

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일

2017년 12월 28일 (28.12.2017) WIPO | PCT



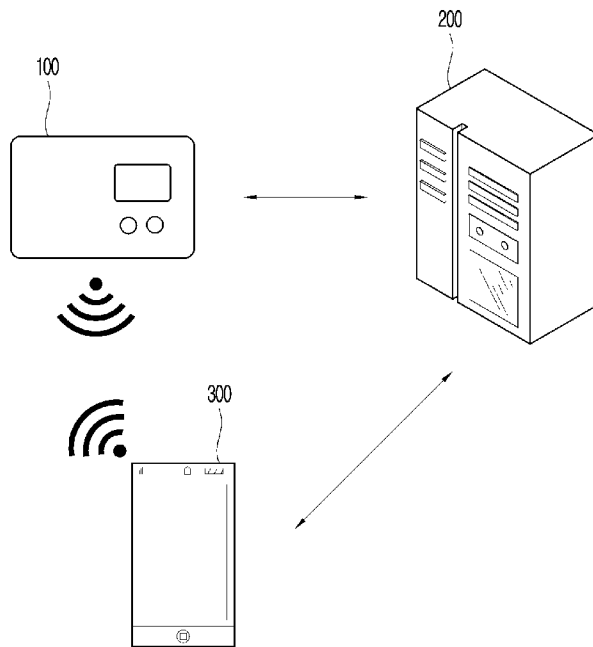
(10) 국제공개번호

WO 2017/222182 A1

- (51) 국제특허분류: *G06Q 20/34* (2012.01) *G06Q 20/40* (2012.01)
G06K 19/07 (2006.01) *G06Q 40/02* (2012.01)
G06Q 20/32 (2012.01) *G06Q 10/06* (2012.01)
G06Q 20/38 (2012.01) *G06Q 10/10* (2012.01)
- (21) 국제출원번호: PCT/KR2017/004982
- (22) 국제출원일: 2017년 5월 12일 (12.05.2017)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2016-0076800 2016년 6월 20일 (20.06.2016) KR
10-2017-0033160 2017년 3월 16일 (16.03.2017) KR
- (71) 출원인: 비씨카드(주) (BCCARD CO., LTD.) [KR/KR];
06654 서울시 서초구 효령로 275, Seoul (KR).
- (72) 발명자: 한강 (HAN, Kang); 16839 경기도 용인시 수지구 정평로 89, 206동 105호, Gyeonggi-do (KR). 이지호 (YI, Ji Ho); 06629 서울시 서초구 서운로 62, 2동 302호, Seoul (KR). 이태훈 (LEE, Tae Hun); 42763 대구시 달서구 월배로11길 33, 107동 2403호, Daegu (KR). 김성원 (KIM, Sung Won); 13560 경기도 성남시 분당구 정자일로 135, B동 2413호, Gyeonggi-do (KR).
- (74) 대리인: 특허법인 하나 (HANA IP LAW FIRM); 06235 서울시 강남구 테헤란로 14길 5, 3층, Seoul (KR).
- (81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN,

(54) Title: METHOD FOR SUPPORTING CARD PAYMENT OF MULTIFUNCTIONAL CARD-TYPE DEVICE, AND MULTIFUNCTIONAL CARD-TYPE DEVICE PERFORMING SAME

(54) 발명의 명칭: 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법 및 이를 수행하는 멀티 기능을 가진 카드형 디바이스



(57) Abstract: According to an embodiment of the present invention, a method by which a multifunctional card-type device supports card payment is provided, the method comprising the steps of: (a) if a first user input is detected, displaying first card identification information that is any one of a plurality of pieces of card identification information that is pre-stored in a memory; (b) if a second user input is not detected during a pre-determined fixed payment waiting time after the first user input is completed, (i) increasing the number of cumulative payment data generation that is recorded in a secure element, and checking whether a newly calculated number



WO 2017/222182 A1

MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

- 국제조사보고서와 함께 (조약 제21조(3))

of cumulative payment data generation exceeds a pre-determined number, or (ii) checking whether the number of cumulative payment data generation that is recorded in the secure element corresponds to the pre-determined number; and (c) generating payment data so as to be able to perform card payment on the basis of first card track information that is stored in the secure element and that is equivalent to the first card identification information, if it is confirmed from the checks that the newly calculated number of cumulative payment data generation does not exceed the pre-determined number, or that the number of cumulative payment data generation that is recorded in the secure element does not correspond to the pre-determined number.

(57) 요약서: 본 발명의 일 실시예에 따르면, 멀티 기능을 가진 카드형 디바이스가, 카드 결제를 지원하는 방법에 있어서, (a) 제1 사용자 입력이 감지되면, 메모리에 미리 저장되어 있는 복수의 카드 식별 정보 중 어느 하나인 제1 카드 식별 정보를 디스플레이 하는 단계; (b) 상기 제1 사용자 입력이 종료된 후, 미리 설정된 소정의 결제대기시간 동안 제2 사용자 입력이 감지되지 않으면, (i) 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수를 증가시키고, 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하는지 확인하거나, (ii) 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수와 대응되는지 확인하는 단계; 및 (c) 상기 확인 결과, 상기 새롭게 계산된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수를 초과하지 않거나, 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수와 대응하지 않는 것으로 확인된 경우, 상기 제1 카드 식별 정보에 상응하는 상기 시큐어 엘리먼트(secure element)에 저장된 상기 제1 카드의 트랙 정보를 기초로 결제 데이터를 생성하여 카드 결제가 수행될 수 있도록 하는 단계를 포함하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법이 제공된다.

명세서

발명의 명칭: 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법 및 이를 수행하는 멀티 기능을 가진 카드형 디바이스 기술분야

- [1] 본 발명은 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법 및 이를 수행하는 멀티 기능을 가진 카드형 디바이스에 관한 것으로, 더욱 상세하게는, 멀티 기능을 가진 카드형 디바이스를 이용한 결제 서비스에 있어서, 결제대기시간 설정을 통해, 설정된 결제대기시간이 초과되면 디스플레이 되고 있는 카드 정보로 결제가 수행될 수 있도록 하고, 누적 결제 데이터 생성 횟수에 대한 제한을 통해, 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수에 횟수가 증가되어 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하거나, 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수와 대응하면 멀티 기능을 가진 카드형 디바이스를 이용한 결제 서비스 이용이 불가능하도록 함으로써, 사용자의 멀티 기능을 가진 카드형 디바이스를 통한 결제 서비스 이용에 있어서, 결제 카드 선택 및 보안 서비스 이용에 대한 편의성을 제공하고자 하는 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법 및 이를 수행하는 멀티 기능을 가진 카드형 디바이스에 관한 것이다.

배경기술

- [2] 최근, 소비자들에게 결제 수단뿐만 아니라 결제에 따른 혜택 서비스가 다양하게 제공됨에 따라 소비자들의 결제 카드 또는 멤버십 카드 이용률이 급증하고 있는 추세를 보이고 있다.
- [3] 하지만, 현재 보급되고 있는 일반적인 카드는, 카드사 별 또는 카드 종류 별 하나의 혜택 또는 결제를 수행할 수 밖에 없어, 소비자가 소지하고 있는 복수의 카드를 들고 다니면서 필요에 따라 카드를 사용해야 하므로, 사용자 입장에서는 결제 또는 포인트 적립에 대한 카드 소지의 불편함이 존재한다.
- [4] 또한, 현재 일반적으로 사용되고 있는 카드는, 별도의 보안 기능이 구비되어 있지 않아, 결제 단말기에 근접, 접촉, 삽입, 또는 스트라이프 처리하기만 하면 결제가 수행되거나 포인트 적립이 수행되므로, 카드 도용의 문제점이 있는 바, 취약한 보안성의 문제가 대두되고 있는 실정이다.
- [5] 따라서, 사용자가 신용 카드 또는 멤버십 카드를 이용하는 데에 있어, 하나의 카드만으로 복수의 카드 사용이 가능하도록 하는 카드 소지의 편의성과 카드 사용에 대한 용이성 및 보안성이 확보될 수 있도록 하는 시스템에 대한 요구가 점차 증대되고 있으며, 상술한 문제점을 해결하기 위한 방안이 시급한 실정이다.

발명의 상세한 설명

기술적 과제

- [6] 본 발명은 전술한 종래기술의 문제점을 해결하기 위한 것으로, 멀티 기능을 가진 카드형 디바이스를 이용한 결제 서비스에 있어서, 결제대기시간 설정을 통해, 설정된 결제대기시간이 초과되면 디스플레이 되고 있는 카드 정보로 결제가 수행될 수 있도록 하고, 누적 결제 데이터 생성 횟수에 대한 제한을 통해, 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수에 횟수가 증가되어 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하거나, 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수와 대응하면 멀티 기능을 가진 카드형 디바이스를 이용한 결제 서비스 이용이 불가능하도록 함으로써, 사용자의 멀티 기능을 가진 카드형 디바이스를 통한 결제 서비스 이용에 있어서, 결제 카드 선택 및 보안 서비스 이용에 대한 편의성을 제공하고자 하는 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법 및 이를 수행하는 멀티 기능을 가진 카드형 디바이스를 제공하는 것을 목적으로 한다.
- [7] 본 발명의 목적들은 이상에서 언급한 목적들로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 명확하게 이해될 수 있을 것이다.

과제 해결 수단

- [8] 상술한 목적을 달성하기 위한 본 발명의 일 실시예에 따르면, 멀티 기능을 가진 카드형 디바이스가, 카드 결제를 지원하는 방법에 있어서, (a) 제1 사용자 입력이 감지되면, 메모리에 미리 저장되어 있는 복수의 카드 식별 정보 중 어느 하나인 제1 카드 식별 정보를 디스플레이 하는 단계; (b) 상기 제1 사용자 입력이 종료된 후, 미리 설정된 소정의 결제대기시간 동안 제2 사용자 입력이 감지되지 않으면, (i) 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수를 증가시키고, 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하는지 확인하거나, (ii) 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수와 대응되는지 확인하는 단계; 및
- [9] (c) 상기 확인 결과, 상기 새롭게 계산된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수를 초과하지 않거나, 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수와 대응하지 않는 것으로 확인된 경우, 상기 제1 카드 식별 정보에 상응하는 상기 시큐어 엘리먼트(secure element)에 저장된 상기 제1 카드의 트랙 정보를 기초로 결제 데이터를 생성하여 카드 결제가 수행될 수 있도록 하는 단계를 포함하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법이 제공된다.
- [10] 상기 (b) 단계에서, 상기 확인 결과, 상기 새롭게 계산된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수를 초과하거나, 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수와 대응되는 것으로 확인된 경우, 상기 멀티 기능을 가진 카드형 디바이스의 상태를

거래 횟수 한도 초과 상태(transaction counter exceed: CE)로 설정하여 상기 메모리에 저장하고, 디스플레이부를 통해 서버와의 동기화가 필요함을 표시하는 것을 특징으로 할 수 있다.

- [11] 상기 (c) 단계는, 상기 제1 카드 식별 정보에 상응하는 상기 시큐어 엘리먼트(secure element)에 저장된 상기 제1 카드의 트랙 정보를 기초로 상기 결제 데이터를 생성한 경우, 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수를 상기 새롭게 계산된 누적 결제 데이터 생성 횟수로 갱신하여 기록하거나 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수를 증가시켜 기록하는 단계를 포함할 수 있다.
- [12] 상기 시큐어 엘리먼트(secure element)에 새롭게 기록된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수와 대응되는 경우, 디스플레이부를 통해 서버와의 동기화가 필요함을 표시하는 것을 특징으로 할 수 있다.
- [13] 상기 시큐어 엘리먼트(secure element)에 새롭게 기록된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수와 대응되지 않는 경우, 상기 메모리 상에서 상기 멀티 기능을 가진 카드형 디바이스의 상태를 결제 서비스 이용 가능 상태(registered: RD)로 유지하고 상태 메시지를 디스플레이 하는 것을 특징으로 할 수 있다.
- [14] 상기 멀티 기능을 가진 카드형 디바이스가 서버에 최초로 등록되면, 상기 멀티 기능을 가진 카드형 디바이스의 상태를 결제 서비스 이용 가능 상태(registered: RD)로 설정하고 상기 메모리에 저장하는 단계를 더 포함하는 것을 특징으로 할 수 있다.
- [15] 일단 상기 멀티 기능을 가진 카드형 디바이스가 결제 서비스 이용 가능 상태(registered: RD)로 설정되면, 더 이상 미등록 상태(not registered: NR)로 상태 전환이 되지 않는 것을 특징으로 할 수 있다.
- [16] 잠금 상태(locked: LD) 설정으로 미리 설정되어 있는 사용자의 입력이 감지되는 경우, 상기 멀티 기능을 가진 카드형 디바이스의 상태를 잠금 상태(locked: LD)로 설정하는 것을 특징으로 할 수 있다.
- [17] 상기 잠금 상태(locked: LD)에서 상기 멀티 기능을 가진 카드형 디바이스 인증이 있는 경우에 한하여 결제 서비스 이용 가능 상태(registered: RD)로 변경이 가능한 것을 특징으로 할 수 있다.
- [18] 상기 (b) 단계는, 상기 제1 사용자 입력이 종료된 후, 상기 미리 설정된 소정의 결제대기시간 동안 제2 사용자 입력이 감지되면, 상기 메모리에 미리 저장되어 있는 복수의 카드 식별 정보 중 어느 하나인 제2 카드 식별 정보를 디스플레이 하는 단계를 포함할 수 있다.
- [19] (e) 사용자 단말기로부터 암호화된 인증 정보를 포함하는 횟수 정보 변경 요청이 수신되면, 수신된 인증 정보를 복호화하여, 복호화된 인증 정보와 상기 시큐어 엘리먼트(secure element)에 미리 저장된 인증 정보와의 대응 여부를 판단하는 단계; 및 (f) 복호화된 인증 정보와 상기 시큐어 엘리먼트(secure

element)에 미리 저장된 인증 정보가 대응되는 것으로 판단된 경우, 상기 시큐어 엘리먼트(secure element)에 기록 또는 설정되어 있는 횃수 정보를 상기 변경 요청된 횃수 정보로 변경하여 기록 또는 설정하는 단계를 더 포함할 수 있다.

[20] 상기 횃수 정보 변경 요청은, 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횃수 초기화 요청 및 상기 미리 설정된 횃수 변경 요청 중 적어도 어느 하나인 것일 수 있다.

[21] (g) 사용자 단말기로부터 암호화 된 인증 정보를 포함하는 상기 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 요청이 수신되면, 수신된 인증 정보를 복호화하여, 복호화된 인증 정보와 상기 메모리에 미리 저장된 인증 정보와의 대응 여부를 판단하는 단계; 및 (h) 복호화된 인증 정보와 상기 메모리에 미리 저장된 인증 정보가 대응되는 것으로 판단된 경우, 상기 메모리에 저장되어 있는 상기 멀티 기능을 가진 카드형 디바이스의 상태 정보를 요청된 상태 정보로 변경하여 저장하는 단계를 더 포함할 수 있다.

