



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0086205
(43) 공개일자 2013년07월31일

- | | |
|---|---|
| <p>(51) 국제특허분류(Int. Cl.)
G06Q 20/36 (2012.01)</p> <p>(21) 출원번호 10-2013-7002184</p> <p>(22) 출원일자(국제) 2011년06월22일
심사청구일자 없음</p> <p>(85) 번역문제출일자 2013년01월28일</p> <p>(86) 국제출원번호 PCT/US2011/041495</p> <p>(87) 국제공개번호 WO 2012/005954
국제공개일자 2012년01월12일</p> <p>(30) 우선권주장
13/165,180 2011년06월21일 미국(US)
61/359,667 2010년06월29일 미국(US)</p> | <p>(71) 출원인
이베이 인크.
미합중국 캘리포니아 산 호세 해밀턴 애비뉴 2145
(우: 95125)</p> <p>(72) 발명자
타베오 세바스티안
미국 캘리포니아주 94061 레드우드 시티 오크 릿지 드라이브 602</p> <p>나만 나다브
이스라엘 텔-아비브 알루뎀 22</p> <p>(74) 대리인
제일특허법인</p> |
|---|---|

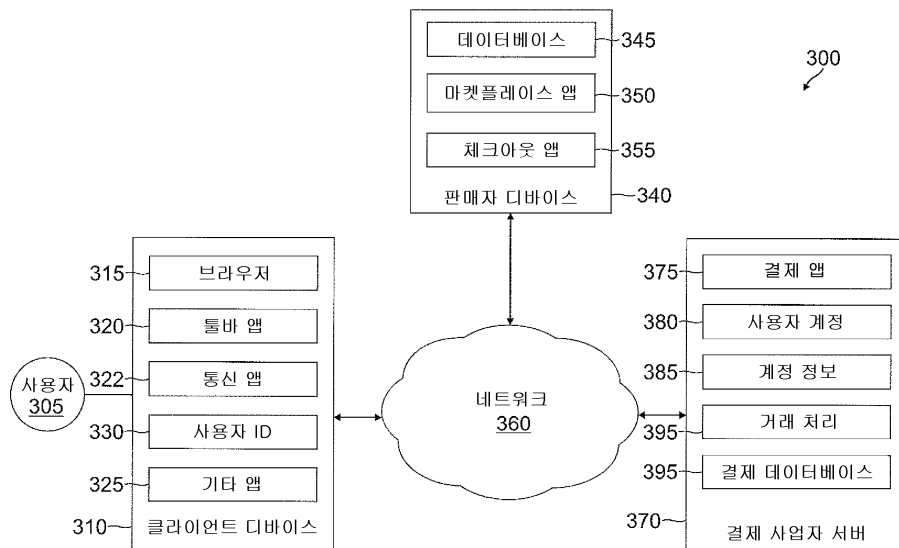
전체 청구항 수 : 총 22 항

(54) 발명의 명칭 전자 지갑

(57) 요약

물리적인 지갑에 소지되는 것과 유사하게 사용자의 스마트폰이 결제와 정보 보유에 이용된다. 거래 세부사항, 사용자 선호도 및 위치에 따라서, 거래를 위해 하나 이상의 "최선의" 펀딩 수단이 사용자를 위해 선택되고, 이때 사용자가 원할 경우 변경도 가능하다. 전화기의 다른 기능 또는 정보에 액세스하는 것은 사용 유형(예컨대 결제 혹은 비결제)과 사용의 세부사항(예컨대 고액 결제 대 소액 결제, 민감성 정보의 이용 대 비민감성 정보의 이용)에 따라 다른 인증/보안 레벨로 바꾸어 요구할 것이다.

대표도



특허청구의 범위

청구항 1

사용자 디바이스를 이용한 결제 거래를 수행하는 방법으로서,
 사용자로부터, 결제를 수행하고자 하는 신호(indication)를 수신하는 단계와,
 프로세서에 의해, 결제 사업자(payment provider)가 갖는 상기 사용자의 계정을 상기 결제 사업자가 액세스하도록 하는 단계와,
 상기 프로세서에 의해, 사용자 선호도, 거래 정보 및 사용자 위치 중 적어도 하나에 기반하여, 상기 계정과 연관된 복수의 펀딩 수단들(funding instruments)중 어느 하나 이상의 펀딩 수단을 상기 결제에 사용할지 결정하는 단계와,
 상기 하나 이상의 펀딩 수단을 이용하여 상기 결제를 처리하는 단계를 포함하는
 결제 거래 수행 방법.

청구항 2

제1항에 있어서,
 상기 사용자로부터 상기 사용자 선호도를 수신하는 단계를 더 포함하고,
 상기 결정하는 단계는 상기 사용자 선호도에 부분적으로 기반하는
 결제 거래 수행 방법.

청구항 3

제1항에 있어서,
 상기 복수의 펀딩 수단은 신용 카드, 직불 카드, 기프트 카드 및 쿠폰중 하나 이상을 포함하는
 결제 거래 수행 방법.

청구항 4

제1항에 있어서,
 상기 결정하는 단계는 상기 결제를 위해 적어도 두 개의 펀딩 수단을 선택하는 단계를 포함하는
 결제 거래 수행 방법.

청구항 5

제1항에 있어서,
 상기 거래 정보는 판매자 및 금액에 대한 정보를 포함하는
 결제 거래 수행 방법.

청구항 6

제1항에 있어서,
상기 결정하는 단계는 상기 사용자 위치에 부분적으로 기반하는
결제 거래 수행 방법.

청구항 7

제1항에 있어서,
상기 결정하는 단계는 사용자의 구매 이력에 부분적으로 기반하는
결제 거래 수행 방법.

청구항 8

제1항에 있어서,
상기 사용자 디바이스의 상이한 이용을 위해 상기 사용자로부터 상이한 보안 설정을 수신하는 단계를 더 포함하
는
결제 거래 수행 방법.

청구항 9

제8항에 있어서,
보다 높은 액수의 결제를 위해서는 보다 높은 수준의 보안 설정이 요구되는
결제 거래 수행 방법.

청구항 10

제8항에 있어서,
보다 민감한 정보의 이용을 위해서는 보다 높은 수준의 보안 설정이 요구되는
결제 거래 수행 방법.

청구항 11

제10항에 있어서,
상기 보다 민감한 정보는 사회 보장 번호, 신용 카드 번호, 은행 계정 번호 및 기프트 카드 번호중 적어도 하나
를 포함하는
결제 거래 수행 방법.

청구항 12

제1항에 있어서,
상기 사용자로부터 변경된 하나 이상의 펀딩 수단을 수신하는 단계와,
상기 변경된 하나 이상의 펀딩 수단을 이용하여 상기 결제를 처리하는 단계를 더 포함하는

결제 거래 수행 방법.

청구항 13

복수의 기계 판독 가능 명령어를 포함하는 영속적 기계 판독 가능 매체(non-transitory machine readable medium)로서,

상기 복수의 기계 판독 가능 명령어는 서버의 하나 이상의 프로세서에 의해 실행될 때, 상기 서버로 하여금,

사용자로부터, 결제를 수행하고자 하는 신호(indication)를 수신하게 하는 단계와,

상기 사용자의 계정을 결제 사업자가 액세스하게 하는 단계와,

사용자 선호도, 거래 정보 및 사용자 위치 중 적어도 하나에 적어도 기반하여, 상기 계정과 연관된 복수의 펀딩 수단들중 어느 하나 이상의 펀딩 수단을 상기 결제에 사용할지 결정하도록 하는 단계와,

상기 하나 이상의 펀딩 수단을 이용하여 상기 결제를 처리하게 하는 단계를 포함하는 방법을 수행하도록 하는

영속적 기계 판독 가능 매체.

청구항 14

제13항에 있어서,

상기 복수의 펀딩 수단은 신용 카드, 직불 카드, 기프트 카드 및 쿠폰중 하나 이상을 포함하는

영속적 기계 판독 가능 매체.

청구항 15

제13항에 있어서,

상기 결정 단계는 상기 결제를 위해 적어도 두 개의 펀딩 수단을 선택하는 것을 포함하는

영속적 기계 판독 가능 매체.

청구항 16

제13항에 있어서,

상기 거래 정보는 판매자 및 금액에 대한 정보를 포함하는

영속적 기계 판독 가능 매체.

청구항 17

제13항에 있어서,

상기 결정 단계는 사용자의 구매 이력에 부분적으로 기반하는

영속적 기계 판독 가능 매체.

청구항 18

제13항에 있어서,

상기 사용자 디바이스의 상이한 이용을 위해 상기 사용자로부터 상이한 보안 설정을 수신하게 하는 것을 더 포함하는

영속적 기계 판독 가능 매체.

청구항 19

제18항에 있어서,

보다 높은 액수의 결제를 위해서는 보다 높은 수준의 보안 설정이 요구되는

영속적 기계 판독 가능 매체.

청구항 20

제18항에 있어서,

보다 민감한 정보의 이용을 위해서는 보다 높은 수준의 보안 설정이 요구되는

영속적 기계 판독 가능 매체.

청구항 21

제20항에 있어서,

상기 보다 민감한 정보는 사회 보장 번호, 신용 카드 번호, 은행 계정 번호 및 기프트 카드 번호중 적어도 하나를 포함하는

영속적 기계 판독 가능 매체.

청구항 22

제13항에 있어서,

상기 방법은,

상기 사용자로부터 변경된 하나 이상의 펀딩 수단을 수신하게 하는 단계와,

상기 변경된 하나 이상의 펀딩 수단을 이용하여 상기 결제를 처리하게 하는 단계를 더 포함하는

영속적 기계 판독 가능 매체.

명세서

기술분야

[0001] 관련 출원에 대한 상호 참조

[0002] 본 출원은, 2010년 6월 29일에 미국 출원된 미국 임시출원 특허 출원번호 제61/359,667호를 우선권 주장하여 2011년 6월 21에 미국 출원된 미국 정규출원 특허 출원번호 제13/165,180호에 대해 우선권을 주장한다.

