호이다.

<52> 카드가 승인되면, 단계 3에서 추가 인증 정보를 위해 카드소지자에게 프람프트가 제시되어, 카드소지자의 신원을 실시간, 대화형, 온라인으로 확인할 수 있다. 발명의 일부 실시예에서, 카드소지자는 비밀번호와 "힌트 질문 및 응답" 쌍을 입력할 것을 요청받을 수 있고, 이는 구매 거래 중 카드소지자의 인증을 위해 사용될 것이다.

<53> 단계 4에 도시되는 바와 같이, 카드소지자 신원이 확인되고 적절한 응답을 받으면, PAS는 발급자 금융회사에 승인 메시지를 전송한다. 단계 5에서, 등록 서버(112)는 계좌 소유자 파일(118)의 레코드를 설정하기 위해 접근제어서버(114)에 카드소지자 정보를 전달한다. 도 1의 계좌 소유자 파일(118)같은 계좌 소유자 파일은 금융회사 BIN 번호, 계좌 번호, 유효기간, 성명, 운전면허번호, 청구지주소, 사회보장번호, 카드소지자 비밀번호, 카드소지자 비밀번호 질문, 카드소지자 비밀번호 응답, 카드소지자 이메일주소, 제 3자의 신원 점수(third party identity scores), 그리고 그 외 다른 정보같은 정보들을 저장할 수 있다.

<54> 발명의 일부 실시예에서, 등록 과정 중 카드소지자는 카드소지자가 인식할 수 있는 개인 보장 메시지(PAM)라 불리는 구의 입력을 요청받을 수 있다. PAM은 지불 거래 중 나중에 발급자에 의해 카드소지자에게 제시된다. 카드소지자가 지정한 PAM을 발급자만이 알기 때문에, PAS와 함께 이용되는 대화창이 카드소지자의 발급자로부터 전달되었다는 것을 카드소지자가 보장받을 수 있다. PAM의 예로는 "하늘은 푸르다"를 들 수 있다.

<55> 카드소지자가 PAS 이용을 위해 어떤 새 클라이언트 소프트웨어나 장치도 필요로하지 않는다는 점을 주목해야 한다. 그러나 일부 경우에, PAS의 칩카드 구현이 칩카드 판독기같은 추가적인 카드소지자 구성성분을 요구할 수 있다. 선호되는 실시예에서, 소비자 등록 과정은 카드소지자와 등록 서버간에 인터넷 사이에서 전송되는 데이터를 보호하기 위해 SSL 채널 암호화같은 보안 프로토콜을 이용한다.

<56> 또한, 소비자 등록 과정 중, 각각의 금융회사는 "이용기간(terms of use)"이나 "데이터 보호 정책(data privacy policy)"을 디스플레이할 수 있다. 각각의 금융회사는 등록 과정을 완료하기 위해 위 기간 및 정책을 수용하거

나 거부할 것을 카드소지자에게 요구할 수 있다. 각 소비자가 받아들이는 "이용기간"과 "데이터 보호 정책"의 버전 번호는 금융회사에 의해 저장되어야 한다.

<57> PAS 시스템 구성원들이 설정되고 카드소지자가 등록된 후, 지불 거래가 PAS를 이용하여 인증될 수 있다. PAS에 의해 인증된 지불 거래가 도 4에 쇠된다. 도 4의 단계 1에서, 카드소지자는 머천트의 전자상거래 사이트를 방문한다. 카드소지자가 구매하고자하는 상품이나 서비스를 선택한 후, 카드소지자는 계산과정을 시작하고 계산 폼을 완료시키며, "구매"버튼을 클릭한다.

<58> "구매"버튼이 클릭된 후, 도 4의 단계 2에 도시되는 바와 같이, 머천트 플러그-인 소프트웨어 모듈이 활성화되어 카드소지자 전용 계좌가 PAS에 등록되어 있는 지를 확인하기 위한 확인 과정이 실행된다. 여기에는 여러 방법이 있으며 이들 방법에 의해 머천트 플러그-인 소프트웨어 모듈이 카드소지자가의 PAS 등록 여부를 결정할 수 있다. 예를 들어, 디렉토리서버, 그리고 카드소지자에 관련된 접근제어서버가 확인되는 2-단계 과정, 접근제어서버만이 확인되는 과정, 그리고 디렉토리서버에서 유지되는 동일 정보를 내장한 캐시 메모리를 머천트가 확인할 수 있는 방법이 있다.

<59> 2-단계 과정에 대하여 이제부터 설명할 것이다. 첫 번째 단계에서, 머천트 플러그-인 소프트웨어 모듈은 카드 계좌번호를 식별하고, 계좌 번호가 PAS 구성원인 발급자 은행에 관련된 번호 범위 내에 있는 지를 확인하고자 디렉토리서버(128)에 질의한다. 계좌번호가 디렉토리서버(128)에 규정된 계좌번호 범위를 벗어날 경우, 발급자와 카드소지자는 PAS에 등록되어 있지 않다. 이 경우에, 머천트는 계좌번호가 PAS에 등록되어 있지 않다는 것을 통지받을 것이고, 머천트 플러그-인 소프트웨어 모듈이 거래 제어를 다시 머천트 프론트(storefront) 소프트웨어에 되돌려보낸다. 이 시점에서, 머천트 프론트 소프트웨어는 거래를 계속할 수도 있고, 카드소지자에 대한 추가 서비스를 거절할 수도 있으며, 대안의 지불 방법으로 계속할 수도 있다.

<60> 다른 한편, 계좌 번호가 디렉토리서버(128)에 존재하는 계좌번호 범위 내에 있다고 결정될 경우, 확인과정의 제 2 단계가 시작된다. 확인과정의 제 2 단계는 카드가 등록되었는 지를 결정하기 위해 카드소지자의 카드 번호를 인증할 수 있는 접근제어서버를 상기 디렉토리가 전달함으로서 시작된다. 카드가 등록되지 않았을 경우, 등록 과정이 종료된다. 카드가 등록되어 있다고 접근제어서버가 표시할 경우, 접근제어 서버는 디렉토리서버를 통해 그 URL 인터넷 주소를 머천트 플러그-인에 되보낸다. 머천트 플러그-인은 카드소지자 클라이언트 장치와 그 상주 브라우저를 통해 접근제어서버를 호출한다. PAS에 여러개의 접근제어서버가 있을 수 있다.

<61> 카드소지자가 PAS에 등록되어있는 지를 확인하기 위한 두 번째 방법은 머천트 플러그-인 소프트웨어 모듈이 디렉토리서버에 먼저 질의하지 않고 직접 접근제어서버에 질의하는 것이다. 세 번째 방법은 앞서 언급한 바와 같이, 머천트가 디렉토리서버에 유지되는 동일한 정보를 내장한 캐시 메모리를 가지는 것이다. 이 방식으로 머천트는 예비 확인을 행할 수 있다.

<62> 한개보다 많은 물리적 디렉토리서버가 PAS 시스템에 존재할 수 있다. 그러나, 단 한개의 논리 디렉토리서버가 존재하는 경우가 선호된다. 다시 말해서, 모든 디렉토리서버들이 동일한 정보를 가지도록 일관되어야 한다.

<63> 카드소지자가 PAS 구성원일 경우, 접근제어 서버는 카드소지자에게 은행 브랜드의 창을 디스플레이한다. 은행 브랜드의 창은 기본 지불 거래 정보를 가지고 있고 PAS 비밀번호에 대한 프람프트를 카드소지자에게 제시한다. 카드소지자는 비밀번호를 입력하고 접근제어서버는 비밀번호를 확인한다. 오늘날 일반화된 것처럼, 카드소지자는 비밀번호를 정확하게 입력하기 위해 어떤 일정 횟수의 시도를 행할 수 있다. 카드소지자가 비밀번호를 정확하게 입력하지 못할 경우, 카드소지자에게는 힌트 질문이 프람프트로 나타나게 되고, 이 질문은 등록 과정에서 만들어진 것이다. 카드소지자가 힌트 질문에 따라 정확한 응답을 입력하기 위해 한번의 기회를 부여받는 것이 선호된다.

<64> 정확한 비밀번호가 즉시 입력되거나 허용된 횟수의 시도 내에서 힌트 질문에 카드소지자가 정확하게 응답할 경우, 지불 인증이 계속된다. 접근제어서버는 서비스 제공자의 키나 발급자의 서명 키를 이용하여 영수증에 디지털 방식으로 서명한다. 이 영수증에는 머천트명, 카드계좌번호, 지불금액, 그리고 지불일자가 기록된다. 영수증 파일(130)은 머천트명, 머천트 URL, 카드계좌번호, 유효기간, 지불금액, 지불일자, 발급자 지불 서명, 그리고 카드소지자 인증 확인값 등의 거래 데이터를 저장한다. 그후 접근제어서버는 카드소지자 브라우저를 통해 머천트 플러그-인을 향하도록 다시 카드소지자를 방향변경시킨다. 이 시점에서, 접근제어서버는 디지털 방식으로 서명한 영수증을 머천트에게 전달하고, 카드소지자가 인증되었는 지 여부를 머천트에게 전달한다. 취득자 도메인(106)의 확인 서버(136)가 머천트 플러그-인(134)에 의해 이용되어, 지불 영수증 서명에 사용되는 디지털 서명을 확인한다. 디지털 서명을 확인한 후, 카드소지자는 인증된 것으로 간주된다. 일부 발명의 실시예에서, 거래

가 완료된 후, 카드소지자는 자신의 카드계좌를 재등록하는 능력과, 차후 온라인 거래에 사용될 새 비밀번호를 생성하는 능력을 가진다.

<65> 카드소지자가 단계 3에서 인증된 후, 단계 4는 특정 카드소지자의 계좌를 승인하기 위한 과정을 개시한다. 구체적으로, 단계4에서, 머천트는 머천트 플러그-인 소프트웨어 모듈을 통해, 비자넷같은 지불 통신망에 승인 메시지를 전송한다. 지불 통신망은 승인 메시지와 ECI를 발급자 금융회사에 전달한다. 승인 메시지는 당 분야에 잘 알려진 메시지이다. 승인 메시지는 발급자에게 전달되어, 특정 계좌가 정상이며 지불 거래의 요청한 구매 금액에 대해 적절한 신용라인을 가지고 있음을 발급자 금융회사가 머천트에게 확인할 수 있다. ECI는 인터넷 상에서 거래가 완료되었음을 나타내고, 이용된 인증 및 메시지 보안 수준(채널 암호화(SSL))을 나타낸다.

<66> 발명의 대안의 실시예에서, 머천트는 승인 메시지와 함께 추가 정보를 제공할 수 있다. 예를 들어, 다음의 정보도 전송될 수 있다. 즉, 카드소지자가 성공적으로 인증되었는 지를 표시하는 플래그, 계좌정보, 디지털서명, 카드소지자 확인값2, 카드인증 확인값(CAVV), 칩카드 EMV 암호문에 의해 인증된 오프라인 PIN, 그리고 보증된 지불을 머천트에게 제공하기 위해 필요한 필드들도 전송될 수 있다. CAVV는 카드소지자를 인증한 접근제어서버에 의해 생성되는 데이터로서, 상기 카드로부터 특정 지불 거래와 주어진 거래에 대한 고유값이다. 승인 거래의 발급자 금융회사 처리가 완료된 후, 구매 거래의 제어가 지불 네트워크를 통해 머천트 프론트 소프트웨어에 되돌아온다. 발급자는 지불통신망을 통해 머천트에게 승인 응답을 되보낸다. 도 4의 단계 5에서, 발급자 금융회사는 거래를 승인하거나 거절할 것이다. 일부 실시예에서, 승인 메시지는 한 벌로 묶일 수 있고 차후에 그룹으로 전송될 수 있다. PAS 인증 정보는 배치 승인 메시지에 또한 포함된다.

<67> 접근제어서버(114)는 다른 여러 기능을 행할 수 있다. 예를 들어, 접근제어서버는 데이터베이스로부터 등록된 계좌를 정지시킬 수 있다. 계좌는 카드소지자에 의해, 또는 발급자에 의해 수동으로 정지될 수 있다. 접근제어서버(114)는 카드소지자가 대체 카드를 수령할 때 단순화된 갱신 등록 과정을 또한 제공한다. 접근제어서버(114)는 고유 접근 제어 정보를 가진 동일한 등록 계좌의 다중 사용자를 지원할 수 있다. 구매거래나 계좌 갱신을 위해 접근제어서버(114)에 대한 연결을 사용자에게 제공할 때, 접근제어서버(114)는 다음의 메카니즘 중 한 개 이상을 통해 등록 계좌의 승인된 카드소지자로 사용자를 확인해줄 수 있다. 상기 메카니즘으로는 통과 명령, 디지털 서명, 온라인 PIN 번호, 또는 칩카드 EMV 암호문에 의한 오프라인 PIN 승인이 있다.

<68> PAS에서는, 머천트가 파일에 카드소지자 계좌 정보를 가지는 기존 시스템과 공동이용할 수 있고, 기존 머천트 승인 및 삭제 시스템과 공동이용할 수 있으며, 여러 머천트에게 서비스를 제공하는 제 3자를 지원할 수 있고, 머천트와 취득자간 다양한 지불 인터페이스를 지원할 수 있으며, 그리고 전자상거래 인디케이터(ECI)의 값을 설정할 때 취득자로부터 지불통신망 승인 메시지에 대한 강제적 충격을 최소화할 수 있다.

<69> 머천트로부터 접근제어서버까지 거래를 전달하기 위한 한가지 방법은 카드소지자 계좌번호를 바탕으로 서버 주소를 제공하는 디렉토리를 가지는 것이다. 이러한 방법에서는 정보 전달을 위한 PAS 요청이 승인된 머천트로부터만 수령가능하다. PAS가 정상 활동을 뛰어넘는 머천트로부터의 활동을 감지하고 보고할 경우, PAS는 머천트에 대한 접근을 거절하여, 이러한 접근이 더 이상 유효하지 않음을 취득자가 표시한다. 이는 머천트 사기 행위가 가능하다고 간주될 때 가능한 경우이다. PAS 시스템에 대한 머천트 인증이 전개될 수 있으나, 전개가 강제사항은 아니다. 머천트 인증은 머천트 사기행위의 최소화를 돕는다.

<70> **PAS 지불 거래에 대한 메시지 흐름 설명**

<71> 도 6은 PAS 구조에서 겹쳐지는 지불 거래 중 전송되는 메시지의 예를 도시한다. 앞서 설명한 바와 같이, 구매 거래는 카드소지자가 브라우저를 통해 머천트 웹사이트를 방문하고 구매할 아이템을 선택할 때 시작된다. 머천트의 지불 시스템은 카드소지자에게 지불 정보를 입력할 것을 요청할 것이다. 일반적으로, 지불 정보 입력은 보안 환경에서 이루어져야 한다. 예를 들어, SSL 암호 프로토콜을 이용하여 이루어질 수 있다. 카드소지자가 거래를 마치려고 함을 표시하면, 머천트의 지불 시스템은 PAS 머천트 플러그-인 소프트웨어 모듈(134)을 호출한다. 선(1a)으로 도시되는 바와 같이, 플러그-인 소프트웨어 모듈(134)은 카드소지자가 서비스에 등록되어 있음을 확인하기 위해 카드소지자의 지불인 인증 번호(PAN)를 내장할 수 있는 접근제어서버의 특정 URL에 대해 디렉토리 서버(128)를 확인한다. 대안으로, 플러그-인 소프트웨어 모듈(134)은 이 정보를 내장한 고유 캐시 메모리를 확인한다. 소프트웨어(134)는 카드소지자 PAN을 이용하여 VerifyEnrollmentReq 메시지를 포맷함으로서 PAN을 검색한다. 아직 구축되지 않은 경우, 머천트 플러그-인 소프트웨어(134)는 접근제어서버(114)나 디렉토리서버(128)와 보안 연결을 구축할 것이고 그 자체를 인증할 것이다. 머천트 플러그-인 소프트웨어(114)는 여러 위치에서 카드소지자 PAN에 대응하는 카드 범위 입력을 찾을 것이다. 검색되는 한가지 위치는 디렉토리 정보의 머천트 플러그-인 소프트웨어 캐시이다. 머천트 플러그-인 소프트웨어 모듈은 디렉토리서버와 접근제어서버를 확인할 수

도 있다.

<72> 머천트 플러그-인 소프트웨어(114)가 검색을 수행한 후, VerifyEnrollmentReq 메시지가 접근제어서버(114)에 라인(1b)에서처럼 직접 전송되거나, 라인(1a)에 나타나는 것처럼 디렉토리서버(128)를 먼저 통과한 후 전송된다. VerifyEnrollmentReq 메시지가 디렉토리서버(128)를 통해 접근제어서버(114)에 전송될 때, 디렉토리서버(128)는 VerifyEnrollmentReq 메시지에 내장된 카드소지자 PAN에 대응하는 레코드를 검색한다. 성공적으로 부합하지 않는 경우에, 디렉토리서버(128)는 어떤 URL 값없이 VerifyEnrollmentRes 메시지를 포맷할 것이고, PAN 등록의 상태에 대한 값(또는 VerifyEnrollmentRes-Status)을 "N"으로 설정할 것이다. VerifyEnrollmentRes 메시지는 그 후 머천트 플러그-인 소프트웨어에 되돌아온다. 다른 한편, 성공적으로 부합할 경우, 디렉토리서버(128)는, 이미 구축되지 않았을 경우, 접근제어서버 URL과 견고한 연결을 구축할 것이고, 그 자체를 인증할 것이다. 그후, VerifyEnrollmentReq 메시지가 접근제어서버 URL에 전송된다. 상기 URL이 가용하지 않을 경우, 머천트 플러그-인은 다음 접근제어서버 URL값으로 진행되어야 하고, 최대 다섯 개까지의 접근제어서버 URL을 검색할 수 있게 한다. 물론, 시도하는 URL 횟수는 가변적이다. 모든 시도에도 불구하고 실패할 경우, VerifyEnrollmentRes 메시지가 머천트 플러그-인에 되돌아와서, VerifyEnrollmentRes-Status를 "N"으로 설정하여 구매 거래가 PAS 거래로 처리될 수 없음을 머천트에게 나타낸다.

<73> VerifyEnrollmentReq 메시지가 접근제어서버(114)에 의해 수령된 후, 접근제어서버는 VerifyEnrollmentReq 메시지로부터 카드소지자 PAN을 수령하여, 계좌 소유자 파일(118)에 대해 이를 확인한다. 접근제어서버(114)는 그 후 VerifyEnrollmentRes 메시지를 포맷한다. 성공적으로 부합할 경우, 접근제어서버는 PAN 등록 상태를 "Y"로 설정하고, 접근제어서버(114)가 내부적으로 PAN과 관련되는 1회용 프록시 PAN을 생성하며, 그리고 VerifyEnrollmentReq 메시지에 URL 필드를 위치하게 한다. 성공적으로 부합하지 않는 경우에, 접근제어서버는 PAN 등록 상태를 "N"으로 설정한다. 그후, 라인(2a)으로 나타나는 바와 같이, 접근제어서버는 VerifyEnrollmentRes 메시지를 디렉토리서버(128)를 통해 머천트 플러그-인에 되보낸다. VerifyEnrollmentReq 메시지가 접근제어서버에 직접 전송될 경우, VerifyEnrollmentRes 메시지가 직접 머천트 플러그-인에 전송된다(라인(2b)).

<74> 디렉토리서버(128)의 캐싱은 CRReq와 CRRes 메시지 쌍을 이용함으로서 촉진될 수 있다. CRReq 메시지는 머천트 플러그-인 모듈로부터 디렉토리서버에 전송되어, 플러그-인 모듈이 그 캐시를 업데이트하기 위해 참가 카드 범위의 리스트를 요청한다. CRRes 메시지는 참가 범위를 내장한 응답이다.

