(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0077793
(43) 공개일자 2009년07월15일

(51) Int. Cl.
G06Q 20/00 (2006.01) *G06Q 30/00* (2006.01)
G06F 21/20 (2006.01)
(21) 출원번호 10-2009-7008350
(22) 출원일자 2007년09월14일
심사청구일자 없음
(85) 번역문제출일자 2009년04월23일
(86) 국제출원번호 PCT/CA2007/001639
(87) 국제공개번호 WO 2008/037062
국제공개일자 2008년04월03일
(30) 우선권주장
11/537,461 2006년09월29일 미국(US)

(71) 출원인
스캠멜, 댄
캐나다 브이3이 3씨9, 브리티쉬 컬럼비아, 코퀴틀램, 햄튼 드라이브 1729
(72) 발명자
굳인, 스튜어트
캐나다 브이3제이 2엘5 브리티쉬 컬럼비아, 코퀴틀램, 포스터 애비뉴 스위트 208-515
(74) 대리인
이재민

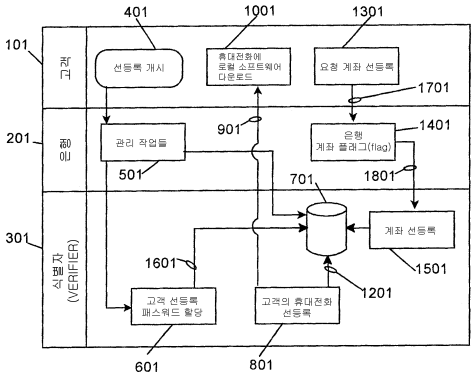
전체 청구항 수 : 총 20 항

(54) 전자상거래에서 사용자의 신원을 확인하기 위한 방법 및 시스템

(57) 요 약

본 발명은 전자상거래의 과정에서 검사기(verifier)를 통해 사용자의 신원을 확인하기 위한 방법 및 시스템이다. 본 발명은, 검사기가 전자상거래를 시작하는 사용자의 신원을 확인하기 위한 신원확인절차를 완료할 때까지, 거래를 차단하기 위한 방법 및 시스템을 제공한다. 상기 방법은 사용자 및 그 사용자의 개인통신장치를 선등록(pre-enrolling)하는 것을 포함한다. 선택적으로, 사용자의 신원확인이 요구되는 그러한 거래들을 플래깅(flagging)하는 것에 의해 하나 또는 그 이상의 거래들이 등록된다. 거래가 개시되는 시점에서, 검사기는 전자상거래를 시작하는 사용자의 휴대용 통신장치에 신원확인요청(IRV: identification verification request)을 보낸다. 이후, 사용자는 상기 신원확인요청에 대한 응답으로 안전한 식별자(identifier)를 제공함으로써 자신의 신원을 확인한다. 선택적으로, 거래가 받아들여지기 전에, 그 거래에 대한 사용자의 승인이 요구된다.

대 표 도 - 도1



특허청구의 범위

청구항 1

전자상거래의 과정에서 식별자(verifier)에 의한 사용자의 신원을 확인하는 방법에 있어서,

(a) 아래의 단계들((a1),(a2))을 포함하는, 사용자를 선등록하는 단계:

(a1) 사용자에게 진실 보안 식별자(bona fide secure identifier)를 할당하는 단계; 및

(a2) 식별자-데이터베이스에 상기 진실 보안 식별자를 저장하는 단계;

(b) 아래의 단계들((b1),(b2))을 포함하는, 사용자 통신장치를 선등록하는 단계:

(b1) 상기 사용자 통신장치와의 통신링크를 열기 위해 사용될 수 있는 사용자 통신장치에 대한 사용자 접속번호를 얻는 단계; 및

(b2) 식별자-데이터베이스에 상기 사용자 접속번호를 저장하는 단계;

(c) 상기 식별자-데이터베이스로부터 상기 사용자 접속번호를 검색하여 불러오는 단계;

(d) 상기 (c)단계를 통해 검색된 사용자 접속번호를 이용하여 상기 식별자와 상기 사용자 통신장치 사이에 통신링크를 여는 단계;

(e) 상기 (d)단계를 통해 열려진 통신링크를 이용하여 상기 식별자로부터 상기 사용자에게로 신원확인요청(IVR)을 보내는 단계;

(f) 상기 사용자로 하여금 추정 보안 식별자(putative secure identifier)를 입력하게 하는 단계;

(g) 상기 (d)단계를 통해 열려진 통신링크를 이용하여 상기 (e)단계의 신원확인요청(IVR)에 대한 응답을 보내는 단계;

(h) 상기 (a2)단계를 통해 저장된 진실 보안 식별자를 검색하여 불러오는 단계;

(i) 상기 (f)단계를 통해 입력된 추정 보안 식별자와 상기 (h)단계를 통해 검색된 진실 보안 식별자를 비교하는 단계; 및

(j) 상기 (i)단계에 따른 비교결과, 상기 추정 보안 식별자와 진실 보안 식별자가 일치하는 경우에 상기 전자상거래의 진행을 허가하는 단계

를 포함하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 2

제 1 항에 있어서,

상기 (g)단계를 통해 보내지는 응답에 상기 (f)단계를 통해 입력된 추정 보안 식별자가 포함되고, 상기 (i)단계는 상기 식별자에 의해 수행되는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 3

제 1 항에 있어서,

상기 (b)단계는,

(b3) 상기 사용자 통신장치에 로컬 소프트웨어(local software)를 다운로드하는 단계

를 더 포함하는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 4

제 3 항에 있어서,

상기 (e)단계를 통해 보내지는 신원확인요청(IVR)에 상기 (h)단계를 통해 검색된 진실 보안 식별자가 포함되고, 상기 (i)단계는 상기 (b3)단계를 통해 다운로드된 로컬 소프트웨어에 의해 수행되며, 상기 (g)단계를 통해 보내

진 응답에 상기 (i)단계의 비교결과가 포함되는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 5

제 3 항에 있어서,

상기 (b3)단계를 통해 다운로드된 로컬 소프트웨어가 상기 (g)단계와 (i)단계 중 적어도 하나를 수행하는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 6

제 3 항에 있어서,

상기 (b3)단계를 통해 다운로드된 로컬 소프트웨어가,

(k) 상기 (e)단계를 통해 보내진 신원확인요청(IVR)을 수신하는 단계;

(l) 표시(display)를 위해 상기 신원확인요청(IVR)을 포맷하는 단계;

(m) 상기 사용자 통신장치에 마련된 입/출력장치에 상기 신원확인요청(IVR)을 표시하는 단계

를 수행하는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 7

제 3 항에 있어서,

상기 (b3)단계를 통해 다운로드된 로컬 소프트웨어가, (ⅰ) 상기 사용자 통신장치에 의해 수신되는 정보를 해독하는 것, (ii) 상기 사용자 통신장치에 의해 보내지는 정보를 암호화하는 것 중 적어도 하나를 수행하는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 8

제 1 항에 있어서,

상기 (e)단계를 통해 보내지는 신원확인요청(IVR) 및 상기 (g)단계를 통해 보내지는 응답 중 적어도 하나는 암호화되는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 9

제 1 항에 있어서,

(n) 상기 사용자 통신장치로 거래승인요청을 보내는 단계;

(o) 상기 (n)단계의 거래승인요청에 대한 응답을 보내는 단계;

(p) 상기 (o)단계에서의 응답이 상기 전자상거래를 승인하는 것인 경우에 상기 전자상거래의 진행을 허가하는 단계

를 더 포함하는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 10

제 9 항에 있어서,

상기 사용자의 계좌를 선등록하는 단계를 더 포함하며,

상기 사용자의 계좌를 선등록하는 단계는 상기 (n)단계 내지 (p)단계를 실행할 것인지 여부를 지시하는 플래그(flag)를 설정(set)하는 단계를 포함하는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 11

제 1 항에 있어서,

상기 사용자의 계좌를 선등록하는 단계를 더 포함하며,

상기 사용자의 계좌를 선등록하는 단계는 상기 (c)단계 내지 (j)단계를 실행할 것인지 여부를 지시하는 플래그(flag)를 설정(set)하는 단계를 포함하는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 12

제 1 항에 있어서,

상기 사용자의 계좌 중 적어도 하나를 선등록하는 단계를 더 포함하며,

상기 사용자의 계좌 중 적어도 하나를 선등록하는 단계는 (ⅰ) 상기 계좌의 접속정보를 얻는 단계, (ii) 상기 계좌접속정보를 식별자-데이터베이스에 저장하는 단계를 포함하는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 13

제 12 항에 있어서,

상기 식별자-데이터베이스에 저장된 계좌접속정보를 이용하여 선등록된 계좌에 상기 식별자가 접속하는 것을 승인하는데 이용될 수 있는 임시거래카드(proxy transaction card)를 상기 사용자에게 발급하는 단계를 더 포함하는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 14

제 13 항에 있어서,

(q) 상기 임시거래카드에 포함된 정보를 이용하여 상기 식별자와의 통신링크를 여는 단계;

(r) 상기 식별자에 의한 접속이 승인된 선등록된 계좌를 상기 사용자에게 표시하는 단계;

(s) 상기 (r)단계를 통해 표시된 계좌 중 상기 식별자가 접속할 계좌를 상기 사용자로 하여금 선택하게 하는 단계;

(t) 상기 식별자가 상기 식별자-데이터베이스에 저장된 계좌접속정보를 이용하여 상기 (s)단계를 통해 선택된 계좌에 접속하는 단계;

(u) 상기 (j)단계에서 상기 전자상거래의 진행이 허가된 경우, 상기 전자상거래를 상기 (s)단계를 통해 접속된 계좌로 통과시키는 단계

를 더 포함하는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 15

제 1 항에 있어서,

상기 (b)단계는,

(b4) 상기 사용자 통신장치에 대한 장치 식별자(device identifier)를 얻는 단계;

(b5) 상기 장치 식별자를 식별자-데이터베이스에 저장하는 단계

를 더 포함하고,

상기 전자상거래에서 사용자의 신원을 확인하기 위한 방법은,

(v) 상기 (b5)단계를 통해 저장된 상기 장치 식별자를 상기 식별자-데이터베이스로부터 검색하여 불러오는 단계;

(w) 상기 사용자 통신장치에 대한 장치 식별자를 얻는 단계;

(x) 상기 (u)단계에서 검색된 장치 식별자와 상기 (w)단계를 통해 얻은 장치 식별자를 비교하는 단계;

(z) 상기 (x)단계를 통해 비교된 장치 식별자들이 일치하지 않는 경우, 상기 전자상거래를 종료하는 단

계

를 더 포함하는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 방법.

청구항 16

전자상거래의 과정에서 식별자(verifier)에 의한 사용자의 신원을 확인하는 시스템에 있어서,

a. 식별자-데이터베이스;

b. 상기 식별자-데이터베이스에 데이터를 입력하고, 상기 식별자-데이터베이스로부터 데이터를 검색하여 불러오는 식별자-컴퓨터;

c. 상기 식별자-컴퓨터에 접속가능하며, 상기 사용자로부터의 통신을 수신하고, 상기 사용자에게로 통신을 전송하기 위한 제1 식별자 통신장치;

d. 상기 사용자에 접속가능하며, 상기 식별자로부터의 통신을 수신하고, 상기 식별자에게로 통신을 전송하기 위한 사용자 통신장치;

e. 상기 사용자로부터의 입력을 수신하고, 상기 사용자에게로의 출력을 표시하는 입/출력장치; 및

f. 상기 사용자 통신장치 및 입/출력장치와 연결되고,

ⅰ) 상기 식별자 통신장치를 통해 상기 사용자 통신장치로 보내지는 상기 식별자-컴퓨터에 의한 신원확인요청(IVR)을 상기 입/출력장치에 표시하는 것

ii) 추정 보안 식별자(putative secure identifier)를 포함하는, 상기 입/출력장치로의 상기 사용자의 입력을 얻는 것

iii) 상기 신원확인요청(IVR)에 대한 응답을 상기 사용자 통신장치로부터 상기 식별자 통신장치로 보내는 것

을 수행하는 사용자-컴퓨터를 포함하고,

상기 사용자-컴퓨터와 식별자-컴퓨터 중 적어도 하나는,

iv) 제1 입력으로서 상기 식별자-데이터베이스로부터 검색된 진실 보안 식별자(bona fide secure identifier)를 수신하는 것

ⅴ) 제2 입력으로서 상기 추정 보안 식별자를 수신하는 것

vi) 상기 제1 입력과 제2 입력을 비교하는 것

vii) 상기 제1 입력과 제2 입력의 일치 여부를 표시하는 확인출력을 생성하는 것

을 수행하며,

상기 확인출력이 상기 제1 입력과 제2 입력의 불일치를 표시하는 경우, 상기 전자상거래는 차단되는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 시스템.

