



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0045400
(43) 공개일자 2009년05월07일

(51) Int. Cl.

G06Q 30/00 (2006.01)

(21) 출원번호 10-2009-7006253

(22) 출원일자 2009년03월26일

심사청구일자 없음

번역문제출일자 2009년03월26일

(86) 국제출원번호 PCT/US2007/077158

국제출원일자 2007년08월29일

(87) 국제공개번호 WO 2008/027998

국제공개일자 2008년03월06일

(30) 우선권주장

60/823,803 2006년08월29일 미국(US)

(71) 출원인

비자 인터내셔널 서비스 어쏘시에이션

미합중국 94404 캘리포니아주 포스터시티 메트로
센터 보우리바드 900

(72) 발명자

도민구예즈, 베네딕토

미합중국, 캘리포니아 94066, 샌 브루노, 메리온
드라이브 2830

(74) 대리인

이만재

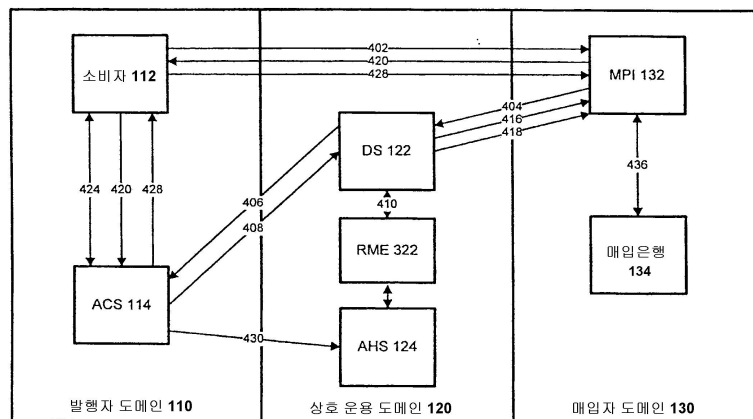
전체 청구항 수 : 총 8 항

(54) 전자 상거래 처리를 위한 방법과 그에 따른 시스템

(57) 요약

상거래 카드를 이용한 부당한 전자 상거래를 이행하는 소비자의 위험을 최소화 하기 위한 방법이 여기에 기술된다. 본 방법은 상인의 웹사이트로부터 상거래를 위한 등록 확인 요청을 수신하고 접근 제어 서버에게 등록 확인 요청을 전송하는 단계; 접근 제어 서버로부터 등록 확인 응답을 수신하고 등록 확인 요청의 최소한 일부에 근거하여 특정 상거래가 위험한지를 결정해 만약 상거래가 위험하지 않다면 상인의 웹사이트로 등록 확인 요청을 전송하고 만약 상거래가 위험하다면 상거래가 위험한 것을 표시하기 위해 등록 확인 요청을 변경하고 변경된 등록 확인 응답을 상인의 웹사이트에 전송하는 단계를 포함한다.

대표도 - 도3



특허청구의 범위

청구항 1

상거래 카드를 이용한 부정한 인터넷 구매 상거래를 이행하는 소비자의 위험을 최소화하는 방법에 있어서,
 상인의 웹사이트로부터 상거래의 등록 확인 요청을 수신하는 단계;
 접근 제어 서버로 상기 등록 확인 요청을 전송하는 단계;
 상기 접근 제어 서버로부터 등록 확인 응답을 수신하는 단계;
 상기 등록 확인 요청의 적어도 일부에 기초하여 상기 상거래가 위험한지의 여부를 결정하는 단계;
 만약 상기 상거래가 위험하지 않은 경우, 상기 상인의 웹사이트로 상기 등록 확인 요청을 전송하는 단계; 및
 만약 상기 상거래가 위험한 경우, 상기 상거래가 위험하다는 점을 표시하기 위해 상기 등록 확인 요청을 변경하는 단계 및 상기 상인의 웹사이트로 상기 변경된 등록 확인 요청을 전송하는 단계를 포함하는 것을 특징으로 하는 상거래 카드를 이용한 부정한 인터넷 구매 상거래를 이행하는 소비자의 위험을 최소화하는 방법.

청구항 2

청구항 1에 있어서,
 상기 등록 확인 요청이 계정 번호를 포함하는 것을 특징으로 하는 상거래 카드를 이용한 부정한 인터넷 구매 상거래를 이행하는 소비자의 위험을 최소화하는 방법.

