(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0107400
(43) 공개일자 2008년12월10일

(51) Int. Cl.
G06Q 20/00 (2008.03) *G06Q 30/00* (2006.01)
(21) 출원번호 10-2008-7021337
(22) 출원일자 2008년08월29일
심사청구일자 없음
번역문제출일자 2008년08월29일
(86) 국제출원번호 PCT/US2007/063239
국제출원일자 2007년03월02일
(87) 국제공개번호 WO 2007/103831
국제공개일자 2007년09월13일
(30) 우선권주장
60778282 2006년03월02일 미국(US)

(71) 출원인
비자 인터내셔날 써비스 어쏘시에이션
미합중국 94404 캘리포니아주 포스터시티 메트로 센터 보우리바드 900
(72) 발명자
도민구에즈, 베네딕토, 에이치.
미합중국, 켈리포니아 94066, 샌 브루노, 메리온 드라이브 2830
피셔, 더글라스
미합중국, 켈리포니아 94040, 마운틴 뷰, 브루커너 써클 1121
리, 티모씨, 무추
미합중국 켈리포니아 95120, 산호세, 올리브 브랜치 레인 1130
(74) 대리인
이만재

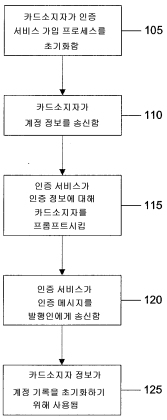
전체 청구항 수 : 총 21 항

(54) 통신 판매 및 전화 판매 트랜잭션에서 2개의 팩터 인증을 실행하는 방법 및 시스템

(57) 요 약

본 발명에 따라 통신 판매 또는 전화 판매를 인증하는 방법은, 카드소지자로부터 인증 정보를 수신하고, 인증 정보를 발행인에게 제공하고, 그 인증 정보가 유효한 지를 판정하는 것을 포함한다. 그 인증 정보가 유효하다면, 그 발행인은 그 트랜잭션이 유효하다는 것을 상인에게 알린다. 실시예에서, 발행인은 인증 정보에 응답해서 카드소지자에 의해 이미 공급된 개인 보증 메시지 및/또는 다른 기밀의 카드소지자 정보를 공급하지 않는다.

대 표 도 - 도1



특허청구의 범위

청구항 1

통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법에 있어서,

카드소지자로부터 트랜잭션 카드에 속하는 MOTO 구매 판매 및 정보를 수신하는 단계와;

가입 요청이 MOTO 트랜잭션에 속하는 것을 표시하는 표지를 구비하는 상기 가입 요청을 인증 서버에 송신하는 단계와;

인증이 상기 트랜잭션 카드에서 가용한지를 표시하는 가입 응답을 상기 인증 서버로부터 수신하는 단계와;

인증이 상기 트랜잭션 카드에 가용한 경우 민감한 카드소지자 정보를 포함하거나 요청하지 않는 인증 프롬프트를 상기 인증 서버로부터 수신하는 단계와;

상기 카드소지자에 의해 제공된 인증 정보를 상기 인증 프롬프트로 입력하는 단계와; 그리고

상기 인증 서버로부터 상기 카드소지자가 인증되는지를 표시하는 인증 응답을 수신하는 단계;를 포함하는 것을 특징으로 하는 통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법.

청구항 2

제 1항에 있어서,

상기 인증 응답이 상기 인증 서버에 의해 디지털적으로 서명되는 것을 특징으로 하는 통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법.

청구항 3

제 2항에 있어서,

상기 인증 응답을 유효화하는 단계를 더 포함하는 것을 특징으로 하는 통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법.

청구항 4

제 1항에 있어서,

상기 인증 정보가 칩 암호, 개인 식별 번호, 정적 패스코드, 1회성 패스코드, 또는 제한된 기간의 패스코드 중 적어도 하나를 포함하는 것을 특징으로 하는 통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법.

청구항 5

제 1항에 있어서,

상기 인증 정보가 동적 패스코드를 포함하는 것을 특징으로 하는 통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법.

청구항 6

제 1항에 있어서,

상기 카드소지자가 인증되지 않는 경우 상기 트랜잭션은 인가되지 않는 것을 특징으로 하는 통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법.

청구항 7

제 1항에 있어서,

상기 민감한 카드소지자 정보가 개인 보증 메시지를 포함하는 것을 특징으로 하는 통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법.

청구항 8

통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법에 있어서,

상인으로부터 트랜잭션 카드에 속하는 정보와, 상기 가입 요청이 MOTO 트랜잭션에 속하는 것을 표시하는 표지를 포함하는 가입 요청을 수신하는 단계와;

인증이 상기 트랜잭션 카드에 대해 가용한지를 표시하는 가입 응답을 상기 상인에게 송신하는 단계와;

인증이 상기 트랜잭션 카드에서 가용한 경우 민감한 카드소지자 정보를 포함하거나 요청하지 않는 인증 프롬프트를 상기 상인에게 송신하는 단계와;

상기 인증 프롬프트로 입력된 인증 정보를 수신하는 단계와; 그리고

상기 상인에게 상기 카드소지자가 인증되는지를 표시하는 인증 응답을 송신하는 단계를 포함하는 것을 특징으로 하는 통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법.

청구항 9

제 8항에 있어서,

상기 인증 응답이 디지털적으로 서명되는 것을 특징으로 하는 통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법.

청구항 10

제 8항에 있어서,

상기 민감한 카드소지자 정보가 개인 보증 메시지를 포함하는 것을 특징으로 하는 통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법.

청구항 11

제 8항에 있어서,

상기 인증 정보가 칩 암호, 개인 식별 번호, 정적 패스코드, 1회성 패스코드, 또는 제한된 기간의 패스코드 중 적어도 하나를 포함하는 것을 특징으로 하는 통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법.

청구항 12

제 9항에 있어서,

상기 인증 정보가 동적 패스코드를 포함하는 것을 특징으로 하는 통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법.

청구항 13

제 8항에 있어서,

상기 트랜잭션이 인가되는 것을 특징으로 하는 통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법.

청구항 14

제 8항에 있어서,

상기 카드소지자가 인증되지 않으면 상기 트랜잭션은 인가되지 않는 것을 특징으로 하는 통신 판매 또는 전화 판매(MOTO) 트랜잭션에서 인증을 실행하는 방법.