청구항 17

제 16 항에 있어서,

상기 사용자-컴퓨터는 상기 식별자에 의해 보내지는 암호화된 신원확인요청(IVR)을 해독하는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 시스템.

청구항 18

제 16 항에 있어서,

상기 사용자-컴퓨터는 상기 신원확인요청(IVR)에 대한 응답을 암호화하는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 시스템.

청구항 19

제 16 항에 있어서,

상기 사용자 통신장치는 개인 통신장치(personal communications device)인 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 시스템.

청구항 20

제 16 항에 있어서,

상기 확인출력을 은행에 전송하기 위한 제2 식별자 통신장치를 더 포함하는 것을 특징으로 하는 전자상거래에서 사용자의 신원을 확인하기 위한 시스템.

명 세 서

기 술 분 야

<1> 본 발명은 전자상거래를 시작하는 사람의 신원을 확인하기 위한 방법 및 시스템에 관한 것이다.

배 경 기 술

<2> 가장 흔한 전자상거래의 유형은 고객이 판매 카드 리더기에 신용카드를 긁어 주로 상품이나 서비스를 요청하는 것이다. 그러한 요청은 또한, 고객에게 신용거래가 제공되어야 한다는 것 또는 고객의 계좌로부터 상인이나 서비스 제공자의 계좌로 돈이 이체되어야 한다는 것과 같은 암묵적 또는 파생적 요청을 포함한다. 전자상거래의 다른 예들로, 특정 방(room)이나 건물에의 출입권한을 얻기 위한 암호화된 카드 또는 생물학적 특징의 사용; 자동 입출금기(automated teller machines(ATMs))에서의 암호화된 카드의 사용; 및 계좌번호가 인터넷을 통해 온라인상의 상인에게 제공되는 환경하에서의 온라인 상업 거래들을 들 수 있다.

<3> 이러한 전자적 요청들은 관련된 모든 당사자들에게 매우 편리하기 때문에, 전자상거래에 따른 다수의 사기 및 보안 문제들이 무시되거나 경시되고 있다. 그 결과, 어느 한 사람의 개인 정보 및 신용 정보가 권한 없는 사람에 의해 취득되어 사용되는 경우 발생하는 신원 도용의 문제가 엄청나게 증가하고 있다. 2004년, 미국 연방거래위원회는 신원 도용의 결과로 초래되는 상업상의 연간 손실이 500억 달러에 이르는 것으로 추정하였다. 개인들의 손실은 약 50억 달러였다. 비자카드사 및 마스터카드사는 사기와 관련된 2000년 손실이 1140억 달러였으며, 지난 4년간 그 손실이 매년 약 10%의 증가추세에 있다고 보고하였다. 2002년에서 2003년에 걸쳐 캐나다에서 발생한 신원 도용과 관련된 손실은 850만 달러에서 2150만 달러로 증가하여, 겨우 1년 만에 2.6배 증가하였다.

<4> 전자상거래 기술의 사용 및 악용이 증가한 기간과 대략 같은 기간 동안, 휴대용 통신장치, 특히 휴대전화의 사용에 있어서의 증가율이 훨씬 컸다. 1973년 손으로 들로 사용하는 휴대전화를 통한 마틴 쿠퍼(Martin Cooper)의 첫 번째 통화 이래 33년 동안, 전세계에서 사용되고 있는 휴대전화의 수는 25억 개로 증가하였고, 그 수는 현재의 전세계 인구의 50%에 육박하는 것이다. 많은 나라에서 휴대전화 가입자의 수는 인구의 100%를 현저하게 초과하고 있다. 휴대용 통신장치만큼 보편적이거나 유비쿼터스(ubiquitous)적인 전자 기술도 없기 때문에, 보안 강화를 위하여 더 활발히 개발되어져야 하는 것으로 평가되고 있다.

<5> 전자상거래와 관련된 보안 문제들의 해결을 위해 전자통신기술과 보안 식별자를 결합하기 위한 많은 시도들이 이루어져 왔다. 일 예로, 미국등록특허 US 6,954,740에는 거래 요청과 함께 비밀번호(PIN: personal identification number)를 전송하는 방식으로 신용카드서명 및 체크거래(check transaction)가 확인되도록 한 시스템이 개시되어 있다. 미국등록특허 US 6,868,391에는 전자상거래를 시작하는 고객이 상점 등의 전자식 금전등록기(POS: point of sale)를 통해 확인기관(verifying entity)에 비밀번호(PIN)를 제공하면, 확인기관은 그 비밀번호(PIN)를 기존의 유효한 비밀번호(PIN)와 비교하도록 한 시스템이 개시되어 있다. 전술한 시스템들이 전자상거래를 위한 보안의 향상을 제공하기는 하지만, 특히 고객의 입장에서 볼 때, 그 실행이 전반적으로 어렵거나 불편하다. 예를 들면, 미국등록특허 US 6,868,391은 고객으로 하여금 전화를 걸어 확인기관에 접속하도록 요구하는데, 이는 고객으로 하여금 식별자(verifier), 즉 확인기관의 전화번호를 알고, 입력하게 한 후, 확인전화를 기다리도록 요구한다.

<6> 전자상거래를 수행하는 동안, 실행하기 쉽고, 이용하기 쉬우며, 실질적으로 사용자에게 평이하고, 사용자가 전화를 걸 필요 없이 전세계 어디서나 이용할 수 있게 유연한, 사용자의 신원을 확인하기 위한 방법 및 시스템이 필요하다.

발명의 상세한 설명

<7> 본 발명은 전자상거래를 시작하는 사용자의 신원을 확인하기 위한 방법에 있어서의 복잡한 문제를 해결한다.

<8> 이하의 정의들은 본 명세서 및 특허청구범위에서 사용된 특정 용어들의 의미 및 의도된 범위를 설명하기 위한 것이다. 상기 정의들에 사용된 예들은 그 정의들을 설명하여 그 의미를 명확하게 하기 위한 것일 뿐, 상기 용어의 정의나 범위를 한정하기 위한 것은 아니다. 여기에서 정의된 용어들은 복수 형태, 단수 형태, 문법에 맞는 동류의 것들 및 대체어들을 포함한다.

<9> "전자상거래"는 상품들 또는 서비스들에 대한 요청 및 상기 요청에 대한 응답을 포함하며, 상기 요청은 상기 상품들 또는 서비스들에 대한 대금의 지불 신청을 포함하고, 상기 요청 및/또는 응답에 있어서의 몇몇 단계는 정보의 전자통신을 수반한다. "서비스들"은 요청된 어떤 행위를 포함하는 것으로 폭넓게 정의된다. 본 명세서에 사용된 "전자상거래"란 용어는 상품들, 거의 모든 유형의 서비스들/행위들을 수반하는 거래들에 적용된다. 비록 본 발명의 바람직한 실시예를 설명하기 위해 사용된 통상적인 전자상거래들이 신용카드를 통한 거래들이지만, 방, 차량, 건물, 대여 금고(deposit box) 또는 창고 시설 등과 같은 안전 장소에 대한 출입권한의 부여; 일정 금액의 예치조건부 신용거래(secured credit) 및 비예치조건부 신용거래(non-secured credit)의 제공; 은행서비스나 기타 금융서비스의 제공; 국경의 통관허가의 제공 등을 포함하는 다른 전자상거래들 역시 본 발명의 범위 속에 포함된다.

<10> "사람"은 개인들, 기관(단체)들, 개인들이나 기관의 집합체들을 포함한다.

<11> "사용자", "고객", "지불인(payer)"은 전자상거래를 통해 상품들이나 서비스들을 얻고자 하는 사람들을 호환하여 지칭하는데 사용된다. 소매 거래들과 관련하여서는 "고객" 및 "지불인"이 주로 사용되고, 소매 거래가 아닌 경우에는 "사용자"가 주로 사용된다. "사용자-컴퓨터"는 본 발명에 따른 방법의 다양한 단계들을 실행하기 위해 사용하는 컴퓨터를 가리킨다.

<12> 본 명세서 및 특허청구범위에서, "공급자(provider)"는 전자상거래를 통해 상품들 및 서비스들을 제공하는 개인들 및 기관(단체)들의 시스템들 및 하위시스템들을 포함하는 광범위하면서도 일반적인 의미를 가지며, 파생적 또는 잠재적 서비스들을 제공하는 제3자들을 포함한다. 예를 들어, 전자 신용카드 거래에 있어서, "공급자"란 용어는 소매업자, 상인 또는 구매된 상품들이나 서비스들에 대한 대가를 받는자를 포함하며, 또한 고객이 신용카드를 사용할 때, 고객에 의해 요청된 신용 대금을 치르는 것과 같은 파생적 서비스를 제공하는 다양한 제3의 금융기관들의 하위시스템을 포함한다.

<13> "은행"은 기능적으로 신용의 연장, 자금의 이체, 금융계좌의 관리 등을 포함하는 전자상거래와 관련된 금융서비스를 제공하기 위해 상호작용하는 기관들의 일 기관이나 그룹을 의미하는 것으로 정의된다. 상기 은행이란 용어는 또한, 예를 들어 비자카드사 및 마스터카드사와 같은 신용카드사 또는 지불금 전송 단체들(payment transfer associations)과 같이, 금융서비스를 제공하기 위해 상호작용하는 기관들의 시스템들 및 하위시스템들을 포함한다. 따라서 상기 은행이란 용어는 전자상거래를 처리함에 있어서, 금융기관들에 의해 수행되는 일련의 기능들을 의미한다.

<14> "식별자(verifier)"는 기능적으로 전자상거래의 일부로서, 신원확인서비스를 제공하는 기관을 의미하는 것으로 정의된다. 상기 식별자는, 수수료를 받고 신원확인서비스를 제공하는 기업과 같이, 거래를 진행하는 당사자들과는 무관한 존재를 의미할 수도 있다. 택일적으로, 상기 식별자 기능은 상품들 및 서비스들의 제공자, 은행, 신용카드사 또는 상기 거래와 관련된 또 다른 당사자에 의한 것에 포함될 수 있다. 이하의 설명 및 도면들에 있어서, 상기 식별자와 공급자가 별개라는 표현은, 양 기관들이 반드시 서로 전혀 다르다는 것을 의미하는 것이 아니며, 상기 식별자의 기능과 상기 은행 및 공급자의 기능이 서로 별개라는 점을 설명하는 것이다. 마찬가지로, "식별자-컴퓨터"란 용어는 기능적으로, 확인 기능을 제공하는 컴퓨터, 서버, 네트워크, 기타 확인 기능을 제공하는 모든 것을 의미하는 것으로 정의되며, 상기 컴퓨터, 서버, 네트워크 등이 어디에 위치하는가 또는 누가 그것들을 소유하거나 통제하는가와는 무관하다. 상기 "식별자-컴퓨터"에 의해 수행되는 단계는 상기 "식별자"에 의해 수행되는 단계와 동등한 것으로 간주되며, 그 반대의 경우도 마찬가지이다.

<15> "식별자-데이터베이스"는 식별자-컴퓨터로 접속할 수 있는 사용자 기록들의 편집을 가리킨다.

<16> "통신장치"는 광범위하게 통신시스템에 연결된 모든 종류의 통신장치들을 포함하며, 상기 통신시스템을 통해 특정인 또는 특정 응용 소프트웨어가 다른 사람 또는 다른 응용 소프트웨어와 통신하게 된다. 상기 통신장치란 용어는 인터넷에 연결된 컴퓨터, 유선시스템(land-line system)에 연결된 전화기, 무선시스템에 연결된 휴대전화

및 기타 유사장치를 포함한다. "개인통신장치"는 사용자가 휴대할 수 있을 정도로 충분히 작고 이동성이 있는 통신장치를 가리키며, 제한 없이, 휴대전화, PDA, 무선 컴퓨터, 블랙베리(Blackberry®)장치, 블루투스(Bluetooth®)장치, 무선 호출기, 삐삐(beeper) 및 기타 무선 송수신기(transceiver) 기능을 갖는 개인장치를 포함한다.

<17> "로컬 소프트웨어(Local software)"는 본 발명을 수행함에 있어서 상기 사용자-컴퓨터에 의해 접속되는 소프트웨어를 가리킨다. 특정 단계를 "수행"하는 로컬 소프트웨어는, 상기 로컬 소프트웨어에 의해 지시된 대로 지정된 기능을 수행하는 사용자-컴퓨터를 가리킨다.