청구항 3

청구항 2에 있어서,
 상기 등록 확인 응답이 카드 소지자의 인증이 상기 계정 번호에 대해 유효한지의 여부를 나타내는 것을 특징으로 하는 상거래 카드를 이용한 부정한 인터넷 구매 상거래를 이행하는 소비자의 위험을 최소화하는 방법.

청구항 4

청구항 1에 있어서,
 상기 상거래가 위험한지의 여부를 결정하는 단계는,
 상기 계정 번호가 이전에 동일한 상인에게서 동일한 금액으로 사용된 적이 있는 지를 확인하는 단계;
 상기 계정 번호의 금액 제한이 초과한지의 여부를 결정하는 단계; 및
 상기 소비자 컴퓨터의 IP 주소에 상응하는 지리적 위치를 대조하는 단계 중 적어도 하나를 포함하는 것을 특징으로 하는 상거래 카드를 이용한 부정한 인터넷 구매 상거래를 이행하는 소비자의 위험을 최소화하는 방법.

청구항 5

청구항 1에 있어서,
 상기 상거래가 위험한 경우, 발행자에게 상기 상거래가 위험하다는 경고를 하기 위해 상기 상거래 카드 발행자에게 경고를 전송하는 단계를 더 포함하는 것을 특징으로 하는 상거래 카드를 이용한 부정한 인터넷 구매 상거래를 이행하는 소비자의 위험을 최소화하는 방법.

청구항 6

청구항 2에 있어서,
 상기 등록 확인 요청이 상기 소비자에 의해 구매된 하나 이상의 품목, 상기 상거래의 총 비용, 상기 상인의 신분 및 상기 소비자의 인터넷 브라우저에 포함된 정보를 더 포함하는 것을 특징으로 하는 상거래 카드를 이용한 부정한 인터넷 구매 상거래를 이행하는 소비자의 위험을 최소화하는 방법.

청구항 7

상거래 카드를 이용한 부정한 인터넷 구매 상거래를 이행하는 소비자의 위험을 최소화하는 하는 방법에 있어서,

상거래 요청을 수신하는 단계로서, 상기 상거래 요청이 상기 상거래에 속한 정보를 포함하고 상기 상거래 요청은 소비자의 계정에 속하는 상거래 요청을 수신하는 단계;

부정한 상거래가 될 수 있는 위험에 있는지의 여부를 결정하기 위해 기록 데이터베이스 내에 포함된 정보와 상기 상거래 요청 정보를 대조하는 단계;

만약 상기 대조가 상기 상거래가 위험하다고 결정한 경우, 상기 상거래가 위험하다는 것을 알리는 상기 상거래 요청에 대한 응답을 전송하는 단계에 대한 상기 응답이 상기 상거래가 위험하다고 알리는 단계; 및

상기 상거래 요청 정보로 상기 기록 데이터베이스 내에 포함된 정보를 갱신하는 단계를 포함하는 것을 특징으로 하는 상거래 카드를 이용한 부정한 인터넷 구매 상거래를 이행하는 소비자의 위험을 최소화하는 방법.

청구항 8

청구항 7에 있어서,

상기 상거래 요청이 상기 소비자에 의해 구매된 하나 이상의 품목, 상기 상거래의 총 비용, 상기 상인의 신분 및 상기 소비자의 인터넷 브라우저에 속한 정보를 포함하는 것을 특징으로 하는 상거래 카드를 이용한 부정한 인터넷 구매 상거래를 이행하는 소비자의 위험을 최소화하는 방법.

명세서

기술분야

- <1> 본 발명은 대체로 전자 상거래 처리를 위한 방법과 그에 따른 시스템에 관한 것이며 특히 CNP 상거래와 관련된 부정한 행동을 조속히 보고하는 방법과 시스템에 관한 것이다.

