



(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0111033  
(43) 공개일자 2014년09월17일

(51) 국제특허분류(Int. Cl.)  
*G06Q 20/32* (2012.01) *G06Q 20/20* (2012.01)

(21) 출원번호 10-2014-7022297

(22) 출원일자(국제) 2012년12월13일  
심사청구일자 없음

(85) 번역문제출일자 2014년08월08일

(86) 국제출원번호 PCT/US2012/069420

(87) 국제공개번호 WO 2013/106159  
국제공개일자 2013년07월18일

(30) 우선권주장  
13/363,592 2012년02월01일 미국(US)  
61/585,714 2012년01월12일 미국(US)

(71) 출원인  
**퀄컴 인코포레이티드**  
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775

(72) 발명자  
**아젠 존**  
미국 92121 캘리포니아주 샌디에고 모어하우스 드라이브 5775

**메넨데즈 호세**  
미국 92121 캘리포니아주 샌디에고 모어하우스 드라이브 5775  
(뒷면에 계속)

(74) 대리인  
**특허법인코리아나**

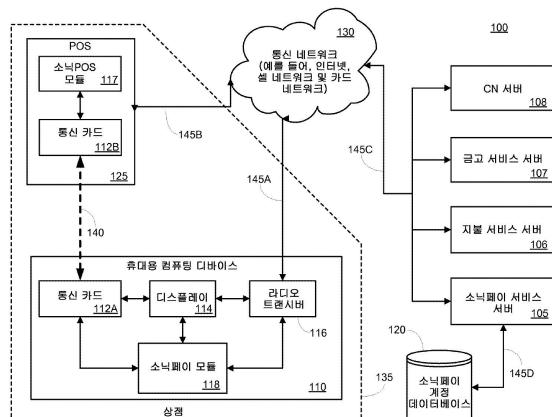
전체 청구항 수 : 총 80 항

(54) 별명의 명칭 휴대용 컴퓨터 디바이스를 이용한 오프라인 지불 거래들을 보안하는 시스템 및 방법

### (57) 요약

기밀성 지불 크레덴셜들을 송신하거나 제시함이 없이 구매 거래를 완료하기 위해 POS 시스템과 연관된 상인 및 PCD 와 연관된 소비자에게 제공하는 시스템 및 방법이 개시된다. 예시적인 실시형태에서, POS 와 PCD 사이에 데이터를 송신하기 위해 사운드가 이용된다. 지불 요청이 PCD 상에 렌더링된다. 소비자는 고유한 암호적 시그내쳐를 통해 검토 및 인가한다. 상인은 그것의 고유한 암호적 시그내쳐의 부가를 통해 승인한다. POS 와 통신하는 원격 서비스는 사전에 등록된 공개 키들을 통해 시그내쳐들을 검증한다. 거래는 그 다음 소비자 계정에 대해 결제된다. 확인이 POS 및 PCD 에 리턴된다. 유리하게, 거래는 PCD 가 온라인으로 됨이 없이 개시되고 완료된다. 또한, 소비자 지불 크레덴셜들은 PCD 상에 저장되거나 PCD 로부터 상인 POS 시스템으로 송신되지 않는다.

## 대 표 도



(72) 발명자

크랄 에릭

미국 92121 캘리포니아주 샌디에고 모어하우스 드  
라이브 5775

로즈 그렉

미국 92121 캘리포니아주 샌디에고 모어하우스 드  
라이브 5775

---

## 특허청구의 범위

### 청구항 1

지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법으로서,

상인과 연관된 POS (point of sale) 시스템에서 지불 요청을 생성하는 단계로서, 상기 지불 요청은 거래 금액을 포함하는, 상기 지불 요청을 생성하는 단계;

상기 POS 시스템으로부터 상기 지불 요청을 송신하는 단계;

상기 지불 요청을 승인하는 제 1 디지털 시그내쳐를 수신하는 단계;

상기 지불 요청을 승인하는 제 2 디지털 시그내쳐를 생성하는 단계; 및

상기 지불 요청과, 상기 제 1 및 제 2 디지털 시그내쳐들을 나타내는 데이터를 송신함으로써 상기 구매 거래를 완료하는 단계로서, 상기 구매 거래의 완료는 상기 상인과 연관된 계정으로 하여금 상기 거래 금액 만큼 입금되도록 하는, 상기 구매 거래를 완료하는 단계를 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법.

### 청구항 2

제 1 항에 있어서,

상기 지불 요청 및 제 1 디지털 시그내쳐는 사운드를 통해 송신되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법.

### 청구항 3

제 1 항에 있어서,

상기 지불 요청 및 제 1 디지털 시그내쳐는 근거리 무선통신 ("NFC") 표준을 통해 송신되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법.

### 청구항 4

제 1 항에 있어서,

상기 제 1 디지털 시그내쳐는 소비자와 고유하게 연관된 개인 키를 이용하여 생성되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법.

### 청구항 5

제 1 항에 있어서,

상기 제 2 디지털 시그내쳐는 상인과 고유하게 연관된 개인 키를 이용하여 생성되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법.

### 청구항 6

제 1 항에 있어서,

상기 제 1 및 제 2 디지털 시그내쳐들은 대응하는 공개 키들의 사용을 통해 검증가능한, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법.

### 청구항 7

제 1 항에 있어서,

상기 상인과 연관된 계정은 소비자와 연관된 계정에서 인출함으로써 입금되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법.

**청구항 8**

제 1 항에 있어서,

상기 상인과 연관된 계정은 제 3 자 지불 서비스와 연관된 저장된 가치 계정으로부터 입금되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법.

**청구항 9**

제 1 항에 있어서,

상기 구매 거래가 완료되었다는 것을 나타내는 영수증을 생성하는 단계를 더 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법.

**청구항 10**

제 9 항에 있어서,

상기 영수증을 송신하는 단계를 더 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법.

**청구항 11**

지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템으로서,

거래 금액을 포함하는 지불 요청을 생성하는 것;

상기 POS 시스템으로부터 상기 지불 요청을 송신하는 것;

상기 지불 요청을 승인하는 제 1 디지털 시그내쳐를 수신하는 것;

상기 지불 요청을 승인하는 제 2 디지털 시그내쳐를 생성하는 것; 및

상기 지불 요청과, 상기 제 1 및 제 2 디지털 시그내쳐들을 나타내는 데이터를 송신함으로써 상기 구매 거래를 완료하는 것으로서, 상기 구매 거래의 완료는 상기 상인과 연관된 계정으로 하여금 상기 거래 금액 만큼 입금되도록 하는, 상기 구매 거래를 완료하는 것

을 수행하기 위한, 상인과 연관된 POS (point of sale) 시스템을 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

**청구항 12**

제 11 항에 있어서,

상기 지불 요청 및 제 1 디지털 시그내쳐는 사운드를 통해 송신되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

**청구항 13**

제 11 항에 있어서,

상기 지불 요청 및 제 1 디지털 시그내쳐는 근거리 무선통신 ("NFC") 표준을 통해 송신되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

**청구항 14**

제 11 항에 있어서,

상기 제 1 디지털 시그내쳐는 소비자와 고유하게 연관된 개인 키를 이용하여 생성되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

**청구항 15**

제 11 항에 있어서,

상기 제 2 디지털 시그내쳐는 상인과 고유하게 연관된 개인 키를 이용하여 생성되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 16

제 11 항에 있어서,

상기 제 1 및 제 2 디지털 시그내쳐들은 대응하는 공개 키들의 사용을 통해 검증가능한, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 17

제 11 항에 있어서,

상기 상인과 연관된 계정은 소비자와 연관된 계정에서 인출함으로써 입금되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 18

제 11 항에 있어서,

상기 상인과 연관된 계정은 제 3 자 지불 서비스와 연관된 저장된 가치 계정으로부터 입금되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 19

제 11 항에 있어서,

상기 구매 거래가 완료되었다는 것을 나타내는 영수증을 생성하는 것을 더 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 20

제 19 항에 있어서,

상기 영수증을 송신하는 것을 더 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 21

지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템으로서,

상인과 연관된 POS (point of sale) 시스템에서 지불 요청을 생성하는 수단으로서, 상기 지불 요청은 거래 금액을 포함하는, 상기 지불 요청을 생성하는 수단;

상기 POS 시스템으로부터 상기 지불 요청을 송신하는 수단;

상기 지불 요청을 승인하는 제 1 디지털 시그내쳐를 수신하는 수단;

상기 지불 요청을 승인하는 제 2 디지털 시그내쳐를 생성하는 수단; 및

상기 지불 요청과, 상기 제 1 및 제 2 디지털 시그내쳐들을 나타내는 데이터를 송신함으로써 상기 구매 거래를 완료하는 수단으로서, 상기 구매 거래의 완료는 상기 상인과 연관된 계정으로 하여금 상기 거래 금액 만큼 입금 되도록 하는, 상기 구매 거래를 완료하는 수단을 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 22

제 21 항에 있어서,

상기 지불 요청 및 제 1 디지털 시그내쳐는 사운드를 통해 송신되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

### 청구항 23

제 21 항에 있어서,

상기 지불 요청 및 제 1 디지털 시그내쳐는 근거리 무선통신 ("NFC") 표준을 통해 송신되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

### 청구항 24

제 21 항에 있어서,

상기 제 1 디지털 시그내쳐는 소비자와 고유하게 연관된 개인 키를 이용하여 생성되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

### 청구항 25

제 21 항에 있어서,

상기 제 2 디지털 시그내쳐는 상인과 고유하게 연관된 개인 키를 이용하여 생성되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

### 청구항 26

제 21 항에 있어서,

상기 제 1 및 제 2 디지털 시그내쳐들은 대응하는 공개 키들의 사용을 통해 검증가능한, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

### 청구항 27

제 21 항에 있어서,

상기 상인과 연관된 계정은 소비자와 연관된 계정에서 인출함으로써 입금되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

### 청구항 28

제 21 항에 있어서,

상기 상인과 연관된 계정은 제 3 자 지불 서비스와 연관된 저장된 가치 계정으로부터 입금되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

### 청구항 29

제 21 항에 있어서,

상기 구매 거래가 완료되었다는 것을 나타내는 영수증을 생성하는 수단을 더 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

### 청구항 30

제 29 항에 있어서,

상기 영수증을 송신하는 수단을 더 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

### 청구항 31

컴퓨터 판독가능 프로그램 코드가 포함된 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품으로서,

상기 컴퓨터 판독가능 프로그램 코드는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법을 구현하도록 실행가능하고,

상기 방법은,

상인과 연관된 POS (point of sale) 시스템에서 지불 요청을 생성하는 단계로서, 상기 지불 요청은 거래 금액을 포함하는, 상기 지불 요청을 생성하는 단계;

상기 POS 시스템으로부터 상기 지불 요청을 송신하는 단계;

상기 지불 요청을 승인하는 제 1 디지털 시그내쳐를 수신하는 단계;

상기 지불 요청을 승인하는 제 2 디지털 시그내쳐를 생성하는 단계; 및

상기 지불 요청과, 상기 제 1 및 제 2 디지털 시그내쳐들을 나타내는 데이터를 송신함으로써 상기 구매 거래를 완료하는 단계로서, 상기 구매 거래의 완료는 상기 상인과 연관된 계정으로 하여금 상기 거래 금액 만큼 입금되도록 하는, 상기 구매 거래를 완료하는 단계를 포함하는, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

### 청구항 32

제 31 항에 있어서,

상기 지불 요청 및 제 1 디지털 시그내쳐는 사운드를 통해 송신되는, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

### 청구항 33

제 31 항에 있어서,

상기 지불 요청 및 제 1 디지털 시그내쳐는 근거리 무선통신 ("NFC") 표준을 통해 송신되는, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

### 청구항 34

제 31 항에 있어서,

상기 제 1 디지털 시그내쳐는 소비자와 고유하게 연관된 개인 키를 이용하여 생성되는, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

### 청구항 35

제 31 항에 있어서,

상기 제 2 디지털 시그내쳐는 상인과 고유하게 연관된 개인 키를 이용하여 생성되는, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

### 청구항 36

제 31 항에 있어서,

상기 제 1 및 제 2 디지털 시그내쳐들은 대응하는 공개 키들의 사용을 통해 검증가능한, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

### 청구항 37

제 31 항에 있어서,

상기 상인과 연관된 계정은 소비자와 연관된 계정에서 인출함으로써 입금되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

### 청구항 38

제 31 항에 있어서,

상기 상인과 연관된 계정은 제 3 자 지불 서비스와 연관된 저장된 가치 계정으로부터 입금되는, 컴퓨터 이용가

능 매체를 포함하는 컴퓨터 프로그램 제품.

#### 청구항 39

제 31 항에 있어서,

상기 방법은, 상기 구매 거래가 완료되었다는 것을 나타내는 영수증을 생성하는 단계를 더 포함하는, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

#### 청구항 40

제 39 항에 있어서,

상기 방법은, 상기 영수증을 송신하는 단계를 더 포함하는, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

#### 청구항 41

지불 요청의 디지털 시그내처를 통해 구매 거래를 완료하기 위한 방법으로서,

소비자와 연관된 휴대용 컴퓨팅 디바이스 ("PCD")에서 지불 요청을 수신하는 단계로서, 상기 지불 요청은 거래 금액을 포함하는, 상기 지불 요청을 수신하는 단계;

상기 지불 요청을 승인하는 디지털 시그내처를 생성하는 단계; 및

상기 PCD로부터 상기 지불 요청 및 상기 디지털 시그내처를 나타내는 데이터를 송신함으로써 상기 구매 거래를 완료하는 단계로서, 상기 구매 거래의 완료는 상기 소비자와 연관된 계정으로 하여금 상기 거래 금액 만큼 인출 되도록 하는, 상기 구매 거래를 완료하는 단계를 포함하는, 지불 요청의 디지털 시그내처를 통해 구매 거래를 완료하기 위한 방법.

#### 청구항 42

제 41 항에 있어서,

상기 지불 요청 및 디지털 시그내처는 사운드를 통해 송신되는, 지불 요청의 디지털 시그내처를 통해 구매 거래를 완료하기 위한 방법.

#### 청구항 43

제 41 항에 있어서,

상기 지불 요청 및 디지털 시그내처는 근거리 무선통신 ("NFC") 표준을 통해 송신되는, 지불 요청의 디지털 시그내처를 통해 구매 거래를 완료하기 위한 방법.

#### 청구항 44

제 41 항에 있어서,

상기 디지털 시그내처는 소비자와 고유하게 연관된 개인 키를 이용하여 생성되는, 지불 요청의 디지털 시그내처를 통해 구매 거래를 완료하기 위한 방법.

#### 청구항 45

제 41 항에 있어서,

상기 디지털 시그내처는 대응하는 공개 키의 사용을 통해 검증가능한, 지불 요청의 디지털 시그내처를 통해 구매 거래를 완료하기 위한 방법.

#### 청구항 46

제 41 항에 있어서,

상기 소비자와 연관된 계정은 상인과 연관된 계정에 입금함으로써 인출되는, 지불 요청의 디지털 시그내처를 통

해 구매 거래를 완료하기 위한 방법.

#### 청구항 47

제 41 항에 있어서,

상기 소비자와 연관된 계정은 제 3 자 지불 서비스와 연관된 저장된 가치 계정인, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법.

#### 청구항 48

제 41 항에 있어서,

상기 구매 거래가 완료되었다는 것을 나타내는 영수증을 수신하는 단계를 더 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법.

#### 청구항 49

제 41 항에 있어서,

상기 영수증을 렌더링하는 단계를 더 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법.

#### 청구항 50

제 41 항에 있어서,

상기 PCD 는 셀룰러 전화기인, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법.

