(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년06월17일
(11) 등록번호 10-2411007
(24) 등록일자 2022년06월15일

(51) 국제특허분류(Int. Cl.)
G06Q 20/08 (2012.01) *G06Q 20/24* (2012.01)
G06Q 20/32 (2012.01)
(52) CPC특허분류
G06Q 20/08 (2013.01)
G06Q 20/24 (2013.01)
(21) 출원번호 10-2018-7024475
(22) 출원일자(국제) 2017년01월16일
심사청구일자 2020년01월10일
(85) 번역문제출일자 2018년08월24일
(65) 공개번호 10-2018-0108713
(43) 공개일자 2018년10월04일
(86) 국제출원번호 PCT/CN2017/071251
(87) 국제공개번호 WO 2017/128975
국제공개일자 2017년08월03일
(30) 우선권주장
201610049675.4 2016년01월25일 중국(CN)
(56) 선행기술조사문헌
KR100845281 B1*
KR1020010025193 A*
KR1020040084346 A*
WO2015148850 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
어드밴스드 뉴 테크놀로지스 씨오., 엘티디.
케이만 군도, 그랜드 케이만 케이와이1-9008, 조지 타운, 27 하스피탈 로드, 케이만 코포레이트 센터
(72) 발명자
첸 싱
중국 항저우 310099 완탕 로드 넘버 18 후앙롱 타임즈 플라자 빌딩 비 17층 앤츠 패턴트 팀 내
왕 레이
중국 항저우 310099 완탕 로드 넘버 18 후앙롱 타임즈 플라자 빌딩 비 17층 앤츠 패턴트 팀 내
란 지에
중국 항저우 310099 완탕 로드 넘버 18 후앙롱 타임즈 플라자 빌딩 비 17층 앤츠 패턴트 팀 내
(74) 대리인
김태홍, 김진희

전체 청구항 수 : 총 11 항 심사관 : 이재근

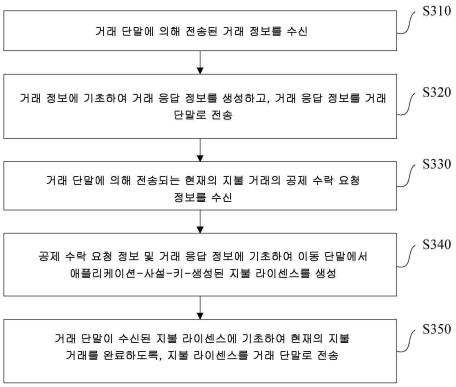
(54) 발명의 명칭 **이동 단말 P2P에 기초한 신용 지불 방법 및 장치**

(57) 요 약

본 개시내용은 이동 단말 P2P에 기초한 신용 지불 방법 및 장치에 대한 것이다. 방법은 거래 단말에 의해 전송된 거래 정보를 수신하는 단계; 거래 정보에 기초해 거래 응답 정보를 생성하고, 거래 응답 정보를 거래 단말로 전송하는 단계; 현재의 지불 거래에 대한, 거래 단말에 의해 전송된 금액 공제 수락 요청 정보를 수신하는 단계;

(뒷면에 계속)

대 표 도 - 도10



금액 공제 수락 요청 정보 및 거래 응답 정보에 따라, 이동 단말에서 애플리케이션 사설 키 생성 지불 라이센스를 생성하는 단계; 지불 라이센스를 거래 단말로 전송하는 단계를 포함한다. 지불 애플리케이션을 인에이블(enable)한 후에, 지불 거래가 신속하게 그리고 안전하게 완료될 수 있도록, 사용자는 이동 단말을 이용함으로써 거래 단말과의 오프라인 신용 지불을 완료할 수 있다.

(52) CPC특허분류
G06Q 20/322 (2013.01)

명 세 서

청구범위

청구항 1

신용 지불을 프로세싱하기 위한 방법에 있어서,

이동 단말에 의해, 거래 단말에 의해 전송된 거래 정보를 수신하는 단계(S310);

상기 이동 단말에 의해, 상기 거래 정보에 기초하여 거래 응답 정보를 생성하는 단계;

상기 이동 단말에 의해, 상기 거래 응답 정보를 상기 거래 단말로 전송하는 단계(S320);

상기 거래 응답 정보를 상기 거래 단말로 전송하는 단계에 응답하여, 상기 이동 단말에 의해, 상기 거래 단말에 의해 전송된 애플리케이션 공개 키 증명서 반환 요청 정보(application public key certificate return request information)를 수신하는 단계(S360);

상기 이동 단말에 의해, 상기 애플리케이션 공개 키 증명서 반환 요청 정보에 기초하여 상기 이동 단말 내의 애플리케이션 공개 키 증명서에 대한 애플리케이션 공개 키 증명서 응답 정보를 생성하고, 상기 이동 단말에 의해, 상기 애플리케이션 공개 키 증명서 응답 정보를 상기 거래 단말로 전송하는 단계(S370);

상기 이동 단말에 의해, 상기 거래 단말에 의해 전송되는 현재의 지불 거래의 공제 수락 요청 정보를 수신하는 단계(S330);

상기 이동 단말에 의해, 상기 공제 수락 요청 정보 및 상기 거래 응답 정보에 기초하여, 이동 단말에서, 애플리케이션 사설 키로 생성되는 지불 인가 라이센스(payment authorization license)를 생성하는 단계(S340); 및

상기 이동 단말에 의해, 상기 거래 단말이 수신된 상기 지불 인가 라이센스에 기초하여 상기 현재의 지불 거래를 완료하도록 상기 지불 인가 라이센스를 상기 거래 단말로 전송하는 단계(S350)

를 포함하고,

상기 이동 단말에서, 상기 애플리케이션 사설 키로 생성되는 지불 인가 라이센스를 생성하는 단계는,

상기 이동 단말에 의해, 상기 이동 단말에 저장된 애플리케이션 사설 키(application private key)를 이용함으로써 상기 공제 수락 요청 정보에 기초하여 서명 데이터를 생성하는 단계(S361);

상기 이동 단말에 의해, 상기 이동 단말에서 사전 생성된 거래 인증 코드(transaction authentication code; TAC) 서브-키(sub-key)를 이용함으로써 상기 공제 수락 요청 정보 및 상기 거래 응답 정보에 기초하여 거래 인증 코드(TAC)를 생성하는 단계(S362); 및

상기 이동 단말에 의해, 상기 서명 데이터 및 상기 TAC를 상기 지불 인가 라이센스로서 이용하는 단계(S363)

를 포함하는 것인, 신용 지불을 프로세싱하기 위한 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 방법은 공공 교통을 위한 지불에 적용되고,

상기 거래 응답 정보는 지불 카드 번호, 이용가능한 한도, 및 진입/진출 플래그(entry/exit flag)를 포함하는 것인, 신용 지불을 프로세싱하기 위한 방법.

청구항 5

제1항에 있어서,

상기 공제 수락 요청 정보는 공제량, 상기 현재의 지불 거래의 날짜, 상기 현재의 지불 거래의 시간, 상기 현재의 지불 거래의 진입/진출 플래그, 및 상기 현재의 지불 거래의 스테이션 정보(station information)를 포함하는 것인, 신용 지불을 프로세싱하기 위한 방법.

청구항 6

제5항에 있어서,

상기 이동 단말에 의해, 현재의 이용가능한 한도를 획득하기 위하여, 현재의 공제 수락 요청 정보 내의 상기 공제량에 기초하여 상기 거래 응답 정보 내의 이용가능한 한도로부터 상기 공제량을 감산하는 단계(S380); 및

상기 이동 단말에 의해, 상기 현재의 이용가능한 한도를, 상기 이동 단말에 대응하는 사용자의 이용가능한 한도로서 이용하는 단계(S390)

를 더 포함하는, 신용 지불을 프로세싱하기 위한 방법.

청구항 7

신용 지불을 프로세싱하기 위한 방법에 있어서,

거래 단말에 의해, 거래 정보를 이동 단말로 전송하는 단계(S410);

상기 거래 단말에 의해, 상기 이동 단말에 의해 전송된 거래 응답 정보를 수신하는 단계(S420);

상기 거래 단말에 의해, 애플리케이션 공개 키 증명서 반환 요청 정보를 상기 이동 단말로 전송하는 단계(S460);

상기 거래 단말에 의해, 상기 이동 단말에 의해 전송된 애플리케이션 공개 키 증명서 응답 정보를 수신하는 단계(S470);

상기 거래 단말에 의해, 상기 거래 단말 상에서 신용 인가 공개 키를 이용함으로써 상기 애플리케이션 공개 키 증명서 응답 정보 내의 애플리케이션 공개 키 증명서 상의 서명을 검증하는 단계(S480);

애플리케이션 공개 키가 검증 동안에 상기 애플리케이션 공개 키 증명서로부터 복원된다고 결정하는 것에 응답하여, 상기 거래 단말에 의해, 상기 거래 응답 정보에 기초하여 현재의 지불 거래의 공제 수락 요청 정보를 생성하는 단계(S430);

상기 거래 단말에 의해, 상기 공제 수락 요청 정보를 상기 이동 단말로 전송하는 단계(S440); 및

지불 인가 라이센스를 수신하는 것에 응답하여, 상기 거래 단말에 의해, 상기 지불 인가 라이센스에 기초하여, 상기 현재의 지불 거래가 완료된 것으로 결정하는 단계(S450)

를 포함하고,

상기 지불 인가 라이센스는 서명 데이터 및 거래 인증 코드(TAC)를 포함하고, 상기 지불 인가 라이센스에 기초하여, 상기 현재의 지불 거래가 완료될 수 있는 것으로 결정하는 것은,

상기 거래 단말에 의해, 상기 애플리케이션 공개 키를 이용함으로써 상기 서명 데이터를 검증하는 단계(S481);

상기 거래 단말에 의해, 상기 서명 데이터가 검증될 때에 거래 로그를 생성하는 단계(S482); 및

미리 결정된 서버가 상기 거래 로그 - 상기 거래 로그는 공제량, 거래 날짜, 거래 순간, 거래 단말 ID, 지불 카드 번호, 이용가능한 한도, 및 상기 TAC를 포함함 - 에 기초하여, 상기 이동 단말에 대응하는 사용자 계좌로부터 대응하는 양의 자금을 공제하도록, 상기 거래 단말에 의해, 상기 거래 로그를 상기 미리 결정된 서버로 전송하는 단계(S483)

를 포함하는 것인, 신용 지불을 프로세싱하기 위한 방법.

청구항 8

삭제

청구항 9

제7항에 있어서,

상기 방법은 공공 교통 지불에 적용되고,

상기 거래 응답 정보는 지불 카드 번호, 이용가능한 한도, 및 진입/진출 플래그를 포함하는 것인, 신용 지불을 프로세싱하기 위한 방법.

청구항 10

제9항에 있어서,

상기 방법은,

상기 거래 단말에 의해, 상기 거래 응답 정보 내의 지불 카드 번호가 미리 결정된 블랙리스트 내에 포함되어 있는지 여부를 결정하는 단계(S401); 및

상기 거래 응답 정보 내의 상기 지불 카드 번호가 상기 미리 결정된 블랙리스트 내에 포함되어 있지 않을 때, 상기 거래 단말에 의해, 애플리케이션 공개 키 증명서 반환 요청 정보를 상기 이동 단말로 전송하는 상기 단계를 수행하는 단계

를 더 포함하는 것인, 신용 지불을 프로세싱하기 위한 방법.

청구항 11

제9항에 있어서,

상기 거래 단말에 의해, 상기 거래 응답 정보 내의 상기 이용가능한 한도가 미리 결정된 임계치 이상인지 여부를 결정하는 단계(S402);

상기 이용가능한 한도가 상기 미리 결정된 임계치 이상일 경우, 상기 거래 단말에 의해, 상기 거래 응답 정보 내의 상기 진입/진출 플래그가 진출된 상태인지 여부를 검사하는 단계(S403); 및

상기 진입/진출 플래그가 진출된 상태일 경우, 상기 거래 단말에 의해, 애플리케이션 공개 키 증명서 반환 요청 정보를 상기 이동 단말로 전송하는 상기 단계를 수행하는 단계(S460)

를 더 포함하는, 신용 지불을 프로세싱하기 위한 방법.

청구항 12

삭제

청구항 13

제7항에 있어서,

상기 거래 단말에 의해, 상기 이동 단말에 대응하는 사용자 아이덴티티 정보를 획득하는 단계(S105)를 더 포함하고, 상기 사용자 아이덴티티는 ID 카드 번호, 이름, 은행 카드 번호, 및 전자메일 주소 중 적어도 하나를 포함하는 것인, 신용 지불을 프로세싱하기 위한 방법.

청구항 14

제1항에 있어서,

상기 거래 단말은 피어 투 피어(peer to peer) 데이터 송신을 사용해 상기 이동 단말과 통신하는 것인, 신용 지불을 프로세싱하기 위한 방법.

청구항 15

제1항 또는 제7항의 방법을 수행하도록 구성되는 복수의 모듈들을 포함하는, 이동 단말에 적용되는 신용 지불을

프로세싱하기 위한 장치.

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

발명의 설명

기 술 분 야

[0001] 본 개시내용은 통신 기술들의 분야에 관한 것으로, 특히, 이동 단말 P2P에 기초한 신용 지불 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 현재, 공공 교통은 지상 교통 및 지하철을 주로 포함한다. 사용자들이 공공 교통 티켓들을 구입할 때, 그들은 현금 또는 선불 카드들을 통상적으로 이용한다. 현금 지불은 공공 교통 시스템을 위하여 주로 이용되고, 사용자는 동전들을 삽입함으로써 티켓을 구매할 수 있다. 사용자들은 대안적으로 선불(pre-paid) 메트로 카드(metro card)들을 얻을 수 있고, 카드를 스캔(scan)하므로써 버스 또는 지하철을 탈 수 있다.

[0003] 사용자가 버스 티켓을 현금을 구입할 때, 많은 버스들은 셀프-서빙(self-serving)하고 있고 교환을 제공하지 않으므로, 사용자는 정확한 양의 요금들을 미리 준비해야 할 필요가 있고, 이것은 사용자가 불편할 수 있다. 또한, 업무의 종료 후에, 버스 시스템 직원은 셀프-서비스 버스 사용자들에 의해 넣어지는 모든 작은 요금들을 계수(count)할 필요가 있어서, 여분의 작업을 직원에게 야기시킨다. 사용자가 공공 교통을 타기 위하여 메트로 카드를 이용할 때, 대부분의 현재의 버스 카드들은 비-접촉(non-contact) 라디오 주파수(radio-frequency; RF) 카드들이므로, 카드를 구부리는 것, 또는 카드의 표면의 긁힘과 같은 사용자-야기된 손상들 및 마모들이 그 통상적인 이용 동안에 메트로 카드에 대해 용이하게 행해진다. 사용자가 공공 교통을 타기 위하여 단일-탑승(single-ride) 카드를 이용할 때, 사용자는 통상적으로 작은 요금들로 단일-탑승 카드들을 구매하고, 직원들은 또한, 작은 요금들을 계수할 필요가 있다.

[0004] 사용자가 공공 교통을 타기 위하여 재이용가능한 선불 카드를 이용할 때, 선불 카드는 미등록되어 있고 그 분실은 보고될 수 없으므로, 재이용가능한 선불 버스 카드가 분실된 후에는, 사용자에게 손실이 야기될 수 있다. 사용자가 또한, 특정된 위치들에서 선불 카드를 구입하고, 충전하고, 환불할 필요가 있고, 이것은 사용자를 불편하게 한다.

발명의 내용

[0005] 관련된 기술들에서의 문제를 극복하기 위하여, 본 개시내용은 이동 단말 P2P에 기초한 신용 지불 방법 및 장치를 제공한다.

[0006] 본 개시내용의 구현예들의 제 1 양태에 따르면, 이동 단말 P2P에 기초한 신용 지불 방법이 제공되고, 이동 단말에 적용되고, 방법은 거래 단말(transaction terminal)에 의해 전송된 거래 정보를 수신하는 단계; 거래 정보에 기초하여 거래 응답 정보를 생성하고, 거래 응답 정보를 거래 단말로 전송하는 단계; 거래 단말에 의해 전송되는 현재의 지불 거래의 공제 수락 요청 정보를 수신하는 단계; 공제 수락 요청 정보 및 거래 응답 정보에 기초하여 이동 단말에서 애플리케이션-사설-키-생성된 지불 라이센스(application-private-key-generated payment license)를 생성하는 단계; 및 거래 단말이 수신된 지불 라이센스(payment license)에 기초하여 현재의 지불 거래를 완료하도록, 지불 라이센스를 거래 단말로 전송하는 단계를 포함한다.

[0007] 거래 정보를 거래 단말로 전송한 후에, 거래 응답 정보는 거래 정보에 대응하고, 방법은 거래 단말에 의해 전송된 애플리케이션 공개 키 증명서 반환 요청 정보(application public key certificate return request information)를 수신하는 단계; 및 애플리케이션 공개 키 증명서 반환 요청 정보에 기초하여 이동 단말에서 애플리케이션 공개 키 증명서에 대한 애플리케이션 공개 키 증명서 응답 정보를 생성하고, 애플리케이션 공개 키 증명서 응답 정보를 거래 단말로 전송하는 단계를 더 포함한다.

[0008] 또한, 이동 단말에서 애플리케이션-사설-키-생성된 지불 라이센스를 생성하는 단계는 이동 단말에서 저장된 애플리케이션 사설 키를 이용함으로써 공제 수락 요청 정보에 기초하여 서명 데이터(signature data)를 생성하는 단계; 이동 단말에서 사전-생성된 TAC 서브-키(sub-key)를 이용함으로써 공제 수락 요청 정보 및 거래 응답 정보에 기초하여 거래 인증 코드(transaction authentication code; TAC)를 생성하는 단계; 및 서명 데이터 및 TAC를 지불 라이센스로서 이용하는 단계를 포함한다.

[0009] 또한, 지불 방법은 공공 교통 지불에 적용되고; 거래 응답 정보는 지불 카드 번호, 이용가능한 한도, 및 진입/진출 플래그(entry/exit flag)를 포함한다.

[0010] 또한, 공제 수락 요청 정보는 공제량, 현재의 지불 거래의 날짜, 현재의 지불 거래의 시간, 현재의 지불 거래의 진입/진출 플래그, 및 현재의 지불 거래의 스테이션 정보(station information)를 포함한다.

[0011] 또한, 방법은 현재의 이용가능한 한도를 획득하기 위하여, 공제 수락 요청 정보에서의 공제량에 기초하여 거래 응답 정보에서의 이용가능한 한도로부터 공제량을 감산하는 단계; 및 현재의 이용가능한 한도를, 이동 단말에 대응하는 사용자의 이용가능한 한도로서 이용하는 단계를 포함한다.

[0012] 본 개시내용의 구현예들의 제 2 양태에 따르면, 이동 단말 P2P에 기초한 신용 지불 방법이 제공되고, 방법은 거래 정보를 이동 단말로 전송하는 단계; 이동 단말에 의해 전송된 거래 응답 정보를 수신하는 단계; 거래 응답 정보에 기초하여 현재의 지불 거래의 공제 수락 요청 정보를 생성하는 단계; 공제 수락 요청 정보를 이동 단말로 전송하는 단계; 및 지불 라이센스를 수신할 때, 지불 라이센스에 기초하여, 현재의 지불 거래가 완료될 수 있는 것으로 결정하는 단계를 포함한다.

[0013] 이동 단말에 의해 전송된 거래 응답 정보를 수신한 후에, 방법은 애플리케이션 공개 키 증명서 반환 요청 정보를 이동 단말로 전송하는 단계; 이동 단말에 의해 전송된 애플리케이션 공개 키 증명서 응답 정보를 수신하는 단계; 거래 단말에서 신용-라이센싱된 공개 키(credit-licensed public key)를 이용함으로써 애플리케이션 공개 키 증명서 응답 정보에서의 애플리케이션 공개 키 증명서 상의 서명을 검증하는 단계; 및 애플리케이션 공개 키가 서명 검증 프로세스 동안에 애플리케이션 공개 키 증명서로부터 복원될 때, 현재의 지불 거래의 공제 수락 요청 정보를 생성하는 단계를 수행하는 단계를 더 포함한다.

[0014] 또한, 지불 방법은 공공 교통 지불에 적용되고; 거래 응답 정보는 지불 카드 번호, 이용가능한 한도, 진입/진출 플래그, 및 최후 거래에 대한 정보를 포함한다.

[0015] 또한, 방법은 거래 응답 정보에서의 지불 카드 번호가 미리 결정된 블랙리스트 내에 포함되는지 여부를 결정하

는 단계; 및 거래 응답 정보에서의 지불 카드 번호가 미리 결정된 블랙리스트 내에 포함되지 않을 때, 애플리케이션 공개 키 증명서 반환 요청 정보를 이동 단말로 전송하는 단계를 수행하는 단계를 포함한다.

