(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0118193
(43) 공개일자 2015년10월21일

(51) 국제특허분류(Int. Cl.)
G06Q 20/42 (2012.01) *G06Q 20/38* (2012.01)
G06Q 20/40 (2012.01)
(52) CPC특허분류
G06Q 20/42 (2013.01)
G06Q 20/38 (2013.01)
(21) 출원번호 10-2015-7026249(분할)
(22) 출원일자(국제) 2007년06월18일
심사청구일자 2015년09월23일
(62) 원출원 특허 10-2009-7000932
원출원일자(국제) 2007년06월18일
심사청구일자 2012년06월12일
(85) 번역문제출일자 2015년09월23일
(86) 국제출원번호 PCT/US2007/071480
(87) 국제공개번호 WO 2008/027642
국제공개일자 2008년03월06일
(30) 우선권주장
60/815,059 2006년06월19일 미국(US)
(뒷면에 계속)

(71) 출원인
비자 유에스에이 인코포레이티드
미합중국, 캘리포니아 94128, 샌프란시스코, 포스트 오피스박스 8999
(72) 발명자
하마드 아이만
미국 캘리포니아 94566 플레즌턴 코르테 몬태나스 6048
페이쓰 패트릭
미국 캘리포니아 94566 플레즌턴 존스 게이트 코트 2810
칼슨 마크
미국 캘리포니아 94019 하프 문 베이 미라몬테스 애비뉴 153
(74) 대리인
리앤목특허법인

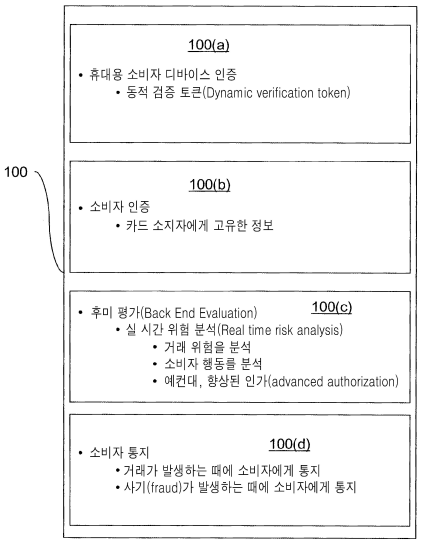
전체 청구항 수 : 총 25 항

(54) 발명의 명칭 **네트워크를 이용하는 거래 인증**

(57) 요 약

향상된 소비자 및 휴대용 소비자 디바이스 인증을 위한 시스템들과 방법이 개시된다. 그러한 시스템들과 방법들은, 부정한 거래들이 행해지는 것을 방지하기 위한 방책으로서, 동적 검증 값들, 시험 질문들 및 소비자 통지를 사용하는 단계를 포함할 수 있다.

대 표 도 - 도2



(52) CPC특허분류
G06Q 20/40 (2013.01)

(30) 우선권주장
60/815,430 2006년06월20일 미국(US)
60/884,089 2007년01월09일 미국(US)

명 세 서

청구범위

청구항 1

상인과 소비자 사이의 거래를 위해 액세스 디바이스에 의해 생성된 인가 요청 메시지를 서버 컴퓨터에 의해서 상기 액세스 디바이스로부터 수신하는 단계로, 상기 인가 요청 메시지는 상기 소비자가 사용하는 휴대용 소비자 디바이스가 상기 상인에서 상기 액세스 디바이스와 상호작용한 이후에 상기 휴대용 소비자 디바이스에 의해서 생성된 제1 동적 데이터 (dynamic data)를 포함하는, 수신 단계;

상기 인가 요청 메시지 내에 수신된 상기 제1 동적 데이터를 이용하여 상기 서버 컴퓨터에 의해서 상기 휴대용 소비자 디바이스를 인증하는 단계로서, 상기 제1 동적 데이터는 각 거래마다 상이하며 그리고 거래-특정 데이터 및 소비자-특정 데이터 중 적어도 하나로부터 생성되며, 상기 휴대용 소비자 디바이스는 상기 제1 동적 데이터가 상기 서버 컴퓨터에 의해 생성된 제2 동적 데이터와 매칭 (match)할 때에 인증되는, 인증 단계; 그리고

[상기 서버 컴퓨터에 의해서 데이터베이스로부터 시험 메시지 (challenge message)를 추출하는 단계로, 상기 시험 메시지는 동적이며, 그리고 상기 시험 메시지는 상기 소비자와 연관된 이전의 거래를 기초로 하는, 추출 단계,

상기 서버 컴퓨터에 의해서 상기 시험 메시지를 상기 액세스 디바이스로 송신하는 단계,

상기 소비자로부터의 시험 응답 (challenge response)을 상기 서버 컴퓨터에 의해 상기 액세스 디바이스로부터 수신하는 단계, 그리고

상기 수신한 시험 응답을 검증하는 단계에 의해서]

상기 서버 컴퓨터에 의해 상기 소비자를 인증하는 단계;를 포함하며,

상기 휴대용 소비자 디바이스 및 상기 소비자는 검증되어, 상기 거래가 인가되었다는 표시를 상기 서버 컴퓨터에 의해 보내며, 상기 표시는 발행기 (issuer) 서버 컴퓨터에 의해서 생성되었던 것인, 방법.

청구항 2

제1항에 있어서,

상기 인가 요청 메시지는 상기 휴대용 소비자 디바이스와 연관된 계좌 번호 그리고 거래를 위한 거래량을 더 포함하며, 그리고 상기 방법은:

상기 거래를 위한 거래량이 미리 정해진 달러 한계보다 더 클 때에 상기 서버 컴퓨터에 의해서 추가의 인증 프로세싱을 수행하는 단계를 더 포함하는, 방법.

청구항 3

제1항에 있어서,

상기 시험 메시지는 시험 질문이며, 그리고 상기 시험 메시지는 기준들의 세트를 기초로 하여 송신되는, 방법.

청구항 4

제3항에 있어서,

상기 기준들의 세트는 거래량, 그 거래의 지리적인 위치, 그리고 상기 소비자의 이전 거래들의 지리적인 위치들 중 하나 이상을 포함하는, 방법.

청구항 5

제1항에 있어서,

상기 휴대용 소비자 디바이스는 카드 또는 이동 전화기 중 하나인, 방법.

청구항 6

제1항에 있어서,

상기 액세스 디바이스는 매장 단말기인, 방법.

청구항 7

제1항에 있어서,

상기 거래-특정 데이터 및 소비자-특정 데이터는:

단말기 ID, 하루 중의 시간, 전화기 번호, SIM 카드 번호, 거래량, 계좌 번호, 서비스 코드, 만료일, 현재 날짜, 단말기로부터의 랜덤한 번호들, 그리고 이전의 거래에 관한 데이터,

중 적어도 하나를 포함하는, 방법.

청구항 8

제1항에 있어서,

상기 제1 동적 데이터 및 제2 동적 데이터는 상기 소비자에게 알려지지 않은 것인, 방법.

청구항 9

제1항에 있어서,

상기 거래의 지리적인 위치의 분석에 기초하여 상기 거래를 위한 추가의 인증 프로세싱을 상기 서버 컴퓨터에 의해 수행하는 단계를 더 포함하는, 방법.

청구항 10

제1항에 있어서,

상기 상인이 부정한 거래들에 대해 높은 경향을 가진다고 분석될 때의 거래를 위한 추가의 인증 프로세싱이 상기 서버 컴퓨터에 의해 수행하는 단계를 더 포함하는, 방법.

청구항 11

제10항에 있어서,

상기 거래를 위한 추가의 인증 프로세싱을 수행하는 것은:

상기 거래를 위한 통지 메시지를 상기 서버 컴퓨터에 의해서 상기 휴대용 소비자 디바이스에게 송신하는 것을 더 포함하는, 방법.

청구항 12

제1항에 있어서,

상기 액세스 디바이스로의 상기 시험 메시지는,

상기 휴대용 소비자 디바이스의 물리적인 위치에 관한 데이터를 요청하는 상기 소비자의 휴대용 소비자 디바이스로의 물음을 포함하며,

상기 물리적인 위치는 인증을 위해서 상기 휴대용 소비자 디바이스에 의해서 상기 액세스 디바이스로 전송되는, 방법.

청구항 13

제1항에 있어서,

상기 인가 요청 메시지는 제1 인가 요청 메시지이며, 그리고 상기 방법은:

상기 시험 응답을 제2 인가 요청 메시지의 일부로서 상기 서버 컴퓨터에 의해 상기 발행기 서버 컴퓨터에게 전

송하는 단계를 더 포함하는, 방법.

청구항 14

제13항에 있어서,

거래 코드에 의한 거래를 위해서 상기 서버 컴퓨터에 의해 상기 제2 인가 요청 메시지를 상기 제1 인가 요청 메시지에 링크하는 단계를 더 포함하는, 방법.

청구항 15

제1항에 있어서,

상기 시험 메시지를 상기 액세스 디바이스로 송신하는 단계는:

상기 시험 메시지를 포함하는 인가 응답 메시지를 상기 서버 컴퓨터에 의해서 생성하는 단계; 그리고

상기 인가 응답 메시지를 상기 거래에 연관된 액세스 디바이스에게 상기 서버 컴퓨터에 의해서 전송하는 단계를 더 포함하는, 방법.

청구항 16

제1항에 있어서,

상기 시험 메시지는 상기 데이터베이스에 저장된 그 소비자의 거래 이력 및 상기 소비자에 관한 실-시간 정보를 이용하여 상기 서버 컴퓨터에 의해서 동적으로 생성되는, 방법.

청구항 17

제16항에 있어서,

상기 시험 메시지는 상기 소비자가 특정의 이전 거래를 수행했는가의 여부를 표시할 것을 상기 소비자에게 요청하는, 방법.

청구항 18

제1항에 있어서,

상기 거래에 관한 실-시간 위험 분석을 상기 서버 컴퓨터에 의해서 수행하는 단계를 더 포함하는, 방법.

청구항 19

제1항에 있어서,

상기 시험 메시지를 위한 데이터를 상기 서버 컴퓨터에 의해서 외부 서버 컴퓨터로부터 추출하는 단계; 및

상기 시험 메시지를 위한 상기 데이터를 상기 서버 컴퓨터에 의해서 상기 데이터베이스에 저장하는 단계를 더 포함하는, 방법.

청구항 20

제1항에 있어서,

상기 상인과 연관된 상인 카테고리를 상기 서버 컴퓨터에 의해서 결정하는 단계; 및

상기 상인 카테고리를 위해 상기 소비자에 의해 제공된 파라미터들을 기초로 하여 상기 거래를 위해 복원하기 위한 여러 시험 메시지들을 상기 서버 컴퓨터에 의해서 결정하는 단계를 더 포함하는, 방법.

청구항 21

제1항에 있어서,

상기 소비자로부터 상기 시험 메시지를 수신하는 것은:

상기 휴대용 소비자 디바이스를 위한 지리적인 위치를 상기 서버 컴퓨터에 의해 상기 휴대용 소비자 디바이스로

부터 수신하는 단계를 더 포함하는, 방법.

청구항 22

제1항에 있어서,

상기 동적 데이터는 다수의 암호화 알고리즘들 중 하나의 암호화 알고리즘에 의해서 암호화되며, 상기 다수의 암호화 알고리즘들 중 상기 하나의 암호화 알고리즘과 연관된 알고리즘 식별자는 상기 인가 요청 메시지 내에 상기 암호화된 동적 데이터와 함께 전송되는, 방법.

청구항 23

제22항에 있어서,

상기 다수의 암호화 알고리즘들 중 상기 하나의 알고리즘을 위한 신뢰도 값을 상기 서버 컴퓨터에 의해서 결정하는 단계;

상기 신뢰도 값을 이용하여 거래에 대한 신용 레벨을 상기 서버 컴퓨터에 의해서 판별하는 단계; 그리고

상기 신용 레벨이 신용 임계값 아래일 때에 상기 서버 컴퓨터에 의해서 추가적인 인증 프로세싱을 수행하는 단계를 더 포함하는, 방법.

청구항 24

서버 컴퓨터로서:

프로세서; 및

상기 프로세서에 연결된 컴퓨터 판독가능 매체를 포함하며,

상기 컴퓨터 판독가능 매체는 이전 항들 중 어느 한 항을 구현하기 위해 상기 프로세서에 의해서 실행가능한 코드를 포함하는, 서버 컴퓨터.

청구항 25

액세스 디바이스; 및

상기 액세스 디바이스에 작동적으로 연결된 서버 컴퓨터를 포함하며,

상기 액세스 디바이스는 프로세서 및 상기 프로세서에 연결된 컴퓨터 판독가능 매체를 포함하며,

상기 컴퓨터 판독가능 매체는 이전 항들 중 어느 한 항을 구현하기 위해 상기 프로세서에 의해서 실행가능한 코드를 포함하는, 시스템.

발명의 설명

기 술 분 야

[0001] 관련된 출원들에 대한 상호-참조들(CROSS-REFERENCES TO RELATED APPLICATIONS).

[0002] 본 출원은 미국 임시 특허 출원 제60/815,059호[2006년 6월 19일 출원], 미국 임시 특허 출원 제60/815,430호[2006년 6월 20일 출원] 및 미국 임시 특허 출원 제60/884,089호[2007년 1월 9일 출원]의 출원일들에 관한 이익을 주장하는 비-임시 특허 출원이다. 이 출원들 모두가 모든 목적들을 위해 그들 전체로서 참조에 의해 본원에 병합된다.

배 경 기 술

[0003] 지불 거래들이 안전하게 행해지는 것을 보증하기 위한 여러 방식들이 있다. 예를 들어, 그 지불 거래를 행하는 사람이 진정한 소비자라는 것을 보증하기 위해서 소비자를 인증하기 위한 여러 상이한 방식들이 있다. 또한 소비자에 의해 사용되고 있는 휴대용 소비자 디바이스를 인증하기 위한 여러 상이한 방식들도 있다.

[0004] 지불 거래들을 인증하는 상이한 방식들이 존재하지만, 부정 거래(fraudulent transaction)들의 위험을 더 감소시키기 위해서 향상된 인증 메커니즘들이 필요하다.

[0005] 본 발명의 실시예들은 위의 문제들 및 다른 문제들을 개별적으로 그리고 집합적으로 다룬다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 상기와 같은 부정 거래의 위험을 더 감소시키기 위한 향상된 인증 메커니즘을 제공한다.

과제의 해결 수단

[0007] 향상된 소비자 및 휴대용 소비자 디바이스 인증을 위한 시스템들 및 방법들이 개시된다. 본 발명의 실시예들은, 지불 카드와 같은 휴대용 소비자 디바이스를 인증하고, 그 휴대용 소비자 디바이스를 사용하여 소비자를 인증하고, 후미 프로세싱(back end processing)을 실행하며, 그리고 구매 거래들의 소비자 통지를 제공하기 위한 방책들을 포함한다.

[0008] 본 발명의 일 실시예는 방법에 관련된다. 그 방법은, 소비자에 대한 인증 프로세스를 실행하는 단계[여기서, 상기 소비자는 거래를 행하기 위해 휴대용 소비자 디바이스를 사용함]; 상기 휴대용 소비자 디바이스에 대한 인증 프로세스를 실행하는 단계[여기서, 상기 휴대용 소비자 디바이스에 대한 인증 프로세스를 실행하는 단계는 상기 휴대용 소비자 디바이스에 연관된 지문(fingerprint) 또는 동적 검증 값(dynamic verification value)을 검증하는 단계를 구비함]; 및 상기 소비자를 인증하는 단계와 상기 휴대용 소비자 디바이스를 인증하는 단계가 실행된 후에 위험 분석(risk analysis)을 실행하는 단계[여기서, 상기 위험 분석은 상기 거래가 인가되어야 하는지 아닌지를 결정함];를 구비한다.

[0009] 본 발명의 일 실시예는 방법에 관련된다. 그 방법은, 휴대용 소비자 디바이스와 통신하는 액세스 디바이스 또는 상기 휴대용 소비자 디바이스에 의해 생성된 동적 데이터(dynamic data)를 사용하여 상기 휴대용 소비자 디바이스를 인증하는 단계; 및 소비자를 인증하는 단계[상기 소비자에게 시험 메시지(challenge message)를 보내는 단계와 상기 소비자로부터 시험 응답(challenge response)을 수신하는 단계를 구비함];를 구비한다.

[0010] 본 발명의 다른 하나의 실시예는 방법에 관련된다. 그 방법은, 휴대용 소비자 디바이스를 사용하여 행해지는 거래에 연관된 인가 요청 메시지를 수신하는 단계[여기서, 상기 휴대용 소비자 디바이스는 휴대용 소비자 디바이스 지문(portable consumer device fingerprint)을 구비하고, 그리고 상기 인가 요청 메시지는 변경된 휴대용 소비자 디바이스 지문과 알고리즘 식별자를 구비함]; 상기 알고리즘 식별자를 사용하여 다수의 알고리즘들 중에서 하나의 알고리즘을 선택하는 단계; 상기 선택된 알고리즘과 상기 변경된 휴대용 소비자 디바이스 지문을 사용하여 상기 휴대용 소비자 디바이스 지문을 결정하는 단계; 상기 휴대용 소비자 디바이스 지문이 저장된 휴대용 소비자 디바이스 지문과 매칭(match)되는지를 결정하는 단계; 시험 메시지(challenge message)를 상기 휴대용 소비자 디바이스에 연관된 소비자에게 보내는 단계; 및 인가 응답 메시지를 상기 소비자에게 보내는 단계[여기서, 상기 인가 응답 메시지는 상기 거래가 승인되는지 아닌지를 지시함];를 구비한다.

[0011] 본 발명의 다른 하나의 실시예는 방법에 관련된다. 그 방법은, 배터리 없는 휴대용 소비자 디바이스(batteryless portable consumer device)를 인증하는 단계[여기서, 상기 휴대용 소비자 디바이스는 안테나를 구비하는 배터리 없는 휴대용 소비자 디바이스를 구비함]; 소비자를 인증하는 단계; 및 거래가 행해지고 있다는 통지 메시지를 상기 소비자에게 보내는 단계;를 구비한다.

[0012] 본 발명의 다른 실시예들은 아래의 상세한 설명에서 제공되는 다른 인증 측면들의 특정한 조합들에 관련된다.

발명의 효과

[0013] 본 발명의 효과는 본 명세서의 해당되는 부분들에 개별적으로 명시되어 있다.

도면의 간단한 설명

[0014] 도 1은 본 발명의 일 실시예에 따른 시스템의 블럭도를 보여준다.

도 2는 본 발명의 일 실시예에 따른 지불 거래 인증 시스템의 측면들에 관한 블럭도를 보여준다.

도 3a 내지 도 3c는 본 발명의 실시예들에 따른 배터리 없는 카드들의 개략도를 보여준다.

도 4는 휴대용 보안 디바이스를 보여준다.

도 5는 신용 카드와 같은 휴대용 소비자 디바이스에 연관된 데이터 필드들을 나타낸다.

도 6은 주요 계좌 번호(PAN: primary account number)의 일부분들을 보여준다.

도 7은 시험 질문 엔진을 구비하는 시스템의 블럭도를 보여준다.

도 8 및 도 9는 소비자를 인증하기 위해 시험 메시지를 사용하는 단계를 구비하는 방법들을 나타내는 흐름도들이다.

도 10a는 알고리즘 ID를 사용할 수 있는 시스템의 블럭도를 보여준다.

도 10b는 도 10a에서의 시스템에서 서버 컴퓨터 내에 존재할 수 있는 모듈들을 보여주는 블럭도이다.

도 11 및 도 12는 본 발명의 실시예들에 따른 방법들을 나타내는 흐름도들이다.

발명을 실시하기 위한 구체적인 내용

[0015] Ⅰ. 예시적인 시스템들 및 지불 거래들

[0016] 본 발명의 실시예들은 다른 타입들의 거래들[예컨대, 금전 전송 거래들]뿐만 아니라 통상적인 구매 거래들을 인증하는 데 이용될 수 있다. 구체적인 인증 시스템들 및 방법들은 거래가 진정하다는 것을 보증하기 위한 소비자[예컨대, 구매자], 휴대용 소비자 디바이스[예컨대, 신용 카드], 및/또는 액세스 디바이스[예컨대, POS 단말기]의 인증에 관련된다.

[0017] 전형적인 구매 거래에서, 소비자는 상인으로부터 상품 또는 서비스들을 구매하기 위해서 휴대용 소비자 디바이스[예컨대, 신용 카드]를 사용한다.

[0018] 도 1은 본 발명의 일 실시예에서 사용될 수 있는 시스템(20)을 보여준다. 시스템(20)은 상인(22) 및 그 상인(22)에 연관된 획득기(24)를 포함한다. 전형적인 지불 거래에서, 소비자(30)는 휴대용 소비자 디바이스(32)를 사용하여 상인(22) 측에서 상품 또는 서비스들을 구매할 수 있다. 획득기(24)는 지불 프로세싱 네트워크(26)를 통해 발행기(28)와 통신할 수 있다.

