(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0141718
(43) 공개일자 2013년12월26일

(51) 국제특허분류(Int. Cl.)
G06Q 20/40 (2012.01)
(21) 출원번호 10-2013-7031931(분할)
(22) 출원일자(국제) 2004년05월11일
심사청구일자 없음
(62) 원출원 특허 10-2012-7024455
원출원일자(국제) 2004년05월11일
심사청구일자 2012년09월19일
(85) 번역문제출일자 2013년12월02일
(86) 국제출원번호 PCT/US2004/014587
(87) 국제공개번호 WO 2005/111957
국제공개일자 2005년11월24일
(30) 우선권주장
10/838,719 2004년05월03일 미국(US)

(71) 출원인
비자 인터내셔날 써비스 어쏘시에이션
미합중국 94404 캘리포니아주 포스터시티 메트로 센터 보우리바드 900
(72) 발명자
거버, 개리 이.
미국, 캘리포니아 94404, 포스터 시티, 세인트 키츠 레인 1401
리, 티모시 미-츄
미국, 캘리포니아 94118, 샌 프란시스코, 아파트 3, 블레이크스트릿 146
(74) 대리인
강명구

전체 청구항 수 : 총 1 항

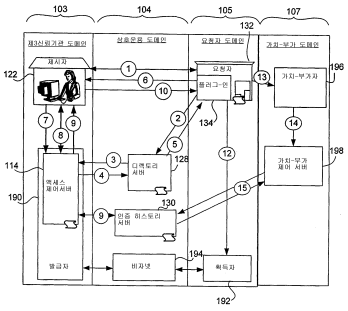
(54) 발명의 명칭 **온라인 인증 서비스 방법**

(57) 요 약

본 발명의 계좌 인증 서비스에서는, 온라인 거래 중 요청자를 위해 계좌 소지자의 신원을 제 3 신뢰 기관이 확인할 수 있다. 온라인 거래 중 계좌 소지자의 신원을 인증하는 과정은, 계좌 소지자로부터 비밀번호를 요청하는 단계, 비밀번호를 확인하는 단계, 그리고 계좌 소지자의 인증이 확인되었는 지 여부를 요청자에게 통지하는 단계로 구성된다. 계좌 인증 서비스의 대안의 실시예는, 고객에 관한 정보가 가치-부가자와 공유되는 가치-부가 구성요소를 포함한다. 고객 정보가 계좌 인증 프로세스의 각 관련자에 의해 수집되기 때문에 해당 고객에 대한 고객 정보가 풍부한 편이다. 가치-부가자는 이 정보를 다양한 방식으로 이용할 수 있다. 모든 관련자들은 고객 정보의 공유로부터 이익을 얻을 수 있다.

예를 들어 가치-부가자는 판매자, 배송자, 보안 조직, 또는 정부 기관일 수 있다. 거래 식별자는 고객과 판매자 간의 특정 거래와, 고객 정보를 식별한다.

대 표 도 - 도8



계좌 인증 시스템을 이용한 가치-부가자와의 거래

특허청구의 범위

청구항 1

온라인 거래 중 제시자의 신원을 인증하기 위해 상기 요청자로부터의 온라인 인증 요청 메시지를 액세스 제어 컴퓨터에 위치하는 제 3 신뢰 기관이 수신하는 단계,

상기 제시자의 컴퓨팅 장치로부터 신원-인증 토큰 그리고 수집된 제시자 정보를 상기 온라인 거래 중 액세스 제어 컴퓨터에 위치하는 상기 제 3 신뢰 기관이 수신하는 단계,

상기 액세스 제어 컴퓨터가 상기 온라인 거래 중 상기 신원-인증 토큰을 상기 제시자에 대해 미리 지정된 토큰과 비교하는 단계,

상기 신원-인증 토큰이 상기 제시자에 대해 미리 지정된 토큰과 일치할 때 상기 제시자가 인증되었음을 상기 요청자에게 통지하는 온라인 인증 응답 메시지를 상기 온라인 거래 중 상기 제 3 신뢰 기관의 상기 액세스 제어 컴퓨터로부터 상기 요청자에게로 전송하는 단계를 포함하는 것을 특징으로 하는 온라인 거래 중 제시자 정보를 제공하는 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 온라인 거래 중 계좌 소지자의 신원을 인증하는 기술에 관한 발명으로서, 특히, 가치-부가자(value-adding party)와의 인증 프로세스에 관련된 정보를 공유 및 이용하는 기술에 관한 발명이다.

배 경 기 술

[0002] 지불 카드(가령, 신용카드, 데빗 카드, 등등)를 이용한 지불 거래 중, 승인되지 않은 이용과 같은 다양한 문제점들을 방지하기 위해 계좌에 대한 카드소지자의 소유권을 확인하는 것이 중요하다. 지불인 인증은 계좌에 대한 카드소지자의 소유권을 확인하는 프로세스이다. 계좌에 대한 카드소지자의 소유권을 인증하기 위한 가장 일반적인 방법은 "카드 제시" 거래 중 판매 위치에서 통상적인 방식으로 발생한다. 카드 제시 거래는 카드소지자의 카드를 판매자가 받아, 지불 카드 단말기에 카드를 그어서, 계좌 상태와 신용 라인 가용성을 확인한 후, 카드 후면의 서명이 구매자의 서명과 일치하는 지를 확인하는 과정들로 이루어진다. 판매자가 이러한 종류의 거래에 대한 세부적 가이드라인을 따를 경우, 판매자는 승인받은 요금에 대한 지불을 적은 할인액 및 수수료로 보장받을 수 있다. 비자 인터내셔널 서비스 어소시에이션같은 서비스 제공자는 이러한 구체적 가이드라인을 제공할 수 있다.

[0003] 온라인이나 메일, 전화 등을 통해 이루어지는 "카드 비-제시" 거래는 판매자에게 보장되지 않는 지불 과정을 포함한다. 이러한 비-대면 거래에서 지불인이 인증되지 않기 때문에 어떤 보장도 제공되지 않는다. 따라서, "카드 비-제시" 거래에 여러가지 위험이 나타날 수 있다. 이러한 위험은 온라인 판매자에 대한 지불 거래의 환불, 판매자 및 카드소지자에 대한 사기 행위, 은행의 예외 항목 처리 비용 증가, 온라인을 통한 상품 및 서비스 구매의 안전성 결여에 대한 인식 증가, 등등과 같은 문제점들을 포함한다. 이러한 위험의 구체적인 예로는, 상품 및 서비스를 온라인을 통해 구매할 때 도난 계좌 정보를 승인없이 이용하는 행위, 카드 계좌 번호를 변조하여 부정 온라인 거래를 행하는 행위, 그리고 네트워크 트래픽으로부터 클리어 텍스트 계좌 정보를 추출하는 행위 등이 있다.

[0004] 전자 상거래가 계속적으로 성장하고 있는 상황에서, 지불인을 인증하는 방법을 제공하는 것은 중요하다. 온라인 거래 종류들의 범위가 주어졌을 때, 거래에 대한 상업적 양태에 관계없이 당사자들의 신원을 인증하는 방법을 제공하는 것이 또한 중요하다. 이는 카드소지자, 판매자, 금융회사 등으로부터 정부 기관까지 모든 거래 참가자들에게 유익한 도움이 될 것이다. 온라인 거래 중 고객을 인증하는 것은, 부정행위, 분쟁, 보상, 환불 등의 경우를 감소시킬 것이고, 이에 따라 각각의 경우에 대한 비용도 감소할 것이다. 고객을 인증하는 것은, 보안 사항을 또한 취급하며, 따라서, 온라인 활동의 성장을 야기할 것이다. 온라인 거래 중 당사자들을 인증하는 데 사용된 기존 시스템들은 폭넓게 채택되지 못하고 있다. 왜냐하면, 이 시스템들은 이용이 쉽지 않고, 복잡한 설계를

가지며, 시스템 참가자에 의해 상당한 초기 투자를 필요로하고, 상호운용성(interoperability)이 부족하기 때문이다. 일부 기존 시스템들은 판매자, 카드소지자, 발급자, 그리고 획득자에 의한 인증서의 생성, 분배, 이용을 추가적인 요건으로 하고 있다. 이러한 인증서는 좀 성가신 존재로 알려져 있다.

[0005] 위의 내용을 살펴볼 때, 온라인 거래시 고객의 신원을 인증하기 위한 개선된 시스템을 제공하려는 노력이 경주되고 있다. 더우기, 이러한 인증 프로세스에 관련된 당사자들에게 가용한 정보를 유익하게 이용하려는 노력이 또한 경주되고 있다.

발명의 내용

해결하려는 과제

[0006] 지불 카드(가령, 신용카드, 데빗 카드, 등등)를 이용한 지불 거래 중, 승인되지 않은 이용과 같은 다양한 문제점들을 방지하기 위해 계좌에 대한 카드소지자의 소유권을 확인하는 것이 중요하다. 지불인 인증은 계좌에 대한 카드소지자의 소유권을 확인하는 프로세스이다. 계좌에 대한 카드소지자의 소유권을 인증하기 위한 가장 일반적인 방법은 "카드 제시" 거래 중 판매 위치에서 통상적인 방식으로 발생한다. 카드 제시 거래는 카드소지자의 카드를 판매자가 받아, 지불 카드 단말기에 카드를 그어서, 계좌 상태와 신용 라인 가용성을 확인한 후, 카드 후면의 서명이 구매자의 서명과 일치하는 지를 확인하는 과정들로 이루어진다. 판매자가 이러한 종류의 거래에 대한 세부적 가이드라인을 따를 경우, 판매자는 승인받은 요금에 대한 지불을 적은 할인액 및 수수료로 보장받을 수 있다. 비자 인터내셔널 서비스 어소시에이션같은 서비스 제공자는 이러한 구체적 가이드라인을 제공할 수 있다.

[0007] 온라인이나 메일, 전화 등을 통해 이루어지는 "카드 비-제시" 거래는 판매자에게 보장되지 않는 지불 과정을 포함한다. 이러한 비-대면 거래에서 지불인이 인증되지 않기 때문에 어떤 보장도 제공되지 않는다. 따라서, "카드 비-제시" 거래에 여러가지 위험이 나타날 수 있다. 이러한 위험은 온라인 판매자에 대한 지불 거래의 환불, 판매자 및 카드소지자에 대한 사기 행위, 은행의 예외 항목 처리 비용 증가, 온라인을 통한 상품 및 서비스 구매의 안전성 결여에 대한 인식 증가, 등등과 같은 문제점들을 포함한다. 이러한 위험의 구체적인 예로는, 상품 및 서비스를 온라인을 통해 구매할 때 도난 계좌 정보를 승인없이 이용하는 행위, 카드 계좌 번호를 변조하여 부정 온라인 거래를 행하는 행위, 그리고 네트워크 트래픽으로부터 클리어 텍스트 계좌 정보를 추출하는 행위 등이 있다.

[0008] 전자 상거래가 계속적으로 성장하고 있는 상황에서, 지불인을 인증하는 방법을 제공하는 것은 중요하다. 온라인 거래 종류들의 범위가 주어졌을 때, 거래에 대한 상업적 양태에 관계없이 당사자들의 신원을 인증하는 방법을 제공하는 것이 또한 중요하다. 이는 카드소지자, 판매자, 금융회사 등으로부터 정부 기관까지 모든 거래 참가자들에게 유익한 도움이 될 것이다. 온라인 거래 중 고객을 인증하는 것은, 부정행위, 분쟁, 보상, 환불 등의 경우를 감소시킬 것이고, 이에 따라 각각의 경우에 대한 비용도 감소할 것이다. 고객을 인증하는 것은, 보안 사항을 또한 취급하며, 따라서, 온라인 활동의 성장을 야기할 것이다. 온라인 거래 중 당사자들을 인증하는 데 사용된 기존 시스템들은 폭넓게 채택되지 못하고 있다. 왜냐하면, 이 시스템들은 이용이 쉽지 않고, 복잡한 설계를 가지며, 시스템 참가자에 의해 상당한 초기 투자를 필요로하고, 상호운용성(interoperability)이 부족하기 때문이다. 일부 기존 시스템들은 판매자, 카드소지자, 발급자, 그리고 획득자에 의한 인증서의 생성, 분배, 이용을 추가적인 요건으로 하고 있다. 이러한 인증서는 좀 성가신 존재로 알려져 있다.

[0009] 위의 내용을 살펴볼 때, 온라인 거래시 고객의 신원을 인증하기 위한 개선된 시스템을 제공하려는 노력이 경주되고 있다. 더우기, 이러한 인증 프로세스에 관련된 당사자들에게 가용한 정보를 유익하게 이용하려는 노력이 또한 경주되고 있다.

과제의 해결 수단

[0010] 본 발명은 온라인 거래 중 제시자의 신원을 인증하는 계좌 인증 서비스를 지향한다. 본 인증 서비스에 따르면, 비밀번호나 토큰 등의 다양한 인증 방법을 이용하여 요청자를 위해 계좌 소지자의 신원을 제 3 신뢰 기관이 확인할 수 있다. 온라인 거래 중 계좌 소지자의 신원을 인증하는 과정은, 계좌 소지자로부터 비밀번호를 요청하는 단계, 비밀번호를 확인하는 단계, 그리고 계좌 소지자의 인증이 확인되었는 지 여부를 요청자에게 통지하는 단계로 구성된다. 계좌 인증 서비스의 대안의 실시예는, 고객에 관한 정보가 가치-부가자와 공유되는 가치-부가 구성요소를 포함한다. 고객 정보가 계좌 인증 프로세스의 각 관련자에 의해 수집되기 때문에 해당 고객에 대한

고객 정보가 풍부한 편이다. 가치-부가자는 이 정보를 다양한 방식으로 이용할 수 있다. 모든 관련자들은 고객 정보의 공유로부터 이익을 얻을 수 있고, 각각의 관련자는 이들이 서로의 이익 창출을 위해 어떻게 서로 도울 수 있는 지에 관해 동의할 수 있다. 고객과 판매자 간의 특정 거래와, 고객 정보를 식별하는 거래 식별자를 이용함으로서, 각 관련자는 고객 정보에 관련된 거래들과 관련 동의사항을 또한 검사할 수 있다.

[0011] 본 발명의 한 방법 실시예는 제시자로부터 신원-인증 비밀번호를 수신하는 단계와, 이 신원-인증 비밀번호를 제시자의 계좌에 대해 미리 지정된 비밀번호와 비교하는 단계를 포함한다. 이 방법은 제시자로부터 수신한 신원-인증 비밀번호가 이 계좌에 대해 미리 지정된 비밀번호와 일치할 때 상기 제시자가 상기 계좌의 실제 소유자임을 요청자에게 통지하는 단계를 또한 포함한다. 이러한 방식으로, 제시자가 계좌의 실제 소유자임을 제 3 신뢰기관이 요청자를 위해 인증할 수 있다. 이 방법은 제시자 정보를 가치-부가자에게 전송하는 단계를 또한 포함한다. 일부 실시예에서, 이 방법은 제시자 정보를 한 세트의 기준에 대해 평가하는 단계와, 이 제시자 정보가 상기 한 세트의 기준을 충족시킬 때 가치-부가자에게 제시자 정보를 전송하는 단계를 또한 포함한다. 이에 따라 가치-부가자가 요망 고객 정보를 수신할 수 있다. 또한, 요청자와 가치-부가자 각각은 제시자 정보가 가치-부가자에게 전달되기 전에 한 세트의 권리 및 의무사항에 동의할 수 있다. 추가적으로, 개별적인 온라인 거래를 검색하고 관련 고객 정보를 검색하기 위해 거래 식별자가 사용될 수 있다.

[0012] 발명의 한 실시예에서, 요청자는 판매자이고 가치-부가자는 배송 회사이다. 배송 회사는 판매자로부터 구매한 품목을 배송하기 위해 고객 정보를 이용할 수 있다. 고객 정보는 품목을 고객에게 배송할 지, 배송하면 어떻게 배송할 지를 결정함에 있어 배송 회사를 도울 수 있다.

[0013] 발명의 또다른 실시예에서, 요청자는 판매자이고 가치-부가자는 후속 판매자이다. 후속 판매자는 고객 정보를 이용하여 자신의 상품이나 서비스를 고객에게 판매할 수 있다. 고객 정보는 후속 판매자가 고객과 대응할 지 여부와, 대응하면 어떻게 대응할 지 여부를 결정하는 것을 도울 수 있다.

[0014] 발명의 또다른 실시예에서, 가치-부가자는 보안 관련사항을 평가하기 위해 고객 정보를 이용하는 보안 조직이다. 보안 조직이 보안 관련사항을 처리할 지 여부와, 처리할 경우 어떻게 처리할 지를 결정함에 있어 고객 정보가 보안 조직을 돕는다.

도면의 간단한 설명

[0015] 도 1은 다양한 종류의 계좌 인증 애플리케이션에 대해 본 발명의 계좌 인증 서비스를 구현하기 위한 시스템 구조의 한 실시예 도면.

도 2는 지불 거래시 본 발명의 인증 서비스를 지원하는 시스템 구조의 한 실시예 도면.

도 3은 본 발명의 한 실시예에 따라 계좌 소지자가 계좌 인증 시스템에 등록하는 프로세스의 도면.

도 4는 계좌 인증 시스템 등록 프로세스 중 계좌 소지자가 정보를 입력할 수 있는 인터넷 웹 페이지의 한 실시예 도면.

도 5는 계좌 소지자가 인터넷에 연결된 컴퓨터를 이용할 때 계좌 인증 시스템에서의 인증된 지불 거래의 도면.

도 6은 계좌 소지자에게 비밀번호를 프람프트로 제시하는 일례의 윈도의 도면.

도 7은 고객이 인터넷에 연결된 컴퓨터를 이용할 때, 계좌 인증 시스템에 겹쳐진 지불 거래 중 전송된 일례의 메시지 도면.

도 8은 가치-부가 양태(value-adding aspect)를 포함하는 온라인 계좌 인증에 관련된 일례의 시스템 구조 및 한 세트의 메시지 흐름 도면.

도 9는 본 발명의 한 실시예를 구현하기에 적합한 통신 네트워크의 도면.

도 10은 온라인 및 오프라인 거래 처리를 제공하기 위한 인터체인지 센터 내에 설비된 시스템의 도면.

도 11은 통신 네트워크의 구성요소들의 또다른 도면.

도 12A와 12B는 본 발명의 실시예들을 구현하기에 적합한 컴퓨터 시스템의 도면.

발명을 실시하기 위한 구체적인 내용

[0016] 본 발명의 상세한 설명은 본 발명에 따른 범용 계좌 인증 시스템 및 프로토콜의 개관을 통해 시작된다. 계좌 인

증 시스템은 참가하는 발급자, 계좌 소지자, 그리고 판매자에 대한 서비스로 제공된다. 그후 도 2-7을 참고하여, 온라인 지불 거래에 관한 계좌 인증 시스템의 한 실시예가 기술된다. 온라인 지불 거래에 대한 설명은 지불 거래 자체, 시스템 설정, 고객 등록, 그리고 구체적 메시지 흐름을 포함한다. 온라인 지불 거래에 대한 설명은, 비-지불 거래에 대한 설명과 유사하다. 지불 및 비-지불 거래는 계좌 소지자의 신원을 인증하는 과정을 포함한다.

[0017] 그후 도 8을 참조하여, 가치-부가 컴포넌트를 포함하는 계좌 인증 프로세스의 한 실시예가 설명된다. 고객에 대한 정보를 가치-부가자와 공유함으로서 가치가 부가된다. 고객 정보는 계좌 인증 프로세스의 각 참가자에 의해 수집되기 때문에 아주 상세한 편이다. 가치-부가자는 이 정보를 다양한 방식으로 이용할 수 있다. 가령, 가치-부가자는 필요 정보를 고객에게 제공하거나 상품을 고객에게 배송할 수 있다. 모든 관련자들은 고객 정보를 공유함으로서 이득을 얻을 수 있고, 각 관련자는 서로가 적절하게 이득을 얻을 수 있는 방식에 관하여 동의할 수 있다. 고객과 판매자 간의 구체적 거래와 고객 정보를 식별하는 거래 식별자를 이용함으로서, 각 관련자는 고객 정보에 관한 임의의 협정 및 거래를 심리할 수도 있다. 본 출원은 이러한 정보 공유에 의해, 다양한 관련자들에게 폭넓게 혜택을 적용할 수 있는 방식을 설명한다.

[0018] **계좌 인증 시스템**

[0019] 본 계좌 인증 시스템은 특정 계좌의 소유자라고 주장하는 자의 신원을 한 관련자가 물리적으로 확인할 수 없는 경우와 같은 거래 중에 계좌 소지자의 계좌 소유권을 인증하도록 설계된다. 예를 들어, 계좌 인증 시스템은 요청자의 이득을 위해 카드 제시자의 신원을 제 3 신뢰 기관(trusted party)이 인증할 때 다양한 거래에 사용될 수 있다. 카드 제시자는 특정 신원을 가진 것으로 제시되는 개인이나 실체에 해당한다. 요청자는 카드 제시자의 신원을 인증해달라고 제 3 신뢰 기관에 요청하는 개인이나 실체에 해당한다. 제 3 신뢰 기관은 카드 제시자의 신원을 인증할 수 있는 실체로서, 카드 제시자와 요청자는 제 3 신뢰 기관에 의한 인증 프로세스 실행을 신뢰한다. 제 3 신뢰 기관은 제시자의 신원에 관하여 오류나 부정 행위의 경우 요청자의 이익을 보호하는 것에 동의할 수 있다. 계좌 인증 시스템의 중요한 부분은 온라인이나 휴대용 전자 장치를 통해 이루어지는 지불 거래의 분야에 있다.

[0020] 그러나, 이 시스템은 지불 거래와는 달리 여러 분야에서 사용될 수 있다. 본 발명의 시스템은 고객의 신원에 대한 인증을 필요로 하는 다양한 비-지불 상황에서 사용될 수 있다. 예를 들어, 비-지불 거래는 인터넷 웹사이트에 접속하여 등록 프로세스와 같은 온라인 형식을 완성시키려는 고객을 인증하는 등의 거래를 포함한다. 비-지불 거래는 소매 뱅킹, 전매 뱅킹, 의료 사업, 보험 사업, 증권 사업, 등등과 같은 여러가지를 포함할 수 있다. 소매 뱅킹은 데빗 카드, 퍼처스 카드(purchase card), 가치 저장 카드(stored value card) 등과 같은 카드에 사용되는 계좌 번호를 포함한다. 비-지불 거래는 ID 카드 및 라이센스같은 사항들에 대해 온라인 형식을 완성하는(즉, 채우는) 과정을 또한 포함한다. 예를 들어, 미국 자동차 협회(AAA)는 이 시스템을 이용하여 고객 중 한 명의 신원을 인증할 수 있고, 전화 카드 회사는 이 시스템을 이용하여 특정 카드 사용자의 신원을 인증할 수 있다.