[0016] 또한, 방법은 거래 응답 정보에서의 이용가능한 한도가 미리 결정된 임계치 이상인지 여부를 결정하는 단계; 이용가능한 한도가 미리 결정된 임계치 이상일 경우, 거래 응답 정보에서의 진입/진출 플래그가 진출된 상태인지 여부를 검사(check)하는 단계; 및 진입/진출 플래그가 진출된 상태일 때, 애플리케이션 공개 키 증명서 반환 요청 정보를 이동 단말로 전송하는 단계를 수행하는 단계를 포함한다.

[0017] 또한, 지불 라이센스는 서명 데이터 및 거래 인증 코드(TAC)를 포함하고, 지불 라이센스에 기초하여, 현재의 지불 거래가 완료될 수 있는 것으로 결정하는 단계는, 애플리케이션 공개 키를 이용함으로써 서명 데이터를 검증하는 단계; 서명 데이터가 검증될 때, 거래 로그를 생성하는 단계; 및 미리 결정된 서버가 거래 로그 - 거래 로그는 공제량, 거래 날짜, 거래 순간, 거래 단말 ID, 지불 카드 번호, 이용가능한 한도, 및 TAC를 포함함 - 에 기초하여, 이동 단말에 대응하는 사용자 계좌로부터 자금의 대응하는 양을 공제하도록, 거래 로그를 미리 결정된 서버로 전송하는 단계를 포함한다.

[0018] 본 개시내용의 구현예들의 제 3 양태에 따르면, 이동 단말 P2P에 기초한 신용 지불 장치가 제공되고, 장치는 거래 단말이 검출될 때, 거래 단말에 의해 전송된 거래 정보를 수신하도록 구성된 제 1 반환 요청 정보 수신 유닛; 거래 정보에 기초하여 거래 응답 정보를 생성하도록 구성된 거래 응답 정보 생성 유닛; 거래 응답 정보를 거래 단말로 전송하도록 구성된 정보 전송 유닛; 거래 단말에 의해 전송되는 현재의 지불 거래의 공제 수락 요청 정보를 수신하도록 구성된 공제 수락 요청 정보 수신 유닛; 공제 수락 요청 정보 및 거래 응답 정보에 기초하여 이동 단말에서 애플리케이션-사설-키-생성된 지불 라이센스를 생성하도록 구성된 애플리케이션-사설-키-생성된 지불 라이센스 생성 유닛; 및 거래 단말이 수신된 지불 라이센스에 기초하여 현재의 지불을 완료하도록, 지불 라이센스를 거래 단말로 전송하도록 구성된 지불 라이센스 전송 유닛을 포함한다.

[0019] 장치는 거래 단말에 의해 전송된 애플리케이션 공개 키 증명서 반환 요청 정보를 수신하도록 구성된 제 2 반환 요청 정보 수신 유닛; 애플리케이션 공개 키 증명서 반환 요청 정보에 기초하여 이동 단말에서 애플리케이션 공개 키 증명서에 대한 애플리케이션 공개 키 증명서 응답 정보를 생성하도록 구성된 애플리케이션 공개 키 증명서 응답 정보 생성 유닛; 및 애플리케이션 공개 키 증명서 응답 정보를 거래 단말로 전송하도록 구성된 공개 키 증명서 응답 정보 전송 유닛을 더 포함한다.

[0020] 또한, 애플리케이션-사설-키-생성된 지불 라이센스 생성 유닛은 이동 단말에서 저장된 애플리케이션 사설 키를 이용함으로써 공제 수락 요청 정보에 기초하여 서명 데이터를 생성하도록 구성된 서명 데이터 생성 모듈; 이동 단말에서 사전-생성된 TAC 서브-키를 이용함으로써 공제 수락 요청 정보 및 거래 응답 정보에 기초하여 거래 인증 코드(TAC)를 생성하도록 구성된 정보 생성 모듈; 및 서명 데이터 및 TAC를 지불 라이센스로서 이용하도록 구성된 지불 라이센스 결정 모듈을 포함한다.

[0021] 또한, 거래 응답 정보는 지불 카드 번호, 이용가능한 한도, 진입/진출 플래그, 및 최후 거래에 대한 정보를 포함한다.

[0022] 또한, 지불 장치가 공공 교통 지불에 적용될 때, 공제 수락 요청 정보는 공제량, 현재의 지불 거래의 날짜, 현재의 지불 거래의 시간, 현재의 지불 거래의 진입/진출 플래그, 및 현재의 지불 거래의 스테이션 정보를 포함한다.

[0023] 또한, 장치는 현재의 이용가능한 한도를 획득하기 위하여, 공제 수락 요청 정보에서의 공제량에 기초하여 거래 응답 정보에서의 이용가능한 한도로부터 공제량을 감산하도록 구성된 현재의 이용가능한 한도 생성 유닛; 및 현재의 이용가능한 한도를, 이동 단말에 대응하는 사용자의 이용가능한 한도로서 이용하도록 구성된 이용가능한 한도 결정 유닛을 포함한다.

[0024] 본 개시내용의 구현예들의 제 4 양태에 따르면, 이동 단말 P2P에 기초한 신용 지불 장치가 제공되고, 장치는 거래 단말에 적용되고, 거래 정보를 이동 단말로 전송하도록 구성된 거래 정보 전송 유닛; 이동 단말에 의해 전송된 거래 응답 정보를 수신하도록 구성된 거래 응답 정보 수신 유닛; 거래 응답 정보에 기초하여 현재의 지불 거래의 공제 수락 요청 정보를 생성하도록 구성된 공제 유닛; 공제 수락 요청 정보를 이동 단말로 전송하도록 구성된 공제 수락 요청 정보 전송 유닛; 및 지불 라이센스가 수신될 때, 지불 라이센스에 기초하여, 현재의 지불 거래가 완료될 수 있는 것으로 결정하도록 구성된 현재의-지불-거래 완료 유닛을 포함한다.

[0025] 장치는 애플리케이션 공개 키 증명서 반환 요청 정보를 이동 단말로 전송하도록 구성된 반환 요청 정보 전송 유닛; 이동 단말에 의해 전송된 애플리케이션 공개 키 증명서 응답 정보를 수신하도록 구성된 공개 키 증명서 응

답 정보 수신 유닛; 및 거래 단말에서 신용-라이센싱된 공개 키를 이용함으로써 애플리케이션 공개 키 증명서 응답 정보에서의 애플리케이션 공개 키 증명서 상의 서명을 검증하도록 구성된 서명 검증 유닛을 더 포함한다.

[0026] 또한, 거래 응답 정보는 지불 카드 번호, 이용가능한 한도, 및 진입/진출 플래그를 포함한다.

[0027] 또한, 장치는 거래 응답 정보에서의 지불 카드 번호가 미리 결정된 블랙리스트 내에 포함되는지 여부를 결정하도록 구성된 블랙리스트 결정 유닛을 더 포함하고; 그리고 반환 요청 정보 전송 유닛은, 거래 응답 정보에서의 지불 카드 번호가 미리 결정된 블랙리스트 내에 포함되지 않을 때, 애플리케이션 공개 키 증명서 반환 요청 정보를 이동 단말로 전송하도록 추가로 구성된다.

[0028] 또한, 장치는 거래 응답 정보에서의 이용가능한 한도가 미리 결정된 임계치 이상인지 여부를 결정하도록 구성된 임계치 결정 유닛; 및 이용가능한 한도가 미리 결정된 임계치 이상일 경우, 거래 응답 정보에서의 진입/진출 플래그가 진출된 상태인지 여부를 검사하도록 구성된 스테이터스 검사 유닛(status checking unit)을 포함한다.

[0029] 또한, 지불 라이센스는 서명 데이터 및 거래 인증 코드(TAC)를 포함하고, 현재의-지불-거래 완료 유닛은 애플리케이션 공개 키를 이용함으로써 서명 데이터를 검증하도록 구성된 서명 검증 모듈; 서명 데이터가 검증될 때, 거래 로그를 생성하도록 구성된 거래 로그 생성 모듈; 및 미리 결정된 서버가 거래 로그 - 거래 로그는 공제량, 거래 날짜, 거래 순간, 거래 단말 ID, 지불 카드 번호, 이용가능한 한도, 및 TAC를 포함함 - 에 기초하여, 이동 단말에 대응하는 사용자 계좌로부터 자금의 대응하는 양을 공제하도록, 거래 로그를 미리 결정된 서버로 전송하도록 구성된 거래 로그 전송 모듈을 포함한다.

[0030] 본 개시내용의 구현예들에서 제공된 기술적 해결책들은 다음의 유익한 효과들을 포함할 수 있다:

[0031] 본 개시내용에서 제공되는 이동 단말 P2P에 기초한 신용 지불 방법 및 장치는 이동 단말 및 거래 단말에 적용가능하다. 지불 애플리케이션을 인에이블(enable)한 후에, 지불 거래가 신속하게 그리고 보안성 있게 완료될 수 있고 온라인 지불이 필요하지 않도록, 사용자는 이동 단말을 이용함으로써 거래 단말과의 오프라인 신용 지불을 완료할 수 있다. 그러므로, 다음의 상황이 회피된다: 관련된 기술에서는, 예를 들어, 사용자가 공공 교통 차량을 탈 때, 사용자는 현금 또는 버스 카드를 오직 이용함으로써 지불 거래 기능을 구현할 수 있다.

[0032] 이전의 일반적인 설명들 및 다음의 상세한 설명들은 단지 예들 및 설명들이고, 본 개시내용을 제한할 수 없다는 것이 이해되어야 한다.

도면의 간단한 설명

[0033] 여기에서의 동반된 도면들은 명세서에서 편입되고, 명세서의 일부가 되고, 본 개시내용에 따르는 구현예들을 도시하고, 본 개시내용의 원리를 설명하기 위하여 명세서와 함께 이용된다.

도 1은 일 예의 구현예에 따른, 신용 인가 시스템(credit authorization system)을 예시하는 개략도이다.

도 2는 일 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 3은 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 4는 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 5는 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 6은 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 7은 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 8은 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 9는 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 10은 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 11은 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 12는 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 13은 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 14는 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 15는 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 16은 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 17은 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 방법을 예시하는 플로우차트이다.

도 18은 도 14에서의 단계(S450)를 예시하는 플로우차트이다.

도 19는 신용 인가 시스템 애플리케이션, 신용 지불 애플리케이션, 및 신용 인가 시스템의 서빙 엔드 사이의 데이터 교환 절차를 예시하는 도면이다.

도 20은 버스 게이트(bus gate)와 신용 인가 시스템 애플리케이션 사이의 데이터 교환을 예시하는 도면이다.

도 21은 버스 게이트와 신용 인가 시스템의 서빙 엔드 사이의 데이터 교환을 예시하는 도면이다.

도 22는 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 장치를 예시하는 개략도이다.

도 23은 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 장치를 예시하는 개략도이다.

도 24는 도 22에서의 애플리케이션-사설-키-생성된 지불 라이센스 생성 유닛을 예시하는 개략도이다.

도 25는 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 장치를 예시하는 개략도이다.

도 26은 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 장치를 예시하는 개략도이다.

도 27은 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 장치를 예시하는 개략도이다.

도 28은 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 장치를 예시하는 개략도이다.

도 29는 또 다른 예의 구현예에 따른, 이동 단말 P2P에 기초한 신용 지불 장치를 예시하는 개략도이다.

도 30은 도 26에서의 현재의-지불-거래 완료 유닛을 예시하는 개략도이다.

발명을 실시하기 위한 구체적인 내용

[0034] 일 예의 구현예들은 여기에서 상세하게 설명되고, 구현예들의 예들은 동반된 도면들에서 제시된다. 다음의 설명이 동반되는 도면들에 관련될 때, 상이한 동반되는 도면들에서의 동일한 번호들은 이와 다르게 특정되지 않으면, 동일한 구성요소 또는 유사한 구성요소들을 나타낸다. 다음의 예의 구현예들에서 설명된 구현예들은 본 개시내용과 일치하는 모든 구현예들을 나타내지는 않는다. 그 대신에, 그것들은 오직, 첨부된 청구항들에서 상세하게 설명되고 본 개시내용의 일부 양태들과 일치하는 장치들 및 방법들의 예들이다.

[0035] 이동 지불은 이동 전화 지불로서 또한 지칭된다. 사용자는 구입된 제품 또는 서비스에 대하여 지불하기 위하여 이동 단말을 이용할 수 있다. 이동 단말은 지불 거래를 완료하기 위하여 근접장 통신(Near Field Communication; NFC)을 통해 거래 단말과 통신할 수 있다. 단거리 통신으로서 또한 지칭된 NFC는 전자 디바이스들이 비-접촉 점-대-점(point-to-point) 데이터 송신을 통해 데이터를 교환하는 것을 허용하는 단거리 고주파수(high-frequency) 무선 주파수 라디오 통신 기술이다. NFC 기술의 보안 특성은 지불과 같은 분야들에서 양호한 적용 전망을 보여준다.

[0036] P2P, 즉, 피어 투 피어(peer to peer)는 NFC 기술의 3 개의 작업 모드들 중의 하나이다. 적외선과 유사하게, P2P 모드는 데이터를 교환하기 위하여 이용될 수 있다. 그러나, P2P 모드에서는, 송신 거리가 더 짧고, 양자의 송신 생성 속력 및 송신 속력은 더 빠르고, 전력 소비는 직외선 모드(블루투스(Bluetooth)와 유사함)보다 더 낮다. NFC 기능을 갖는 2 개의 디바이스들은 피어-투-피어 데이터 송신; 예를 들어, 음악 다운로드, 사진 교환, 또는 디바이스 주소록 동기화를 구현하기 위하여 서로 무선으로 링크될 수 있다. 그러므로, NFC를 통해, 데이터 또는 서비스는 디지털 카메라, PDA, 컴퓨터, 및 이동 전화와 같은 복수의 디바이스들 사이에서 교환될 수 있다. 본 개시내용의 구현예들에서, 이동 단말은 신용 지불 거래를 완료하기 위하여, NFC 기술의 P2P 방법으로 버스 게이트와 데이터를 교환한다.

[0037] 당해 분야의 당업자에 의한 본 개시내용의 더 양호한 이해 및 구현을 용이하게 하기 위하여, 단말들 사이에서 데이터를 어떻게 송신하고 프로세싱할 것인지와 같은, 본 개시내용의 구현예들에서 수반된 이동 단말, 거래 단말, 및 서버 사이의 상관성이 간략하게 먼저 설명된다. 더 양호한 설명을 위한, 이동 지불과 같은 본 개시내용

의 폭넓은 적용으로 인해, 본 개시내용은 고객들이 공공 교통 요금들을 구입하기 위하여 이동 전화 신용 지불을 이용하는 시나리오에 의해 예시된다.

[0038] 도 1에서 도시된 바와 같이, 본 개시내용의 구현예에서 제공된 신용 인가 시스템은 이동 단말(100), 거리 단말(200), 및 서버(300)를 포함한다. 이동 단말(100)은 지불 거래 기능을 갖는 이동 전화일 수 있다. 거래 단말(200)은 버스 게이트일 수 있고, 버스 게이트는 버스 시스템 또는 지하철 시스템에서 이용된 POS 단말이다. 서버(300)는 신용 인가 시스템에서 서빙하고 있다. 이동 단말(100)을 이용함으로써 거래 단말(200)과의 지불 거래를 행하기 전에, 사용자는 서버(300)를 이용함으로써 이동 단말(100)의 신용 지불 거래 기능을 먼저 인에이블할 필요가 있고, 그 다음으로, 이동 단말(100)을 이용함으로써 거래 단말(200)과의 지불 거래를 행할 수 있다. 게다가, 거래 단말(200)은 이동 단말(100)의 거래 로그를 서버(300)로 주기적으로 업로드하고, 서버(300)는 이동 단말(100)에 대응하는 계좌로부터 자금들의 대응하는 양을 공제하고, 그 양을 버스 회사에 지불한다.

[0039] 본 개시내용에서 제공된 이 구현예에서는, 2 개의 애플리케이션들이 이동 단말 상에서 설치될 수 있다. 하나는 신용 지불 애플리케이션, 예를 들어, 신용 지불 애플리케이션 애플릿(credit payment application applet)이다. 자바 카드(Java card)에 대하여, Sun Microsystems Inc.는 애플릿을 자바 카드 상에서 작동하기 위한 객체(object)로서 설정한다. 이동 단말 상의 다른 애플리케이션은 신용 인가 시스템 애플리케이션일 수 있다. 이동 단말 상의 이전의 2 개의 애플리케이션들의 기능들은 하나의 애플리케이션을 이용함으로써 구현될 수 있다. 그것은 본 구현예에서 제한되지는 않는다.

[0040] 거래 단말(200)은 아이덴티티 보안성 인증(identity security authentication)을 통과하고 충분한 신용 한도를 가지는 사용자만이 버스 신용 지불 애플리케이션을 인에이블할 수 있다는 것을 보장하기 위하여, 엄격한 아이덴티티 보안성 인증 메커니즘을 이용한다.

[0041] 신용 지불 애플리케이션 애플릿은 NFC 기능을 갖는 이동 단말(100) 상에서 설치된다. 애플리케이션 사설-공개 키 쌍은 개인화(personalization) 동안에 생성된다. 애플리케이션 사설 키는 신용 지불 애플리케이션에서 저장되고, 신용 지불 애플리케이션은 애플리케이션 사설 키의 데이터가 임의의 조건에서 도난될 수 없다는 것을 보장한다. 애플리케이션 공개 키는 신용 인가 시스템에서 사설 키를 이용함으로써 애플리케이션 공개 키 증명서로서 서명되고, 신용 지불 애플리케이션에서 저장된다. 신용 인가 시스템에서의 공개 키는 거래 단말(200)에 대하여 제공되고, 저장 위치는 거래 단말(200)에 의해 결정된다. 그것은 공개 키이므로, 보안성에 대해 요건이 부과되지 않는다.

[0042] 신용 지불 거래를 제공할 때, 신용 지불 애플리케이션에서의 애플리케이션 공개 키 증명서를 판독한 후에, 거래 단말(200)은 애플리케이션 공개 키를 복원하기 위하여, 신용 인가 시스템에서 공개 키를 이용함으로써 애플리케이션 공개 키 증명서를 검증한다. 신용 지불 애플리케이션은 애플리케이션 사설 키를 이용함으로써 지불 인가 라이센스(payment authorization license)를 생성한다. 거래 단말(200)은 애플리케이션 공개 키를 이용함으로써 지불 인가 라이센스를 검증하고, 그 다음으로, 검증이 통과한 후에 인가 라이센스에서의 보안성 인자(security factor)를 검사한다. 보안성을 확인한 후에, 거래 단말(200)은 신용 회계(credit accounting)를 수행하고, 그 다음으로, 특정된 시간에서 대응하는 신용 계좌를 정산한다. 지불 보안성을 보장하기 위하여, 이용 횟수들, 한도, 또는 간격 시간의 수량이 특정된 임계치를 초과할 때, 이동 단말은 사용자 아이덴티티 정보 및 승인 인가를 다시 검증하기 위하여 네트워크로 접속될 필요가 있다.

[0043] 관련된 기술적 문제를 해결하기 위하여, 본 개시내용의 구현예는 이동 단말에 의한 신용 지불을 인에이블하는 프로세스에 적용된, 이동 단말 P2P에 기초한 신용 지불 방법을 제공한다. 도 2에서 도시된 바와 같이, 방법은 다음의 단계들을 포함할 수 있다.

[0044] 단계(S110)에서는, 이동 단말 상에서 신용 인가 시스템 애플리케이션을 이용함으로써 애플리케이션 인가 요청을 미리 결정된 서버로 전송한다.

[0045] 신용 인가 시스템 애플리케이션은 이동 단말 상에서 설치되고, 이동 단말은 인가 시스템 애플리케이션을 이용함으로써 애플리케이션 인가 요청을 신용 인가 시스템의 서버로 전송할 수 있다.

[0046] 단계(S120)에서는, 미리 결정된 서버에 의해 전송되는 애플리케이션 공개 키 증명서 및 애플리케이션 사설 키를 수신한다.

[0047] 수신된 애플리케이션 인가 요청에 기초하여, 신용 인가 시스템의 서버는 키들의 쌍, 즉, 애플리케이션 공개 키 및 애플리케이션 사설 키를 생성한다. 서버는 애플리케이션 공개 키 증명서를 생성하기 위하여, 서버 상에서 로컬로 저장된 인가된 사설 키를 이용함으로써 애플리케이션 공개 키를 서명하고, 획득된 애플리케이션 공개 키

증명서 및 애플리케이션 사설 키를 이동 단말로 전송한다.

[0048] 단계(S130)에서는, 이동 단말 상의 신용 지불 애플리케이션에서 애플리케이션 공개 키 증명서 및 애플리케이션 사설 키를 저장한다.

[0049] 이동 단말은 이동 단말 상의 신용 지불 애플리케이션에서, 서빙 엔드(serving end)에 의해 전송되는 애플리케이션 공개 키 증명서 및 애플리케이션 사설 키를 저장한다.

[0050] 단계(S140)에서는, 신용 지불 데이터 취득 요청이 미리 결정된 서버로 전송된다.

[0051] 단계(S150)에서는, 미리 결정된 서버에 의해 전송된 신용 지불 데이터가 수신되고, 이동 단말의 신용 지불 기능은 신용 지불 데이터에 기초하여 인에이블된다.