[0019] 소비자(30)는 개인, 또는 상품이나 서비스들을 구매할 수 있는 사업체와 같은 조직일 수 있다.

[0020] 휴대용 소비자 디바이스(32)는 어떤 적당한 형태에 있을 수 있다. 예를 들어, 적당한 휴대용 소비자 디바이스들은 그들이 소비자의 지갑 및/또는 주머니에 들어맞을 수 있도록[예컨대, 주머니-사이즈(pocket-sized)] 핸드-헬드(hand-held) 및 컴팩트(compact) 형태일 수 있다. 그들은 스마트 카드(smart card)들, 마이크로프로세서 없이 마그네틱 스트립(magnetic strip)을 갖춘 보통의 신용 카드(credit card) 또는 차변 카드(debit card), Exxon-Mobil Corp.로부터 상업적으로 이용가능한 Speedpass™와 같은 키 체인 디바이스(keychain device)들 등을 포함할 수 있다. 휴대용 소비자 디바이스들의 다른 예시들은 셀룰러 전화기(cellular phone)들, 개인 디지털 보조기(PDA: personal digital assistant)들, 페이저(pager)들, 지불 카드(payment card)들, 보안 카드(security card)들, 액세스 카드(access card)들, 스마트 미디어(smart media), 트랜스폰더(transponder)들 등을 포함한다. 또한 휴대용 소비자 디바이스들은 차변 디바이스(debit device)들[예컨대, 차변 카드(debit card)], 신용 디바이스(credit device)들[예컨대, 신용 카드(credit card)], 또는 저장 값 디바이스(stored value device)들[예컨대, 저장 값 카드(stored value card)]일 수 있다.

[0021] 지불 프로세싱 네트워크(26)는 인가 서비스(authorization service)들, 예외 파일 서비스(exception file service)들, 그리고 정산 및 결산 서비스(clearing and settlement service)들을 지원하고 배달하기 위해 이용되는 데이터 프로세싱 서브시스템들, 네트워크들, 및 동작들을 포함할 수 있다. 예시적인 지불 프로세싱 네트워크는 VisaNet™을 포함할 수 있다. VisaNet™과 같은 지불 프로세싱 네트워크들은 신용 카드 거래들, 차변 카드 거래들, 및 다른 타입들의 상업 거래들을 처리할 수 있다. VisaNet™은 특히 인가 요청들을 처리하는 VIP 시스템(Visa Integrated Payments system)과 정산 및 결산 서비스들을 실행하는 베이스 Ⅱ 시스템(Base Ⅱ system)을 포함한다.

[0022] 지불 프로세싱 네트워크(26)는 서버 컴퓨터를 포함할 수 있다. 서버 컴퓨터는 전형적으로 강력한 컴퓨터 또는 컴퓨터들의 집단이다. 예를 들어, 서버 컴퓨터는 큰 메인프레임, 미니컴퓨터 집단, 또는 유닛(unit)으로서 기능하는 한 그룹의 서버들일 수 있다. 일 예시에서, 서버 컴퓨터는 웹 서버에 연결된 데이터베이스 서버일 수 있다. 지불 프로세싱 네트워크(26)는 인터넷을 포함하는 어떤 적당한 유선 또는 무선 네트워크를 이용할 수 있

다.

[0023] 상인(22)은 휴대용 소비자 디바이스(32)와 상호작용할 수 있는 액세스 디바이스(34)를 가지거나 그 액세스 디바이스로부터 통신들을 수신할 수 있다. 본 발명의 실시예들에 따른 액세스 디바이스들은 어떠한 적당한 형태일 수 있다. 액세스 디바이스들의 예시들은 매장 디바이스{POS(point of sale) device}들, 셀룰러 전화기들, PDA들, 개인 컴퓨터(PC)들, 태블릿 PC(tablet PC)들, 핸드헬드 특화된 판독기(handheld specialized reader)들, 셋-탑 박스(set-top box)들, 전자 캐쉬 등록기(ECR: electronic cash register)들, ATM(automated teller machine)들, 가상 캐쉬 등록기(VCR: virtual cash register)들, 키오스크(kiosk)들, 보안 시스템들, 액세스 시스템들 등을 포함한다.

[0024] 액세스 디바이스(34)가 매장 단말기이면, 어떤 적당한 매장 단말기가 카드 판독기들을 포함하여 사용될 수 있다. 카드 판독기들은 어떤 적당한 접촉 동작 모드 또는 비접촉 동작 모드를 포함할 수 있다. 예를 들어, 예시적인 카드 판독기들은 휴대용 소비자 디바이스들(32)과 상호작용하기 위해 RF(radio frequency) 안테나들, 마그네틱 스트라이프 판독기들 등을 포함할 수 있다.

[0025] 전형적인 구매 거래에서, 소비자(30)는 신용 카드와 같은 휴대용 소비자 디바이스(32)를 사용하여 상인(22)에게서 상품 또는 서비스를 구매한다. 소비자의 휴대용 소비자 디바이스(32)는 상인(22) 측의 매장 단말기{POS(point of sale) terminal}와 같은 액세스 디바이스(34)와 상호작용할 수 있다. 예를 들어, 소비자(30)는 신용 카드를 소지할 수 있고 POS 단말기의 적당한 슬롯(slot)을 통해 그것을 스와이핑(swipe)할 수 있다. 대안적으로, 매장 단말기는 비접촉 판독기일 수 있고, 휴대용 소비자 디바이스(32)는 비접촉 카드와 같은 비접촉 디바이스일 수 있다.

[0026] 인가 요청 메시지가 획득기(24)로 전달된다. 인가 요청 메시지를 수신한 후에, 그 인가 요청 메시지는 지불 프로세싱 네트워크(26)로 보내진다. 그러면 지불 프로세싱 네트워크(26)는 그 인가 요청 메시지를 휴대용 소비자 디바이스(32)의 발행기(28)로 전달한다.

[0027] 발행기(28)가 인가 요청 메시지를 수신한 후에, 현재의 거래가 인가되는지 또는 인가되지 않는지를 지시하기 위해서 발행기(28)는 인가 응답 메시지를 지불 프로세싱 네트워크(26)로 되보낸다[단계 56]. 그러면 지불 프로세싱 네트워크(26)는 그 인가 응답 메시지를 획득기(24)로 전달한다. 그러면 획득기(24)는 그 응답 메시지를 상인(22)에게 되보낸다.

[0028] 상인(22)이 인가 응답 메시지를 수신한 후에, 상인(22) 측의 액세스 디바이스(34)는 그 인가 응답 메시지를 소비자(30)에 대하여 제공한다. 그 응답 메시지는 액세스 디바이스(24)에 의해 디스플레이될 수 있고, 또는 영수증 상에 프린트될 수 있다.

[0029] 그 날의 말미에, 정규의 정산 및 결산 프로세스가 지불 프로세싱 네트워크(26)에 의해 행해질 수 있다. 정산 프로세스는 소비자의 계좌에 부기(posting)하는 것과 소비자의 결산 위치를 조정하는 것을 돕기 위해 획득기와 발행기 간에 금융 상세들(financial details)을 교환하는 프로세스이다. 정산과 결산은 동시에 발생할 수 있다.

[0030] Ⅱ. 거래 인증(Transaction Authentication)

[0031] 개념적인 블럭도(100)를 보여주는 도 2를 참조한다. 위에서 설명된 바와 같은 구매 거래의 인증은 다양한 측면들을 가질 수 있다. 그러한 측면들은 휴대용 소비자 디바이스 인증{100(a)}, 소비자 인증{100(b)}, 실 시간 위험 분석(real time risk analysis)을 포함하는 후미 프로세싱{back end processing. 100(c)}, 그리고 구매 거래의 소비자 통지{100(d)}를 포함한다.

[0032] 휴대용 소비자 디바이스 인증은 휴대용 소비자 디바이스의 인증에 관련된다. 즉, 휴대용 소비자 디바이스 인증 프로세스에서, 구매 거래에서 사용되고 있는 휴대용 소비자 디바이스가 진정한 휴대용 소비자 디바이스인지 또는 위조된 휴대용 소비자 디바이스인지에 관한 결정이 행해진다. 휴대용 소비자 디바이스의 인증을 향상시키기 위한 구체적이고 예시적인 기법들은 다음을 포함한다.

[0033] - 마그네틱 스트라이프 카드(magnetic stripe card)들과 같은 휴대용 소비자 디바이스들 상에 동적 CVV

[0034] - 카드 보안 특징들 [현존하는 것 그리고 새로운 것]

[0035] - 비접촉 칩들(Contactless chips) [한정된 용도]

[0036] - 마그네틱 스트라이프 식별(Magnetic stripe identification)

[0037] - 카드 검증 값들(Card Verification Values) [CVV 및 CVV2]

[0038] - 접촉 EMV 칩들

[0039] 소비자 인증은 거래를 행하고 있는 사람이 사실상 그 휴대용 소비자 디바이스의 소유자 또는 인가된 사용자인지 아닌지에 관한 결정에 관련된다. 통상적인 소비자 인증 프로세스들은 상인들에 의해 행해진다. 예를 들어, 상인들은 신용 카드 소지자와의 영업 거래를 행하기 전에 신용 카드의 소지자에게 운전자 면허를 보여달라고 요구할 수 있다. 소비자를 인증하기 위한 다른 방식들이 바람직할 수 있다. 왜냐하면 상인 측에서의 소비자 인증이 모든 경우에서 발생하지는 않기 때문이다. 소비자 인증 프로세스를 향상시키기 위한 가능한 방식들의 구체적인 예시들은 적어도 다음을 포함한다.

[0040] - 지식 기반 시험 응답들(Knowledge-based challenge-responses)

[0041] - 하드웨어 토큰들(Hardware tokens) [다중 솔루션 옵션들]

[0042] - 일회용 패스워드들(OTPs: one time passwords) [한정된 용도]

[0043] - AVS들 [독립형 솔루션으로서는 아님]

[0044] - 서명들(Signatures)

[0045] - 소프트웨어 토큰들(Software tokens)

[0046] - PIN들 [온라인/오프라인]

[0047] - 사용자 ID들/패스코드들(User IDs/Passcodes)

[0048] - 2 채널 인증 프로세스들 [예컨대, 전화기를 통해]

[0049] - 생체인식(Biometrics)

[0050] 후미 프로세싱(Back end processing)은 발행기 또는 지불 프로세싱 네트워크, 또는 비-상인(non-merchant) 위치에서 발생할 수 있는 프로세싱에 관련된다. 아래에서 상세하게 설명되듯이, 행해지고 있는 어떤 거래들이 진정하다는 것을 보증하기 위해서 지불 거래의 "후미(back end)"에서 다양한 프로세스들이 실행될 수 있다. 또한 후미 프로세싱은 인가되어서는 안되는 거래들을 방지할 수 있고, 인가되어야 하는 거래들을 허용할 수 있다.

[0051] 최근에는 소비자 통지가 거래 인증의 다른 측면이다. 일부 경우들에서, 소비자는 구매 거래가 발생하고 있다는 것 또는 발생했다는 것을 통지받을 수 있다. 소비자의 휴대용 소비자 디바이스를 사용하여 거래가 발생하고 있다는 것을 그 소비자가 통지받았으나[예컨대, 셀 전화기를 통해] 사실상 그 소비자는 그 거래를 행하고 있지 않다면, 그 거래가 발생하는 것을 방지하기 위해 적당한 단계들이 취해질 수 있다. 소비자 통지 프로세스들의 구체적인 예시들은 다음을 포함한다.

[0052] - SMS를 통한 구매 통지

[0053] - e 메일을 통한 구매 통지

[0054] - 전화기에 의한 구매 통지

[0055] 위에서 설명된 어느 측면들에 관한 구체적인 상세들은 아래에서 제공된다. 구체적인 측면들의 구체적인 상세들은 본 발명의 실시예들의 사상과 범위를 벗어나지 않으면서 어떤 적당한 방식으로 조합될 수 있다. 예를 들어, 휴대용 소비자 디바이스 인증, 소비자 인증, 후미 프로세싱 및 소비자 거래 통지는 본 발명의 일부 실시예들에서 모두 조합될 수 있다. 그러나, 본 발명의 다른 실시예들은 개별적인 측면들 각각에 관련되거나 그 개별적인 측면들의 구체적인 조합들에 관련되는 구체적인 실시예들을 지향할 수 있다.

[0056] Ⅲ. 휴대용 소비자 디바이스 인증

[0057] 다양한 휴대용 소비자 디바이스 인증 프로세스들에 대하여 향상들이 행해질 수 있다. 그러한 향상들의 예시들이 아래에서 제공된다.

[0058] A. 동적인 카드 검증 값들(dCVVs: Dynamic card verification values)

[0059] 지불 거래에서 사용되고 있는 휴대용 소비자 디바이스가 사실상 진정한 휴대용 소비자 디바이스인지를 보증하기 위해서, "동적인(dynamic)" 데이터가 휴대용 소비자 디바이스로부터 제공될 수 있다. 동적인 데이터는 매번 변경될 수 있는 데이터이고, 따라서 정적인(static) 데이터[예컨대, 이름]보다 더 안전하다. 예를 들어, 휴대용 소비자 디바이스 인증 프로세스는 동적인 CVV(card verification value)와 같은 "동적인(dynamic)" 검증 데이터를 포함할 수 있다.

[0060] 비교적으로, "정적인(static)" 데이터는 매번 변경되지 않는 데이터일 수 있다. 예를 들어, 오늘날, 신용 카드들은 카드들의 후면 상에 프린트된 카드 검증 값들(CVV 값들)을 가진다. 이 값들은 사용되고 있는 휴대용 소비자 디바이스가 진정하다는 것을 검증하는 데 이용될 수 있다. 예를 들어, 신용 카드를 이용하여 전화기 또는 인터넷을 통해 구매 거래를 행하는 때에, 상인은 신용 카드의 후면 상의 CVV 값을 요구할 수 있다. CVV 값은 호출자(caller)가 사실상 진정한 휴대용 소비자 디바이스를 소유한다는 것을 보증하기 위해 신용 카드 번호에 매칭될 수 있다. 현재의 CVV들이 가지는 하나의 문제는 그들이 정적(static)이라는 것이다. 그들이 도난되어 사용될 수 있다.

[0061] 동적인 CVV("dCVV")가 모든 목적들을 위해 그 전체로서 참조에 의해 여기에 병합되는 미국 특허출원 제10/642,878호에 설명되어 있다. 미국 특허출원 제10/642,878호는 주요 계좌 번호(PAN: primary account number), 만료일, 서비스 코드 및 자동 거래 카운터(automatic transaction counter)를 포함하는 정보를 이용하는 검증 값의 생성을 설명한다. 이 검증 값은 상인으로부터 서비스 제공자[예컨대, 지불 프로세싱 조직(payment processing organization) 또는 발행기(issuer)]에게 전송되며, 서비스 제공자 측에서 그것은 가능한 승인을 위해 디코딩되어 평가된다. 자동 거래 카운터는 휴대용 소비자 디바이스가 사용되는 회수를 추적하고, 발행기 측에서 수신되는 카운터 값과 발행기에서의 카운터 간의 불일치가 있으면, 이것은 가능한 데이터 조작(data skimming) 또는 부정한 사용(fraudulent use)을 지시할 수 있다.

[0062] dCVV 또는 다른 동적인 데이터는 어떤 적당한 보안 데이터 전송 프로세스를 이용하여 전송될 수 있고, ECC(elliptical curve cryptography) 또는 AEC(advanced encryption cryptography)뿐만 아니라 DES(dynamic encryption standard)를 이용할 수 있다. 어떤 대칭 또는 비대칭 암호 엘리먼트들이 이용될 수 있다.

[0063] dCVV 프로세스의 다른 보안 향상들은 긴 DES 번호 및 긴 카운터의 사용을 포함할 수 있다.

[0064] B. 특정한 입력 데이터에 의해 생성되는 dCVV들

[0065] 상이한 데이터 또는 상이한 타입들의 가변 정보를 이용하여 상이한 동적 검증 값들을 생성함으로써 선행의 dCVV 프로세스들에 대한 향상을 도모하는 것이 바람직하다. 예를 들어, 어느 휴대용 소비자 디바이스가 정확한 디바이스라는 것을 검증하기 위해서 더 많은 거래 및/또는 사용자 특정 데이터가 동적으로 변경될 수 있다. 이것은 단지 단일의 카운터를 사용하는 것보다 더 안전할 것이다. 예를 들어, 특정한 정보는 단말기 ID, 그날의 시간, 전화기 번호, SIM 카드 번호, 거래량, 계좌 번호, 서비스 코드[2 디지트(two digits)], 만료일, 현재 날짜, 단말기로부터의 랜덤한 번호들 등을 포함할 수 있다. 그 특정한 정보는 바람직하게는 카운터와 같은 적어도 하나의 동적인(dynamic) 데이터 엘리먼트, 그날의 시간, 구매 계좌 등을 포함한다. 다른 실시예들에서, 동적인 검증 값을 생성하는 데 사용된 그 특정한 정보는 거래가 발생하는 그날의 시간과 같은 동적인 소비자 특정 정보나 거래 특정 정보, 구매 계좌, 이전의 거래 데이터 등을 포함한다. 이러한 것들의 어떤 것, 일부 또는 모든 것은 검증 값을 생성하는 데 이용될 수 있으며 그 정보의 다른 특정한 부분들은 새로운 dCVV를 생성하기 위해 동적으로 변경될 수 있다. 그러면 그 새로운 dCVV는 미국 특허출원 제10/642,878호에 설명된 일반 프로세스 스킴(scheme)과 유사한 방식 또는 상이한 방식으로 처리될 수 있다. 하나의 특정한 예시에서, 이전의 거래에 관한 데이터[예컨대, 이전의 구매 계좌, 이전 거래의 시간 등]는 미래의 거래들에 대하여 휴대용 소비자 디바이스를 인증하는 데 이용될 수 있는 동적인 데이터 엘리먼트일 수 있다. 그러한 dCVV 방법들에 관한 추가적인 상세들을 본 출원과 동일한 날에 "Verification Value System and Method"라는 명칭으로 출원된 미국 특허출원[대리인 문서

번호: 16222U-031900US]에서 찾을 수 있다.

[0066] C. 거절되는 dCVV 거래들의 수를 감소시킴

[0067] 위에서 설명된 dCVV 프로세스들은 유용하다. 그러나, 휴대용 소비자 디바이스로부터 전송되어 서비스 제공자의 서버에서 수신되는 동적 데이터[예컨대, 카운터 값]가 발행기의 서버에서 생성되는 상응하는 동적 데이터[다른 하나의 상응하는 카운터 값]와 매칭되지 않는 여러 경우들이 있을 수 있다. 예를 들어, 때때로, 상인이 거래 데이터를 제때에 발행기로 전달하지 않을 수 있다. 이러한 경우가 발생하면, 소비자에 의해 행해지는 미래의 거래들이 부주의로 인해 거절될 수 있다. 예를 들어, 소비자에 의해 사용된 휴대용 소비자 디바이스의 카운터는 어느 거래가 행해진 것으로 거래 회수를 카운팅하였으나, 발행기의 서버에 있는 카운터가 상응하는 거래 카운트를 보유하지 못하면, 1 이상의 상인들로부터의 거래 데이터의 지연된 수신 때문에, 그 소비자의 거래들의 일부는 부주의로 인해 거절될 수 있다. 조작된 거래들을 승인하지 않으면서 가능한 한 많은 거래들을 승인하는 것이 바람직하다.

[0068] 이 문제에 대한 솔루션은 잠재적인 에러를 위한 일정한 마진(margin)이 있도록 거래 카운터의 범위를 넓히는 것[또는 시간, 날짜 등과 같은 어떤 다른 가변 데이터의 허용한계(tolerance)를 넓히는 것]을 포함할 수 있다. 예를 들어, 소비자의 휴대용 소비자 디바이스는 그 안에 현재 총 거래 100을 가지는 카운터를 가질 수 있다. 그 소비자가 POS 단말기에서 거래를 행하는 경우에, 인가 메시지가 POS 단말기로부터 발행기의 서버 또는 지불 프로세싱 네트워크의 서버로 보내질 수 있다. 그 인가 메시지는 이것이 소비자 A에 대하여 거래 번호 100이라는 것을 지시할 수 있다. 그러면 발행기의 서버는 상응하는 카운터 범위를 체크한다. 수신된 거래 카운터가 발행기에 의해 결정된 상응하는 카운터 범위 내에 들면, 그 거래는 승인된다. 예를 들어, 그 상응하는 카운터 범위는 98과 102 사이일 수 있다. 소비자의 카운터가 100이어서 98과 102 사이에 들기 때문에, 그 거래는 승인된다. 이와 같이, 발행기의 서버에 있는 카운터가 소비자의 휴대용 소비자 디바이스 상의 카운터와 약간 상이한 값을 가지더라도, 그 거래는 부주의로 인해 거절되지 않을 것이다. 실제의 데이터 조작이 발생하거나 소비자의 지불 계좌 번호가 인가없이 사용되고 있는 경우에는, 발행기 서버 측의 카운터가 소비자의 휴대용 소비자 디바이스 상의 실제 카운터와 현격하게 상이할 것이다.