[0003] 발명의 분야

[0004] 본 발명은 전반적으로 모바일 디바이스를 이용한 결제(payments)에 관한 것으로, 보다 구체적으로는 모바일 디바이스를 이용하여 지능적으로 결제하는 것에 관한 것이다

배 경 기 술

- [0005] 전자 결제는 전통적인 물리적 결제를 진행하지 않는 사용자에게 여러 이점들을 제공하므로 점점 더 바람직한 결제 방법이 되고 있다. 물리적 결제에서는 사용자가 펀딩 수단(funding instrument)을 소지하고, 결제를 행할 준비가 되면 이 펀딩 수단을 제시해야만 한다. 물리적 펀딩 수단의 예로는, 현금, 수표, 신용 카드, 직불 카드, 쿠폰, 상품권, 기프트 카드 등이 있다. 이러한 물리적 수단은 사용자의 주머니나 가방 또는 지갑 속에서 공간을 차지할 수 있다. 소비자는 이러한 공간을 줄이기 위해 항상 모든 펀딩 수단을 소지하지 않을 수도 있고, 그 결과, 매장(POS:a point of sale)에서 소비자가 원하는 펀딩 수단을 이용하려고 해도 해당 펀딩 수단을 이용할 수 없는 일이 생길 수도 있다. 또한 이 물리적 펀딩 수단은 분실 또는 도난의 가능성도 있다. 그러므로, 물리적인 "지갑"은 성가시고 불편하며 분실하기 쉽다.
- [0006] 이를 개선하기 위해, 모바일 디바이스가 예컨대 캘리포니아주 산호세 소재의 PayPal, Inc. 같은 결제 사업자(payment provider)를 통해 결제를 수행하는데 이용된다. 이러한 결제 사업자는 전형적으로 소비자가 사용자의 모바일 디바이스를 통해, 예컨대 바코드의 이용, 결제 사업자와 판매자 사이의 통신 및 기타의 방법을 통해 결제를 수행하도록 한다. 인증 및/또는 허가 이후에, 결제가 결제 사업자와 사용자 계정을 통해 이루어지는데, 이때 계정은 예컨대 사용자의 은행 또는 신용 카드같은 펀딩 소스를 통해 자금을 지원한다. 펀딩 소스는 전형적으로 사용자에게 의해 선택된 한 개의 디폴트 소스이다.
- [0007] 비록 이러한 결제 방법이 소비자로 하여금 신용카드, 은행카드 및 현금을 소지하지 않아도 되게 할지라도, 사용자는 여전히 결제 사업자 서비스를 이용할지, 모바일 디바이스의 다른 결제 서비스를 이용할지, 또는 물리적 펀딩 수단을 이용할지를 결정해야만 한다. 이것은 또한 물리적 지갑의 경우와 같은 불편함일 수 있는데, 그 이유는 사용자가 여전히 많은 가능한 펀딩 수단들 중 어떤 것을 특정 구매에서 이용할 것인지 결정해야 하기 때문이다. 이것은 사용자가 해당 거래에서 "최선의" 선택이 아닌 결제 수단을 선택하는 결과를 초래할 수도 있다.
- [0008] 그러므로, 종래의 결제 방법이 갖는 전술한 단점들을 극복할 수 있는 결제 해결법에 대한 필요성이 존재한다.

발명의 내용

과제의 해결 수단

- [0009] 일 실시예에 따르면, 소비자는 PayPal사와 같은 결제 사업자와 계정을 갖는다. 계정은 적어도 하나의 펀딩 소스를 포함하고, 바람직하게는 몇 개의 펀딩 소스를 포함한다. 사용자가 예컨대 매장(POS)에서 구매 혹은 결제를 수행할 준비가 되면, 결제 사업자는 금액, 구매 유형, 판매자, 위치 등을 포함한 거래 정보에 기초하여 어떤 펀딩 소스(예를 들면, Visa, AMEX, 각양각색의 리워드 프로그램이 연계된 신용카드, 페이펄, 은행 계정, 쿠폰, 기프트 카드 등등)를 사용할 것인지 결정한다. 이 결정은 사용자 선택의 선호도, 사용자의 결제 이력, 목표, 판매자 선호 또는 장려 결제 소스 혹은 논리의 조합에 기반할 수 있다. 예를 들면, 특정 가게에서 특정 카드를 사용할 경우에 할인 혜택이나 다른 보상이 제공될 수도 있고, 사용자가 목표에 대한 충분한 리워드 포인트를 얻는 카드를 주로 이용하고자 할 수도 있으며, 사용자가 특정 카드를 최대 월별 금액 혹은 거래 금액으로 제한하고자 할 수도 있고, 힐튼 호텔에서는 AMEX Hilton 카드가 사용되도록 선택될 수도 있다.
- [0010] 이것은 사용자가 카드를 사용할지 혹은 다른 펀딩 수단을 사용할지 결정하는데 드는 시간과 노력을 상당히 감소시킨다. 또한 이것은 사용자가 펀딩의 일부로서 쿠폰을 이용하는 것을 도와준다.
- [0011] 결제 사업자는 또한 펀딩 소스로부터 판매자에게 직접적으로 결제를 제공할 수 있어서 수령인(recipient)은 결제 사업자와 계정을 가질 필요가 없다. 이것은 사용자가 결제 사업자 계정을 갖지 않는 경우에도 적용될 수 있다.
- [0012] 다른 실시예에 따르면, 상이한 인증 또는 보안 레벨이 사용자 디바이스의 상이한 사용자들에 대해 적용된다. 예를 들면, 결제는 어떤 한 유형의 인증을 요구하는 반면, (예컨대 정보 전송 또는 디스플레이같은) 비결제(non-payments)는 다른 유형의 인증을 요구할 수 있을 것이다. 결제 혹은 비결제가 이루어지는 동안, 추가의 상이한 보안 레벨이 존재할 수 있다. 예를 들어, 고수준의 보안은 고액 결제에 요구될 것이며, 또한 사회 보장 번호(social security number), 신용 카드 번호 등과 같은 보다 민감한 정보의 이용 혹은 디스플레이를 요구할

것이다.

- [0013] 본 발명의 이런 저런 특징과 이점들은 첨부 도면과 함께 이하에 설명된 실시예들의 상세한 설명으로부터 보다 쉽게 명확해질 것이다.

도면의 간단한 설명

- [0014] 도 1은 일 실시예에 따라 사용자의 전자 지갑으로부터 결제를 진행하기 위해 결제 사업자가 수행하는 프로세스를 도시하는 흐름도이다.

도 2는 일 실시예에 따라 상이한 인증 레벨과 함께 사용자의 모바일 디바이스를 디지털 지갑으로서 이용하는 프로세스를 도시하는 흐름도이다.

도 3은 일 실시예에 따라 본 명세서에 설명된 프로세스를 구현하기에 적합한 네트워크화된 시스템의 블록도이다.

도 4는 일 실시예에 따른 도 3에서 하나 이상의 구성요소를 구현하기에 적합한 컴퓨터 시스템의 블록도이다.

본 개시물의 실시예들과 그들의 이점들은 이후의 상세한 설명을 참조함으로써 가장 잘 이해된다. 유사한 참조 부호가 하나 이상의 도면에 예시된 동일한 요소를 식별하는데 이용되며, 여기에 도시된 것들은 본 개시물의 실시예를 예시하기 위한 목적일 뿐, 제한적인 의도는 아님을 이해해야 할 것이다.

발명을 실시하기 위한 구체적인 내용

- [0015] 다양한 실시예들에 따르면, 사용자의 모바일 디바이스의 스마트 디지털 지갑은 사용자에게 거래 정보, 사용자 선호도, 사용자 이력 및/또는 펀딩 수단 정보에 기반하여 어떤 펀딩 수단을 이용할 것인지에 대하여 권고(recommendations) 혹은 결정(decisions)을 제공한다. 또한 이 전자 지갑은 사용자 선호도, 거래 금액, 위치 및 기타 요소에 부분적으로 기반하여 결제를 행하기 위해 상이한 보안 레벨로 맞춤화(customized)될 수 있다. 따라서, 사용자의 모바일 디바이스는 물리적인 펀딩 수단을 대체하는 전자 지갑으로서 이용될 수 있으면서, 물리적 지갑으로는 불가능한 다양한 이점들도 제공할 수 있다.

- [0016] 도 1은 일 실시예에 따라 사용자의 전자 지갑으로부터 결제를 처리하기 위해 결제 사업자가 수행하는 프로세스(100)를 도시하는 흐름도이다. 단계(102)에서, 결제 사업자는 사용자가 아이템에 대한 결제를 수행할 준비가 되었다는 신호(indication)를 수신한다. 본원에서 사용되는 아이템이란, 물리적 상품, 디지털 상품, 서비스, 기부, 그리고 사용자가 그와 관련하여 결제를 행하는 모든 것을 포함할 것이다. 이 실시예에서, 사용자는 상점에서처럼 물리적 위치 혹은 결제와 관련한 매장(POS)에 있다. 다른 실시예에서는, 사용자가 PC에서처럼 컴퓨팅 디바이스를 통해 온라인 쇼핑을 할 수도 있고, 결제를 수행할 수도 있다.

- [0017] 전술한 지시는 몇 가지 방식으로 수신될 수 있다. 일 예로는, 사용자가 구매시점에 사용자 모바일 디바이스로 결제 앱에 액세스하는 것으로, 이것은 모바일 디바이스를 통해 결제 사업자를 콜(call)한다. 사용자는 사용자의 계정에 액세스하여 모바일 디바이스를 통해 결제를 가능하게 하기 위해 크레덴셜(credentials)에 진입할 것이다. 다른 예로는, 판매자가 판매자 디바이스를 통해 구매시점에 결제 사업자에게로 구매 거래를 통신하는 것이다. 이것은 사용자가 체크아웃 프로세스를 시작하는 시점, 체크아웃 프로세스를 진행중인 시점, 혹은 모든 아이템이 스캔되어 합산이 이루어진 이후의 시점일 수 있다. 일 실시예로, 단계(102)에서 통신된 최소 정보는 사용자가 결제를 수행하고자 한다는 요구와 사용자 신원/ 계정 정보 정도이다. 후자의 정보는 결제 사업자가 사용자의 계정과 계정 관련 데이터를 액세스할 수 있게 한다.

- [0018] 일단 사용자의 계정이 액세스되면, 결제 사업자는 단계(104)에서 결제와 관련하여 사용자의 계정에 어떠한 디폴트 설정이 존재하는지를 판정한다. 디폴트 설정은 예컨대 사용자가 정의한 선호도처럼 사용자에게 의해 결정될 수도 있고, 예컨대 결제 이력처럼 결제 사업자에 의해 결정될 수도 있으며, 혹은 이 둘의 조합으로 결정될 수도 있다. 디폴트 설정은 사용자 계정과 연관된 펀딩 수단의 이용에 대한 정보를 포함한다. 예를 들어, 사용자는 사용자 계정과 관련한 몇몇 펀딩 소스로서 아메리칸 익스프레스 힐튼 리워드 신용카드, 씨티은행 데빗 카드 혹은 은행 계정, 비자 사우스웨스트 에어라인 리워드 신용카드, 비자 기프트 카드를 소유할 수 있을 것이다. AMEX 카드가 주요 펀딩 소스이고, 그 다음이 비자 기프트 카드, 기타 다른 카드 등의 특별한 순서가 정해질 수 있을 것이다. 따라서 구매시에 AMEX 카드가 우선적인 펀딩 수단일 것이다. 그러나 AMEX 카드가 허용되지 않는 판매자/사이트/장소에서처럼 AMEX 카드가 이용될 수 없는 상황이 존재할 수도 있고, AMEX 카드가 거절되는 상황

(예컨대 유효기간 만기, 한도 제한, 부정 사용 의심 등)이 존재할 수도 있다. 만약 AMEX를 이용할 수 없다면, 비자 기프트 카드가 다음으로 선택될 것이다. 그러나 비자 기프트 카드도 잔액이 소진되어 이용할 수 없는 경우가 있을 수 있다. 그러면 그 다음의 펀딩 수단이 시도될 것이다.