<75> 발급자 접근제어서버가 VerifyEnrollmentRes 메시지를 되돌려보낸 후, PAS 시스템은 카드소지자 클라이언트 장치가 QueryCardholderReq 및 QueryCardholderRes 메시지 쌍을 이용함으로서 분산형 인증 능력을 가지는 지를 확인한다. 머천트 플러그-인은 분산형 PAS 카드소지자 모듈이 상주하는 지를 결정하기 위해 카드소지자 클라이언트 장치(122)에 QueryCardholderReq 메시지를 포맷하고 전송할 것이다. QueryCardholderReq 메시지 전송은 도 6에서 라인(3)으로 나타난다. 분산형 인증 옵션이 QueryCardholderRes 메시지에 되돌아올 경우, 머천트 플러그-인은 인증 단계들을 실행하기 위해 PAS 카드소지자 클라이언트 소프트웨어와 직접 통신할 수 있을 것이다. QueryCardholderRes 메시지 전송이 도 6에서 라인(4)으로 표시된다.

<76> VerifyEnrollmentRes-Status가 "Y"와 다른 값을 가질 경우, 구매 거래가 PAS 거래로 처리될 수 없다는 것이 머천트에게 통지된다. 그러나, VerifyEnrollmentRes-Status 가 Y의 값을 가질 경우, 머천트 플러그-인은 지불 요청 메시지 PAReq를 포맷할 것이다. 머천트 플러그-인은 카드소지자 클라이언트 장치 브라우저를 통해 발급자 접근제어서버에 PAReq 메시지를 전송할 것이다(라인(5)).

<77> 추가적으로, QueryCardholderReq 및 QueryCardholderRes 메시지를 이용함으로서, VerifyCardholderReq와 VerifyEnrollmentRes 메시지가 제거될 수 있다. 카드소지자 클라이언트 소프트웨어는 소프트웨어에 내장되는 발급자 접근제어 서버 URL로 전개될 수 있다. 머천트 플러그-인은 QueryCardholderReq와 QueryCardholderRes 메시지를 먼저 완료할 것이다. PAS 카드소지자 클라이언트 소프트웨어가 감지되면, 지불인 인증 요청(PAReq) 메시지가 접근제어서버나 카드소지자 클라이언트 소프트웨어에 전송될 수 있고, 이때 VerifyEnrollmentReq와 VerifyEnrollmentRes를 실행할 필요가 없다.

<78> 머천트 플러그-인이 지불인 인증 요청(PAReq)을 발급자 접근제어 서버에 전달한 후, 접근제어서버는 카드소지자에게 한개의 창을 디스플레이한다. 발급자 로고, 서비스 기구 마크나 브랜드 로고, 머천트명, 머천트 위치(URL), 총 구매금액 및 통화, 구매일자, 카드번호, 설치/순환 지불 항목, 설명에 대한 주문 설명이나 링크, 이 정보에 대한 링크나 판매 조건 및 특별한 항목, 개인 보장 메시지(PAM), 그리고 카드소지자 비밀번호에 대한 프람프트처럼, 다른 아이템에 추가하여, 창은 지불인 인증 응답(PARes)에 내장된 지불 세부사항을

디스플레이한다.

<79> 그후 접근제어서버는 적절한 비밀번호 입력을 위해 카드소지자에게 프람프트를 제시할 것이다. 접근제어서버는 카드소지자 입력을 수령하고, 계좌 소지자 파일(118)에 대해 이를 유효화시킨다. PAS로 인해, 정확한 비밀번호를 입력하기 위해 수많은 실패 시도(가령, 세 번의 시도)를 허용할 것이다. 물론, 시도 횟수는 변경가능하다. 성공적이지 못한 마지막 시도 이후, PAS는 힌트 질문을 디스플레이할 것이다. 카드소지자는 정확한 힌트 질문 응답을 입력해야할 것이다. 카드소지자와 관련된 힌트 질문이 디스플레이된다. 카드소지자는 정확한 응답을 입력하기 위해 한번 이상의 시도를 제공받는다. 카드소지자가 정확하지 않은 응답을 제공할 경우, 머천트는 PAS 거래가 완료될 수 없음을 통지받을 수 있다. 카드소지자가 정확하게 응답할 경우, 거래는 비밀번호가 일치한것처럼 다루어져야 한다. 계좌번호에 대해 한번보다 많은 입력이 있을 경우, 여러 카드소지자 이름이 드랍 다운 창에 디스플레이된다. 카드소지자는 자신의 이름을 선택할 수 있다.

<80> 비밀번호가 일치할 때, 접근제어서버는 지불 응답 메시지 PARes를 발생시키고 디지털 방식으로 서명한다. 접근제어 서버는 SaveReceipt 메시지를 발생시켜서 영수증 파일(130)과 영수증 관리자(131)에 전송한다(라인(7)). 라인(7a)에서처럼, SaveReceipt 메시지가 영수증 파일(130)로부터 발급자 승인 및 지불 시스템(138)에 전달되어서, 발급자가 지불 승인 요청을 지불인에 의해 인증된 거래와 실시간으로 부합하게 한다. SaveReceipt 메시지를 발급자 승인 및 지불 시스템(138)에 전송함으로서, 발급자는 승인 요청이 인증된 구매를 위한 것인 지 동시에 결정할 수 있다. 접근제어서버는 머천트 서버 플러그-인에 서명된 PARes를 다시 방향변경시킬 것이다(라인(6)).

<81> 서명한 PARes가 머천트 플러그-인에 다시 전송된 후, 플러그-인이 다시 활성화된다. 인증 상태가 "Y"일 경우, 플러그-인은 PARes 메시지를 확인 서버(136)에 전송한다. 확인 서버 기능이 머천트 플러그-인에 의해 제공될 경우, 머천트 플러그-인은 PARes 서명을 확인하고 서명 확인 결과를 되보낸다. 서명이 확인될 수 없는 경우, 머천트 플러그-인은 거래가 PAS 거래로 취급될 수 없음을 머천트에게 통지할 것이다. 인증 상태가 "N"일 경우, 머천트는 추가 정보를 요청하는 카드소지자에게 프람프트를 보내야하고, 카드소지자에게 다른 지불 카드나 지불 형태를 이용하라고 주문하여야 하며, 또는 비-승인 지불 거래로 지불 거래를 처리하여야 한다.

<82> 취득자 도메인(106)이 확인 서버를 내장할 경우, 확인 서버(136)는 PARes 상의 서명을 확인한다. 확인 서버(136)는 서명 확인 결과를 머천트 플러그-인에 되보낸다. 서명이 확인될 수 없는 경우, 머천트 플러그-인은 머천트에게, 거래가 PAS 거래로 취급될 수 없음을 통지한다. 다른 한편, 서명이 확인되면, 머천트는 인증된 지불 승인으로 계속된다. PARes 메시지가 머천트로부터 그 취득자 지불 프로세서(140)로 또한 전달될 수 있다(라인(6a)). PARes 메시지는 취득자로부터 통신망(142)을 통해 발급자에게 전달될 수 있다. 따라서, 지불인 인증 결과는 표준 지불 승인 과정의 일부로 발급자에게 가용하도록 만들어진다.

<83> 여러 채널의 전송에 관련된 보안 문제가 논의된다. 기준선으로, 모든 전송 채널이 128비트 SSL을 이용하여 암호화되는 것이 선호된다. 카드소지자와 머천트간 채널은 두 채널을 포함한다. 머천트는 서비스 기구에 의해 승인된 인증서 당국으로부터 얻은 SSL 인증서를 이용함으로서 카드소지자가 지불 정보를 입력할 때 사용되는 연결을 보호하여야 한다. 머천트는 서비스 기구에 의해 승인된 인증서 당국으로부터 얻은 SSL 인증서를 이용함으로서 카드소지자로부터 머천트 플러그-인까지 PARes 메시지를 전송하는 데 사용되는 연결을 보호하여야 한다.

<84> 카드소지자와 접근제어서버간 채널은 서비스 조직에 의해 승인된 인증서 당국으로부터 얻은 SSL 인증서를 이용함으로서 접근제어서버에 의해 암호화되어야 한다. 이 채널은 두 용도로 사용된다. 먼저, 머천트 플러그-인으로부터 접근제어서버까지 PAReq 메시지를 전송하기 위해, 두 번째로, 접근제어서버로부터 카드소지자에게로 서명한 PARes 메시지를 전송하기 위해 사용된다.

<85> 카드소지자와 등록 서버간 채널은 서비스 기구에 의해 승인된 인증서 당국으로부터 얻은 SSL 인증서를 이용하여 등록 서버에 의해 암호화되어야 한다. 이 채널은 카드소지자 등록 정보를 수령하는 데 사용된다.

<86> 머천트와 디렉토리서버간 채널, 그리고 디렉토리서버와 접근제어서버간 채널은 VerifyEnrollmentReq와 VerifyEnrollmentRes 메시지에 내장된 PAN 데이터와, VerifyEnrollmentRes 메시지에 내장된 접근제어서버 URL 주소를 보호하기 위해 서비스 기구에 의해 발급된 SSL 암호화 인증서를 통해 보호되어야 한다.

<87> 접근제어서버와 카드소지자간 채널은 카드소지자의 비밀번호와 카드소지자에 의해 입력되는 비밀번호에 대한 프람프트를 보호하기 위해 암호화되어야 한다. 이 채널은 서비스 기구에 의해 승인된 인증서 당국으로부터 얻은 SSL 인증서로 보호되어야 한다.

<88> **중앙집중형 및 분산형 조직구조 실시예**

<89> 도 7과 8은 중앙집중형 구조를 도시하고 도 9와 10은 분산형 조직구조를 도시한다. 도 7-10은 등록 및 지불 과정 중 메시지 흐름을 나타낸다.

<90> 도 7은 발명의 한 실시예에 따르는 중앙집중형 PAS 구조에 대한 메시지 흐름도이다. 앞서 언급한 바와 같이, 중앙집중형 접근법에서는 소프트웨어나 데이터가 카드소지자 시스템에 저장될 필요가 없고, 카드소지자의 비밀번호는 중앙 데이터 저장 사이트(AHF)에 저장된다.

<91> 중앙집중형 구조(700)는 카드소지자 클라이언트 장치, 예를 들어, 개인용 컴퓨터(PC)(702)와, PAS(704)로 구성된다. 카드소지자 클라이언트 장치(702)는 카드소지자로 하여금 PAS에 접근할 수 있게 하는 인터넷 브라우저(706)를 지원한다. PAS(704)는 한개 이상의 등록 서버(708)를 포함한다. PAS 시스템의 여러 다른 성분은 중앙집중형 구조를 단순화시키기 위해 도시되지 않았다. 중앙집중형 등록 과정은 단계 1에서, 즉, 카드소지자가 은행 인터넷 사이트와 특정 등록 페이지로 이동하여 PAS에 등록할 때, 시작된다. 단계 2에서 카드소지자의 질문에 따라, 등록 서버(708)는 카드소지자에게 인증 질문을 제시한다. 단계 3에서, 카드소지자는 인증 질문에 답변하고, 필요한 비밀번호를 제공한다.

<92> 등록 서버는 단계 4에서 확인 과정을 통해 응답을 확인한다. 확인과정의 결과는 등록 서버(708)에 되돌아온다(단계 5). 단계 6에서, 데이터베이스 및 디렉토리서버가 업데이트된다. 단계 7에서, 카드소지자에게 등록 여부 확인이 통지된다.

<93> 도 8은 발명의 한 실시예에 따르는 카드소지자 클라이언트 장치(702), PAS(704), 그리고 머천트 시스템(720) 사이에서 이루어지는 중앙집중형 지불 흐름을 도시한다. 도 8에서, PAS(704)는 디렉토리서버(710), 접근제어서버(712), 그리고 영수증 데이터베이스(714)를 포함하는 것으로 도시된다. 머천트 서버는 프론트 소프트웨어 프로그램(storefront software program)(722), PAS에 의해 제공되는 머천트 플러그-인 소프트웨어 모듈(724), 그리고 지불 시스템(726)을 포함한다. 중앙집중형 지불 흐름은 카드소지자가 단계 1에서 머천트의 전자상거래 웹사이트에서 쇼핑할 때 시작된다. 카드소지자가 계산 과정을 시작할 때, 단계 2는 카드소지자가 디렉토리서버(710)에 등록되었는 지를 머천트 플러그-인 모듈(724)이 확인한다는 것을 보여준다. 카드소지자가 등록되어 있으면, 디렉토리서버는 발급자의 접근제어서버 URL 주소를 머천트 플러그-인에 되보낸다. 단계 3에서, 머천트 플러그-인 모듈(724)은 PAReq 메시지를 접근제어서버(712)에 전송한다. PAReq 메시지에 따라, 카드소지자는 결국 비밀번호를 입력한다. 비밀번호가 접근제어서버에 의해 성공적으로 확인될 경우, 단계 4에서, 디지털 방식으로 서명한 PARes 메시지가 접근제어서버(712)로부터 머천트 플러그-인 모듈에 전송되며, 거래가 인증되었음을 머천트에게 알린다. 거래 상태는 단계 5에서 지불 시스템(726)에 전달된다. 거래를 마치기 위해, 단계6에서, 머천트의 스토어프론트 소프트웨어(722)는 지불 데이터를 지불 시스템에 전송한다.

<94> 도 9는 발명의 한 실시예에 따르는 분산형 PAS 구조의 등록 흐름도이다. 앞서 언급한 바와 같이, 분산형 구조는 카드소지자 시스템에 소프트웨어와 데이터를 저장한다. 분산형 접근법에서는, 카드소지자 클라이언트 장치 상의 PAS 카드소지자 모듈 내 메카니즘을 통해 머천트가 카드소지자의 PAS 참가를 결정한다. 분산형 조직구조(900)는 인터넷 브라우저(904)를 포함하는 한개 이상의 카드소지자 클라이언트 장치(902)와, 등록 서버(908)를 포함하는 PAS(906)를 포함한다. 분산형 접근법에서는 디렉토리서버가 없다는 사실을 주목하라. 카드소지자가 단계 1에서 PAS에 등록하기 위해 은행 전용 인터넷 등록 페이지에 들어갈 때 등록 과정이 시작된다. 단계 2에서, 카드소지자는 인증 질문을 제시받는다. 단계 3에서, 카드소지자는 인증 질문에 대한 응답을 등록 서버(908)에 되보낸다. 카드소지자는 확인과정을 통해 단계 4에서 확인된다. 확인과정의 결과는 단계 5에서 등록 서버(908)에 되돌아온다. 카드소지자가 확인될 경우, 카드소지자 소프트웨어 모듈(910)과 인증서가 단계 6의 카드소지자에게 제공된다. 이들은 등록 서버로부터 인터넷 사이에서 다운로드된다.

<95> 도 10은 발명의 한 실시예에 따르는 분산형 PAS 구조의 지불 흐름도이다. 머천트 모듈(950)은 프론트 소프트웨어(952), 머천트 플러그-인 소프트웨어 모듈(954), 그리고 지불 시스템(956)을 포함한다. 지불 과정은 단계 1에서, 카드소지자가 머천트의 전자상거래 웹사이트에서 쇼핑을 하고 계산을 할 때 시작된다. 단계 2에서, 카드소지자 소프트웨어 모듈(910)이 카드소지자 클라이언트 장치 내에 있는 지를 머천트가 확인한다. 카드소지자 소프트웨어 모듈(910)이 존재할 경우, 머천트 모듈(954)은 중앙집중형 구조에서 접근제어서버와는 달리, 카드소지자 소프트웨어 모듈(910)에 PAReq 메시지를 전송한다. 발급자 접근제어서버의 인터넷 URL 주소를 알고있는 카드소지자 PAS 소프트웨어 모듈은 PAReq 메시지를 접근제어서버에 전달한다. 접근제어서버는 카드소지자 모듈과 대화하여, 카드소지자에게 비밀번호를 묻는다. 카드소지자에 의해 제시되는 비밀번호가 AHF 상의 동일 카드소지자에 대한 비밀번호와 같을 경우, 카드소지자가 인증된다. 그후 접근제어서버는 PARes 메시지로 머천트 모듈에 응답

한다(단계 4).

<96> 인증 과정의 상태 및 관련 데이터는 단계 5에서 지불 시스템(956)에 전달된다. 거래 영수증이 단계 6의 영수증 데이터베이스(960)에 전달된다. 거래와 지불을 완료하기 위해, 단계 7에서 프론트(storefront)로부터 지불 시스템에 데이터가 전송된다.

<97> **칩카드 실시예**

<98> 지불인 인증 서비스(PAS)의 칩카드 실시예는 (칩카드나 스마트카드라고도 알려진) 집적회로 카드를 이용하는 카드소지자와 칩카드 판독기를 포함한다. 칩카드 실시예는 온라인 구매 거래에서 또다른 수준의 인증을 추가한다. 앞서 설명한 PAS가 온라인 구매시 카드소지자의 신원 인증 능력을 제공하였고, PAS의 칩카드 실시예는 카드소지자가 실제 칩카드를 소지하는 지를 인증하는 능력을 역시 제공한다. 칩카드 인증을 확인하기 위해 사용될 수 있는 방법에는 여러 가지가 있다. 한가지 접근법은 칩에 의해 발생되는 시크릿을 이용하는 것으로서, 이는 발급자의 접근제어서버에 의해 확인될 수 있다.

<99> 칩카드 실시예는 카드 인증에 추가하여 본 문서에서 앞서 설명한 바와 같이 카드소지자를 인증하는 데 PAS를 이용할 수 있다. 접근제어서버에 PAS 비밀번호를 제공하기 위해 두 기술이 사용될 수 있다. 첫 번째 기술에서는 칩카드의 칩카드 신용 및 데빗 장치가 카드소지자에게 PAS 비밀번호를 입력하라고 프람프트를 제시한다. 카드소지자는 앞서 설명한 것과 마찬가지 방식으로 비밀번호를 입력한다. 비밀번호는 접근제어서버에 전달된다.

<100> 두 번째 기술에서는 PAS 비밀번호가 칩카드에 의해 접근제어서버에 자동적으로 공급된다. 이 기술은 칩카드에 저장된 비밀번호를 이용하여, 칩카드를 카드소지자가 이용할 수 있도록 하기 위해 카드소지자를 인증한다. 이 접근법은 "접근(ACCESS)" 애플릿이라 불리는 카드 상의 애플릿을 이용한다. 왜냐하면, 애플릿이 카드 및 그 상주 응용장치에 범용 접근을 제공하기 때문이고 카드소지자의 인증에 사용될 수 있기 때문이다. 접근 애플릿은 카드 상의 응용장치에 접근을 정지시킬 수 있다. 단일 범용 "접근" 비밀번호를 제시하고 카드소지자가 인증되면, 접근 애플릿은 카드소지자에게 여러 서비스나 응용프로그램에 접근하게 한다. 예를 들어, 단일 "접근" 비밀번호를 제시함으로서, 애플릿은 카드 상에 저장된 비밀번호를 이용할 수 있다.

<101> 일반적으로, 칩카드 실시예에 대한 설정 과정 및 인증 과정은 종래 카드 실시예와 동일하다. 칩카드 실시예와 종래 칩카드 실시예간 차이점은 아래 설명에서 드러날 것이다.