배경기술

- <2> 신용 카드, 직불 카드, 비용 가치 카드, 은행 카드, 고객 우대 카드, 스마트 카드 등의 상거래 카드를 이용한 상거래 동안, 권한이 없는 사용과 같은 다양한 문제를 피하기 위해 계정에 대한 카드 소지자의 소유권을 확인하는 것이 중요하다. 카드 소지자의 인증은 계정이 카드 소지자에 의해 소유된다는 것을 확인하기 위한 과정이다. 예를 들어, 판매 대리인이 상거래 카드의 서명과 영수증 상의 카드 소지자 서명이 일치하는지 확인할 때 "카드 제시" 거래 동안 카드 소지자의 인증이 실행된다.
- <3> 기술적 향상은 사업체와 개인이 다수의 환경 내에서 상거래를 시작할 수 있도록 허용한다. 예를 들어, 카드 소지자는 종래의 "직접" 상거래, 인터넷을 통한 상거래, 전화를 통한 상거래 및 우편 시스템을 통한 상거래를 할 수 있다. 대다수의 경우에, 카드 소지자는 서비스 제공자를 직접 방문하지 않고도 상거래를 이행하는 편리성을 바란다. 그러므로 카드 소지자는 교통 시간을 소비할 필요가 없으며 자신의 집에서의 개인적 자유 내에서 상거래를 이행함에 의해 소매 상가에서 쇼핑을 하거나 은행 앞에서 줄을 서는 등과 같은 혼란을 감소시킬 수 있다.
- <4> 카드 소지자에게 제공되는 이러한 편리성과 상인에게 주어지는 가외 매출로 인해 "카드 불제시"("Card not present", "CNP) 상거래 양은 최소한 일부적으로 증가하고 있다. 하지만 이러한 CNP 상거래 양이 증가할수록 부정 상거래와 이러한 상거래로 인한 금전적 손실 또한 증대하고 있다.
- <5> 도 1은 선행 기술에 따른 규정된 상거래 처리 시스템의 체계적 도식을 도시한다. 도 1에서 도시된 바와 같이, 상거래 처리 시스템은 논리적으로 발행자 도메인(110), 상호 운용 도메인(120) 및 매입자 도메인(130)으로 나누어진다. 발행자 도메인(110)은 소비자(112)와 접근 제어 서버(114)("ACS")를 포함한다. 상호 운용 도메인(120)은 디렉토리 서버(122)("DS")와 인증 기록 서버(124)("AHS")를 포함한다. 매입자 도메인(130)은 상인 구매 인터페이스(132)("MPI")와 매입 은행(134)을 포함한다. 선들은 연결된 실체 간에 이행된 데이터 전송을 나타낸다. 이러한 데이터 전송은 도 2에 참고하여 더 자세히 기술된다.
- <6> 도 2는 선행 기술에 따른 규정된 CNP 상거래를 도시한다. 도 2에서 도시된 바와 같이, 소비자는 장바구니에 품목을 담고 상거래를 기록완료(finalizes)한다(205). MPI(132)는 등록 확인 요청을 DS(122)로 전송해 소비자(112)의 등록을 확인하게 한다(210). 만약 소비자의 카드 번호가 인증에 관여하는 카드 범위 내에 있을 경우, DS(122)는 요청을 ACS(114)로 보낸다(215). ACS(114)는 특정 카드 번호의 인증이 유효한지를 표시하는 등록 확인 응답과 함께 DS(122)에 응답한다(220). DS(122)는 등록 확인 응답을 MPI(132)에게 보낸다(225). 만약 소비

자의 카드 번호가 관여하는 카드 범위 내에 존재하지 않을 경우, DS(122)는 응답(230)을 생성하고 MPI(132)로 전송한다.

- <7> 만약 카드 인증이 유효한 경우, MPI(132)는 소비자의 인터넷 브라우저(112)를 통해 지불인 인증 요청(235)을 ACS(114)로 보낸다. ACS(114)는 지불인 인증 요청(240)을 수신하고 소비자(112)의 카드 번호가 적합한 것으로 인증한다(245). 예를 들어, 소비자(112)는 비밀번호, 칩 암호, 개인 신분 확인 번호 또는 이와 같은 것을 이용해 인증될 수 있다. ACS(114)는 지불인 인증 요청에 대한 응답을 포맷하고 선택적으로 디지털 방식으로 서명한다(250). ACS(114)는 그 다음 소비자의 인터넷 브라우저를 통해 응답을 MPI(132)에게 전송한다(255). 게다가, ACS(114)는 응답의 사본(지불인 인증 상거래 요청 형식으로)을 AHS(124)에게 전송할 수 있다(260).
- <8> MPI(132)는 그 다음 지불인 인증 응답을 수신하고(265) 만약 응답 서명이 ACS(114)에 의해 서명된 경우 응답 서명을 유효하게 한다(270). MPI(132)는 인증 교환(275)을 이것의 매입자(134)와 함께 시작한다.
- <9> 부정을 제기하는 데 있어 한 가지의 문제점은 특정한 소비자의 계정 번호에 부정이 발생한다는 사실을 상인과 발행자에게 어떻게 빨리 제공할 수 있는지를 결정하는 것이다. 부정이 발생한다는 알림이 없다면 사기꾼은 계정 번호를 이용해 계속적으로 부정한 상거래를 제출할 수 있다.
- <10> 수상한 행동을 위한 조속한 경고 감지를 제공하는 방법과 시스템이 요구된다.
- <11> CNP 상거래와 관련된 수상한 행동을 보고하는 방법과 시스템이 요구된다.
- <12> CNP 상거래 처리 시스템 또는 인증 논리를 활동적으로 관리하지 않는 발행자에게 경고를 제공하기 위한 방법과 시스템이 더 요구된다.
- <13> 본 발명의 기술은 상기 나열된 하나 또는 그 이상의 문제점들을 해결하는데 그 목적이 있다.

