(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년09월22일
(11) 등록번호 10-1067191
(24) 등록일자 2011년09월16일

(51) Int. Cl.
G06F 21/00 (2006.01) *G06F 9/06* (2006.01)
H04L 9/00 (2006.01)
(21) 출원번호 10-2010-7000597
(22) 출원일자(국제출원일자) 2007년09월04일
심사청구일자 2010년03월02일
(85) 번역문제출일자 2010년01월11일
(65) 공개번호 10-2010-0036313
(43) 공개일자 2010년04월07일
(86) 국제출원번호 PCT/US2007/077503
(87) 국제공개번호 WO 2009/029116
국제공개일자 2009년03월05일
(30) 우선권주장
11/844,408 2007년08월24일 미국(US)
(56) 선행기술조사문헌
US06078902 A
US20030161473 A1
전체 청구항 수 : 총 20 항

(73) 특허권자
베네도르 코퍼레이션
미국 캘리포니아주 93021-3552 무어파크 마야 서클 14183
(72) 발명자
칼롯, 리차드, 에프.
미국 캘리포니아주 93021-3552 무어파크 마야 서클 14183
(74) 대리인
정영수

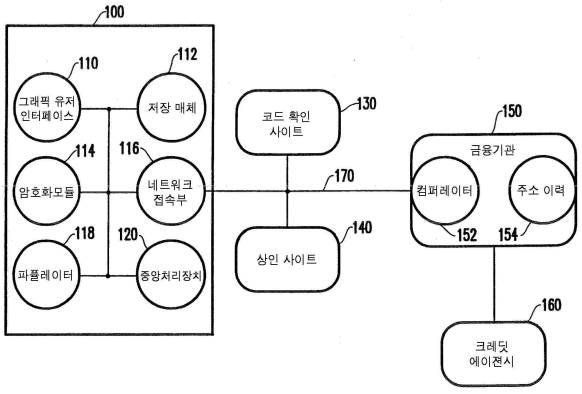
심사관 : 경연정

(54) 네트워크를 통한 트랜잭션 보안 방법

(57) 요 약

본 발명에 따른 시스템 및 방법은 전자적으로 저장가능한 아이템의 구매를 포함하여 컴퓨터 네트워크를 통한 구매 트랜잭션을 용이하게 한다. 본 발명의 실시예는 "고객 정보"를 암호화 스트림으로 암호화하고, 암호화 스트림이 구매 트랜잭션에서 고객으로부터 상인에게로 전송되게 한다. 검증 주체는 동일성 인증 및 결제 승인을 위하여 상인에 의해 전송된 암호화 스트림을 수신한다. 그 다음, 검증 주체는 암호화 스트림에 포함된 식별자를 검증하고, 검증 주체로부터 동일성 인증 및 결제 승인을 상인에게 전송한다. 상인에 의해, 암호화 스트림 또는 유일한 트랜잭션 식별자가 구매한 전자 아이템에 부가되어 개인화된 전자 아이템을 생성하게 된다.

대 표 도 - 도1



특허청구의 범위

청구항 1

이름 식별자, 고객 나이 식별자, 주소 식별자 및 고객 약정 식별자를 포함하는, 고객 정보를 암호화 스트림으로 암호화하는 단계;

구매된 전자 아이템의 구매 트랜잭션에 있어서 상기 암호화 스트림이 상기 고객으로부터 상인에게 전송되게 하는 단계;

상기 암호화 스트림이 검증 주체로 라우팅되게 하는 단계;

상기 검증 주체에 의하여 상기 암호화 스트림에 기초한 동일성 인증 및 결제 승인 중 적어도 하나를 포함하는 유일한 트랜잭션 식별자를 생성하는 단계;

상기 유일한 트랜잭션 식별자를 생성하기 위하여 상기 검증 주체에 의하여 상기 암호화 스트림을 고객 정보를 포함하는 별개의 데이터베이스와 상호 비교하는 단계;

상기 검증 주체에 의하여 상기 유일한 트랜잭션 식별자를 상기 상인에게 전송하는 단계로서, 상기 암호화 스트림과 상기 유일한 트랜잭션 식별자는 상기 고객의 개인 결제 정보를 결여하고 있는 단계;

개인화된 전자 아이템을 생성하기 위하여, 상기 상인에 의하여 상기 암호화 스트림 및 상기 유일한 트랜잭션 식별자 중 적어도 하나가 상기 구매된 전자 아이템에 부가되게 하는 단계; 및

상기 개인화된 전자 아이템이 상기 상인으로부터 상기 고객에게 제공되게 하는 단계;를 포함하고,

다른 고객에게 제공된 각각의 상기 개인화된 전자 아이템은 각각의 암호화 스트림의 유일성 때문에 서로 상이한 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 2

제 1 항에 있어서, 상기 고객 정보를 암호화하는 단계는,

a) 상기 고객이 제1 컴퓨터 디바이스를 사용하여 상기 검증 주체에 접속하는 단계;

b) 상기 제1 컴퓨터 디바이스로부터 하드웨어 식별자를 읽어오는 단계;

c) 상기 하드웨어 식별자를 상기 암호화 스트림에 편입시키는 단계; 및

d) 상기 고객이 모든 구매 트랜잭션에서 사용하기를 원하는 추가적인 컴퓨터 디바이스에 대하여 상기 a 내지 c 단계를 반복하는 단계;

를 더 포함하는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 3

제 2 항에 있어서, 상기 암호화 스트림을 상기 고객으로부터 상기 상인에게 전송되게 하는 단계는,

상기 암호화 스트림을 상기 상인에게 실제 전송하기 이전에, 상기 실제 전송을 하는 컴퓨터 디바이스로부터 시간 및 날짜 스탬프 및 제2 세트의 하드웨어 식별자를 상기 암호화 스트림에 편입시키는 단계; 및

비-암호화 라우팅 식별자를 상기 암호화 스트림에 부가하는 단계;

를 더 포함하는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 4

제 1 항에 있어서, 상기 동일성 인증 및 상기 결제 승인은 상기 구매 트랜잭션에서 상기 고객의 실제 존재를 상기 상인에게 확인시키고, 그 결과 상기 상인은 상기 실제 고객과 거래하고 있다는 확신을 가지게 되는 것을 특

징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 5

제 1 항에 있어서, 상기 각각의 암호화 스트림의 유일함은 상기 구매된 전자 아이템의 인증되지 않은 복사본의 출처가 상기 검증 주체를 통하여 식별되게 하는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 6

이름 식별자, 고객 나이 식별자, 주소 식별자 및 고객 약정 식별자를 포함하는, 고객 정보를 암호화 스트림으로 암호화하는 단계;

구매된 전자 아이템의 구매 트랜잭션에 있어서 상기 암호화 스트림이 상기 고객으로부터 상인에게 전송되게 하는 단계;

상기 암호화 스트림이 검증 주체로 라우팅되게 하는 단계;

상기 검증 주체에 의하여 상기 암호화 스트림에 기초한 동일성 인증 및 결제 승인 중 적어도 하나를 포함하는 유일한 트랜잭션 식별자를 생성하는 단계;

상기 유일한 트랜잭션 식별자를 생성하기 위하여 상기 검증 주체에 의하여 상기 암호화 스트림을 고객 정보를 포함하는 별개의 데이터베이스와 상호 비교하는 단계;

상기 검증 주체에 의하여 상기 동일성 인증 및 상기 결제 승인 중 적어도 하나를 상기 상인에게 전송하는 단계로서, 상기 암호화 스트림, 상기 동일성 인증 및 상기 결제 승인은 상기 고객의 개인 결제 정보를 결여하고 있는 단계;

개인화된 전자 아이템을 생성하기 위하여, 상기 상인에 의하여 상기 암호화 스트림, 상기 동일성 인증 및 상기 결제 승인 중 적어도 하나가 상기 구매된 전자 아이템에 부가되게 하는 단계; 및

상기 개인화된 전자 아이템이 상기 상인으로부터 상기 고객에게 제공되게 하는 단계;를 포함하고,

다른 고객에게 제공된 각각의 상기 개인화된 전자 아이템은 각각의 암호화 스트림의 유일성 때문에 서로 상이한 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 7

제 6 항에 있어서, 상기 고객 정보를 암호화하는 단계는,

a) 상기 고객이 제1 컴퓨터 디바이스를 사용하여 상기 검증 주체에 접속하는 단계;

b) 상기 제1 컴퓨터 디바이스로부터 하드웨어 식별자를 읽어오는 단계;

c) 상기 하드웨어 식별자를 상기 암호화 스트림에 편입시키는 단계; 및

d) 상기 고객이 모든 구매 트랜잭션에서 사용하기를 원하는 추가적인 컴퓨터 디바이스에 대하여 상기 a 내지 c 단계를 반복하는 단계;

를 더 포함하는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 8

제 7 항에 있어서, 상기 암호화 스트림을 상기 고객으로부터 상기 상인에게 전송되게 하는 단계는,

상기 암호화 스트림을 상기 상인에게 실제 전송하기 이전에, 상기 실제 전송을 하는 컴퓨터 디바이스로부터 시간 및 날짜 스탬프 및 제2 세트의 하드웨어 식별자를 상기 암호화 스트림에 편입시키는 단계; 및

비-암호화 라우팅 식별자를 상기 암호화 스트림에 부가하는 단계;

를 더 포함하는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 9

제 6 항에 있어서, 상기 동일성 인증 및 상기 결제 승인은 상기 구매 트랜잭션에서 상기 고객의 실제 존재를 상기 상인에게 확인시키고, 그 결과 상기 상인은 상기 실제 고객과 거래하고 있다는 확신을 가지게 되는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 10

제 6 항에 있어서, 상기 상호 비교하는 단계는 상기 동일성 인증 및 결제 승인을 행하기 이전에, 모든 요구되는 인증 정보가 상기 암호화 스트림내에 포함되어 있는지 여부를 확인하는 단계를 포함하는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 11

이름 식별자, 고객 나이 식별자, 주소 식별자 및 고객 약정 식별자 중 적어도 하나를 포함하는, 고객 정보를 암호화 스트림으로 암호화하는 단계;

구매된 전자 아이템의 구매 트랜잭션에 있어서 상기 암호화 스트림이 상기 고객으로부터 상인에게 전송되게 하는 단계;

상기 암호화 스트림이 검증 주체로 라우팅되게 하는 단계;

상기 검증 주체에 의하여 상기 암호화 스트림에 기초한 유일한 트랜잭션 식별자를 생성하는 단계;

상기 유일한 트랜잭션 식별자를 생성하기 위하여 상기 검증 주체에 의하여 상기 암호화 스트림을 고객 정보를 포함하는 별개의 데이터베이스와 상호 비교하는 단계;

상기 검증 주체에 의하여 상기 유일한 트랜잭션 식별자를 상기 상인에게 전송하는 단계로서, 상기 암호화 스트림 및 상기 유일한 트랜잭션 식별자는 상기 고객의 개인 결제 정보를 결여하고 있는 단계;

개인화된 전자 아이템을 생성하기 위하여, 상기 상인에 의하여 상기 암호화 스트림이 상기 구매된 전자 아이템에 부가되게 하는 단계; 및

상기 개인화된 전자 아이템이 상기 상인으로부터 상기 고객에게 제공되게 하는 단계;를 포함하고,

다른 고객에게 제공된 각각의 상기 개인화된 전자 아이템은 각각의 암호화 스트림의 유일성 때문에 서로 상이한 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 12

제 11 항에 있어서, 상기 고객 정보를 암호화하는 단계는,

a) 상기 고객이 제1 컴퓨터 디바이스를 사용하여 상기 검증 주체에 접속하는 단계;

b) 상기 제1 컴퓨터 디바이스로부터 하드웨어 식별자를 읽어오는 단계;

c) 상기 하드웨어 식별자를 상기 암호화 스트림에 편입시키는 단계; 및

d) 상기 고객이 모든 구매 트랜잭션에서 사용하기를 원하는 추가적인 컴퓨터 디바이스에 대하여 상기 a 내지 c 단계를 반복하는 단계;

를 더 포함하는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 13

제 12 항에 있어서, 상기 암호화 스트림을 상기 고객으로부터 상기 상인에게 전송되게 하는 단계는,

상기 암호화 스트림을 상기 상인에게 실제 전송하기 이전에, 상기 실제 전송을 하는 컴퓨터 디바이스로부터 시간 및 날짜 스탬프 및 제2 세트의 하드웨어 식별자를 상기 암호화 스트림에 편입시키는 단계; 및

비-암호화 라우팅 식별자를 상기 암호화 스트림에 부가하는 단계;

를 더 포함하는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 14

제 11 항에 있어서, 상기 유일한 트랜잭션 식별자는 상기 구매 트랜잭션에서 상기 고객의 실제 존재를 상기 상인에게 확인시키고, 그 결과 상기 상인은 상기 실제 고객과 거래하고 있다는 확신을 가지게 되는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 15

제 11 항에 있어서, 상기 각각의 암호화 스트림의 유일함은 상기 구매된 전자 아이템의 인증되지 않은 복사본의 출처가 상기 검증 주체를 통하여 식별되게 하는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 16

고객 약정 식별자를 포함하는 고객 정보를 암호화 스트림으로 암호화하는 단계;

상품 및 서비스 중 하나를 포함하는 구매를 위한 구매 트랜잭션에 있어서 상기 암호화 스트림이 상기 고객으로부터 상인에게 전송되게 하는 단계;

상기 암호화 스트림이 검증 주체로 라우팅되게 하는 단계;

상기 검증 주체에 의하여 상기 암호화 스트림에 기초한 동일성 인증 및 결제 승인 중 적어도 하나를 포함하는 유일한 트랜잭션 식별자를 생성하는 단계;

상기 유일한 트랜잭션 식별자를 생성하기 위하여 상기 검증 주체에 의하여 상기 암호화 스트림을 고객 정보를 포함하는 별개의 데이터베이스와 상호 비교하는 단계; 및

상기 검증 주체에 의하여 상기 동일성 인증 및 상기 결제 승인 중 적어도 하나를 상기 상인에게 전송하는 단계로서, 상기 암호화 스트림, 상기 동일성 인증 및 상기 결제 승인은 상기 고객의 개인 결제 정보를 결여하고 있는 단계;

를 포함하는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 17

제 16 항에 있어서, 상기 고객 정보를 암호화하는 단계는,

a) 상기 고객이 제1 컴퓨터 디바이스를 사용하여 상기 검증 주체에 접속하는 단계;

b) 상기 제1 컴퓨터 디바이스로부터 하드웨어 식별자를 읽어오는 단계;

c) 상기 하드웨어 식별자를 상기 암호화 스트림에 편입시키는 단계; 및

d) 상기 고객이 모든 구매 트랜잭션에서 사용하기를 원하는 추가적인 컴퓨터 디바이스에 대하여 상기 a 내지 c 단계를 반복하는 단계;

를 더 포함하는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 18

제 17 항에 있어서, 상기 암호화 스트림을 고객으로부터 상기 상인에게 전송되게 하는 단계는,

상기 암호화 스트림을 상기 상인에게 실제 전송하기 이전에, 상기 실제 전송을 하는 컴퓨터 디바이스로부터 시간 및 날짜 스탬프 및 제2 세트의 하드웨어 식별자를 상기 암호화 스트림에 편입시키는 단계; 및

비-암호화 라우팅 식별자를 상기 암호화 스트림에 부가하는 단계;

를 더 포함하는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 19

제 16 항에 있어서, 상기 동일성 인증 및 상기 결제 승인은 상기 구매 트랜잭션에서 상기 고객의 실제 존재를 상기 상인에게 확인시키고, 그 결과 상기 상인은 상기 실제 고객과 거래하고 있다는 확신을 가지게 되는 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 방법.

청구항 20

삭제

청구항 21

고객 컴퓨터내에 위치하고, 이름 식별자, 고객 나이 식별자, 주소 식별자 및 고객 약정 식별자를 포함하는 고객 정보를 암호화 스트림으로 암호화하기 위하여 부착되는 인코더;

상기 고객 컴퓨터내에 위치하고, 구매된 전자 아이템의 구매 트랜잭션에 있어서 상기 암호화 스트림이 상기 고객 컴퓨터로부터 상인 컴퓨터로 전송되게 하는 전송 에이젼트;

상기 상인 컴퓨터에 작동되게 연결되고, 상기 고객 컴퓨터 및 상기 상인 컴퓨터로부터 별개로 분리되어 있는 검증기;

상기 검증기에 작동되게 연결되고 상기 고객 정보를 포함하는 데이터베이스;를 포함하고,

상기 전송 에이젼트는 상기 암호화 스트림이 상기 상인 컴퓨터로부터 상기 검증기로 전송되도록 구성되고,

상기 검증기는 상기 데이터베이스에 기초한 동일성 인증 및/또는 결제 승인을 포함하는 유일한 트랜잭션 식별자를 생성하고, 상기 유일한 트랜잭션 식별자를 생성하기 위하여 상기 검증 주체에 의하여 상기 암호화 스트림을 고객 정보를 포함하는 별개의 데이터베이스와 상호 비교하고, 상기 유일한 트랜잭션 식별자를 상기 상인에게 전송하도록 구성되고,

상기 암호화 스트림 및 상기 유일한 트랜잭션 식별자는 상기 고객의 개인 결제 정보를 결여하고 있고,

상기 상인으로부터 상기 고객에게 제공되는 개인화된 전자 아이템을 생성하기 위하여, 상기 상인에 의하여 상기 암호화 스트림 및 상기 유일한 트랜잭션 식별자 중 적어도 하나가 상기 구매한 전자 아이템에 부가되고,

다른 고객에게 제공된 각각의 상기 개인화된 전자 아이템은 각각의 암호화 스트림의 유일성 때문에 서로 상이한 것을 특징으로 하는 네트워크를 통한 트랜잭션 보안 시스템.

명 세 서

기 술 분 야

[0001] 관련 출원에 대한 상호 참조

[0002] 본 출원서는 2004년 10월 21일에 출원되어 현재 계류중인 미국 특허출원 제10/970,051호[발명의 명칭:컴퓨터 네트워크를 통한 안전한 구매 트랜잭션을 제공하는 방법 및 장치]의 일부 계속 출원이며, 상기 미국 특허출원은 2000년 12월 1일 출원되어 미국특허 제6,839,692호로 등록된 미국 특허출원 제09/726,304호의 일부 계속 출원이며, 상기 양자 모두는 본 명세서에 충분히 구체화되어 있다.

[0003] 본 출원서는 또한 마찬가지로 본 명세서에 충분히 구체화되어 있으며, 2007년 2월 16일 출원되어 현재 계류중인 가출원 제60/890,230호[발명의 명칭:구매한 미디어 또는 미디어 콘텐츠에 대한 암호화된 개별 약정 식별자"에 기초하여 우선권을 주장하였다.