[0052] 신용 지불 데이터는 개인화 스크립트(personalization script)일 수 있고, 개인화 스크립트는 지불 카드 번호, 신용 한도, 이용가능한 한도, 및 TAC 서브-키를 포함한다. 지불 카드 번호는 각각의 사용자의 신용 지불 애플리케이션을 위하여 신용 인가 시스템에 의해 생성된 고유한 문자 코드이다. 이용가능한 한도는 사용자가 현재 이용할 수 있는 자금의 양이다. TAC 서브-키는 TAC 부모 사설 키(parent private key)를 이용함으로써 카드 번호 해시(card number hash)에 기초하여 신용 인가 시스템에서 서버에 의해 획득된다.

[0053] 본 개시내용에서 제공된 또 다른 구현예에서는, 도 2에 기초하여, 도 3에서 도시된 바와 같이, 단계(S110) 전에, 방법은 다음의 단계들을 더 포함할 수 있다.

[0054] 단계(S101)에서는, 이동 단말의 디바이스 파라미터 정보를 획득한다.

[0055] 이동 단말의 디바이스 파라미터 정보는 이동 단말의 하드웨어 정보일 수 있다. 디바이스 파라미터 정보에 기초하여, 이동 단말이 지불 거래의 하드웨어 조건을 충족시키는지 여부, 예를 들어, 이동 단말이 NFC 기능을 가지는지 여부가 먼저 검사될 필요가 있다. 확실히, 디바이스 파라미터 정보는 또한, 이동 단말의 디바이스 모델, ROM 버전(version), (안드로이드(Android)와 같은) 시스템 모델, 애플리케이션 버전 등과 같은 정보일 수 있다.

[0056] 단계(S102)에서는, 디바이스 파라미터 정보를 미리 결정된 서버로 전송한다.

[0057] 서버가 수신된 디바이스 파라미터 정보에 기초하여, 이동 단말이 신용 지불을 인에이블하기 위한 하드웨어 조건을 충족시키는지 여부를 결정하도록, 이동 단말은 이동 단말의 획득된 디바이스 파라미터 정보를 신용 인가 시스템의 서버로 전송한다.

[0058] 단계(S103)에서는, 미리 결정된 서버에 의해 전송된 신용 지불 인에이블 정보가 수신되는지 여부를 검사한다.

[0059] 이동 단말이 신용 지불을 인에이블하기 위한 하드웨어 조건을 충족시킬 경우, 서버는 신용 지불 인에이블 정보를 이동 단말로 전송한다. 신용 지불 인에이블 정보는 신용 지불 애플리케이션 인에이블 페이지(credit payment application enabling page)일 수 있다.

[0060] 이동 단말이 신용 지불을 인에이블하기 위한 하드웨어 조건을 충족시키지 않을 경우, 서버는 신용 지불 인에이블 정보를 이동 단말로 전송하지 않는다.

[0061] 미리 결정된 서버에 의해 전송된 신용 지불 인에이블 정보가 수신될 때, 단계(S104)가 수행된다.

[0062] 단계(S104)에서는, 이동 단말이 신용 지불을 인에이블하기 위한 하드웨어 조건을 충족시키는 것으로 결정하고, 단계(S110)가 수행된다.

[0063] 이동 단말이 신용 지불을 인에이블하기 위한 하드웨어 조건을 충족시키는지 여부를 검사하는 것에 추가하여, 도 2에 기초하여, 단계(S110) 전에, 도 4에서 도시된 바와 같이, 이동 단말이 보안성 인증 조건을 충족시키는지 여부가 추가로 검사될 필요가 있다. 그러므로, 본 개시내용에서 제공된 또 다른 구현예에서, 본 개시내용에서 제공된 이동 단말 P2P에 기초한 신용 지불 방법은 다음의 단계들을 더 포함할 수 있다.

[0064] 단계(S105)에서는, 이동 단말에 대응하는 사용자 아이덴티티 정보를 획득한다.

[0065] 사용자 아이덴티티 정보는 사용자의 ID 카드 번호, 명칭, 은행 카드 번호, 전자메일 주소, 알리페이(Alipay) 계좌 등과 같은 정보일 수 있다.

[0066] 단계(S106)에서는, 미리 결정된 서버가 수신된 사용자 아이덴티티 정보에 기초하여, 이동 단말이 신용 지불을 인에이블하기 위한 보안성 인증 조건을 충족시키는지 여부를 결정하도록, 사용자 아이덴티티 정보를 미리 결정된 서버로 전송한다.

[0067] 서버가 사용자 아이덴티티 정보를 검증하도록, 예를 들어, 은행 카드 번호가 서비스를 정상적으로 제공하는지 여부, 또는 사용자 계좌가 나쁜-신용 거래 레코드(bad-credit transaction record)를 가지는지 여부를 검증하도록, 이동 단말은 사용자 아이덴티티 정보를 신용 인가 시스템에서의 서버로 전송한다.

[0068] 단계(S107)에서는, 미리 결정된 서버에 의해 전송된 보안성 인증 성공 정보가 수신되는지 여부를 검사한다.

[0069] 이동 단말에 의해 전송된 사용자 정보를 수신한 후에, 서버는 사용자 정보를 검사한다. 이동 단말이 신용 지불을 인에이블하기 위한 보안성 인증 조건을 충족시킬 경우, 서버는 보안성 인증 성공 정보를 이동 단말로 전송한다.

[0070] 미리 결정된 서버에 의해 전송된 보안성 인증 성공 정보가 수신될 때, 단계(S108)가 수행된다. 단계(S108)에서는, 이동 단말이 신용 지불을 인에이블하기 위한 보안성 인증 조건을 충족시키는 것으로 결정하고, 단계(S110)가 수행된다.

[0071] 이동 단말이 서버 엔드에 의해 전송된 보안성 인증 성공 정보를 수신할 때, 이동 단말은 이동 단말이 신용 지불을 인에이블하기 위한 보안성 인증 조건을 충족시키는 것으로 결정한다.

[0072] 이동 단말이 서버 엔드에 의해 전송된 보안성 인증 성공 정보를 수신하지 않을 때, 이동 단말은 이동 단말이 신용 지불을 인에이블하기 위한 보안성 인증 조건을 충족시키지 않는 것으로 결정한다.

[0073] 도 2에 기초하여, 단계(S110) 전에, 도 5에서 도시된 바와 같이, 관련된 애플리케이션은 추가로 이동 단말 상에서 설치될 필요가 있다. 그러므로, 본 개시내용에서 제공된 이동 단말 P2P에 기초한 신용 지불 방법은 다음의 단계들을 더 포함한다.

[0074] 단계(S160)에서는, 미리 결정된 설치 파일들을 획득하기 위한 요청을 미리 결정된 서버로 전송한다.

[0075] 미리 결정된 설치 파일들은 신용 지불 애플리케이션을 포함한다.

[0076] 단계(S170)에서는, 미리 결정된 서버에 의해 전송된 미리 결정된 설치 파일들을 획득한다.

[0077] 단계(S180)에서는, 이동 단말 상에서 미리 결정된 설치 파일들을 설치하고, 단계(S110)가 수행된다.

[0078] 신용 지불 애플리케이션 및 등록 스크립트가 이동 단말 상에서 별도로 설치된 후에, 이동 단말의 사용자 개인화가 완료된다. 이와 같이, 이동 단말 상에서 신용 지불 기능을 인에이블하는 절차가 완료된다. 이전의 구현예들에 기초하여, 이동 단말이 신용 지불 기능을 인에이블하는 신용 인가 시스템의 서버 측 상의 실행 절차는 이하에서 상세하게 설명된다.

[0079] 본 개시내용에서 제공된 또 다른 구현예에서는, 도 6에서 도시된 바와 같이, 본 개시내용에서 제공된 이동 단말 P2P에 기초한 신용 지불 방법에서의 서버(신용 인가 시스템의 서빙 엔드)의 실행 절차는 다음의 단계들을 포함할 수 있다.

[0080] 단계(S210)에서는, 이동 단말에 의해 전송된 애플리케이션 인가 요청을 수신한다.

[0081] 단계(S220)에서는, 애플리케이션 인가 요청에 기초하여 애플리케이션 공개 키 및 애플리케이션 사설 키를 별도로 생성한다.

[0082] 단계(S230)에서는, 애플리케이션 공개 키 증명서를 생성하기 위하여, 로컬로 저장된 인가 사설 키를 이용함으로써 애플리케이션 공개 키를 서명한다.

[0083] 단계(S240)에서는, 애플리케이션 공개 키 증명서 및 애플리케이션 사설 키를 이동 단말로 별도로 전송한다.

[0084] 수신된 애플리케이션 인가 요청에 기초하여, 신용 인가 시스템의 서버는 키들의 쌍, 즉, 애플리케이션 공개 키 및 애플리케이션 사설 키를 생성한다. 서버는 애플리케이션 공개 키 증명서를 생성하기 위하여, 로컬로 저장된 인가 사설 키를 이용함으로써 애플리케이션 공개 키를 서명하고, 획득된 애플리케이션 공개 키 증명서 및 애플리케이션 사설 키를 이동 단말로 별도로 전송한다.

[0085] 단계(S250)에서는, 이동 단말에 의해 전송된 신용 지불 데이터 취득 요청을 수신한다.

[0086] 단계(S260)에서는, 신용 지불 데이터 취득 요청에 기초하여 이동 단말에 대응하는 신용 지불 데이터를 생성하고, 이동 단말이 수신된 신용 지불 데이터에 기초하여 이동 단말의 신용 지불 기능을 인에이블하도록, 신용 지불 데이터를 이동 단말로 전송한다.

[0087] 신용 지불 데이터는 개인화 스크립트일 수 있고, 개인화 스크립트는 지불 카드 번호, 신용 한도, 이용가능한 한도, 및 TAC 서브-키를 포함한다. 지불 카드 번호는 각각의 사용자의 신용 지불 애플리케이션을 위하여 신용 인가 시스템에 의해 생성된 고유한 문자 코드이다. 이용가능한 한도는 사용자가 현재 이용할 수 있는 자금의 양이다. TAC 서브-키는 TAC 부모 사설 키를 이용함으로써 카드 번호 해시에 기초하여 신용 인가 시스템에서 서버에 의해 획득된다.

[0088] 도 6에 기초하여, 도 7에서 도시된 바와 같이, 본 개시내용에서 제공된 또 다른 구현예에서는, 버서(신용 인가 시스템의 서빙 엔드)가 이동 단말에 의해 전송된 디바이스 파라미터 정보에 기초하여, 이동 단말이 신용 지불을 인에이블하기 위한 하드웨어 조건을 충족시키는지 여부를 결정한다. 그러므로, 단계(S210) 전에, 본 개시내용의 구현예에서 제공된 이동 단말 P2P에 기초한 신용 지불 방법은 다음의 단계들을 더 포함할 수 있다.

[0089] 단계(S201)에서는, 이동 단말에 의해 전송된 디바이스 파라미터 정보를 수신한다.

[0090] 이동 단말이 신용 지불 기능을 인에이블하는 프로세스에서, 이동 단말은 네트워크 등을 이용함으로써 신용 인가 시스템의 서빙 엔드(즉, 서버)와 통신할 수 있다. 신용 인가 시스템의 서빙 엔드는 이동 단말에 의해 전송된 디바이스 파라미터 정보를 수신할 수 있다.

[0091] 단계(S202)에서는, 디바이스 파라미터 정보에 기초하여, 이동 단말이 신용 지불을 인에이블하기 위한 하드웨어 조건을 충족시키는지 여부를 결정한다.

[0092] 이동 단말에 의해 전송된 파라미터 정보는 이동 단말의 디바이스 모델, ROM 버전, (안드로이드와 같은) 시스템 버전, 애플리케이션 버전 등과 같은 정보일 수 있다. 서버는 이동 단말에 의해 전송된 정보에 기초하여, 이동 단말이 NFC 기능을 가지는지 여부 등을 검사할 수 있다.

[0093] 서버가 이동 단말이 신용 지불을 인에이블하기 위한 하드웨어 조건을 충족시키는 것을 검사할 경우, 서버는 신용 지불 인에이블 정보를 이동 단말로 전송한다. 신용 지불 인에이블 정보는 신용 지불 애플리케이션 인에이블 페이지일 수 있다. 사용자는 이동 단말의 신용 지불 애플리케이션 인에이블 인터페이스 상에서 사용자 정보를 입력할 수 있고, 사용자 아이덴티티 정보를 서빙 엔드로 업로드할 수 있다.

[0094] 서버가 이동 단말이 신용 지불을 인에이블하기 위한 하드웨어 조건을 충족시키지 않는다는 것을 검출할 경우, 서버는 신용 지불 인에이블 정보를 이동 단말로 전송하지 않는다.

[0095] 이동 단말이 신용 지불을 인에이블하기 위한 하드웨어 조건을 충족시킬 때, 단계(S203)에서는, 신용 지불 인에이블 정보를 이동 단말로 전송하고, 단계(S210)가 수행된다.

[0096] 이동 단말에 의해 전송된 디바이스 파라미터 정보를 검사하는 것에 추가하여, 신용 인가 시스템에서의 서버는 추가로, 이동 단말에 의해 전송된 사용자 아이덴티티 정보를 검사하고, 이동 단말에 대응하는 사용자가 보안성 인증 조건을 충족시키는지 여부를 결정할 필요가 있다. 그러므로, 도 6에 기초하여, 도 8에서 도시된 바와 같이, 이동 단말의 신용 지불 기능을 인에이블하는 프로세스에서, 단계(S210) 전에, 본 개시내용에서 제공된 이동 단말 P2P에 기초한 신용 지불 방법은 다음의 단계들을 더 포함할 수 있다.

[0097] 단계(S204)에서는, 이동 단말에 의해 전송된 사용자 아이덴티티 정보를 수신한다.

[0098] 사용자 아이덴티티 정보는 사용자의 ID 카드 번호, 명칭, 은행 카드 번호, 전자메일 주소, 알리페이 계좌 등과 같은 정보일 수 있다.

[0099] 단계(S205)에서는, 사용자 아이덴티티 정보에 기초하여, 이동 단말이 신용 지불을 인에이블하기 위한 보안성 인증 조건을 충족시키는지 여부를 결정한다.

[0100] 예를 들어, 서버는 사용자 아이덴티티 정보에서의 은행 카드 번호가 나쁜 거래 레코드이든지 간에, 서비스를 정상적으로 제공하는지 여부를 검사할 수 있다.

[0101] 서버가 이동 단말이 신용 지불을 인에이블하기 위한 보안성 인증 조건을 충족시킨다는 것을 검출할 경우, 서버는 보안성 인증 성공 정보를 이동 단말로 전송한다.

[0102] 이동 단말이 신용 지불을 인에이블하기 위한 보안성 인증 조건을 충족시킬 때, 단계(S206)에서는, 보안성 인증 성공 정보를 이동 단말로 전송하고, 단계(S210)가 수행된다.

[0103] 이동 단말이 신용 지불을 인에이블할 때, 신용 지불 애플리케이션은 추가로 설치될 필요가 있고, 이 설치 파일들은 신용 인가 시스템에서의 서버에 의해 이동 단말로 전송될 필요가 있다. 그러므로, 도 6에 기초하여, 도 9

에서 도시된 바와 같이, 본 개시내용의 또 다른 구현예에서, 단계(210) 전에, 본 개시내용에서 제공된 이동 단말 P2P에 기초한 신용 지불 방법은 다음의 단계들을 더 포함할 수 있다.

[0104] 단계(S207)에서는, 미리 결정된 설치 파일들을 획득하기 위한, 이동 단말에 의해 전송된 요청을 수신한다.

[0105] 미리 결정된 설치 파일들은 신용 지불 애플리케이션을 포함한다.

[0106] 단계(S208)에서는, 미리 결정된 설치 파일들을 획득하기 위한 요청에 기초하여 미리 결정된 설치 파일들을 이동 단말로 별도로 전송하고, 단계(S210)가 수행된다.

[0107] 본 개시내용의 이전의 구현예들은 이동 단말에서 신용 지불을 인에이블하는 프로세스를 설명한다. 일부 시나리오들에서, 신용 지불 인에이블 프로세스는 다른 방법들로 획득될 수 있고, 예를 들어, 이동 단말 상에서 미리 결정되거나, 신용 지불 기관(credit payment authority)으로의 등록 애플리케이션을 통해 획득된다. 신용 지불 인에이블 프로세스는 여기에서 제한되지 않는다.

[0108] 관련된 기술들에서의 문제를 해결하기 위하여, 본 개시내용의 구현예는 이동 단말과 거래 단말 사이의 신용 지불 프로세스에 적용된, 이동 단말 P2P에 기초한 신용 지불 방법을 제공한다. 도 10에서 도시된 바와 같이, 방법은 다음의 단계들을 포함할 수 있다.

[0109] 단계(S310)에서, 거래 단말에 의해 전송된 거래 정보를 수신한다.

[0110] 사용자가 이동 단말을 보유하고 지불 거래를 행하기 위하여 버스 게이트에 접근할 때, 버스 게이트가 라디오 주파수 필드를 생성할 수 있으므로, 이동 단말이 버스 게이트에 접근할 때, 즉, 이동 단말이 버스 게이트에 의해 생성된 라디오 주파수 필드에 진입할 때, 이동 단말은 버스 게이트에 의해 생성된 라디오 주파수 필드를 검출할 수 있고, 버스 게이트는 또한, 이동 단말을 검출한다. 이 상황에서, 통신 접속은 버스 게이트와 이동 단말 사이에서 확립되고, 버스 게이트는 거래 정보를 이동 단말로 전송하고, 이동 단말은 버스 게이트에 의해 전송된 거래 정보를 수신한다.

[0111] NFC 데이터 교환 포맷(NFC data exchange format; NDEF) 메시지를 어떻게 교환할 것인지는 P2P 모드에서 설명된다는 것이 주목할 가치가 있다.

[0112] 단계(S320)에서는, 거래 정보에 기초하여 거래 응답 정보를 생성하고, 거래 응답 정보를 거래 단말로 전송한다.

[0113] 단계(S330)에서는, 거래 단말에 의해 전송되는 현재의 지불 거래의 공제 수락 요청 정보를 수신한다.

[0114] 이동 단말에 의해 전송된 애플리케이션 공개 키 증명서를 수신한 후에, 버스 게이트는 애플리케이션 공개 키 증명서의 검증을 수행하고, 현재의 지불 거래 공제 정보를 생성하고, 공제 정보를 이동 단말로 전송한다. 이동 단말은 버스 게이트에 의해 전송된 공제 정보를 수신한다.

[0115] 단계(S340)에서는, 공제 수락 요청 정보 및 거래 응답 정보에 기초하여 이동 단말에서 애플리케이션-사설-키-생성된 지불 라이센스를 생성한다.

[0116] 이동 단말에 의해 생성된 지불 라이센스는 서명 데이터 및 거래 인증 코드(TAC)를 포함한다.

[0117] 단계(S350)에서는, 거래 단말이 수신된 지불 라이센스에 기초하여 현재의 지불 거래를 완료하도록, 지불 라이센스를 거래 단말로 전송한다.

[0118] 이동 단말에 의해 전송된 지불 라이센스를 수신한 후에, 버스 게이트는 지불 라이센스를 검증한다. 라이센스가 검증될 경우. 현재의 지불 거래가 완료되는 것으로 결정된다.

[0119] 이동 단말을 감지한 후에, 버스 게이트는 SNEP 겟 요청 메시지(SNEP get request message)를 앙상블(ensemble)할 수 있고, SNEP 겟 요청 메시지를 버스 신용 지불 애플리케이션으로 전송할 수 있다. 메시지의 정보 필드 식별자 메시지는 카드 정보 판독이다. SNEP 겟 요청 메시지를 수신한 후에, 버스 신용 지불 애플리케이션은 반환될 필요가 있는 데이터를 SNEP 응답 메시지로 조립하고, SNEP 응답 메시지는 카드 번호, 이용가능한 한도, 진입/진출 플래그, 및 최후 거래에 대한 정보를 포함하고; SNEP 응답 메시지를 게이트로 반환한다. 최후 거래에 대한 정보는 스테이션 정보, 거래 데이터, 거래 시간 등을 포함한다.

[0120] SNEP 요청 메시지는 P2P로 SNEP 클라이언트에 의해 SNEP 서버로 전송된 요청 메시지인 것이 주목할 가치가 있다. 2 개의 타입들의 SNEP 요청 메시지들: 겟 메시지(get message) 및 풋 메시지(put message)가 있다. 겟 메시지는 서버가 데이터를 반환할 것을 요청하고, 풋 메시지는 서버가 데이터를 수락할 것을 요청한다. SNEP 겟 요청 메시지 및 SNEP 풋 요청 메시지는 명세서에서 구별된다. SNEP 응답 메시지는 P2P로 SNEP 서버에 의해

SNEP 클라이언트로 반환된 응답 메시지이다. 겟 메시지는 데이터를 반환할 것을 요청하고, 풋 메시지는 성공 또는 실패를 표시하는 응답 코드를 반환할 것을 요청한다.