[0019] 디폴트 설정은 필요에 따라 변경될 수 있다. 예를 들어, 사용자가 다가올 휴가때 숙박하기 위해 힐튼 포인트를 누적시키기를 위해서 AMEX 카드를 첫번째로 선택할 수 있다. 그러나 일단 포인트가 충분히 쌓이거나 혹은 더 이상 필요가 없어지면, 사용자는 AMEX 카드를 비자 카드로 대체하여 재빨리 공짜 비행을 위한 포인트를 누적할 수 있을 것이다. 이러한 변경은 결제 사업자와의 사용자 계정 페이지를 통해 사용자에게 의해 행해질 수 있다.

[0020] 만약 디폴트 설정이 존재한다면, 이러한 설정은 단계(106)에서 적용된다. 또한 시스템은 단계(108)에서 사용자의 펀딩 수단중 어떤 것과 관련하여 위치 기반 제한이나 규칙이 존재하는지 판정한다. 예를 들어, 미국내에서는 특정 기프트 카드 또는 쿠폰만이 이용될 수 있다. 캘리포니아에서는 다른 쿠폰만이 이용될 수 있다. 비자 기프트 카드는 어디서든지 이용될 수 있지만 알칸사스 이용될 경우에는 보너스를 받을 수 있다. 이 보너스는 기프트 카드에 10% 적립될 수 있다. 최근의 지진의 여파로 알칸사스 경제를 돕기 위해 알칸사스에서 더 많은 소비가 이루어지기를 위해서 알칸사스에서는 비자 카드를 사용하도록 할 수 있을 것이다.

[0021] 만약 적어도 하나의 위치 기반 규칙이 존재한다면, 사용자의 위치(혹은 POS)가 단계(110)에서 결정된다. 이것은 사용자의 모바일 디바이스와 연계된 위치 서비스 혹은 기능을 통해서 이루어질 것이다. 따라서 사용자가 결제를 수행할 준비가 되면, 사용자의 위치가 사용자의 모바일 디바이스를 통해 공지될 것이다. 전형적으로 위치는 POS 시점이다. 사용자 위치가 다른 방식으로 결정될 수도 있다. 일 예가 판매자가 사용자의 신원을 결제 사업자에게로 통신하는 것인데, 이때 결제 사업자에게는 사용자가 판매자와 함께 있음이 통지되고, 이 판매자의 위치는 결제 사업자에게 알려져 있다. 결제 사업자는 하나 이상의 위치 기반 규칙들을 단계(112)에서 적용한다. 이것은 사용자가 정의한 선호도의 우선순위를 그에 따라 변경하는 것을 포함한다.

[0022] 시스템은 단계(114)에서 판매자 혹은 사용자를 통해서 거래 세부사항을 수신한다. 거래 세부사항은 예컨대 내역, 유형, 수량, 가격 같은 스캔된 아이템 혹은 구매될 아이템에 대한 정보와, 예컨대 이름, 계정 번호, 주요 주소, 세부적인 가게 주소, 전화 번호, 거래일시 같은 판매자 정보와, 세금과 적용된(혹은 적용될) 할인/쿠폰/리워드 등을 포함한 거래 금액을 포함한다.

[0023] 이러한 정보와 다른 적용 가능한 정보를 이용하여, 단계(116)에서, 사용자에게 현재 거래에서 이용하기에 "최선인" 하나 이상의 펀딩 수단이 결정된다. 이 결정은 사용자, 판매자, 위치 및 거래에 대해 수신된 이용가능한 모든 정보 혹은 일부 정보를 처리하는 것을 포함할 수 있다. 예를 들어, 특정 판매자는 특정 펀딩 수단만(예컨대 신용 카드중에 비자 카드 및 마스터 카드만)을 허용하고, 특정 펀딩 수단(예컨대 AMEX 혹은 쿠폰)은 허용하지 않을 수 있으며, 혹은 특정 펀딩 수단(예컨대 가게 브랜드를 차용한 신용 카드)를 이용하는 것에 대해 리워드나 다른 우대조치를 제공할 수도 있을 것이다.

[0024] 다른 예로서, 특정 쿠폰이나 기프트 카드가 거래중인 하나 이상의 구매에 적용가능할 수 있다. 이러한 쿠폰 혹은 기프트 카드는 이후에 사용을 위해 선택될 것이다. 특정 쿠폰, 기프트 카드 등은 도래하는 유효기간 만기일을 가질 것이다. 거래 일자와 적용 가능 펀딩 수단의 유효기간 만기일에 기반하여, 적합한 펀딩 수단이 해당 거래에 이용되도록 선택될 수 있다. 예를 들어, 만기일이 근접한 펀딩 수단이 유효기간 만기일이 더 늦은 펀딩 수단보다 우선할 수 있을 것이다.

[0025] 일단 펀딩 수단들이 현재 거래에서 선택되면, 단계(118)에서 사용자에게 사용자의 모바일 디바이스상에 선택(들)이 제시된다. 사용자는 각각의 펀딩 수단이 어디에 적용될 것이며, 만약 적합하다면 적용될 금액과 함께 어떻게 적용될 것인지를 보게된다. 예를 들어, 특정 구매 혹은 아이템이 구매에 적용될 기프트 카드, 바우처 혹은 쿠폰에서 특정 금액만 허용할 수도 있다.

[0026] 다음, 결제 사업자는 단계(120)에서 사용자가 선택된 펀딩 수단을 확인했는지를 결정한다. 이 결정은 사용자가 디바이스를 가볍게 두드리거나(tapping) "확인" 등의 링크/버튼을 선택함으로써 이루어지는 확인(confirmatio n)처럼 전자 신호를 사용자 디바이스로부터 수신하는 것을 포함할 것이다. 승인이 수신되면, 단계(122)에서 선택된 펀딩 수단으로 거래가 처리될 것이다. 거래의 처리는 결제 사업자를 통하는데, 결제 사업자는 결제 세부사항을 사용자 디바이스나 판매자를 통해 수신하여, 하나 이상의 결제가 승인될 수 있는지 결정하고, 즉시 혹은 나중에 사용자 계정에서 인출하여 판매자 계정에 입금하며, 거래와 관련한 결제가 승인되었는지 혹은 거부되었는지에 대한 통지를 사용자 및/또는 판매자에게 전송한다. 또한 이 처리는 사용자를 통해 곧장 이루어질 수도 있다. 예를 들어, 사용자는 간단히 물리적인 신용 카드를 제공할 수 있고, 이런 경우에 처리는 판매자와 기존

의 신용 카드 처리 방식을 통한다.

[0027] 만약 사용자가 선택된 펀딩 소스를 확인하지 않으면, 이 사용자는 예를 들어 하나 이상의 상이한 펀딩 소스를 추가하거나, 하나 이상의 펀딩 소스를 삭제하거나, 혹은 펀딩 소스를 다르게 적용(예컨대 기프트 카드의 사용 금액을 축소)하거나 하는 등, 선택을 변경하려는 것일 수도 있다. 예를 들어, 결제 사업자가 사용자가 이전에 설정한 선호도(사용자가 호텔 보너스 포인트를 적립하고자 원했음)에 기반하여 AMEX 카드를 선택했다더라도, 사용자가 더 이상 포인트를 필요로 하지 않을 수 있다. 이것은 사용자가 이미 충분한 포인트량을 획득했기 때문일 수도 있고, 체류하려던 호텔이 변경되었기 때문일 수도 있으며, 다른 이유일 수도 있다. 또한 사용자가 아직 사용자 선호도를 변경하지 않았을 수도 있다. 결과적으로, 사용자는 AMEX 카드를 비자 카드로 대체할 수 있다.

[0028] 다른 실시예로, 사용자는 사용자 디바이스를 통해 선택된 펀딩 수단을 변경할 수 있다. 예를 들어, 사용자는 변경을 위해 펀딩 소스를 선택할 수 있을 것이다. 선택된 펀딩 소스는 삭제될 수도 있고 혹은 사용자 디바이스를 통한 사용자 조치에 따라 변경될 수도 있다. 이용가능한 펀딩 소스들로 이루어진 목록에서 선택함으로써 신규 펀딩 소스가 추가될 수도 있다. 이 목록은 어떠한 형식도 취할 수도 있으며, 드롭 다운 메뉴나 브라우저 혹은 앱상에 새창 열기등의 여러 방식으로 액세스될 수 있다.

[0029] 선택된 펀딩 소스들에 대해 한 번 이상의 변경이 사용자에게 의해 수행된 이후, 이 변경들은 단계(124)에서 결제 사업자에게 통신되어 수신된다. 수신 즉시, 결제 사업자는 사용자가 변경한 결제 수단 선택을 단계(126)에서 사용자에게 전송한다. 사용자는 변경된 결제 선택을 예컨대 사용자 디바이스상에서 살펴보고, 전송한 단계들을 이용하여 확인하거나 또는 필요하다면 다시 변경할 수 있다. 사용자가 결제 수단을 확인하면, 결제는 단계(122)에서 처리될 수 있다.

[0030] 전송한 여러 단계들과 결정들은 상이한 순서로 수행될 수도 있으며, 하나 이상이 누락되도록 선택될 수도 있으며, 마찬가지로 추가적인 단계와 결정들이 더해질 수도 있음을 유의하라.

[0031] 결국, 사용자는 사용자 설정 선호도, 위치, 거래 세부사항, 판매자, 일시 및 기타 요소들에 기반하여 결제 사업자로부터의 선택을 이용하여 거래를 결제하기에 "최선인" 펀딩 수단을 이용할 수 있게 된다. 결제는 사용자의 모바일 디바이스를 통해서 이루어질 수 있고, 이로써 사용자가 예컨대 현금, 신용 카드, 직불 카드, 수표, 쿠폰 및 기프트 카드 같은 물리적인 펀딩 수단을 소지할 필요가 없어진다.

[0032] 도 2는 일 실시예에 따라 상이한 인증 레벨과 함께 사용자 모바일 디바이스를 디지털 지갑으로서 이용하는 프로세스(200)를 보여주는 흐름도이다. 전형적인 물리적 지갑은 전송한 것과 같은 펀딩 수단뿐만 아니라 예컨대 의료 보험 카드, 항공 보너스 마일리지 카드번호, 호텔 로열티 카드 번호, 사회 보장 카드, 자동차 클럽 카드 등과 같은 많은 비결제 카드를 담고 있을 수 있다. 스마트폰이나 태블릿 같은 모바일 디바이스는 이러한 사용자 개인 정보를 저장할 수 있으며, 따라서 모바일 디바이스는 결제 수단과 사용자 정보 모두를 포함할 수 있다는 점에서 물리적인 지갑과 더 유사해질 수 있다.

[0033] 결제에 모바일 디바이스를 이용하기 위해, 사용자는 통상적으로 패스워드 혹은 PIN을 입력해야 하고, 또한 사용자/디바이스 식별자가 모바일 디바이스를 통해 결제 사업자에게 자동적으로 통신되지 않을 경우에는 사용자가 예컨대 사용자 이름, 이메일 주소 혹은 전화 번호 같은 사용자/디바이스 식별자도 입력해야 한다. 이것은 성가시고 시간이 걸리는 일이며, 특히 모바일 디바이스와 연계된 소형의 물리적 키패드 및 가상 키패드를 이용해야 하는 것이다. 그러나, 이러한 인증은 펀딩 수단을 보호하기 위해 필요하며, 비인증된 사용자가 사용자의 계정으로 결제를 수행하지 못하게 하는 데에도 필요하다.