[0004] 본 발명의 실시예는 일반적으로 인터넷과 같은 컴퓨터 네트워크를 통하여 당사자 사이에 상품 및 서비스를 판매하는 것을 포함하여 전자상거래 및 유사한 거래 관계를 보안하고, 전자 문서, 전자 프리젠테이션, 전자 작품과 같은 배포된 전자 아이템을 추적하고, 암호화된 개별 약정 식별자를 배포된 전자 아이템내에 저장하는 방법 및 시스템에 관한 것이다.

배 경 기 술

[0005] Ⅰ. 최초에 개시된 출원 제10/970,051호 및 미국 특허 제6,839,692호[우선일:2000년, 12월 1일]의 배경기술 및 기술 요약

[0006] 본 발명은 네트워크를 통하여 이루어지는 구매 트랜잭션에 대한 보안을 제공하는 시스템에 관한 것이고, 보다 상세하게는 암호화된 정보를 단지 저장 및 제공하는 개량된 보안 시스템에 관한 것이다.

[0007] 또한, 본 발명은 네트워크를 통하여 이루어지는 구매 트랜잭션에 대하여 시간 및 가격 제한을 포함하여 고객 제어 규칙을 제공하는 시스템에 관한 것이다.

[0008] 퍼스널 컴퓨터 및 퍼스널 컴퓨터를 연결시키는 네트워크의 인기 증가로 말미암아 최근 수 십년 동안 전자 상거래가 급격하게 증가하고 있다. 매우 인기있는 네트워크 중 하나의 예는 월드 와이드 웹(WWW) 또는 인터넷이다. 그러나, 전자 상거래를 방해하는 하나의 측면은 편리하고 안전한 결제 시스템을 제공할 수 없다는 것이다.

[0009] 종래의 많은 전자상거래 결제 시스템은 성가시고 유저에게 친숙하지 않은 복잡한 패스워드/인코딩 알고리즘을 요한다. 다른 종래의 전자상거래 결제 시스템은 모든 당사자가 보안 형식에 동의할 것을 요한다. 그러한 시스템은 "클럽"에 가입하고 특정 인코딩 포맷에 동의한 사람들만 이용할 수 있다는 불편함을 겪게 된다. 상인 사이트가 현재 네트워크(예컨대, 인터넷)에 추가 및 폐쇄되는 속도를 고려해 볼 때, 상인에게 특정 포맷에 따르게 함은 비현실적이다.

[0010] 다른 전자상거래 결제 시스템은 제3자 벤더에게 선결제를 요구하고, 차례로 적립금에 대하여 코드화된 신용을 발행한다. 그러나, 온라인 거래에 또 다른 문제를 야기시키는 것에 더하여, 이러한 "지갑" 및 "인터넷 캐시" 프로그램은 또한 고객 정보를 노출시키는 또 다른 문제를 야기하게 된다. 추가적으로, 이러한 시스템은 고객 및 상인 모두가 이러한 시스템의 다양한 버젼에 참가하기 위하여 등록할 것을 요구한다.

[0011] 또 다른 전자상거래 결제 시스템은 사용자로 하여금 본질적으로 전유하고 설치 및 사용이 불편한 특정 하드웨어(예컨대, 신용카드 리더기)를 구매할 것을 요구한다. 또한, 만약 구매가 다른 컴퓨터에서 이루어지면 사용자가 하드웨어 디바이스를 이동할 것이 요구되고, 이는 이러한 타입의 결제 시스템을 방해하게 된다.

[0012] 어떠한 결제 시스템이라 할지라도, 종래의 시스템에 의해 공유되는 공통의 난제는 트랜잭션을 완료하기 위해서 개인 정보를 상인, 잠재적인 제3자, 및 상인의 금융기관에 제공해야만 한다는 것이다. 이러한 요구사항은 인지하든 인지하지 않든 고객의 노출 때문에 종래 시스템에 큰 장애물이 된다. 고객이 추가적인 하드웨어를 구매하든 또는 단지 개인 정보를 제3자 벤더에게 맡기든, 고객 정보는 결국 누군가의 데이터베이스에 저장된다. 이러한 저장된 기록의 취약성은 잠재적인 고객 및 정책 수립자에게 깊은 염려의 문제이다.

[0013] 상기 문제점은 고객이 인터넷과 같은 네트워크 환경을 통하여 비즈니스를 거래하기 위하여 개인 정보, 민감한 정보 및/또는 기밀 정보를 얼마나 많이 노출시켜야 하느냐의 문제이다.

[0014] 따라서, 본 발명의 목적은 컴퓨터 네트워크를 통한 구매 트랜잭션을 안전하게 하는 구조 및 방법을 제공하는 것에 있다. 본 발명은 고객 코드와 같은 고객 정보를 고객 컴퓨터의 저장 매체에 암호화한다(상기 고객 컴퓨터는 컴퓨터 네트워크에 연결되어 있다). 그 다음, 본 발명은 컴퓨터 네트워크를 통한 구매 트랜잭션에 있어서 상기 고객 코드를 상인에게 제공하고, 상기 고객 코드를 컴퓨터 네트워크를 통하여 금융기관에 전달하거나 또는 상인으로 하여금 전달하게 한다. 금융기관은 고객 코드를 해독하고, 정보를 확인하고, 컴퓨터 네트워크를 통하여

구매 인증 결정을 상인에게 리턴한다.

[0015] 본 발명의 중요한 특징은 신용카드 번호("고객 코드")와 같이 암호화된 고객 정보가 상인에게 이용될 수 없고, 그 결과 상인의 보안 또는 비밀 위탁에 취약하지 않다는 것이다. 고객 코드는 단지 고객의 저장 매체에 저장되고, 그것은 암화화된 형태로 되어 있다. 이는 고객이 신용카드 번호와 같이 어떠한 암호화된 정보를 상인에게 노출시키지 않으면서도 상인 트랜잭션을 완료할 수 있게 해 준다. 금융기관은 특히 고객 주소와 금융기관에 의해 유지관리되는 고객의 주소 이력 정보를 비교한다. 고객은 하나 이상의 인증된 발송 주소를 가질 수 있다. 단지 고객 주소와 이력 주소가 일치할 때만 구매 인증 결정이 승인된다. 만약 인증이 부정확한 주소 정보에 기초하여 승인되지 않으면, 금융기관에 대한 옵션은 1)정확한 주소로 트랜잭션을 승인하는 것; 2)인증 코드를 발행하기 이전에 고객이 고객 주소 정보를 업데이트한다는 조건으로 승인하는 것; 3)인증을 거절하는 것이다.

[0016] 고객 정보가 네트워크 환경에 노출되기 이전에 고객 정보를 보안화하는 것이 고객이 온라인상에서 자신의 신용 편익을 이용하는 것을 제어 및 확대시키게 해 준다. 이는 본 발명과 종래의 전자상거래 결제 시스템 사이의 주된 차이점이다.

[0017] 본 발명은 고객이 개인키 또는 액세스 코드에 의해 자신의 정보에 액세스하는 것을 허용하지만, 단지 금융기관 및 그 에이젼트만이 암호키 또는 코드를 가지고 있다. 따라서, 본 발명은 장애요소 또는 제3자를 추가하지 않음은 물론, 그러한 정보를 무수한 데이터베이스에 노출시키지 않으면서 고객 정보를 안전하게 사용할 수 있게 해 준다. 바람직한 실시예에서, 고객 코드는 암화화된 신용카드 정보를 포함한다.

[0018] 다른 실시예에서, 본 발명은 많은 고객 코드를 저장 매체에 암호화할 수 있다. 각각의 고객 코드는 유일한 결제 방법을 포함할 수 있다. 대안적으로, 하나의 그룹의 고객 코드는 결제를 위하여 단 하나의 신용 기관과 제휴할 수 있고, 여기서 상기 그룹내의 각각의 고객 코드는 상이한 사용자 이름을 포함한다. 이는 상기 그룹내의 각각의 고객 코드가 유일한 신용 한도를 포함하게 하고, 고객이 단 하나의 신용 기관에 대하여 추가적인 사용자를 인증할 수 있도록 해 준다. 본 발명은 또한 고객 코드를 해제하기 위하여 고객 컴퓨터에서 패스워드를 사용한다.

[0019] 또 다른 실시예에서, 본 발명은 고객 컴퓨터에서 동작하는 시스템을 포함한다. 본 발명에 따른 시스템은 고객 컴퓨터의 저장 매체에 고객 코드와 같은 고객 정보를 암호화하도록 설계된 암호화기 및 컴퓨터 네트워크를 통한 구매 트랜잭션에 있어서 상기 고객 코드를 상인에게 제공하도록 설계된 파퓰레이터를 포함한다. 고객 컴퓨터는 컴퓨터 네트워크를 통하여 상기 고객 코드를 금융기관에 전달하도록 설계된 네트워크 접속부를 포함한다. 금융기관은 상기 고객 코드를 해독하고 컴퓨터 네트워크를 통하여 구매 인증 결정을 상인에게 리턴한다.

[0020] 바람직하게는, 상기 고객 코드는 암호화된 고객 주소 정보를 포함하고, 상기 시스템은 금융기관에 위치한 컴퍼레이터를 더 포함한다. 상기 컴퍼레이터는 고객 주소와 금융기관에 의해 유지관리되는 고객의 주소 이력을 비교한다. 상기 구매 인증 결정은 고객 주소와 이력 주소가 일치할 경우에만 승인된다.

[0021] 상기 시스템은 선택적으로 상기 고객 컴퓨터 외부에 있는 중간 코드 확인 사이트를 포함할 수 있고, 이는 컴퓨터 네트워크에 연결된다. 상기 중간 코드 확인 사이트는 컴퓨터 네트워크를 통하여 상기 고객 코드를 금융기관에 전달하기 이전에 상기 고객 코드를 수신한다. 상기 중간 확인 사이트는 고객 코드가 적합한 암호화 포맷을 가지는지를 확인한다.

[0022] 상기 암호화기는 또한 저장 매체에 복수의 고객 코드를 암호화할 수 있다. 상술한 바와 같이, 고객 코드 각각은 유일한 결제 시스템을 포함할 수 있고, 또는 한 그룹의 고객 코드는 결제를 위한 단 하나의 신용 기관과 제휴할 수 있다. 상기 그룹내의 각각의 고객 코드는 또한 상이한 사용자 이름 및 유일한 신용 한도를 포함할 수 있다. 또한, 본 발명에 따른 시스템은 그래픽 유저 인터페이스를 포함할 수 있고, 이는 고객 코드를 해제시키기 위하여 고객 컴퓨터상에서 패스워드를 수신할 수 있다.

[0023] Ⅱ. 미국 가출원 제60/890,230호를 우선권 주장한 일부 계속 출원[우선일:2007년, 2월 16일]의 배경기술 및 기술 요약

[0024] 인터넷은 인간이 의사 소통하는 방법 및 인간이 비즈니스를 하는 방법을 변화시켜 왔다. 그러한 변화와 함께, 인터넷상에서 어떤 일을 하는 방식 또한 진화되어 왔다. 컴퓨터 및 기술이 새로운 시대를 열게 됨에 따라, 소프트웨어는 디스크에 담겨 팔렸다. 디지털 음악 및 영화와 같은 다운가능하거나 전송가능한 미디어 또한 곧 마찬가지일 것이다. 이러한 움직임은 특정 개인 및 그룹이 그러한 제품의 비인증된 복사 및 판매로부터 이익을

얻는 방법을 추구하게 하고, 이는 두개의 기본적 비즈니스가 되었다. 하나는 다른 사람의 작품을 표절/복사함으로써 이익을 추구하는 비즈니스이고, 다른 하나는 그러한 표절/복사 행위를 방지하는 비즈니스이다. 인터넷이 점진적으로 진화함에 따라서, 이러한 미디어 콘텐츠는 점점 더 다운로드되어 공유되고 있고, 이는 또 다른 복잡함과 걱정을 야기시키고 있다.

[0025] 유사하게, 최근까지 성인 산업 및 게임 산업과 관련된 사이트와 같이 콘텐츠 민감한 웹사이트가 인기를 얻고 있고 법규를 파괴해 오고 있는데, 이는 인터넷의 특성 및 하나의 관할 및 집행가능한 기준이 없기 때문이었다. 자기-규제 및 실행을 과하기 위하여 비용이 많이 들고 복잡한 시도가 많이 이루어지고 있지만, 미성년자를 보호하고 논의의 여지는 있지만 국제 관할인 곳을 통하여 상거래를 규제하는 것이 잘해봐도 어렵다는 것이 판명되었다. 복합적인 문제는 개인의 권리, 및 거주하는 관할에 따라 사적인 권리 및 법적 보호 범위가 달라질 수 있는 그룹의 권리를 위반하지 않으면서, 종래의 "비즈니스 장소"를 가지지 않는 구조를 어떻게 규제하는냐이다. 여기서, 상기 사적인 권리 및 법적 보호 범위는 인터넷을 통한 가상-사법권 및 상거래를 규제하기 위한 모든것과 상호 균형을 이루어어야 한다. 가상 환경을 통한 가상 상거래는 그러한 권리의 보호 및 실행을 위하여 권리 및 사법권에 관한 약정을 정할 필요를 가져왔다. 그러나, "계정 도용" 및 "계정 사기"로부터 고객 계정을 보호하고, 고객과 상인 양자를 위한 트랜잭션을 보호하는 동안, 전자상거래의 특성은 추가적으로 고객을 식별할 필요를 초래한다.

[0026] 현재, 벤더는 인터넷 트랜잭션에서 많은 리스크를 가지고 있다. 만약 미성년자가 부모의 신용카드, 직불카드 또는 선불 카드를 "무단 사용"하거나, 누군가가 다른 사람의 계정을 도용하거나, 누군가가 작정하고 그들 나이를 잘못 전달해 제한된 사이트에 입장하게 되면, 결제에 대한 벤더의 주장은 부인될 수 있다. 이러한 것들 모두는 그들이 제공하는 모든 것들에 대한 보상을 추구하는 전자상거래 상인에게는 실제적인 문제점이다. 이는 상인이 트랜잭션에 대한 리스크를 당연하게 생각하고, 사인된 영수증이 없을 경우("사인 없음") 발행 은행이 아니기 때문이다. 결과적으로 이로부터 수백만 달러의 사기, 트랜잭션에 대한 부인 및 지불 거절이 발생하며, 이는 비용 및 리스크를 증대시킨다.

[0027] 전술한 취지에서, 본 개시내용은 구매하거나 그 밖에 컴퓨터 네트워크를 통하여 인수한 미디어에 임베디드될 수 있고, 거래 인증, 판매 접수 및/또는 판매 기록에 임베디드된 저장가능한 버전의 고객 암호화 개별 약정 식별자를 생성, 기록, 검증 및 제조하여, "사람 존재"/"서명 존재" 식별자를 생성할 수 있는 방법, 시스템 및 구조를 제공하는 것이다.

[0028] 본 방법은 어떠한 또는 모든 사용자 암호화 약정 식별자를 사용하는 것을 포함하고, 상기 약정 식별자는 사용자의 하드 드라이브 또는 다른 유사한 목적의 컴퓨터 저장 시스템에 저장하기 이전 또는 저장하는 동안에 생성된다. 상기 방법 및 시스템은 이름, 주소, 또는 신용/직불/선불 카드 번호와 같은 암호화된 정보의 어떠한 것도 예컨대 미디어 구매 트랜잭션을 함께 수행하는 벤더에게 노출시키지 않으면서 암호화 약정 식별자가 사용되게 하는 것을 포함한다. 다르게 말하면, 본 실시예에 의하면 고객의 계정 및 정보를 벤더 및 그들의 데이터베이스에 일치되게 등록 및 노출시킬 필요가 없어진다.

[0029] 상기 방법 및 시스템은 상기 암호화된 약정 식별자가 다운로드가능한 미디어에 임베디드되는 방식으로 사용자에게 적절한 사용 및 구매 조건을 확인시키는 수단으로 이용될 수 있게 한다. 상기 방법 및 시스템은 유일한 사용자 리포팅 및 대응 패스워드 식별자와 함께 서브-계정을 생성 및 관리한다. 상기 방법 및 시스템은 주된 인증/등록 사용자에게 계정 및 모든 서브-계정에 대한 관리 책임을 부가한다. 암호화된 식별자는 상기 방법 및 시스템이 구매한 미디어의 액세스 및 사용, 기간 및 구매한 것에 대한 특권을 보장 및 제한할 수 있게 하고, 그 결과 저작권 및 다른 보호책의 동의된 집행을 가능하게 한다.

[0030] 보다 구체적으로는, 본 개시내용은 문학 작품, 음악 작품(레코딩) 및 비디오 작품(영화, 쇼, 비디 등)과 같은 전자적으로 저장가능한 아이템(이는 본 명세서에서 종종 전자 아이템으로 인용된다)의 컴퓨터 구매 트랜잭션을 용이하게 하는 시스템 및 방법을 제공하고, 여기서 고객은 저작권과 같은 권리를 고수하는 법률 시행에 동의한다.

[0031] 여기에 개시된 실시예는 "고객 정보"를 암호화 스트림(이는 때때로 고객 식별자(CID) 코드로서 인용된다)로 암호화한다. 그러한 고객 식별자 정보는 이름 식별자(이는 고객의 공식적 이름일 수도 있고 아닐 수도 있다), 가능한 고객 나이 식별자(이는 생년월일, 특정 나이, 나이 범위, 나이 분류일 수 있다), 가능한 주소 식별자(이는 고객의 주소 또는 상이한 주소일 수도 있다) 및 구매 트랜잭션을 용이하게 하는 검증 주체 또는 금융기관과 고객 간의 계약 약정을 포함 또는 식별하는 고객 약정 식별자를 포함한다.

[0032] 암호화 스트림의 구성요소가 식별 및 합치되면, 단일의 유일한 식별자가 (컴퓨터 식별자를 포함하여) 고객 정보의 그러한 특정 스트림을 위치확인 및 식별하기 위하여 검증 주체에 의해 채택될 수 있다. 고객 정보는 단지 검증 데이터베이스에 저장되고, 단지 식별자 및 POS 컴퓨터 식별자가 벤더에게 (비-암호화 BIN 또는 신용카드 발급사 라우팅 넘버와 함께) 암호화 스트림으로 전송될 수 있다.

[0033] 본 프로그램 및 관계자의 하나의 목적은 고객의 계정 보호를 가능하게 함과 동시에, 트랜잭션과 관련된 모든 당사자에 의해 신뢰받을 수 있는 "서명 존재 인증 트랜잭션"을 일으키는 것이다.

[0034] 여기서, 본 실시예는 구매한 전자 아이템을 위한 구매 트랜잭션에 있어서 암호화 스트림이 상기 고객으로부터 상인에게로 전송되게 한다. 검증 주체는 결제 프로세싱 이전에 동일성 인증 및 결제 승인을 위하여 상인에 의해 (구매 가격과 결합되어) 전송되는 상기 암호화 스트림을 수신한다. 상기 검증 주체로는 카드 발급사 또는 카드 발급사의 처리자 또는 에이젼트(예컨대, 검증 주체)를 들 수 있다. 그 다음, 검증 주체는 동일성 인증 및 결제 승인을 하기 위하여 상기 암호화 스트림을 상기 고객 정보를 포함하는 별개의 데이터베이스와 상호 비교한다. 그 다음, 검증 주체는 동일성 인증 및 결제 승인을, 고객과 트랜잭션을 하는 상인에게 전송하고, 모든 당사자의 사전-약정에 의해 "서명 존재" 인증된 트랜잭션으로 결제를 위한 트랜잭션을 처리한다.