[0021] 도 1은 다양한 종류의 계정 인증 애플리케이션에 대해 계좌 인증 시스템을 구현하기 위한 시스템 구조(100)의 한 실시예를 도시한다. 시스템 구조(100)는 세개의 도메인을 포함한다. 즉, 제 3 신뢰 기관 도메인(103), 상호운용 도메인(104), 그리고 요청자 도메인(105)을 포함한다. 제 3 신뢰 기관 및 요청자 도메인은 기능적 영역을 규정하는 데, 이 기능적 영역 내에서, 제 3 신뢰 기관이나 요청자에 의해 제어되는 구성요소들이 존재한다. 상호운용 도메인 역시 기능적 영역을 규정하는 데, 이 기능적 영역 내의 구성요소들은 제 3 신뢰 기관, 요청자, 또는 그외 다른 관련자(가령, 서비스 조직)에 의해 이용될 수 있다.

[0022] 제 3 신뢰 기관 도메인(103)은 제 3 신뢰 기관에 의해 주로 제어되는 구성요소들을 포함한다.

[0023] 제 3 신뢰 기관의 예로는 지불 카드를 소비자에게 발급하는 금융 회사(즉, 발급 은행)가 있다. 구체적으로, 발급자, 또는 카드 발급자는 카드 공급자로부터 수령한 새 카드를 개인별화하여, 이 카드를 고객에게 발급한다. 개인별화는 카드 공급자에 의해 또는 개별화 사무국에 의해 수행될 수도 있다. 발급자는 금융 회사 말고도, 통신 네트워크 오퍼레이터, 서비스 조직, 판매자, 또는 그외 다른 조직, 또는 발급자의 대리인과 같은 적절한 발급 실체일 수 있다. 요청자 도메인(105)은 요청자에 의해 주로 제어되는 구성요소들을 포함한다. 요청자는 계좌 소지자의 신원을 인증해달라고 요청하는 실체이다. 가령, 요청자는 신용 카드 계좌의 소유자라고 주장하는 사람의 신원을 인증하고자 하는 판매자일 수 있다. 획득자는 지불 기법에서 요청자들을 등록하여 요청자들의 계좌를 관리하는 금융회사일 수 있다. 획득자는 온라인 판매자로부터 통신 네트워크에 정보를 전달하기도 한다. 다른 실시예에서, 판매자는 정보를 통신 네트워크에 직접 전달할 수도 있다.

[0024] 상호운용 도메인(104)은 인터넷에 의해 지원될 수 있으며, 제 3 신뢰 기관과 요청자에 의해 모두 사용되는 구성요소들을 포함한다.

[0025] 제 3 신뢰 기관(103)은 발급자 계좌 소지자 시스템(110), 등록 서버(112), 액세스 제어 서버(ACS)(114), 그리고 계좌 소지자 파일(118)을 포함한다. 시스템이 사용될 구체적 분야에 따라 제 3 신뢰 기관 도메인(103) 내에 추가적인 구성요소들이 포함된다. 예를 들어, 아래의 지불 거래에서, 각 도메인의 추가적인 구성요소들은, 지불 거래에 대해 계좌 소지자 신원을 인증할 목적으로 존재한다.

[0026] 등록 서버(112)는 웹 인터페이스를 통해 일련의 질문들을 제시함으로서 계좌 인증 시스템에 대한 계좌 소지자의 등록을 관리하는 컴퓨터이다. 이러한 일련의 질문들은 계좌 소지자가 답변하게 되고 제 3 신뢰 기관에 의해 확인되게 된다. 도 1에 도시되는 바와 같이, 제 3 신뢰 기관은 등록 서버(112)를 동작시킨다. 그러나, 비자같은 서비스 조직이 제 3 신뢰 기관 대신에 등록 서버(112)를 동작시킬 수 있다. 제 3 신뢰 기관은 계좌 소지자의 신원을 비준하기 위해 등록 프로세스 중 외부 실체에 의해 제공되는, 웹에 의해 구현되는, 대화형 "신원 인증 서비스"를 이용할 수 있다.

[0027] ACS(114)는 계좌 인증 시스템에 의해 제공되는 계좌 인증 서비스에 대해 등록된 계좌 소지자의 데이터베이스를 가지는 컴퓨터이다. ACS(114)는 각 계좌 소지자에 대한 계좌 및 비밀번호 정보를 포함한다. 계좌 인증 거래 중, ACS(114)는 디지털 방식으로 설명한 영수증을 인증 요청자에게 제공하고, 계좌 인증 시스템에 대한 액세스를 제어하여, 이 서비스에 대한 계좌 소지자 참가를 비준한다. 카드 발급자나 서비스 조직(가령, 비자)은 제 3 신뢰 기관을 위해 ACS(114)를 동작시킨다. 신원 인증 서비스가 어떤 추가적인 계좌 소지자 소프트웨어의 이용을 요건으로 하는 것은 아니지만, 부가적인 계좌 소지자 소프트웨어 및 하드웨어가 전개될 수 있다. 부가적인 계좌 소지자 소프트웨어는 디지털 인증서, 집적 회로 카드(칩 카드), 그리고 칩 카드 판독기같은 추가적인 인증 기술들을 지원할 수 있다. 본 발명에서, 인증서를 요건으로 하는 시스템 참가자는 발급 금융 회사뿐이다.

[0028] 계좌 소지자 파일(118)은 계좌 인증 시스템으로 성공적으로 등록된 계좌 소지자에 관한 정보를 저장하는, 제 3 신뢰 기관에 의해 운영되는 데이터베이스이다. 발급자 계좌 소지자 시스템(110)(또는 제 3 신뢰 기관 계좌 소지자 시스템)은 계좌 소지자에 관한 정보를 지니며 제 3 신뢰 기관에 의해 제어된다. 이러한 정보는 계좌, 정보, 계좌 소비자에 의해 이용되는 서비스, 등등에 관한 것이다. 발급자 계좌 소지자 시스템(110) 내의 일부 정보는 계좌 인증 서비스에 계좌 소지자를 등록하는 데 사용된다.

[0029] 요청자 도메인(105)의 요청자(180)는 계좌 소지자의 인증을 원하는 것이 일반적이다. 요청자(180)는 인증 프로토콜을 촉진시키는 요청 플러그-인 소프트웨어(182)를 관리한다. 요청 플러그-인 소프트웨어 모듈(182)은 제 3의 웹사이트나 요청자의 웹사이트에 포함된 소프트웨어 모듈이다. 플러그-인 소프트웨어 모듈(182)은 계좌 인증 시스템과 요청자의 처리 소프트웨어(가령, 판매자의 지불 처리 소프트웨어) 간에 인터페이스를 제공한다.

[0030] 상호운용 도메인(104)은 디렉토리 서버(128)를 포함하고, 인터넷에 의해 지원되며, 제 3 신뢰 기관 및 요청자 모두에 의해 사용되는 구성요소들을 포함한다. 디렉토리 서버(128)는 요청자로부터 특정 ACS(가령, ACS(114))까지 인증 요청을 전달한다. 디렉토리 서버(128)는 카드 기법 관리자나 서비스 조직(가령, 비자)에 의해 동작한다. 상호운용 도메인(104)은 인터넷과는 다른 네트워크에 의해 지원될 수도 있다.

[0031] **지불 거래용 계좌 인증 시스템**

[0032] 지불 거래 영역에서 계좌 소지자를 인증하는 시스템 구조에 대한 설명이 이제부터 이어질 것이다. 지불 거래의 인증 프로세스는 비-지불 거래의 인증 프로세스와 유사하다.

[0033] 지불 거래에서 인증 시스템 및 프로토콜에 대한 이용예가 아래에 설명된다. 인증 시스템은 계좌 소지자가 온라인으로 쇼핑할 때, 계좌 소지자가 아이템을 쇼핑카트에 담을 때, 온라인 판매자의 결제 페이지로 진행할 때, 그리고 온라인 판매자의 결제 형식을 완성시킬 때 유용하다. 인증 프로세스는 요망 품목이나 서비스를 구매하기로 결정한 후, 가령, 소비자가 "구매" 버튼을 클릭한 후, 구현될 수 있다. 인증 프로세스는 소비자의 지불 거래시이와는 다른 시간에 시작될 수도 있다. 인증 프로세스는 지불 네트워크의 여러 지점에 포함된 소프트웨어를 이용함으로서 소비자에게 투명한 모드로 대게 수행된다. 시스템은 계좌 소지자와 계좌 소지자의 금융 회사가 인증 서비스에 참가하는 것을 비준한다. 그후 계좌 소지자로부터 앞서 등록된 비밀번호를 요청함으로서 소비자가 자신의 신원을 확인할 수 있는 윈도가 생성된다. 소비자의 신원이 확인되면, 소비자의 인증에 관한 통지 및 지불 정보가 판매자에게 다시 전달된다. 그후, 통상적으로 수행되는 바와 같이, 지불 거래가 판매자에 의해

처리된다. 예를 들어, 판매자는 계좌 소지자의 브라우저에 주문 확인 메시지를 전송할 수 있다.

[0034] 도 2는 지불 거래의 인증 서비스를 지원하는 시스템 구조(200)의 한 실시예를 도시한다. 도 1의 일반적 시스템 구조(100)에서처럼, 구조(200)는 세개의 도메인, 즉, 발급자 도메인(102), 상호운용 도메인(104), 그리고 획득자 도메인(106)으로 나누어진다. 발급자 도메인(102)과 획득자 도메인(106)은 도 1의 제 3 신뢰 기관 도메인(103) 및 요청자 도메인(105)과 유사하다.

[0035] 발급자 도메인(102)은 등록 사이트(108), 발급자 계좌 소지자 시스템(110), 계좌 소지자 클라이언트 장치(122), 등록 서버(112), 액세스 제어 서버(ACS)(114), 발급자나 요청자 신원 인증 컴포넌트(116), 그리고 계좌 소지자 파일(118)을 포함한다. 부가적으로, 발급자 도메인(102)은 승인받은 계좌 소지자(120)의 발급자 파일을 포함할 수 있다. 계좌 소지자는 특정 신원을 가진 것으로 계좌를 제시할 수 있기 때문에 "제시자"라고도 불린다. 등록 서버(112)는 웹 인터페이스를 통해 일련의 질문들을 제시함으로서 계좌 인증 시스템에서의 계좌 소지자 등록을 관리하는 컴퓨터이다. 이 질문들에 계좌 소지자들이 답변하게 되고, 발급자들이 이를 확인하게 된다. 등록 서버(112)는 인터넷을 통해 인터넷 지불 게이트웨이 서비스(124)에 연결되고, 이 서비스(124)는 비자넷(VisaNet)과 같은 통신 네트워크(126)에 연결된다. 인터넷 지불 게이트웨이 서비스(124)에 의해 등록 서버(112)가 통신 네트워크(126)와 통신을 행할 수 있다. 지불 게이트웨이 서비스(124)를 통한 연결에 의해, 등록 서버(112)가 발급자의 승인 시스템(127)에 질의하여, 등록된 계좌 소지자가 액티브 카드 계좌를 가졌는 지를 결정할 수 있다. 등록 사이트(108)는 계좌 인증 시스템에 의해 제공되는 계좌 인증 서비스에 참가하기 위해 계좌 소지자가 등록할 수 있는 인터넷 웹 사이트이다.

[0036] 계좌 소지자 클라이언트 장치(122)는 계좌 인증 시스템에 참가하는 계좌 소지자에 의해 이용된다. 구체적으로, 계좌 소지자 클라이언트 장치(122)는 개인용 컴퓨터, 이동 전화, PDA, 또는 대화형 케이블 TV 등과 같이 인터넷에 액세스할 수 있는 임의의 장치일 수 있다. 일부 실시예에서, 계좌 소지자 클라이언트 장치(122)는 인터넷에 연결될 수 없다. 그러나 이러한 장치는 계좌 소지자에 의해 여전히 이용될 것이다. 왜냐하면, 클라이언트 장치(122)로부터의 입력 및 출력 메시지들이 전용 노드를 통해 전달되기 때문이다. 이 전용 노드들은 비-인터넷 기반 메시지들을 취급할 수 있는 노드들이다. 예를 들어, 음성이나 텍스트 메시지에 기초하여 메시지들을 송신 및 수신하는 이동 전화들은 차별화된 방식으로 메시지들을 전달함으로서 계좌 인증 시스템에 여전히 사용될 수 있다. 단문 메시지 서비스(SMS)는 메시징 시스템의 공공연한 예에 해당한다. 대화형 음성 응답(IVR) 유닛은 음성 채널을 통한 자동 교환에 사용될 수 있다. 이러한 메시지 전달 배열은 비-인터넷 장치에 대한 다음 문단의 내용에서 더욱 상세하게 설명될 것이다.

[0037] 발급자 계좌 소지자 시스템(110)은 계좌 소지자에 관한 정보를 지닌 발급자-제어 시스템이다. 이 시스템 정보는 계좌 소지자에 의해 이용되는 서비스, 계좌 정보에 관한 정보, 등등을 포함한다. 발급자 계좌 소지자 시스템 내의 정보의 일부는 계좌 인증 시스템에 계좌 소지자를 등록하기 위한 프로세스에 사용될 수 있다.

[0038] 발급자나 요청자의 신원 인증 데이터베이스(116)는 계좌 소지자에 관하여 발급자나 요청자가 기존에 가지고 있던 정보를 포함한다. 데이터베이스(116)는 계좌 소지자의 신원을 확인하기 위해 계좌 소지자들을 등록하는 프로세스에서 발급자에 의해 이용된다. 가령, 계좌 소지자 등록 프로세스 중 계좌 소지자에 의해 입력되는 정보는, 인증 데이터베이스(116)의 파일에 기입력된 정보와 일치하여야 한다. 따라서, 계좌 인증 시스템에 의해 제공된 서비스를 계좌 소지자가 성공적으로 등록할 수 있다. 제 3 신뢰 기관은 Equifax같은 회사일 수 있다.

[0039] 상호운용 도메인(104)은 디렉토리 서버(128), 인증 히스토리 서버(130), 그리고 영수증 매니저(131)를 포함한다. 디렉토리 서버(128)는 판매자로부터 특정 ACS까지 인증 요청을 전달한다. 디렉토리 서버(128)는 비자와 같은 서비스 조직에 의해 운영된다. 인증 히스토리 서버(130)와 영수증 매니저(131)는 인증된 각각의 지불 거래에 대해 서명된 영수증(가령, 아래 설명되는 지불 요청 응답 메시지의 사본)을 저장한다. 인증 히스토리 서버(130)는 어떤 거래가 인증되었는 지를 확인하는 정보를 포함하며, 분쟁 해결 프로세스 중 추가적인 정보를 제공한다. 인증 히스토리 서버(130)와 영수증 매니저(131)는 서비스 조직에 의해 운영된다. 발급자, 획득자, 또는 판매자는 디지털 방식으로 서명된 영수증의 사본을 유지관리할 수도 있다.

[0040] 획득자 도메인(106)은 판매자(132)와 검증 서버(validation server)(136)를 포함한다. MPI(134)는 판매자(132)의 위치에 위치한다. MPI(134)는 판매자의 전자 상거래 웹사이트에 통합된 소프트웨어 모듈이다. MPI(134)는 계좌 인증 시스템과 판매자의 지불 처리 소프트웨어 간에 인터페이스를 제공한다.

[0041] MPI(134)는 도 1의 요청 플러그-인 소프트웨어 모듈(182)과 같은 소프트웨어 모듈이다. "판매자"의 기술자

(descriptor)는 플러그-인 소프트웨어 모듈을 이용하는 요청자의 종류를 표시하기 위해 MPI(134)에 이용된다. 그러나, 본 명세서 내에서의 플러그-인 소프트웨어 모듈(134)은, 플러그-인 소프트웨어 모듈(134)을 설명하는 데 사용되는 표현에 관계없이, 기본적으로 동일한 방식으로 기능한다. 본 명에서에서 용어의 이용을 단순화하기 위해, "판매자"의 표현이 플러그-인 소프트웨어 모듈을 설명하는 데 사용될 것이다. 그러나, 플러그-인 소프트웨어 모듈(134)을 판매자인 요청자에 의해 이용하기에 적합한 것으로만 제한하는 것으로 판단하여서도 아니된다. 더우기, MPI는 판매자 플러그-인 소프트웨어 모듈의 약자로 사용될 것이다.

[0042] 검증 서버(136)는 지불 거래 중 계좌 인증 시스템에 의해 판매자에게 되돌아오는 영수증에 서명하는 데 사용되는 카드 발급자의 디지털 시그너처를 검증한다. 대안의 실시예에서, 검증 서버(136)의 기능은 MPI(134) 내에 포함될 수 있어서, 별도의 검증 서버(136)가 필요치 않게 된다. 검증 서버(136)는 판매자, 획득자, 또는 서비스 조직에 의해 운영된다.

[0043] 일부 실시예에서, 계좌 인증 시스템은 전자 지갑같은 다른 계좌 소지자 애플리케이션과 상호운영될 수 있고, 이 서비스는 전자 상거래 마크업 랭기지(ECML 소프트웨어)와 호환되도록 동작할 수 있다. 계좌 인증 시스템은 분쟁 해결 과정을 구현하는 기능을 또한 제공한다. 예를 들어, 판매자는 분쟁 해결 및 환불을 위해 계좌 소지자 인증의 증거를 제공하기에 충분한 정보를 유지할 수 있다.

[0044] **<u>설정 및 등록 과정</u>**

[0045] 지불 및 비-지불 거래 모두에 대해 계좌 인증 시스템을 설정하는 과정이 아래에 설명된다. 먼저, 계좌 인증 시스템을 이용할 수 있도록 다양한 시스템 참가자를 설정하는 데 요구되는 과정들이 설명될 것이다. 그후, 계좌 인증 시스템에 등록하기 위한 계좌 소지자의 프로세스가 설명될 것이다. 이 단계들 이후, 지불 거래의 실제 승인에 관하여 설명이 이어질 것이다.

[0046] 계좌 인증 시스템을 설정하는 과정은, 시스템 내의 모든 참가자들에 대한 설정 과정들을 포함한다. 이 설정 과정들은 지불 및 비-지불 거래의 승인에 대해 동일한 것이 일반적이다. 이 참가자들은 판매자나 그외 다른 인증 요청자, 금융 회사, 또는 그외 다른 제 3 신뢰 기관, 그리고 계좌 소지자 등등과 같은 실체들을 포함한다.

[0047] 계좌 인증 시스템에 서명한 온라인 판매자같은 요청자들은 도 1의 플러그-인 소프트웨어 모듈(182)이나 도 2의 모듈(134)같은 플러그-인 소프트웨어 모듈들을 수용한다. 플러그-인 소프트웨어 모듈은 요청자에 의해 사용되는 연산 플랫폼과 서버 소프트웨어에 대해 전용화되어야 한다. 계좌 인증 시스템 내에 참가하는 금융회사들과 같은 요청자들은 주문형 등록 사이트 템플릿에 포함되도록 서비스 로고 및 마케팅 디자인을 제공할 것이다. 은행들을 확보하고 있는 제 3 신뢰 기관은 서비스 조직 인증 기관(CA) 루트 인증서, 클라이언트 인증용 서비스 조직 인증 기관(CA) SSL 인증서, 그리고 일체형 서포트를 판매자에게 제공하여야 한다.

[0048] 계좌 인증 시스템을 이용하기 위해 제 3 신뢰 기관이 설정되기 전에, 제 3 신뢰 기관 도메인에 명시된 모든 계좌 인증 시스템 하드웨어 및 소프트웨어의 사본을 확보하여 설치하여야 한다. 발급자 금융 회사같은 제 3 신뢰 기관들은 계좌 소지자 신원 확인 프로세스에 사용하도록 계좌 인증 시스템에 신원 인증 정책과 참가 은행 식별 번호(BIN) 정보를 또한 제공할 것이다. 부가적으로, 발급자는 계좌 소지자 파일(118)에 미리 로딩하기 위해 계좌 인증 시스템에 계좌 소지자 인증 정보를 제공할 수 있다. 미리 로딩함으로서, 다량의 계좌 소지자 서포트를 촉진시킬 수 있다. 예를 들어, 제 3 신뢰 기관이 계좌 인증 서비스에 대한 모든, 또는 대부분의 계좌 소지자의 계좌 인증 서비스를 활성화시키고자 할 때, 제 3 신뢰 기관은 모든 계좌 소지자에게 개인 식별 번호(PIN)를 전송할 수 있다. PIN은 각 계좌 소지자가 미리 로딩한 비밀번호에 액세스하는 데 사용될 수 있다. 이러한 방식으로, 등록 프로세스가 촉진된다. 왜냐하면, 각 계좌 소지자가 형식적인 등록 프로세스를 거칠 필요가 없기 때문이다. 계좌 소지자가 미리 로딩된 비밀번호를 첫번째로 이용한 후, 계좌 소지자는 비밀번호를 기억하기에 쉽고 새롭게 지정할 수 있는 옵션을 가진다.

[0049] 계좌 소지자 인증 정보는 회사 ID(business identification), 국가 코드, 카드 계좌 번호, 카드 유효 기간, 계좌 소지자 성명, "참가 BIN" 데이터에 명시된 발급자 전용 인증 데이터(가령, 엄마의 결혼전 성명), 그리고 그외 다른 정보 등과 같은 정보들을 포함한다. 그외 다른 정보의 예로는, 청구지 주소, 배송 주소, 사회 보장 번호, 전화 번호, 계좌 잔고, 거래 내역, 그리고 운전 면허 번호 등등이 있다. 제 3 신뢰 기관은 카드 계좌 포트폴리오에 대한 계좌 번호 범위와, ACS IP 어드레스(URL)를 디렉토리 서버에 또한 제공하여야 한다. 계좌 인증 시스템의 지불 장치와 관련하여, 이 서비스는 은행 브랜드의 웹 사이트를 통해 제공될 수 있고, 이 웹 사이트는 계좌 소지자 등록을 가능하게 한다.

[0050] 도 3은 한 실시예에 따른 계좌 인증 시스템으로 계좌 소지자가 등록하는 프로세스를 도시한다. 단계 1에 도시되

는 바와 같이, 계좌 소지자는 제 3 신뢰 기관(가령, 발급자 금융 회사)에 의해 유지되는 등록 서버 인터넷 웹사이트를 방문한다. 계좌 소지자는 자신의 계좌 번호를 등록함으로서 계좌 인증 시스템에 등록한다. 가령, 지불 거래를 이용할 때, 계좌 소지자는 자신의 신용 카드, 데빗 카드, 또는 체크 카드 계좌 번호를 등록할 수 있다. 비-지불 거래의 경우, 계좌 소지자는 보험 회사나 증권 회사에 보유된 계좌 번호를 등록할 수 있다. 계좌 소지자는 한개 이상의 카드를 등록할 수 있다.

[0051] 단계 2에서, 계좌 소지자는 메인 계좌 번호(PAN), 성명, 그리고 카드 유효 기간 등등과 같은 정보를 입력한다. 이때, 계좌 소지자는 추가 정보를 입력할 수도 있다. 가령, 주소, 이메일 주소, 구매자 ID, 계좌 확인 값, 계좌 소지자-전용 비밀번호, 그리고 발급자-전용 인증 정보 등이 입력될 수 있다. 이 정보는 도 4에 도시된 페이지(300)같은 등록 웹사이트의 페이지에서 입력될 수 있다.