발명의 상세한 설명

- <14> 본 발명의 방법을 설명하기 전에, 본 발명이 설명된 특정한 방법론, 시스템 및 재료로, 그것들이 변화해도, 제한되지 않는 것으로 이해된다. 또한, 본 설명에서 사용된 용어가 특정한 버전 또는 실시예만을 설명할 목적이 아니고 첨부된 청구항만에 의해 제한되는 본 발명의 범위를 제한하지 않는다.
- <15> 여기 및 청구된 청구항에 사용된 바와 같이, 단일 형태 "a", "an" 및 "the"는 그 문맥이 다르게 명백히 표시하지 않는 한 복수의 레퍼런스를 포함한다. 그러므로, 예를 들어, "상거래"에 대한 레퍼런스는 하나 이상의 상거래 및 당업자가 알고 있는 등가물에 대한 레퍼런스이다. 다르게 표현되게 언급하지 않으면, 본원에서 사용된 모든 정의되지 않은 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 동등한 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 하여되지 않는다.
- <16> 하나의 실시예에서, 부정한 인터넷 구매 상거래의 위험을 최소화하기 위한 방법은 상인의 웹사이트로부터 등록 확인 요청을 수신하는 단계, 접근 제어 서버에 등록 확인 요청을 전송하는 단계, 접근 제어 서버로부터 등록 확인 응답을 수신하는 단계, 등록 확인 요청의 최소한의 일부에 근거하여 상거래가 위험한지를 결정하는 단계, 만약 상거래가 위험하지 않은 경우 상인의 웹사이트에 등록 확인 요청을 전송하는 단계 및 만약 상거래가 위험한 경우 이를 표시하기 위해 등록 확인 응답을 변경하고 변경된 등록 확인 응답을 상인의 웹사이트에 전송하는 단계를 포함한다.
- <17> 하나의 실시예에서, 부정한 인터넷 구매 상거래의 위험을 최소화하기 위한 방법은 사용자 계정에 속한 상거래 요청을 수신하는 것과 계정에 속한 정보를 담는 단계, 기록 데이터 베이스 내에 포함된 정보와 상거래 요청 정보를 비교하여 계정이 부정한 행위에 처할 위험에 있는지를 결정하는 단계, 만약 대조 후 상거래가 위험하다면 이를 표시하도록 상거래 요청에 대한 응답을 변경하는 단계 및 상거래 요청 정보로 기록 데이터 베이스 내에 포함된 정보를 갱신하는 단계를 포함한다.

실시예

- <24> 도 3은 실시예에 따른 전형적인 상거래 처리 시스템의 체계적 도식을 도시한다. 도 3은 도 1의 선행 기술적 상거래 처리 시스템과 위험 관리 엔진(risk management engine, "RME")(322)의 도입으로 인해 달라진다.