[22] 한편, 본 발명의 다른 실시예에 따르면, 하나 이상의 제어 수단으로 되어 있으며, 사용자에게 의해 입력되면, 입력 신호를 제어부로 전달하는 사용자 입력부; 제어부로부터 전달되는 카드 식별 정보 또는 멀티 기능을 가진 카드형 디바이스 상태 정보를 디스플레이 하는 디스플레이부; 하나 이상의 카드 식별 정보 각각에 상응하는 카드 트랙 정보 및 인증 정보가 저장되어 있으며, 누적 결제 데이터 생성 횃수가 기록되어 있는 시큐어 엘리먼트(secure element); 하나 이상의 카드 식별 정보, 멀티 기능을 가진 카드형 디바이스 상태 정보 및 인증 정보가 저장되어 있는 메모리; 상기 시큐어 엘리먼트(secure element)에 저장된 카드 트랙 정보를 기초로 결제 데이터를 생성하고, 생성한 결제 데이터를 기초로 카드 결제를 수행하는 결제부; (i) 제1 사용자 입력이 감지되면, 상기 메모리에 미리 저장되어 있는 복수의 카드 식별 정보 중 어느 하나인 제1 카드 식별 정보가 디스플레이 되도록 제어하고, (ii) 제1 사용자 입력이 종료된 후, 미리 설정된 소정의 결제대기시간 동안 제2 사용자 입력이 감지되지 않으면, 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횃수에 횃수를 증가시켜 새롭게 계산된 누적 결제 데이터 생성 횃수의 미리 설정된 횃수 초과 여부가 확인되거나, 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횃수의 미리 설정된 횃수 대응 여부가 확인되도록 제어하고, (iii) 확인 결과, 새롭게 계산된 누적 결제 데이터 생성 횃수가 미리 설정된 횃수를 초과하지 않거나, 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횃수가 미리 설정된 횃수와 대응하지 않는 것으로 확인된 경우, 상기 제1 카드 식별 정보에 상응하는 상기 시큐어 엘리먼트(secure element)에 저장된 제1 카드의 트랙 정보를 기초로 결제 데이터가 생성되어 카드 결제가 수행될 수 있도록 제어하는 제어부; 사용자 단말기 또는 외부 서버와의 통신을 수행하는 통신부; 및 멀티 기능을 가진 카드형 디바이스가 충전될 수 있도록 하는 충전부를 포함하는, 멀티 기능을 가진 카드형 디바이스가 제공된다.

발명의 효과

- [23] 본 발명의 일 실시예에 따르면, 결제대기시간 초과 여부에 따라 멀티 기능을 가진 카드형 디바이스 내에 저장되어 있는 결제 카드 정보가 자동 선택되어 결제가 수행될 수 있도록 함으로써, 사용자 입장에서는, 제한된 사용자 입력부의 구성에도 불구하고, 1회의 입력만으로 최적화된 카드 식별 정보 조회 및 결제 카드 선택이 가능하다는 장점이 있다.
- [24] 또한, 본 발명의 일 실시예에 따르면, 사용자에게 의해 설정된 횡수를 기준으로 누적 결제 데이터 생성 횡수 정보에 기초한 멀티 기능을 가진 카드형 디바이스 결제 서비스가 제공되며, 누적된 결제 데이터 생성 횡수가 미리 설정된 횡수에 대응되거나, 누적된 결제 데이터 생성 횡수에 횡수가 증가되어 새롭게 계산된 누적 결제 데이터 생성 횡수가 미리 설정된 횡수를 초과하면 사용자에게 알림이 제공되므로, 사용자가 특정 거래횡수만큼만 결제가 수행될 수 있도록 하여, 별도의 보안 설정 및 보안 정보 입력을 수행하지 않아도 거래횡수제한에 따른 자동적인 보안 설정을 할 수 있다는 효과가 있다.
- [25] 본 발명의 효과는 상기한 효과로 한정되는 것은 아니며, 본 발명의 상세한 설명 또는 특허청구범위에 기재된 발명의 구성으로부터 추론 가능한 모든 효과를 포함하는 것으로 이해되어야 한다.

도면의 간단한 설명

- [26] 도 1은 본 발명의 일 실시예에 따른 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 시스템의 구성을 개략적으로 도시한 도면이다.
- [27] 도 2는 본 발명의 일 실시예에 따른 멀티 기능을 가진 카드형 디바이스의 구성을 도시한 블록도이다.
- [28] 도 3은 본 발명의 일 실시예에 따른 멀티 기능을 가진 카드형 디바이스가 카드 결제를 지원하는 과정을 도시한 순서도이다.
- [29] 도 4는 본 발명의 일 실시예에 따른 미리 설정된 결제대기시간 내에 사용자 입력이 감지되는 경우, 멀티 기능을 가진 카드형 디바이스를 통해 지원되는 카드 결제의 과정을 도시한 순서도이다.
- [30] 도 5는 본 발명의 일 실시예에 따른 거래 횡수 한도 초과 상태(transaction counter exceed: CE)의 경우, 멀티 기능을 가진 카드형 디바이스를 통해 지원되는 카드 결제의 과정을 도시한 순서도이다.
- [31] 도 6은 본 발명의 일 실시예에 따른 인증 절차를 통해 횡수 정보 변경 또는 멀티 기능을 가진 카드형 디바이스 상태 정보 변경이 가능하도록 하는 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 과정을 도시한 순서도이다.
- [32] 도 7은 본 발명의 일 실시예에 따른 멀티 기능을 가진 카드형 디바이스의 상태 정보 변경 순환 구조를 개략적으로 도시한 도면이다.

발명의 실시를 위한 최선의 형태

- [33] 이하에서는 첨부한 도면을 참조하여 본 발명을 설명하기로 한다. 그러나 본

발명은 여러 가지 상이한 형태로 구현될 수 있으며, 따라서 여기에서 설명하는 실시예로 한정되는 것은 아니다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

- [34] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 부재를 사이에 두고 "간접적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 구비할 수 있다는 것을 의미한다.
- [35] 본 명세서에서, 멀티 기능을 가진 카드형 디바이스 상태 정보는, 거래 횟수 한도 초과 상태(transaction counter exceed: CE), 결제 서비스 이용 가능 상태(registered: RD), 미등록 상태(not registered: NR), 잠금 상태(locked: LD), 종료 상태(terminated: TE) 중 어느 하나일 수 있다.
- [36] 거래 횟수 한도 초과 상태(transaction counter exceed: CE)는, 멀티 기능을 가진 카드형 디바이스 내 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수에 횟수가 증가되어 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하거나, 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수와 대응되는 것으로 확인됨에 따라 사용자의 결제 서비스 이용이 불가능한 상태를 의미할 수 있으며, 멀티 기능을 가진 카드형 디바이스 내 통신부와 사용자 단말기와의 인증 절차를 통해 결제 서비스 이용 가능 상태(registered: RD), 잠금 상태(locked: LD), 종료 상태(terminated: TE) 중 어느 하나의 상태 정보로 변경될 수 있다.
- [37] 결제 서비스 이용 가능 상태(registered: RD)는, 멀티 기능을 가진 카드형 디바이스가 서버에 등록된 상태를 의미할 수 있으며, 멀티 기능을 가진 카드형 디바이스 내 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수에 횟수가 증가되어 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하거나, 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수와 대응되는 것으로 확인되면, 서버와의 별도 통신 없이 거래 횟수 한도 초과 상태(transaction counter exceed: CE)의 상태 정보로 변경될 수 있다. 또한, 멀티 기능을 가진 카드형 디바이스 내 통신부와 사용자 단말기와의 인증 절차를 통해 잠금 상태(locked: LD), 종료 상태(terminated: TE) 중 어느 하나의 상태 정보로 변경될 수 있다.
- [38] 미등록 상태(not registered: NR)는, 멀티 기능을 가진 카드형 디바이스가 서버에 등록되어 있지 않은 상태를 의미할 수 있으며, 멀티 기능을 가진 카드형 디바이스 내 통신부와 사용자 단말기와의 인증 절차를 통해 결제 서비스 이용 가능 상태(registered: RD)의 상태 정보로 변경될 수 있다.
- [39] 잠금 상태(locked: LD)는, 멀티 기능을 가진 카드형 디바이스가 이용될 수

없도록 잠겨있는 상태를 의미할 수 있으며, 멀티 기능을 가진 카드형 디바이스 내 통신부와 사용자 단말기와의 인증 절차를 통해 결제 서비스 이용 가능 상태(registered: RD)의 상태 정보로 변경될 수 있다.

- [40] 종료 상태(terminated: TE)는, 멀티 기능을 가진 카드형 디바이스가 더 이상 사용될 수 없는 상태를 의미할 수 있다.
- [41] 이하 첨부된 도면을 참고하여 본 발명의 실시예를 상세히 설명하기로 한다.
- [42] 도 1은 본 발명의 일 실시예에 따른 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 시스템의 구성을 개략적으로 도시한 도면이다.
- [43] 도 1을 참조하면, 본 발명의 일 실시예에 따른 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 시스템은, 멀티 기능을 가진 카드형 디바이스(100), 서버(200) 및 사용자 단말기(300)를 포함한다.
- [44] 먼저, 멀티 기능을 가진 카드형 디바이스(100)와 서버(200)뿐만 아니라 서버(200)와 사용자 단말기(300)는 각각 통신망으로 연결되어 있을 수 있으며, 여기서, 통신망은 유선 및 무선 등과 같은 그 통신 양태를 가리지 않고 구성될 수 있다. 근거리 통신망(LAN: Local Area Network), 도시권 통신망(MAN: Metropolitan Area Network), 광역 통신망(WAN: Wide Area Network) 등 다양한 통신망으로 구성될 수 있다.
- [45] 멀티 기능을 가진 카드형 디바이스(100)는 카드 식별 정보와 카드 트랙 정보를 매칭하여 저장하고 있을 수 있으며, 이는 사용자에게 의해 등록될 수 있다.
- [46] 멀티 기능을 가진 카드형 디바이스(100)는 제1 사용자 입력이 감지되면, 메모리에 미리 저장되어 있는 복수의 카드 식별 정보 중 어느 하나인 제1 카드 식별 정보를 디스플레이 할 수 있다.
- [47] 멀티 기능을 가진 카드형 디바이스(100)는 디스플레이 되고 있는 카드 식별 정보에 대해, 제1 사용자 입력이 종료된 후, 미리 설정된 소정의 결제대기시간 내에 제2 사용자 입력이 감지되지 않는 경우, 시큐어 엘리먼트(secure element)에 기록되어 있는 멀티 기능을 가진 카드형 디바이스(100)의 누적 결제 데이터 생성 횟수를 증가시켜, 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하는지 확인하거나 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수와 대응되는지 확인할 수 있다. 시큐어 엘리먼트(secure element)는, 일반적으로 카드형 디바이스에 구비된 IC칩일 수 있다.
- [48] 본 발명의 일 실시예에 따르면, 멀티 기능을 가진 카드형 디바이스(100)는 디스플레이 되고 있는 카드 식별 정보에 대해, 제1 사용자 입력이 종료된 후, 미리 설정된 소정의 결제대기시간 내에 제2 사용자 입력이 감지되는 경우, 메모리에 미리 저장되어 있는 복수의 카드 식별 정보 중 다른 하나인 제2 카드 식별 정보를 디스플레이 할 수 있다.
- [49] 멀티 기능을 가진 카드형 디바이스(100)는 시큐어 엘리먼트(secure element)에 기록되어 있는 누적 결제 데이터 생성 횟수에 횟수를 증가시켜 새롭게 계산된

누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하는 것으로 확인되거나, 시큐어 엘리먼트(secure element)에 기록되어 있는 누적 결제 데이터 생성 횟수가 미리 설정된 횟수와 대응하는 것으로 확인된 경우, 거래 횟수 한도 초과 상태(transaction counter exceed: CE)를 메모리에 저장하고, 이를 디스플레이부를 통해 디스플레이 하여 사용자에게 알릴 수 있다. 디스플레이부를 통해 거래 횟수 한도 초과 상태(transaction counter exceed: CE)를 표시하는 경우, 멀티 기능을 가진 카드형 디바이스(100)는 거래 횟수 한도 초과 상태(transaction counter exceed: CE) 해제를 위해 서버와의 동기화가 필요함을 표시하는 화면을 더 디스플레이 하여 사용자에게 알릴 수 있다.

- [50] 멀티 기능을 가진 카드형 디바이스(100)는 시큐어 엘리먼트(secure element)에 기록되어 있는 누적 결제 데이터 생성 횟수에 횟수를 증가시켜 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하지 않는 것으로 확인되거나, 시큐어 엘리먼트(secure element)에 기록되어 있는 누적 결제 데이터 생성 횟수가 미리 설정된 횟수와 대응하지 않는 것으로 확인된 경우, 제1 카드 식별 정보에 상응하는 시큐어 엘리먼트(secure element)에 저장된 제1 카드의 트랙 정보를 기초로 결제 데이터를 생성하여 카드 결제가 수행되도록 할 수 있다.
- [51] 멀티 기능을 가진 카드형 디바이스(100)는 제1 카드 식별 정보에 상응하는 시큐어 엘리먼트(secure element)에 저장된 제1 카드의 트랙 정보를 기초로 결제 데이터를 생성한 경우, 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수를 새롭게 계산된 누적 결제 데이터 생성 횟수로 갱신하여 기록하거나 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수를 증가시켜 기록할 수 있다.
- [52] 멀티 기능을 가진 카드형 디바이스(100)는 상태 정보를 디스플레이 하여 사용자에게 알릴 수 있다.
- [53] 본 발명의 일 실시예에 따르면, 멀티 기능을 가진 카드형 디바이스(100)는 시큐어 엘리먼트(secure element)에 새롭게 기록된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수와 대응되는 경우, 디스플레이부를 통해 서버(200)와의 동기화가 필요함을 표시할 수 있다.
- [54] 본 발명의 다른 실시예에 따르면, 멀티 기능을 가진 카드형 디바이스(100)는 시큐어 엘리먼트(secure element)에 새롭게 기록된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수와 대응되지 않는 경우, 메모리 상에서 멀티 기능을 가진 카드형 디바이스(100)의 상태를 결제 서비스 이용 가능 상태(registered: RD)로 유지하고, 상태 메시지를 디스플레이 할 수 있다.
- [55] 본 발명의 또 다른 실시예에 따르면, 멀티 기능을 가진 카드형 디바이스(100)는 멀티 기능을 가진 카드형 디바이스(100)가 서버(200)에 최초로 등록되면, 멀티 기능을 가진 카드형 디바이스(100)의 상태를 결제 서비스 이용 가능 상태(registered: RD)로 설정하고 메모리에 저장함과 동시에 해당 상태 메시지를

디스플레이 할 수 있다.