<102> PAS의 칩카드 실시예는 도 10A, 11, 12, 12A, 13을 들어 설명될 것이다. 도 10A는 칩카드 지불인 인증 서비스 구조의 한 실시예를 도시하고, 도 11은 인증된 지불 거래의 PAS 칩카드 및 카드소지자 인증의 일반적 설명을 제공하며, 도 12는 겹쳐진 과정 흐름과 함께 시스템 구조 배치의 조합을 도시하고, 도 12A는 칩카드로 지불인 인증 서비스를 이용하여 지불 거래 중 보다 상세한 메시지 흐름을 도시한다. 도 13은 칩카드 지불인 인증 시스템의 또다른 실시예를 설명하는 데 사용된다. 특히, 도 13은 칩 카드 상에 존재할 수 있는 여러 응용프로그램에 대한 접근 제어에 사용되는 접근 응용프로그램의 특징을 추가한 칩카드 실시예를 도시한다.

<103> 도 10A는 칩카드 지불인 인증 서비스의 한 실시예에 대한 고도의 시스템 구조도면이다. 지불 거래는 카드소지자가 카드소지자 클라이언트 장치(122)를 이용하여 머천트의 전자상거래 웹사이트에 접근할 때 시작한다. 카드소지자 클라이언트 장치(122)는 발급자 접근제어서버(114)에 연결되어, 칩 지불인 인증 접근제어서버 플러그-인(115)을 가진다. 발급자 접근제어서버(114)는 계좌 소유자 파일(118)에 연결되고, 다시 영수증파일(130)에 연결된다. 머천트(132)는 지불인 인증 서비스에 참가하기 위해 머천트 플러그-인 소프트웨어 모듈(134)을 이용한다. 머천트(132)는 디렉토리서버(128), 확인서버(136), 취득자 지불 프로세서(182)에 연결된다. 취득자 지불 프로세서(182)는 지불 통신망(126)에 연결되고, 다시 발급자(180)에게 연결된다.

<104> 도 11은 칩카드 시스템을 이용하여 지불 거래의 일반적 설명을 제공하는 순서도이다. 지불 거래는 블록 1100에서 시작한다. 즉, 온라인 머천트 웹사이트에서 카드소지자가 쇼핑을 하고 계산웹페이지에서 쇼핑을 마치려고할 때 지불거래가 시작된다. 블록 1110에서는, 가령, 카드소지자가 "구매" 버튼을 클릭한 후, 카드소지자가 PAS 등록 참가자임을 PAS가 확인한다. 그후 블록 1120에서, 머천트 플러그-인 모듈은 관련 접근제어서버에 PAReq 메시지를 전송하고, 이어서 카드소지자 클라이언트 장치가 칩카드 판독기를 포함한다는 것을 카드소지자 클라이언트 장치의 PAS 카드소지자 모듈을 통해 접근 서버가 확인하는, 블록 1130으로 진행된다. 카드소지자가 칩카드 판독기를 가지지 않을 경우, 지불 거래가 종료되거나 또다른 지불 방법이 사용되어야 한다.

<105> 카드소지자 클라이언트 장치가 칩카드 판독기를 가지고 있을 경우, 블록 1140에서, 소비자는 자신의 칩카드를 칩카드 판독기 내로 밀어넣는다. 블록 1150에서, 카드소지자 클라이언트 장치의 카드소지자 모듈은 칩카드에 내장된 비밀정보를 바탕으로 암호문을 발생시키도록 칩카드에 요청한다. 블록 1160에서, 카드소지자는 PAS 비밀번

호 입력을 요구받는다. 블록 1170에서, 칩카드에 의해 생성된 암호문가 카드소지자가 입력한 비밀번호가 인증을 위해 접근제어서버에 전송된다.

<106> 블록 1180에서, 도 4에서처럼 앞서 설명한 비-칩카드 PAS 시스템에 대해 설명한 것과 유사한 방법으로 PAS 비밀번호를 확인한다. 접근제어서버는 접근제어서버의 여러 구성성분의 정보를 이용하여 이 칩카드에 대한 암호문의 또다른 사본을 독립적으로 발생시킨다(도 12 참조). PAS 비밀번호가 부합하면, 카드소지자의 신원이 인증된다. 블록 1190에서, 각각의 칩카드와 접근제어서버에 의해 발생된 암호문이 부합할 경우, 실제 칩카드가 카드소지자에 의해 이용되고 있음이 확인된다. 블록 1195에서, 지불 응답 메시지가 접근제어 서버에 의해 머천트 플러그-인 소프트웨어 모듈에 다시 전달된다. 지불 응답 메시지는 카드 승인 확인값(CAVV)을 내장하여, 카드소지자가 인증되었고 실제 카드가 카드소지자 클라이언트 장치에서 사용되고 있고 적법한 카드임을 머천트에게 알린다. 구매 거래는 앞서 설명한 것과 마찬가지로 진행된다.

<107> 도 12에서는 발명의 한 실시예에 따르는 칩카드 시스템 구조에 겹쳐지는 지불 과정이 설명된다. 칩카드 인증 구조(1500)는 카드소지자 클라이언트 장치(1510), 발급자의 접근제어서버(1520), 카드소지자(1530), 칩카드(1540), 그리고 요청자(1550)를 포함한다. PAS 등록의 요청자는 통상적으로 머천트이다. 카드소지자 클라이언트 장치(1510)는 디스플레이 장치(1512), 단말기 소프트웨어(1514), PIN 패드나 키입력장치(1516), 그리고 카드 판독기(1518)를 포함한다. 카드판독기(1518)는 전기-기계적 장치로서, 카드 수용 장치나 인터페이스 장치(IFD)와 기능적으로 동등한 단말기 장치로 이용하기 위해 그 안으로 칩카드가 삽입된다.

<108> 접근제어서버(1520)는 PAS 인증 소프트웨어(1522), 하드웨어 보안 모듈(1524), 카드소지자 데이터베이스(1526), 시스템 소프트웨어(1528)를 포함한다. 칩카드(1540)는 비자 스마트 데빗 신용 장치(VSDC)같은 칩카드 신용 및 데빗 장치(1542)를 포함한다. VSDC 장치가 본 명세서에서 언급되는 상황에서 범용 데빗 및 신용 장치가 이용될 수 있다.

<109> 요청자(1550)는 특정 지불 거래에 관련된 머천트이다. 발급자 서버(1520)는 칩카드 암호문을 확인할 수 있는 발급자에 의해, 또는 발급자 대신에 제 3 자에 의해 운영되는 접근제어서버이다. 이 서버는 요청자(1550)와 카드소지자 클라이언트 장치(1510)간에 인터페이스로 작용한다. 카드소지자 클라이언트 장치(1510)는 개인용컴퓨터, 이동전화, 셋톱박스, 또다른 그 외 다른 유사성분들처럼, 카드소지자(1530), 칩카드(1540), 그리고 발급자의 접근제어서버(1520) 사이에서 인터페이스로 작용하는 소프트웨어와 구성성분들의 시스템이다.

<110> 카드소지자(1530)는 카드소지자 클라이언트 장치(1510)의 제어 하에 있는 자로서, 카드 삽입, PIN 입력, 또는 카드소지자 클라이언트 장치(1510)의 구성성분들이 적절히 동작하는 지 여부 확인 등의 기능을 실행할 수 있다. 칩카드(1540)는 가령 비자 스마트 데빗 신용 장치처럼, 칩카드 신용 및 데빗 장치를 내장하는 발급자로부터의 지불 카드이다.

<111> 도 12의 원들을 참고하여, 다음은 칩카드 지불 인증 과정 중 발생하는 것을 설명하는 간단한 시나리오다. 단계 1에서, 칩카드가 인증이 요구되는 것을 머천트같은 요청자들이 결정하고, 발급자 접근제어서버에 칩카드 인증 실행을 요청한다.

<112> 단계 2에서, 지불 요청 메시지로부터 인증될 카드에 대한 주계좌번호(PAN)을 얻은 발급자 접근제어서버는, VSDC 인증 요청이라 불리는 메시지를 카드소지자 클라이언트 장치에 전송한다.

<113> 단계 3에서, 발급자 접근제어서버로부터 요청에 따라 동작하는 카드소지자 클라이언트 장치는 카드 인증을 시도한다. 먼저, 필요한 구성성분들이 존재하고 동작하는 지를 결정한다. 디스플레이 장치에 메시지를 띄움으로서, 카드소지자 클라이언트 장치는 카드소지자에게 칩카드를 칩카드 판독기 내로 삽입할 것을 요청한다.

<114> 단계 4에서, 카드소지자는 카드 판독기에 칩카드를 삽입함으로서 응답하고, 카드가 삽입되었음을 알리는 메시지를 카드소지자 클라이언트 장치에 발생시키며, 또는 카드 판독기가 얼마나 정교한 지에 따라, 카드소지자 클라이언트 장치는 카드를 지금 읽을 수 있는 지 결정하기 위해 경로 번호 5를 이용하여 카드 판독기에 투표할 필요가 있다.

<115> 단계 5에서, 카드소지자 클라이언트 장치는 칩카드 및 칩카드 상의 VSDC 장치를 초기화하고, 차후 확인을 위해 칩카드로부터 암호문 회송을 전달하도록 서로와 통신한다.

<116> 단계 6에서, 칩카드와 통신하는 과정에서 여러 교환이 발생한다. 칩카드는 카드소지자가 PIN을 입력할 것을 요청할 수 있다. 만약 그러하다면, 카드소지자 클라이언트 장치는 PIN 패드나 그 외 다른 키입력 장치를 이용하여 PIN을 입력함을 카드소지자에게 알린다.

<117> 단계 7에서, 단계 5와 6의 카드로부터 메시지를 전송하고 응답을 수신하면서, 카드소지자 클라이언트 장치는 이제 발급자 접근제어서버에 전송할 VSDC 인증 응답을 구성하는 데 필요한 정보를 모으고 있다. VSDC 인증 응답 메시지에 제공되는 정보를 이용하는 접근제어서버는 비밀번호를 통해 카드소지자를 인증하고 암호문을 통해 칩카드를 인증하려 시도한다.

<118> 단계 8에서, 발급자의 접근제어서버는 지불 응답 메시지를 통해 머천트나 요청자에게 응답하고, 카드소지자와 칩카드 인증 과정의 결과를 함께 답변한다.

<119> VSDC 인증 서비스의 각 실체의 주요 기능적 능력이 이제부터 설명될 것이다. 요청자나 머천트는 다음과 같은 기능을 한다. 즉, 칩카드 VSDC 인증 과정을 개시하기 위해 발급자 접근제어서버에 신호를 보내거나 트리거링하고, VSDC 인증을 실행하기 위해 필요한 데이터를 발급자 접근제어서버에 제공하고, 발급자 접근제어서버에 의해 제공되는 VSDC 인증결과를 이용한다.

<120> 발급자의 접근제어서버는 다음과 같은 기능을 한다. 즉, 암호문 확인에 필요한 암호 키를 안전하게 저장하며, VSDC 인증 처리 수행을 위해 필요한 데이터를 수집하고, VSDC 인증 요청 메시지를 카드소지자 클라이언트 장치 소프트웨어에 전송함으로서 VSDC 인증 처리를 개시하며, 첨부된 하드웨어 보안 모듈(HSM)에서 카드소지자 클라이언트 장치를 통해 칩카드로부터 전달된 암호문을 확인하고, 그리고 지불 응답 메시지를 통해 요청자나 상인에게 암호문 확인 결과를 제공한다.

<121> 카드소지자 클라이언트 장치는 다음과 같은 기능을 한다. 즉, 발급자 접근제어서버와 통신하고, VSDC 인증 요청 메시지를 수신하며, 카드 삽입/제거 및 PIN 입력을 위해 카드소지자와 통신하며, 칩카드와 통신하고, VSDC 인증에 필요한 데이터를 칩카드에 전송하며, VSDC 인증에 필요한 데이터를 칩카드로부터 수신하고, 암호문을 칩카드로부터 수신하며, 그리고 카드에 의해 발생된 암호문을 발급자 접근제어서버에 전송한다. 카드소지자 클라이언트 장치는 비밀번호를 입력하도록 카드소지자에게 요청하고, 입력된 비밀번호를 접근제어서버에 전달한다.

<122> 카드소지자는 칩카드를 카드 판독기에 넣고, 칩카드 환경이 준비된 상태인 지를 결정하며, PIN을 입력하고, 칩카드를 카드 판독기로부터 빼내고, 비밀번호를 입력하는 이러한 기능들을 한다.

<123> **상세한 메시지 흐름 예**

<124> 도 12A는 칩카드(1540), 카드소지자 클라이언트 시스템(1510), 그리고 발급자의 접근제어서버(1520) 사이에 메시지 흐름을 상세하게 설명한다. 이 메시지 흐름은 칩카드 지불 인증 처리가 실행되는 방식을 규정한다. 메시지 흐름은 인증 과정의 단계들을 따라 진행하는 하향식으로 조직된다.

<125> 이 문단은 발생하는 순서대로 VSDC 인증 처리 단계들을 간단하게 설명한다.

<126> 4.2.2.1 VSDC 인증 요청 - 발급자의 접근제어서버는 VSDC 인증 처리를 시작한다.

<127> 4.3.2.1 개시 - 카드소지자 클라이언트 장치 소프트웨어는 칩카드를 카드 판독기에 삽입하라고 카드소지자에게 프람프트를 띄운다.

<128> 4.3.2.2 응용프로그램 선택 - 카드소지자 클라이언트 장치 소프트웨어는 VSDC 응용프로그램을 칩카드로부터 선택한다.

<129> 4.3.2.3 응용프로그램 개시 - 카드소지자 클라이언트 시스템 장치와 칩카드는 VSDC 인증 처리를 개시한다.

<130> 4.3.2.4 응용프로그램 데이터 판독 - 카드소지자 클라이언트 시스템 장치는 칩카드로부터 응용프로그램 데이터를 판독한다.

<131> 4.3.2.5 카드소지자 확인(부가적) - 카드소지자 클라이언트 장치 소프트웨어는 카드소지자 확인을 위해 오프라인 PIN 확인을 수행한다.

<132> 4.3.2.6 단말기 동작 분석 - 카드소지자 클라이언트 시스템 장치는 칩카드에 암호문 발생을 요청한다.

<133> 4.3.2.7 완료 - 카드소지자 클라이언트 장치 소프트웨어는 VSDC 인증 과정을 완료한다.

<134> 4.2.1.2 VSDC 인증 응답 - 카드소지자 클라이언트 장치 소프트웨어는 암호문과 나머지 데이터를 발급자 접근제어서버에 되보낸다.

<135> 카드소지자 클라이언트 장치 소프트웨어와 칩카드간 흐름을 발생시키는 데 관련된 메시지 흐름 및 기능이 설명될 것이다. VSDC 인증 요청은 과정 시작을 위해 카드소지자 클라이언트 장치 소프트웨어를 호출하도록 발급자

접근제어서버로부터 카드소지자 클라이언트 장치 소프트웨어에 필요한 데이터를 전송하는 메시지이다. VSDC 인증 응답은 카드소지자 클라이언트 장치 소프트웨어로부터의 지원 데이터와 암호문을 발급자 접근제어서버로 되보내는 메시지이다.

<136> 이제부터, 메시지 및 과정 흐름이 상세하게 설명될 것이다.

<137> VSDC 인증 요청은 VSDC 인증 과정을 시작하기 위해 카드소지자 클라이언트 장치 소프트웨어를 호출하는 메시지이다. 이 메시지는 암호문 생성을 위해 칩카드에 대해 필요한 데이터를 내장한다.

<138> 발급자의 접근제어서버는 여기서 나열한 필요 데이터를 얻거나 발생시켜야 한다. 즉, 승인 금액, 응용프로그램 식별자, (VSDC 응용프로그램의) 응용프로그램 수준, 응용프로그램 선호 명칭, 단말기 국가 코드, 거래 통화 코드, 거래일자, 거래종류, 예측불가능한 번호를 얻거나 발생시켜야 한다.

<139> 이 데이터들의 소스는 VSDC 인증이 동작중인 인증 환경에 따라 변화한다. 발급자의 접근제어서버는 카드소지자 클라이언트 장치 소프트웨어에 이 데이터들을 운반하기 위해 VSDC 인증 요청을 구축하여야 한다. 이 메시지는 카드소지자 클라이언트 장치 소프트웨어와 칩카드 사이에서 과정을 시작하기 위해 카드소지자 클라이언트 장치 소프트웨어를 호출하여야 한다.

<140> 카드소지자 클라이언트 장치 소프트웨어는 개시 과정을 시작하여야 한다(선호됨).

<141> **4.2.1.2 VSDC 인증 응답**

<142> VSDC 인증 응답은 암호문과 나머지 지원 데이터를 발급자 접근제어서버에 운반하는 메시지이다. VSDC 인증 응답 메시지는 VSDC 인증 처리 중 오류와 예외가 발생할 때 상태 코드를 전달하는 데 또한 사용된다. VSDC 인증 응답 메시지는 카드소지자 비밀번호를 접근제어서버에 제공하기 위해 또한 이용된다.

<143> 카드소지자 클라이언트 장치 소프트웨어는 아래 표 1에 설명되는 모든 필요 데이터를 얻어야 한다.

<144> **표 1**

<145>

데이터요소	소스
암호문	제 1 GENERATE AC 응답 메시지로부터
도출키인덱스	제 1 GENERATE AC 응답 메시지로부터 (DKI는 발급자 응용프로그램 데이터의 한 구성성분)
암호문버전번호	제 1 GENERATE AC 응답 메시지로부터 (암호문 버전 번호는 발급자 응용프로그램 데이터의 구성성분)
응용프로그램교환프로파일(AIP)	GET PROCESSING OPTIONS 응답 메시지로부터
응용프로그램거래카운터(ATC)	제 1 GENERATE AC 응답 메시지로부터
카드확인결과(CVR)	제 1 GENERATE AC 응답 메시지로부터(CVR은 발급자 응용프로그램 데이터의 구성성분)
단말기확인결과(TVR)	카드소지자 클라이언트 장치 소프트웨어로부터
PAN순서번호	READ RECORD 응답 메시지로부터
상태코드	카드소지자 클라이언트 장치 소프트웨어로부터
예비1	"0000000000000000000"에 의해 제출됨
예비2	규정되지 않은 포맷과 내용, 10바이트

<146> 카드소지자 클라이언트 장치 소프트웨어는 발급자 접근제어서버에 이 데이터들을 운반하기 위해 VSDC 인증 응답 메시지를 구축하여야 한다.

<147> 발급자의 접근제어서버는 VSDC 인증 응답으로부터 데이터를 불러들여야 하고, 암호문과 카드소지자 비밀번호를 확인하여야 한다. 발급자의 접근제어서버는 카드소지자 클라이언트 장치 소프트웨어와 칩카드 사이에 과정이 성공적으로 완료될 때, 그리고 오류나 예외사항이 발생할 때 상태 코드를 내장한 VSDC 인증 응답을 수령한다. 발급자의 접근제어서버는 오류와 예외사항이 발생할 때 카드소지자로부터 질의에 응답하기 위해, 그리고 칩카드와 카드소지자 클라이언트 장치 소프트웨어 사이에 발생하는 과정을 분석하기 위해 상기 정보를 발급자가 이용할 수 있도록, 카드소지자 클라이언트 장치 소프트웨어로부터 상기 데이터를 저장할 수 있다.

<148> 발급자 접근제어서버에서의 부가적 과정 - 인증환경이 요청할 경우, 발급자 접근제어서버는 인증 결과를 머천트나 요청자에게 전송할 필요가 있다. 일부 환경에서는, 암호문 인증이 이루어졌는지 그리고 성공적인 지를 발급자 접근제어서버가 전송할 수 있다. 주: VSDC 인증 응답은 카드소지자 클라이언트 장치 소프트웨어가 오류나 다른 이유로 인해 조기에 종료되는 경우에도 항상 전송된다.

