(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0024903
(43) 공개일자 2020년03월09일

(51) 국제특허분류(Int. Cl.)
G06Q 20/32 (2012.01) *G06Q 20/34* (2012.01)
G06Q 20/36 (2012.01) *H04M 15/00* (2006.01)
H04W 4/24 (2009.01) *H04W 4/80* (2018.01)
H04W 84/16 (2009.01) *H04W 84/18* (2009.01)
H04W 88/06 (2009.01)
(52) CPC특허분류
G06Q 20/325 (2013.01)
G06Q 20/3276 (2013.01)
(21) 출원번호 10-2020-7003208
(22) 출원일자(국제) 2018년07월02일
심사청구일자 없음
(85) 번역문제출일자 2020년02월03일
(86) 국제출원번호 PCT/SG2018/050321
(87) 국제공개번호 WO 2019/009803
국제공개일자 2019년01월10일
(30) 우선권주장
201741023345 2017년07월03일 인도(IN)

(71) 출원인
지피 네트워크 아시아 피티이. 엘티디.
싱가포르, 싱가포르 068809, #38-01 오유이 다운타운, 센턴 웨이, 6
(72) 발명자
소마선다람, 마니카바사감
인도, 방갈로 560037, 슈리람 스판다나, 샬라가타로드, #304, 비6.
(74) 대리인
윤앤리특허법인(유한)

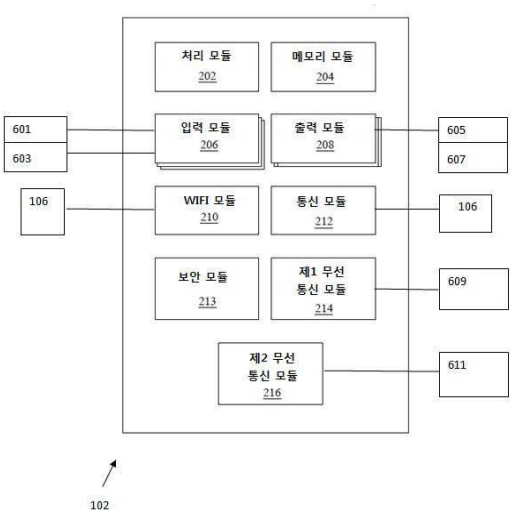
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 **결제 처리**

(57) 요 약

결제 단말기를 운영하기 위한 방법으로서, 방법은, 활성화 입력을 수신하는 단계, 및 활성화 입력에 응답하여 제1 형태의 외부 결제 장치와 통신하기 위한 제1 무선 신호 및 제2 형태의 외부 결제 장치와 통신하기 위한 제2 무선 신호를 출력하는 단계를 포함한다. 제1 무선 신호 및 제2 무선 신호는 각각 서로 다른 제1 프로토콜 및 제2 프로토콜로 포맷된다. 방법은 제1 무선 신호 및 제2 무선 신호 중 하나에 대한 응답을 수신하고, 응답에 대응하여 제1 무선 신호 및 제2 무선 신호 중 다른 하나의 출력을 종료하는 단계를 더 포함한다.

대 표 도 - 도6



(52) CPC특허분류
G06Q 20/3278 (2013.01)
G06Q 20/354 (2013.01)
G06Q 20/3672 (2013.01)
H04M 15/68 (2013.01)
H04M 15/93 (2013.01)
H04W 4/24 (2013.01)
H04W 4/80 (2018.02)
H04W 84/16 (2013.01)
H04W 84/18 (2013.01)

명 세 서

청구범위

청구항 1

결제 단말기를 운영하는 방법으로서, 상기 방법은:

활성화 입력을 수신하는 단계,

상기 활성화 입력에 응답하여, 제1 형태의 외부 결제 장치와 통신하기 위한 제1 무선 신호 및 제2 형태의 외부 결제 장치와 통신하기 위한 제2 무선 신호를 출력하는 단계,

상기 제1 무선 신호 및 상기 제2 무선 신호 중 하나에 대한 응답을 수신하는 단계, 및

상기 응답에 대응하여, 상기 제1 무선 신호 및 상기 제2 무선 신호 중 다른 하나의 출력을 종료하는 단계를 포함하고,

상기 제1 무선 신호 및 상기 제2 무선 신호는 각각 서로 다른 제1 프로토콜 및 제2 프로토콜로 포맷되는(formatted) 것을 특징으로 하는 방법.

청구항 2

제1항에 있어서, 통신 채널을 설정하기 위해 상기 외부 결제 장치를 인증하기 위한 상기 응답을 처리하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 3

제1항에 있어서, 상기 외부 결제 장치를 인증하기 위한 상기 응답을 처리하는 단계, 및 상기 처리하는 단계 이후에 상기 종료하는 단계를 실행하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 4

제1항에 있어서, 상기 무선 신호는 NFC 신호 및 불루투스 신호를 포함하는 것을 특징으로 하는 방법.

청구항 5

제1항에 있어서,

통신 채널을 설정하기 위해 상기 외부 결제 장치를 인증하기 위한 상기 응답을 처리하고, 상기 통신 채널로부터 사용자를 나타내는 데이터를 수신하는 단계;

입력에서, 거래 금액을 나타내는 데이터를 수신하고, 사용자를 나타내는 상기 데이터 및 거래 금액을 나타내는 데이터를 서버로 전송하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 6

제1항에 있어서,

통신 채널을 설정하기 위해 상기 외부 결제 장치를 인증하기 위한 상기 응답을 처리하고, 상기 통신채널로부터 사용자를 나타내는 데이터 및 현재의 거래를 식별하기 위한 일회성 검증기를 수신하는 단계;

입력에서, 거래 금액을 나타내는 데이터를 수신하고, 사용자를 나타내는 상기 데이터, 상기 일회성 검증기를 나타내는 데이터, 및 거래 금액을 나타내는 데이터를 서버에 전송하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 7

제6항에 있어서, 상기 통신 채널을 통하여 새로운 일회성 검증기를 출력하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 8

제1항에 있어서, 상기 제1 무선 신호 및 상기 제2 무선 신호 중 어느 것이 응답되는지를 나타내는 서버 정보와 통신하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 9

처리 장치, 및 결제 단말기가 활성화 입력에 응답하게 하여 제1 형태의 외부 결제 장치와 통신하기 위한 제1 무선 신호를 출력하고 또한 제2 형태의 외부 결제 장치와 통신하기 위한 제2 무선 신호 출력하도록 상기 처리 장치를 제어하기 위한 명령을 보유하는 저장장치를 구비한 외부 장치와 무선으로 통신하기 위한 상기 결제 단말기로서,

상기 제1 무선 신호 및 상기 제2 무선 신호는 각각 서로 다른 제1 프로토콜 및 제2 프로토콜로 포맷되며, 상기 제1 무선 신호 및 상기 제2 무선 신호 중 하나에 대한 응답의 수신에 대응하여 상기 제1 무선 신호 및 상기 제2 무선 신호 중 다른 하나의 출력을 종료하는 것을 특징으로 하는 결제 단말기.

청구항 10

제9항에 있어서, 활성화 신호를 제공하기 위한 키패드, 상기 처리 장치의 제어 하에 정보를 표시하기 위한 디스플레이, 및 서버와 통신하기 위한 출력 장치를 더 구비하는 것을 특징으로 하는 결제 단말기.

청구항 11

제9항에 있어서, 모두 상기 처리 장치의 제어하에서, 상기 제1 무선 신호를 출력하도록 구성된 제1 무선 장치 및 상기 제2 무선 신호를 출력하도록 구성된 제2 무선 장치를 구비하는 것을 특징으로 하는 결제 단말기.

청구항 12

제9항에 있어서, 보안 키용 저장장치를 포함하는 보안 장치를 더 구비하고, 상기 보안 장치는 상기 키를 사용하여 상기 단말기용 데이터를 암호화 또는 암호 해제하도록 구성되는 것을 특징으로 하는 결제 단말기.

청구항 13

제9항에 있어서, 상기 제1 무선 신호를 출력하도록 구성된 개인 영역 네트워크 장치를 구비하는 것을 특징으로 하는 결제 단말기.

청구항 14

제9항에 있어서, 상기 제2 무선 신호를 출력하도록 구성된 근거리 통신 장치를 구비하는 것을 특징으로 하는 결제 단말기.

발명의 설명

기 술 분 야

[0001] 본 발명은 결제 기술 분야와 관련이 있다.

배 경 기 술

[0002] 현금이 없는 결제는 편의상 주로 사용된다. 이러한 결제에는 카드 또는 휴대폰이 포함될 수 있다. 현금을 사용하지 않는 전자 거래를 구현하기 위해 휴대폰을 사용하는 동안 인터넷 연결이 제한된다.

[0003] 인터넷의 범위가 넓어지더라도, 모바일 장치를 사용하는 사용자가 항상 인터넷에 연결되어 있는지 확실하지 않다. 또한, 인터넷의 사용은 세계의 일부 지역 사회에 적절하지 않을 수도 있다. 이러한 경우, 휴대폰을 통한 전자 거래를 완료하는 것이 불가능할 수 있다.

[0004] 또한, 통상적으로, 판매자는 상이한 형태의 디지털 결제를 가능하게 하기 위해 상이한 형태의 결제 단말기를 배치해야 할 수 있다. 예를 들어, 판매자는 카드를 사용한 결제를 수락하기 위해 결제 단말기를 배치해야 할 수 있다. 또한, 판매자는 휴대 전화를 통한 결제를 지원하기 위해 또다른 단말기를 배치해야 할 수도 있다. 이러한 추가적인 단말기가 배치되더라도, 단말기는 NFC와 같은 특정 형태의 통신 기술을 사용하는 휴대 전화만 지원할

수 있다.

[0005] 이러한 상황을 개선할 필요가 있다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0006] 제1 측면에서, 두 프로토콜 또는 방법 중 하나에 응답할 수 있는 장치가 단말기와 근접한 경우 통신이 발생할 수 있도록, 결제 단말기는 2개의 통신 프로토콜 또는 방법에 대응하는 신호를 출력하는데 사용된다.

[0007] 제2 측면에서, 결제 단말기가 제공되며 두 가지 다른 통신 방법을 사용하여 통신할 수 있다. 사용 중에, 결제 단말기는 두 가지 방법 중 하나를 사용하여 휴대폰 또는 결제 카드와 같은 결제 장치와의 통신을 시작하기 위해 두 방법 모두에 관련된 신호를 출력한다. 두 방법 중 하나에 의해 통신이 설정되고 다른 방법은 종료된다.

[0008] 제3 측면에서, 활성화 입력을 수신하는 단계, 및 활성화 입력에 응답하여 제1 형태의 외부 결제 장치와 통신하기 위한 제1 무선 신호 및 제2 형태의 외부 결제 장치와 통신하기 위한 제2 무선 신호를 출력하는 단계를 포함하는 결제 단말기를 운영하는 방법이 제공되며, 제1 및 제2 무선 신호는 각각 서로 다른 제1 및 제2 프로토콜로 포맷되고(formatted), 제1 및 제2 무선 신호 중 하나에 대한 응답을 수신하고, 응답에 대응하여, 제1 및 제2 무선 신호 중 다른 하나의 출력을 종료한다.

[0009] 방법은 외부 결제 장치를 인증하기 위한 응답을 처리하여 통신 채널을 설정하는 단계를 더 포함할 수 있다.

[0010] 방법은 외부 결제 장치를 인증하기 위해, 그리고 처리 단계 후에 종료 단계를 구현한 후에, 응답을 처리하는 단계를 더 포함할 수 있다.

[0011] 무선 신호는 NFC 신호 및 블루투스 신호를 포함할 수 있다.

[0012] 방법은 통신 채널을 설정하기 위해 외부 결제 장치를 인증하기 위한 응답을 처리함으로써 통신 채널로부터 사용자를 나타내는 데이터를 수신하는 단계; 입력에서, 거래 금액을 나타내는 데이터를 수신하고, 사용자를 나타내는 데이터 및 거래 금액을 나타내는 데이터를 서버로 전송하는 단계를 더 포함할 수 있다.

[0013] 방법은 통신 채널을 설정하기 위해 외부 결제 장치를 인증하기 위한 응답을 처리하고, 통신 채널로부터 사용자를 나타내는 데이터 및 현재 거래를 식별하기 위한 일회성 검증기를 수신하는 단계; 입력에서, 거래량을 나타내는 데이터를 수신하고 사용자를 나타내는 데이터 일회성 검증기를 나타내는 데이터 및 거래 금액을 나타내는 데이터를 서버로 전송하는 단계를 더 포함할 수 있다.

[0014] 방법은 통신 채널을 통해 새로운 일회성 검증기를 출력하는 단계를 더 포함 할 수 있다.

[0015] 방법은 제1 및 제2 무선 신호 중 어느 것이 응답되는지를 나타내는 정보를 서버와 통신하는 단계를 더 포함할 수 있다.

[0016] 제4 측면에서, 처리 장치를 갖는 외부 장치와 무선으로 통신하기 위한 결제 단말기, 및 결제 단말기가 제1 형태의 외부 결제 장치와 통신하기 위한 제1 무선 신호 및 제2 형태의 외부 결제 장치와 통신하기 위한 제2 무선 신호를 출력하기 위해 활성화 입력에 응답하게 하도록 처리 장치를 제어하기 위한 명령을 보유하는 저장장치가 개시되고, 제1 및 제2 무선 신호는 각각 서로 다른 제1 및 제2 프로토콜로 포맷되고, 제1 및 제2 무선 신호 중 하나에 대한 응답을 수신하여 제1 및 제2 무선 신호 중 다른 하나의 출력을 종료하는 것에 대응하여 응답한다.

[0017] 결제 단말기는 활성화 신호를 제공하기 위한 키패드, 처리 장치의 제어하에 정보를 표시하기 위한 디스플레이, 및 서버와 통신하기 위한 출력 장치를 더 포함 할 수 있다.

[0018] 결제 단말기는 처리 장치의 제어하에, 제1 무선 신호를 출력하도록 구성된 제 1 무선 장치 및 제2 무선 신호를 출력하도록 구성된 제2 무선 장치를 더 포함할 수 있다.

[0019] 결제 단말기는 보안 키용 저장장치를 포함하는 보안 장치를 더 포함할 수 있고, 보안 장치는 키를 사용하여 단말기용 데이터를 암호화 또는 암호해제하도록 구성된다.

[0020] 개인 영역 네트워크 장치는 제1 무선 신호를 출력하도록 구성될 수 있다.

[0021] 근거리 통신 장치는 제2 무선 신호를 출력하도록 구성될 수 있다.