[0034] 전화기에는 결제의 인증 레벨을 필요로 하지 않는 다른 데이터 또는 기능들이 존재할 수 있다. 예를 들어, 항공기 보너스 마일리지 카드번호 혹은 이 카드 번호의 전송은 결제 관련 전송 정도의 보안 레벨을 요구하지 않을 수도 있다. 예컨대 사용자의 사회 보장 번호 같은 다른 정보는 추가의 보안을 요구할 수 있을 것이다. 결제도 상이한 보안 레벨을 허용할 수 있을 것이다. 예를 들어, \$20 미만의 결제 거래는 \$200 이상의 결제 거래 정도로 높은 보안을 요구하지는 않을 것이다. 그러므로, 도 2는 모바일 디바이스 혹은 이 모바일 디바이스의 사용자가 모바일 디바이스를 이용하여 상이한 정보 혹은 거래에 대해 어떻게 인증될 수 있는지 그 예를 예시한다.

[0035] 단계(202)에서, 현재 이용중인 모바일 디바이스가 결제에 사용될 것인지 결정이 행해진다. 결제 거래는 전형적으로 더 강한 인증을 요구할 것이다. 이 결정은 모바일 디바이스를 통해 사용자로부터 예컨대 결제 앱 선택 같은 지시를 수신하는 것을 포함하거나, 혹은 판매자와 같은 수취인으로부터 수취인 디바이스를 통해 사용자 혹은 지불자 식별 같은 지시를 수신하는 것을 포함할 수 있다. 만약 모바일 디바이스가 결제 거래에 이용될 것이라

면, 단계(204)에서, 결제 거래의 금액이 특정 금액 X보다 많은지에 대한 결정이 행해진다. 이 금액은 사용자나 결제 사업자에 의해 설정될 수 있다. 더 높은 금액은 전형적으로 더 강한 인증을 요구할 것이다. 이 금액은 결제 사업자가 사용자 계정에서 자금을 이용하는 것과, 쿠폰, 기프트 카드, 바우처 등을 이용하는 것과, 신용 카드처럼 다른 펀딩 소스를 이용하는 것중 적어도 하나를 포함할 수 있다.

[0036] 만약 예상 결제 금액이 X 이하이면, 단계(206)에서 결제 사업자는 사용자에게 제 1 인증 레벨 Auth1을 이용하여 인증할 것을 요구할 것이다. Auth1은 간단히 사용자에게 모바일 디바이스를 잠금 해제(unlock)하거나 결제 앱을 액세스할것을 요구할 것이다. 만약 예상 결제 금액이 X 이상이면, 단계 (208)에서 사용자에게 Auth1보다 더 강력한 제 2 인증 레벨 Auth2을 통해 인증할 것을 요구할 것이다. Auth2의 일 예로서, 단계(206)에서 요구되었던 것과 함께 사용자 PIN, 생체 정보, 패스워드 혹은 기타 데이터를 입력하는 것이 있다.

[0037] 만약 단계(202)에서 결정된 것처럼 현재의 거래가 결제를 위한 것이 아니라면, 단계(210)에서 "민감한" 혹은 "기밀의(confidential)" 정보와 관련된 거래인지가 결정될 것이다. 민감한 정보의 예로서, 사용자의 사회 보장 번호, 은행 계정 번호, 패스워드, 보안 코드를 포함하는 신용 카드 번호, 직불 카드 번호 등등이 있다. 모바일 디바이스에 저장된 덜 민감한 정보의 예로는, 항공기 로열티 프로그램, 호텔 로열티 프로그램, 판매자 로열티 프로그램 등과 관련한 계정 번호, 의료 보험 정책 번호, 치과 보험 정책 번호, AAA 멤버십 번호 등등이 있다. 사용자는 예컨대 특정 데이터 또는 데이터의 유형을 지명함으로써 어떤 정보가 민감한 것이고 어떤 정보가 덜 민감한 것인지 결정할 것이다.

[0038] 단계(212)에서, 거래가 민감한 정보의 노출이나 전송을 수반할 때 사용자는 제 2 인증 레벨 Auth3에서 인증할 것이 요구된다. 일 실시예로, Auth3은 Auth1보다 더 강력한 인증이지만 Auth2보다는 약한 것이다. 다른 실시예에서는, Auth3이 Auth2와 동일한 것이다. Auth3은 사용자가 예컨대 이메일 주소, 전화 번호 혹은 사용자 이름과 같은 식별자를 입력하는 것을 요구할 수 있다.

[0039] 만약 정보가 덜 민감한 것이면, 사용자는 단계(214)에서 제 4 인증 레벨 Auth4을 이용하여 인증할 것이 요구될 것이다. Auth4는 Auth1과 동일한 것이다. 다른 실시예에서, Auth4는 Auth1, Auth2 및 Auth3보다 더 약한 것이다. 예를 들어, Auth4는 단순히 사용자가 모바일 디바이스를 이용 가능한 상태로 만드는 것으로, 디바이스의 소지만을 요구할 뿐 어떠한 인증도 사실상 요구하지 않는 것이다.

[0040] 전술한 인증 레벨들은 단지 예시를 위한 것으로 제한적인 것은 아님을 유의하라. 예를 들어, 추가의 인증 레벨이 활용될 수도 있다. 이것은 다수의 거래 금액 임계치에 기반하여 상이한 레벨을 갖는 둘 이상의 결제용 인증 레벨 때문일 것이다. 정보도 민감성 및 비민감성의 둘 이상의 카테고리로 나누어질 수 있을 것이다. 더 나아가, 거래가 결제를 위한 것인지 그리고 거래가 모바일 디바이스내에 저장된 민감성 정보를 수반하는지에 대한 결정에 추가적으로 혹은 이를 대체하여 결정들이 포함될 수 있을 것이다.

[0041] 특정 인증 레벨이 요청/요구된 이후에, 요청된 정보는 단계(216)에서 사용자로부터 예컨대 사용자 모바일 디바이스를 통해 수신된다. 이 정보는 사용자가 예컨대 키패드, 키보드, 터치패드, 터치 스크린 혹은 기타 데이터 입력 장치를 통해 요청된 정보를 입력함으로써 수신될 것이다. 일단 수신되면, 정보는 단계(218)에서 결제 사업자에 의해 처리된다. 이 처리는 수신된 정보가 요청된 것인지, 그리고 수신된 정보가 기대했던 것인지를 결정하는 것을 포함할 것이다. 이것은 사용자의 계정을 액세스하는 것과 사용자의 인증 정보를 검토하는 것을 통해서 이루어질 수 있다.

[0042] 이후에 단계(220)에서 사용자가 인증될 수 있는지 결정된다. 이 결정은 결제 사업자와 관련한 전형적인 인증 프로시저를 포함하는 것으로, 부정 사용 탐지, 계정 정지, 거래 한도 등등을 포함한다.

[0043] 만약 사용자가 인증되면, 거래는 단계(222)로 이동한다. 거래는 결제 프로세스, 통신, 데이터/정보의 디스플레이 또는 액세스, 혹은 모바일 디바이스의 그 밖의 사용과 함께 진행될 수 있다. 그러나 만약 사용자 인증이 실패하면, 거래는 사용자가 인증될 때까지 진행이 허용되지 않을 것이다. 따라서, 결제 사업자는 동일한 인증 요청이나 상이한 인증 요청을 이용하여 사용자가 한 번 이상의 추가적인 인증 시도를 할 수 있게 허용할 것이다. 예를 들어, 사용자에게 보안 질문이 문의될 수 있을 것이다.

[0044] 이에 따라, 결제 사업자(및/또는 사용자)는 지갑이나 지갑의 일부분에 대한 액세스에 링크될 상이한 보안 레벨들을 설정할 수 있다. 일 예로서, 사용자는 쿠폰이나 일부 로열티 성분(예컨대 항공기 보너스 마일리지 카드 혹은 영화 극장 리워드 카드)를 보호하는 것에 대해서는 관심이 없을 수 있지만, 신용 카드 혹은 결제 수단을 보호하는 것에 대해서는 주의를 기울일 것이다. 지갑과 관련한 기본적인 디폴트 보안 설정은 고수준의 보안(이것은 사용자와 더 많은 마찰이나 상호 작용을 초래함)을 통한 거래의 속도일 것이다. 그러나 "보다 스마트한"

지갑은 약간의 사용자 상호작용과 더 나은 보안이 결제 사업자에 의해 제공될 수 있다.

[0045] 예를 들어, 사용자는 모든 거래에 대해 사용자에게 아무 것도 문의되지 않도록 결정할 수 있다. 전자 지갑이 적절히 트리거만 된다면, 거래는 계속 진행될 것이다. 보다 호기심이 있는 어떤 사용자는 모든 거래를 살펴볼 수 있고, 전자 지갑을 통해 진행되는 거래의 정보와 관련해 프롬프트되도록 요청할 것이다. 보다 보안을 원하는 다른 사용자들은 PIN, 패스워드 혹은 지문/생체 요소를 입력함으로써 거래의 실제 확인이 프롬프트되도록 결정할 수 있다. 보안 레벨은 전술한 바와 같이 거래 금액에도 링크될 수 있다. 예를 들어, \$20 미만은 어떠한 조치도 요구되지 않고, \$20에서 \$50 사이는 사용자에게 통지하는 프롬프트가 발생하며, \$50 이상은 PIN을 입력한다. 이러한 레벨들은 유연성이 있으며, 사용자에게 의해 결정되지만 결제 사업자에 의해 관리되는 리스크 프로파일에도 확인/연계된다.

[0046] 따라서, 전술한 것들을 이용하여 사용자의 모바일 디바이스를 설정하고 이 모바일 디바이스를 상이한 거래 혹은 사용에 대해 이용할 때 사용자는 다중의 보안 선택을 가질 수 있다. 이것은 사용자가 전화기를 이용할 때마다 패스워드/PIN 혹은 생체 정보를 입력하는 것을 요구하지 않으면서도 사용자가 부정 사용에 덜 노출되게 할 수 있다. 또한 다중 보안 선택은 고액 결제 또는 극도의 민감성 정보의 액세스에 대해 강화된 혹은 더 강력한 인증을 요구함으로써 모바일 디바이스의 사기성 이용으로부터 사용자를 보호할 수 있다.

[0047] 전술한 이러한 디지털 지갑에는 사용자 프로파일, 리스크 프로파일 및 선불 충전값(stored value)을 포함한 몇 개의 구성요소가 존재한다. 사용자는 전자 지갑에 대해 사용자 프로파일을 생성할 수 있다. 전형적으로, 사용자가 더 많은 정보를 제공할수록 지갑은 "더 스마트"해진다. 결제 사업자는 각각의 거래와 관련해 펀딩 수단에 대해 보다 근거있는 결정(informed decision)을 내리는데 이러한 정보를 이용할 수 있다. 사용자가 프로파일에 무엇을 입력할 것인지에 대한 예로서, 소비 선호도, 소비 한도, 목표, 선호하는 펀딩 수단 등을 들 수 있다. 사용자 프로파일은 예컨대 프로파일 정보를 변경함으로써 사용자에게 의해 변경될 수 있다. 또한 프로파일은 사용자 거래에 기반하여 결제 사업자에 의해 변경될 수도 있다. 예를 들어, 만약 사용자가 결제 사업자가 제안하거나 제시하는 펀딩 수단들을 계속해서 변경하면, 결제 사업자는 사용자 선호도를 반영하여 그에 따라 사용자 프로파일을 변경할 수 있을 것이다.