청구항 15

상인 시스템 및 인증 서버를 포함하는 시스템에서 트랜잭션 카드를 사용하는 온라인 지불 트랜잭션에서 인증을

실행하는 방법에 있어서,

물건값 계산 프로세스를 상기 상인 시스템에서 초기화하기 위해 물건값 계산 요청을 카드소지자로부터 수신하는 단계와;

상기 카드 소지자를 인증 정보에 대해 프롬프트시켜서 상기 카드소지자에게 민감한 카드소지자 정보를 포함하지 않는 인증 윈도우를 디스플레이하는 단계와;

상기 인증 서버에 상기 카드소지자에 의해 상기 윈도우로 입력된 인증 정보를 포함하는 인증 요청을 송신하는 단계와;

상기 인증 서버로부터 상기 카드소지자가 인증되는지를 표시하는 인증 응답 을 수신하는 단계와;

상기 가입 요청이 전자 상거래 트랜잭션에 속하는 지를 표시하는 표지 및 인증 요청을 상기 인증 서버에 송신하는 단계와; 그리고

지불 네트워크로부터 상기 트랜잭션 카드에 연결된 계정이 인가되는지를 표시하는 인가 응답을 수신하는 단계; 를 포함하는 것을 특징으로 하는 상인 시스템 및 인증 서버를 포함하는 시스템에서 트랜잭션 카드를 사용하는 온라인 지불 트랜잭션에서 인증을 실행하는 방법.

청구항 16

제 15항에 있어서,

상기 인증 요청이 계정 번호를 포함하는 것을 특징으로 하는 상인 시스템 및 인증 서버를 포함하는 시스템에서 트랜잭션 카드를 사용하는 온라인 지불 트랜잭션에서 인증을 실행하는 방법.

청구항 17

제 15항에 있어서,

상기 인증 정보가 칩 암호, 개인 식별 번호, 정적 패스코드, 1회성 패스코드, 또는 제한된 기간의 패스코드 중 적어도 하나를 포함하는 것을 특징으로 하는 상인 시스템 및 인증 서버를 포함하는 시스템에서 트랜잭션 카드를 사용하는 온라인 지불 트랜잭션에서 인증을 실행하는 방법.

청구항 18

제 15항에 있어서,

상기 인증 정보가 동적 패스코드를 포함하는 것을 특징으로 하는 상인 시스템 및 인증 서버를 포함하는 시스템에서 트랜잭션 카드를 사용하는 온라인 지불 트랜잭션에서 인증을 실행하는 방법.

청구항 19

제 15항에 있어서,

상기 트랜잭션이 인가되는 것을 특징으로 하는 상인 시스템 및 인증 서버를 포함하는 시스템에서 트랜잭션 카드를 사용하는 온라인 지불 트랜잭션에서 인증을 실행하는 방법.

청구항 20

제 15항에 있어서,

상기 민감한 카드소지자 정보가 개인 보증 메시지를 포함하는 것을 특징으로 하는 상인 시스템 및 인증 서버를 포함하는 시스템에서 트랜잭션 카드를 사용하는 온라인 지불 트랜잭션에서 인증을 실행하는 방법.

청구항 21

제 15항에 있어서,

상기 카드소지자가 인증되지 않으면 상기 트랜잭션은 인가되지 않는 것을 특징으로 하는 상인 시스템 및 인증 서버를 포함하는 시스템에서 트랜잭션 카드를 사용하는 온라인 지불 트랜잭션에서 인증을 실행하는 방법.

명 세 서

배 경 기 술

<1> 신용 카드, 지불(debit) 카드, 은행 카드, 고객 우대 카드, 스마트 카드 및/또는 등과 같은 트랜잭션 카드를 사용해서 트랜잭션할 때, 비인가된 사용과 같은 각종 문제를 방지하기 위해 카드소유자의 계정 소유를 입증하는 것이 중요하다. 카드소지자 인증은 카드소지자가 소유자인지를 입증하는 프로세스이다. 예를 들어, 상인의 대리인은 트랜잭션 카드의 서명이 수납시 카드소지자의 서명과 일치하는 것을 입증할 때, "카드 제시" 트랜잭션시의 카드소지자 인증이 실행된다.

<2> 기술 개선에 따라 기업 및 개인에게 다양한 환경의 트랜잭션을 가능하게 한다. 예를 들어, 카드소지자는 종래의 "직접" 트랜잭션, 인터넷을 경유한 트랜잭션, 전화를 통한 트랜잭션 및 통신 시스템을 통한 트랜잭션을 할 수 있다. 여러 경우에, 카드소지자는 서비스 제공자에 직접 방문하지 않고 트랜잭션을 실행하는 편리성을 원한다. 그렇게 할 때, 카드소지자는 자신의 집의 프라이버시로부터 그 트랜잭션을 실행함에 의해 예를 들어 소매 환경의 쇼핑 또는 은행의 줄서기에 관련된 운전 소요 시간을 없애고 혼란을 감소시킬 수 있다.

<3> 카드 제시 안된(Card not present("CNP")) 트랜잭션량이 카드소지자에 제공된 편리성 및 상인에게 제공된 특매로 인해 적어도 부분적으로 증가하고 있다. 그러나, CNP 트랜잭션량이 증가함에 따라, 그 트랜잭션에서 사기 트랜잭션 및 금전 손실이 또한 증가하고 있다.

<4> 동적 패스코드(예를 들어, Barclay PLC에 의한) 및 토큰 인증(예를 들어, MasterCard International Inc.에 의한)과 같은 각종의 솔루션이 전자상거래 및/또는 온라인 뱅킹 트랜잭션을 더 안전하게 되도록 제안되었다. 그러나, 그런 기술적 솔루션은 그 트랜잭션에 의해 제시된 특정한 도전으로 인해 통신 판매 및 전화 판매("MOTO")용으로는 구현되지 못했다.

<5> 예를 들어, MOTO 트랜잭션이 정적 패스코드를 사용할 때 안전의 취약성이 야기될 수 있다. 비인가된 제 3자는 트랜잭션을 인터셉트함에 의해 정적 패스코드를 얻을 수 있고 그 송신된 데이터를 역으로 분석해서 계정 정보 및 패스코드를 판정한다. 그 비인가된 제 3자는 예를 들어, 카드소지자 및 상인간에 또는 상인 및 발행인간에 통과된 정보를 인터셉트하는 사람일 수 있다. 대안적으로, 그 비인가된 제 3자가 상인 및/또는 그 대리인일 수 있다.

<6> 안정성을 증가시키기 위한 솔루션은 트랜잭션 카드의 카드 입증값 2("CCV2") 필드에 저장된 정보, 주소 입증 서비스, 만료일, 인가 제어로부터의 정보 등과 같은 정적 데이터를 사용한다. CCV2 필드는 카드소지자가 트랜잭션 카드를 소유하고 있다는 것을 보여준다. 카드소지자가 CCV2 정보를 상인에게 제공할 때, 상인은 인가 요구시 발행인에게 CCV2를 포함시키고, 제공된 CCV2 정보가 유효한 지를 인가 응답이 상인에게 알려준다.