RME(322)는 상거래가 위험한지의 여부를 결정할 때 사용된다. RME(322)는 상거래에 사용된 카드 번호, 구매된 하나 또는 그 이상의 아이템, 품목이 구매되는 상인, 상거래의 총 비용, 소비자의 인터넷 브라우저에 속한 정보(예로 IP 주소) 및 이와 같은 상거래 정보를 수신한다. 상거래 정보에 기초하여, RME(322)는 상거래가 위험한지의 여부(즉, 잠재적으로 부정함)를 결정하기 위해 하나 또는 그 이상의 위험 처리 기준을 사용한다. 전형적인 위험 처리 기준은 제한 없이 소비자의 계정 번호가 동일한 상인에게서 같은 금액으로 이전에 사용된 여부("속도 확인"), 소비자 계정 번호의 금액 제한이 초과된 여부("제한 확인") 및 소비자 컴퓨터의 IP 주소 확인("지리적 위치 확인")을 포함한다. RME(322)는 상거래가 위험한지의 여부를 결정하는 것을 지원하기 위해 AHS(124)에 저장된 상거래 데이터를 사용한다. 하나의 실시예에서, RME(322)는 어떤 상거래가 처리되는지에 따라 지역, 나라, 멤버 또는 그와 같은 다른 기준을 사용한다. 만약 상거래 또는 계정이 위험하다고 판단되면 RME(322)는 발행자 또는 상인의 시스템에 잠재적 위험을 경고하기 위한 경고를 전송한다. 하나의 실시예에서, 상거래는 완료하도록 허용될 수 있지만 하나 또는 그 이상의 기준에 충족하는 그 이후의 상거래는 거절된다.

<25> 도 4는 실시예에 따른 전형적인 상거래 흐름의 순서도를 도시한다. 도 4에서 도시된 바와 같이, 소비자는 MPI(132)를 통해 하나 또는 그 이상의 품목을 선택하며 구매될 품목을 기록완료한다(402). MPI(132)는 소비자의 등록을 확인하기 위해 등록 확인 요청("VEReq")을 DS(122)로 전송한다(404). 만약 소비자의 카드 번호가 인증에 관여하는 카드 범위 내에 있을 경우, DS(122)는 VEReq를 적합한 ACS에 전송한다(406). ACS(114)는 카드 번호의 인증이 유효한지를 표시하는 DS(122)에 등록 확인 응답("VERes")을 제공한다(408). DS(122)는 상거래가 위험한지의 여부를 결정하기 위해 RME(322)를 실시한다. 만약 RME(322)가 상거래가 위험하지 않다고 결정한 경우, DS(122)는 ACS(114)에 의해 제공된 VERes를 MPI(132)로 전송한다(312). 만약 RME(322)가 상거래가 위험하다고 결정한 경우, ACS(114)에 의해 제공된(408) VERes는 상거래가 위험하거나 권한이 없다는 것을 표시하기 위해 변경된다(414). 하나의 실시예에서, 현재의 상거래는 위험 여부와 상관없이 변경되지 않은(414) 상태로 완료되도록 허용된다. 이러한 실시예에서, 만약 상거래가 위험하거나 권한이 없다고 결정된 경우, 예를 들어 동일한 계정 번호를 갖는 그 이후의 상거래는 위험 또는 권한이 없는 상거래라고 표시되도록 변경된다(414). 변경된 VERes는 그 후 MPI(132)로 전송된다(416). 만약 소비자의 카드 번호가 관여하는 카드 범위 내에 존재하지 않을 경우, DS(122)는 VERes를 생성하고 MPI(132)로 전송한다(418).

<26> 만약 소비자 카드의 인증이 유효하면, MPI(132)는 소비자의 인터넷 브라우저(112)를 통해 ACS(114)로 지불인 인증 요청("PAREq")를 전송한다(420). ACS(114)는 PAREq를 수신(422)하며 카드 번호에 기초한 적합한 방식으로 소비자(112)를 인증한다(424). 예를 들어, 소비자(112)는 비밀번호, 칩 암호, 개인 신분 확인 번호 또는 이와 유사한 것들을 이용해 인증된다(424). ACS(114)는 PAREq에게 지불인 인증 응답("PAREs")을 포맷하고 디지털 방식으로 서명한다(426). ACS(114)는 그 다음 소비자의 인터넷 브라우저를 통해 MPI(132)로 PAREs를 전송한다(428). 덧붙여, ACS(114)는 지불인 인증 상거래 요청("PATransReq")을 AHS(124)로 전송한다(430). AHS(124)는 이전에 이행되었던 상거래에 포함된 정보의 저장소이다. PATransReq는 제한 없이 예를 들어 상인명, 상거래 확인자, 구매된 상품 및 서비스, 구매 금액, 구매 유통액, 구매 날짜, 구매 시간 및 이와 같은 것을 포함한다. MPI(132)는 PAREs를 수신하고(432) PAREs 서명을 유효하게 한다(434). MPI(132)는 그 다음 매입자(134)와 함께 인증 교환을 시작한다(436).