#### 청구항 51

지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템으로서,

거래 금액을 포함하는 지불 요청을 수신하는 것;

상기 지불 요청을 승인하는 디지털 시그내쳐를 생성하는 것; 및

상기 PCD 로부터 상기 지불 요청 및 상기 디지털 시그내쳐를 나타내는 데이터를 송신함으로써 상기 구매 거래를 완료하는 것으로서, 상기 구매 거래의 완료는 상기 소비자와 연관된 계정으로 하여금 상기 거래 금액 만큼 인출 되도록 하는, 상기 구매 거래를 완료하는 것

을 수행하기 위한, 소비자와 연관된 휴대용 컴퓨팅 디바이스 ("PCD") 를 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 52

제 51 항에 있어서,

상기 지불 요청 및 디지털 시그내쳐는 사운드를 통해 송신되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 53

제 51 항에 있어서,

상기 지불 요청 및 디지털 시그내쳐는 근거리 무선통신 ("NFC") 표준을 통해 송신되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 54

제 51 항에 있어서,

상기 디지털 시그내쳐는 소비자와 고유하게 연관된 개인 키를 이용하여 생성되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

**청구항 55**

제 51 항에 있어서,

상기 디지털 시그내쳐는 대응하는 공개 키의 사용을 통해 검증가능한, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

**청구항 56**

제 51 항에 있어서,

상기 소비자와 연관된 계정은 상인과 연관된 계정에 입금함으로써 인출되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

**청구항 57**

제 51 항에 있어서,

상기 소비자와 연관된 계정은 제 3 자 지불 서비스와 연관된 저장된 가치 계정인, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

**청구항 58**

제 51 항에 있어서,

상기 구매 거래가 완료되었다는 것을 나타내는 영수증을 수신하는 것을 더 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

**청구항 59**

제 58 항에 있어서,

상기 영수증을 렌더링하는 것을 더 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

**청구항 60**

제 51 항에 있어서,

상기 PCD 는 셀룰러 전화기인, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

**청구항 61**

지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템으로서,

소비자와 연관된 휴대용 컴퓨팅 디바이스 ("PCD") 에서 지불 요청을 수신하는 수단으로서, 상기 지불 요청은 거래 금액을 포함하는, 상기 지불 요청을 수신하는 수단;

상기 지불 요청을 승인하는 디지털 시그내쳐를 생성하는 수단; 및

상기 PCD 로부터 상기 지불 요청 및 상기 디지털 시그내쳐를 나타내는 데이터를 송신함으로써 상기 구매 거래를 완료하는 수단으로서, 상기 구매 거래의 완료는 상기 소비자와 연관된 계정으로 하여금 상기 거래 금액 만큼 인출되도록 하는, 상기 구매 거래를 완료하는 수단을 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

**청구항 62**

제 61 항에 있어서,

상기 지불 요청 및 디지털 시그내쳐는 사운드를 통해 송신되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

**청구항 63**

제 61 항에 있어서,

상기 지불 요청 및 디지털 시그내쳐는 근거리 무선통신 ("NFC") 표준을 통해 송신되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 64

제 61 항에 있어서,

상기 디지털 시그내쳐는 소비자와 고유하게 연관된 개인 키를 이용하여 생성되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 65

제 61 항에 있어서,

상기 디지털 시그내쳐는 대응하는 공개 키의 사용을 통해 검증가능한, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 66

제 61 항에 있어서,

상기 소비자와 연관된 계정은 상인과 연관된 계정에 입금함으로써 인출되는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 67

제 61 항에 있어서,

상기 소비자와 연관된 계정은 제 3 자 지불 서비스와 연관된 저장된 가치 계정인, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 68

제 61 항에 있어서,

상기 구매 거래가 완료되었다는 것을 나타내는 영수증을 수신하는 수단을 더 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 69

제 68 항에 있어서,

상기 영수증을 렌더링하는 수단을 더 포함하는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 70

제 61 항에 있어서,

상기 PCD 는 셀룰러 전화기인, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 시스템.

#### 청구항 71

컴퓨터 판독가능 프로그램 코드가 포함된 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품으로서,

상기 컴퓨터 판독가능 프로그램 코드는, 지불 요청의 디지털 시그내쳐를 통해 구매 거래를 완료하기 위한 방법을 구현하도록 실행가능하고,

상기 방법은,

소비자와 연관된 휴대용 컴퓨팅 디바이스 ("PCD") 에서 지불 요청을 수신하는 단계로서, 상기 지불 요청은 거래 금액을 포함하는, 상기 지불 요청을 수신하는 단계;

상기 지불 요청을 승인하는 디지털 시그내처를 생성하는 단계; 및

상기 PCD로부터 상기 지불 요청 및 상기 디지털 시그내처를 나타내는 데이터를 송신함으로써 상기 구매 거래를 완료하는 단계로서, 상기 구매 거래의 완료는 상기 소비자와 연관된 계정으로 하여금 상기 거래 금액 만큼 인출 되도록 하는, 상기 구매 거래를 완료하는 단계를 포함하는, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

#### 청구항 72

제 71 항에 있어서,

상기 지불 요청 및 디지털 시그내처는 사운드를 통해 송신되는, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

#### 청구항 73

제 71 항에 있어서,

상기 지불 요청 및 디지털 시그내처는 근거리 무선통신 ("NFC") 표준을 통해 송신되는, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

#### 청구항 74

제 71 항에 있어서,

상기 디지털 시그내처는 소비자와 고유하게 연관된 개인 키를 이용하여 생성되는, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

#### 청구항 75

제 71 항에 있어서,

상기 디지털 시그내처는 대응하는 공개 키의 사용을 통해 검증가능한, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

#### 청구항 76

제 71 항에 있어서,

상기 소비자와 연관된 계정은 상인과 연관된 계정에 입금함으로써 인출되는, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

#### 청구항 77

제 71 항에 있어서,

상기 소비자와 연관된 계정은 제 3 자 지불 서비스와 연관된 저장된 가치 계정인, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

#### 청구항 78

제 71 항에 있어서,

상기 방법은, 상기 구매 거래가 완료되었다는 것을 나타내는 영수증을 수신하는 단계를 더 포함하는, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

#### 청구항 79

제 78 항에 있어서,

상기 방법은, 상기 영수증을 렌더링하는 단계를 더 포함하는, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

## 청구항 80

제 71 항에 있어서,

상기 PCD 는 셀룰러 전화기인, 컴퓨터 이용가능 매체를 포함하는 컴퓨터 프로그램 제품.

## 명세서

### 기술분야

[0001]

2012년 1월 12일 출원되고 양도된 출원 번호 제 61/585,714 호인 "SYSTEM AND METHOD FOR SECURE OFFLINE PAYMENT TRANSACTIONS USING A PORTABLE COMPUTING DEVICE" 라는 제목의 미국 출원에 대해 35 U.S.C. § 119(e) 하의 우선권이 주장되고, 그 전체 내용들은 참조에 의해 본원에 통합된다.

### 배경기술

[0002]

비현금 통화 유형들이 오늘날의 사회에서 아주 흔하다. 소비자들은, 임의의 수의 계정 유형들과 연관될 수도 있는 지불 토큰들을 상인들에게 제공함으로써 상품들 및 서비스들을 구매하기 위한 거래들에 일상적으로 참여한다. 보안되거나 보안되지 않은 크레디트의 라인들과 연관된 "크레디트 카드 (credit card)" 토큰들 (tokens) 및 저장된 가치 계정들 (stored value accounts) 과 연관된 "기프트 카드 (gift card)" 또는 "데빗 카드 (debit card)" 토큰들은 오늘날 시장에서 사용되는 비현금 통화의 통상적인 예들이다.

[0003]

토큰들에 의해 표현된 지불 크레덴셜들 (credentials) 은, 그 크레덴셜들이 허가되지 않은 사용자에 의해 유용되지 않도록, 본질적으로 비밀이고 보호되어야 한다. 그렇기는 하지만, 물리적인 크레디트 카드의 사용자는, 예를 들어, 매장에서 구매 거래 (purchase transaction) 를 완료하기 위해 상인에게 지불 크레덴셜들을 자유롭게 넘겨주어야 한다. 이러한 지불 크레덴셜들의 보안되지 않은 사용을 나타내는 통상적인 시나리오는 소비자가 식당에서 식사에 대한 지불을 위해 크레디트 카드를 사용하는 것이다. 많은 이러한 경우들에서, 소비자는 계산서를 검토한 다음, 토큰 상의 지불 크레덴셜들이 거래 동안 및 거래 후에 보호될 것이라고 믿고 그의 물리적인 크레디트 카드를 실제로 서버에 넘겨준다.

[0004]

스마트폰들과 같은 휴대용 컴퓨팅 디바이스들 (portable computing devices) ("PCD") 을 사용하는 일부 지불 시스템들 및 방법들은 매장에서 물리적인 지불 토큰을 이용하는 고유한 불안을 해결한다. 이들 시스템들에서, 소비자 및 상인은 통상적으로 "클라우드에서 (in the cloud)" 거래를 완료하도록 요구된다. 원격 서비스에서 거래의 결제를 동시에 허가하기 위해 상인은 그의 POS (point of sale) 시스템을 이용하고 소비자는 그의 PCD 를 이용한다. 몇몇 이러한 방법들은 소비자가 POS 에서 크레덴셜들을 렌더링하고 클라우드에서 결제를 허가하는 것을 필요로하는 한편, 다른 방법들은 전체 거래를 원격으로 수행할 수도 있다. 특히, 이러한 시스템 및 방법들이 지불 크레덴셜들의 물리적인 제시를 필수적으로 요구하는 것은 아님에도 불구하고, 상인 및 소비자 양자 모두가 거래를 수행하기 위해 "온라인 (online)" 이어야 한다는 것은 정말로 단점이다. 또한, 몇몇 이러한 시스템들 및 방법들은 지불 크레덴셜들이 PCD 에 저장되고/되거나 거래 프로세스 동안 디지털로 전송되는 것을 요구하고, 따라서, 크레덴셜들의 보안을 잠재적으로 손상시킨다.

[0005]

지불 크레덴셜들을 이용하여 거래들을 결제하기 위한 임의의 시스템 및 방법의 핵심은 인증의 발행, 즉, 그들 크레덴셜들과 연관된 계정이 인출되기 전에 소비자가 지불 크레덴셜들을 사용하도록 허가되는 것을 제공하는 것이다. 현재의 시스템들 및 방법들은, 크레덴셜들의 사용자의 인증 동안이든 거래 결제의 실제 프로세스 동안이든 간에, 지불 크레덴셜들의 기밀성이 손상되는 것을 야기할 수 있다. 또한, POS 에서 지불 거래들을 결제하기 위해 PCD 를 이용하는 현재의 시스템들 및 방법들은 PCD 가 거래 동안 온라인일 것을 요구한다. 따라서, PCD 를 이용하여 오프라인 (offline) 으로 지불 거래들을 수행하기 위한 시스템 및 방법이 당해 기술 분야에서 필요하다. 또한, 지불 크레덴셜들이 PCD 상에 저장되고/되거나 PCD 로부터 POS 시스템으로 전송되는 것을 요구함이 없이 PCD 를 이용하여 오프라인으로 지불 거래를 수행하는 시스템 및 방법이 당해 기술분야에서 필요하다.

### 발명의 내용

### 과제의 해결 수단

[0006]

소비자의 PCD 와 상인의 POS 시스템 사이에 공유된 암호적 인가들 (cryptographic authorizations) 을 이용하

여 구매 거래 (purchase transaction) 를 완료하기 위한 방법들 및 시스템들의 다양한 실시형태들이 설명된다. 실시형태들에 따르면, 구매 거래를 수행하기 이전에, PCD 와 연관된 소비자 및 POS 시스템과 연관된 상인 양자는 원격 서비스와의 등록 프로세스를 완료했을 것이다. 예시적인 실시형태에 따라 구매 거래를 수행하기 위해, 소비자 PCD 및 상인 POS 시스템은 상점 환경에서 물리적으로 근접할 수도 있다. 하지만, 특히, 구매 거래들이 소비자 PCD 와 상인 POS 시스템 사이에 원격 통신 등을 통해 수행될 수도 있음에 따라, 어떤 실시형태들은 소비자 PCD 와 상인 POS 시스템이 물리적으로 근접하도록 요구하지 않을 것이라는 것이라는 생각된다.

[0007] 판매시점에서, 소비자 PCD 는 상인 POS 시스템으로부터 송신된 지불 요청 (payment request) 을 수신한다. 지불 요청은, 소비자가 POS 시스템과 연관된 상인으로부터 구매하기를 희망하는 상품 또는 서비스에 대한 청구서 (invoice) 에 상당할 수도 있다. 지불 요청은 POS 시스템으로부터 PCD 로 무선으로 송신될 수도 있고, 몇몇 실시형태들에서, 일련의 가청 톤들 (audible tones) 을 이용하여 무선으로 송신된다. 따라서, 이러한 예시적인 사운드-기반 실시형태들에서, POS 시스템 및 PCD (110) 는 사운드를 통해 데이터를 송신 및 수신하도록 구성되는 마이크로폰 및 스피커들을 구비한다.

[0008] PCD 에서 지불 요청의 수신 시, PCD 는 소비자에 의한 검토를 위해 지불 요청을 렌더링 (render) 하도록 동작가능할 수도 있다. 검토 후, 소비자는, PCD 로 하여금 사용자와 연관된 고유한 개인 키 (private key) 로 지불 요청을 디지털로 사인 (sign) 하게 하는 개인 식별 번호 (personal identification number; PIN) 를 입력함으로써 지불 요청을 승인할 수도 있다. 암호 기술분야에서 이해되는 바와 같이, 개인 키는 상보적인 공개 키 (public key) 의 홀더 (holder) 에 대해 소비자의 아이덴티티 (identity) 를 확인시키는 기능을 할 수도 있다. 디지털 시그내처 (digital signature) 는 다시 POS 시스템으로 송신되고, 이 POS 시스템에서, 상인과 연관된 디지털 시그내처가 또한 부가되며, 따라서, 상인의 거래의 승인을 나타낸다. 지불 요청 및 고유한 디지털 시그내처들은 후속하여 네트워크 연결을 통해 상인 POS 시스템으로부터 원격 서비스로 포워딩된다.

[0009] 지불 요청의 승인을 나타내는, 거래 당사자들 (상인 및 소비자) 의 디지털 시그내처들을 수신 시, 원격 서비스는, 소비자 및 상인 각각의 아이덴티티들을 확인하는데 사용하기 위해 소비자 및 상인에 의해 그 서비스에 사전에 업로드된 공개 키를 이용할 수도 있다. 몇몇 실시형태들에서, 원격 서비스는, 소비자와 연관된 복수의 계정들 (accounts) 중 어떤 하나가 지불 요청 총액에 따라 인출되어야하는 것을 사인된 지불 요청 내에 포함된 소비자의 프로파일 (profile) 또는 데이터로부터 결정할 수도 있다. 또한, 시스템의 몇몇 실시형태들은 사전정의된 규칙들 또는 알고리즘들에 따라 소비자 계정들을 선택하기 위한 수단을 포함할 수도 있다는 것이 생각된다.

[0010] 일단 당사자들의 아이덴티티들이 확인되면, 원격 서비스는 사전에 등록된 소비자 계정에 대해 포인팅하는 토큰을 식별하기 위해 데이터베이스에 쿼리 (query) 할 수도 있다. 그 서비스는 그 다음, 토큰 및 지불 요청을 게이트웨이/카드 프로세서에 포워딩 (forwarding) 함으로써 식별된 소비자 계정에 대해 거래를 결제하기 위해 토큰을 레버리지 (leverage) 한다. 게이트웨이/카드 프로세서는 그 다음, 금고 서비스 (vault service) 로부터 소비자의 지불 크레덴셜들을 요청하기 위해 그 토큰을 이용할 수도 있다. 일단 지불 크레덴셜들이 금고 서비스로부터 수신되면, 크레디트 카드 프로세싱의 기술분야에서 이해되는 바와 같이, 카드 프로세서는 그 크레덴셜들을 이용하여 지불 요청의 금액 만큼 연관된 계정에 대해 인출한다. 몇몇 실시형태들에서, 거래가 소비자 계정에 대해 결제되었다는 확인 (confirmation) 이 원격 서비스에 의해 저장되고 POS 시스템에 리턴된다. 후속하여, POS 시스템은 영수증 (receipt) 을 생성하고 이를 소비자의 PCD 에 무선으로 송신할 수도 있다.

[0011] 유리하게, 예시적인 방법들을 통해 완료된 구매 거래는, 소비자 PCD 가 온라인이거나 그 외에 원격 서비스와 통신하는 일 없이 일어난다. 즉, PCD 와 POS 시스템 사이에서 송신되는 데이터는 완전히 상점 내의 2 개의 컴퓨포넌트들 사이에서 무선으로 교환된다. 또한, 구매 거래는, 소비자 지불 크레덴셜들이 PCD 상에 저장되거나 그 문제를 위해 PCD 시스템으로부터 상인 POS 시스템으로 송신되는 일 없이 개시 및 완료된다.

## 도면의 간단한 설명

[0012] 도면들에서, 동일한 참조 부호들은 다르게 표시되지 않는 한 다양한 도들에 걸쳐 동일한 부분들을 지칭한다. "102A" 또는 "102B" 와 같은 문자 표시들을 갖는 참조 부호들에 대해, 문자 표시들을 갖는 참조 부호들에 있어서, 문자 표시들은 동일 도면에 존재하는 2 개의 유사한 부분들 또는 엘리먼트들을 차별화할 수도 있다. 참조 부호들에 대한 문자 표시들은 참조 부호가 모든 도면들에서 동일한 참조 부호를 갖는 모든 부분들을 포함하는 것으로 의도되는 경우 생략될 수도 있다.

도 1 은 소비자의 PCD 와 상인의 POS 시스템 사이에 공유된 암호적 인가들을 이용하여 구매 거래를 완료하기 위한 시스템의 예시적인 컴포넌트들을 나타내는 하이 레벨 다이어그램이다.