[0069] 본 발명의 이러한 실시예들은 잘못된 거래 거부들의 수를 감소시키는 것을 도울 수 있다. 대안적인 또는 추가적인 인증 조치로서, POS 단말기로부터 수신된 거래 카운터와 발행기의 서버 측의 거래 카운터가 매칭되지 않는다는 것을 발행기의 서버가 발견한 경우에 또는 그 카운터가 발행기의 서버 컴퓨터에 의해 결정된 소정의 카운터 범위 내에 들지 않는 경우에, 발행기는 소비자에게 시험 질문[예컨대, 당신의 생일은 언제입니까?]을 제공할 수 있다. 소비자가 그 시험 질문에 대해 정확하게 대답하면, 그 거래는 승인된다. 질문이 정확하게 대답되지 않으면, 그 거래는 승인되지 않는다. 그러한 실시예들에서 이용될 수 있는 가능한 시험 메시지들과 시험 질문들에 관한 추가적인 상세들은 아래에서 제공된다.

[0070] 다른 실시예들에서, 카운터[또는 다른 동적인 데이터 엘리먼트]가 소정의 범위 내에 드는 경우에, 추가적 인증 프로세싱[예컨대, 소비자에게 시험 질문을 보냄]을 실행할 것인지 아니면 추가적 인증 프로세싱을 실행하지 않을 것인지에 관한 결정은 다른 인자(factor)들에 기초할 수 있다. 예를 들어, 카운터 또는 동적인 데이터 엘리먼트가 소정의 범위에 들면, 분석되고 있는 거래가 소정의 달러 한계[예컨대, 1000 달러 이상]보다 더 큰 경우 또는 부정한 거래들을 일으키는 경향이 높다는 것을 지시하는 위치 또는 상인으로부터 그 분석되고 있는 거래가 행해지고 있는 경우에만, 추가적 인증 프로세싱이 발생할 수 있다. 따라서, 본 발명의 실시예들은 추가적인 인증 프로세싱을 실행할 것인지 아닌지를 결정하는 때에 고려될 수 있는 다른 변수들을 포함할 수 있다.

[0071] 검증 값들과 함께 사용되는 동적인 데이터 엘리먼트들과 관련하여 범위들을 사용하는 실시예들에 관한 추가 상세들이 본 출원과 동일한 날에 "Verification Error Reduction System"이라는 명칭으로 출원된 미국 특허출원[대리인 문서 번호: 16222U-031800US]에 있다. 그 미국 특허출원은 모든 목적들을 위해 그 전체로서 참조에 의해 여기에 병합된다.

[0072] D. dCVV들을 생성할 수 있는 휴대용 소비자 디바이스들

[0073] 카운터들과 같은 가변적인 거래 데이터를 제공할 수 있는 여러 상이한 휴대용 소비자 디바이스들이 생성될 수 있다. 이런 종류의 휴대용 소비자 디바이스의 예시는 마그네틱-스트라이프 카드(magnetic-stripe card)를 포함한다. 마그네틱-스트라이프 카드는 그것의 마그네틱 스트라이프 상에 제공된 데이터를 재기록할 수 있다. 마그

네틱 기록 헤드(magnetic write head)와 같은 재기록 디바이스(re-writing device)는 마그네틱 스트라이프 상의 데이터를 재기록하는 데 사용될 수 있다. 모든 목적들을 위해 그 전체로서 참조에 의해 여기에 병합되는 미국 특허 제7,044,394호가 그런 타입의 카드를 설명하는 특허이다. 그 카드 내에 배터리(battery)가 있고 그 배터리는 재기록 디바이스를 위한 전원을 공급할 수 있다.

[0074] 지불 카드들에서 배터리들의 사용이 일부의 경우들에서는 특히 바람직하지 않다. 예를 들어, 배터리들은 대체되어야 하며 사용환경에 어울리는 방식으로 배치되어야 한다. 또한, 배터리-전원공급 카드가 어느 주어진 순간에 충분한 전력을 가지지 못하면, 그 카드에 의해 행해지는 특정한 거래가 의도된 대로 발생되지 않을 수 있다. 게다가, 소비자가 그의 지갑에 다수의 배터리-전원공급 카드들을 가지는 경우에는, 비행기 여행 중에 이것이 잠재적인 보안 이슈들을 일으킬 수 있다. 따라서, 배터리 없는 카드들이 선호된다.

[0075] 일부 실시예들에서, 휴대용 소비자 디바이스들은 카운터를 구비할 수 있는 칩(chip)을 포함하는 배터리 없는 카드들[또는 다른 배터리 없는 형태의 인자들]이다. 이 배터리 없는 카드들은 내부 배터리 대신에 어떤 외부 전원에 의해 전원공급된다. 외부 전원들의 예시들은 POS 단말기들과 거래 계산기들과 같은 액세스 디바이스들을 포함한다. 본 발명의 실시예들에서, 배터리 없는 카드들이 POS 단말기와 같은 외부 전원에 의해 전원공급될 때마다, 카운터 값[또는 다른 가변적인 데이터]이 그 배터리 없는 카드에 의해 생성될 수 있다. 여러 구체적인 실시예들이 도 3a 내지 도 3c에 도시되어 있다.

[0076] 도 3a는 플라스틱 몸체{202(a)}를 포함하는 마그네틱 스트라이프 카드(202)를 보여준다. 마그네틱 스트라이프{202(e)}는 플라스틱 몸체{202(a)} 상에 있다. 플라스틱 몸체{202(a)}는 카드 소지자의 이름과 같은 정보를 가질 수 있는 엠보싱된 영역(embossed region), 카드 번호 및 만료일(미도시)을 포함할 수 있다. 프로세서{202(b)}[예컨대, 마이크로프로세서]가 플라스틱 몸체{202(a)} 상에 있고, 판독-기록 디바이스{202(d)}와 안테나{202(c)}가 프로세서{202(b)}에 접속된다. 이 예시에서, 안테나{202(c)}는 비접촉 카드 판독기(미도시)로부터 전력을 수신할 수 있는 코일 와이어(coil of wire)이다.

[0077] 사용 중에, 안테나{202(c)}는 마그네틱 스트라이프 카드(202)가 외부의 비접촉 판독기(미도시)와 통신할 수 있도록 하여, 계좌 번호 및 옵션으로 카운터 정보[또는 다른 가변적인 데이터]가 마그네틱 스트라이프{202(e)}로부터 프로세서{202(b)}와 판독-기록 디바이스{202(d)}를 통해 얻어질 수 있도록 한다. 동시에, 안테나{202(c)}는 판독-기록 디바이스{202(d)}가 마그네틱 스트라이프{202(e)} 상의 동적인 데이터[예컨대, 카운터]를 변경할 수 있도록, 일시적으로 프로세서{202(b)}와 판독-기록 디바이스{202(d)}에 전원을 공급하는 데 또한 사용될 수 있다. 이와 같이, 이 예시에서 설명되듯이, 본 발명의 실시예들은 휴대용 소비자 디바이스 인증 거래에서 사용될 수 있는 동적인 데이터를 제공할 수 있는 배터리 없는 마그네틱-스트라이프 카드를 사용하는 것을 포함할 수 있다.

[0078] 도 3a에서의 예시가 마그네틱 스트라이프{202(e)}에 대한 판독-기록 디바이스{202(d)}를 포함하고 있지만, 다른 실시예들에서 판독-기록 디바이스는 플래쉬 메모리 칩 등과 같은 휘발성 또는 반-휘발성 반도체이용 메모리 디바이스(volatile or semi-volatile solid-state memory device)에 데이터를 기록 및/또는 판독할 수 있는 로직으로 구현될 수 있다.

[0079] 본 발명의 다른 하나의 카드 실시예(204)가 도 3b에 도시되어 있다. 도 3a 및 도 3b에서, 비슷한 참조 번호들은 비슷한 엘리먼트들을 가리킨다. 그러나, 도 3b에는 전도성 접촉 영역{202(f)}이 도시되어 있고, 안테나 대신에 그 전도성 접촉이 프로세서{202(b)}에 접속된다. 이 예시에서, 접촉 영역{202(f)}은 그것이 카드 판독기(미도시)에서의 상응하는 접촉 영역과 인터페이스하고 전기적으로 접촉할 수 있도록 다수의 전기적 접촉들을 포함할 수 있다. 카드(204)가 사용되는 경우에, 전력은 전도성 접촉{204(f)}을 통해 프로세서{202(b)}로 공급될 수 있고, 판독-기록 디바이스{202(d)}는 위에서 설명한 바와 같이 기능할 수 있다.

[0080] 도 3c는 본 발명의 일 실시예에 따른 다른 하나의 마그네틱 스트라이프 카드(206)를 보여준다. 그것은 인터페이스 영역{202(g)}과 같은 휴대용 소비자 디바이스 판독기 인터페이스 영역을 포함한다. 인터페이스 영역{202(g)}은 위에서 설명된 안테나{202(c)} 형태 또는 전기적 전도성 접촉{202(f)} 형태를 취할 수 있다. 전력은 위에서 설명된 바와 같이 인터페이스 영역{202(g)}을 통해 프로세서{202(b)}와 판독-기록 디바이스{202(d)}로 공급될 수 있다.

[0081] 그러나, 이 실시예에서, 반-정적 디스플레이{semi-static display. 202(h)}가 프로세서{202(b)}에 접속된다. 구매 거래 동안에 프로세서{202(b)}가 카드 판독기에 의해 전원공급될 때마다, 프로세서{202(b)}는 디스플레이{202(h)}가 동적인 카드 검증 값(dCVV: dynamic card verification value)과 같은 검증 값을 디스플레이하도록

할 수 있다. 그 dCVV는 소비자에게 보여질 수 있고, 소비자가 진정한 카드를 가진다는 것을 검증하기 위해서 메일 지시, 전화기 또는 인터넷 구매 거래(mail order, telephone, or Internet purchase transaction)에서 사용될 수 있다. 이 예시에서, 동일한 또는 상이한 dCVV 값[또는 다른 동적인 데이터]이 카드 판독기로 전기적으로 전송될 수 있고, 후속하여 추가적인 검증을 위해 인가 요청 메시지 내에서 발행기로 전송될 수 있다.

[0082] 도 4는 도 3a 내지 도 3c에 도시된 타입의 카드들로 전원을 공급하는 데 이용될 수 있는 보안 디바이스(300)를 보여준다. 보안 디바이스(300)는 하우징{300(a)} 상에 데이터 입력 영역{300(b)}[예컨대, 키(key)들]을 가질 수 있다. 하우징{300(a)}은 위에서 설명된 바와 같은 배터리 없는 카드를 받을 수 있는 슬롯{300(d)}을 규정할 수 있다. 또한 하우징{300(a)} 상에 디스플레이{300(c)}가 존재한다.

[0083] 보안 디바이스(300)는 마이크로프로세서, 배터리들 및 메모리를 포함할 수 있다. 그 메모리는 소비자 구매 거래를 위해 일회용 거래 코드 또는 번호를 생성하기 위한 컴퓨터 코드를 구비한다. 또한 일회용 거래 코드를 생성하기 위한 로직은 카드를 소지하고 있는 사람이 사실상 인가된 카드 소지자라는 것을 발행기, 상인 또는 다른 당사자가 검증할 수 있도록 다른 서버 또는 컴퓨터[예컨대, 발행기의 서버] 상에 존재할 수 있다. 이 예시에서, 보안 디바이스(300)는 견고한 보안 토큰(hard security token)으로서의 특징을 가질 수 있고, 소비자를 인증하는 것을 돕는 데 사용될 수 있다.

[0084] 사용 동안에, 소비자는 위에서 설명된 바와 같은 배터리 없는 마그네틱 스트라이프 카드를 슬롯{300(d)}에 삽입할 수 있다. 그러면 일회용 거래 코드가 스크린{300(c)} 상에 디스플레이될 수 있다. 카드가 보안 디바이스(300)에 삽입되는 경우에, 보안 디바이스(300)에서의 전원으로부터의 전력이 카드에서의 프로세서와 판독-기록 디바이스에 전원을 공급하여 그 카드 상의 동적인 데이터[예컨대, 카운터]가 변경될 수 있도록 한다. 이와 같이, 보안 디바이스(300)는 거래에 대한 일회용 거래 번호를 생성할 수 있고, 또한 배터리 없는 카드에 일시적으로 전력을 공급하여 그 카드에서 카운터[또는 다른 동적인 엘리먼트]가 변경될 수 있도록 한다. 동적인 데이터를 가질 수 있는 배터리 없는 카드와 보안 디바이스(300) 양자 모두를 사용하는 시스템은 휴대용 소비자 디바이스와 소비자 양자 모두를 유리하게 인증할 수 있다.

[0085] 배터리 없는 휴대용 소비자 디바이스들을 사용하는 실시예들에 관한 추가 상세들이 본 출원과 동일한 날에 "Batteryless Portable Consumer Device"라는 명칭으로 출원된 미국 특허출원[대리인 문서 번호: 16222U-031700US]에 있다. 그 미국 특허출원은 모든 목적들을 위해 그 전체로서 참조에 의해 여기에 병합된다.

[0086] E. 마스킹된 주요 계좌 번호들{Masked PANs(primary account numbers)}

[0087] 휴대용 소비자 디바이스를 인증하는 다른 하나의 방식은 마스킹된 PAN 또는 주요 계좌 번호(primary account number)를 사용하는 것이다. 이 예시에서, 전송된 PAN의 일부분이 마스킹되거나 동적으로 변경된다. PAN은 BIN 번호 또는 은행 식별 번호(bank identification number)와 같은 식별 번호 부분을 포함한다. 식별 번호 부분들의 다른 예시들은 상인 위치, 금융 기관 위치, 또는 심지어 IP 주소를 포함한다. PAN 및 BIN 번호의 마지막 4 디지트(digit)들은 동일하게 유지될 것이며, 반면에 PAN에서 다른 번호들은 변경된다. 동적으로 변경되는 이 번호들은, 소비자가 이상하게 생각하지 않도록, 소비자가 수령하는 지불 카드 영수증 상에서 전형적으로 마스킹된다(masked).

[0088] 도 5는 구매 거래에서 상인으로부터 발행기로 전송되는 데이터에 대한 데이터 필드들의 개략도를 보여준다. 그 데이터 필드는 PAN, 만료일, 서비스 코드, PIN CVV 및 임의의 데이터 필드들(discretionary data fields)을 포함한다.

[0089] 휴대용 소비자 디바이스에서의 메모리[예컨대, 마그네틱 스트라이프]에 존재할 수 있는 예시적인 PAN(380)이 도 6에 도시되어 있다. 이 예시에서, PAN(380)의 처음의 6 디지트들[즉, 처음 말단 부분] "123456"{380(a)}은 BIN 번호에 상응할 것이다. 다음의 6 디지트들{380(b)}은 변경될 수 있거나 실제 PAN의 6 디지트들과 상이할 수 있고, 이 예시에서 "XXXXXX"로 표시되어 있다. 마지막의 4 디지트들{380(c)}[즉, 마지막 말단 부분]은 이 예시에서 "9999"이고, 동일하게 유지될 것이다. BIN을 동일하게 유지하고 마지막의 4 디지트들을 동일하게 유지함으로써, 거래는 상인 및 소비자에게 실제의 거래처럼 보일 것이다. 바람직한 실시예에서, 중간의 6 디지트들은 카운터 등을 이용하여 동적으로 변경된다. 이것은 어떤 비인가된(unauthorized) 사람이 실제의 PAN을 결정하는 것을 더욱 더 어렵게 한다.

[0090] 일 실시예에서, 휴대용 소비자 디바이스의 메모리에 존재하는 PAN의 중간 부분은 실제 PAN의 중간 부분과 상이할 것이다. 메모리에 존재하는 PAN은 제2의 PAN으로 언급될 수 있고, 반면에 실제의 PAN은 제1의 PAN으로 언급

될 수 있다. 적당한 알고리즘 또는 룩-업 테이블[예컨대, 발행기에 저장되거나 POS 디바이스와 같은 액세스 디바이스에 저장된]이 제1의 PAN과 제2의 PAN을 링크하는 데 이용될 수 있다. 예를 들어, PAN 번호의 중간 6 디지트들이 제1의 PAN[예컨대, 1234566666669999]에서는 666666일 수 있고, 반면에 중간 6 디지트들이 소비자의 휴대용 소비자 디바이스에 있는 메모리에 저장된 제2의 PAN[예컨대, 1234562222229999]에서는 222222일 수 있다. 일 실시예에서, 제2의 PAN은 POS 단말기에서 수신될 수 있고, 그 POS 단말기는 그 제2의 PAN을 제1의 PAN으로 변환할 수 있으며, 그 제1의 PAN은 프로세싱 및/또는 인가를 위해 POS 단말기로부터 발행기로 전송될 수 있다. 다른 하나의 실시예에서, 제2의 PAN은 발행기로 전송될 수 있고, 그 발행기는 그 제2의 PAN을 제1의 PAN으로 변환할 수 있으며 그 이후에 거래를 처리 및/또는 인가할 수 있다.

[0091] 이 실시예에서, 발행기는 사용되고 있는 휴대용 소비자 디바이스가 진정하다는 것을 검증하기 위해서 제1의 PAN과 제2의 PAN 양자 모두를 수신할 수 있다. 비인가된(unauthorized) 사람이 제1의 PAN을 사용하려고 하는 경우에, 그 비인가된 사람은 제2의 PAN을 알지 못할 것이고 그 제2의 PAN을 알지 못하고는 구매 거래를 부정하게 행하지 못할 것이다. 대안적으로, 비인가된 사람이 제2의 PAN을 전기적으로 가로채거나(intercept) "조작하는(skim)" 경우에, 그 비인가된 사람은 제1의 PAN을 알지 못하고는 구매 거래를 행할 수 없을 것이다.

[0092] 다른 하나의 실시예에서, PAN의 중간 부분은 동적으로 변경될 수 있다. 예를 들어, 휴대용 소비자 디바이스가 사용되는 때마다 PAN의 중간 부분을 동적으로 변경시키기 위해서 적당한 알고리즘 또는 카운터가 사용될 수 있다. 비인가된 사람이 PAN을 전기적으로 가로채고 제1의 PAN을 알더라도, 제2의 PAN은 동적으로 변경될 것이다. 비인가된 사람이 제1의 PAN을 알고 제2의 PAN을 한번 가로챘더라도, 그 가로챈 제2의 PAN은 쓸모없을 것이다. 왜냐하면 그것이 동적으로 변경되는 제2의 PAN이기 때문이다. 이 경우에, 그 비인가된 사람은 제1의 PAN 및 제2의 PAN과 함께 PAN을 동적으로 변경하는 데 이용된 알고리즘을 알아내야 한다. 따라서, 이 실시예는 특히 안전한 거래들을 행하는 데 유용하다.

[0093] 마스킹된 주요 계좌 번호들을 이용하는 실시예들에 관한 추가 상세들이 2007년 6월 12일에 "Track Data Encryption"이라는 명칭으로 출원된 미국 특허출원 제11/761,821호에 있다. 그 미국 특허출원은 모든 목적들을 위해 그 전체로서 참조에 의해 여기에 병합된다.

[0094] VI. 소비자 인증

[0095] 위에서 언급한 바와 같이, 여러 소비자 인증 프로세스들이 본 발명의 실시예들에서 이용될 수 있다. 소비자의 인증을 향상시키기 위한 가능한 방식들의 구체적인 예시들은 다음을 포함한다.

[0096] - 지식 기반 시험 응답들(Knowledge-based challenge-responses)

[0097] - 하드웨어 토큰들(Hardware tokens) [다중 솔루션 옵션들]

[0098] - 일회용 패스워드(OTP: one time passwords) [한정된 용도]

[0099] - AVS [독립형 솔루션으로서는 아님]

[0100] - 서명들(Signatures)

[0101] - 소프트웨어 토큰(Software token)

[0102] - PIN들 [온라인/오프라인]

[0103] - 사용자 ID들/패스코드들(User IDs/Passcodes)

[0104] - 전화기를 통한 2 채널 인증

[0105] - 생체인식(Biometrics)

[0106] 위에서 설명하였듯이, 다양한 메커니즘들이 소비자를 인증하는 데 이용될 수 있고, 그 메커니즘들은 사용자 입력 없음[예컨대, 자동-소프트웨어 보안 토큰(auto-software security token)], 한정된 사용자 입력[예컨대, 사용자가 버튼을 누름], 또는 완전 사용자 입력[예컨대, 생체인식(biometrics)]을 이용할 수 있다.