- [56] 본 발명의 또 다른 실시예에 따르면, 멀티 기능을 가진 카드형 디바이스(100)는 멀티 기능을 가진 카드형 디바이스(100)가 결제 서비스 이용 가능 상태(registered: RD)로 설정되면, 더 이상 미등록 상태(not registered: NR)로 상태 전환이 되지 않음에 따라, 더 이상 미등록 상태(not registered: NR) 메시지를 디스플레이 하지 않을 수 있다.
- [57] 본 발명의 또 다른 실시예에 따르면, 멀티 기능을 가진 카드형 디바이스(100)는 잠금 상태(locked: LD) 설정으로 미리 설정되어 있는 사용자의 입력이 감지되는 경우, 멀티 기능을 가진 카드형 디바이스(100)의 상태를 잠금 상태(locked: LD)로 설정하여 해당 상태 메시지를 디스플레이 할 수 있다.
- [58] 본 발명의 또 다른 실시예에 따르면, 멀티 기능을 가진 카드형 디바이스(100)는 잠금 상태(locked: LD)에서 인증이 정상적으로 완료된 경우에 한하여 결제 서비스 이용 가능 상태(registered: RD)로 변경이 가능함에 따라, 인증 완료 시 결제 서비스 이용 가능 상태(registered: RD)의 메시지를 디스플레이 할 수 있다.
- [59] 멀티 기능을 가진 카드형 디바이스(100)는 사용자 단말기(300)로부터 암호화된 인증 정보를 포함하는 핏수 정보 변경 요청이 수신되면, 수신된 인증 정보를 복호화하여, 복호화된 인증 정보와 시큐어 엘리먼트(secure element)에 미리 저장되어 있는 인증 정보와의 대응 여부를 판단함으로써, 판단 결과에 따라 요청 수신된 핏수 정보에 대한 변경을 수행할 수 있다. 수신되는 핏수 정보 변경 요청은, 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 핏수 초기화에 대한 요청이거나 미리 설정된 핏수 변경에 대한 요청일 수 있다.
- [60] 본 발명의 일 실시예에 따르면, 복호화된 인증 정보와 시큐어 엘리먼트(secure element)에 미리 저장되어 있는 인증 정보가 대응되는 것으로 판단된 경우, 시큐어 엘리먼트(secure element)에 기록 또는 설정되어 있는 핏수 정보를 변경 요청된 핏수 정보로 변경하여 기록 또는 설정할 수 있다.
- [61] 멀티 기능을 가진 카드형 디바이스(100)는 사용자 단말기(300)로부터 암호화된 인증 정보를 포함하는 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 요청이 수신되면, 수신된 인증 정보를 복호화하여, 복호화된 인증 정보와 메모리에 미리 저장되어 있는 인증 정보와의 대응 여부를 판단함으로써, 판단 결과에 따라 요청 수신된 멀티 기능을 가진 카드형 디바이스 상태 정보에 대한 변경을 수행할 수 있다.
- [62] 본 발명의 일 실시예에 따르면, 복호화된 인증 정보와 메모리에 미리 저장되어 있는 인증 정보가 대응되는 것으로 판단된 경우, 메모리에 저장되어 있는 멀티 기능을 가진 카드형 디바이스 상태 정보를 변경하여 저장할 수 있다.
- [63] 서버(200)는 멀티 기능을 가진 카드형 디바이스(100)와 사용자 단말기(300) 간의 정보 전송을 전달하는 역할을 수행하는 네트워크 서버일 수 있으며, 사용자 단말기(300)로부터 수신되는 인증 정보 전송 요청에 따라 인증 정보를 암호화하여 제공하는 보안 인증 관련 서버일 수 있다.

- [64] 서버(200)는 사용자 단말기(300)로부터 암호화 된 인증 정보를 포함하는 횡수 정보 변경 요청 또는 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 요청이 수신되면, 수신된 암호화 된 인증 정보를 포함하는 횡수 정보 변경 요청 또는 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 요청을 멀티 기능을 가진 카드형 디바이스(100)로 전송할 수 있다.
- [65] 서버(200)는 멀티 기능을 가진 카드형 디바이스(100)로부터 수신되는 횡수 정보 변경 결과 또는 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 결과를 사용자 단말기(300)로 전송할 수 있다.
- [66] 서버(200)는 사용자 단말기(300)가 멀티 기능을 가진 카드형 디바이스(100) 내에 저장된 정보 변경을 위해 인증 정보 전송을 요청하는 경우, 인증 정보를 암호화 하여 사용자 단말기(300)에 제공할 수 있다.
- [67] 사용자 단말기(300)는 휴대폰, 스마트폰, PDA(Personal Digital Assistant), PMP(Portable Multimedia Player), 태블릿 PC 등과 같이 터치 스크린 패널이 구비된 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있으며, 이 외에도 데스크탑 PC, 태블릿 PC, 랩탑 PC, 셋탑 박스를 포함하는 IPTV와 같이, 애플리케이션을 설치하고 실행할 수 있는 기반이 마련된 장치도 포함할 수 있다.
- [68] 사용자 단말기(300)는 멀티 기능을 가진 카드형 디바이스(100)를 이용한 카드 결제 서비스를 제공하는 애플리케이션을 설치하여 메모리에 저장할 수 있다. 예를 들어, 사용자 단말기(300)는 횡수 정보 변경 요청 서비스, 암호화 된 인증 정보 전송 서비스, 멀티 기능을 가진 카드형 디바이스(100)와의 무선 통신 연동 서비스, 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 요청 서비스 등 다양한 서비스를 제공하는 멀티 기능을 가진 카드형 디바이스(100)를 이용한 결제 서비스를 제공하는 애플리케이션을 다운로드 하여 설치할 수 있다.
- [69] 사용자 단말기(300)는 서버(200)로 인증 정보 전송을 요청하여, 멀티 기능을 가진 카드형 디바이스(100)를 통해 인증 절차가 수행될 수 있도록 하는 암호화 된 인증 정보를 제공 받을 수 있다.
- [70] 사용자 단말기(300)는 멀티 기능을 가진 카드형 디바이스(100) 내에 저장된 횡수 정보를 변경하고자 하는 경우, 암호화 된 인증 정보를 무선 통신을 통해 멀티 기능을 가진 카드형 디바이스(100)로 전송하여, 인증 절차에 따라 횡수 정보가 변경되도록 할 수 있다.
- [71] 사용자 단말기(300)는 멀티 기능을 가진 카드형 디바이스(100) 내에 저장된 멀티 기능을 가진 카드형 디바이스 상태 정보를 변경하고자 하는 경우, 암호화 된 인증 정보를 무선 통신을 통해 멀티 기능을 가진 카드형 디바이스(100)로 전송하여, 인증 절차에 따라 거래횡수정보가 변경되도록 할 수 있다.
- [72] 사용자 단말기(300)는 요청한 횡수 정보 또는 멀티 기능을 가진 카드형 디바이스 상태 정보 변경이 완료됨에 따라, 멀티 기능을 가진 카드형 디바이스(100)로부터 횡수 정보 또는 멀티 기능을 가진 카드형 디바이스 상태

정보 변경 결과를 수신할 수 있다.

[73] 도 2는 본 발명의 일 실시예에 따른 멀티 기능을 가진 카드형 디바이스(100)의 구성을 도시한 블록도이다.

[74] 도 2를 참조하면, 본 발명의 일 실시예에 따른 멀티 기능을 가진 카드형 디바이스(100)는 사용자 입력부(110), 디스플레이부(120), 메모리(130), 시큐어 엘리먼트(secure element)(140), 제어부(150), 결제부(160), 통신부(170) 및 충전부(180)를 포함한다.

[75] 사용자 입력부(110)는 하나 이상의 제어 수단으로 구성되어 있을 수 있으며, 사용자에게 의해 입력되면, 제어부(150)로 입력 신호를 전달할 수 있다.

[76] 디스플레이부(120)는 제어부(150)로부터 전달되는 카드 식별 정보 또는 멀티 기능을 가진 카드형 디바이스 상태 정보를 디스플레이 할 수 있다.

[77] 본 발명의 일 실시예에 따르면, 디스플레이부(120)는 제1 사용자 입력이 감지되면, 제어부(150)를 통해 메모리(130)에 저장되어 있는 복수의 카드 식별 정보 중 어느 하나인 제1 카드 식별 정보를 디스플레이 할 수 있으며, 이를 통해 사용자가 결제하고자 하는 카드 식별 정보를 선택하도록 할 수 있다.

[78] 본 발명의 다른 실시예에 따르면, 디스플레이부(120)는 사용자 입력이 감지되면, 제어부(150)를 통해 메모리(130)에 저장되어 있는 멀티 기능을 가진 카드형 디바이스 상태 정보를 디스플레이 할 수 있다.

[79] 본 발명의 또 다른 실시예에 따르면, 디스플레이 되고 있는 카드 식별 정보에 대해서 제1 사용자 입력이 종료된 후, 결제대기시간 내에 제2 사용자 입력이 감지되지 않아, 디스플레이 되고 있는 카드 식별 정보로 결제가 수행되는 경우, 디스플레이부(120)는 디스플레이 되고 있는 카드 식별 정보에 매칭되어 시큐어 엘리먼트(secure element)(140)에 저장되어 있는 카드 트랙 정보를 기초로 생성된 결제 관련 정보를 제어부(150)를 통해 전달받아 디스플레이 함으로써, 디스플레이 화면을 통해 결제가 수행되도록 할 수 있다. 디스플레이 가능한 결제 관련 정보는, 바코드, QR 코드, 카드 번호, 유효 기간 정보 중 어느 하나일 수 있다.

[80] 메모리(130)는 카드 식별 정보, 멀티 기능을 가진 카드형 디바이스 상태 정보 등을 저장할 수 있는데, 예를 들면, 신용카드의 이미지, 신용카드의 명칭, 멀티 기능을 가진 카드형 디바이스(100)의 잠금 상태, 누적거래횟수 초과에 따른 결제 서비스 이용 불가 상태 등이 저장되어 있을 수 있으며, 이에 한정되지 않는다.

[81] 메모리(130)는 사용자 입력이 감지됨에 따라, 제어부(150)로부터 카드 식별 정보 요청을 수신할 수 있으며, 미리 저장되어 있는 복수의 카드 식별 정보 중 어느 하나인 제1 카드 식별 정보를 제어부(150)로 전송함으로써, 디스플레이부(120)를 통해 제1 카드 식별 정보가 제공되도록 할 수 있다.

[82] 메모리(130)는 시큐어 엘리먼트(secure element)(140)에서 멀티 기능을 가진 카드형 디바이스(100)의 누적 결제 데이터 생성 횟수에 횟수가 추가된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하는 것으로 확인되거나, 누적 결제

데이터 생성 횟수가 미리 설정된 횟수와 대응되는 것으로 확인되면, 멀티 기능을 가진 카드형 디바이스(100)의 거래 횟수 한도 초과 상태(transaction counter exceed: CE)를 저장할 수 있으며, 이에 따라 멀티 기능을 가진 카드형 디바이스 상태 정보를 결제 서비스 이용 불가 상태로 설정하여 저장할 수 있다.

- [83] 메모리(130)는 거래 횟수 한도 초과 상태(transaction counter exceed: CE)가 저장되어 있는 상태에서 제어부(150)로부터 카드 식별 정보 요청이 수신되면, 제어부(150)로 거래 횟수 한도 초과 상태(transaction counter exceed: CE)를 전송함으로써, 더 이상의 멀티 기능을 가진 카드형 디바이스(100)를 이용한 결제 서비스 이용이 불가하도록 할 수 있다.
- [84] 메모리(130)는 시큐어 엘리먼트(secure element)에 새롭게 기록된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수와 대응되지 않는 경우, 멀티 기능을 가진 카드형 디바이스(100)의 결제 서비스 이용 가능 상태(registered: RD)를 유지하여 저장할 수 있다.
- [85] 메모리(130)는 멀티 기능을 가진 카드형 디바이스(100)가 서버(200)에 최초로 등록되면, 멀티 기능을 가진 카드형 디바이스 상태 정보를 결제 서비스 이용 가능 상태(registered: RD)로 설정하여 저장할 수 있다.
- [86] 본 발명의 일 실시예에 따르면, 메모리(130)는 멀티 기능을 가진 카드형 디바이스 상태 정보가 결제 서비스 이용 가능 상태(registered: RD)로 설정 및 저장되어 있으면, 더 이상 미등록 상태(not registered: NR)로 전환되어 설정 및 저장될 수 없다.
- [87] 메모리(130)는 제어부(150)에서 잠금 상태(locked: LD) 설정으로 미리 설정되어 있는 사용자의 입력이 감지되는 경우, 멀티 기능을 가진 카드형 디바이스 상태 정보를 잠금 상태(locked: LD)로 설정하여 저장할 수 있다.
- [88] 본 발명의 일 실시예에 따르면, 메모리(130)는 잠금 상태(locked: LD)에서 멀티 기능을 가진 카드형 디바이스 인증이 수행된 경우에 한하여 결제 서비스 이용 가능 상태(registered: RD)로 상태 정보 변경을 수행할 수 있다.
- [89] 메모리(130)는 사용자 입력이 감지됨에 따라 제어부(150)로부터 멀티 기능을 가진 카드형 디바이스 상태 정보 요청이 수신되면, 저장되어 있는 멀티 기능을 가진 카드형 디바이스 상태 정보를 제어부(150)로 전송할 수 있다.
- [90] 메모리(130)는 제어부(150)를 통해 통신부(170)로부터 암호화 된 인증 정보를 포함하는 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 요청이 전달되면, 암호화 된 인증 정보를 복호화하고, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보를 비교하여, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보가 대응되는 것으로 판단된 경우, 요청 수신된 멀티 기능을 가진 카드형 디바이스 상태 정보를 변경하여 저장함으로써, 사용자의 인증 절차를 통해 멀티 기능을 가진 카드형 디바이스 상태가 임의로 변경되도록 할 수 있다. 메모리(130)는 멀티 기능을 가진 카드형 디바이스 상태 정보를 변경하여 저장함에 따라, 변경된 멀티 기능을 가진 카드형 디바이스 상태 정보를 제어부(150)를 통해 통신부(170)로

전달할 수 있다.

- [91] 예를 들어, 현재 멀티 기능을 가진 카드형 디바이스(100)가 결제 서비스 이용 상태로 설정되어 있으며, 제어부(150)를 통해 통신부(170)로부터 암호화 된 인증 정보가 포함된 멀티 기능을 가진 카드형 디바이스 잠금 상태 변경 요청이 전달되면, 메모리(130)는 암호화 된 인증 정보를 복호화하고, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보를 비교하여, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보가 대응되는 것으로 판단된 경우, 멀티 기능을 가진 카드형 디바이스(100)를 잠금 상태로 변경할 수 있다. 또한, 메모리(130)는 잠금 상태로 변경된 멀티 기능을 가진 카드형 디바이스 상태 정보를 제어부(150)를 통해 통신부(170)로 전달할 수 있다.
- [92] 시큐어 엘리먼트(secure element)(140)는 메모리(130)에 저장되어 있는 카드 식별 정보와 매칭된 카드 트랙 정보가 저장되어 있을 수 있으며, 멀티 기능을 가진 카드형 디바이스(100)의 누적 결제 데이터 생성 횟수가 기록되어 있을 수 있으며, 사용자에게 의해 미리 설정된 횟수가 설정되어 있을 수 있다. 예를 들면, 신용카드 번호, 유효기간, 비밀번호, 신용카드 번호에 상응하는 결제 처리가 가능한 바코드 또는 QR 코드 등이 저장되어 있을 수 있으며, IC칩의 형태로 되어 있을 수 있으나, 이에 제한되지 않는다.
- [93] 시큐어 엘리먼트(secure element)(140)는 제어부(150)로부터 결제 요청이 전달되면, 기록된 누적 결제 데이터 생성 횟수에 횟수를 증가시켜, 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정되어 있는 횟수를 초과하지 않는지 여부를 판단하거나, 기록된 누적 결제 데이터 생성 횟수가 미리 설정되어 있는 횟수와 대응되지 않는지 여부를 판단할 수 있다.
- [94] 시큐어 엘리먼트(secure element)(140)는 횟수를 증가시킴에 따라 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정되어 있는 횟수를 초과하지 않는 것으로 판단되거나, 기록되어 있는 누적 결제 데이터 생성 횟수가 미리 설정되어 있는 횟수와 대응되지 않는 것으로 판단된 경우, 기록되어 있는 누적 결제 데이터 생성 횟수에 횟수를 추가 누적함에 따라, 누적 결제 데이터 생성 횟수를 갱신하여 재기록할 수 있으며, 제어부(150)로부터 요청된 결제 처리를 수행하기 위해, 결제 요청에 포함되어 전달된 카드 식별 정보에 상응하는 카드 트랙 정보를 제어부(150)를 통해 결제부(160)로 전송하거나 디스플레이부(120)로 전송할 수 있다.
- [95] 예를 들어, 기록되어 있는 누적 결제 데이터 생성 횟수가 3회로 기록되어 있고, 사용자에게 의해 미리 설정되어 있는 횟수는 5회라고 가정하고, 시큐어 엘리먼트(secure element)가 IC칩의 형태로 되어 있다면, 제어부(150)로부터 신용카드 A에 대한 결제 요청이 수신된 경우, IC칩은 기록되어 있는 3회의 누적 결제 데이터 생성 횟수에 횟수를 1회 추가하여, 새롭게 계산된 4회의 누적 결제 데이터 생성 횟수가 미리 설정된 횟수인 5회를 초과하지 않는 것으로 판단하거나, 기록되어 있는 3회의 누적 결제 데이터 생성 횟수가 미리 설정된

횃수인 5회와 대응되지 않는 것으로 판단하여, 기록되어 있는 3회의 누적 결제 데이터 생성 횃수를 1회의 거래횃수를 추가한 4회의 누적거래횃수로 갱신하여 재기록할 수 있으며, 신용카드 A에 상응하여 미리 저장되어 있는 신용카드 A에 대한 결제 바코드 정보를 제어부(150)를 통해 디스플레이부(120)로 전달함으로써, 결제 정보가 디스플레이 됨에 따라 결제가 수행되도록 하거나, 신용카드 A에 상응하여 미리 저장되어 있는 신용카드 A에 대한 신용카드 A 트랙 정보를 제어부(150)를 통해 결제부(160)로 전달함으로써 결제가 수행되도록 할 수 있다.