<27> 도 5는 하나의 실시예에 따른 전형적인 상거래 처리 시스템의 대체적인 체계적 도식을 도시한다. 도 5는 경고가 제공되는 방식에 있어서 도 3의 방식과 다르다. 따라서, 상거래 처리 동안 다른 실체(entities)는 서로 교통(communicate)한다.

<28> 도 6은 하나의 실시예에 따른 전형적인 상거래 흐름의 대체적인 순서도를 도시한다. 도 6에서 도시된 바와 같이, 소비자는 MPI(132)를 통해 하나 또는 그 이상의 품목을 구매하고 구매한 품목을 기록완료(602)한다. MPI(132)는 소비자의 등록을 확인하기 위해 VEReq를 DS(122)로 전송한다(604). 만약 소비자의 카드 번호가 관여하는 카드 범위 내에 있을 경우, DS(122)는 VEReq를 적합한 ACS로 전송한다. ACS(114)는 카드 번호의 인증이 유효한지의 여부를 나타내는 DS(122)로 VERes를 제공한다(608). DS(122)는 MPI(132)로 VERes를 전송한다(610). 만약 소비자의 카드 번호가 관여하는 카드 범위 내에 존재하지 않을 경우, DS(122)는 VERes를 생성하고 MPI(132)에게 전송한다(612).

<29> 만약 소비자의 카드의 인증이 유효한 경우, MPI(132)는 소비자의 인터넷 브라우저(112)를 통해 ACS(114)로 PAREq를 전송한다. ACS(114)는 PAREq를 수신한다(616). DS(122)는 상거래가 위험한 계정에서 온 건지의 여부를 결정하기 위해 RME(322)를 실시한다. 만약 RME(322)가 계정이 위험하다고 판단한 경우, RME는 그 계정의 MPI 거절 지불인 인증에 ACS(114)가 응답하도록(622) 지시하는 데이터를 전송한다(620). 다른 방법으로는, ACS(114)가 카드 번호에 기초한 적절한 방식으로 소비자를 인증한다(624). 예를 들어, 소비자는 비밀번호, 칩 암호, 개인

신분 확인 번호 또는 이와 유사한 것으로 인증될 수 있다. ACS(114)는 PAREq로 PAREs를 포맷하고 디지털 방식으로 서명한다(626). ACS(114)는 그 다음 소비자의 인터넷 브라우저를 통해 MPI(132)로 PAREs를 전송한다(628). 덧붙여, ACS(114)는 AHS(124)로 PATransReq를 전송한다(630). PATransReq는 제한 없이 예를 들어 상인명, 상거래 확인자, 상품 또는 서비스의 상세 사항, 구매 금액, 구매 유통액, 구매 일자, 구매 시간 및 이와 같은 것을 포함한다. MPI(132)는 PAREs를 수신하고(132) PAREs 서명을 유효하게 한다(634). 상인(132)는 매입자(134)와 함께 인증 교환을 시작한다(636).

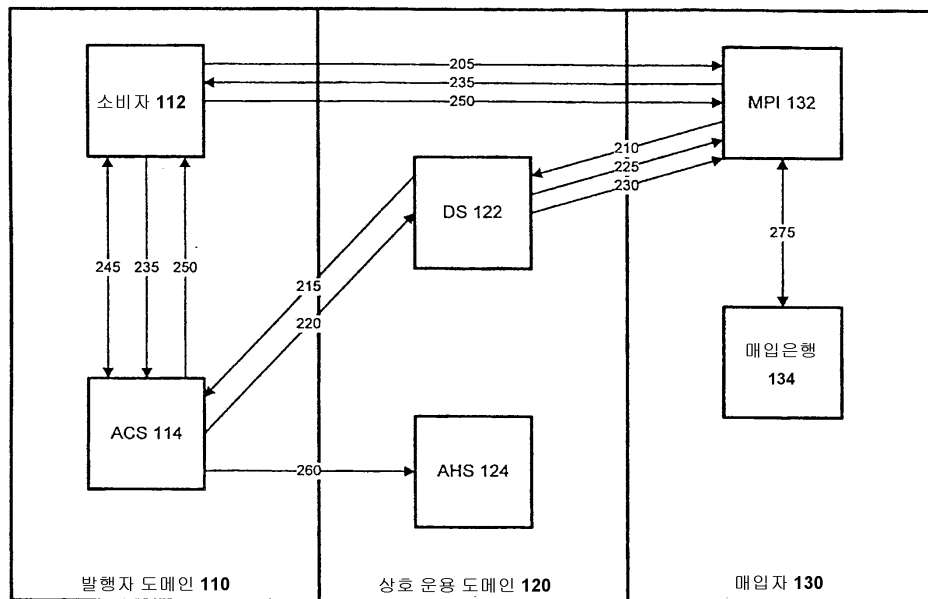
<30> 상기 개시되고 다른 특성 및 기능, 또는 그 대안예가 다수의 다른 시스템 또는 애플리케이션에 바람직하게 결합됨을 알 수 있다. 또한, 본원에서 여럿의 예견되지 않거나 예상되지 않는 대안예, 변형예, 변화 또는 개선점이 본 기술에 숙련된 자에 의해 계속해서 이루어질 수 있음을 알 수 있다.