[0121] 반환 요청 정보는 SNEP 겟 요청 메시지와 동등하고, 거래 응답 정보는 SNEP 응답 메시지와 동등하다.

[0122] 본 개시내용의 이 구현예에서 제공된 방법에서는, 사용자가 이동 단말을 이용함으로써 거래 단말과의 지불 거래를 행할 때, 이동 단말은 거래 단말에 의해 전송된 관련된 명령어 정보에 기초하여, 애플리케이션 공개 키 증명서 및 생성된 지불 인가 라이센스를 거래 단말로 성공적으로 전송하고, 거래 단말은 이동 단말에 의해 전송된 정보에 기초하여 현재의 지불 거래를 완료한다. 관련된 기술들에서의 문제와 비교하면, 본 개시내용의 이 구현예에서 제공된 신용 지불 방법에서는, 이동 단말을 이용함으로써 거래 단말과의 거래를 행할 때, 신용 소비가 추후의 지불 거래 프로세스에서의 이동 단말의 사용자 계좌에 대하여 이용되도록, 사용자는 별도로 이동 단말 및 거래 단말을 오프라인으로 되게 할 수 있다. 사용자가 거래에서 현금을 이용함으로써 야기된 자산 손실 위험으로부터 보호될 수 있도록, 계좌는 이동 단말을 이용함으로써 사용자가 구입을 행한 후에만 정산된다.

[0123] 도 10에서의 방법의 개량으로서, 본 개시내용의 또 다른 구현예에서, 도 11에서 도시된 바와 같이, 단계(S320) 후에, 방법은 다음의 단계들을 더 포함할 수 있다.

[0124] 단계(S360)에서는, 거래 단말에 의해 전송된 애플리케이션 공개 키 증명서 반환 요청 정보를 수신한다.

[0125] 단계(S370)에서는, 애플리케이션 공개 키 증명서 반환 요청 정보에 기초하여 이동 단말 상에서 애플리케이션 공개 키 증명서에 대한 애플리케이션 공개 키 증명서 응답 정보를 생성하고, 애플리케이션 공개 키 증명서 응답 정보를 거래 단말로 전송한다.

[0126] 애플리케이션 공개 키 증명서 응답 정보는 애플리케이션 공개 키 증명서 반환 요청 정보에 대응하고, 데이터 송신 및 수신 포맷 요건을 충족시킨다.

[0127] 본 개시내용의 본 구현예에서, 거래 단말이 이동 단말에 의해 전송된 인가 라이센스에 기초하여 현재의 지불 거래를 완료할 수 있도록, 이동 단말이 지불 인가 라이센스를 어떻게 생성하는지를 상세하게 설명하기 위하여, 도 10에서의 방법의 개량으로서, 본 개시내용의 또 다른 구현예에서는, 도 12에서 도시된 바와 같이, 단계(S340)는 다음의 단계들을 더 포함할 수 있다.

[0128] 단계(S361)에서는, 이동 단말에서 저장된 애플리케이션 사설 키를 이용함으로써 공제 수락 요청 정보에 기초하여 서명 데이터를 생성한다.

[0129] 애플리케이션 사설 키는 이동 단말 상에서 사전-생성되고 저장된다. 신용 지불 애플리케이션은 서명 데이터를 생성하기 위하여, 애플리케이션 사설 키를 이용함으로써 공제 정보를 서명한다. 공제 정보는 공제량, 현재의 지불 거래의 날짜 및 시간, 현재의 지불 거래 서명 상의 진입/진출 플래그, 및 현재의 지불 거래의 스테이션 정보를 포함한다.

[0130] 단계(S362)에서는, 이동 단말 상에서 사전-생성되는 TAC 서브-키를 이용함으로써 공제 수락 요청 정보 및 거래 응답 정보에 기초하여 TAC를 생성한다.

[0131] 공제 수락 요청 정보는 공제 정보를 포함하고, 거래 응답 정보는 거래 정보를 포함한다. 이동 단말 상의 신용 지불 애플리케이션은 TAC를 생성하기 위하여, 공제 정보 및 거래 정보에 기초하여 공제가능한 양, 현재의 지불 거래의 날짜, 현재의 지불 거래의 시간, 지불 카드 번호, 이용가능한 한도, 및 신용 한도를 암호화한다. 신용 한도는 오프라인 모드에서 신용 인가 시스템에 의해 사용자에게 인가된 최대 이용가능한 양이다.

[0132] 단계(S363)에서는, 서명 데이터 및 TAC를 지불 인가 라이센스로서 이용한다.

[0133] 신용 지불 애플리케이션은 서명 데이터 및 TAC를 별도로 지불 인가 라이센스로서 버스 게이트로 전송할 수 있거나, 서명 데이터 및 TAC를 함께 신용 인가 라이센스로서 버스 게이트로 전송할 수 있다.

[0134] 게다가, 거래 응답 정보는 지불 카드 번호, 이용가능한 한도, 진입/진출 플래그, 및 최후 거래에 대한 정보를 포함한다. 지불 카드 번호는 각각의 사용자의 신용 지불 애플리케이션을 위하여 신용 인가 시스템에 의해 생성된 고유한 문자 코드이다. 이용가능한 한도는 사용자가 현재 이용할 수 있는 자금의 양이다. TAC 서브-키는 TAC 부모 사설 키를 이용함으로써 카드 번호 해시에 기초하여 신용 인가 시스템에서 서버에 의해 획득된다. 최후 거래에 대한 정보는 스테이션 정보, 거래 데이터, 거래 시간 등을 포함한다.

[0135] 도 10에 기초하여, 도 13에서 도시된 바와 같이, 본 개시내용의 또 다른 구현예에서는, 방법은 다음의 단계들을

더 포함할 수 있다.

[0136] 단계(S380)에서는, 현재의 이용가능한 한도를 획득하기 위하여, 공제 수락 요청 정보에서의 공제량에 기초하여 거래 응답 정보에서의 이용가능한 한도로부터 공제량을 감산한다.

[0137] 단계(S390)에서는, 현재의 이용가능한 한도를, 이동 단말 상에서 사용자에 대응하는 이용가능한 한도로서 이용한다.

[0138] 이동 단말과 거래 단말 사이의 거래 지불 프로세스를 상세하게 설명하기 위하여, 본 개시내용의 구현예는 이동 단말 P2P에 기초한 신용 지불 방법을 제공한다. 거래 단말 측 상에서의 실행 절차에서는, 도 14에서 도시된 바와 같이, 방법은 다음의 단계들을 포함할 수 있다.

[0139] 단계(S410)에서는, 거래 정보를 이동 단말로 전송한다.

[0140] 단계(420)에서는, 이동 단말에 의해 전송된 거래 응답 정보를 수신한다.

[0141] 단계(S430)에서는, 거래 응답 정보에 기초하여 현재의 지불 거래의 공제 수락 요청 정보를 생성한다.

[0142] 단계(S440)에서는, 공제 수락 요청 정보를 이동 단말로 전송한다.

[0143] 단계(S450)에서는, 지불 라이센스가 수신될 때, 지불 라이센스에 기초하여, 현재의 지불 거래가 완료될 수 있는 것으로 결정한다.

[0144] 방법은 신용 지불 거래 프로세스에서의 이동 단말 측 상의 실행 절차에 대응하는, 신용 지불 거래 프로세스에서의 버스 게이트 측 상의 실행 절차를 도시하므로, 버스 게이트와 이동 단말 사이의 데이터 교환은 여기에서 다시 설명되지 않는다. 세부사항들에 대하여, 이전의 구현예에서의 이동 단말 측 상의 실행 절차를 참조한다.

[0145] 구현예들에서의 거래 정보, 거래 응답 정보, 공개 키 증명서 반환 요청 정보, 공개 키 증명서 응답 정보 등은 데이터 교환 프로세스에서의 포맷 요건을 충족시키기 위하여 이용된다는 것이 주목할 가치가 있다. 예를 들어, 거래 응답 정보는 거래 정보를 포함하는 응답 정보로서 이해될 수 있고, 공개 키 증명서 응답 정보는 공개 키 증명서를 포함하는 응답 정보로서 이해될 수 있다.

[0146] 게다가, 거래 응답 정보는 지불 카드 번호, 이용가능한 한도, 진입/진출 플래그, 및 최후 거래에 대한 정보를 포함한다.

[0147] 도 14에 기초하여, 도 15에서 도시된 바와 같이, 본 개시내용에서 제공된 또 다른 구현예에서는, 단계(S420) 후에, 방법은 다음의 단계들을 더 포함할 수 있다.

[0148] 단계(S460)에서는, 애플리케이션 공개 키 증명서 반환 요청 정보를 이동 단말로 전송한다.

[0149] 단계(S470)에서는, 이동 단말에 의해 전송된 애플리케이션 공개 키 증명서 응답 정보를 수신한다.

[0150] 단계(S480)에서는, 거래 단말에서 신용-라이센싱된 공개 키를 이용함으로써 애플리케이션 공개 키 증명서 응답 정보에서의 애플리케이션 공개 키 증명서 상의 서명을 검증한다.

[0151] 방법은 신용 지불 거래 프로세스에서의 이동 단말 측 상의 실행 절차에 대응하는, 신용 지불 거래 프로세스에서의 버스 게이트 측 상의 실행 절차를 도시하므로, 버스 게이트와 이동 단말 사이의 데이터 교환은 여기에서 다시 설명되지 않는다. 세부사항들에 대하여, 이전의 구현예에서의 이동 단말 측 상의 실행 절차를 참조한다.

[0152] 도 14에 기초하여, 도 16에서 도시된 바와 같이, 본 개시내용에서 제공된 또 다른 구현예에서는, 방법은 다음의 단계들을 더 포함할 수 있다.

[0153] 단계(S401)에서는, 거래 응답 정보에서의 지불 카드 번호가 미리 결정된 블랙리스트 내에 포함되는지 여부를 결정한다.

[0154] 거래 응답 정보에서의 지불 카드 번호가 미리 결정된 블랙리스트 내에 포함되지 않을 때, 단계(S460)가 수행된다.

[0155] 블랙리스트는 거래 단말, 즉, 버스 게이트에서 미리 결정될 수 있다. 이동 단말에 대응하는 사용자 아이덴티티 정보는 블랙리스트에서의 정보와 비교된다. 사용자 아이덴티티 정보가 블랙리스트에서 존재할 경우, 이 거래 지불 절차는 악의적인 거래를 회피하기 위하여 정지된다.

[0156] 도 14에 기초하여, 도 17에서 도시된 바와 같이, 본 개시내용에서 제공된 또 다른 구현예에서는, 방법은 다음의

단계들을 더 포함할 수 있다.

[0157] 단계(S402)에서는, 거래 응답 정보에서의 이용가능한 한도가 미리 결정된 임계치 이상인지 여부를 결정한다.

[0158] 이용가능한 한도가 미리 결정된 임계치 이상일 경우, 단계(S403)에서는, 거래 응답 정보에서의 진입/진출 플래그가 진출된 상태인지 여부를 검사한다.

[0159] 거래 정보에서의 진입/진출 플래그가 진출된 상태일 경우, 단계(S460)가 수행된다.

[0160] 사용자의 이용가능한 한도는 신용 지불 거래가 계속될 필요가 있는지 여부를 결정하기 위하여 검사된다. 사용자의 이용가능한 한도가 이 거래의 공제량보다 더 작을 때, 악의적인 지불 거래가 회피될 수 있도록, 이 신용 지불 거래는 정지된다.

[0161] 본 단계는 이동 단말에 의해 전송된 거래 응답 정보에 기초하여, 이동 단말에 대응하는 사용자 계좌의 이용가능한 한도가 현재의 지불 거래를 지불하기에 충분한지 여부를 검사하기 위하여 버스 게이트에 의해 주로 이용된다. 이용가능한 한도가 불충분할 경우, 현재의 지불 거래는 거절된다. 이용가능한 한도가 충분할 경우, 버스 게이트는 거래 응답 정보에서의 진입/진출 플래그가 0인지 여부를 검사한다. 진입/진출 플래그가 0이 아닐 경우, 현재의 지불 거래는 거절된다. 진입/진출 플래그가 0일 경우, 현재의 지불 거래는 계속된다. 진입/진출 플래그가 1일 때, 그것은 이동 단말을 보유하는 사용자가 "진입된" 상태에 있다는 것을 표시하고, 그러므로, 현재의 지불 거래는 거절된다는 것이 주목할 가치가 있다. 진입/진출 플래그가 0일 때, 그것은 이동 단말을 보유하는 사용자가 "진출된" 상태에 있다는 것을 표시하고, 현재의 지불 거래가 행해지도록, 계좌가 정산될 수 있다.

[0162] 도 14에 기초하여, 도 18에서 도시된 바와 같이, 본 개시내용에서 제공된 또 다른 구현예에서는, 단계(S450)는 다음의 단계들을 포함할 수 있다.

[0163] 단계(S481)에서는, 애플리케이션 공개 키를 이용함으로써 서명 데이터를 검증한다.

[0164] 애플리케이션 공개 키는 이동 단말에 의해 전소오딘 지불 인가 라이센스로부터 버스 게이트에 의해 복원되고, 애플리케이션 공개 키는 서명 데이터에서의 관련된 정보가 애플리케이션 공개 키에서의 대응하는 정보와 정합하는지 여부를 검사한다. 긍정일 경우, 서명 검증이 통과한다.

[0165] 단계(S482)에서는, 서명 데이터가 검증될 때에 거래 로그를 생성한다.

[0166] 버스 게이트가 서명 데이터를 검증한 후에, 현재의 지불의 거래 로그가 생성된다. 거래 로그는 공제량, 거래 날짜, 거래 시간, 거래 단말 ID, 지불 카드 번호, 이용가능한 한도, 및 TAC를 포함한다.

[0167] 단계(S483)에서는, 미리 결정된 서버가 거래 로그에 기초하여 이동 단말에 대응하는 사용자 계좌로부터 자금의 대응하는 양을 공제하도록, 거래 로그를 미리 결정된 서버로 전송한다.

[0168] 거래 로그는 공제량, 거래 날짜, 거래 시간, 거래 단말 ID, 지불 카드 번호, 이용가능한 한도, 및 TAC를 포함한다. 지불 라이센스는 서명 데이터 및 TAC를 포함한다.

[0169] 본 개시내용에서 제공된 또 다른 구현예에서, 도 19에서 도시된 바와 같이, 본 개시내용은 이동 단말 P2P에 기초한 신용 지불 방법을 제공한다. 이 구현예에서, 이동 전화는 이동 단말을 나타내고, 신용 인가 시스템의 서빙 엔드는 서버를 나타낸다. 이동 전화가 신용 지불 기능을 인에이블할 때, 이동 전화 상의 신용 인가 시스템 애플리케이션, 이동 전화 상의 신용 지불 애플리케이션, 및 신용 인가 시스템의 서빙 엔드 사이의 절차는 다음의 단계들을 포함한다:

[0170] 단계(1001): 이동 전화의 디바이스 파라미터 정보를 획득한다.

[0171] 단계(1002): 디바이스 파라미터 정보를 업로드한다.

[0172] 단계(1003): 이동 전화가 신용 지불을 인에이블하기 위한 하드웨어 조건을 충족시키는지 여부를 결정한다.

[0173] 단계(1004): 결정 결과를 반환한다.

[0174] 단계(1005): 결정 결과는 신용 지불 애플리케이션 인에이블 페이지를 디스플레이하고 있다.

[0175] 단계(1006): 사용자 아이덴티티 정보를 업로드한다.

[0176] 단계(1007): 이동 전화가 신용 지불을 인에이블하기 위한 보안성 인증 조건을 충족시키는지 여부를 결정한다.

[0177] 단계(1008): 결정 결과를 반환한다.

[0178] 단계(1009): 사용자는 신용 지불 애플리케이션을 인에이블할 것을 선택한다.

[0179] 단계(1010): 신용 지불 애플리케이션을 활성화한다.

[0180] 단계(1011): 활성화 성공 결과를 반환한다.

[0181] 단계(1012): 애플리케이션 사설 키, 애플리케이션 공개 키 증명서, 및 신용 지불 데이터를 요청한다.

[0182] 단계(1013): 사설-공개 키 쌍을 생성하고, 신용-인가된 사설 키를 이용함으로써 애플리케이션 공개 키 증명서를 생성하고, 지불 카드 번호를 생성하고, 해싱(hashing)을 통해 애플리케이션 TAC 서브-키 및 신용 지불 데이터를 생성한다.

[0183] 단계(1014): 애플리케이션 사설 키, 애플리케이션 공개 키 증명서, 및 신용 지불 데이터를 반환한다.

[0184] 단계(1015): 애플리케이션 사설 키, 애플리케이션 공개 키 증명서, 및 신용 지불 데이터를 전송한다.

[0185] 단계(1016): 애플리케이션 사설 키, 애플리케이션 공개 키 증명서, 및 신용 지불 데이터를 저장한다.

[0186] 단계(1017): 개인화 결과를 반환한다.

[0187] 단계(1018): 신용 지불 인에이블 결과를 전송한다.

[0188] 단계(1019): 인에이블 결과를 레코딩한다.

[0189] 단계(1020): 프로세싱 완료 통지를 반환한다.

[0190] 단계(1021): 신용 지불 애플리케이션이 성공적으로 인에이블된다는 것을 표시하는 프롬프트(prompt)를 사용자에게 제공한다.

[0191] 본 개시내용에서 제공된 또 다른 구현예에서, 도 20에서 도시된 바와 같이, 본 개시내용은 이동 단말 P2P에 기초한 신용 지불 방법을 제공한다. 이동 단말이 지불 거래를 수행하는 프로세스에서, 이동 단말과 버스 게이트 사이의 데이터 교환 절차는 다음과 같다:

[0192] 단계(2001): SNEP-요청([카드 정보 판독] 겟)을 전송한다.

[0193] 단계(2002): 반환될 필요가 있는 데이터를 판독한다.

[0194] 단계(2003): SNEP-응답을 반환한다(지불 카드 번호, 이용가능한 한도, 진입/진출 플래그, 및 최후 거래에 대한 정보를 반환함).

[0195] 단계(2004): 블랙리스트 결정을 수행하고; 지불 카드 번호가 블랙리스트에서 존재할 경우, 거절 정보의 프롬프트를 제공한다.

[0196] 단계(2005): 이용가능한 한도 및 진입/진출 플래그를 검사하고; 이용가능한 한도 또는 진입/진출 플래그가 미리 결정된 조건을 충족시키지 않을 경우, 거절 정보의 프롬프트를 제공한다.

[0197] 단계(2006): SNEP-요청([애플리케이션 공개 키 증명서 판독] 겟)을 전송한다.

[0198] 단계(2007): SNEP-응답(애플리케이션 공개 키 증명서)을 반환한다.

[0199] 단계(2008): 신용 인가 시스템에서 저장된 공개 키를 판독하고, 애플리케이션 공개 키 증명서 상의 서명을 검증한다. 서명 검증이 실패할 경우, 거절 정보의 프롬프트를 제공한다. 서명 검증이 통과할 경우, 파싱(parsing)을 통해 애플리케이션 공개 키를 획득한다.

[0200] 단계(2009): 공제량을 계산한다.

[0201] 단계(2010): SNEP-요청((지불: 공제량, 거래 시간, 진입/진출 플래그, 및 (정지와 같은) 거래 정보) 풋)을 전송한다.

[0202] 단계(2011): 서명 데이터 및 TAC를 포함하는 지불 인가를 생성한다.

[0203] 단계(2012): 서명 데이터 및 TAC를 반환한다.

[0204] 단계(2013): 애플리케이션 공개 키를 이용함으로써 서명 데이터를 검증한다. 서명 검증이 통과할 경우, 거래

로그를 레코딩한다. 서명 검증이 실패할 경우, 거절 정보의 프롬프트를 제공한다.

[0205] 게다가, 도 21에서 도시된 바와 같이, 버스 게이트는 추가로, 거래 로그를 신용 인가 시스템으로 주기적으로 업로드하고 블랙리스트를 업데이트할 필요가 있다. 본 개시내용에서 제공된 이동 단말 P2P에 기초한 신용 지불 방법에서는, 버스 게이트(거래 단말)와 신용 인가 시스템의 서버 엔드 사이의 데이터 교환 절차가 다음과 같다:

[0206] 단계(3001): 거래 로그를 주기적으로 업로드한다.

[0207] 단계(3002): 정산을 수행하고, 시스템에서의 블랙리스트가 업데이트되는지 여부를 질의하고, 긍정일 경우, 블랙리스트를 반환할 것을 준비한다.

[0208] 단계(3003): 거래 로그 수신 결과 및 블랙리스트를 반환한다.

[0209] 단계(3004): 지불 카드 번호가 블랙리스트에서 존재하는지 여부를 검사한다.

[0210] 단계(3005): 버스 게이트는 블랙리스트를 업데이트한다.

[0211] 단계(3006): 업데이트한다.

[0212] 단계(3007): 업데이트된 완료 결과를 반환한다.

[0213] 버스 게이트 관리 시스템은 버스 게이트에서 위치될 수 있다.