도 2 는 도 1 시스템에 포함될 수도 있는 PCD 와 POS 시스템의 예시적인 양태들을 나타내는 기능적 블록도이다.

도 3 은 도 1 의 시스템의 양태들에 대한 예시적인 컴퓨터 구조의 다이어그램이다.

도 4 는 도 2 에 대응하는 무선 전화를 포함하는 PCD 의 예시적이고 비제한적 양태의 다이어그램이다.

도 5 는, 소비자의 PCD 와 상인의 POS 시스템 사이에 공유된 암호적 인가들을 이용하여 구매 거래를 완료하기 위한 시스템의 소비자 사용자를, 지불 크레덴셜 금고 서비스로, 등록하기 위한 예시적인 방법을 나타내는 논리적 흐름도이다.

도 6 은, 소비자의 PCD 와 상인의 POS 시스템 사이에 공유된 암호적 인가들을 이용하여 구매 거래를 완료하기 위한 시스템의 소비자 사용자를, 제 3 자 지불 서비스로, 등록하기 위한 예시적인 방법을 나타내는 논리적 흐름도이다.

도 7 은, 소비자의 PCD 와 상인의 POS 시스템 사이에 공유된 암호적 인가들을 이용하여 구매 거래를 완료하기 위한 시스템의 상인 사용자의 카드 네트워크 프로세서 크레덴셜들을 등록하기 위한 예시적인 방법을 나타내는 논리적 흐름도이다.

도 8 은, 소비자의 PCD 와 상인의 POS 시스템 사이에 공유된 암호적 인가들을 이용하여 구매 거래를 완료하기 위한 시스템의 상인 사용자의 제 3 자 지불 서비스 계정을 등록하기 위한 예시적인 방법을 나타내는 논리적 흐름도이다.

도 9 는, 소비자의 PCD 와 상인의 POS 시스템 사이에 공유된 암호적 인가들을 이용하여 카드 네트워크 프로세서를 통해 구매 거래를 완료하기 위한 예시적인 방법을 나타내는 논리적 흐름도이다.

도 10 은, 소비자의 PCD 와 상인의 POS 시스템 사이에 공유된 암호적 인가들을 이용하여 제 3 자 지불 서비스 계정을 통해 구매 거래를 완료하기 위한 예시적인 방법을 나타내는 논리적 흐름도이다.

### 발명을 실시하기 위한 구체적인 내용

[0013] "예시적인" 이라는 단어는 본원에서 "예, 경우, 또는 예시로서 기능하는" 것을 의회하기 위해 사용된다. "예시적인" 것으로서 본원에 설명된 임의의 양태는 다른 양태들에 대해 바람직하거나 이로운 것으로서 해석될 필요는 없다.

[0014] 이 설명에서, "애플리케이션 (application)" 및 "앱 (app)" 이라는 용어들은, 객체 코드, 스크립트들, 바이트 코드, 마크업 언어 파일들, 및 패치들과 같은 실행가능한 콘텐츠를 갖는 파일들을 또한 포함할 수도 있다. 또한, 본원에서 지칭되는 "애플리케이션" 또는 "앱" 은 오픈될 필요가 있을 수도 있는 문서들 또는 액세스될 필요가 있을 수도 있는 다른 데이터 파일들과 같은, 성질상 실행가능하지 않은 파일들을 또한 포함할 수도 있다.

[0015] "콘텐츠 (content)" 라는 용어는 객체 코드, 스크립트들, 바이트 코드, 마크업 언어 파일들, 및 패치들과 같은 실행가능한 콘텐츠를 갖는 파일들을 또한 포함할 수도 있다. 또한, 본원에서 지칭된 "콘텐츠" 는, 오픈될 필요가 있을 수도 있는 문서들 또는 액세스될 필요가 있을 수도 있는 다른 데이터 파일들과 같은, 성질상 실행 가능하지 않은 파일들을 또한 포함할 수도 있다.

[0016] 이 설명에서 사용된 바와 같이, "컴포넌트", "데이터베이스", "모듈", "시스템" 등의 용어들은, 하드웨어, 펌웨어, 하드웨어와 소프트웨어의 결합, 소프트웨어, 또는 실행 중의 소프트웨어 중 어느 일방과 같은 컴퓨터 관련 엔티티를 지칭하는 것으로 의도된다. 예를 들어, 모듈은, 프로세서 상에서 실행되는 프로세스, 프로세서, 오브젝트, 실행가능체, 실행 스레드, 프로그램, 및/또는 컴퓨터일 수도 있고, 하지만 이에 한정되는 것은 아니다. 예시적으로, 컴퓨팅 디바이스 상에서 실행되는 애플리케이션 및 그 컴퓨팅 디바이스 양자 모두는 모듈일 수도 있다. 하나 이상의 모듈들은 프로세스 및/또는 실행 스레드 내에 상주할 수도 있고, 모듈은 하나의 컴퓨터 상에 국부화될 수도 있고, 및/또는 2 개 이상의 컴퓨터들 사이에 분포될 수도 있다. 또한, 이들 모듈들은 다양한 데이터 구조들이 저장된 다양한 컴퓨터 판독가능 매체로부터 실행될 수도 있다. 모듈들은, 하나 이상의 데이터 패킷들 (로컬 시스템, 분산 시스템에서, 및/또는 신호에 의해 다른 시스템들과 인터넷 또는 로컬 WiFi 와 같은 네트워크를 통해 다른 모듈과 상호작용하는 하나의 모듈로부터의 데이터) 을 갖는 신호에 따라서 등과 같이 로컬 및/또는 원격 프로세스들에 의해 통신할 수도 있다.

[0017] 이 설명에서, "모바일 디바이스" 및 "휴대용 컴퓨팅 디바이스" ("PCD")라는 용어들은, 배터리와 같은 제한된 용량의 전력 공급기를 통해 동작하고 펜과 같은 어떤 능동 냉각 디바이스들을 갖지 않는 임의의 디바이스를 설명하기 위해 사용된다. 배터리로 동작되는 PCD들은 수십년동안 사용되고 있음에도 불구하고, 제3세대 ("3G") 무선 기술의 출현과 연계된 재충전가능한 배터리들에서의 기술적인 진보들은 수많은 PCD들이 다수의 성능들을 갖는 것을 가능하게 하였다. 따라서, PCD는 셀룰러 전화기, 위성 전화기, 페이저, PDA, 스마트폰, 내비게이션 디바이스, 스마트북 또는 리더, 미디어 플레이어, 전술한 디바이스들의 결합, 태블릿으로 무선 접속을 갖는 랩톱 컴퓨터, 그 외 기타일 수도 있다.

[0018] 본원에 설명된 시스템 및 방법의 실시형태들은, POS에서의 보안 디지털 사인을 통해, 당해 기술분야에서의 전술한 필요성들 및 당해 기술분야에서의 다른 필요성들에 대한 솔루션을 제공하는 것을 모색한다. 토큰에 의해 지불하기 위한 임의의 시스템의 핵심은 인증 (authentication)이고, 이것은 토큰 홀더에게 토큰과 연관된 지불 크레덴셜들에 의해 표현되는 자원에 대한 액세스를 그에게 주기 전이라고 그가 말하는 것을 제공한다. 토큰 시스템에 의한 지불에서의 인증의 필연적 결과로서, 구매 거래를 완료하기 위해 그들을 이용하는 동안에도, 지불 크레덴셜들에 대해 비밀을 유지하기를 희망하는 것이다. 따라서, 시스템들 및 방법들의 실시형태들은 일정 지불 크레덴셜들과 연관된 소비자가, 상인 또는 그의 POS 시스템에 대해 기밀성 지불 크레덴셜들을 송신하는 것, 웬더링하는 것, 또는 그외에 드러내는 것 없이 POS에서 구매 거래를 완료하는 것을 가능하게 한다.

[0019] 예시적인 실시형태들은, 소비자들 및 상인들이, 프로세스에서 소비자의 지불 크레덴셜들을 드러냄이 없이, 소비자의 PCD와 상인의 POS 시스템 사이에 구매 및 승인/인가 데이터를 송신하기 위해 가청 또는 초음파 송신물들을 이용하여 보안 모바일 지불 거래들을 수행하는 것을 가능하게 한다. 소비자의 PCD와 상인의 POS 시스템은, 거래에 대한 당사자들에 의해 액세스가능하지 않은 보안 채널들을 통해 후위 (backend) 시스템에서 상인의 계정에 입금하고 소비자의 계정에서 인출함으로써 거래가 종국적으로 결제되기 전에 당사자들 사이에 구매 거래 데이터 및 승인/인가 데이터가 교환될 수 있도록, 시스템의 전위 (front end)에서 페어링된다 (paired).

[0020] 특히, 비록 일부 실시형태들은 소비자 PCD와 상인 POS 간에 비-기밀성 데이터를 교환하기 위해 사운드 (sound)를 이용할 수도 있는 것이 고려되지만, 다른 실시형태들은 비제한적으로 근거리 무선통신 (near field communications; NFC), QR 코드를 등과 같이, 페어링된 디바이스들 사이에 데이터를 공유하기 위해 다른 프로토콜들을 이용할 수도 있는 것이 고려된다. 그렇기는 하지만, PCD와 POS 시스템 사이에 데이터를 송신하기 위해 사운드를 이용하는 실시형태들의 이점은, 상인과 소비자 모바일 디바이스들이 이미 필요한 하드웨어 컴포넌트들 (즉, 마이크로폰 및 스피커)을 포함할 수도 있기 때문에, 기존의 모바일 지불 시스템들에 솔루션을 통합하는 것의 용이성이다.

[0021] 어떤 실시형태들은 소비자 및 상인 양자 모두가 지불 거래를 수행하기 이전에 온라인 등록할 것을 필요로 한다. 유리하게, 일단 상인 및 소비자가 온라인 등록 프로세스를 완료하면, 소비자는, 구매 시에 상인의 POS와 오직 인가 데이터만이 공유되기 때문에, 상인과 구매 거래를 완료하기 위해 온라인이도록 요구되지 않는다. 지불 거래를 개시하기 위해, 지불 요청이 상인의 POS 시스템으로부터 소비자의 PCD로 송신된다. 지불 요청은, 상인 ID, 항목 설명들, 총 가격들 등을 나타내는 데이터를 포함할 수도 있고, 하지만 이에 한정되는 것은 아니다. 지불 요청 수신 시에, 소비자의 PCD는 소비자에 의한 승인을 위해 그것을 웬더링할 수도 있다.

지불 요청이 만족스러운 경우에, 소비자는, PCD의 사용자 인터페이스를 이용하여 개인 식별 번호 ("PIN")를 입력함으로써, 그 지불 요청을 디지털로 사인하고 그에 의해 그것을 승인할 수도 있다. PIN의 입력은 PCD로 하여금, 소비자의 인가의 증거로서 기능하도록 암호화된 디지털 시그내쳐를 송신함으로써 상인의 POS 시스템에 응답하게 한다. 특히, 소비자 PCD로부터 상인 POS 시스템으로 송신된 디지털 시그내쳐는 특정 구매 거래와 고유하게 연관되고, 따라서, 그것은 사기성 거래를 생성하기 위해 상인 또는 다른 당사자에 의해 다시 사용될 수 없다.

[0022] 일단 POS 시스템이 사용자로부터 디지털로 사인된 지불 요청을 수신하면, 상인은 그 자신의 개인 키를 이용하여 지불 요청을 디지털로 사인함으로써 지불 요청을 또한 승인할 수도 있다. 상인 POS는 그 다음, 사인된 지불 요청을 소비자 및 상인 양자 모두가 사전에 등록한 원격 서비스에 송신할 수도 있다. 소비자 및 상인의 시그내쳐들 및 신원 (identification)을 검증하기 위해 공개 키들을 이용하여, 암호 기술분야에서 통상의 지식을 가진 자에 의해 이해되는 바와 같이, 원격 서비스는 카드 네트워크, 지불 서비스 등에 대해 프록시를 통해 구매 거래를 처리 및 결제하는 것을 진행 (즉, 일 당사자와 연관된 계정에 입금 및 타방과 연관된 계정에서 인출) 할 수도 있다. 지불 거래는 완료되고, 유리하게는, 소비자와 연관된 지불 크레덴셜들은 POS에서 공유

되지 않았다.

[0023] 이제 도면들로 가서, 소비자의 PCD 와 상인의 POS 시스템 사이에 공유된 암호적 인가들을 이용하여 구매 거래를 완료하기 위한 예시적인 시스템들 및 방법들이 자세히 설명된다. 도 1 을 참조하면, 소비자의 PCD (110) 와 상인의 POS 시스템 (125) 사이에 공유된 암호적 인가들을 이용하여 구매 거래를 완료하기 위한 시스템 (100) 의 예시적인 컴포넌트들을 나타내는 하이 레벨 다이어그램이 도시된다. 예시적인 시스템 (100) 의 도시된 컴포넌트들은 상인 POS 단말기 또는 등록기 (125) 와 상점 (135) 에서 그룹핑된 PCD (110) 를 포함한다. 상인 POS 단말기 또는 등록기 (125) 는, 비제한적으로 금전 등록기, 데스크톱 컴퓨터, 랩톱 컴퓨터, 개인 휴대 정보 단말기, 태블릿 컴퓨터, 스캐너, 셀룰러 "스마트" 폰 등과 같이 상품들 또는 서비스들에 대한 지불에서 데이터를 수신하도록 동작가능한 임의의 컴포넌트, 애플리케이션 또는 시스템일 수도 있다. 이와 같이, 당해 기술 분야에서 통상의 지식을 가진 자 (이하, '당업자' 라 함) 는, 상인 POS 단말기 또는 등록기는, 후속하는 도면들과 관련하여 보다 자세히 설명될 PCD (110) 에 대해 형태 및 기능 면에서 비교가능할 수도 있다.

[0024] 중요하게, 몇몇 실시형태들에서 상점 (135) 은 PCD (110) 및 POS 시스템 (125) 이 물리적으로 근접한 장소일 수도 있는 한편, 다른 실시형태들은, PCD (110) 와 POS 시스템 (125) 이 물리적으로 공동 위치되지 않는, 웹사이트 또는 원격통신과 같이, 구매 거래들을 위한 가상 상점 (135) 을 포함할 수도 있다는 것이 고려된다.

[0025] PCD (110) 와 연관된 소비자와 POS 시스템 (125) 과 연관된 상인 사이의 구매 거래를 유효화하기 위한 레버리징 시스템 (100) 은 많은 유용한 애플리케이션들을 갖는다. 간단하게, 그리고 예시를 위한 기초를 제공하기 위해, 개시된 시스템들 및 방법들의 몇몇 실시형태들의 양태들이 적합하게 설명될 수도 있는 비제한적인 애플리케이션 시나리오는 PCD (110) 의 사용자가 고유한 지불 크레덴셜들을 갖는 복수의 가치 계정들 (value accounts) 과 연관되는 것을 고려할 수도 있다. 복수의 가치 계정들은 PCD (110) 의 사용자와 고유하게 연관되고, 크레디트 계정 및/또는 저장된 가치 계정들 (예를 들어, 상인-특정 기프트 카드 계정들) 의 임의의 조합을 포함할 수도 있다. 추가적으로 예시하면, 상인 시설은 가상이든 물리적이든, 상점 (135) 에 의해 표현될 수도 있다.

[0026] PCD (110) 와 연관된 사용자/소비자는 "소닉페이 (SonicPay)" 모듈 (118) 을 실행하는 PCD (110) 를 이용하여 상인의 가게 (135) 에 진입한다. 상인의 가게 (135) 는, PCD (110) 가 데이터를 온라인으로 무선으로 송신 할 수 없는, 즉, 수신을 갖지 않는 지하 쇼핑몰에 위치한다. 소비자는 POS 시스템 (125) 과 연관된 상인에 대해 구매를 위한 상품들을 제시한다. 상인은 구매를 위한 상품들을 "입력 (rings up)" 하고, 소비자에게 구매 총액을 제공하고, 지불 방법에 대해 묻는다.

[0027] 당업자에게 알려진 바와 같이, 소비자는 비제한적으로 현금, 크레디트, 기프트 카드, 데빗 카드 등을 포함하는 임의의 수의 지불 방법들을 선택할 수도 있다. 특히, 본질적으로 익명인 현금에 의한 지불을 제외하고는, 지불의 종래 방법들의 각각은 소비자가 상인에게 지불 크레덴셜들의 형태로 기밀성, 또는, 의사-기밀성 데이터를 제공할 것을 요구한다. 하지만, 예시적인 시나리오에서, PCD (110) 와 연관된 소비자는 "소닉페이" 시스템에 의한 지불을 선정하고, PCD (110) 로 하여금 POS 시스템 (125) 으로부터의 지불 요청에 대해 "리스닝 (listen)" 하게 한다. 예시적인 시스템들 및 방법들과 관련된 "소닉 (sonic)" 이라는 용어의 사용은 본 개시를 PCD (110) 와 POS 시스템 (125) 사이에 데이터를 전송하기 위한 수단으로서 사운드의 사용에 제한하지 않는다는 것을 이해하여야 한다. 오히려, 다양한 실시형태들은 포토다이오드들 사이의 광, QR 코드들, NFC 태그들, 단파장 라디오 송신들 등을 비제한적으로 포함하는, PCD (110) 와 POS 시스템 (125) 사이에 데이터를 송신하기 위한 다른 오프라인 수단을 이용할 수도 있는 것이 고려된다.