<7> 그러한 정적 인증 방법의 하나의 단점은 인증값이 각 트랜잭션에 대해 변화하지 않는다는 것이다. 따라서, 아주 짧은 시간 주기동안 카드에 접근한 제 3자가 카드소지자의 인식없이 그 정보를 복제할 수 있고 그것을 사용할 수 있다.

<8> 정적 인증 방법의 다른 단점은 그 방법이 카드소지자를 인가하는 것과 대조적으로 트랜잭션 카드 제시만을 통상적으로 입증한다는 것이다. 그러나, 카드소지자 인증은 트랜잭션 입증보다 더 강한 안정성을 제공한다. 예를 들어, 카드소지자 인증은 카드 발행인에게 충분한 비-거절 증거를 제공하여, 트랜잭션 카드가 인증되지 않을 때, 상인의 지불거절을 가능하게 한다.

<9> 동적 인증 기술은 MOTO 환경에서 카드소지자 인증을 용이하게 하기 위해 또한 고안되었다. 그런 기술은 음성 인증, 소리 인증(즉, 동적 소리를 발생시키는 트랜잭션 카드) 및 동적 패스코드를 포함한다. 그 동적 인증 기술의 하나의 단점은 그들이 MOTO 인증 솔루션을 구현하는 데 필요로 되는 요구된 솔루션의 일부만을 나타낸다는 것이다. 그 기술은 솔루션을 기반 구조층에 나타내지 않아서 상인이 인증 데이터를 카드소지자로부터 수신하고 그 데이터를 트랜잭션 카드 발행인에게 송신한다. 상인은 그 동적 정보를 수락하고 진행시키기 위해 시스템을 구현할 필요가 있다. 또한, 매수자는 동적 정보를 트랜잭션 카드 발행인에게 통과시키기 위해 시스템을 구현할 필요가 있다.

<10> 따라서, 카드소지자 및 상인은 사기적인 MOTO 트랜잭션이 자주 발생하고 사기가 아닌 트랜잭션의 정보가 사기 목적으로 도난당하는 것에 관심을 갖는다. MOTO 트랜잭션에 비인가된 접근을 방지시키는 방법 및 시스템이 필요로 된다.

<11> MOTO 트랜잭션을 안전하게 실행하는 방법 및 시스템이 필요하다.

<12> MOTO 트랜잭션에 사기적인 접근을 방지하기 위해 MOTO 환경에서 2개의 팩터 인증을 실행하는 방법 및 시스템이 더 필요하다.

<13> 본 개시는 상기 언급된 문제를 해결하기 위한 것이다.

<14>

발명의 상세한 설명

<15> 본 발명의 방법, 시스템 및 재료를 설명하기 전에, 본 발명이 설명된 특정한 방법론, 시스템 및 재료로, 그것들이 변화해도, 제한되지 않는 것으로 이해된다. 또한, 본 설명에서 사용된 용어가 특정한 버젼 또는 실시예만을 설명할 목적이고 첨부된 청구항만에 의해 제한되는 본 발명의 범위를 제한하지 않는다.

<16> 여기 및 청구된 청구항에 사용된 바와 같이, 단일 형태 "a", "an" 및 "the"는 그 문맥이 다르게 명백히 표시하지 않는 한 복수의 레퍼런스를 표함한다. 그러므로, 예를 들어, "카드소지자"에 대한 레퍼런스는 값, 데이터 및/또는 정보의 교환에서 하나 이상의 사람에 대한 레퍼런스이다. 다르게 표현되게 언급하지 않으면, 본원에서 사용된 모든 정의안된 기술 및 과학 용어는 본 기술에 보통의 기술을 가진 자에 의해 일반적으로 이해되듯이 같은 의미인 반면에 모든 정의된 기술 및 과학 용어는 언급된 정의에 의해 보통의 기술을 가진 자에 의해 일반적으로 이해되듯이 같은 의미로 된다. 본원에 설명된 것과 비슷하거나 동동한 방법, 재료 및 장치가 사용될 수 있지만, 양호한 방법, 재료 및 장치가 현재 설명된다. 본원에서 언급된 모든 공개 사항이 참고문헌과 결부된다. 본원의 아무것도 본 발명이 종래의 발명에 의한 그 공개보다 선행할 자격으로 되지 않는 것으로 허여되지 않는다.

<17> 실시예에서, 통신 판매 또는 전화 판매 트랜잭션을 인증하는 방법은, 카드소지자로부터 상인에 의해 인증 정보를 수신하고, 인증 정보를 발행인에게 제공하고, 그 인증 정보의 유효 여부를 그 발행인에 의해 판정하는 것이다. 인증 정보가 유효하다면, 그 발행인은 트랜잭션의 유효성을 상인에게 알린다. 그렇치 않으면, 발행인은 그 인증 정보가 무효라는 것을 상인에게 알린다. 실시예에서, 인증 정보는 트랜잭션 카드, 계정 또는 카드소지자를 인증하기 위해 사용될 수 있는 동적 패스코드, 정적 패스코드, 생체 인식과 같은 정보 또는 기타 정보를 포함한다. 예를 들어, 그런 정보는 소리, 소리 생체 인식, 사업 식별, 국가 코드, 카드 계정 번호, 카드 만료일, 카드소지자 성명, "참여한 PIN" 데이터에서 특정화된 발행인의 특정 인증 데이터(예를 들어, 어머니의 처녀때 성명), 요금청구 주소, 선적 주소, 사회 안전 번호, 전화 번호, 계정 대조표, 트랜잭션 이력 및/또는 운전자의 면허 번호를 포함한다. 실시예에서, 발행인은 상인이 인증을 MOTO 트랜잭션의 일부로서 초기화했는 지를 판정한다. 실시예에서, 발행인은, 상인이 인증 정보를 송신한다면, 그 인증 정보에 응답해서 카드소지자에 의해 이미 공급된 개인 보증 메시지 및/또는 기타의 카드소지자 정보를 공급하지 않는다.

실 시 예

<22> 온라인 환경에서 설정, 인가, 등록 및 안전하게 트랜잭션하는 예시용 방법이 현재 설명된다. 초기에, 인증 서비스는 설정된다. 그 인증 서비스를 설정하는 것은 시스템에서 각 참여자에 대해 초기화 절차를 실행하는 것을 포함한다. 그 참여자들은 상인, 금융 기관(즉, 발행인), 매수자 및 카드소지자와 같은 복수의 엔티티를 포함한다. 인증 서비스에 서명하는 상인은 온라인 환경에서 상인 플러그-인 소프트웨어 모듈을 수신한다. 실시예에서, 플러그-인 소프트웨어 모듈은 상인의 컴퓨팅 플랫폼 및 상업 서버 소프트웨어에 대해 특히 설계된다. 인증 서비스에 참여하는 발행인은 주문제조된 인증 서비스 등록 사이트 템플릿으로 결합하기 위해 은행 로고 및 마켓팅 설계를 제공할 수 있다. 매수자는 서비스 회사 인증 기관("CA")의 최상위 인증서, 즉 서비스 회사 인증 기관 SSL 인증서를 클라이언트 인증 및/또는 집중 지원용으로 상인에게 또한 제공한다.