[0035] 상기 동일성 인증 및 상기 결제 승인은 상기 구매 트랜잭션에서 상기 고객의 실제 존재를 상기 상인에게 확인시키고, 그 결과 상기 상인은 상기 실제 고객과 거래하고 있고, 상기 고객은 고객-카드발급사 사이의 약정하에 인증된 트랜잭션에 의해 구속됨에 동의한다는 확신을 가지게 된다.

[0036] 고객-카드발급사 사이의 약정은 여기에 구현된 실시예의 편리함과 계정 보호에 대한 답례로, 부분적으로 제3자 트랜잭션에서 그러한 약정의 사용 및 신뢰를 기대한다.

[0037] 본 실시예에서, 상기 암호화 스트림은 고객 및 카드 발급사(예컨대, 은행)에 의해 및 상호 간에 합의된 식별자(반드시 개인 고객 정보일 필요가 없다)를 포함하고, 동일성 인증 및 결제 승인은 고객 및 카드 발급사에 의해 및 상호 간에 기대되고 합의된 바와 같은 유일한 트랜잭션에 제한되는 정보를 포함한다. 그러한 식별자는 암호화 스트림이 해독된다 할지라도 거의 소용 없을 것이다.

[0038] 본 실시예의 또 다른 특징은 개인화된 전자 아이템을 생성하기 위하여 상인에 의해 암호화 스트림 또는 트랜잭션 검증이 다운로드가능한 디지털 미디어와 같이 구매한 전자 아이템에 부가될 수 있다. 상기 암호화 스트림 또는 유일한 트랜잭션 검증(이는 전체 또는 별개로 종종 "트랜잭션 식별자"로 인용된다)은 감추어져 일 수 있고, 그 결과 고객은 상기 개인화된 전자 아이템으로부터 상기 트랜잭션 식별자를 제거할 수 없다. 게다가, 만약 상기 암호화 스트림 또는 트랜잭션 식별자가 부분적으로 또는 전체적으로 제거되면, 상기 개인화된 전자 아이템은 작동하지 않게 될 수 있다(그 결과, 개인화된 전자 아이템은 열리지 않을 수 있거나 또는 재생되지 않을 수 있다). 따라서, 개인화된 전자 아이템은 항상 상기 트랜잭션 식별자를 유지하고, 그러한 전자 아이템을 구매한 고객이 (검증 주체를 통하여) 식별되도록 해 준다. 또한, 상기 트랜잭션 식별자는 그 구매한 전자 아이템의 모든 복사본이 트랜잭션 식별자를 가지도록 하는 방식으로 부가된다. 따라서, 개인화된 전자 아이템의 모든 복사본은 트랜잭션 식별자를 가지며, 상인으로부터 전자 아이템을 처음에 구매한 고객(복사본의 출처)은 항상 검증 주체 보안 데이터베이스를 참조함으로써 식별될 수 있다. "트랜잭션 식별자"는 검증 주체에 의해 리턴되는 것이며, 이는 유일한 식별자이기 때문에 또한 미디어 임베디드 식별자로서 사용될 수 있다.

[0039] 개인화된 전자 아이템을 생성하기 위하여 트랜잭션 식별자가 구매한 전자 아이템에 부가된 다음, 상기 개인화된 전자 아이템은 상인으로부터 고객에게 제공된다. 상이한 고객에게 배포되는 각각의 개인화된 전자 아이템은 다른 트랜잭션 식별자 각각의 유일함 때문에 상이하며, 이는 최초 전자 아이템을 구매한 고객이 그 아이템의 복사본에서 식별될 수 있게 한다. 게다가, 트랜잭션 식별자 각각의 유일함은 구매한 아이템의 비인증된 복사본의 출처가 검증 주체에 의해 유지되는 보안 데이터베이스를 통하여 식별되게 한다.

[0040] (고객이 셋업하거나 신용카드 발급사와의 계정을 변경할 때) 고객을 등록하는 동안 및 전자 아이템을 구매하는 동안, 고객에게는 그들의 정보가 모든 개인화된 전자 아이템의 복사본에 남겨진다는 알림 또는 경고가 제시된다. 게다가, 전자 아이템을 구매하는 동안, 유사한 알림 또는 경고가 고객에게 전자 아이템의 인증되지 않은 사용 또는 복사에 대하여 가해지는 조건 및 페널티를 지킬 것을 동의한다는 것을 알리기 위하여 디스플레이되고, 개인화된 전자 아이템이 열기, 재생 등이 될 때 마다(또는 처음의 몇 번), 동일한 경고가 디스플레이된다. 그러한 지속적인 경고는 음악과 같이 어떠한 다운로드가능한 미디어에 적용되거나 적용되지 않을 수 있다. 그러한 경고는 고객이 상인의 권리를 위반하여(예컨대, 불법적인 업로딩 또는 복사) 개인화된 전자 아이템의 복사본을 다른 사람에게 제공하지 못하도록 의도된 것이다. 왜냐하면, 고객은 상기 경고를 통하여 불법적 업로딩

또는 복사가 암호화 스트림을 사용하는 검증 주체에 의해 추적될 수 있고, 그러한 경고에 게재된 조건 및 조항을 지키는 것에 동의한다는 것을 인지하게 되기 때문이다. 유사하게 인증된 사용 및 수락 경고문이 또한 나이, 나이에 근거한 판매 가격 또는 거주지 등에 기초하여 액세스에 대응하여 채택될 수 있다. 본 실시예는 광범위한 고객 식별을 가능하게 하여, 전자 상거래를 권장, 촉진하고, 나아가 전자 상거래 및 그와 관련된 당사자들을 보호한다.

[0041] 저작권 경고 등은 다운로드된 후에는 오디오 미디어에 적용되지 않을 수 있다. 이러한 경고는 고객이 트랜잭션의 조건과 같은 경고문에 포함된 조항 및 조건을 지킬 것을 동의하고, 카드 발급사와의 약정 가맹 조항을 지킬 것을 동의하고, 조항 및 조건의 위반에 대하여 책임을 진다는 것을 동의하는 전제하에, 어떠한 다운로드가 이루어지기 이전에 중요하다. 당사자들은 그들의 행동 및 의도에 대하여 책임지는 것에 동의하는 것이다.

[0042] 고객 정보의 암호화는 예컨대 아래와 같이 수행될 수 있다. 첫째, 고객이 제1 컴퓨터 디바이스를 사용하여 카드 발급사에 접속하고, 카드 발급사는 소프트웨어를 제1 컴퓨터 디바이스에 다운로드한다. 벤더(이는 종종 "상인"으로 상호 변경되게 인용된다)는 또한 검증 주체와의 등록을 위하여 고객을 카드 발급사 사이트로 리디렉팅함으로써 카드 발급사를 위한 등록 에이젼트로서 역할을 할 수 있다. 예컨대, 이러한 이점은 기존의 신용카드 사용자가 그의 카드를 프로그램하에 등록하면 그러한 사용/고객은 인터넷과 같은 컴퓨터 네트워크상에서 그러한 "카드"의 사용을 선택적으로 제한할 수 있고, 이는 다른 사람에 의하여 "카드"가 비인증되게 사용되는 것을 방지할 수 있다. 고객은 유효한 발송주소, (나이 그룹 분류를 위한) 생년월일, 은행 계정 번호, 신용카드 번호 등과 같은 기존의 민감한 정보의 제공 또는 저장에 동의한다. (은행 계정 번호 및 신용카드 번호와 같이) 특정한 고객 정보 항목은 고객 컴퓨터 디바이스에 저장되지 않고, 그 대신 비록 코드화된 또는 비-코드화된 식별자가 그러한 정보를 특히 참조하기 위해 사용될 수 있지만, 단지 신용카드 발급사 및/또는 검증 주체의 데이터베이스에만 유지된다. 고객 정보의 다른 항목 또는 식별자(이름, 주소, 나이 참조 등)가 암호화 스트림을 생성하기 위하여 암호화될 수 있고, 암호화 스트림은 고객 컴퓨터 디바이스에 저장되고, 부분적 또는 전체적으로 암호화 이전에 코드화 또는 비-코드화될 수 있다.

[0043] 여기서, 용어 "크레딧이슈어(credit issuer)"는 고객에게 신용을 제공하는 주체에 대한 축약어이다. 이는 상인, 벤더, 은행, 금융기관 등일 수 있다. 게다가, 그러한 모든 크레딧이슈어는 검증 주체를 포함할 수 있고, 에이젼트로 활동할 수 있다. 따라서, 용어 "크레딧이슈어"는 전술한 모든 것을 나타내기 위해 사용된다. 본 문서에서 논의된 바와 같이, 크레딧이슈어는 여러 형태 중 하나일 수 있다. 하나의 형태는 신용 카드, 직불카드 또는 유사한 타입의 발급 카드이다. 또 다른 형태의 발급자는 기존의 신용카드 보유자와 같은 기존의 신용 수단 보유자로 하여금 처리자로서 역할을 할 수 있는 단일 주체와 사용하기를 희망하는 모든 "카드"를 등록시키게 하는 주체일 수 있다. 또 다른 형태는 Microsoft® 또는 Yahoo!® 또는 Google®과 같은 비-카드/비-은행 형태일 수 있다. 이러한 형태는 개별적으로 개인에 대한 신용 한도를 정하고, 인터넷과 같은 네트워크를 통하여 개인이 사용할 수 있는 식별가능한 신용액을 제공한다. 당업자라면 여기서 언급되지 않았지만, 본 실시예의 일 구성요소일 수 있는 다른 타입의 크레딧이슈어가 있을 수 있음을 이해할 것이다.

[0044] 신용은 네트워크를 통하여 비즈니스를 하는 참여 벤드와 함께, 종종 검증기로서 기능하는 크레딧이슈어 또는 그 처리자에 의해 처리된다(이러한 대안은 종래의 신용카드가 네크워크 형태의 컴퓨터에 필요하지 않을 수 있고, 합법적인 상거래 흐름을 추적하면서 그 트랜잭션과 관련된 당사자를 보호할 필요가 필수적이라는 것을 인지하게 된다). 벤더는 등록을 위해 크레딧이슈어에게 고객을 알아보게 함으로써 이러한 프로그램을 장려할 수 있다. 이는 고객 및 고객 계정을 보호하고, 벤더의 판매 시장성을 증진시키고, 벤더에게 결제를 확신시키고, 지불 거절 및 사기를 감소시키고, 이 모든 것은 벤더의 손익 계산을 향상시킨다.

[0045] 은행 및 소프트웨어 회사는 소프트웨어를 "방문자"의 컴퓨터에 다운로드하지 않고도, 컴퓨터의 계정을 읽기 및 확인할 수 있다. 그러나, 소프트웨어는 다른 태스크를 수행하기 위하여 다운로드 또는 그 밖에 설치될 수 있다. 고객 인증과 함께 크레딧이슈어는 제1 컴퓨터 디바이스로부터 (마드보더, 하드디스크, 프로세서 등과 같은) 유일한 하드웨어 식별자를 읽기 및 등록한다. 이러한 유일한 하드웨어 식별자는 또한 암호화 스트림에 편입된다. 그 다음, 동일한 단계가 예컨대 고객이 다수의 컴퓨터 및 컴퓨터 디바이스를 소유하고 액세스하고자 한다면, 미래의 구매 트랜잭션에 사용하기 위하여 인증 및 등록하기를 원하는 모든 추가적인 컴퓨터 디바이스에 대하여 반복된다. 그러한 프로세스는 고객이 신용카드 발급사와의 계정을 셋업 또는 변경할 때 행해질 수 있다.

[0046] 검증 주체, 금융기관, 및/또는 크레딧이슈어(예컨대, 은행)는 이러한 프로그램을 지원하는 모든 벤더에 의해 신뢰될 최초 계약/약정을 포함하여 상기 암호화 스트림의 구성요소를 고객에게 셋업한다. 상인은행/구매자 약정

서의 조항하에서 벤더가 신뢰하는 것은 크레딧이슈어와 고객 간의 약정이다. 또한, 검증 주체는 크레딧이슈어일 수 있고, 또는 크레딧이슈어에 의해 이용되고, 고객 정보를 포함하는 데이터베이스에 액세스할 수 있는 처리자 또는 에이젼트일 수 있다.

[0047] 고객 형태의 일부 예로는 1)신규 고객(이는 컴퓨터 네트워크 신용; 새로운 신용카드; 새로운 직불카드 또는 급여 직불카드와 같이 "충전된" 카드의 다른 형태를 신청하게 된다); 2)기존의 관계자(인터넷과 같은 컴퓨터 네트워크를 통한 구매를 이용할 수 있는 상기 1번에 기재된 타입과 같은 기존의 신용 수단의 보유자); 3)기존의 신용 수단을 가진 신규 고객(상기 1번에 기재된 타입과 같은 기존의 신용 수단/카드를 가진 사람으로서, 이는 그러한 "카드"의 일부 또는 모두를, "프로그램"이 등록된 "카드" 모두에 부가되게 하는 단일 주체에 선택적으로 등록할 수 있는 사람이다)를 포함한다.

[0048] 상기 "신용"은 기존의 신용카드, 직불카드 등의 형태일 수 있고, 또는 그러한 신용을 다양한 규범과 규칙을 따르는 식별가능한 개인에게 일종의 전자 레터 신용 또는 전자신용으로 확장시키는 다른 출처로부터 새롭게 발급된 "신용" 형태일 수 있다.

[0049] 고객 식별자 및 다른 정보를 크레딧이슈어(은행은 아마 기존의 고객 정보를 그 데이터베이스에 가지고 있을 것이다)에 등록하는 과정 동안에, 고객 및 크레딧이슈어는 고객의 존재를 확인하기 위하여 등록된 디바이스의 하드웨어 정보와 함께 식별자가 존재한다는 것에 대한 약정을 하게 된다.

[0050] 나이 동일함과 같은 고객 정보의 구성요소는 비록 생년월일 또는 유일한 워드가 암호화 스트림의 부분일지라도, 암호화 스트림에 저장되기 보다는 데이터베이스로부터 추정될 수 있다.

[0051] 또 다른 실시예에서, 암호화 스트림을 상인에게 전송하기 위한 근접한 시간에, 상인이 다름 아닌 고객과 거래하고 있다는 것을 더 확인시키기 위한 하나의 프로세스로서, (암호화 스트림을 전송하는 프로세스의 일 부분으로서) 암호화 스트림을 상인에게 실제 전송하기 이전에, 본 방법은 상기 암호화 스트림에, 제2 세트의 하드웨어 식별자 및 암호화 스트림을 실제 전송하는 컴퓨터 디바이스로부터의 시간 및 날짜 스탬프를 편입시킬 수 있다. 따라서, 비도덕적인 사람이 암호화된 스트림의 부적절한 복사본을 획득할 수 있고, 필수적인 신용카드 발급사로 하여금 암호화 스트림 생성 및 전송 소프트웨어를 제공함과 함께, (상인에 등록된 고객 컴퓨터 중 하나가 아닌) 컴퓨터에서 암호화 스트림의 부적절한 복사본을 사용하면, 암호화 스트림의 전송 직전에 읽기되는 제2 하드웨어 식별자가 암호화 스트림내의 제2 하드웨어 식별자와 매칭되지 않게 되고, 트랜잭션은 검증 주체에 의해 승인되지 않을 것이다. 유사하게는, 시간 및 날짜 스탬프는 상인에게 제공되는 암호화 스트림이 제한된 시간(예컨대, 분, 시, 날 등) 동안 단지 유효하도록 하기 위하여 사용될 수 있다. 게다가, 그러한 프로세스는 실제 고객 이외의 누군가가 아닌, 실제 고객과 거래하고 있다는 것을 상인에게 추가적으로 확신시키기 위하여, 검증 주체에 의해 수행되는 "고객 존재" 검증 프로세스를 강화시킨다. 고객 존재 및 조항에 대한 약정을 검증함에 더하여, 고객이 암호화 스트림/서명을 사용할 때마다, 본 실시예는 크레딧이슈어가 프로그램에 벤더 사기 또는 유출이 있는 특정 벤더를 승인하지 않도록 할 수 있다. 이는 벤더 뿐만 아니라 고객을 보호하기 위하여 제공된다.

[0052] 고객 컴퓨터 디바이스에 암호화 스트림을 생성하기 위하여 표준 크레딧이슈어 소프트웨어 프로그램을 사용하고 검증 단계를 위해 암호화 스트림을 상인에게 전송하는 것은 상기 소프트웨어가 상주하는 디바이스가 식별될 것임을 보증한다. 따라서, 그러한 식별자가 암호화 스트림내의 식별자와 매칭되지 않으면, 트랜잭션은 승인되지 않을 것이다.

[0053] 본 실시예는 또한 크레딧이슈어에 의해 고객 컴퓨터내에 위치된 인코더를 사용하는 하나 또는 그 이상의 시스템을 포함한다. 상기 인코더는 고객 식별자 정보를 암호화 스트림으로 암호화한다. 또한, 크레딧이슈어는 고객 컴퓨터 및 상인 컴퓨터에 전송 에이젼트를 위치시킨다. 상기 전송 에이젼트는 구매한 전자 아이템의 구매 트랜잭션에 있어서 상기 암호화 스트림이 상기 고객 컴퓨터로부터 상기 상인 컴퓨터로 전송되게 한다.

[0054] 검증 주체는 트랜잭션의 검증 단계 동안에 고객 컴퓨터 및/또는 상인 컴퓨터 양쪽에 작동되게 연결된 검증기를 구비한다. 본 발명의 실시예에서, 고객 정보의 보안을 향상시키기 위하여, 상기 검증기는 검증 주체내에 유지됨으로써 고객 컴퓨터 및 상인 컴퓨터로부터 분리되도록 유지된다. 고객 지불 정보에 대한 데이터베이스는 검증 주체내에 유지될 수 있고, 또는 검증 주체로부터 분리되게 유지될 수 있다. 어느 쪽의 상황이든지, 데이터베이스는 단지 검증기에 작동되게 연결되고, 고객이든 상인이든 그러한 데이터베이스에 액세스할 수 없다.

[0055] 본 방법의 각 단계를 실행하기 위하여, 전송 에이젼트는 결제 승인을 위하여 암호화 스트림을 상인 컴퓨터로부터 검증기로 전송하도록 설계된다. 상기 검증기는 더우기 상기 데이터베이스 정보에 기초하여 동일성 인증 및 결제 승인을 행하고, 그 동일성 인증 및 결제 승인을 상인에 전송하도록 설계된다. 또한, 암호화 스트림 또는

유일한 동일성 인증 및 결제 승인이 상인에 의해 구매한 전자 아이템에 추가되어, 개인화된 전자 아이템을 생성하고, 그러한 전자 아이템을 상인으로부터 고객에게 제공하도록 설계된다.