[0214] 본 개시내용의 이전의 구현예들은 버스를 위한 신용 지불을 예로서 이용함으로써 설명된다. 이전의 구현예들은 또한, 오프라인 업무 지불 및 지하철 지불과 같은 다른 시나리오들에 적용될 수 있다는 것이 이해될 수 있다. 특정 적용 시나리오들에서의 상이한 구현예들이 있을 수 있다.

[0215] 이전의 방법 구현예들의 설명들을 이용함으로써, 당해 분야의 당업자는 본 개시내용이 소프트웨어 및 필요한 범용 하드웨어 플랫폼을 이용함으로써 구현될 수 있고, 하드웨어에 의해 구현될 수 있지만, 많은 상황들에서, 전자가 바람직한 구현예라는 것을 명확하게 이해할 수 있다. 이러한 이해에 기초하여, 본질적으로 본 개시내용의 기술적 해결책들, 또는 현존하는 기술에 기여하는 일부는 소프트웨어 제품의 형태로 구현될 수 있다. 컴퓨터 소프트웨어 제품은 저장 매체에서 저장되고, 본 개시내용의 구현예들에서 설명된 방법들의 단계들 중의 전부 또는 일부를 수행할 것을 (개인용 컴퓨터, 서버, 네트워크 디바이스 등일 수 있는) 컴퓨터 디바이스에 명령하기 위한 몇몇 명령어들을 포함한다. 저장 매체는 판독-전용 메모리(read-only memory; ROM), 랜덤 액세스 메모리(random access memory; RAM), 자기 디스크, 또는 광학 디스크와 같은, 프로그램 코드를 저장할 수 있는 임의의 매체를 포함한다.

[0216] 게다가, 이전의 구현예들의 구현예로서, 본 개시내용의 구현예는 이동 단말 P2P에 기초한 신용 지불 장치를 추가로 제공한다. 장치는 이동 단말에서 위치된다. 도 22에서 도시된 바와 같이, 장치는 제 1 반환 요청 정보 수신 유닛(10), 거래 응답 정보 생성 유닛(20), 정보 전송 유닛(30), 공제 수락 요청 정보 수신 유닛(40), 애플리케이션-사설-키-생성된 지불 인가 생성 유닛(50), 및 지불 인가 전송 유닛(60)을 포함한다.

[0217] 제 1 반환 요청 정보 수신 유닛(10)은 거래 단말에 의해 전송된 거래 정보를 수신하도록 구성된다.

[0218] 거래 응답 정보 생성 유닛(20)은 거래 정보에 기초하여 거래 응답 정보를 생성하도록 구성된다.

[0219] 정보 전송 유닛(30)은 거래 응답 정보를 거래 단말로 전송하도록 구성된다.

[0220] 공제 수락 요청 정보 수신 유닛(40)은 거래 단말에 의해 전송되는 현재의 공제 거래의 공제 수락 요청 정보를 수신하도록 구성된다.

[0221] 애플리케이션-사설-키-생성된 지불 인가 생성 유닛(50)은 공제 수락 요청 정보 및 거래 응답 정보에 기초하여 이동 단말에서 애플리케이션-사설-키-생성된 지불 인가를 생성하도록 구성된다.

[0222] 지불 인가 전송 유닛(60)은 거래 단말이 수신된 지불 인가에 기초하여 현재의 지불 거래를 완료하도록, 지불 인가를 거래 단말로 전송하도록 구성된다.

[0223] 본 개시내용의 또 다른 구현예에서는, 도 22에 기초하여, 도 23에서 도시된 바와 같이, 장치는 거래 단말에 의해 전송된 애플리케이션 공개 키 증명서 반환 요청 정보를 수신하도록 구성된 제 2 반환 요청 정보 수신 유닛(70); 애플리케이션 공개 키 증명서 반환 요청 정보에 기초하여 이동 단말에서 애플리케이션 공개 키 증명서에 대한 애플리케이션 공개 키 증명서 응답 정보를 생성하도록 구성된 애플리케이션 공개 키 증명서 응답 정보 생성 유닛(80); 및 애플리케이션 공개 키 증명서 응답 정보를 거래 단말로 전송하도록 구성된 공개 키 증명서 응

답 정보 전송 유닛(90)을 더 포함한다.

[0224] 본 개시내용의 또 다른 구현예에서는, 도 22에 기초하여, 도 24에서 도시된 바와 같이, 애플리케이션-사설-키-생성된 지불 인가 생성 유닛(50)은 이동 단말에서 저장된 애플리케이션 사설 키를 이용함으로써 공제 수락 요청 정보에 기초하여 서명 데이터를 생성하도록 구성된 서명 데이터 생성 모듈(51); 이동 단말 상에서 사전-생성되는 TAC 서브-키를 이용함으로써 공제 수락 요청 정보 및 거래 응답 정보에 기초하여 거래 인증 코드(TAC)를 생성하도록 구성된 정보 생성 모듈(52); 및 서명 데이터 및 TAC를 지불 인가로서 이용하도록 구성된 지불 인가 결정 모듈(53)을 포함한다.

[0225] 본 개시내용의 또 다른 구현예에서는, 도 22에 기초하여, 도 25에서 도시된 바와 같이, 장치는 현재의 이용가능한 한도를 획득하기 위하여, 공제 수락 요청 정보에서의 공제량에 기초하여 거래 정보에서의 이용가능한 한도로부터 공제량을 감산하도록 구성된 현재의 이용가능한 한도 생성 유닛(91); 및 현재의 이용가능한 한도를, 이동 단말에서의 사용자에 대응하는 이용가능한 한도로서 이용하도록 구성된 이용가능한 한도 결정 유닛(92)을 더 포함한다.

[0226] 본 개시내용의 구현예는 이동 단말 P2P에 기초한 신용 지불 장치를 추가로 제공한다. 장치는 거래 단말에서 위치된다. 도 26에서 도시된 바와 같이, 장치는 거래 정보 전송 유닛(11), 거래 응답 정보 수신 유닛(12), 공제 유닛(13), 공제 수락 요청 정보 전송 유닛(14), 및 현재의-지불-거래 완료 유닛(15)을 포함한다.

[0227] 거래 정보 전송 유닛(11)은 거래 정보를 이동 단말로 전송하도록 구성된다.

[0228] 거래 응답 정보 수신 유닛(12)은 이동 단말에 의해 전송된 거래 응답 정보를 수신하도록 구성된다.

[0229] 공제 유닛(13)은 거래 응답 정보에 기초하여 현재의 지불 거래 공제의 공제 수락 요청 정보를 생성하도록 구성된다.

[0230] 공제 수락 요청 정보 전송 유닛(14)은 공제 수락 요청 정보를 이동 단말로 전송하도록 구성된다.

[0231] 지불 거래 완료 유닛(15)은 지불 인가 라이센스가 수신될 때, 지불 인가 라이센스에 기초하여, 현재의 지불 거래가 완료되는 것으로 결정하도록 구성된다.

[0232] 본 개시내용의 또 다른 구현예에서는, 도 26에 기초하여, 도 27에서 도시된 바와 같이, 장치는 애플리케이션 공개 키 증명서 반환 요청 정보를 이동 단말로 전송하도록 구성된 반환 요청 정보 전송 유닛(16); 이동 단말에 의해 전송된 애플리케이션 공개 키 증명서 응답 정보를 수신하도록 구성된 공개 키 증명서 응답 정보 수신 유닛(17); 및 거래 단말에서 신용-라이센싱된 공개 키를 이용함으로써 애플리케이션 공개 키 증명서 응답 정보에서의 애플리케이션 공개 키 증명서 상의 서명을 검증하도록 구성된 서명 검증 유닛(18)을 더 포함한다.

[0233] 본 개시내용의 또 다른 구현예에서는, 도 26에 기초하여, 도 28에서 도시된 바와 같이, 장치는 블랙리스트 결정 유닛(191)을 더 포함한다.

[0234] 블랙리스트 결정 유닛(191)은 거래 응답 정보에서의 지불 카드 번호가 미리 결정된 블랙리스트 내에 포함되는지 여부를 결정하도록 구성된다.

[0235] 반환 요청 정보 전송 유닛(192)은, 거래 응답 정보에서의 지불 카드 번호가 미리 결정된 블랙리스트 내에 포함되지 않을 때, 애플리케이션 공개 키 증명서 반환 요청 정보를 이동 단말로 전송하도록 추가로 구성된다.

[0236] 본 개시내용의 또 다른 구현예에서는, 도 21에 기초하여, 도 29에서 도시된 바와 같이, 장치는 거래 응답 정보에서의 이용가능한 한도가 미리 결정된 임계치 이상인지 여부를 결정하도록 구성된 임계치 결정 유닛(193); 및 이용가능한 한도가 미리 결정된 임계치 이상일 경우, 거래 응답 정보에서의 진입/진출 플래그가 진출된 상태인지 여부를 검사하도록 구성된 스테이터스 검사 유닛(194)을 더 포함한다.

[0237] 본 개시내용의 또 다른 구현예에서는, 도 26에 기초하여, 도 30에서 도시된 바와 같이, 지불 인가 라이센스는 서명 데이터 및 거래 인증 코드(TAC)를 포함하고, 현재의 지불 거래 완료 유닛(15)은 애플리케이션 공개 키를 이용함으로써 서명 데이터를 검증하도록 구성된 서명 검증 모듈(151); 서명 데이터가 검증될 때, 거래 로그를 생성하도록 구성된 거래 로그 생성 모듈(152); 및 미리 결정된 서버가 거래 로그 - 거래 로그는 공제량, 거래 날짜, 거래 순간, 거래 단말 ID, 지불 카드 번호, 이용가능한 한도, 및 TAC를 포함함 - 에 기초하여, 이동 단말에 대응하는 사용자 계좌로부터 자금의 대응하는 양을 공제하도록, 거래 로그를 미리 결정된 서버로 전송하도록 구성된 거래 로그 전송 모듈(153)을 포함한다.

[0238] 장치 구현예들에 관하여, 각각의 모듈이 동작하는 특정 방식은 대응하는 방법 구현예들에서 상세하게 설명되었고, 세부사항들은 단순화를 위하여 여기에서 반복되지 않는다.

[0239] 본 개시내용은 많은 일반-목적 또는 특수 목적 컴퓨터 시스템 환경들 또는 구성들에 적용될 수 있다는 것이 이해될 수 있다. 예를 들어, 개인용 컴퓨터, 서버 컴퓨터, 핸드헬드 디바이스 또는 휴대용 디바이스, 평판 패널 디바이스, 멀티-프로세서 시스템, 마이크로프로세서-기반 시스템, 셋톱 박스, 프로그래밍가능한 소비 전자 디바이스, 네트워크 PC, 미니컴퓨터, 메인프레임 컴퓨터, 및 이전의 시스템들 또는 디바이스들 중의 임의의 하나를 포함하는 분산된 컴퓨팅 환경.

[0240] 본 개시내용은 컴퓨터, 예를 들어, 프로그램 모듈에 의해 실행된 명령어들의 일반적인 맥락에서 설명될 수 있다. 일반적으로, 프로그램 모듈은 특정한 태스크를 실행하거나 특정한 추상적인 데이터 타입을 구현하기 위한 루틴, 프로그램, 객체, 컴포넌트, 데이터 구조 등을 포함한다. 본 개시내용은 또한, 분산된 컴퓨팅 환경들에서 실시될 수 있다. 분산된 컴퓨팅 환경들에서, 태스크들은 통신 네트워크를 통해 접속되는 원격 프로세싱 디바이스들에 의해 실행된다. 분산된 컴퓨팅 환경에서, 프로그램 모듈은 저장 디바이스들을 포함하는 로컬 및 원격 컴퓨터 저장 매체들의 양자에서 위치될 수 있다.

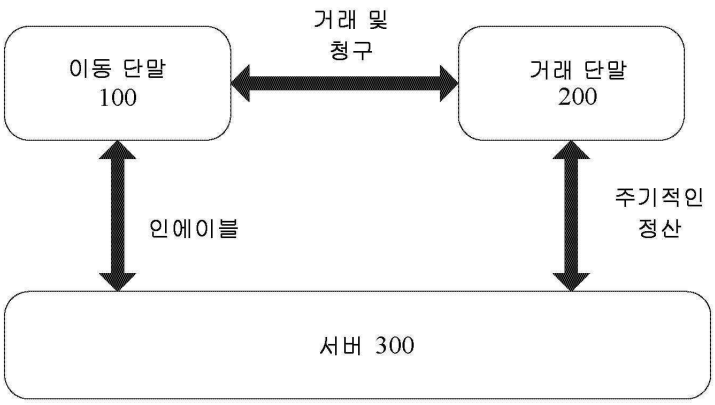
[0241] 명세서에서, "제 1" 및 "제 2"와 같은 관계 용어들은 또 다른 것으로부터 하나의 엔티티 또는 동작을 구별하기 위하여 오직 이용되고, 임의의 실제적인 관계 또는 순서가 이 엔티티들 또는 동작들 사이에서 존재한다는 것을 반드시 요구하거나 암시하지는 않는다는 것을 주목할 가치가 있다. 게다가, 용어들 "포함한다(include)", "포함한다(comprise)", 또는 그 임의의 다른 변종은 비-배타적 포함을 포괄하도록 의도된 것이어서, 구성요소들의 리스트를 포함하는 프로세스, 방법, 물품, 또는 디바이스는 그 구성요소들을 포함할 뿐만 아니라, 명백히 열거되지 않은 다른 구성요소들을 포함하거나, 이러한 프로세스, 방법, 물품, 또는 디바이스에 내재하는 구성요소들을 더 포함한다. "~을 포함한다(includes a…)"에 의해 설명된 구성요소는 구성요소를 포함하는 프로세스, 방법, 물품, 또는 디바이스에서의 또 다른 동일한 구성요소를 더 많은 제약들 없이 더 포함한다.

[0242] 당해 분야의 당업자는 명세서를 고려하고 여기에서 개시되는 본 개시내용을 실시한 후에, 본 개시내용의 다른 구현 해결책들을 용이하게 생각해낼 수 있다. 본 출원은 본 개시내용의 임의의 변동, 기능, 또는 적응적 변경을 포괄하도록 의도된다. 이 변동들, 기능들, 또는 적응적 변경들은 본 개시내용의 일반적인 원리들을 준수하고, 본 개시내용에서 개시되지 않은 기술 분야에서의 보편적인 지식 또는 보편적으로 이용된 기술적 수단을 포함한다. 명세서 및 구현예들은 단지 예들로서 고려되고, 본 개시내용의 실제적인 범위 및 사상은 다음의 청구항들에 의해 지적된다.

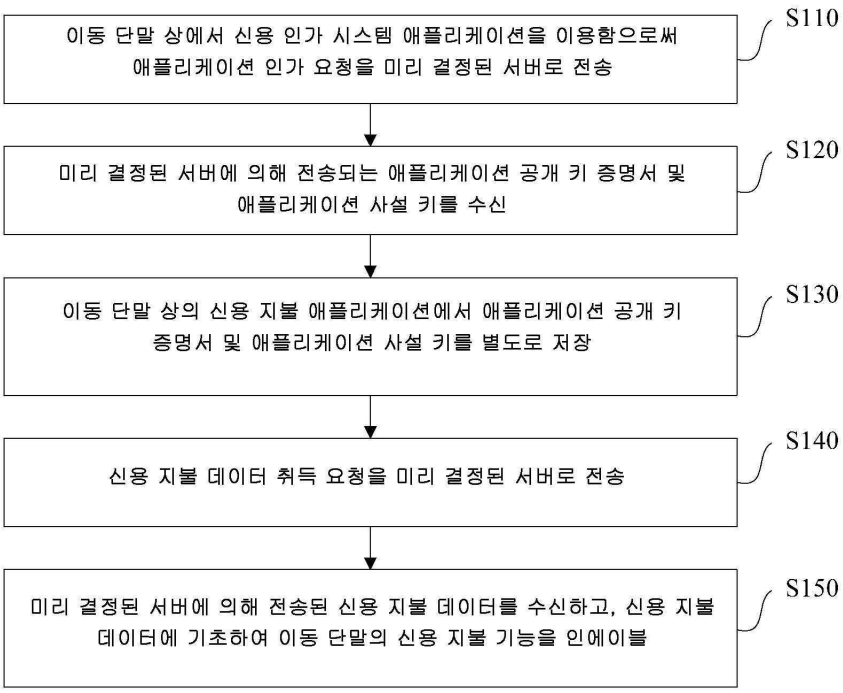
[0243] 본 개시내용은 위에서 설명되고 동반되는 도면들에서 도시되는 정확한 구조들로 제한되지 않고, 수정들 및 변경들은 본 개시내용의 범위로부터 이탈하지 않으면서 행해질 수 있다는 것이 이해되어야 한다. 본 개시내용의 범위는 첨부된 청구항들에 의해 오직 제한된다.

도면

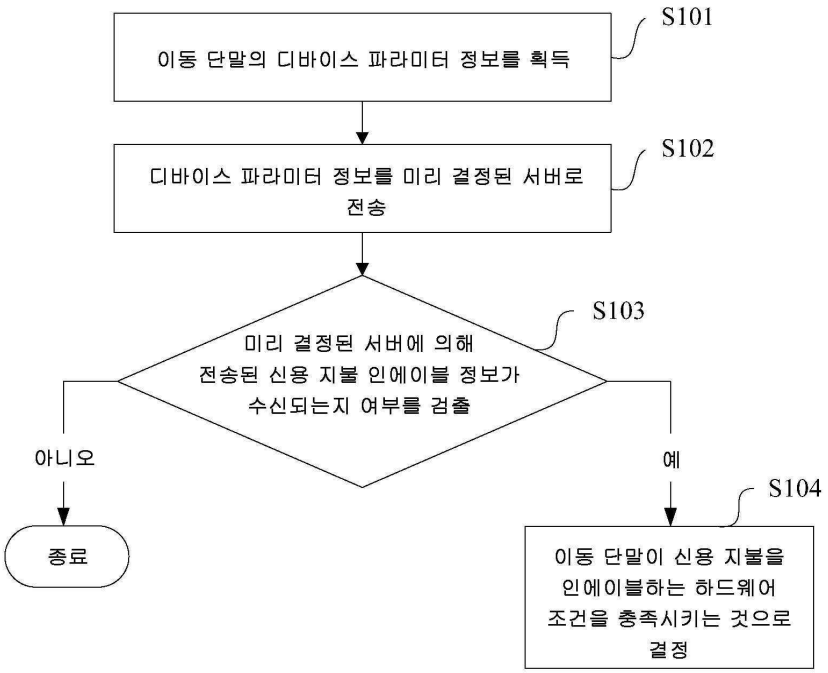
도면1



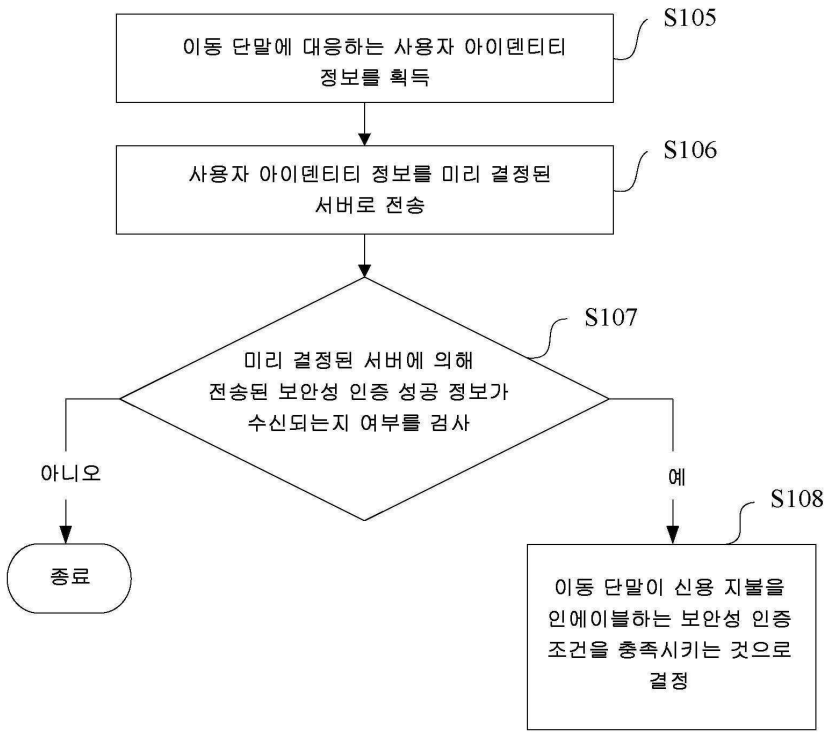
도면2


이동 단말 상에서 신용 인가 시스템 애플리케이션을 이용함으로써 애플리케이션 인가 요청을 미리 결정된 서버로 전송
S110
미리 결정된 서버에 의해 전송되는 애플리케이션 공개 키 증명서 및 애플리케이션 사설 키를 수신
S120
이동 단말 상의 신용 지불 애플리케이션에서 애플리케이션 공개 키 증명서 및 애플리케이션 사설 키를 별도로 저장
S130
신용 지불 데이터 취득 요청을 미리 결정된 서버로 전송
S140
미리 결정된 서버에 의해 전송된 신용 지불 데이터를 수신하고, 신용 지불 데이터에 기초하여 이동 단말의 신용 지불 기능을 인에이블
S150