- [96] 본 발명의 일 실시예에 따르면, 시큐어 엘리먼트(secure element)(140)는 기록되어 있는 누적 결제 데이터 생성 횃수에 횃수가 추가되어 새롭게 계산된 누적 결제 생성 횃수가 미리 설정되어 있는 횃수를 초과하는 것으로 판단되거나, 기록되어 있는 누적 결제 데이터 생성 횃수가 미리 설정되어 있는 횃수와 대응되는 것으로 판단된 경우, 거래 횃수 한도 초과 상태(transaction counter exceed: CE)를 제어부(150)로 전송하여, 메모리(130)에 거래 횃수 한도 초과 상태(transaction counter exceed: CE)가 저장될 수 있도록 할 수 있다.
- [97] 시큐어 엘리먼트(secure element)(140)는 제1 카드 식별 정보에 상응하는 제1 카드의 트랙 정보를 기초로 결제 데이터를 생성한 경우, 기록된 누적 결제 데이터 생성 횃수를 새롭게 계산된 누적 결제 데이터 생성 횃수로 갱신하여 기록하거나, 기록된 누적 결제 데이터 생성 횃수를 증가시켜 기록할 수 있으며, 새롭게 기록된 누적 결제 데이터 생성 횃수가 미리 설정된 횃수와 대응되는 경우, 제어부(150)를 통해 디스플레이부(120)에 서버(200)와의 동기화가 필요함이 표시되도록 할 수 있다.
- [98] 예를 들어, 기록되어 있는 누적 결제 데이터 생성 횃수가 4회로 기록되어 있고, 사용자에게 의해 미리 설정되어 있는 횃수는 5회라고 가정했을 때, 기록되어 있는 누적 결제 데이터 생성 횃수가 4회로 기록되어 있는 상태에서 결제 데이터가 생성된 경우, 시큐어 엘리먼트(secure element)(140)는 기록되어 있는 누적 결제 데이터 생성 횃수를 4회에서 5회로 증가시켜 기록할 수 있으며, 이에 따라 새롭게 증가시켜 기록한 누적 결제 데이터 생성 횃수가 사용자에게 의해 미리 설정되어 있는 횃수와 대응되므로, 결제가 완료됨과 동시에 시큐어 엘리먼트(secure element)(140)는 제어부(150)를 통해 디스플레이부(120)에 서버(200)와의 동기화가 필요함이 표시되도록 할 수 있다.
- [99] 시큐어 엘리먼트(secure element)(140)는 제어부(150)를 통해 통신부(170)로부터 암호화 된 인증 정보를 포함하는 횃수 정보 변경 요청이 전달되면, 암호화 된 인증 정보를 복호화하고, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보를 비교하여, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보가 대응하는 것으로 판단된 경우, 요청 수신된 횃수 정보를 변경하여 저장함으로써, 사용자의 인증 절차를 통해 멀티 기능을 가진 카드형 디바이스(100)에 대한 횃수 정보가 임의로 변경되거나 관리되도록 할 수 있다. 시큐어 엘리먼트(secure

element)(140)는 멀티 기능을 가진 카드형 디바이스(100)의 횡수 정보를 변경하여 기록 또는 설정함에 따라, 변경된 횡수 정보를 제어부(150)를 통해 통신부(170)로 전달할 수 있다. 거래 횡수 변경 요청은, 기록된 누적 결제 데이터 생성 횡수 초기화 요청 또는 미리 설정되어 있는 횡수 변경 요청일 수 있다.

- [100] 예를 들어, 시큐어 엘리먼트(secure element)가 IC칩으로 되어 있는 멀티 기능을 가진 카드형 디바이스(100)에서 사용자가 미리 설정되어 있는 누적 결제 데이터 생성 제한 횡수를 5회에서 7회로 변경하고자 하는 경우, 제어부(150)를 통해 통신부(170)로부터 암호화 된 인증 정보가 포함된 누적 결제 데이터 생성 제한 횡수 변경 요청이 전달되면, IC칩은 암호화 된 인증 정보를 복호화하고, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보를 비교하여, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보가 대응되는 것으로 판단된 경우, 미리 설정되어 있는 5회의 누적 결제 데이터 생성 제한 횡수를 7회로 변경하여 저장할 수 있다. 또한, IC칩은 7회로 수정된 누적 결제 데이터 생성 제한 횡수 변경 결과를 제어부(150)를 통해 통신부(170)로 전달할 수 있다.
- [101] 결제부(160)는 시큐어 엘리먼트(secure element)(140)로부터 제어부(150)를 통해 카드 트랙 정보가 전달되면, 전달된 카드 트랙 정보를 기초로 결제 데이터를 생성하여, 생성된 결제 데이터를 기초로 결제가 수행되도록 할 수 있다.
- [102] 구체적으로, 결제부(160)는 시큐어 엘리먼트(secure element)(140)로부터 제어부(150)를 통해 카드 트랙 정보가 전달되면, 전달된 카드 트랙 정보를 기초로 결제 데이터를 생성하고, 생성된 결제 데이터가 제어부(150)를 통해 통신부(170)로 전달되도록 하여, 근거리 무선 통신에 의한 결제 단말기와 의 정보 송수신 등 비접촉 방식을 통해 결제 데이터를 기초로 결제가 수행될 수 있도록 할 수 있다.
- [103] 본 발명의 일 실시예에 따르면, 결제부(160)는 시큐어 엘리먼트(secure element)(140)로부터 제어부(150)를 통해 전달된 카드 트랙 정보를 기초로 생성한 결제 정보가 멀티 기능을 가진 카드형 디바이스(100)의 스크래치 방식 등 접촉식 방식으로 인식됨에 따라 결제 단말기에 전송되도록 할 수 있다.
- [104] 본 발명의 다른 실시예에 따르면, 결제부(160)는 시큐어 엘리먼트(secure element)(140)로부터 제어부(150)를 통해 전달된 카드 트랙 정보를 제어부(150)를 통해 디스플레이부(120)에 전달함으로써, 디스플레이부(120)를 통해 결제 정보가 노출되어, 비접촉 방식을 이용한 결제가 수행될 수 있도록 할 수 있다.
- [105] 예를 들어, 결제부(160)는 디스플레이부(120)를 통해 바코드 형태의 결제 정보가 노출되도록 하여, 결제 단말기가 디스플레이 된 바코드를 인식함에 따라 결제 처리가 수행되도록 할 수 있다.
- [106] 제어부(150)는 사용자 입력부(110)로부터 입력 신호가 전달됨에 따라, 제1 사용자 입력이 감지되면, 메모리(130)로 카드 식별 정보를 요청할 수 있다.
- [107] 제어부(150)는 메모리(130)로부터 미리 저장되어 있는 복수의 카드 식별 정보 중 어느 하나인 제1 카드 식별 정보를 전달 받을 수 있으며, 전달 받은 제1 카드

식별 정보를 디스플레이부(120)로 전달하여, 제1 카드 식별 정보가 디스플레이부(120)를 통해 디스플레이 되도록 제어할 수 있다.

- [108] 제어부(150)는 제1 사용자 입력이 종료된 후, 미리 설정된 소정의 결제대기시간 내에 사용자 입력부(110)로부터 제2 사용자 입력에 대한 입력 신호가 전달되지 않는 경우, 시큐어 엘리먼트(secure element)(140)로 디스플레이 되고 있는 제1 카드 식별 정보에 대한 결제 요청을 전달함으로써, 시큐어 엘리먼트(secure element)(140)에서 멀티 기능을 가진 카드형 디바이스(100)에 대한 누적 결제 데이터 생성 횟수가 확인되도록 제어할 수 있다.
- [109] 본 발명의 일 실시예에 따르면, 제어부(150)는 제1 사용자 입력이 감지된 후, 미리 설정된 소정의 결제대기시간 내에 사용자 입력부(110)로부터 제2 사용자 입력에 대한 입력 신호가 전달되는 경우, 메모리(130)로 카드 식별 정보를 재요청할 수 있으며, 메모리(130)로부터 미리 저장되어 있는 복수의 카드 식별 정보 중 다른 하나인 제2 카드 식별 정보를 전달 받아, 전달 받은 제2 카드 식별 정보를 디스플레이부(120)로 전달하여, 제2 카드 식별 정보가 디스플레이부(120)를 통해 디스플레이 되도록 제어할 수 있다.
- [110] 제어부(150)는 시큐어 엘리먼트(secure element)(140)에서 기록되어 있는 누적 결제 데이터 생성 횟수에 횟수가 추가되어 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정되어 있는 횟수를 초과하지 않는 것으로 확인되거나, 시큐어 엘리먼트(secure element)(140)에서 기록되어 있는 누적 결제 데이터 생성 횟수가 미리 설정되어 있는 횟수와 대응하지 않는 것으로 확인된 경우, 디스플레이 되고 있는 제1 카드 식별 정보에 매칭되어 시큐어 엘리먼트(secure element)(140)에 저장되어 있는 제1 카드의 트랙 정보를 전달 받을 수 있으며, 전달된 제1 카드의 트랙 정보를 결제부(160)로 전달하여, 결제부(160)를 통해 결제 데이터가 생성됨에 따라 결제가 수행되도록 제어할 수 있다.
- [111] 본 발명의 일 실시예에 따르면, 제어부(150)는 시큐어 엘리먼트(secure element)(140)에서 기록되어 있는 누적 결제 데이터 생성 횟수에 횟수가 추가되어 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정되어 있는 횟수를 초과하는 것으로 확인되거나, 시큐어 엘리먼트(secure element)(140)에서 기록되어 있는 누적 결제 데이터 생성 횟수가 미리 설정되어 있는 횟수와 대응하는 것으로 확인된 경우, 시큐어 엘리먼트(secure element)(140)로부터 거래 횟수 한도 초과 상태(transaction counter exceed: CE) 정보를 전달받을 수 있으며, 거래 횟수 한도 초과 상태(transaction counter exceed: CE)에 따른 멀티 기능을 가진 카드형 디바이스(100)의 결제 서비스 이용 불가 상태를 전달 받을 수 있다.
- [112] 제어부(150)는 시큐어 엘리먼트(secure element)(140)로부터 전달 받은 거래 횟수 한도 초과 상태(transaction counter exceed: CE)를 메모리(130)로 전달하여, 거래 횟수 한도 초과 상태(transaction counter exceed: CE)가 메모리(130)에 저장되도록 제어할 수 있다. 또한, 제어부(150)는 거래 횟수 한도 초과 상태(transaction counter exceed: CE)를 디스플레이부(120)로 전달하여, 멀티

기능을 가진 카드형 디바이스(100)를 이용한 결제 서비스 이용 불가 상태가 사용자에게 알려지도록 할 수 있다.

- [113] 본 발명의 다른 실시예에 따르면, 제어부(150)는 메모리(130)에 거래 횟수 한도 초과 상태(transaction counter exceed: CE)가 저장되어 있는 상태에서, 사용자 입력부(110)로부터 입력 신호가 전달되면, 메모리(130)에 카드 식별 정보를 요청하여, 메모리(130)로부터 저장되어 있는 거래 횟수 한도 초과 상태(transaction counter exceed: CE)가 전달되면, 이를 디스플레이부(120)로 전달함으로써, 더 이상의 결제가 수행되지 않고 결제가 요청되는 즉시 거래 횟수 한도 초과 상태(transaction counter exceed: CE)가 디스플레이 되도록 제어할 수 있다.
- [114] 본 발명의 또 다른 실시예에 따르면, 제어부(150)는 사용자 입력부(110)로부터 입력 신호가 전달되면, 메모리(130)로 멀티 기능을 가진 카드형 디바이스(100)에 대한 상태 정보 전달을 요청할 수 있으며, 메모리(130)로부터 요청한 멀티 기능을 가진 카드형 디바이스(100)에 대한 상태 정보가 전달되면, 전달된 멀티 기능을 가진 카드형 디바이스(100)의 상태 정보를 디스플레이부(120)로 전달하여 현재 멀티 기능을 가진 카드형 디바이스(100)에 대한 상태 정보가 디스플레이 되도록 제어할 수 있다.
- [115] 제어부(150)는 통신부(170)를 통해 사용자 단말기(300)로부터 암호화 된 인증 정보를 포함한 횟수 정보 변경 요청이 전달되면, 이를 시큐어 엘리먼트(secure element)(140)로 전달하여, 시큐어 엘리먼트(secure element)(140)에서 인증 정보 검증 절차를 통한 횟수 정보 변경이 수행되도록 제어할 수 있다. 또한, 제어부(150)는 시큐어 엘리먼트(secure element)(140)에서 횟수 정보 변경이 완료됨에 따라 전달되는 횟수 정보 변경 결과를 통신부(170)로 전달할 수 있다.
- [116] 본 발명의 일 실시예에 따르면, 제어부(150)는 무선 통신을 이용하여 통신부(170)를 통해 사용자 단말기(300)로부터 암호화 된 인증 정보를 포함한 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 요청이 전달되면, 이를 메모리(130)로 전달하여, 메모리(130)에서 인증 정보 검증 절차를 통한 멀티 기능을 가진 카드형 디바이스 상태 정보 변경이 수행되도록 제어할 수 있다. 또한, 제어부(150)는 메모리(130)에서 멀티 기능을 가진 카드형 디바이스 상태 정보 변경이 완료됨에 따라 전달되는 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 결과를 통신부(170)로 전달할 수 있다.
- [117] 통신부(170)는 사용자 단말기(300)와의 근거리 무선 통신을 통해 정보 송수신을 수행하거나 서버(200)와의 무선 통신을 통해 사용자 단말기(300)와의 정보 송수신을 수행할 수 있다.
- [118] 본 발명의 일 실시예에 따르면, 통신부(170)는 사용자 단말기(300) 또는 외부 서버(200)와의 무선 통신을 통해 사용자 단말기(300)로부터 암호화 된 인증 정보를 포함하는 횟수 정보 변경 요청이 수신되면, 수신된 암호화 된 인증 정보를 포함하는 횟수 정보 변경 요청을 제어부(150)로 전달할 수 있다. 또한,

통신부(170)는 시큐어 엘리먼트(secure element)(140)에서 횡수 정보 변경이 완료됨에 따라, 제어부(150)를 통해 전달되는 거래횡수정보 변경 결과를 전달 받을 수 있다.