[0028] 도 1 로 돌아가서, 예시적인 시나리오에서, 소닉POS 모듈 (117) 은 통신 카드 (112B) 로 하여금, 무선 통신 링크 (140) 를 통해 PCD (110) 에 지불 요청을 송신하게 한다. 지불 요청은, 구매를 위해 제시된 항목들의 설명들, 총 가격들 등을 비제한적으로 포함하는 데이터를 나타낼 수도 있다. PCD (110) 는 그 다음, 소비자에 의한 검사를 위해 디스플레이 (114) 상에 지불 요청을 렌더링할 수도 있고, 그 지불 요청이 만족스러운 경우에, 소비자는 PCD (110) 에 고유 개인 식별 번호 ("PIN") 를 입력함으로써 응답할 수도 있다. PIN 의 입력은 소닉페이 모듈 (118) 로 하여금, 디지털 시그내처를 암호로 사인된 지불 요청 형태로 POS 시스템 (125) 에 링크 (140) 를 통해 다시 역으로 송신하도록 통신 카드 (112A) 를 레버리지하게 할 것이다. 소닉POS 모듈 (117) 은 그 다음, POS 시스템 (125) 이 지불 요청 및 양 디지털 시그내처들을 통신 네트워크 (130) 를 통해 소닉페이 서비스 서버 (105) 로 송신하기 전에, 상인과 연관된 디지털 시그내처를 지불 요청에 부착할 수도 있다.

[0029] 소닉페이 서비스 서버 (105) 는 소비자 및 상인과 연관된 계정들을 식별하기 위해 데이터베이스 (120) 에 쿼리하고 상인 및 소비자의 신원을 검증하기 위해 디지털 시그내처들을 이용할 수도 있다. 몇몇

실시형태들에서, 사인된 지불 요청은 소비자의 지불 계정 선호(들)을 포함할 수도 있다. 소닉페이 서비스 서버 (105)는, 사전 등록 프로세스 동안 소비자에 의해 진술되었을 수도 있거나 소비자로부터의 사인된 지불 요청에 의해 표시될 수도 있는 바와 같이, 소비자의 지불 크레덴셜들을 이용하여 거래를 결제하기 위해 지불 서비스 서버 (106) 또는 금고 서비스 서버 (107)와 통신할 수도 있다. 예를 들어, 소닉페이 서비스 서버 (105)는, PayPal™ 계정과 같은, 소비자와 연관된 계정에 대해 인출하기 위해, 그리고 상인과 연관된 계정에 입금하기 위해, 지불 서비스 서버 (106)와 통신할 수도 있다. 대안적으로, 소닉페이 서비스 서버 (105)는, 카드 네트워크 (Card Network) ("CN") 서버 (108)를 통해 액세스가능한 VISA™ 또는 MasterCard™와 같은 소비자의 크레디트 계정으로 하여금 인출되게 하고, 상인의 계정으로 하여금 입금되게 하기 위해, 금고 서비스 서버 (107)와 통신할 수도 있다.

[0030] 일단 디지털 시그내처들 및 연관된 구매 요청 데이터가 소닉페이 서비스 서버 (105)에서 수신되면, 소비자의 디지털 시그내처는 검증될 수도 있고, 소비자의 저장된 프로파일이 계정 데이터베이스 (120)에서 연관된 저장된 가치 계정들에 대해 쿼리될 수도 있다. 특히, 소비자와 연관된 가치 계정들은 크레디트 유형의 것이거나 저장된 가치 계정 유형의 것일 수도 있다. 하지만 예시적인 시나리오의 목적을 위해, 데이터베이스 (120)의 쿼리는, 소비자가 상인과 연관된 기프트 카드 계정을 갖는 것을 결정한다고 가정한다. 이러한 실시형태에서, 소닉페이 서비스 서버 (105)는, 금고 서비스 및 CN 서버들 (107, 108)과 연관된 크레디트 계정에 대해 거래의 밸런스 (balance)를 결산하기 전에 기프트 카드 계정에 대해 인출하기 위해 사전정의된 규칙들 알고리즘을 레버리지할 수도 있다.

[0031] 도 1 예시에서 묘사된 다양한 컴포넌트들에 관해, PCD (110) 및 POS 시스템 (125)의 예시적인 실시형태들은 원격 통신, 실시간 소프트웨어 업데이트들, 확장된 데이터 스토리지 등을 고려한다. 유리하게, 도 1에서 묘사된 예시적인 시스템 (100)과 같은 컴퓨터 시스템을 통해 통신하도록 구성된 PCD 들 (110) 및 POS 시스템들 (125)의 실시형태들은, 다른 것들 중에서도 특히 소프트웨어 업그레이드들, 콘텐츠 업데이트들, 데이터베이스 쿼리들, 등록 및 계정 설정, 데이터 송신 등을 위해, 셀룰러 네트워크들, PSTN 들, 케이블 네트워크들, 카드 발행자 네트워크들 및 인터넷을 비제한적으로 포함하는 통신 네트워크들 (130)을 레버리지할 수도 있다. PCD (110) 및/또는 POS 시스템 (125)과 관련하여 유용할 수도 있고 인터넷 또는 다른 네트워킹된 시스템을 통해 액세스 가능할 수도 있는 다른 데이터가 당업자에 의해 이해된다.

[0032] 도시된 컴퓨터 시스템 (100)은, 광역 네트워크 ("WAN"), 로컬 영역 네트워크 ("LAN"), 인터넷, 또는 다른 유형들의 네트워크들의 조합의 어느 것 또는 전부를 포함하는 네트워크 (130)에 커플링될 수도 있는 서버들 (105, 106, 107)을 포함할 수도 있다. 서버라는 용어는 단일 서버 시스템 또는 다중 시스템들 또는 다중 서버들을 지칭할 수도 있는 것으로 이해되어야 한다. 소닉페이 서비스 서버 (105)는, 사용자 계정 데이터베이스에 추가하여 데이터/서비스 데이터베이스를 포함할 수도 있는, 데이터베이스 (120)에 커플링될 수도 있다. 데이터베이스 (120)는, 비제한적으로, 디바이스 설정들, 소프트웨어 업데이트들, 사용자의 매뉴얼들, 고장해결 매뉴얼들, 사용자-특정 PCD 설정들, PCD 사용자-특정 컨택트 또는 계정 정보, 사용자-특정 컨택트 또는 계정 정보, 이력적 콘텐츠, 유효화 알고리즘들, 암호적 키들, 필터들/규칙들 알고리즘들, 오디오/비디오 데이터 등에 관련된 다양한 레코드들을 저장할 수도 있다.

[0033] 서버 (105)가 네트워크 (130)에 커플링될 때, 서버 (105)는, 개인 휴대 정보 단말기들 ("PDAs"), 셀룰러 전화기들 또는 다른 스마트 디바이스들과 같은 데스크톱 또는 랩톱 컴퓨터들, 씬 클라이언트들 (thin clients), 핸드헬드 디바이스들로 이루어질 수도 있는 다양한 상이한 PCD 들 (110)과 네트워크 (130)를 통해 통신할 수도 있다. 각 PCD (110)는, 비제한적으로 초기 등록 프로세스를 포함하는 다양한 시간들에서 서버 (105) 및 그것의 다양한 애플리케이션들에 액세스하기 위해 웹 브라우징 소프트웨어 또는 기능을 실행 또는 수행시킬 수도 있다. 상보적 디바이스에 직접 아니면 테더 (tether)를 통해 네트워크 (130)에 액세스할 수도 있는 임의의 디바이스는 컴퓨터 시스템 (100)에 따른 PCD (110)일 수도 있다. PCD 들 (110), 및 비제한적으로 데이터/서비스 데이터베이스 (120)와 연관된 데이터베이스 서버 (구체적으로 묘사되지는 않음) 또는 POS (125)와 같은, 시스템 (100) 내의 다른 컴포넌트들은 다양한 유형들의 통신 링크들 (145)에 의해 네트워크 (130)에 커플링될 수도 있다.

[0034] 각 PCD (110)는 디스플레이 (114), 무선 통신 하드웨어 (112), 라디오 트랜시버 (116), 및 소닉페이 모듈 (118)을 포함할 수도 있다. 디스플레이 (114)는, 액정 디스플레이 ("LCD"), 플라즈마 디스플레이, 유기발광 다이오드 ("OLED") 디스플레이, 터치 작동 디스플레이, 및 음극선관 ("CRT") 디스플레이, 점자 표시기, LED 뱅크, 및 세그먼트화된 디스플레이와 같은 임의의 유형의 디스플레이 디바이스를 포함할 수도 있다.

PCD (110) 는 소닉페이 모듈 (118) 에 대해 수행, 실행 또는 인터페이싱할 수도 있다. 소닉페이 모듈 (118) 은 인터넷 웹 브라우저를 위한 플러그-인 (plug-in) 의 일부일 수도 있는 멀티미디어 플랫폼을 포함할 수도 있다.

[0035] 소닉페이 모듈 (118) 은, 무선 통신 하드웨어 (112), 라디오 트랜시버 (116), 및 디지털 시그내처와 연관된 계정에 대해 지불 요청을 렌더링하고/하거나 지불 요청을 인가하기 위한 임의의 저장된 또는 취출가능한 콘텐츠와 작업하도록 설계된다. PCD (110) 가 상점 (135) 내에서 레버리지될 때, PCD 사용자, 구매 거래, 상인 상점 (135) 등과 연관된 다양한 콘텐츠는 디스플레이 (114) 상에 렌더링될 수도 있다.

[0036] 도 2 를 참조하면, 예시적인 PCD (110) 및/또는 POS 시스템 (125) 은 비제한적으로 WiFi 카드와 같은 무선 통신 하드웨어 (112) 를 포함할 수도 있다. PCD (110) 및 POS (125) 는 또한, 무선 통신 하드웨어 (112A, 112B) 및/또는 셀룰러 라디오 트랜시버들 (116A, 116B) 로부터 지불 요청을 각각 수신 및 송신하기 위해 소닉페이 모듈 (118) 및 소닉POS 모듈 (117) 을 각각 포함할 수도 있다. 소닉페이 및 소닉POS 모듈들 (118, 117) 은 또한, 암호 기술분야의 당업자에 의해 이해될 수 있는 바와 같이, 각각과 연관된 사용자들을 식별하고 일정 구매 거래의 인가를 검증하기 위해 유용한 디지털 시그내처들을 송신할 수도 있다.

[0037] 모듈들 (117, 118) 은 통신 애플리케이션 프로그래밍 인터페이스들 ("API") (111) 을 통해 무선 통신 하드웨어 (112) 를 통해 데이터를 전송하도록 구성될 수도 있다. 이와 같이, 당업자는 소닉페이 및/또는 소닉POS 모듈 (118, 117) 은 통합형 설계에서의 그것의 모듈의 일부로서 통신 API (111) 및/또는 무선 통신 하드웨어 (112) 를 포함하도록 설계될 수도 있다는 것을 인식할 것이다. 또한, 소닉POS 모듈 (117) 은, 시스템 (100) 실시형태에서 묘사된 바와 같이, 예시적인 서버 (105) 에, 구매 거래 인가 또는 확인 데이터 및 다른 정보를 송신 및 수신하기 위해 라디오 API (115B) 를 통해 셀룰러 라디오 트랜시버 (116B) 와 인터페이스하도록 구성될 수도 있다. 심지어 더 나아가, 모듈들 (117, 118) 은 가정 포맷으로 비-기밀성 정보를 중계하기 위해 당업자에게 알려질 수도 있는 문자 음성 변환 (text to speech) ("TTS") 모듈 (미도시) 을 레버리지하도록 구성될 수도 있다. 따라서, 당업자는 또한, 모듈 (117, 118) 이 통합형 설계에서의 그것의 모듈의 일부로서 라디오 API (115) 및/또는 셀룰러 라디오 트랜시버 (116) 및/또는 TTS 모듈을 또한 포함할 수도 있다는 것을 인식할 것이다.

[0038] PCD (110) 는, 사전등록 데이터, 개인 식별 번호 (PIN), 보안 키, 또는 소닉페이 모듈 (118) 에 의해 생성된 다른 데이터와 같은 데이터를 링크 (145) 를 통해 소닉페이 서비스 서버 (105) 에 송신하기 위해 셀룰러 라디오 트랜시버 (116) 를 레버리지하도록 구성될 수도 있다. 무선 링크 (145) 는 셀룰러 전화 네트워크 상에 확립된 보안 채널을 포함할 수도 있다. 또한, 통신 링크들 (145) 은 일반적으로, 비제한적으로, 라디오-주파수 ("RF") 링크들, 적외선 링크들, 음향 링크들, 다른 무선 매체들, 광역 네트워크들 ("WAN"), 로컬 영역 네트워크들 ("LAN"), 인터넷, 공중 교환 전화망 ("PSTN"), 및 페이징 네트워크의 임의의 조합을 포함하는 무선 및 유선 링크들의 임의의 조합을 포함할 수도 있다.

[0039] 예시적인 PCD (110) 및/또는 POS 시스템 (125) 은 또한, 비제한적으로, 구매 거래 데이터 및 디지털 시그내처 데이터 뿐만 아니라 소닉페이 서비스 사용자와 연관된 데이터 또는 계정들과 관련된 소닉페이에 추가되는, 소닉 페이로부터 추출 또는 도출되는 데이터를 포함하는 다양한 데이터를 일시적으로 이든 영구적으로 저장하기 위한 컴퓨터 판독가능 저장/메모리 컴퓨포넌트 (119) 를 포함할 수도 있다. 구매 거래 데이터에 추가된 데이터, 구매 거래 데이터로부터 추출 또는 도출된 데이터는, 사용자 ID, 거래 ID, PCD (110) 와 연관된 디렉토리 번호 (directory number) ("DN") 또는 호출 라인 ID (calling line ID) (CLID"), 상인 ID, 네트워크 명칭, 해시 (hash) 값, 코덱 키, 암호화 또는 암호화해제 데이터, 계정 번호들, 및, 비제한적으로, 구매되는 항목, 구매되는 항목의 가격, 구매 디스카운트율 또는 계정들, 고객 로열티 데이터, 판매 세금 비율 또는 액, 상인 종업원 신원 등에 관련된 데이터와 같은 다른 계정 관련 데이터를 포함할 수도 있다.

[0040] 이제 도 3 으로 가서, 도 1 의 시스템 (100) 을 위한 예시적인 컴퓨터 아키텍처의 다이어그램이 묘사된다. 예시적인 아키텍처 (101) 는 PCD (110), POS 시스템 (125), 및 소닉페이 서비스 서버 (105) 를 포함할 수도 있다. 소닉페이 서비스 서버 (105) 는 모바일 전화 네트워크와 같은 무선 통신 링크 (145) 를 통해 PCD (110) 및 POS 시스템 (125) 에 접속될 수도 있다. 이미 언급한 바와 같이, 서버 (105) 라는 용어는 단일 서버 시스템 또는 다중 시스템들 또는 다중 서버들을 지칭할 수도 있다는 것을 이해하여야 한다. 본 발명의 범위로부터 벗어남이 없이 그리고 컴퓨터 아키텍처 설계 제약들에 의존하여 다양한 서버 배열들이 선택될 수도 있다는 것을 당업자는 이해할 것이다.

[0041] 도 3 에 도시된 바와 같이, PCD (110), POS (125), 및 소닉페이 서비스 (105) 는 각각 프로세서 (109) 및 그 프

로세서 (109)에 커플링된 메모리 (119)를 포함할 수도 있다. 메모리 (119)는 본원에 설명된 방법 단계들 중 하나 이상을 실행하기 위한 명령들을 포함할 수도 있다. 또한, 프로세서 (109) 및 메모리 (119)는 본원에 설명된 방법 단계들 중 하나 이상을 실행하기 위한 수단으로서 기능할 수도 있다. 표시된 바와 같이, 메모리 (119A)는 또한 소닉페이 모듈 (118)을 포함할 수도 있고, 메모리 (119B)는 소닉POS 모듈 (117)을 포함할 수도 있으며, 메모리 (119C)는 소닉페이 서비스 모듈 (121) 및 규칙 모듈 (122)을 포함할 수도 있다. 규칙 모듈 (122)은, 소비자와 연관된 복수의 저장된 가치 계정들 중 어느 것이 사용된 지불 요청에 응답하여 인출될 수도 있는지를 결정하기 위해 레버리지될 수도 있다. 소닉페이 모듈 (118)은, 도 1과 관련하여 상기 설명된 다양한 메커니즘들에 따라, POS 시스템 (125)으로부터 수신된 지불 요청을 렌더링하고 POS (125)에 지불 요청을 인가하는 디지털 시그내처를 다시 송신하도록 동작할 수도 있다. 규칙 알고리즘들, 전파를 위한 콘텐츠, 가치 계정 레코드들, PCD 사용자 이력 데이터 등의 저장을 위한 데이터베이스 (120)가 또한 소닉페이 서비스 서버 (105)에 연결될 수도 있다.