<23> 발행인이 인증 서비스를 사용하기 전에, 발행인은 발행인 도메인에서 특정화된 인증 소프트웨어 프로그램의 복제를 얻을 수 있고 하드웨어 시스템 및 인증 서비스 소프트웨어를 설치할 수 있다. 발행인은 카드소지자 입증 프로세서에서 사용되게 하기 위해 동일성 인증 방법 및 참여한 사업 식별 번호(BIN)를 그 인증 서비스에 또한 제공한다. 실시예에서, 발행인은 인증 정보를 인증 서비스에 제공한다. 인증 정보의 프리-로딩(pre-loading)이 방대한 양의 카드소지자를 지원할 수 있게 한다. 예를 들어, 발행인이 인증 서비스에 대해 모든 또는 대부분의 카드소지자를 활성화시키길 원할 때, 발행인은 개별 식별 번호(PIN)를 각 카드소지자에 할당한다. 그 후에, 각 카드소지자가 그 할당된 PIN을 인증 정보에 접근시키기 위해 사용할 수 있다. 이런 방법에서, 각 카드소지자가 공식 가입 프로세스의 완료를 요구하지 않으므로 그 가입 프로세스는 신속 처리될 수 있다. 인증 정보는 트랜잭션 카드, 계정 또는 카드소지자를 인증하기 위해 사용될 수 있는 동적 패스코드, 정적 패스코드, 생체 인식과

같은 정보 또는 기타 정보를 포함한다. 예를 들어, 그런 정보는 소리, 소리 생체 인식, 사업 식별, 국가 코드, 카드 계정 번호, 카드 만료일, 카드소지자 성명, "참여한 PIN" 데이터에서 특정화된 발행인의 특정 인증 데이터(예를 들어, 어머니의 처녀때 성명), 요금청구 주소, 선적 주소, 사회 안전 번호, 전화 번호, 계정 대조표, 트랜잭션 이력 및/또는 운전자의 면허 번호를 포함한다. 발행인은 그들의 카드 계정 포트폴리오 및 접근 제어 서버("ACS") IP 주소 또는 URLs(Uniform Resource Locators)의 계정 번호 범위를 디렉토리 서버에 제공한다. 실시예에서, 인증 서비스는 은행 상표가 붙은 웹 사이트를 통해 제공되어, 카드소지자로 하여금 인증 서비스에 등록하도록 허여한다. 대안의 실시예에서, 정보는 통신 서비스, 전화 및/또는 다른 통신 수단을 통해 송신된다.

<24> 도 1은 실시예에 따라 인증 서비스에 카드소지자를 등록하는 예시용 프로세스를 도시한다. 도 1에 도시했듯이, 카드소지자가 발행인에 의해 유지된 가입 웹 사이트를 방문한다(105). 대안의 실시예에서, 카드소지자는 전화, 통신 및/또는 다른 통신 수단에 의해 발행인과 접촉할 수 있다. 카드소지자는 하나 이상의 트랜잭션 계정 번호를 그 서비스에 공급함에 의해 인증 서비스에 등록할 수 있다. 카드소지자는 PAN(Primary Account Number), 카드소지자 성명, 카드 만료일, 주소, 이메일 주소, 구매자 식별값, 계정 입증값, 카드소지자의 특정한 패스워드 및/또는 인증 정보와 같은 정보를 송신한다(110).

<25> 카드소지자가 그 요청된 정보를 인증 서비스에 보낸 후, 그 서비스는 카드소지자가 발행인에 의해 등록된 카드 범위 내에 있다는 것을 입증할 수 있다. 인증 서비스는 예를 들어, 제 3자 및/또는 발행인에 의해 유지된 인증 데이터베이스를 사용해서 카드소지자의 동일성을 또한 입증할 수 있다. 실시예에서, 발행인은 승인된 카드소지자의 발행인 제공된 파일을 사용해서 카드소지자의 동일성을 입증할 수 있다. 실시예에서, 발행인은 상태 확인 인가를 분석해서 카드소지자의 동일성을 입증할 수 있다. 실시예에서, 발행인은 발행인에 의해 제공된 인증 데이터베이스에서 응답을 프리-로드된 정보에 비교해서 카드소지자의 동일성을 입증할 수 있다.

<26> 그 특정화된 PAN이 발행인 가입된 카드 범위 내에 있지 않다면, 그 가입은 거절될 수 있고, 그 가입 프로세스는 종료된다. 그 PAN이 가입된 카드 범위 내에 있다면, 예를 들어, 1달러의 인가는 VisaNet와 같은 서비스 회사 지불 네트워크를 통해 발행인에게 지출된다. 실시예에서, 그 1달러 트랜잭션의 인가는 발행인으로 하여금 카드 계정 상태를, 주소 입증 서비스를 사용해서 주소를, 및 카드 입증값2("CVV2")을 입증하도록 허여한다. 대안 또는 추가의 정보가 인가 프로세스동안 입증될 수 있다. 실시예에서, CVV2 필드는 트랜잭션 카드의 서명 스트립상에 통상적으로 인쇄되는 3-디지트값일 수 있다.

<27> 카드가 승인되면, 인증 서비스는 카드소지자의 동일성을 입증하기 위해 카드소지자로 하여금 추가의 인증 정보로 프롬프트할 수 있다(115). 그 카드소지자는 연속 판매 트랜잭션동안 카드소지자의 동일성을 인증하기 위해 패스워드 및 "힌트 질의 및 응답"을 제공할 수 있다.

<28> 카드소지자의 동일성이 입증되고 알맞은 응답이 복귀될 때, 인증 서비스가 인가 메시지를 발행인에게 보낸다(120). 가입 서버는 계정 홀더 파일의 기록을 초기화하기 위해 카드소지자 정보를 ACS에 통과시킨다(125). 계정 홀더 파일은 금융기관 BIN 번호, 계정 번호, 만료일, 성명, 운전자 면허 번호, 요금청구 주소, 사회 안전 번호, 카드소지자 패스워드, 카드소지자 패스워드 질의, 카드소지자 패스워드 응답, 카드소지자 이메일 주소, 제 3자 동일성 스코어와 같은 정보 및 다른 정보를 저장한다.