<18> "사용자 접속번호"는 사용자의 통신장치에 접속하기 위해 사용되는 알파벳 등의 문자와 숫자를 조합한 것 또는 기타 데이터 표현(data representation)을 가리킨다.

<19> "신원확인요청(IVR: identity verification request)"은 식별자에 의해 생성된 후, 사용자에게 전달되어 사용자에게 신원확인을 요구하는 전자적 요청을 가리킨다.

<20> "보안 식별자(secure identifier)"는 사람의 신원을 확인하기 위해 사용되는 보안 데이터 표현(secure data representation)을 나타내는 일반적인 용어이다. 상기 보안 식별자란 용어는, 예를 들면, 사람이나 기관의 신원을 확인하기 위해 사용될 수 있는 알파벳 등의 문자와 숫자를 조합한 것, 패스워드, 암호, 비밀번호, PIN, 기타 생물학적 특징과 같은 디지털 표현(사람의 경우) 등을 포함한다. 상기 예들에 있어서, "패스워드"의 사용이 다른 유형의 보안 식별자들을 배제하는 것을 의미하지는 않으며, 실제로는 전술한 모든 유형을 대표하는 것을 의미한다. "추정 보안 식별자(putative secure identifier)"는 신원확인요청(IVR)에 대응하여 제공되는 보안 식별자를 가리킨다. "진실 보안 식별자(bona fide secure identifier)"는 추정 보안 식별자와 비교되는 주지의 유효 보안 식별자를 가리킨다.

<21> 본 발명은 휴대통신기술을 응용하여 전자상거래에 있어서의 정확한 사용자 신원확인을 제공하는데 따른 문제점을 해소하는 방법 및 시스템이다. 본 발명에 따른 상기 방법은 여러 응용들 및 실시예들을 갖지만, 이하에서는 그 중의 일부가 개시되며, 그 기본 방법은 최소 상품들이나 서비스들을 제공하는 공급자, 전자상거래를 통해 상기 상품들이나 서비스들을 얻고자 하는 사용자 또는 고객, 요청자의 신원이 충분히 확인되지 않은 각 거래를 차단하는 게이트 키퍼(gate keeper)로 작용하는 식별자를 포함한다.

<22> 본 발명에 따른 방법에 있어서, 사용자 및 사용자의 통신장치는 은행, 식별자 또는 기타 기관에 의해 운영되는 신원확인프로그램에 선등록된다. 사용자의 하나 또는 그 이상의 계좌들이 상기 신원확인프로그램에 선등록된다. 이러한 선등록은 정보를 식별자-데이터베이스에 입력하는 것 및 사용자의 통신장치에 결합되거나 또는 통합된 사용자-컴퓨터에 로컬 소프트웨어를 다운로드하는 것을 포함한다. 계좌의 선등록은 데이터베이스 기록에 플래그(flag)를 세팅(setting)하는 것처럼 간단하며, 상기 플래그는 상기 계좌에 접속하려는 시도가 사용자 신원확인 단계를 거쳐야할 것인지 여부를 지적하며, 또는 상기 계좌의 선등록은 상기 계좌의 번호와 접속 인증 데이터를 식별자-데이터베이스에 입력하여 사용자가 상기 계좌에 접속함에 있어서 식별자로 하여금 프록시(proxy) 역할을 하도록 하는 것을 포함할 수 있다. 옵션으로서, 상기 계좌의 선등록은 추가로 또는 선택적으로 데이터베이스에 플래그를 세팅하는 것을 수반하여 상기 계좌에 접속하려는 시도가 거래인증단계를 거쳐야할 것인지 여부를 지적한다.

<23> 선등록 절차의 결과로 상기 식별자-데이터베이스에 저장된 정보는 식별자-컴퓨터에 의해 접속가능하며, 상기 식별자-컴퓨터는 상기 데이터베이스에 데이터를 기입하는 것 및 상기 데이터베이스로부터 데이터를 불러오거나 검색하는 것이 가능하다. 상기 식별자-데이터베이스에 있는 사용자의 기록은 사용자를 위한 진실 보안 식별자(bona fide secure identifier) 및 사용자의 통신장치의 사용자 접속번호를 포함한다. 금융거래와 관련된 본 발명에 따른 방법 및 시스템에 있어서, 데이터베이스는 또한 어떤 계좌들이 신원확인 및 거래인증을 받아야 하는 것인지를 결정하는 다양한 플래그들(flags)을 포함한다.

<24> 사용자(또는 누구든지)가 플래그된 계좌(flagged account)에 접속을 시도하는 경우, 상인으로부터 식별자-컴퓨터로 신호가 전송되며, 이후, 식별자-데이터베이스에 저장된 사용자 식별번호를 이용하여 사용자의 통신장치와 연결된 통신링크를 열도록 하는 시도가 이루어진다. 사용자의 통신장치에 대한 통신링크가 열리면, 식별자-컴퓨터는 사용자의 통신장치로 암호화된 신원확인요청("IVR")을 전송한다. 상기 통신장치 및 입/출력장치와 연결된 사용자-컴퓨터는 상기 신원확인요청을 중간에서 수신하여 상기 신원확인요청의 암호를 해독하고 그것을 상기 입/출력장치에 표시하는 것을 포함하는 처리과정을 수행한다. 즉, 사용자로부터의 입력을 수신하여 출력을 사용자에게 표시한다. 또한, 상기 사용자-컴퓨터는 사용자로부터 입력을 얻어 상기 입력에 기초하여 상기 신원확인요

청에 대한 응답을 전송한다. 사용자의 통신장치를 소유한 사람이 진실한 사용자인 경우, 상기 사용자-컴퓨터는 상기 신원확인요청에 대한 대응으로 상기 입/출력장치에 (정확한) 추정 보안 식별자(putative secure identifier)를 입력한다. 일 실시예에서, 상기 추정 보안 식별자는 사용자의 통신장치에 있는 로컬 소프트웨어에 의해 암호화되어, 열려있는 상기 통신링크를 통해 상기 식별자-컴퓨터로 전송된다. 상기 식별자-컴퓨터는 상기 추정 보안 식별자를 수신하여 암호해독을 한 후, 상기 데이터베이스로부터 검색된 진실 보안 식별자와 비교한다. 비교결과, 상기 추정 보안 식별자와 진실 보안 식별자가 일치하는 경우, 식별자-컴퓨터는 거래에 대한 차단을 해제하여 상기 거래가 완료처리될 수 있도록 한다.

<25> 옵션으로서, 본 발명에 따른 방법은 사용자가 가까운 장래에 특정 전자상거래를 인증하는 단계들을 추가로 포함할 수 있고, 추가될 수 있는 상기 단계는 상기 사용자 신원확인단계와의 구별을 위해 "거래인증(transaction authorization)"으로 지칭될 수 있다. 본 발명의 구체적 적용에 있어서, 상기 거래인증단계는 상기 신원확인단계와 동시에 완료되거나 또는 예를 들어, 식별자-컴퓨터가 거래인증요청(transaction authorization request)으로 불리는 제2의 암호화된 요청을 사용자의 개인통신장치로 전송하는 경우와 같이, 완전히 별개로 완료될 수 있다. 상기 거래인증요청은 상기 통신장치의 입/출력장치에 표시됨으로써 사용자로 하여금 거래의 양, 상인 및 기타 세부사항들을 확인할 수 있게 한다. 거래를 승인 또는 거부하기 위해, 사용자는 상기 거래인증요청에 대한 응답을 전송하며, 상기 응답은 "리턴(return)"키를 누르는 것에 지나지 않는 것일 수 있다. 상기 응답이 거래를 승인하는 것인 경우, 거래차단은 해제되어 상기 거래가 진행된다. 몇몇 적용례에 있어서, 사용자의 거래에 대한 승인에 앞서 사용자의 신원이 확인된다. 다른 적용례에 있어서, 사용자의 신원확인에 앞서 거래인증단계를 먼저 수행하는 것이 더 효율적일 수 있다.

<26> 상기 방법의 이점은 전술한 조합을 이용하는 것 또는 전자상거래에 있어서 추가적인 보안 장벽들을 세우기 위해 사용자의 휴대전화번호와 보안 식별자의 조합을 이용하는 것이다. 사용자의 신용카드가 도난당하거나 횡령된 경우, 그 신용카드를 이용한 도둑의 거래 개시에 대한 시도는, 식별자-컴퓨터가 사용자의 휴대전화로 신원확인요청(IVR)을 전송하는 것에 의해, 사용자에게로의 즉각적인 통보로 귀결된다. 도난당한 신용카드를 사용하고자 시도하는 도둑은, 그와 같은 사용이 피해자의 전화를 울리게 함으로써 누군가가 도난당한 신용카드로 거래를 개시하고자 시도한다는 사실을 사용자에게 알린다는 것을 전혀 인지하지 못한다. 설사 사용자의 휴대전화와 신용카드가 모두 도난당하거나 횡령된 경우라도, 그 도둑이 사용자의 보안 식별자를 알지 못하는 한, 도둑에 의해 도난당한 신용카드를 이용하여 개시된 어떠한 전자상거래도 실패하게 될 것이다. 게다가, 현재 휴대전화에 대한 GPS 위치추적기능이 보편적인 관계로, 허위확인조회의 시도는 도난당한 휴대전화의 위치추적작업을 실행시킬 수 있다.

<27> 상기 방법의 다양한 실시예들은 그 유용성을 대폭 확장한다. 예를 들면, 상기 방법은 제2의 당사자를 대신하여 일 당사자에 의해 개시된 전자상거래를 식별자로 하여금 통제하도록 허용하는 것에 알맞을 수 있다. 또한, 예를 들면, 직원이 회사의 신용카드를 소지하여 사용하는 경우, 식별자-컴퓨터는 판매시점에서 그 직원의 휴대전화로 신원확인요청(IVR)을 전송하고, 그 직원의 신원이 확인되면, 식별자-컴퓨터는 고용주의 유선전화 또는 휴대전화로 거래인증요청을 전송함으로써 고용주로 하여금 거래가 요청되었음을 알게끔 하고, 거래가 완료되기에 앞서 그 거래를 승인할 것인지 아니면 거부할 것인지를 결정하게 할 수 있다.

<28> 또 다른 선택적인 실시예에서, 식별자는 사용자에게 임시거래카드(proxy transaction card)를 발행하여, 사용자 신원확인을 개시하는데 이용되도록 하고, 이후 사용자의 신용카드계좌에 대한 거래를 승인함으로써 사용자가 신용카드를 가지고 다닐 필요가 없게 하고, 사용자의 거래은행이 개입됨 없이 상인의 거래은행과 식별자 사이에서의 정보의 흐름을 허용할 수 있다. 따라서 식별자는 사용자의 하나 또는 그 이상의 계좌에 대한 게이트웨이(gateway)로서 작용하며, 상기 게이트웨이는, 사용자가 식별자로부터의 신원확인요청(IVR)에 대응하여 사용자의 통신장치에 정확한 보안 식별자를 입력하는 경우에만 열릴 수 있도록 한다.

<29> 첨부된 도면들과 연계한 이하의 설명들을 통해 본 발명의 전술한 목적 및 다른 목적들이나 특징들, 이점들이 더욱 분명해질 것이다.

<30> 본 발명에 따른 방법 - 단계(phase) Ⅰ: 선등록(pre-enrollment)

<31> 본 발명에 따른 방법은 수 많은 적용성을 가지며 폭넓은 다양한 환경에서 사용될 수 있는 잠재성을 갖기 때문에, 가능한 모든 적용례들을 개시하는 것이 불가능하다. 본 발명을 실행하는 데 있어, 현재까지 알려진 가장 바람직한 방식을 대표하는 본 발명에 따른 방법 및 시스템의 상대적으로 간단한 예가 본 명세서에서 개시된다. 본 발명의 다양한 적용성을 설명하기 위해, 많은 변형예들이 개시된다. 본 명세서를 통해, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자(이하, '당업자')는 본 발명을 실행할 수 있으며, 본 발명을 응용하여 많

은 다양하고 유용한 결과를 얻을 수 있을 것이다.

<32> 도 1 내지 도 3에 도시된 실시예는, "고객" 또는 "지불인"이 본 발명을 이용하여 신용카드계좌, 예를 들어 비자카드사 및 마스터카드사와 같은 지불금 전송기관(payment transfer association)에 의해 관리운영되는 신용카드의 보호방법을 보여준다. 앞서 언급된 바와 같은 금융기관들은 집합적으로 총칭하여 "은행"을 지칭한다. 소매업자, 상인 또는 기타 대가를 지불받는 자에게 고객이 신용카드를 제시하는 것은 상품들/서비스들에 대한 신청 및 상기 상품들/서비스들의 대가지급을 위한 고객의 계좌에 대한 신용연장의 요청을 함께 구성한다. 도 1은 사용자, 사용자의 통신장치 및 사용자의 계좌를 확인 프로그램에 선등록하는 절차를 보여준다. 도 2는 전자상거래 중에 본 발명을 이용하여 사용자의 신원을 확인하는 절차를 보여준다.