[0022] 제5 측면에서, 결제 처리를 위한 시스템이 제공된다. 시스템은 제1 무선 통신 모듈 및 제2 무선 통신 모듈을 포함하는 결제 단말기를 포함한다. 제1 모듈은 제2 통신 방법과는 다른 제1 통신 방법을 사용하여 근접 통신을 개시 및 설정할 수있다. 제2 모듈은 제2 통신 방법을 사용하여 근접 통신을 개시 및 설정할 수 있다. 결제 단말기는 거래를 시작하기 위한 입력을 수신하고; 제1 모듈과 제2 모듈이 각각의 방법을 사용하여 통신의 시작을 시도하도록 구성된다. 통신 모듈 중 어느 것이 성공적인지에 따라 결제 단말기와 외부 객체 사이의 통신이 개시될 수 있도록, 제1 및 제2 방법 중 하나에 의해 통신될 수 있는 외부 객체는 결제 단말기와 근접할 수 있다.

[0023] 제1 무선 통신 모듈은 개인 영역 네트워크 모듈일 수 있다. 제2 무선 통신 모듈은 근거리 통신 모듈일 수 있다. 결제 단말기는 전술한 거래가 종료될 때까지 제1 무선 통신 모듈 및 제2 통신 모듈을 사용하여 임의의 다른 외부 객체와의 통신 채널을 설정하기 위한 시도를 종료하도록 더 구성될 수 있다. 외부 객체는 카드 및 휴대용 통신 장치 중 하나일 수 있으며, 결제 단말기는 설정된 통신이 카드의 근거리 통신 태그 중 하나와 관련되어 있는지, 휴대용 통신 장치의 근거리 통신 모듈 또는 휴대용 통신 장치의 개인 영역 네트워크 모듈인지를 식별하도록 더 구성될 수 있다. 결제 단말기는 또한 설정된 통신이 카드의 근거리 통신 태그 중 하나와 통신하는지 여부, 휴대용 통신 장치의 근거리 통신 모듈 또는 휴대용 통신 장치의 개인 영역 네트워크 모듈인지를 서버와 통신하도록 구성될 수 있다. 외부 객체는 휴대용 통신 장치일 수 있고, 결제 단말기는, 휴대용 통신 장치와의 통신을 설정할 때, 적어도 거래에 연결되어 결제를 시도하는 사용자를 식별하는 데이터를 수신하고; 적어도 사용자를 식별하는 데이터, 가맹점을 식별하는 데이터, 및 결제 금액을 식별하는 데이터를 서버로 통신하여 거래를 처리함으로써, 휴대용 통신 장치가 인터넷을 사용하지 않고 결제할 수 있게 하도록 구성될 수 있다. 결제 단말기는, 외부 객체로부터 위치 검증 데이터를 수신하고; 위치 검증 데이터에 기초하여, 결제 단말기를 사용하여 결제가 수락될 수 있는지를 검증하고; 결제를 수락할 수 없는 것으로 확인되면 거래를 거부하거나 또는 결제가 승인될 수 있는 것으로 확인되면 거래를 처리하도록 더 구성될 수 있다. 외부 객체는 근거리 통신이 가능한 카드일 수 있고, 결제 단말기는 카드로부터 사용자를 식별하는 데이터 및 일회성 검증기로서 사용될 데이터를 판독하고; 카드에 새로운 일회성 검증기를 작성하며; 사용자를 식별하는 데이터와 일회성 검증기로 사용될 데이터를 서버에 전달하도록 구성되며, 일회성 검증기는 일회성 검증기가 현재 거래에 대한 카드에서 거래를 거부하거나 거래를 진행할 것으로 예상되는 카드인지 확인하는 데 사용된다. 결제 단말기는, 각각의 거래에 대해, 고유한 일회성 검증기인 서버로 통신하도록 더 구성될 수 있고, 일회성 검증기는 현재의 거래가 거래를 거부하거나 또는 거래를 진행하기 위해 결제 단말기로부터 예상되는 것이 있는지를 검증하는데 사용될 수 있다. 외부 객체는 휴대용 통신 장치일 수 있고, 결제 단말기는 휴대용 통신 장치로부터 사용자를 식별하는 데이터 및 일회성 검증기로서 사용될 데이터를 수신하고; 휴대용 통신 장치에서 새로운 일회성 검증기를 업데이트하며; 사용자를 식별하는 데이터와 일회성 검증기로 사용될 데이터를 서버에 전달하도록 구성될 수 있으며, 일회성 검증기는 일회성 검증기가 현재의 거래가 거래를 거부하거나 거래를 진행하기 위해 휴대용 통신 장치로부터 예상되는 것인지 검증하는데 사용된다.

[0024] 또다른 측면에서, 결제 처리 방법이 제공된다. 방법은 결제 단말기에서 거래를 개시하기 위한 입력을 수신하는 단계를 포함한다. 그후에, 결제 단말기에 제공된 제1 무선 통신 모듈 및 제2 무선 통신 모듈은 외부 객체와의 통신 채널을 설정하려고 시도한다. 제1 무선 통신 모듈은, 제2 무선 통신 모듈이 설정될 수 있는 제2 통신 채널과 다른, 제1 통신 채널을 사용하여 근접 통신을 설정할 수 있다. 방법은, 통신 모듈 중 하나가 외부 객체와의 통신 채널을 성공적으로 설정하는 것에 기초하여, 제1 무선 통신 모듈 및 제2 무선 통신 모듈 중 하나를 사용하여 외부 객체와 통신 채널을 설정하는 단계를 더 포함한다.

[0025] 또다른 측면에서, 결제 처리를 위한 시스템이 제공된다. 시스템은 개인 영역 네트워크(PAN) 모듈을 포함하는 결제 단말기를 포함한다. 결제 단말기는 PAN 모듈이 식별자를 브로드 캐스팅하도록 구성된다. 시스템은 휴대용 통신 장치를 더 포함한다. 장치는 결제 단말기에 의해 브로드 캐스팅된 식별자를 수신하고; 브로드 캐스팅된 식별자의 신호 강도가 제1 임계값을 초과하는 경우, 결제 단말기의 PAN 모듈과 통신 채널을 설정하기 위한 요청을 자동으로 전송하며; 통신 채널이 설정되면 결제 단말기의 PAN 모듈 사이의 신호 강도가 거래가 완료될 때까지 제1 임계값 아래로 떨어지더라도 결제 채널의 PAN 모듈과 통신을 계속 유지하도록 구성된다.

[0026] 또다른 측면에서, 결제 처리 방법이 제공된다. 방법은 결제 단말기의 개인 영역 네트워크 모듈에 의해 식별자를 브로드 캐스팅하는 단계; 휴대용 통신 장치에 의해, 결제 단말기에 의해 브로드 캐스팅된 식별자를 수신하는 단계; 브로드 캐스팅된 식별자의 신호 강도가 제1 입계값을 초과하는 경우, 휴대용 통신 장치에 의해 결제 단말기

의 개인 영역 네트워크 모듈과의 통신 채널 설정 요청을 자동으로 전송하는 단계를 포함한다. 방법은, 휴대용 통신 장치와 결제 단말기의 개인 영역 네트워크 모듈 사이의 신호 강도가 제1 입계값 아래로 떨어지더라도, 통신 채널이 설정되면, 거래가 완료될 때까지 휴대용 통신 장치와 결제 단말기의 개인 영역 네트워크 모듈 사이의 통신을 유지하는 단계를 더 포함한다.

[0027] 또한, 결제를 처리하기 위한 시스템이 제공되고, 시스템은: 개인 영역 네트워크 모듈을 포함하는 결제 단말기 - 결제 단말기는 개인 영역 네트워크 모듈이 식별자를 브로드 캐스팅하도록 구성된다 -; 및 휴대용 통신 장치를 포함하고, 휴대용 통신장치는 결제 단말기에 의해 브로드 캐스팅된 식별자를 수신하고; 브로드 캐스팅된 식별자의 신호 강도가 제1 입계값을 초과하는 경우, 결제 단말기의 개인 영역 네트워크 모듈과 통신 채널을 설정하기 위해 자동으로 요청을 전송하며; 통신 채널이 설정되면, 휴대용 통신 장치와 결제 단말기의 개인 영역 네트워크 모듈 사이의 신호 강도가 제1 입계값 아래로 떨어지더라도, 거래가 완료될 때까지 결제 단말기의 개인 영역 네트워크 모듈과 계속 통신을 유지하도록 구성된다.

[0028] 제1 입계값은 휴대용 통신 장치와 결제 단말기가 서로 20cm 내에 있도록 통신 채널을 설정하도록 구성될 수 있다. 제1 입계값은 휴대용 통신 장치와 결제 단말기가 통신 채널을 설정하기 위해 서로 10cm 내에 있도록 구성될 수 있다.

[0029] 제1 입계값은 휴대용 통신 장치와 결제 단말기가 통신 채널을 설정하기 위해 서로 미리 구성된 거리 내에 있도록 구성될 수 있다.

[0030] 휴대용 통신 장치와 결제 단말기의 개인 영역 네트워크 모듈 사이의 신호 강도가 제2 입계값 아래로 떨어지는 경우, 결제 단말기 또는 휴대용 통신 장치 중 적어도 하나는 설정된 통신 채널을 종료하도록 구성될 수 있다.

[0031] 제2 입계값은 원격으로 재구성 가능할 수 있다.

[0032] 결제 단말기는 통신 채널을 설정할 때, 적어도 거래에 연결된 결제를 시도하는 사용자를 식별하는 데이터를 수신하고; 거래를 처리하기 위해 적어도 사용자를 식별하는 데이터, 판매자를 식별하는 데이터, 및 결제 금액을 식별하는 데이터를 서버에 전달하여 휴대용 통신 장치가 인터넷을 사용하지 않고 결제할 수 있게 하도록 구성될 수 있다.

[0033] 결제 단말기는, 휴대용 통신 장치를 사용하여 결제하는 사용자의 계좌 잔고에 대응하는 데이터를 서버로부터 수신하고; 계좌 잔고에 대응하는 데이터를 통신 채널을 통해 휴대용 통신 장치로 전달하도록 더 구성될 수 있다.

[0034] 결제 단말기는, 거래 정보에 대응하는 데이터를 서버로부터 수신하고; 통신 채널을 통해 거래 정보에 대응하는 데이터의 적어도 일부를 휴대용 통신 장치에 전달하도록 더 구성될 수 있다.

[0035] 결제 단말기는 사용자의 계좌 잔고를 표시하지 못할 수 있고, 휴대용 통신 장치는 거래를 게시한 사용자의 계좌 잔고를 표시하도록 구성된다.

[0036] 식별자는 호환성을 식별하는 데이터를 포함할 수 있고, 휴대용 통신 장치에 의해 수신된 식별자가 호환성을 식별하는 데이터를 포함하는 경우, 휴대용 통신 장치는 통신 채널의 설정을 자동으로 요청하기 위한 결제 단말기를 고려하도록 구성된다.

[0037] 결제 단말기는, 전달될 금액을 나타내는 입력을 수신하고; 금액을 나타내는 입력이 수신된 후, 식별자의 브로드 캐스팅을 시작하기 위한 입력을 수신하며; 통신 채널이 설정되면, 금액에 대응하는 데이터 및 결제 단말기에 연결된 판매자를 휴대용 통신 장치로 전달하도록 구성될 수 있고, 판매자에 대응하는 금액 및 정보는 휴대용 통신 장치에 디스플레이된다.

[0038] 제1 임계값은 원격으로 재구성 가능할 수 있다.

[0039] 개인 영역 네트워크 모듈은 BLUETOOTH 저에너지 모듈 또는 BLUETOOTH 모듈 중 하나일 수 있다.

[0040] 또한, 결제를 처리하기 위한 방법이 개시되고, 방법은: 결제 단말기의 개인 영역 네트워크 모듈에 의해 식별자를 브로드 캐스팅하는 단계; 휴대용 통신 장치에 의해, 결제 단말기에 의해 브로드 캐스팅된 식별자를 수신하는 단계; 브로드 캐스팅된 식별자의 신호 강도가 제1 입계값을 초과하는 경우, 휴대용 통신 장치에 의해, 결제 단말기의 개인 영역 네트워크 모듈과의 통신 채널 설정 요청을 자동으로 전송하는 단계; 및 일단 통신 채널이 설정되면, 휴대용 통신 장치와 결제 단말기의 개인 영역 네트워크 모듈 사이의 신호 강도가 제1 입계값 아래로 떨어지더라도, 휴대용 통신 장치와 결제 단말기의 개인 영역 네트워크 모듈 사이의 통신을 거래가 완료될 때까지 유지하는 단계를 포함한다.

도면의 간단한 설명

[0041] 도 1은 결제를 처리하기 위한 시스템(100)을 도시한다.

도 2는 시스템(100)의 결제 단말기(102)의 블록도이다.

도 3a 내지 도 3f는 시스템(100)에 의한 결제를 처리하는 예시적인 방법의 흐름도이다.

도 4a는 결제 단말기(102)에 입력된 금액을 도시한다.

도 4b는 결제를 위해 사용자에 의해 개방된 스마트폰(104b)의 애플리케이션의 사용자 인터페이스를 도시한다.

도 4c는 결제 단말기(102)를 검색하는 스마트폰(104b)의 애플리케이션의 사용자 인터페이스를 도시한다.

도 4d는 스마트폰(104b)이 결제 단말기(102)에 가까이 온 후 BLE 채널을 통해 결제 단말기(102)와 페어링된 스마트폰(104b)을 도시한다.

도 4e는 스마트폰(104b)의 애플리케이션의 사용자 인터페이스를 도시하며, 사용자는 결제를 승인하기 위한 입력을 제공하고 있다

도 4f는 스마트폰(104b)의 애플리케이션의 사용자 인터페이스를 도시하며, 거래가 처리되고 있는 것으로 도시되어 있다.

도 4g는 스마트폰(104b)의 애플리케이션의 사용자 인터페이스를 도시하며, 성공적인 거래 후 거래 정보가 디스플레이된다.

도 5a는 예시적인 거래 패킷의 개략적인 다이어그램을 도시한다.

도 5b는 다른 거래 패킷을 도시한다.

도 6은 결제 단말기에 대한 일부 연결이 어떻게 수행될 수 있는지를 나타내는 결제 단말기의 실시예의 개략적인 블록도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0042] 아래의 서술에서, 전화 또는 스마트폰에 대한 언급은 특정 형태의 휴대용 통신 장치에 대해 제한적이지 않다. 용어는 편의를 위해 사용되며 의도는 모든 형태의 휴대용 통신 장치를 포괄하는 것이다.