도면의 간단한 설명

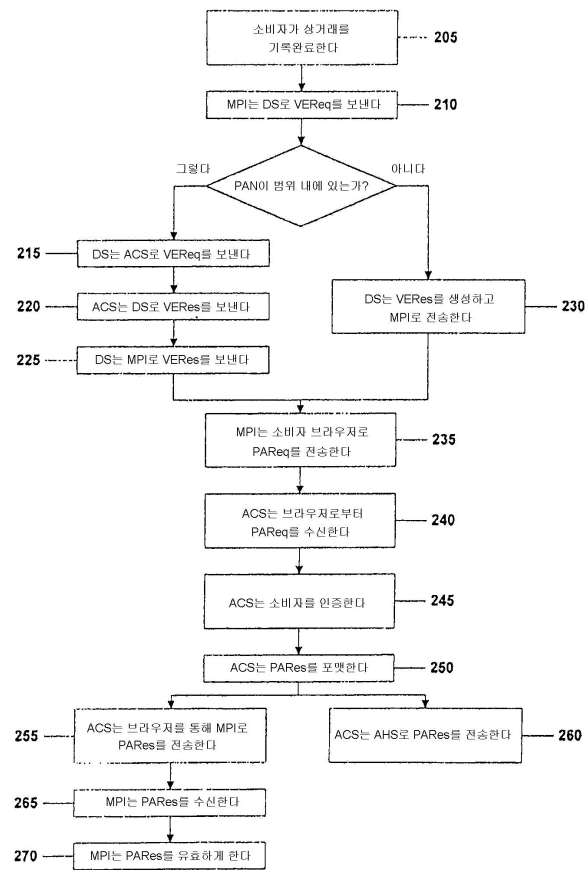
- <18> 도 1은 선행 기술에 따른 규정된 상거래 처리 시스템의 체계적 도식을 도시하는 도면;
- <19> 도 2는 선행 기술에 따른 규정된 CNP 상거래 흐름의 순서도를 도시하면 도면;
- <20> 도 3은 실시예에 따른 전형적인 상거래 처리 시스템의 체계적 도식을 도시하는 도면;
- <21> 도 4는 실시예에 따른 전형적인 상거래 처리 흐름의 순서도를 도시하는 도면;
- <22> 도 5는 실시예에 따른 전형적 상거래 처리 시스템의 대체적인 체계적 도식을 도시하는 도면; 및
- <23> 도 6은 실시예에 따른 전형적 상거래 흐름의 대체적인 순서도를 도시하는 도면이다.