[0042] 도 4를 참조하면, 이 도면은 도 2와 대응하는 무선 전화를 포함하는 PCD (110)의 예시적이고 비제한적인 양태의 다이어그램이다. 도시된 바와 같이, PCD (110)는 함께 커플링된 디지털 신호 처리기 (109A) 및 아날로그 신호 처리기 (426)를 포함하는 온-칩 시스템 (422)을 포함한다. 도 4에 도시된 바와 같이, 디스플레이 제어기 (428) 및 터치스크린 제어기 (430)가 디지털 신호 처리기 (109A)에 커플링된다. 온-칩 시스템 (422) 외부의 터치스크린 디스플레이 (114)는 디스플레이 제어기 (428) 및 터치스크린 제어기 (430)에 커플링된다.

[0043] 도 4는, 비디오 인코더 (434), 예를 들어, 위상 반전 주사선 (phase-alternating line) ("PAL") 인코더, SECAM (sequential couleur avec memoire) 인코더, NTSC (national television system(s) committee) 인코더, 또는 임의의 다른 비디오 인코더가 디지털 신호 처리기 (109A)에 커플링되는 것을 더 나타낸다. 또한, 비디오 증폭기 (436)는 비디오 인코더 (434) 및 터치스크린 디스플레이 (114)에 커플링된다. 비디오 포트 (438)는 비디오 증폭기 (436)에 커플링된다. 범용 직렬 버스 ("USB") 제어기 (440)가 디지털 신호 처리기 (424)에 커플링된다. 또한, USB 포트 (442)는 USB 제어기 (440)에 커플링된다. 메모리 (119A) 및 가입자 식별 모듈 (subscriber identity module) ("SIM") 카드 (446)가 또한 디지털 신호 처리기 (109A)에 커플링될 수도 있다. 또한, 디지털 카메라 (448)가 디지털 신호 처리기 (109A)에 커플링될 수도 있다. 예시적인 양태에서, 디지털 카메라 (448)는 고체 활성 소자 ("CCD") 카메라 또는 상보형 금속-산화물 반도체 ("CMOS") 카메라이다.

[0044] 도 4에 추가로 도시된 바와 같이, 스테레오 오디오 CODEC (450)은 아날로그 신호 처리기 (426)에 커플링될 수도 있다. 또한, 오디오 증폭기 (452)는 스테레오 오디오 CODEC (450)에 커플링될 수도 있다. 예시적인 양태에서, 제 1 스테레오 스피커 (454) 및 제 2 스테레오 스피커 (456)는 오디오 증폭기 (452)에 커플링되고, 지불 요청의 수신에 응답하여 부근의 POS 시스템 (125)에 디지털 시그내처를 나타내는 가청의 또는 초음파의 데이터를 전송하기 위해 이용될 수도 있다.

[0045] 도 4는 마이크로폰 증폭기 (458)가 또한 스테레오 오디오 CODEC (450)에 커플링될 수도 있는 것을 보여준다. 추가적으로, 마이크로폰 (460)은 마이크로폰 증폭기 (458)에 커플링될 수도 있고, POS 시스템 (125)으로부터의 지불 요청을 나타내는 가청의 또는 초음파의 송신물을 수신하도록 동작가능하다. 특정 양태에서, 주파수 변조 ("FM") 라디오 튜너 (462)는 스테레오 오디오 CODEC (450)에 커플링될 수도 있다. 또한, FM 안테나 (464)는 FM 라디오 튜너 (462)에 커플링된다. 또한, 스테레오 헤드폰들 (468)은 스테레오 오디오 CODEC (450)에 커플링될 수도 있다.

[0046] 도 4는 라디오 주파수 ("RF") 트랜시버 (116)가 아날로그 신호 처리기 (426)에 커플링될 수도 있는 것을 더 나타낸다. RF 스위치 (470)는 RF 트랜시버 (116) 및 RF 안테나 (472)에 커플링될 수도 있다. 도 4에 도시된 바와 같이, 키패드 (474)는 아날로그 신호 처리기 (426)에 커플링될 수도 있다. 또한, 마이크로폰 (476)을 갖는 모노 헤드셋이 아날로그 신호 처리기 (426)에 커플링될 수도 있다.

[0047] 또한, 바이브레이터 (vibrator) 디바이스 (478)가 아날로그 신호 처리기 (426)에 커플링될 수도 있다. 전력 공급기 (480)가 온-칩 시스템 (422)에 커플링될 수도 있는 것이 또한 도시된다. 특정 양태에서, 전력 공급기 (480)는 전력을 필요로 하는 PCD (110)의 다양한 컴포넌트들에 전력을 제공하는 직류 ("DC") 전력 공급기이다. 또한, 특정 양태에서, 전력 공급기는 AC 전원에 연결된 DC 변환기로 교류 ("AC")로부터 도출되는 재충전가능 DC 배터리 또는 DC 전력 공급기이다.

[0048] 도 4는 또한, PCD (110)가 소닉페이 모듈 (118)을 포함할 수도 있는 것을 나타낸다. 소닉페이 모듈

(118) 은 디지털 시그내처를 통해 지불 요청을 인가하기 위해 소닉POS 모듈 (117) 과 통신할 수도 있다.

[0049] 도 4 에 도시된 바와 같이, 터치스크린 디스플레이 (114), 비디오 포트 (438), USB 포트 (442), 카메라 (448), 제 1 스테레오 스피커 (454), 제 2 스테레오 스피커 (456), 마이크로폰 (460), FM 안테나 (464), 스테레오 헤드폰들 (468), RF 스위치 (470), RF 안테나 (472), 키패드 (474), 모노 헤드셋 (476), 바이브레이터 (478), 및 전력 공급기 (480) 는 온-칩 시스템 (422) 외부에 있다.

[0050] 특정 양태에서, 본원에 설명된 방법 단계들의 하나 이상은 소닉페이 모듈 (118) 과 같이, 컴퓨터 프로그램 명령들로서 메모리 (119A) 에 저장될 수도 있다. 이들 명령들은 본원에 설명된 방법들을 수행하기 위해 디지털 신호 처리기 (109A), 아날로그 신호 처리기 (426), 또는 다른 처리기에 의해 실행될 수도 있다.

[0051] 또한, 처리기들 (109A, 426), 메모리 (119A), 거기에 저장된 명령들, 또는 이들의 조합은 본원에 설명된 방법 단계들 중 하나 이상을 수행하기 위한 수단으로서 기능할 수도 있다.

[0052] 도 5 는, 소비자의 PCD (110) 와 상인의 POS 시스템 (125) 사이에 공유된 암호적 인가들을 이용하여 구매 거래를 완료하기 위해 시스템 (100) 의 소비자 사용자를, 지불 크레덴셜 금고 서비스 (107) 에 등록하기 위한 예시적인 방법 (500) 을 나타내는 논리적 흐름도이다. 블록 505 에서 시작하여, 소닉페이 클라이언트 모듈 (118) 이 실행되고 있는 PCD (110) 와 연관된 소비자는 사용자 프로파일 및 지불 크레덴셜들을 금고 서비스 (107) 에 업로드한다. 사용자 프로파일 및 지불 크레덴셜들은, 카드 네트워크 거래들의 기술분야에서의 당업자에 의해 이해되는 바와 같이, 소비자와 연관된 계정에 대해 인출되도록 카드 네트워크 (108) 를 통해 거래들을 라우팅하기 위해 유용한 기밀성 주제를 나타낸다. 사용자 프로파일 및 지불 크레덴셜들은, 소비자의 명칭, 청구서 발송지, 크레디트 계정 번호(들), 크레디트 카드 검증 번호(들), 크레디트 카드 PIN(들), 비밀번호(들) 등으로 이루어질 수도 있고, 하지만 이에 한정되는 것은 아니다.

[0053] 블록 510 에서, 금고 서비스 (107) 는, 지불 크레덴셜 보관의 기술분야에서 이해되는 바와 같이, 업로드된 사용자 프로파일 및 지불 크레덴셜들에 대한 포인트로서 기능하는 PCD (110) 에 토큰을 리턴한다. 블록 515 에서, 소닉페이 클라이언트 모듈 (118) 이 실행되는 PCD (110) 와 연관된 소비자는, 당업자에 의해 이해되는 바와 같이, PCD (110) 의 사용자 인터페이스를 통해 개인 식별 번호 ("PIN") 를 입력한다. 블록 520 에서, 소닉페이 클라이언트 모듈 (118) 은 암호적 키 쌍을 생성하고, 그 키 쌍의 개인 키 부분을 암호화하고, 공개 키 부분을 소닉페이 서비스 (105) 에 포워딩한다. 이 시점에서, 암호 기술분야의 당업자에 의해 이해되는 바와 같이, 소닉페이 서비스 (105) 는 소닉페이 클라이언트 모듈 (118) 에 의해 유지된 사설 키와 연관된 소비자의 아이덴티티를 검증하기 위해 공개 키를 이용할 수도 있다. 블록 525 에서, 소닉페이 서비스 (105) 는 PCD (110) 와 연관된 소비자에 대한 사용자 ID 를 생성한다.

[0054] 특히, 블록 525 의 결말에서, 소비자는 소닉페이 서비스에 기밀성 지불 크레덴셜들을 업로드함이 없이 소닉페이 서비스에 성공적으로 등록하였다. 즉, 지불 크레덴셜들은 금고 서비스에서 안전하게 저장되고, 소닉페이 서비스는, 소비자 프로파일, 소비자의 디지털 시그내처/인가를 검증하기 위한 공개 키, 및 금고 서비스에서 보안 지불 크레덴셜들을 포인팅하는 토큰을 구비한다. 전체 등록 프로세스 (500) 는 PCD (110) 와 연관된 소비자와 POS 시스템 (125) 과 연관된 상인 사이의 구매 거래 이전에 통신 링크 (145A) 를 통해 온라인으로 수행된다.

[0055] 도 6 은, 소비자의 PCD (110) 와 상인의 POS 시스템 (125) 사이에 공유된 암호적 인가들을 이용하여 구매 거래를 완료하기 위해 시스템 (100) 의 소비자 사용자를, 제 3 자 지불 서비스 (106) 에 등록하기 위한 예시적인 방법 (600) 을 나타내는 논리적 흐름도이다. 블록 605 에서 시작하여, 소닉페이 클라이언트 모듈 (118) 이 실행되는 PCD (110) 와 연관된 소비자는, 당업자에 의해 이해되는 바와 같이, PCD (110) 의 사용자 인터페이스를 통해 개인 식별 번호 ("PIN") 를 입력한다. 블록 610 에서, 소닉페이 클라이언트 모듈 (118) 은 임호적 키 쌍을 생성하고, 그 키 쌍의 개인 키 부분을 암호화하고, 공개 키 부분을 소닉페이 서비스 (105) 에 포워딩한다. 이 시점에서, 암호 기술분야에서의 당업자에 의해 이해되는 바와 같이, 소닉페이 서비스 (105) 는 소닉페이 클라이언트 모듈 (118) 에 의해 유지된 개인 키와 연관된 소비자의 아이덴티티를 검증하기 위해 공개 키를 이용할 수도 있다.

[0056] 블록 615 에서, 소닉페이 서비스 (105) 는 PCD (110) 와 연관된 소비자에 대한 사용자 ID 를 생성하고, 그 다음, 블록 620 에서, PCD (110) 의 소비자와 연관되고 지불 서비스 (106) 에 의해 관리되는 저장된 가치 계정에 액세스함에 있어 사용하기 위해 제 3 자 지불 서비스 (106) 로부터 사전승인 키를 요청한다. 사전승인 키를 역으로 수신 시, 블록 625 에서, 소닉페이 서비스 (105) 는 지불 서비스 사전승인 키 소닉페이 서비스 사용자 ID 를 PCD (110) 의 소닉페이 클라이언트 모듈 (118) 에 리턴한다. 블록 630 에서, 소닉페이 클라이언트 모듈 (118) 은 지불 서비스에서 수신한 사전승인 키를 사용하여 지불 서비스에 대한 접근권한을 확보한다.

트 모듈 (118) 은 사용자 ID 를 저장한다.      블록 635 에서, PCD (110) 의 소비자는 당업자에 의해 이해되는 바와 같이, 통신 링크 (145A) 를 통해 지불 서비스 (106) 에 로그인할 수도 있다.      일단 로그인되면, 소비자는 소닉페이 서비스 (105) 가 저장된 가치 계정에 대한 제한된 액세스를 가지도록 인가하기 위해 제공된 사전승인 키를 이용할 수도 있다.      등록 프로세스는 완료된다.      특히, 소비자와 연관된 사용자 ID 및 디지털 시그내처가 제공되는 경우, 소닉페이 서비스 (105) 는 소비자의 아이덴티티를 검증하고 제 3 자 지불 서비스 (106) 에 대한 인가된 액세스를 용이하게 하기 위해 대응하는 공개 키를 이용할 수도 있다.      이와 같이, 소닉페이 서비스 (105) 는 소비자에 의해 인가된 거래를 결제하기 위해 소비자를 대신하여 저장된 가치 계정에 대해 인출할 수도 있다.

[0057]      도 7 은 소비자의 PCD (110) 와 상인의 POS 시스템 (125) 사이에 공유된 암호적 인가들을 이용하여 구매 거래를 완료하기 위해 시스템 (100) 의 상인 사용자의 카드 네트워크 프로세서 크레덴셜들을 등록하기 위한 예시적인 방법 (700) 을 나타내는 논리적 흐름도이다.      블록 705 에서 시작하여, 소닉POS 모듈 (117) 이 실행되는 POS 시스템 (125) 과 연관된 상인은 프로파일 및 카드 네트워크 프로세서 크레덴셜들을 소닉POS 모듈 (117) 에 입력한다.      사용자 프로파일 및 프로세서 크레덴셜들은, 당업자에 의해 이해되는 바와 같이, POS 시스템 (125) 의 사용자 인터페이스를 통해 입력될 수도 있다.      상인 사용자 프로파일 및 프로세서 크레덴셜들은, 카드 네트워크 거래 기술분야에서의 당업자에 의해 이해되는 바와 같이, 상인과 연관된 계정에 대해 입금되도록 카드 네트워크 (108) 를 통해 거래들을 라우팅하기 위해 유용한 기밀성 주제를 나타낸다.      상인 사용자 프로파일 및 프로세서 크레덴셜들은 상인의 명칭 또는 식별자, 주소, 계정 번호(들), PIN(들), 비밀번호(들) 등으로 이루어질 수도 있고, 하지만 이에 한정되는 것은 아니다.

[0058]      블록 710 에서, 소닉POS 클라이언트 모듈 (117) 이 실행되는 POS 시스템 (125) 과 연관된 상인은, 당업자에 의해 이해되는 바와 같이, POS (125) 의 사용자 인터페이스를 통해 개인 식별 번호 ("PIN") 를 입력한다.      블록 715 에서, 소닉POS 클라이언트 모듈 (117) 은 암호적 키 쌍을 생성하고, 그 키 쌍의 개인 키 부분을 암호화하고, 공개 키 부분을 상인 프로파일 및 프로세서 크레덴셜들과 함께 소닉페이 서비스 (105) 에 포워딩한다.      이 시점에서, 암호 기술분야에서의 당업자에 의해 이해되는 바와 같이, 소닉페이 서비스 (105) 는 소닉POS 클라이언트 모듈 (117) 에 의해 유지된 개인 키와 연관된 상인의 아이덴티티를 검증하기 위해 공개 키를 이용할 수도 있다.

[0059]      블록 720 에서, 소닉페이 서비스 (105) 는 프로세서 크레덴셜들 및 프로파일을 이용하여 카드 네트워크 (108) 의 게이트웨이 프로세서로 그들의 정확성을 검증할 수도 있다.      결정 블록 725 에서, 크레덴셜들이 실패하는 경우, 프로세스는 블록 730 으로 이동하고, 여기서, 상인은 새로운 크레덴셜들/프로파일을 재입력 또는 제공하도록 요청된다.      결정 블록 725 에서 크레덴셜이 인증되는 경우, 그다음, 블록 735 에서, 소닉페이 서비스 (105) 는 POS 시스템 (125) 과 연관된 상인에 대해 사용자 ID 를 생성한다.      블록 740 에서, 사용자 ID 를 포함하는 확인이 상인 POS 시스템 (125) 에 리턴되어 등록이 완료된 것을 나타낼 수도 있다.