[0043] 사용자가 결제할 때 인터넷을 사용할 필요 없이 결제를 처리할 수 있는 시스템이 개시된다. 결제는, 예를 들어, 근거리 통신(NFC) 가능 카드, 또는 NFC 또는 저에너지 블루투스(Bluetooth low energy, BLE) 기술을 갖춘 스마트폰을 사용하여 이루어질 수 있다.

[0044] 판매자 위치에 배치된 결제 단말기에 의해 결제가 촉진된다. 결제 단말기는 개인 영역 네트워크 모듈(BLE 모듈) 및 NFC 모듈을 포함할 수 있다. 일 실시예에서, 거래가 시작될 때, 결제 단말기는 결제를 하기 위해 소비자/사용자에 의해 제시된 외부 객체와 BLE 및 NFC를 동시에 사용하여 통신을 개시하도록 구성된다. 외부 객체는 NFC 지원 카드 또는 NFC 또는 BLUETOOTH 저에너지(BLE) 기술을 갖춘 스마트폰일 수 있으며, 외부 객체에 애플리케이션이 설치되어 결제 단말기와 거래 할 수 있다.

[0045] 또다른 실시예에서, 거래 단말기는 일정 기간 동안 BLE 및 NFC 중 하나를 시도한 다음, BLE 및 NFC 중 다른 하나를 시도하는데 실패한 경우, 그리고 필요하다면 BLE 및 NFC 모두를 반복하여 시도하는 것을 반복하도록 구성된다.

[0046] 일 실시예에서, 결제 단말기가 BLE 및 NFC 중 하나를 통해 외부 객체와의 통신 채널을 설정하는 데 성공하면, 결제 단말기는 개시된 거래가 종료될 때까지 (다른 외부 객체와의 통신을 시도하는 것으로부터) 다른 기술을 비활성화하도록 구성된다.

[0047] 또다른 실시예에서, 결제 단말기는 2개의 출력 중 다른 하나의 신호 응답을 검출하자마자 2개의 출력 중 하나를 방출하는 것을 중단한다. 이는 배터리로 구동되는 단말기에서 배터리 전원을 절약할 수 있게 한다.

[0048] 일 실시예에서, 결제 단말기와의 통신 채널은 NFC를 통해 설정되고, 사용자는 결제 단말기 근처에 카드 또는 NFC 지원 스마트폰을 가져온다. 결제 단말기는 전화기의 카드/NFC 모듈로부터 데이터를 판독하고 백엔드 서버와 통신하여 시작된 결제 거래를 처리한다. 판매자는 어떤 통신 수단을 사용할 것인지에 관해 결제 단말기에 지시

하지 않고, 결제 단말기는 자동적으로 스스로 어떤 통신 수단을 사용할 것인지를 결정한다는 것에 주의한다.

[0049] 일 실시예에서, 결제 단말기와의 통신 채널은 BLE를 통해 설정되고, 사용자는 BLE 가능 스마트폰을 결제 단말기 근처에 가져온다. 결제 단말기는 전화기의 BLE 모듈로부터 데이터를 수신하여 백엔드 서버와 통신하여 시작된 결제 거래를 처리한다. 이 경우조차도, 판매자는 어떤 통신 수단을 사용할 것인지에 관해 결제 단말기에 지시하지 않고, 결제 단말기는 자동적으로 스스로 어떤 통신 수단을 사용할 것인지를 결정한다는 것에 주의한다.

[0050] BLE의 경우, 결제 단말기는 BLE를 통해 설정된 통신 채널을 통해 사용자 계좌에서 공제된 금액 및 잔액과 같은 (백엔드 서버로부터 수신된) 거래 정보를 사용자의 스마트폰으로 전송한다. 따라서, 사용자는 결제할 수 있을 뿐만 아니라 인터넷이나 SMS 또는 이와 유사한 대안을 사용하지 않고도 거래 및 계정을 업데이트할 수 있다.

[0051] 도 1을 참조하면, 결제 처리 시스템(100)은 NFC 지원 카드(104a) 및 휴대용 통신 장치(104b)와 같은 외부 객체를 통해 결제를 수신할 수 있는 결제 단말기(102)를 갖는다. 사용중인 결제 단말기(102)는 통신 네트워크(108)를 통해 서버(106)와 통신한다.

[0052] 결제 단말기(102)는, 예를 들어, 다른 컴퓨팅 장치 중에서, 카드 판독기, 스마트폰, POS 시스템, 태블릿, 패블릿, 컴퓨터, 및 랩탑일 수 있다.

[0053] 이제, 도 2를 참조하면, 결제 단말기(102)의 실시예는 처리 모듈(202), 메모리 모듈(204), 입력 모듈(206), 출력 모듈(208), WIFI 모듈(210), 통신 모듈(212), 보안 모듈(213), 제1 무선 통신 모듈(214) 및 제2 무선 통신 모듈(216)을 포함한다. 메모리 모듈(204)은 처리 모듈(202)에 연결되는 버스에 연결된다. 처리 모듈(202)은 버스(123)에 의해 다른 모든 모듈에 연결된다. 처리 모듈(202)은 결제 단말기(102)의 기능을 수행하기 위해 메모리 모듈(204)에 저장된 실행 가능한 명령의 제어 하에서 동작하고, 일반적으로 이들의 기능을 수행하기 위해 장치의 다른 모듈을 호출한다.

[0054] 이제, 도 6을 참조하면, 이러한 실시예에서, 입력 모듈(206)은 키패드(601) 및 스타일러스(603)에 연결된다. 출력 모듈(208)은 디스플레이 스크린(605) 및 프린터(607)에 연결된다. WiFi 모듈은 무선 링크를 통해 서버(106)에 연결된 것으로 도시되어 있고, 통신 모듈(212)은 유선 링크를 통해 서버(106)에 연결된 것으로 도시되어 있다. 사용시 아마도 서버(106)에 대한 링크 중 하나만이 이용될 것이라는 것이 이해될 것이다. 제1 무선 통신 모듈(214)은 NFC 안테나에 연결되고, 제2 무선 통신 모듈은 블루투스 안테나(611)에 연결된다. 일부 실시예에서, 안테나는 각각의 무선 통신 모듈과 일체형이다.

[0055] 도 2로 되돌아가면, 처리 모듈(202)은 하나 이상의 프로세서의 형태로 구현되며 하드웨어, 컴퓨터 실행 가능 명령어, 펌웨어, 또는 이들의 조합으로 적절하게 구현될 수 있다. 처리 모듈(202)의 컴퓨터 실행 가능 명령 또는 펌웨어 구현은 서술된 다양한 기능을 수행하기 위해 임의의 적절한 프로그래밍 언어로 작성된 컴퓨터 실행 가능 또는 기계 실행 가능 명령을 포함할 수 있다.

[0056] 일 실시예에서, 메모리 모듈(204)은 하드 디스크 드라이브, eMMC, SSD, 또는 EEPROM과 같은 영구 메모리를 포함한다. 메모리 모듈은 프로세서(202)에 의해 구현되는 데이터 및 실행 가능한 프로그램 명령을 저장하도록 구성될 수 있다. 메모리 모듈(204)은 1차 메모리가 하드 와이어 메모리이고 2차 메모리가 SD 카드와 같은 탈착 가능한 메모리인 1차 및 2차 메모리의 형태로 구현될 수 있다. 메모리 모듈(204)은 프로세서(202) 상에 로드 가능하고 실행 가능한 추가 데이터 및 프로그램 명령뿐만 아니라 이들 프로그램의 실행 동안 생성된 데이터를 저장할 수 있다. 또한, 메모리 모듈(204)은 랜덤 액세스 메모리 및/또는 디스크 드라이브와 같은 휘발성 메모리, 또는 비휘발성 메모리일 수 있다. 메모리 모듈(204)은 컴팩트 플래시 카드, 메모리 스틱, 스마트 미디어, 멀티미디어 카드, 보안 디지털 메모리, 또는 임의의 다른 메모리 저장 장치와 같은 탈착 가능한 메모리를 포함할 수 있다.

[0057] 현재 서술된 실시예에서, 입력 모듈(206)은 다른 입력 장치 중에서 키패드, 터치 스크린, 마우스, 마이크, 및 스타일러스와 같은 입력 장치를 위한 인터페이스를 제공한다. 출력 모듈(208)은 특히 디스플레이 스크린, 스피커, 프린터, 및 햅틱 피드백 장치와 같은 출력 장치를 위한 인터페이스를 제공한다.

[0058] 현재 서술된 실시예에서, 입력 모듈(206) 및 출력 모듈(208)은 또한 결제 단말기(102)와 NFC 지원되는 카드(104a), 서버(106)가 있는 휴대용 통신 장치(104b)로부터 단말기에 의해 도출된 데이터 사이에서 데이터를 교환하는데 사용된다.

[0059] 일 실시예에서, WIFI 모듈은 통신 네트워크(108)를 통해 서버(106)와 통신하기 위해 결제 단말기(102)에 의해 사용된다.

[0060] 일 실시예에서, 통신 모듈(212)은 통신 네트워크(108)를 통해 서버(106)와 통신하기 위해 결제 단말기(102)에

의해 사용된다. 일 실시예에서, 통신 모듈(212)은 GPRS 모듈이다. 다른 실시예에서, 통신을 가능하게 하는 다른 모듈이 사용된다.

[0061] 실시예들에서, 통신 모듈(212)은 모뎀, (이더넷 카드와 같은) 네트워크 인터페이스 카드, 통신 포트, 또는 PC 메모리 카드 국제 협회(Personal Computer Memory Card International Association, PCMCIA) 슬롯을 포함한다. 일 실시예에서, 통신 모듈(212)은 유선 및 무선 프로토콜 모두를 지원하는 장치를 포함한다. 일 실시예에서, 전자 신호 형태의 데이터는 통신 모듈(212)을 통해 전송된다. 다른 실시예들에서, 다른 신호 중에서 하나 이상의 전자기, 광학이 사용된다.

[0062] 일 실시예에서, 결제 단말기는 디지털 키를 사용하여 단말기(102)와 외부 객체(104) 사이에서 교환되는 데이터를 암호화, 암호 해제, 및 인증한다. 이러한 실시예에서의 키는 보안 모듈(213)에 유지된다. 이러한 보안 모듈에는 장치에서 사용되는 모든 키가 있으며, 이러한 보안 모듈은 일회용 기록 전용 장치이다. 키는 보안 환경에서 보안 모듈(213)에 기록된다. 보안 모듈(213)은 키가 모듈로부터 직접 판독될 수 없도록 설계된다. 암호화가 필요한 경우, 데이터는 보안 모듈(213) 내로 펌핑되며, 보안 모듈(213)은 키를 사용한 처리 후에 암호화된 데이터를 반환한다. 보안 모듈(213)로부터 직접 키에 액세스할 수 있는 방법은 없으므로 키의 안전을 보장할 수 있다. 마찬가지로, 데이터를 해독하기 위해, 데이터는 보안 모듈(213) 내로 펌핑되어 해독된 데이터를 반환하기 위한 키를 사용하여 데이터가 처리된다.

[0063] 보안 모듈(213)은 소프트웨어, 펌웨어, 하드웨어, 또는 이들의 조합의 형태로 배치될 수 있다.

[0064] 일 실시예에서, 제1 무선 통신 모듈(214)은 개인 영역 네트워크 모듈(본원에서는, 모듈이라 한다)이다. 현재 서술된 실시예에서, PAN 모듈은 BLUETOOTH 저에너지(BLE) 모듈이다. 다른 실시예들에서, 현재 상황에서 BLE와 유사한 기술이 사용될 수 있다.

[0065] 일 실시예에서, 제2 무선 통신 모듈(216)은 근거리 통신 모듈(본원에서는, NFC 모듈이라 한다)이다. 다른 실시예들에서, 현재 상황에서 NFC와 유사한 기술이 사용될 수 있다.

[0066] 따라서, 결제 단말기(102)는 제2 무선 통신 모듈(216)이 설정될 수 있는 제2 통신 채널 또는 프로토콜(예를 들어, NFC)과 상이한 제1 통신 채널 또는 프로토콜(예를 들어, BLE)을 사용하여 외부 객체(104)와 근접 통신을 설정할 수 있는 제1 무선 통신 모듈(214)을 갖는다는 것에 주의할 수 있다.

[0067] 이제, 도 2 및 도 6과 관련하여 동작하는 결제 단말기의 실시예에 대한 고 레벨의 설명이 제공될 것이다.

[0068] 최초로, 처리 모듈(202)의 프로세서는 휴지 상태에 있고, 이러한 실시예에서 2개의 무선 통신 모듈(214, 216)도 휴지 상태이다. 단말기는 키패드(601)로부터 버스(123)를 통해 처리 모듈(202)의 휴지 프로세스를 중단시키는 입력 모듈(206)로의 입력에 의해 "활성화된다(woken)." 처리 모듈은 메모리 모듈(204)로부터 버스(123)를 통해 명령을 수신하여 버스(123)를 통한 출력을 제1 및 제2 무선 통신 모듈(214, 216)에 제공하기 위해 명령을 처리하며, 제1 및 제2 무선 통신 모듈 각각은 외부 장치(104)를 검색하기 위해 탐색 신호(즉, BLE 및 각각의 NFC 신호)를 보내기 시작한다. 탐색 신호는 각각의 안테나(609, 611)를 통해 전송된다.

[0069] 2개의 탐색 신호 중 하나에 대한 응답이 2개의 안테나(609, 611) 중 하나에 의해 수신될 때, 각각의 무선 통신 모듈은 버스(123)를 통해 처리 모듈(202)을 호출하고, 메모리 모듈(204)에 저장된 명령에 기초하여, 처리 모듈(202)은 다른 각각의 무선 통신 모듈에게 그 질문 신호의 방출을 중단하도록 지시한다. 단순화를 위해, 제1 무선 통신 모듈인 BLE 모듈(214)이 응답을 수신하여 제2 무선 통신 모듈(216)이 휴지 상태로 이동하도록 지시되었다고 가정한다.

[0070] 안테나(609)를 통해 외부 장치(104)로부터 수신된 데이터는 버스(123)를 따라 저장된 디지털 키를 사용하여 처리 모듈(202)의 제어하에 있는 데이터를 해독하는 본원의 다른 부분에서 서술된 보안 모듈(213)로 전달된다. 이는 결제 단말기가 외부 장치(104)(예, 전화 애플리케이션 또는 카드)를 인증할 수 있게 한다. 적절할 경우, 그리고 인증이 수행된 후, 일부 정보는 예를 들어 "입력량," "입력 핀"과 같은 동작을 수행하도록 사용자/판매자에게 지시하기 위한 디스플레이를 위해 스크린(605)으로 전송된다.