<29> 그 인증 서비스 참여자가 초기화되고 카드소지자가 등록된 후, 지불 트랜잭션이 그 인증 서비스를 사용해서 인증될 수 있다. 도 2는 실시예에 따라 온라인 지불 트랜잭션을 인증하는 예시적인 프로세스를 도시한다. 도 2에 도시했듯이, 카드소지자가 상인의 상업 웹 사이트를 방문한다(205). 카드소지자가 구매용 제품 또는 서비스를 선택한 후, 카드소지자는 물건값 계산 프로세스를 시작하여, 물건값 계산 양식을 작성하고 "구매" 버튼을 클릭한다(210)

<30> "구매" 버튼이 선택된 후(210), 상인 플러그-인 소프트웨어 모듈이 활성화된다. 상인 플러그-인 소프트웨어는 카드소지자의 특정화된 계정이 인증 서비스에 등록되는 지를 판단하기 위해 입증 프로세스를 실행한다(215). 입증은 ⅰ) 그 카드소지자와 관련된 ACS 및 디렉토리 서버가 확인되는 프로세스, ii) ACS만이 확인되는 프로세스, iii) 그 상인이 디렉토리 서버와 유사한 정보를 포함하는 캐시 메모리를 확인한는 프로세스를 사용해서 실행된다(215).

<31> 상인 플러그-인 소프트웨어 모듈은 PAN이 인증 서비스 참여자인 발행인 은행과 관련된 번호 범위 내에 있는 것을 입증하기 위해 PAN을 식별하고 디렉토리 서버에 질의한다. 그 계정 번호가 디렉토리 서버에 형성된 PANs 범위 내에 있지 않다면, 카드소지자가 인증 서비스에 등록되지 못한다. 이런 경우에, 그 상인은 그 계정 번호가 등록되지 않는 것을 인식할 수 있고, 상인 플러그-인 소프트웨어 모듈이 트랜잭션의 제어를 상인 스토어프런트

(storefront) 소프트웨어에 복귀시킬 수 있다. 이런 관점에서, 상인 스토어프런트 소프트웨어는 트랜잭션을 진행시키고, 또한 서비스를 카드소지자에게 거절하거나, 대안의 지불 방법을 진행시킨다.

<32> PAN이 디렉토리 서버에 의해 수락된 PANs 범위 내에 있다면, 그 디렉토리는 카드소지자를 인증할 수 있는 ACS에 PAN을 보내서 그 카드가 가입되는 지를 판단한다. 카드가 가입되지 않는다면, 입증 프로세스가 종료된다. ACS는 카드가 가입되는 것으로 표시하면, ACS는 그 URL을 디렉토리 서버를 통해 상인 플러그-인 소프트웨어 모듈로 복귀한다. 상인 플러그-인 소프트웨어는 카드소지자 클라이언트 장치 및 그것에 있는 브라우저를 통해 ACS를 인보크한다. 다수의 ACS는 인증 서비스에 저장될 수 있다.

<33> 실시예에서, 상인 플러그-인 소프트웨어는 카드소지자의 등록을 인증 서비스로 입증하기 위해 ACS에 질의할 수 있다. 실시예에서, 상인은 디렉토리 서버에 저장된 같은 정보를 사실상 포함하는 캐시 메모리에 접근할 수 있어서 카드소지자의 등록을 인증 서비스로 입증시킨다. 실시예에서, 하나 이상의 물리적인 디렉토리 서버가 인증 서비스에 있을 지라도, 인증 서버는 하나만의 논리 디렉토리 서버를 포함한다.

<34> 카드소지자가 인증 서비스 참여자라면, ACS가 발행인 상표가 붙은 윈도우를 카드소지자에게 디스플레이할 수 있다. 발행인 상표가 붙은 윈도우는 기본적인 지불 트랜잭션 정보를 포함하고 카드소지자를 인증 정보로 프롬프트시킨다. 카드소지자는 ACS에 의해 인증 정보를 입증용으로 입력할 수 있다.

<35> 올바른 인증 정보가 즉시 입력되거나 올바른 응답이 허여된 시도 횟수내에서 힌트 질의로 제공되면 지불 인증은 계속된다. ACS는 발행인의 서명 키 및/또는 서비스 제공자 키를 사용해서 수신을 디지털적으로 서명할 수 있다. 그 수신은 상인 성명, 카드 계정 번호, 지불 계정 및 지불일을 포함한다. 수신 파일은 상인 성명, 상인 URL, 카드 계정 번호, 만료일, 지불 계정, 및 지불일, 발행인 지불 서명 및/또는 카드소지자 인증 입증값을 저장할 수 있다. 그런후, ACS는, 카드소지자가 상인에 인증되었는 지에 관해서, 카드소지자를 카드소지자의 브라우저를 통해 상인 플러그-인 소프트웨어 모듈로 리다이렉트시킬 수 있고 디지털적으로 서명된 수신 및 그 판정을 통과시킨다. 상인 플러그-인 소프트웨어 모듈은 유효 서버를 사용하여 지불 수신을 서명하기 위해 사용된 디지털 서명을 입증시킨다. 디지털 서명을 입증시킨 후, 카드소지자가 "인증"될 수 있다. 트랜잭션 완료후, 카드소지자는 트랜잭션 카드 계정을 재등록할 수 있고/있거나 새로운 인증 정보를 생성할 수 있어서 미래의 트랜잭션에 사용된다.

<36> 카드소지자 인증후, 특정한 카드소지자의 계정이 인가된다. 특히, 상인은 인가 메시지를 상인 플러그-인 소프트웨어 모듈을 통해 VisaNet와 같은 지불 네트워크로 보낸다(220). 지불 네트워크는 그 인가 메시지 및 ECI(Electronic Commerce Indicator)를 발행인에게 전송할 수 있다. 그 발행인은 인가 메시지를 수신하여 발행인이, 특정 계정이 양호한 지위에 있고 그 요청된 트랜잭션에 대해 가용한 충분한 신용을 갖는 것을, 상인에게 입증할 수 있다. ECI는 그 트랜잭션이 인터넷을 통해 완료되는 것을 표시하여 알맞은 메시지 안정성 및 인증 레벨이 사용된다.

<37> 발행인이 인증 트랜잭션을 프로세스 한 후에, 구매 트랜잭션의 제어가 지불 네트워크를 경유해서 상인의 스토어프런트 소프트웨어로 복귀될 수 있다. 그 발행인은 인가 응답을 지불 네트워크를 경유해서 상인에게 복귀시킬 수 있다(225). 그 인가 응답은 트랜잭션을 인가 또는 거절할 수 있다.