[0056] 본 실시예의 다양한 태양은 이어지는 명세서 및 도면을 참조하면 보다 명확히 이해되어질 것이다. 그러나, 본 발명의 바람직한 실시예 및 다양한 특정 실시태양이 도시되어져 있지만, 여기에 제한되지 않는다는 것에 유념해야 할 것이다. 본 실시예의 기술사상을 벗어나지 않는 범위내에서 다양한 변경 및 수정이 이루어질 수 있고, 본 발명의 실시예는 그러한 변형 실시예 전부를 포함한다.

도면의 간단한 설명

[0057] 본 발명의 실시예는 하기 도면을 참조하여 이어지는 발명의 상세한 설명으로부터 보다 명확히 이해되어질 것이다.

도 1은 본 발명의 일 실시예에 따른 개략적 구성도이다.

도 2는 본 발명의 일 실시예를 도시하는 순서도이다.

도 3은 본 발명의 일 실시예를 도시하는 순서도이다.

도 4는 본 발명의 일 실시예에 따른 시스템의 개략도이다.

도 5는 본 발명의 일 실시예에 따른 시스템의 개략도이다.

도 6은 본 발명의 실시예에 따른 암호화 스트림의 개략도이다.

도 7은 본 발명의 실시예에 따른 방법을 도시하는 순서도이다.

도 8은 본 발명의 실시예에 따른 방법을 도시하는 순서도이다.

도 9는 본 발명의 실시예에 따른 방법을 도시하는 순서도이다.

도 10은 본 발명의 실시예에 따른 시스템을 도시하는 개략도이다.

발명을 실시하기 위한 구체적인 내용

[0058] 본 발명의 실시예 및 그러한 실시예로부터 얻을 수 있는 다양한 특징 및 이점은 이어지는 도면에 도시되고, 이어지는 명세서에서 기술되어지는 비-제한적 실시예를 참조하여 보다 명확히 설명되어진다. 도면에 도시된 특징들은 필수적으로 일정한 비율로 확대 및 축소하여 그려진 것이 아님에 주의해야 한다. 널리 알려진 구성 및 처리 기술에 대한 기술은 본 발명의 실시예를 불필요하게 불명료하게 하지 않기 위하여 생략되어진다. 여기서 사용된 실시예는 본 발명의 실시예가 구현될 수 있는 방법에 대한 이해를 쉽게하고 동종 업종의 당업자가 본 발명의 실시예를 실시할 수 있도록 하기 위하여 단지 의도된 것이다. 따라서, 본 발명의 일례들은 본 발명의 실시예에 따른 권리범위를 제한하는 것으로 해석되어서는 안된다.

[0059] Ⅰ. 최초에 개시된 출원번호 제10/970,051호 및 미국 특허 제6,839,692호[우선일:2000년, 12월 1일]의 상세한 기술내용

[0060] 지금 도면들, 보다 구체적으로는 도 1을 참조하면, 본 발명의 바람직한 실시예에 대한 개략도가 도시되어 있다. 보다 구체적으로는, 도 1은 네트워크(170)에 연결된 개인 컴퓨터(100)를 나타낸다. 나아가, 코드 확인 사이트(130), 상인 사이트(140), 금융 기관(150) 및 크레딧 에이젼시(160)이 또한 상기 네트워크(170)에 연결되어 있다. 도 1에 도시된 특징적 배열은 본 발명을 설명하기 위하여 임의적으로 선택된다. 종래 기술에서 통상적 지식을 가진 자라면 아이템의 많은 다른 배열이 본 발명에 의해 활용될 수 있음을 알 수 있다.

[0061] 개인 컴퓨터(100)(이는 때때로 "고객 컴퓨터"로 불려진다)는 네트워크(170)와 연결할 수 있는 모든 형태의 컴퓨터 디바이스를 포함한다. 따라서, 고객 컴퓨터(100)는 표준 데스크탑 개인 컴퓨터, 모바일 컴퓨터, 개인 디지털 어시스턴트, 휴대폰 등을 포함할 수 있다. 바람직한 실시예에서, 고객 컴퓨터(100)는 그래픽 유저 인터페이스(GUI)(110) 및 자기적 하드 드라이브 또는 다른 읽기/쓰기 저장 디바이스와 같은 저장 매체(112)를 포함한다.

또한, 고객 컴퓨터(100)는 암호화 모듈(114), 네트워크 접속부(116), 파퓰레이터(118,populator) 및 중앙 처리 장치(CPU)(120)를 포함한다.

[0062] 금융 기관(150)은 크레딧 에이젼시(160)으로부터 얻은 주소 이력(154)에 대한 데이터베이스 및 아래 기술된 바와 같이 고객 주소를 확인하기 위하여 사용되는 컴퍼레이터(152)를 포함한다.

[0063] 도 1에 도시된 시스템의 동작은 도 2의 순서도에서 설명된다. 보다 구체적으로는, 본 발명에 따른 시스템은 고객 컴퓨터(100)에 부가된다. 바람직하게는, 고객은 그래픽 유저 인터페이스(110)를 사용하여 단계(200)으로 도시된 바와 같이 패스워드를 입력하고, 이는 본 발명에 따른 시스템에 대한 추후의 액세스를 가능하게 한다. 그 다음, 고객은 사회 보장 번호, 주소, 생년월일, 친척 이름, 신용카드 정보, 은행 정보, 고용 정보 등과 같은 개인 정보를 그래픽 유저 인터페이스(110)를 통하여 본 발명의 시스템에 제공한다. 상기 암호화 모듈(114)은 즉시 상기 정보를 암호화하고, 그 암호화된 정보를 단계(202)으로 나타낸 바와 같이 상기 저장 매체(112)에 고객 코드로 저장한다.

[0064] 본 발명의 중요한 특징은 고객 개인 정보가 단지 암호화된 형태로 저장된다는 것이다. 따라서, 권한 없는 유저가 그 사용자의 저장 매체(112)에 액세스할지라도, 고객 개인 정보는 그 암호화된 특성 때문에 안전할 것이다.

[0065] 상기 암호화 프로세스는 다음의 3개의 구성요소로 이루어진다.

[0066] 1)암호화 코드 그 자체, 이는 금융 기관에 의해 유지되는 해독 코드와 쌍으로 이루어진다.

[0067] 2)고객 개인 키, 패스워드 및/또는 고객 액세스 코드[이는 상기 암호화된 정보에 액세스하기 위하여 고객에 의해 생성 및 관리되는 코드임]

[0068] 3)고객 컴퓨터 시스템 식별자, 이는 상기 암호화된 정보가 상기 고객 컴퓨터상에서만 단지 엑세스될 수 있도록 요구한다. 일단 고객 정보가 입력되면, 상기 3개의 구성요소 및 상기 모든 정보의 재입력에 대한 필요가 모든 전자상거래 트랜잭션(예컨대, 이중 키 또는 공개 키) 동안 모든 당사자에게 명백하게 될 것이다.

[0069] 상기 암호화 코드가 권한 없는 자의 손에 넘어갈지라도, 상기 정보에 대한 액세스시에는 여전히 고객 지정 저장 시스템(예컨대, 고객 컴퓨터 시스템 식별자)으로부터 상기 정보에 엑세스해야될 뿐만 아니라 상기 고객 개인 키를 필요로 하게 된다. 권한 없는 유저가 상기 정보에 액세스하기 위하여 해독 코드를 필요로 하는데, 이러한 코드는 단지 금융 기관(크레딧이슈어) 및 그들의 인증 기관에 의해 유지 관리된다. 본 발명의 바람직한 실시예에 따른 "공개 키" 또는 "이중 키" 포맷 구성요소는 고객 정보의 보안을 향상시킨다.

[0070] 비록 권한없는 유저가 전술한 보안책을 극복한다 할지라도, 본 발명은 유저가 인증한 발송 주소를 제공할 것을 요구하는데, 이는 고객에 이메일로 확인받고, 금융 기관과의 별개의 보안 트랜잭션을 필요로 하는 과정이다. 그러한 단계는 권한없는 액세스를 실행할 수 없게 한다.

[0071] 본 발명의 또 다른 실시예에서, 유저는 다중 고객 코드를 생성할 수 있는데, 그 다중 고객 코드 각각은 상이한 크레딧 에이젼시(예컨대, 상이한 신용 카드)을 포함한다. 따라서, 본 발명은 유저로 하여금 그 유저가 소유하는 신용 카드 각각에 대한 고객 코드를 생성하게 할 수 있다.

[0072] 또한, 많은 고객 코드가 동일한 신용 카드에 대하여 생성될 수 있다. 이러한 추가적인 고객 코드는 상이한 지출 한도를 포함할 수 있다. 이는 유저가 예산 목적 또는 다른 유사한 이유로 상이한 고객 코드를 생성할 수 있도록 해 준다. 예컨대, 본 발명에 의하면, 유저는 개인 또는 비즈니스 예산의 상이한 아이템에 대한 고객 코드를 생성할 수 있다. 지출 한도에 도달하자 마자, 예산 정보가 변경되거나 업데이트될 때까지 어떠한 추가적인 트랜잭션(구매)가 이루어질 수 없다. 그러한 예산 플랜은 주기적인 예산이 자동으로 실행되도록 자동으로 업데이트될 수 있다. 이러한 일례로는 특정 기간, 예컨대 1년 동안 인터넷 서비스 제공자(ISP)에게 다달이 부가되는 비용을 지불하기 위하여 신용 카드를 사용하는 하나의 고객 코드를 포함할 수 있다. 고객 코드는 매달 ISP 요금에 대한 한달 한도 및 그 트랜잭션에 대한 열두달 한도를 포함한다. 본 발명의 실시예에 따라 고객이 얻을 수 있는 추가적인 이점은 정해진 한도를 변경함으로써 언제든지 트랜잭션을 수정 또는 취소할 수 있다는 점이다.

[0073] 유사하게, 부모는 그 자녀들 각각에 대한 고객 코드를 생성할 수 있고, 그 각각의 고객 코드는 잠재적으로 상이한 지출 한도를 포함한다. 일 실시예에서, 상기 지출 한도는 주기적인 용돈을 제공하기 위하여 주기적으로 업데이트될 수 있다. 본 발명의 이러한 태양은 부모로 하여금 자녀에 대하여 매달 인터넷-용돈을 정할 수 있도록 해 준다. 부모는 주기적 한도(예컨대 매달 또는 매주)와 함께 개별적으로 권한부여된 고객 코드를 생성할 수

있다. 이러한 효과는 부모가 권한부여된 서브-계정의 생성 및 사용을 관리할 수 있다는 점이다.

[0074] 본 발명의 이러한 태양에 따른 효과는 금융 기관이 크레딧에 대하여 고객에게 권한을 주는 것을 지속적으로 관리할 수 있다는 것이다. 그러나, 고객은 그러한 크레딧의 증대된 제어관리 및 사용을 향유할 수 있을 것이다.

[0075] 바람직하게는, 상기 고객 코드는 유저의 이름, 주소 및 신용카드 번호를 암호화된 형태로 포함한다. 고객 코드가 생성되고 저장 매체(112)에 암호화된 형태로 저장되면, 본 발명은 고객이 네트워크(170)를 통하여 구매하기를 원할 때까지 고객 컴퓨터(100)의 백그라운드에서 동작하게 된다. 구매할 때, 그래픽 유저 인터페이스(110)는 유저에게 상이한 지불 옵션(고객 코드)을 제공한다. 유저가 적절한 고객 코드를 선택한 후에, 파퓰레이터(118)는 단계(204)로 도시된 바와 같이 상인 사이트(140)로 지향된 네트워크(170)상에 고객 코드를 전송하라는 명령을 내림으로써 상기 고객 코드를 상기 상인 사이트(140)로 전송할 준비를 하게 된다.

[0076] 단계(204)에서의 기능 동작은 도 3에 보다 상시히 도시된다. 보다 구체적으로는, 본 발명은 고객 코드에 대하여 파퓰레이터(118)를 사용하여 상인 사이트(140)에 적절한 "체크아웃" 박스를 자동으로 파퓰레이팅시키는 것을 제공한다. 도 3에 도시된 바와 같이, 고객이 상인 사이트의 체크아웃(구매) 창에 이르를 때, 커서를 적절한 박스(예컨대, 신용카드 번호 필드, 고객 코드 데이터 필드 등)내에 위치시킨다(302). 많은 상인 사이트(140)는 고객 코드 데이터 필드를 위한 공간을 가지지 않을 수 있다. 따라서, 본 발명은 신용카드 번호(또는 다른 유사한 지불 필드)가 상인 사이트에 의해 사용되게 할 수 있다. 암호화된 고객 코드 데이터 필드는 신용카드 번호보다 더 길다. 따라서, 본 발명을 수용하기 위하여 상인 사이트(140)에 의해 요구되는 유일한 변경은 보다 긴 암호화 데이터 스트링이 신용카드 번호 필드에 의해 받아들여지게 하는 것이다.

[0077] 유저가 상기 적절한 박스에 커서를 위치시키고, 미리 설정된 기능 키를 키보로 누르면(또는 그래픽 유저 인터페이스상의 버튼을 선택하면), 사용자 ID 및 패스워드 입력 팝업 창(306)이 뜨게 된다. 적절한 사용자 ID 및 패스워드를 입력하자 마자, 전체 고객 코드가 상인 사이트의 필드로 이동(쓰기)된다. 유저는 그들의 이름, 주소 등을 입력할 필요가 없는데, 이는 모든 그러한 정보가 고객 코드에 포함되어 있기 때문이다. 아래에서 설명되는 바와 같이, 크레딧 트랜잭션이 승인되자 마자, 금융 기관(150)은 이름, 발송 주소 및 크레딧 승인 번호(신용카드 번호가 아님)를 상인 사이트(140)로 리턴하게 되고, 그 결과 유저는 그러한 정보를 입력할 필요가 없다.

[0078] 만약 다중 고객 코드가 상이한 신용 카드에 대하여 설정되어 있으면, 유저는 고객 코드를 선택할 수 있는데, 이러한 고객 코드는 구매를 위하여 충분한 신용 한도, 바람직한 이자율 등을 가진 신용 카드에 관한 정보를 포함한다. 고객 코드 그 자체는 암호화된 개인 정보 데이터 스트림이고, 이는 다소 길 수 있다. 따라서, 그래픽 유저 인터페이스는 간략화된 이름으로 된 유저-친화적인 선택 메뉴를 제공한다. 예컨대, 일 실시예에서, 신용카드 약어로 된 풀-다운 메뉴가 제공되어, 사용자가 사용될 고객 코드를 선택할 수 있도록 한다. 유저가 단지 하나의 고객 코드를 설정했다면, 상기 풀-다운 메뉴는 단지 단 하나의 고객 코드 약어를 포함할 것이다. 유사하게는, 상이한 예산 카테고리 또는 자녀 이름이 적절한 고객 코드를 선택하기 위하여 상기 풀-다운 메뉴에 약어 이름으로 활용될 수 있다.

[0079] 사용자 ID들은 고객 코드 약어이다. 사용자 ID/패스워드가 정확하지 않으면(310), 에러 메시지가 생성되고, 프로세싱은 사용자 ID/패스워드를 다시 입력받기 위하여 박스(304)로 리턴하게 된다. 널리 알려진 바와 같이, 사용자 ID/패스워드의 재입력은 제한된 횟수만큼 허용된다.

[0080] 만약 패스워드/사용자 ID가 정확하면(308), 고객은 상술한 바와 같이 매달 자동 ISP 지불과 같이 지불(312)에 관한 규칙을 셋업하는 옵션을 가진다. 지불에 대하여 특별한 규칙이 설정되지 않으면, 단 하나의 직접 지불 규칙으로 간주되고 프로세싱은 박스(316)으로 진행된다. 반면, 지불 규칙이 설정되면, 또 다른 윈도우 팝-업(314)이 마법사를 통하여 트랜잭션 양, 전체 크레딧 한도, 및/또는 타임 프레임 등과 같은 지불 옵션을 설치하도록 한다.

[0081] 단계(316)에서, 본 발명은 이전에 암호화된 민감한 고객 데이터를 취하고, 그것에 구매 특정 트랜잭션 번호 및 규칙(있을 경우에만)을 부가하게 된다. 본 발명은 또한 필요한 경로 설정 정보를 부가하지 이전에 그러한 추가적 데이터(트랜잭션 번호, 규칙 등)을 암호화하고, 자동으로 완전한 고객 코드를 고객 코드 데이터 필드 또는 신용카드 필드(302)로 파퓰레이트시킨다. 상술한 바와 같이, 고객 코드는 신용카드 번호, 규칙, 트랜잭션 번호, 고객 이름 및 주소 등을 포함하는 다수의 데이터 조각의 암호화된 데이터 스트링이다.

[0082] 도 2를 다시 참조하면, 일 실시예에서 본 발명은 단계(208)에 도시된 바와 같이, 고객 코드를 상인 사이트(140)로 직접 전송한다. 또 다른 실시예에서, 코드 확인 사이트(130)(단계 206)가 이용된다. 본 실시예에서, 고객 코드는 파퓰레이터(118)에 의해 상인 사이트(140) 대신에 코드 확인 사이트(130)로 향하게 된다. 크레딧 에

이젼시에 의해 제어 및 관리되는 코드 확인 사이트(130)는 크레딧 에이젼시으로 하여금 주기적으로 공개 키(예컨대, 암호화 코드 및 해독 코드)를 업데이트 또는 변경하도록 함으로써 적절한 포맷을 가지는지 여부를 판단하게 한다. 만약 고객 코드가 코드 확인 유닛(130)에 의해 부적합한 것으로 판단되면, 단계(212)에 도시된 바와 같이 고객 코드가 부적합함을 나타내는 에러 리포트가 발행된다. 만약 고객 코드가 적합하면, 단계(214)에 도시된 바와 같이, 고객 코드는 코드 확인 유닛(130)에 의해 상인 사이트(140)로 전송된다.

[0083] 고객 코드를 수신하자 마자, 상인 사이트(140)는 고객 코드를 금융 기관(150)으로 전달한다. 본 발명의 중요한 특징은 기밀 정보가 언제라도 암호화되지 않은 형태로 상인에게 제공되지 않는다는 것이다. 따라서, 상인은 그러한 정보에 대한 책임감을 경감할 수 있다.

[0084] 단계(218)에 도시된 바와 같이, 고객 코드를 해독한다. 그 다음, 신용 거래가 용인할 수 있는지 여부(예컨대, 고객이 이용가능한 충분한 신용을 가지는지 여부)를 확인하는 동안, 컴퓨레이터(152)를 사용하여 상품이 보내지는 발송 주소와 크레딧 에이젼시(160)에 의해 제공되는 발송 주소(154)의 데이터 베이스 이력을 비교한다. 본 발명의 이러한 태양은 아이템이 범죄자에 의해 고객 주소 이외의 다른 주소로 부적절하게 빼돌려지는 것을 방지한다.