[0071] 이러한 명령에 대한 응답은 입력 모듈(206), 예를 들어 키패드(601)에 대한 입력에 의해 수신된다. 이는 처리 모듈(202)에 의해 처리되고, 처리 결과에 따라, 명령 및 응답의 추가 라운드를 용이하게 하기 위해 더 많은 정보가 스크린(605) 상에 디스플레이되거나, 또는 거래 정보가 서버(106)로 전송하기에 충분하다.

[0072] 적절한 때에, 처리 모듈(202)은 WiFi 모듈들(210) 및 통신 모듈(212) 중 하나에 단말기(102)에 의해 수신되고

처리된 데이터에 기초하여 서버(106)와 상호 작용하도록 지시한다.

[0073] 단말기(102)로부터 수신된 데이터에 응답하여, 서버(106)는 WiFi 모듈(210) 및 통신 모듈(212) 중 하나를 통해 데이터를 반환한다. 이러한 데이터는 버스(123)를 통해 처리 모듈(202)에 의해 처리되고, 적절한 경우, 데이터로부터 도출된 정보는 디스플레이 스크린(605) 및/또는 프린터(607) 상의 출력 모듈(208)을 통해 디스플레이된다.

[0074] 거래가 완료되면 처리 모듈은 휴지 상태로 돌아간다.

[0075] 거래를 처리하는 동안, 단말기(102)는 데이터를 외부 장치(104)에 전송할 수 있으며, 이러한 데이터는 일반적으로 보안 모듈(213)에 저장된 키에 의해 암호화된다. 다른 데서 서술된 바와 같이, 외부 장치로 전송된 데이터는 예를 들어 보안 목적을 위한 일회성 코드를 포함할 수 있다.

[0076] 도 3a 내지 3f에서, 결제 단말기(102), 외부 객체(104)(이러한 문서의 판독을 용이하게 하기 위해 외부 객체(104a, 104b)의 형태은 일부 경우 외부 객체(104)로 지칭됨), 및 서버(106)의 일 실시예에 의해 수행되는 작업이 논의된다.

[0077] 단계(302)에서, 결제 단말기(102)는 청구될 금액을 나타내는 입력을 수신한다. 예로서, 판매자는 결제 단말기(102) 내에 또는 위에 제공된 물리적 또는 디지털 키패드를 사용하여 충전될 금액을 나타내는 입력을 수신한다. 예로서, 도 4a를 참조하면, 판매자는 Rs. 350의 금액을 입력했으며, 이는 판매자가 사용자/고객으로부터 받으려고 하는 금액이다.

[0078] 단계(304)에서, 결제 단말기(102)는 외부 객체(104)와의 거래를 개시하기 위한 입력을 수신한다. 예로서, 다시 도 4a를 참조하면, 금액을 입력한 후에, 결제 단말기(102)의 사용자는 리턴 키를 눌러 즉시 입력을 제공한다. 리턴 키를 누르는 것은 이전 단계에서 논의된 금액의 확인 및 현재 단계에서 논의된 입력으로 해석될 수 있다.

[0079] 단계(306)에서, 개시 입력에 응답하여, 결제 단말기(102)(예를 들어, 결제 단말기(102)의 처리 모듈(202))는 제1 무선 통신 모듈(214)(이하, 이러한 문서를 보다 용이하게 판독할 수 있게 하는 BLE 모듈(214)로 지칭된다) 및 제2 무선 통신 모듈(216)(이하, 이러한 문서를 보다 용이하게 판독할 수 있게 하는 NFC 모듈(216)로 지칭된다)이 외부 객체(104)와의 통신을 설정하도록 시도하게 한다. 예로서, 모듈들(214, 216)은 개시 입력에 응답하여 스위치온 될 수 있고, 그 후 통신 채널을 설정하려고 시도할 수 있다. 대안적으로, 두 모듈(214, 216)은 이미 스위치온 되어(그러나 "휴지" 또는 "절전" 모드) 있을 수 있으나, 이러한 경우에서, 외부 객체(104)와의 통신 채널을 개시 및 설정하려고 시도하기 시작한다.

[0080] 단계(308)에서, BLE 모듈(214) 및 NFC 모듈(216) 모두는 통신 채널을 설정하려고 시도한다. 예로서, BLE 모듈(214)의 경우에, BLE 모듈(214)은 그 식별자의 브로드 캐스팅을 시작할 수 있다. 다른 한편으로, NFC 모듈(216)의 경우, NFC 모듈(216)은 전자기장을 생성한다. 판매자는 모듈들(214, 216) 중 어느 것이 사용되어야 하는가를 특정하지 않고, 결제 단말기(102)는 통신 채널의 설정을 시도하기 위해 모듈(214, 216) 모두를 사용하도록 구성되어, 적절한 기간에 인증 후에 적절한 모듈들(214, 216) 중 하나를 통해 통신 채널을 설정한다는 것에 주의할 수 있다.

[0081] 도 3b의 단계(310)를 참조하면, 외부 객체(104)는 외부 객체(104)가 NFC인지 또는 BLE 지원인지를 결정하는 것처럼 보이나, 단계(310)는 설명을 위해서만 제시된다는 것이 분명히 이해된다는 것에 주의할 수 있다. 전술한 바와 같이, 외부 객체(104)는 NFC 지원 카드(104a)(예를 들어, 신용 카드, 직불 카드, 액세스 카드, 기업 카드, 또는 푸드 카드) 또는 BLE 또는 NFC 기능 중 하나 이상을 갖는 휴대용 통신 장치(104b)(예를 들어, 스마트폰)일 수 있다는 것을 이해할 수 있다. 나중에 BLE 가능 휴대용 통신 장치(104b)의 경우의 거래 흐름에 대해 논의할 것이다. 이제, 외부 객체(104)가 NFC 가능 카드(104a) 또는 NFC 가능 휴대용 통신 장치(104b) 인 시나리오를 논의한다. 이들 중 하나가 사용되어야 하는 NFC 및 BLE 성능을 갖는 휴대용 통신 장치(104b)의 경우, 기본 애플리케이션 설정, 애플리케이션의 사용자 정의 설정, 또는 모듈의 가용성에 의해 정의될 수 있다는 것에 주의할 수 있다.

[0082] 단계(312)를 참조하면, 외부 객체(104)는 검출을 위해 결제 단말기(102)에 근접해 있다. 예를 들어, 판매자가 결제를 승인할 준비가 되어 있는 결제 단말기(102)를 구비하면, 사용자/고객은 NFC 카드(104a) 또는 NFC 장치(104b)를 결제 단말기(102)에 (NFC에 필요한 정도로) 근접하게 할 수 있다.

[0083] 설명에 의해서, 일부 실시예들에서, NFC 카드/장치(104a, 104b)는 실시예의 결제 단말기(102) 만이 실시예의 NFC 카드/장치와 정확하게 상호 작용할 수 있도록 암호화된 데이터를 전송한다. 이로 인해 카드/장치가 "잠기는

(locking)" 현상이 발생한다.

[0084] 단계(314)를 참조하면, 결제 단말기(102)는 외부 객체(104)를 인증함으로써 이를 감지하고 잠금 해제를 시도한다. 인증이 성공적으로 수행되면 통신 채널이 설정된다. 즉, 인증이 성공적일 경우에만 거래가 송신될 것이다.

[0085] 따라서, NFC 카드(104a) 또는 NFC 장치(104b)를 검출한 후, 결제 단말기(102)는, 통신 모듈(214, 216) 중 어느 것이 외부 객체(104)와의 통신 채널을 성공적으로 개시했는지에 기초하여, 제1 무선 통신 모듈(214) 및 제2 무선 통신 모듈(216) 중 하나를 사용하여 외부 객체(104)와 통신 채널을 설정했다. 이러한 경우, 결제 단말기(102)는 제2 무선 통신 모듈(216)(NFC 모듈(216))을 사용하여 외부 객체(104)와의 통신 채널을 설정하였다. 따라서, 이와 같이 설정된 통신 채널은 NFC 채널로 지칭될 수 있다.

[0086] 본 실시예에서, BLE 및 NFC 신호 중 하나에 대한 응답이 수신되면, 결제 단말기(102)는 전술한 거래가 완료될 때까지 제1 무선 통신 모듈(214) 및 제2 무선 통신 모듈(216)을 사용하여 임의의 다른 외부 객체와의 통신 채널을 설정하려는 시도를 종료한다.

[0087] 또다른 실시예에서, 통신 채널을 설정하면, 결제 단말기로부터 출력 신호에 대한 응답을 수신할 뿐만 아니라, 데이터 통신이 시작되고, 결제 단말기가 현재의 거래가 완료될 때까지 추가적인 출력으로부터의 통신 모듈에 응답하지 않는 다른 단말기를 종료시킬 수 있도록 외부 장치가 인증된다.

[0088] 설정된 NFC 채널을 사용하여, 결제 단말기(102)는 외부 객체(104)를 잠금 해제하기 위해 외부 객체(104)와 협력한다. 카드/장치 레벨 및 결제 단말기(102)에 배치된 알려진(또는 미래에 개발될 수 있는) 보안 기술이 NFC 카드(104a) 또는 NFC 장치(104b)의 잠금을 해제하는데 사용될 수 있다. 결제 단말기(102)가 잠금 해제에 실패한 경우, 본 실시예에서 거래는 종료된다(거래 종료).

[0089] 단계(316)를 참조하면, 잠금 해제가 성공적이지 않으면, 결제 단말기(102)는 카드 메모리로부터 사용자 토큰을 판독한다. 사용자 토큰은 신용 카드의 카드 번호와 유사한 거래에 연결된 결제를 시도하는 사용자를 식별하는 데이터이다.

[0090] 일 실시예에서, 사용자 토큰을 판독하는 것 외에도, 외부 객체(104)는 일회성 검증기로서 사용되는 데이터를 저장한다. 이러한 실시예에서, 저장된 일회성 검증기는 또한 보안을 개선하기 위해 결제 단말기(102)에 의해 판독된다.

[0091] 일회성 검증기는 시도된 각각의 거래에 대해 고유한 데이터로 이해될 수 있다. NFC 카드(104a)의 경우에, 거래를 처리하기 위해 결제 단말기(102)에 의해 기존의 일회성 검증기가 판독될 때마다 새로운 일회성 검증기가 카드(104a)에 기록 될 수 있다는 것에 더 주의할 수 있다. 일부 스마트폰은 이러한 데이터를 NFC 모듈에 기록하는 것을 허용하지 않을 수 있으며, 이러한 경우 전술한 예에서 구현된 일회성 검증기의 제공이 제공되지 않을 수있다는 것에 더 주의할 수 있다.

[0092] 설명에 의해서, 도 5a를 참조하면, 거래 데이터 패킷(500)은 일반적으로 고객 토큰(501), 고객 식별자(503), 거래 금액(505), 및 판매자 ID(507)를 포함한다. 사용자가 단말기에서 요금을 결제했거나 결제하려고 할 때 해커가 데이터를 스니핑(sniff)할 수 있는 경우, 해커가 동일한 단말기에서 동일한 금액을 여러 번 결제 할 수 있다. 이를 때때로 "재전송 공격(replay attack)" 이라고 한다. 따라서, 합법적인 거래와 재전송 공격을 구분하는 것이 바람직하다.

[0093] 본 실시예에서, "재전송 공격"을 감지할 수 있는 안전 메커니즘이 있다. 재전송 공격에서, 해커는 두 장치 간에 교환되는 데이터를 스니핑하고 동일한 데이터를 여러 번 재전송한다. 시스템이 이러한 공격을 감지하고 플래그를 지정할 수 있도록 하기 위해, 매번 데이터 패킷에 새로운 것을 도입해야 한다. 실시예에서, 도 5b를 참조하면, 이는 a) 각각의 거래 후 카드의 카운터를 유지 및 증가시키고, 및 b) 데이터 패킷의 일부로서 결제 장치에 타임 스탬프를 전송하는 것 중 하나 또는 이들 모두에서 달성된다.

[0094] 따라서, 본 실시예의 패킷(520)은 고객 토큰(501), 고객 식별자(503), 거래 금액(505), 및 가맹점 ID(507) 뿐만 아니라 카드/장치에 저장된 카운터 번호(509) 및 또한 거래의 타임 스탬프(511)를 포함한다.

[0095] 일 실시예에서, 모바일 장치(104b)(또는 BLE를 통해 전송된 데이터)의 NFC 카드(104a) 또는 NFC 모듈로부터 판독된 데이터는 결제 단말기(102)가 수집하는 데이터가 NFC 카드(104a) 또는 모바일 장치(104b)의 NFC 모듈(또는 모바일 장치의 BLE를 통해)로부터 온 것인지를 식별할 수 있게 하는 데이터를 포함한다. 따라서, 결제 단말기(102)(또는 서버(106) 또는 양쪽 모두)는 설정된 통신은 카드(104a)의 근거리 통신 태그 중 하나와의 통신인지, 휴대용 통신 장치(104b)의 근거리 통신 모듈인지, 또는 휴대용 통신 장치(104b)의 개인 영역 네트워크 모듈

(214)인지를 식별할 수 있다는 것에 주의할 수 있다. 이러한 제공은 서버(106)가 거래를 처리하는 데 필요한 데이터 세트를 설정할 수 있게 한다. 예로서, 모바일 장치(104b)로부터의 NFC 모듈의 경우, (앞서 설명한 제약 조건으로 인해) 거래를 처리하는 데 일회성 검증기가 필요하지 않을 수도 있는 반면에, NFC 카드(104a)의 경우, 일회성 검증기가 필요하다.

[0096] 일 실시예에서, NFC 카드/장치(104a, 104b)로부터 판독되거나 BLE를 통해 수신된 데이터는 위치 검증 데이터를 포함한다. 즉, 결제 단말기(102)는 외부 객체(104)로부터 위치 검증 데이터를 수신한다. 위치 검증 데이터는 결제 단말기(102)를 사용하여 결제가 수락될 수 있는지를 검증하는데 사용된다.

[0097] 일 실시예에서, 데이터는 외부 객체(104)(예를 들어, 카드(104a))에 기록되고, 단말기는 단말기가 해당 장소에 있는 경우를 제외하고 해당 코드가 있는 카드를 거부하도록 설정되어 있다. 회사 매점과 같은 완전 폐쇄 그룹의 결제 환경에서, 결제 장치는 한 회사에서만 결제를 수락할 것으로 예상되며, 수표는 결제 장치 레벨 자체에서 로컬로 결제된다. 장치가 특정 식별자(회사 식별자)로 채워진 고객 카드를 찾지 못하면 즉시 거래가 거부된다. 서버 호출이 필요하지 않다.