[0052] 계좌 소지자가 등록 사이트(108)에서 요청받은 정보를 입력한 후, 계좌 인증 시스템은 계좌 소지자의 PAN이, 상호운용 도메인(104)의 디렉토리 서버(128)에서 제 3 신뢰 기관에 의해 등록되는 카드 범위 내에 있음을 확인한다. 계좌 소지자는 다양한 방법들을 이용하여 확인될 수 있다. 먼저, 방금 언급한 바와 같이, 계좌 소지자 신원은 요청자 인증 데이터베이스를 통해, 또는, 제 3 신뢰 기관의 고유 인증 데이터베이스를 통해 확인될 수 있다. 추가적으로, 제 3 신뢰 기관에 의해 제공되는 승인된 계좌 소지자(120)의 파일을 이용함으로서, 제 3 신뢰 기관에 상태 체크 승인을 전송함으로서, 그리고 금융 회사에서 제공한 미리 로딩된 정보에 응답들을 비교함으로서, 확인이 수행될 수 있다.

[0053] PAN이 등록된 카드 범위 내에 없을 경우, 등록은 거절되고 등록 프로세스가 종료된다. 지불 거래 시에, PAN이 등록 카드 범위 내에 있을 경우, 1달러(또는 그외 다른 통상적 값)에 대한 승인이 서비스 조직 지불 네트워크(가령, 비자넷)을 통해 발급자 금융 회사에 제출될 것이다. 1달러 거래의 승인에 의해, 발급자는 카드 계좌 상태, 주소 확인 서비스를 이용한 주소, 그리고 계좌 소지자 확인 값 2(CVV2)를 확인할 수 있다. CVV2는 지불 카드의 후면의 서명란에 인쇄된 세자리 숫자이다. 비-지불 거래 시에, PAN이 등록 카드 번호 범위 내에 있을 경우 1달러 거래가 요구되지 않는다.

[0054] 단계 3에서, 대화형의 실시간 온라인 세션에서 계좌 소지자의 신원을 확인하기 위해 추가적인 승인 정보에 대한 프람프트가 계좌 소지자에게 제공된다. 일부 실시예에서, 계좌 소지자는 비밀번호 입력을 요구받을 수 있고, 인증 거래 중 계좌 소지자를 인증하는 데 사용될 "힌트 질문 및 답변"을 또한 요구받을 수도 있다.

[0055] 단계 4에 도시되는 바와 같이, 계좌 소지자의 신원이 확인되고 적절한 응답이 나타날 경우, 승인 메시지가 발급자 금융 회사에 전달된다. 그후 단계 5에서, 등록 서버(112)는 계좌 소지자 정보를 ACS(114)에 전달하여, 계좌 소지자 파일(118)에 레코드를 설정한다. 계좌 소지자 파일(118)은 금융 회사 BIN 번호, 계좌 번호, 유효 기간, 성명, 운전면허번호, 청구지 주소, 사회 보장 번호, 계좌 소지자 비밀번호, 계좌 소지자 비밀번호 질문, 계좌 소지자 비밀번호 답변, 계좌 소지자 이메일 주소, 요청자 식별 점수, 그리고 그외 다른 정보 등등과 같은 정보를 저장할 수 있다.

[0056] 일부 실시예에서, 등록 프로세스 중, 계좌 소지자는 개인 확인 메시지(PAM: Personal Assuarance Message)라 불리는 어구를 입력할 것을 요청받을 수 있다. 즉, 계좌 소지자를 인식할 수 있는 어구를 입력할 것을 요청받을 수 있다. PAM은 인증 프로세스 중 제 3 신뢰 기관에 의해 계좌 소지자에게 나중에 제시된다. 제 3 신뢰 기관만이 계좌 소지자의 지정 PAM을 알기 때문에, 계좌 소지자는 계좌 인증 시스템을 이용하여 사용된 대화 윈도가 제 3 신뢰 기관으로부터 전달되었음을 보장받을 수 있다. PAM의 한가지 예는 "the sky is blue"이다.

[0057] 인증 시스템을 이용함에 있어 계좌 소지자에게 어떤 클라이언트 소프트웨어나 장치가 요구되지 않는다. 선호되는 실시예에서, 계좌 소지자 등록 프로세스는 SSL 채널 암호화와 같은 보안 프로토콜을 이용하여, 계좌 소지자와 등록 서버 사이에서 인터넷을 통해 전송되는 데이터를 보호할 수 있다.

[0058] 또한, 등록 프로세스 중, 각각의 제 3 신뢰 기관은 자체 "이용 표현(terms of use)"과 "데이터 보호 정책(data privacy policy)"을 디스플레이할 수 있다. 각각의 제 3 신뢰 기관은 등록 프로세스를 완료하기 위해 등록하는 계좌 소지자가 표현 및 정책을 수락하거나 거절할 수 있게 하는 기능을 가진다. 각 계좌 소지자에 의해 수락된 "이용 표현"이나 "데이터 보호 정책"의 버전 번호가 제 3 신뢰 기관에 의해 저장되어야 한다.

[0059] **지불 거래**

[0060] 모든 참가자들이 설정되고 계좌 소지자들이 등록된 후, 계좌 인증이 수행된다. 도 5는 코어 계좌 인증 시스템을 이용하는 인증된 지불 거래를 설명한다. 이때, 계좌 소지자는 인터넷에 연결된 컴퓨터를 이용한다. 도 5의 단계 1에서, 계좌 소지자는 인터넷 상의 판매자 전자 상거래 사이트를 방문한다. 계좌 소지자는 카드 소지자라고도

불릴 수 있다. 왜냐하면, 지불 거래에서, 계좌 소지자가 보유한 가장 흔한 종류의 계좌가 신용카드, 데빗카드, 또는 체크 카드 계좌이기 때문이다. 계좌 소지자가 구매하고자 하는 상품이나 서비스를 선택한 후, 계좌 소지자는 결제 프로세스를 시작하고, 결제 형식을 완성한 후, "구매" 버튼을 누른다.

[0061] 도 5의 단계 2에 도시되는 바와 같이 "구매" 버튼이 선택된 후, MPI가 활성화되고, 계좌 소지자의 특정 계좌가 계좌 인증 시스템에 등록되어 있는 지를 결정하기 위해 확인 프로세스가 수행된다. 계좌 소지자가 계좌 인증 시스템에 등록되어 있는 지를 MPI가 결정하는 방법에는 여러가지가 있다. 가령, 디렉토리 서버가 먼저, 계좌 소지자에 관련된 ACS가 그후에 확인되는 2-단계 프로세스, ACS만이 확인되는 프로세스, 그리고, 디렉토리 서버에 보유된 동일 정보를 지닌 캐쉬 메모리를 판매자가 확인할 수 있는 방법 등이 사용될 수 있다.

[0062] 2-단계 프로세스에 대한 설명이 이어질 것이다. 도 2를 참고하여 설명이 이루어진다. 제 1 단계에서, MPI는 카드 계좌 번호를 인식한 후, 계좌 인증 시스템의 참가자인 발급자 은행에 연계된 숫자들의 범위 내에 해당 계좌 번호가 있는 지 확인하기 위해 디렉토리 서버(128)에 질의한다. 계좌 번호가 디렉토리 서버(128)에 규정된 계좌 번호 범위 내에 없을 경우, 발급자와 계좌 소지자는 등록되어 있지 않다. 이 경우에, 계좌 번호가 등록되어 있지 않다는 사실이 판매자에게 통지되고, MPI(134)는 거래의 제어를 판매자의 판매 소프트웨어에 되보낸다. 이 때, 판매자의 판매 소프트웨어는 거래를 진행할 수도 있고, 계좌 소지자에 대한 추가 서비스를 거절할 수도 있고, 또는 대안의 지불 방법을 진행할 수도 있다.

[0063] 다른 한편, 계좌 번호가 디렉토리 서버(128)에 존재하는 계좌 번호들의 범위 내에 있다고 결정되면, 확인 프로세스의 제 2 단계가 시작된다. 확인 프로세스의 제 2 단계는 계좌 번호가 등록되어 있는 지를 결정하기 위해 디렉토리 서버(128)가 ACS에 해당 계좌 번호를 전송할 때 시작된다. 카드가 등록되어 있지 않을 경우, 등록 프로세스가 종료된다. 카드가 등록되어 있다고 ACS가 표시하면, ACS는 디렉토리 서버를 통해 해당 URL 인터넷 어드레스를 MPI에 되보낸다. MPI는 그후 계좌 소지자 클라이언트 장치 및 상주 브라우저를 통해 ACS를 호출한다. 다시 한번, 계좌 인증 시스템에 ACS가 여러개 있을 수 있다는 점에 주목하기 바란다.

[0064] 계좌 소지자가 계좌 인증 시스템에 등록되어 있는 지를 확인하기 위한 제 2 확인 방법은 디렉토리 서버(128)에 먼저 질의하지 않고 MPI(134)가 ACS(114)에 직접 질의하는 것이다. 앞서 언급한 세번째 방법은, 디렉토리 서버(128)에 유지된 동일 정보를 지닌 캐쉬 메모리를 판매자가 구비하는 것이다. 이러한 방식으로 판매자는 예비 확인을 행할 수 있다.

[0065] 계좌 인증 시스템에 두개 이상의 물리적 디렉토리 서버가 존재할 수 있다. 그러나, 한개의 로직 디렉토리 서버만이 존재하는 것이 바람직하다. 다시 말해서, 모든 디렉토리 서버들은 동일한 정보를 지니도록 일관성을 가져야 한다.

[0066] 계좌 소지자가 계좌 인증 시스템의 참가자일 경우, ACS(114)는 계좌 소지자에게 은행 브랜드의 윈도를 디스플레이한다. 은행 브랜드의 윈도는 기본적인 지불 거래 정보를 포함하며, 인증 비밀번호나 토큰을 계좌 소지자에게 프람프트로 묻는다. 인증 비밀번호를 계좌 소지자에게 프람프트로 질의하는 일례의 윈도(500)가 도 6에 도시되어 있다. 계좌 소지자는 인증 비밀번호를 입력하고, ACS(114)는 승인 비밀번호를 확인한다. 윈도(500)의 크기 및 배열은 계좌 소지자에 의해 사용되는 장치의 매개변수들에 따라 변한다. 오늘날 잘 알려진 바와 같이, 계좌 소지자는 인증 비밀번호를 정확하게 입력할 수 있는 기회를 몇차례 제공받을 수 있다. 계좌 소지자가 인증 비밀번호를 정확하게 입력할 수 없는 경우, 계좌 소지자는 계좌 소지자의 등록 프로세스 중 구축했던 힌트 질문을 프람프트로 제시받을 수 있다. 계좌 소지자는 힌트 질문에 따라 정확한 답변을 입력할 기회를 한번 제공받는 것이 바람직하다.

[0067] 정확한 인증 비밀번호나 토큰이 즉시 입력되거나 계좌 소지자가 힌트 질문에 정확한 답변을 제공할 경우 지불 인증이 계속된다. ACS는 발급자의 시그너처 키나 서비스 제공자의 키를 이용하여 디지털 방식으로 영수증에 서명한다. 이 영수증은 판매자 명칭, 카드 계좌 번호, 지불 금액, 그리고 지불일을 포함할 것이다. 일부 실시예에서, 이 영수증은 지불 인증 응답(PARes: Payment Authentication Response) 메시지의 사본이거나, PARes 메시지로부터 복제한 정보 필드들 중 일부분을 가진 메시지이다. 인증 히스토리 서버(130)는 다음의 거래 데이터를 저장한다. 즉, 판매자 명칭, 판매자 URL, 카드 계좌 번호, 유효 기간, 지불 금액, 지불일, 발급자 지불 시그너처, 그리고 계좌 소지자 인증 확인 값을 저장한다. 그후 ACS는 계좌 소지자를 계좌 소지자 브라우저를 통해 MPI에 접하게 한다. 이때, ACS는 디지털 방식으로 서명한 영수증을 판매자에게 건네며(redirection), 계좌 소지자가 인증되었는 지 여부에 관한 결정사항을 함께 건넨다. 검증 서버(validation server)(136)는 획득자 도메인(106)에서 MPI(134)에 의해 이용되어, 지불 영수증에 서명하는 데 사용되는 디지털 시그너처를 확인한다. 디지털 시그너처를 확인한 후, 계좌 소지자는 "인증되었다"고 간주된다. 일부 실시예에서, 거래가 완료된 후, 계좌

소지자는 자신의 카드 계좌를 재등록하는 기능을 또한 가지며, 차후 온라인 구매를 위해 사용할 새 비밀번호를 생성할 수 있다.

[0068] 계좌 소지자가 단계 3에서 인증된 후, 단계 4는 특정 계좌 소지자의 계좌를 승인하기 위한 프로세스를 개시한다. 승인은 계좌 소지자가 적절한 이용을 가지고 있는 지, 그리고 특정 구매를 위해 적합한 상태에 있는지를 확인하는 프로세스를 의미한다. 이와는 대조적으로, 인증은 계좌 소지자의 신원을 확인하는 프로세스를 의미한다. 단계 4에서, 판매자는 MPI를 이용하여 승인 메시지를 지불 네트워크(가령, 비자넷)에 전송한다. 지불 네트워크는 승인 메시지와 전자 상거래 표시자(ECI)를 발급자 금융 회사에 전달한다. 승인 메시지는 당 분야에 잘 알려진 흔히 사용되는 메시지이다. 승인 메시지는 발급자에게 전달되어, 특정 계좌가 적절한 상태에 있고 요청받은 지불 거래 금액에 대해 적절한 신용 한도를 가지고 있다는 것을 발급자 금융 회사가 판매자에게 확인해 줄 수 있다. ECI는 거래가 인터넷 상에서 완료되었음을 표시하고, 사용되는 인증과 메시지 보안의 레벨을 표시한다.

[0069] 대안의 실시예에서, 판매자는 승인 메시지와 함께 추가 정보를 제공할 수 있다. 예를 들어, 다음의 정보가 전달될 수도 있다. 즉, 계좌 소지자가 성공적으로 인증되었는 지를 표시하는 플래그, 계좌 정보, 디지털 시그너처, 계좌 소지자 확인 값 2, 거래 식별자, 칩 카드 유로페이(Europay), 마스터카드(Mastercard), 비자(EMV) 암호문에 의해 인증된 오프라인 PIN, 그리고 판매자에게 지불 보증을 제공하기 위한 필드들이 전달될 수 있다. 승인 거래의 발급자 금융 회사 처리가 완료되면, 지불 거래의 제어가 지불 네트워크를 통해 판매자의 판매 소프트웨어에게로 복귀한다. 발급자는 그후 승인 응답을 지불 네트워크를 통해 판매자에게 되보낸다. 도 5의 단계 5에서, 발급자 금융 회사는 거래를 승인하거나 거절할 것이다. 일부 실시예에서, 승인 메시지는 배치(batch)화되어 차후에 그룹으로 전송될 수 있다. 인증 정보가 배치 승인 메시지에 또한 포함된다.

[0070] 거래 식별자는 계좌 소지자를 인증한 ACS에 의해 생성되며, 해당 지불 카드 및 해당 지불 카드로부터의 특정 지불 거래에 대한 고유 값에 해당한다. 발급자는 거래 식별자를 이용하여, 차후 분쟁이 생길 때와 같은 다양한 용도로, 인증된 지불 거래를 독자적으로 식별한다. 거래 식별자는 특정 온라인 거래에 관한 사항들같이, 레코드를 독자적으로 식별하기에 적합한 데이터의 여러 형태를 취할 수 있다. 한 구현예에서(가령, 지불 거래), 거래 식별자는 카드 인증 확인 값(CAVV)이다. 다음의 설명에서, 거래 식별자는 CAVV로 불릴 수 있다. 그러나, 다양한 종류의 거래 식별자가 역시 사용될 수 있음을 이해하여야 한다.

[0071] 액세스 제어 서버(ACS)(114)는 다양한 다른 명령들을 취급할 수 있다. 가령, ACS는 데이터베이스로부터 등록된 계좌를 정지시킬 수 있다. 계좌는 수동으로, 또는 계좌 소지자에 의해, 또는 발급자에 의해 정지될 수 있다. ACS(114)는 계좌 소지자가 갱신 카드를 수령할 때 단순화된 갱신 등록 프로세스를 제공할 수도 있다. ACS(114)는 고유 액세스 제어 정보를 이용하여 동일 등록 계좌의 다중 사용자들을 지원할 수 있다. 지불 거래나 계좌 업데이트를 위해 ACS(114)에 대한 연결을 사용자에게 제공할 때, ACS(114)는 다음 메커니즘 중 한가지 이상을 통해 등록 계좌의 승인된 계좌 소지자로 사용자를 검증할 수 있다. 즉, 다음 메커니즘이란 패스 어구(pass phrase), 디지털 시그너처, 온라인 PIN 번호, 칩 카드 EMV 암호문에 의한 오프-라인 PIN 승인에 해당한다.

[0072] 판매자(132)는 판매자가 계좌 소지자 계좌 정보를 가지는 기존 시스템과 상호운용될 수 있고, 기존 판매자 승인 및 삭제 시스템과 상호운용될 수 있으며, 다중 판매자에게 서비스를 제공하는 제 3 자를 지원할 수 있고, 판매자와 획득자간 다양한 지불 인터페이스를 지원할 수 있으며, 전자 상거래 표시자(ECI)의 값을 설정할 때 획득자로부터 지불 네트워크 승인 메시지에 대한 강제적 영향을 최소화시킬 수 있다.

[0073] 판매자로부터 ACS까지 거래를 전달하기 위한 한가지 방법은 계좌 소지자의 계좌 번호에 기초하여 서버의 어드레스를 제공하는 디렉토리를 가지는 것이다. 이러한 방법에서, 정보를 전달하기 위한 요청은 인증된 판매자로부터만 수용될 수 있다. 판매자로부터의 활동이 정상 활동을 벗어날 경우, 계좌 인증 시스템은 이러한 액세스가 더 이상 유효하지 않음을 획득자를 통해 표시하는 판매자에 대한 액세스를 거부할 수 있다. 이는 판매자 사기 가능성이 높을 경우에 해당할 수 있다. 계좌 승인 시스템에 대한 판매자 인증이 전개될 수 있으나, 필수사항은 아니다. 판매자 승인은 판매자 사기행위를 최소화시킬 수 있다.

[0074] 도 7은 코어 계좌 인증 시스템을 이용하여 지불 거래 중 전송되는 구체적 메시지들을 도시한다. 이 경우에 소비자는 한 실시예에 따라 인터넷에 연결된 컴퓨터를 이용한다. 도 7의 메시지들은 도 2에 도시되는 지불 시스템 구조에 겹쳐진다. 메시지와 각 메시지 내의 데이터 필드들에게 특정 이름이 부여되지만, 이 이름들은 인증 프로토콜의 성능에 영향을 미치지 않는다. 따라서, 아래 설명되는 메시지 및 데이터 필드에 여러 다른 이름들이 부여될 수 있다. 대안의 실시예에서, 도 7에 기술된 특정 메시지들이 변경되거나 생략될 수 있고, 인증 프로세스의 전체 목적에 영향을 미치지 않으면서 추가 메시지들이 추가될 수 있다. 기능 추가와 통신 병렬화 등과 같은

다양한 이유로 다양한 메시지들이 변경되거나 추가되거나 생략될 수 있다. 본 명세서에서의 프로세스의 메시지 흐름도 위와 같은 이유로 대안의 실시예에서 변경될 수 있다.

[0075] 앞서 언급한 바와 같이, 계좌 소지자가 브라우저를 통해 판매자 웹사이트를 방문하고 구매 아이템을 선택할 때 지불 거래가 시작된다. 판매자의 지불 시스템은 계좌 소지자에게 지불 정보를 입력할 것을 요청한다. 일반적으로, 지불 정보의 입력은 보안 환경에서 이루어져야 한다. 가령, SSI 암호화 프로토콜을 이용하여 이루어져야 한다. 계좌 소지자가 거래 완료할 상태에 이르렀다고 표시하면, 판매자의 지불 시스템은 MPI(134)를 호출한다. 그 후, 라인(1a)에 의해 표시되는 바와 같이, MPI(134)는 계좌 소지자가 이 서비스에 등록하였음을 검증하기 위해 계좌 소지자의 PAN을 지닌 ACS의 특정 URL에 대하여 디렉토리 서버(128)를 확인한다. 대안으로, MPI(134)는 이 정보를 지닌 자체 캐쉬 메모리를 확인한다. MPI(134)는 ACS(114)를또한 확인하여, 계좌 소지자의 PAN이 계좌 인증 시스템에 등록되어 있음을 확인한다. MPI(134)가 자체 캐쉬를 확인할 수 있는 경우에, MPI(134)는 디렉토리(128)의 콘텐트들을 로컬 캐쉬에 복제하는 기능을 가져야 한다. 이 기능이 사용될 경우, 판매자는 계좌가 등록된 범위의 일부분인 지를 캐쉬로부터 즉시 결정할 수 있다. 판매자가 이 기능을 구현할 경우, 캐쉬의 콘텐트들은 만료되어 매 24시간마다 리프레시되어야 한다. MPI(134)가 로딩될 때, 그리고 그후 규칙적 시간 구간마다, 캐쉬가 요청받아야 한다.

[0076] MPI(134)는 계좌 소지자 PAN을 이용하여 등록 확인 요청(VEReq) 메시지를 포매팅함으로서 PAN을 검색한다. 앞서 구축된 것이 아닌 경우에, MPI(134)는 디렉토리 서버(128)나 ACS(114)와의 보안 연결을 구축하여 이를 인증할 것이다. MPI(134)는 여러 위치에서 계좌 소지자 PAN에 대응하는 카드 범위 입력을 검색할 것이다.

[0077] MPI(134)가 검색을 수행한 후, VEReq 메시지는 ACS(114)에 직접 전송되거나(라인(1b) 참조), 디렉토리 서버(128)를 통과한 후 전송된다(라인(1a) 참조). VEReq 메시지가 디렉토리 서버(128)를 통해 ACS(114)에 전송될 때, 디렉토리 서버(128)는 VEReq 메시지에 포함된 계좌 소지자 PAN에 대응하는 레코드를 검색한다. 성공적이지 못한 매치의 경우에, 디렉토리 서버(128)는 URL 값이 없는 등록 확인 응답(VERes) 메시지를 포매팅할 것이고, PAN 등록의 상태, 또는 VERes-Status의 값을 "N"으로 설정할 것이다. VERes 메시지는 MPI로 되돌아온다. 다른 한편, 성공적인 매치의 경우, 디렉토리 서버(128)는 ACS URL과의 보안 연결을 구축하여 인증을 행할 것이다. 그 후, VEReq 메시지는 ACS URL에 전달된다. 이 URL이 가용하지 않을 경우, MPI는 다음 ACS URL값으로 진행하여야 하고, 최대 5개까지의 ACS URL을 검색하여야 한다. 물론, 시도되는 URL의 수는 가변적이다. 이 모든 시도에서 성공하지 못할 경우, VEReq 메시지는 "N"으로 표시된 VERes-Status와 함께 MPI로 되돌아와, 계좌 인증 시스템을 이용하여 지불 거래를 처리할 수 없음을 판매자에게 표시한다.