[0048] 다른 구성요소인 사용자의 리스크 프로파일은 결제 사업자로부터의 파라미터 혹은 정보에 부분적으로 기반할 것이다. 예를 들어, 검증된 주소와 결제 수단(예컨대 사용자의 결제 사업자 계정과 링크되어 검증된 은행 계정)과 함께 결제 사업자 서비스를 장기간 이용하는 사용자는, 방금 등록하여 자신의 계정에 링크/검증된 어떠한 은행 계정도 갖고 있지 않은 사용자보다 더 나은 리스크 프로파일을 가질 것이다. 사용자 리스크 프로파일을 구성하는데 이용될 수 있는 다른 요소는 사용자의 모바일 디바이스의 제품/모델이다(예를 들어 이것이 결제 사업자에게 등록(전화 번호뿐만 아니라 하드웨어/소프트웨어 구성, 브라우저 등등)되는 경우). 주요 리스크 프로파일이 클라우드에 저장될 수도 있지만, 특히 선불 충전값을 이용하는 "오프라인" 거래에 대한 파라미터의 특정 세트와 함께 서브넷 버전이 모바일 디바이스상에 저장될 수 있다.

[0049] 선불 충전값은 사용자가 결제를 위해 결제 사업자에게 잔고로 유지하는 현금이다. 결제 사업자는 사용자의 모바일 디바이스상에 이 잔고의 "가격예측(extrapolation)"을 생성할 것이다. 이 선불 충전값은 사용자의 리스크 프로파일에 링크될 것이다. 예를 들어, 만약 우수한 리스크 프로파일을 갖는 사용자가 자신의 결제 사업자 계정에 \$500의 잔고를 갖는다면, 결제 사업자는 사용자가 \$400의 선불 충전값 혹은 최대 \$500의 선불 충전값에 액세스하는 것을 승인할 것이다. 검증되지 않은 계정을 가지며 결제 사업자에게 신규 가입한 사용자는 결제 사업자에게 \$500의 잔고를 갖는다하더라도, 단지 \$5 혹은 \$50의 선불 충전값 긴급 액세스만 허용되거나, 또는 해당 사용자에게 대해 결제 사업자가 용인할 수 있는 리스크의 정도라고 간주되는 소정 금액의 선불 충전값 긴급 액세스만 허용될 것이다.

[0050] 일 실시예로, 결제 사업자는 클라우드내에 남은 잔고에 대해 소비중인 선불 충전값을 강제로 검증하는 능력을 필요로 하는 동적 선불 충전값 관리 시스템을 보유한다. 모바일 디바이스에 기반한 데이터로 결제 사업자는 계좌 잔고에 대한 선불 충전값 소비 이력을 지속적으로 실시간 피드백할 수 있다. 그러나, 제한적인 기능을 갖는 일부 모바일 디바이스나 로우 배터리 모드 상태인 모바일 디바이스의 경우에는, 결제 사업자가 이 이력을 피드백할 수 없을 수도 있고, 오프라인/온라인 클라우드 모드에서 액세스의 레벨을 승인해야만 할 것이다. 일 실시예로, 사용자는 마지막 지하철을 타려고 하는 중이고, 이 사용자의 모바일 디바이스는 NFC-가능형이지만 배터리가 거의 소진된 상태이다. 그러나 지하철 회사의 비접촉 관독기는 사용자 디바이스상의 NFC 칩에 대해 작동하여 티켓 및/또는 결제를 검색하도록 단시간에 충분한 에너지를 증진시켜서 게이트를 통과하는 액세스를 승인하도록 설정되어 있다. 이 시점에서, 결제 사업자는 클라우드에 대한 검증을 피드백하는 옵션을 갖지 않을 수도

있지만, "전자 지갑"은 필요한 오프라인 자금을 제공할 수 있다(그리고 장래의 동기화를 위해 거래 이력 로그에 등록할 수도 있다). 이렇게 함으로써, 결제 사업자는 리스크를 감수하지만 사용자가 자신이 기대했던 것 즉, 온라인 결제 거래와 동일한 경험을 하게 만든다.

[0051] 결제 사업자는 선불 충전값 잔고에 대해 적용되는 오프라인 거래 이력 로그로부터 오프라인 거래를 관리할 수 있다. 그러나, 리스크 프로파일에 기반하여, 결제 사업자는 전자 지갑의 이 기능에 예컨대 거래 횟수, 거래 금액, 오프라인 시간 등등의 파라미터를 연계시키고, 선불 충전값 잔고와 전자 지갑을 갱신시키도록 클라우드에 대한 접속을 유지시킬 것이다.

[0052] 사용자와 리스크 프로파일을 관리하기 위해, 전자 지갑의 일부 기능(예를 들면, 사용자 위치, 특정 핸드셋의 사용자 선호도, 거래 로그 이력 등등)을 트리거하도록 데이터를 매칭시키는 것과 함께 백-엔드 모듈이 전자 지갑의 "스마트" 또는 지능 부분을 담당할 것이다. 이것은 결제 사업자 시스템의 일부 구성요소에 의해 관리될 수 있다. 이렇게 하고 "중간" 버퍼를 생성함으로써, 결제 사업자는 보다 빠른 서비스를 모바일 디바이스에게 전달할 수 있으며, 리스크 프로파일에 대해 선불 충전값을 보다 잘 관리하면서도 결제 사업자 코어 시스템에 상주하는 주요 사용자 계정을 필요에 따라 보호/차단할 수 있다.

[0053] 기술적인 관점에서, 지갑은 모바일 디바이스에 상주하는 애플리케이션이며, 클라우드내의 결제 사업자에게 링크될 수 있을 것이다. 지갑의 일부 구성요소(예컨대, 사용자 인터페이스)는 Java 애플릿, 위젯 또는 네이티브 형식 같은 정규 애플리케이션일 수 있다. 그러나, 보안 기능(피싱 방지, 스푸핑 방지 메커니즘 등)은 기본 기능과 별개로 생각할 필요가 있고, 모바일 디바이스상의 "확실히 믿을 수 있는" 요소/구성요소에서 런치되어야 할 것이다. 이것은 하드웨어 및/또는 소프트웨어 구성요소일 수 있다. 이러한 구성요소의 예로서, ARM의 TrustZone, Embedded Secure Element, MicroSD 카드 또는 SIM 카드가 있다. 일 실시예로, 전자 지갑 또는 계정은 클라우드내에 줄곧 유지되고, 이것을 보호하는 이 메커니즘은 사용자나 모바일 디바이스에 전혀 노출되지 않는다. 이런 이유로, 사용자와 리스크 프로파일은 다르게 관리된다.

[0054] 이후의 설명은 전자 지갑 사용 케이스의 일 예를 제시한다. Costco 고객은 AMEX Costco 브랜드명 카드를 갖는다. 이 고객은 정기적으로 자신의 집 근처 Costco 매장에 간다. 매장/상점에서 이 사용자의 결제 이력을 모니터링함으로써, 사업자는 사용자가 AMEX 카드를 이용해서 90%의 사용빈도로 결제함을 알 것이다. 나머지 10%는 직불 카드를 이용한 결제이다. 이 두 결제 수단은 사용자의 결제 사업자 계정에 등록된다.

[0055] (매장 혹은 상점을 결제 사업자가 알고 있거나 또는 결제 사업자가 영업장 주소 등록을 생성했다고 가정하고) 전자 지갑을 이용함으로써, 사용자는 자신에게 다음과 같이 제안되는 디폴트 결제 수단을 가질 수 있다. 즉,

[0056] 1) 결제 수단 #1 (제 1 순위): AMEX Costco 카드

[0057] 2) 결제 수단 #2 (제 2 순위): 직불 카드

[0058] 3) 결제 수단 #3 (선불 충전값) : 현실 세계에서 결제 사업자 잔고 증액

[0059] 사용자는 원하는 대로 편집 또는 변경할 수 있다.

[0060] 이 선택은 사용자 프로파일과, 사용자의 특정 위치(GPS 위치 활용)와, 그리고 (가능하다면) 사용자의 모바일 디바이스에 전송되어 전자 지갑에 의해 판독된 매장 "무선" 신호에 의해(예컨대 NFC 태그, 블루투스(기존의 페어링) 등을 통해) 트리거될 것이다. 데이터를 삼각측량함으로써, 전자 지갑은 결제 수단의 선택을 향상시킬 수 있을 것이다.

[0061] 사용자가 금전 등록기에 도착하면, 사용자는 예컨대 NFC 채널, 원격/온라인 세션 등을 통해 결제 사업자에게 연결한다. 금액, 매장, 판매자, 구매 유형 등의 거래 정보가 결제 사업자에게 통신되고, 그와 함께 사용자 및/또는 POS의 위치 및 기타 정보가 결제 사업자에 의해 요구된다. 결제 사업자는 사용자의 계정과 선호도에 액세스하여, 어떤 펀딩 수단 혹은 어떠한 펀딩 수단의 조합을 자동적으로 이용할 것인지 결정한다.

[0062] 도 3은 본 발명의 일 실시예에 따라 전술한 것처럼 전자 지갑을 이용한 거래를 취급하도록 구성된 네트워크 시스템(300)의 블록도이다. 시스템(300)은 네트워크(360)를 통해 통신하는 사용자 디바이스(310), 판매자 디바이스(340) 및 결제 사업자 서버(370)를 포함한다. 결제 사업자 서버(370)는 예컨대 캘리포니아 산호세 소재의 PayPal사와 같은 결제 사업자에 의해 보유될 것이다. 발송자 혹은 고객인 사용자(305)는 결제 사업자 서버(370)를 이용하여 거래를 수행하기 위해 사용자 디바이스(310)를 활용한다. 본원에서 설명하고 있는 거래란, 결제, 정보 전송, 정보 디스플레이 등을 포함하여 사용자 디바이스를 이용하여 수행되는 모든 적절한 조치를 연

급함을 유의하라.