<33> 먼저, 도 1을 참조하면, 고객(101), 은행(201) 및 식별자(301)가 어떻게 상호작용하여 상기 선등록 절차를 수행하는지에 대한 바람직한 실시예를 보여준다. 상기 식별자(301)는 은행(201)에 소프트웨어 및 서버를 제공한다. 확인 소프트웨어(verification software) 및 관련 하드웨어가 물리적으로 은행의 구내에 있을 뿐만 아니라 은행에 의해 운영된다는 점에서, 상기 은행은 "식별자-컴퓨터"의 물리적 통제하에 있다. 고객이 은행에 접속하여 사용자 신원확인 서비스를 요구하는 것에 의해 상기 선등록 절차가 개시된다(401). 은행은 전술한 요구의 접수(기록), 고객의 신원확인과 같은 필요한 관리 작업들(501)을 완료한다. 결과데이터는 데이터베이스(701)에 갱신된다.

<34> 고객은, 신원정보 및 잊어버린 패스워드를 전자적으로 되찾기 위해 사용될 수 있는 정보를 포함하는 필요한 데이터를 식별자에 제공하는 것(601)에 의해, 확인 프로그램에 선등록된다. 진실한 패스워드가 고객에게 할당된다. 이러한 모든 정보는 식별자-데이터베이스(701)에 있는 고객 기록에 입력된다(1601). 비록 상기 식별자-데이터베이스 및 은행의 데이터베이스가 단일 기관으로 표현되지만, 데이터베이스들의 물리적 통합체는, 이하에서 상세히 논의되는 바와 같이, 별개의 서버들에서 운영되는 별개의 데이터베이스들로 이용되는 것으로 이해되어야 한다.

<35> 다음 단계는 고객이 접속하는 휴대전화를 선등록하는 것(801)이다. 먼저, 사용자는 고객의 휴대전화와의 통신 링크를 열기 위해 사용될 수 있는 사용자 접속번호를 식별자에게 제공하고, 식별자는 데이터베이스(701)에 상기 사용자 접속번호를 저장한다(1201). 이후, 식별자는 제공된 상기 사용자 접속번호를 이용하여 휴대전화에 전화를 건다(901). 이후, 상기 열려진 통신 링크를 통해 식별자는 사용자의 g휴대전화로 통합된 사용자-컴퓨터에 로컬 소프트웨어를 다운로드한다(1001). 상기 로컬 소프트웨어는, 이하에서 설명되는 바와 같이, 신원확인절차 과정에서 필요하다. 상기 사용자-컴퓨터는 본 발명의 구체적인 실행에 의존하는 독립형 컴퓨터이거나 또는 많은 유형의 통신장치들 중 어느 하나로 통합된 컴퓨터일 수 있음을 주지해야 한다. 이 점에서, 식별자는 선택적으로 상기 휴대전화로부터 특정 전화를 식별하는데 이용될 수 있는 장치식별정보를 얻을 수 있다. 실시예들에서, 상기 사용자-컴퓨터는 노트북 컴퓨터, PDA이거나 또는 휴대통신장치가 아닌 기타 컴퓨터이며, 식별자는 상기 컴퓨터의 CPU의 일련번호를 얻을 수 있다. 이후, 이러한 통신장치의 데이터는 데이터베이스(701)에 기록된다.

<36> 선등록의 마지막 단계는 서비스에 의해 보호되어야 할 특정 계좌를 선등록하는 것(1301)이다. 고객은 어떤 계좌를 사용자 신원확인 서비스에 의해 보호받을 것인지를 결정한다. 각 개별 거래중, 식별자가 고객의 신원을 확인할 때까지, 전술한 계좌들을 통한 거래가 차단된다. 고객은 등록될 계좌 또는 계좌들을 지정한다(1701). 은행은 상기 지정된 계좌들을 플래그(flag)하고(1401), 식별자에게 통지한다(1801). 식별자는 데이터베이스(701)에 해당 사항을 기입함으로써 상기 계좌들을 선등록한다(1501). 선택적으로, 은행은 상기 확인 플래그(verification flag)를 은행의 데이터베이스에 보존하고, 이후 상기 플래그된 계좌(flagged account)에 대한 접속이 시도될 때마다 확인서비스에 대해 공지할 수도 있다. 상기 계좌들을 플래깅(flagging)하는 가장 효율적인 방법은 구체적인 애플리케이션(application) 및 당사자들의 재원에 의해 결정될 것이다. 가장 중요한 점은, 식별자가 고객의 신원을 확인할 때까지, 지정된 계좌들을 이용한 거래들이 차단된다는 것이다.

<37> 본 예에서는, 오직 한 사람, 한 고객이 전자상거래들을 개시한다. 그러나 복수의 잠재적 사용자들이 있을 수 있고, 그 경우 필요한 데이터를 식별자에 제공하는 단계(601)에서 그들의 신원 데이터와 휴대전화번호들 역시 식별자에게 제공되어 데이터베이스(701)에 입력된다.

<38> 전술한 선등록 절차는 온라인 또는 유선 및/또는 무선 통신시스템을 통해 쉽고 편리하게 고객에 의해 개시될 수 있다. 상기 소프트웨어 다운로드 단계(1001)는 식별자가 고객의 휴대전화와의 통신 링크를 여는 것에 의해 가장 편리하게 수행될 수 있다. 선등록의 전체 절차는 몇 분 내에 완료된다. 상기 식별자가 은행과 별개의 기관이라 하더라도, 상기 선등록 절차가 반드시 식별자를 직접 수반할 필요는 없다. 은행은 자체적으로 상기 선등록 절차를 수행할 수 있고, 그 경우 식별자는 고객에게 투명한 상태로 남는다. 예를 들어, 특정 신원확인회사가 본 발

명에 따른 방법을 실행하기 위해 필요한 소프트웨어 및 서버들을 은행에 제공하는 것에 대해 은행과 계약을 맺을 수도 있다. 이후, 만일 은행이 신원확인절차를 운영한다면, 그 은행은 "은행" 및 "식별자"의 기능 모두를 실현하게 될 것이다.

<39> 강조되는 점은 상기 선등록 절차의 순서가 고정된 것이 아니라 다양한 변형성의 여지가 있다는 것이다. 예를 들어, 고객이 선등록을 요구(401)하자마자 상기 계좌를 플래깅(flagging)하는 것(1401)이 수행될 수도 있다.

<40> 본 발명에 따른 방법 - 단계(phase) Ⅱ: 고객 신원확인

<41> 도 2는 고객이 식별자(301)를 통해 선등록된 계좌를 이용하여 소매업자(102)로부터 거래의 일환으로 상품들/서비스들을 구매하기 위해 은행으로부터 신용의 연장을 얻기 위한 단계들의 순서를 보여준다.

<42> 고객은 소매업자(102)에게 카드를 제시함으로써 전자상거래를 개시한다(202). 상기 카드는 카드 리더기(card reading device)에 긁어짐으로써, 은행(201)으로 현재 일반적으로 사용되는 공중 전화 교환망(PSTN: public switch telephone network)을 통해 전자통신을 전송한다(302). 은행은 고객의 계좌에 거래를 이행하기에 충분한 신용이나 자금이 존재하는지 여부를 알아보기 위해 은행의 데이터베이스에 있는 고객의 계좌정보를 조회한다(502). 만일 문제가 있는 경우, 상기 거래는 차단되고, 그 사실이 소매업자에게 통지될 수 있다(2902). 만일 문제가 없는 경우, 은행은 고객의 계좌가 플래그된(flagged) 것인지 여부를 확인하기 위해 데이터베이스에 문의한다(402).

<43> 만일 상기 계좌가 플래그된(flagged) 것이 아니라면(602), 그 거래는 사용자 신원확인 단계를 무시하고, 통상의 인증절차들을 계속 진행한다(2502).

<44> 본 예에서, 고객은 도 1에 도시된 바와 같은 신원확인 서비스를 위해 계좌를 선등록하고, 그에 따라 상기 계좌는 플래그 되었다. 그 결과, 상기 거래는 고객의 신원이 확인될 때까지 차단된다(3002). 신원확인절차를 개시(702)하기 위한 메시지가 은행으로부터 식별자에게 전송된다. 식별자는 데이터베이스로부터 고객의 휴대전화를 위한 사용자 접속번호를 검색하여 불러오고, 예를 들어 무선 프로토콜(protocol) 및 네트워크를 이용하여 고객의 휴대전화와의 통신링크를 연다(1002). 질문 신호가 고객의 휴대전화로 전송되고, 고객의 휴대전화에 수신된 상기 신호는 선등록 중에 상기 휴대전화에 다운로드된(1001, 도 1 참조) 로컬 소프트웨어를 불러낸다(802). 상기 휴대전화가 꺼져 있거나 아무런 응답이 없는 경우, 신원확인절차는 실패하게 되고, 거래는 종료된다. 유사하게, 상기 신원확인절차가 완료되기 전 어느 때라도 전화연결 또는 통신링크가 끊어지는 경우, "시간초과(timed-out)"의 경우와 마찬가지로 그 거래는 실패하게 된다.

<45> 고객의 전화가 응답하는 경우, 사용자-컴퓨터는 식별자-컴퓨터로부터 자동으로 거래정보를 탐색하고(1202), 식별자-컴퓨터는 사용자-컴퓨터에 상기 거래정보를 전송(1402)함으로써 응답하며(1102), 상기 거래정보는 신원확인요청(IVR)을 포함한다. 사용자-컴퓨터는 상기 신원확인요청(IVR)을 수신하고, 사용자의 입/출력장치에 표시하기 위해 상기 신원확인요청(IVR)을 포맷한다.

<46> 상기 신원확인요청(IVR)의 포맷은 이용가능하고 우선시되는 기술들 및 휴대용 통신장치의 유형이 무엇이냐에 따라 달라지지만, 현재 대부분의 지역에서 문자 메시지가 선호되고 있다. 상기 신원확인요청(IVR)은 본질적으로 고객으로 하여금 패스워드를 입력하도록 유인한다.

<47> 선택적으로, 식별자-컴퓨터는 적법한 통신장치가 접속되었는지 여부를 확인하기 위해 사용자의 전화로부터 장치식별번호를 얻어 데이터베이스에 기록된 장치식별번호와 비교할 수도 있다. 이 과정은 사용자-컴퓨터가 거래정보를 탐색하는 경우(1202), 편리하게 수행될 수 있다.

<48> 고객은 자신의 휴대전화의 입/출력장치에 추정 패스워드(putative password)를 입력하고(1802), 입력된 추정 패스워드는 사용자-컴퓨터에 의해 포맷되어 신원확인요청(IVR)에 대한 응답으로 식별자-컴퓨터로 전송된다(1602). 상기 추정 패스워드는 식별자-컴퓨터에 의해 수신되어 데이터베이스(701)로부터 검색된 진정한 패스워드와 비교된다(1502).

<49> 상기 추정 패스워드가 진정한 패스워드와 일치하지 않는 경우, "승인 불가"라는 메시지가 사용자-컴퓨터로 전송되어(1702), 고객으로 하여금 패스워드를 다시 입력하도록 요구한다. 패스워드의 입력을 통한 승인시도가 미리 설정된 횟수를 초과하면, 거래는 종료되고, 그 사실이 은행에 통보된다(1302). 이 점에서, 고객에게 전화를 걸어 거래실패를 알리거나, 경찰에 신고하거나, 추가적인 거래시도를 차단하거나, 카드를 정지시키는 것 등과 같은 다양한 보호조치 또는 구제조치가 은행, 소매업자 및/또는 식별자에 의해 취해질 수 있다. 구체적인 적용에 따라 달라질 수 있으나, 추정 패스워드가 승인되기에 앞서 통신링크가 끊기는 경우, 그 거래는 보안위반으로 처

리되거나 또는 은행 및/또는 소매업자에게 적절한 통지를 하는 것과 함께 간단히 종료될 수 있다.

<50> 상기 추정 패스워드가 진정한 패스워드와 일치하는 경우, "신원 확인" 신호가 생성되고(902), 계좌에 대한 차단은 해제되며(3002), 은행에 대한 통지(2402)와 상인에 대한 통지(2202) 및 고객의 휴대전화로의 승인메시지 전송(2602)을 포함하여 거래의 진행이 허용된다.