<149> 카드소지자 클라이언트 장치 소프트웨어와 칩카드 상의 VSDC 응용프로그램 간에 흐름을 발생시키는 데 관련된 메시지 흐름 및 기능들이 이제부터 설명될 것이다. 먼저, 칩카드 메시지 흐름에 대한 카드소지자 클라이언트 장치 소프트웨어 기능의 처리 흐름 개관이 제공된다. 이 기능들은 개시, 응용프로그램 선택, 응용프로그램 개시, 응용프로그램 데이터 판독, 카드소지자 확인, 단말기 작용 분석, 그리고 완료이다.

<150> 개시는 칩카드가 카드 판독기 내에 삽입되고 처리 준비가 되었음을 카드소지자 클라이언트 장치 소프트웨어가 어떻게 보장하는 지를 설명한다. 응용프로그램 선택은 VSDC 인증 과정동안 칩카드 상의 VSDC 응용프로그램을 카드소지자 클라이언트 장치 소프트웨어가 어떻게 선택해 나가는 지를 설명한다. 응용프로그램 개시는 카드소지자 클라이언트 장치 소프트웨어가 칩카드 상의 VSDC 응용프로그램을 어떻게 개시하는 지를 설명한다. 응용프로그램 데이터 판독은 칩카드로부터 VSDC 응용프로그램 데이터를 카드소지자 클라이언트 장치 소프트웨어가 어떻게 판독하는 지를 설명한다. 카드소지자 확인은 카드소지자 확인을 카드소지자 클라이언트 장치 소프트웨어가 어떻게 실행하는 지를 설명한다. 단말기 동작 분석은 암호문을 발생시키도록 카드소지자 클라이언트 장치 소프트웨어가 칩카드에게 어떻게 요청하는 지를 설명한다. 완료는 카드소지자 클라이언트 장치 소프트웨어가 칩카드 처리를 종료하고 그 처리를 종료하는 방법을 설명한다.

<151> 각 흐름 및 메시지에 대한 상세한 설명이 제공될 것이다.

<152> **4.3.2.1 개시** - 개시 단계는 두개의 서브-단계로 구성된다. 하나는 카드소지자 클라이언트 장치에 대한 카드 환경의 개시이고, 다른 하나는 칩카드에 대한 개시이다.

<153> 카드소지자 클라이언트 장치 소프트웨어는 카드 판독기와 카드 판독기를 동작시키기 위해 필요한 그관련 장치 지원 소프트웨어가 카드 삽입 가능하다는 것을 보장해야한다. 카드 환경이 준비되지 않았을 경우, 카드소지자 클라이언트 장치 소프트웨어는 카드소지자 클라이언트 장치에서의 조건이 정확하게 설정되었음을 확인하기 위해 카드소지자와 통신하여야 한다. 카드소지자와의 통신은 카드 판독기가 적절히 부착되었는 지, 전력이 온 상태인지, 그리고 카드 판독기 드라이버 소프트웨어의 정확한 버전이 설치되었는 지와 같은 질문을 하는 과정을 포함한다. 카드소지자 클라이언트 장치 소프트웨어는 카드 환경이 준비될 수 없다고 결정될 때 VSDC 인증 과정을 종료할 수 있다. 카드소지자 클라이언트 장치 소프트웨어가 과정을 중단할 경우, 모든 일련의 단계들을 건너뛰고 적절한 상태 코드와 함께 VSDC 인증 응답 메시지를 발급자 서비스에게 되돌려보내야 한다.

<154> 서브 단계 "4.3.2.1.2 칩카드에 대한 개시"가 실패하면, 제어는 이 서브단계로 되돌아가, 카드소지자 클라이언트 장치 소프트웨어가 칩카드 삽입을 카드소지자에게 제시하는 프람프트를 띄운다. 카드소지자 클라이언트 장치 소프트웨어는 카드 삽입을 요청하고 "칩카드에 대한 개시"로 되돌아간 후, 칩카드가 응답에 실패할 경우, VSDC 인증 과정을 종료할 수 있다. 카드소지자 클라이언트 장치 소프트웨어가 VSDC 인증 과정을 종료할 때, 모든 일련의 단계들을 건너뛰어야 하고, VSDC 인증 응답 메시지를 적절한 상태 코드와 함께 발급자 접근제어서버에 전송하여야 한다.

<155> 칩카드에 대한 개시 - 이 서브 과정에서 카드소지자 클라이언트 장치 소프트웨어는 처리 준비가 되었는 지를 결정하기 위해 칩카드와 통신한다.

<156> 카드소지자 클라이언트 장치 소프트웨어는 칩카드를 재설정하여야 한다(선호됨). 칩카드는 카드소지자 클라이언트 장치 소프트웨어에 재설정에 대한 답변(ANSWER TO RESET; ATR)을 되보내고, 그렇지 않을 경우 ATR을 되보내는 데 실패한다.

<157> 카드소지자가 클라이언트 장치 소프트웨어가 ATR을 수신하면, 다음 단계인 응용프로그램 선택으로 진행한다. 칩카드가 표준으로 설정된 시간 내에 ATR을 돌려보내지 못하면, 카드소지자 클라이언트 소프트웨어는 "4.3.2.1.1 카드소지자 클라이언트 장치 상의 카드 환경에 대한 개시"로 되돌아갈 수 있고, 또는 VSDC 인증 처리를 종료할 수 있다. 카드소지자 클라이언트 장치 소프트웨어가 VSDC 인증 과정을 종료할 때, 모든 일련의 단계들을 건너뛰어야 하고, 적절한 상태 코드와 함께 VSDC 인증 응답 메시지를 발급자 서버에 전송하여야 한다.

<158> **4.3.2.2. 응용프로그램 선택**

<159> 응용프로그램 선택은 카드소지자 클라이언트 장치 소프트웨어가 칩카드로부터 VSDC 응용프로그램을 선택하는 처

리 단계이다.

<160> 카드소지자 클라이언트 장치 소프트웨어에서의 처리는 아래의 사항들을 포함한다.

<161> a) 카드소지자 클라이언트 장치 소프트웨어는 응용프로그램 선택을 실행하여야 한다(선호됨).

<162> b) 보안요청사항에 부합하기 위해, 카드소지자 클라이언트 장치 소프트웨어는 외부적 선택 방법만을 이용하여, VSDC 인증 요청에서 공급되는 바와 같이 AID(응용프로그램 ID)를 가진 선택(SELECT) 명령을 전송하여야 한다.

<163> c) 첫 번째 SELECT 명령에 대한 응답이 첨자없이 AID를 되돌려보낼 경우, 카드 상에서 요청된 AID에 대한 응용프로그램의 사례가 한가지만 존재한다. 처리과정은 아래의 g)로 이어진다.

<164> d) 카드 상에서 요청한 AID에 대한 응용프로그램의 사례가 여러 가지 있음을 표시하는 첨자를 가진 AID를 첫 번째 SELECT 명령에 대한 응답이 되돌려보낸 경우, 처리과정은 아래의 단계 e)~g)로 이어진다.

<165> e) 요청한 AID를 되돌리기 위한 응용프로그램의 추가적 사례가 없음을 카드가 표시할 때까지 AID를 이용하여 일련의 SELECT 명령을 발급함으로서, 각각의 AID가 되돌아옴에 따라, 카드소지자 클라이언트 장치 소프트웨어는 각각의 AID에 대해 대응하는 응용프로그램 라벨과 응용프로그램 선호 명칭과 함께 AID의 리스트를 구성한다.

<166> f) VSDC 인증 요청에 공급되는 바와 같이 응용프로그램 라벨과 응용프로그램 선호 명칭을 이용하여, 카드소지자 클라이언트 장치 소프트웨어는 일치점을 찾기 위해 종래 단계에서 만들어진 리스트를 검색한다. 부합하는 리스트 참가자의 AID를 이용하여 SELECT 명령이 카드에 발급된다. 어떤 부합점도 발견되지 않으면, 적절한 상태 코드가 아래의 "예외 처리"에서 나타나는 바와 같이 VSDC 인증 응답에서의 복귀하도록 설정된다.

<167> g) 카드소지자 클라이언트 장치 소프트웨어에 대한 응용프로그램 선택이 완료된다. 카드에 한개의 적절한 응용프로그램이 있어서, 앞서 단계 c)에서 선택된다. 또는, 여러개의 적절한 응용프로그램 사이에서 결정되고, 앞서 단계 f)에서 그 중 하나가 선택된다.

<168> h) 카드소지자 클라이언트 장치 소프트웨어와 칩카드가 VSDC에 추가하여 여러 응용프로그램을 지원할 때, 어느 다른 응용프로그램들이 어떤 순서로 실행될 지를 결정하는 것이 발급자의 책임이다.

<169> 칩카드는 응용프로그램 선택을 실행한다.

<170> 예외 처리 - VSDC 응용프로그램이 발견되지 않으면, 카드소지자 클라이언트 장치 소프트웨어는 VSDC 인증 과정을 종료하여야 한다(선호됨). 카드소지자 클라이언트 장치 소프트웨어가 VSDC 인증 과정을 종료할 때, 모든 일련의 단계들을 건너뛰고, 적절한 상태코드와 함께 VSDC 인증 응답을 발급자 서버에 전송하여야 한다(선호됨).

<171> **4.3.2.3 응용프로그램 개시**

<172> 응용프로그램 개시는 카드소지자 클라이언트 장치 소프트웨어가 거래 처리를 시작 중임을 칩카드에 신호하는 처리 단계이다.

<173> 카드소지자 클라이언트 장치 소프트웨어는 응용프로그램을 개시하여야 한다(선호됨). 카드소지자 클라이언트 장치 소프트웨어는 VSDC 응용프로그램을 개시하기 위해 칩카드에 GET PROCESSING OPTIONS 명령을 전송하여야 한다(선호됨).

<174> 칩카드는 GET PROCESSING OPTIONS 명령에 응답한다.

<175> 카드소지자 클라이언트 장치 소프트웨어는 VSDC 인증 응답을 만들기 위해 차후 단계에서 사용될 응용프로그램 교환 프로파일을 저장하여야 한다(선호됨). 지정학적 제한을 부여하는 것은 VSDC 응용프로그램의 부가적 기능 중 하나이다.

<176> 이용 조건이 만족스럽지 못함을 표시하는 오류 코드와 함께 GET PROCESSING OPTIONS 명령에 칩카드가 응답할 때, VSDC 인증 처리는 반드시 종료되어야 한다.

<177> 카드가 거래를 종료할 경우, 카드소지자 클라이언트 소프트웨어 장치는 모든 일련의 단계들을 건너뛰어야 하고 적절한 상태코드와 함께 VSDC 인증 응답 메시지를 발그바 서버에 전송하여야 한다(선호됨). 주: VSDC 인증 과정의 종료 후 취해야할 동작을 결정하는 것은 발급자의 책임이다. 이러한 결정 및 결과적 동작은 본 발명의 범위를 벗어난다.

<178> **4.3.2.4 응용프로그램 데이터 판독** - 응용프로그램 데이터 판독은 칩카드 상에서 VSDC 응용프로그램 파일의 레코드를 카드소지자 클라이언트 장치 소프트웨어가 판독하는 처리단계이다.

<179> 카드소지자 클라이언트 장치 소프트웨어는 VSDC 응용프로그램 데이터를 판독하여야 한다. 카드소지자 클라이언트 장치 소프트웨어는 VSDC 응용프로그램으로부터 필요한 데이터를 불러내기 위해 READ RECORD 명령을 전송하여야 한다(선호됨). 카드소지자 클라이언트 장치 소프트웨어는 VSDC 인증 응답의 구성을 위해 차후 용도로 PAN 순서 번호 값을 유지해야한다(선호됨).

<180> VSDC 응용프로그램은 READ RECORD 명령에 응답한다.

<181> **4.3.2.5 카드소지자 확인** - 카드소지자 확인은 오프라인 PIN 확인 방법을 이용함으로서 카드소지자 클라이언트 장치 소프트웨어가 카드소지자를 확인할 수 있는 처리 단계이다. 주: 카드소지자 확인은 적절한 비자 보안 가이드라인에 부합하게 구현되어야 한다.

<182> 실행 조건 - 이 단계는 조건부이다. 즉, 카드소지자 확인이 카드소지자 클라이언트 장치 소프트웨어로 카드 상에서 구현되고 가용할 경우에만 요구된다.

<183> 카드소지자 클라이언트 장치 소프트웨어는 오프라인 플레인텍스트 PIN 확인 방법을 이용하여 카드소지자를 확인하여야 한다(선호됨). 오프라인 암호화 PIN 확인 방법이나 온라인 PIN 확인이 지원되지 않는다.

<184> 칩카드는 오프라인 플레인텍스트 PIN 확인을 실행한다. 첫 번째 GENERATE AC 명령에 따라, 칩카드는 CVR의 오프라인 PIN 확인 결과를 제공한다.

<185> **4.3.2.6 단말기 동작 분석** - 단말기 동작 분석은 카드소지자 클라이언트 장치 소프트웨어가 칩카드에게 암호문 발생을 요청하는 과정의 단계이고, 이는 확인을 위해 발급자 서버에 전달될 것이다.

<186> 카드소지자 클라이언트 장치 소프트웨어는 단말기 동작 분석을 실행하여야 한다(선호됨). 카드소지자 클라이언트 장치 소프트웨어는 "머천트 POS 단말기"의 역할을 가정해야하고, 다음의 예외사항을 가진 단말기처럼 행동해야 한다.

<187> a) 발급자 동작 코드 및 단말기 동작 코드 처리: 카드소지자 클라이언트 장치 소프트웨어는 단말기 확인 결과를 칩카드 발급자 동작 코드나 단말기 동작 코드와 비교하면 안된다.

<188> b) GENERATE AC 명령: 카드소지자 클라이언트 장치 소프트웨어는 ARQC만을 요청함으로서 GENERATE AC 명령을 만들어야 한다(선호됨). 즉, 단말기 동작 분석중 AAC나 TC를 요청하면 안된다.

<189> 단말기 확인 결과(TVR) 값 - 단말기 확인 결과는 카드소지자 클라이언트 장치에 의해 실행되는 여러 응용프로그램 기능의 출력의 레코드이다. POS 단말기에서의 표준 VSDC 처리와 다른 점이라면, 일부 값들이 VSDC 인증에 대해 정적(static)이라는 것이다. 정적인 비트에 할당될 값들은 아래에 표시된다. 동적으로 설정되는 값을 가지는 비트들은 VSDC 인증 과정의 코스 중 카드소지자 클라이언트 장치에 의해 설정될 것이다.

<190> 칩카드는 암호문을 생성한다.

<191> **4.3.2.7 완료** - 완료는 카드소지자 클라이언트 장치 소프트웨어가 칩카드 처리를 종료하는 처리 단계이다.

<192> 처리 변화 - 카드소지자 클라이언트 장치 소프트웨어 처리는 GENERATE AC 응답 메시지를 바탕으로 변해야 한다(선호됨). 카드소지자 클라이언트 장치 소프트웨어는 완료를 실행하여야 한다(선호됨). 카드소지자 클라이언트 장치 소프트웨어가 온라인 승인(ARQC)에 대해 첫번째 GENERATE AC 명령을 발급할 경우에도 VSDE 응용프로그램은 거래 오프라인(AAC)을 거절하는 권리를 칩카드에 제공한다. 따라서, 클라이언트 카드소지자 장치 소프트웨어는 VSDC 인증 과정 중 ARQC나 AAC를 되돌려보낼 것이다. GENERATE AC의 출력이 ARQC나 AAC인 지를 결정하기 위해, 발급자 접근제어서버가 CVR을 확인할 수 있다.

<193> VSDC 인증은 칩카드로부터의 응답이 오프라인 거절(AAC)임에도 불구하고 과정을 계속해야한다(선호됨). 응답이 거절되었다고 표시됨에도 되돌아온 암호문이 카드 인증에 사용될 수 있기 때문에 처리가 계속될 수 있다. VSDC 인증은 암호문 종류에 상관없이 카드 인증을 위해 암호문을 필요로한다.

<194> 4.3.2.7.1 카드 응답은 ARQC

<195> 이 문단은 칩카드가 승인 요청 암호문(Authorization ReQuest Cryptogram; ARQC)을 되돌려보낼 때 처리 흐름을 설명한다. VSDC 인증의 경우에는 이러한 해석이 관련이 없다. 왜냐하면, 승인이 요청되지 않을 것이고 VSDC 인증이 항상 "온라인"과정이기 때문이다. GENERATE AC 명령을 발급하는 목적은 확인을 위해 카드가 암호문을 되돌려보내게 하는 것이다.

<196> 칩카드로부터 ARQC로 첫 번째 GENERATE AC 응답을 수령한 후, 카드소지자 클라이언트 장치 소프트웨어는 아래의 과정을 실행하여야 한다(선호됨).

<197> 카드소지자 클라이언트 장치 소프트웨어는 발급자 서버에 전송하기 위해 칩카드로부터 전송되는 아래의 데이터 요소를 제외하고는 어떤 다른 데이터도 유지하지 않으며 오직 암호문만 유지한다. 표 2 참조.

<198> **표 2**

<199>

데이터	요소 소스
암호문	첫 번째 GENERATE AC 응답 메시지로부터
도출 키 인덱스(DKI)	첫 번째 GENERATE AC 응답 메시지로부터 (DKI는 발급자 응용프로그램 데이터의 구성성분)
암호버전번호	첫 번째 GENERATE AC 응답 메시지로부터 (암호버전번호는 발급자응용프로그램 데이터의 구성성분)
응용프로그램거래카운터(ATC)	첫 번째 GENERATE AC 응답 메시지로부터
카드확인결과(CVR)	첫 번째 GENERATE AC 응답 메시지로부터 (CVR은 발급자 응용프로그램 데이터의 구성성분)

<200> 카드소지자 클라이언트 장치 소프트웨어는 VSDC 인증 응답을 준비하고 전송하기 위해 차후 단계에 필요한 정보를 저장하여야 한다(선호됨). 그후, 카드소지자 클라이언트 장치 소프트웨어는 온라인 승인 응답이 발급자에 의해 승인되지 않는 거래를 표시하는 것처럼 칩카드에 최종 GENERATE AC 명령을 발급하여야 한다(선호됨). 이는 카드소지자 클라이언트 장치 소프트웨어가 AAC를 요청한다는 것을 의미한다. 주: VSDC 인증 처리에는 어떤 승인 요청/응답 메시지도 없다.

<201> CDOL2에 나열된 데이터 소스 - 카드소지자 클라이언트 장치 소프트웨어가 최종 GENERATE AC 명령의 데이터 필드 내 칩카드에 전송하는 데이터 요소는 아래 표 3에 표시되는 소스로부터 얻어야 한다(선호됨).

<202> **표 3**

<203>

데이터 요소	소스
승인 금액	네트워크-기반 VSDC 인증 요청 메시지로부터
다른 금액	네트워크-기반 VSDC 인증 요청 메시지로부터
단말기국가코드	네트워크-기반 VSDC 인증 요청 메시지로부터
단말기확인결과(TVR)	카드소지자 클라이언트 장치 소프트웨어로부터
거래통화코드	네트워크-기반 VSDC 인증 요청 메시지로부터
거래일자	네트워크-기반 VSDC 인증 요청 메시지로부터
거래종류	네트워크-기반 VSDC 인증 요청 메시지로부터
예측불가능한번호	네트워크-기반 VSDC 인증 요청 메시지로부터

<204> 칩카드는 최종 GENERATE AC 명령에 대한 응답을 AAC로 되돌려보낸다.

<205> 카드소지자 클라이언트 장치 소프트웨어는 칩카드로부터 최종 GENERATE AC 명령까지 응답을 무시하여야 한다(선호됨). 카드소지자 클라이언트 장치 소프트웨어는 칩카드로부터 수신한 무관한 데이터를 메모리로부터 삭제함으로서 보안 요청사항과 부합하여야 한다(선호됨). 주: 앞서 단계들로부터 모든 종래 비사용 데이터를 이때까지 보안 요구사항과 부합하면서 삭제하였다고 가정한다.