- [119] 본 발명의 다른 실시예에 따르면, 통신부(170)는 사용자 단말기(300) 또는 외부 서버(200)와의 무선 통신을 통해 사용자 단말기(300)로부터 암호화 된 인증 정보를 포함하는 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 요청이 수신되면, 수신된 암호화 된 인증 정보를 포함하는 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 요청을 제어부(150)로 전달할 수 있다. 또한, 통신부(170)는 메모리(130)에서 멀티 기능을 가진 카드형 디바이스 상태 정보 변경이 완료됨에 따라, 제어부(150)를 통해 전달되는 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 결과를 전달 받을 수 있다.
- [120] 충전부(180)는 별도의 충전 장치와 접촉 또는 비접촉 방식으로 연결되어, 멀티 기능을 가진 카드형 디바이스(100)가 충전되도록 할 수 있다.
- [121] 도 3은 본 발명의 일 실시예에 따른 멀티 기능을 가진 카드형 디바이스(100)가 카드 결제를 지원하는 과정을 도시한 순서도이다.
- [122] 먼저, 사용자 입력부(110)에서 제1 사용자 입력이 이루어지면(S301), 사용자 입력부(110)는 제어부(150)로 입력 신호를 전달할 수 있다(S302).
- [123] 입력 신호가 전달되면, 제어부(150)는 제1 사용자 입력을 감지함에 따라 메모리(130)로 카드 식별 정보 요청을 전달할 수 있다(S303).
- [124] 메모리(130)는 제어부(150)의 요청에 의해 미리 저장되어 있는 복수의 카드 식별 정보 중 어느 하나인 제1 카드 식별 정보를 제어부(150)로 전달할 수 있으며(S304), 제어부(150)는 메모리(130)로부터 전달 받은 제1 카드 식별 정보를 디스플레이부(120)로 전달함으로써, 제1 카드 식별 정보가 멀티 기능을 가진 카드형 디바이스(100)의 디스플레이부(120)에 디스플레이 되도록 할 수 있다(S305).
- [125] 만약, 제1 사용자 입력이 종료된 후, 미리 설정된 결제대기시간 내에 사용자 입력부(110)의 제2 사용자 입력이 감지되지 않아, 결제대기시간이 초과된 경우, 제어부(150)는 디스플레이부(120)를 통해 디스플레이 되고 있는 제1 카드 식별 정보에 대한 결제 요청을 시큐어 엘리먼트(secure element)(140)로 전달할 수 있다(S306).
- [126] 예를 들어, 메모리(130)에서 전달된 신용카드 A의 식별 정보가 디스플레이부(120)를 통해 디스플레이 되고 있으며, 미리 설정된 결제대기시간이 10초라고 가정했을 때, 제1 사용자 입력이 종료된 후 10초가 지나면, 멀티 기능을 가진 카드형 디바이스(100)는 신용카드 A로 결제 카드가 자동 선택되게 되며, 신용카드 A에 대한 결제 처리를 진행하게 된다.
- [127] 제어부(150)로부터 결제 요청을 전달 받은 시큐어 엘리먼트(secure element)(140)는 기록되어 있는 멀티 기능을 가진 카드형 디바이스(100)의 누적 결제 데이터 생성 횡수를 확인하여, 기록되어 있는 누적 결제 데이터 생성

- 횃수에 횃수 증가된 누적 결제 데이터 생성 횃수가 미리 설정되어 있는 횃수를 초과하지 않는지, 또는 기록되어 있는 누적 결제 데이터 생성 횃수가 미리 설정되어 있는 횃수와 대응되지 않는지에 대한 여부를 판단할 수 있다(S307).
- [128] 누적 결제 데이터 생성 횃수 확인을 통해, 기록되어 있는 누적 결제 데이터 생성 횃수에 횃수 증가된 누적 결제 데이터 생성 횃수가 미리 설정되어 있는 횃수를 초과하지 않는 것으로 판단되거나, 기록되어 있는 누적 결제 데이터 생성 횃수가 미리 설정되어 있는 횃수와 대응되지 않는 것으로 판단된 경우, 기록되어 있는 누적 결제 데이터 생성 횃수에 거래횃수를 1회 추가하여 갱신 및 재기록할 수 있다(S308).
- [129] 예를 들어, 시큐어 엘리먼트(secure element)(140)에 미리 설정되어 있는 횃수가 5회이며, 시큐어 엘리먼트(secure element)(140)에 기록된 누적 결제 데이터 생성 횃수가 3회라고 가정하면, 제어부(150)로부터 결제 요청이 전달된 경우, 시큐어 엘리먼트(secure element)(140)는 3회의 누적 결제 데이터 생성 횃수를 4회로 갱신하여 재기록할 수 있다.
- [130] 이후, 시큐어 엘리먼트(secure element)(140)는 제어부(150)로부터 전달된 결제 요청에 포함된 제1 카드 식별 정보에 상응하는 제1 카드 트랙 정보를 제어부(150)로 전달할 수 있으며(S309), 제1 카드 트랙 정보를 전달 받은 제어부(150)는 제1 카드 식별 정보에 대한 제1 카드 트랙 정보를 결제부(160)로 전달하여, 제1 카드 식별 정보에 대한 결제가 수행되도록 할 수 있다(S310).
- [131] 본 발명의 일 실시예에 따르면, 제어부(150)로 전달된 제1 카드 식별 정보에 대한 결제 관련 정보는 디스플레이부(120)로 전달되어 비접촉 방식을 통한 결제가 수행될 수 있다.
- [132] 제어부(150)로부터 제1 카드 트랙 정보를 전달 받는 결제부(160)는 제1 카드 트랙 정보를 기초로 결제 데이터를 생성하여(S311), 생성한 결제 데이터를 기초로 결제를 수행할 수 있다(S312).
- [133] 본 발명의 일 실시예에 따르면, 결제부(160)에서 결제 데이터가 생성됨에 따라 결제가 수행 완료된 경우, 시큐어 엘리먼트(secure element)(140)는 기록된 누적 결제 데이터 생성 횃수에 횃수를 증가시켜 새롭게 갱신하여 계산된 누적 결제 데이터 생성 횃수가 미리 설정된 횃수와 대응되는 것으로 판단되면, 판단되는 즉시 제어부(150)로 서버(200)와의 동기화가 필요함을 전송하고, 제어부(150)가 디스플레이부(120)로 이를 전송함으로써, 디스플레이부(120)를 통해 서버(200)와의 동기화가 필요함이 표시될 수 있다.
- [134] 도 4는 본 발명의 일 실시예에 따른 미리 설정된 결제대기시간 내에 사용자 입력이 감지되는 경우, 멀티 기능을 가진 카드형 디바이스(100)를 통해 지원되는 카드 결제의 과정을 도시한 순서도이다.
- [135] 먼저, 사용자 입력부(110)에서 제1 사용자 입력이 이루어지는 단계부터(S401), 메모리(130)에 미리 저장된 복수의 카드 식별 정보 중 어느 하나인 제1 카드 식별 정보가 멀티 기능을 가진 카드형 디바이스(100)의 디스플레이부(120)에

- 디스플레이 되는 단계까지는(S405), 도 3과 동일하므로 설명을 생략하기로 한다.
- [136] 이 후, 제1 사용자 입력이 종료된 후, 미리 설정된 결제대기시간 내에 사용자에게 의해 사용자 입력부(110)에서 제2 사용자 입력이 이루어져(S406), 사용자 입력부(110)로부터 제2 사용자 입력에 대한 입력 신호가 전달되면(S407), 제어부(150)는 메모리(130)로 카드 식별 정보 요청을 전달할 수 있다(S408).
- [137] 카드 식별 정보 요청을 전달 받은 메모리(130)는 미리 저장된 복수의 카드 식별 정보 중 다른 하나인 제2 카드 식별 정보를 제어부(150)로 전달할 수 있으며(S409), 제어부(150)는 메모리(130)로부터 전달 받은 제2 카드 식별 정보를 디스플레이부(120)로 전달함으로써, 제2 카드 식별 정보가 멀티 기능을 가진 카드형 디바이스(100)의 디스플레이부(120)에 디스플레이 되도록 할 수 있다(S410).
- [138] 예를 들어, 메모리(130)에서 전달된 신용카드 A가 디스플레이부(120)를 통해 디스플레이 되고 있으며, 미리 설정된 결제대기시간이 10초라고 가정했을 때, 제1 사용자 입력이 종료된 후, 8초 후에 사용자 입력부(110)를 통해 제2 사용자 입력이 감지되었다면, 멀티 기능을 가진 카드형 디바이스(100)에서는 디스플레이부(120)를 통해 신용카드 B가 디스플레이 될 수 있다.
- [139] 도 5는 본 발명의 일 실시예에 따른 거래 횟수 한도 초과 상태(transaction counter exceed: CE)의 경우, 멀티 기능을 가진 카드형 디바이스(100)를 통해 지원되는 카드 결제의 과정을 도시한 순서도이다.
- [140] 먼저, 사용자 입력부(110)에서 제1 사용자 입력이 이루어지는 단계부터(S501), 시큐어 엘리먼트(secure element)(140)가 기록되어 있는 멀티 기능을 가진 카드형 디바이스(100)의 누적 결제 데이터 생성 횟수를 확인하여, 기록되어 있는 누적 결제 데이터 생성 횟수에 횟수를 증가시킴에 따라 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정되어 있는 횟수를 초과하는지에 대한 여부 판단 또는 기록되어 있는 누적 결제 데이터 생성 횟수가 미리 설정되어 있는 횟수와 대응하는지에 대한 여부를 판단하는 단계까지는(S507), 도 3과 동일하므로 설명을 생략하기로 한다.
- [141] 누적 결제 데이터 생성 횟수 확인을 통해, 기록되어 있는 누적 결제 데이터 생성 횟수에 횟수를 증가시킴에 따라 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정되어 있는 횟수를 초과하는 것으로 판단되거나, 기록되어 있는 누적 결제 데이터 생성 횟수가 미리 설정되어 있는 횟수와 대응하는 것으로 판단된 경우, 시큐어 엘리먼트(secure element)(140)는 거래 횟수 한도 초과 상태(transaction counter exceed: CE)를 제어부(150)로 전달할 수 있다(S508).
- [142] 시큐어 엘리먼트(secure element)(140)로부터 거래 횟수 한도 초과 상태(transaction counter exceed: CE)를 전달 받은 제어부(150)는 거래 횟수 한도 초과 상태(transaction counter exceed: CE)를 메모리(130)로 전달하여(S509), 메모리(130)에 거래 횟수 한도 초과 상태(transaction counter exceed: CE)가 저장되도록 할 수 있으며(S510), 거래 횟수 한도 초과 상태(transaction counter

exceed: CE)를 디스플레이부(120)로 전달하여 사용자가 거래 횟수 한도 초과 상태(transaction counter exceed: CE)에 따른 멀티 기능을 가진 카드형 디바이스(100)를 이용한 결제 서비스 이용 불가 상태를 인지할 수 있도록 할 수 있다(S511).

[143] 이 후, 멀티 기능을 가진 카드형 디바이스(100)의 거래 횟수 한도가 초과되어 멀티 기능을 가진 카드형 디바이스(100)를 이용한 결제 서비스 이용이 불가능한 상태에서, 사용자 입력부(110)에서 제2 사용자 입력이 이루어짐에 따라(S512), 사용자 입력부(110)로부터 제어부(150)에 제2 사용자 입력에 대한 입력 신호가 전달된 경우(S513), 제어부(150)는 메모리(130)로 카드 식별 정보 요청을 전달할 수 있으며(S514), 이에 따라 메모리(130)는 저장되어 있는 거래 횟수 한도 초과 상태(transaction counter exceed: CE)를 제어부(150)에 전달함으로써(S515), 더 이상의 결제 처리 수행이 진행되지 않도록 할 수 있다.

[144] 또한, 제어부(150)는 거래 횟수 한도 초과 상태(transaction counter exceed: CE)를 다시 한번 디스플레이부(120)에 전달함으로써, 사용자가 거래 횟수 한도 초과 상태(transaction counter exceed: CE)에 따른 멀티 기능을 가진 카드형 디바이스(100)를 이용한 결제 서비스 이용 불가 상태를 인지할 수 있도록 할 수 있다(S516).

[145] 예를 들어, 시큐어 엘리먼트(secure element)(140)에 미리 설정되어 있는 횟수가 5회이며, 시큐어 엘리먼트(secure element)(140)에 기록되어 있는 누적거래횟수가 5회라고 가정하면, 제어부(150)로부터 결제 요청이 전달된 경우, 시큐어 엘리먼트(secure element)(140)는 제어부(150)로 거래 횟수 한도 초과 상태(transaction counter exceed: CE)를 전달할 수 있으며, 이에 따라, 디스플레이부(120)에 거래 횟수 한도 초과에 따른 멀티 기능을 가진 카드형 디바이스(100)를 이용한 결제 서비스 이용 불가 상태가 디스플레이 되어 사용자에게 제공될 수 있다. 또한, 메모리(130)는 제어부(150)로부터 전달된 거래 횟수 한도 초과 상태(transaction counter exceed: CE)를 저장함으로써, 거래 횟수 한도 초과 상태(transaction counter exceed: CE)가 저장된 이후부터 사용자 입력부(110)가 입력되어 제어부(150)로부터 카드 식별 정보 요청이 수신되는 경우, 즉시 제어부(150)로 저장된 거래 횟수 하도 초과 상태를 전송하여, 거래 횟수 한도 초과 상태(transaction counter exceed: CE)가 디스플레이부(120)를 통해 디스플레이 되도록 할 수 있다.

[146] 즉, 메모리(130)에 거래 횟수 한도 초과 상태(transaction counter exceed: CE) 정보가 저장됨에 따라 결제가 제한된 상태에서는 제어부(150)가 시큐어 엘리먼트(secure element)(140)를 참조하지 않고도 결제 서비스 이용 불가 상태임을 사용자에게 알릴 수 있다.

[147] 도 6은 본 발명의 일 실시예에 따른 인증 절차를 통해 횟수 정보 변경 또는 멀티 기능을 가진 카드형 디바이스 상태 정보 변경이 가능하도록 하는 멀티 기능을 가진 카드형 디바이스(100)의 카드 결제 지원 과정을 도시한 순서도이다.