[0107] 또한, 다양한 "보안 토큰들(security tokens)"이 사용자를 인증하는 것을 돕는 데 이용될 수 있다. 보안 토큰은 실제의 정보나 데이터를 검증하는 데 이용될 수 있는 한 항목의 정보 또는 한 조각의 정보이다. 예를 들어, PIN

이 보안 토큰일 수 있고 소비자가 거래를 행하는 때에 소비자의 신원을 검증하는 데 이용될 수 있다. 다른 하나의 예시에서, 시험 질문과 상응하는 대답이 소비자를 인증하는 것을 돕는 보안 토큰으로 고려될 수 있다. 후자의 예시가 "양-방향 채널(bi-directional channel)"을 가지는 토큰의 예시이며, 정보가 소비자에게 흐르고 그 소비자는 그 자신이 인증될 수 있도록 발행기와 같은 다른 당사자에게 정보를 되보낸다.

[0108] A. 지식 기반 시험들(Knowledge based challenges)

[0109] 본 발명의 실시예들에서, 상인, 지불 프로세싱 조직, 발행기, 또는 다른 어떤 적당한 실체(entity)는 소비자를 인증하기 위해서 그 소비자에게 시험 질문들을 제기할 수 있다. 그 시험 질문들은 정적(static)일 수도 있고[정적인 경우에는 각 구매 거래에 대하여 동일한 질문들을 물음] 동적(dynamic)일 수도 있다[동적인 경우에는 매번 상이한 질문들을 물을 수 있음].

[0110] 묻는 질문들은 또한 정적(static) 또는 동적(dynamic)[반-동적(semi-dynamic) 또는 완전 동적(fully dynamic)] 대답들을 가질 수 있다. 예를 들어, 질문 "당신의 생일은 언제입니까?"는 정적인 대답을 요구한다. 왜냐하면 그 대답이 변하지 않기 때문이다. 질문 "당신의 지프-코드(zip-code)는 무엇입니까?"는 반-동적인 대답을 요구한다. 왜냐하면 그것은 변할 수 있지만 드물게 변할 수 있기 때문이다. 마지막으로, 질문 "당신은 어제 오후 4시에 무엇을 구매하였습니까?"는 동적인 대답을 요구한다. 왜냐하면 그 대답은 빈번히 변하기 때문이다. 이와 같이, 바람직한 실시예들에서, 시험 질문들은 바람직하게 발행기가 소유하고 있을 것 같은 "실 시간(real time)" 정보에 근거할 수 있다. 예를 들어, 소비자는 "당신은 지난 밤에 멕시코 식당에서 외식하였습니까?"와 같은 좀 더 구체적인 질문을 받을 수 있다. 좀 더 구체적인 지식에 기반하는 소비자 시험들을 제공함으로써, 소비자에 대한 인증이 보증된다.

[0111] 일 실시예에서, 본 방법은 휴대용 소비자 디바이스를 사용하는 구매 거래와 같은 거래를 행하는 단계를 포함한다. 그 휴대용 소비자 디바이스는 신용 카드 또는 그 종류의 다른 것일 수 있다. 그 구매 거래는 매장 단말기(point of sale terminal)와 같은 액세스 디바이스를 가지는 상인 측에서 발생할 수 있다.

[0112] 소비자는 매장 단말기와 같은 액세스 디바이스와 상호작용하여 프로세스를 개시하기 위해 휴대용 소비자 디바이스를 사용할 수 있다. 매장 단말기는 개시하여 인가 요청 메시지를 생성할 수 있고, 그 인가 요청 메시지는 이후 지불 프로세싱 네트워크로 그리고 후속적으로 그 휴대용 소비자 디바이스의 발행기로 보내질 수 있다. 지불 프로세싱 네트워크 또는 발행기에 의해 인가 요청 메시지가 수신되면, 그것은 분석된다. 그러면 특성상 동적 또는 반-동적일 수 있는 시험 메시지(challenge message)가 생성되어 그 소비자에게 보내진다. 그 시험 메시지는 액세스 디바이스로 또는 소비자의 휴대용 소비자 디바이스[예컨대, 그 휴대용 소비자 디바이스가 이동 전화기인 경우]로 되보내질 수 있다.

[0113] 그러면 소비자는 그 시험 메시지에 대한 응답을 제공한다. 그 시험 응답 메시지가 소비자로부터 수신된다. 그러면 그 시험 응답 메시지가 검증되고, 그것이 검증되면 그 거래가 인가되는지[예컨대, 그 소비자의 계좌에 충분한 자금이 있는지 또는 그 소비자의 계좌에 충분한 신용이 있는지]를 결정하기 위해 인가 응답 메시지가 분석된다. 그 거래가 인가되면, 발행기 및 지불 프로세싱 네트워크는 그 소비자에게 인가 응답 메시지를 보낸다. 인가 응답 메시지는 그 거래가 인가되는지 아닌지를 지시한다.

[0114] 위와 아래에서 설명되는 구체적인 실시예들에서, 시험 질문들이 상세하게 설명되지만, 본 발명의 실시예들이 그것들만으로 한정되는 것은 아니다. 본 발명의 실시예들은 시험 질문들을 포함할 수 있는 시험 메시지들의 사용에 일반적으로 관련될 수 있다. 일부 실시예들에서는, 아래에서 더 자세하게 설명되듯이, 시험 메시지들이 소비자에 의해 읽혀지거나 읽혀지지 않을 수 있으며, 직접적인 또는 간접적인 방식들로 소비자의 진정성(authenticity)을 시험할 수 있다. 시험 질문들의 예시들은 소비자의 휴대용 소비자 디바이스에 관련되는 질문[예컨대, 당신의 카드 상에 있는 CVV 또는 카드 검증 값(card verification value)은 무엇입니까?], 소비자의 위치에 관련되는 질문[예컨대, 당신의 지프 코드(zip code)는 무엇입니까?], 소비자의 이동 전화기 또는 일반 전화기에 관련되는 질문[예컨대, 당신의 이동 전화기 번호는 무엇입니까?], 소비자의 개인 정보에 관련되는 질문[예컨대, 당신 어머니의 결혼 전 성(maiden name)은 무엇입니까?] 등을 포함한다. 소비자에 의해 구체적으로 대답되는 질문들이 아닌 시험 메시지들의 예시들은 자동적으로 전화기에게 그것의 위치나 전화기 번호에 관해 질문하여 그러한 정보의 복원을 야기하는 메시지들을 포함한다. 시험 메시지의 다른 예시는 전화기에게 코드[또는 다른 인증 토큰(authentication token)]를 공급하는 메시지일 수 있으며, 액세스 디바이스 측에서 그 코드의 사용은 소비자를 인증한다.

[0115] B. 시험 메시지들을 사용하는 시스템들

[0116] 도 7은 본 발명의 일 실시예에 따른 예시적인 시스템(420)을 보여준다. 본 발명의 다른 실시예들에 따른 다른 시스템들은 도 7에 도시된 것보다 다소 많거나 적은 컴포넌트들을 포함할 수 있다.

[0117] 도 7에 도시된 시스템(420)은 상인(422) 및 그 상인(422)에 연관된 획득기(424)를 포함한다. 전형적인 지불 거래에서, 소비자(430)는 휴대용 소비자 디바이스(432)를 사용하여 상인(422) 측에서 상품 또는 서비스들을 구매할 수 있다. 획득기(424)는 지불 프로세싱 네트워크(426)를 통해 발행기(428)와 통신할 수 있다.

[0118] 소비자(430)는 개인, 또는 상품이나 서비스들을 구매할 수 있는 사업체와 같은 조직일 수 있다. 다른 실시예들에서, 소비자(430)는 단순히 금전 전송 거래와 같은 어떤 다른 타입의 거래를 행하고자 하는 사람일 수 있다. 옵션으로 소비자(430)는 무선 전화기(435)를 작동시킬 수 있다.

[0119] 휴대용 소비자 디바이스(432)는 어떤 적당한 형태에 있을 수 있다. 적당한 휴대용 소비자 디바이스들이 위의 도 1[예컨대, 휴대용 소비자 디바이스 32]에 설명되어 있다.

[0120] 지불 프로세싱 네트워크(426)는 도 1에서의 지불 프로세싱 네트워크(26)와 유사하거나 상이할 수 있다. 도 7에 도시된 바와 같이, 지불 프로세싱 네트워크(426)는 시험 질문 엔진(challenge question engine){426(a)-1}을 구비할 수 있는 서버{426(a)}를 구비할 수 있다. 또한 그 서버{426(a)}는 거래 이력 데이터베이스{426(b)} 및 시험 질문 데이터베이스{426(c)}와 통신할 수 있다. 아래에서 더 자세하게 설명되는 바와 같이, 시험 질문 엔진{426(a)-1}은 시험 질문 데이터베이스{426(c)}로부터 시험 질문들을 단순히 추출할 수 있다. 대안적으로 또는 추가적으로, 시험 질문 엔진{426(a)-1}은 거래 이력 데이터베이스{426(b)}에 있는 정보를 이용하여 시험 질문들을 생성할 수 있다.

[0121] 아래에서 더 자세하게 설명되듯이, 시험 질문들은 특성상 정적(static) 또는 동적(dynamic)일 수 있다. 예를 들어, 시험 질문 엔진{426(a)-1}은 인가 요청 메시지를 수신할 수 있고, 그 인가 요청 메시지는 구매량뿐만 아니라 소비자의 계좌 번호를 포함할 수 있다. 그러면 그것은 소비자의 계좌 번호 및 그 소비자의 계좌 번호와 연관된 어떤 소비자 정보를 찾을 수 있다. 이후 그것은 시험 질문 데이터베이스{426(c)}로부터 적당한 질문들을 복원하거나 스스로 적당한 시험 질문들을 생성할 수 있다. 예를 들어, 일부의 경우들에서, 시험 질문 엔진{426(a)-1}은 인가 요청 메시지를 수신한 후에 시험 질문 데이터베이스{426(c)}로부터 질문 "당신의 이동 전화기 번호는 무엇입니까?"를 복원할 수 있다. 대안적으로, 시험 질문 엔진{426(a)-1}은 "당신은 지난 밤에 맥도날드에서 이 신용 카드를 사용했습니까?"와 같은 동적인 질문을 생성할 수 있다. 지난 밤에 소비자(420)가 있었던 특정 식당에 관계되는 정보는 거래 이력 데이터베이스{426(b)}로부터 복원될 수 있다.

[0122] 시험 질문 데이터베이스{426(c)}에는 어떤 적당한 타입의 질문들이 담겨져 있을 수 있다. 그 질문들은 지난 위치[예컨대, 소비자의 현재 집, 소비자가 최근에 방문했던 도시] 또는 현재 위치[예컨대, 현재 소비자가 있는 가게의 현재 위치], 소비자가 지금 방문하고 있거나 과거에 방문했던 상인의 타입 또는 이름, 소비자의 가족 또는 개인 데이터[예컨대, 이름, 전화기 번호, 사회 보안 번호 등] 등에 관련될 수 있다. 시험 질문 데이터베이스{426(c)}에 있는 질문들은 시험 질문 엔진{426(a)-1}에 의해 생성되어 후속적으로 시험 질문 데이터베이스{426(c)}에 저장될 수 있다.

[0123] 대안적으로 또는 추가적으로, 시험 질문들은 외부 소스(external source)로부터 생성되어 후속적으로 시험 질문 데이터베이스{426(c)}에 저장될 수 있다. 예를 들어, 소비자(430)는 구체적인 시험 질문들을 인터넷과 같은 통신 매체(미도시)를 통해 서버{426(a)}로 공급하기 위해 개인 컴퓨터 상의 브라우저(browser) 등을 이용할 수 있다.

[0124] 일부 실시예들에서, 소비자는 그에게 또는 그녀에게 물어지는 시험 질문들의 종류들 및/또는 양을 결정할 수 있다. 예를 들어, 소비자는 소비자가 보석 가게를 방문할 경우에는 3 개의 시험 질문들이 물어지기를 원하지만 소비자가 패스트푸드 식당을 방문할 경우에는 단지 하나의 시험 질문이 물어지기를 원한다는 것을 규정할 수 있다. 소비자에 의해 제기되는 질문들의 타입들은 상인 타입, 구매 빈도 등에 근거할 수 있다. 사용자-정의 인가 파라미터들에 관련하는 일부 개념들은 모든 목적들을 위해 그 전체로서 참조에 의해 여기에 병합되는 미국 특허 출원 제10/093,002호[2002년 3월 5일 출원됨]에 설명되어 있다.

[0125] 바람직한 실시예들에서, 시험 질문들은 거래 이력 데이터베이스{426(b)}에 있는 지난 거래 데이터로부터 도출된다. 소비자(430)는 매번 지불 프로세싱 네트워크(26)[및/또는 발행기(428)]에 의해 많은 거래들을 행할 수

있다. 이 소비자 거래 정보는 매번 거래 이력 데이터베이스{426(b)}에 저장될 수 있고, 시험 질문들은 그 거래 정보를 이용하여 생성될 수 있다. 지난 거래 정보는 소비자(430)를 인증하기 위한 좋은 토대를 제공한다. 왜냐하면 소비자(430)는 소비자(430)가 과거에 행한 거래들에 대해서 알 것이기 때문이다. 예를 들어, 소비자(430)가 이전 날에 뉴욕에서 호텔 방에 대하여 지불하기 위해서 그의 신용 카드를 사용했을 수 있고, 다음날에 그 소비자는 "당신은 어제 뉴욕에서 호텔에 머물렀습니까?"와 같은 질문을 받을 수 있다. 다른 예시에서, 소비자(430)가 이전 날에 2000 달러 이상의 아이템을 구매했을 수 있고, 다음날에 그 소비자는 "당신은 어제 2000 달러 이상의 구매를 했습니까?"라는 질문을 받을 수 있다. 소비자(430)에게 제시되는 질문들/대답들은 특성상 자유 형태일 수 있거나, 소비자가 선택할 수 있는 다중 선택(multiple choice) 또는 참-거짓 대답(true-false answer)들과 같은 미리-정해진(pre-formatted) 대답들을 포함할 수 있다.

[0126] 상인(422)은 휴대용 소비자 디바이스(432)와 상호작용할 수 있는 액세스 디바이스(434)를 가지거나 그 액세스 디바이스로부터 통신들을 수신할 수 있다. 적당한 타입들의 액세스 디바이스들이 위에서 설명되어 있다[예컨대, 도 1에서의 액세스 디바이스 34].

[0127] 액세스 디바이스(434)가 매장 단말기이면, 어떤 적당한 매장 단말기가 카드 판독기들을 포함하여 사용될 수 있다. 카드 판독기들은 어떤 적당한 접촉 동작 모드 또는 비접촉 동작 모드를 포함할 수 있다. 예를 들어, 예시적인 카드 판독기들은 휴대용 소비자 디바이스들(432)과 상호작용하기 위해 RF(radio frequency) 안테나들, 마그네틱 스트라이프 판독기들 등을 포함할 수 있다.

[0128] 발행기(428)는 소비자(430)와 연관된 계좌를 가질 수 있는 은행 또는 다른 조직일 수 있다. 발행기(426)는 시험 질문 엔진{428(a)-1}을 가질 수 있는 서버{428(a)}로 동작할 수 있다. 거래 이력 데이터베이스{426(b)}와 시험 질문 데이터베이스{428(c)}는 서버{428(a)}와 통신할 수 있다. 발행기 서버{428(a)}, 시험 질문 엔진{428(a)-1}, 거래 이력 데이터베이스{426(b)} 및 시험 질문 데이터베이스{428(c)}는 지불 프로세싱 네트워크 서버{428(a)}, 시험 질문 엔진{428(a)-1}, 거래 이력 데이터베이스{428(b)} 및 시험 질문 데이터베이스{428(c)}와 동일한 방식으로 또는 다른 방식으로 동작할 수 있다. 엘리먼트들 426(a), 426(a)-1, 426(b) 및 426(c)에 관한 위의 설명들은 엘리먼트들 428(a), 428(a)-1, 428(b) 및 428(c)에 적용될 수 있다.

[0129] 본 발명의 실시예들이 위에 설명된 실시예들로 한정되지는 않는다. 예를 들어, 별개의 기능적 블럭들이 발행기, 지불 프로세싱 네트워크 및 획득기에 대하여 도시되었으나, 어떠한 실체들(entities)은 그 기능들의 어떤 적당한 조합 또는 그 기능들 모두를 실행할 수 있으며 본 발명의 실시예들에 포함될 수 있다. 추가적인 컴포넌트들 또한 본 발명의 실시예들에 포함될 수 있다.

[0130] C. 시험 메시지들을 사용하는 방법들

[0131] 본 발명의 실시예들에 따른 방법들이 도 7 및 도 8을 참조하여 설명될 수 있다. 전형적인 구매 거래에서, 소비자(430)는 신용 카드와 같은 휴대용 소비자 디바이스(432)를 사용하여 상인(422)에게서 상품 또는 서비스를 구매한다. 소비자의 휴대용 소비자 디바이스(432)는 상인(422) 측의 매장 단말기{POS(point of sale) terminal}와 같은 액세스 디바이스(434)와 상호작용할 수 있다[단계 502]. 예를 들어, 소비자(430)는 신용 카드를 소지할 수 있고 POS 단말기의 적당한 슬롯(slot)을 통해 그것을 스와이핑(swipe)할 수 있다. 대안적으로, 매장 단말기는 비접촉 판독기일 수 있고, 휴대용 소비자 디바이스(432)는 비접촉 카드와 같은 비접촉 디바이스일 수 있다.

[0132] 제 1 인가 요청 메시지가 획득기(424)로 전달된다. 획득기(424)가 제 1 인가 요청 메시지를 수신한 후에, 그 제 1 인가 요청 메시지는 지불 프로세싱 네트워크(426)로 보내진다[단계 504]. 그러면 제 1 인가 요청 메시지는 지불 프로세싱 네트워크 서버{426(a)}에서 수신되고, 지불 프로세싱 네트워크 서버{426(a)}는 시험(challenge)이 필요한지를 결정한다.

[0133] 시험이 필요한지를 결정하는 데 다양한 기준들이 사용될 수 있다. 예를 들어, 지불 프로세싱 네트워크 서버{426(a)}는 특정 거래가 고가의 거래[예컨대, 1000 달러 이상]이고 따라서 시험이 적당하다고 결정할 수 있다. 다른 예시에서, 지불 프로세싱 네트워크 서버{426(a)}는 현재의 거래에 관해 의심스러운 점이 있다고 결정할 수 있고 그에 따라서 시험이 적당하다고 결정할 수 있다. 예를 들어, 지불 프로세싱 네트워크 서버{426(a)}는 휴대용 소비자 디바이스(432)가 그 소비자의 본래 주(home state)와 상이한 위치에서 현재 사용되고 있으며 그 소비자의 최근 구매 이력이 그 소비자가 여행하고 있지 않다는 것을 암시한다고 결정할 수 있다.

[0134] 그 현재의 거래에 대하여 시험이 적당하다고 결정되면, 시험 질문 엔진{426(a)-1}은 (로컬 또는 원격) 시험 질문을 가져올 수 있다[단계 508]. 일부 실시예들에서, 시험 질문 엔진{426(a)-1}은 시험 질문 데이터베이스

{426(c)}로부터 질문을 복원할 수 있다.

[0135] 이 시점에서, 제 1 인가 요청 메시지를 발행기(426)로 보내지 않고, 지불 프로세싱 네트워크(426)는 제 1 인가 응답 메시지를 상인(422)과 획득기(424)를 거쳐 액세스 디바이스(434)에게 되보낸다[단계 510]. 제 1 인가 응답 메시지는 시험 질문 엔진{426(a)-1}에 의해 이전에 얻어진 시험 요청(challenge request)을 나타내는 데이터를 담고 있을 수 있다. 제 1 인가 응답 메시지는 초기 거절(initial decline)로서의 특징을 가질 수 있다. 왜냐하면 그것은 거래의 승인을 지시하지 않기 때문이다.

[0136] 액세스 디바이스(434)에서 시험 질문이 수신되면, 소비자(430)는 액세스 디바이스(434)에게 시험 응답을 공급한다. 시험 응답은 어떠한 적당한 방식으로[예컨대, 키패드, 비접촉 판독기 등을 통해서] 액세스 디바이스(434)에게 공급될 수 있다. 액세스 디바이스(434)가 시험 응답을 수신하면, 액세스 디바이스(434)는 그 시험 응답을 상인(422)과 획득기(424)를 통해 지불 프로세싱 네트워크 서버{426(a)}로 전달하고, 그것은 그들에 의해 수신된다[단계 512]. 그 시험 응답 메시지는 제 2 인가 요청 메시지의 일부분일 수 있다.

[0137] 그러면 지불 프로세싱 네트워크 서버{426(a)}는 그 시험 응답 메시지를 검증한다[단계 514]. 시험 응답 메시지가 검증되지 않으면, 지불 프로세싱 네트워크 서버{426(a)}는 그 거래가 승인되지 않는다는 것을 지시하는 응답 메시지를 액세스 디바이스(434)로 되보낼 수 있다. 대안적으로 또는 추가적으로, 지불 프로세싱 네트워크 서버{426(a)}는 액세스 디바이스(434)로 다른 시험 질문을 보낼 수 있다. 반면에, 그 시험이 검증되면, 지불 프로세싱 네트워크 서버{426(a)}는 소비자(430)가 지불 프로세싱 네트워크(426)에 의해 제기된 어떤 시험들을 충족했다는 지시와 함께 제 2 인가 요청 메시지를 발행기(428)로 보낼 수 있다[단계 516].