- [0063] 사용자 디바이스(310), 판매자 서버(340) 및 결제 사업자 서버(370)는 각각 예컨대 프로그램 코드 및/또는 하나 이상의 컴퓨터 판독가능 매체에 저장된 데이터 같은 명령어를 실행하기 위한 하나 이상의 프로세서, 메모리 및 기타 적합한 구성요소를 포함하여, 본원에 설명된 다양한 애플리케이션, 데이터 및 단계들을 구현할 것이다. 예를 들어, 이러한 명령어들은 시스템(300)의 여러 구성요소들에 대해 내장 및/또는 외장되는 메모리나 데이터 저장 장치같은 하나 이상의 컴퓨터 판독 가능 매체내에 기억될 수도 있고, 또는 네트워크(360)를 통해 액세스 가능할 수도 있다.
- [0064] 네트워크(360)는 단일 네트워크로 구현될 수도 있고, 혹은 다중 네트워크의 조합으로 구현될 수도 있다. 예를 들어, 다양한 실시예로, 네트워크(360)가 인터넷이나 하나 이상의 인트라넷, 지상통신선 네트워크, 무선 네트워크 및/또는 기타 적절한 유형의 네트워크를 포함할 수 있다.
- [0065] 사용자 디바이스(310)는 네트워크(360)를 통해 유선 및/또는 무선 통신하도록 구성된 모든 적절한 하드웨어와 소프트웨어를 이용하여 구현될 것이다. 예를 들어, 일 실시예로, 사용자 디바이스는 개인용 컴퓨터(PC), 스마트폰, 휴대 정보 단말기(PDA), 랩탑 컴퓨터 및/또는 Apple™사의 iPad™처럼 데이터를 송수신할 수 있는 기타 유형의 컴퓨터 장치로 구현될 수 있다.
- [0066] 사용자 디바이스(310)는 하나 이상의 브라우저 애플리케이션(315)을 포함할 수 있고, 이것은 예컨대 네트워크(360)를 통해 입수 가능한 정보를 사용자(305)가 브라우즈할 수 있게 하는 편리한 인터페이스를 제공하는데 이용될 것이다. 예를 들어, 일 실시예로, 브라우저 애플리케이션(315)은 로열티 사이트를 액세스하는 것을 포함해서 인터넷을 통해 이용 가능한 정보를 보여주도록 구성된 웹 브라우저로서 구현될 수 있을 것이다. 사용자 디바이스(310)는 또한 하나 이상의 툴바 애플리케이션(320)을 포함할 수 있고, 이것은 예를 들어 사용자(305)에 의해 선택된 동작들에 대한 응답으로서 원하는 태스크를 수행하는 클라이언트측 프로세싱을 제공하는데 이용될 수 있을 것이다. 일 실시예로, 툴바 애플리케이션(320)은 이후에 본원에서 설명되는 것처럼 브라우저 애플리케이션(315)과 함께 사용자 인터페이스를 디스플레이할 수 있을 것이다.
- [0067] 사용자 디바이스(310)는 또한 사용자 디바이스(310)에 원하는 특징들을 제공하도록 특별한 실시예로서 희망될 수 있는 다른 애플리케이션(325)을 더 포함할 수 있다. 예를 들면, 다른 애플리케이션(325)으로서, 클라이언트측 보안 특징을 구현하는 보안 애플리케이션, 네트워크(360)를 통해 적절한 애플리케이션 프로그래밍 인터페이스(APIs)와 인터페이스하는 프로그램 방식의 클라이언트 애플리케이션, 또는 기타 유형의 애플리케이션 등이 있다. 애플리케이션(325)은 또한 사용자(305)로 하여금 네트워크(360)를 통해 이메일, 전화 통화 및 문자를 송수신할 수 있게 하는 이메일, 텍스트, 음성 및 IM 애플리케이션 뿐만 아니라, 사용자로 하여금 통신하고 정보를 전송하고 결제를 수행하고 그 밖에 전술한 것처럼 결제 사업자를 통해 전자 지갑을 활용할 수 있게 하는 애플리케이션도 포함할 수 있다. 사용자 디바이스(310)는 하나 이상의 사용자 식별자(330)를 포함하는데, 이것은 예를 들면 운영 체제 레지스트리 엔트리, 브라우저 애플리케이션(315)과 연계된 쿠키, 사용자 디바이스(310)의 하드웨어와 연계된 식별자들, 혹은 예컨대 결제/사용자/디바이스 인증에 이용되는 그 밖의 적절한 식별자들로 구현될 수 있다. 일 실시예로, 사용자 식별자(330)는 본원에 더 설명되듯이 사용자(305)를 결제 사업자에게 보유된 특정 계정과 연계시키기 위해 결제 서비스 사업자에 의해 이용될 것이다. 통신 애플리케이션(322)은 연관 인터페이스와 함께 사용자 디바이스(310)가 시스템(300)내에서 통신할 수 있게 한다.
- [0068] 판매자 서버(340)는 예를 들어 네트워크(360)를 통해 수신될 결제와 맞바꿀 다양한 상품 및/또는 서비스를 제공하는 판매자 혹은 상인에 의해 보유될 것이다. 판매자 서버(340)는 POS 또는 온라인 구매 및 거래를 위해 이용될 것이다. 일반적으로, 판매자 서버(340)는 돈을 수신하는 자선 단체 뿐만 아니라 소매상인 및 음식점을 포함한 누군가 혹은 어떤 엔티티에 의해 보유될 것이다. 판매자 서버(340)는 사용자(305)가 둘러보고 구매할 수 있는 이용 가능한 상품 및/또는 서비스(예컨대 일괄적으로 아이템이라 칭함)를 식별하는 데이터베이스(345)를 포함한다. 따라서 판매자 서버(340)는 네트워크(360)를 통해 사용자 디바이스(310)의 브라우저(315)로 정보를 제공하도록 구성될 수 있는 마켓플레이스 애플리케이션(350)을 포함한다. 일 실시예로, 사용자(305)는 데이터베이스(345)에서 식별되는 다양한 상품, 식료품 아이템 또는 서비스를 살펴보기 위해서 네트워크(360)를 건너 브라우저 애플리케이션을 통해 마켓플레이스 애플리케이션(350)과 상호 작용할 수 있다.
- [0069] 판매자 서버(340)는 또한 마켓플레이스 애플리케이션(350)에 의해 식별되는 상품 혹은 서비스를 사용자(305)가 구매하는 것을 도와주도록 구성될 수 있는 체크아웃 애플리케이션(355)을 포함한다. 체크아웃 애플리케이션(355)은 전자 지갑으로부터 선택된 펀딩 수단을 이용하여 네트워크(360)를 건너 결제 서비스 사업자 서버(370)를 통해 사용자(305)로부터, 혹은 사용자를 대신하여 결제 정보를 수용하도록 구성될 것이다. 예를 들어, 체크

아웃 애플리케이션(355)은 결제 서비스 사업자 서버(370)로부터 결제 확인을 수신하여 처리하고, 더불어 결제 사업자에게로 거래 정보를 전송하고 결제 사업자로부터 정보(예컨대 거래 ID)를 수신한다.

[0070] 결제 사업자 서버(370)는 예를 들어 사용자(305)와 판매자 서버(340) 사이에 결제를 제공하는 온라인 결제 서비스 사업자에 의해 보유될 수 있다. 이와 관련하여, 결제 사업자 서버(370)는 상품 혹은 서비스의 구매, 정보의 통신/디스플레이, 사용자 디바이스(310)의 사용자(305)에 의한 결제의 전송, 그리고 전송한 것들을 용이하게 하기 위해 네트워크(360)를 통해 사용자 디바이스(310) 및/또는 판매자 서버(340)와 상호작용하도록 구성된 하나 이상의 결제 애플리케이션(375)을 포함한다.

[0071] 결제 사업자 서버(370)는 또한 다수의 사용자 계정(380)을 보유하고 있고, 이들 각각은 각각의 사용자와 연계된 계정 정보(385)를 포함하고 있다. 예를 들어, 계정 정보(385)는 계정 번호, 패스워드, 디바이스 식별자, 사용자 이름, 전화 번호, 신용 카드 정보, 은행 정보, 또는 사용자(305)에 의한 온라인 거래를 용이하게 하는데 이용될 수 있는 그 밖의 재정 정보처럼 디바이스 사용자의 개인적인 재정 정보를 포함할 것이다. 바람직하게는, 사용자의 보너스 포인트 뿐만 아니라 사용자에게 의해 행해진 구매와 이용되는 펀딩 소스를 추적 관리하기 위해 체크아웃 애플리케이션(355)과 함께 거래하는 동안 결제 애플리케이션(375)이 사용자(305)를 대신하여 판매자 서버(340)와 상호작용하도록 구성될 것이다.

[0072] 결제 애플리케이션(375)의 일부를 구성하거나 혹은 별개로 구성될 수 있는 거래 처리 애플리케이션(390)은 결제 데이터베이스(395)에 저장 및 처리하기 위해 사용자 디바이스 및/또는 판매자 서버(340)로부터 정보를 수신하도록 구성될 것이다. 거래 처리 애플리케이션(390)은 본원에 설명된 것처럼 다양한 선택된 펀딩 수단을 이용한 주문 및 결제를 처리하기 위해 사용자(305)로부터의 정보를 처리하는 하나 이상의 애플리케이션을 포함할 수 있다. 이런 맥락에서, 거래 처리 애플리케이션(390)이 개별 사용자로부터의 구매와 연계된 주문의 세부사항을 저장할 수도 있을 것이다. 결제 애플리케이션(375)은 또한 사용자(305)와 관련한 계정의 존재를 결정하여 관리하도록 구성될 수 있을 뿐만 아니라 필요하다면 사용자/모바일 디바이스를 위한 전자 지급의 설정, 관리 및 사용처럼 신규 계정을 생성하도록 구성될 수도 있다.

[0073] 도 4는 본원의 하나 이상의 실시예를 구현하기에 적합한 컴퓨터 시스템(400)의 블록도이다. 다양한 실시예에서, 사용자 디바이스는 네트워크와 통신할 수 있는 개인용 컴퓨터 장치(예컨대 스마트폰, 컴퓨터 태블릿, 개인용 컴퓨터, 랩탑, PDA, 블루투스 디바이스, 키 FOB, 배지(badge) 등)를 포함할 것이다. 판매자 및/또는 결제 사업자는 네트워크와 통신할 수 있는 네트워크 컴퓨터 장치(예컨대 네트워크 서버)를 활용할 수 있다. 사용자, 판매자 및 결제 사업자가 활용하는 각각의 디바이스는 다음과 같은 방식으로 컴퓨터 시스템(400)으로서 구현될 수 있다.

[0074] 컴퓨터 시스템(400)은 컴퓨터 시스템(400)의 다양한 구성요소들 사이에 정보 데이터, 신호 및 정보를 통신할 수 있는 버스(402) 혹은 그 밖의 통신 메커니즘을 포함한다. 구성요소중에는 예컨대 키패드/키보드에서 키를 선택하거나 하나 이상의 버튼 혹은 링크를 선택하거나 대응하는 신호를 버스(402)로 전송하는 등의 사용자 조치를 처리하는 입력/출력(I/O) 요소(404)도 포함된다. I/O 요소(404)는 또한 디스플레이(411) 및 커서 컨트롤(413)(키보드, 키패드, 마우스 등등)같은 출력 요소를 포함할 수도 있다. 선택적인 오디오 입력/출력 요소(405)는 사용자로 하여금 음성을 사용하여 정보를 입력하면 이를 오디오 신호로 변환할 수 있게 하기 위해 포함된다. 오디오 I/O 요소(405)는 사용자가 오디오를 들을 수 있게도 할 것이다. 트랜시버 혹은 네트워크 인터페이스(406)는 네트워크(360)를 건너 컴퓨터 시스템(400)과 예컨대 사용자 디바이스, 판매자 서버 혹은 결제 사업자 서버같은 다른 디바이스들 사이에 신호를 송신 및 수신한다. 일 실시예로, 비록 다른 송신 매체와 방법이 사용될 수 있더라도 송신은 무선으로 이루어진다. 마이크로 컨트롤러, 디지털 신호 프로세서(DSP) 혹은 그 밖의 처리 구성요소일 수 있는 프로세서(412)가 다양한 신호를 처리하여, 컴퓨터 시스템(400)에 디스플레이하거나 통신 링크(418)를 통해 다른 디바이스로 송신한다. 프로세서(412)는 또한 쿠키 혹은 IP 주소같은 정보를 다른 디바이스로 전송하는 것을 제어할 수도 있다.