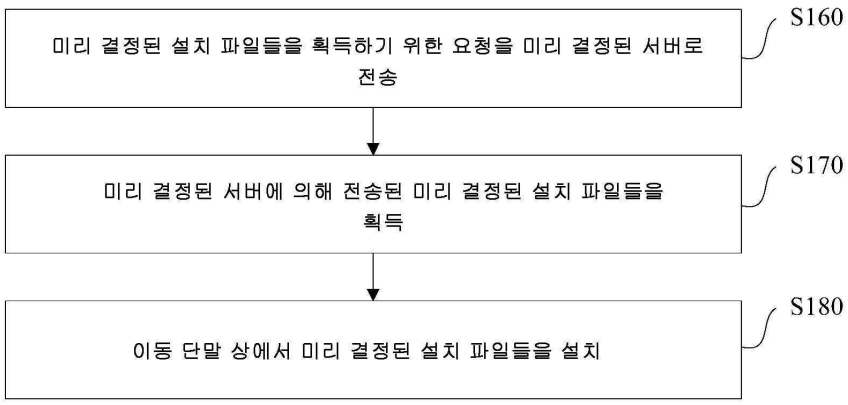
도면3


이동 단말의 디바이스 파라미터 정보를 획득
S101
디바이스 파라미터 정보를 미리 결정된 서버로 전송
S102
미리 결정된 서버에 의해 전송된 신용 지불 인에이블 정보가 수신되는지 여부를 검출
S103
아니오
예
종료
이동 단말이 신용 지불을 인에이블하는 하드웨어 조건을 충족시키는 것으로 결정
S104

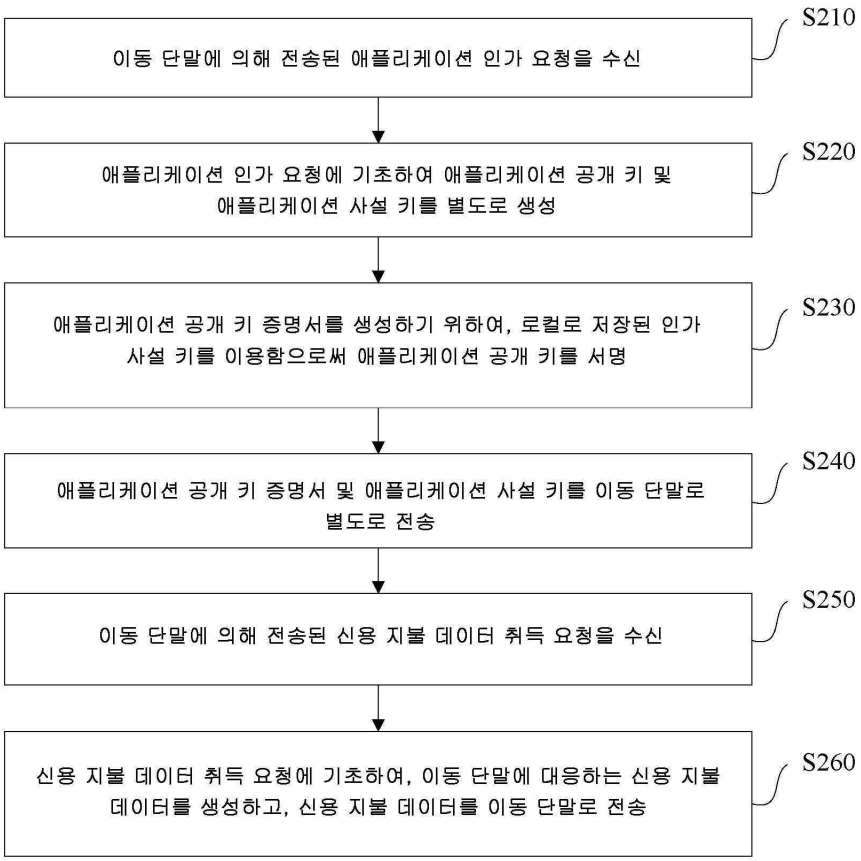
도면4


이동 단말에 대응하는 사용자 아이덴티티 정보를 획득
S105
사용자 아이덴티티 정보를 미리 결정된 서버로 전송
S106
미리 결정된 서버에 의해 전송된 보안성 인증 성공 정보가 수신되는지 여부를 검사
S107
아니오
예
종료
S108
이동 단말이 신용 지불을 인에이블하는 보안성 인증 조건을 충족시키는 것으로 결정

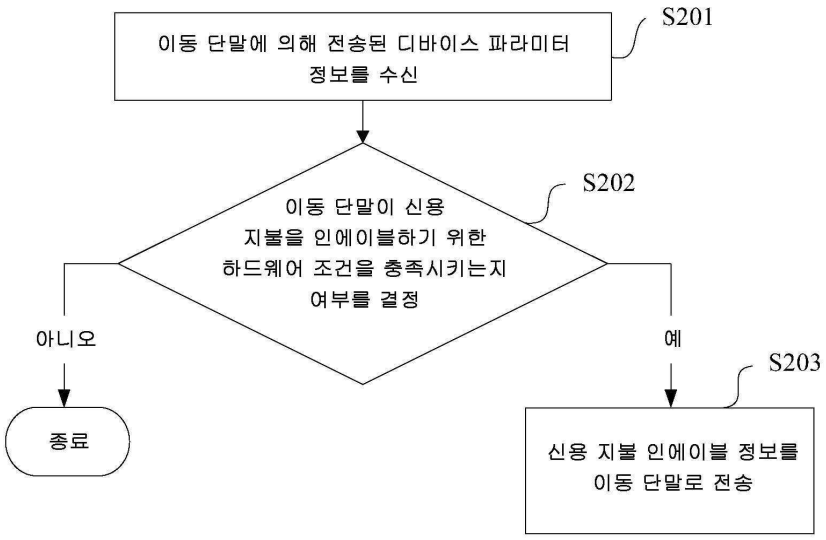
도면5


미리 결정된 설치 파일들을 획득하기 위한 요청을 미리 결정된 서버로 전송
S160
미리 결정된 서버에 의해 전송된 미리 결정된 설치 파일들을 획득
S170
이동 단말 상에서 미리 결정된 설치 파일들을 설치
S180

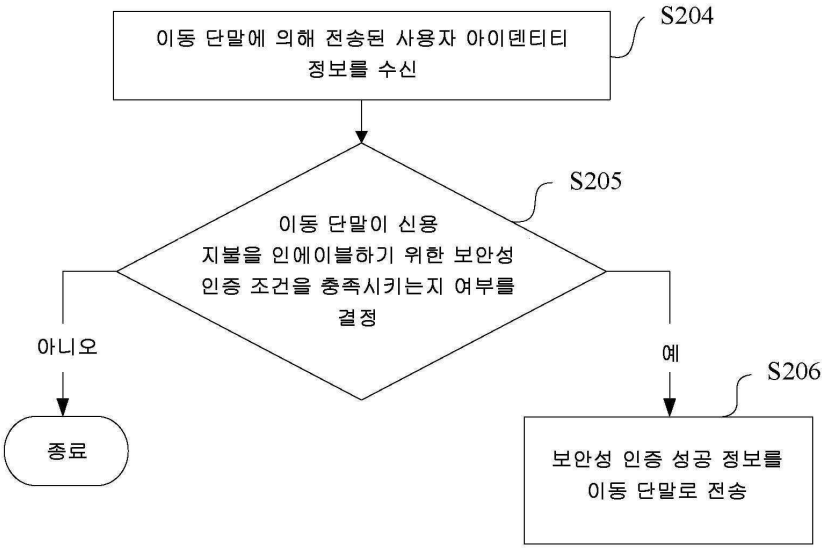
도면6


이동 단말에 의해 전송된 애플리케이션 인가 요청을 수신
S210
애플리케이션 인가 요청에 기초하여 애플리케이션 공개 키 및 애플리케이션 사설 키를 별도로 생성
S220
애플리케이션 공개 키 증명서를 생성하기 위하여, 로컬로 저장된 인가 사설 키를 이용함으로써 애플리케이션 공개 키를 서명
S230
애플리케이션 공개 키 증명서 및 애플리케이션 사설 키를 이동 단말로 별도로 전송
S240
이동 단말에 의해 전송된 신용 지불 데이터 취득 요청을 수신
S250
신용 지불 데이터 취득 요청에 기초하여, 이동 단말에 대응하는 신용 지불 데이터를 생성하고, 신용 지불 데이터를 이동 단말로 전송
S260

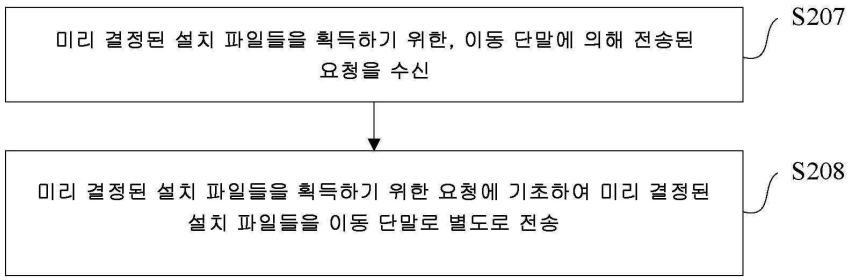
도면7


이동 단말에 의해 전송된 디바이스 파라미터 정보를 수신
S201
이동 단말이 신용 지불을 인에이블하기 위한 하드웨어 조건을 충족시키는지 여부를 결정
S202
아니오
예
종료
S203
신용 지불 인에이블 정보를 이동 단말로 전송

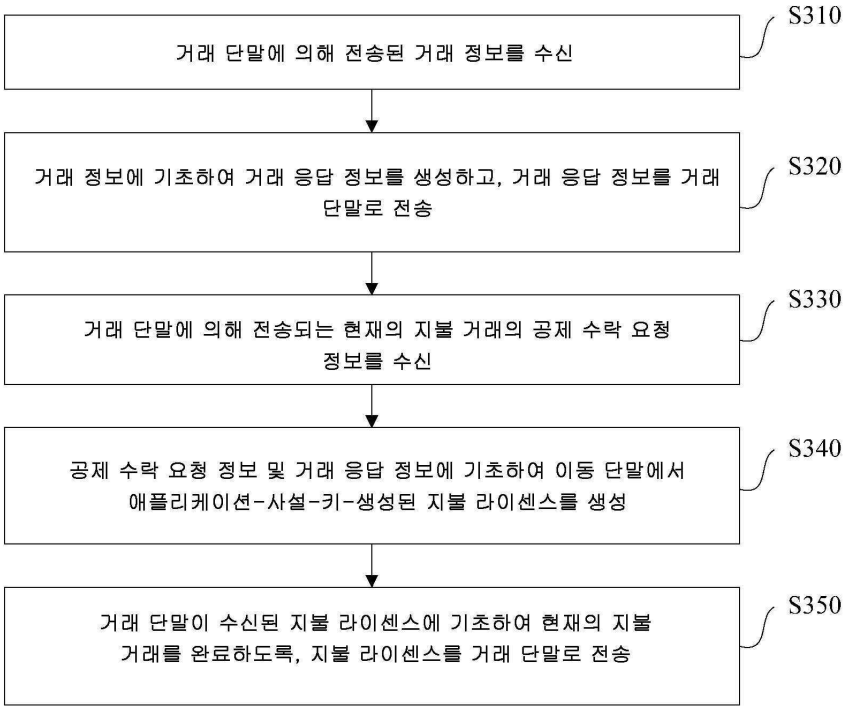
도면8


이동 단말에 의해 전송된 사용자 아이덴티티 정보를 수신
S204
이동 단말이 신용 지불을 인에이블하기 위한 보안성 인증 조건을 충족시키는지 여부를 결정
S205
아니오
예
종료
보안성 인증 성공 정보를 이동 단말로 전송
S206

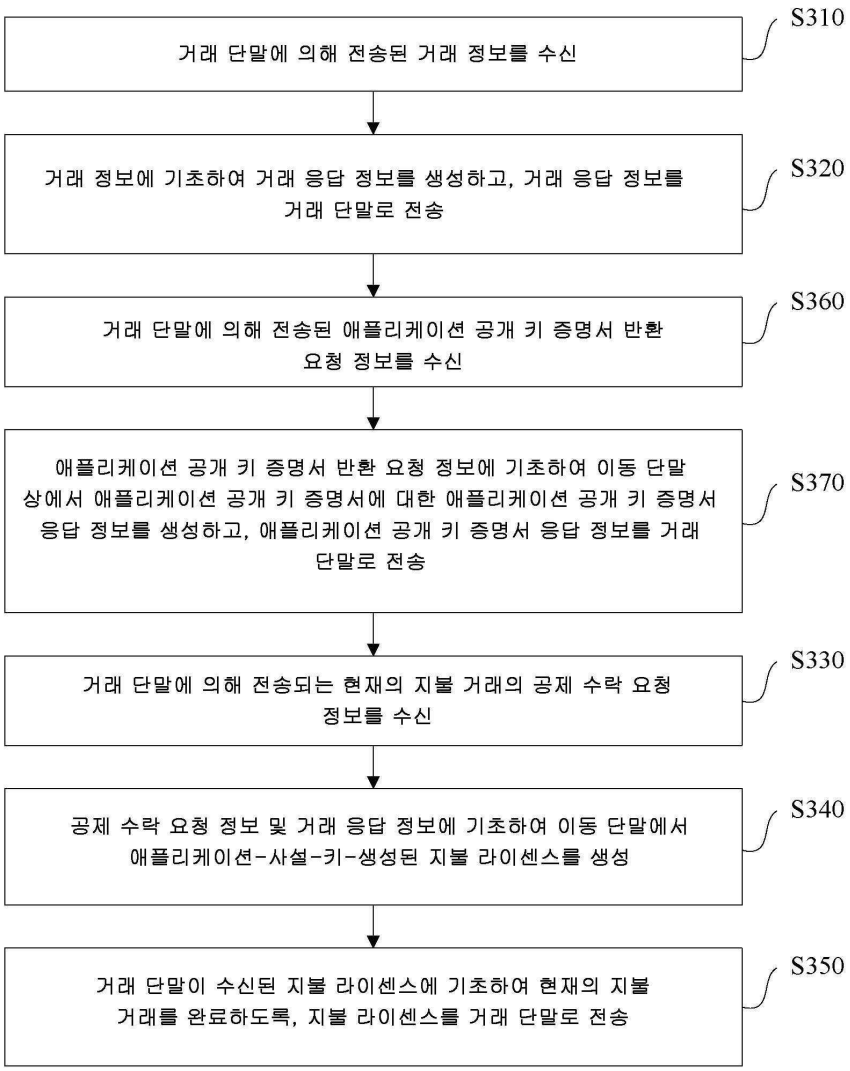
도면9


미리 결정된 설치 파일들을 획득하기 위한, 이동 단말에 의해 전송된 요청을 수신
S207
미리 결정된 설치 파일들을 획득하기 위한 요청에 기초하여 미리 결정된 설치 파일들을 이동 단말로 별도로 전송
S208

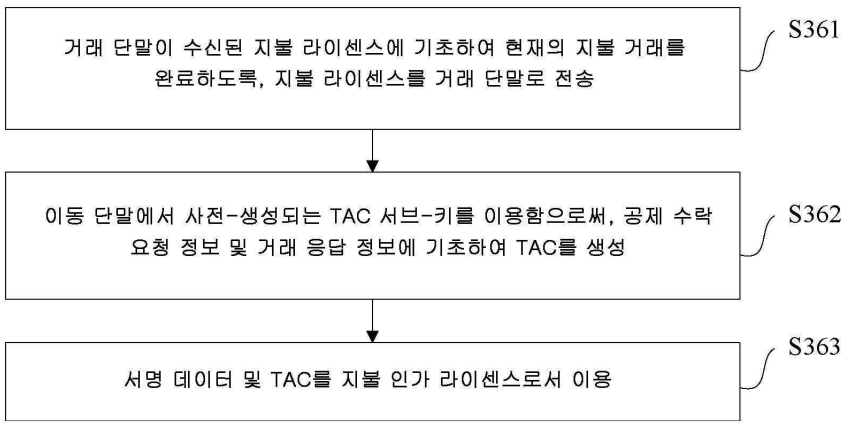
도면10


거래 단말에 의해 전송된 거래 정보를 수신
S310
거래 정보에 기초하여 거래 응답 정보를 생성하고, 거래 응답 정보를 거래 단말로 전송
S320
거래 단말에 의해 전송되는 현재의 지불 거래의 공제 수락 요청 정보를 수신
S330
공제 수락 요청 정보 및 거래 응답 정보에 기초하여 이동 단말에서 애플리케이션-사설-키-생성된 지불 라이센스를 생성
S340
거래 단말이 수신된 지불 라이센스에 기초하여 현재의 지불 거래를 완료하도록, 지불 라이센스를 거래 단말로 전송
S350

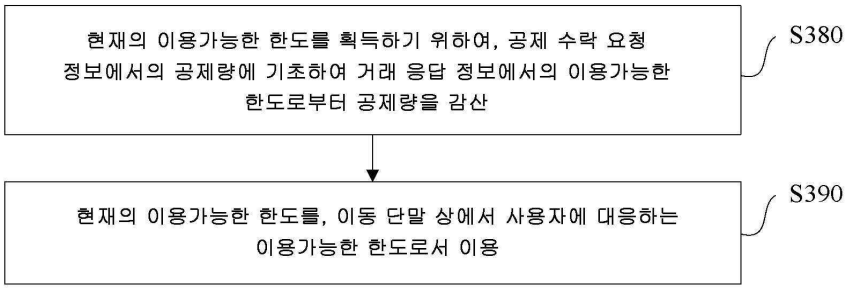
도면11


S310
거래 단말에 의해 전송된 거래 정보를 수신
S320
거래 정보에 기초하여 거래 응답 정보를 생성하고, 거래 응답 정보를 거래 단말로 전송
S360
거래 단말에 의해 전송된 애플리케이션 공개 키 증명서 반환 요청 정보를 수신
S370
애플리케이션 공개 키 증명서 반환 요청 정보에 기초하여 이동 단말 상에서 애플리케이션 공개 키 증명서에 대한 애플리케이션 공개 키 증명서 응답 정보를 생성하고, 애플리케이션 공개 키 증명서 응답 정보를 거래 단말로 전송
S330
거래 단말에 의해 전송되는 현재의 지불 거래의 공제 수락 요청 정보를 수신
S340
공제 수락 요청 정보 및 거래 응답 정보에 기초하여 이동 단말에서 애플리케이션-사설-키-생성된 지불 라이센스를 생성
S350
거래 단말이 수신된 지불 라이센스에 기초하여 현재의 지불 거래를 완료하도록, 지불 라이센스를 거래 단말로 전송

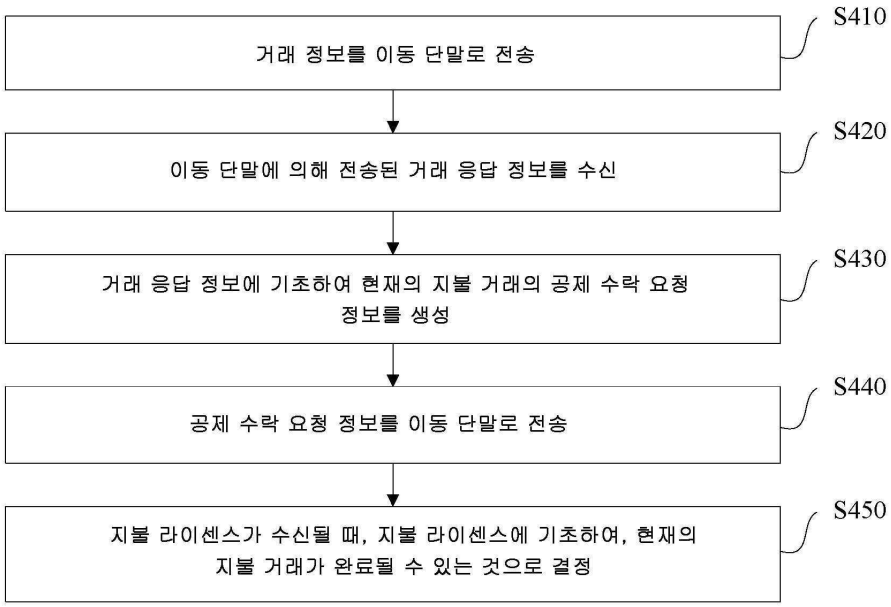
도면12


S361
거래 단말이 수신된 지불 라이센스에 기초하여 현재의 지불 거래를 완료하도록, 지불 라이센스를 거래 단말로 전송
S362
이동 단말에서 사전-생성되는 TAC 서브-키를 이용함으로써, 공제 수락 요청 정보 및 거래 응답 정보에 기초하여 TAC를 생성
S363
서명 데이터 및 TAC를 지불 인가 라이센스로서 이용