[0085] 본 발명의 일 실시예에서, 고객은 크레딧 에이젼시와 직접 다수의 인증된 발송 주소를 설정할 수 있다. 이러한 주소는 회사 또는 가정과 같은 대안적인 주소를 포함할 수 있다. 각각의 주소는 개별 고객 코드와 같은 개별 암호화 시퀀스와 함께 고객 저장 매체에 입력 및 저장된다. 고객이 신규 고객 코드를 셋업할 때, 고객에 대한 신규 인증 주소가 네트워크(170)를 통하여 고객 컴퓨터(100)로부터 크레딧 에이젼시(160)으로 직접 (이메일 또는 유사한 전자적 전송에 의해) 전송되며, 크레딧 에이젼시(160)의 데이터베이스에 고객과 연관된 인증 주소 리스트로 추가된다.

[0086] 단계(220)에 도시된 바와 같이, 만약 발송 주소가 데이터베이스(154)의 주소와 일치하고, 고객이 충분한 신용을 가지면, 인증 코드, 이름, 주소 및 다른 필요한 정보가 단계(224)에 도시된 바와 같이 상인 사이트(140)로 전송된다. 이 경우에 용어 "일치"는 두개의 주소가 실질적으로 매칭되어야만 하는 것을 의미한다. 따라서, 거리 번호 또는 우편 번호의 일부분이 부정확하거나 또는 거리 이름의 스펠링이 약간 틀릴지라도, 트랜잭션은 승인되고 정확한 주소가 상인에게 제공된다. 그러나, 발송 주소가 그 고객에 대한 인증된 주소와 일치하지 않는 주소이면(예컨대, 상이한 주, 상이한 시, 상이한 거리명 등), 에러 리포트가 상인 사이트(140)로 발행되고, 부적합합 트랜잭션임을 나타내는 이메일이 고객에게 발송된다.

[0087] 크레딧 에이젼시는 일반적으로 인증을 결정하는 것을 돕기 위하여 주소를 사용한다. 그러나, "일치된" 주소를 구성하는 기준은 달라진다. 본 발명은 주소를 "바로 잡음"으로써 이러한 인증에서 에러 및 사기를 제거하는 시스템을 안출한 것이다. 그 다음, 상품이 단지 인증되거나 정확히 정정된 주소로 발송되는 것을 보증하는 것은 상인의 책임이다. 본 발명의 이러한 태양은 고객이 "가로채기"를 하여 모든 인증되지 않은 발송을 리턴시킬 수 있어 보안 레이어를 추가하게 된다.

[0088] 본 발명의 일 실시예에서, 고객은 "비-영구적" 발송 주소를 일시적으로 추가하기 위하여 "룰 마법사"[314]를 사용하고, 이는 고객이 선물 등을 다른 사람에게 발송할 수 있도록 해 준다. 고객의 컴퓨터 시스템 식별자 및 패스워드가 이러한 되풀이되지 않는 변화를 위한 "마법사"에 액세스하기 위하여 필요하다. 부가적으로, 비-인증된 주소로의 이러한 발송에 대한 확인 메일이 고객에게 이메일 발송되고, 그 결과 고객은 사기적 트랜잭션이 시도되고 있는지 여부를 경계하게 될 것이다.

[0089] 상술한 바와 같이, 상인 사이트(140)는 고객 코드를 수신하기 위하여 적절히 포맷 형성된 입력 필드(이는 현재 신용 카드 필드일 수 있다)를 포함하는 것이 바람직하다. 상기 입력 필드 포맷은 크레딧 에이젼시(160)에 의해 설정되고, 유사하게는 금융 기관(150)에 의해 요구되어진다. 상대적으로 적은 수의 크레딧 에이젼시(160)(Visa®, MasterCard®, American Express® 등)이 있다. 크레딧 에이젼시(160)은 일반적으로 크레딧 에이젼시(160)과 거래하는 모두 많은 다수의 금융 기관(150)에 의해 제공되는 정보 포맷을 그대로 받아 사용할 수 있다. 이번에는, 금융 기관(150)과 거래하기를 원하는 상인 사이트(140)는 금융 기관(150)(및 교대로 크레딧 에이젼시(160))의 데이터 포맷 요구사항을 따라야만 한다. 따라서, 본 발명은 인터넷과 같이 많은 수의 상인 사이트(140)를 지속적으로 추가 및 폐쇠시키는 네트워크에 적용가능하다. 보다 구체적으로는, 상인 사이트들(140)이 네트워크에 추가되기 때문에, 각각의 상인 사이트(140)는 금융 기관(150)의 요구사항을 따를 것이고, 그들의 상인 사이트(140)에 특별화된 고객 코드 데이터 필드 포맷을 포함할 것이다. 따라서, 유저는 고객 구매를 가능하게 하는 방대한 다수의 웹 사이트상에서 고객 코드 데이터 필드를 찾아야만 한다.

[0090] 다른 말로 하면, 본 발명은 상인(140)에 의해 활용될 수 있는 포맷(이는 잠재적으로 신용카드사 마다 다를 수 있다)을 설정하기 위하여 비교적 적은 숫자의 국가 크레딧 에이젼시(160)과 동작하게 된다. 제한된 숫자의 크레딧 에이젼시(160)이 대부분의 온라인 신용 구매 트랜잭션을 제어하기 때문에, 고객 코드 입력 필드의 포맷이 대다수 상인 사이트(140)에 제공될 것이다. 따라서, 본 발명은 유저에게 금융 기관과 거래하기를 원하는 모든 상인 사이트(140)[이는 구매 트랜잭션을 완료하기를 원하는 모든 상인 사이트이다]로의 가상적인 액세스를 제공한다.

[0091] 크레딧 에이젼시(160)은 고객이 신용(예컨대, 그들의 신용 카드)을 사용하도록 하는 비즈니스를 행한다. 본 발명은 추가적인 제어 및 유용한 특징과 함께 고객에 대한 보안을 창출하기 때문에, 크레딧 에이젼시는 그들의 신용 편익에 대한 판촉적 이점을 이끌어낼 수 있다. 게다가, 이러한 이로운 특징은 특별한 단계를 요하지 않는다. 본 발명의 이점은 고객 정보를 반복적으로 재입력하거나 또는 제3자의 데이터베이스에 그러한 정보를 포스팅하는 것을 포함하는 단계를 제거한 것에 있다.

[0092] 본 발명의 중요한 안전성 특징은 상인 사이트(140)가 신용 카드 번호와 같은 고객의 기밀 정보에 결코 액세스를 얻을 수 없다는 것이다. 반대로, 상인 사이트(140)는 단지 고객(100)으로부터 암호화된 고객 코드를, 금융 기관(150)으로부터 트랜잭션 승인 코드(및 가능하게는 정정된 주소)를 단지 수신한다. 따라서, 네트워크(170)을 통한 전술한 모든 트랜잭션이 가로채어 지거나 또는 상인 사이트가 레코드에 대한 인증되지 않은 액세스를 겪게 될지라도, 고객의 신용 카드 정보는 안전할 것이다.

[0093] 게다가, 본 발명은 종래의 보안 네트워크 트랜잭션과 관련된 많은 문제점을 회피한다. 보다 구체적으로는, 본 발명의 모든 구성요소는 트랜잭션이 완료되기 위하여 적절한 기능을 하고 있어야만 한다. 종래의 시스템은 모든 트랜잭션에 대하여 하나의 레벨의 보안을 제공하고, 그 결과 데이터베이스가 뚫리게 되면 그러한 "보안" 사이트의 모든 기록이 액세스 가능하다. 본 발명은 추가적인 레벨의 보안을 생성하여 개인 기록을 보호한다.

[0094] 상술한 바와 같이, 본 발명으로부터 얻을 수 있는 이점은 개개의 고객 온라인 신용 및 그러한 신용의 고객 제어 및 유연한 사용에 보안을 포함시키는 것이다.

[0095] Ⅱ. 미국 가출원 제60/890,230호를 우선권 주장한 일부 계속 출원[우선일:2007년, 2월 16일]의 상세한 기술내용

[0096] 본 발명은 개인적 트랜잭션에서의 개인적 계약-인터넷 상거래와 관련된 개개의 당사자를 위한 규정된 권리 및 보호를 정의하는 계약을 생성하는 시스템 및 방법을 제공함으로써, 인터넷이라는 가상의 전세계적인 특성에 의해 커버되는 많은 실제 사법권에 대한 규제의 문제를 해결한다. 서로에 대한 신뢰의 유효한 기대(예컨대, 각 당사자가 "성년"이거나 그렇지 않다면 그러한 트랜잭션과 관련되거나 책임을 질 수 있도록 인증된 사람이라는 기대)를 가지는 각각의 당사자간에 동의되는 집행가능한 조항을 생성하고, 그러한 약정하에서 식별된 모든 구매 조항을 지킬 것이라는 약정을 포함하여 그러한 약정 및 각각의 트랜잭션 행위를 충실히 지키는 방법을 생성함으로써, 본 발명은 그들의 경제 활동의 가상 환경에 기초한다기 보다는 각 당사자의 자산 사법권에 기초하여 사법적이고 시행가능한 권리를 만든다.

[0097] 본 실시예는 고객과 크레딧이슈어 사이에 생성된 계약("고객 약정")에 중점을 둔다. 고객 약정은 검증기로 역할하거나 또는 인증된 처리자 또는 에이젼트를 통하여 역할하는 크레딧이슈어가 고객과 다양한 참여 벤더 사이의 트랜잭션을 인증 및 검증하도록 허용한다. 다양한 고객-벤더 약정은 고객-크레딧이슈어 약정에 기초하여 기대 및 허용되고, 다양하고 직접 또는 간접적인 크레딧이슈어-벤더 약정은 또한 고객-크레딧이슈어 약정에 기초하여 기대 및 허용된다. 또한, 검증 주체 사이에 약정 또는 계약이 있을 수 있는데. 이러한 검증 주체는 독립 주체 또는 신용카드, 직불카드 및/또는 선불카드를 발급하는 금융기관 또는 다른 가능한 금융 제공자 및 개인 고객과 결합될 수 있다.

[0098] 고객 약정은 본 실시예에서 모든 활동의 중심이다. 그러한 고객 약정은 고객이 지켜야할 규칙 및 조항을 정한다. 즉, 컴퓨터 네트워크를 통하여 개인의 계정을 보안화하는 대가는 온라인상에서 개인에게 동일성을 정하는 구성요소(즉, 개인과 그 컴퓨터를 사용하거나 또는 액세스할 수 있는 다른 사람을 차별화시키는 다른 식별자와 함께 등록된 컴퓨터)에 동의할 때마다 그들 트랜잭션을 법적으로 지킬 것이라는 고객의 약정인 것이다. 이러한 약정은 구매(즉, 책임 및 지불에 대한 약정) 및 모든 저작권 또는 거기에 부착된 상표권을 존중하는 것과 같은 조항에 대한 약정 및 그러한 등록된 권리를 포함하여 형사 및 민사 처벌에 대하여 법적 및 개인적으로 책임을 질 것이라는 약정을 포함한다. 가장 중요하게는, 크레딧이슈어-고객 약정/계약은 크레딧이슈어가 고객 약정을 참조할 수 있도록 해 주고, 그러한 조항이 모든 검증된 고객-벤더 약정/트랜잭션에 대하여 충실하게 지켜지도록 한다. 모든 크레딧이슈어-벤더 약정에 직접 또는 간접으로 적용된 고객 약정은 벤더로 하여금 고객-벤더 약정

을 검증함에 있어서 크레딧이슈어-고객 약정에 의지하게 한다. 다른 말로 하면, 벤더 지불은 이러한 지불 디바이스를 채택하여 보장되고, 이는 개인으로 하여금 그들의 안전한 계정을 개시, 등록 또는 인도할 것을 요하지 않는다.

[0099] 고객 약정은 본 실시예하에서 제어/관리되는 관련된 트랜잭션 행위에 대하여 핵심으로서 기능한다. 이러한 관련 행위는 컴퓨터 네트워크를 통한 고객과 상인간의 검증가능한 모든 트랜잭션(이러한 트랜잭션은 상품 또는 서비스와 같은 것을 위한 트랜잭션일 수 있다); 및 상인과 금융 주체간의 직접 또는 간접적인 계약("벤더 약정")에 의해 궁극적으로 이루어지는 트랜잭션(그러한 계약하에서 고객-벤더 트랜잭션에 대한 벤더의 고려는 보장 또는 "확고"해 질 것이다)을 포함한다. 고객 약정서 조항 하에서, 상인의 고려는 지불, 신용 가치와 같은 것, 상인의 제품 사용 또는 판매 조항에 대한 약정 또는 그 계약이 포함하는 고객과 상인간의 모든 다른 약정 조항, 및 검증 주체가 처음의 트랜잭션 동안 상인에게 추인해 주는 형태일 수 있다.

[0100] 본 실시예하에서 이루어진 계약은 특히 이용 약관, 제3자 신뢰 및 재판관할권을 포함한다. 따라서, 본 실시예를 사용하여 당사자는 분쟁을 조정하기 위한 적절한 관할권이 상인의 사업장 위치, 상인과 거래하는 고객의 위치 또는 선택되는 모든 다른 위치라는 것에 동의할 수 있다. 이용 약관은 상인이 단지 확인/검증된 고객과 거래하고 있고, 상인이 지불 거부를 겪을 필요 없이 비용 결제 받을 수 있다는 것을 보증하기 위한 ("서명 존재"와 유사한) "사람 존재" 개런티를 포함한다. 이러한 사람 존재 개런티는 트랜잭션이 이루어질 때 모든 등록 고객 검증 요소가 존재하고 이것이 검증 주체에 의해 확인될 때, 완성된다.

[0101] 검증 주체는 고객-크레딧이슈어 약정서 및 벤더-크레딧이슈어 약정서의 조항하에서 트랜잭션의 양쪽 측면을 검증한다. 이는 예컨대 구매/"서명 존재"의 확인, 저작권 보호 약정 또는 나이 검증과 같은 모든 조항이 시행 가능하고 신뢰되게 한다. 본질적으로, 크레딧이슈어가 가진 모든 고객 정보는 실제적으로 고객 정보 또는 고객 계정을 노출시킴 없이 제3자에 의해 신뢰될 수 있다. 이러한 점에서, 크레딧이슈어는 고객 및 상인 양측을 대표하여 신용 보유자 기능을 하고, 검증 주체는 각각의 개인 트랜잭션에 대하여 검증/확인하게 된다. 이는 트랜잭션에 대하여 확고하거나 조건부 승인된 형태의 구성요소일 수 있고, 이는 고객 계정 및 상인 권리를 보호하고, 벤더가 별개로 신뢰하는 구성요소일 수 있다.

[0102] 인터넷과 같은 네트워크를 통한 일반적인 구매 조항은 본질적으로 은행 발급 신용 카드 또는 직불카드의 사용과 관련된다. 상기 트랜잭션이 신용카드 또는 선불카드 형태에 기초하든 아니든, 발급 은행은 그 지불이 실제로 상인에게 지급될 때까지 승인카드에 기초한 신용을 제공하는 기능을 한다. 일반적인 관행으로서, 이러한 지불 절차는 두개의 햇(hat)을 가진 은행, 즉 "발행 은행" 및 "수취 은행"의 햇을 가진다. 발행 은행은 상품, 서비스 등을 구매함에 있어서 고객이 사용할 신용 및 카드를 발급한다. 수취 은행은 그러한 신용 카드의 사용에 의해 생성된 데빗을 수취(및 지불)하는데 동의한다. 인터넷을 통한 종래의 신용 카드 거래 조항하에서, "발행 은행"으로 기능하는 은행은 지불 및 미지불 잔액에 대한 이자를 요하는 조항에 따라 카드 사용을 위한 약정을 이용한다. 별개 타입의 약정하에서, "수취 은행"으로 기능하는 은행은 그들 중 상인이 신용카드 사용자의 동일성을 확인하고 카드소유자가 구매한 모든 물품에 대한 영수증에 사인을 할 것을 요한다. 이러한 신용카드 거래의 과도하게 간단화됨은 인터넷 또는 컴퓨터 연결된 상거래의 모든 유사 시스템을 통한 트랜잭션을 위하여 비인증된 신용카드 사용 및 동일성 인증의 문제점을 지적하기에 충분하다.

[0103] 벤더-크레딧이슈어 약정은 자격있는 벤더를 보호하는 추가적인 역할을 한다. 전자상거래 사기 중 하나의 요소는 벤더 사기이다. 알려지거나 의심받는 사기 이력을 가진 벤더는 그들의 약정서가 취소되게 할 수 있고, 그 밖에 저작권과 같은 다른 보호책 및 여기서 제공되는 서명-존재 지불 조항에 대한 액세스를 부인되게 할 수 있다. 이러한 벤더 자격확인 단계는 고객을 보호할 뿐만 아니라 사기를 막기 위하여 필요하다.

[0104] 그러한 문제점 측면에서, 여기에 개시된 시스템 및 프로세스는 암호화 코드("암호화 스트림")을 사용하고, 이는 제3자 검증 주체가 상인에게 고객의 존재를 확인시키고, 고객의 크레딧이슈어와의 약정을 확인시킨다. 이러한 약정 조항은 검증 주체로 하여금 고객 동일성 및 "서명 존재" 지불을 포함하여 벤더와의 트랜잭션 조항을 지킬 것이라는 약정을 확인하게 한다. 대안적으로, 암호화 스트림에서 고객 약정의 식별자를 단지 참조하기 보다는, 트랜잭션의 전체 수취 및 조항이 암호화되어 암호화 스트림내에 포함될 수 있다.

[0105] 고객-벤더 약정은 크레딧이슈어-고객 약정서의 조항 및 그것에 의존한 크레딧이슈어-벤더 약정서의 조항하에서 검증되고, 이는 처음의 두개 약정서의 동의된 구속력에 의해 고객-벤더 약정서의 조항을 보증하게 된다. 고객-벤더 약정서는 다른 두개의 약정서의 기대되는 결과이며, 이는 그러한 시점에서 크레딧이슈어 또는 처리자와 같은 에이젼트가 고객의 존재 및 (고객의 요청에 따른) 트랜잭션 조항에의 동의를 확인하면, 모든 당사자는 별개의 약정서의 해당 부분에 의해 구속됨을 기대할 수 있다. 이는 검증가능한 암호화 스트림의 존재에 의해 얻을

수 있는 것이다.

[0106] 따라서, 일부 실시예에서, (검증 주체/크레딧이슈어와 고객 간의) 별개 고객 약정서 및 (상인과 그 상인 은행 간의) 별개 상인 약정서는 고객 및 상인이 (고객 및 상인 간의) 고객 약정서에 참여할 것을 요하고, 이는 상인과 고객 간에 구매 트랜잭션이 일으날 때 생성된다.

[0107] 본 실시예는 고객에 대한 추가적인 보호책으로서 크레딧이슈어에게 벤더를 차단하는 능력을 제공한다. 본 실시예에서, 신규 고객 약정이 상인과 고객 간의 각 구매 트랜잭션에 대하여 생성될 수 있고, 이는 특히 특정 트랜잭션에 적용될 수 있다면 고객의 존재, 동일성, 나이 등에 관하여 구속력 있는 표현을 하게 하고, 상인 또는 미디어의 지식 재산권을 준수할 것을 고객에게 강제한다.