[0098] 결제를 수락할 수 없다고 판단되면 거래가 거부된다. 반면에, 결제가 승인 될 수 있음을 확인하면 거래가 처리된다. 논의되는 검증은 결제 단말기(102)에 의해 수행될 수 있다.

[0099] 대안적으로, 검증은 서버(106) 또는 양쪽 모두에 의해 수행될 수 있다.

[0100] 다른 경우에, 결제 장치가 일반 소매점에 있는 경우, 점검은 서버(106)에서 일어난다. 고객 식별자는 서버로 전송되는 데이터 패킷의 일부이기도 하다. 백엔드에는 특정 고객 식별자가 있는 고객이 특정 위치에서 결제하는 것을 금지하는 규칙이 설정되어 있다(예를 들어, 리콜될 판매자 ID 507로 식별되면 거래 데이터 패킷의 일부이기도 하다).

[0101] 구현 예로서, 회사는 캠퍼스에 배치된 푸드 코트 내에서 사용하기 위해 직원에게 NFC 카드(104a)를 발급했을 수 있다. 카드(104a)가 캠퍼스 외부의 결제 단말기(102)에서 결제하기 위해 사용되는 경우, 결제 단말기(102)(또는 서버(106))는 위치 확인 데이터를 판독하면 거래를 거절할 수 있다.

[0102] 이제, 단계(318)를 참조하면, 결제 단말기(102)는 새로운 일회성 검증기를 외부 객체(104)에 기록한다. 예로서, 새로운 일회성 검증기는 NFC 카드(104a)에 기록된다. 모바일 장치(104b)의 NFC 모듈이 그러한 기록을 허용하는 경우, NFC 지원 모바일 장치(104b)의 경우에도, 새로운 일회성 검증기는 실시 예에서 모바일 장치(104b)의 NFC 모듈에 기록된다. 새로운 일회성 검증기는 다음 거래에 사용된다. 새로운 일회성 검증기는 기존의 일회성 검증기와 비교하여 구성 당 증분/감소일 수 있다. 대안적으로, 일회성 검증기는 랜덤하게 생성된 코드일 수 있으며, 이는 알려진 로직에 기초할 수 있다. 일 실시예에서, 새로운 일회성 검증기는 결제 단말기(102)에 의해 생성된다. 단계(320)에서, (이러한 조항이 제공되는 경우). 새로운 일회성 검증기는 모바일 장치(104b)의 NFC 카드(104a) 또는 NFC 모듈에 기록된다

[0103] 일회성 검증기는 각 거래에 대해 외부 객체(104)로부터 수집된 데이터에 신선도를 추가한다는 것에 주의해야 한다. 예로서, 또한 일정한 (일반적으로 수행되는 바와 같이) 사용자 토큰만 수집해야 하는 경우, 사용자 토큰에 액세스할 수 있는 악성 시스템은 사용자 토큰을 오용하여 거래를 수행할 수 있다.

[0104] 단계(322)를 참조하면, 결제 단말기(102)는 사용자 토큰, 일회성 검증기(있는 경우), 가맹점 ID, 단말기 ID, 결제 단말기(102)의 일회성 검증기, 사용자 데이터 및 거래 정보를 얻는 데 사용되는 소스(NFC 카드/모바일 또는 BLE)를 번들링한다. 일 실시예에서, 결제 단말기(102)는 또한 새로운 일회성 검증기를 번들링할 수 있다. 외부 객체(104)에 대응하는 일회성 검증기와는 별도로, 결제 단말기(102)에 대한 일회성 검증기가 있을 수도 있다는 것에 주의해야 한다. 따라서, 잘못 사용될 경우, 결제 단말기(102)에 관한 정보(예를 들어, 가맹점 ID 또는 단말기 ID)를 갖는 로그(rogue) 시스템에 여전히 저항(resistance)이 표시될 수 있다. 일 실시예에서, 사용자는 거래를 승인하기 위해 결제 단말기(102)로의 통신 뿐만 아니라 PIN을 통신해야 할 수 있다. 일부 실시예에서, PIN은 특정한 미리 설정된 금액을 초과하는 거래에만 요구될 수 있다.

[0105] 또한, 결제 단말기(102)는 인증 및 보안 데이터를 다른 데이터와 함께 번들하여 보안 기능을 향상시킬 수 있다.

[0106] 단계(324)를 참조하면, 결제 단말기(102)는 번들 정보를 서버(106)에 전송한다. 결제 단말기(102)는 정보를 서버(106)에 전송하기 위해 WIFI 모듈(2)을 사용할 수 있다. 대안적으로, 결제 단말기(102)는 GPRS 모듈을 사용하여 정보를 서버(106)에 전송할 수 있다. 대안적으로, 결제 단말기는 서버(106)와 통신하기 전에 보안 목적으로 보안 모듈(213)을 사용하여 번들 정보를 암호화할 수 있다.

[0107] 단계(326)를 참조하면, 서버(106)는 결제 단말기(102)로부터 번들 정보를 수신한다.

[0108] 단계(328)를 참조하면, 서버(106)는 거래를 처리한다. 종래가 아닌 단계에서 주의를 끌지 않도록 거래 처리와 관련된 종래의 단계는 논의되지 않는다. 외부 객체(104)의 일회성 검증기 및 결제 단말기(102)의 일회성 검증기는 결제 요청이 거절되어야 하는지 또는 추가로 처리되어야 하는지 여부를 결정하는데 사용된다. 일회성 검증기(결제 단말기(102)에 대응)는 현재의 거래가 거래를 거부하거나 거래를 진행하기 위해 결제 단말기(102)로부터 일회성 검증기가 예상되는 것인지 검증하는데 사용된다. 이와 같이, 일회성 검증기는 일회성 검증기가 현재 거래가 거래를 거부하거나 거래를 진행하기 위해 외부 객체(104)로부터 예상되는 것인지 여부를 검증하는데 사용된다.

[0109] 일 실시예에서, 결제 단말기(102)는 외부 객체(104)에 대응하는 새로운 일회성 검증기를 서버(106)로 전달할 수 있어서, 서버(106)는 다음 거래에서 외부 엔티티(104)로부터 무엇을 예상할 수 있는 것인지를 알 수 있다.

[0110] 일 실시예에서, 외부 객체(104) 또는 결제 단말기(102)의 새로운 일회성 검증기는 이전의 일회성 검증기와 비교하여 알려진 변경이다. 따라서, 서버(106)는 거래를 거절하거나 진행하기 위해 이전 검증기와 일회성 검증기를 검증하면 된다.

[0111] 일 실시예에서, 서버(106)는 다음 거래에서 사용하기 위해 결제 단말기(102)용의 새로운 일회성 검증기를 전송한다.

[0112] 외부 객체(104)로부터 일회성 검증기가 없는 경우, 예상했던 경우, 또는 잘못된 일회성 검증기의 경우, 이와 같이, 서버(106)는 결제 단말기(102)에 대해 문제가 해결될 때까지 외부 객체(104)가 거래를 수행하는 것을 차단할 수 있다.

[0113] 단계(330)를 참조하면, 서버(106)는 거래 정보를 결제 단말기(102)에 전송한다. 거래 정보는 성공적인 결제 또는 결제 거부에 대응하는 정보를 포함할 수 있다. 거래 정보는 또한 다른 정보 중에서 판매자의 계좌에 입금된 금액에 대응하는 정보 및/또는 결제한 사용자/고객에 대한 선택된 정보를 포함할 수 있다.

[0114] 단계(332)를 참조하면, 결제 단말기(102)는 서버(106)로부터 거래 정보를 수신한다. 수신된 정보 중 일부는 결제 단말기(102)에 의해 출력(예를 들어, 디스플레이)될 수 있다. 일부 실시예에서, 거래 정보 중 일부는 결제 단말기(102)에 의해 출력되는 것이 방지될 수 있지만, 이러한 정보는 외부 장치(104)(예를 들어, 전화기)에 출력될 수 있다.

[0115] 단계(334)를 참조하면, 거래가 완료되면, 결제 단말기(102)는 다음 거래(예를 들어, 02에서 시작)를 위해 준비될 수 있다

[0116] 블록(310)을 참조하면, 회수될 수 있듯이, 사용자/고객이 NFC 카드(104a) 또는 NFC 지원 스마트폰(104b)을 사용하여 결제할 수 있다는 것을 고려하여 서술되었다. 이제 사용자가 결제를 하기 위해 BLE 성능을 갖는 휴대용 통신 장치(104b)(예를 들어, 스마트폰)를 사용하는 시나리오를 참조한다.

[0117] BLE가 본 발명에 필수적인 것은 아니며, 다른 프로토콜, 예를 들어 "정상적인" Bluetooth 또는 WiFi도 작동할 수 있음을 이해해야 한다.

[0118] 또한, 도 3 시리즈의 다른 도면과 함께 도 3e를 참조할 수 있다. 전술한 바와 같이, 단계(308)를 참조하면, 결제 단말기의 NFC 모듈(216) 및 BLE 모듈(214) 모두는 통신 채널을 설정하려고 시도할 수 있다. 전술한 바와 같이, BLE 모듈(214)의 경우에, BLE 모듈(214)은 그 식별자의 브로드 캐스팅을 시작할 수 있다. 식별자는 호환성을 식별하는 데이터를 포함할 수 있다.

[0119] 예로서, 또한 도 3e 및 4b를 참조하면, 사용자는 휴대용 통신 장치(104b)에서 결제 애플리케이션을 열고 "지금 결제" 아이콘을 활성화시킨다. 애플리케이션은 BLE 지원 스마트폰(104b)의 BLE 모듈이 결제 단말기(102)를 검색하도록 한다(도 4c 참조).

[0120] 복수의 결제 단말기가 있는 실시예에서, 결제 단말기는 전형적으로 동일한 강도로 신호를 방사하지만, 물론 2개의 단말기가 임의의 특정 휴대용 통신 장치(스마트폰)로부터 등거리에 있을 가능성은 거의 없다. 연결 준비(페어)를 나타내는 신호의 방사는 당 업계에서 때때로 "광고"로 지칭되고 전형적으로 데이터 패킷을 방출하는 것으로 구성된다. "페어(pair)"라는 용어는 제한적이지 않다.

[0121] 휴대용 통신 장치(스마트폰)에서 수신된 신호 강도는 스마트폰에 의해, 예를 들어 스마트폰에서 실행되는 애플리케이션에 의해 측정되고, 근처에서 이용 가능한 각각의 결제 단말기에 대한 스마트폰의 위치를 결정하는데 사

용된다.

[0122] 페어링의 제1 단계로서, 단계(30)에서, 도 3e에서, 애플리케이션은 주변을 스캔하고 연결할 수 있는 '적격 후보' 목록을 생성한다. 애플리케이션은 휴대용 통신 장치(스마트폰)가 의도된 결제 단말기와만 페어링되도록 구성된다. 예를 들어, 판매자는 고객에게 애플리케이션을 열고 전화기를 결제 단말기-A에 가까이 가져와 결제를 시작하도록 요청한다. 이후에, 애플리케이션이 대신하여 (적절한 모든 결제 단말기 중에서) 가장 가까운 결제 단말기를 결정한다. 판매자가 고객에게 휴대 전화를 결제 단말기-A에 가까이 가져 오라고 요청했기 때문에, 애플리케이션은 다른 단말기가 몇 미터 떨어져 있는 반면에 결제 단말기-A가 단지 몇 인치 떨어져 있다는 것을 알 것이며, 따라서 단말기-A와 페어링을 요청할 것이다.

[0123] 신호 강도 로직(가장 가까운 가용성 있는 결제 단말기와의 연결을 설정한다)은 연결 설정에만 사용된다.

[0124] 전화기가 결제 단말기와 페어링되어 연결이 설정되면, 애플리케이션에서 연결을 끊기로 결정할 때까지 연결은 활성 상태로 유지된다. 전화기가 단말기에서 철수되고 애플리케이션이 단말기와 계속 통신하여 거래가 완료되더라도 연결은 활성 상태로 유지된다. 애플리케이션이 거래가 완료된 것을 결정하면, 애플리케이션은 연결을 끊고 단말기를 해제한다.

[0125] 단말기는 2대의 전화기와 동시에 페어링될 수 없도록 구성되어 있다. 전화기가 페어링되거나 단말기에 연결되면, 전화기와 단말기 간의 통신 채널은 독점적이다. 즉, 다른 전화기는 단말기와 페어링되거나 통신할 수 없다. 단말기는 해당 전화기에 대해 효과적으로 잠겨 있으며 애플리케이션 또는 결제 단말기를 물리적으로 재설정해야만 잠금이 해제될(전화기와의 연결이 끊어질) 수 있다.

[0126] 일 실시예에서, 이러한 "잠금"은 페어링이 이루어질 때 광고를 중지하도록 구성되는 단말기에 의해 수행된다. 하나의 예에서, 스마트폰의 애플리케이션은 광고를 중지하라는 지시를 단말기에 발행한다. 또다른 예에서, 단말기는 페어링이 발생하자마자 스마트폰으로부터 입력 없이 광고를 중단하도록 구성된다.

[0127] 결제 단말기의 프로세서는 이러한 명령을 수신하고, 저장된 명령에 응답하여 명령을 처리하며, 프로세서의 성능 및 페어링의 존재에 대한 광고를 일시적으로 비활성화시킨다.

[0128] 일 실시예에서, 스마트폰(104b)의 애플리케이션은 식별자에 존재하는 호환성을 식별하는 데이터를 참조함으로써 호환 결제 단말기(102)를 찾는다. 예를 들어. 광고하는 BLE 또는 BLUETOOTH 장치가 여러 개 있을 수 있으나, 애플리케이션은 결제를 위해 고려될 수있는 결제 단말기(102)를 식별하는 데에만 관심이 있다(따라서 요청을 페어링으로 보내기 위해 고려된다).

[0129] 신호 강도가 제1 임계값 이상이 되도록 사용자가 휴대용 통신 장치를 결제 단말기에 근접하게 이동시켰으며, 도 3e에 도시된 바와 같이, 단계(31)에서, 스마트폰(104b)은 그 결제 단말기(102)에 페어링 요청을 보낸다.

[0130] 일 실시예에서, 결제 단말기(102)로부터의 신호 강도가 제1 임계값을 초과하는 경우, 페어링 요청이 단지 전송된다.

[0131] 또다른 실시예에서, 사용자가 "지금 결제" 아이콘을 활성화하거나 스마트폰이 거래를 시작하도록 지시하자마자 페어링 요청이 전송된다.