<51> 사용자-컴퓨터와 식별자-컴퓨터 사이의 전송은 암호화되어 이루어진다. 로컬 소프트웨어는 고객으로부터의 어떠한 입력 없이도 자동으로 암호화된 유입 신호를 해독하고, 출력 신호를 암호화한다. 식별자가 고객의 전화로 전화를 거는 것에 의해 통신라인이 열려있기 때문에, 고객은 식별자의 전화번호를 알 필요가 없을 뿐만 아니라 그 번호로 전화를 걸 필요가 없고, 고객의 전화에 있는 로컬 소프트웨어는 식별자로부터 유입되는 메시지를 자동으로 확인하여 고객 전화의 입/출력장치에 표시하고, 출력 정보를 포맷하여 식별자에게 전송한다.

<52> 본 발명에 따른 방법 - 단계(phase) Ⅲ: 거래 인증 및 완료

<53> 도 2의 노드(node, 2502)에서, 고객의 신원이 확인되고, 거래가 완료되도록 진행된다. 본 발명의 실시예들에서, 신원확인요청(IVR)은 묵시적 또는 명시적으로 거래 인증에 대한 요청을 포함하며, 그 인증은 고객이 보안 식별자를 입력함으로써 유효해 진다. 다른 실시예들에서, 고객으로 하여금 별도의 단계에서 거래를 인증하게 하는 것이 바람직하다. 이는 식별자-컴퓨터에 의한 사용자-컴퓨터로의 인증 요청의 전송과, 고객으로부터의 적절한 응답의 제공을 기다리는 것에 의해 이루어진다. 만일 고객이 그 거래를 인증하지 않거나 전화가 끊기는 경우, 그 거래는 실패한다.

<54> 2402 및 2302 단계들에서, 은행은 신원확인절차 및 다른 선택적 거래인증의 단계들에 대한 결과를 통보받는다. 2202 단계에서, 소매업자 역시 그 거래의 상황을 통보받으며, 고객은 2602 단계에서 통보받게 되며, 그와 같은 통보는 고객의 휴대전화를 통해 곧바로 이루어지거나 또는 예를 들어 고객의 월별 보고서를 통해 미래의 특정 시점에서 이루어질 수 있다. 거래가 승인되면, 그 거래는 완료된다.

<55> 본 발명에 따른 시스템

<56> 본 발명에 따른 시스템은 전술한 예들로 요약되는 방법을 실행하는 신규하고 자명하지 않은 조합에 있는 하드웨어 및 소프트웨어 요소들을 포함한다. 본 발명은 다양한 변형성 및 폭넓은 적용가능성을 갖기 때문에, 본 발명이 취할 수 있는 모든 형태들이나 실시예들을 설명하거나 심지어 예상하는 것은 가능하지 않다. 본 명세서에 개시된 본 발명에 따른 시스템은 다소 기본적인 것이며, 이를 기초로 본 발명이 속하는 기술분야의 통상의 지식을 가진 자가 본 발명의 범위 내에서 많은 자명한 변경 및 개선을 할 수 있을 것이다.

<57> 도 3은 본 발명에 따른 시스템의 주요 요소들의 도식적 요약을 나타내며, 신용카드거래의 예를 이용하여 상기 주요 요소들이 어떻게 상호작용하는지를 설명한다.

<58> 고객(103)은 무선 송수신기(403), 사용자-컴퓨터(603)에 의해 운영되는 로컬 소프트웨어, 고객과 휴대용 통신장치를 인터페이스로 연결하기 위한 입/출력장치(503)를 포함하여 구성되는 휴대전화(2303) 또는 다른 휴대용 통신장치를 갖는다. 사용자-컴퓨터는 입/출력장치 및 무선 송수신기와 연결되며, 로컬 소프트웨어를 통해 유입되는 신원확인요청(IVR)을 입/출력장치에 표시하고, 신원확인요청(IVR)에 대한 응답을 출력 데이터로 포맷하며, 무선 송수신기를 통해 식별자에게 출력 데이터를 전송한다.

<59> 통신장치(2303)의 사용자-컴퓨터는 식별자(203)의 제1 통신장치(2403)와의 무선링크인 통신링크에 접속한다(1503). 상기 제1 식별자 통신장치는 식별자-컴퓨터(903)와 연결된다. 상기 식별자-컴퓨터는 소프트웨어를 통해 식별자-데이터베이스(703)에 접속하여 상기 식별자-데이터베이스로부터 데이터를 읽거나 상기 식별자-데이터베이스에 데이터를 기록할 수 있고, 상기 식별자-데이터베이스는 제1 식별자 통신장치(2403) 및 제2 식별자 통신장치(803)에 의해 수신된 데이터 및 전송된 데이터를 포함한다.

<60> 제2 식별자 통신장치(803)는 통신링크(1803)를 통해 은행/공급자 통신장치(1103)와 통신한다. 상기 통신링크는 공중 전화 교환망(PSTN)과 같은 무선통신 또는 유선네트워크로서 실행될 수 있다. 상기 식별자 통신장치들의 제1 및 제2 송수신기 기능을 결합하는 것이 기술적으로 가능하지만, 현재 일반적으로 이용가능한 기술을 이용하는 경우, 앞서 설명한 접근법이 전술한 기능들을 분리하는 것의 유연성 및 통신속도 측면에서 바람직하다.

<61> 실행에 따라 달라질 수 있지만, 사용자-컴퓨터나 식별자-컴퓨터 또는 양자 모두 데이터베이스(703)로부터 제1 입력으로서 진실 보안 식별자를 수신하고, 고객의 입/출력장치(503)를 통해 제2 입력으로서 추정 보안 식별자를 수신하여 양자를 비교하며, 상기 제1 입력이 제2 입력과 일치하는지 여부를 나타내는 확인 출력을 생성하기에 접합하다. 만일 상기 제1 입력이 제2 입력과 일치하지 않는 경우, 그 거래의 진행을 차단되거나 차단된 상태로

남게 된다.

<62> 은행/공급자(303)는 계좌 데이터를 읽고 쓰기 위해 접속되는 계좌 데이터베이스(1003)를 통해 은행-컴퓨터 상에서 운영되는 계좌접속 소프트웨어를 통제관리한다. 주목할 점은, 본 발명의 많은 적용례에서, 은행/공급자가 인원확인서비스를 제공하고 관리 및 운영한다는 것이다. 그러한 경우들에 있어서, 식별자의 데이터베이스(703) 및 은행/공급자의 계좌 데이터베이스(1003)는 하나 또는 복수개의 서버들 상에서 운영되는 물리적으로 동일한 데이터베이스일 수 있다. 또한, 주목할 점은, 본 발명에 따른 비금융적 적용례에서 상품들/서비스들의 공급자는 금융서비스 기관들이 개입하거나 또는 그렇지 않은 거래의 당자사임을 분명하게 나타내기 위해, 도면상 기관(303)이 "은행/공급자"로 지명된다는 것이다. 본 발명에 따른 전술한 비금융적 적용의 예가 이하에서 제공된다.

<63> 바람직한 실시예에 따르면, 계좌 데이터베이스(1003)는 잔액, 신용한도 총액, 거래내역 기타 등등의 구체적인 계좌 데이터를 포함한다. 특히 중요한 것은 고객의 신원확인이 필요한지 여부를 나타내는 각 계좌기록에 있어서의 플래그(flag)이다. 상기 계좌 데이터베이스는 또한 고객의 이름, 전화번호, 주소 기타 등등의 구체적인 고객 데이터를 포함한다. 계좌관리 소프트웨어(1203)의 운영권을 갖는 은행 및 소매기관들이 계좌 데이터베이스(1003)를 이용할 수 있다.

<64> 본 발명의 실시예들에서, 식별자는 은행과 별개의 기관이며, 식별자-데이터베이스(703)는 오직 식별자(203)만이 직접 이용할 수 있다. 그러나 식별자-컴퓨터(903)의 관리하에, 정보는 통신링크(1803)를 통해 은행/공급자 사이에서 이동된다. 마찬가지로, 정보는 통신링크(1503) 및 식별자-컴퓨터(903)를 통해 사용자-컴퓨터(603)와 식별자-데이터베이스(703) 사이에서 이동된다. 최종적으로, 정보는 전자상거래의 요청이라는 형태로 고객(103)으로부터 은행/공급자(303)로 이동된다. 이러한 통신은 전자적 방식 또는 비전자적 방식으로 실행될 수 있다.

<65> 전술한 바와 같이, 본 발명에 따른 방법은 거래가 완료되기 전에 그 거래의 인증을 위한 선택적 단계들을 포함한다. 상기 인증 단계의 포함을 위해 어떠한 추가적인 물리적 요소들도 요구되지 않는다. 식별자-데이터베이스(703)나 은행/공급자 데이터베이스(1003) 중 어느 하나의 고객기록 부분에 약간의 데이터가 입력되면 된다. 선택적 또는 추가적으로, 승인을 위해 필요한 것이 상인에 의해 만들어질 수 있다.

<66> 본 발명에 따른 시스템의 특히 유용한 한 가지 이점은 상인의 전자식 금전등록기(POS) 컴퓨터를 다시 프로그래밍하거나 기존의 통신 네트워크를 변경할 필요가 없다는 것이다. 또한, 본 발명에 따른 시스템은 식별자-컴퓨터 및 사용자-컴퓨터로 제한된 소프트웨어로 실행될 수 있다.

<67> 로컬 소프트웨어(local software)

<68> 본 발명의 다양한 실시예들에 따른 유틸리티의 범위와 복잡화의 정도는 통신장치에 다운로드되는 로컬 소프트웨어를 실행하는 사용자-컴퓨터에 의해 수행될 수 있는 기능들에 의해 주로 결정된다. 실시예에 따라 달라질 수 있지만, 상기 로컬 소프트웨어는 식별자-컴퓨터로부터 전달되는 신호의 수신기능, 통신장치로의 입력정보 및 통신장치로부터의 출력정보의 암호화/해독화기능, 사용자 통신장치의 입/출력장치에의 정보표시기능, 식별자-컴퓨터로의 응답전달기능, 추정 보안 식별자와 진실 보안 식별자의 비교기능, 신원확인 내역의 기록기능 등을 갖는다.

<69> 로컬 소프트웨어의 다운로딩은 식별자-컴퓨터와 사용자-컴퓨터 사이의 통신링크를 통해 간편하게 이루어질 수 있으나, 다른 많은 대안 기술들 역시 본 발명을 이해한 후의 당업자에게는 자명한 사항이 될 것이다. 예를 들면, 상기 로컬 소프트웨어는 식별자가 제공한 칩에 다운로드될 수 있다. 또는 통신장치가 그 제조시점에서 로컬 소프트웨어를 다운로드한 전용장치일 수 있다.

<70> 암호화(encryption)

<71> 본 발명의 많은 예상가능한 적용례들은 개인보안정보 및 금융보안정보의 전달을 수반한다. 따라서 그러한 적용례들에 있어서, 무선 네트워크를 통해 전달되는 상기 정보는 필수적으로 암호화되어야 한다. 본 발명의 다양한 응용 소프트웨어들(603, 1203, 903)은 모두 각 송수신기들을 통과하는 정보를 암호화하고 해독하기 위한 기능을 포함한다. 보통 사용되는 암호화 프로토콜 및 방법들이 사용하기에 적합하다. 본 발명을 이해한 후의 당업자라면 과도한 실험을 거치지 않고서도 본 발명에 따른 암호화/해독화 절차들을 실행할 수 있을 것이다.

<72> 사용자 통신장치

<73> 고객의 신원을 확인하기 위해 사용되지 않는 경우, 통상의 통신목적을 위해 사용되는 유형의 휴대전화 상에서 본 발명이 실행될 것이지만, 본 발명은 식별자가 고객에게 제공한 전용의 통신장치를 이용함으로써 쉽게 실행될 수 있다. 그러한 전용 통신장치는 호출기나 삐삐(beeper) 보다 크지 않은 패키지(package) 내에서 필요한 모든

기능을 포함한다. 실행에 따라 달라질 수 있지만, 고객과의 입/출력 인터페이스는 단일의 LED나 삐삐와 같이 간단할 수도 있고, 스트리밍 문자메시지(streaming text message)나 음성합성장치(voice synthesizer)와 같이 복잡할 수도 있다.

<74> 송수신기의 유형이나 기관들에 의해 채용된 통신링크에 의해 본 발명이 제한되지는 않는다. 특히 고객과 식별자 사이의 통신을 위해, 무선통신이 많은 적용례에서 바람직하지만, 본 발명의 절차들을 수행하기 위해 사용될 수 있는 현존하는 다른 통신기술이나 미래에 실행될 수 있는 통신기술도 본 발명의 특허청구범위에 속하는 것으로 여겨진다.