[0108] 검증 주체는 상인을 대신하여, 고객의 동일성 및 트랜잭션을 보호하고 (나이, 계정, 거주지역, 저작권 조항 등에 구속되거나 존중하는 약정과 같은) 트랜잭션의 다른 조항 및 지불을 보호하기 위하여 고객과 크레딧이슈어 간의 약정 조항 및 다른 당사자와의 약정에 구속된다.

[0109] (구매 트랜재션이 일어날 때) 암호화 스트림이 생성되기 이전에, 어떤 구성요소가 개인 고객의 동일성을 확인하고, 그러한 고객이 고객 약정 조항을 지킬 것에 동의하였는지를 확인하기 위하여 존재해야만 한다. 이러한 일련의 구성요소는 다른 것들 중에서, 이름(필수적으로 카드 소유자의 이름일 필요는 없다), 발송 또는 거주상태를 확인하기 위한 주소(필수적으로 카드 소유자의 청구서 주소일 필요는 없다), 금융 주체와 함께 고객의 유일한 크레딧 넘버 또는 ID, 및 컴퓨터의 등록된 하드웨어 동일성 또는 고객이 그러한 트랜잭션에 대하여 인증하고자 하는 컴퓨터를 포함할 수 있다. 암호화 스트림은 이름, 주소, 고객 약정 식별자, 컴퓨터 하드웨어 식별자 등과 같은 그러한 구성요소 일부로부터 생성되지만, 고객 신용카드 번호 또는 은행 계정 번호와 같은 민감한 정보를 포함하지는 않는다. 또한, BIN(은행 ID 번호) 또는 암호화되지 않는 IP 어드레스와 같은 다른 라우팅 식별자가 라우팅 목적으로 암호화 스트림에 부가된다.

[0110] 등록 동안에 생성되는 신용발급자와 고객간의 계약 조항하에서, 암호화 스트림에 요구되는 모든 구성요소가 검증 주체가 상인과의 트랜잭션 동안에 고객의 존재를 확인하도록 하기 위하여 존재한다. 상인은 그러한 정보가 암호화되어 있기 때문에, 고객의 동일성을 인지하지 못할 수도 있다. 검증 주체가 모든 코드화된 구성요소의 존재를 확인하면, 트랜잭션이 확인되고, 상인은 그러한 정보가 요구되고, 고객의 서명을 수신하고 고객의 동일성을 확인하는 상인의 요구가 충족되어지면(즉, 상인이 결제 받게 되거나 또는 나이 검증과 같은 그러한 트랜잭션 조항 및/또는 저작권에 대한 리소스를 가지게 되면) 상인은 발송할 주소를 지시받게 된다.

[0111] 본 발명은 크레딧이슈어와의 약정을 함에 있어서 고객에 의해 생성된 조항을 이용한다. 본 약정은 고객의 암호화 스트림에서 요구되는 모든 구성요소가 존재할 경우에 모든 트랜잭션에 대하 고객이 책임을 지는 것으로 간주한다. 상기 약정은 또한 저작권 보호와 같이 이용 약관에 대하여 동의하는 기록으로서 고객에 의해 구매되는 모든 디지털 미디어와 함께 상기 암호화 스트림이 다운로드되게 한다.

[0112] 본 발명은 일 측면은 모든 구성요소가 존재하는 상태에서 사용될 때, 개인 고객에 유일한 서명으로 기능하고 트랜잭션에서 고객의 존재를 확인시키는 계약적으로 동의된 "코드"를 생성, 검증 및 (필요할 때)임베드하는 시스템 및 방법을 개시한다. 상인은 고객 약정서에서 트랜잭션을 위하여(동일성 및 사법권을 또한 확인하는) 고객에 의해 동의된 조항에 의존할 권리를 가진다. 본 발명은 모든 당사자를 그러한 트랜잭션의 조항에 계약적으로 구속시키는 대신에, 계정 보호를 제공한다. 따라서, 본 발명은 인터넷 구매 트랜잭션을 개시하는 고객의 프라이버시 및 계정을 보호할 수 있는 능력을 제공함과 동시에, 또한 상품, 서비스 등을 제공하는 상인의 권리 및 경제적 이점을 보호한다. 본 실시예는 고객의 계정을 보호하고, 이는 약정의 조항이 위반 또는 침해되지 않으면, 암호화 상태 및/또는 보호 상태로 유지된다.

[0113] "코드"의 제거는 상기 미디어를 미국 특허 공개 제2007/0061580호[이는 워터마크 또는 코드의 부존재가 구매 상품이 전자 저장 미디어로부터 액세스되는 것을 방지하는 것과 관련되어 있다)에 기술된 바와 같이 사용할 수 없게 할 것이다. 구매 조항 및 저작권 보호를 위반하여 복제된 다수의 미디어 복사본에서의 "코드"의 존재는 상인에게 크레딧이슈어의 약정 조항 및 사법권 하에서 다수의 복사본에 대하여 고객에 책임을 지울 수 있는 능력을 제공한다. 따라서, 고객 약정은 구매 동안에 특별히 동의한 저작권 보호에 대한 위반행위에 대한 기소 수단이다.

[0114] 정리하면, 본 발명은 다양한 권리의 보호 및 실행을 위한 합의된 사법권을 정하여, 부분적으로 고객의 계정 및 금융 정보를 포함하는 고객의 권리, 및 상인의 지불 및 상인의 관리를 포함하는 상인의 권리, 및 상품 및/또는 서비스의 소유권을 보호함으로써, 인터넷과 같은 컴퓨터 네트워크를 통한 상거래를 촉진, 보호 및 검증하는 방

법, 시스템, 구조를 개시한다. 따라서, 본 실시예는 고객 및 상인의 동의에 의해 크레딧이슈어 및 검증 주체에게 계약 능력을 제공함으로서 트랜잭션에 대한 당사자간의 구속력있는 계약을 생성한다. 본 실시예는 고객의 계정을 보호하고 그것이 보상되는 것임을 상인에게 보증하는 한편, 그 트랜잭션의 구성요소로 가치있는 계정 및 크레딧이 충족됨을 확인한다. 따라서, 본 발명은 트랜잭션이 완료되도록 하기 위하여 모든 암호화 스트림 요소가 존재하고 검증될 것을 요구함으로써, 트랜잭션에 대하여 "인증 존재" 요소를 정하고, 그 트랜잭션에 "서명 존재" 요소를 정하고, 고객 나이(예컨대 "18 이상" 또는 "21 이상" 또는 "65 이상")를 정하고, 거주지 또는 발송 주소를 정하고, 고객 약정과 연계된 고객/판매자를 정하고 고객의 계정(이는 필수적으로 온라인상으로 노출시키거나 저장하지 않는다)을 정하기 위하여 사용될 수 있다.

[0115] 도면을 참조하면, 본 발명의 실시예는 컴퓨터 네트워크(404)를 통한 거래를 보장하기 위한 방법 및 시스템을 제공한다. 도 4에 도시된 바와 같이, 고객(402), 상인(450) 및 검증 주체(420) 및/또는 금융기관(440) 사이에 생성된 약정서가 검증 주체(420)에 의해 저장된다. 검증 주체(420)는 도 5에 도시된 바와 같이 금융 기관(크레딧이슈어)(440)내에 포함될 수 있고, 또는 도 4에 도시된 바와 같이 그로부터 분리되어 있을 수 있다. 도 4가 단일의 고객 컴퓨터(410), 단일의 검증 주체(420), 단일의 금융 기관(440) 및 단일의 상인(450)만을 도시하고 있지만, 동 기술분야에서 통상의 지식을 가진 자라면, 도 4가 본 발명이 어떻게 구현될 수 있는지를 단지 일례로 나타내고 있을 뿐이고, 도 5에 도시된 바와 같이 다수의 고객 컴퓨터(410), 다수의 검증 주체(420), 다수의 금융기관(440), 다수의 상인 등으로 구현될 수 있음을 인지할 수 있을 것이다. 따라서, 검증 주체(420)는 각각의 구매 트랜잭션 당 하나씩 다수의 약정서(422)를 저장하고 있다.

[0116] 본 방법은 신용카드 발급사/검증 주체(440/420)와 함께 고객 약정서(들)(422)를 등록 및 저장하는 단계를 포함한다. 고객 정보는 데이터베이스(430)에 저장되고, 그러한 데이터베이스는 도 5에 도시된 바와 같이 카드 발급사/검증 주체(440/420)내에 있을 수 있고, 또는 도 4에 도시된 바와 같이 카드 발급사/검증 주체(440/420)로부터 분리되어 있을 수 있다. 당업자가 이해하는 바와 같이, 단지 하나의 데이터베이스(430)가 도 4에 도시되어 있지만, 다수의 데이터베이스(430)가 있을 수 있고, 그 중 일부 데이터베이스는 카드 발급사/검증 주체내에 포함될 수 있다. 게다가, 고객 컴퓨터(410)는 하나 또는 그 이상의 컴퓨터 네트워크를 통하여 상인(450) 및 검증 주체(420)에 접속된다.

[0117] 고객 컴퓨터(410)의 인코더(412)에 액세스하기 위하여 패스워드가 사용된다. 인코더(412)는 고객 등록 과정 동안에 상기 검증 주체(420)에 의해 고객 컴퓨터(410)에 다운된다. 인코더(412)는 고객 정보를 암호화하여 암호화 스트림(414)을 형성하고, 그러한 암호화 스트림은 고객 컴퓨터(410)에 저장된다. 고객 정보는 고객 컴퓨터에 암호화되지 않은 형태로 저장되지 않는다. 게다가, 암호화 스트림은 신용카드 번호, 은행 계정 번호 등과 관련된 어떠한 개인적인 고객 금융 정보를 포함하지 않으며, 그러한 정보는 단지 데이터베이스(430)에 저장된다.

[0118] 또한, 검증 주체는 고객 컴퓨터(410) 및 상인(450)에게 전송 에이전트(416, 456)를 다운로드한다. 전송 에이젼트(416)는 구매한 전자 아이템(454)을 위한 구매 트랜잭션에 있어서 암호화 스트림(414)이 고객 컴퓨터로부터 상인 컴퓨터(450)로 전송되게 한다.

[0119] 검증 주체(420)는 고객 컴퓨터(410) 및 상인 컴퓨터(450) 양쪽에 작동되게 연결된 검증기(424)를 구비한다. 본 발명의 실시예에서, 고객 정보의 보안을 향상시키기 위하여, 상기 검증기(424)는 신용카드 발급사/검증 주체(440/420)내에 유지됨으로써 고객 컴퓨터(410) 및 상인 컴퓨터로부터 분리되도록 유지된다. 고객 지불 정보에 대한 데이터베이스(430)는 신용카드 발급사/검증 주체(440/420)내에 유지될 수 있고, 또는 검증 주체(420)으로부터 분리되게 유지될 수 있다. 어느 쪽의 상황이든지, 데이터베이스(430)는 단지 검증기(424)에 작동되게 연결되고, 고객이든 상인이든 그러한 데이터베이스에 액세스할 수 없다.

[0120] 본 발명의 각 단계를 실행하기 위하여, 전송 에이젼트(416)는 결제 승인을 위하여 암호화 스트림(414)을 상인 컴퓨터(45)로부터 검증기(424)로 (트랜잭션의 금액과 함께) 전송하도록 설계된다. 상기 검증기(424)는 더우기 상기 데이터베이스(430)에 기초하여 결제 승인을 발생시키고, 그 결제 승인을 상인(450)에 전송하도록 설계된다. 또한, 상인에 의해, 암호화 스트림(414) 및/또는 트랜잭션 식별자가 구매된 전자 아이템에 부가되어, 개인화된 전자 아이템(454)(도 6에 도시됨)을 생성하고, 그러한 전자 아이템을 상인(450)으로부터 고객 컴퓨터(410)로 제공하도록 설계된다.

[0121] 암호화 스트림(414)은 고객 이름, 고객 발송 주소, 고객 생년월일 및 고객 하드웨어 컴퓨터 식별자와 같은 정보를 포함할 수 있다. 고객 발송 주소는 상인(450)에게 제공되는 암호화 스트림(414)에 따라 결정되는 복수의 유효한 발송 주소 중 하나를 포함할 수 있다. 따라서, 본 방법은 고객이 각각의 상이한 유효 발송 주소를 가지는

복수의 저장된 암호화 스트림(414)으로부터 선택할 수 있도록 해 준다. 본 방법은 컴퓨터 네트워크(404)를 통한 트랜잭션에 있어서 식별자 코드(CID 및 라우팅 식별자(416)의 일부로서 컴퓨터 식별자와 함께 상기 선택된 암호화 스트림을 상인(450)에게 제공한다.

[0122] 상기 암호화 스트림(414)는 라우팅 식별자(416)에 의해 컴퓨터 네트워크(404)를 통하여 검증 주체(420)으로 전달된다. 검증 주체(420)는 암호화 스트림(414)을 해독하고, 고객 발송 주소 식별자, 이름 식별자, 나이 식별자, 또는 다른 식별자를 검증 주체에 의해 유지관리되는 고객의 인증된 대응 식별자와 비교한다. 여기서, 이름, 나이, 주소 등의 "식별자"는 실제 이름, 주소 등일 수 있거나 또는 데이터베이스(430)에서 이름, 주소, 나이 등을 찾아보기 위하여 검증 주체에 의해 사용되는 알파벳-숫자 코드일 수 있다. 모든 것이 순조롭게 진행되면, 검증 주체(420)는 컴퓨터 네트워크(404)를 통하여 인증 결정을 상인(450)에게 리턴한다. 따라서, 검증 주체(420)는 동일성 인증, 결제 승인 등을 일으킬 수 있다(상인에게 리턴해 줄 수 있다). 검증 주체(420)는 검증 주체(420)와의 고객 약정(422)에 따라 검증된 고객의 존재 및 전자 서명의 조건이 충족되는지를 확인하고, 이는 고객이 트랜잭션의 책임을 짐을 상인(450)에게 추인하는 것이다.

[0123] 또한, 각각의 암호화 스트림(414)은 다른 암호화 스트림(414)의 지불 방법과 상이한 유일한 지불 방법을 포함할 수 있다. 대안적으로, 하나의 그룹의 암호화 스트림(414)은 지불을 위한 단일 신용 기관을 식별할 수 있지만, 상기 그룹내의 각각의 암호화 스트림(414)은 상이한 사용자 이름, 상이하게 인증 및 등록된 디바이스/컴퓨터, 상이한 나이 검증 방법 및/또는 상이한 고객 주소를 포함할 수 있다.

[0124] 서비스 또는 (스테레오 장치, 필터, 서적, 식료품, 의류, 가구, 컴퓨터 등과 같은) 유형의 상품을 포함하는 구매 트랜잭션을 위하여, 본 발명은 고객 검증 및 결제 승인을 제공할 수 있다. 그러나, 컴퓨터 네트워크를 통하여 부적절하게 공유될 수 있는 가능성이 있는 전자 아이템을 포함하는 구매 트랜잭션을 위하여, 본 발명은 암호화 스트림 또는 트랜잭션 식별자를 상기 전자 아이템에 부가할 수 있다. 따라서, 약정서(422)의 부분으로서, 고객은 암호화 스트림(414) 및 라우팅 식별자(416)가 도 6에 도시된 바와 같이 상인(450)으로부터 구매한 미디어 또는 미디어 컨텐츠(454)에 임베디드, 임프린트 및/또는 부착될 수 있다는 것에 동의한다. 암호화 스트림(414)을 상인(450)에게 전송하기 이전에, 검증 주체는 암호화 스트림을 부가할 수 있고, 이러한 암호화 스트림은 그 암호화 스트림(414)에 고객 약정서 또는 고객 약정서 식별자, 또는 트랜잭션 식별자를 포함할 수 있어, 상기 고객(402)과 상인(450) 사이의 고객 약정서(422)가 기꺼이 액세스될 수 있도록 해 준다.

[0125] 이러한 프로세스는 또한 고객의 약정서(422)에 제정된 바와 같이, 상인(404)의 권리에 대한 집행 관할권을 제정한다. 검증 결정은 단지 상기 데이터베이스(430)내에 있는 상기 암호화 스트림(414) 및 고객 정보가 일치할 경우에만 승인된다. 그러한 방법은 검증 주체(420)로부터 트랜잭션 확인 이메일을 고객(414)에게 전송할 수 있다. 암호화 스트림(414/CID)은 단지 암호화된 형태로 고객 저장 매체(408)에 저장된다.

[0126] 도 7의 순서도에 도시된 바와 같이, 개시된 방법은 문학 작품, 음악 작품(레코딩), 비디오 작품(영화, 쇼, 비디오 등) 등과 같이 전자적으로 저장가능한 아이템(이는 때때로 여기서 전자 아이템으로 인용된다)에 대하여 컴퓨터를 이용한 구매 트랜잭션을 용이하게 한다.

[0127] 첫째, 단계(700)에 있어서, 고객은 검증 주체와의 고객 약정을 입력한다. 그 다음, 단계(702)에서 본 실시예는 암호화 스트림(704)를 생성하기 위하여 "고객 정보"를 암호화한다. 데이터 암호화 기술은 예컨대 미국특허 제7,257,225호 및 제7,251,326호에 개시되어 있고, 그러한 프로세스의 상세 내용은 상기 개시된 실시예에 중점을 두기 위하여 여기서 제공되지 않는다. 그러한 고객 정보는 이름 식별자(이는 고객의 공식적 이름일 수도 있고 아닐 수도 있다), 고객 나이 식별자(이는 특정 나이일 수도 있고, 나이 범위일 수도 있고, 나이 분류일 수도 있다), 주소 식별자(이는 고객의 주소 또는 상이한 주소일 수도 있다)를 포함한다.

[0128] 단계(706)에서, 본 실시예는 구매한 전자 아이템의 구매 트랜잭션에서 암호화 스트림이 고객으로부터 상인에게 전송되게 한다. 검증 주체는 단계(708)에서 결제 승인을 위하여 상인에 의해 전송된 암호화 스트림을 수신한다. 그 다음, 검증 주체는 동일성 인증 및/또는 결제 승인을 포함하는 유일한 트랜잭션 식별자를 생성하기 위하여, 상기 암호화된 스트림을 고객 지불 정보(단계 710)를 포함하는 별도의 데이터베이스와 상호 비교한다.

[0129] 상기 검증 주체는 단계(714)에서 상기 유일한 트랜잭션 식별자를 상기 검증 주체로부터 상인에게 전송한다. 상기 동일성 인증 및 결제 승인은 구매 트랜잭션에서의 고객의 실제 존재를 상인에게 확인시키고, 그 결과 상인은 고객 이외의 다른 주체와 거래하고 있지 않다는 확신, 즉 다름 아닌 실제 고객과 거래하고 있다는 확신을 가지게 된다.