[0060]      도 8 은 소비자의 PCD (110) 와 상인의 POS 시스템 (125) 사이에 공유된 암호적 인가들을 이용하여 구매 거래를 완료하기 위해 시스템 (100) 의 상인 사용자의 제 3 자 지불 서비스 계정을 등록하기 위한 예시적인 방법 (800) 을 나타내는 논리적 흐름도이다.      블록 805 에서 시작하여, 소닉POS 모듈 (117) 이 실행되는 POS 시스템 (125) 과 연관된 상인은, 당업자에 의해 이해되는 바와 같이, POS 시스템 (125) 의 사용자 인터페이스를 통해 PIN 을 입력한다.      블록 810 에서, 소닉POS 모듈 (117) 은, 암호 기술분야에서의 당업자에 의해 이해되는 바와 같이, 공개/개인 키 쌍을 생성한다.      블록 815 에서, POS 시스템 (125) 은 그 키 쌍의 공개 키 부분 및 지불 서비스 계정 데이터를 소닉페이 시스템 (105) 에 송신한다.      특히, 공개 키로, 소닉페이 시스템 (105) 은 블록 810 에서 생성된 개인 키를 포함하는 상인의 디지털 시그내처를 쉽게 검증할 수도 있다.      블록 820 에서, 소닉페이 시스템 (105) 은 상인 프로파일, 계정 데이터, 및 키와 연관하여 사용자 ID 를 생성하고, 블록 825 에서, 그 ID 를 상인 POS 시스템 (125) 에 포워딩한다.      POS 시스템 (125) 에서 ID 를 수신하면, 소닉POS 모듈 (117) 은, 상인과 연관된 다양한 계정 및 키 데이터에 소닉페이 시스템 (105) 을 포인팅하기 위해 나중에 사용될 수도 있는 ID 를 저장한다.      특히, 지불 서비스 (106) 의 상인 계정 데이터로, 소닉페이 시스템 (105) 은 상인을 대신하여 거래를 결제하기 위해 상인 계정에 입금할 수도 있다.

[0061]      도 9a 및 도 9b 는 소비자의 PCD (110) 와 상인의 POS 시스템 (125) 사이에 공유된 암호적 인가들을 이용하여 카드 네트워크 프로세서 (108) 를 통해 구매 거래를 완료하기 위한 예시적인 방법 (900) 을 나타내는 논리적 흐름도이다.      방법 (900) 을 시작하기 이전에, PCD (110) 와 연관된 소비자 및 POS 시스템 (125) 과 연관된 상인 양자 모두는 도 5 및 도 7 과 각각 관련하여 개괄되고 설명된 예시적인 방법들에 따라 등록 프로세스를 완료하였을 것이다.      블록 905 에서, 소비자 PCD (110) 및 상인 POS 시스템 (125) 은 상점 (135) 에서 물리적으

로 근접한다. 특히, 상점이라는 용어는 PCD (110) 와 POS 시스템 (125) 이 서로 물리적으로 근접한 것을 나타내는 것으로만 의미되고, 어떤 방식으로든 상점의 환경을 제한하는 것으로 의미되지 않는다는 것을 이해할 것이다. 즉, 상점은 PCD (110) 와 POS 시스템 (125) 양자 모두에 대해 물리적으로 또는 가상적으로 공통인 임의의 장소일 수도 있다. 예를 들어, 어떤 실시형태들은 모바일 환경에서 구매 거래들을 수행하도록 동작가능할 수도 있고, 이 모바일 환경에서, PCD (110) 및 POS 시스템 (125) 어느 것도 정적이지 않다. 또한, PCD (110) 와 POS 시스템 (125) 사이의 사운드 기반 통신들에 의존하는 실시형태들과 같은 일정 실시형태들은 본원에 설명된 방법들 및 그들의 균등물들을 이용하여 원격통신 링크를 통해 구매 거래들을 수행할 수도 있는 것이 또한 고려된다.

[0062]

방법 (900) 으로 돌아와서, 블록 905 에서, 소비자 PCD (110) 는 POS 시스템 (125) 으로부터 송신된 지불 요청을 수신한다. 지불 요청은, 본질적으로, 소비자가 POS 시스템 (125) 과 연관된 상인으로부터 구매하기를 희망하는 상품 또는 서비스에 대한 청구서 등이다. 예를 들어, 소비자는 \$9.99 가격의 항목을 그 항목을 구매할 의도로 상인의 카운터에 놓았을 수도 있다. 상인은 그러면 그 항목을 "입력" 하였을 수도 있고, 그에 의해, 세금을 추가하여 총 \$10.50 의 가격이 될 수도 있다. 지불 요청은, 예에서, \$10.50 의 총 가격을 나타낼 것이고, 상인은 소비자에게 항목을 구매하기 위해 \$10.50 을 송금하도록 요청한다. 또한, 전술한 바와 같이, 지불 요청은 비제한적으로 사운드, 광, 라디오 송신 등을 포함하는 임의의 수의 방식들을 통해 POS 시스템 (125) 으로부터 PCD (110) 로 무선으로 송신될 수도 있다. 일정 실시형태들에서, POS 시스템 (125) 및 PCD (110) 는 사운드를 통해 데이터를 송신 및 수신하도록 구성되는 마이크로폰들 및 스피커들을 구비한다. 몇몇 이러한 실시형태들에서, 모든 실시형태들인 사운드 주파수가 사용자들에게 가청이도록 요구하는 것은 아니지만, 사운드는 PCD (110) 및 POS 시스템 (125) 의 사용자들에 대해 가청일 수도 있다. 예를 들어, 몇몇 실시형태들에서, 사운드는 바로 가까이서 일어나고 있는 다른 거래들과 간섭하지 않도록 빨리 감쇄되는 주파수에 있을 수도 있다. 또한, 몇몇 실시형태들에서, 가청 톤이 사용자들에게 프로세스를 통지하기 위해 사용되는 동안 사용자들에 대해 들리지 않는 주파수에서 데이터가 POS 시스템 (125) 과 PCD (110) 사이에 송신될 수도 있다.

[0063]

방법 (900) 으로 돌아가서, 결정 블록 (910) 에서, PCD (110) 와 연관된 소비자는 지불 요청을 검토하고 그것이 만족스러운지를 결정할 수도 있다. 상기 예에서, 항목에 대한 \$10.50 가격이 소비자에게 수용가능하지 않은 경우에는, 블록 915 에서 소비자는 구매를 거절할 수도 있다. 몇몇 실시형태들에서, 구매 거절은 PCD (110) 로 하여금, 소비자가 거래를 거절하였다는 것을 나타내는 신호를 POS 시스템 (125) 에 리턴하게 할 수도 있고, 다만, 이러한 것이 모든 실시형태들에서 요구되는 것은 아니다. 블록 910 에서, 소비자는 지불 요청을 승인하고, 그 다음, 몇몇 실시형태들에서, 소비자는 블록 920 에서 팁을 추가하는 것, 수정제안을 하는 것 등과 같이 지불 요청을 수정할 수도 있다.

[0064]

일단 지불 요청이 소비자에 의한 승인을 위한 상태에 있으면, 블록 925 에서, 소비자는 PIN 을 입력하고, 이는 PCD (110) 로 하여금 지불 요청을 디지털로 사인하는 것을 야기한다. 전술한 바와 같이, 디지털 시그내쳐는 사용자와 연관된 고유한 개인 키를 이용하여 생성되고, 상보적 공개 키의 허더에게 소비자의 아이덴티티를 나타내도록 기능한다. 사인된 지불 요청은 POS 시스템 (125) 으로 다시 역으로 송신되고 블록 930 에서 수신된다. 블록 935 에서, 소닉POS 모듈 (117) 은 상인의 디지털 시그내쳐를 블록 930 에서의 지불 요청 및 소비자 디지털 시그내쳐에 부가할 수도 있다. 블록 940 에서, 지불 요청 및 고유한 디지털 시그내쳐들의 다발이 소닉POS 시스템 (125) 으로부터 소닉페이 서비스 (105) 로 포워딩된다.

[0065]

지불 요청의 승인을 나타내는 거래 당사자들 (상인 및 소비자) 의 디지털 시그내쳐들을 수신 시에, 블록 945 에서, 소닉페이 서비스 (105) 는 예시적인 등록 방법들 (500 및 700) 에서 업로드된 공개 키를 이용하여 거래 당사자들의 아이덴티티를 검증할 수도 있다. 블록 950 에서, 소닉페이 서비스는 사용자의 프로파일 또는 사인된 지불 요청으로부터, 소비자와 연관된 복수의 계정들 중 어떤 하나 (또는 그 이상) 가 지불 요청 총액에 따라 인출되어야하는 것을 결정할 수도 있다. 하지만, 소닉페이 서비스의 일부 실시형태들은 사전정의된 규칙들 또는 알고리즘들에 따라 소비자 계정들을 선택하기 위한 규칙 모듈 (122) 을 포함할 수도 있는 것이 고려된다. 예를 들어, 규칙 모듈 (122) 은 보상 포인트를 최대화하고 사전에 로딩된 기프트 계정들의 이점을 취하도록 소비자 계정들을 선택하도록 구성될 수도 있다.

[0066]

방법 (900) 으로 돌아가서, 블록 955 에서, 디지털 시그내쳐를 통해 소비자를 식별한 소닉페이 서비스 (105) 는 소비자의 사전에 등록된 지불 계정에 포인팅하는 토큰을 식별하기 위해 데이터베이스 (120) 에 쿼리할 수도 있다. 블록 960 에서, 소닉페이 서비스 (105) 는, 카드 네트워크 거래의 기술분야에서의 당업자에 의해 이해되는 바와 같이, 토큰 및 지불 요청을 게이트웨이/카드 프로세서에 포워딩함으로써 식별된 소비자 계정에 대해

거래를 결제하기 위해 토큰을 레버리지한다. 블록 965에서, 토큰 및 결재 거래가 게이트웨이 프로세서 (108)에서 수신되고, 블록 970에서, 프로세서는 금고 서비스 (107)로부터 연관된 지불 크레덴셜들을 요청하기 위해 토큰을 이용한다.

[0067] 블록 975에서, 게이트웨이 (108)는 금고 서비스 (107)로부터 지불 크레덴셜들을 수신하고, 지불 요청의 금액 만큼 연관된 계정에서 인출하기 위해 그 크레덴셜들을 이용한다. 몇몇 실시형태들에서, 블록 980에서, 소비자 계정에 대해 거래가 결제되었다는 확인이 네트워크 (130)의 통신 링크들을 통해 POS 시스템 (125)으로 리턴된다. 소닉페이 서비스는 블록 985에서 거래를 나타내는 데이터를 저장하여 소비자가 그것을 후일 그 것을 액세스할 수도 있도록 할 수도 있다. 블록 990에서, 소닉POS 모듈 (117)은 영수증을 생성하고 이것을 사용자의 PCD (110)에 무선으로 송신할 수도 있으며, 사용자의 PCD (110)에서 소닉페이 모듈 (118)은 그 영수증이 PCD (110)의 디스플레이 상에 렌더링되게 할 수도 있다.

[0068] 유리하게, 예시적인 방법 (900)을 통해 완료된 구매 거래는 소비자 PCD (110)가 온라인으로 됨이 없이 일어난다. 즉, 프로세스 동안 PCD (110)로부터 송신되고 PCD (110)에 의해 수신된 데이터는 PCD (110) 및 POS 시스템 (125)으로부터 무선으로 완전히 상점 (135) 내에서 교환된다. 또한, 구매 거래는 소비자의 기밀성 지불 크레덴셜들이 PCD (110) 상에 저장되거나, 그 문제를 위해, PCD (110)로부터 상인 POS 시스템 (125)으로 송신될 필요 없이 일어난다.

[0069] 도 10a 및 도 10b는 소비자의 PCD (110)와 상인의 POS 시스템 (125) 사이에 공유된 암호적 인가들을 이용하여 제 3 자 지불 서비스 (106) 계정을 통해 구매 거래를 완료하기 위한 예시적인 방법 (1000)을 나타내는 논리적 흐름도이다. 방법 (1000)의 블록들 (1005 내지 1045) (도 10a)은 방법 (900)의 블록들 (905-945)과 상관성이 있다. 하지만, 블록 1050에서, 방법 (1000)은 방법 (900)과 상이하다. 블록 1050에서, 소닉페이 서비스 (105)는 지불 요청과 연관된 거래 금액을 도 8의 등록 프로세스 동안 수신된 사전승인 키와 함께 지불 서비스 (106)에 포워딩한다. 블록 1055에서, 거래 금액이 상인 계정에 대해 입금되었다는 것을 나타내는 리턴 키가 지불 서비스로부터 수신된다. 블록 1060에서, 확인이 소닉POS 시스템 (125)으로 리턴될 수도 있고, 거래 데이터가 상인에 의한 나중의 쿼리를 위해 소닉페이 서비스 (105)에 의해 저장될 수도 있다. 블록 1070에서, 구매 거래에 대한 영수증이 방법 (900)의 블록 (990)과 관련하여 설명되었던 것과 유사하게, POS 시스템 (125)에 의해 생성되고 PCD (110)에 무선으로 송신될 수도 있다.

[0070] 유리하게, 예시적인 방법 (1000)을 통해 완료된 구매 거래는 소비자 PCD (110)가 온라인으로 됨이 없이 일어난다. 즉, 프로세스 동안 PCD (110)로부터 송신되고 PCD (110)에 의해 수신된 데이터는 PCD (110)와 POS 시스템 (125) 사이에 무선으로 완전히 상점 (135) 내에서 교환된다. 또한, 구매 거래는 소비자의 기밀성 지불 크레덴셜들이 PCD (110) 상에 저장되거나, 그 문제를 위해, PCD (110)로부터 상인 POS 시스템 (125)으로 송신될 필요 없이 일어난다.

[0071] 이 명세서에서 설명된 프로세스들 또는 프로세스 흐름들에서의 어떤 단계들 또는 블록들은 자연스럽게 본 발명이 설명된 바와 같이 기능하도록 다른 것들로 진행한다. 하지만, 본 발명은, 이러한 순서 또는 시퀀스가 본 발명의 기능성을 변경하지 않는 경우 설명된 단계들 또는 블록들의 순서에 제한되지 않는다. 즉, 몇몇 단계들 또는 블록들은, 본 발명의 범위 및 사상으로부터 벗어남이 없이 다른 단계들 또는 블록들 전에, 후에, 또는 병행하여 (실질적으로 동시에) 수행될 수도 있다. 몇몇 경우들에서, 어떤 단계들 또는 블록들은 본 발명으로부터 벗어남이 없이 생략되거나 수행되지 않을 수도 있다. 또한, 몇몇 경우들에서, 본 개시에서 고유한 단계들 또는 블록들로서 묘사되고 설명된 다수의 행위들은 단일 단계 또는 블록 내에 포함될 수도 있다. 또한, "그 후", "그 다음", "다음으로", "후속하여" 등과 같은 단어들은 단계들 또는 블록들의 순서를 제한하는 것으로 의도되지 아니한다. 이들 단어들은 단순히 독자를 예시적인 방법의 설명을 관통하도록 안내하기 위해 사용된다.

[0072] 추가적으로, 프로그래밍 기술분야에서의 당업자는 예를 들어 이 명세서에서의 흐름도들 및 연관된 설명에 기초하여 어려움 없이 개시된 발명을 구현하기 위해 컴퓨터 코드를 쓰거나 적절한 하드웨어 및/또는 회로들을 식별할 수 있다. 따라서, 프로그램 코드 명령들 또는 상세한 하드웨어 디바이스들의 특정 세트의 개시는 본 발명을 어떻게 실시하고 이용하는지에 관한 적당한 이해를 위해 필수적인 것으로 고려되지 않는다. 청구된 컴퓨터 구현된 프로세스들의 창의적인 기능성은 다양한 프로세스 흐름들을 나타낼 수도 있는 도면들과 함께 상기 설명에서 보다 자세히 설명되었다.

[0073] 하나 이상의 예시적인 양태들에서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어, 또는 이들의 임의의 조합으로 구현될 수도 있다. 소프트웨어로 구현되는 경우, 기능들은 컴퓨터-판독가능 매체 상의 하나 이상의 명령

들 또는 코드로서 저장되거나 송신될 수도 있다. 컴퓨터-관독가능 매체는 한 장소에서 다른 장소로의 컴퓨터 프로그램의 전달을 용이하게 하는 임의의 매체를 포함하는 컴퓨터 저장 매체 및 통신 매체 양자 모두를 포함한다.