[0132] 추가적인 실시예에서, 애플리케이션은 예를 들어 디스플레이 스크린 상에 페어링이 가능한 하나 이상의 단말기의 표시를 표시하고, 사용자는 이들 중 하나를 선택하여, 시퀀스를 페어링하는 요청이 개시되게 하는 선택을 한다.

[0133] 예로써, 다수의 호환 결제 단말기(102)를 가진 판매자 위치를 고려한다. 스마트폰(104b)의 애플리케이션은 이들 결제 단말기(102)를 모두 식별하고 후보를 식별할 수 있으나, 이들 중 어느 하나에 페어링 요청이 전송되어야 하는지를 결정해야 한다.

[0134] 일 실시예에서, 단일 결제 단말기(102)가 식별되는 시나리오에서도, 신호 강도가 제1 임계값을 초과하지 않으면 페어링 요청이 전송되지 않는다. 실제로, BLE를 채널로 사용하여 결제하는 경우에도 사용자 환경은 "탭앤 페이(tap-and-pay)"와 유사하다. 사용자는 스마트폰(104b)을 결제 단말기(102)에 가까이 가져가서(도 4d 참조) 신호 강도를 증가시켜, 애플리케이션이 결제 단말기(102)와의 페어링을 요청하게 한다. 따라서, 브로드 캐스팅된 식별자의 신호 강도가 제1 임계값을 초과하는 경우, 스마트폰(104b)은 결제 단말기(102)의 개인 영역 네트워크 모듈(214)과 통신 채널을 설정하기 위한 요청을 자동으로 전송한다는 것을 이해해야 한다.

[0135] 제1 임계값은 휴대용 통신 장치(104a)와 결제 단말기(102)가 통신 채널을 설정하기 위해 서로 미리 구성된 거리

내에 있도록 구성된다. 제1 임계값은 소프트웨어 업데이트를 통해 원격으로 재구성되거나 결제 단말기(102)에서 구성될 수 있다.

[0136] 일 실시예에서, 제1 임계값은 휴대용 통신 장치(104b)와 결제 단말기(102)가 통신 채널을 설정하기 위해 서로 대략 20cm 내에 있도록 구성된다.

[0137] 또다른 실시예에서, 제1 임계값은 휴대용 통신 장치(104b)와 결제 단말기(102)가 통신 채널을 설정하기 위해 서로 대략 10 cm 내에 있도록 구성된다.

[0138] 제1 임계값의 구성으로, 휴대용 통신 장치(104b)와 결제 단말기(102) 간의 대략적인 거리를 설정하여 페어링이 진행될 수 있음을 이해해야 한다.

[0139] 도 3e에서, 단계(32)에서, 결제 단말기(102)는 페어링 요청을 수신한다. 요청을 수신한 결제 단말기(102)는 잘 알려진 프로토콜을 사용하여 스마트폰(104b)과 협력하여 요청을 성공적으로 페어링 또는 거절한다. 페어링이 성공적일 경우, 결제 단말기(102)는 제1 무선 통신 모듈(214)(BLE 모듈(214))을 사용하여 외부 객체(104)와의 통신 채널(BLE 채널)을 설정했다.

[0140] 통신 채널이 설정(페어링)되면, 스마트폰(104b)과 결제 단말기(102)의 개인 영역 네트워크 모듈(214) 사이의 신호 강도가 제1 임계값 아래로 떨어지는 경우, 스마트폰은 결제 단말기(102)의 개인 영역 네트워크 모듈과의 통신을 계속 유지한다. 실제로, 사용자는 스마트폰(104b)을 결제 단말기(102)에 가까이 가져와 스마트 폰(104b)이 결제 단말기(102)와 페어링되게 한다. 그 후에, 사용자는 스마트폰(104b)을 철회할 수 있지만, 통신 채널은 유지되어 사용자의 경험을 개선하고 거래 처리가 보다 신뢰성 있게 된다.

[0141] 일 실시예에서, 스마트폰(104b)과 결제 단말기(102)의 개인 영역 네트워크 모듈(214) 사이의 채널에서의 신호 강도가 제2 임계값 아래로 떨어지면, 결제 단말기(102) 또는 스마트폰(104b) 중 적어도 하나는 설정된 통신 채널을 종료하도록 구성된다. 제2 임계값은 제어 가능할 수 있다. 제2 임계값은 원격으로 또는 장치에서 재구성될 수 있다.

[0142] 도 3e에서, 단계(33)에서, 결제 단말기(102)는 거래 정보를 스마트폰(104b)으로 전송한다. 정보는 BLE 채널을 통해 전송된다. 이러한 정보는 무엇보다도 양도 될 금액 및 판매자 정보를 포함할 수 있다.

[0143] 도 3e에서, 단계(34) 및 도 4d 및 4e에서, 스마트폰(104b)은 결제 단말기(102)에 의해 전송된 거래 정보를 수신한다.

[0144] 도 3e에서, 단계(35) 및 도 4e에서, 사용자는 아이콘을 활성화함으로써, 스마트폰(104b)이 결제 승인을 전송하고 거래를 용이하게 하기 위해 데이터를 통신하게 할 수 있다. (NFC와 관련하여 논의된 관련 데이터에 더하여) 통신되는 데이터는 실시간 데이터를 포함할 수 있다. 실시간 데이터는 시간에 대응하는 데이터를 포함 할 수 있다. 일회성 검증기는 스마트폰(104b)에 의해 생성될 수 있다. 일 실시예에서, 사용자는 거래를 승인하기 위해 PIN을 전달해야 할 수도 있다. 일부 실시예에서, PIN은 사전 구성된 특정 금액을 초과하는 거래에만 필요할 수 있다.

[0145] 도 3f에서, 단계(36)에서, 결제 단말기(102)는 승인 및 데이터를 수신하고, 이러한 거래 모드에 적용될 수 있는 바와 같이, 단계(322)와 관련하여 앞서 논의 된 단계들 및 후속 단계들이 수행될 수 있다.

[0146] 이제 구체적으로 단계 332(도 3d), 37 및 38(도 3f)을 참조하면, 결제 단말기(102)는 서버(106)로부터 거래 정보를 수신한다. 이전에 논의된 바와 같이, 수신 된 데이터에 기초하여 서버(106)는 데이터가 BLE 채널을 통해 결제 단말기(102)에 의해 수신되었다는 것을 알고 있다. 따라서, BLE 채널은 거래에 대응하는 업데이트를 사용자에게 제공하는데 사용될 수 있다. 따라서, 서버(106)에 의해 전송된 전형적인 데이터와는 별개로, 스마트폰(104b)을 사용하여 결제하는 사용자의 계좌 잔고에 대응하는 데이터를 서버(106)는 송신하고 결제 단말기(102)는 수신한다. 결제 단말기(102)는 BLE 채널을 통해 계좌 잔고에 대응하는 데이터를 스마트폰(104b)에 전달한다(도 4g 참조). 따라서, 사용자는 인터넷을 사용하지 않고 결제할 수 있을 뿐만 아니라 인터넷을 사용하지 않고도 거래에 대한 업데이트를 받을 수 있다.

[0147] 단계(38)를 완료하면, 스마트폰(104)에서 실행되는 애플리케이션은 결제 단말기(102)가 있는 통신 채널을 통해 명령을 전송한다. 이러한 명령은 다른 스마트폰과의 추가 거래가 가능하도록 단말기가 광고를 시작하도록 지시한다. 명령은 결제 단말기에 의해 수신되고, 단말기의 메모리에 저장된 명령에 따라 결제 단말기의 처리 회로에 의해 처리되어 광고가 재개된다.

[0148] 일 실시예에서, 단말기(102)에는 또한 물리적 재설정 장치, 예를 들어 재설정 키가 제공되어 판매자는 필요할 경우 광고를 재활성화할 수 있다. 또다른 실시예에서, 재설정은 원격으로 수행될 수 있지만, 경우에 따라 물리적인 재설정 장치를 사용하는 것보다 덜 안전할 수 있다.

[0149] 재설정 키는 작동될 때 결제 단말기가 광고를 시작할 수 있는 대기 상태로 재부팅되게 하거나, 단순히 "광고 중지" 명령을 무시하고 "광고 재개" 명령을 처리 회로로 전송할 수 있다.

[0150] 일 실시예에서, 결제 단말기(102)는 서버(106)로부터 거래 정보에 대응하는 데이터를 수신하고, 거래 정보에 대응하는 데이터의 적어도 일부를 통신 채널을 통해 스마트폰(104b)에 통신하도록 추가로 구성된다.

[0151] 일 실시예에서, 결제 단말기(102)는 사용자의 계좌 잔고를 표시할 수 없다. 그러나, 휴대용 통신 장치(104b)는 거래를 게시한 사용자의 계좌 잔고를 표시하도록 구성된다. 계좌 잔액에 대응하는 데이터는 사용자의 스마트폰(104b) 만이 전술한 데이터를 해독할 수 있도록 암호화될 수 있다.

[0152] 실시예들의 측면들을 불필요하게 모호하게 하지 않기 위해, 상이한 단계들에서 전형적으로 사용되는 암호화, 복호화, 인증, 및 보안 기술들 중 일부는 논의되지 않음에 주의해야 한다.

[0153] 전술 한 공정은 일련의 단계로서 기술되며, 이는 단지 예시를 위해 수행된 것이다. 따라서, 일부 단계가 추가될 수 있거나, 일부 단계가 생략될 수 있거나, 단계의 순서가 재배열되거나, 일부 단계가 동시에 수행될 수 있는 것으로 고려된다.

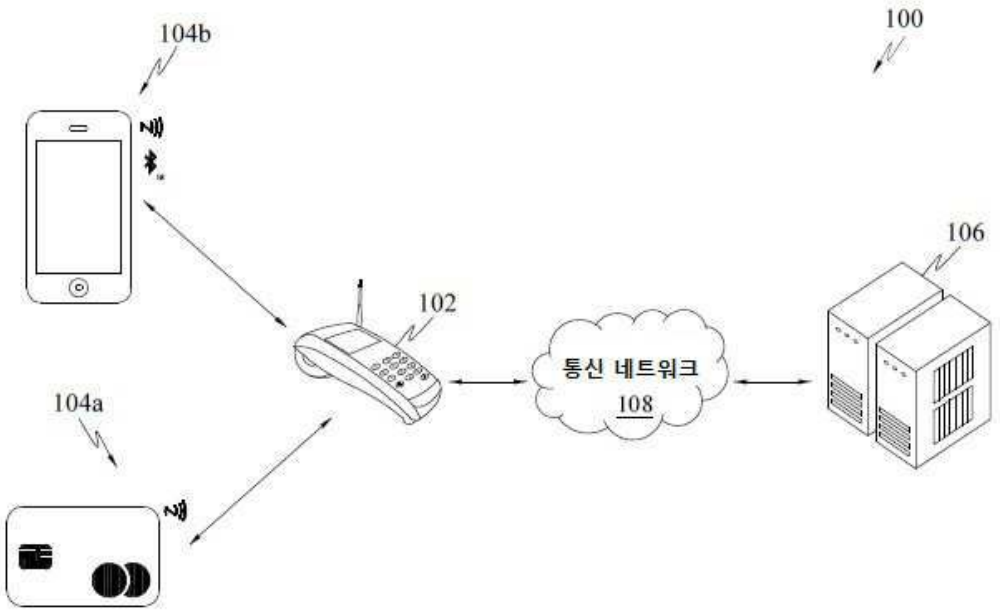
[0154] 본원에 서술된 예시적인 실시예들은 컴퓨터, 하드웨어, 또는 소프트웨어와 하드웨어의 조합으로 설치된 소프트웨어를 포함하는 운영 환경에서 구현될 수 있다.

[0155] 실시예가 특정 예시적인 실시예를 참조하여 서술되었지만, 본원에 서술된 시스템 및 방법의 더 넓은 사상 및 범위를 벗어나지 않고 이들 실시예에 대한 다양한 수정 및 변경이 이루어질 수 있음이 명백할 것이다. 따라서, 명세서 및 도면은 제한적인 의미가 아니라 예시적인 것으로 간주되어야 한다.

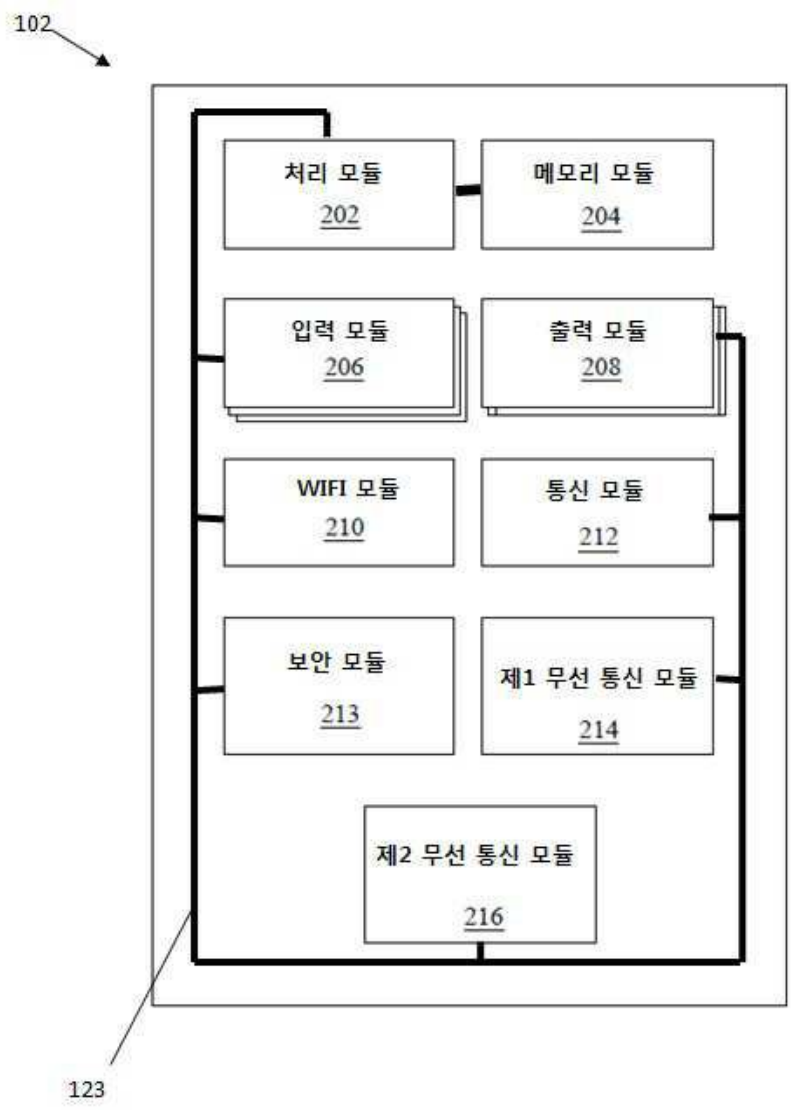
[0156] 본 발명은 단지 예로서 서술되었다는 것이 이해될 것이다. 첨부된 청구 범위의 사상 및 범위를 벗어나지 않으면서 본원에 서술된 기술에 대해 다양한 변형이 이루어질 수 있다. 개시된 기술은 독립형 방식으로 또는 서로 조합하여 제공될 수 있는 기술을 포함한다. 따라서, 하나의 기술과 관련하여 서술된 특징은 다른 기술과 조합하여 제시될 수도 있다.