<206> **카드 응답은 AAC**

<207> 이 서브문단은 칩카드가 응용프로그램 인증 암호문(AAC)을 돌려보낼 때의 처리 흐름을 도시한다. VSDC 인증의 경우에, 이러한 해석은 관련이 없다. 왜냐하면, 승인이 요청되지 않았기 때문이다. GENERATE AC 명령을 발급하는 목적은 칩카드 인증을 위해 암호문을 카드가 되보내게 하는 것이다.

<208> **접근 응용프로그램을 갖춘 칩카드 실시예**

<209> 도 12A의 메시지 흐름에 대한 설명이 완료된 이상, 접근 응용프로그램을 이용하는 칩카드 장치의 실시예들이 이제부터 제시될 것이다.

<210> 칩카드 시스템의 추가적 실시예들은 칩카드 시스템의 추가적 특징으로 부가적으로 이용될 수 있는 접근 응용프로그램을 포함한다. 접근 응용프로그램은 칩카드에 대한 접근을 제어하기 위해 사용되며, 칩카드 상에 위치할 수 있는 여러 응용프로그램에 대한 접근을 제어하기 위해 사용된다. 접근 응용프로그램은 "접근응용프로그램이나 애플릿"으로 불릴 수 있다. 접근응용프로그램은 칩카드에 위치하는 나머지 응용프로그램에 대한 접근을 제어한다. 이 방식으로, 접근 응용프로그램은 칩카드 및 그 관련 응용프로그램을 이용하려 시도하는 자의 신원을 확인할 수 있다. 칩카드를 이용하려 시도하는 자가 정확한 사용자 신원 번호나 스트링, 비밀번호를 입력할 경우, 승인된 자가 칩카드를 사용하려한다고 간주된다. 이 경우에, 접근 응용프로그램은 칩카드 상의 모든 응용프로그램의 잠금장치를 해제하여, 사용될 수 있도록 한다. 응용프로그램 잠금장치 해제에 추가하여, 접근 응용프로그램은 칩카드 상의 응용프로그램에 대한 비밀번호를 이용할 수 있게 한다. 접근 응용프로그램의 일부 실시예에서, 접근 응용프로그램에 따라 정확한 정보를 입력한 후 일부 선택된 숫자의 응용프로그램만이 잠금장치를 해제할 것이다.

<211> 카드소지자가 입력하거나 발급자 접근제어서버가 확인하는 비밀번호나 비밀값에 대해 여러 기준이 있다. 표 4에 도시되는 바와 같이, 시크릿 #1, #2, #3는 서로 다른 값들이다(그리고 이들 중 어느것도 금융 ATM이나 POS PIN이 아니다).

<212> **표 4: 비밀번호 및 비밀값**

<213>

시크릿#1	칩-기반 지불인 인증을 위해 칩카드 접근 응용프로그램에 접근할 수 있게 하는 카드소지자에 의해 규정된 비밀번호. 일부 실시예에서, 시크릿#1은 PAS 응용프로그램을 포함하여 스마트카드 상의 모든 응용프로그램을 스마트카드 상의 접근 프로그램이 개방하게 한다.
시크릿#2	칩-기반 지불인 인증을 위해 카드소지자를 접근제어서버가 확인할 수 있도록 칩카드 접근 응용프로그램에 의해 되돌아오는 발급자에 의해 규정되는 비밀번호. 카드소지자는 스마트카드 상의 응용프로그램을 불러오는 데 비밀번호가 자동적으로 사용되기 때문에 이 비밀번호를 알 필요가 없다.
시크릿#3	PAS의 비-칩카드 실시예에 사용되는 비밀번호(코어 시스템). 접근제어서버로 하여금 카드소지자를 확인하게 하는 카드소지자에 의해 규정되는 비밀번호. 이 비밀번호나 시크릿은 칩카드 접근이 카드상에서 가용하지 않을 때 카드소지자를 확인하는 데 사용될 수도 있다.

<214> 도 13은 범용 접근 응용프로그램과 칩카드를 이용하여 지불인 인증 서비스에 사용되는 구성성분들의 시스템 도면이다. 도 13의 시스템 도면은 칩카드(1540), 칩카드 판독기(1518), 카드소지자 클라이언트 장치(122), 접근제어서버(114), 데이터베이스(1240)를 도시한다. 칩카드(1540)는 접근 애플릿(1202)과 칩카드 신용 및 데빗 응용프로그램(1204)을 포함한다. 접근 애플릿(1202)은 시크릿#2인 비밀번호를 저장하고, 이는 칩카드 상의 여러 응용프로그램에 대한 잠금장치를 해제하는 데 사용된다. 카드소지자 클라이언트 장치는 지불인 인증 응용프로그램(1542)을 포함한다.

<215> 온라인 구매 거래시에, 접근 애플릿(1202)은 카드소지자에게 ID와 비밀번호(시크릿 #1) 입력 프람프트를 띄울 것이다. 카드소지자가 정확한 사용자 ID와 비밀번호를 입력할 경우, 칩카드 상의 응용프로그램에 대한 잠금장치를 해제하기 위해 시크릿 #2가 자동적으로 이용된다. 그후 칩카드 시스템을 이용하는 PAS 시스템은 본 명세서에서 앞서 설명한 바와 같이 진행될 수 있다.

<216> 이러한 보다 상세한 설명은 카드소지자 클라이언트 장치 소프트웨어에 의해 지원되어야 하는 처리과정 및 명령들을 설명하며, 이는 칩카드 판독기, 카드소지자의 인터넷 브라우저, 그리고 접근제어서버 사이의 통신을 촉진시킨다.

<217> 여러 기본 처리과정 및 명령들이 이제부터 설명될 것이다. 먼저, 카드소지자 클라이언트 장치 소프트웨어는 접근제어서버로부터의 메시지에 의해 활성화될 것이다. (클라이언트는 시간기한을 갖추어 구현될 수 있다. 가령, 클라이언트가 30분후 시간만료될 것이다). 그후, 카드소지자 클라이언트 장치 소프트웨어는 순응하는 칩판독기의 존재를 확인할 것이고, 칩기반 지불인 인증 거래를 처리할 수 있다고 접근제어서버에 응답할 것이다. 카드소지자 클라이언트 장치 소프트웨어는 칩카드 프로그램(가령, VSDC 응용프로그램)이 암호문을 발생시키도록, 적절

한 머천트 및 접근제어서버 데이터를 내장한 접근제어서버로부터 메시지를 수령할 것이다. 이러한 칩카드 프로그램의 예는 비자 스마트 데빗 신용 응용프로그램(VSDC)로서, 유로페이, 마스터카드, 비자(EMV) 칩카드 표준의 비자식 구현이다. 암호문은 카드와 각각으 거래에 특정한 카드에 의해 발생되는 암호값이다. 접근제어서버는 하드웨어 보안 모듈의 암호 키를 이용하는 암호문을 확인할 수 있다. VSDC 응용프로그램은 재래식 POS 머천트에게서 발생하는 대면 거래에 사용되는 응용프로그램과 같은 응용프로그램이다.

<218> 접근제어서버로부터 메시지를 수신한 후, 카드소지자 클라이언트 장치 소프트웨어는 규정된 데이터 요소 내 UID와 시크릿 #2의 존재를 확인할 것이다. 가용하지 않을 경우, 카드소지자 클라이언트 장치 소프트웨어는 카드소지자에게 칩카드 삽입과 시크릿#1 입력을 요청하여, 칩카드 접근 프로그램에 대해 확인을 하고 시크릿#2와 사용자 ID(UID)를 불러올 수 있다.

<219> 카드소지자가 칩-기반 지불인 인증된다고 확인되면, 카드소지자 클라이언트 장치 소프트웨어는 온라인 칩카드 인증을 실행하기 위해 암호문과 관련 데이터를 얻도록 VSDC 구매 거래를 실행할 것이다.

<220> VSDC 구매 거래의 실행은 카드소지자 클라이언트 장치 소프트웨어와 VSDC 칩 응용프로그램 각각이 취할 여러 단계들을 포함한다. 카드소지자 클라이언트 장치 소프트웨어는 한개 이상의 SELECT 명령을 카드에 발급함으로서 외부 선택 방법을 이용하여 응용프로그램 선택을 실행할 것이다. 카드소지자 클라이언트 장치 소프트웨어는 PDOL이 응용프로그램 선택으로부터 파일 제어 정보(FCI) 내에 존재할 경우, PDOL을 포함하는 GET PROCESSING OPTIONS 명령을 발급할 것이다. 그후 VSDC 칩 응용프로그램은 GET PROCESSING OPTIONS 명령으로부터 응답으로 응용프로그램 파일 로케이터(AFL)와 응용프로그램 교환 프로파일(AIP)을 되보낼 것이다.

<221> 카드소지자 클라이언트 장치 소프트웨어는 AFL에 의해 지정되는 VSDC 칩 응용프로그램 레코드를 판독하기 위해 필요한 READ RECORD 명령을 발급할 것이다. 주: 칩은 VSDC 구매 거래를 완료하는 데 필요한 모든 데이터를 되보낼 것이고, 이뿐 아니라 인터넷 지불 인증에 사용되는 데이터도 되보낼 것이다. 카드소지자 클라이언트 장치 소프트웨어는 정확한 데이터를 분석할 필요가 있다. 카드소지자 클라이언트 장치 소프트웨어는 처리 제한 확인사항을 실행할 것이고, CVM 리스트 처리를 회피하며, 바닥 한계 및 새 카드 확인을 제외하고는 단말기 위험 관리를 회피할 것이다. 모든 거래는 바닥 한계 위에서 이루어질 것이다. 카드소지자 클라이언트 장치 소프트웨어는 TVR 거래가 바닥 한계를 넘는 비트를 '1'로 설정할 것이다. 카드소지자 클라이언트 장치 소프트웨어는 단말기 동작 분석을 실행할 것이고 GENERATE AC 명령의 ARQC (온라인) 암호문을 항상 요청할 것이다. 이 명령은 접근제어서버로부터 예측불가능한 번호와 거래 일자를 포함한 CDOL1 데이터를 포함할 것이다. 카드소지자 클라이언트 장치 소프트웨어는 대해 바뀌지 않는 데이터를 지원하면서 칩에 의해 되돌아오는 암호문을 확인을 위해 접근제어서버에 전달할 것이다. 마지막으로, 카드소지자 클라이언트 장치소프트웨어는 AAC를 요청하는 GENERATE AC 명령을 발급할 것이다. 이는 VSDC 카드 응용프로그램에 대한 거래를 종료할 것이다. 제 2 GENERATE AC 명령을 발급한 후, 거래로부터 모든 정보는 카드소지자 클라이언트 소프트웨어에 의해 잊혀져야 한다.

<222> 다음 과정은 머천트 플러그인이 PAReq 메시지를 접근제어서버에 전송한 후 일어난다. 먼저, 접근제어서버는 카드소유자의 PC가 칩에 의해 동작하는 지를 결정하여야 한다(주: PAN이 칩에 의해 동작하는 것으로 등록될 수 있으나, 이 단계는 현재 거래에 사용중인 PC가 칩판독기를 가지지 않거나 칩에 의해 동작하지 않는 경우에 필요하다). 접근제어서버는 PC가 칩에 의해 동작하지 않거나 칩을 판독할 수 없을 경우 두가지 다른 동작을 발급자가 설정할 수 있어야 한다.

<223> 옵션 #1은 카드쇠자자에게 시크릿#3 프람프트를 제시한다. 옵션#2는 어떤 카드소지자로 하여금 어떤 칩카드 인증도 실행하지 않으며, "적용불가한" 응답으로 PARes 거래 상태 필드를 채운다. 접근제어서버는 PAReq로부터 적절한 모든 머천트 정보를 추출하여야 하고, 암호문 발생을 위해 칩카드에 요청하기 위해 필요한 카드소지자 클라이언트 장치 소프트웨어에 적절한 접근제어서버 정보와 이 데이터를 제공하여야 한다.

<224> 접근제어서버는 카드소지자의 클라이언트 장치 소프트웨어에 암호문을 지원하는 정보를 전송하고, 시크릿#2와 고유 식별자(UID)에 대한 요청을 전송한다. 카드소지자 클라이언트 장치 소프트웨어는 앞서 실행된 칩-동작 계산 과정으로부터 시크릿#2(비밀번호)와 UID를 얻는 응용프로그램을 호출한다. 시크릿#2가 이 과정을 통해 가용하지 않을 경우, 카드소지자 클라이언트 장치 소프트웨어는 접근 애플릿을 호출함으로서 칩카드로부터 시크릿#2를 얻고, 칩카드 상에서 접근 애플릿내로부터 시크릿#2와 UID를 얻는다. 접근 애플릿이 칩카드에 존재하지 않을 경우, 카드소지자 클라이언트 장치 소프트웨어는 카드소지자에게 시크릿#3(PAS 비밀번호)를 입력할 것을 요청한다.

<225> 시크릿#2와 UID를 얻은 후, 카드소지자 클라이언트 장치 소프트웨어는 VSDC 거래를 시작하여 암호 요청을 발생

시키고 칩카드로부터 암호문을 얻는다. 시크릿#2를 얻지 못한 경우, 카드소지자 클라이언트 장치 소프트웨어는 VSDC 애플릿을 불러오지 않는다.

<226> 카드소지자 클라이언트 장치 소프트웨어는 암호 확인을 위해 접근제어서버에 대한 지원 데이터, 암호문, 시크릿#2를 접근제어서버에 되돌려보낸다. 접근제어서버는 카드소지자 클라이언트 장치 소프트웨어의 입력을 받아들이고 이를 계좌 소유자 데이터베이스에 대해 확인한다. 주계좌번호(PAN)에 대해 한개보다 많은 계좌 소유자 데이터베이스 입력(시크릿#2)이 있을 경우, 엔트리 중 하나(시크릿#2)가 카드소지자 클라이언트 장치 소프트웨어에 의해 제어접근서버에 전달되는 시크릿#2와 부합할 경우 카드소지자가 확인(승인)된다.

<227> 접근제어서버는 암호문을 복제하고 이를 카드소지자 클라이언트 장치 소프트웨어에 의해 접근제어서버에 전달된 칩카드로부터의 암호문과 비교함으로서 카드를 확인한다. 접근제어서버는 PARes 메시지를 생성하고, 카드소지자 브라우저를 통한 연결을 이용하여 PARes 메시지를 머천트에게 되돌려보낸다.

<228> 접근제어서버는 PARes를 디지털방식으로 서명하고, PARes 거래 상태, 거래 세부사항, ECI, 값, 카드 종류를 나타내는 칩카드 코드, 지불조건, 그리고 카드 인증 결과를 설정하며, 서명한 PARes를 다시 머천트에게 전송하고, 그리고 SaveReceipt 메시지를 영수증 관리자(131)에 발생시킨다(SaveReceipt 메시지는 PATrans 메시지라 불릴 수 있다).

<229> 두 종류의 칩카드는 비자스마트 데빗/신용(VSC) 응용프로그램을 운반한다. 첫 번째는 접근 비밀번호나 시크릿#1을 이용하여 카드 상의 접근 응용프로그램을 통해 카드소지자를 오프라인으로 확인할 수 있는 카드이다. 접근비밀번호는 카드소지자로부터 얻을 수 있고, 브라우저 상에서 카드소지자 클라이언트 장치 소프트웨어에 전달된다. 제공된 접근 비밀번호가 정확할 경우, 칩카드 접근 응용프로그램은 시크릿#2와 UID를 카드소지자 클라이언트 장치 소프트웨어로 되보낸다. 두 번째로, 카드소지자를 오프라인으로 확인할 수 없는 카드(즉, VSDC 응용프로그램만을 내장한 카드)가 있다. 이 경우에 브라우저 상의 카드소지자 클라이언트 장치 소프트웨어는 카드소지자에게 시크릿#3에 대한 프람프트를 제시하고, 카드소지자 인증을 이루기 위해 접근제어서버에 제공된다.

<230> 접근제어서버로부터 제어를 부여받은 후 카드소지자 클라이언트 장치 소프트웨어에 관련된 흐름이 이제부터 제시될 것이다. 카드소지자 클라이언트 장치 소프트웨어는 카드소지자의 PC가 칩카드동작되는 지를 먼저 결정하여야 한다. 그렇지 않을 경우, 거래는 코어 지불인 인증을 통해 처리된다. PC가 칩카드에 의해 동작될 경우, 단계 2에서, 칩카드 상의 접근 응용프로그램을 통해 시크릿 #2를 얻고, 또는 카드소지자에 대한 프람프트를 통해 시크릿#3을 얻는다.

<231> 시크릿#2와 UID, 또는 시크릿#3가 제공될 경우, 칩 상의 VSDC 응용프로그램을 호출하여, 자기띠 이미지(MSI) 데이터 요소를 불러들이고, 접근제어서버의 암호문 재생성을 행하는 데 필요한 칩데이터를 불러들이며, 그리고 ARQC 암호문을 발생시킨다. 시크릿#2와 시크릿#3가 제공되지 않을 경우, VSDC 애플릿이 호출되지 않는다.

<232> 카드 이증을 위해 다음 데이터를 접근제어서버에 전송한다. 즉, ARQC 암호문, 자기띠 이미지(MSI), 그리고 접근제어서버에 의한 암호문 재생성을 지원하는 데이터를 접근제어서버에 전송한다. 부가적으로 MSI 데이터가 판독될 수 있다.

<233> 그후 카드소지자 인증을 위해 시크릿#2와 UID, 또는 시크릿#3를 접근제어서버에 전송한다.

<234> 일반적으로, 칩카드소지자들은 코어 지불인 인증을 통해 존재하는 카드없이 인터넷 상에서 구매 거래를 실행하게 될 것이다. 또한, 발급자에 의해 분배되는 카드소지자 클라이언트 장치 소프트웨어는 모든 종류의 VSDC 카드를 지원하여야 한다. 인증은 비자 스마트 데빗/신용 애플릿의 풀버전과 제한된 버전을 구현하는 칩-기반 지불 응용프로그램을 수용하여야 한다. 초기에 칩-기반 지불 응용프로그램은 개방 플랫폼 카드 상의 제한된 VSDC 특징을 지원할 것이다. 이 제한된 VSDC 지불 애플릿, "점프 스타트"는 MSI, 온라인 카드 인증, 그리고 오프라인 정적 데이터 인증(SDA)의 "풀" VSDC 특징을 지원한다. 그러나, SDA는 인터넷 거래중 실행되지 않는다. 거래로부터의 모든 정보는 거래 종료시 지불인 인증 카드소지자 클라이언트 장치소프트웨어에 의해 잊혀져야 한다.

<235> 접근제어서버는 카드소지자 클라이언트 장치 소프트웨어가 가용하지 않거나 칩카드를 판독할 수 없을 때 취할 여러 다른 동작을 가능하게 하도록 발급자에 의해 설정가능하다. 옵션 #1에서는 접근제어 서버가 카드소지자에게 시크릿 #3의 수동 입력에 대한 프람프트를 띄우고, 옵션#2에서는 어떤 인증도 실행되지 않으며, "적용불가" 응답이 머천트에게 되돌아온다.

<236> 칩카드소지자들은 카드없이 인터넷 상에서 구매 거래를 실행할 수 있다. 카드소지자들은 머천트 계산 폼을 수동으로 채우고 발급자가 이 접근법을 택할 경우 시크릿#3를 수동으로 입력하도록 접근제어서버에 의해 프람프트를

받을 것이다.