도면

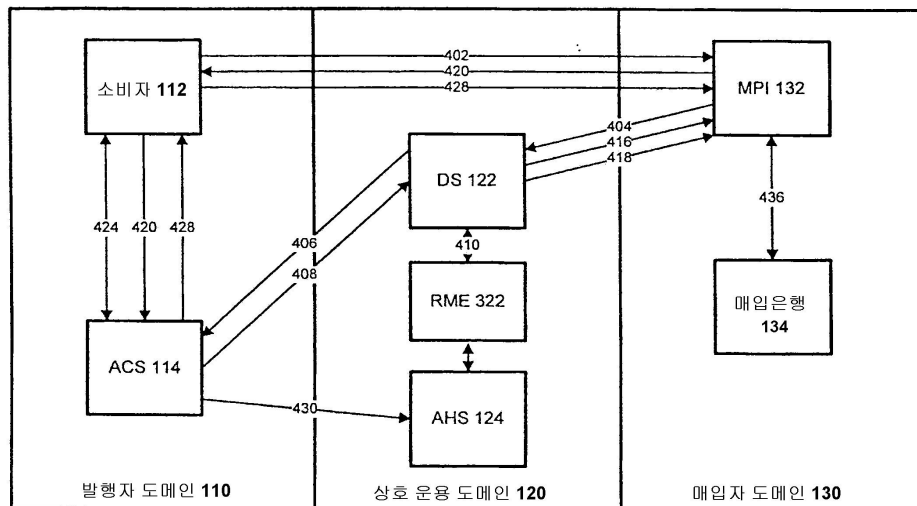
도면1



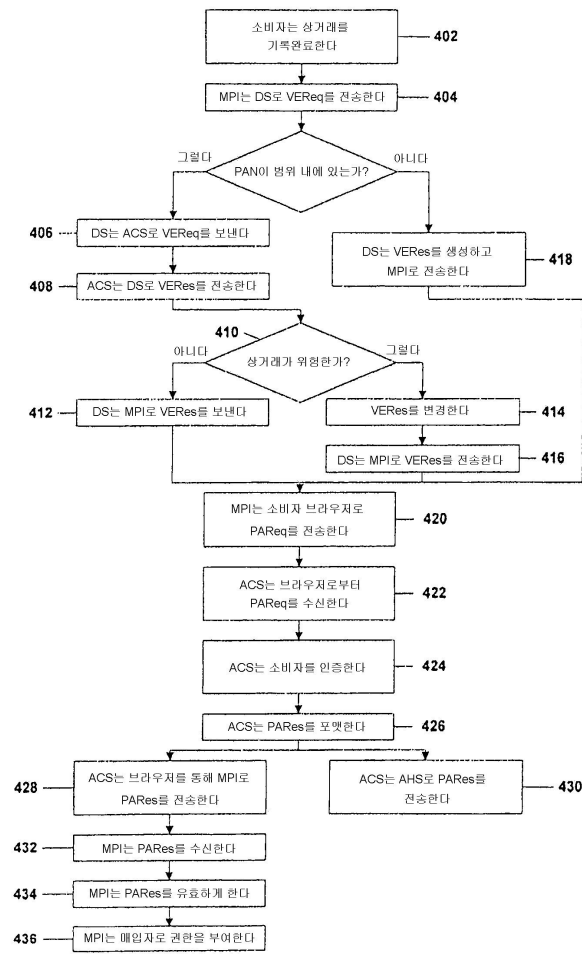
도면2



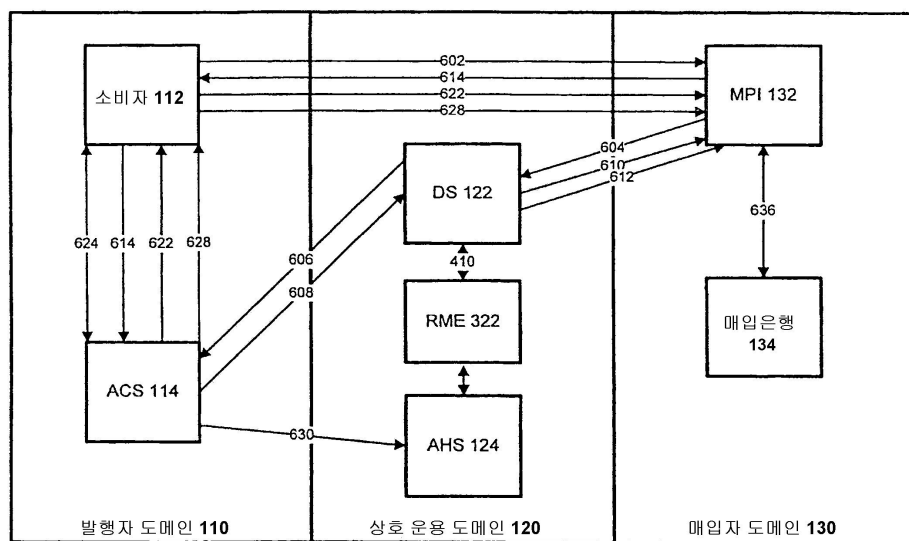
도면3



도면4



도면5



도면6