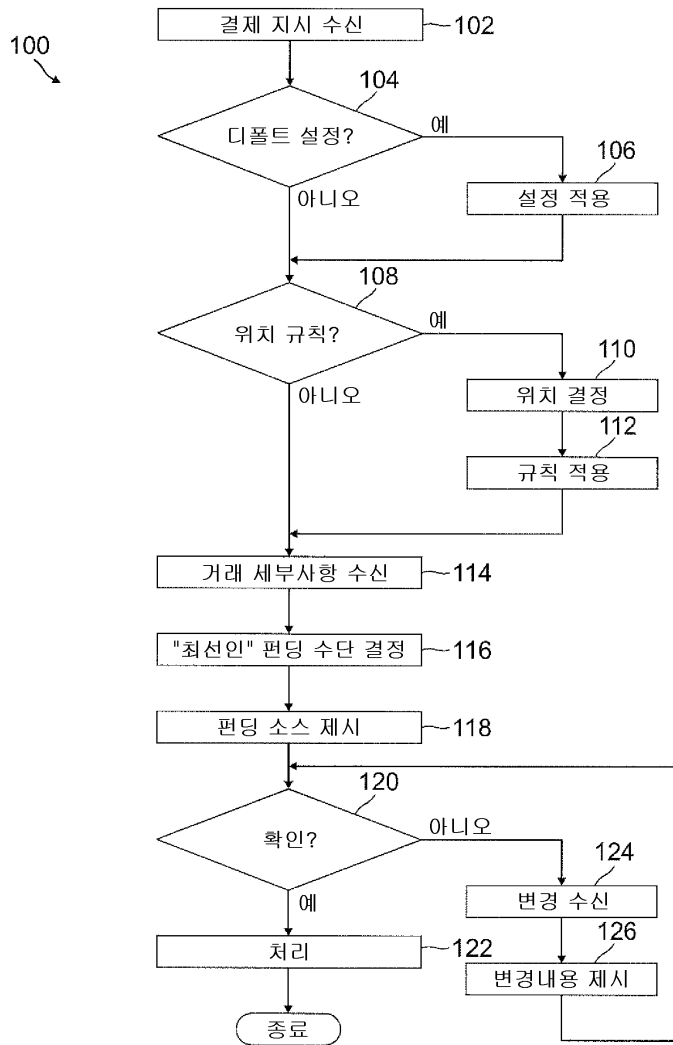
[0075] 컴퓨터 시스템(400)의 구성요소들로서, 시스템 메모리 요소(414)(예컨대 RAM), 정적 저장장치 요소(416)(예컨대 ROM) 및/또는 디스크 드라이브(417)이 포함된다. 컴퓨터 시스템(400)은 시스템 메모리 요소(414)내에 포함된 하나 이상의 명령어 시퀀스를 실행함으로써 프로세서(412)와 다른 구성요소들을 이용해 특정 동작을 수행한다. 로직이 컴퓨터 판독 가능 매체에 인코딩된 것이고, 이때 컴퓨터 판독 가능 매체란, 실행을 위해 프로세서(412)에 명령어를 제공함에 관여하는 모든 매체를 일컫는다. 이러한 매체는 비휘발성 매체, 휘발성 매체 및 전송 매체를 포함한 많은 형태를 취할 수 있으며, 제한적인 것은 아니다. 다양한 구현예에서, 비휘발성 매체는 광학 또는 자기 디스크를 포함하고, 휘발성 매체는 시스템 메모리 요소(414)같은 동적 메모리를 포함하며, 전송 매체

는 버스(402)를 구성하는 유선을 포함한 동축 케이블, 구리선 및 광섬유를 포함한다. 일 실시예로, 로직은 영구적인 컴퓨터 판독 가능 매체로 인코딩된다. 일 예로, 전송 매체는 전파 통신, 광 통신 및 적외선 데이터 통신동안 발생하는 음향과 또는 광파의 형태를 취할 수 있다.

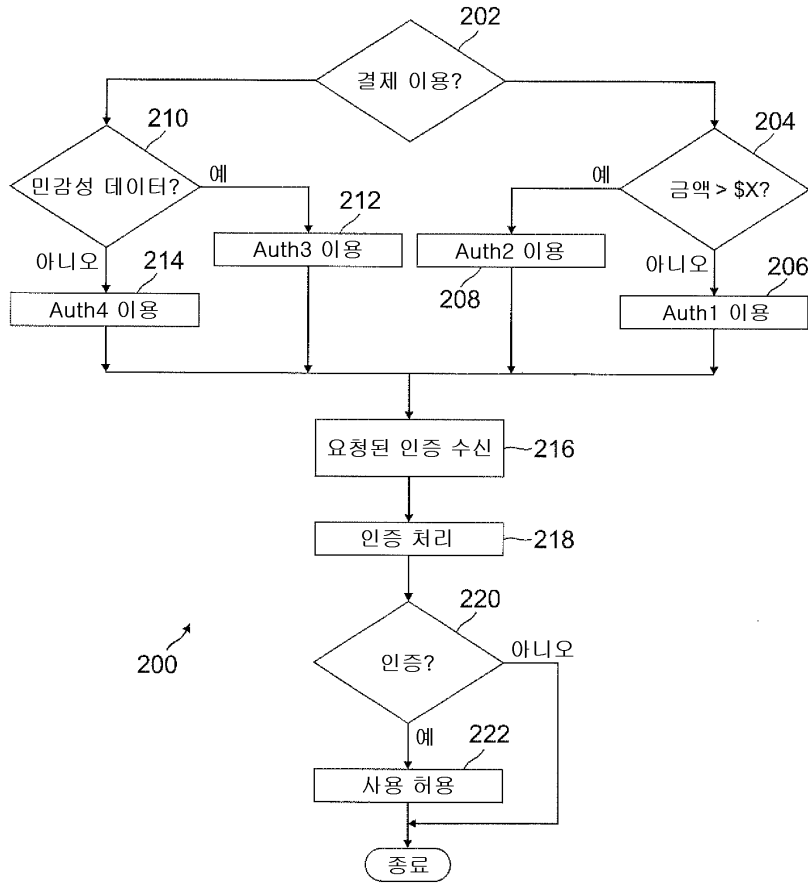
- [0076] 컴퓨터 판독 가능 매체의 몇몇 흔한 형태의 예를 들면, 플로피 디스크, 플렉시블 디스크, 하드 디스크, 자기 테이프, 기타 자기 매체, CD-ROM, 기타 광학 매체, 펀치 카드, 페이퍼 테이프, 천공 패턴을 갖는 기타 물리적 매체, RAM, PROM, EPROM, FLASH-EPROM, 기타 다른 메모리 칩이나 카트리지, 혹은 컴퓨터가 판독하도록 되어 있는 그 밖의 다른 매체가 있다.
- [0077] 본원의 다양한 실시예에서, 본 개시물의 내용을 실시하기 위한 명령어 시퀀스의 실행은 컴퓨터 시스템(400)에 의해 수행될 것이다. 본 발명의 다양한 다른 실시예로, 통신 링크(418)에 의해 네트워크(예컨대 LAN, WLAN, PTSN 및/또는 전기통신, 모바일 및 셀룰러폰 네트워크를 포함한 그 밖의 여러 유무선 네트워크)에 접속된 복수의 컴퓨터 시스템들(400)이 서로 협력하여 본 개시물의 내용을 실시하도록 명령어 시퀀스를 수행할 수도 있다.
- [0078] 적용가능하다면, 본원에 제시된 다양한 실시예들은 하드웨어, 소프트웨어 또는 하드웨어와 소프트웨어의 조합으로 구현될 수 있을 것이다. 또한, 적용가능하다면, 본원에 설정된 다양한 하드웨어 구성요소들 및/또는 소프트웨어 구성요소들은 본원의 사상을 이탈하지 않는 범위내에서 소프트웨어, 하드웨어 및/또는 이 둘을 모두 포함하는 복합적인 구성요소들로 결합될 수 있을 것이다. 적용가능하다면, 본원에 설정된 다양한 하드웨어 구성요소 및/또는 소프트웨어 구성요소는 본원의 사상을 이탈하지 않는 범위내에서 소프트웨어, 하드웨어 또는 이 둘을 포함하는 부분 구성요소들로 분리될 수 있을 것이다. 또한, 적용가능하다면, 소프트웨어 구성요소들이 하드웨어 구성요소들로 구현되거나 혹은 그 반대의 경우도 고려해볼 수 있을 것이다.
- [0079] 본원에 따르면, 프로그램 코드 및/또는 데이터같은 소프트웨어가 하나 이상의 컴퓨터 판독 가능 매체상에 기억될 수 있다. 또한 본원에서 식별되는 소프트웨어는 하나 이상의 범용 혹은 전용 컴퓨터 및/또는 컴퓨터 시스템, 네트워크 및/또는 그 밖의 대응물을 이용하여 구현될 수 있을 것이다. 적용가능하다면, 본원에 설명된 다양한 단계들의 순서는 본원의 특징을 제공하기 위해 변경될 수 있고, 복합 단계들로 조합될 수도 있으며, 부분 단계들로 분리될 수도 있다.
- [0080] 전술한 개시 내용들은 본 발명을 특정 형태로 제한하거나 혹은 개시된 특별한 사용 분야로 한정하려는 의도는 아니다. 이와 같은 맥락으로, 본원에 명시적으로 설명되었든 암시되었든간에 본 발명의 다양한 대체 실시예 및/또는 변형 실시예들이 본 개시내용의 견지에서 가능함을 고려해야 한다. 따라서, 당업자라면 본원의 전술한 실시예로부터 본원의 사상을 벗어나지 않으면서 세부사항과 그 형태를 변경할 수 있음을 인지할 것이다. 그러므로 본원은 오로지 특허청구범위에 의해서만 한정된다.