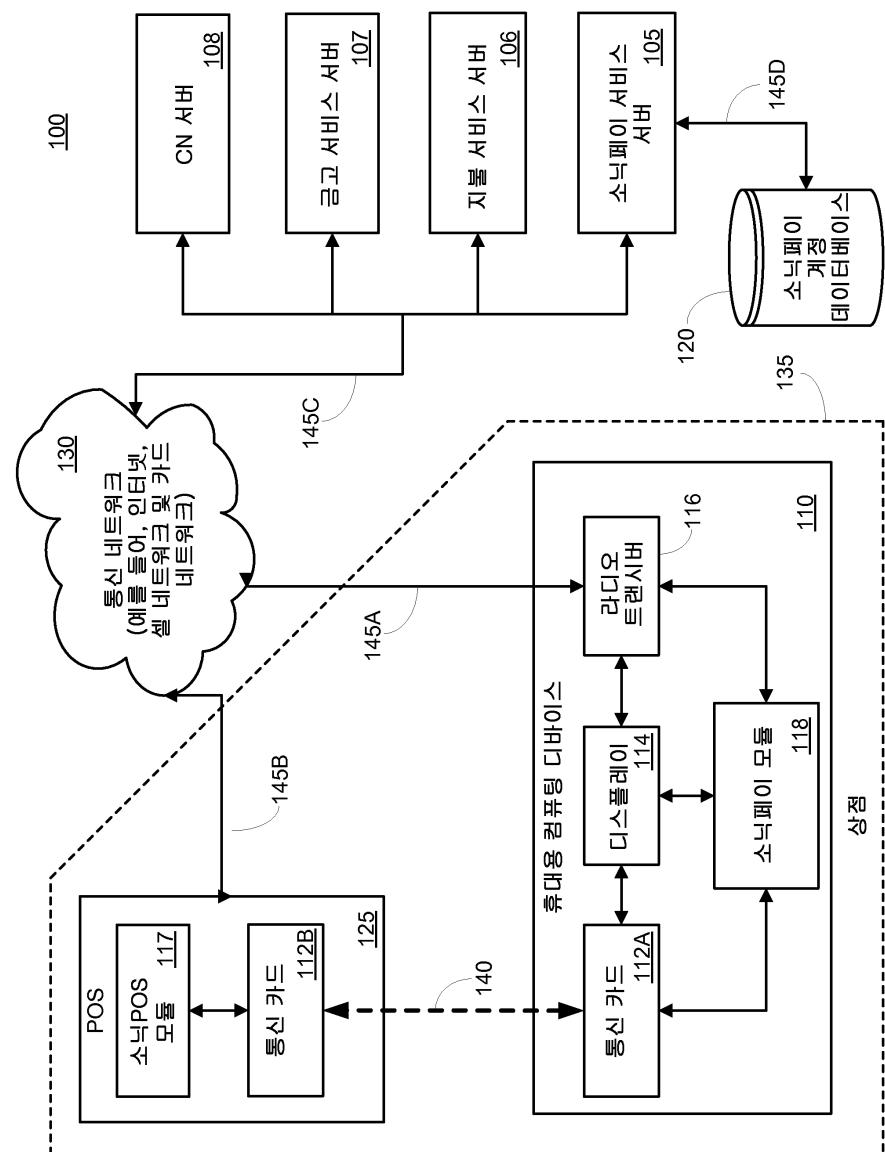
[0074] 저장 매체는 컴퓨터에 의해 액세스될 수도 있는 임의의 이용가능한 매체일 수도 있다. 제한이 아닌 예시로서, 이러한 컴퓨터-관독가능 매체는 RAM, ROM, EEPROM, CD-ROM 또는 다른 광학 디스크 스토리지, 자기 디스크 스토리지 또는 다른 자기적 저장 디바이스들, 또는 명령들 또는 데이터 구조들의 형태로 원하는 프로그램 코드를 운반 또는 저장하기 위해 이용될 수도 있고 컴퓨터에 의해 액세스될 수도 있는 임의의 다른 매체를 포함할 수도 있다. 또한, 임의의 연결이 적절하게 컴퓨터-관독가능 매체로 지정된다. 예를 들어, 소프트웨어가 동축 케이블, 광섬유 케이블, 트위스트 페어, 디지털 가입자 회선 ("DSL"), 또는 적외선, 라디오, 및 마이크로파와 같은 무선 기술들을 이용하여 웹사이트, 서버, 또는 다른 원격 소스로부터 송신되는 경우, 그 동축 케이블, 광섬유 케이블, 트위스트 페어, DSL, 또는 적외선, 라디오, 음향 및 마이크로파와 같은 무선 기술들은 매체의 정의 내에 포함된다.

[0075] 본원에서 사용된 디스크 (disk) 및 디스크 (disc) 는 콤팩트 디스크 ("CD"), 레이저 디스크, 광학 디스크, 디지털 다기능 디스크 ("DVD"), 플로피 디스크, 및 블루-레이 디스크를 포함하고, 여기서, 디스크 (disk) 들은 통상적으로 데이터를 자기적으로 재생하는 한편, 디스크 (disc) 들은 데이터를 레이저들을 이용하여 광학적으로 재생한다. 상기한 것들의 조합들 또한 컴퓨터-관독가능 매체의 범위 내에 포함되어야 한다.

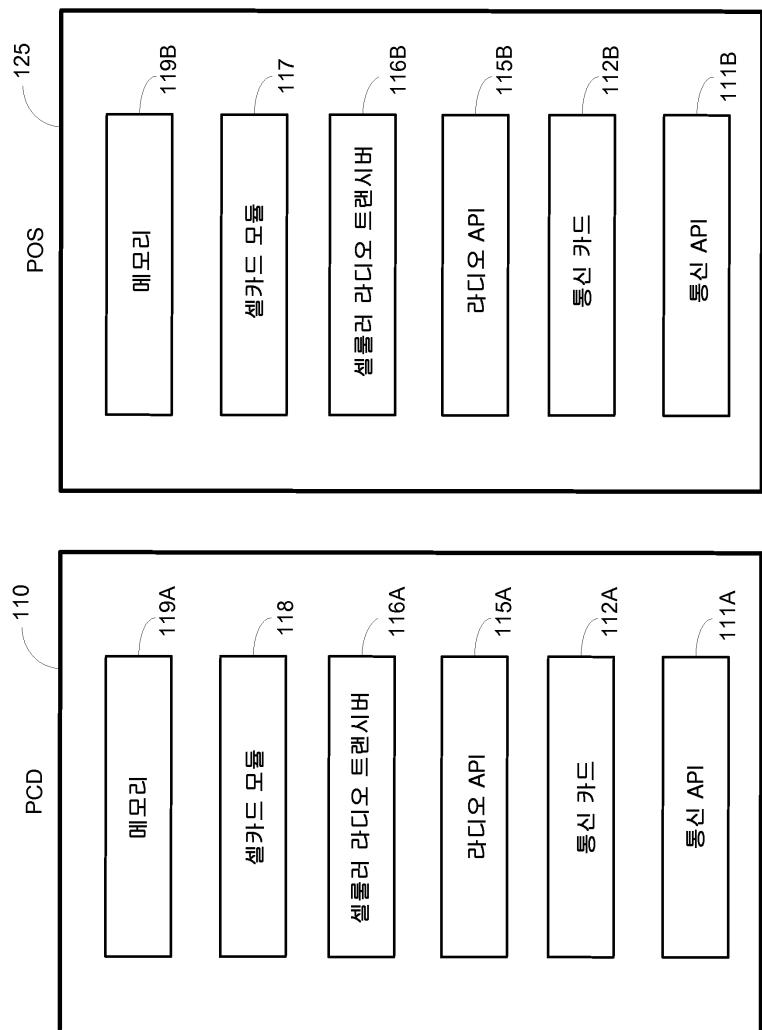
[0076] 따라서, 비록 선택된 양태들이 자세하게 예시되고 설명되었음에도 불구하고, 다양한 치환물들 및 변경물들이 이하의 청구항들에 의해 정의된 바와 같이 본 발명의 사상 및 범위로부터 벗어남이 없이 그 안에서 이루어질 수도 있다는 것이 이해될 것이다.