[0130] 상술한 바와 같이, 상기 암호화 스트림(704) 및 동일성 인증 및 결제 승인(710)은 신용 카드 정보, 은행 계정 정보 등과 같은 고객의 개인적 지불 정보를 포함하고 있지 않고, 유일한 트랜잭션 식별자 형태를 가질 수 있다. 따라서, 심지어 암호화 스트림이 해독된다 할지라도, 고객의 지불 정보는 공개되거나 사용가능하지 않을 것이다. 따라서, 고객으로부터 제공되는 암호화 스트림은 행해지는 구매 트랜잭션에 특유한 데이터 또는 정보를 포함하도록 하기 위하여 상인에게 제공되기 이전에 검증 주체에 의해 변경될 수 있다. 또는 암호화 스트림과 함께 유일한 트랜잭션 식별자가 수반될 수 있다. 그러한 변경된 암호화 스트림 또는 유일한 트랜잭션 식별자는 본 실시예의 본래 암호화 스트림 대신에 사용될 수 있다. 따라서, 본래 암호화 스트림, 변경된 암호화 스트림, 및/또는 유일한 트랜잭션 식별자가 고객에게 제공되기 이전에 전자 아이템에 부가될 수 있다.

[0131] 단계(716)에 도시된 바와 같이, 컴퓨터 네트워크를 통하여 부적절하게 복사 및 배포될 수 있는 가능성을 가진 전자 아이템을 다루는 본 실시예에 있어서, 상인에 의해, 암호화 스트림 및/또는 유일한 트랜잭션 식별자가 구매된 전자 아이템에 부가되고, 그 결과 개인화된 전자 아이템(718)을 생성하게 된다. 암호화 스트림 또는 트랜잭션 식별자는 숨겨질 수 있고, 그 결과 고객은 개인화된 전자 아이템으로부터 상기 암호화 스트림 또는 트랜잭션 식별자를 제거할 수 없다. 정보를 디지털로 저장하는 기술은 공지되어 있다(그러한 상세 내용은 미국 특허 제6,691,229 및 제5,809,160호에 구체적으로 기재되어 있다). 게다가, 상기 개인화된 전자 아이템은 만약 상기 암호화 스트림 또는 트랜잭션 식별자가 제거되면 작동하지 않도록 제조될 수 있다(즉, 개인화된 전자 아이템이 열리지 않거나 재생되지 않는 등과 같이 작동하지 않는다). 암호화 스트림 또는 워트마크를 이용하여 디지털 작품에 대한 엑세스를 제한하는 기술은 또한 공지되어 있다(그러한 상세 내용은 미국 특허 7,062,069호에 구체적으로 기재되어 있다).

[0132] 따라서, 상기 개인화된 전자 아이템은 항상 암호화 스트림을 유지하고, 전자 아이템을 구매한 고객이 (검증 주체를 통하여) 식별되도록 해 주고, 구매한 전자 아이템의 모든 복사본은 상기 암호화 스트림 또는 트랜잭션 식별자를 포함할 것이다. 따라서, 개인화된 전자 아이템의 모든 복사본이 암호화 스트림을 가지기 때문에, 상인으로부터 전자 아이템을 본래 구매한 고객(복사본의 출처)이 항상 식별되어질 수 있다.

[0133] 암호화 스트림 또는 트랜잭션 식별자를 구매된 전자 아이템에 부가한 다음, 상기 개인화된 전자 아이템은 단계(720)에서 상인으로부터 고객에서 제공된다. 다른 고객에게 배포된 각각의 개인화된 전자 아이템은 다른 암호화 스트림 또는 트랜잭션 식별자 각각의 유일함 때문에 상이하고, 이는 본래 전자 아이템을 구매한 고객이 전자 아이템의 복사본에서 식별되게 해 준다. 게다가, 각각의 암호화 스트림 또는 트랜잭션 식별자의 유일함은 구매한 전자 아이템의 인증되지 않은 복사본의 출처가 검증 주체를 통하여 식별되게 해 준다. 따라서, 단계(722)에 도시된 바와 같이, 본 방법은 잠재적으로 개인화된 전자 아이템에 포함된 암호화 스트림으로부터 고객을 식별하는 단계를 포함한다.

[0134] (고객이 셋업하거나 신용카드 발급사와의 계정을 변경할 때) 고객을 등록하는 동안 및 전자 아이템을 구매하는 동안, 고객에게는 그들의 정보가 모든 개인화된 전자 아이템의 복사본에 남겨진다는 알림 또는 경고가 제시된다. 게다가, 전자 아이템을 구매하는 동안, 유사한 알림 또는 경고가 고객에게 전자 아이템의 인증되지 않은 사용 또는 복사에 대하여 가해지는 조건 및 페널티를 지킬 것을 동의한다는 것을 알리기 위하여 디스플레이되고, 개인화된 전자 아이템이 열기, 재생 등이 될 때 마다(또는 처음의 몇 번), 동일한 경고가 디스플레이된다. 그러한 경고는 고객이 상인의 권리를 위반하여(예컨대, 불법적인 업로딩 또는 복사) 개인화된 전자 아이템의 복사본을 다른 사람에게 제공하지 못하도록 의도된 것이다. 왜냐하면, 고객은 상기 경고를 통하여 불법적 업로딩 또는 복사가 암호화 스트림을 사용하는 검증 주체에 의해 추적될 수 있고, 그러한 경고에 게재된 조건 및 조항을 지키는 것에 동의한다는 것을 인지하게 되기 때문이다. 유사하게 인증된 사용 및 수락 경고문이 또한 나이, 나이에 근거한 판매 가격 또는 거주지 등에 기초하여 액세스에 대응하여 채택될 수 있다. 본 실시예는 광범위한 고객 식별을 가능하게 하여, 전자 상거래를 권장, 촉진하고, 나아가 전자 상거래 및 그와 관련된 당사자들을 보호한다.

[0135] 고객 정보(702)의 암호화는 도 8에 도시된 바와 같이 수행된다. 첫째, 고객은 제1 컴퓨터 디바이스(800)를 사용하여 신용카드 발급사에 접속하고, 검증 주체는 몇몇 소프트웨어를 상기 제1 컴퓨터 디바이스(802)에 다운한다. 고객은 유효한 발송 주소, 생년월일(또는 나이 그룹 분류), 은행 계정 번호, 신용카드 번호 등과 같은 존재하는 민감한 정보에 대한 액세스 권한을 검증 주체(804)에게 제공하거나 또는 그러한 권한을 허용함에 동의한다. (은행 계정 번호 및 신용카드 번호와 같은) 고객 정보의 어떤 항목은 고객의 컴퓨터 디바이스에 저장되지 않지만, 그 대신 비록 코드화된 또는 비-코드화된 식별자가 그러한 정보를 특히 참조하기 위해 사용될 수 있지만, 단지 신용카드 발급사 및/또는 검증 주체의 데이터베이스에만 유지된다. 고객 정보의 다른 항목 또는 식별자(이름, 주소, 나이 참조 등)가 암호화 스트림을 생성하기 위하여 암호화될 수 있고, 암호화 스트림은 고객 컴

퓨터 디바이스에 저장되고, 부분적 또는 전체적으로 암호화 이전에 코드화 또는 비-코드화될 수 있다.

[0136] 고객 인증과 함께, 신용카드 발급사는 단계(806)에서 제1 컴퓨터 디바이스로부터 (마드보드, 하드 드라이브,, 프로세스 등의 시리얼 넘버와 같은) 유일한 하드웨어 식별자를 읽기 및 등록한다. 이러한 유일한 하드웨어 식별자는 또한 단계(808)에서 암호화 스트림으로 편입될 수 있다. 그 다음, 동일한 단계가 고객이 미래의 구매 트랜잭션에 사용하기 위하여 인증 및 등록하기를 원하는 모든 추가적인 컴퓨터 디바이스에 대하여 반복된다. 그러한 프로세스는 고객이 신용카드 발급사와의 계정을 셋업 또는 변경할 때 행해질 수 있다.

[0137] "공용" 또는 "미등록" 컴퓨터의 사용 또한 본 발명에 의해 커버된다. 만약 "미등록" 컴퓨터로부터 "발급자 계정"을 액세스하고 그들의 존재하는 계정하에서 그러한 컴퓨터의 "제한된" 승인을 받게 되면, 개인에게 비상 액세스를 허용하는 것이 가능하다. 상기 컴퓨터의 승인은 시간 제한(예컨대, 단 한번의 구매를 위한 15 분) 또는 사용 제한(예컨대, 한번의 사용/한번의 구매)하에서 이루어질 수 있다.

[0138] 또 다른 실시예에서, 암호화 스트림을 상인에게 전송하기 위한 근접한 시간에, 상인이 다름 아닌 고객과 거래하고 있다는 것을 더 확인시키기 위한 하나의 프로세스로서, (암호화 스트림을 전송하는 프로세스의 일 부분으로서) 암호화 스트림을 상인에게 실제 전송하기 이전에, 본 방법은 상기 암호화 스트림에, 제2 세트의 하드웨어 식별자, 및 암호화 스트림을 실제 전송하는 컴퓨터 디바이스로부터의 시간 및 날짜 스탬프를 편입시킬 수 있다. 따라서, 도 9에 도시된 바와 같이, 단계(900)에서 하드웨어 식별자가 암호화 스트림에 부가된 이후에, 본 방법은 단계(902)에서 상인에 접속된 실제 컴퓨터로부터 제2 세트의 하드웨어 식별자를 읽기한다. 그 다음, 이러한 제2 세트의 하드웨어 식별자(및 어쩌면 시간 및 날짜 스탬프)가 단계(904)에서 암호화 스트림에 부가되고, (양쪽 세트의 하드웨어 식별자를 가지는) 변경된 암호화 스트림이 단계(906)에서 상인에게 전송된다.

[0139] 따라서, 비도덕적인 사람이 암호화된 스트림의 부적절한 복사본을 획득할 수 있고, 필수적인 신용카드 발급사로 하여금 암호화 스트림 생성 및 전송 소프트웨어를 제공함과 함께, (상인에 등록된 고객 컴퓨터 중 하나가 아닌) 컴퓨터에서 암호화 스트림의 부적절한 복사본을 사용하면, 암호화 스트림의 전송 직전에 읽기되는 제2 하드웨어 식별자가 암호화 스트림내의 제2 하드웨어 식별자와 매칭되지 않게 되고, 트랜잭션은 검증 주체에 의해 승인되지 않을 것이다. 유사하게는, 시간 및 날짜 스탬프는 상인에게 제공되는 암호화 스트림이 제한된 시간(예컨대, 분, 시, 날 등) 동안 단지 유효하도록 하기 위하여 사용될 수 있다. 게다가, 그러한 프로세스는 실제 고객 이외의 누군가가 아닌, 실제 고객과 거래하고 있다는 것을 상인에게 추가적으로 확신시키기 위하여, 검증 주체에 의해 수행되는 "고객 존재" 검증 프로세스를 강화시킨다.

[0140] 본 발명의 실시예는 전적으로 하드웨어 구현, 전적으로 소프트웨어 구현, 또는 하드웨어 및 소프트웨어 구성요소를 포함하는 구현 형태를 취할 수 있다. 일 실시예에서, 본 발명은 소프트웨어로 구현되고, 이러한 소프트웨어는 펌웨어, 상주 소프트웨어, 마이크로코드 등에 제한되지 않는다.

[0141] 게다가, 본 발명의 실시예는 컴퓨터 또는 모든 명령어 실행 시스템에 의해 또는 접속되어 사용하기 위한 프로그램 코드를 제공하는 컴퓨터-사용가능 또는 컴퓨터-판독가능 매체로부터 액세스할 수 있는 컴퓨터 프로그램 제품 형태를 취할 수 있다. 컴퓨터-사용가능 또는 컴퓨터 판독가능 매체는 명령어 실행 시스템, 장치 또는 디바이스에 의해 또는 접속되어 사용하기 위한 프로그램을 포함, 저장, 통신, 전파 또는 이송시킬 수 있는 모든 장치일 수 있다.

[0142] 상기 매체는 전자 시스템, 자성 시스템, 광학 시스템, 전자자성 시스템, 적외선 시스템, 또는 반도체 시스템(또는 장치 또는 디바이스) 또는 보급 매체일 수 있다. 컴퓨터-판독가능한 매체의 일례로는 반도체 또는 고체 상태의 메모리, 자기 테이프, 지움가능한 컴퓨터 디스켓, 랜덤 액세스 메모리(RAM), 리드-온리 메모리(ROM), 단단한 자기 디스크 및 광 디스크를 들 수 있다. 광 디스크의 현재 일례로는 콤팩트 디스크-리드 온리 메모리(CD-ROM), 콤팩트 디스트-리드/라이트(CD-R/W) 및 DVD를 들 수 있다.

[0143] 프로그램 코드를 저장 및/또는 실행하기에 적합한 데이터 처리 시스템은 시스템 버스를 통하여 메모리 구성요소에 직접 또는 간접적으로 연결된 적어도 하나의 프로세서를 포함한다. 상기 메모리 구성요소는 프로그램 코드의 실제 실행 동안 이용되는 로컬 메모리, 대용량 저장체 및 코드가 실행 동안 대용량 저장체로부터 검색되어야만 하는 횟수를 줄이기 위하여 적어도 일부 프로그램 코드를 일시적으로 저장하는 캐쉬 메모리를 포함할 수 있다.

[0144] (키포드, 디스플레이, 포인팅 디바이스 등을 포함하지만, 그에 제한되지 않는) 입력/출력(I/O) 디바이스가 직접 또는 개재하는 I/O 컨트롤러를 통하여 시스템에 연결될 수 있다. 네트워크 어댑터는 또한 시스템에 연결될 수 있고, 이는 데이터 처리 시스템이 개재하는 사유 또는 공용 네트워크를 통하여 다른 데이터 처리 시스템 또는

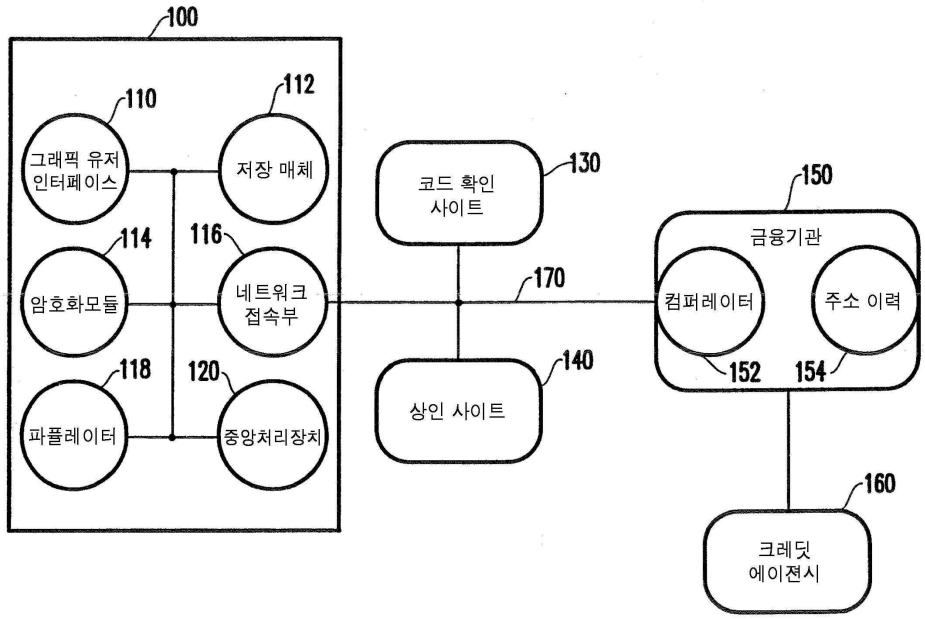
원격 프린터 또는 저장 매체에 연결될 수 있게 한다. 모뎀, 케이블 모뎀 및 이더넷 카드는 현재 네트워크 어댑터로 이용가능한 타입의 단지 몇몇이다.

[0145] 본 발명의 실시예를 실시하기 위한 대표적인 하드웨어 환경이 도 10에 도시되어 있다. 개략적인 도면은 본 발명의 일 실시예에 따른 정보 핸들링/컴퓨터 시스템의 하드웨어 구조를 도시한다. 상기 시스템은 적어도 하나의 프로세서 또는 중앙 처리 유닛(CPU)(10)를 포함한다. 상기 CPU(10)는 시스템 버스(12)를 경유하여 랜덤 액세스 메모리(RAM)(14), 리드-온리 메모리(ROM)(16) 및 입력/출력(I/O) 어댑터(18)와 같은 다양한 디바이스에 상호 연결된다. I/O 어댑터(18)는 디스크 유닛(11) 및 테이프 드라이브(13) 또는 시스템에 의해 판독가능한 다른 프로그램 저장 매체와 같은 주변 장치에 연결될 수 있다. 시스템은 프로그램 저장 매체에서 본 발명의 명령어를 판독하고 한 명령어를 본 발명의 실시예에 따른 방법을 실행하기 위하여 그러한 명령어를 따르게 된다. 상기 시스템은 키보드(15), 마우스(17), 스피커(24), 마이크로폰(22) 및/또는 사용자의 입력을 얻기 위하여 버스(12)에 연결된 터치 스크린 디바이스(도시되지 않음)와 같은 다른 유저 인터페이스 디바이스를 연결시키는 유저 인터페이스 어댑터(19)를 더 포함한다. 추가적으로, 통신 어댑터(20)는 버스(12)를 데이터 처리 네트워크(25)에 연결시키고, 디스플레이 어댑터(21)는 버스(12)를 예컨대 모니터, 프린터 또는 트랜스미터와 같은 출력 디바이스로 구현될 수 있는 디스플레이 디바이스(23)에 연결시킨다.