[0078] VEReq 메시지를 ACS(114)에서 수신한 후, ACS는 VEReq 메시지로부터 계좌 소지자 PAN을 수령하고, 이를 계좌 소지자 파일(118)에 대해 검증한다. ACS(114)는 그후 VERes 메시지를 포매팅한다. 성공적인 매치가 이루어질 경우, ACS는 PAN 등록의 상태를 "Y"로 설정하고, ACS가 내부적으로 PAN과 상관시킬 단일 이용 프록시 PAN을 생성하여, VEReq 메시지에 URL 필드를 배치한다. 성공적이지 못한 매치의 경우, ACS는 PAN 등록의 상태를 "N"으로 설정한다. 그후 라인(2a)에 의해 표시되는 바와 같이, ACS는 디렉토리 서버(128)를 통해 MPI에 VERes 메시지를 되돌려보낸다. VEReq 메시지가 ACS에 직접 전송되는 경우에, VERes 메시지는 라인(2b)로 표시되는 바와 같이 MPI에게로 직접 전송된다.

[0079] MPI(134) 내에서 디렉토리 서버(128)의 데이터를 캐쉬하는 것은, CRReq 와 CRRes 메시지 쌍을 이용함으로서 촉진될 수 있다. CRReq 메시지는 MPI로부터 디렉토리 서버에게로 전송되며, 참가하는 카드 범위들의 리스트를 요청하여, MPI가 해당 캐쉬를 업데이트하게 한다. CRRes 메시지는 참가 범위를 포함하는 응답이다.

[0080] 일부 실시예에서, 계좌 인증 시스템은 QueryAccountholderReq 및QueryAccountholderRes 메시지 쌍을 이용하여 계좌 소지자 클라이언트 장치가 인증 기능을 분배하였는 지를 확인한다. MPI는 QueryAccontholderReq 메시지를 포맷하고 계좌 소지자 클라이언트 장치(122)에 이러한 질의를 전송하여, 분배된 계좌 인증 계좌 소지자 모듈이 존재하는 지를 결정한다. QueryAccontholderReq 메시지의 전송은 라인(3)에 의해 도 7에 도시되어 있다. QueryAccontholderRes 메시지에 어떤 분배된 인증 옵션이 되돌아올 경우, MPI는 인증된 단계들을 수행하기 위해 계좌 소지자 클라이언트 소프트웨어와 직접 통신할 것이다. QueryAccontholderRes 메시지의 전송은 라인(4)에 의해 도 7에 도시된다. 추가적으로, QueryAccontholderReq와 QueryAccontholderRes 메시지를 이용함으로서, VEReq 및 VERes 메시지가 제거될 수 있다. 계좌 소지자 클라이언트 소프트웨어는 소프트웨어에 포함된 발급자의

ACS URL을 이용하여 전개될 수 있다. MPI는 QueryAccontholderReq와 QueryAccontholderRes 메시지를 먼저 완성할 것이다. 계좌 소지자 클라이언트 소프트웨어가 검출되면, PAReq 메시지는 VEReq 와 VERes 메시지를 수행할 필요없이 계좌 소지자 클라이언트 소프트웨어나 ACS에 전송될 수 있다.

[0081] VERes-Status 가 "Y" 값을 가지지 않을 경우, 계좌 승인 시스템을 이용하여 지불 거래를 처리할 수 없다는 사실이 판매자에게 통지된다. 그러나, VERes-Status가 "Y"의 값을 가질 경우, MPI(134)는 지불인 인증 요청 메시지(PAReq)를 포매팅할 것이다. MPI(134)는 PAReq 메시지를 계좌 소지자 클라이언트 장치 브라우저를 통해 발급자의 ACS 서버에 전송할 것이다(라인(5) 참조).

[0082] MPI가 PAReq 메시지를 발급자의 ACS에 전달한 후, ACS는 계좌 소지자에게 윈도를 디스플레이한다. 이 윈도는 발급자의 로고, 서비즈 조직 마크나 브랜드 로고, 판매자 명칭, 판매자 위치(URL), 총구매 금액 및 통화, 구매일, 카드 번호, 설치/AS 지불 기간, 주문 설명서나 주문 설명서에 대한 링크, 특별 판매 기간 및 조건이나 이 정보에 대한 링크, 개인별 보장 메시지(PAM), 계좌 소지자의 비밀번호에 대한 프람프트, 또는 그외 다른 종류의 인증 토큰 등등과 같은 아이템에 추가하여, 지불인 인증 응답(PARes)에 포함된 지불 세부사항들을 디스플레이한다.

[0083] ACS는 계좌 소지자에게 적절한 비밀번호를 입력할 것을 프람프트로 제시한다. ACS는 계좌 소지자 입력을 수신하여, 이를 계좌 소지자 파일(118)과 검증한다. 계좌 인증 시스템은 정확한 비밀번호를 입력하기 위해 다수의 실패 시도(가령, 3회 가능)를 허용할 것이다. 물론, 허용되는 시도 횟수는 가변적이다. 마지막 시도에 실패하면, 계좌 인증 시스템은 힌트 질문을 디스플레이할 것이다. 계좌 소지자는 정확한 힌트 질문 응답을 입력해야 한다. 계좌 소지자에 관련된 힌트 질문이 이때 디스플레이된다. 계좌 소지자에게는 정확한 응답을 입력할 기회가 한번 이상 제공된다. 계좌 소지자가 틀린 응답을 제공할 경우, 계좌 인증 시스템을 이용한 거래가 완료될 수 없음을 판매자가 통지받는다. 계좌 소지자가 정확한 응답을 제공할 경우, 거래는 비밀번호가 일치한 것처럼 취급되어야 한다. 한 계좌 번호에 대해 두개 이상의 입력사항이 존재할 경우, 다양한 계좌 소지자 성명이 드롭 다운 윈도에 디스플레이될 것이다. 계좌 소지자는 자신의 성명을 선택할 수 있다.

[0084] 비밀번호가 일치하면, ACS는 PARes 메시지를 발생시켜 디지털 방식으로 서명할 것이다. ACS는 SaveReceipt 메시지를 발생시켜 이를 인증 히스토리 서버(130)와 영수증 매니저(131)에 전달한다(라인(7) 참조). 라인(7a)으로 도시되는 바와 같이, SaveReceipt 메시지는 인증 히스토리 서버(130)로부터 발급자 승인 및 결제 시스템(138)으로 또한 전달될 수 있어서, 발급자가 지불 승인 요청을 지불인 인증 거래와 실시간으로 매치시킬 수 있다. SaveReceipt 메시지를 발급자의 승인 및 결제 시스템(138)에 전달함으로서, 발급자는 승인 요청이 인증된 구매에 대한 것인 지를 동시에 결정할 수 있다. ACS는 그후 서명된 PARes 메시지를 다시 MPI로 리디렉션시킬 것이다(라인(6) 참조).

[0085] 서명한 PARes 메시지가 MPI(134)로 다시 전송된 후, MPI(134)는 다시 활성화된다. 인증 상태가 "Y"일 경우, MPI(134)는 PARes 메시지를 검증 서버(136)에 전송한다. 검증 서버 기능이 MPI(134)에 의해 제공될 경우, MPI(134)는 PARes 메시지 시그너처를 검증하고, 시그너처 검증 결과를 리턴시킨다. 시그너처가 검증될 수 없을 경우, MPI(134)는 계좌 인증 시스템을 이용하여 거래를 처리할 수 없음을 판매자에게 통지할 것이다. 인증 상태가 "N"일 경우, 판매자는 추가 정보를 요청하는 프람프트를 계좌 소지자에게 전달하여야 하며, 다른 지불 카드나 다른 형태의 지불을 이용할 것을 계좌 소지자에게 요청하여야 한다. 또는, 이 지불 거래를 비-인증 지불 거래로 처리하여야 한다.

[0086] 획득자 도메인(106)이 검증 서버를 포함하는 경우, 비준 서버(136)는 PARes 메시지 상의 시그너처를 검증한다. 검증 서버(136)는 시그너처 검증의 결과를 MPI(134)에게로 리턴시킨다. 시그너처가 검증될 수 없는 경우, MPI는 계좌 인증 시스템을 이용하여 거래를 처리할 수 없음을 판매자에게 통지한다. 다른 한편, 시그너처가 검증될 경우, MPI는 인증된 지불 승인을 진행한다. PARes 메시지는 판매자로부터 그 획득자 지불 프로세서(140)에게로 또한 전달될 수 있다(라인(6a) 참조). PARes 메시지는 그후 획득자로부터 통신 네트워크(142)를 통해 발급자에게 전달될 수 있다. 따라서, 지불인 인증 결과는 표준 지불 승인 프로세스의 일부분으로 발급자에게 가용하게 이루어진다.

[0087] 이제 다양한 전송 채널에 관련된 보안 문제점들에 대해 설명할 것이다. 기본 라인으로서, 모든 전송 채널들은 128-비트 SSL을 이용하여 암호화되는 것이 바람직하다. 계좌 소지자와 판매자 간의 채널은 두개의 채널을 포함한다. 판매자는 계좌 소지자가, 서비스 조직에서 승인한 인증서 기관으로부터 얻은 SSL 인증서를 이용하여 지불 정보를 입력할 때 사용되는 연결을 보안화하여야 한다. 판매자는 서비스 조직에서 승인한 인증서 기관으로부터 얻은 SSL 인증서를 이용함으로서 계좌 소지자로부터 MPI까지 PARes 메시지를 전달하는 데 사용되는 연결을 또한

보안화하여야 한다.

[0088] 계좌 소지자와 ACS 간의 채널은 서비스 조직에 의해 승인된 인증서 기관으로부터 얻은 SSL 인증서를 이용함으로서 ACS에 의해 암호화되어야 한다. 이 채널은 두 용도로 사용된다. 첫번째는 MPI로부터 ACS까지 PAReq 메시지를 전송하는 것이고, 두번째는 ACS로부터 계좌 소지자에게로 서명된 PARes 메시지를 전송하는 것이다.

[0089] 계좌 소지자와 등록 서버간의 채널은 서비스 조직에 의해 승인된 인증서 기관으로부터 얻은 SSL 인증서를 이용하여 등록 서버에 의해 암호화되어야 한다. 이 채널은 계좌 소지자 등록 정보를 수용하는 데 사용된다.

[0090] 판매자와 디렉토리 서버 간의 채널과, 디렉토리 서버와 ACS 서버 간의 채널은, VEReq 및 VERes 메시지에 포함된 PAN 데이터와, VERes 메시지에 포함된 ACS URL 어드레스를 보호하기 위해, 서비스 조직에 의해 발급된 SSL 암호화 인증서를 통해 보안화되어야 한다.

[0091] ACS와 계좌 소지자 간의 채널은 계좌 소지자 간의 채널은, 계좌 소지자의 비빌번호에 대한 프람프트와, 계좌 소지자가 입력한 비밀번호를 보호하기 위해 암호화되어야 한다. 이 채널은 서비스 조직에 의해 승인된 인증서 기관으로부터 얻은 SSL 인증서로 보호되어야 한다.

[0092] 대부분의 거래에서, 지불 인증 요청 및 응답 메시지는 메시지 버전 번호, 판매자 식별자, 판매자 국가 코드, 주문 번호, 구매일, 구매 금액, 거래 상태, 구매 기간 및 조건 등등을 포함하는 필드들을 포함한다. 또한, QueryAccontholderRes 메시지는 메시지 버전 번호, 판매자 명칭, 주문 번호, 구매 일자, 구매 금액, 카드 유효기간, 그리고 거래 기타사항등등과 같은 필드들을 포함하는 것이 일반적이다. 이 메시지들은 XML 포맷을 취할 수 있다.

[0093] 비-구매 인증 거래에서, 지불 인증 요청, 지불 인증 응답, 그리고 QueryAccontholderRes 메시지는 메시지 확장 필드들을 포함할 수 있다. 당 분야에 잘 알려진 바와 같이, 메시지 확장 필드들은 확장자가 부착되는 메시지에 대해 추가 요소들을 규정하는 데이터 필드에 해당한다. 이 추가 요소들은 비-지불 거래같은 특정 거래들을 추가적으로 촉진시키는 데 사용될 수 있다.

[0094] **가치 부가 컴포넌트를 이용한 계좌 인증 프로세스**

[0095] 도 8은 가치-부가 양태를 포함하는 온라인 계좌 인증에 관련된 일례의 시스템 구조 및 일례의 메시지 흐름들을 도시한다. 가치-부가 양태는 계좌 인증 프로세스를 통해 수거된 정보를 가치-부가자와 공유하는 과정을 포함한다. 이러한 정보는 제시자에게 관련되며, 발급자나 제 3 신뢰 기관, 그리고 요청자에 의해 수거될 수 있다. 제시자 정보는 고도의 진실성을 가진 것으로 평가된다. 왜냐하면, 제시자(122)의 인증을 위한 기준으로 기능하기 때문이다. 제시자 정보는 거래 식별자와 함께 표시될 수 있다. 이 식별자는 이 정보가 본 발명의 인증 처리로부터 발원하였음을 알리며, 구체적 온라인 거래를 식별한다. 가치-부가 정보는 배송, 차후 판매, 보안사항 확인, 그리고 작업 흐름 관리, 등등과 같은 다양한 용도로 가치-부가자(196)에 의해 사용될 수 있다. 모든 관련자들은 제시자 정보를 공유함으로서 이익을 얻을 수 있고, 각각의 관련자는 이들이 서로 이익을 어떻게 공유할 수 있는지에 대하여 동의할 수 있다. 예를 들어, 요청자와 가치-부가자는 제시자 정보의 공유에 기초하여 추가 계약 사항에 동의할 수 있다.

[0096] 가치-부가자(196)에 제시자 정보를 전달하는 과정을 포함하는 인증 프로세스는 도 8을 참고하여 설명될 것이다. 도 8은 지불 거래에 기초하여 설명될 것이다. 이러한 설명에 이어, 도 8은 비-지불 거래에 기초하여 다시 설명될 것이다. 도 8은 도 7의 메시지들을 단순화된 형태로 제시한다.

[0097] 도 8의 계좌 인증 시스템 구조는 발급자 도메인(102), 상호운용 도메인(104), 획득자 도메인(106), 그리고, 가치-부가 도메인(107)을 포함한다. 발급자 도메인(102)은 제시자(122), ACS(114), 그리고 발급자(190)를 포함한다. 제시자(122)는 사람 제시자와 제시자 클라이언트 장치(가령, 컴퓨터 단말기나 이동형 컴퓨팅 장치)를 나타낸다. 발급자(190)는 제시자에게 지불 카드를 발급할 수 있는 카드-발급 은행에 해당한다. 상호운용 도메인(104)은 비자 디렉토리(128), 인증 히스토리 서버(130), 그리고 비자넷(194)을 포함한다. 비자 디렉토리(128)는 이 경우에 비자(Visa)에 의해 제어되는 디렉토리이다. 획득자 도메인(106)은 요청자(132), MPI(134), 그리고 획득 은행(192)을 포함한다. 요청자(132)는 다양한 종류의 관련자일 수 있다. 그러나 요청자(132)가 일반적으로 판매자이기 때문에 이 판매자라는 용어가 요청자 대신에 사용될 수 있다. 가치-부가 도메인(107)은 가치-부가자(196)와 가치-부가 제어 서버(198)를 포함한다.

[0098] 도 8의 지불 거래는 화살표 1-14를 통해 설명된다. 지불 거래는 제시자가 판매자 웹사이트를 브라우징할 때, 자신이 구매하고자 하는 아이템을 쇼핑카트에 추가할 때, 그리고 구매를 완료할 때, 단계 1에서 시작된다. 이때,

판매자(132)는 지불 거래를 진행하기 위해 필요한 데이터를 가지며, 이 데이터는 PAN, 유효기간, 그리고 어드레스 정보를 포함한다.

[0099] 단계 2에서, MPI(134)는 제시자의 메인 계좌 번호(그리고 사용자 장치 정보)를 비자 디렉토리 서버(128)에 전송하여, 제시자 PAN이 계좌 인증 시스템에 등록되어 있는 지를 확인한다. 이 프로세스는 판매자 결제 프로세스 중 제시자로부터 최종 "구매" 클릭 확인 후 발생한다. "구매" 클릭이 이루어진 후, 판매자의 소프트웨어는 MPI(134)를 호출하여 등록 확인 요청(VEReq) 메시지를 포매팅한다. MPI(134)는 비자 디렉토리 서버(128)와의 보안 연결을 현재 구현하고 있는 지를 결정한다. 보안 연결이 구축되지 않았을 경우, MPI(134)는 비자 디렉토리 서버(134)와의 SSL 연결을 구축한다. 판매자(132)가 SSL 클라이언트 인증서를 발급하였음을 비자 디렉토리 서버 구성이 표시할 경우, 비자 디렉토리 서버(128)는 판매자(132)에게 SSL 세션의 구축 중 SSL 클라이언트 인증서를 제시할 것을 요구할 것이다. 보안 연결이 구축된 후, MPI(134)는 VEReq 메시지를 비자 디렉토리 서버(128)에 전달한다. 다양한 실시예에서, "구매" 클릭 확인은 다양한 구매 주문 확인 프로세스들을 이용하여 완성될 수 있다.

[0100] VEReq 메시지는, 인증 과정 중 전송된 그외 다른 메시지와 함께, 가치-부가 자와 제시자 정보를 공유하는 과정이 온라인 인증 프로세스에 포함된다는 사실을 표시하는 인디케이터를 포함할 수 있다.

[0101] 단계 3에서, 비자 디렉토리 서버(128)가 PAAN이 참가 카드 범위 내에 있다고 결정하면, 비자 디렉토리 서버(128)는 적절한 ACS(가령, ACS(114))에 질의하여, PAN에 대한 인증이 가용한 지를 결정한다. 이 과정은 비자 디렉토리 서버(128)가MPI(134)로부터 VEReq 메시지를 수신한 후 발생한다. 비자 디렉토리 서버(128)가 PAN이 참가 카드 범위 내에 있음을 확인하기 위해, 비자 디렉토리 서버(128)는 VEReq 메시지의 구문(syntax)을 검증하고, 검증에 실패할 경우 에러 신호(Error)를 리턴시킨다. 비자 디렉토리 서버(128)는 VEReq 메시지 데이터를 검증하여, 소정 요건에 부합함을 보장한다. 먼저, 획득자 BIN은 참가 획득자를 표현하여야 한다. 두번째로, 판매자 ID는 획득자 BIN에 의해 식별된 획득자의 참가 판매자를 나타내야 한다. 세번째로, 획득자의 비자 영역이 계좌 인증 서비스에 대한 판매자 비밀번호를 요구할 경우, 이 비밀번호에 대한 값이 수신되어 있어야 하고 비밀번호는 획득자 BIN 및 판매자 ID의 조합에 대해 유효하여야 한다. 이중 어떤 요건에 부합하지 않을 경우, 비자 디렉토리 서버(128)는 등록 확인 응답(VERes)을 포매팅하고, 이 VERes는 "N"으로 설정된 PAN 인증 가용과, 무효 요청 메시지를 포함한다. VERes가 계좌 식별자, ACS URL, 그리고 지불 프로토콜의 데이터 필드들을 포함하는 것은 아니다. 비자 디렉토리 서버(128)가 VERes 메시지를 MPI(134)에 리턴시킨 후, 지불 거래는 다양한 방식으로 진행될 수 있다. 예를 들어, 지불 거래는 성공적으로 종료될 수 있고, 또는 지불 거래가 비-인증 거래로 진행될 수 있고, 또는, 제시자가 다른 계좌 번호를 이용하려 시도할 수 있다.

[0102] 비자 디렉토리 서버(128)는 VEReq 메시지에 수신된 제시자 PAN을 포함하는 카드 범위를 명시하는 레코드를 검색한다. 제시자 PAN이 발견되지 않을 경우, 비자 디렉토리 서버(128)는 "N"으로 설정된 PAN 인증 가용을 포함하는 VERes 메시지를 포매팅한다. 이 VERes 메시지는 계좌 식별자, ACS URL, 지불 프로토콜, 그리고 무효 요청의 데이터 필드들을 포함하지 않는다. 비자 디렉토리 서버(128)는 VERes 메시지를 MPI(134)에 리턴시키고, 계좌 인증은 다시 가능한 정지점에 도달한다(아래 설명됨).

[0103] 제시자 PAN이 비자 디렉토리 서버(128)에 없을 경우, 비자 디렉토리 서버(128)는 적절한 ACS와의 보안 연결을 현재 구성하고 있는 지 여부를 결정한다. 비자 디렉토리 서버(128)는 보안 연결이 아직 구축되지 않았을 경우 ACS와의 SSL 연결을 구축한다. 비자 디렉토리 서버(128)의 SSL 클라이언트 인증서와, ACS의 서버 인증서는 SSL 세션의 구축 중 제시되고 검증되어야 한다. 시도한 제 1 URL이 가용하지 않을 경우, 각각의 뒤이은 URL 값(제공될 경우에 한함)이 시도될 것이다. 비자 디렉토리 서버(128)는 각 ACS에 대해 부가적으로 설정된 최대 네개의 대안의 URL에 연결하려 시도할 수 있다. 비자 디렉토리 서버(128)가 각 시도에서 URL과 연결될 수 없을 경우, 비자 디렉토리 서버(128)는 "N"으로 설정된 PAN 인증 가용을 포함하는 VERes 메시지를 포매팅한다. 하지만 VERes 메시지는 계좌 식별자, ACS URL, 지불 프로토콜, 또는 무효 요청의 데이터 필드들을 포함하지 않는다. 그 후 비자 디렉토리 서버(128)는 VERes 메시지를 MPI(134)에 리턴시키고, 계좌 인증 프로세스를 가능한 정지점으로 전달한다.

[0104] URL과의 성공적 연결이 이루어진 후, 비자 디렉토리 서버(128)는 VEReq 메시지로부터 비밀번호 필드들을 제거하고, 이 메시지를 ACS URL에 전달한다.

[0105] 단계 4에서, ACS(114)는 PAN에 대한 인증이 가용한 지를 결정하고, 그후, 이 결정사항을 비자 디렉토리 서버(128)에 표시한다. 이 프로세스는 ACS가 VEReq 메시지를 비자 디렉토리 서버(128)를 통해 수신한 후에 발생한다. ACS(114)는 VERqeq 메시지의 구문(syntax)을 검증하고, 검증에 실패할 경우 에러 신호(Error)를 리턴

시킨다. 지불 거래를 인증할 수 없을 때, 그 대신에 인증 시도의 증거를 제공하는 것이 가능할 수도 있다. ACS(114)는 VEReq 메시지로부터의 제시자 PAN을 이용하여, ACS(114) 내에 위치한 제시자 데이터베이스에 질의하여, 제시자가 등록되어 있는 지를 결정한다. PAN이 발견되지 않을 경우, ACS(114)는 "N"으로 설정된 PAN 인증 가용을 포함하는 VERes 메시지를 포매팅하며, 이때, 상기 VERes 메시지는 계좌 식별자, ACS URL, 지불 프로토콜, 그리고 무효 요청의 데이터 필드들을 포함하지 않는다. ACS(114)는 그후 VERes 메시지를 비자 디렉토리 서버(128)에 전달한다.

[0106] 단계 5에서, 비자 디렉토리 서버(128)는 ACS(114)의 결정사항을 MPI(134)에 전달한다. 비자 디렉토리 서버(128)의 관점으로부터, 이 프로세스는 비자 디렉토리 서버(128)가 VEReq 메시지를 ACS URL에 전달한다. ACS(114)의 관점으로부터, 이 프로세스는 ACS(114)가 VERes 메시지를 비자 디렉토리 서버(128)에 전달한 후 발생한다.