도면

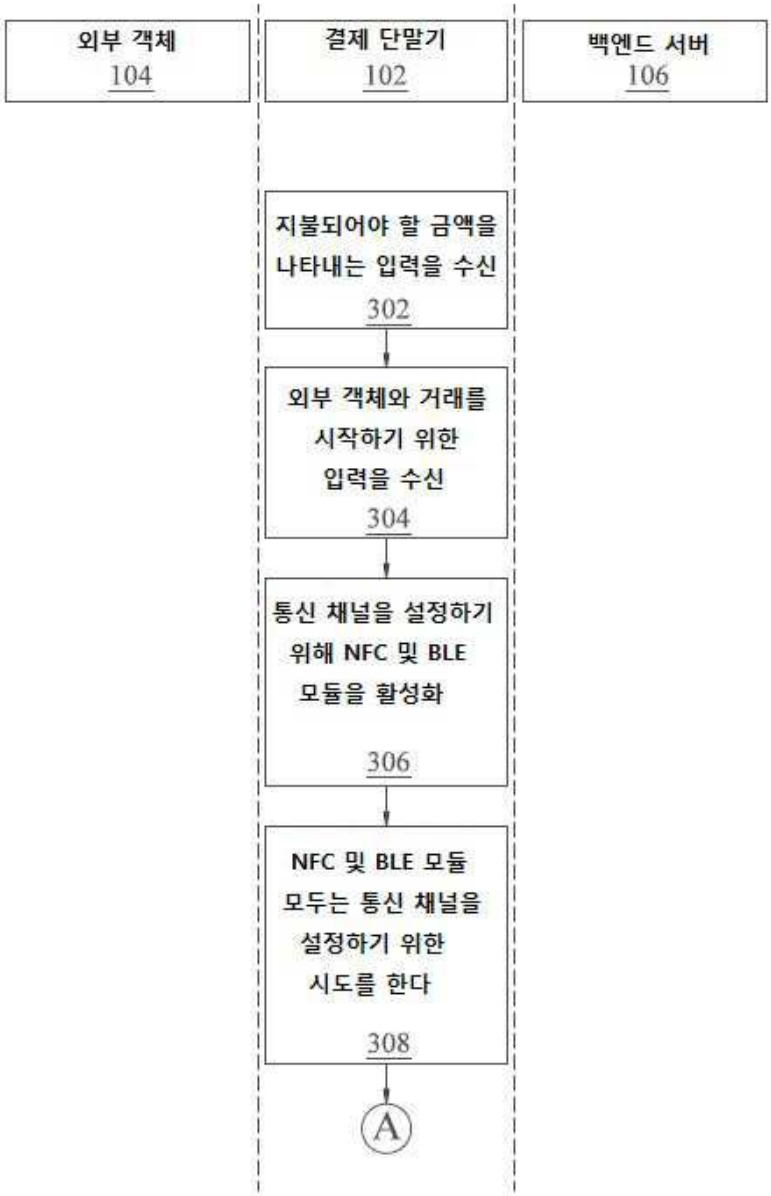
도면1



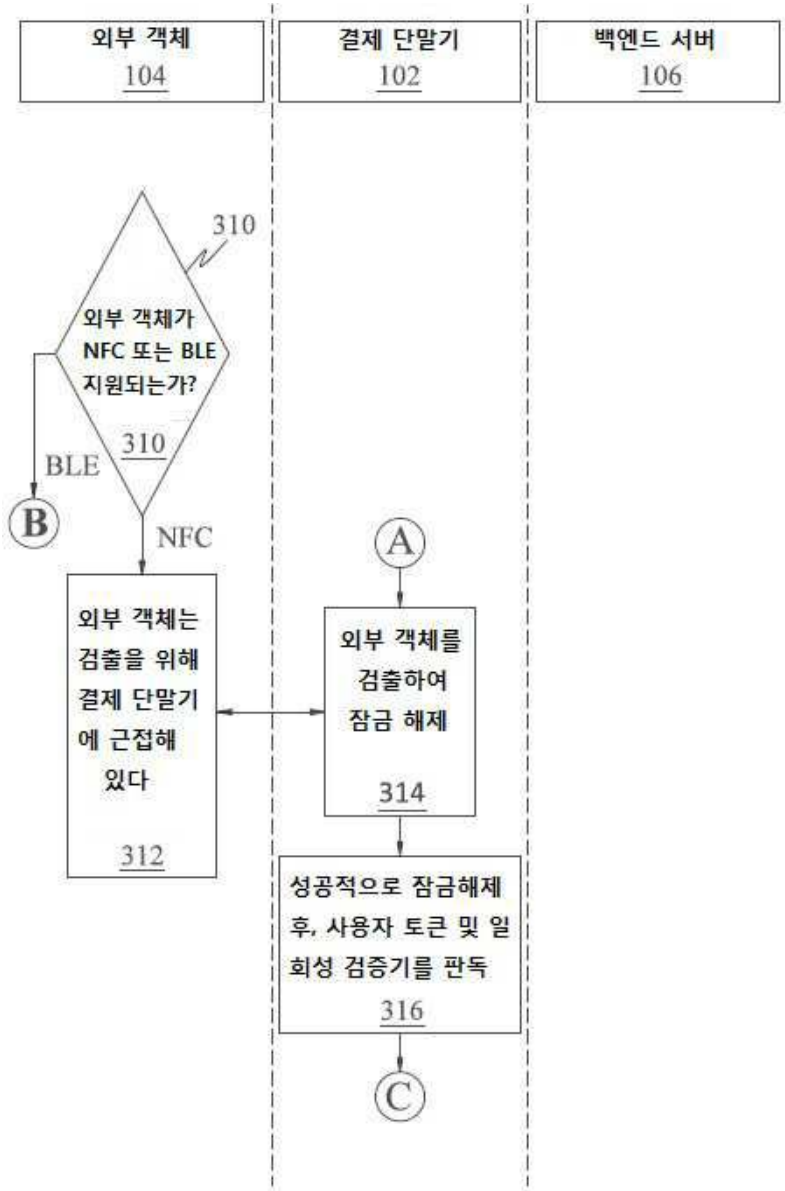
도면2


102
처리 모듈
202
메모리 모듈
204
입력 모듈
206
출력 모듈
208
WIFI 모듈
210
통신 모듈
212
보안 모듈
213
제1 무선 통신 모듈
214
제2 무선 통신 모듈
216
123

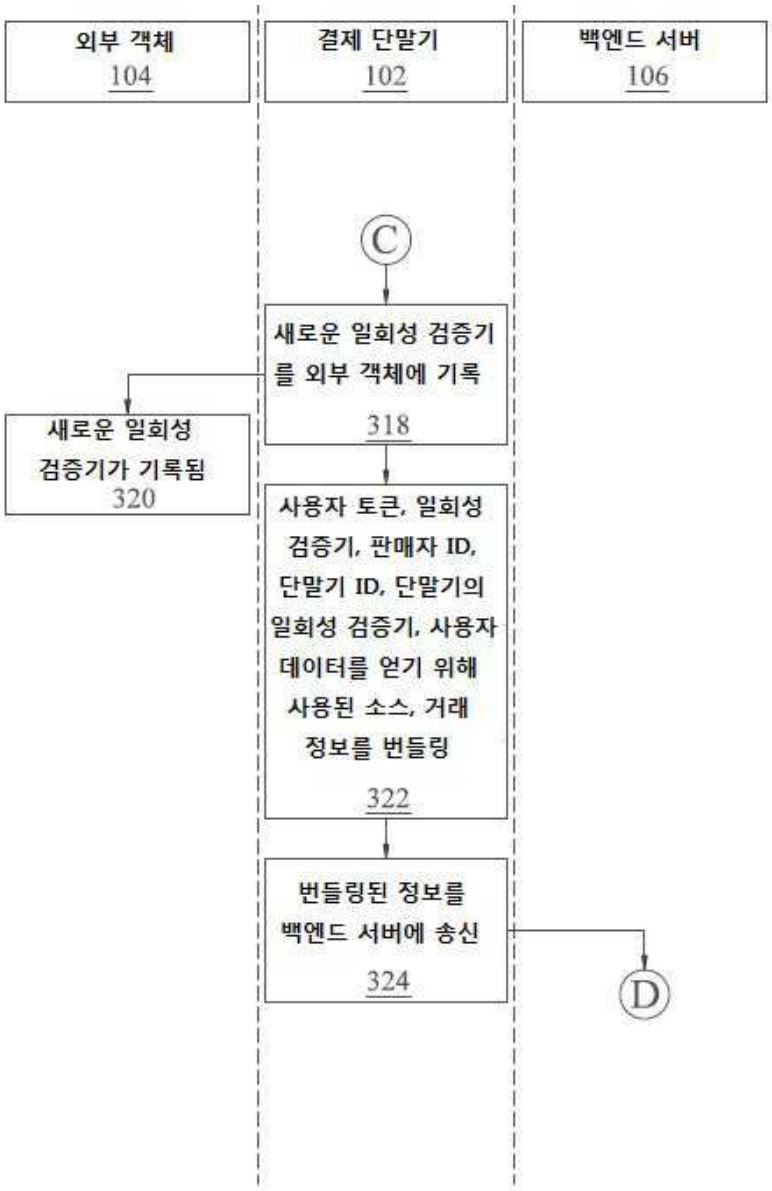
도면3a


외부 객체
104
결제 단말기
102
백엔드 서버
106
지불되어야 할 금액을 나타내는 입력을 수신
302
외부 객체와 거래를 시작하기 위한 입력을 수신
304
통신 채널을 설정하기 위해 NFC 및 BLE 모듈을 활성화
306
NFC 및 BLE 모듈 모두는 통신 채널을 설정하기 위한 시도를 한다
308
A

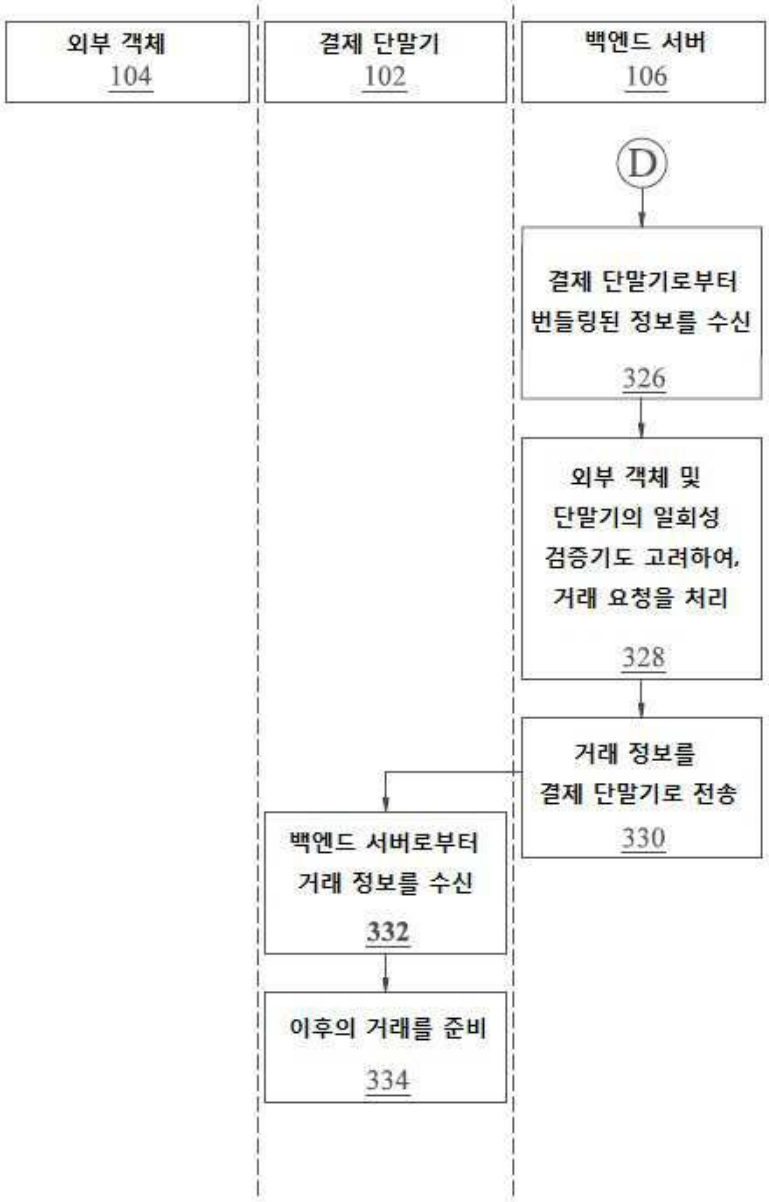
도면3b


외부 객체
104
결제 단말기
102
백엔드 서버
106
310
외부 객체가 NFC 또는 BLE 지원되는가?
310
BLE
NFC
B
A
외부 객체는 검출을 위해 결제 단말기에 근접해 있다
312
외부 객체를 검출하여 잠금 해제
314
성공적으로 잠금해제 후, 사용자 토큰 및 일회성 검증기를 판독
316
C