[0138] 발행기(428)가 제 2 인가 요청을 수신한 후에, 발행기(28)는, 발행기 서버{428(a)}를 이용하여, 그 거래가 인가되는지 또는 인가되지 않는지를 결정한다[단계 518]. 소비자(430)가 불충분한 자금 또는 신용을 가지기 때문에 거래가 인가되지 않을 수 있다. 소비자(430)가 충분한 자금 또는 신용을 가지면, 발행기(428)는 그 거래가 인가된다는 것을 지시하는 제 2 인가 응답 메시지를 지불 프로세싱 네트워크(426), 획득기(424) 및 상인(422)을 통해 액세스 디바이스(434)로 되보낼 수 있다[단계 522].

[0139] 그 날의 말미에, 정규의 정산 및 결산 프로세스가 지불 프로세싱 네트워크(426)에 의해 행해질 수 있다. 정산 프로세스는 소비자의 계좌에 부기(posting)하는 것과 소비자의 결산 위치를 조정하는 것을 돕기 위해 획득기와 발행기 간에 금융 상세들(financial details)을 교환하는 프로세스이다. 정산과 결산은 동시에 발생할 수 있다.

[0140] 또한 여러 대안적인 실시예들도 가능하다. 예를 들어, 지불 프로세싱 네트워크(426) 대신에 또는 지불 프로세싱 네트워크(426)와 함께, 발행기(428)는 시험 질문들을 생성하여 그들을 소비자(430)에게 보낼 수 있다. 발행기(428)에 의해 동작되는 시험 질문 엔진{428(b)-1}, 거래 이력 데이터베이스{428(b)} 및 시험 질문 데이터베이스{426(c)}는 위에서 설명된 지불 프로세싱 네트워크(426)에 의해 동작되는 시험 질문 엔진{426(a)-1}, 거래 이력 데이터베이스{426(b)} 및 시험 질문 데이터베이스{426(c)}와 동일한 방식 또는 상이한 방식으로 사용될 수 있다.

[0141] 위에서 설명된 실시예들에서, 지불 프로세싱 네트워크(426)[및/또는 발행기(428)]로 보내지는 두 개의 인가 요청 메시지들이 있다. 이것이 바람직한데 왜냐하면 현존하는 지불 프로세싱 시스템들이 지불 인가 프로세스 동안에 액세스 디바이스(434)와 발행기(428) 사이의 다양한 포인트들에서 설정되는 "타이머들(timers)"을 가지기 때문이다. 그 타이머들은 지불 인가 프로세스 동안에 다양한 이벤트들이 얼마나 오랫동안 발생하여야 하는지를 정한다. 그 타이머들은 획득기(424), 지불 프로세싱 네트워크(426) 및 발행기(428)에서 컴퓨터 코드로서 설정되어 구현될 수 있다. 예를 들어, 획득기(424), 지불 프로세싱 네트워크(426) 및 발행기(428)에서 타이머들은 각각 3초, 6초 및 10초로 설정될 수 있다. 인가 요청 메시지가 그 각각의 시간들 내에 수신되지 않으면, 어떠한 이벤트가 촉발될 수 있다. 예를 들어, 인가 요청 메시지가 발행기(428)에서 10초 내에 수신되지 않으면, 상인(422)은 인가 요청 메시지를 다시 제출할 것을 요청하는 에러 메시지가 액세스 디바이스(434)로 되보내질 수 있다. 인가 프로세스 동안에 그리고 인가 요청 메시지가 발행기(428)에 도달하기 전에 시험 요청이 생성되면, 발행기의 타이머는 에러가 발생했다는 것을 지시하는 이벤트를 촉발할 수 있다. 단일의 인가 프로세스 동안에 시험 요청들 및 응답들을 생성하는 것은 지불 시스템에서 이미 존재하는 타이머들과 잠재적으로 충돌할 수 있다.

[0142] 두 개의 별개 인가 프로세스들에서 적어도 두 개의 인가 요청 메시지들을 사용함으로써, 위에서 설명된 타이머들은 영향을 받지 않아 유리하다. 타이머들은 소비자(430)에게 시험 질문들을 보내도록 변경될 필요가 없다. 이것은 본 발명의 실시예들이 현존하는 지불 기초 구조(payments infrastructure)와 함께 이용될 수 있도록 해주며, 본 발명의 실시예들에서는 광범위한 변경들이 필요하지 않다. 비교적으로, 지불 인가 프로세스 동안에 단일

의 인가 요청 메시지를 이용하여 시험 질문의 복원이 발생하면, 이것은 인가 요청 메시지를 지연시킬 수 있고 지불 프로세싱 시스템에 존재하는 타이머들에서 변경들을 초래할 수 있다.

[0143] 적어도 두 개의 인가 요청 메시지들은 은행 식별 번호(BIN:bank identification number)들, 거래량, 계좌 번호들, 서비스 코드들 등과 같은 정보를 가질 수 있다. 또한 그것들은 행해지고 있는 거래에 대한 동일한 거래량, 및/또는 상이한 거래량을 담고 있을 수 있다. 예를 들어, 제 1 인가 요청 메시지는 실제의 거래량을 가질 수 있고, 제 2 인가 요청 메시지는 제로 달러량(zero dollar amount), 또는 거래량을 갖춘 이전의 인증 요청이 이미 제출되었다는 것을 지시하기 위한 다른 식별자를 가질 수 있다. 일부 실시예들에서는 제 1 및 제 2 인가 요청들을 링크하기 위해서 거래 코드가 사용될 수 있다.

[0144] 도 8에서 설명된 방법은 "닫혀진 채널(closed channel)" 프로세스로서의 특징을 가질 수 있다. 왜냐하면 액세스 디바이스(434)가 시험 질문을 수신하고 그 시험 질문에 대한 응답을 제공하기 때문이다. 그러나, 본 발명의 다른 실시예들은 "열린 채널(open channel)" 솔루션들을 사용할 수 있고, 거기에서는 시험 질문이 제 1 인가 응답 메시지를 보낸 액세스 디바이스 외의 디바이스로 보내질 수 있다.

[0145] 본 발명의 실시예들에 따른 열린 채널 방법들의 예시들은 도 7 및 도 9를 참조하여 설명될 수 있다. 전형적인 구매 거래에서, 소비자(430)는 신용 카드와 같은 휴대용 소비자 디바이스(432)를 사용하여 상인(422)에게서 상품 또는 서비스를 구매한다. 소비자의 휴대용 소비자 디바이스(432)는 상인(422) 측의 매장(POS: point of sale) 단말기와 같은 액세스 디바이스(434)와 상호작용할 수 있다[단계 602]. 예를 들어, 소비자(30)는 신용 카드를 소지할 수 있고 POS 단말기의 적당한 슬롯(slot)을 통해 그것을 스와이핑(swipe)할 수 있다. 대안적으로, 매장 단말기는 비접촉 판독기일 수 있고, 휴대용 소비자 디바이스(432)는 비접촉 카드와 같은 비접촉 디바이스일 수 있다.

[0146] 제 1 인가 요청 메시지가 획득기(424)로 전달된다. 제 1 인가 요청 메시지가 수신된 후에, 그 제 1 인가 요청 메시지는 지불 프로세싱 네트워크(426)로 보내진다[단계 604]. 그 제 1 인가 요청 메시지는 지불 프로세싱 네트워크 서버{26(a)}에서 수신되고, 지불 프로세싱 네트워크 서버{426(a)}는 시험(challenge)이 필요한지를 결정한다.

[0147] 시험이 필요한지를 결정하는데 다양한 기준들이 사용될 수 있다. 예를 들어, 지불 프로세싱 네트워크 서버{426(a)}는 특정 거래가 고가의 거래[예컨대, 1000 달러 이상]이고 따라서 시험이 적당하다고 결정할 수 있다. 다른 예시에서, 지불 프로세싱 네트워크 서버{426(a)}는 현재의 거래에 관해 의심스러운 점이 있다고 결정할 수 있고 그에 따라서 시험이 적당하다고 결정할 수 있다.

[0148] 그 현재의 거래에 대하여 시험이 적당하다고 결정되면, 시험 질문 엔진{426(a)-1}은 (로컬 또는 원격) 시험 질문을 가져올 수 있다[단계 608]. 일부 실시예들에서, 시험 질문 엔진{426(a)-1}은 시험 질문 데이터베이스{426(c)}로부터 질문을 복원할 수 있다.

[0149] 제 1 인가 요청 메시지를 발행기(426)로 보내지 않고, 그리고 제 1 인가 응답 메시지를 액세스 디바이스(434)로 되보내지 않고, 지불 프로세싱 네트워크(426)는 제 1 인가 응답 메시지를 소비자의 이동 전화기(435) 또는 다른 타입의 액세스 디바이스로 되보낸다[단계 610]. 제 1 인가 응답 메시지는 소비자의 이동 전화기(435)로 되보내질 수 있다. 이것은 직접적으로 또는 어떤 중간 실체(intermediate entity)를 통해 행해질 수 있다. 제 1 인가 응답 메시지는 시험 질문 엔진{426(a)-1}에 의해 이전에 얻은 시험 요청(challenge request)을 나타내는 데이터를 담고 있을 수 있다. 제 1 인가 응답 메시지는 초기 거절(initial decline)로서의 특징을 가질 수 있다. 왜냐하면 그것은 거래의 승인을 지시하지 않기 때문이다.

[0150] 이동 전화기(435)에서 시험 질문이 수신되면, 소비자(430)는 액세스 디바이스(434)에 시험 응답을 공급한다[단계 612]. 그러면 액세스 디바이스(434)는 그 시험 응답을 상인(422)과 획득기(424)를 통해 지불 프로세싱 네트워크 서버{426(a)}로 전달하고, 그것은 그들에 의해 수신된다[단계 614]. 그 시험 응답 메시지는 제 2 인가 응답 메시지의 일부분일 수 있다.

[0151] 소비자가 능동적으로 대답하는 시험 질문들이 상세하게 설명되었으나, 다른 타입의 시험 요청들이 이동 전화기(435)로 보내질 수도 있음을 주의한다. 예를 들어, 일부 경우들에서, 시험 요청들은 소비자(430)에 의해 능동적으로 제공되는 대답을 필요로 하지 않을 수 있다. 시험 요청들에 대한 수동적인 대답들이 제공될 수 있다. 예를 들어, 일부 실시예들에서, 이동 전화기(435)에 공급된 시험 요청은 이동 전화기(435)의 물리적 위치에 관한 물음일 수 있다. 이동 전화기(435)는 GPS 디바이스 또는 다른 위치 디바이스를 가질 수 있고, 이 정보[또는 암호문(cryptogram) 등]는 지불 프로세싱 네트워크(426)로 전송될 수 있으며, 지불 프로세싱 네트워크(426)는 이 위

치 정보를 이용하여 소비자(434)를 인증할 수 있다.

[0152] 지불 프로세싱 네트워크 서버{426(a)}가 시험 응답 메시지를 수신하면, 지불 프로세싱 네트워크 서버{426(a)}는 그 시험 응답 메시지를 검증한다[단계 616]. 시험 응답 메시지가 검증되지 않으면, 지불 프로세싱 네트워크 서버{426(a)}는 그 거래가 승인되지 않는다는 것을 지시하는 응답 메시지를 액세스 디바이스(434)로 되보낼 수 있다. 대안적으로 또는 추가적으로, 지불 프로세싱 네트워크 서버{426(a)}는 액세스 디바이스(434) 및/또는 이동 전화기(435)로 다른 시험 메시지를 보낼 수 있다. 반면에, 그 시험이 검증되면, 지불 프로세싱 네트워크 서버{426(a)}는 소비자(430)가 지불 프로세싱 네트워크(426)에 의해 제기된 어떤 시험들을 충족했다는 지시(indication)와 함께 제 2 인가 요청 메시지를 발행기(428)로 보낼 수 있다[단계 618].

[0153] 발행기(428)가 제 2 인가 요청을 수신한 후에, 발행기(428)는 발행기 서버{428(a)}를 이용하여 그 거래가 인가되는지 또는 인가되지 않는지를 결정한다[단계 620]. 소비자(430)가 불충분한 자금 또는 신용을 가지기 때문에 거래가 인가되지 않을 수 있다. 소비자(430)가 충분한 자금 또는 신용을 가지면, 발행기(428)는 그 거래가 인가된다는 것을 지시하는 제 2 인가 응답 메시지를 지불 프로세싱 네트워크(426), 획득기(424) 및 상인(422)을 통해 액세스 디바이스(434)로 되보낼 수 있다[단계 622].

[0154] 그 날의 말미에, 정규의 정산 및 결산 프로세스가 지불 프로세싱 네트워크(426)에 의해 행해질 수 있다. 정산 프로세스는 소비자의 계좌에 부기(posting)하는 것과 소비자의 결산 위치를 조정하는 것을 돕기 위해 획득기와 발행기 간에 금융 상세들(financial details)을 교환하는 프로세스이다. 정산과 결산은 동시에 발생할 수 있다.

[0155] 또한 여러 대안적인 실시예들도 가능하다. 예를 들어, 지불 프로세싱 네트워크(426) 대신에 또는 지불 프로세싱 네트워크(426)와 함께, 발행기(428)는 시험 질문들을 생성하여 그들을 이동 전화기(435)로 보낼 수 있다. 발행기(428)에 의해 동작되는 시험 질문 엔진{428(b)-1}, 거래 이력 데이터베이스{428(b)} 및 시험 질문 데이터베이스{426(c)}는 위에서 설명된 지불 프로세싱 네트워크(426)에 의해 동작되는 시험 질문 엔진{426(a)-1}, 거래 이력 데이터베이스{426(b)} 및 시험 질문 데이터베이스{426(c)}와 동일한 방식 또는 상이한 방식으로 사용될 수 있다.

[0156] 다른 실시예에서, 시험 질문을 보내는 대신에, 지불 프로세싱 네트워크 서버{426(a)}는 소비자의 이동 전화기(435)로 전자 쿠폰(electronic coupon)을 보낼 수 있다. 지불 프로세싱 네트워크(426)는 시험이 적당하다고 결정할 수 있고 전자 쿠폰을 전화기(435)로 보낼 수 있다. 그 전자 쿠폰을 수신하면, 소비자는 액세스 디바이스(434)에서 그 쿠폰을 사용하도록 촉구될 수 있다. 소비자(430)가 액세스 디바이스(434)에서 그 쿠폰을 사용하면, 액세스 디바이스(434)는 그 쿠폰을 지불 프로세싱 네트워크(426)로 전달하고, 지불 프로세싱 네트워크(426)에 의한 그 쿠폰의 수신은 그 소비자(430)가 인증된다는 것을 지시한다. 그 소비자(430)가 진정한 소비자라고 추정한다. 왜냐하면 비-진정(non-authentic) 소비자라면 그 소비자의 전화기(435)를 소유하고 있지 않을 것이기 때문이다.

[0157] 시험들을 사용하는 실시예들에 관한 추가 상세들이 2007년 6월 14일에 "Consumer Authentication System and Method"라는 명칭으로 출원된 미국 특허출원 제11/763,240호[대리인 문서 번호: 16222U-031600US]에 설명되어 있다. 그 미국 특허출원은 모든 목적들을 위해 그 전체로서 참조에 의해 여기에 병합된다.

[0158] Ⅶ. 다른 거래 인증 기법들

[0159] A. 알고리즘 식별자(algorithm identifier)들을 이용하는 방법들

[0160] 본 발명의 실시예들에서, 지불 프로세싱 조직 또는 다른 실체(entity)는 상이한 회사들에 의해 제공되는 상이한 보안 기술들을 지원할 수 있다. 상이한 보안 기술들은 휴대용 소비자 디바이스 지문(portable consumer device fingerprint)들을 사용할 수 있다. 예를 들어, 두 개의 지불 카드들 상의 두 개의 마그네틱 스트라이프들은 동일한 소비자 데이터[예컨대, 계좌 번호 정보]를 저장할 수 있지만, 그 두 개의 마그네틱 스트라이프들의 마그네틱 구조들은 상이할 수 있다. 구체적인 마그네틱 구조는 지불 카드에 연관된 지문 또는 "DNA"의 예시일 수 있다. 도둑이 마그네틱 스트라이프 상에 저장된 소비자 데이터를 비인가(unauthorized) 신용 카드로 복사했다면, 그 비인가 신용 카드의 마그네틱 스트라이프는 인가된 신용 카드와는 상이한 마그네틱 구조 또는 지문을 가질 것이다. 비인가된 카드의 사용에 응답하여 인가 요청 메시지를 수신하는 후미 서버 컴퓨터(back end server computer)는 지문이 인가 요청 메시지 내에 존재하기 않기 때문에 그 비인가된 신용 카드가 실제의 신용 카드가 아니라고 결정할 것이다. Magtek™ 및 Semtek™이 이러한 타입의 기술을 제공하는 두 회사들이다.

각각의 회사는 후속하는 인증 프로세스에서 지문이 발행기나 다른 실체로 보내지기 전에 각자의 지문을 변경[예컨대, 암호화]하기 위해서 매장 단말기에서 각자의 고유한 알고리즘을 사용한다.

[0161] 본 발명의 실시예들에서, 휴대용 소비자 디바이스 지문은 어떤 적당한 식별 메커니즘을 포함할 수 있다. 그 식별 메커니즘은, 그 휴대용 소비자 디바이스에 연관된 계좌 번호 또는 만료일과 같은 정적인(static) 소비자 데이터와는 관계없이, 어떤 사람이 휴대용 소비자 디바이스를 식별할 수 있도록 해준다. 전형적으로, 소비자 데이터와는 달리, 휴대용 소비자 디바이스 지문 데이터는 소비자에게 알려지지 않는다. 예를 들어, 일부 실시예들에서, 그 지문 데이터는 휴대용 소비자 디바이스들의 재료 물질들에 관한 특성에 관련될 수 있다. 예를 들어, 위에서 언급하였듯이, 휴대용 소비자 디바이스 지문은 지불 카드 내의 마그네틱 스트라이프에서 마그네틱 입자(magnetic particle)들의 특정한 미세 구조(microscopic structure) 내에 삽입될 수 있다. 일부 경우들에서, 어떠한 두 개의 마그네틱 스트라이프들도 동일한 휴대용 소비자 디바이스 지문을 가지지 않을 것이다.

[0162] 휴대용 소비자 디바이스 지문들은 다른 형태들을 취할 수 있다. 예를 들어, QSecure™라고 불리는 회사로부터 유래하는 다른 하나의 카드 검증 기술이 있다. QSecure™에 의해 제공되는 기술은 지불 카드에서 칩에 의해 생성될 수 있는 동적인 CVV(card verification value)를 사용한다. 그 칩은 마그네틱 스트라이프 아래에 있을 수 있고, 동적인 CVV 또는 그 동적인 CVV에 관련된 번호를 마그네틱 스트라이프에 기록할 수 있다. 이 경우에, 그 동적인 CVV는 특정한 휴대용 소비자 디바이스를 식별하는 휴대용 소비자 디바이스 지문으로서 동작할 수 있다. 동적인 CVV는 지불 거래 동안에 매장 디바이스로 보내질 수 있다. 매장 디바이스에서의 구체적인 알고리즘은 동적인 CVV가 인증을 위해 지불 카드의 발행기로 보내지기 전에 그 동적인 CVV를 변경[예컨대, 암호화]할 수 있다. 발행기, 지불 프로세싱 조직 또는 다른 실체는 그 변경된 동적 CVV를 수신할 수 있고, 그것을 그것의 원래 형태로 복원할 수 있다. 그러면 그 동적인 CVV는, 그것이 독립적으로 도출된 동적 CVV에 상응하는지를 알기 위해서, 후미 서버 컴퓨터(back end server computer)에 의해 체크될 수 있고, 그럼으로써 휴대용 소비자 디바이스를 인증한다. 이 예시에서, 동적인 CVV값은 또한, 그것이 특성상 동적(dynamic)일지라도, 휴대용 소비자 디바이스 지문으로 간주될 수 있다.

[0163] 본 발명의 실시예들은 많은 상이한 타입들의 휴대용 소비자 디바이스 지문 시스템들이 단일의 지불 프로세싱 시스템에서 함께 사용될 수 있도록 해준다. 본 발명의 실시예들에서, 상이한 식별자 또는 ID가 각 타입의 POS 단말기에서 각 타입의 알고리즘에 할당된다. 예를 들어, 발행기나 지불 프로세싱 조직과 같은 후미 실체(back end entity)는 아래의 표 1에서의 것들과 같은 알고리즘 식별자들을 사용할 수 있다.