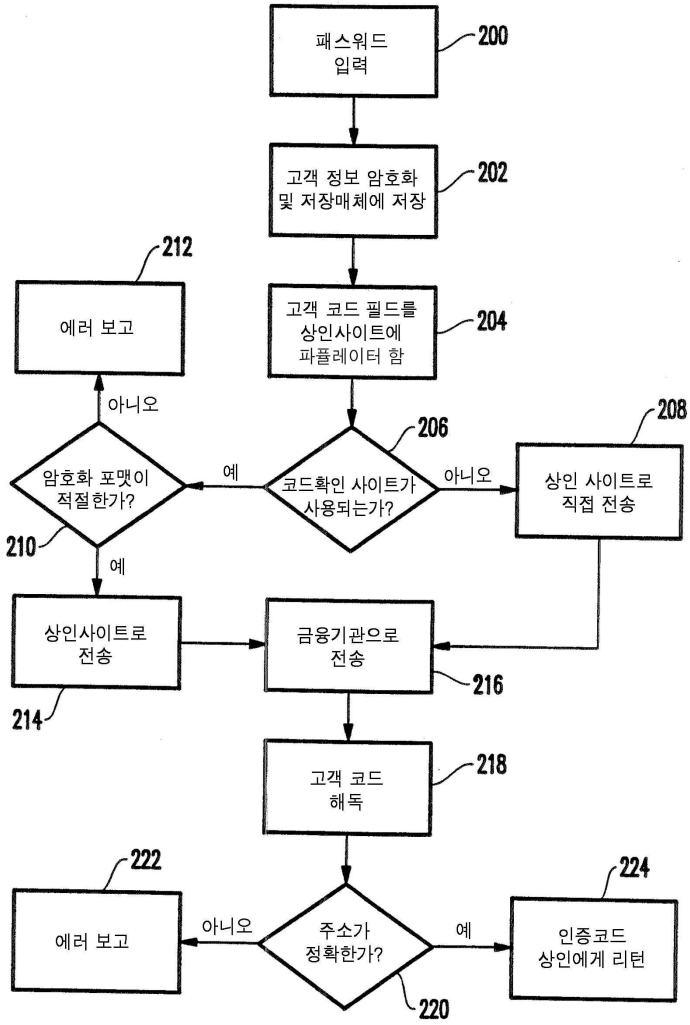
[0146] 전술한 본 발명의 실시예는 본 발명의 일반적인 특징을 충분히 개시하고 있지만, 본 발명의 기술적 사상을 벗어나지 않는 범위내에서 현존하는 지식을 적용하여 특정한 실시예로서 쉽게 변경 및/또는 수정될 수 있고, 따라서 그러한 수정 및 변경은 개시된 실시예와 동등한 의미 및 범위내로 해석되어야 할 것이다. 여기서 사용된 표현 또는 용어는 설명을 위하여 사용되는 것이고 제한되지 않음을 이해해야 할 것이다. 따라서, 본 발명의 실시예가 바람직한 실시예로 기재되었지만, 당업자라면 첨부된 청구항의 기술사상 및 범위내에서 변경 실시될 수 있음을 인지해야 할 것이다.

도면

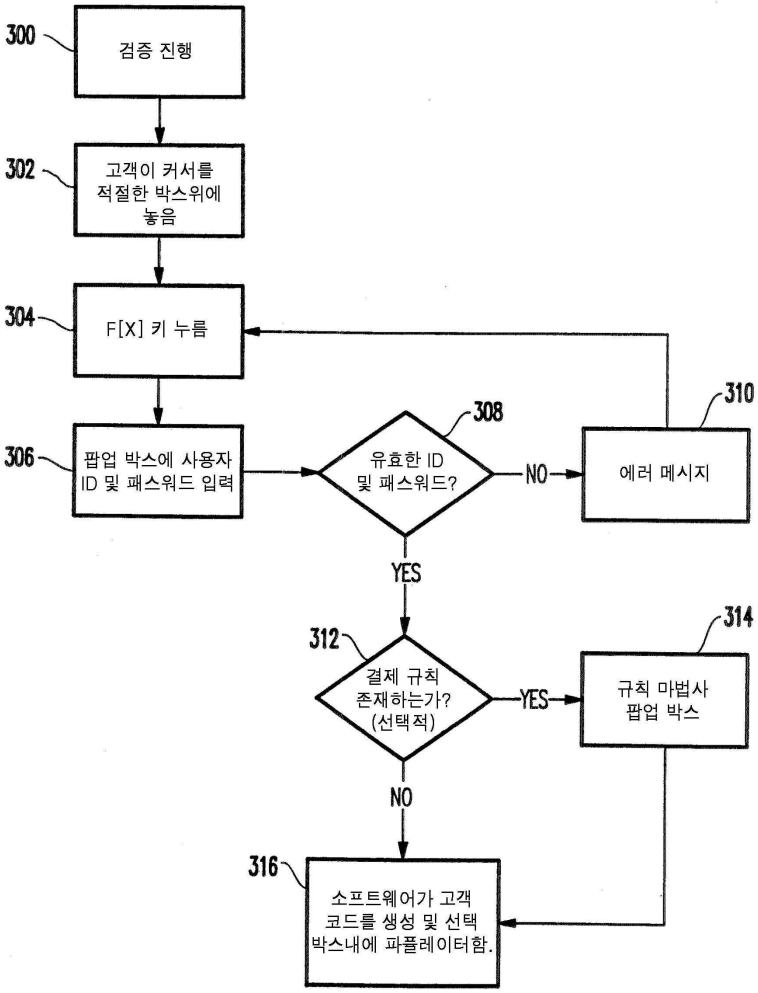
도면1



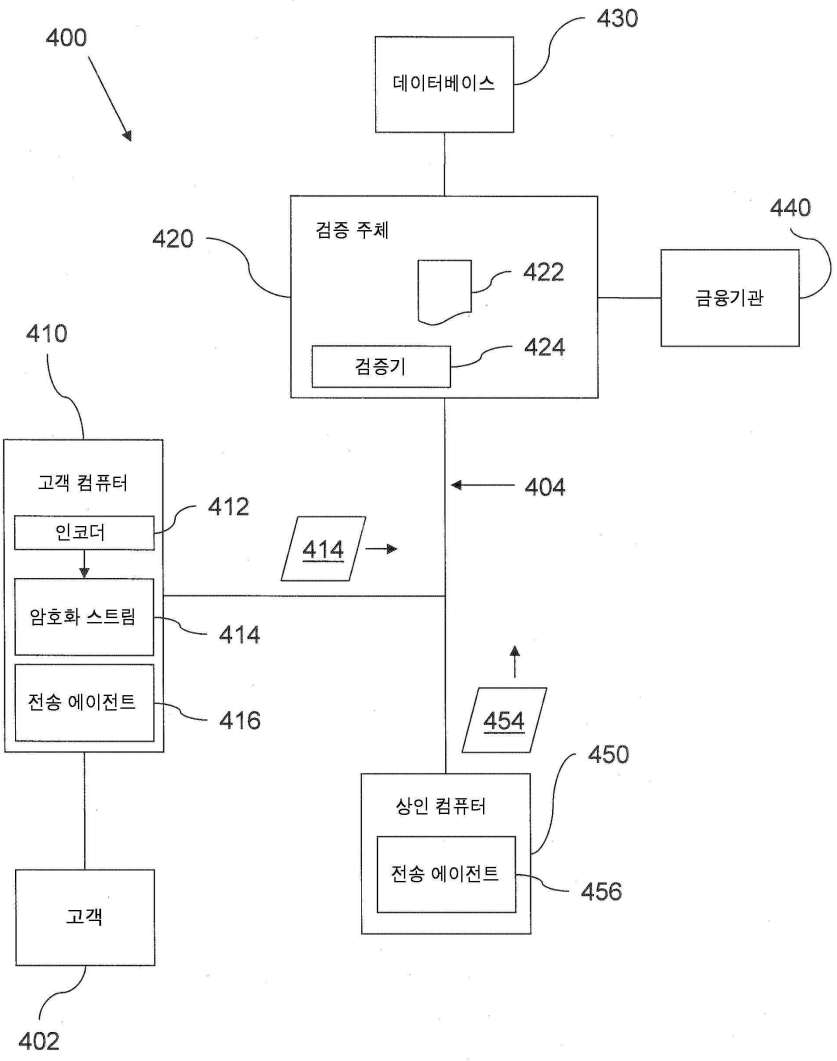
도면2


패스워드 입력
200
고객 정보 암호화 및 저장매체에 저장
202
고객 코드 필드를 상인사이트에 파플레이터 함
204
코드확인 사이트가 사용되는가?
206
아니오
상인 사이트로 직접 전송
208
예
암호화 포맷이 적절한가?
210
아니오
에러 보고
212
예
상인사이트로 전송
214
금융기관으로 전송
216
고객 코드 해독
218
주소가 정확한가?
220
아니오
에러 보고
222
예
인증코드 상인에게 리턴
224

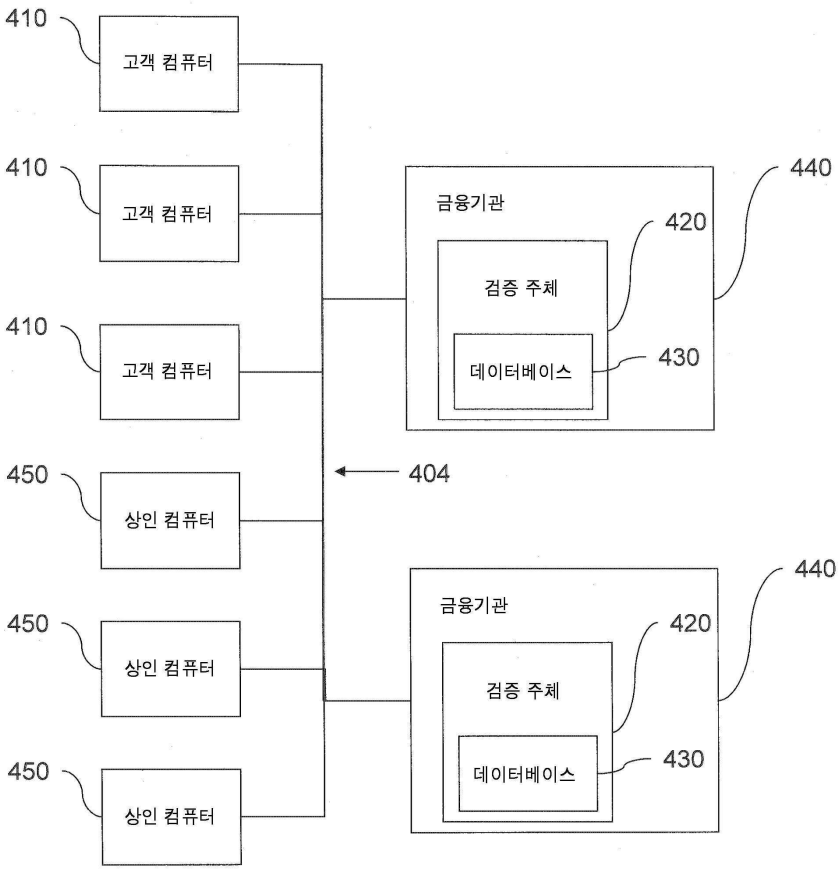
도면3


300
검증 진행
302
고객이 커서를 적절한 박스위에 놓음
304
F[X] 키 누름
306
팝업 박스에 사용자 ID 및 패스워드 입력
308
유효한 ID 및 패스워드?
NO
310
에러 메시지
YES
312
결제 규칙 존재하는가? (선택적)
YES
314
규칙 마법사 팝업 박스
NO
316
소프트웨어가 고객 코드를 생성 및 선택 박스내에 파플레이터함.

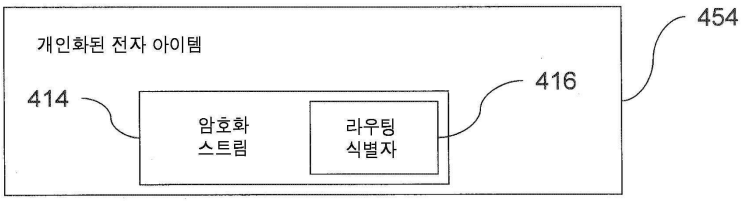
도면4


400
430
데이터베이스
420
검증 주체
422
440
금융기관
424
검증기
410
고객 컴퓨터
404
412
인코더
414
414
암호화 스트림
416
전송 에이전트
454
450
상인 컴퓨터
456
전송 에이전트
고객
402

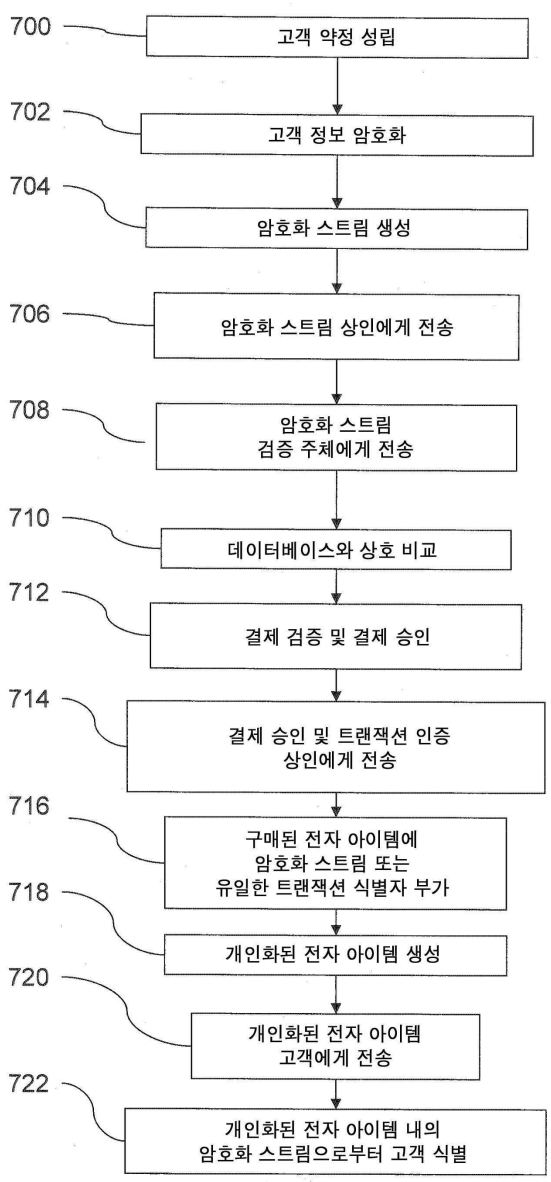
도면5


410
고객 컴퓨터
410
고객 컴퓨터
410
고객 컴퓨터
450
상인 컴퓨터
450
상인 컴퓨터
450
상인 컴퓨터
404
금융기관
420
검증 주체
430
데이터베이스
440
금융기관
420
검증 주체
430
데이터베이스
440

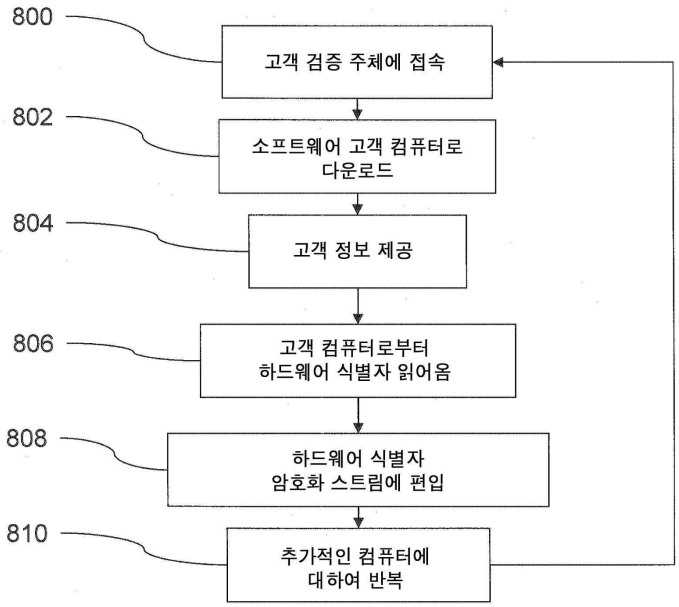
도면6


개인화된 전자 아이템
414
암호화 스트림
라우팅 식별자
416
454

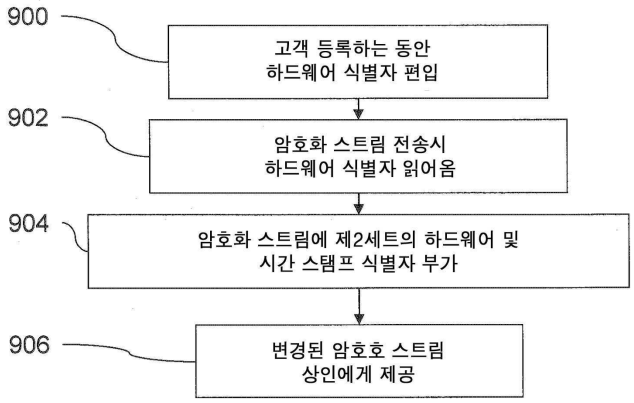
도면7


700
고객 약정 성립
702
고객 정보 암호화
704
암호화 스트림 생성
706
암호화 스트림 상인에게 전송
708
암호화 스트림
검증 주체에게 전송
710
데이터베이스와 상호 비교
712
결제 검증 및 결제 승인
714
결제 승인 및 트랜잭션 인증
상인에게 전송
716
구매된 전자 아이템에
암호화 스트림 또는
유일한 트랜잭션 식별자 부가
718
개인화된 전자 아이템 생성
720
개인화된 전자 아이템
고객에게 전송
722
개인화된 전자 아이템 내의
암호화 스트림으로부터 고객 식별

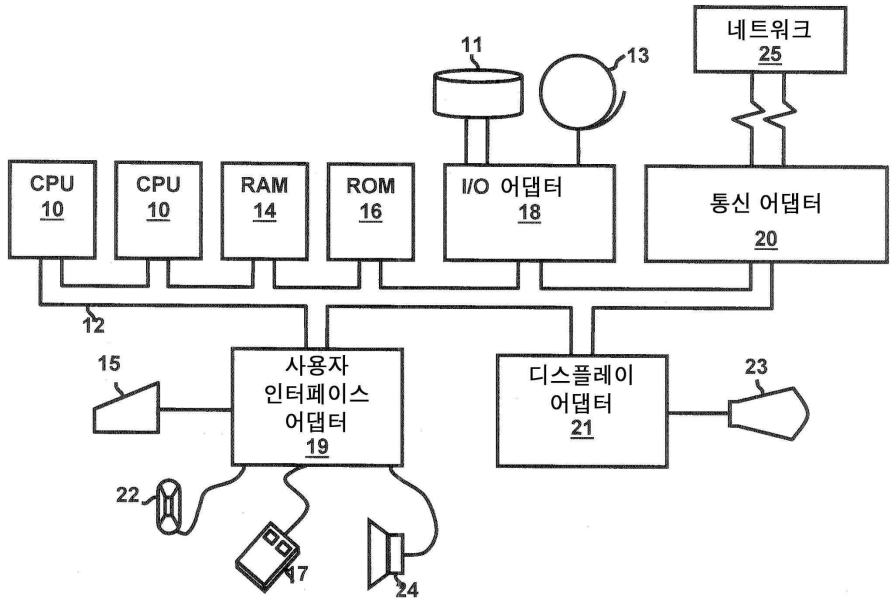
도면8


800
고객 검증 주체에 접속
802
소프트웨어 고객 컴퓨터로 다운로드
804
고객 정보 제공
806
고객 컴퓨터로부터 하드웨어 식별자 읽어옴
808
하드웨어 식별자 암호화 스트림에 편입
810
추가적인 컴퓨터에 대하여 반복

도면9


900
고객 등록하는 동안 하드웨어 식별자 편입
902
암호화 스트림 전송시 하드웨어 식별자 읽어옴
904
암호화 스트림에 제2세트의 하드웨어 및 시간 스탬프 식별자 부가
906
변경된 암호호 스트림 상인에게 제공

도면10


네트워크
25
11
13
CPU
10
CPU
10
RAM
14
ROM
16
I/O 어댑터
18
통신 어댑터
20
12
15
사용자
인터페이스
어댑터
19
디스플레이
어댑터
21
23
22
17
24