<237> **선호되는 지불 통신망**

<238> 도 14는 본 발명의 한 실시예를 구현하기에 적절한 통신망(800)을 도시한다. 본 발명은 적절한 통신망을 이용할 수 있고 아래 설명되는 것과는 다른 하드웨어, 다른 소프트웨어, 또는 다른 프로토콜들을 포함할 수 있다. 아래 설명되는 통신망은 도 1의 통신망(126)의 선호되는 실시예이다. 통신망(800)은 은행카드, 여행자 및 유흥카드, 그리고 그 외 다른 개별적 라벨 및 전문직 카드를 이용하여 구매 및 현금 거래를 지원하는 전역 통신망이다. 통신망은 타통신망에 대한 ATM 거래, 종이 수표를 이용한 거래, 스마트카드를 이용한 거래, 그리고 다른 금융회사를 이용한 거래를 지원하기도 한다.

<239> 이 거래들은 통신망 승인, 삭제, 지불 서비스를 통해 처리된다. 구매를 마치거나 현금이 나오기 전에 판매 거래를 발급자가 허락하거나 거절할 때 승인(authorization)이 이루어진다. 삭제(clearing)는 고객 계좌로 배달을 위해 거래가 취득자로부터 발급자로 전달될 때이다. 지불(settlement)은 삭제된 모든 거래에 대한 각각의 구성원의 알짜 금융 위치를 계산하고 결정하는 과정이다. 자금의 실제 교환은 별도의 과정이다.

<240> 거래는 이중 메시지나 단일 메시지 거래로 승인되고 삭제되며 지불될 수 있다. 이중 메시지 거래는 두 번 전송된다. 먼저는 승인 결정에 필요한 정보만으로, 후에는 삭제 및 지불을 위한 추가 정보로 전송된다. 단일 메시지 거래는 승인을 위해 한번만 전송되고, 삭제 및 지불 정보도 함께 내장한다. 통상적으로, 승인, 삭제, 지불은 모두 온라인으로 이루어진다.

<241> 통신망(800)의 주성분은 교환 센터(802), 접근점(804, 806), 그리고 처리 센터(808, 810)이다. 수취인 은행 및 제 3 자 승인 대리인같은 다른 실체들이 접근점을 통해 통신망에 또한 연결될 수 있다. 교환 센터는 세계 어디에도 위치할 수 있는 데이터 처리센터이다. 한 실시예에서, 미국에 두개, 영국과 일본에 각각 한개씩 위치한다. 각각의 교환센터는 통신망 거래 처리를 실행하는 컴퓨터 시스템을 가진다. 교환센터는 통신망의 통신설비에 대한 제어점으로 작용하고, IBM SNA 프로토콜을 바탕한 위성 연결이나 고속 리스선 연결을 포함한다. 교환센터를 원격 실체에 연결하는 라인(820, 822)은 IBM SNA-LU0 통신 프로토콜에 바탕한 위성연결이나 전용 고대역폭 전화회로를 이용한다. 메시지는 ISO 8583 표준의 어떤 적절한 구현을 이용하여 이 라인들 상에서 전송된다.

<242> 접근점(804, 806)은 센터의 호스트 컴퓨터와 교환센터간 인터페이스 역할을 하는 처리센터에 위치하는 소형 컴퓨터 시스템이다. 접근점은 거래의 승인, 삭제, 지불을 지원하는 교환센터와 호스트간 파일 및 메시지 전송을 촉진시킨다. 링크(826,828)는 통상적으로 센터 내 국부 링크이며, 센터에 의해 선호되는 것처럼 독점적 메시지 포맷을 이용한다.

<243> 데이터 처리 센터는 머천트 및 사업 위치를 지원하고 고객 데이터 및 대금청구 시스템을 관리하는 처리 시스템을 내장한다. 각각의 처리 센터가 한개나 두개의 교환 센터에 링크되는 것이 선호된다. 가장 가까운 교환센터에 프로세서가 연결되고, 통신망이 인터럽트를 느끼면 통신망은 자동적으로 거래를 보조 교환 센터로 이동시킨다. 각각의 교환 센터는 모든 나머지 교환 센터에 또한 링크된다. 이 링크는 한개 이상의 교환 센터를 통해 처리센터들이 서로 통신할 수 있게 한다. 또한, 처리 센터들이 교환센터를 통해 다른 프로그램의 통신망에 접근할 수 있다. 더욱이, 모든 링크가 여러 백업을 가지는 점을 통신망이 보장한다. 통신망 한점으로부터 다른 한점으로의 연결이 고정 링크가 아니다. 대신에, 교환 센터는 어느 주어진 전송 시기에 가장 최적으로 가능한 경로를 선택한다. 잘못된 링크에 대한 재이동은 자동적으로 이루어진다.

<244> 도 15는 온라인 및 오프라인 거래 처리를 제공하기 위해 교호나 센터 내에 위치하는 시스템(840)을 도시한다. 이중 메시지 거래의 경우, 승인 시스템(842)이 승인을 제공한다. 시스템(842)은 온라인 및 오프라인 기능을 지원하고, 그 파일은 내부시스템표, 고객 데이터베이스, 그리고 머천트 중앙 파일을 포함한다. 시스템(842)의 온라인 기능은 이중 메시지 승인 처리를 지원한다. 이 처리는 루팅, 카드소지자 및 카드 확인 및 스탠드-인 처리, 그리고 파일관리같은 그 외 다른 기능을 포함한다. 오프라인은 보고, 대금청구, 회복 게시판 생성들을 포함한다. 보고는 승인 보고서, 예외 파일, 그리고 조언 파일 보고서, POS 보고서, 그리고 대금청구 보고서를 포함한다. 시스템(842)으로부터 시스템(846)까지 브리지는 시스템(842)을 이용하는 멤버로 하여금 시스템(846)을 이용하여 멤버들과 통신할 수 있게 하고, 통신망 외부와 접하는 SMS 게이트웨이에 접근하게 할 수 있다.

<245> 삭제 및 지불 시스템(844)은 이전에 승인된 이중 메시지 거래를 삭제하고 지불한다. 전역 원칙으로 주 6일 동작할 경우, 시스템(844)은 재정적 및 비재정적 정보를 모으고, 멤버간 보고서를 분배한다. 이는 요금을 계산하고, 대금을 청구하며, 총계를 지불하고, 그리고 조정을 돕기 위해 보고서를 생성한다. 브리지는 시스템(844) 처리 센터와 시스템(846) 처리 센터 사이에 인터체인지를 형성한다.

<246> 단일 메시지 시스템(846)은 전체 금융거래를 처리한다. 시스템(846)은 이중 메시지 승인 및 삭제 거래를 또한 처리할 수 있고, 브리지를 이용하여 시스템(842)과 통신할 수 있으며 필요할 때마다 통신망 외부에 접근한다. 시스템(846)은 비자,플러스 인터링크, 그리고 그 외 다른 카드거래를 처리한다. SMS 파일은 시스템 접근 및 처리를 제어하는 내부 시스템 표와, PIN 확인 및 스탠드-인 처리 승인에 사용되는 카드소지자 데이터의 파일을 내장하는 카드소지자 데이터베이스를 포함한다. 시스템(846) 온라인 기능은 실시간으로 카드소지자 거래 처리를 실행하고 승인 및 총 재정적 거래에 대한 예외를 처리한다. 시스템(846)은 조정 및 지불 총계를 누적한다. 시스템(846) 오프라인 기능들은 지불 및 대금전송요청을 처리하고, 집ㄹ 및 동작 보고를 제공한다. 지불 서비스(848)는 인터링크를 포함한 시스템(844, 846)의 지불기능을 모든 상품 및 서비스에 대한 단일 서비스로 통합한다. 삭제는 시스템(844, 846)에 의해 별도로 계속 실행된다.

<247> 도 16은 통신망(800)의 구성성분들 도면이다. 통합된 지불 시스템(850)은 모든 온라인 승인 및 재정적 요청 거래를 처리하기 위한 주된 시스템이다. 시스템(850)은 이중 메시지 및 단일 메시지 처리를 보고한다. 두 경우에, 지불은 별도로 이루어진다. 세 개의 메인 소프트웨어 구성성분들은 공통 인터페이스 기능(852), 승인 시스템(842), 그리고 단일 메시지 시스템(846)이다.

<248> 공통 인터페이스 기능(852)은 교환 센터에서 수신되는 각각의 메시지에 필요한 처리를 결정한다. 메시지 소스(시스템(842, 844, 846)), 처리 요청 종류, 그리고 처리 네트워크를 바탕으로 적절한 루팅을 선택한다. 이 구성성분은 초기 메시지 편집을 실행하고, 필요할 경우 ATL지를 분석하며, 내용이 기본 메시지 구성규칙과 부합함을 보장한다. 기능(852)은 메시지를 시스템(842)이나 시스템(846) 목적지까지 전달한다.

<249> **컴퓨터 시스템 실시예**

<250> 도 17A와 17B는 본 발명의 실시예들을 구현하기에 적절한 컴퓨터 시스템(900)을 도시한다. 도 17A는 컴퓨터 시스템의 한가지 가능한 물리적 형태를 도시한다. 물론, 컴퓨터 시스템은 집적 회로로부터, 인쇄회로보드, 그리고 소형 휴대용 장치, 초대형 수퍼컴퓨터까지 여러 물리적 형태를 가질 수 있다. 컴퓨터 시스템(900)은 모니터(902), 디스플레이 장치(904), 하우징(906), 디스크 드라이브(908), 키보드(910), 그리고 마우스(912)를 포함한다. 디스크(914)는 컴퓨터 시스템(900) 내외로의 데이터 전송에 사용되는 컴퓨터-판독 매체다.

<251> 도 17B는 컴퓨터 시스템(900)에 대한 블록 도표의 한 예다. 시스템 버스(920)에 부착되는 것은 매우다양한 서브시스템들이다. 프로세서(922)가 메모리(924)를 포함하는 기억장치에 연결된다. 메모리(924)는 RAM과 ROM을 포함한다. 당 분야에 잘 알려진 바와 같이, ROM은 데이터 및 명령을 CPU에 단방향으로 전송하는 역할을 하고, RAM은 양방향으로 전송하는 역할을 한다. 이 두 종류의 메모리는 아래 설명되는 적절한 컴퓨터-판독 매체를 포함할 수 있다. 거치식 디스크(926)는 CPU(922)에 양방향으로 연결된다. 거치식 디스크는 추가적인 데이터 저장 용량을 제공하고, 아래 설명되는 컴퓨터-판독 매체를 포함할 수 있다. 거치식 디스크(926)MS 프로그램, 데이터 등의 저장에 사용될 수 있고, 주기억장치보다 느린 보조기억 매체(가령, 하드디스크)이다. 거치식 디스크(926) 내에 유지되는 정보는 메모리(924)의 가상 메모리로 표준 방식으로 통합될 수 있다. 탈착식 디스크(914)는 아래 설명되는 컴퓨터-판독 매체 형태를 취할 수 있다.

<252> CPU(922)는 디스플레이 장치(904), 키보드(910), 마우스(912), 스피커(930)같은 다양한 입/출력 장치에 연결된다. 일반적으로, 입/출력 장치는 비디오 디스플레이장치, 트랙볼, 마우스, 키보드, 마이크로폰, 터치식 디스플레이 장치, 트랜스듀서 카드판독기, 자기나 종이테이프 판독기, 태블릿, 스타일러스, 음성이나 필기 인식기, 바이오메트릭스 판독기, 또는 그 외 다른 컴퓨터 중 하나일 수 있다. CPU(922)는 네트워크 인터페이스(940)를 이용하여 또다른 컴퓨터나 통신망에 연결될 수 있다. 이러한 네트워크 인터페이스로, CPU가 통신망으로부터 정보를 수신할 수 있고, 또는 앞서 설명한 방법 단계들을 실행하는 과정에서 통신망에 정보를 출력할 수도 있다. 더욱이, 본 발명의 방법 실시예들은 CPU(922) 단독으로 실행될 수도 있고, 처리 부분을 공유하는 원격 CPU와 연계하여 인터넷같은 통신망 상에서 실행될 수 있다.

<253> 게다가, 발명의 실시예들은 여러 컴퓨터-구현 동작을 실행하기 위해 컴퓨터 코드를 가지는 컴퓨터-판독 매체를 가진 컴퓨터 저장 프로덕트에 또한 관련된다. 이 매체 및 컴퓨터 코드는 본 발명의 용도로 특별히 설계 및 고안된 것일 수도 있고, 당 분야에 통상적 종류의 것일 수도 있다. 컴퓨터-판독 매체의 예로는 하드디스크, 플라피 디스크, 자기테이프같은 자기매체, CD-ROM, 홀로그래픽 장치같은 광학 매체, 플롭티컬 디스크같은 자기광학 매체, 그리고 전용 집적회로(ASIC), 프로그래머블 논리 장치(PLD), 그리고 ROM 및 RAM 소자처럼 프로그램 코드를 저장하고 실행하도록 특별히 고안된 하드웨어 장치들을 들 수 있다. 컴퓨터 코드의 예는 컴파일러에 의해 생성되는 머신 코드와, 인터프리터를 이용하여 컴퓨터에 의해 실행되는 더 높은 수준의 코드를 내장한 파일이 있다.

도면의 간단한 설명

<11> 도 1은 지불인 인증 서비스(PAS)를 지원할 수 있는 조직구조의 한 실시예 도면.

<12> 도 2는 본 발명의 한 실시예에 따른 PAS로 카드소지자가 등록하는 과정의 도면.

<13> 도 3은 PAS에 대한 등록 과정 중 카드소지자가 정보를 입력할 수 있는 인터넷 웹페이지의 한 실시예 도면.

<14> 도 4는 본 발명의 한 실시예에 따른 PAS-인증 지불 거래의 도면.

<15> 도 5는 카드소지자에게 비밀번호를 제시하는 윈도우의 예 도면.

<16> 도 6은 PAS 조직구조에 겹쳐지는 지불 거래 중 전송되는 메시지의 예 도면.

<17> 도 7은 본 발명의 중앙화된 실시예에 따라 중앙화된 PAS 조직구조에서의 메시지 흐름 도면.

<18> 도 8은 본 발명의 중앙화 실시예에 따라 카드소지자 클라이언트 장치, PAS, 그리고 머천트 시스템 사이에 발생하는 중앙화 지불 흐름의 도면.

<19> 도 9는 본 발명의 분산 실시예에 따라 분산 PAS 조직구조의 등록 흐름 도면.

<20> 도 10은 본 발명이 분산 실시예에 따라 분산 PAS 조직구조의 지불 흐름 도면.

<21> 도 10A는 칩카드 지불인 인증 서비스의 한 실시예에 대한 고도의 시스템 구조 도면.

<22> 도 11은 지불인 인증 서비스의 칩카드 실시예를 이용하여 지불 거래의 한 예를 설명하는 순서도.

<23> 도 12는 본 발명의 한 실시예에 따르는 칩카드 인증 과정의 시스템 구조도면.

<24> 도 12A는 칩카드, 카드소지자 클라이언트 시스템, 그리고 발급자의 접근제어서버간 메시지 흐름의 상세도.

<25> 도 13은 지불인 인증 서비스의 접근 제어 시스템 실시예에 사용되는 구성성분들의 시스템도표.

<26> 도 14는 본 발명의 한 실시예를 구현하기에 적절한 통신망 도면.

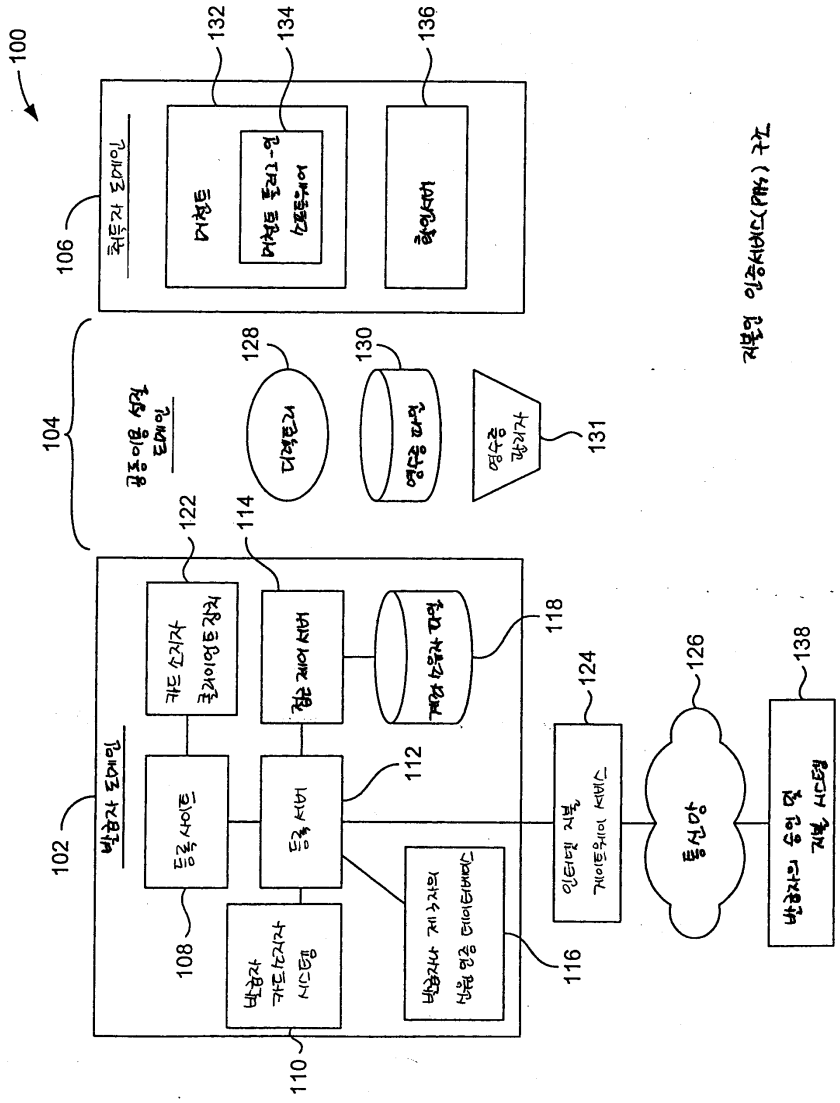
<27> 도 15는 온라인 및 오프라인 거래 처리를 제공하기 위해 교환 센터 내 만들어진 시스템 도면.

<28> 도 16은 통신망의 구성성분들의 또다른 도면.