- [148] 도 6에 도시된 (a)와 같이, 사용자 입력부(110)에서의 사용자 입력으로 인해 현재 멀티 기능을 가진 카드형 디바이스 상태 정보가 디스플레이 될 수 있다.
- [149] 먼저, 사용자 입력부(110)를 통해 제1 사용자 입력이 이루어지면(S601a), 사용자 입력부(110)는 제어부(150)로 입력 신호를 전달할 수 있다(S602a).
- [150] 입력 신호가 전달되면, 제어부(150)는 메모리(130)로 멀티 기능을 가진 카드형 디바이스 상태 정보를 요청할 수 있으며(S603a), 메모리(130)는 제어부(150)로 현재 저장되어 있는 멀티 기능을 가진 카드형 디바이스 상태 정보를 전달할 수 있다. 이 후, 제어부(150)는 메모리(130)로부터 전달 받은 멀티 기능을 가진 카드형 디바이스 상태 정보를 디스플레이부(120)로 전송함으로써, 현재 멀티 기능을 가진 카드형 디바이스 상태가 어떠한 상태로 설정되어 있는지 디스플레이 되도록 할 수 있다.
- [151] 예를 들어, 메모리(130)에 결제 서비스 이용 가능 상태가 저장되어 있으면, 사용자에게 의해 사용자 입력부(110)가 입력되는 경우, 결제 서비스 이용 가능 상태가 디스플레이부(120)를 통해 디스플레이 될 수 있으며, 메모리(130)에 멀티 기능을 가진 카드형 디바이스 잠금 상태가 저장되어 있으면, 사용자에게 의해 사용자 입력부(110)가 입력되는 경우, 멀티 기능을 가진 카드형 디바이스 잠금 상태가 디스플레이부(120)를 통해 디스플레이 될 수 있다.
- [152] 본 발명의 일 실시예에 따르면, 메모리(130)로부터 전달된 멀티 기능을 가진 카드형 디바이스 상태 정보가 멀티 기능을 가진 카드형 디바이스 미등록 상태인 경우, 제어부(150)는 디스플레이부(120)로 멀티 기능을 가진 카드형 디바이스 등록 화면을 전달하여, 멀티 기능을 가진 카드형 디바이스 등록 화면이 디스플레이 되도록 제어할 수 있다.
- [153] 도 6에 도시된 (b)와 같이, 사용자가 무선 통신을 통해 핏수 정보를 변경할 수 있다.
- [154] 먼저, 통신부(170)가 서버(200) 또는 사용자 단말기(300)와의 무선 통신을 수행할 수 있다(S601b). 이 때, 서버(200)는 인증 서버일 수 있으며, 사용자 단말기(300)와 멀티 기능을 가진 카드형 디바이스(100)의 정보 송수신을 연결해주는 네트워크 서버일 수 있다. 또한, 사용자 단말기(300)와의 무선 통신은, NFC, 블루투스 등의 근거리 무선 통신일 수 있다.
- [155] 통신부(170)는 서버(200) 또는 사용자 단말기(300)와의 무선 통신을 통해 사용자 단말기(300)로부터 암호화 된 인증 정보 및 핏수 정보 변경 요청을 수신할 수 있다. 이 때, 사용자 단말기(300)로부터 수신되는 암호화 된 인증 정보는, 사용자 단말기(300)의 요청에 의해 보안 및 인증 서비스 관련 서버로부터 사용자 단말기(300)에 발급된 인증 정보일 수 있으며, 암호화 되어 있는 상태로 발급된 인증 정보일 수 있다. 또한, 암호화 된 인증 정보에는, 사용자 고유 정보가 포함되어 있을 수 있다.
- [156] 이 후, 통신부(170)는 무선 통신을 통해 사용자 단말기(300)로부터 수신된 암호화 된 인증 정보를 포함하는 핏수 정보 변경 요청을 제어부(150)를 통해

- 시큐어 엘리먼트(secure element)(140)로 전달할 수 있다(S602b, S603b).
- [157] 통신부(170)로부터 암호화 된 인증 정보를 포함하는 횡수 정보 변경 요청을 전달 받은 시큐어 엘리먼트(secure element)(140)는 전달된 암호화 된 인증 정보를 복호화하여, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보와의 대응 여부를 판단하는 검증 절차를 수행할 수 있다(S604b).
- [158] 인증 정보 검증 절차를 통해, 사용자 단말기(300)로부터 수신되어 복호화 된 인증 정보가 시큐어 엘리먼트(secure element)(140)에 미리 저장되어 있는 인증 정보와 대응되는 것으로 판단되면, 시큐어 엘리먼트(secure element)(140)는 무선 통신을 통해 사용자 단말기(300)로부터 요청된 횡수 정보 변경을 수행하여, 변경된 횡수 정보를 저장할 수 있다(S605b).
- [159]
- [160] *예를 들어, 사용자 단말기(300)로부터 암호화 된 인증 정보와 함께 누적 결제 데이터 생성 횡수 초기화 요청이 수신된 경우, 통신부(170)는 제어부(150)를 통해 시큐어 엘리먼트(secure element)(140)에 암호화 된 인증 정보를 포함하는 누적 결제 데이터 생성 횡수 초기화 요청을 전달할 수 있으며, 시큐어 엘리먼트(secure element)(140)는 전달된 암호화 된 인증 정보를 복호화하고, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보의 대응 여부 판단을 통한 검증을 수행하여, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보가 대응되는 것으로 판단된 경우, 기록되어 있는 누적 결제 데이터 생성 횡수를 초기화 할 수 있다. 즉, 기록되어 있는 누적 결제 데이터 생성 횡수가 5회인 경우, 이를 삭제하여 누적 결제 데이터 생성 횡수를 0회로 재기록할 수 있다.
- [161] 한편, 사용자 단말기(300)로부터 암호화 된 인증 정보와 함께 미리 설정된 누적 결제 데이터 생성 제한 횡수 변경 요청이 수신된 경우, 통신부(170)는 제어부(150)를 통해 시큐어 엘리먼트(secure element)(140)에 암호화 된 인증 정보를 포함하는 미리 설정된 누적 결제 데이터 생성 제한 횡수 변경 요청을 전달할 수 있으며, 시큐어 엘리먼트(secure element)(140)는 전달된 암호화 된 인증 정보를 복호화하고, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보의 대응 여부 판단을 통한 검증을 수행하여, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보가 대응되는 것으로 판단된 경우, 설정되어 있는 누적 결제 데이터 생성 제한 횡수를 사용자가 변경하고자 하는 횡수로 정정할 수 있다. 즉, 미리 설정되어 있는 누적 결제 데이터 생성 제한 횡수가 5회인 상태에서 사용자 단말기(300)로부터 인증 정보와 함께 누적 결제 데이터 생성 제한 횡수 7회 변경의 요청이 수신되었다면, 시큐어 엘리먼트(secure element)(140)는 누적 결제 데이터 생성 제한 횡수를 7회로 정정하여 재설정 할 수 있다.
- [162] 또한, 시큐어 엘리먼트(secure element)(140)는 변경 완료된 횡수 정보를 제어부(150)를 통해 통신부(170)로 전달할 수 있다(S606b, S607b).
- [163] 본 발명의 일 실시예에 따르면, 제어부(150)를 통해 시큐어 엘리먼트(secure

element)(140)로부터 핏수 정보 변경 결과를 전달 받은 통신부(170)는 사용자의 설정에 따라, 무선 통신을 통해 핏수 정보 변경 결과를 사용자 단말기(300)로 전송할 수 있다.

- [164] 도 6에 도시된 (c)와 같이, 사용자가 무선 통신을 통해 멀티 기능을 가진 카드형 디바이스 상태 정보를 변경할 수 있다.
- [165] 먼저, 통신부(170)가 서버(200) 또는 사용자 단말기(300)와의 무선 통신을 수행할 수 있다(S601c). 이 때, 서버(200)는 인증 서버일 수 있으며, 사용자 단말기(300)와 멀티 기능을 가진 카드형 디바이스(100)의 정보 송수신을 연결해주는 네트워크 서버일 수 있다. 또한, 사용자 단말기(300)와의 무선 통신은, NFC, 블루투스 등의 근거리 무선 통신일 수 있다.
- [166] 통신부(170)는 서버(200) 또는 사용자 단말기(300)와의 무선 통신을 통해 사용자 단말기(300)로부터 암호화 된 인증 정보 및 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 요청을 수신할 수 있다. 이 때, 사용자 단말기(300)로부터 수신되는 암호화 된 인증 정보는, 사용자 단말기(300)의 요청에 의해 보안 및 인증 서비스 관련 서버로부터 사용자 단말기(300)에 발급된 인증 정보일 수 있으며, 암호화 되어 있는 상태로 발급된 인증 정보일 수 있다. 또한, 암호화 된 인증 정보에는, 사용자 고유 정보가 포함되어 있을 수 있다.
- [167] 이 후, 통신부(170)는 무선 통신을 통해 사용자 단말기(300)로부터 수신된 암호화 된 인증 정보를 포함하는 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 요청을 제어부(150)를 통해 메모리(130)로 전달할 수 있다(S602c, S603c).
- [168] 통신부(170)로부터 암호화 된 인증 정보를 포함하는 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 요청을 전달 받은 메모리(130)는 전달된 암호화 된 인증 정보를 복호화하여, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보와의 대응 여부를 판단하는 검증 절차를 수행할 수 있다(S604c).
- [169] 인증 정보 검증 절차를 통해, 사용자 단말기(300)로부터 수신되어 복호화 된 인증 정보가 메모리(130)에 미리 저장되어 있는 인증 정보와 대응되는 것으로 판단되면, 메모리(130)는 무선 통신을 통해 사용자 단말기(300)로부터 요청된 멀티 기능을 가진 카드형 디바이스 상태 정보 변경을 수행하여, 변경된 멀티 기능을 가진 카드형 디바이스 상태 정보를 저장할 수 있다(S605c).
- [170] 예를 들어, 사용자 단말기(300)로부터 암호화 된 인증 정보와 함께 멀티 기능을 가진 카드형 디바이스 잠금 상태 설정 요청이 수신된 경우, 통신부(170)는 제어부(150)를 통해 메모리(130)에 암호화 된 인증 정보를 포함하는 멀티 기능을 가진 카드형 디바이스 잠금 상태 설정 요청을 전달할 수 있으며, 메모리(130)는 전달된 암호화 된 인증 정보를 복호화하고, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보의 대응 여부 판단을 통한 검증을 수행하여, 복호화 된 인증 정보와 미리 저장되어 있는 인증 정보가 대응되는 것으로 판단된 경우, 미리 저장 또는 설정되어 있는 결제 서비스 이용 가능 상태의 멀티 기능을 가진 카드형 디바이스 상태 정보를 요청된 멀티 기능을 가진 카드형 디바이스 잠금

설정 상태로 변경할 수 있다. 이에 따라, 인증된 사용자의 권한에 의해 임의로 멀티 기능을 가진 카드형 디바이스(100)가 잠금 설정되고, 타인의 사용이 불가능하도록 할 수 있다. 반면, 잠금 상태로 설정되어 있는 멀티 기능을 가진 카드형 디바이스 상태 정보에서 인증이 완료된 사용자의 요청에 의해 결제 서비스 이용 가능 상태로 멀티 기능을 가진 카드형 디바이스 상태가 변경될 수 있다.

- [171] 또한, 메모리(130)는 변경 완료된 멀티 기능을 가진 카드형 디바이스 상태 정보를 제어부(150)를 통해 통신부(170)로 전달할 수 있다(S606c, S607c).
- [172] 본 발명의 일 실시예에 따르면, 제어부(150)를 통해 메모리(130)로부터 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 결과를 전달 받은 통신부(170)는 사용자의 설정에 따라, 무선 통신을 통해 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 결과를 사용자 단말기(300)로 전송할 수 있다.
- [173] 도 7은 본 발명의 일 실시예에 따른 멀티 기능을 가진 카드형 디바이스(100)의 상태 정보 변경 순환 구조를 개략적으로 도시한 도면이다.
- [174] 먼저, 멀티 기능을 가진 카드형 디바이스(100) 내 시큐어 엘리먼트(secure element)(140)에서 기록된 누적 결제 데이터 생성 횟수에 횟수가 증가되어 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하거나 시큐어 엘리먼트(secure element)(140)에 기록된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수와 대응되는 것으로 확인되면, 멀티 기능을 가진 카드형 디바이스(100)는 거래 횟수 한도 초과 상태(transaction counter exceed: CE)일 수 있다.
- [175] 멀티 기능을 가진 카드형 디바이스(100) 내 통신부(170)와 사용자 단말기(300)와의 인증이 성공적으로 이루어짐에 따라, 제어부(150)로부터 잠금 명령이 수신되면, 멀티 기능을 가진 카드형 디바이스(100)의 상태 정보가 거래 횟수 한도 초과 상태(transaction counter exceed: CE)에서 잠금 상태(locked: LD)로 설정 변경될 수 있으며(701), 제어부(150)로부터 종료 명령이 수신되면, 멀티 기능을 가진 카드형 디바이스(100)의 상태 정보가 잠금 상태(locked: LD)에서 종료 상태(terminated: TE)로 설정 변경되거나(702), 거래 횟수 한도 초과 상태(transaction counter exceed: CE)에서 종료 상태(terminated: TE)로 설정 변경될 수 있다(703). 이 때, 잠금 명령 또는 종료 명령은 사용자의 제어에 의해 사용자 단말기(300)로부터 통신부(170)를 통해 제어부(150)로 수신된 것일 수 있다.
- [176] 또한, 멀티 기능을 가진 카드형 디바이스(100) 내 통신부(170)와 사용자 단말기(300)와의 인증이 성공적으로 이루어짐에 따라, 제어부(150)로부터 잠금 해제 명령이 수신되면, 멀티 기능을 가진 카드형 디바이스(100)의 상태 정보가 잠금 상태(locked: LD)에서 결제 서비스 이용 가능 상태(registered: RD)로 설정 변경될 수 있으며(704), 반면, 제어부(150)로부터 잠금 명령이 수신되면, 멀티 기능을 가진 카드형 디바이스(100)의 상태 정보가 결제 서비스 이용 가능 상태(registered: RD)에서 잠금 상태(locked: LD)로 설정 변경될 수 있다(705). 이

- 때, 잠금 명령 또는 잠금 해제 명령은 사용자의 제어에 의해 사용자 단말기(300)로부터 통신부(170)를 통해 제어부(150)로 수신된 것일 수 있다.
- [177] 한편, 멀티 기능을 가진 카드형 디바이스(100)가 최초로 등록되면, 제어부(150)로부터 결제 서비스 활성화 명령이 전달되어, 멀티 기능을 가진 카드형 디바이스(100)의 상태 정보가 미등록 상태(not registered: NR)에서 결제 서비스 이용 가능 상태(registered: RD)로 설정 변경될 수 있다(706). 이 때, 결제 서비스 활성화 명령은 멀티 기능을 가진 카드형 디바이스(100)가 최초로 등록됨에 따라 자체적으로 생성되어 전달될 수 있다.
- [178] 또한, 멀티 기능을 가진 카드형 디바이스(100) 내 통신부(170)와 사용자 단말기(300)와의 인증이 성공적으로 이루어짐에 따라, 제어부(150)로부터 종료 명령이 수신되면, 멀티 기능을 가진 카드형 디바이스(100)의 상태 정보가 결제 서비스 이용 가능 상태(registered: RD)에서 종료 상태(terminated: TE)로 설정 변경될 수 있다(707).
- [179] 한편, 멀티 기능을 가진 카드형 디바이스(100) 내 시큐어 엘리먼트(secure element)(140)에서 기록된 누적 결제 데이터 생성 횟수에 횟수가 증가되어 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하는 것으로 확인되거나, 시큐어 엘리먼트(secure element)(140)에 기록된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수와 대응되는 것으로 확인되면, 제어부(150)로부터 거래 횟수 한도 초과 상태 명령이 전송됨에 따라 결제 서비스 이용 가능 상태(registered: RD)의 멀티 기능을 가진 카드형 디바이스 상태 정보가 거래 횟수 한도 초과 상태(transaction counter exceed: CE)로 설정 변경될 수 있다(708). 이 때, 거래 횟수 한도 초과 상태 명령은 시큐어 엘리먼트(secure element)(140)에서 생성되어 제어부(150)로 전송되는 것일 수 있다.
- [180] 반면, 멀티 기능을 가진 카드형 디바이스(100) 내 통신부(170)와 사용자 단말기(300)와의 인증이 성공적으로 이루어짐에 따라, 제어부(150)로부터 누적 거래 데이터 생성 횟수 초기화 명령이 수신되면, 멀티 기능을 가진 카드형 디바이스(100)의 상태 정보가 거래 횟수 한도 초과 상태(transaction counter exceed: CE)에서 결제 서비스 이용 가능 상태(registered: RD)로 설정 변경될 수 있다(709). 이 때, 누적 거래 데이터 생성 횟수 초기화 명령은 사용자의 제어에 의해 사용자 단말기(300)로부터 통신부(170)를 통해 제어부(150)로 수신된 것일 수 있다.
- [181] 이와 같이, 본 발명의 일 실시예에 따르면, 결제대기시간 초과 여부에 따라 멀티 기능을 가진 카드형 디바이스 내에 저장되어 있는 결제 카드 정보가 자동 선택되어 결제가 수행될 수 있도록 함으로써, 사용자 입장에서는, 제한된 사용자 입력부의 구성에도 불구하고, 1회의 입력만으로 최적화된 카드 식별 정보 조회 및 결제 카드 선택이 가능하다는 장점이 있다.
- [182] 또한, 본 발명의 일 실시예에 따르면, 사용자에게 의해 설정된 횟수를 기준으로 누적 결제 데이터 생성 횟수 정보에 기초한 멀티 기능을 가진 카드형 디바이스

결제 서비스가 제공되며, 누적된 결제 데이터 생성 횟수가 미리 설정된 횟수에 대응되거나, 누적된 결제 데이터 생성 횟수에 횟수가 증가되어 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하면 사용자에게 알림이 제공되므로, 사용자가 특정 거래횟수만큼만 결제가 수행될 수 있도록 하여, 별도의 보안 설정 및 보안 정보 입력을 수행하지 않아도 거래횟수제한에 따른 자동적인 보안 설정을 할 수 있다는 효과가 있다.