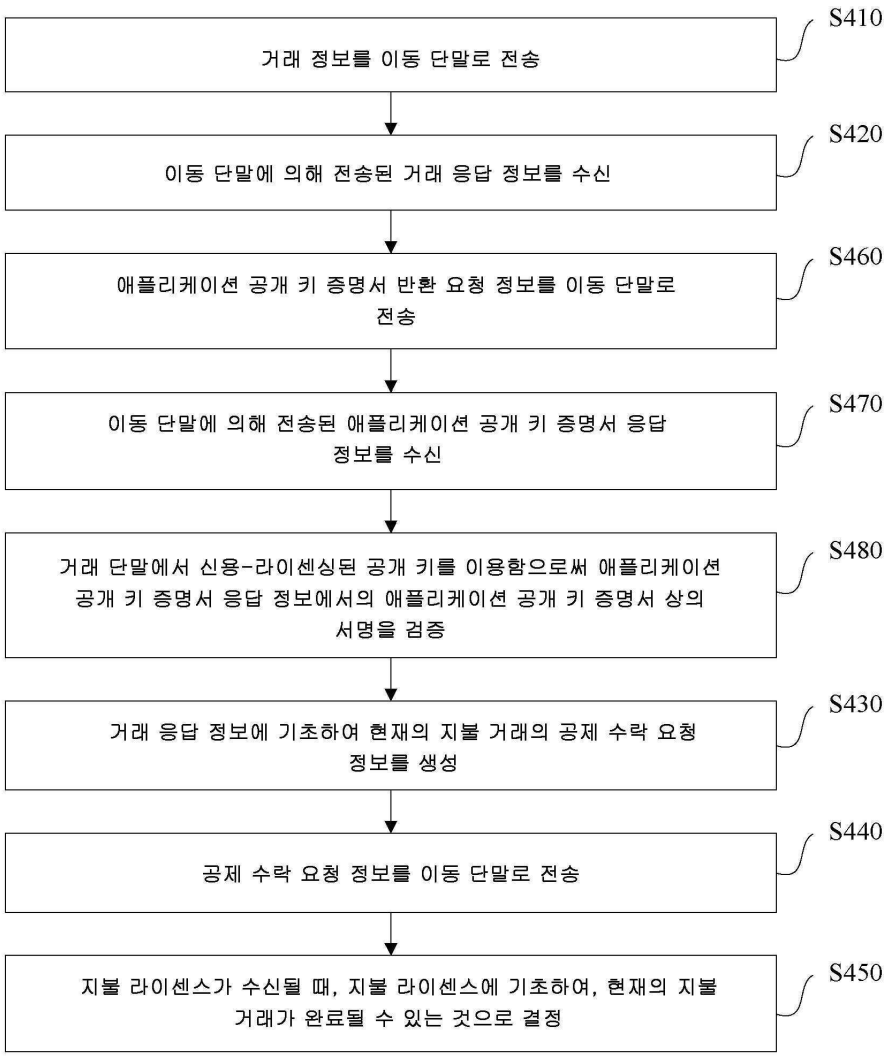
도면13


현재의 이용가능한 한도를 획득하기 위하여, 공제 수락 요청 정보에서의 공제량에 기초하여 거래 응답 정보에서의 이용가능한 한도로부터 공제량을 감산
S380
현재의 이용가능한 한도를, 이동 단말 상에서 사용자에 대응하는 이용가능한 한도로서 이용
S390

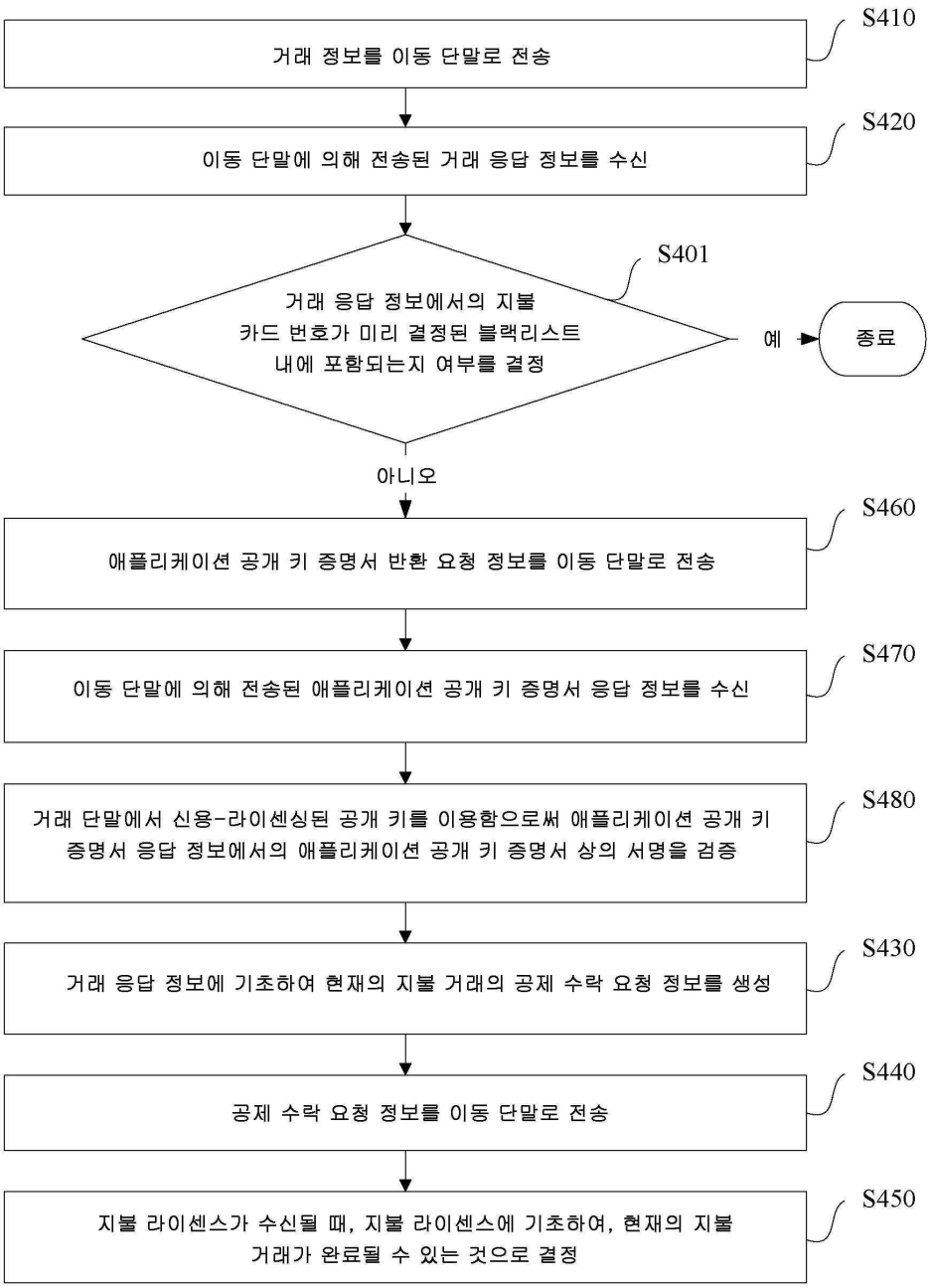
도면14


거래 정보를 이동 단말로 전송
S410
이동 단말에 의해 전송된 거래 응답 정보를 수신
S420
거래 응답 정보에 기초하여 현재의 지불 거래의 공제 수락 요청 정보를 생성
S430
공제 수락 요청 정보를 이동 단말로 전송
S440
지불 라이센스가 수신될 때, 지불 라이센스에 기초하여, 현재의 지불 거래가 완료될 수 있는 것으로 결정
S450

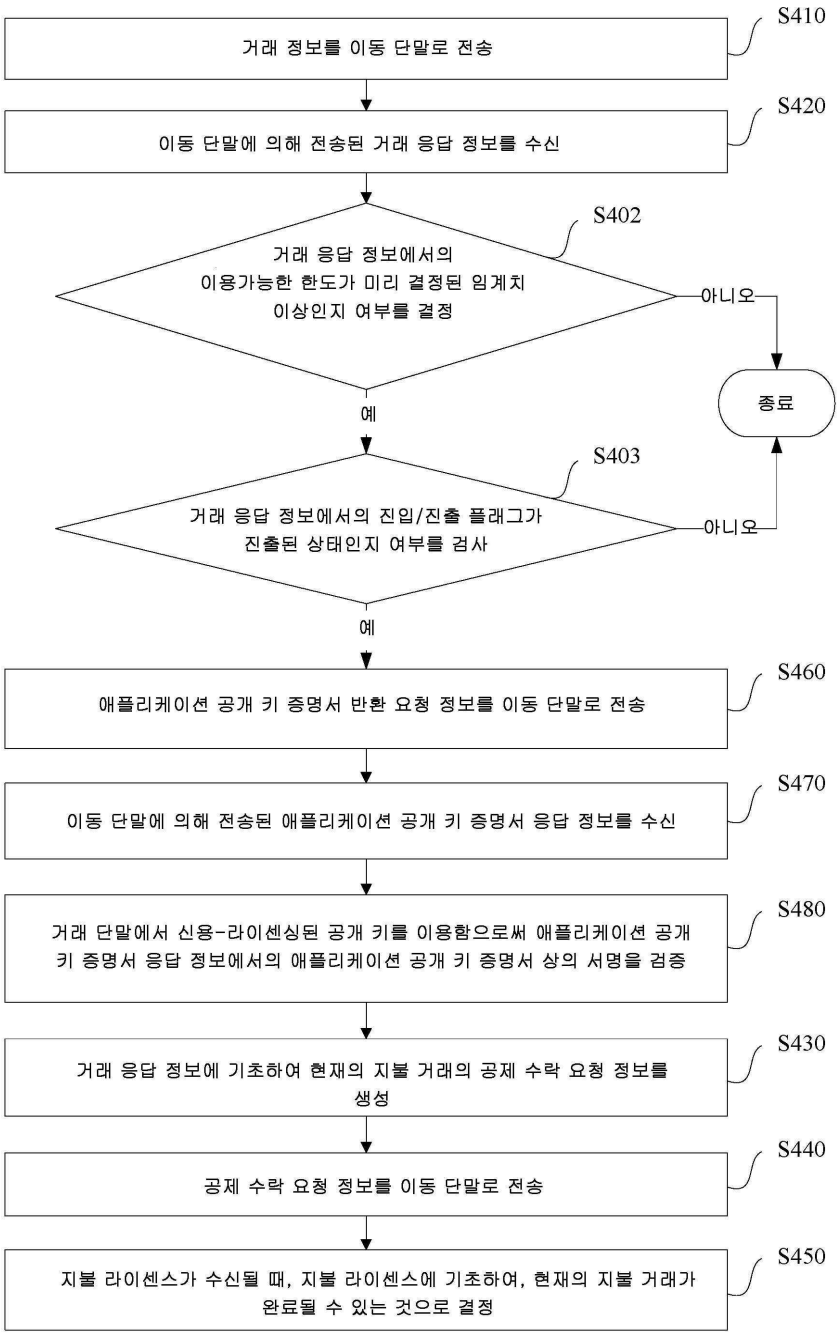
도면15


거래 정보를 이동 단말로 전송
S410
이동 단말에 의해 전송된 거래 응답 정보를 수신
S420
애플리케이션 공개 키 증명서 반환 요청 정보를 이동 단말로 전송
S460
이동 단말에 의해 전송된 애플리케이션 공개 키 증명서 응답 정보를 수신
S470
거래 단말에서 신용-라이센싱된 공개 키를 이용함으로써 애플리케이션 공개 키 증명서 응답 정보에서의 애플리케이션 공개 키 증명서 상의 서명을 검증
S480
거래 응답 정보에 기초하여 현재의 지불 거래의 공제 수락 요청 정보를 생성
S430
공제 수락 요청 정보를 이동 단말로 전송
S440
지불 라이센스가 수신될 때, 지불 라이센스에 기초하여, 현재의 지불 거래가 완료될 수 있는 것으로 결정
S450

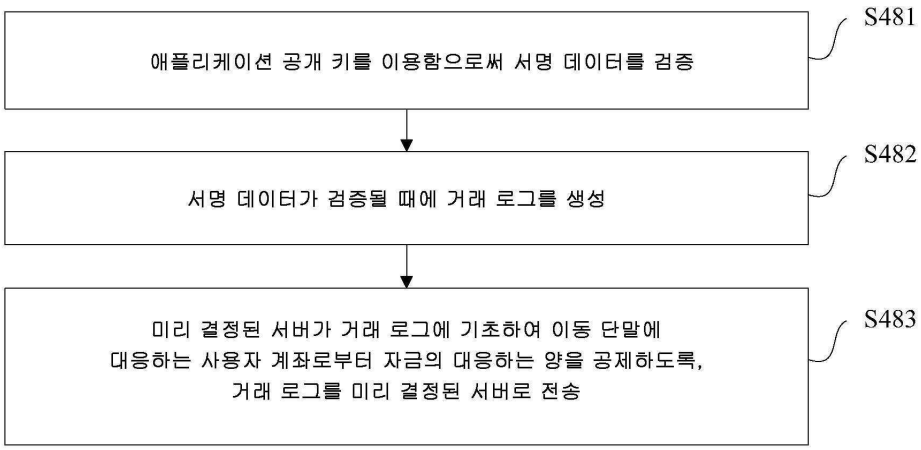
도면16


S410
거래 정보를 이동 단말로 전송
S420
이동 단말에 의해 전송된 거래 응답 정보를 수신
S401
거래 응답 정보에서의 지불
카드 번호가 미리 결정된 블랙리스트
내에 포함되는지 여부를 결정
예
종료
아니오
S460
애플리케이션 공개 키 증명서 반환 요청 정보를 이동 단말로 전송
S470
이동 단말에 의해 전송된 애플리케이션 공개 키 증명서 응답 정보를 수신
S480
거래 단말에서 신용-라이센싱된 공개 키를 이용함으로써 애플리케이션 공개 키
증명서 응답 정보에서의 애플리케이션 공개 키 증명서 상의 서명을 검증
S430
거래 응답 정보에 기초하여 현재의 지불 거래의 공제 수락 요청 정보를 생성
S440
공제 수락 요청 정보를 이동 단말로 전송
S450
지불 라이센스가 수신될 때, 지불 라이센스에 기초하여, 현재의 지불
거래가 완료될 수 있는 것으로 결정

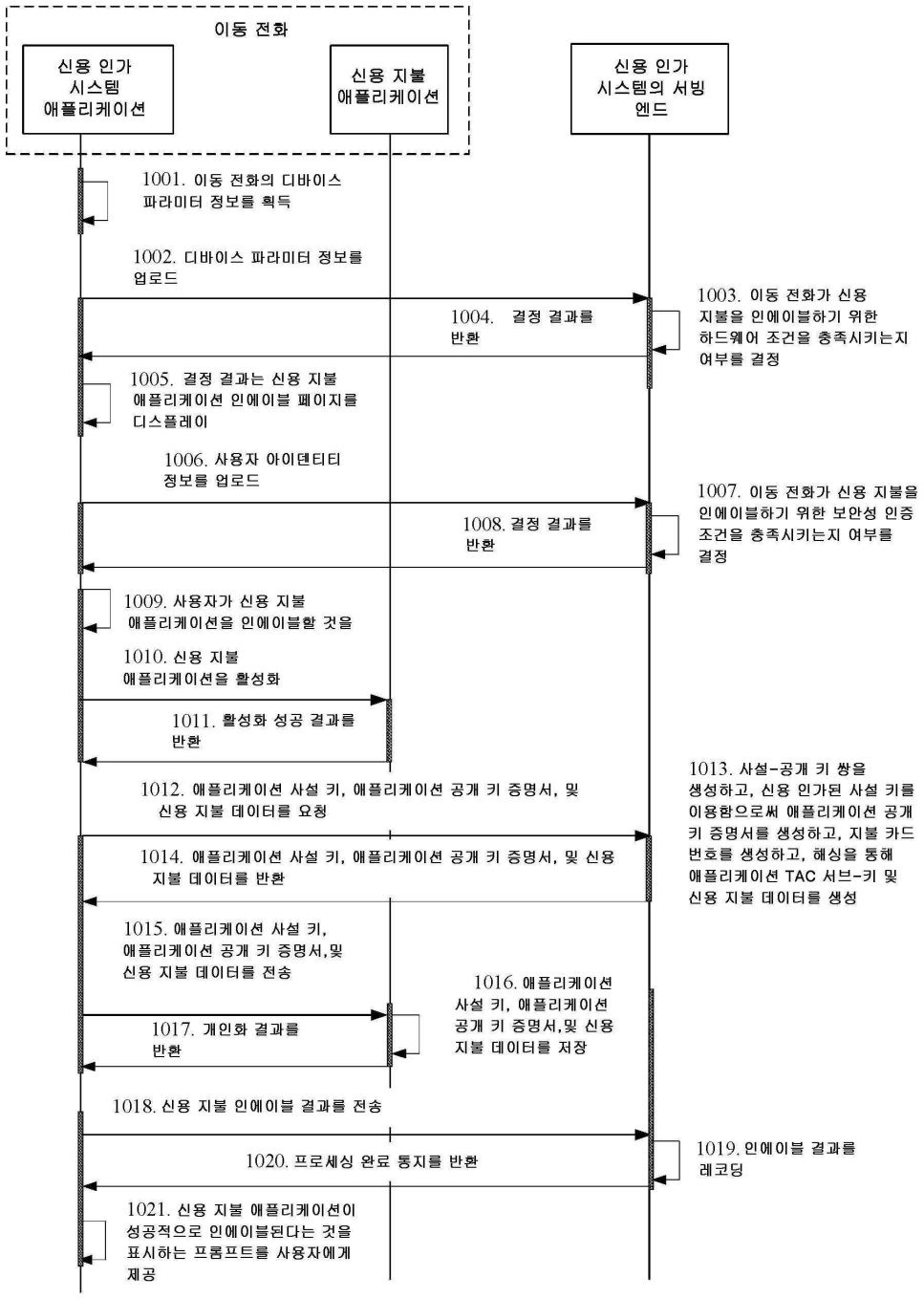
도면17


S410
거래 정보를 이동 단말로 전송
S420
이동 단말에 의해 전송된 거래 응답 정보를 수신
S402
거래 응답 정보에서의
이용가능한 한도가 미리 결정된 임계치
이상인지 여부를 결정
아니오
종료
예
S403
거래 응답 정보에서의 진입/진출 플래그가
진출된 상태인지 여부를 검사
아니오
예
S460
애플리케이션 공개 키 증명서 반환 요청 정보를 이동 단말로 전송
S470
이동 단말에 의해 전송된 애플리케이션 공개 키 증명서 응답 정보를 수신
S480
거래 단말에서 신용-라이센싱된 공개 키를 이용함으로써 애플리케이션 공개
키 증명서 응답 정보에서의 애플리케이션 공개 키 증명서 상의 서명을 검증
S430
거래 응답 정보에 기초하여 현재의 지불 거래의 공제 수락 요청 정보를
생성
S440
공제 수락 요청 정보를 이동 단말로 전송
S450
지불 라이센스가 수신될 때, 지불 라이센스에 기초하여, 현재의 지불 거래가
완료될 수 있는 것으로 결정