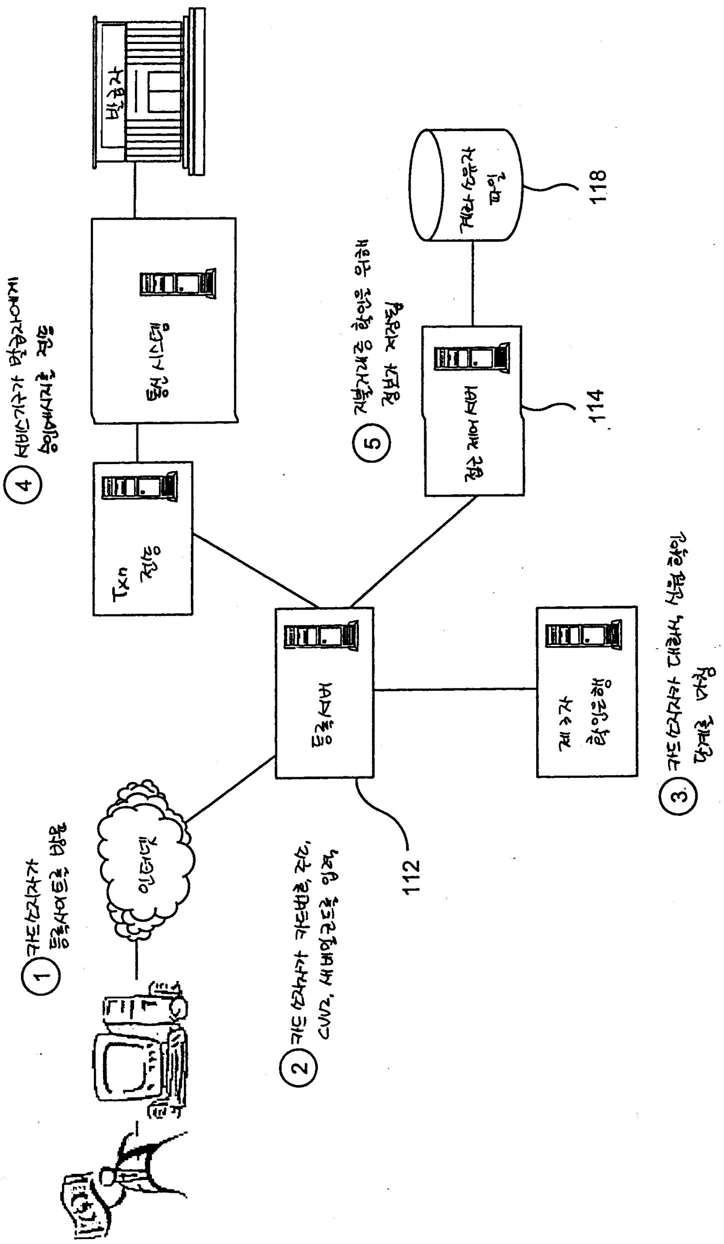
<29> 도 17A와 17B는 본 발명의 실시예들을 구현하기에 적절한 컴퓨터 시스템 도면.

도면

도면1

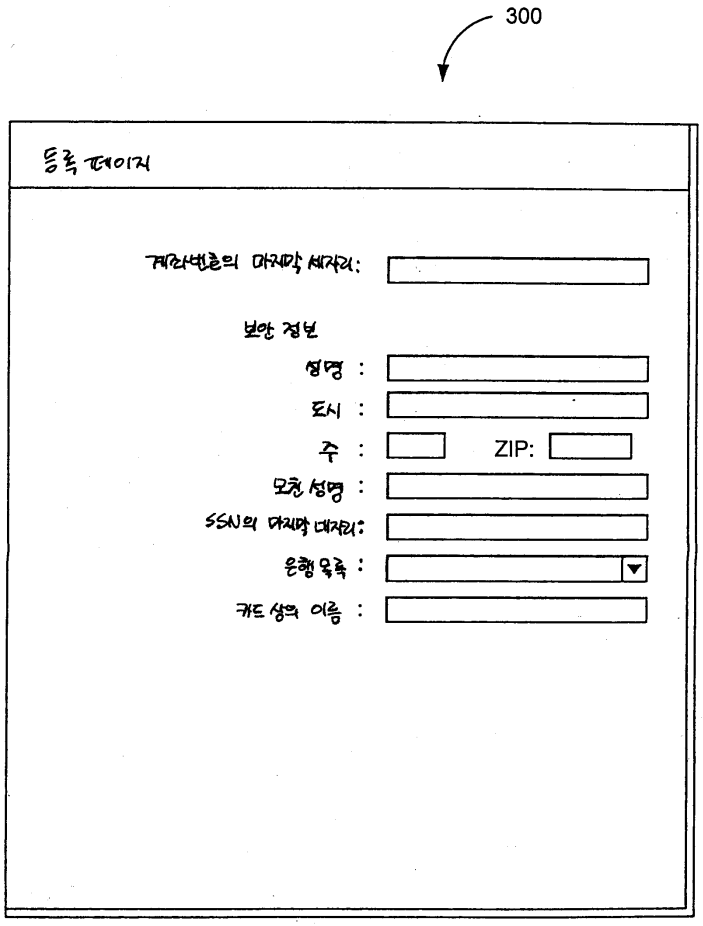

100
106
취득자 도메인
132
134
136
104
결합이용 상점 도메인
128
130
131
122
114
112
118
124
126
138
102
108
110
116
통신망

도면2

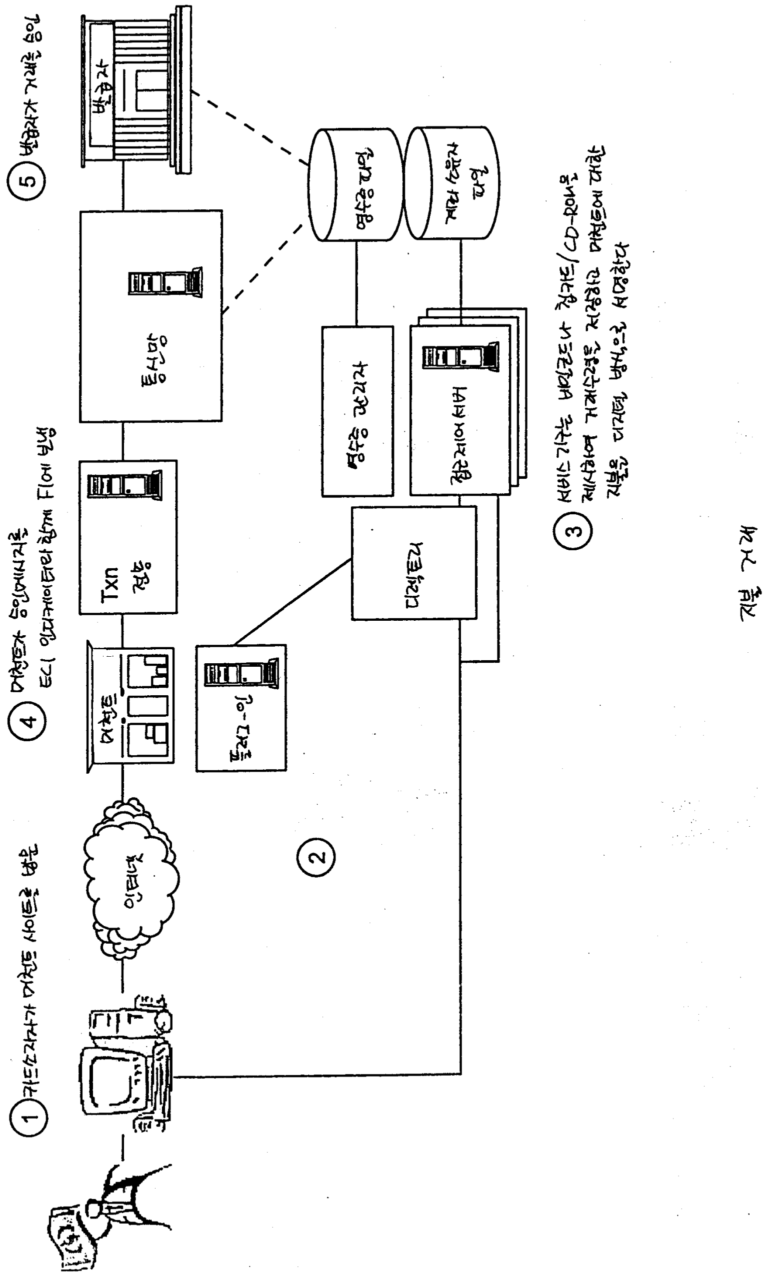

① 카드소지자가 등록사이트를 방문
인터넷
등록서버
112
Txn 전송
통신 시스템
발급자
접근 제어 서버
114
계좌 소유자 파일
118
제3자 확인은행

카드 소지자 등록

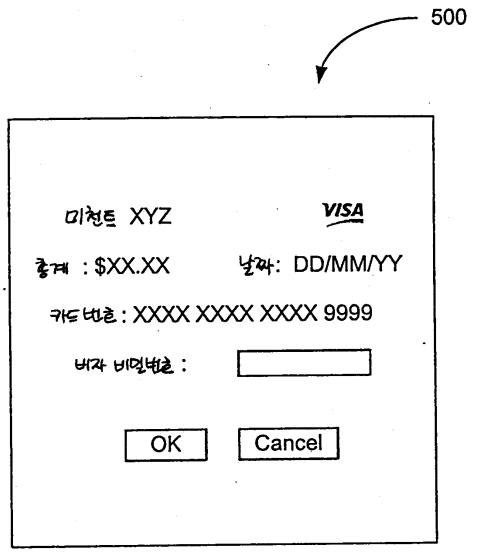
도면3


300
등록 페이지
계좌번호의 마지막 세자리:
보안 정보
성명 :
도시 :
주 :
ZIP:
모친 성명 :
SSN의 마지막 네자리:
은행목록 :
카드 상의 이름 :

도면4



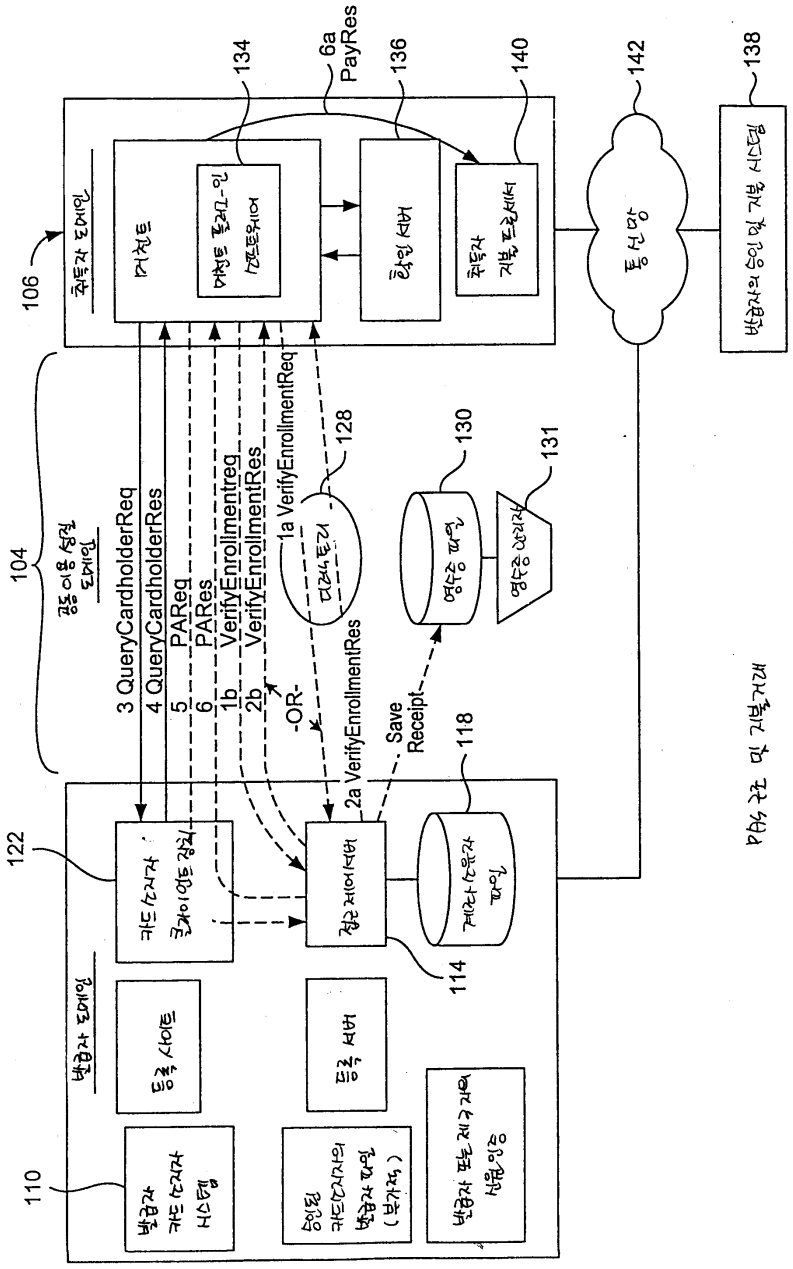
도면5



지불거래

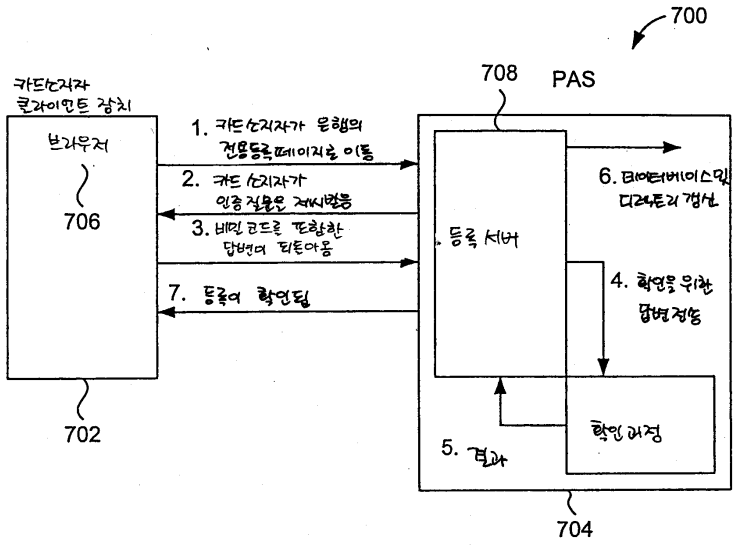
카드 및 지자 비밀번호 프람프트

도면6


106
머천트
134
6a PayRes
136
140
142
138
104
3 QueryCardholderReq
4 QueryCardholderRes
5 PAReq
6 PARes
1b VerifyEnrollmentReq
2b VerifyEnrollmentRes
-OR-
1a VerifyEnrollmentReq
128
130
131
2a VerifyEnrollmentRes
Save Receipt
118
122
114
110