- [183] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.
- [184] 본 발명의 범위는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

청구범위

- [청구항 1] 멀티 기능을 가진 카드형 디바이스가, 카드 결제를 지원하는 방법에 있어서,
 (a) 제1 사용자 입력이 감지되면, 메모리에 미리 저장되어 있는 복수의 카드 식별 정보 중 어느 하나인 제1 카드 식별 정보를 디스플레이 하는 단계;
 (b) 상기 제1 사용자 입력이 종료된 후, 미리 설정된 소정의 결제대기시간 동안 제2 사용자 입력이 감지되지 않으면, (i) 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수를 증가시키고, 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하는지 확인하거나, (ii) 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수와 대응되는지 확인하는 단계; 및
 (c) 상기 확인 결과, 상기 새롭게 계산된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수를 초과하지 않거나, 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수와 대응하지 않는 것으로 확인된 경우, 상기 제1 카드 식별 정보에 상응하는 상기 시큐어 엘리먼트(secure element)에 저장된 상기 제1 카드의 트랙 정보를 기초로 결제 데이터를 생성하여 카드 결제가 수행될 수 있도록 하는 단계를 포함하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법.
- [청구항 2] 제 1항에 있어서,
 상기 (b) 단계에서,
 상기 확인 결과, 상기 새롭게 계산된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수를 초과하거나, 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수가 상기 미리 설정된 횟수와 대응되는 것으로 확인된 경우, 상기 멀티 기능을 가진 카드형 디바이스의 상태를 거래 횟수 한도 초과 상태(transaction counter exceed: CE)로 설정하여 상기 메모리에 저장하고, 디스플레이부를 통해 서버와의 동기화가 필요함을 표시하는 것을 특징으로 하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법.
- [청구항 3] 제 1항에 있어서,
 상기 (c) 단계는,
 상기 제1 카드 식별 정보에 상응하는 상기 시큐어 엘리먼트(secure element)에 저장된 상기 제1 카드의 트랙 정보를 기초로 상기 결제 데이터를 생성한 경우, 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수를 상기 새롭게 계산된 누적 결제 데이터 생성

- 횃수로 갱신하여 기록하거나 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횃수를 증가시켜 기록하는 단계를 포함하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법.
- [청구항 4] 제 3항에 있어서,
상기 시큐어 엘리먼트(secure element)에 새롭게 기록된 누적 결제 데이터 생성 횃수가 상기 미리 설정된 횃수와 대응되는 경우, 디스플레이부를 통해 서버와의 동기화가 필요함을 표시하는 것을 특징으로 하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법.
- [청구항 5] 제 3항에 있어서,
상기 시큐어 엘리먼트(secure element)에 새롭게 기록된 누적 결제 데이터 생성 횃수가 상기 미리 설정된 횃수와 대응되지 않는 경우, 상기 메모리 상에서 상기 멀티 기능을 가진 카드형 디바이스의 상태를 결제 서비스 이용 가능 상태(registered: RD)로 유지하고 상태 메시지를 디스플레이 하는 것을 특징으로 하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법.
- [청구항 6] 제 1항에 있어서,
상기 멀티 기능을 가진 카드형 디바이스가 서버에 최초로 등록되면, 상기 멀티 기능을 가진 카드형 디바이스의 상태를 결제 서비스 이용 가능 상태(registered: RD)로 설정하고 상기 메모리에 저장하는 단계를 더 포함하는 것을 특징으로 하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법.
- [청구항 7] 제 6항에 있어서,
일단 상기 멀티 기능을 가진 카드형 디바이스가 결제 서비스 이용 가능 상태(registered: RD)로 설정되면, 더 이상 미등록 상태(not registered: NR)로 상태 전환이 되지 않는 것을 특징으로 하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법.
- [청구항 8] 제 1항에 있어서,
잠금 상태(locked: LD) 설정으로 미리 설정되어 있는 사용자의 입력이 감지되는 경우, 상기 멀티 기능을 가진 카드형 디바이스의 상태를 잠금 상태(locked: LD)로 설정하는 것을 특징으로 하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법.
- [청구항 9] 제 8항에 있어서,
상기 잠금 상태(locked: LD)에서 상기 멀티 기능을 가진 카드형 디바이스 인증이 있는 경우에 한하여 결제 서비스 이용 가능 상태(registered: RD)로 변경이 가능한 것을 특징으로 하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법.
- [청구항 10] 제 1항에 있어서,
상기 (b) 단계는,

상기 제1 사용자 입력이 종료된 후, 상기 미리 설정된 소정의 결제대기시간 동안 제2 사용자 입력이 감지되면, 상기 메모리에 미리 저장되어 있는 복수의 카드 식별 정보 중 어느 하나인 제2 카드 식별 정보를 디스플레이 하는 단계를 포함하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법.

- [청구항 11] 제 1항에 있어서,
 (e) 사용자 단말기로부터 암호화 된 인증 정보를 포함하는 횡수 정보 변경 요청이 수신되면, 수신된 인증 정보를 복호화하여, 복호화된 인증 정보와 상기 시큐어 엘리먼트(secure element)에 미리 저장된 인증 정보와의 대응 여부를 판단하는 단계; 및
 (f) 복호화된 인증 정보와 상기 시큐어 엘리먼트(secure element)에 미리 저장된 인증 정보가 대응되는 것으로 판단된 경우, 상기 시큐어 엘리먼트(secure element)에 기록 또는 설정되어 있는 횡수 정보를 상기 변경 요청된 횡수 정보로 변경하여 기록 또는 설정하는 단계를 더 포함하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법.

- [청구항 12] 제 11항에 있어서,
 상기 횡수 정보 변경 요청은,
 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횡수 초기화 요청 및 상기 미리 설정된 횡수 변경 요청 중 적어도 어느 하나인 것으로 하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법.

- [청구항 13] 제 1항에 있어서,
 (g) 사용자 단말기로부터 암호화 된 인증 정보를 포함하는 상기 멀티 기능을 가진 카드형 디바이스 상태 정보 변경 요청이 수신되면, 수신된 인증 정보를 복호화하여, 복호화된 인증 정보와 상기 메모리에 미리 저장된 인증 정보와의 대응 여부를 판단하는 단계; 및
 (h) 복호화된 인증 정보와 상기 메모리에 미리 저장된 인증 정보가 대응되는 것으로 판단된 경우, 상기 메모리에 저장되어 있는 상기 멀티 기능을 가진 카드형 디바이스의 상태 정보를 요청된 상태 정보로 변경하여 저장하는 단계를 더 포함하는, 멀티 기능을 가진 카드형 디바이스의 카드 결제 지원 방법.

- [청구항 14] 하나 이상의 제어 수단으로 되어 있으며, 사용자에게 의해 입력되면, 입력 신호를 제어부로 전달하는 사용자 입력부;
 제어부로부터 전달되는 카드 식별 정보 또는 멀티 기능을 가진 카드형 디바이스 상태 정보를 디스플레이 하는 디스플레이부;
 하나 이상의 카드 식별 정보 각각에 상응하는 카드 트랙 정보 및 인증 정보가 저장되어 있으며, 누적 결제 데이터 생성 횡수가 기록되어 있는 시큐어 엘리먼트(secure element);

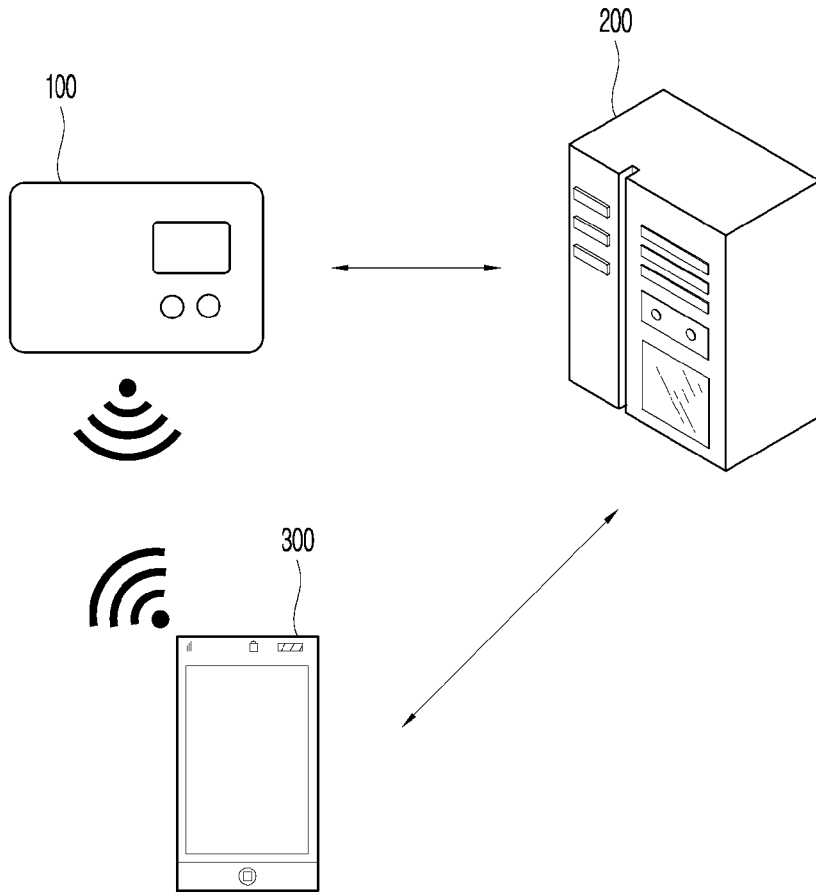
하나 이상의 카드 식별 정보, 멀티 기능을 가진 카드형 디바이스 상태 정보 및 인증 정보가 저장되어 있는 메모리;

상기 시큐어 엘리먼트(secure element)에 저장된 카드 트랙 정보를 기초로 결제 데이터를 생성하고, 생성한 결제 데이터를 기초로 카드 결제를 수행하는 결제부;

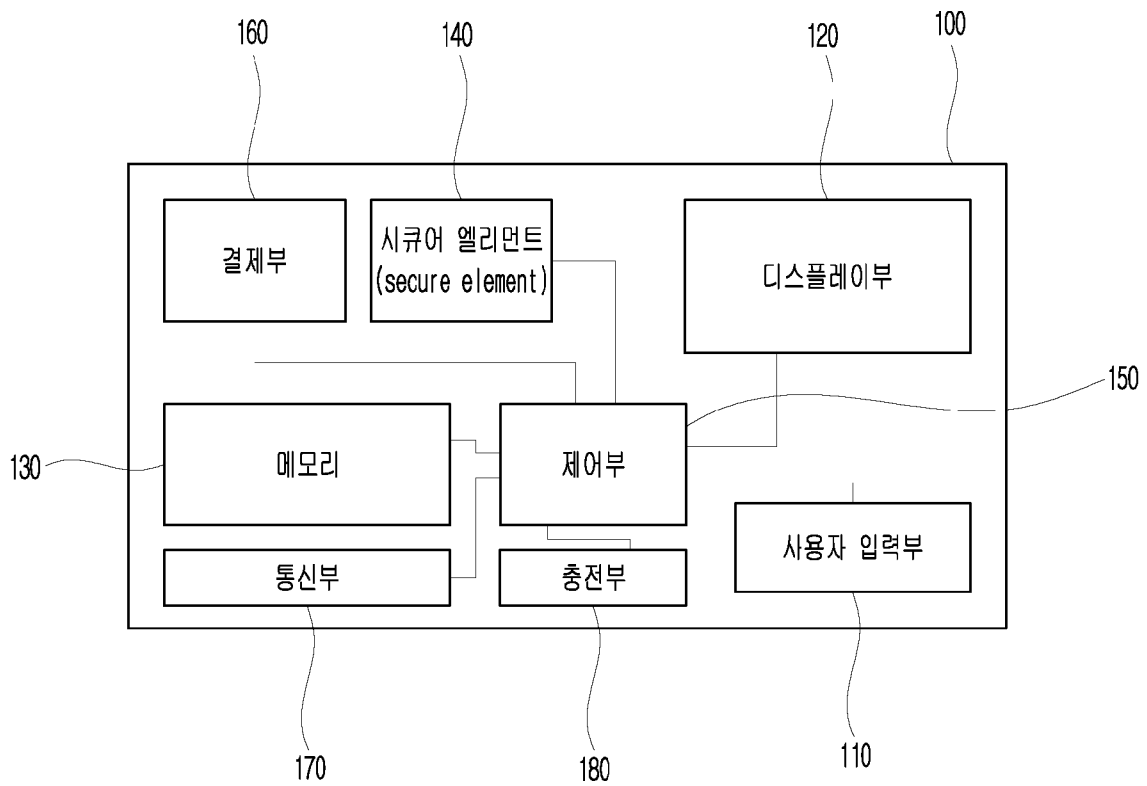
(i) 제1 사용자 입력이 감지되면, 상기 메모리에 미리 저장되어 있는 복수의 카드 식별 정보 중 어느 하나인 제1 카드 식별 정보가 디스플레이 되도록 제어하고, (ii) 제1 사용자 입력이 종료된 후, 미리 설정된 소정의 결제대기시간 동안 제2 사용자 입력이 감지되지 않으면, 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수에 횟수를 증가시켜 새롭게 계산된 누적 결제 데이터 생성 횟수의 미리 설정된 횟수 초과 여부가 확인되거나, 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수의 미리 설정된 횟수 대응 여부가 확인되도록 제어하고, (iii) 확인 결과, 새롭게 계산된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수를 초과하지 않거나, 상기 시큐어 엘리먼트(secure element)에 기록된 누적 결제 데이터 생성 횟수가 미리 설정된 횟수와 대응하지 않는 것으로 확인된 경우, 상기 제1 카드 식별 정보에 상응하는 상기 시큐어 엘리먼트(secure element)에 저장된 제1 카드의 트랙 정보를 기초로 결제 데이터가 생성되어 카드 결제가 수행될 수 있도록 제어하는 제어부;

사용자 단말기 또는 외부 서버와의 통신을 수행하는 통신부; 및 멀티 기능을 가진 카드형 디바이스가 충전될 수 있도록 하는 충전부를 포함하는, 멀티 기능을 가진 카드형 디바이스.