<75> 바람직한 실시예에서, 고객과 식별자 사이의 무선통신링크(1503)가 채용되지만, 본 발명은 휴대용 통신장치나 무선통신장치를 사용하지 않더라도 쉽게 실행될 수 있도록 충분히 유연하다는 것이 본 명세서를 통해 이해될 수 있을 것이다. 예를 들면, 고객은 고정된 지리적 위치 및 전적으로 유선통신시스템을 통한 기능을 가질 수 있다. 그와 같은 경우, 식별자와 고객 사이의 통신은 유선을 통하거나, 예를 들어 인스턴트 메신저(instant messenger) 타입의 프로토콜을 이용하는 인터넷을 통해 이루어질 수 있고, 고객의 컴퓨터는 본 발명을 수행하기 위해 필요한 다양한 요구들 및 정보의 송수신기로서 작용한다.

<76> 보안 식별자 프로세싱(secure identifier processing)

<77> 전술한 실시예들에서, 신원확인요청(IVR)에 대한 응답으로 고객은 식별자에게 자신의 보안 식별자를 전송한다(도 2의 1602 참조). 이 전송은 당연히 암호화된 것이다. 대응되는 기술은 식별자-컴퓨터가 식별자-데이터베이스(703)로부터 고객의 진실 보안 식별자를 검색하여, 상기 신원확인요청(IVR)이 전송된 시점에서 상기 진실 보안 식별자를 사용자-컴퓨터(603)로 전송하는 것이다. 이 전송 역시 당연히 암호화된 것이다. 사용자-컴퓨터는 신원확인요청(IVR)에 대한 응답으로 고객이 입력한 추정 보안 식별자와 상기 진실 보안 식별자를 로컬 소프트웨어를 통해 비교한다. 상기 두 개의 식별자들이 일치하는 경우, 사용자-컴퓨터는 자동으로 식별자-컴퓨터로 확인신호를 보낸다. 두 개의 식별자들이 일치하지 않는 경우, 미확인 신호가 보내진다. 식별자가 고객에게 진실 보안 식별자를 보내거나 또는 고객이 식별자에게 추정 보안 식별자를 보내는지와 관계없이, 어느 경우이든 보안 식별자의 암호화, 전송 및 해독화는 각 거래를 위해 오직 한 번만 이루어진다.

<78> 세 번째 접근법은 본 발명의 몇몇 실시예들이 동등하게 만족스럽다는 것을 증명할 수 있다. 이 접근법에서, 상기 선등록 절차 중에, 진실 보안 식별자가 고객의 휴대전화에 다운로드된다. 상기 진실 보안 식별자는 이후, 상기 휴대전화의 소프트웨어에 삽입된 상태로 남게 된다. 식별자-컴퓨터가 사용자-컴퓨터에 신원확인요청(IVR)을 보내면, 고객은 추정 보안 식별자를 입력한다. 사용자-컴퓨터는 고객이 입력한 추정 보안 식별자를 상기 진실 보안 식별자와 비교한다. 상기 추정 보안 식별자와 진실 보안 식별자가 일치하는 경우, 사용자-컴퓨터는 식별자-컴퓨터로 확인신호를 보낸다. 많은 예들에서, 상기 확인신호는 단일 비트에 불과하기 때문에 암호화할 필요는 없다. 전술한 실시예들에서, 금융정보나 계좌번호의 전송을 수반하지 않기 때문에, 암호화된 데이터를 전송할 필요없이, 본 발명을 실행하는 것이 가능하다. 이는 특정 목적을 수행하기 위한 작은 통신장치를 이용한 실행에 있어 특히 바람직하다.

<79> 복잡한 고객 기관들(complex customer entities)

<80> 본 발명의 많은 다양한 변형예들 중 하나에서, 고객은 예를 들어, 본인(당사자) 및 하나 또는 그 이상의 중개인들(agents)을 포함하는 복잡한 기관일 수 있다. 고용주/피고용인, 부모/자녀, 배우자들이 전술한 복잡한 고객들의 예가 될 수 있다. 문제가 되는 것은, 전자상거래를 개시하는 일 기관이나 중개인과, 그 거래를 승인하고 책임을 지는 본인이나 별개의 기관이 서로 다를 수 있다는 점이다.

<81> 이러한 실시예에서, 식별자-컴퓨터로부터의 신원확인요청(IVR)이 전술한 바와 같이, 중개의 휴대전화로 전달된다. 상기 신원확인요청(IVR)은 도 1에 도시된 바에 따라 중개의 사용자-컴퓨터에 의해 처리된다. 중개인은 자신의 패스워드를 입력하고, 그 패스워드는 식별자에게 전달되어 식별자-컴퓨터에 의해 처리된다(1502). 이후, 승인절차가 진행되며, 그 승인절차에서 식별자-컴퓨터는 식별자-데이터베이스로부터 본인(당사자)의 휴대전화번호를 검색하여 본인(당사자)에게 전화를 걸어 중개인에 의해 개시된 거래의 승인을 요청한다. 만일 그 거래가 승인되는 경우, 그 거래는 계속 진행하여 완료된다. 만일 그 거래가 승인되지 않는 경우, 그 거래는 종료된다. 이러한 개선은 본인(당사자)이 월별 청구서를 받을 때 가지 기다렸다가 거래에 대해 사후승인할 필요없이 사전에 거래에 대해 승인하는 것을 가능케 한다.

<82> 다른 대안으로서, 본 발명에 따른 시스템은 신원확인절차와 승인절차가 모두 본인(당사자)에 의해 이루어질 수 있도록 쉽게 설치될 수 있다. 이 경우, 비록 거래가 중개인에 의해 개시되더라도, 식별자-컴퓨터는

본인(당사자)과 통신하여 본인(당사자)의 신원을 확인한다.

<83> 본인(당사자)이 고정된 위치에 있는 경우, 본인(당사자)의 통신장치가 반드시 휴대용이거나 무선방식일 필요는 없다. 예를 들어, 회사의 회계사무소가 식별자-컴퓨터로부터의 승인요청에 대한 처리에 책임이 있을 수 있고, 그 경우 식별자-컴퓨터와의 통신에 있어 상기 회계사무소의 유선전화가 가장 편리할 수 있다. 그럼에도 불구하고, 중개인 및 본인(당사자) 모두 무선통신장치를 통해 통신하는 것 역시 본 발명의 범위 내에 속한다.

<84> 본 발명의 비영리적 적용례들

<85> 전술한 설명들을 이해한 후에는, 본 발명의 잠재적이고도 유용한 다른 다양한 적용례들 역시 본 발명이 속하는 기술분야의 통상의 지식을 가진 자에게 당연한 것이 될 것이다. 예를 들어, 본 발명은 전자식으로 관리되는 호텔 룸이나 그 밖의 보안장소에의 출입권한을 얻기 위한 출입카드를 이용하는 개인의 신원확인에 이용될 수 있고, 문을 여는 것에 대한 요청이 전술한 전자상거래의 요청에 대응된다.

<86> 전술한 바와 같은 본 발명에 따른 비금융적 거래의 적용이 도 4에 도시되어 있다. 손님(104)은 자신의 키-카드를 긁어 방으로 들어가고자 한다(404). 종래 기술에서 보통 행해지는 바와 같이, 코드는 상기 키-카드로부터 읽혀져, 보안 컴퓨터에 의해 확인된다(504). 코드가 일치하지 않거나, 다른 사람이 존재하는 경우, 경보가 울리게 되고(1404), 출입은 거부되며, 보안직원에 의해 조사를 받게 된다.

<87> 상기 코드가 유효한 경우, 호텔의 컴퓨터는 손님의 신원확인에 대한 요청으로 상기 방이 플래그된(flagged) 것인지 여부에 대해 결정한다(1504). 이것은 예를 들면 체크인할 때, 손님에 의해 요청된 옵션일 수 있다. 만일 신원확인에 대한 요구가 필요없는 경우, 방으로의 입장을 기록(log)하고(1604), 그 방의 잠금이 해제된다(604). 만일 그 방이 손님의 신원확인을 위해 플래그된 경우에는, 메시지가 식별자에게 전달되며, 상기 식별자는 손님의 신원확인을 시작한다(1304). 손님이 체크인할 때, 식별자-데이터베이스에 미리 저장된 손님의 휴대전화에 대한 사용자 접속번호를 이용하여, 식별자는 손님의 휴대전화에 전화를 걸고, 손님에게 신원확인요청(IVR)을 보낸다. 손님의 휴대전화가 울리면(704), 사용자-컴퓨터가 활성화되고, 상기 요청을 수신하여 그 확인요청을 처리하며, 이를 상기 휴대전화의 입/출력 장치에 표시한다. 이러한 단계들은 상기 신원확인요청(IVR)의 해독을 포함하여 앞선 신용카드의 예와 유사 또는 동일하다.

<88> 손님의 방으로 들어가고자 하는 시도가 손님 본인에 의한 것이 아닐 경우, 손님의 휴대전화가 울리게 될 것이며, 그에 따라 손님은 누군가가 자신의 키-카드를 소지하여 자신의 방에 들어가고자 한다는 것을 경고받게 될 것이다. 이후, 손님은 호텔이나 경찰에 연락을 취할 것이다.

<89> 방에 들어가고자 하는 사람이 손님 본인인 경우, 손님이 자신의 휴대전화의 키패드에 추정 패스워드를 입력하면(804), 그 추정 패스워드는 암호화처리되어 식별자-컴퓨터에 전달된다. 식별자-컴퓨터는 상기 추정 패스워드를 수신하고 해독하여, 식별자-데이터베이스에 저장된 진실한 패스워드와 일치하는지 여부를 평가한다(1704). 일치하지 않는 경우, 그 사실이 손님에게 통지되고, 손님은 다시 추정 패스워드를 입력하게 된다(904). 실패된 시도 횟수가 미리 결정된 횟수를 초과하면, 경보가 발해지고(1904), 보안직원이 조사하게 된다(1404).

<90> 상기 추정 패스워드가 확인되면(1704), 방으로의 입장이 허용되고(1204), 호텔은 그 방으로의 입장을 기록(log)하며(1104), 그 방의 잠금이 해제된다(1004).

<91> 호텔 방에 대한 출입권한을 얻기 위한 전술한 실시예는 빌딩, 차량, 창고 사물함 또는 안전 대여 금고와 같은 특정 장소에 대한 출입권한을 얻는데 사용되도록 쉽게 변형될 수 있다.

<92> 서비스들 및 이익들을 얻기 위한 다양한 상업적 및 비상업적 전자상거래에 본 발명이 편리하게 적용될 수 있음을 이해할 수 있을 것이다. 예를 들면, 국경에서, 미리 획득한 비자로 특정 국가로의 입국에 대한 허가를 요청하는 이주자가 그 비자 또는 패스포트를 제시하고, 상기 비자 또는 패스포트를 리더기에 긁음으로써 개인회사 또는 정부기관일 수 있는 식별자에게 신원확인에 대한 요청을 개시할 수 있다. 상기 식별자는 상기 이주자의 휴대전화에 전화를 걸어 신원확인요청(IVR)을 보낸다. 상기 휴대전화가 울려 상기 이주자가 상기 신원확인요청(IVR)에 대한 응답으로 보안 식별자를 입력하면, 국경의 요원들은 상기 이주자의 신원에 대한 즉각적인 확인을 얻게 된다. 상기 휴대전화가 전혀 울리지 않는 경우, 국경의 요원은 이주자가 제시한 비자 또는 패스포트를 위조서류들로 의심하게 될 것이고, 그에 따라 필요한 적절한 조치를 취할 것이다. 만일 상기 휴대전화가 울리기는 하나, 그 이주자가 올바른 보안 식별자를 제공하지 않는 경우, 국경의 요원은 그 휴대전화 및 서류가 도난당한 것으로 의심하게 될 것이고, 그에 따라 필요한 적절한 조치를 취할 것이다.

<93> 식별자 발행 임시거래카드(verifier-issued proxy transaction card)

<94> 사용자의 하나 또는 그 이상의 신용카드들을 대체하고, 식별자가 사용자의 하나 또는 그 이상의 계좌들에 접속하는 것을 사용자가 승인하는데 사용되는 임시거래카드를 식별자가 사용자에게 발급하는 본 발명에 따른 방법의 일 실시예가 도 5에 요약되어 있다. 이 실시예에서, 선등록 단계 중, 사용자는 식별자에게 하나 또는 그 이상의 계좌들 - 이 실시예에서는 비자카드 계좌 - 에 접속하기 위한 계좌접속정보 및 비임시적(standing) 승인을 제공한다. 고객이 단순히 자신의 비자카드를 식별자에게 주는 것에 의해 계좌에 대한 선등록이 이루어질 수 있고, 식별자는 상기 카드를 리더기에 긁어 상기 계좌접속정보를 얻어 식별자-데이터베이스에 저장할 수 있다. 선등록하는 동안, 상기 신용카드 계좌접속정보는 사용자에 의해 제공된 다른 데이터와 함께 전술한 바와 같이 식별자-데이터베이스에 저장된다. 이 실시예에서, 선등록, 데이터의 저장 및 검색, 신용카드 회사와의 통신들은 사용자의 은행의 필수적인 개입 없이, 식별자 회사에 의해 모두 수행된다.