표 1

[0164]

알고리즘 식별자 (Algorithm Identifier)	알고리즘의 설명 (Description of Algorithm)
01	회사 A 마그네틱 스트라이프 지문 암호 알고리즘
02	회사 B 마그네틱 스트라이프 지문 암호 알고리즘
03	회사 C 동적인 CVV 암호 알고리즘

[0165] 표 1에서 보여지듯이, 알고리즘 ID는 어떠한 적당한 형태를 취할 수 있다. 예를 들어, 알고리즘 ID들은 단순히 1, 2, 또는 3 디지트 번호들일 수 있다.

[0166] POS 단말기가 인가 요청 메시지를 발행기로 보내는 경우에, 그 인가 요청 메시지는 POS 단말기와 연관된 특정한 알고리즘 ID와 변경된 휴대용 소비자 디바이스 지문을 담고 있을 수 있다. 인가 요청 메시지가 후미 서버 컴퓨터에 의해 수신되는 경우에, 그것은 어떤 알고리즘이 휴대용 소비자 디바이스 지문을 암호화하는 데 사용되었는

지를 결정할 수 있다. 그 후미 서버 컴퓨터는 암호화된 휴대용 소비자 디바이스 지문을 복호화할 수 있고, 그 휴대용 소비자 디바이스 지문이 후미 데이터베이스(back end database)에 저장되어 있는 휴대용 소비자 디바이스 지문과 상응하는지를 결정할 수 있다. 휴대용 소비자 디바이스 지문은 상응하는 소비자 데이터[예컨대, 계좌 번호]와 함께, 휴대용 소비자 디바이스를 사용할 소비자에게 휴대용 소비자 디바이스를 발행하는 프로세스의 일부로서, 후미 데이터베이스에 이전에 저장되었을 것이다.

[0167] 그러한 알고리즘 식별자들을 사용하여, 본 발명의 실시예들은 상이한 기술들을 단일의 지불 프로세싱 시스템으로 효과적으로 집적시킬 수 있다. 예를 들어, 소비자는 사무실 공급물들에 대해 5.00 달러를 지불하기 위해서 POS(point of sale) 단말기를 통해 지불 카드를 스와이핑(swipe)할 수 있다. 그 단말기는 회사 A에 의해 생성된 암호화 알고리즘을 담고 있을 수 있다. 그 암호화 알고리즘은 지불 카드에서 마그네틱 스트라이프의 마그네틱 구조 내에 삽입된 지문을 암호화할 수 있다. 그러면 POS 단말기는 인가 요청 메시지를 후미 서버 컴퓨터로 보낼 수 있다. 그 인가 요청 메시지는 구매량, 소비자의 계좌 번호와 같은 소비자 데이터, 암호화된 지문, 그리고 회사 A에 의해 생성된 암호화 알고리즘에 구체적으로 연관되는 알고리즘 식별자를 포함하는 정보를 담고 있을 수 있다. 후미 서버 컴퓨터는 POS(point of sale) 단말기로부터 인가 요청 메시지를 복원할 수 있다. 그러면 그것은 어떤 알고리즘이 지문을 암호화하는 데 사용되었는지를 결정할 수 있고, 후속하여 그 지문을 복호화할 수 있다. 지문이 결정되면, 후미 서버 컴퓨터는 그 수신된 지문이 저장된 지문과 상응하는지를 결정할 수 있다. 상응한다면, 그 지불 카드는 인증된다.

[0168] 알고리즘 식별자들을 활용하는 방법들 및 시스템들에 관한 다른 상세들이 아래에서 제공된다.

[0169] B. 신용 평가 방법들(Confidence Assessment Methods)

[0170] 일부 실시예들에서, 후미 프로세서 또는 후미 서버 컴퓨터는 또한 휴대용 소비자 디바이스가 인증된다고 결정하기 전에 어느 거래가 유효성에 관해 요구되는 신용 임계값을 충족하는지를 결정할 수 있다. 신용 임계값이 충족되지 않으면, 추가적인 인증 프로세스들이 실행될 수 있다. 그러한 추가적인 인증 프로세스들은 1 이상의 시험 질문들 및/또는 통지 메시지들을 소비자에게 보내는 것을 포함할 수 있다.

[0171] 예시적으로, 후미 서버 컴퓨터는 소비자가 지불 카드를 사용하여 사무실 공급물들에 대해 지불하려고 한 후에 POS 단말기로부터 인가 요청 메시지를 수신할 수 있다. 후미 서버 컴퓨터는 위의 표 1에 있는 3 개의 카드 검증 기술들 중의 하나가 존재하고 그 지불 카드와 연관된 어떠한 의심스러운 거래들이 최근에 없다고 결정할 수 있다. 그 이후에, 거래가 지불 카드의 발행기에 의해 인가된다면, 후미 서버 컴퓨터는 그 거래가 유효[즉, 신용 임계값이 충족됨]하다고 결정하고 진행할 수 있다. 반대로, 예전 카드[old (legacy) card]와 판독기가 거래를 행하는 데 사용되고, 위의 표 1에 있는 3 개의 카드 보호 기술들 중의 어느 것도 사용되지 않으며, 최근에 그 지불 카드와 연관된 의심스러운 행위가 있다면, 서버 컴퓨터는 신용 임계값이 충족되지 않아 추가적인 인증 프로세스들이 서버 컴퓨터에 의해 개시될 수 있다고 결정할 수 있다. 예를 들어, 승인 전에 동적인 시험 물음이 소비자에게 보내질 수 있고, 소비자는 거래가 발생한다는 것을 통지받을 수 있다.

[0172] 거래 신용 결정들은 또한 어느 알고리즘이 다른 것보다 더 믿을 만할 수 있다는 것을 고려할 수 있다. 후미 서버 컴퓨터는 전단(front end)에서[예컨대, POS 단말기에서] 사용된 알고리즘을 평가하고, 그 거래가 진행되어야 하는지 아닌지를 결정할 수 있다. 예를 들어, 후미 서버 컴퓨터는 회사 A로부터의 알고리즘이 90%의 신뢰도를 가지고 회사 B로부터의 알고리즘이 50%의 신뢰도를 가진다고 결정할 수 있다.

[0173] 왜 상이한 알고리즘들이 상이한 레벨들의 신뢰도를 가질 수 있는지에 대하여 여러 이유들이 있다. 예를 들어, 단말기의 민감도에 의거하여, 카드가 스와이핑되는 방식에 의거하여, 그리고 카드의 연도(aging of the card)에 의거하여, 일부 알고리즘들은 데이터를 더 정확하게 다룰 수 있다. 이 예시에서, 회사 B로부터의 알고리즘이 존재하고 최근에 지불 카드에 연관된 의심스러운 행위가 있었다는 것을 지시하는 인가 요청 메시지를 서버 컴퓨터가 수신한다면, 추가적인 인증 프로세싱이 개시될 것이다. 반면에, 회사 A로부터의 알고리즘이 존재하고 최근에 의심스러운 행위가 있었다는 것을 지시하는 인가 요청 메시지를 서버 컴퓨터가 수신한다면, 후미 서버 컴퓨터는 추가적인 인증 프로세싱을 개시하지 않을 것이다.

[0174] 예시적으로, McDonalds는 회사 A와 관계를 가지고 Taco Bell은 회사 B와 관계를 가질 수 있다. 그들은 그들의 매장 디바이스들에서 상이한 알고리즘들을 사용할 수 있다. 각각이 2 개의 상이한 알고리즘들을 사용하여 2 세트의 데이터를 배달한다. 그들이 Visa와 같은 지불 프로세싱 조직으로 되돌아 오는 경우에, 그것은 데이터를 회사 A 알고리즘으로부터 및/또는 회사 B 알고리즘으로부터 유래하는 것으로 식별할 수 있다. 신용 레벨이 결정될

수 있도록 가중치(weight)가 알고리즘들에 부여될 수 있다. 신용 레벨[또는 임계값]이 만족되지 않으면, 추가적인 인증 프로세싱이 발생할 수 있다.

[0175] C. 알고리즘 식별자들과 신용 평가를 사용하는 예시적 시스템들

[0176] 도 10a는 본 발명의 일 실시예에서 사용될 수 있는 시스템(720)을 보여준다. 시스템(720)은 다수의 상인들{722(a), 722(b), 722(c)} 및 그 상인들{722(a), 722(b), 722(c)}에 연관된 다수의 획득기들{724(a), 724(b), 724(c)}을 포함한다. 전형적인 지불 거래들에서, 소비자들{730(a), 730(b), 730(c)}은 그들의 휴대용 소비자 디바이스들{732(a), 732(b), 732(c)}을 사용하여 상인들{722(a), 722(b), 722(c)}에게서 상품 또는 서비스들을 구매할 수 있다. 소비자들{730(a), 730(b), 730(c)}은 개인들, 또는 사업체들과 같은 조직들일 수 있다. 획득기들{724(a), 724(b), 724(c)}은 지불 프로세싱 네트워크(726)를 통해 발행기들{728(a), 728(b), 728(c)}과 통신할 수 있다. 발행기들{728(a), 728(b), 728(c)}은 각각 소비자들{730(a), 730(b), 730(c)}에게 휴대용 소비자 디바이스들{730(a), 730(b), 730(c)}을 발행할 수 있다.

[0177] 예시적으로, 액세스 디바이스 A{732(a)}는 알고리즘 식별자 "01"을 가지는 알고리즘에 연관될 수 있는 회사 A에 의해 생산될 수 있다. 액세스 디바이스 B{732(b)}는 회사 B에 의해 생산될 수 있고, 알고리즘 식별자 "02"를 가지는 알고리즘에 연관될 수 있다. 액세스 디바이스 C{732(c)}는 회사 D에 연관될 수 있고, 그것에 연관된 알고리즘을 가지지 않을 수 있다.

[0178] 휴대용 소비자 디바이스들{732(a), 732(b), 732(c)}은 어떤 적당한 형태에 있을 수 있다. 예를 들어, 적당한 휴대용 소비자 디바이스들{732(a), 732(b), 732(c)}은 그들이 소비자의 지갑 및/또는 주머니에 들어맞을 수 있도록[예컨대, 주머니-사이즈(pocket-sized)] 핸드-헬드(hand-held) 및 컴팩트(compact) 형태일 수 있다. 적당한 휴대용 소비자 디바이스들은 위에서 설명된 바 있다[예컨대, 도 1에서 휴대용 소비자 디바이스 32].

[0179] 또한 상인들{722(a), 722(b), 722(c)}은 휴대용 소비자 디바이스들{732(a), 732(b), 732(c)}과 상호작용할 수 있는 각각의 액세스 디바이스들{734(a), 734(b), 734(c)}을 가지거나, 그 각각의 액세스 디바이스들{734(a), 734(b), 734(c)}로부터 통신들을 수신할 수 있다. 적당한 타입들의 액세스 디바이스들은 위에서 설명된 바 있다[예컨대, 도 1에서 액세스 디바이스 34].

[0180] 액세스 디바이스가 매장 단말기이면, 어떤 적당한 매장 단말기가 카드 판독기들을 포함하여 사용될 수 있다. 카드 판독기들은 어떤 적당한 접촉 동작 모드 또는 비접촉 동작 모드를 포함할 수 있다. 예를 들어, 예시적인 카드 판독기들은 휴대용 소비자 디바이스들{732(a), 732(b), 732(c)}과 상호작용하기 위해 RF(radio frequency) 안테나들, 마그네틱 스트라이프 판독기들 등을 포함할 수 있다.

[0181] 지불 프로세싱 네트워크(726)는 위에서 설명된 어떠한 특징들을 포함할 수 있다[예컨대, 도 1에서 지불 프로세싱 네트워크(26)에 관해서]. 그것은 서버 컴퓨터{726(a)}를 포함할 수 있다.

[0182] 서버 컴퓨터{726(a)}는 어떤 적당한 수의 소프트웨어 모듈들을 구비할 수 있고, 그들은 어떤 적당한 타입일 수 있다. 도 10b에 도시된 바와 같이, 서버 컴퓨터{726(a)}는 알고리즘 식별 모듈{726(a)-1}과 신용 평가 모듈{726(a)-2}을 구비할 수 있다. 또한 그것은 복호화 모듈{726(a)-3}과 데이터 포맷기 모듈{726(a)-4}을 구비할 수 있다.

[0183] 알고리즘 식별 모듈{726(a)-1}은 복호화 모듈{726(a)-3}과 함께, 알고리즘 ID와 변경된 휴대용 소비자 디바이스 지문을 포함하는 수신된 인가 요청 메시지를 검토할 수 있다. 수신된 알고리즘 ID로부터, 그것은 어떤 알고리즘이 휴대용 소비자 디바이스 지문을 변경[예컨대, 암호화]시키는 데 사용되었는지를 결정할 수 있다. 알고리즘 ID, 휴대용 소비자 디바이스 지문을 변경하거나 변경된 휴대용 소비자 디바이스 지문을 복원하는 데 사용된 알고리즘(들), 그리고 소비자 데이터[예컨대, 계좌 번호] 간의 상응성(correspondence)을 식별하는 데 룩 업 테이블(lookup table) 등이 사용될 수 있다. 일부 경우들에서, 알고리즘이 암호화 프로세스에서의 키(key)일 수 있다. 서버 컴퓨터{726(a)}는 인가 요청 메시지에서의 변경된 휴대용 소비자 디바이스 지문으로부터 휴대용 소비자 디바이스 지문을 결정[예컨대, 복호화함으로써]하는 데 사용될 수 있다. 휴대용 소비자 디바이스 지문이 결정되면, 이 정보는 그것이 휴대용 소비자 디바이스에 연관된 소비자 데이터[예컨대, 계좌 번호]에 링크되는 저장된 지문에 상응하는지를 결정하기 위해서 분석될 수 있다.

[0184] 신용 평가 모듈{726(a)-2}은 다양한 조각들의 정보로부터 신용 평가를 생성할 수 있다. 그러한 정보는 사용된 휴대용 소비자 디바이스의 타입[예컨대, 전화기는 지불 카드보다 더 안전할 것이다], 휴대용 소비자 디바이스

지문을 암호화하는 데 사용된 알고리즘의 타입[예컨대, 일부 암호화 알고리즘들은 다른 것들보다 더 안전하다] 등을 포함할 수 있다. 신용 모듈{726(a)-2}을 사용하여, 서버 컴퓨터{726(a)}는 후속적으로 추가적인 인증 프로세스들이 발생할 필요가 있는지를 결정할 수 있다. 그러한 추가적인 인증 프로세스들은 시험 질문들 및/또는 거래가 발생하고 있다는 소비자 통지를 구비할 수 있다.

[0185] 신용 평가 모듈{726(a)-2}은 여러 거래 변수들에 기초하여 거래를 "채점(score)"할 수 있다. 이 점수(score)가 소정의 임계값을 초과하면, 그 거래는 유효한 것으로 간주될 수 있고 추가적인 인증 프로세싱이 발생할 필요가 없다. 반대로, 그 점수(score)가 소정의 임계값을 초과하지 않으면, 그 거래는 의심스러운 것으로 특징지어질 수 있고 추가적인 인증 프로세스들이 개시될 수 있다.

[0186] 데이터 포맷기 모듈{726(a)-4}은 데이터가 신용 평가 모듈{726(a)-2}에 의해 사용될 수 있도록 데이터를 포맷하는 데 사용될 수 있다. 일부 경우들에서, 상이한 회사들로부터의 상이한 POS 단말기들로부터 오는 데이터는 복호화 모듈{726(a)-3}에 의해 복호화될 수 있고, 상이한 포맷들일 수 있다. 데이터 포맷기는 데이터가 신용 평가 모듈{726(a)-2}에 의해 사용될 수 있도록 어떠한 데이터를 포맷할 수 있다.

[0187] 본 발명의 실시예들이 위에 설명된 실시예들로 한정되지는 않는다. 예를 들어, 별개의 기능적 블럭들이 발행기, 지불 프로세싱 네트워크 및 획득기에 대하여 도시되었으나, 어떠한 실체들(entities)은 그 기능들 모두를 실행할 수 있으며 본 발명의 실시예들에 포함될 수 있다. 추가적인 컴포넌트들 또한 본 발명의 실시예들에 포함될 수 있다.

[0188] D. 지문들과 식별자들을 사용하기 위한 예시적 방법들

[0189] 본 발명의 실시예들에 따른 다양한 방법들이 도 10 내지 도 12를 참조하여 설명될 수 있다. 도 11 및 도 12는 흐름도들을 포함한다.

[0190] 도 11에 도시된 일부 또는 모든 단계들은 본 발명의 실시예들에 포함될 수 있다. 예를 들어, 본 발명의 일부 실시예들은 인가 요청 메시지에서의 휴대용 소비자 디바이스 지문이 후미 데이터베이스(back end database)에 저장된 휴대용 소비자 디바이스 지문과 매칭되는지를 결정하기 위해서 알고리즘 식별자들을 사용할 수 있고, 거래가 인가된다고 결정하기 전에 거래 신용 프로세싱을 실행하지 않을 수 있다. 다른 실시예들에서, 거래 신용 프로세스는 휴대용 소비자 디바이스들을 인증하기 위해 휴대용 소비자 디바이스 지문들을 사용하지 않고 실행될 수 있다. 그러나, 바람직한 실시예들에서, 알고리즘 식별자들, 휴대용 소비자 디바이스 지문들 및 거래 신용 프로세싱은 휴대용 소비자 디바이스들과 거래들을 전체로서 인증하는 데 사용될 수 있다.

[0191] 또한, 도 11과 도 12에 도시된 흐름도들이 특정한 순서로 실행되고 있는 특정한 단계들을 보여주고 있으나, 본 발명의 실시예들은 상이한 순서의 단계들을 포함하는 방법들을 포함할 수 있다. 또한 이것은 본 출원에서 설명되는 다른 흐름도들 또는 프로세스들에도 적용된다.

[0192] 도 10a와 도 11을 참조한다. 소비자 A{730(a)}는 상인 A{732(a)} 측의 액세스 디바이스 A{734(a)}와 상호작용하기 위해 휴대용 소비자 디바이스 A{732(a)}를 사용할 수 있다[단계 802]. 휴대용 소비자 디바이스{732(a)}는 신용 카드일 수 있고, 액세스 디바이스 A{734(a)}는 매장 단말기일 수 있으며, 상인 A{732(a)}는 주유소(gas station)일 수 있다. 소비자 A{730(a)}는 휴대용 소비자 디바이스 A{732(a)}를 사용하여 상인 A{722(a)}로부터 가스(gas)를 구매하고자 할 수 있다.

[0193] 휴대용 소비자 디바이스 A{732(a)}가 상인 A{722(a)} 측의 액세스 디바이스 A{734(a)}와 인터페이스한 후에, 액세스 디바이스 A{734(a)}는 휴대용 소비자 디바이스 A{732(a)}로부터 소비자 데이터 및 마그네틱 스트라이프 지문 데이터와 같은 휴대용 소비자 디바이스 지문 데이터를 판독한다[단계 804]. 그 소비자 데이터는 소비자가 전형적으로 인식하고 있는 정보를 포함할 수 있다. 소비자 데이터의 예시들은 소비자의 계좌 번호, 만료일 및 서비스 코드를 포함한다. 위에서 언급한 바와 같이, 휴대용 소비자 디바이스 지문 데이터는 전형적으로 소비자에게 알려지지 않지만 휴대용 소비자 디바이스를 인증하는 데 사용되는 데이터이다. 이 예시에서, 휴대용 소비자 디바이스 지문 데이터는 마그네틱 스트라이프 지문 데이터일 수 있다. 또한 그 마그네틱 스트라이프 지문 데이터는, 마그네틱 스트라이프의 마그네틱 구조에 삽입되며 그리고 특정한 회사에 의해 제조된 액세스 디바이스를 사용해서만 판독가능한 데이터를 구비할 수 있다.

[0194] 액세스 디바이스 A{734(a)}가 휴대용 소비자 디바이스 A{734(a)}로부터 소비자 데이터를 얻으면, 알고리즘 식별자를 포함하는 인가 요청 메시지가 생성된다[단계 806]. 그 인가 요청 메시지는 소비자 데이터[예컨대, 계좌 번

호], 구매량에 관한 데이터, 그리고 휴대용 소비자 디바이스 지문 데이터를 포함할 수 있다. 액세스 디바이스 A{734(a)}는 수신된 지문 데이터를 그것이 인가 요청 메시지로 통합되기 전에 액세스 디바이스 A{734(a)} 내의 메모리에 저장된 알고리즘 A를 사용하여 변경[예컨대, 암호화]시킬 수 있다. 일부 실시예들에서, 휴대용 소비자 디바이스 지문과 알고리즘 식별자는 필드 55(Field 55)라고 불리는 보충적 데이터 필드에 저장될 수 있다.