<38> MOTO 트랜잭션에서, 상인은 인증 정보 교환시 카드소지자를 발행인에 리다이렉팅함에 의해 카드소지자의 인증을 초기화할 수 있다. 카드소지자가 MOTO 트랜잭션에서 발행인에게 직접 연결하지 않으므로, 카드소지자는 인증 정보를 상인에게 제공할 수 있다. 그 후에, 상인은 카드소지자를 위해 그 정보를 제출한다. 따라서, MOTO 트랜잭션에서 상인은 카드소지자가 "카드 제시" 또는 전자 상거래 트랜잭션에서 통상적으로 실행하는 기능을 실행한다. 실시예에서, 인증 정보가 상인으로 하여금 사기적인 방법으로 인증 정보를 사용하지 못하게 하고 다르게는 안정성을 위협받지 않게 하기 위해 동적 생성된다. 그 트랜잭션 시스템은, 상인이 정보를 상인으로부터 요청함에 의해 카드소지자를 대신해서 정보를 입력하는 지를, 판정할 수 있다. 따라서, MOTO 트랜잭션 실행시, 개인 보증 메시지와 같은 민감한 카드소지자 정보는 상인에 송신되지 않는다. 실시예에서, 식별자는 MOTO 트랜잭션이 실행되는 지를 표시할 수 있다.

<39> 소정의 기능은 상인이 MOTO 트랜잭션에서 카드소지자를 위해 작동할 때 사용하기에 적합하지 않다. 예를 들어, 미래의 트랜잭션에서 카드소지자를 입증하기 위해 트랜잭션동안 인증 정보를 생성하도록 카드소지자를 동작시키는 기능성은 MOTO 트랜잭션의 프로세스에서 동작 될 수 없다. 그런 특성은, 상인이 트랜잭션에서 데이터 엔트리를 실행할 때, 알맞지 않다. 유사하게, 발행인이 위험 경감 목적으로 트랜잭션 창출자의 위치를 트랙킹하면, 그런 기능성은, 상인이 인증 정보에 입력하는, MOTO 트랜잭션에 대해 동작될 수 없다.

<40> 도 3은 실시예에 따라 MOTO 트랜잭션을 인증하는 예시적인 프로세스를 도시한다. 도 3에 도시했듯이, 카드소지자는 예를 들어, 전화 또는 통신 서비스를 통한 구매에서 카달로그로부터 아이템을 선택하고 완료한다(305). 상인은 구매를 위한 가입 요청을 예를 들어 디렉토리 서버에 보낸다(310). MOTO 트랜잭션 표지는 가입 요청에 포함될 수 있다. 그 표지는 트랜잭션이 MOTO 트랜잭션이고 카드소지자가 인증을 직접 제공하지 않는 것을 표시한다. 상인에게 카드소지자에 의해 제공되고 디렉토리 서버로 이송되는 카드 번호가 참여한 카드 범위내에 있다면(315), 디렉토리 서버는 가입 요청을 예를 들어, 알맞은 ACSs에 송신한다(320). ACSs는 인증이 카드에 가용한지를 표시하는 가입 응답으로써 디렉토리 서버에 응답한다(325). 카드 번호가 참여한 범위에 있지 않다면, 디렉토리 서버는 트랜잭션을 거부하는 가입 응답을 생성한다(330). 가입 응답은 상인에게 보내진다(335).

<41> 인증이 가용하다고 가정하면, 상인은 인증 요청을 상인의 브라우저를 통해 ACS에 송신한다(340). ACS는 인증 요청을 수신하고(345) 카드소지자를 카드 번호에 알맞게 인증한다(350). 예를 들어, 카드소지자는 인증 정보, 칩 암호, PIN 등을 제공하기 위해 요청된다. ACS는 트랜잭션이 카드소지자의 계정 식별자를 가입 요청과 비교함에 의해 MOTO 트랜잭션이라는 것을 판정할 수 있다. ACS는 카드소지자 정보 필드가 카드소지자에게 기밀로 되지 않아서 상인에게 디스플레이하기에 알맞은 것을 또한 판정할 수 있다. 예를 들어, 개인 보증 메시지는 상인에게 디스플레이하기에 알맞지 않게 된다. ACS는 인증 응답을 상인의 브라우저를 통해 상인에게 송신하기(355)전에 인증 응답 메시지를 포맷할 수 있고 디지털적으로 서명할 수 있다. 실시예에서, ACS는 미래의 입증을 위해 입증 응답을 입증 이력 서버에 보낸다. 상인은 인증 응답을 수신하고(360) 인증 응답 서명을 유효화한다(365). 유효화되면, 상인은 그 트랜잭션을 그 매수자에게 인가할 수 있다(370).

<42> 실시예에서, 카드소지자는 인증 정보를 생성하는 동적 방법을 구비할 수 있다. 인증 정보를 생성하는 방법은 변화하고 본원에서 명백하게 제약받지 않는다. 예를 들어, 카드소지자는 1회성 패스코드 목록을 포함하는 인쇄된 시트 및/또는 제한된 기간의 패스코드를 구비하고 있다. 카드소지자는 동적 패스코드 장치, 동적 패스코드를 생성하는 트랜잭션 카드 및/또는 판독기, 및/또는 동적 패스코드를 생성하기 위해 생체 인식을 사용하는 트랜잭션 카드를 또한 발행시킬 수 있다.

<43> MOTO 트랜잭션을 실행하는 이전 방법에 대한 개선점은 전자 상거래 및/또는 온라인 뱅킹 환경에서 사용된 기초적인 트랜잭션 시스템에 상당한 변형없이 카드소지자의 인증을 가능하게 한다. 그러한 것으로서, 본원에서 설명되는 개선된 MOTO 트랜잭션은 기초적인 기반 구조에 실질적인 변형없이 안전성을 향상시킬 수 있다.

<44> 실시예에서, 정적 패스코드가 사용될 수 있다. 그것은 카드소지자에게 추가의 편리성을 제공한다. 실시예에서, 정적 패스코드는 카드소지자가 상인을 대신해서 발행인에게 직접 패스코드를 제공하는 MOTO 트랜잭션에서 사용될 수 있다.

<45> 도 4는 양호한 실시예에 따라 MOTO 트랜잭션을 인증하는 예시용 프로세스의 흐름도를 도시한다. 도 4에 도시했듯이, 소비자를 대표한 MOTO 오퍼레이터는 상인 웹 사이트상에서 상인 쇼핑 카드를 사용해서 하나 이상의 기능을 실행할 수 있다(405). 실시예에서, 그 하나 이상의 기능이 물건을 선택하고; 물건량을 추가, 제거 및/또는 갱신하고; 선택된 물건의 누계를 유지하는 것들 중 하나 이상을 포함한다. 그런후, MOTO 오퍼레이터는 물건값 계산 프로세스를 실행한다(410). 예를 들어, 소비자를 대표한 MOTO 오퍼레이터는 선적 정보에 입력하고, 지불 정보를 입력하고/하거나 트랜잭션을 완료한다.