[0107] 비자 디렉토리 서버(128)는 VERes 메시지를 판독하며, 이 메시지는 대응하는 VERes 나 Error 를 포함한다. 비자 디렉토리 서버(128)는 VEres 메시지의 구문을 검증하고, 검증에 실패할 경우 ACS(114)에 에러 신호를 리턴시킨다. ACS로부터 수신한 메시지가 구문론적으로 정확할 경우, 비자 디렉토리 서버(128)는 VERes 나 Error를 MPI(134)에 전달한다. ACS로부터 수신한 메시지가 구문론적으로 정확하지 않을 경우, 비자 디렉토리 서버(128)는 "N"으로 설정된 PAN 인증 가용을 포함하는 VERes 메시지를 포매팅하고, 이 VERes 메시지는 계좌 식별자, ACS URL, 지불 프로토콜, 또는 무효 요청을 포함하지 않는다. 비자 디렉토리 서버(128)는 VERes 메시지를 MPI(132)에 리턴시키고, 계좌 인증 프로세스를 종료시킨다. MPI(134)의 관점에서 볼 때, 이 프로세스는 MPI(134)가 VEReq 메시지를 비자 디렉토리 서버(128)에 전달한 직후에 발생한다. 비자 디렉토리 서버(128)의 관점에서 볼 때, 이는 비자 디렉토리 서버가 VERes 메시지를 MPI에 전달한 직후 발생한다. MPI(134)는 응답을 판독하고, 이 응답은 대응하는 VERes 나 Error를 포함한다. Error 메시지가 수신되면, 계좌 인증 프로세스가 중지된다.

[0108] 상술한 바와 같은 여러가지 이유로 계좌 인증이 종료될 때, 판매자는 결제 과정으로부터 가용 정보를 이용하여 정상 지불 승인을 진행할 수 있다. 이 경우에, 판매자 지불 시스템은 인증되지 않은 전자 상거래로 거래를 처리하여야 한다. 이는 본 출원의 범위를 벗어난다. 전자 상거래 식별자는 결제 과정의 특성과 인증 결과에 대응하는 값으로 설정되어야 한다. 판매자가 결제 과정 중 제시자에 의해 선택되는 계좌를 이용하여 인증된 거래를 처리할 수 없을 경우, 판매자는 대안의 계좌를 선택하는 옵션을 소비자에게 제시하거나 거래를 포기할 수 있다. 대안의 계좌가 선택되면, 인증 과정이 반복될 수 있다.

[0109] 대안의 실시예에서, 각 지불 거래(단계 2-5)에 대한 계좌 인증 시스템에 제시자의 참가를 확인하기 위해 비자 디렉토리 서버에 질의할 필요성은, 비자 디렉토리 서버의 콘텐트들을, 판매자(132)의 로컬 캐쉬 메모리 장치에 복제함으로서 방지할 수 있다. 이 기능이 사용될 경우, 판매자(132)는 계좌가 등록된 범위의 일부분인 지를 캐쉬로부터 즉시 결정할 수 있다. 판매자(132)의 로컬 캐쉬를 이용하는 이 대안의 기술에서는, MPI(134)가 카드 범위 요청(CRReq) 메시지를 포매팅하고, 이 를 비자 디렉토리 서버(128)에 전송한다. 이것이 첫번째로 캐쉬가 로딩되는 경우일 때(또는 캐쉬가 넘칠 경우나 리로딩될 필요가 있을 경우), 시리얼 번호 요소가 CRReq에 포함되지 않으며, 이는 비자 디렉토리 서버(128)가 참가 카드 범위들의 전체 리스트를 리턴시키는 결과를 도출한다. 그렇지 않을 경우, MPI(134)는 가장 최근에 처리된 CRRes로부터 시리얼 번호를 포함하여야 하며, 이는 비자 디렉토리 서버가 이전 CRRes 이후 변화만을 리턴시키는 결과를 도출할 것이다. 시리얼 번호는 비자 디렉토리 서버(128)의 카드 범위 데이터베이스의 현 상태를 규정하는 값이다. 비자 디렉토리 서버(128)는 MPI(134)에 이 시리얼 번호를 제공한다. 리턴시키는 특정 비자 디렉토리 서버에만 이 특정 값이 의미가 있다.

[0110] 비자 디렉토리 서버(128)는 CRReq의 구문을 검증하고, 검증에 실패할 경우 Error를 리턴시킨다. 비자 디렉토리 서버(128)는 참가 범위를 포함하는 카드 범위 응답(CRRes)을 포매팅하고 이를 MPI(134)에 전송한다. 비자 디렉토리 서버(128)는 이 응답에서 시리얼 번호를 포함한다. MPI(134)는 다음날의 CRReq 메시지와 함께 포함되도록 이 값을 유지하여야 한다. MPI(134)는 CRRes의 구문을 검증하고, 검증에 실패할 경우 비자 디렉토리 서버(128)에 Error를 전송하여야 한다. MPI(134)는 로컬 캐쉬를 업데이트한다. 리스트는 리턴되는 순서로 처리되어야 하며, 액션 요소에 의해 표시되는 바와 같이 범위들이 추가되거나 삭제된다. CRRes가 시리얼 번호에 대하여 에러 조건을 표시할 경우, MPI는 캐쉬를 클리어하여야 하며, 시리얼 번호없이 CRReq를 제출하여야 한다.

[0111] 제시자의 PAN에 대하여 인증이 가용할 경우, MPI(134)는 제시자 클라이언트 장치(122)를 통해 ACS(114)에 지불인 인증 요청(PAReq)을 전송한다. 단계 6은 제시자 클라이언트 장치(122)에 전달되는 PAReq 메시지를 나타낸다. 이 프로세스는 MPI(134)가 비자 디렉토리 서버(128)로부터 VERes 메시지를 수신한 직후 발생한다. MPI(134)는 VERes의 구문을 검증하고, 검증에 실패할 경우 Error를 비자 디렉토리 서버에 전송하여야 한다. MPI(134)는 VERes의 계좌 식별자를 포함하는 PAReq 메시지를 포매팅한다.

[0112] 본 인증 프로세스의 실시예는 판매자(132)와 발급자(190) 간의 제시자 관련 정보 공유 과정을 포함한다. 발급자(190)와 판매자(132) 각각은 단일 거래 또는 다중 거래에 대해 제시자에 관한 넓은 범위의 정보를 수집할 수 있다. 이러한 정보는 제시자의 구매 습관에 관한 정보를 포함할 수 있다. 이러한 정보는 다양한 관련자, 가령, 판매자(132), 발급자(190), 그리고 가치-부가자(196)에게 유용할 수 있다. 이러한 고객 정보는 PAReq 및 PARes 메시지들 내에 이 정보를 포함시킴으로서 인증 과정 중 판매자(132)와 발급자(190) 간에 공유될 수 있다. 따라서, 단계 6에서, 판매자(132)는 제시자(122)에 관련된 정보를 PAReq 메시지 내에 포함할 수 있다.

[0113] MPI(134)는 다음의 필드들을 포함하는 형식을 구성한다. 즉, PAReq, TermURL(최종 응답이 전달되어야할 판매자 URL), 그리고 MD(Merchant Data) 필드들을 포함하는 형식을 구성한다. MD 필드는 판매자에게 리턴되어야할 판매자 상태 데이터를 저장한다. 이 필드는 판매자 시스템이 세션 상태를 취급하는 여러 다른 방식을 수용하는 데 사용한다. 판매자 시스템이 추가적인 도움없이 최종 포스트를 원 쇼핑 세션과 상관시킬 수 있을 경우, MD 필드는 빈 상태가 될 수 있다. 판매자 시스템이 주어진 쇼핑 세션에 대한 상태를 유지하지 않을 경우, MD는 이 세션을 계속하기 위해 판매자에게 필요한 데이터를 모두 운반할 수 있다. 이 필드의 콘텐트가 판매자에 따라 변하기 때문에, ACS는 콘텐트에 관한 가정없이 불변으로 이를 유지하여야 한다.

[0114] MPI(134)는, 제시자 브라우저가 이 형식을 ACS에 전달하게 함으로서, VERes에서 수신한 ACS URL에 제시자 브라우저를 통해 PAReq를 전달한다. 모든 연결사항들은 제시자 브라우저를 수용하기 위한 HTTP들이다.

[0115] 단계 7은 제시자 클라이언트 장치(122)로부터 ACS(114)까지 전송되는 PAReq 메시지를 나타낸다. 이 프로세스는 MPI(134)로부터 PAReq 를 포함하는 포스트를 수ACS(114)가 수신한 후 발생한다. 다음의 설명은 제시자 인증이 비밀번호를 이용하여 수행되는 경우에 적용된다. 칩 카드에 대한 적용예에 의존하는 등의 다른 방법들이 사용될 수도 있다. ACS(114)는 PAReq 메시지를 검증하고, 검증에 실패할 경우 Error를 리턴시킨다. 비준에 실패할 경우, ACS(114)는 "N"으로 설정된 거래 상태와 무효 요청을 가진 PARes 메시지를 포매팅한다.

[0116] 단계 8에서, ACS는 PAN에 적용할 수 있는 프로세스들을 이용하여 제시자를 인증한다. 이 프로세스들은 발급자(190)와 제시자(122) 간에 앞서 구축된 비밀번호나 PIN을 요청하는 기술들과, 제시자에게 데이터 챌린지를 제시하는 기술들을 포함한다. 데이터 챌린지는 가령, 제시자의 신원이나 제시자 클라이언트 장치(122)의 신원을 인증하기 위해 제시자 클라이언트 장치(122)에게 특정 데이터 응답을 제공할 것을 ACS(114)가 요청하는 과정을 포함할 수 있다. 한 예에서, 제시자(122)를 인증하는 특정 암호문을 클라이언트 제시자 장치에게 생성하도록 ACS(114)가 요청할 수 있다. 대안으로, ACS(114)는 승인 시도의 증거를 생성할 수 있다. ACS(114)는 적절한 값으로 PARes 메시지를 포매팅하고, 디지털 시그너처를 이 응답 메시지에 적용한다. ACS(114)는 비밀번호, 데이터 응답, 또는 암호문을, ACS 내에 위치한 제시자 데이터베이스에 대해 검증한다. ACS(114)는 각각의 온라인 거래에 대해 CAVV와 같은 거래 식별자를 또한 생성한다. 특정 온라인 거래에 관련되면서, 거래 식별자는 판매자(132)와 발급자(190) 간에 공유되는 고객 정보에 또한 관련된다.

[0117] 단계 9에서, ACS(114)는 제시자 클라이언트 장치(122)에 PARes 메시지를 리턴시킨다. 제시자(122)와 거래 식별자에 관한, 발급자(190)에 의해 유지되는 정보는 PARes 메시지 내에 포함시킴으로서 판매자에게 전송될 수 있다.

[0118] ACS(114)는 PARes 및 MD 필드들을 포함하는 형식을 구성한다. ACS(114)는, 제시자 브라우저로 하여금 이 형식을 MPI에 전달하게 함으로서, 서명된 PARes를 제시자의 브라우저를 통해 판매자의 URL에 전달한다. 이 과정에서, 팝업이 닫히고 제어는 판매자의 브라우저 윈도로 리턴된다.

[0119] 이 시점에서, ACS(114)는 선택한 데이터를 인증 히스토리 서버(130)에 또한 전달할 수 있다. 예를 들어, ACS(114)는 인증 히스토리 서버(130)에 전달되는 지불인 인증 거래(PATransReq)를 포매팅한다.

[0120] 인증 과정 중 유지되고 전달되는 제시자 정보는 판매자(132)와 발급자(190)에 의해 저장될 수 있다. 각각의 관련자는 고객 정보 전체, 또는 그 일부분을 저장할 수 있다. 대안으로, 고객 정보의 전부 또는 일부분이 인증 서버(130) 내에 저장될 수 있다.

[0121] 단계 10에서, 제시자 클라이언트 장치는 PARes 메시지를 MPI(134)에 전달한다.

[0122] 단계 11에서, MPI(134)는 ACS(114)에 의해 PARes 메시지에 구성된 디지털 시그너처를 검증한다. 디지털 시그너처의 검증은 ACS(114) 자체에 의해 실행될 수도 있고, PARes 메시지를 별도의 검증 서버에 전달함으로서 수행될 수도 있다. 검증 프로세스는 비자 루트 인증서를 이용하여 PARes 시그너처를 검증한다. 별도의 검증 서버를 이용하여 구현될 경우, MPI(134)는 PARes를 검증 프로세스로 전송하고, 검증 프로세스는 비자 루트 인증서를 이용

하여 PARes의 시그너처를 검증하며, 검증 프로세스는 시그너처 검증의 결과를 MPI에 리턴시킨다.

[0123] 단계 12에서, 판매자(132)는 획득자(192)와의 승인 교환을 진행한다.

[0124] 단계 13에서, 판매자(132)는 소유하고 있는 고객 정보를 평하기 위해 소정의 기준 세트를 이용한다. 고객 정보 세트가 이 기준을 만족시킬 경우, 고객 정보와 거래 식별자는 가치-부가자(196)에게 전달된다. 이 기준은 가치-부가자(196)가 고객 정보를 수신하고자 하는 지를 결정할 다양한 문제점들을 해결할 것이다. 이러한 기준은 인증 프로세스가 어떻게 동작하는 지에 관한 세부적인 예들을 통해 상세하게 설명될 것이다.

[0125] 단계 14에서, 가치-부가자(196)는 가치-부가 제어 서버(198)같은 데이터베이스에 고객 정보와 거래 식별자를 저장한다.

[0126] 단계 15는 가치-부가 제어 서버(198)와 인증 히스토리 서버(130) 간의 통신을 표현한다. 이 통신은 다양한 용도로 구현될 수 있다. 이러한 용도들은 가령, 판매자(132)와 가치-부가자(196) 간의 거래 완료, 분쟁 해결, 데이터 검색 등을 포함한다.

[0127] 본 발명의 다양한 가치-부가 실시예에 대한 추가적 세부사항들이 다음 단락에서 논의될 것이다.

[0128] **가치부가자로서의 배송 회사**

[0129] 도 8에 도시되는 인증 시스템 및 프로세스는 배송자(200a)라 불리는 배송 회사가 가치-부가자(196)인 경우에 해당하는 실시예에 따라 설명될 것이다. 본 실시예에서, 제시자(122)는 제품을 판매자(132)로부터 구매하며, 이 제품은 제시자의 주거지나 그외 다른 우편 주소로 배송되어야한다. 배송자에게 전달되는 제시자(고객) 정보에 따라, 배송자(196)가 상품을 제시자(122)에게 배송할 수 있다. 상술한 바와 같이, 고객 정보는 인증 프로세스로부터 발원하기 때문에 높은 진실성과 풍부성을 가진다. 따라서, 이 정보의 가치는 판매자(132)와 가치-부가자(196)가 거래에 진입하기 위한 기초수단으로 기능한다. 거래 종류의 범위는 크게 변할 수 있다. 한 예에서, 배송자(196)는 배송자(196)가 제품을 저렴한 비용으로 판매자(132)와 제시자(122)에게 배송하고자 하는 정도로 고객 정보의 진실성과 풍부성에 의존한다. 이는 제시자(122)가 패키지를 다시 판매자에게 배달할 것을 전혀 요청한 바 없음을 고객 정보가 표시하기 때문에 해당하는 경우일 수 있다. 추가적으로, 판매자(132)는, 제시자(122)에 의한 반송 요청에 관련된 비용이나 책임으로부터 배송자(196)를 분리시키기에 편한 정도까지 이러한 고객 정보에 의존할 수 있다.

[0130] 인증 및 가치-부가 프로세스는 도 8에 도시된 단계들에 의해 표현되는 바와 같이 인증 프로세스를 시작한다. 단계 6과 7에서, 판매자(132)는 발급자(190)에게 전달된 PAReq 메시지에서 유지되는 고객 정보를 포함할 수 있다. 단계 9와 10에서, 발급자(190)는 판매자(132)에게 전달된 PARes 메시지에서 발급자(190)가 관리하는 고객 정보를 포함할 수 있다. 발급자(190)는 거래 식별자를 또한 발생시키며, 이 거래 식별자는 특정 온라인 거래 및 고객 정보에 관련되어 있다.

[0131] 고객 정보는 가령, 1) 성명, 우편 주소, 이메일 주소, 전화 번호, 그리고 팩스 번호같은 고객 연락 정보, 2) 완납 및 체납 횟수같은 고객 지불 내역, 그리고 3) 선호 배송 방법, 반송 요청없이 이루어진 배송 횟수, 그리고 정시 배송 횟수와 같은 배송 내역을 포함할 수 있다. 고객 정보는 발급자(190)와 판매자(132)에 의해 수거될 수 있는 임의의 종류의 정보를 포함할 수 있다.

[0132] 또한 단계 9에서, 고객 정보는 판매자(132)와 발급자(190) 중 하나, 또는 둘 모두에 의해 저장된다. 대안으로, 고객 정보가 인증 히스토리 서버(130)같은 데이터베이스에 저장된다.

[0133] 단계 13에서, 판매자(132)는 고객 정보를 소정의 기준에 대해 평가하여, 이러한 정보가 배송자(196)에게 전달되어야 하는 지를 결정한다. 이 기준은 형식을 갖추어 형성되어, 배송자(196)가 어려움없이 임무를 완수할 수 있다는 등의 내용을 고객 정보가 표시할 경우 고객 정보가 배송자(196)에게 전달된다. 이 기준은 고객에 대한 가용 히스토리 정보를 검사함으로서 고객에 대한 배송 위험을 분석하는 것을 돕는다. 이러한 기준의 예로는, 1) 고객이 해당 판매자와 몇번 이상 구매 거래를 행하였는가? 2) 배송 주소가 미국같은 특정 국가 내의 주소인가? 3) 고객이 구매에 대한 비용 지불에 실패한 적이 있는가? 4) 요청한 고객이 배송 물품을 반송시킨 적이 있는가? 5) 새 고객인가? 6) 이 거래가 금액 한도를 넘었는가? 7) 배송 주소가 확인되었는가? 8) 배송될 지역(국가)이 위험 국가인가 안전한 국가인가? 등등이 있다. 판매자(132)나 배송자(196), 또는 둘 모두가 이 기준을 설정할 수 있다.

[0134] 고객 정보가 판매자의 기준을 만족시키면, 고객 정보와 거래 식별자가 배송자(196)에게 전달된다. 발급자(190)가 거래 식별자를 발생시키기 때문에, 배송자(196)는 정보의 진실성을 확신한다. 고객 정보에 의존하여, 배송자

(196)는 제품을 고객(122)에게 배송하며, 배송이 위험없이 그리고 추가비용없이 이루어질 수 있다는 소정의 보장 레벨이 보장된다. 고객 정보가 제공하는 배송자(196)에 대한 어려움없는 거래의 보장으로 인해, 판매자(132)와 배송자(196)는 서로에게 추가 고려사항을 제공할 수 있다. 가령, 배송자(196)는 판매자(132)와 고객(122)에게 저렴한 비용으로 제품을 기꺼이 배송할 수 있다. 또한, 판매자(132)는 배송자(196) 대신에 배송을 행하는 위험의 일부분을 가정할 수 있고, 또는 판매자(132)가 배송 비용을 배송자(196)와 부분적으로 함께 하는 데 동의할 수 있다.

[0135] 단계 14에서, 배송자(196)는 가치-부가 제어 서버(198)에, 거래 식별자와 함께 거래 정보를 저장한다. 배송자(196)는 배송 라벨에 인쇄된 거래 식별자를 이용하여 고객(122)에게 제품을 배송할 수 있다.

[0136] 단계 15는 다양한 용도로 거래 식별자를 관련 고객 정보와 함께 불러오는 과정을 포함한다. 이러한 용도는 가령, 판매자(132)와 가치-부가자(196) 간의 거래 완수, 분쟁 해결, 그리고 데이터 검색 등을 포함한다. 거래 식별자는 세부 거래사항에 해당하며, 따라서, 각 거래의 히스토리를 검색하는 데 유용하다. 이에 따라, 발급자(190), 판매자(132), 그리고 가치-부가자(196)가 각 거래에 관한 정보를 확인할 수 있다. 본 발명은 고객이 구매를 행하지 않았다고 변명하는 경우와 같은 구매 사기 행위로부터 판매자들을 보호할 수 있다. 본 발명은 또한, 배송받지 않았다고 고객이 주장하는 경우와 같은 배송 사기 행위로부터 배송 회사들을 보호할 수 있다.

[0137] 고객 정보는 푸시(push) 상황 또는 풀(pull) 상황에서 인증 히스토리 서버(AHS)(130)로부터 불러들여질 수 있다. 푸시 상황은 이벤트 발생이 예상되고 따라서 고객 정보가 수신자, 즉, 가치-부가자(196)에게 밀려 제공되는 경우에 해당한다. "풀" 상황은 불규칙적으로 발생하는 이벤트의 경우에 수신자에 의해 고객 정보가 요청되어 전달되는 경우에 해당한다. 예를 들어, 고객 정보는 AHS(130) 내에 저장된 고객 정보 및 거래 식별자에 대해 확인을 필요로하는 분쟁이 발생하는 경우에만 발급될 수 있다.

[0138] 고객 정보와 거래 식별자는 AHS(130)로부터 불러들여져 거래를 완료하게 된다. 이 거래들은 고객 정보의 공유에 기초하며, 각 당사자들이 동의하는 추가 항목들을 포함한다. 이 거래들은 가치-부가 거래라고 불린다. 왜냐하면, 다양한 관련자들이 이익을 얻을 수 있는 추가 거래에 대한 기본사항으로 이러한 고객 정보가 기능하기 때문이다. 예를 들어, 가치-부가 거래에 대한 관련자는 추가적인 사업 기회를 얻을 수 있고, 상품이나 서비스에 대한 경쟁력있는 비용을 얻을 수 있으며, 보다 이로운 계약 항목들을 얻을 수 있다. 일부 거래들은 소정의 항목들에 따라 배송자(196)와 판매자(132) 간의 상품 배송에 관한 협정을 포함한다. 이러한 항목들은 판매자(132)에게 부과될 저렴한 배송 비용을 포함할 수 있고, 판매자(132)에 의한 위험 및 책임 보증을 포함할 수 있다. 고객 정보와 거래 식별자를 확인함으로서, 판매자(132)와 배송자(196)는 배송자(196)가 소정의 배송사항을 구현하였음을 확인할 수 있다. 그후, 예를 들어, 판매자(132)는 할인된 배송 대금을 배송자(196)에게 지불할 수 있다. 고객 정보와 거래 식별자를 불러들여 거래를 완료하는 것은, 이러한 정보를 불러들이는 것이 이러한 거래를 완수하기 위한 정규적 프로세스일 때, 푸시 거래에 해당한다.