<95> 신용카드 계좌 데이터가 식별자-데이터베이스에 입력된 후, 식별자는 사용자에게 임시거래카드(proxy transaction card)를 발급한다. 상기 임시거래카드는 그 크기 및 모양이 신용카드와 유사하며, 자성띠(magnetic strip)를 갖는다. 상기 임시거래카드에 있는 자성띠는 오직 소매업자와 식별자 사이의 통신링크를 열기 위해 필요한 최소한의 정보를 포함할 필요가 있다.

<96> 이 실시예에서 사용된 "소매업자"란 용어는, 도 5에 "소매업자/상인의 은행"으로 표시된 것처럼, 상인 및 그 상인의 은행이나 자금이 예치될 다른 금융기관을 모두 포함한다. 따라서 상기 임시거래카드로부터 읽어진 데이터는 전자식 금전등록기(POS)로부터 상인의 은행으로 전달되며, 이후 식별자와의 통신링크는 305 단계에서 열린다. 이러한 구체적인 내용은 본 발명에 따른 시스템을 적용하는 기관들의 구체적인 필요에 따라 달라질 수 있으나, 어느 경우이든, 정보의 흐름은 사용자에게는 보이지 않는다.

<97> 판매시점에서, 사용자(101)는 상기 임시거래카드를 제시함으로써 소매업자/상인의 은행(102)과 거래를 시작한다. 소매업자는 상기 임시거래카드를 자성 리더기에 긁어 상기 임시거래카드의 자성띠에 있는 정보를 읽는다. 상기 소매업자는 거래물품 및 구매총액과 같은 거래의 상세내용을 입력한다. 통신링크는 상기 임시거래카드로부터 얻어진 통신정보를 이용하는 식별자-컴퓨터와 소매업자/상인의 은행 사이에 열리고, 거래정보는 식별자에게 전달된다(305).

<98> 옵션으로서, 고객은 식별자가 제공한 임시거래카드를 통해 접속될 수 있는 계좌를 하나 이상 원할 수도 있다. 그 경우, 상기 임시거래카드의 자성띠는 이용가능한 계좌들 및 각 계좌와 관련된 단순한 식별자(simple identifier)의 목록을 포함하며, 이 경우의 식별자는 보안 식별자일 필요는 없다. 상기 임시거래카드가 소매업자에 의해 긁어질 때, 이용가능한 계좌들의 목록이 소매업자의 스크린에 표시된다. 소비자는 어떤 계좌가 사용될 것인지 및 식별자에게 그 계좌에 대한 어떤 식별자가 보내질 것인지를 지시하며, 본 실시예에서는 비자카드 계좌 #1(VISA® account #1)을 그 예로 들 수 있다.

<99> 소매업자로부터의 통신을 수신하자마자, 식별자는 식별자-데이터베이스로부터 사용자의 1번 비자카드 계좌의 데이터를 검색하고, 도 2에 도시된 방법과 유사한 방법을 이용하여 사용자의 신원확인을 개시한다(605). 간단하게, 식별자는 사용자의 휴대전화로 신원확인요청(IVR)을 보내(705), 선등록하는 동안, 상기 휴대전화에 다운로드된 로컬 소프트웨어를 활성화시킨다. 이후, 사용자-컴퓨터는 통신링크가 올바르게 작동한다는 것을 표시하는 것으로 식별자-컴퓨터에 응답한다(805). 상기 식별자-컴퓨터는 열려진 통신링크를 통해 사용자의 휴대전화로 암호화된 신원확인요청(IVR)을 보낸다. 사용자는 휴대전화에 자신의 비밀번호(PIN)나 패스워드 또는 기타 추정 보안 식별자를 입력한다(1005). 상기 추정 보안 식별자는 암호화되어 다시 식별자에게 전달되고, 식별자-데이터베이스로부터 검색된 진실 보안 식별자와 비교되어 진다(1105). 만일 상기 추정 보안 식별자와 진실 보안 식별자가 일치하지 않을 경우, 그 거래는 거부되고(1505), 그 사실이 소매업자에게 통보되며(705), 사용자에게도 통보된다(1805). 물론, 전술한 바와 같이, 거부절차는 복수의 시도들을 허용하며, 시간초과 여부의 분석 및 경찰에의 신고나 다른 적절한 대응들의 개시를 포함할 수 있다. 이러한 단계들이 도 5에 도시되어 있지는 않다. 사용자가 직불할 계좌로 어떤 것을 선택하였는지와 관계없이, 동일한 확인단계들 및 동일한 보안 식별자가 이용된다. 따라서 사용자는 많은 계좌들 중 어느 하나에 접속하기 위해 오직 하나의 비밀번호(PIN)나 패스워드를 기억할 필요가 있다.

<100> 다른 대안으로서, 본 발명에 따른 시스템은 사용자의 이용가능한 계좌들의 목록이 임시거래카드에 포함되는 것이 아니라 식별자-데이터베이스에 존재하도록 설치될 수 있다. 일단 임시거래카드가 긁어져 소매업자/상인의 은행과 식별자 사이에 통신링크가 열리게 되면, 식별자는 식별자-데이터베이스로부터 이용가능한 계좌들의 목록을 검색하고, 사용자와의 사이에 통신링크를 열어 사용자 통신장치로 그 이용가능한 계좌들의 목록을 전송한다. 이후, 사용자는 사용자 통신장치에 선택한 계좌를 입력한다.

<101> 상기 추정 보안 식별자와 진실 보안 식별자가 일치하는 경우(1105), 식별자는 적당한 신용 제공자(105)(즉, 비자카드 계좌 #1(VISA® account #1)와의 통신링크를 연다. 이것은 선등록하는 동안, 사용자가 식별자에게 계좌접속정보를 제공했기 때문에 가능하다. 식별자-컴퓨터는 상기 신용 제공자에게 계좌정보 및 계류중인 거래의 상세 내역을 전달(1905)함으로써 상기 거래를 선택된 계좌로 통과시킨다. 이후, 상기 신용 제공자는 사용자의 계좌가 상기 거래를 충족시키기 위해 이용할 수 있는 충분한 신용이 있는지 여부를 결정하기 위해 자신의 데이터베이스에 조회하여, 상기 거래를 승인(1305)할 것인지 아니면 거부(1405)할 것인지를 결정한다. 전술한 결정은 식별자-컴퓨터에 전달되며(1605), 식별자-컴퓨터는 자신의 데이터베이스에 적절한 주석을 달고, 소매업자에게 통지하며(1705), 사용자에게도 통지하여(1805), 상기 거래가 신용 제공자로부터의 지시에 따라 완료되거나 취소될 수 있도록 한다. 상기 거래의 개시와 관련된 전술한 모든 단계들의 진행은 사람의 중재 없이 자동으로 수행될 수 있다.

<102> 본 발명은 다음과 같은 중요한 많은 이점이 있다. 첫째, 소비자는 신용카드들이나 그 카드들과 관련된 계좌들의 확인을 위한 정보를 수반할 필요가 없다. 따라서 식별자가 발급한 임시거래카드가 일반 신용카드가 된다. 왜냐하면, 고객은 상인이나 고객의 통신장치로 어떠한 계좌정보도 전송할 필요없이, 상기 임시거래카드를 통해 안전하게 고객의 모든 신용카드 계좌들에 접속할 수 있기 때문이다. 둘째, 고객은 자신의 모든 신용카드 계좌들에 접속하기 위한 하나의 비밀번호(PIN)만 기억하면 된다. 셋째, 사용자가 세계 어디에서 자신의 임시거래카드를 제시하든지 간에, 전자식 금전등록기(POS)로부터 사용자의 계좌들과 관련된 어떠한 계좌번호나 기타 정보도 전송되지 않는다. 오직 계좌정보만이 중앙 집권화된 식별자로부터 신용 제공자로 전송된다. 그 결과, 계좌정보의 전송에 대한 보안이 효율적으로 관리될 수 있을 뿐만 아니라, 크게 향상될 수 있다. 넷째, 식별자가 신용카드 제공자에 대한 게이트웨이(gateway)로서 작용하기 때문에, 소비자의 은행은 전자상거래에 수반될 필요가 없다. 정보의 흐름은 소매업자와 식별자 사이, 식별자와 사용자 사이, 식별자와 신용카드 제공자 사이에서 이루어진다.

<103> 지금까지의 전술한 상세한 설명을 통해, 본 발명의 신규함, 유용성 및 본 발명을 구성하고 실행하는 수단들이 쉽게 이해될 수 있을 것이다. 전술한 본 발명의 바람직한 실시예들에 대한 설명은 현 시점에서 본 발명자가 알고 있는 가장 바람직한 방식(best mode)을 대표한다. 본 발명이 전술한 실시예들만으로 한정되어서는 안 되며, 본 명세서의 특허청구범위 내에 포함될 수 있는 모든 실시예들을 포함하는 것으로 이해되어야 한다.

도면의 간단한 설명

<104> 도 1은 본 발명에 따른 방법에 있어서의 선등록(pre-enrolling) 단계를 나타낸 다이어그램이다.

<105> 도 2는 신용카드 전자상거래에 적용된 본 발명에 따른 방법의 플로차트이다.

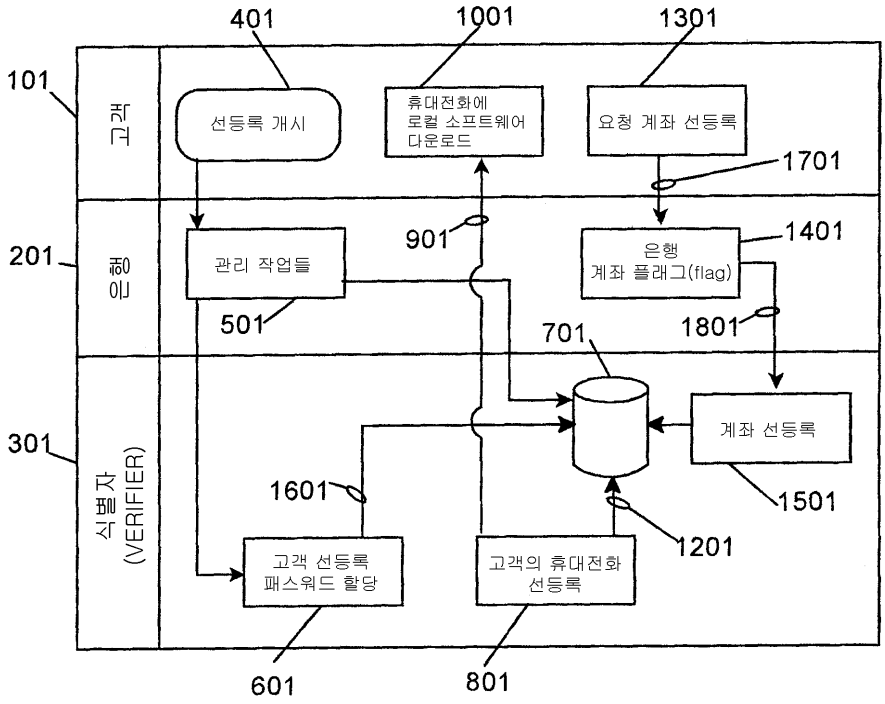
<106> 도 3은 본 발명에 따른 시스템의 다양한 구성요소들 및 그들의 상호작용을 나타낸 다이어그램이다.

<107> 도 4는 방(room)에의 출입을 허가하기 위한 전자상거래에 적용된 본 발명에 따른 방법의 플로차트이다.