[0195] 상이한 타입들과 사이즈들의 지문들이 상이한 제조자들에 의해 제공되는 상이한 휴대용 소비자 디바이스들로부터 유래할 수 있다. 이 상이한 지문들은 지불 프로세싱 시스템을 통한 전송이 전송되고 있는 특정한 지문에 상관없이 균일하도록 표준 사이즈의 데이터 필드에 삽입될 수 있다. 예를 들어, 일부 경우들에서, 데이터 필드를 가득 채우기 위해서 제로(zero)들과 같은 문자(character)들을 데이터 필드에 패딩(pad)하는 것이 바람직하다. 예를 들어, 데이터 필드는 64 바이트의 사이즈를 가질 수 있다. 어느 타입의 휴대용 소비자 디바이스로부터의 지문은 54 바이트일 수 있고, 반면에 다른 타입의 휴대용 소비자 디바이스로부터의 지문은 56 바이트일 수 있다. 추가적인 패딩 문자들은 2 문자 알고리즘 식별자(two character algorithm identifier)와 함께 64 바이트 필드에 존재할 수 있다. 그 패딩 문자들은 필드 내에 소정의 방식으로 배치될 수 있다.

[0196] 본 발명의 실시예들에서, 이전에 설명된 알고리즘 식별자는 휴대용 소비자 디바이스 지문을 암호화하는 데 사용된 알고리즘을 식별할 수 있을 뿐만 아니라, 그 식별된 알고리즘은 그 지문을 그것의 원래 형태로 복원하여 그것이 평가될 수 있도록 하는데 사용될 수 있다. 예를 들어, 알고리즘 식별자는 수신되는 변경된 지문을 그것의 원래 형태로 복원하여 그것이 평가될 수 있도록 하기 위해서, 어떠한 패딩 문자들을 제거하는 데 사용될 수 있는 알고리즘을 식별하는 데 사용될 수 있다.

[0197] 인가 요청 메시지는 상인 A{722(a)}와 연관된 획득기 A{724(a)}를 통해 액세스 디바이스{734(a)}로부터 지불 프로세싱 네트워크(726)로 보내진다[단계 808]. 다른 실시예들에서, 액세스 디바이스{734(a)}는 획득기 A{724(a)}를 통하는 대신에, 인가 요청 메시지를 지불 프로세싱 네트워크로 직접 보낼 수 있다.

[0198] 인가 요청 메시지가 지불 프로세싱 네트워크(726)에 의해 수신된 후에, 지불 프로세싱 네트워크(726)의 서버 컴퓨터{726(a)}는 그 인가 요청 메시지를 분석하고 인가 요청 메시지에 있는 알고리즘 ID를 이용하여 알고리즘을 선택한다[단계 810]. 선택된 알고리즘 ID와 선택된 알고리즘은 알고리즘 데이터베이스{726(c)}로부터 선택될 수 있다. 알고리즘 데이터베이스{726(c)}는 다양한 액세스 디바이스들[예컨대, 액세스 디바이스 A{732(a)}와 액세스 디바이스 B{734(b)}]과 연관될 수 있는 다수의 알고리즘 ID들과 다수의 알고리즘들을 담고 있을 수 있다.

[0199] 알고리즘이 식별된 후에, 휴대용 소비자 디바이스 지문이 지불 프로세싱 네트워크(726)의 서버 컴퓨터{726(a)}에 의해 결정된다[단계 812]. 선택된 알고리즘은 인가 요청 메시지에 존재하는 변경된 휴대용 소비자 디바이스 지문을 복원[예컨대, 복호화]하는 데 사용된다.

[0200] 서버 컴퓨터{726(a)}는 결정된 휴대용 소비자 디바이스 지문이 데이터베이스 내에 이전에 저장된 지문과 상응하는지를 결정한다[단계 814]. 서버 컴퓨터{726(a)}는 인가 요청 메시지를 분석한 후에 인가 요청 메시지로부터 소비자의 계좌 번호와 같은 소비자 데이터를 얻거나 소비자 데이터베이스{726(b)}로부터 추가적인 소비자 데이터를 얻을 수 있다. 소비자 데이터가 결정되면, 서버 컴퓨터{726(a)}는 소비자 데이터베이스{726(b)}로부터 휴대용 소비자 디바이스 지문을 얻을 수 있다. 그러면 서버 컴퓨터{726(a)}는 인가 요청 메시지에서의 휴대용 소비자 디바이스 지문과 소비자 데이터베이스{726(b)}에서의 휴대용 소비자 디바이스 지문이 매칭되는지를 결정한다.

[0201] 소비자 데이터베이스{726(b)}로부터 얻어진 휴대용 소비자 디바이스 지문이 인가 요청 메시지로부터 얻어지는 이전에 저장된 휴대용 소비자 디바이스 지문과 상응하지 않으면, 추가적인 인증 프로세스들이 실행되거나, 그 거래가 거부된다는 것을 지시하는 인가 응답 메시지가 소비자 A{722(a)}에게 되보내질 수 있다[단계 822]. 추가적인 인증 프로세싱은 소비자에게 거래가 발생하고 있다는 것을 통지하는 거래 통지 메시지를 소비자 A{722(a)}에게[예컨대, 소비자의 셀 전화기나 소비자의 컴퓨터로] 보내는 단계를 포함할 수 있다. 그 통지 메시지는 그 거래가 진정하다는 것을 소비자 A{722(a)}가 확인할 것을 요청할 수 있다. 대안적으로 또는 추가적으로, 시험 질문들과 같은 다른 타입들의 시험들이 소비자 A{722(a)}에게 보내질 수 있다. 시험 질문들과 같은 시험들이 2007년 6월 14일에 "Consumer Authentication System and Method"라는 명칭으로 출원된 미국 특허출원 제 11/763,240호[대리인 문서 번호: 16222U-031600US]에 더 상세하게 설명되어 있다. 그 미국 특허출원은 모든 목적들을 위해 그 전체로서 참조에 의해 여기에 병합된다.

[0202] 일부 실시예들에서, 인가 요청 메시지로부터 얻어진 지문이 소비자 데이터베이스{726(b)}에서의 지문과 매칭되면, 서버 컴퓨터{726(a)}는 거래 신용 임계값이 만족되는지를 옵션으로 결정할 수 있다[단계 815]. 그 신용 임

계값이 만족되지 않으면, 추가적인 인증 프로세싱이 실행될 수 있다[단계 823]. 그러나, 그 신용 임계값이 만족되면, 인가 요청 메시지가 발행기 A{428(a)}로 전달될 수 있다[단계 816].

[0203] 거래 신용 임계값은 거래를 진정한 것으로 또는 잠재적으로 의심스러운 것으로 채점(score)하기 위해서 어떤 개수의 거래 특징들을 취할 수 있다. 그러한 거래 특징들은 액세스 디바이스[예컨대, 액세스 디바이스가 새로운 또는 예전(old) 기술을 사용하는지, 액세스 디바이스가 데이터를 암호화하기 위해 보안 암호화 알고리즘을 사용하는지 등], 휴대용 소비자 디바이스[예컨대, 휴대용 소비자 디바이스가 전화기인지, 예전 기술을 갖춘 마그네틱 스트라이프 카드인지, 새로운 기술을 갖춘 마그네틱 스트라이프 카드인지 등] 등에 관련될 수 있다.

[0204] 위에서 언급된 바와 같이, 지불 프로세싱 시스템에서, 어느 주어진 시간에 서로 함께 상호작용하는 액세스 디바이스들과 휴대용 소비자 디바이스들의 많은 상이한 조합들이 있을 수 있다. 액세스 디바이스들과 휴대용 소비자 디바이스들의 그러한 상이한 조합들은 상이한 레벨들의 잠재적 진정성(potential authenticity)을 가질 수 있는 거래들을 개시할 수 있다. 예를 들어, 도 10a를 참조할 때, 액세스 디바이스 A{734(a)}는 인가 요청 메시지에서의 데이터를 암호화하기 위해 회사 A로부터의 암호화 알고리즘을 사용할 수 있고, 액세스 디바이스 B{734(b)}는 회사 B로부터의 암호화 알고리즘을 사용할 수 있으며, 액세스 디바이스 C{734(c)}는 어떠한 암호화 기술도 사용하지 않을 수 있다. 암호화 알고리즘 A는 암호화 알고리즘 B보다 더 믿을 만한 암호화 알고리즘으로 간주될 수 있다. 결과적으로, 액세스 디바이스 A{734(a)}로부터의 인가 요청 메시지들은 액세스 디바이스 B{734(b)}나 액세스 디바이스 C{734(c)}로부터의 인가 요청 메시지들보다 더 높은 레벨의 잠재적 진정성을 가질 수 있다. 액세스 디바이스 A{734(a)}가 아니라 액세스 디바이스 B{734(b)}와 액세스 디바이스 C{734(c)}에 의해 거래들이 실행되는 경우에 추가적인 인증 프로세싱이 실행될 수 있다. 다른 하나의 예시에서, 휴대용 소비자 디바이스들 A, B, C{732(a), 732(b), 732(c)} 모두가 높은 보안 휴대용 소비자 디바이스들이면, 단지 액세스 디바이스 C{734(c)}로부터 오는 인가 요청 메시지들만이 추가적인 인증 프로세싱을 필요로 할 것이다. 왜냐하면, 단지 액세스 디바이스 C{734(c)}만이 암호화 알고리즘을 포함하고 있지 않기 때문이다. 이 예시에서 설명되듯이, 추가적인 인증 프로세싱이 실행될 필요가 있는지 아닌지를 결정하기 위한 임계값은 변할 수 있고, 소정의 규칙들에 따라 설정될 수 있다.

[0205] 인가 요청 메시지가 발행기 A{728(a)}에 의해 수신된 후에, 발행기 A는 거래가 인가되는지를 결정할 수 있다. 거래가 인가되지 않으면[예컨대, 소비자 A의 계좌에서의 불충분한 자금 또는 신용으로 인해서], 추가적인 인증 프로세싱이 실행되거나 거래가 거절된다는 것을 지시하는 인가 응답 메시지가 소비자 A{730(a)}에게 보내질 수 있다[단계 824].

[0206] 거래가 발행기 A{728(a)}에 의해 승인되면, 인가 응답 메시지가 지불 프로세싱 네트워크(726), 획득기 A{724(a)}, 상인 A{722(a)} 및 액세스 디바이스 A{734(a)}를 통해 소비자 A{730(a)}에게 되보내질 수 있다.

[0207] 그 날의 말미에, 정규의 정산 및 결산 프로세스가 지불 프로세싱 네트워크(726)에 의해 행해질 수 있다. 정산 프로세스는 소비자의 계좌에 부기(posting)하는 것과 소비자의 결산 위치를 조정하는 것을 돕기 위해 획득기와 발행기 간에 금융 상세들(financial details)을 교환하는 프로세스이다. 정산과 결산은 동시에 발생할 수 있다.

[0208] 위에서 설명된 방법들과 시스템들을 사용하는 실시예들에 관한 추가 상세들이 본 출원과 동일한 날에 "Portable Consumer Device Verification System and Method"라는 명칭으로 출원된 미국 특허출원[대리인 문서 번호: 16222U-031400US]에 설명되어 있다. 그 미국 특허출원은 모든 목적들을 위해 그 전체로서 참조에 의해 여기에 병합된다.

[0209] 위에서 설명된 본 발명은 모듈(modular) 또는 집적(integrated) 방식으로 컴퓨터 소프트웨어를 이용하여 제어 로직의 형태로 구현될 수 있다는 점이 이해되어야 한다. 여기에 제공된 개시 및 교시들에 기초하여, 당업자는 본 발명을 하드웨어 및 하드웨어와 소프트웨어의 조합을 이용하여 구현하기 위한 다른 방식들 및/또는 방법들을 알 것이다.

[0210] 본 출원에서 설명된 어떠한 소프트웨어 컴포넌트들 또는 기능들은 예를 들어 통상적인 또는 객체-지향(object-oriented) 기법들을 이용하는 예컨대 Java, C++ 또는 Perl과 같은 어떤 적당한 컴퓨터 언어를 이용하여 프로세서에 의해 실행될 소프트웨어 코드로서 구현될 수 있다. 그 소프트웨어 코드는 일련의 명령(instruction)들 또는 커맨드(command)들로서 RAM(random access memory), ROM(read only memory), 하드-드라이브(hard-drive)나 플로피 디스크(floppy disk)와 같은 마그네틱 매체, 또는 CD-ROM 같은 광 매체와 같은 컴퓨터 판독가능 매체 상에 저장될 수 있다. 그러한 컴퓨터 판독가능 매체는 단일의 계산 장치에 또는 그 내부에 존재할 수도 있고, 시

스템이나 네트워크 내의 상이한 계산 장치들에 또는 그 내부에 존재할 수도 있다.

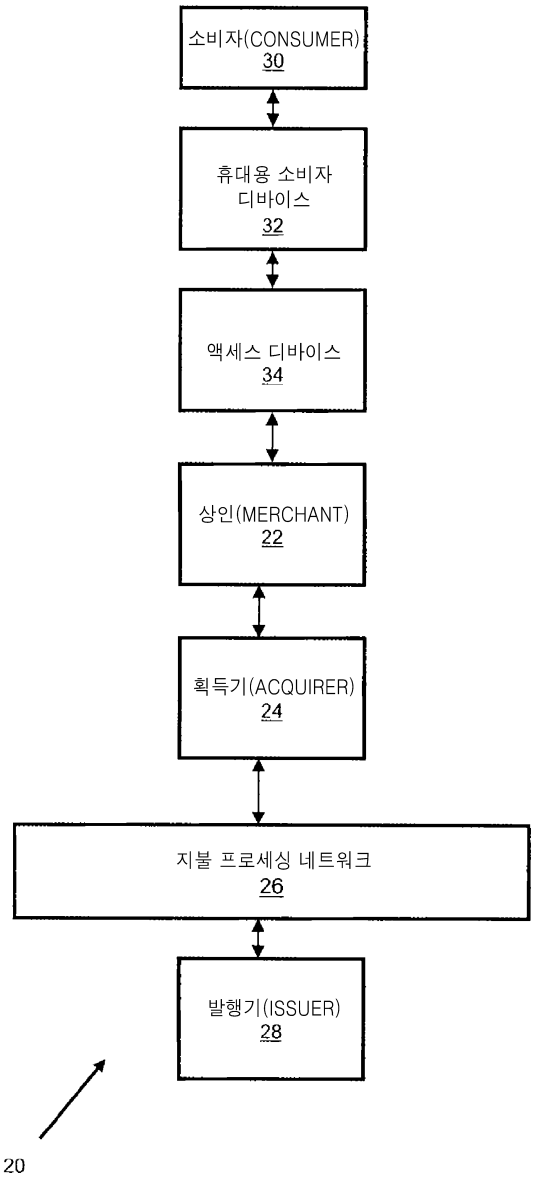
[0211] 위의 설명은 예시적일 뿐이며 제한적이지 않다. 본 개시의 검토에 기초할 때 본 발명의 많은 변형들이 당업자에게 명백하게 될 것이다. 그러므로, 본 발명의 범위는 위의 설명으로만 결정되는 것이 아니라 그 대신에 현재 청구항들[그들의 전범위 및 그 균등물들 포함]에 의해 결정되어야 한다.

[0212] 어떤 실시예로부터의 1 이상의 특징들은 본 발명의 범위를 벗어나지 않으면서 다른 실시예로부터의 1 이상의 특징들과 조합될 수 있다.

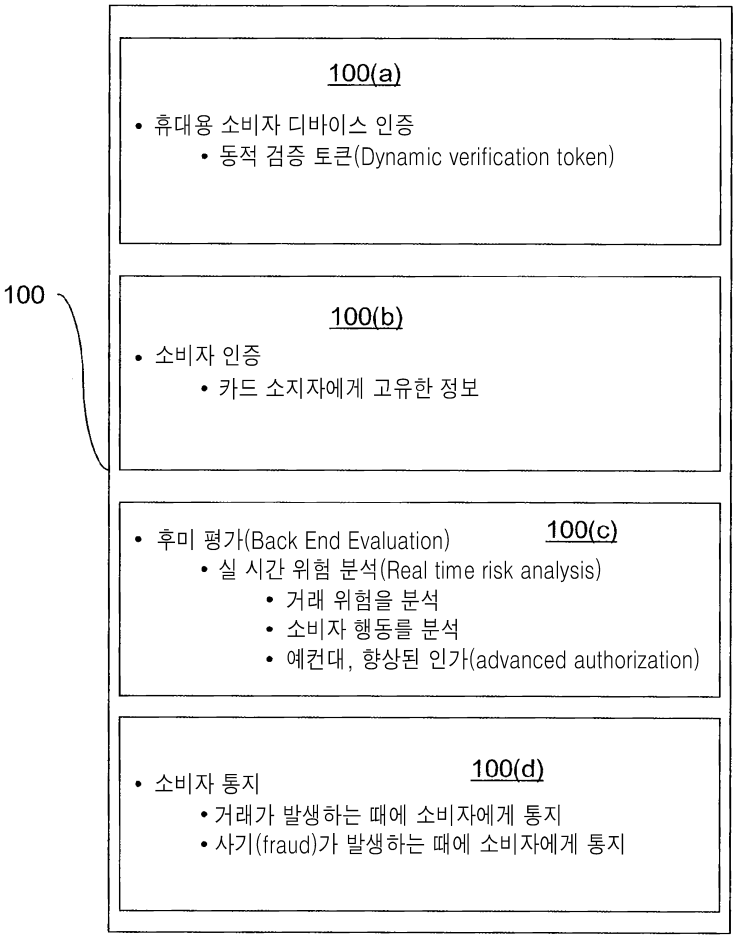
[0213] "어느(a)", "어떤(an)" 또는 "그(the)"와 같은 기재는 특별히 다르게 지시되지 않으면 "하나 또는 그 이상(one or more)"을 의미하도록 의도된다.

도면

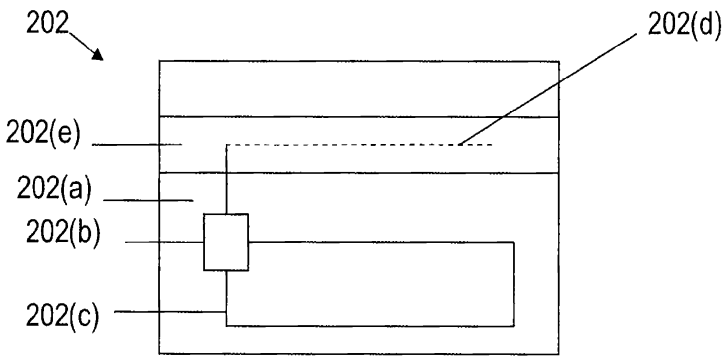
도면1



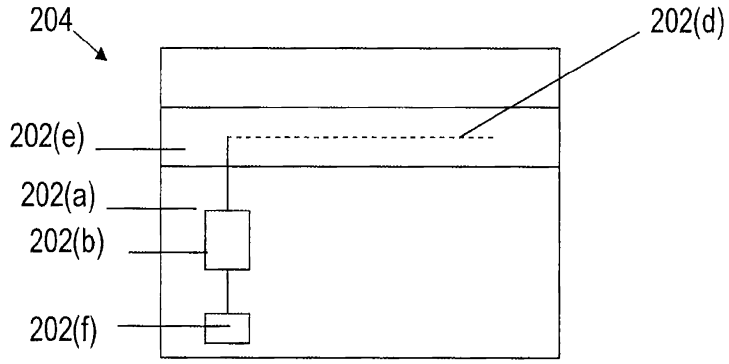
도면2


100
100(a)
• 휴대용 소비자 디바이스 인증
• 동적 검증 토큰(Dynamic verification token)
100(b)
• 소비자 인증
• 카드 소지자에게 고유한 정보
• 후미 평가(Back End Evaluation)
100(c)
• 실 시간 위험 분석(Real time risk analysis)
• 거래 위험을 분석
• 소비자 행동를 분석
• 예컨대, 향상된 인가(advanced authorization)
• 소비자 통지
100(d)
• 거래가 발생하는 때에 소비자에게 통지
• 사기(fraud)가 발생하는 때에 소비자에게 통지

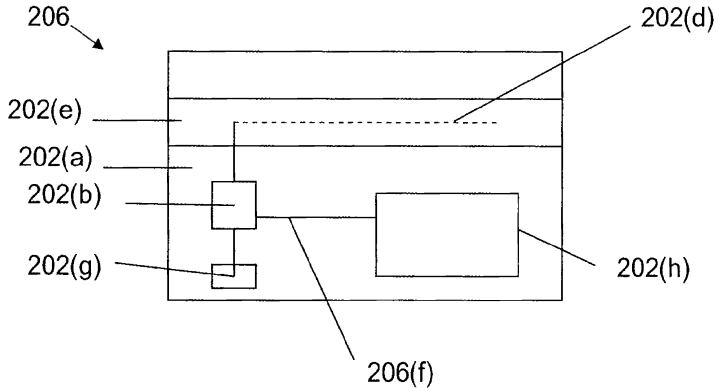
도면3a


202
202(d)
202(e)
202(a)
202(b)
202(c)