[0139] 고객 정보와 거래 식별자는 분행 해결 상황에서도 유용하다. 부쟁은 판매자(132), 고객(122), 그리고 배송자(196) 간에 발생할 수 있다. 분쟁들은 AHS(130)로부터의 정보를 이용하여 거래에 관한 사실들을 입증함으로서 해결될 수 있다. 분쟁이 발생하면, 고객 정보가 거래 식별자들이 이러한 정보가 저장된 위치로부터 풀(pull)된다. 판매자와 배송자 간의 분쟁은 각 관련자 간의 가치-부가 거래의 충족에 관련된 사항일 수 있다. 예를 들어, 배송 서비스에 대한 지불에 대한 불일치가 발생할 경우, 판매자(132)는 이러한 정보를 이용하여, 협정에 따라 할인 배송 비용으로의 배송이 배송자(196)에 의해 이루어졌음을 입증할 수 있다. 또는, 배송이 제대로 이루어지지 않았거나 배송 중 상품이 손상되었다고 고객이 불만을 토로할 때, 배송자(196)는 이러한 거래에 대한 책임이 판매자(132)에 의해 보증되었음을 입증할 수 있다. 일부 사례에서, 책임은 발급자(190)에 의해 보증될 수 있다.

[0140] 고객 정보와 거래 식별자들은 데이터 검색용으로 판매자(132), 발급자(190), 그리고 배송자(196) 각각에 의해 사용될 수 있다. 각 관련자들은 그들의 거래를 통해, 특정 고객에 관한 정보를 얻을 수 있다. 이 고객 정보들이 분석되어 이 고객들의 습관 및 취향을 결정할 수 있다. 이러한 습관 및 취향은 판매자(132), 배송자(196), 그리고 발급자(190) 각각의 마케팅 용도에 맞게 사용될 수 있다. 판매자(132)는 고객의 습관 및 취향에 관한 정보를 이용하여, 고객에 대한 차후 판매 및 마케팅 전략을 결정할 수 있다. 배송자(196)는 위험 분석 등을 위해 이러한 정보를 이용하여, 문제를 일으키지 않으면서 고객에게 물품을 배송할 가능성을 결정할 수 있다. 발급자(190)는 이러한 정보를 이용하여, 고객에게 차후 계좌를 발급함에 있어서의 위험 레벨을 결정할 수 있고, 신용 레벨이 증가하여야 하는 지를 결정할 수 있다.

[0141] 추가적으로, 이 정보는 다른 관련자들의 특성을 결정하기 위해 임의의 관련자에 의해 이용될 수 있다. 예를 들어, 판매자와 협정을 체결하는 것이 현명한 사업적 결정인 지를 배송자가 결정할 수 있다. 이러한 분석을 수행

하기 위해, 고객 정보를 분석하여, 판매자의 부정행위 히스토리, 환불 히스토리, 해당 고객들에 대한 빈번한 배송 국가, 등등을 결정할 수 있다. 이러한 정보가 특정 판매자와의 거래가 배송에 용이하다고 나타날 경우, 배송자는 이러한 판매자들과의 사업을 적극적으로 추진할 것을 결정할 수 있다. 판매자들은 이러한 데이터를 분석하여, 그들의 배송 필요성을 특정 배송자를 이용하여 만족시킬 수 있는 지를 결정할 수 있다. 예를 들어, 고객 데이터는 어떤 배송자들이 높은 배송 성공률 및 정시 배송 실적을 가지고 있는 지를 보여줄 수 있다.

[0142] 판매자(132)나 발급자(190), 또는 둘 모두가 고객 정보를 가지고 있는 실시예에서, 고객 정보와 거래 식별자는 각 실체로부터 불러들여질 수 있다.

[0143] 발명의 배송 구현을 위한 대안의 실시예에서, 판매자(132)는 특정 거래에 대한 고객 데이터 및 거래 식별자의 사본들을 여러 배송자에게 보낼 수 있다. 고객 데이터가 인증 프로세스로부터의 발원 원인으로 인해 높은 수준의 진실성을 가지기 때문에, 각각의 배송자(196)는 이 거래에 대해 배송을 실행하는 데 관심을 가질 수 있다. 고객 정보의 진실성이 거래에 관한 정보의 인증(가령, 배송 주소)을 보장하기 때문에, 각 배송자(196)들이 관심을 가질 수 있다. 더욱 중요한 점은, 고객 정보가 판매자의 기준을 통과한 후 배송자(196)에게 전달되었기 때문에, 각 배송자(196)는 배송 거래에서 문제점에 직면할 가능성이 낮다는 것이다. 이에 대한 대안으로서, 배송자(196)는 특정 거래에 관련된 위험 레벨을 알 수 있다. 더우기, 판매자(132)나 발급자(190)가 이 거래로 인한 위험 비용을 보증하는 데 동의하였을 수 있기 때문에, 배송자(196)가 이 거래를 위해 제품을 배송하는 데 관심을 가질 수 있다. 이 거래 및 고객에 대해 이만큼 알 경우, 각 배송자(196)는 배송 가격에 대해 판매자(132)에게 입찰할 수 있다. 판매자(132)는 그후 제품 배송을 위해 배송자(196)들 중 하나를 선택할 수 있다.

[0144] **가치-부가자로서 후속 판매자**

[0145] 도 8에 도시되는 인증 및 정보 공유 프로세스의 대안의 실시예에서, 가치-부가자(196)는 후속 판매자(follow-on merchant)(196)이다. 본 실시예에서, 본 발명은 후속 판매자(196)에 대해 수입 기회를 증가시키고, 일부 경우에 판매자(132) 및 발급자(190)의 경우에도 수입 기회를 증가시킨다. 후속 판매자(196)는 판매자(132)로부터 고객 정보 및 거래 식별자를 수신하고, 이 정보를 이용하여 자체 상품 및 서비스를 고객(122)에게 판매한다. 후속 판매자(196)는 임의의 종류의 상품이나 서비스를 제공할 수 있다. 하지만, 이 상품이나 서비스는 판매자(132)가 판매한 상품이나 서비스에 어떤 방식으로든 관련될 가능성이 높다. 고객(122)이 판매자(132)와의 거래 품목에 관련된 사항을 구매할 가능성이 높기 때문에 판매자(132)로부터의 고객 정보는 가치가 있다. 판매자(132)와 후속 판매자(196)는 고객 정보에 기초하여 서로 다양한 협정을 맺을 수 있다.

[0146] 이 프로세스는 도 8에 제시된 바와 같은 단계들에 따라 인증 프로세스를 시작한다. 단계 6, 7, 9, 10에서, 판매자(132)와 후속 판매자(196)는 앞서 언급한 바와 같이 PAReq 및 PARes 메시지에 고객(122)에 관한 정보를 포함시킴으로서 고객 정보를 공유한다. 또한, 발급자(190)는 거래 식별자를 발생시키는 데, 이 거래 식별자는 특정 온라인 거래 및 고객 정보와 관련된다. 고객 정보 및 거래 식별자는 발급자(190), 판매자(132) 각각에 의해 저장되며, 또는 인증 히스토리 서버(130)같은 단일 데이터베이스 내에 저장된다.

[0147] 단계 13에서, 판매자(132)는 고객 정보와 거래 식별자를 후속 판매자(196)에게 전달해야 할지를 결정하기 위해 고객 정보를 평가한다. 이러한 고객 정보는 고객이 소비하는 평균 대금, 고객이 소비하는 최대 금액, 고객이 어느 회사 제품을 구매하는 지, 고객이 언제 구매하는 지, 고객이 무엇에 대해 구매를 하는 지, 고객의 성별, 고객에 관한 인구학적 정보 등등에 관련된다. 고객의 특성에 관한 분석 범위가 매우 크다는 것을 이해하여야 한다. 고객 정보가 이 기준을 통과하면, 그 정보는 단계 13에서 후속 판매자(196)에게로 전달된다.

[0148] 고객 정보 및 거래 식별자를 수신한 후, 단계 14에서, 후속 판매자(196)는 고객 데이터 및 거래 식별자를 데이터베이스(가령, 가치 부가 제어 서버(198))에 저장한다. 이때, 후속 판매자(196)는 고객 정보를 이용하여 특정 고객에 집중된 판매 전략을 활용할 수 있다. 고객 정보는 후속 판매자(196)에게 여러 고객에 대한 판매 전략을 어떻게 편성할 것인 지를 알려줄 수 있다. 예를 들어, 고객이 특정 거래에 대해 소비하는 금액에 관한 정보는, 고객(122)이 관심있어하는 상품이나 서비스의 금액 수준을 후속 판매자(196)에게 알려줄 것이다. 또한, 판매자(132)에 의해 판매된 상품이나 서비스에 관한 정보는, 고객(122)이 구매하고자 하는 관련 상품이나 서비스의 종류를 후속 판매자(196)에게 알려줄 것이다. 예를 들어, 고객이 판매자(132)로부터 CD 플레이어를 구매하였을 경우, 후속 판매자(196)는 소정의 CD들을 고객(122)에게 판매할 수 있을 것이다. 이러한 거래는 "보완형 상품(complementary goods)" 거래라 불릴 수 있다. 예를 들어, 다른 보완형 상품으로는 코들리스 드릴(cordless drill)과 충전형 배터리, 면도기와 면도날, 잔디깍는 기계와 비료 등을 들 수 있다.

[0149] 고객 정보의 수신은 후속 판매자(196)로부터의 협약에 따른 조건형일 수 있다. 따라서, 고객 정보로부터 발생하

는 후속 판매자(196)에 의한 판매자의 판매액의 일부분을 판매자(132)나 발급자(190)에게 제공하는 방식을 취할 수 있다. 이러한 판매 및 이와 유사한 속성의 판매는 "업-셀(up-sells)" 또는 "크로스-셀(cross-sells)"이라 불린다. 고객 정보의 수신은 판매자(132)와 후속 판매자(196) 간의 다양한 협정에 따라 조건형으로 구성될 수 있다. 상술한 바와 같이, 고객 정보는 후속 판매자(196)에게 가치있다. 왜냐하면, 이는 내용적으로 풍부하고 고도의 진실성을 가지기 때문이다. 고객 정보는 판매자(132)나 발급자(190)가 이를 수집하기 때문에 그 내용이 풍부하다. 판매자(132)와 발급자(190) 각각은 고객에 관한 소정의 정보 종류들을 수집함에 있어 각자 독자적 위치에 있다. 마지막으로, 고객 정보는 단계 1-12에 의해 설명된 인증 프로세스를 통과하였기 때문에 고도의 진실성을 가진다.

[0150] 단계 15는, 판매자(132)와 후속 판매자(196) 간의 거래 완수, 분쟁 해결, 데이터 검색 등등과 같은 다양한 용도로 관련 고객 정보와 함께 거래 식별자를 불러들이는 과정들을 포함한다. 단계 15는 판매자(132)와 후속 판매자(196) 간의 협정을 완성하는 것을 요구받을 수 있다. 이에 따르면, 후속 판매 대금의 일부분을 판매자(132)에게 보내기 전에 후속 판매자(196)에 의한 판매 금액에 관한 정보가 확인된다. 예를 들어, 고객 정보와 거래 식별자는 판매자(132)나 후속 판매자(196)에 의해 불러들여져, 후속 판매가 고객 정보의 결과였는 지를 확인한다. 그 후, 이러한 확인에 따라, 대금이 판매자(132)에게 전달된다. 이러한 상황에서, 고객 정보는 협정에 따라 사업의 정규적 코스로 판매자에게 푸시(push)될 수 있고, 또는 이견이 해결되어야할 때만 고객 정보가 풀(pull)될 수 있다.

[0151] 분쟁 해결의 경우에, 고객 정보와 거래 식별자가 판매자(132), 후속 판매자(196), 또는 고객(122) 간의 분쟁의 경우에 불러들여진다. 분쟁은 판매자(132)와 후속 판매자(196) 간의 협정이 위반되었을 때 발생할 수 있다. 다시, 판매자(132)가 고객 정보를 후속 판매자(196)에게 전송하는 것에 동의할 때, 후속 판매자(196)는 고객 정보로부터 발생하는 임의의 판매를 공유할 것을 요구받을 수 있다. 그후, 고객 정보는 후속 판매자(196)로부터 판매자(132)로 인한 지불에 관한 분쟁이 발생할 때 풀(pull)될 수 있다. 이러한 관련자들은 고객 정보와 거래 식별자들을 매칭시켜서, 후속 판매자(196)에 의한 소정의 판매가 고객 정보에 기반하여 완료되었는 지를 확인할 수 있다.

[0152] 고객 정보에 관한 일부 협정은 발급자(190)에 관한 사항을 포함할 수 있다. 즉, 발급자(190)가 후속 판매자(196)에 의해 구현된 임의의 판매액의 일부를 기대할 수 있다.

[0153] 고객 정보는 데이터 검색용으로 사용될 수도 있다. 이 경우에, 발급자(190), 판매자(132), 그리고 후속 판매자(196) 각각이 서로 고객에 관한 지식을 얻을 수 있다. 고객 정보에 관한 이들의 분석은 서로간의 차후 거래가 유익할 수 있는 지를 관련자들에게 알릴 수 있다.

[0154] **가치 부가자로서 다양한 관련자**

[0155] 계좌 인증 및 가치-부가 시스템의 대안의 실시예에서, 다양한 종류의 관련자들은 고객(122), 판매자(132), 그리고 가치-부가자(196)의 역할을 취할 수 있다. 고객(122)과 판매자(132)의 역할은 온라인으로 서로 상호작용하는 임의의 관련자일 수 있으며, 이때, 판매자(132)가 고객의 신원 인증을 요구한다. 여러 상거래 상황을 상상해볼 수 있다. 즉, 판매자(132)가 고객(122)에게 어떤 종류의 상품이나 서비스를 판매하는 경우를 상상해볼 수 있다. 그러나, 비-상거래적인 상황도 여러가지 상상해볼 수 있다. 일부 상황들은 운전면허, 낚시 면허, 건축 면허, 사회보장 지불, 그리고 학교 학급 등록 등과 같은 사항을 위한 온라인 등록을 포함할 수 있다. 한 관련자(가령, 판매자(132))가 또다른 관련자(가령, 고객(122))의 신원 인증을 요청할 것임을 이해하여야 한다.

[0156] 판매자(132)같은 신원 인증자에 의해 평가되는 기준은, 다양한 종류의 가치-부가자(196)에 관련될 수 있다. 이 기준은 가치-부가자(196)가 고객(122)같은 관련자에 관한 정보를 수신하고 자 하는 지에 관련될 수 있다. 이때, 이 고객(122)같은 관련자의 신원은 본 발명에 의해 인증된 것이다. 단계 13에서 전송된 고객 정보는 여러 다른 가치-부가자(196) 각각에 관련될 수 있다. 고객(122)이 운전 면허에 응시할 경우, 고객 정보는 고객의 운전 기록, 차량, 주행로, 그리고 공통적인 목적지 등에 관련될 수 있다. 가치-부가자(196)는 운전에 관련된 고객(122)에게 상품이나 서비스를 판매하고자 하는 임의의 관련자일 수 있다. 가령, 가치-부가자(196)가 매연 검사 회로, 정비소, 또는 자동차보험 회사일 수 있다. 또다른 실시예에서, 가치-부가자(196)가 운전에 관련된 사항을 전혀 판매하지 않을 수 있다. 그러나, 가치부가자(196)는 고객(122)이 관심있어하는 상품이나 서비스를 여전히 판매할 수 있다. 예를 들어, 고객이 어떤 종류의 차량을 몰고 있고 따라서 고객(122)이 어떤 조류의 상품이나 서비스에 관심있어 한다는 것을 고객 정보가 표시할 수 있다. 고객 정보로부터 다양한 종류의 관계들이 추출될 수 있고, 따라서, 이 고객 정보는 가치-부가자(196)에게 유용할 수 있다.

[0157] 고객(122)이 낚시 면허를 땄을 때, 가치-부가자(196)는 낚시 장비 가게, 여행사, 또는 의류 점포일 수 있다. 또한, 가치-부가자(196)는 낚시에 직접 관련된 회사일 필요가 없다. 가치-부가자(196)에 전달된 고객 정보는 낚시에 대한 고객의 선호도에 관련될 수 있다. 판매자(132)에 의해 평가된 기준은 어떤 종류의 낚시 장비를 고객(122)이 선호하는 지, 어떤 종류의 낚시를 고객(122)이 선호하는 지, 고객(122)이 낚시하고픈 장소가 어디인지, 고객(122)이 어떤 종류의 의복을 입는 지 등등을 결정할 수 있다.

[0158] 고객 정보가 가치-부가자에게 작업흐름 용도로 전달될 수도 있다. 가령, 고객(122)이 판매자(132)로부터 건축허가나 면허에 응시한 후, 다음 레벨의 승인을 위해 또다른 정부 기관에 고객 정보를 전송할 필요가 있을 수 있다. 예를 들어, 화재 대리인은 건축 중 화재 안전 검사를 하기 위해 고객 정보를 수신할 필요가 있다.

[0159] 판매자(132)와 가치-부가자(196)는 고객 정보와 거래 식별자들의 공유에 기초하여 서로 가치-부가 관계에 진입할 수도 있다.

[0160] 일부 실시예에서, 판매자(132)는 고객 정보와 거래 식별자를 여러 가치-부가자에게 제공할 수 있다. 판매자(132)는 가치-부가자(196)의 각 종류에 대한 동일한 기준 세트나 서로 다른 기준 세트를 평가할 수 있다. 각각의 가치-부가자(196)는 서로 평행하게 또는 순서대로 작업의 수행을 진행한다. 가치-부가자(196)가 실시간으로 작업을 실행하여, 고객(122)이 각 가치-부가자(196)로부터 즉시 통지를 수신할 수 있고, 또는 작업이 오프-라인 방식으로 수행될 수도 있다.

[0161] 상술한 바와 같이, 단계 15는 판매자(132), 가치-부가자(196), 그리고 발급자(190) 간의 협정을 완성하기 위한 다양한 용도로 사용될 수 있다.

[0162] **가치 부가자로서 보안 조직**

[0163] 본 발명의 일부 실시예는 국가 보안과 같은 보안 용도로 사용될 수 있다. 이러한 실시예에서, 가치-부가자(196)는 보안 관련사항에 대한 정보(데이터)를 리뷰하기 위한 임무를 부여받은 정부 기관이나 조직일 수 있다. 판매자(132)는 고객(122)과 온라인으로 거래를 수행하는, 임의의 상거래적, 비-상거래적, 정부기관형, 또는 비-정부기관형 기관일 수 있다. 예를 들어, 판매자는 항공 예약 회사, 하드웨어 점포, 화학제품 공급사, 또는 비행 훈련 학교일 수 있다. 고객 정보의 일부 또는 모든 전달은 프라이버시 및 시민권에 관한 법률에 의해 조절될 수 있다.

[0164] 판매자(132)는 보안 관련 기준에 대해 고객 정보를 평가하고, 이러한 기준에 부합할 때 고객 식별자와 함께 이 정보를 가치-부가자(196)에게 전달한다. 예를 들어, 이 기준은 고객의 구매 품목, 면허 등록, 여행 목적지, 여행 빈도, 그리고 그외 다른 보안 관련 사항일 수 있다. 고객 정보와 거래 식별자를 수신하면, 가치-부가자(196)는 그 감독 작업을 수행할 수 있다.

[0165] 거래 식별자는 고객 정보를 문서화하여 보안 실적 사항이 정확하게 검색될 수 있도록 하는 데 유용하다. 이는 가령, 보안 프로토콜의 정부 지시 조사의 경우에 유용할 수 있다. 구체적으로, 판매자(132)는 보안 프로토콜을 정확하게 따름을 입증할 것을 요구받을 수 있다. 일부 상황에서, 판매자(132)는 법원이 지시한 소환장에 응답하고 있다. 고객 정보와 거래 식별자는 인증 히스토리 서버(130)로부터 푸시되거나 풀된다(단계 150). 단계 15는 판매자(132), 보고자, 그리고 가치-부가자(196) 간의 협정을 완료하는 데 사용될 수도 있다. 예를 들어, 판매자(132)는 유용한 정보를 보고하기 위해 신용이나 인지도를 수신할 수 있다. 이러한 신용은 고객 정보에 관한 소스, 날짜, 그리고 그외 다른 세부사항들을 증명하기 위해 거래 식별자를 이용한 후 수신할 수 있다. 단계 15는 보안 관련사항의 데이터 검색을 위해 인증 히스토리 서버(130)로부터 데이터를 "풀"하기 위해 다양한 관련자들에 의해 사용될 수 있다. 고객 정보가 발급자(190) 및 판매자(132)로부터 수집되기 때문에, 고객 정보는 그 양이 풍부할 것이며, 감독 용도로 매우 유용할 수 있다.

[0166] 일부 실시예에서, 가치-부가자(196) 및 판매자(132)는 실시간으로 서로와 통신하여, 가치-부가자(196)가 고객 정보를 수신한 직후 판매자(132)에게 메시지를 전송할 수 있게 한다.이러한 방식으로, 즉각적인 액션이 취하여져서 불필요한 상황을 방지하거나 해결할 수 있다.

[0167] **선호되는 시스템 네트워크**

[0168] 도 9는 발명의 한 실시예를 구현하기에 적합한 통신 네트워크(800)를 도시한다. 본 발명은 적절한 통신 네트워크를 이용할 수 있고, 아래 설명되는 여러 다른 하드웨어, 여러 다른 소프트웨어, 그리고 여러 다른 프로토콜에 관계할 수 있다. 아래 설명되는 네트워크는 도 2의 통신 네트워크(126)의 선호되는 실시예이다. 네트워크(800)는 은행 카드, 여행 및 엔터테인먼트 카드, 그리고 그외 다른 프라이빗 라벨 카드를 이용하는 구매 및 현금 거

래를 지원하는 전역 통신 네트워크일 수 있다. 이 네트워크는 다른 네트워크에 대한 ATM 거래, 종이 수표를 이용하는 거래, 스마트 카드를 이용하는 거래, 그리고 그외 다른 금융 회사를 이용하는 거래를 또한 지원한다.

[0169] 이 거래들은 네트워크의 승인, 삭제 및 청산 서비스를 통해 처리된다. 승인은 구매가 완료되거나 현금이 전달되기 전에 발급자가 판매를 허락하거나 거절할 때에 해당한다. 삭제는 고객 계좌로 전송하기 위해 획득자로부터 발급자에게 거래가 전달될 때에 해당한다. 청산은 삭제된 모든 거래들에 대한 각 멤버의 알짜 금융 위치를 연산하고 결정하는 프로세스이다. 실제 대금 교환은 별도의 프로세스이다.

[0170] 거래는 이중 메시지나 단일 메시지 거래로 승인되고, 삭제되고, 청산될 수 있다. 이중 메시지 거래는 두번 전달된다. 첫번째는, 승인 결정에 필요한 정보만으로, 두번째는, 삭제 및 청산에 필요한 추가 정보로 전달된다. 단일 메시지 거래는 승인을 위해 한번 전달되며, 삭제 및 청산 정보도 포함한다. 일반적으로, 승인, 삭제, 그리고 청산은 모두 온라인 방식으로 이루어진다.