도면

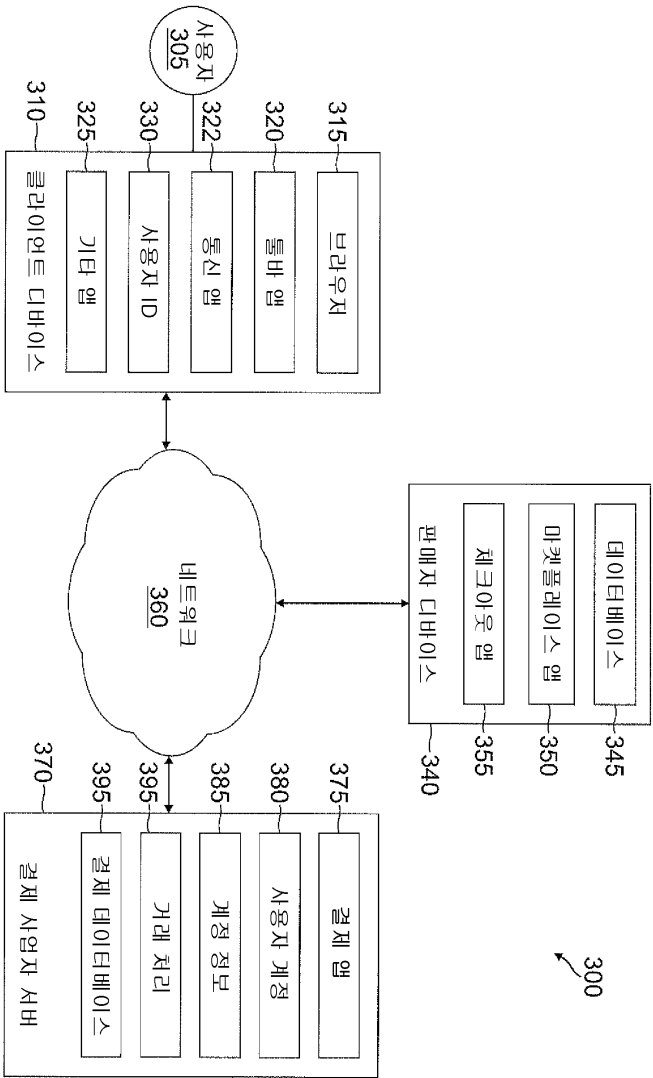
도면1



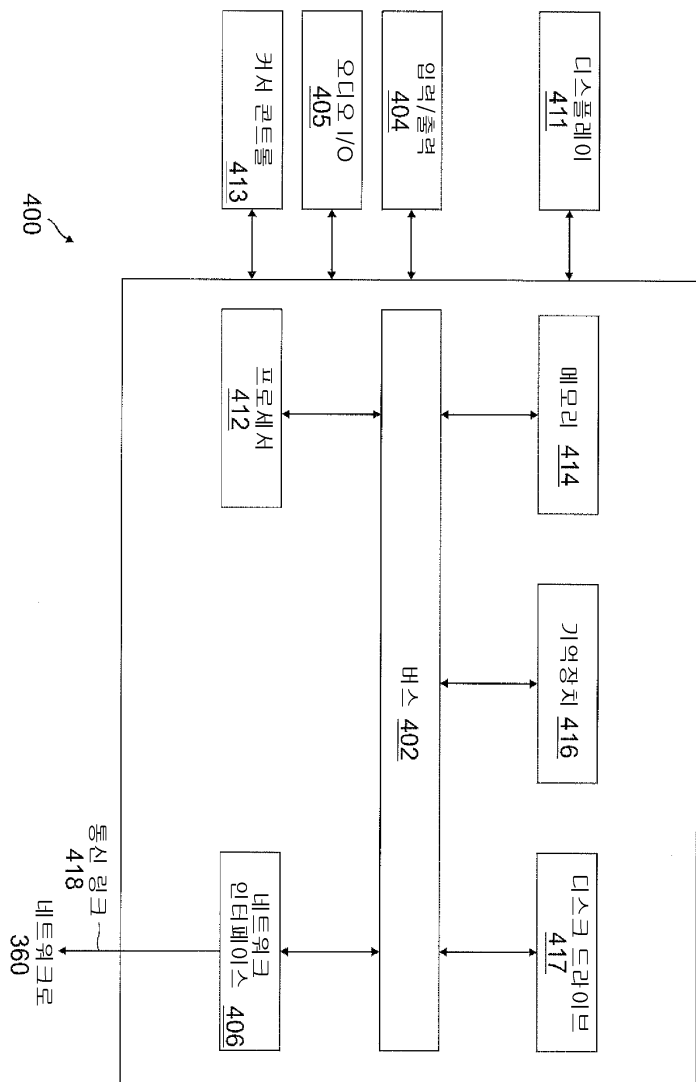
도면2



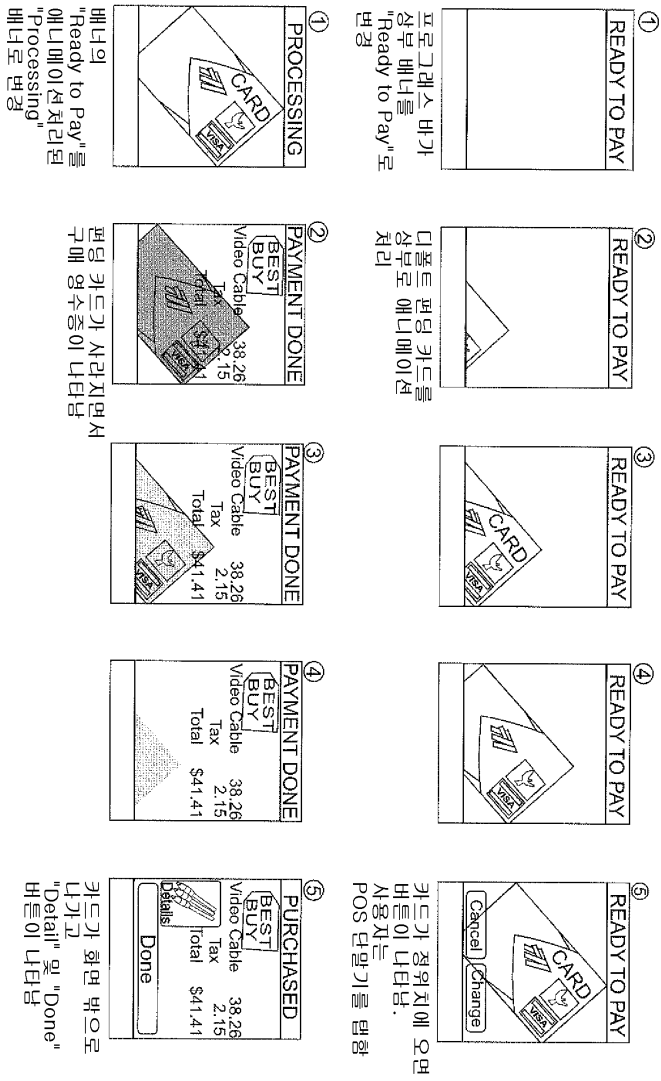
도면3



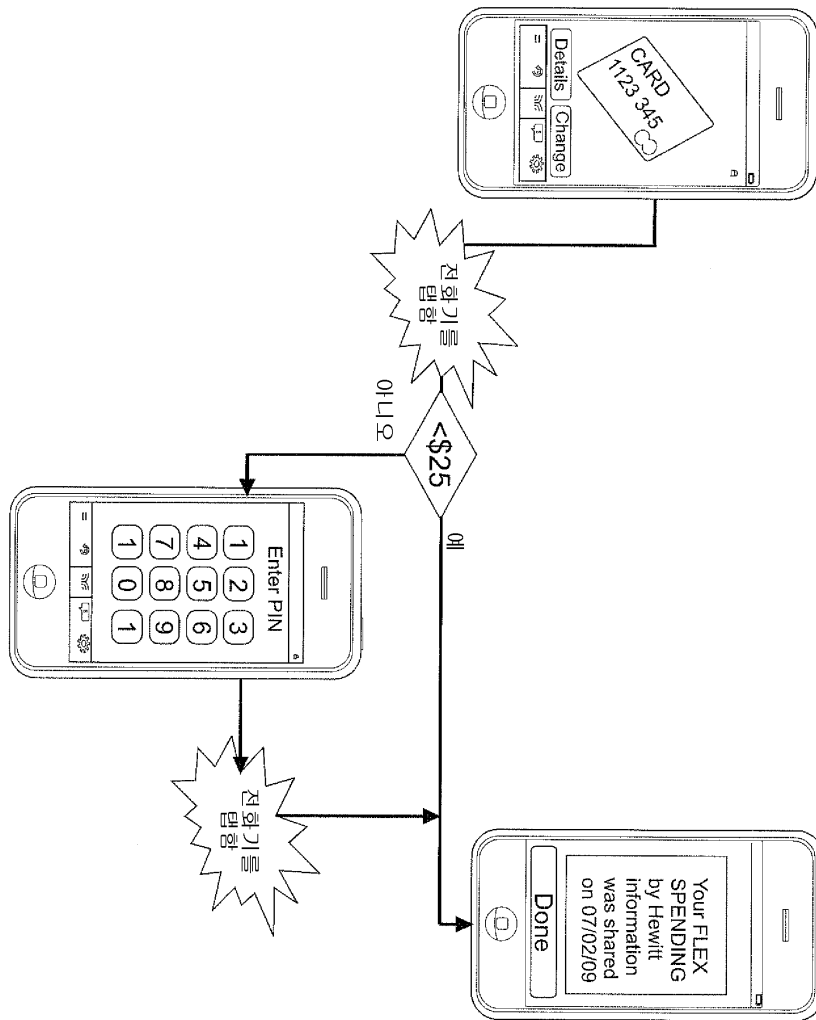
도면4



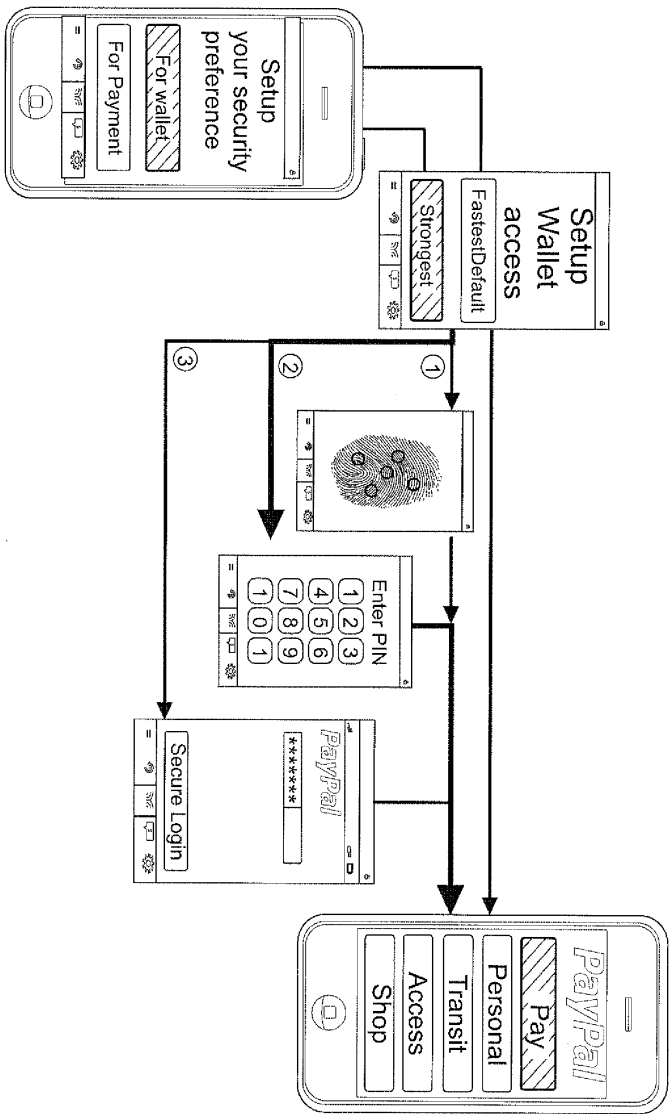
도면5a



도면5b



도면5c



도면5d