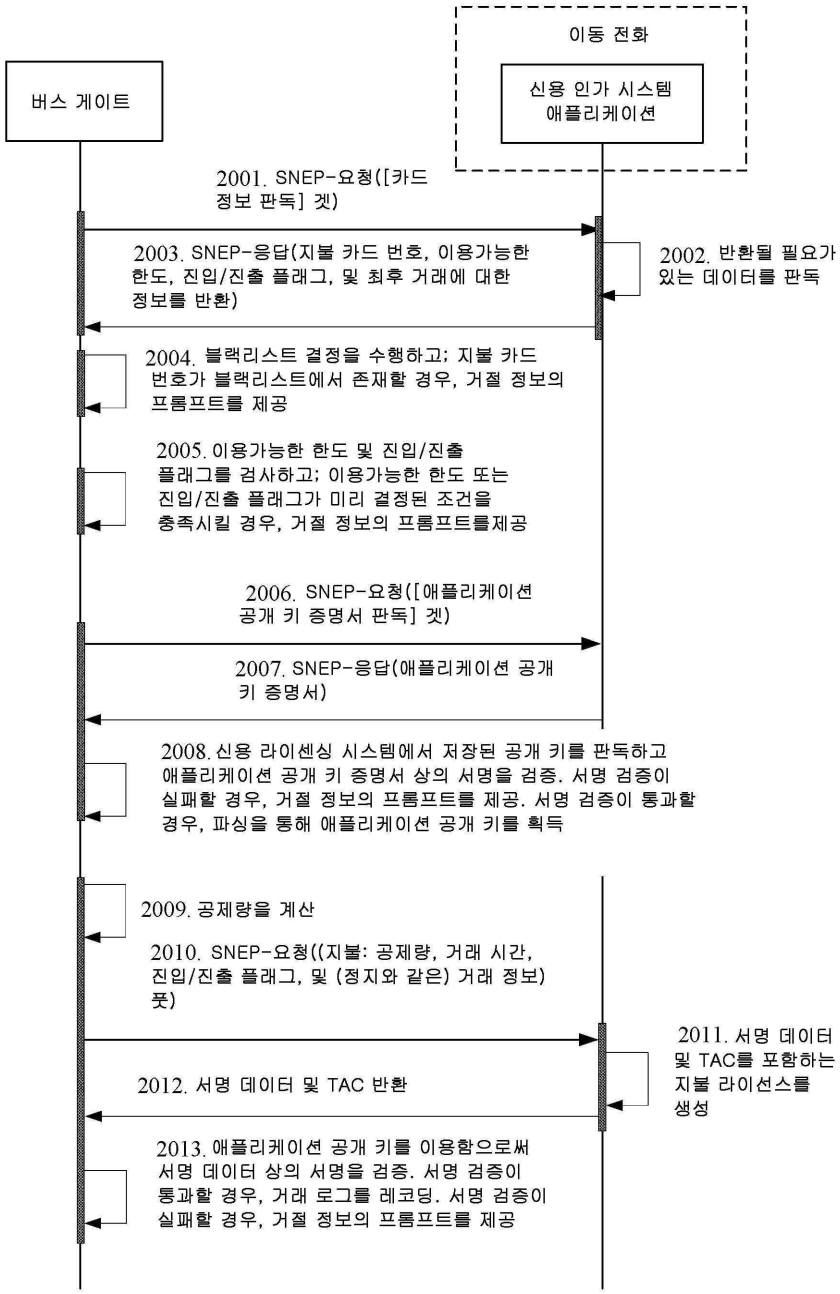
도면18


애플리케이션 공개 키를 이용함으로써 서명 데이터를 검증
S481
서명 데이터가 검증될 때에 거래 로그를 생성
S482
미리 결정된 서버가 거래 로그에 기초하여 이동 단말에
대응하는 사용자 계좌로부터 자금의 대응하는 양을 공제하도록,
거래 로그를 미리 결정된 서버로 전송
S483

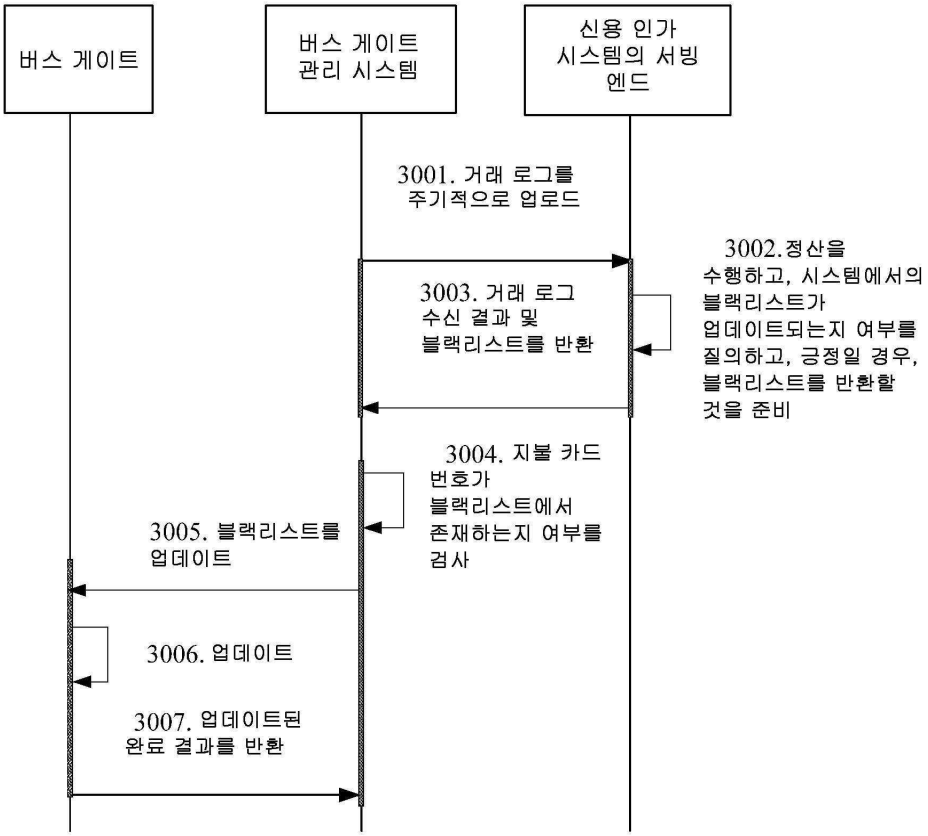
도면19


이동 전화
신용 인가 시스템 애플리케이션
신용 지불 애플리케이션
신용 인가 시스템의 서빙 엔드
1001. 이동 전화의 디바이스 파라미터 정보를 획득
1002. 디바이스 파라미터 정보를 업로드
1003. 이동 전화가 신용 지불을 인에이블하기 위한 하드웨어 조건을 충족시키는지 여부를 결정
1004. 결정 결과를 반환
1005. 결정 결과는 신용 지불 애플리케이션 인에이블 페이지를 디스플레이
1006. 사용자 아이덴티티 정보를 업로드
1007. 이동 전화가 신용 지불을 인에이블하기 위한 보안성 인증 조건을 충족시키는지 여부를 결정
1008. 결정 결과를 반환
1009. 사용자가 신용 지불 애플리케이션을 인에이블할 것을
1010. 신용 지불 애플리케이션을 활성화
1011. 활성화 성공 결과를 반환
1012. 애플리케이션 사설 키, 애플리케이션 공개 키 증명서, 및 신용 지불 데이터를 요청
1013. 사설-공개 키 쌍을 생성하고, 신용 인가된 사설 키를 이용함으로써 애플리케이션 공개 키 증명서를 생성하고, 지불 카드 번호를 생성하고, 해싱을 통해 애플리케이션 TAC 서브-키 및 신용 지불 데이터를 생성
1014. 애플리케이션 사설 키, 애플리케이션 공개 키 증명서, 및 신용 지불 데이터를 반환
1015. 애플리케이션 사설 키, 애플리케이션 공개 키 증명서,및 신용 지불 데이터를 전송
1016. 애플리케이션 사설 키, 애플리케이션 공개 키 증명서,및 신용 지불 데이터를 저장
1017. 개인화 결과를 반환
1018. 신용 지불 인에이블 결과를 전송
1019. 인에이블 결과를 레코딩
1020. 프로세싱 완료 통지를 반환
1021. 신용 지불 애플리케이션이 성공적으로 인에이블된다는 것을 표시하는 프롬프트를 사용자에게 제공

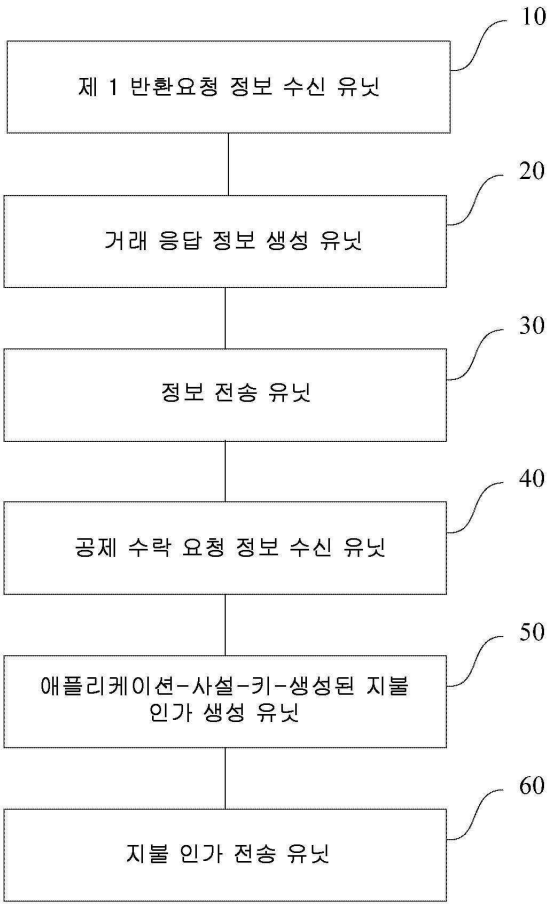
도면20


이동 전화
신용 인가 시스템 애플리케이션
버스 게이트
2001. SNEP-요청([카드 정보 판독] 겟)
2003. SNEP-응답(지불 카드 번호, 이용가능한 한도, 진입/진출 플래그, 및 최후 거래에 대한 정보를 반환)
2002. 반환될 필요가 있는 데이터를 판독
2004. 블랙리스트 결정을 수행하고; 지불 카드 번호가 블랙리스트에서 존재할 경우, 거절 정보의 프롬프트를 제공
2005. 이용가능한 한도 및 진입/진출 플래그를 검사하고; 이용가능한 한도 또는 진입/진출 플래그가 미리 결정된 조건을 충족시킬 경우, 거절 정보의 프롬프트를제공
2006. SNEP-요청([애플리케이션 공개 키 증명서 판독] 겟)
2007. SNEP-응답(애플리케이션 공개 키 증명서)
2008. 신용 라이센싱 시스템에서 저장된 공개 키를 판독하고 애플리케이션 공개 키 증명서 상의 서명을 검증. 서명 검증이 실패할 경우, 거절 정보의 프롬프트를 제공. 서명 검증이 통과할 경우, 파싱을 통해 애플리케이션 공개 키를 획득
2009. 공제량을 계산
2010. SNEP-요청((지불: 공제량, 거래 시간, 진입/진출 플래그, 및 (정지와 같은) 거래 정보) 풋)
2011. 서명 데이터 및 TAC를 포함하는 지불 라이선스를 생성
2012. 서명 데이터 및 TAC 반환
2013. 애플리케이션 공개 키를 이용함으로써 서명 데이터 상의 서명을 검증. 서명 검증이 통과할 경우, 거래 로그를 레코딩. 서명 검증이 실패할 경우, 거절 정보의 프롬프트를 제공

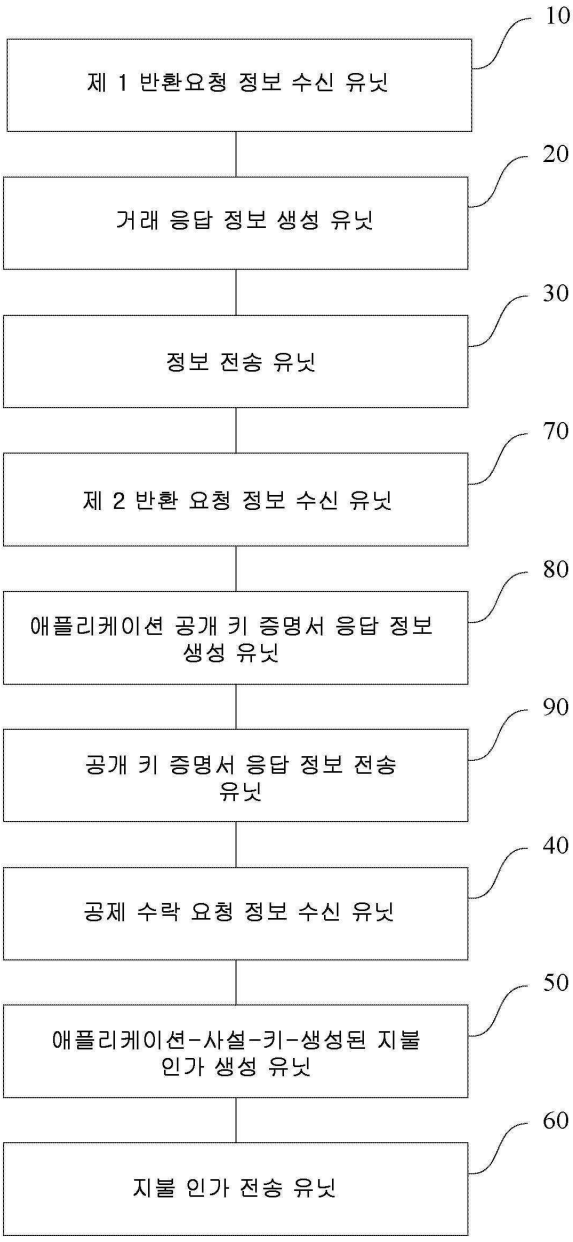
도면21


버스 게이트
버스 게이트 관리 시스템
신용 인가 시스템의 서빙 엔드
3001. 거래 로그를 주기적으로 업로드
3002.정산을 수행하고, 시스템에서의 블랙리스트가 업데이트되는지 여부를 질의하고, 긍정일 경우, 블랙리스트를 반환할 것을 준비
3003. 거래 로그 수신 결과 및 블랙리스트를 반환
3004. 지불 카드 번호가 블랙리스트에서 존재하는지 여부를 검사
3005. 블랙리스트를 업데이트
3006. 업데이트
3007. 업데이트된 완료 결과를 반환

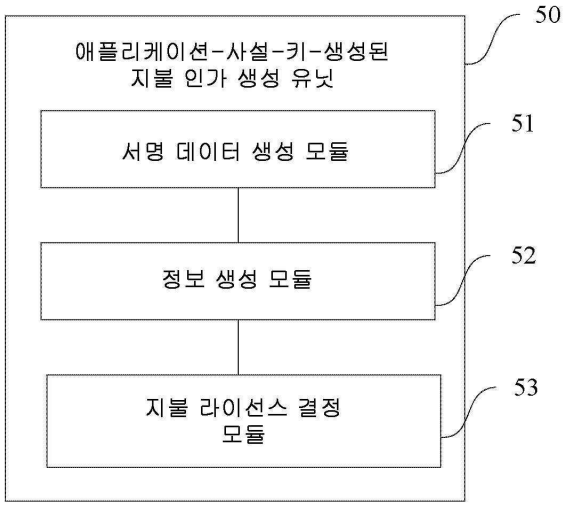
도면22


10
제 1 반환요청 정보 수신 유닛
20
거래 응답 정보 생성 유닛
30
정보 전송 유닛
40
공제 수락 요청 정보 수신 유닛
50
애플리케이션-사설-키-생성된 지불 인가 생성 유닛
60
지불 인가 전송 유닛

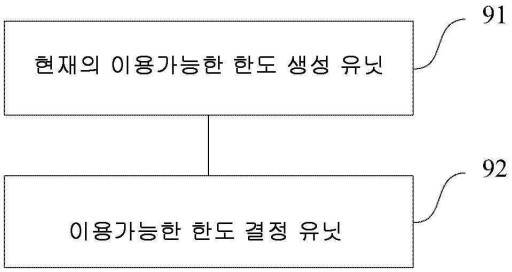
도면23


10
제 1 반환요청 정보 수신 유닛
20
거래 응답 정보 생성 유닛
30
정보 전송 유닛
70
제 2 반환 요청 정보 수신 유닛
80
애플리케이션 공개 키 증명서 응답 정보 생성 유닛
90
공개 키 증명서 응답 정보 전송 유닛
40
공제 수락 요청 정보 수신 유닛
50
애플리케이션-사설-키-생성된 지불 인가 생성 유닛
60
지불 인가 전송 유닛

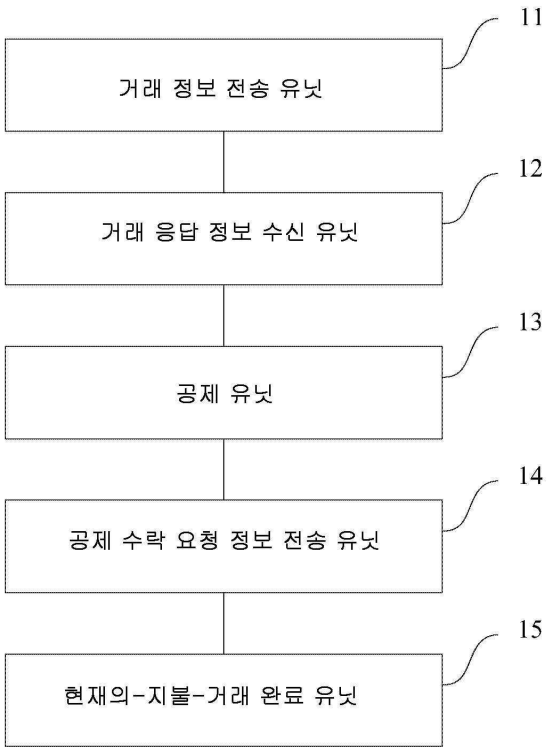
도면24



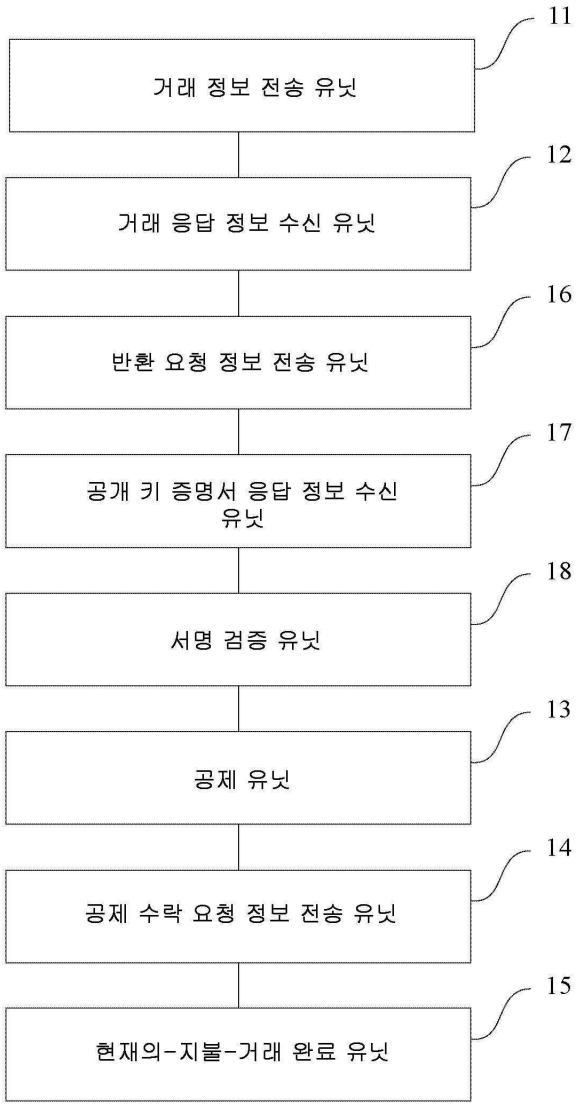
도면25



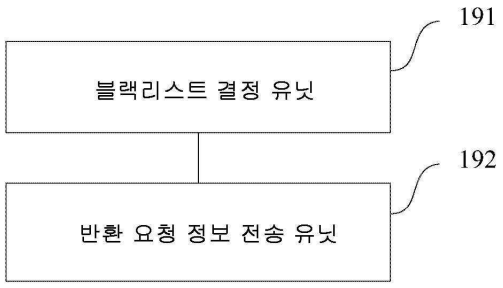
도면26



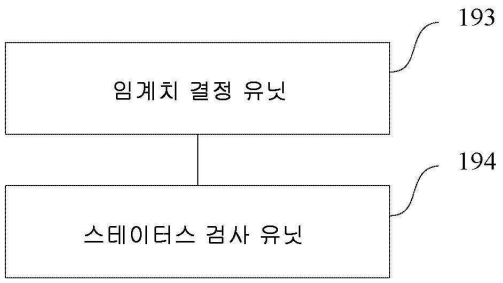
도면27


11
거래 정보 전송 유닛
12
거래 응답 정보 수신 유닛
16
반환 요청 정보 전송 유닛
17
공개 키 증명서 응답 정보 수신 유닛
18
서명 검증 유닛
13
공제 유닛
14
공제 수락 요청 정보 전송 유닛
15
현재의-지불-거래 완료 유닛

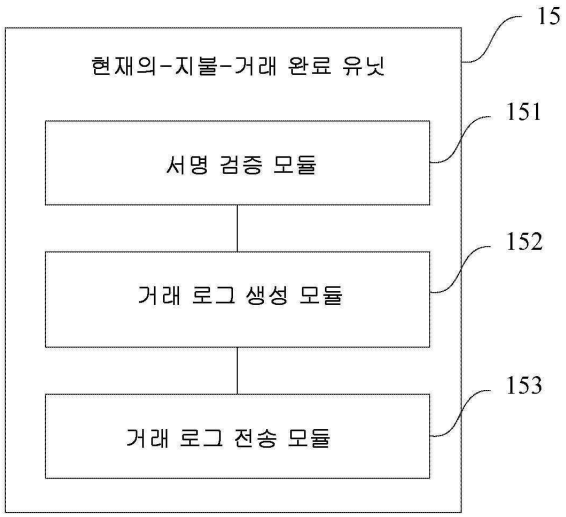
도면28


191
블랙리스트 결정 유닛
192
반환 요청 정보 전송 유닛

도면29


193
임계치 결정 유닛
194
스테이터스 검사 유닛

도면30


15
현재의-지불-거래 완료 유닛
151
서명 검증 모듈
152
거래 로그 생성 모듈
153
거래 로그 전송 모듈