[0171] 통신 네트워크(800)의 주 구성요소들은 인터체인지 센터(802), 액세스 포인트(804, 806), 그리고 처리 센터(808, 810)들을 포함한다. 그외 다른 실체, 가령, 어음 수신 은행, 요청자 승인 기관 등은 액세스 포인트를 통해 네트워크에 연결될 수 있다. 인터체인지 센터는 세계 어디에나 위치할 수 있는 데이터 처리 센터이다. 한 실시예에서, 미국에 두개, 영국과 일본에 한개씩 위치한다. 각 인터체인지 센터는 네트워크 거래 처리를 수행하는 컴퓨터 시스템을 구비하고 있다. 인터체인지 센터는 네트워크의 통신 설비들에 대한 제어 지점으로 기능하며, 이는 IBM SNA 프로토콜에 기초한 고속 리스 라인이나 위성 연결을 포함한다. 원격 실체에 인터체인지 센터들을 연결하는 라인(820, 822)들이 IBM SNA-LUO 통신 프로토콜에 기초하여 전용 고대역폭 전화 회로나 위성 연결을 이용하는 것이 바람직하다. 메시지들은 ISO 8583 표준의 적절한 구현을 이용하여 이 라인들을 통해 전달된다.

[0172] 액세스 포인트(804, 806)는 처리 센터의 호스트 컴퓨터와 인터체인지 센터 사이에서 인터페이싱을 행하는 처리 센터에 위치하는 소형 컴퓨터 시스템인 것이 일반적이다. 액세스 포인트는 거래의 승인, 삭제, 그리고 청산을 지원하는 인터체인지 센터와 호스트 간의 메시지 및 파일들의 전송을 촉진한다. 링크(826, 828)들은 센터 내의 로컬 링크들에 해당하며, 센터에 의해 선호되는 독점 메시지 포맷을 이용한다.

[0173] 데이터 처리 센터(획득자, 발급자, 또는 그외 다른 실체 내에 위치함)는 판매자 및 사업 위치를 지원하는 처리 시스템으로서, 고객 데이터 및 대금 청구 시스템을 관리한다. 각각의 처리 센터가 한개나 두개의 인터체인지 센터에 링크되는 것이 바람직하다. 프로세서들은 가장 가까운 인터체인지 센터에 연결되며, 네트워크가 인터럽션을 맞이할 경우, 네트워크는 2차 인터체인지 센터로 거래를 자동적으로 루팅시킨다. 각각의 인터체인지 센터는 다른 모든 인터체인지 센터에 링크되어 있다. 이러한 링크에 의해 처리 센터들이 한개 이상의 인터체인지 센터들을 통해 서로 통신할 수 있다. 또한, 처리 센터들은 인터체인지 센터를 통해 다른 프로그램들의 네트워크에 액세스할 수 있다. 더우기, 네트워크는 모든 링크들이 다중 백업을 가지는 것을 보장한다. 네트워크의 한 포인트로부터 또다른 포인트로의 연결은 고정 링크를 이용하지 않는다. 대신에, 인터체인지 센터는 주어진 전송 시간에 가장 가능한 경로를 선택한다. 오류 링크 주변의 리루팅(rerouting)은 자동적으로 이루어진다.

[0174] 도 10은 온라인 및 오프라인 거래 처리를 제공하기 위해 인터체인지 센터 내에 포함되는 시스템(840)들을 도시한다. 이중 메시지 거래의 경우에, 승인 시스템(842)은 승인을 제공한다. 시스템(842)은 온라인 및 오프라인 기능을 지원하고, 그 파일은 내부 시스템 표, 고객 데이터베이스, 그리고 판매자 중앙 파일을 포함한다. 시스템(842)의 온라인 기능들은 이중 메시지 승인 처리를 지원한다. 이러한 처리는 루팅, 제시자 및 카드 확인 및 독립형 처리, 그리고 파일 유지등과 같은 다른 기능을 포함한다. 오프라인 기능은 리포팅, 대금청구, 그리고 복원 게시 발생 등을 포함한다. 리포팅은, 승인 리포트, 예외 파일 및 충고 파일 리포트, POS리포트, 그리고 대금청구 리포트들을 포함한다. 시스템(842)으로부터 시스템(846)으로의 브리지는 시스템(842)을 이용하는 멤버들이 시스템(846)을 이용하는 멤버들과 통신할 수 있게 하고 SMS 게이트웨이를 이용하여 외부 네트워크에 액세스할 수 있게 한다.

[0175] 삭제 및 청산 시스템(844)은 앞서 승인된 이중 메시지 거래를 삭제하고 청산한다. 전역 원칙 하에 주 6일 동작함으로서, 시스템(844)은 금융 및 비-금융 정보를 수집하고 멤버들 간에 리포트를 분배한다. 이는 수수료, 요금, 그리고 청산 비용 전체를 또한 연산하며, 조정을 돕기 위해 리포트를 생성한다. 시스템(844) 처리 센터와 시스템(846) 처리 센터 간에 인터체인지가 브리지에 의해 형성된다.

[0176] 단일 메시지 시스템(846)은 풀 금융 거래(full finantial transactions)를 처리한다. 시스템(846)은 이중 메시지 승인 및 삭제 거래를 또한 처리할 수 있고, 브리지를 이용하여 시스템(842)과 통신하며 외부 네트워크에 액세스한다. 시스템(846)은 비자(Visa), 플러스 인터링크(Plus Interlink), 그리고 그외 다른 카드 거래를 처리한

다. SMS 파일들은 시스템 액세스 및 처리를 제어하는 내부 시스템 표와, 제시자 데이터베이스를 포함한다. 제시자 데이터베이스는 PIN 확인 및 독립 처리 승인을 위해 사용되는 제시자 데이터의 파일들을 포함한다. 시스템(846)은 실시간 제시자 거래 처리를 실행하고, 승인 및 풀 금융 거래(full finantial transactions)를 위한 예외 처리를 실행한다. 시스템(846)은 조정 및 청산 합계를 또한 누적한다. 시스템(846)은 오프-라인 기능들은 청산 및 대금 전달 요청들을 처리하고, 청산 및 활동 보고를 제공한다. 청산 서비스(848)는 Interlink를 포함한 시스템(844, 846)의 청산 기능들을 모든 제품 및 서비스들에 대한 단일 서비스로 조정한다. 삭제는 시스템(844) 및 시스템(846)에 의해 개별적으로 계속 수행된다.

[0177] 도 11은 통신 네트워크(800)의 구성요소들의 또다른 도면이다. 일체형 지불 시스템(850)은 모든 온라인 거래 및 금융 요청 거래를 처리하기 위한 메인 시스템이다. 시스템(850)은 이중 메시지와 단일 메시지 처리를 모두 보고한다. 두 경우 모두, 청산이 개별적으로 이루어진다. 세개의 메인 소프트웨어 구성요소들은 공통 인터페이스 평션(852), 승인 시스템(842), 그리고 단일 메시지 시스템(846)에 해당한다.

[0178] 공통 인터페이스 평션(852)은 인터체인지 센터에서 수신한 각각의 메시지에 대해 요구되는 처리를 결정한다. 이는 메시지의 소스(시스템(842, 844, 846)), 처리 요청의 종류, 그리고 처리 네트워크에 기초하여, 적절한 루팅을 선택한다. 이 구성요소는 초기 메시지 편집을 실행하고, 메시지를 분석하며, 콘텐트가 기본 메시지 구성 규정에 부합함을 보장한다. 공통 인터페이스 평션(852)은 메시지들을 해당 시스템(842)이나 시스템(846) 목적지로 전달한다.

[0179] **컴퓨터 시스템 실시예**

[0180] 도 12A와 12B는 본 발명의 실시예들을 구현하기에 적합한 컴퓨터 시스템(900)을 도시한다. 도 12A는 컴퓨터 시스템의 한가지 가능한 물리적 형태를 도시한다. 물론, 컴퓨터 시스템은 집적 회로, 인쇄 회로 보드(PCB), 그리고 소형 핸드헬드 장치로부터 거래한 수퍼 컴퓨터까지 다양한 물리적 형태를 취할 수 있다. 컴퓨터 시스템(900)은 모니터(902), 디스플레이(904), 하우징(906), 디스크 드라이브(908), 키보드(910), 그리고 마우스(912)를 포함한다. 디스크(914)는 컴퓨터 시스템(900) 내외로 데이터를 전송하는 데 사용되는 컴퓨터 판독형 매체이다.

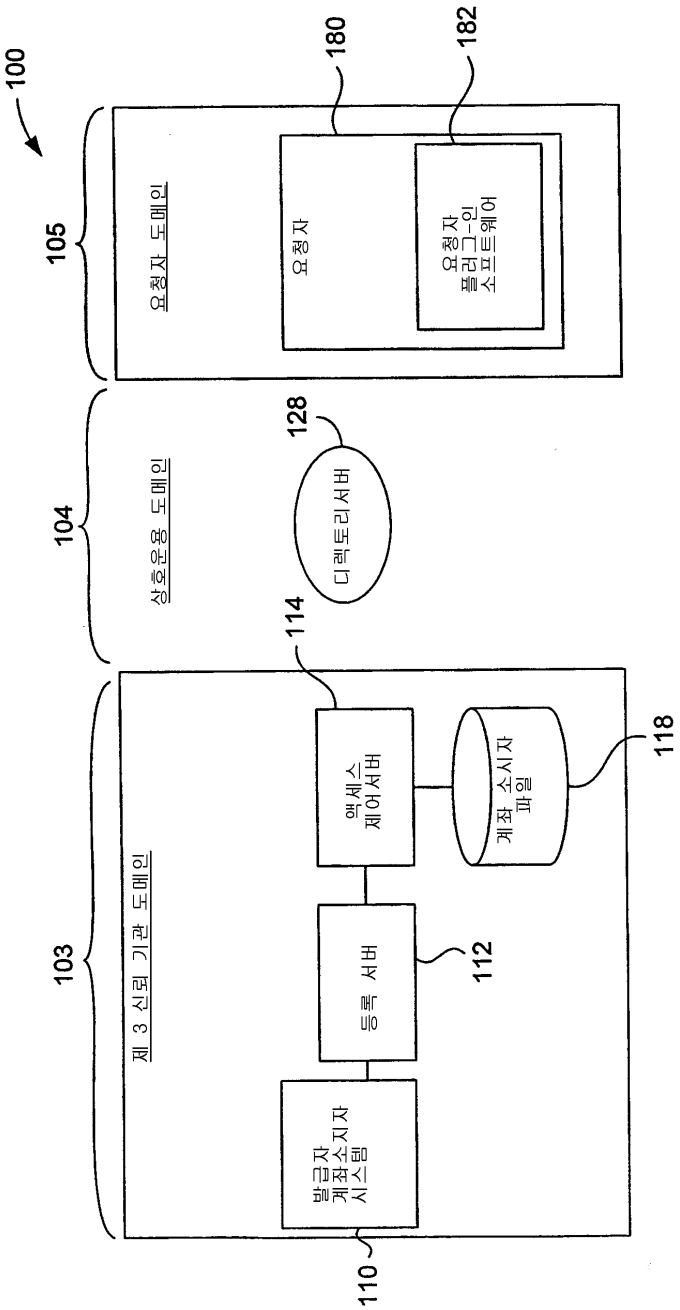
[0181] 도 12B는 컴퓨터 시스템(900)의 블록도표의 한 예다. 다양한 서브시스템들이 시스템 버스(920)에 부착된다. 프로세서(922)(CPU라고도 불림)는 메모리(924)를 포함하는 기억 장치에 연결된다. 메모리(924)는 RAM과 ROM을 포함한다. 당 분야에 잘 알려진 바와 같이, ROM은 데이터 및 명령을 CPU에 일방향으로만 전달하는 기능을 하며, RAM은 데이터 및 명령들을 양방향으로 전달하는 데 사용된다. 이 두 종류의 메모리들은 아래 설명되는 컴퓨터-판독형 매체에 해당할 수 있다. 고정 디스크(926)가 CPU(922)에 양방향으로 또한 연결된다. 고정 디스크는 추가적인 데이터 기억 용량을 제공하며, 아래 설명되는 컴퓨터 판독형 매체에 해당할 수 있다. 고정 디스크(926)는 프로그램, 데이터, 등을 저장하는 데 사용되며, 주기억장치에 비해 일반적으로 느린 보조 기억 장치(가령, 하드 디스크)에 해당한다. 고정 디스크(926) 내에 보유된 정보는 메모리(924)에서 가상 메모리로 표준 방식으로 통합될 수 있다. 탈착식 디스크(914)가 또한 아래 설명되는 컴퓨터 판독형 매체에 해당할 수 있다.

[0182] CPU(922)는 디스플레이(904), 키보드(910), 마우스(912), 그리고 스피커(930)같은 다양한 입/출력 장치들에 또한 연결된다. 일반적으로, 입/출력 장치는, 비디오 디스플레이, 트랙볼, 마우스, 키보드, 마이크로폰, 터치식 디스플레이, 트랜스듀서 카드 리더기, 자기식 또는 페이퍼식 테이프 리더기, 태블릿, 스타일러스, 음성 또는 수기 인식기, 생체 정보 리더기, 또는 그외 다른 컴퓨터에 해당한다. CPU(922)는 네트워크 인터페이스(940)를 이용하여 또다른 컴퓨터나 통신 네트워크에 연결될 수 있다. 이러한 네트워크 인터페이스를 이용하여, CPU가 네트워크로부터 정보를 수신할 수 있고, 또는, 상술한 방법 단계들을 수행하는 과정에서 네트워크에 정보를 출력할 수 있다. 더우기, 본 발명의 방법 실시예들은 CPU(922)에서만 전적으로 실행될 수도 있고, 처리과정의 일부분을 공유하는 원격 CPU와 연계하여 인터넷같은 네트워크를 통해 실행될 수도 있다.

[0183] 추가적으로, 본 발명의 실시예들은 컴퓨터에 의해 구현되는 다양한 동작들을 실행하는 컴퓨터 코드들을 저장한 컴퓨터-판독형 매체를 구비한 컴퓨터 기억 프로덕트에 추가적으로 관련된다. 이 매체 및 컴퓨터 코드는 본 발명을 위해 특별히 고안되고 설계된 것일 수도 있고, 컴퓨터 소프트웨어 분야에서 통상의 지식을 가진 자에게 쉽게 다가올 수 있는 잘 알려진 사항일 수도 있다. 컴퓨터 판독형 매체의 예로는, 하드 디스크, 플라피 디스크, 자기 테이프같은 자기식 매체, CD-ROM, 홀로그래픽 장치같은 광학식 매체, 플롭티컬 디스크같은 자기-광학식 매체, ASIC, PLD(프로그래머블 로직 디바이스), ROM 및 RAM같은 프로그램 코드를 저장 및 실행하도록 특별하게 고안된 하드웨어 장치들이 있다. 컴퓨터 코드의 예로는, 컴파일러에 의해 생성되는 머신 코드, 그리고, 인터프리터를 이용하여 컴퓨터에 의해 실행되는 하이 레벨 코드를 지닌 파일들이 있다.