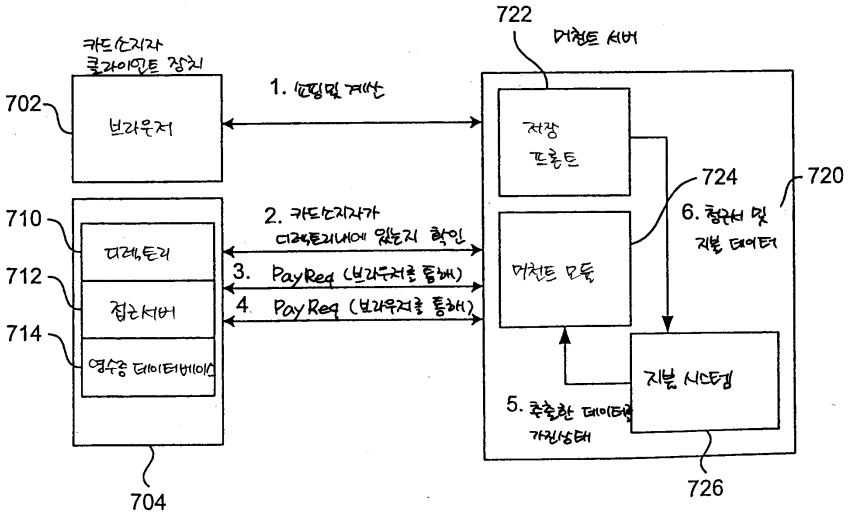
도 6

도면7



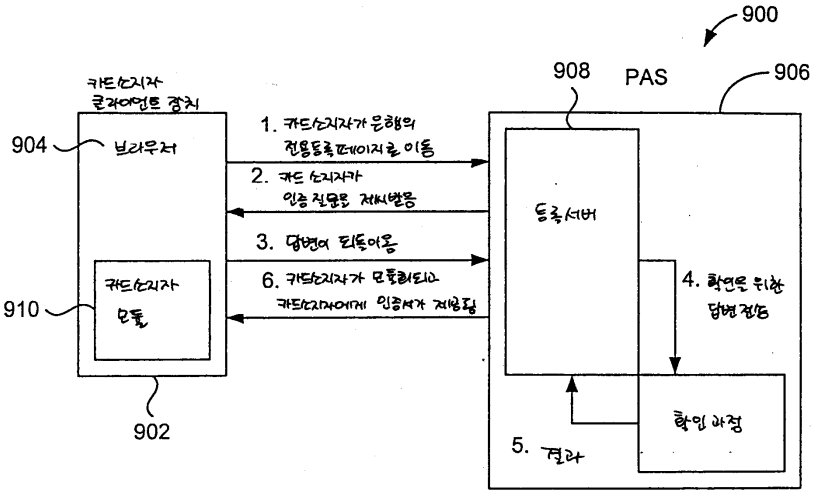
중앙 집중식, 등록 흐름도

도면8



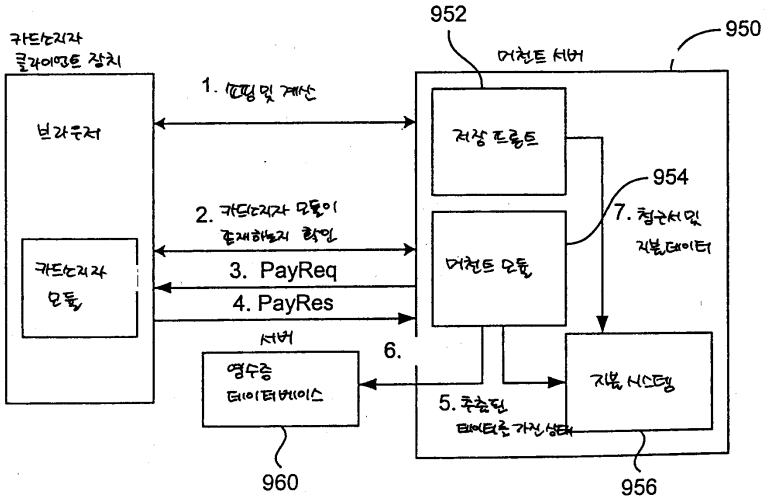
중앙집중식 지불 흐름도

도면9



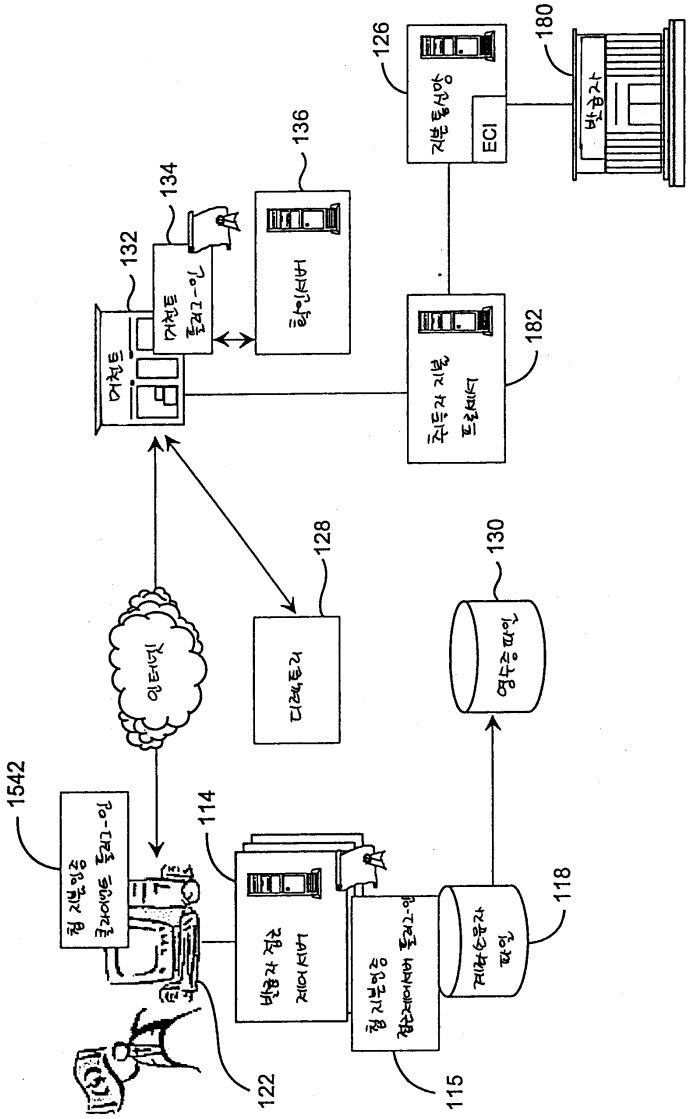
분산 등록 흐름도

도면10



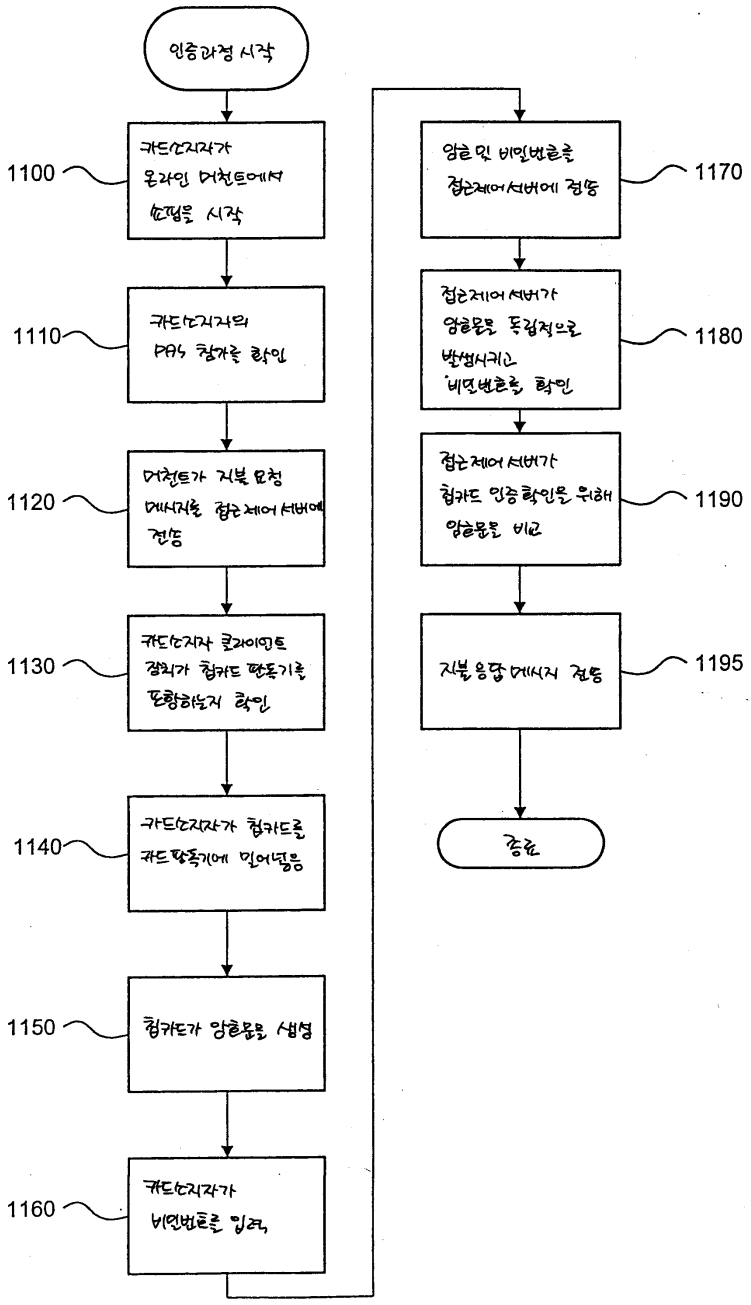
분산형 지불 흐름도

도면10a

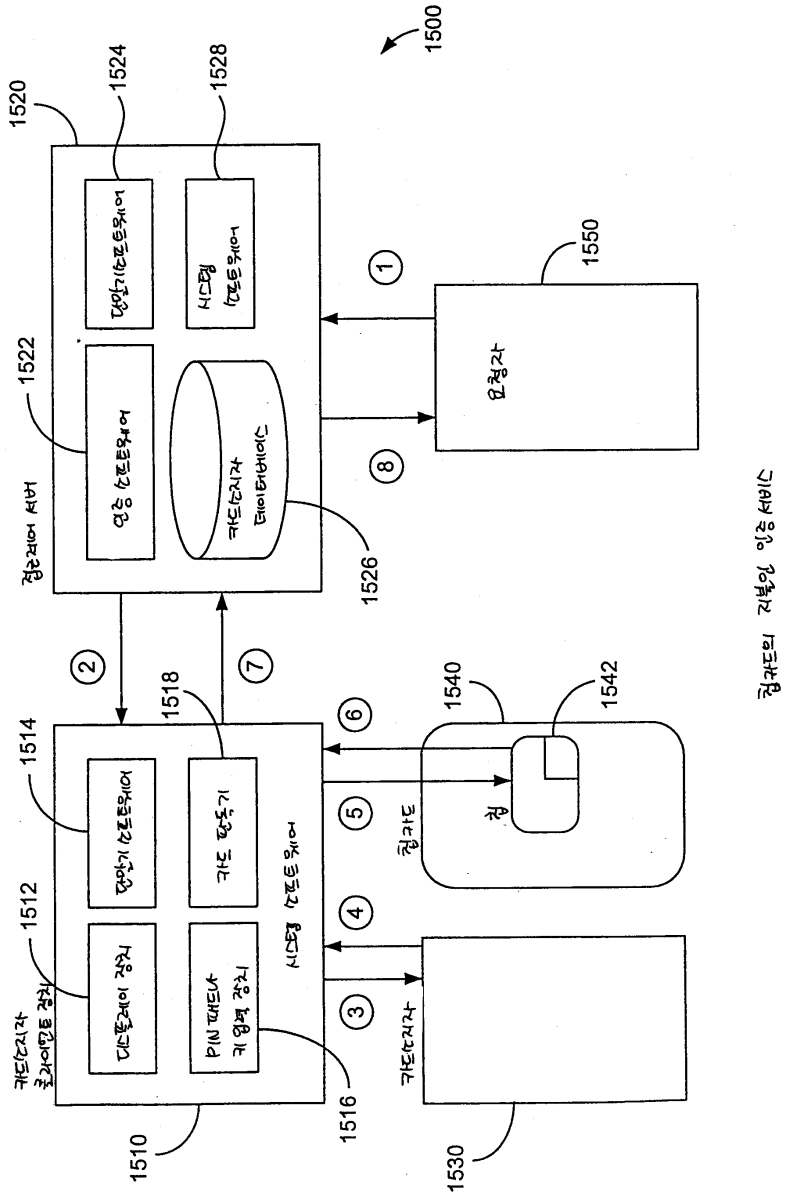


칩 카드 거래 인증 서비스 구조

도면11

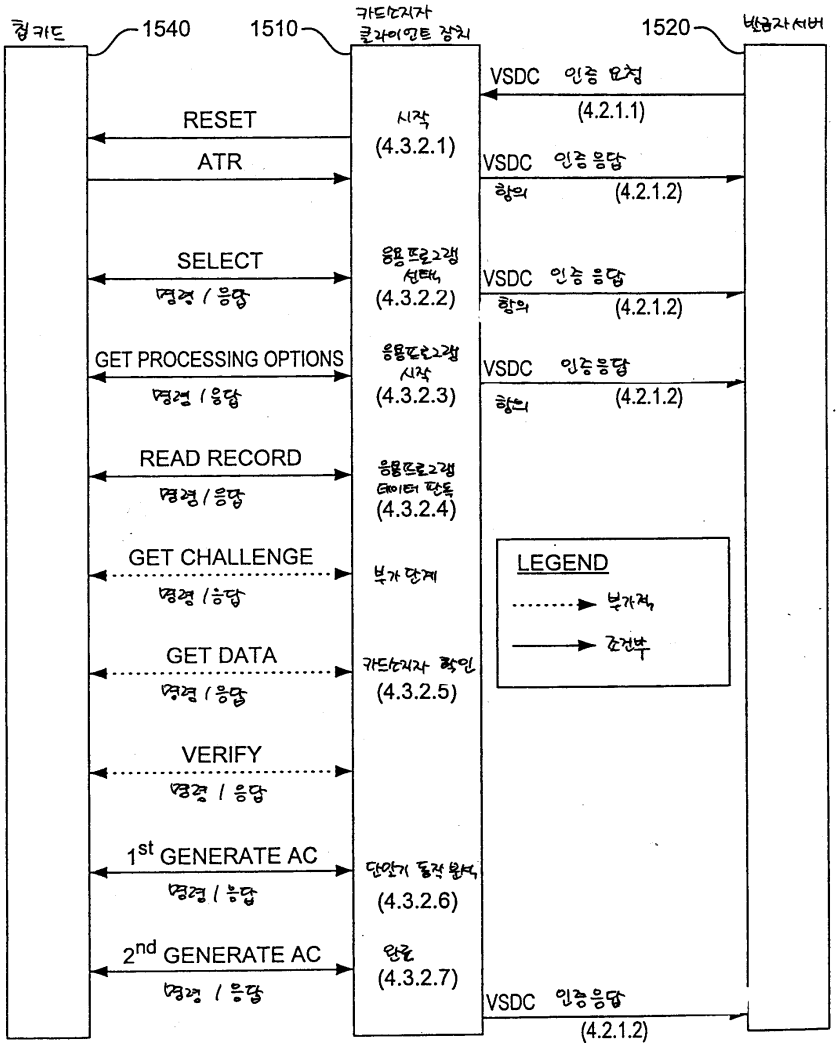

인증과정 시작
1100
카드소지자가 온라인 머천트에서 쇼핑을 시작
1110
카드소지자의 PAS 참가를 확인
1120
머천트가 지불 요청 메시지를 접근제어 서버에 전송
1130
카드소지자 클라이언트 장치가 칩카드 판독기를 포함하는지 확인
1140
카드소지자가 칩카드를 카드판독기에 삽입
1150
칩카드가 암호문을 생성
1160
카드소지자가 비밀번호를 입력
1170
암호문 및 비밀번호를 접근제어서버에 전송
1180
접근제어 서버가 암호문을 독립적으로 발생시키고 비밀번호를 확인
1190
접근제어 서버가 칩카드 인증확인을 위해 암호문을 비교
1195
지불응답 메시지 전송
종료

도면12


1500
1520
1524
1528
1522
1526
1550
요청자
1514
1518
1512
1516
1510
1540
1542
칩
칩카드
1530
카드단자기

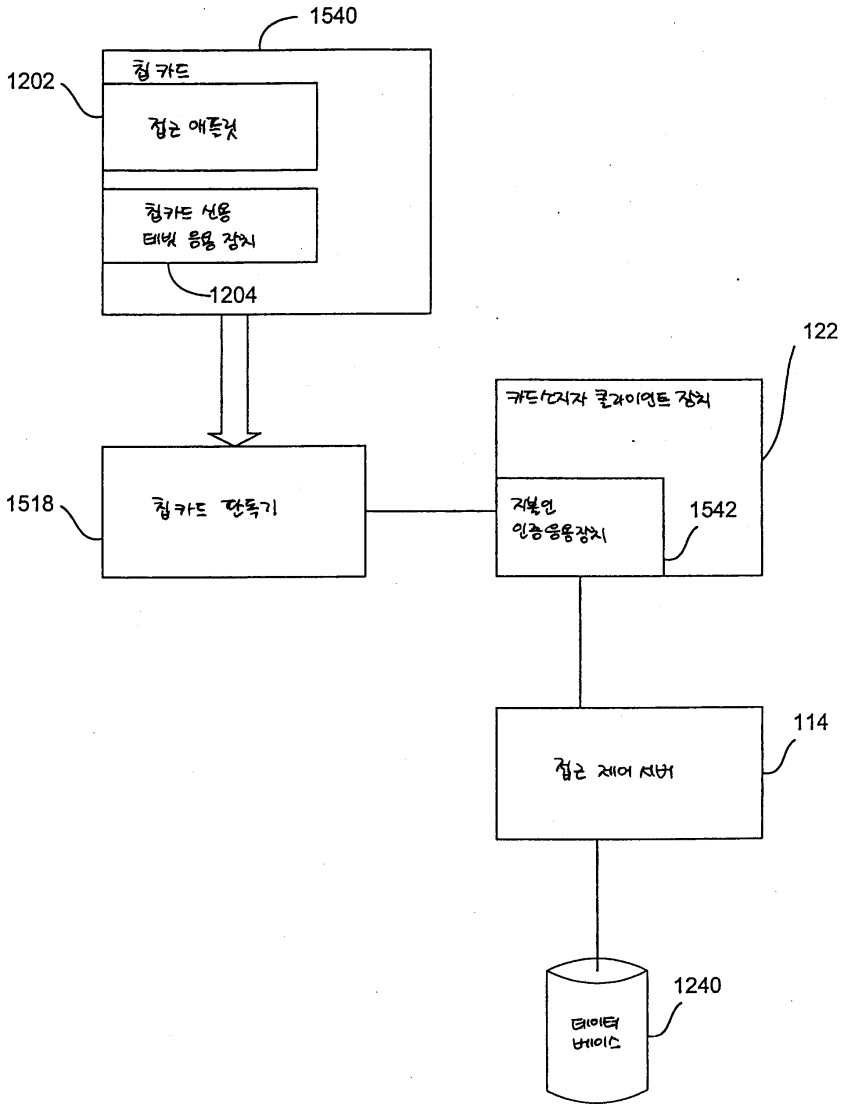
- 42 -

도면12a



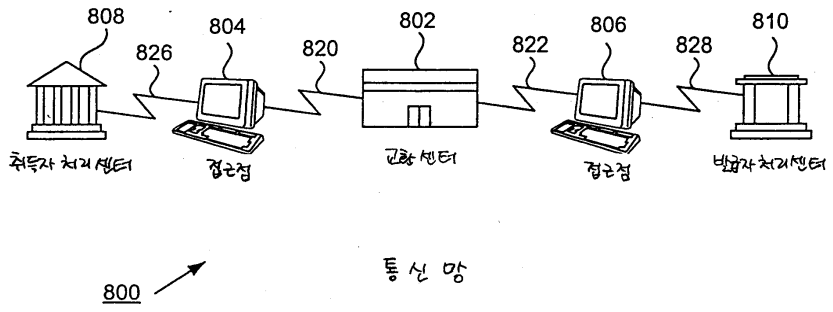
칩카드가 있는 지불의
인증서비스에 대한 상세 메시지 흐름도

도면13

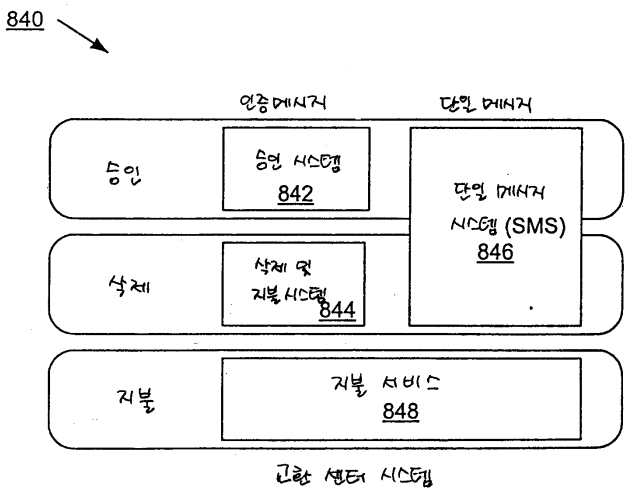


칩카드 및 범용접근응용장치가 있는 PAS

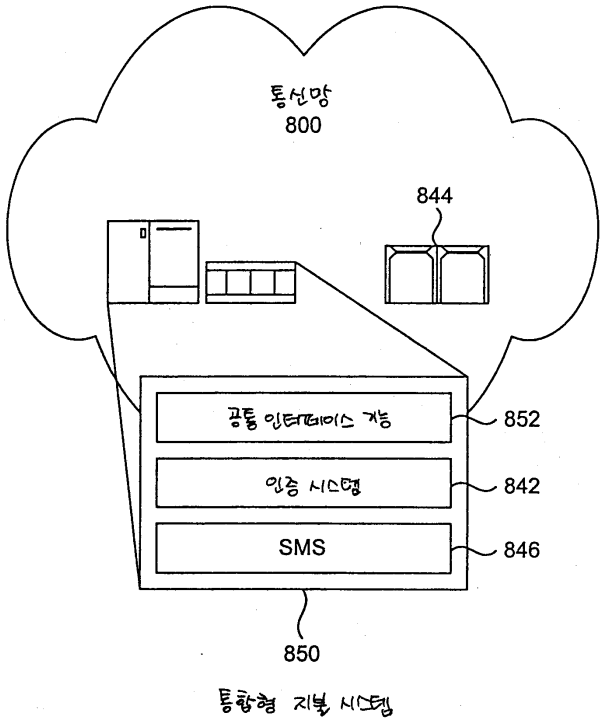
도면14



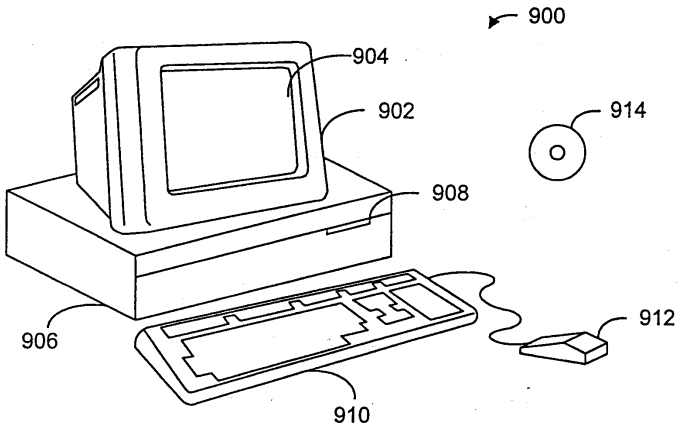
도면15


840
인증 메시지
단일 메시지
승인
승인 시스템
842
단일 메시지
시스템 (SMS)
846
상계
상계 및
지불 시스템
844
지불
지불 서비스
848
고객 센터 시스템

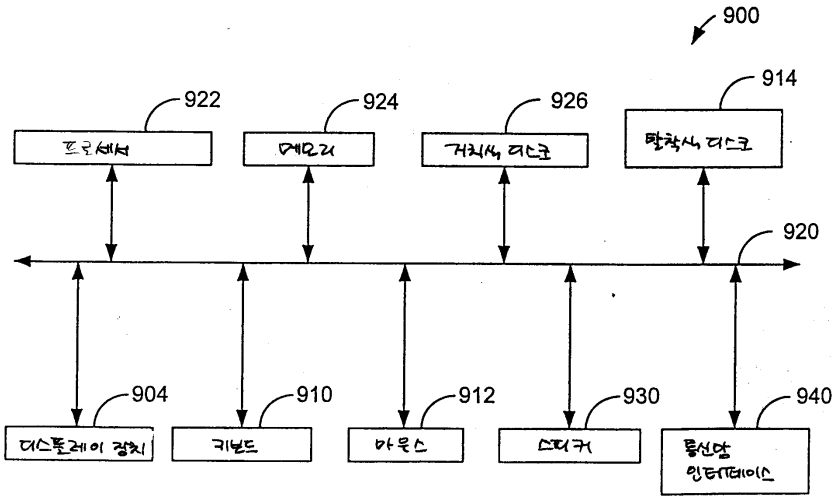
도면16


통신망
800
844
공통 인터페이스 기능
852
인증 시스템
842
SMS
846
850
통합형 지불 시스템

도면17a


900
904
902
914
908
912
906
910

도면17b


900
922
924
926
914
920
904
910
912
930
940