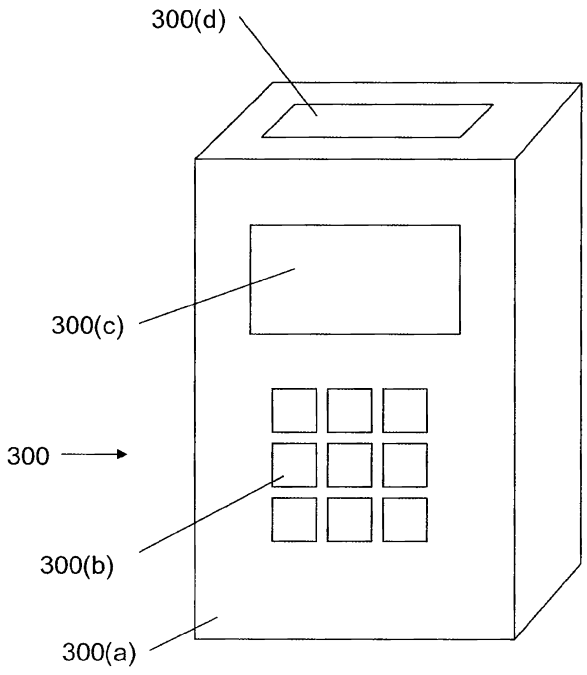
도면3b



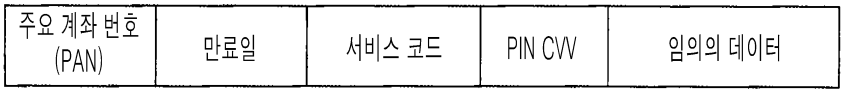
도면3c



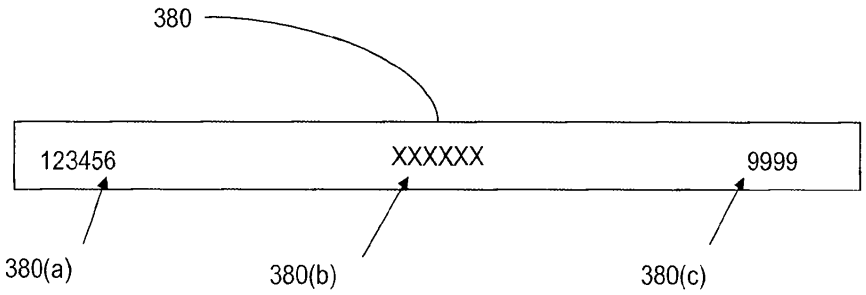
도면4



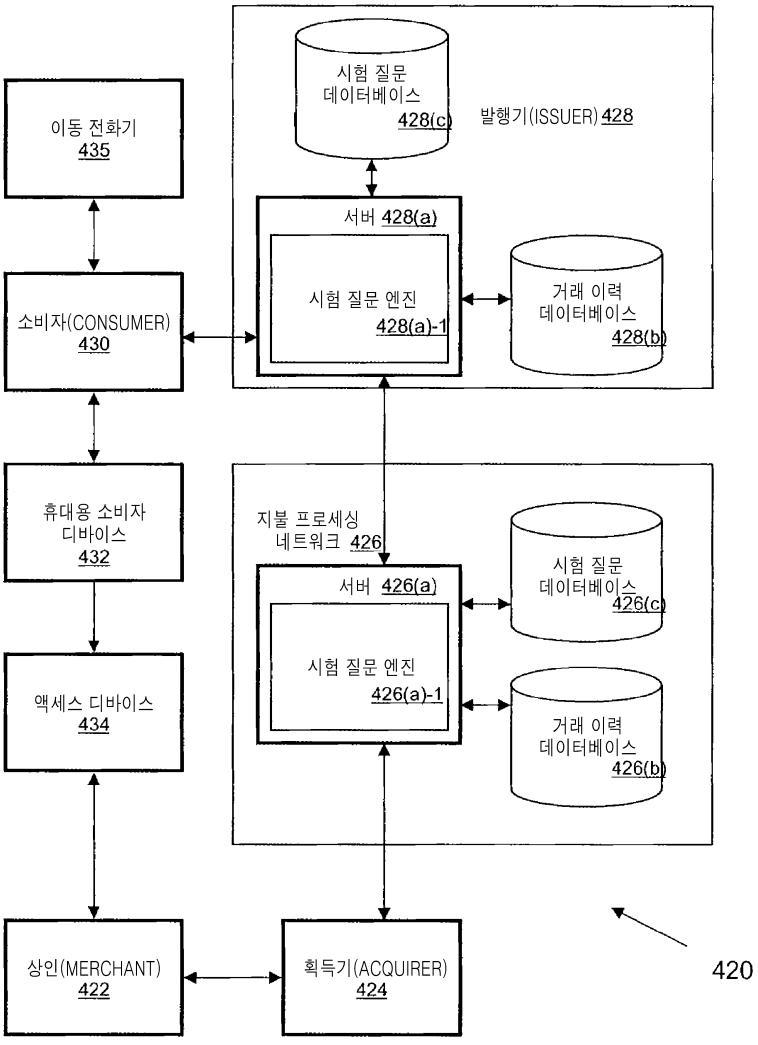
도면5


주요 계좌 번호 (PAN)
만료일
서비스 코드
PIN CVV
임의의 데이터

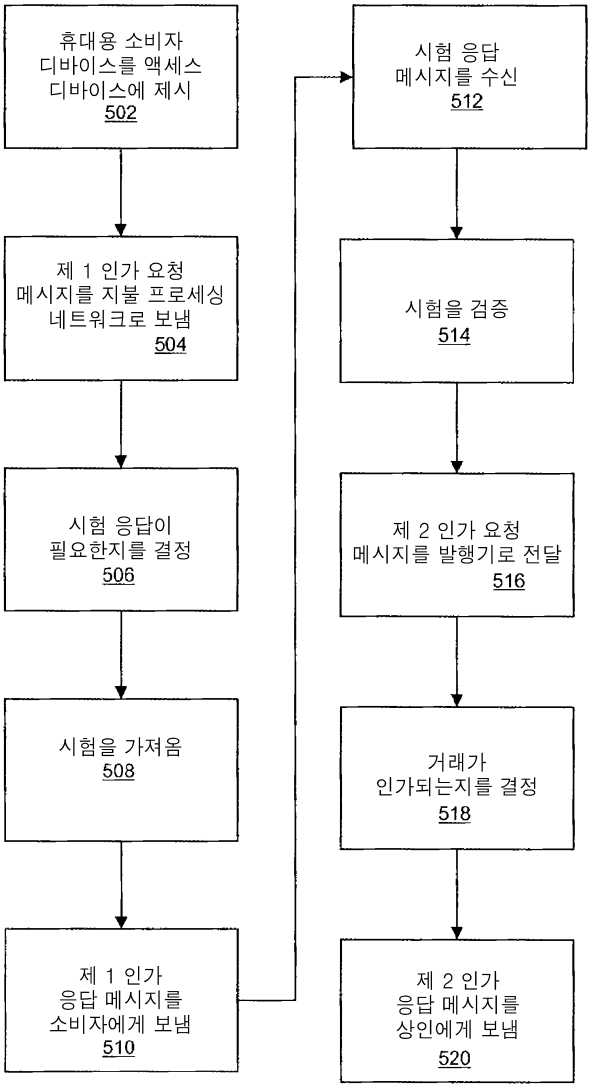
도면6


380
123456
XXXXXX
9999
380(a)
380(b)
380(c)

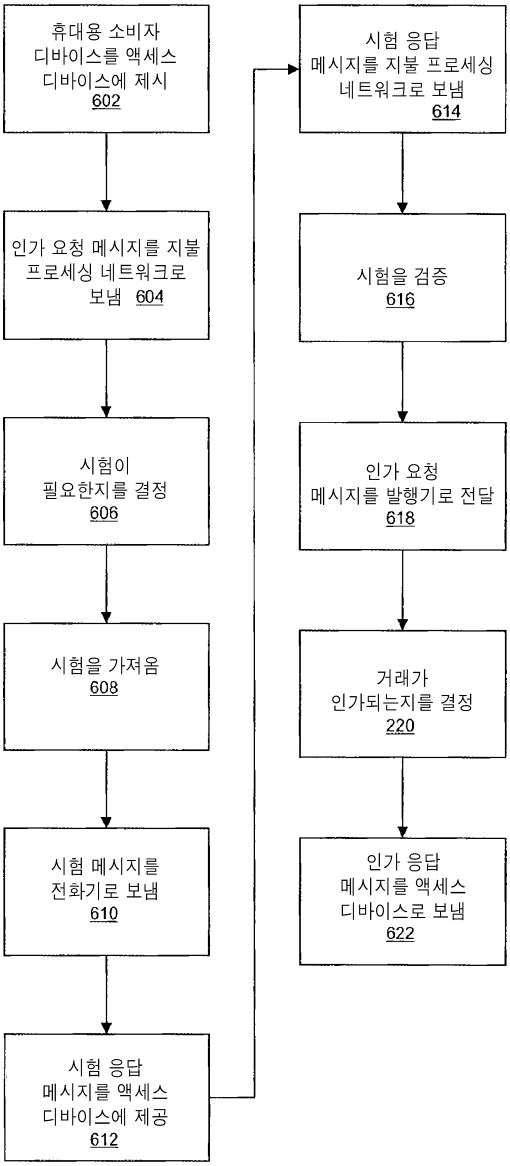
도면7


시험 질문 데이터베이스 428(c)
발행기(ISSUER) 428
서버 428(a)
시험 질문 엔진 428(a)-1
거래 이력 데이터베이스 428(b)
이동 전화기 435
소비자(CONSUMER) 430
휴대용 소비자 디바이스 432
액세스 디바이스 434
지불 프로세싱 네트워크 426
서버 426(a)
시험 질문 엔진 426(a)-1
시험 질문 데이터베이스 426(c)
거래 이력 데이터베이스 426(b)
상인(MERCHANT) 422
획득기(ACQUIRER) 424
420

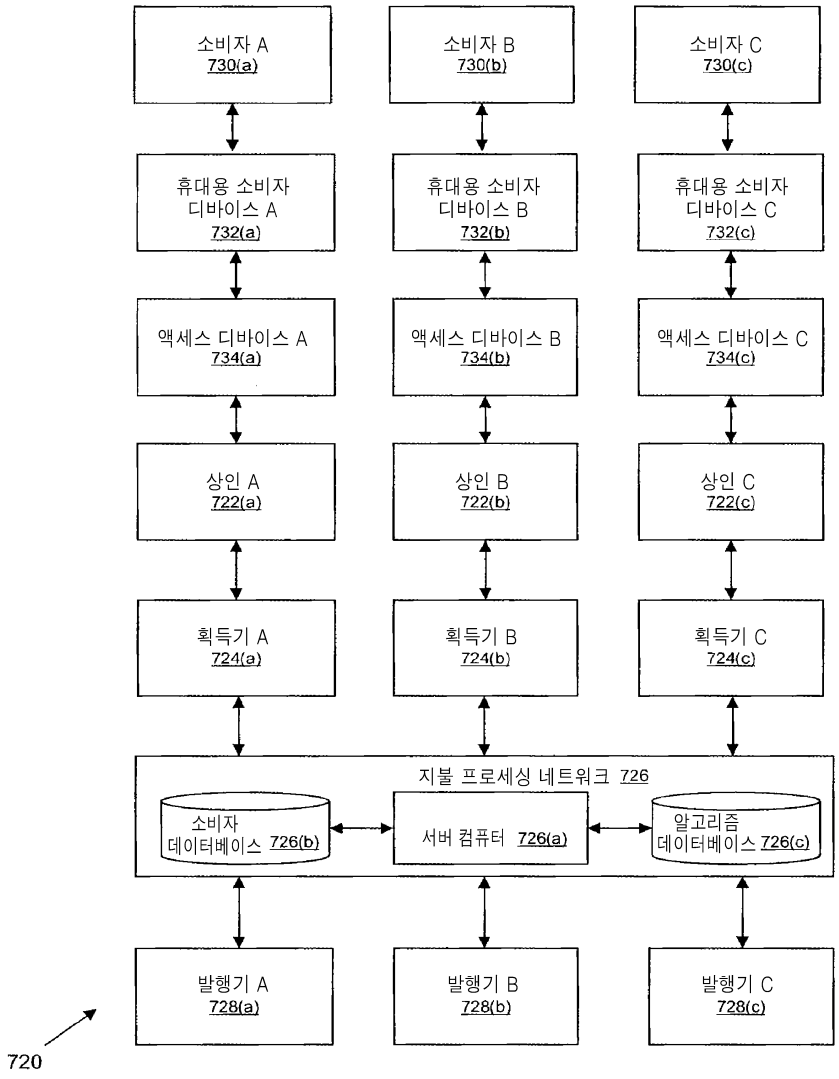
도면8


휴대용 소비자 디바이스를 액세스 디바이스에 제시 502
제 1 인가 요청 메시지를 지불 프로세싱 네트워크로 보냄 504
시험 응답이 필요한지를 결정 506
시험을 가져옴 508
제 1 인가 응답 메시지를 소비자에게 보냄 510
시험 응답 메시지를 수신 512
시험을 검증 514
제 2 인가 요청 메시지를 발행기로 전달 516
거래가 인가되는지를 결정 518
제 2 인가 응답 메시지를 상인에게 보냄 520

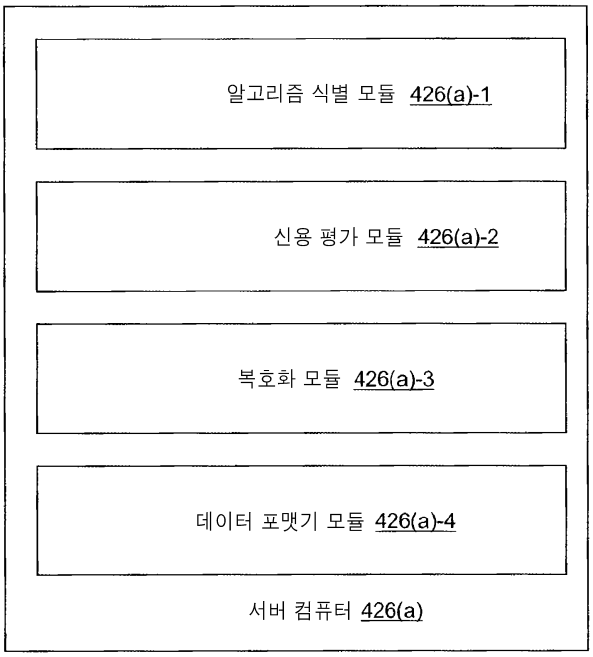
도면9


휴대용 소비자 디바이스를 액세스 디바이스에 제시 602
인가 요청 메시지를 지불 프로세싱 네트워크로 보냄 604
시험이 필요한지를 결정 606
시험을 가져옴 608
시험 메시지를 전화기로 보냄 610
시험 응답 메시지를 액세스 디바이스에 제공 612
시험 응답 메시지를 지불 프로세싱 네트워크로 보냄 614
시험을 검증 616
인가 요청 메시지를 발행기로 전달 618
거래가 인가되는지를 결정 220
인가 응답 메시지를 액세스 디바이스로 보냄 622

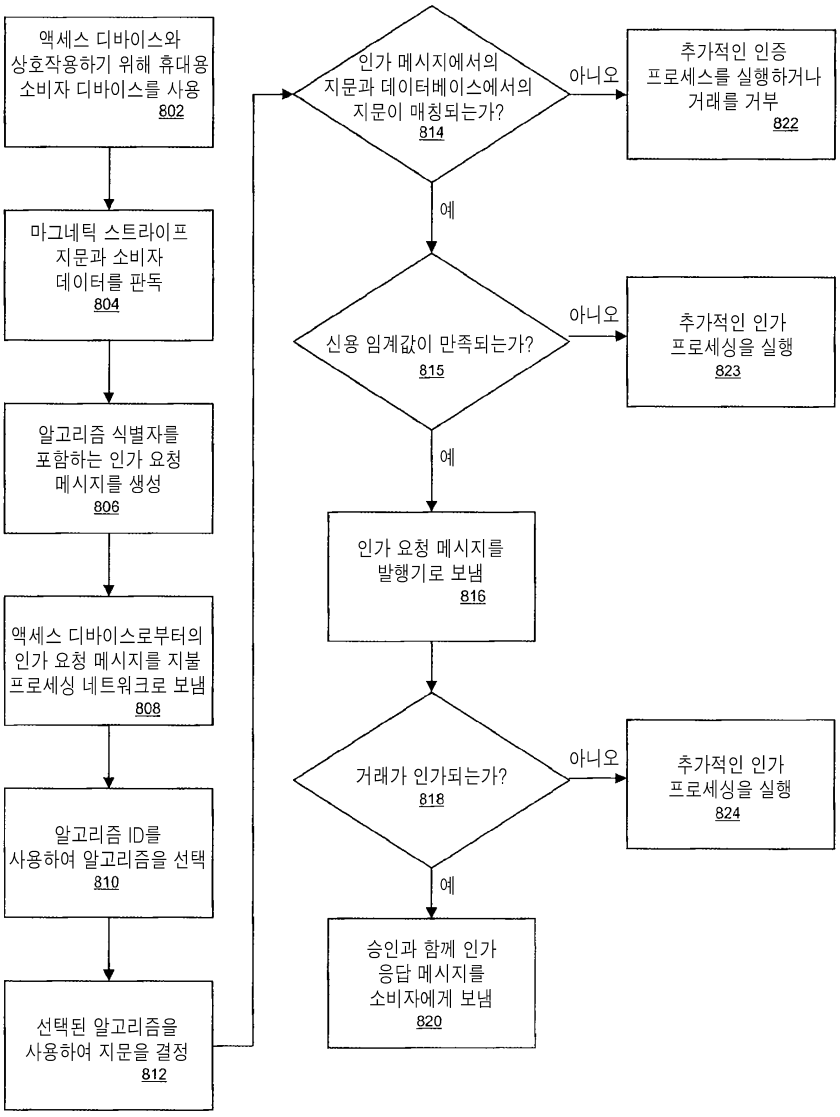
도면10a


소비자 A
730(a)
소비자 B
730(b)
소비자 C
730(c)
휴대용 소비자 디바이스 A
732(a)
휴대용 소비자 디바이스 B
732(b)
휴대용 소비자 디바이스 C
732(c)
액세스 디바이스 A
734(a)
액세스 디바이스 B
734(b)
액세스 디바이스 C
734(c)
상인 A
722(a)
상인 B
722(b)
상인 C
722(c)
획득기 A
724(a)
획득기 B
724(b)
획득기 C
724(c)
지불 프로세싱 네트워크 726
소비자 데이터베이스 726(b)
서버 컴퓨터 726(a)
알고리즘 데이터베이스 726(c)
발행기 A
728(a)
발행기 B
728(b)
발행기 C
728(c)
720

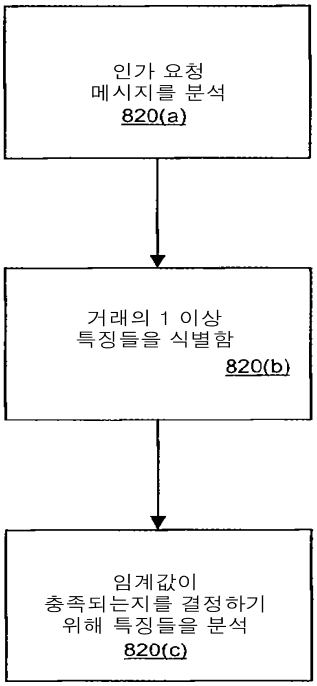
도면10b


알고리즘 식별 모듈 426(a)-1
신용 평가 모듈 426(a)-2
복호화 모듈 426(a)-3
데이터 포맷기 모듈 426(a)-4
서버 컴퓨터 426(a)

도면11


액세스 디바이스와 상호작용하기 위해 휴대용 소비자 디바이스를 사용
802
마그네틱 스트라이프 지문과 소비자 데이터를 판독
804
알고리즘 식별자를 포함하는 인가 요청 메시지를 생성
806
액세스 디바이스로부터의 인가 요청 메시지를 지불 프로세싱 네트워크로 보냄
808
알고리즘 ID를 사용하여 알고리즘을 선택
810
선택된 알고리즘을 사용하여 지문을 결정
812
인가 메시지에서의 지문과 데이터베이스에서의 지문이 매칭되는가?
814
아니오
추가적인 인증 프로세스를 실행하거나 거래를 거부
822
예
신용 임계값이 만족되는가?
815
아니오
추가적인 인가 프로세싱을 실행
823
예
인가 요청 메시지를 발행기로 보냄
816
거래가 인가되는가?
818
아니오
추가적인 인가 프로세싱을 실행
824
예
승인과 함께 인가 응답 메시지를 소비자에게 보냄
820

도면12


인가 요청
메시지를 분석
820(a)
거래의 1 이상
특징들을 식별함
820(b)
임계값이
충족되는지를 결정하기
위해 특징들을 분석
820(c)