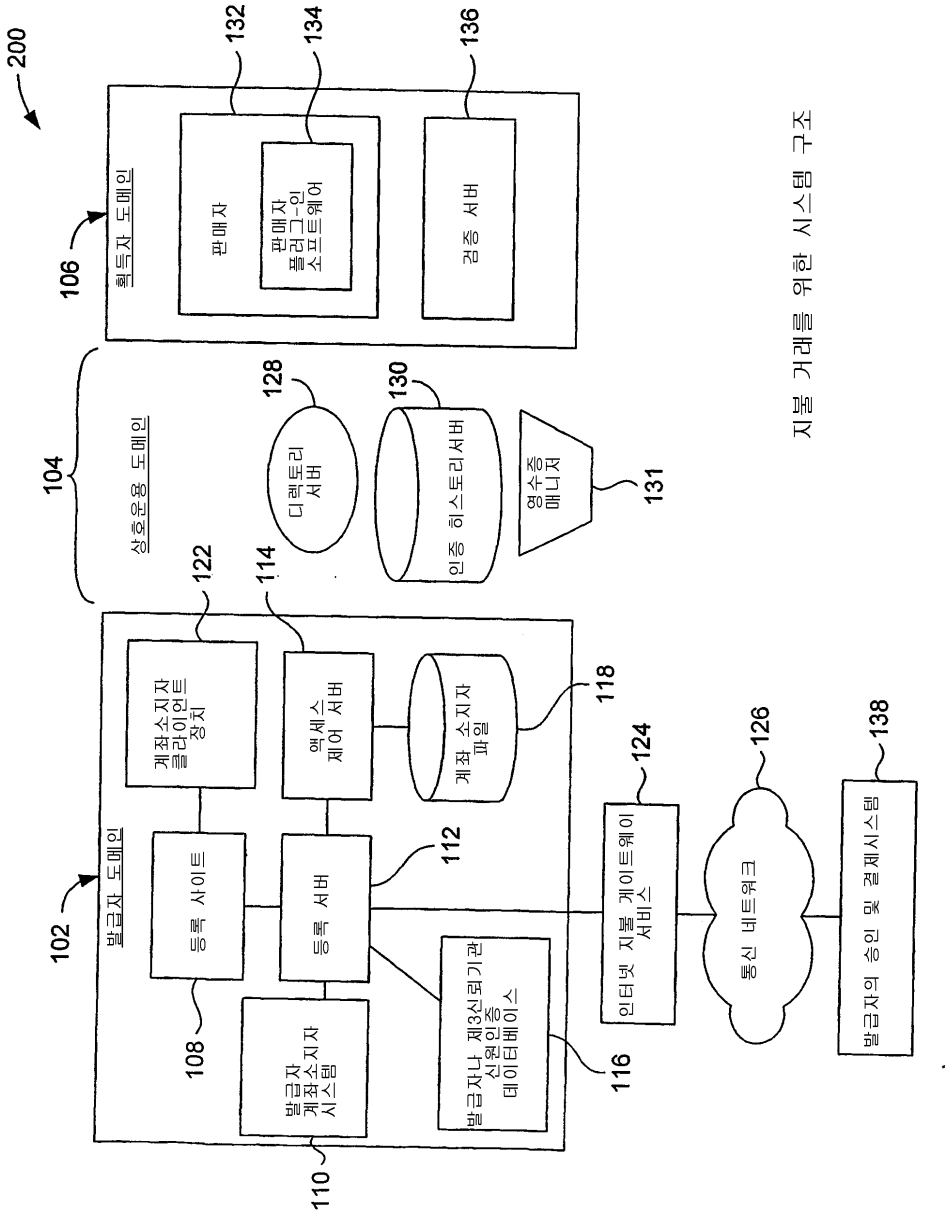
도면

도면1



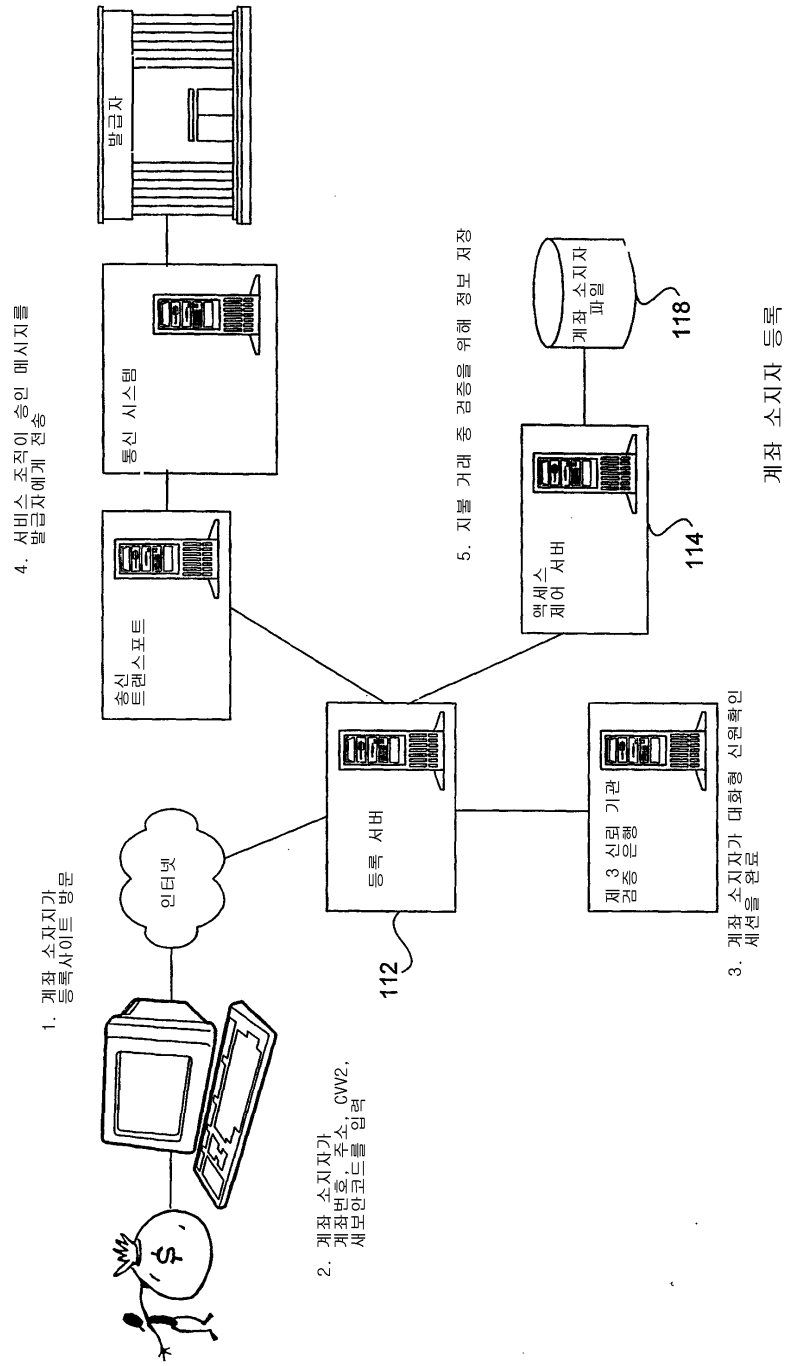
계좌 인증 시스템 구조

도면2

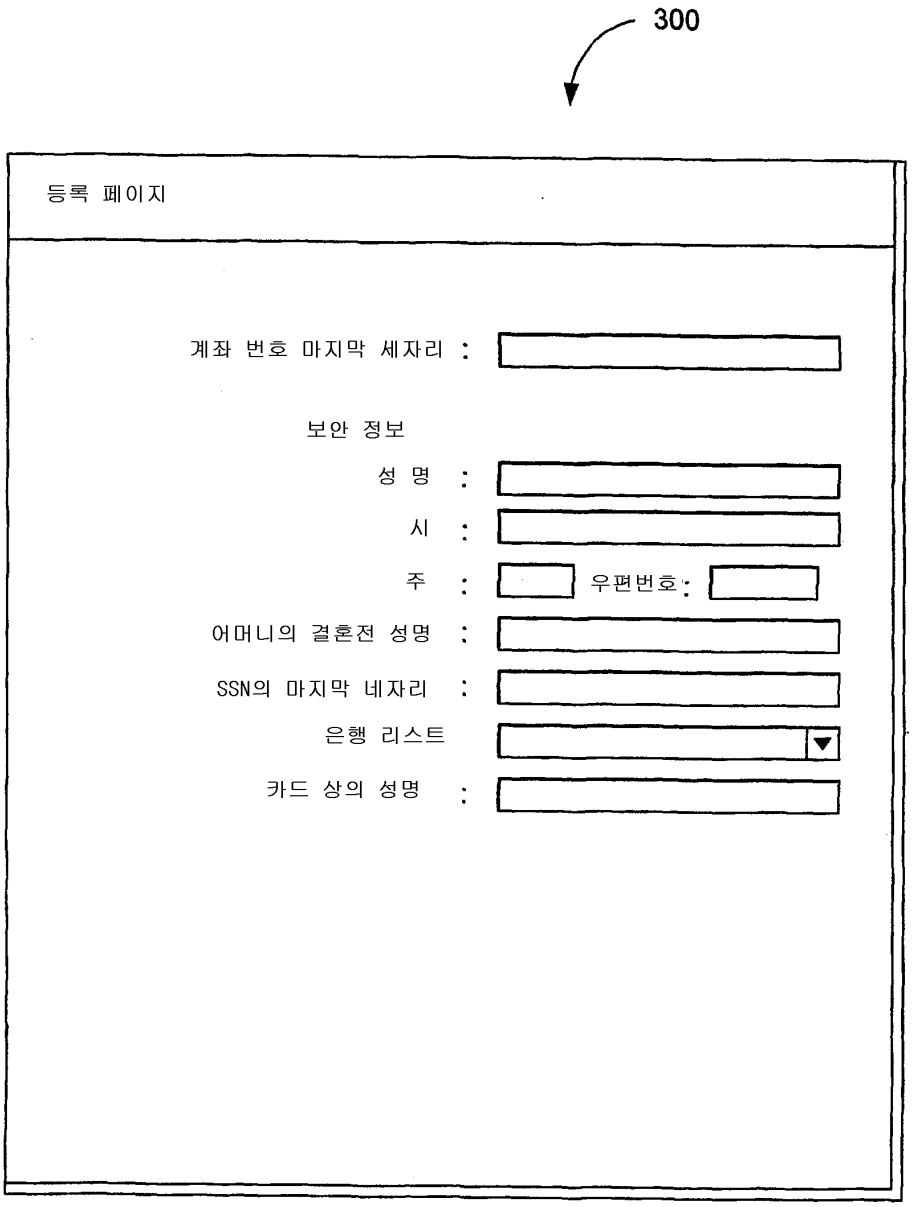


지불 거래를 위한 시스템 구조

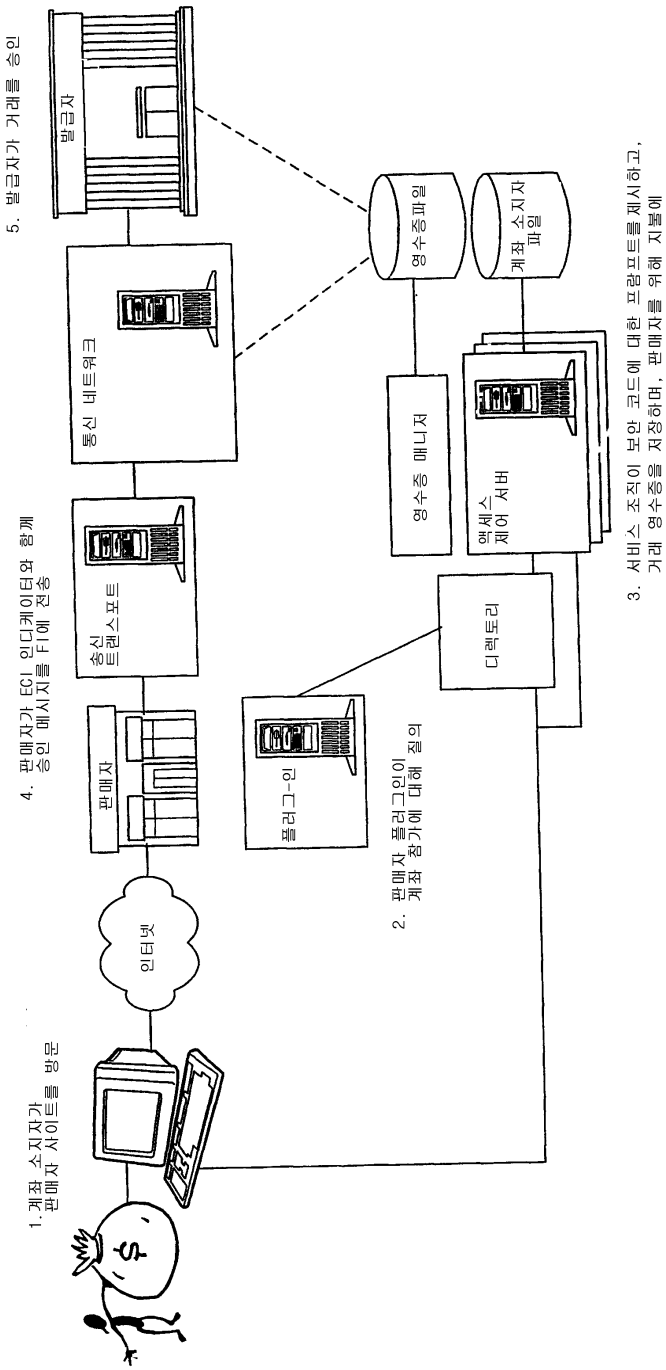
도면3


1. 계좌 소지자가
등록사이트 방문
2. 계좌 소지자가
계좌번호, 주소, CVV2,
새보안코드를 입력
3. 계좌 소지자가 대화형 신원확인
세션을 완료
4. 서비스 조직이 승인 메시지를
발급자에게 전송
5. 지불 거래 중 검증을 위해 정보 저장
인터넷
등록 서버
112
제 3 신뢰 기관
검증은행
송신
트랜스포트
통신 시스템
발급자
액세스
제어 서버
114
계좌 소지자
파일
118
계좌 소지자 등록

도면4

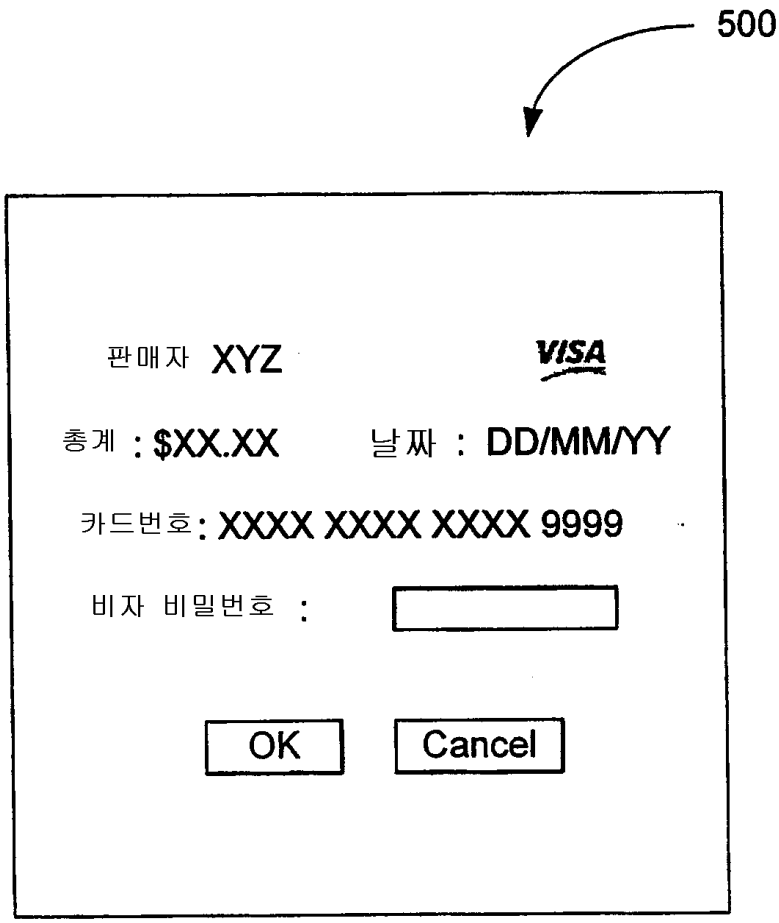

300
등록 페이지
계좌 번호 마지막 세자리 :
보안 정보
성 명 :
시 :
주 :
우편번호 :
어머니의 결혼전 성명 :
SSN의 마지막 네자리 :
은행 리스트
카드 상의 성명 :

도면5



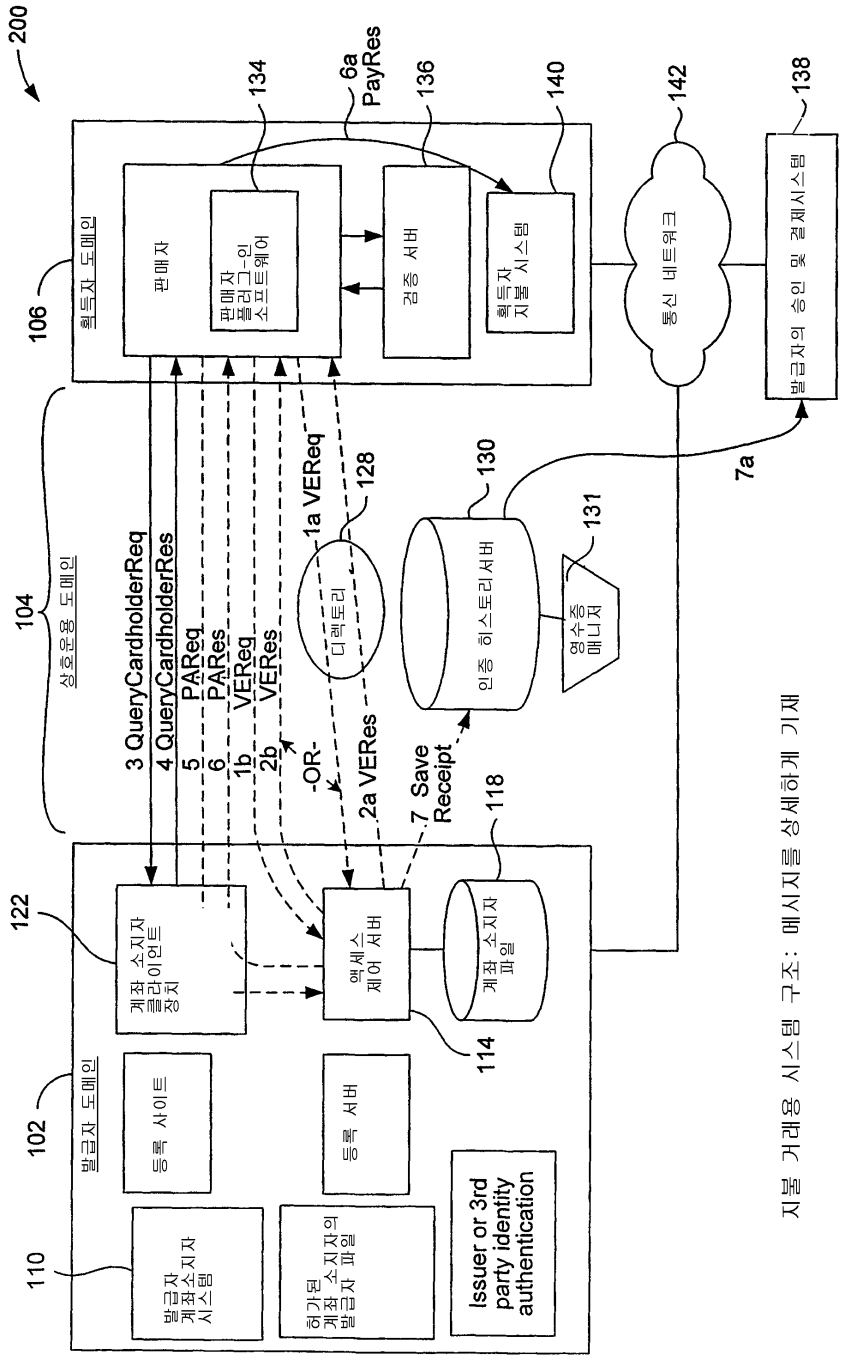
계좌 인증 시스템에서의 지불 거래

도면6



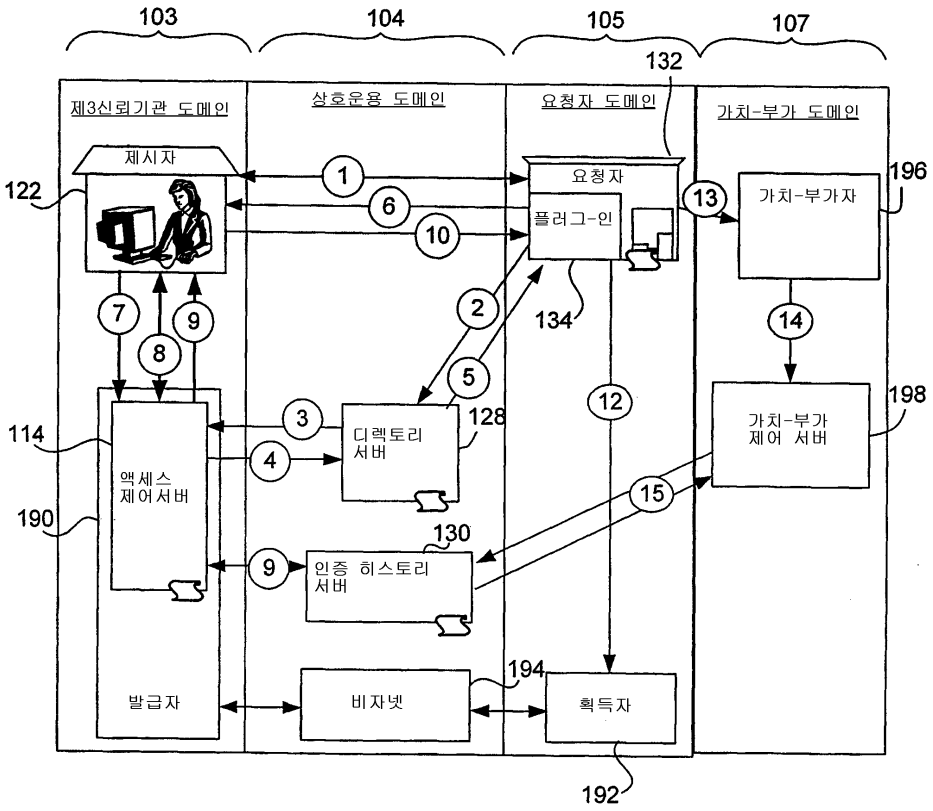
지불 거래 계좌 소지자 비밀번호 포맷

도면7



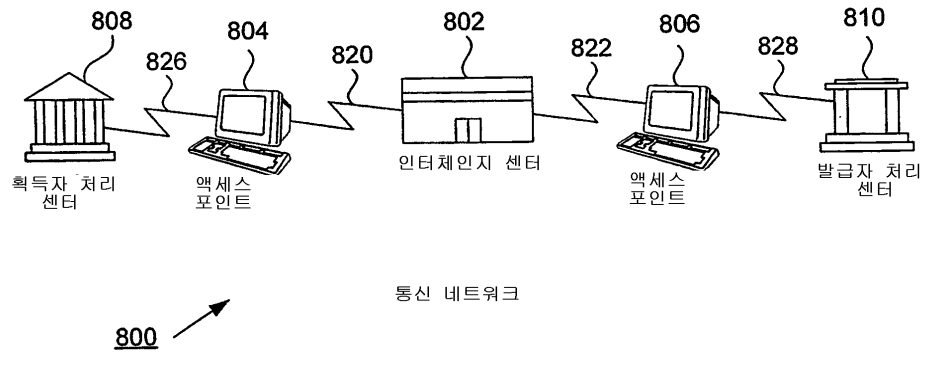
지불 거래용 시스템 구조: 메시지를 상세하게 기재

도면8

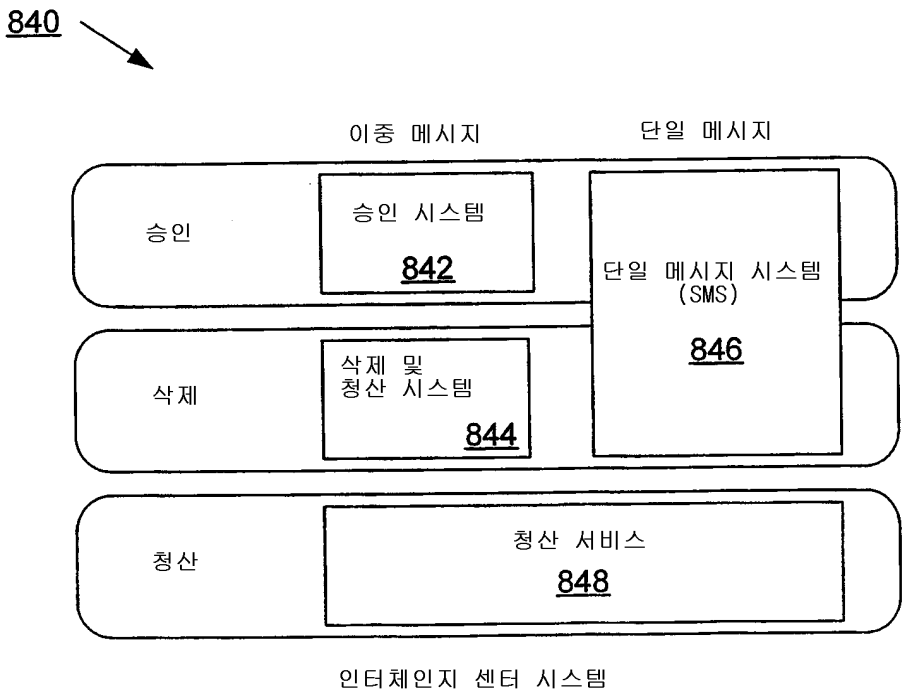


계좌 인증 시스템을 이용한 가치-부가자와의 거래

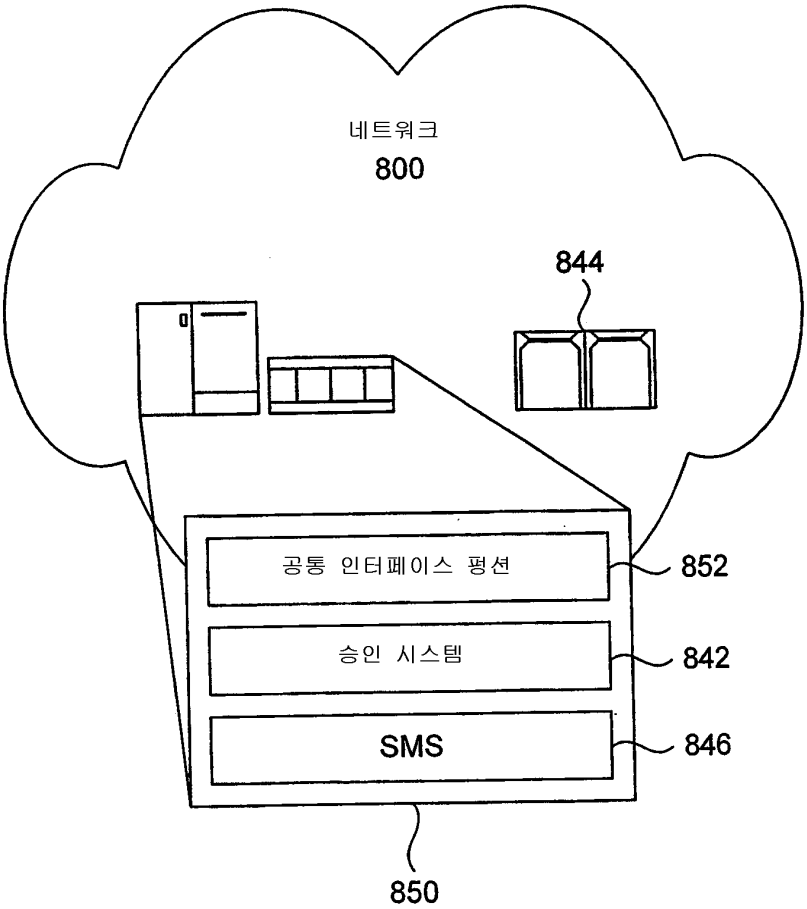
도면9



도면10

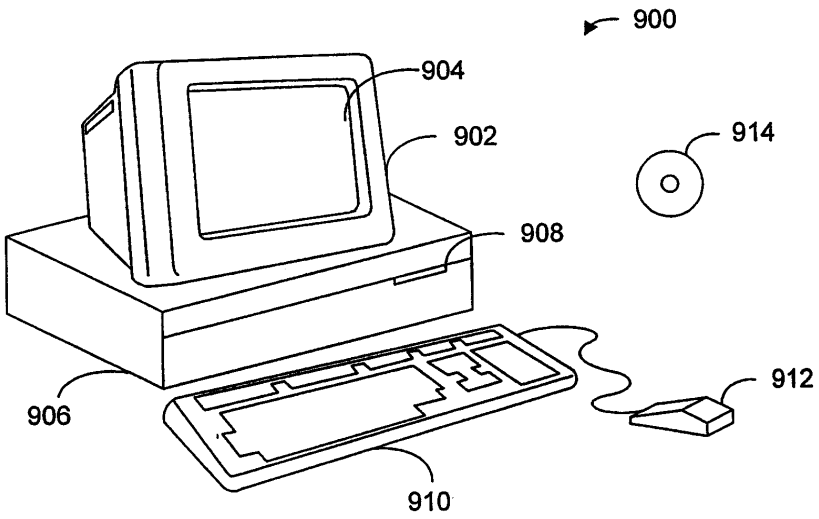

840
이중 메시지
단일 메시지
승인
승인 시스템
842
단일 메시지 시스템
(SMS)
846
삭제
삭제 및
청산 시스템
844
청산
청산 서비스
848
인터체인지 센터 시스템

도면11

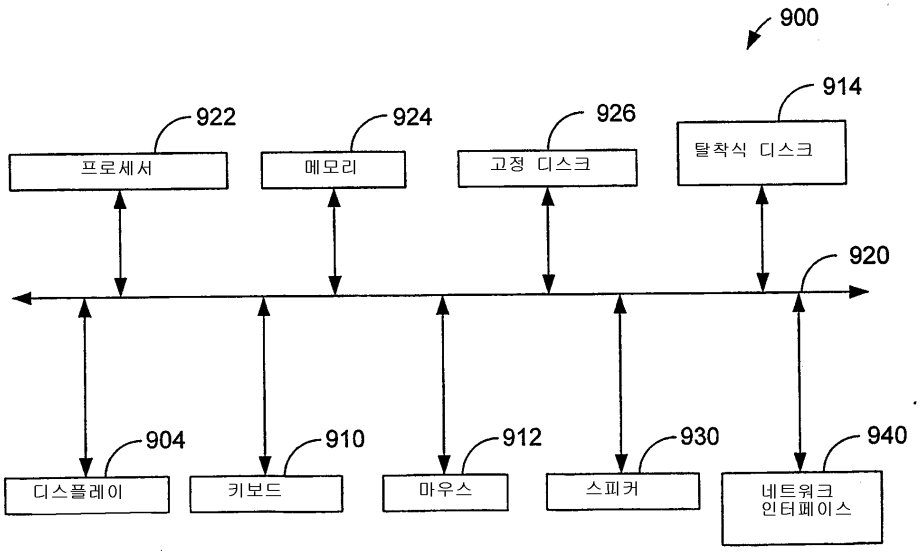


일체형 지불 시스템

도면12a



도면12b


900
914
922
924
926
탈착식 디스크
프로세서
메모리
고정 디스크
920
904
910
912
930
940
디스플레이
키보드
마우스
스피커
네트워크
인터페이스