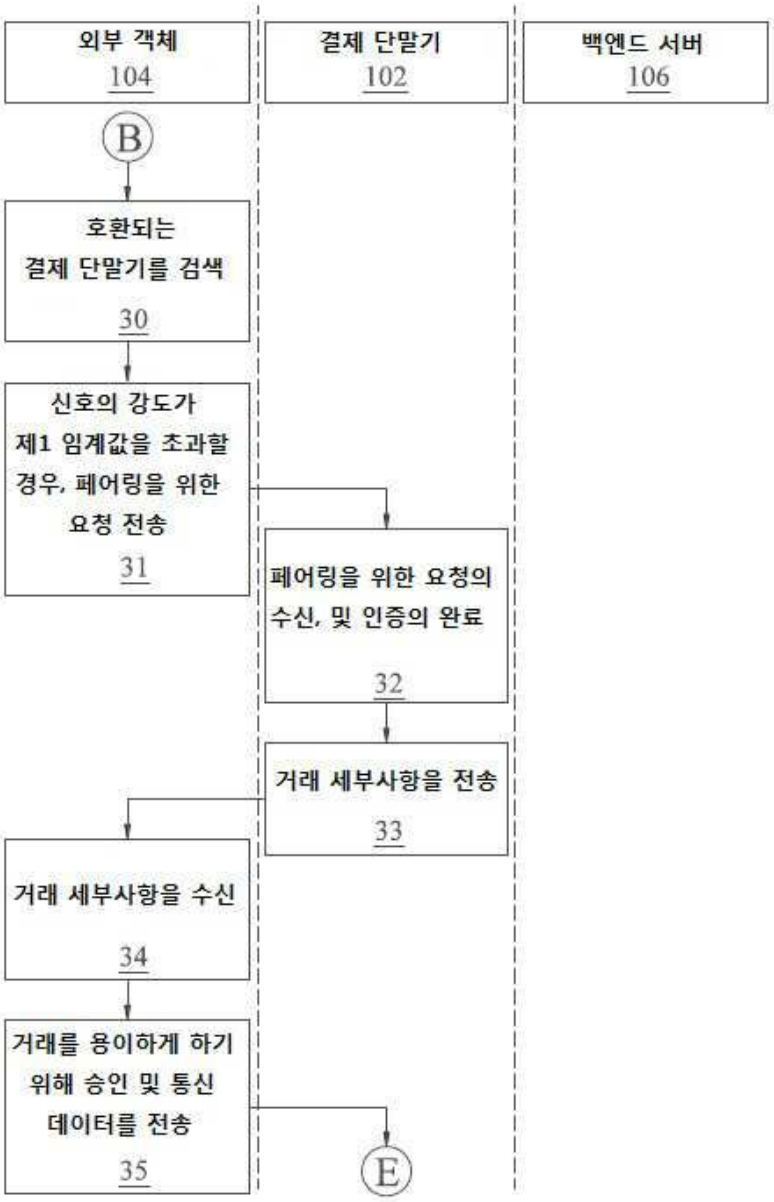
도면3c


외부 객체
104
결제 단말기
102
백엔드 서버
106
C
새로운 일회성 검증기를 외부 객체에 기록
318
새로운 일회성 검증기가 기록됨
320
사용자 토큰, 일회성 검증기, 판매자 ID, 단말기 ID, 단말기의 일회성 검증기, 사용자 데이터를 얻기 위해 사용된 소스, 거래 정보를 번들링
322
번들링된 정보를 백엔드 서버에 송신
324
D

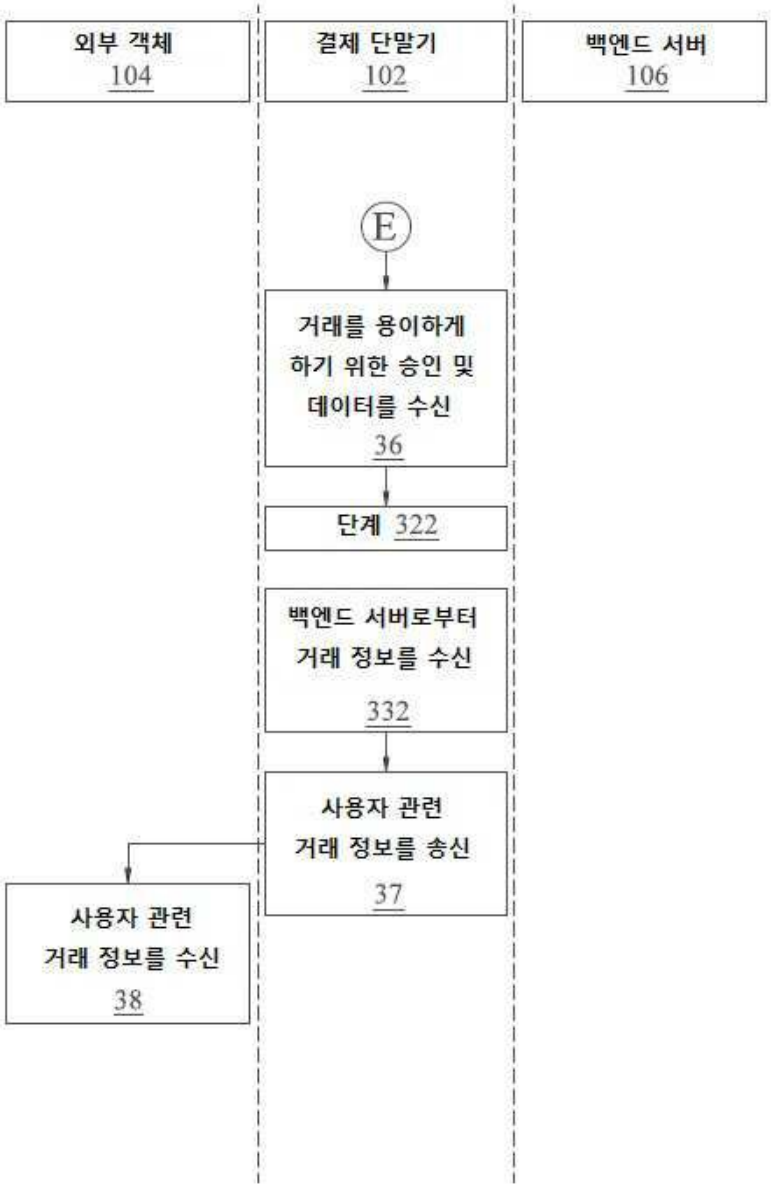
도면3d


외부 객체
104
결제 단말기
102
백엔드 서버
106
D
결제 단말기로부터
번들링된 정보를 수신
326
외부 객체 및
단말기의 일회성
검증기도 고려하여,
거래 요청을 처리
328
거래 정보를
결제 단말기로 전송
330
백엔드 서버로부터
거래 정보를 수신
332
이후의 거래를 준비
334

도면3e


외부 객체
104
결제 단말기
102
백엔드 서버
106
B
호환되는
결제 단말기를 검색
30
신호의 강도가
제1 임계값을 초과할
경우, 페어링을 위한
요청 전송
31
페어링을 위한 요청의
수신, 및 인증의 완료
32
거래 세부사항을 전송
33
거래 세부사항을 수신
34
거래를 용이하게 하기
위해 승인 및 통신
데이터를 전송
35
E

도면3f

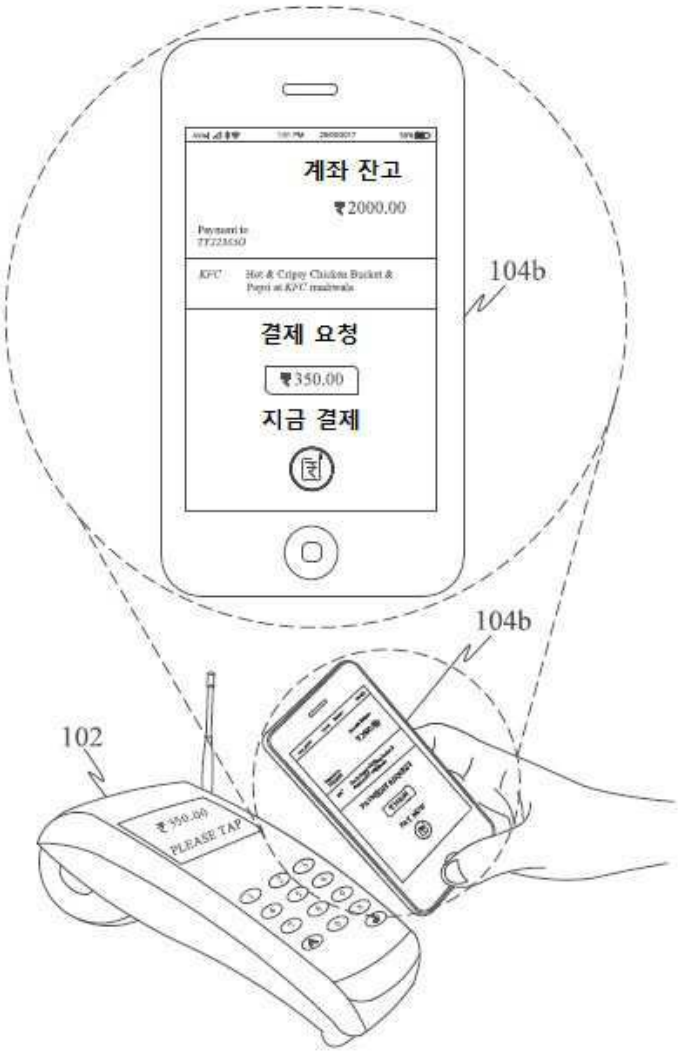

외부 객체
104
결제 단말기
102
백엔드 서버
106
E
거래를 용이하게 하기 위한 승인 및 데이터를 수신
36
단계 322
백엔드 서버로부터 거래 정보를 수신
332
사용자 관련 거래 정보를 송신
37
사용자 관련 거래 정보를 수신
38

도면4a

도면4b

도면4c

도면4d



도면4e

도면4f


계좌 잔고
₹2000.00
Payment to
KFC
Hot & Crispy Chicken Bucket & Pepsi at KFC madiwala
₹350.00
결제가 진행중...
결제가 진행중입니다...
기다려 주시기 바랍니다...
104b

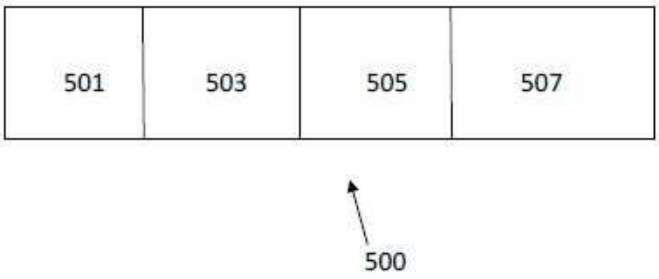
Processing...
102

도면4g

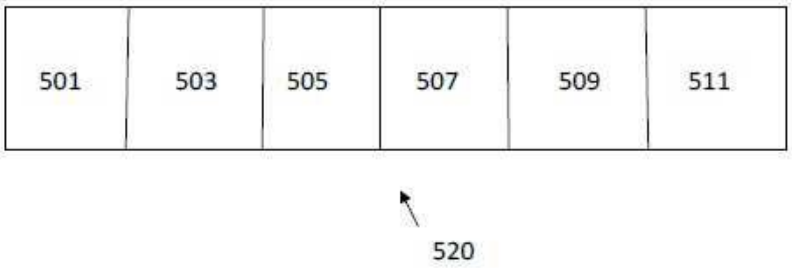

Payment to
KFC
Hot & Crispy Chicken Bucket & Pepsi at KFC madiwala
결제 완료
104b
계좌 잔고
₹1650.00
완료


PAYMENT RECEIVED
102

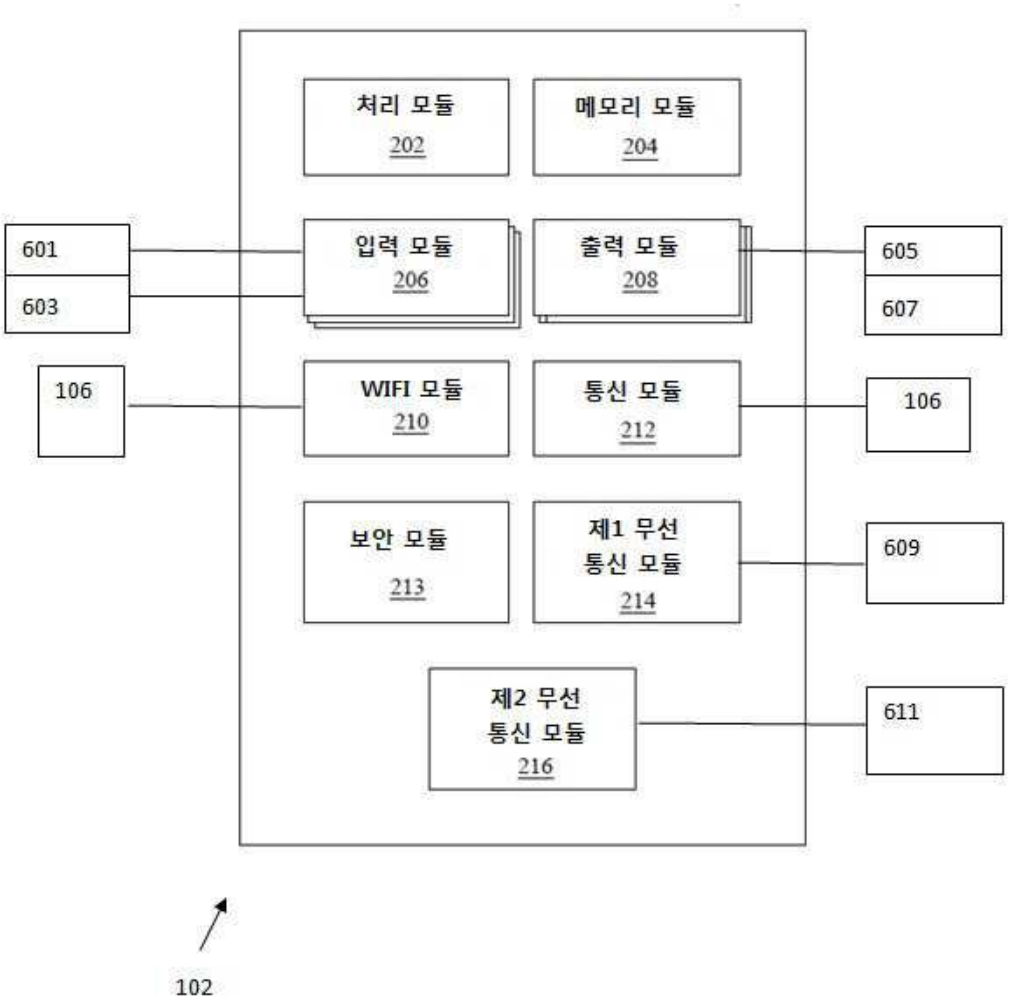
도면5a


501
503
505
507
500

도면5b


501
503
505
507
509
511
520

도면6


처리 모듈
202
메모리 모듈
204
601
603
입력 모듈
206
출력 모듈
208
605
607
106
WIFI 모듈
210
통신 모듈
212
106
보안 모듈
213
제1 무선
통신 모듈
214
609
제2 무선
통신 모듈
216
611
102