<46> 실시예에서, 입증 프로세스는 초기화된다. 예를 들어, 상인 플러그-인 소프트웨어는 VEReq(Verify Enrollment Request)를 발행인 ACS에 송신한다(415). 실시예에서, VEReq는 MOTO 트랜잭션용으로 세트되는 MOTO 트랜잭션 표지를 포함한다. MOTO 트랜잭션 표지는 트랜잭션이 MOTO 트랜잭션이고, 카드소지자가 인증을 직접 제공하지 않는다는 것을 표시한다. ACS는 MOTO 트랜잭션 표지가 VEReq에서 세트되는 지를 판정한다(420). 그렇다면, ACS는 MOTO 트랜잭션에 맞춰진 VERes로써 MOTO 오퍼레이터에 응답한다(425). 실시예에서, VERes는 인증이 트랜잭션에서 가용한지를 표시하는 정보를 포함한다.

<47> 인증이 카드에 대해 가용하다면, MOTO 오퍼레이터가 PAReq(Payer Authentication Request)를 상인의 브라우저를 통해 ACS에 송신한다(430). ACS는 PAReq를 수신하고(435) 카드 번호를 토대로 알맞은 카드소지자를 인증한다(440).실시예에서, ACS는 상기 설명된 VEReq/VERes 프로세스를 토대로 한 MOTO 트랜잭션으로서 계정 식별자를 인식할 수 있다. ACS는 MOTO 오퍼레이터에 송신하기 위해 PARes(Payer Authentication Respose)를 생성한다(445). 실시예의 MOTO 트랜잭션에서, ACS는 개인 보증 메시지, 패스워드 등과 같은 민감한 카드소지자 정보를 송신할 수 없다. 실시예의 MOTO 트랜잭션에서, ACS는 사기 검출 목적으로 고객의 구매 위치를 트랙킹하는 쇼핑 특성동안 활성화되지 못한다. MOTO 오퍼레이터는 PARes를 수신하고(450), 선택적으로 발행인을 인증하는 트랜잭션에 속하는 정보를 디스플레이한다. MOTO 오퍼레이터는 화폐값이 일반적으로 MOTO 오퍼레이터에 이송되는 트랜

잭션 인증 프로세스에 있게 된다.

<48> 상기 개시되고 다른 특성 및 기능, 또는 그 대안예가 다수의 다른 시스템 또는 애플리케이션에 바람직하게 결합됨을 알 수 있다. 또한, 본원에서 여럿의 예견되지 않거나 기대안한 대안예, 변형예, 변화 또는 개선점이 본 기술에 숙련된 자에 의해 계속해서 이루어질 수 있음을 알 수 있다.

<49>

도면의 간단한 설명

<18> 도 1은 실시예에 따라 인증 서비스에 카드소지자를 등록하는 예시용 프로세스 도시도.

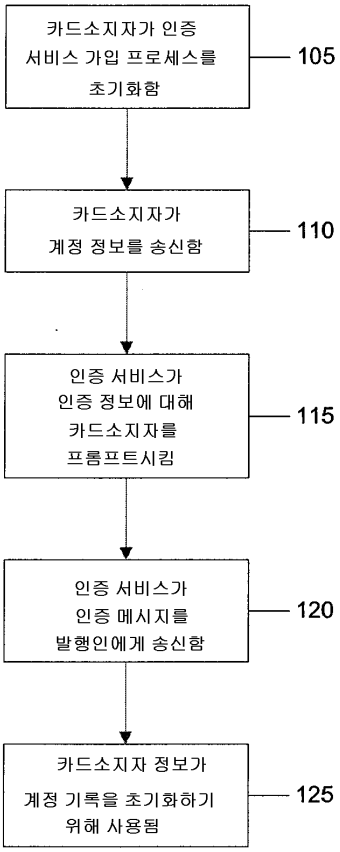
<19> 도 2는 실시예에 따라 인증된 지불 트랜잭션에 대한 예시용 프로세스 도시도.

<20> 도 3은 실시예에 따라 MOTO 트랜잭션을 인증하는 예시용 프로세스의 흐름도.

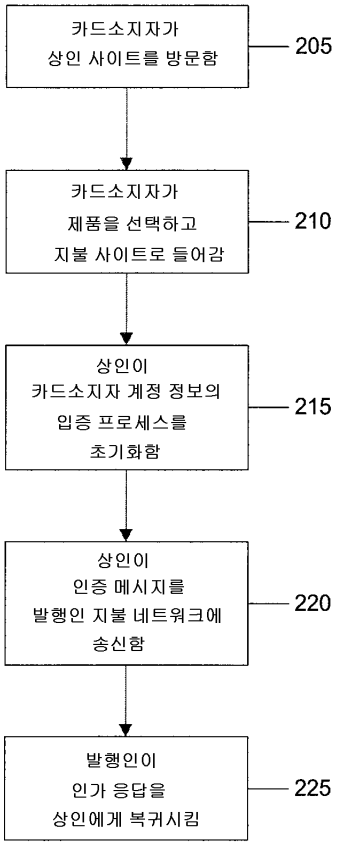
<21> 도 4는 양호한 실시예에 따라 MOTO 트랜잭션을 인증하는 예시용 프로세스의 흐름도.