도면

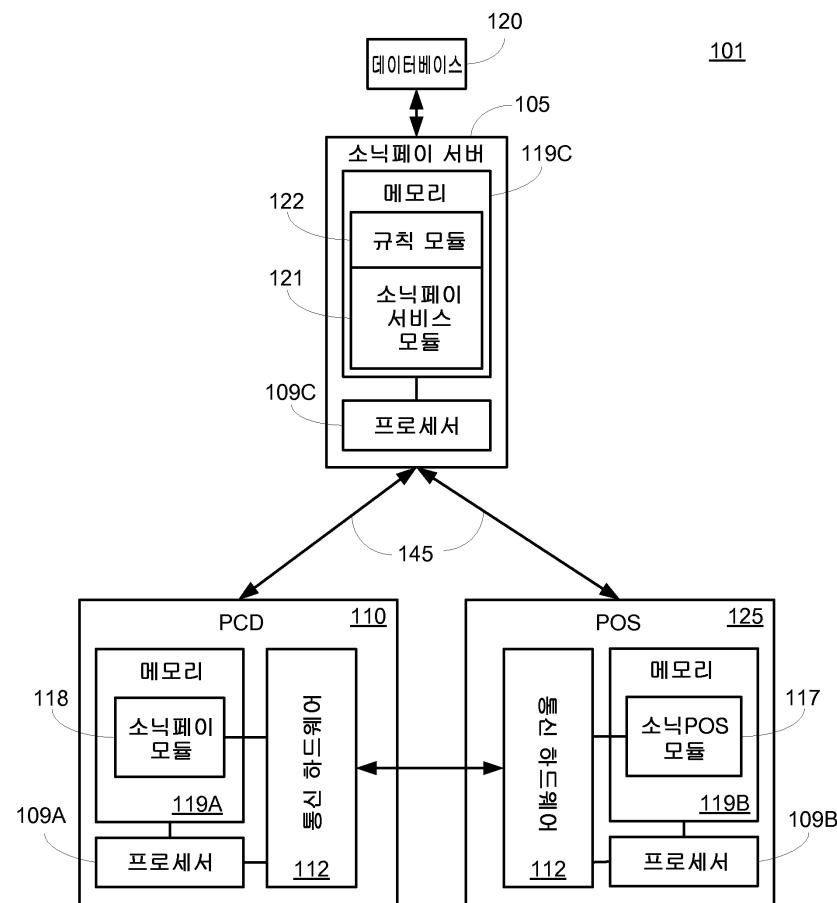
도면1



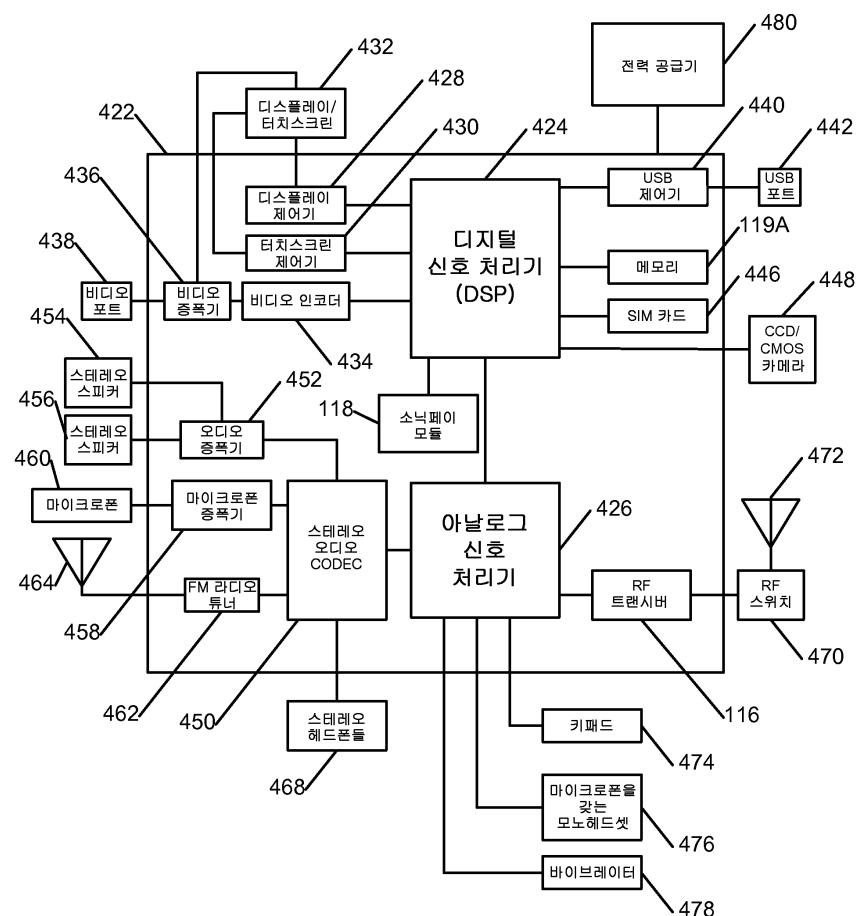
## 도면2



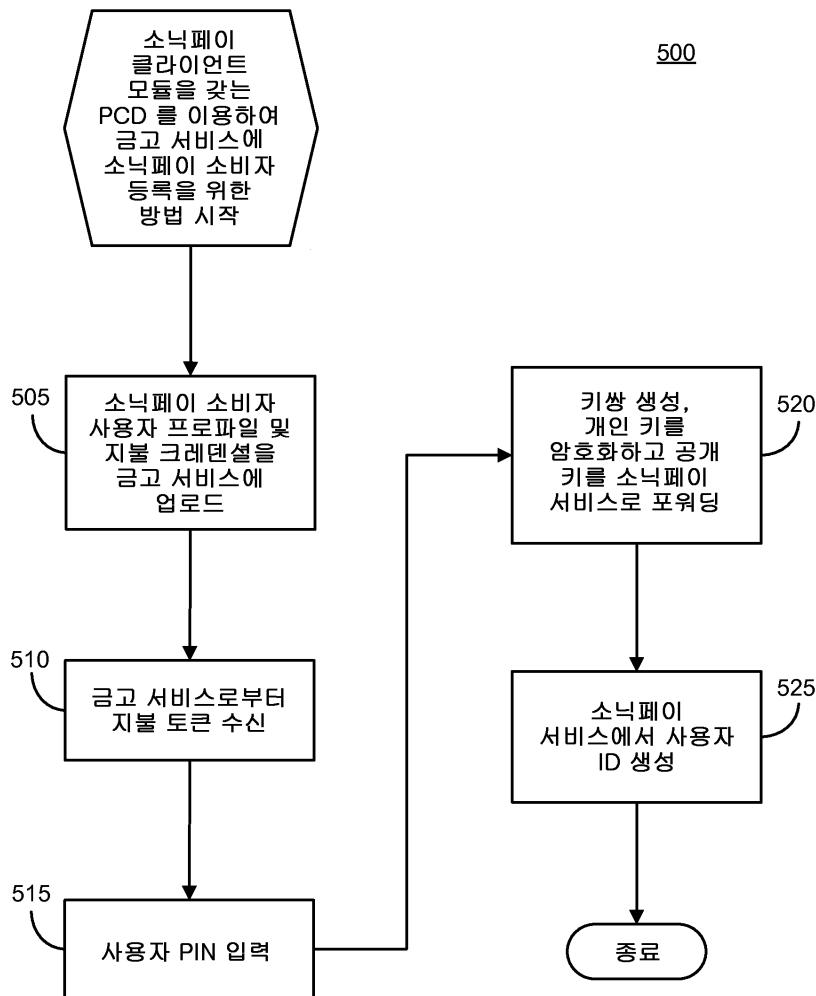
## 도면3



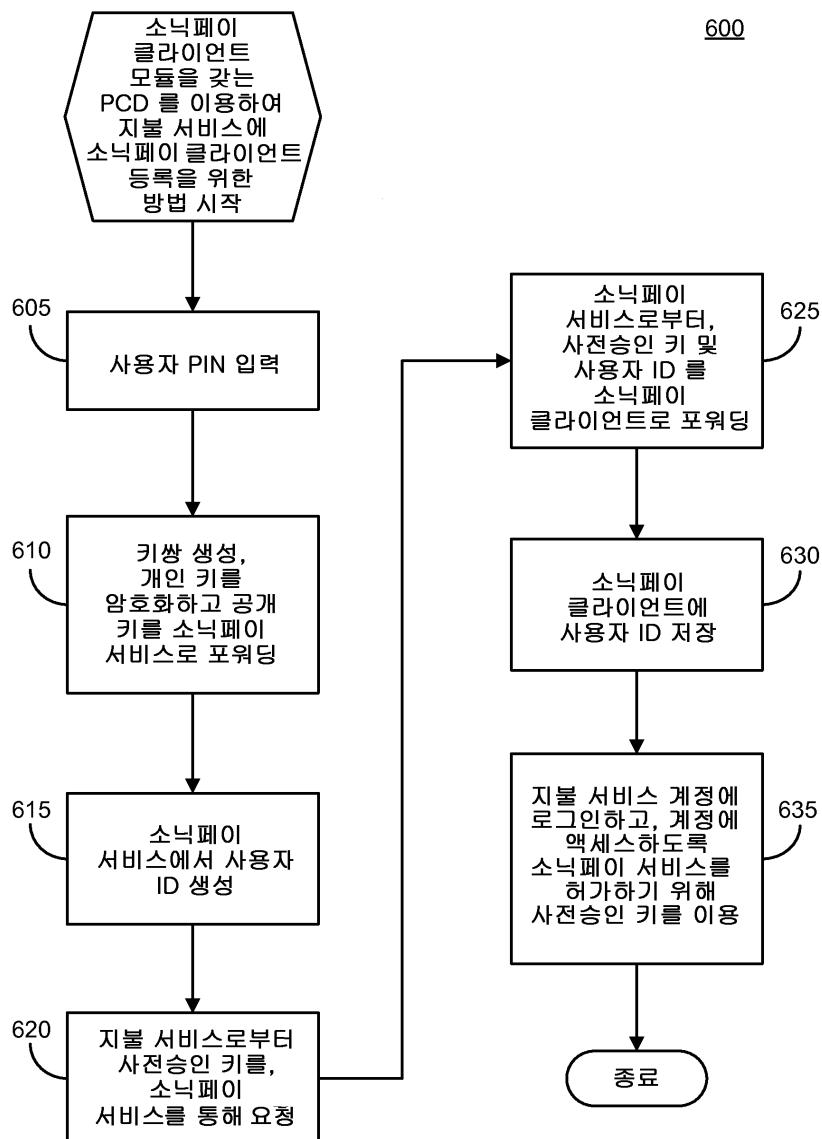
## 도면4



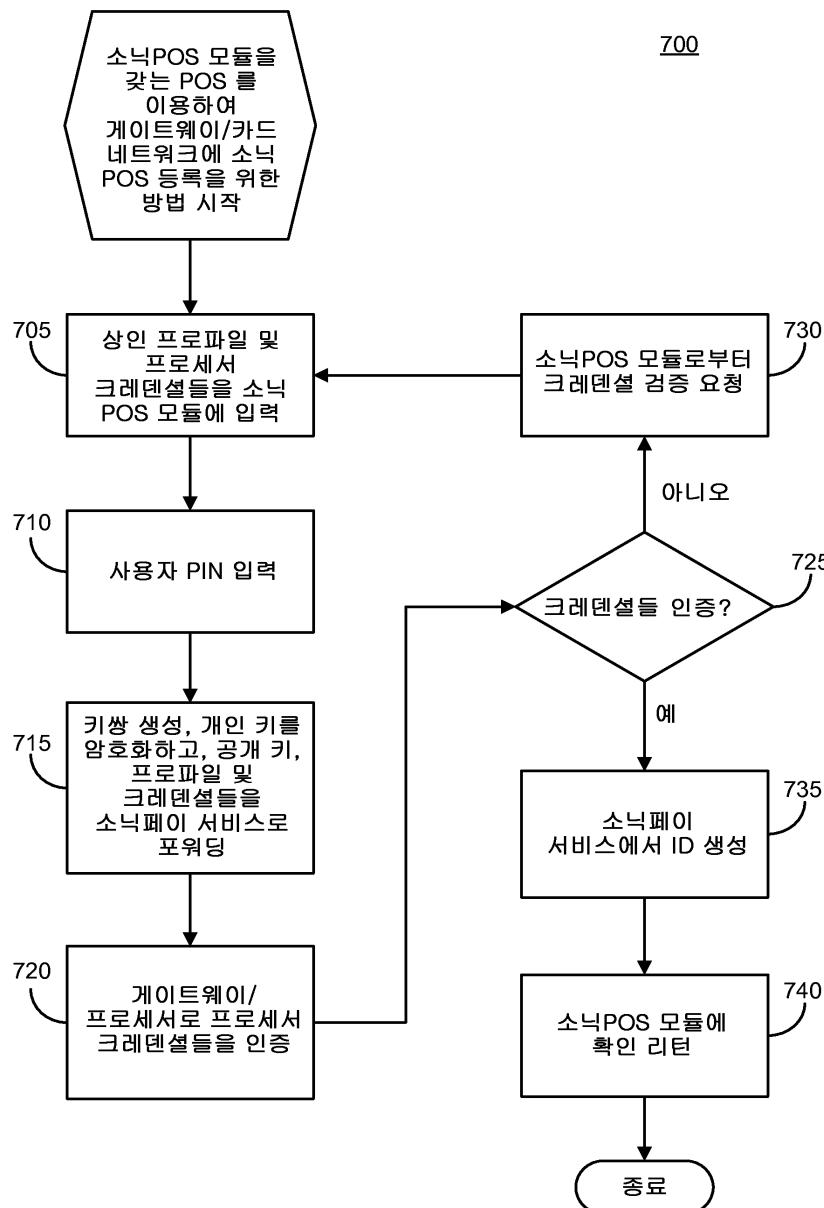
## 도면5



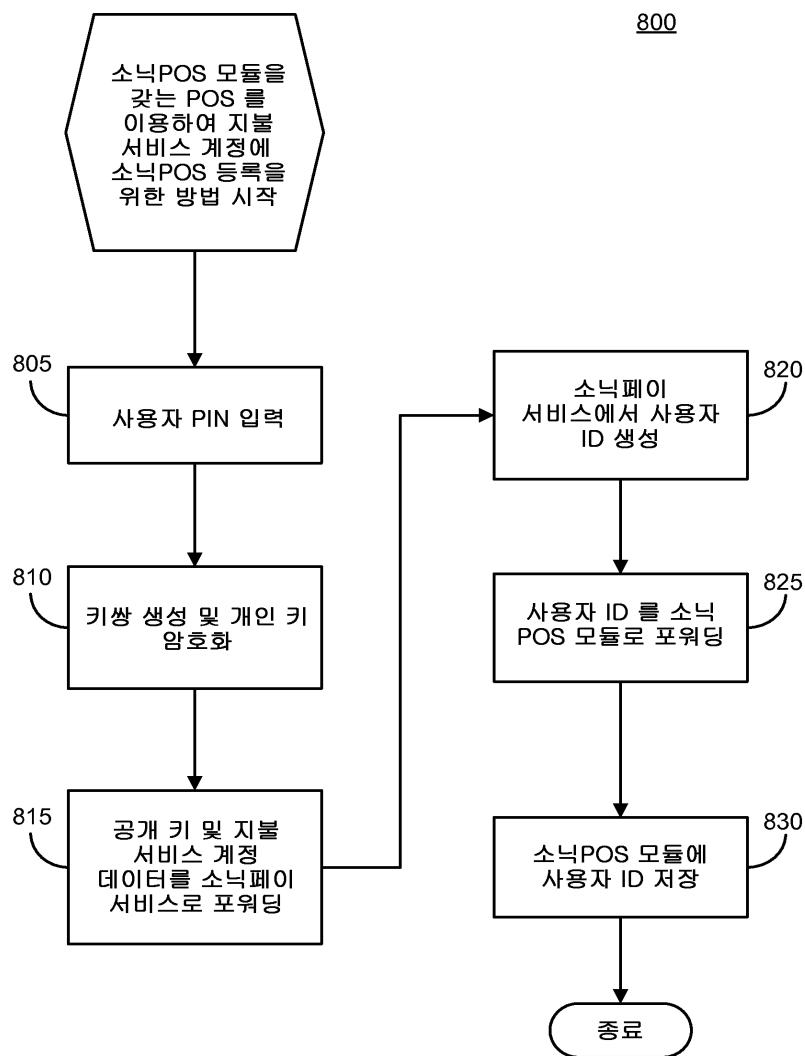
## 도면6



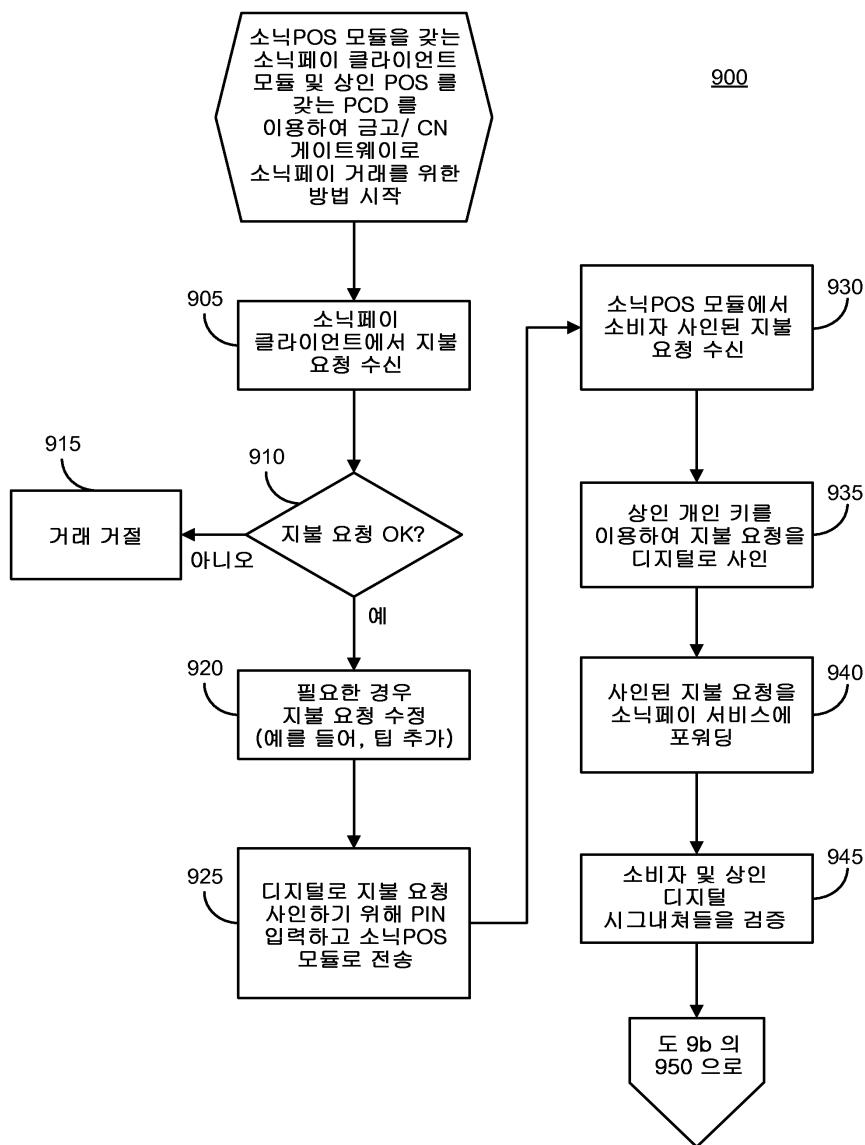
## 도면7



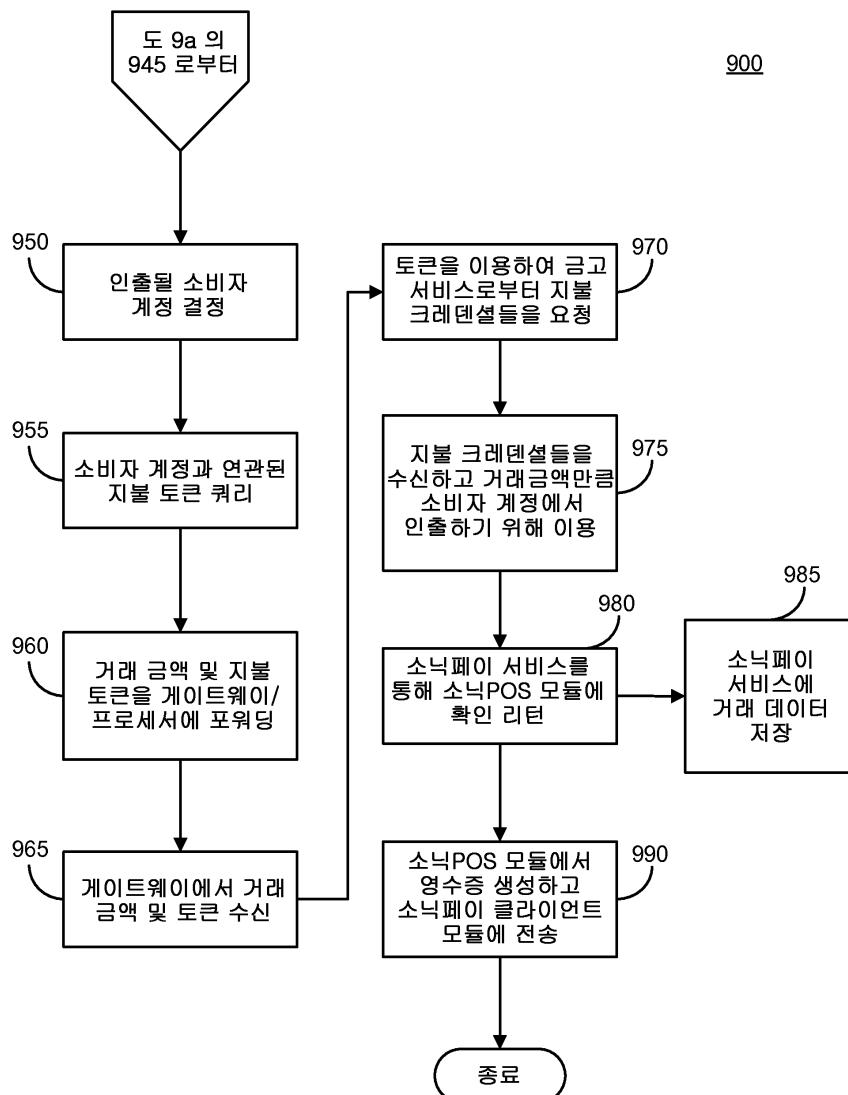
## 도면8



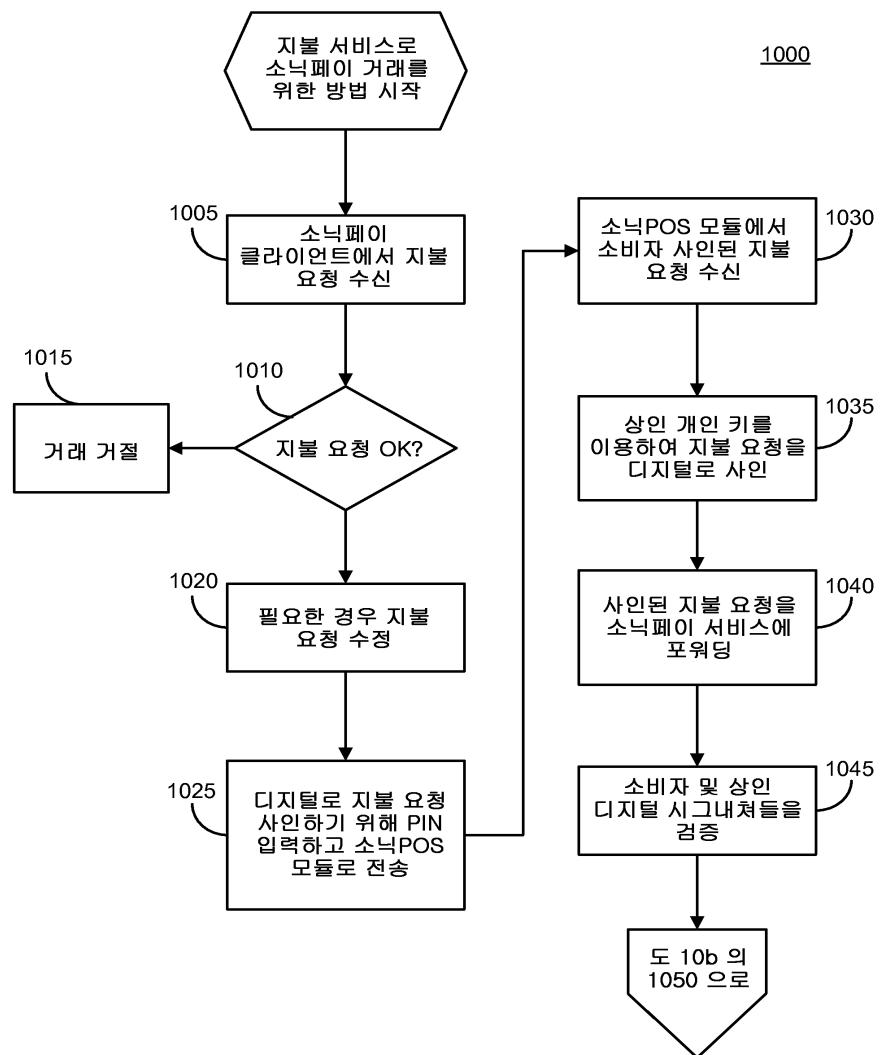
## 도면9a



## 도면9b



## 도면10a



## 도면10b