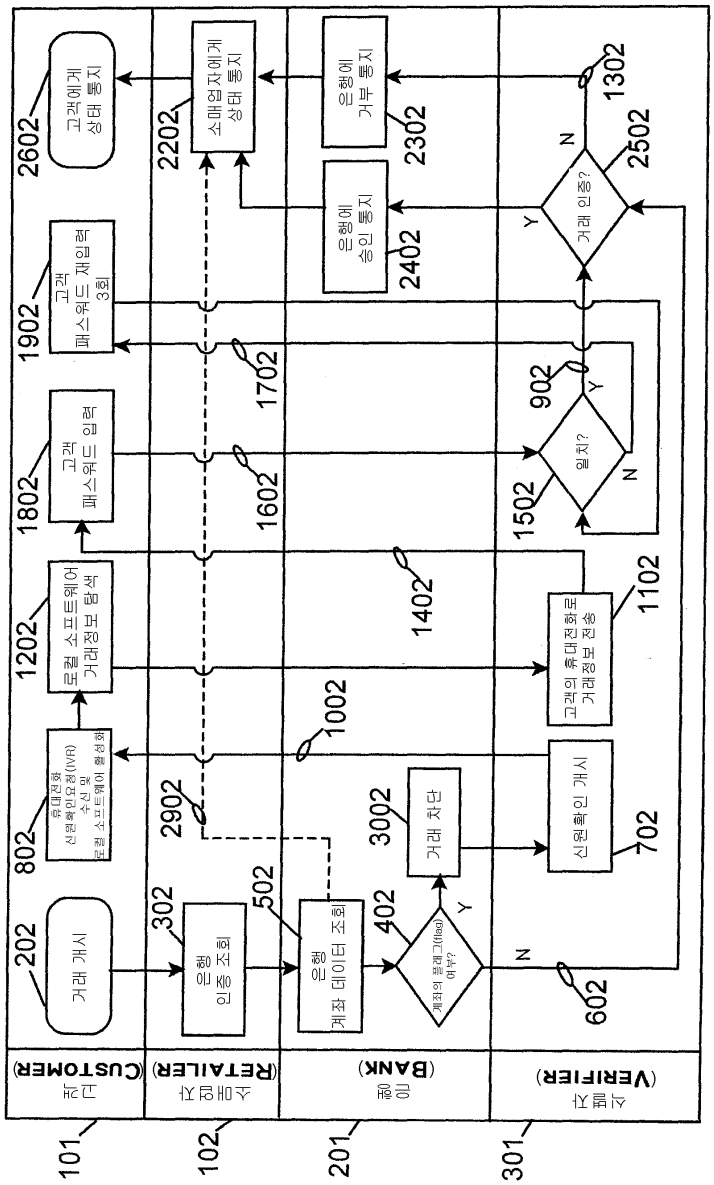
<108> 도 5는 검사기-발행 임시 거래카드(verifier-issued proxy transaction card)에 기초한 본 발명에 따른 방법의 플로차트이다.

도면

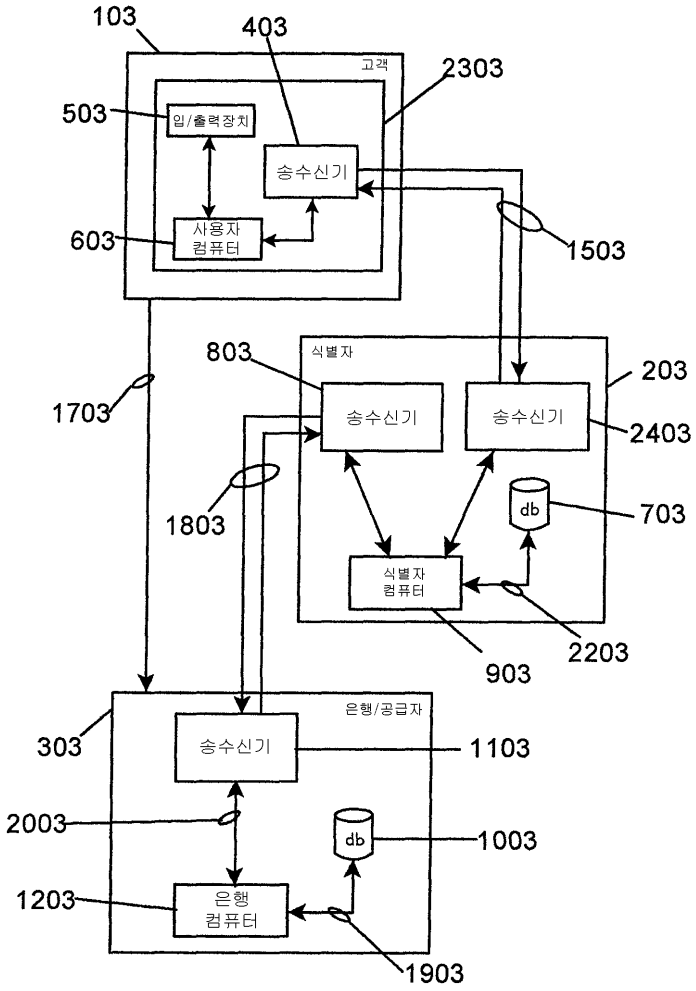
도면1


401
1001
1301
101
고객
선등록 개시
휴대전화에
로컬 소프트웨어
다운로드
요청 계좌 선등록
1701
201
은행
관리 작업들
901
은행
계좌 플래그(flag)
1401
501
701
1801
301
식별자
(VERIFIER)
계좌 선등록
1601
1501
1201
고객 선등록
패스워드 할당
고객의 휴대전화
선등록
601
801

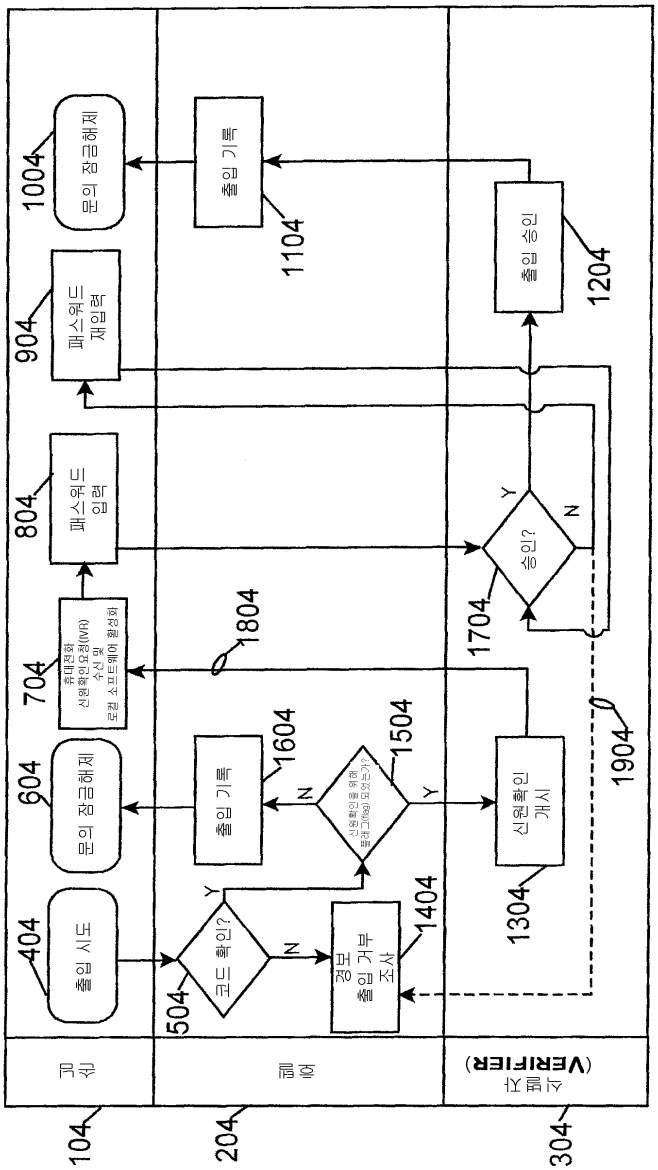
도면2


(CUSTOMER)
고객
(RETAILER)
소매업자
(BANK)
은행
(VERIFIER)
검증자
101
102
201
301
202
거래 개시
802
휴대전화
신원확인요청(IVR)
수신 및
로컬 소프트웨어 활성화
1202
로컬 소프트웨어
거래정보 탐색
1802
고객
패스워드 입력
1902
고객
패스워드 재입력
3회
2602
고객에게
상태 통지
302
은행
인증 조회
2902
2202
소매업자에게
상태 통지
502
은행
계좌 데이터 조회
1002
402
계좌의 플래그(flag)
여부?
Y
N
3002
거래 차단
2402
은행에
승인 통지
2302
은행에
거부 통지
1402
602
신원확인 개시
702
고객의 휴대전화로
거래정보 전송
1102
1502
일치?
902
Y
N
1602
1702
거래 인증?
1302
2502
Y
N

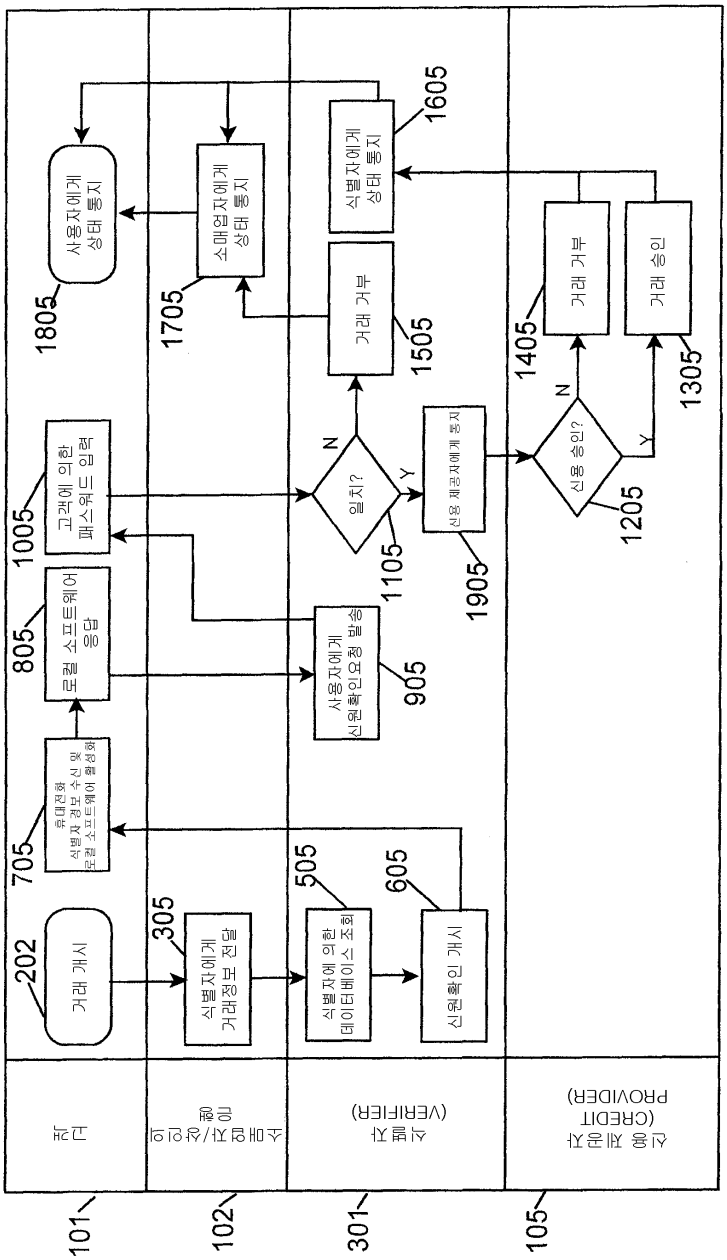
도면3


103
403
고객
2303
503
입/출력장치
송수신기
603
사용자
컴퓨터
1503
803
식별자
203
1703
송수신기
송수신기
2403
1803
db
703
식별자
컴퓨터
903
2203
은행/공급자
303
송수신기
1103
2003
db
1003
1203
은행
컴퓨터
1903

도면4


104
204
304
출입 시도
문의 잠금해제
패스워드 입력
패스워드 재입력
문의 잠금해제
출입 기록
출입 승인
404
604
804
904
1004
1104
1204
코드 확인?
출입 기록
출입 거부 조사
신원확인 개시
승인?
504
1604
1404
1304
1704
Y
N

도면5


101
102
301
105
202
305
505
605
705
805
1005
1105
1205
1305
1405
1505
1605
1705
1805
1905
거래 개시
식별자에게 거래정보 전달
식별자에 의한 데이터베이스 조회
신원확인 개시
휴대전화 식별자 경보 수신 및 로컬 소프트웨어 활성화
로컬 소프트웨어 응답
고객에 의한 패스워드 입력
사용자에게 신원확인요청 발송
일치?
N
Y
신용 제공자에게 통지
신용 승인?
N
Y
거래 거부
거래 승인
식별자에게 상태 통지
소매업자에게 상태 통지
사용자에게 상태 통지
판매자
소매업자/상인
식별자 (VERIFIER)
신용 제공자 (CREDIT PROVIDER)