도면

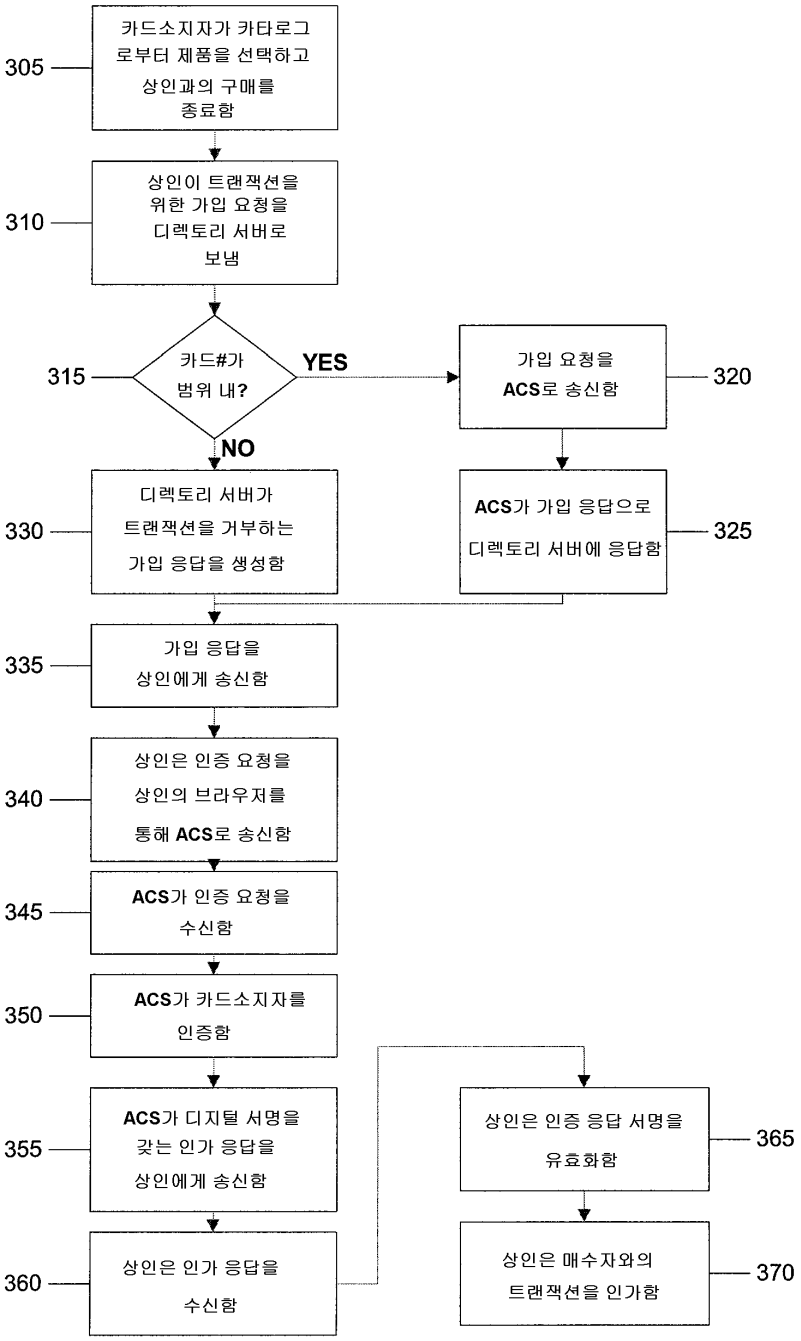
도면1



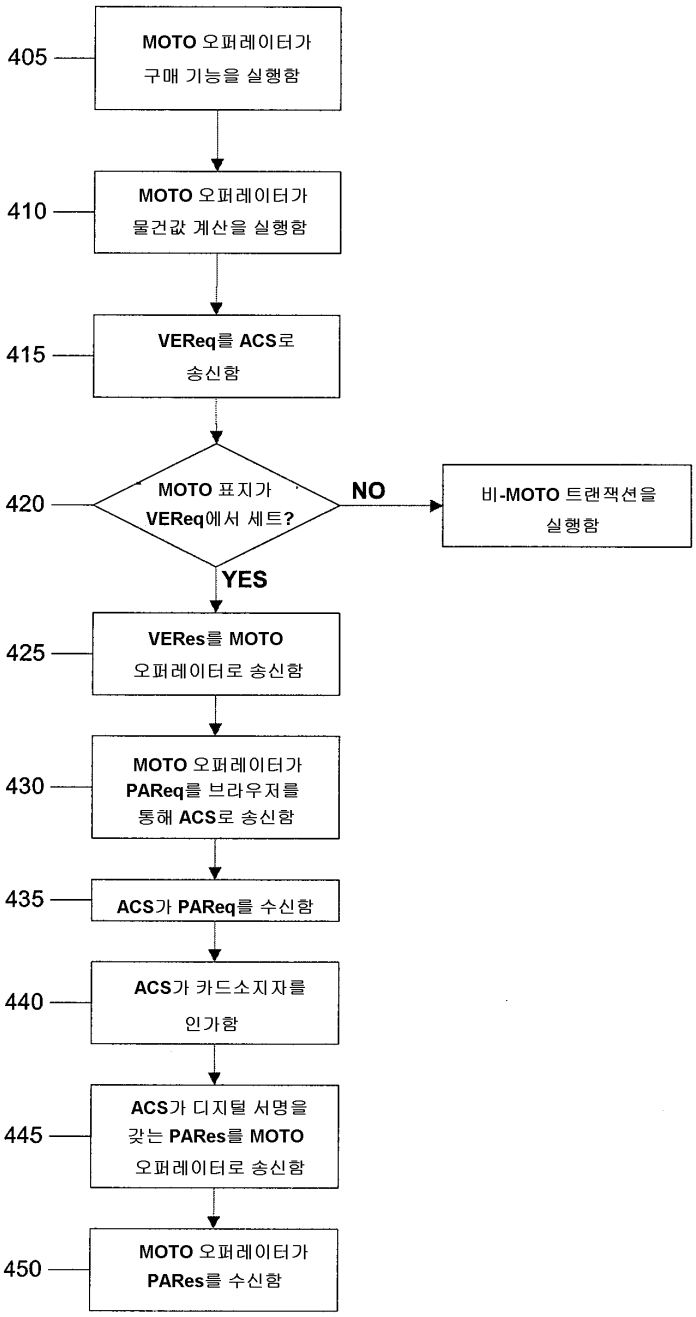
도면2


카드소지자가
상인 사이트를 방문함
205
카드소지자가
제품을 선택하고
지불 사이트로 들어감
210
상인이
카드소지자 계정 정보의
입증 프로세스를
초기화함
215
상인이
인증 메시지를
발행인 지불 네트워크에
송신함
220
발행인이
인가 응답을
상인에게 복귀시킴
225

도면3


305
카드소지자가 카타로그로부터 제품을 선택하고 상인과의 구매를 종료함
310
상인이 트랜잭션을 위한 가입 요청을 디렉토리 서버로 보냄
315
카드#가 범위 내?
YES
NO
320
가입 요청을 ACS로 송신함
325
ACS가 가입 응답으로 디렉토리 서버에 응답함
330
디렉토리 서버가 트랜잭션을 거부하는 가입 응답을 생성함
335
가입 응답을 상인에게 송신함
340
상인은 인증 요청을 상인의 브라우저를 통해 ACS로 송신함
345
ACS가 인증 요청을 수신함
350
ACS가 카드소지자를 인증함
355
ACS가 디지털 서명을 갖는 인가 응답을 상인에게 송신함
360
상인은 인가 응답을 수신함
365
상인은 인증 응답 서명을 유효화함
370
상인은 매수자와의 트랜잭션을 인가함

도면4


405
MOTO 오퍼레이터가 구매 기능을 실행함
410
MOTO 오퍼레이터가 물건값 계산을 실행함
415
VEReq를 ACS로 송신함
420
MOTO 표지가 VEReq에서 세트?
NO
비-MOTO 트랜잭션을 실행함
YES
425
VERes를 MOTO 오퍼레이터로 송신함
430
MOTO 오퍼레이터가 PAReq를 브라우저를 통해 ACS로 송신함
435
ACS가 PAReq를 수신함
440
ACS가 카드소지자를 인가함
445
ACS가 디지털 서명을 갖는 PARes를 MOTO 오퍼레이터로 송신함
450
MOTO 오퍼레이터가 PARes를 수신함