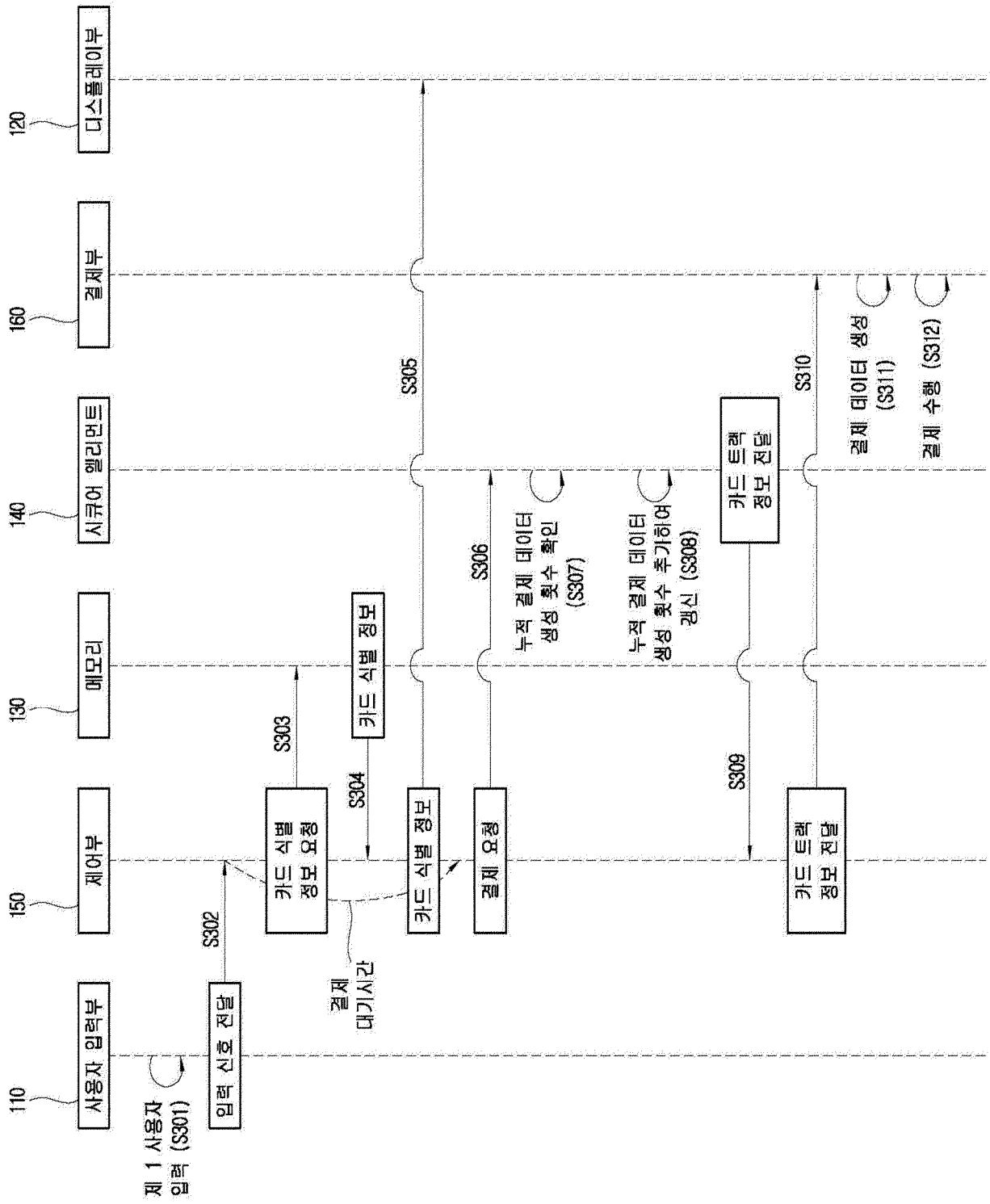
[도1]



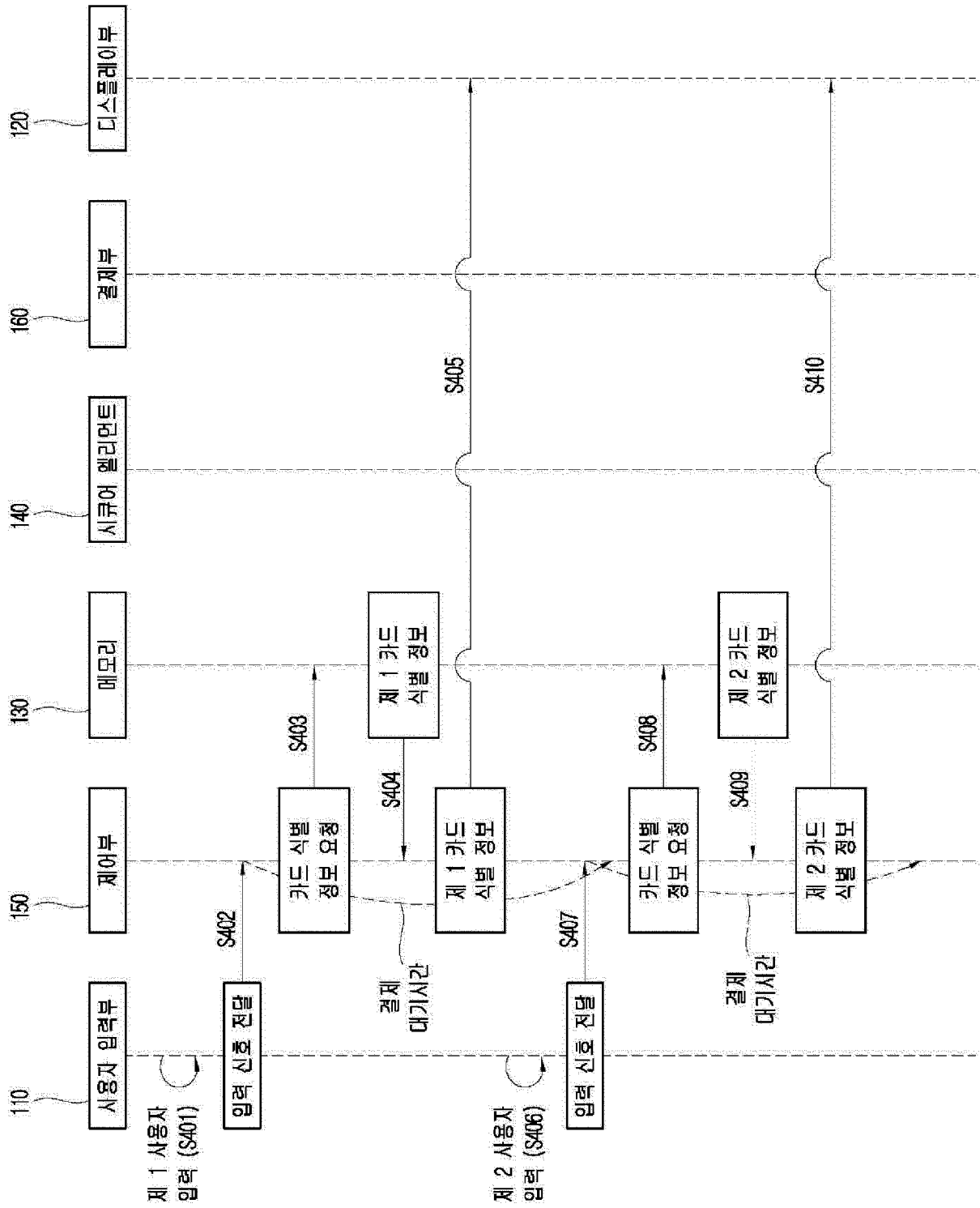
[도2]



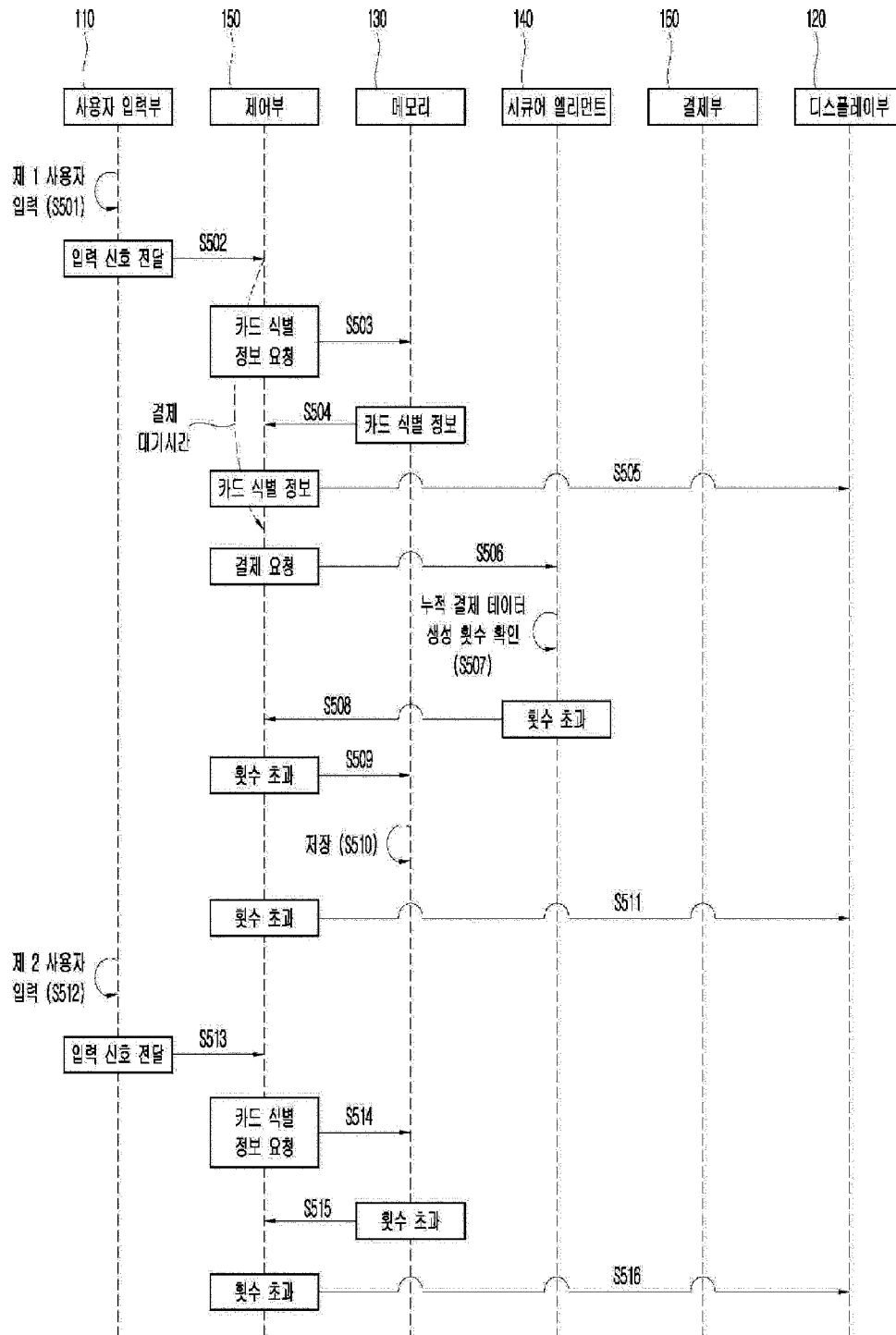
[도3]



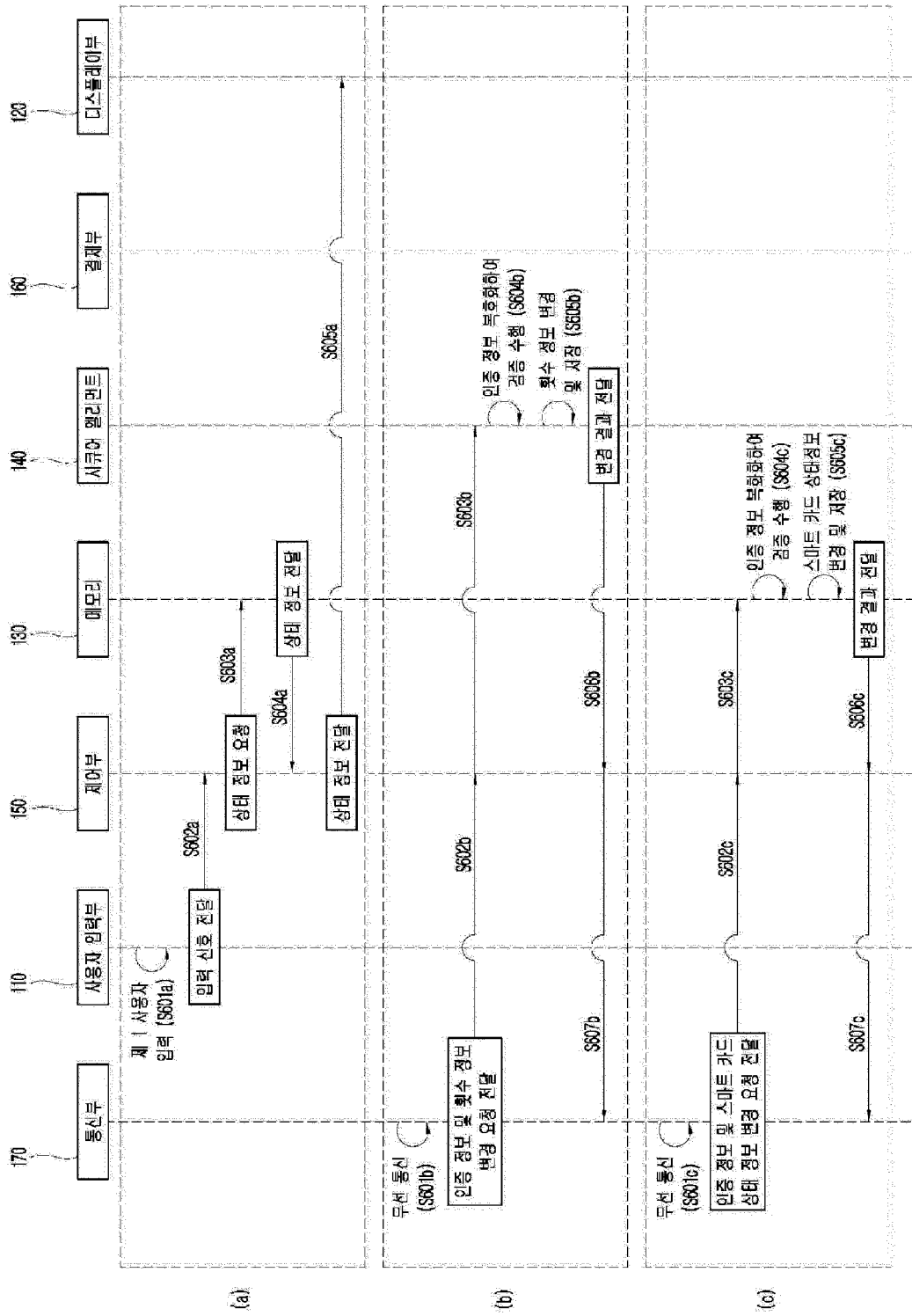
[도4]



[도5]



[도6]

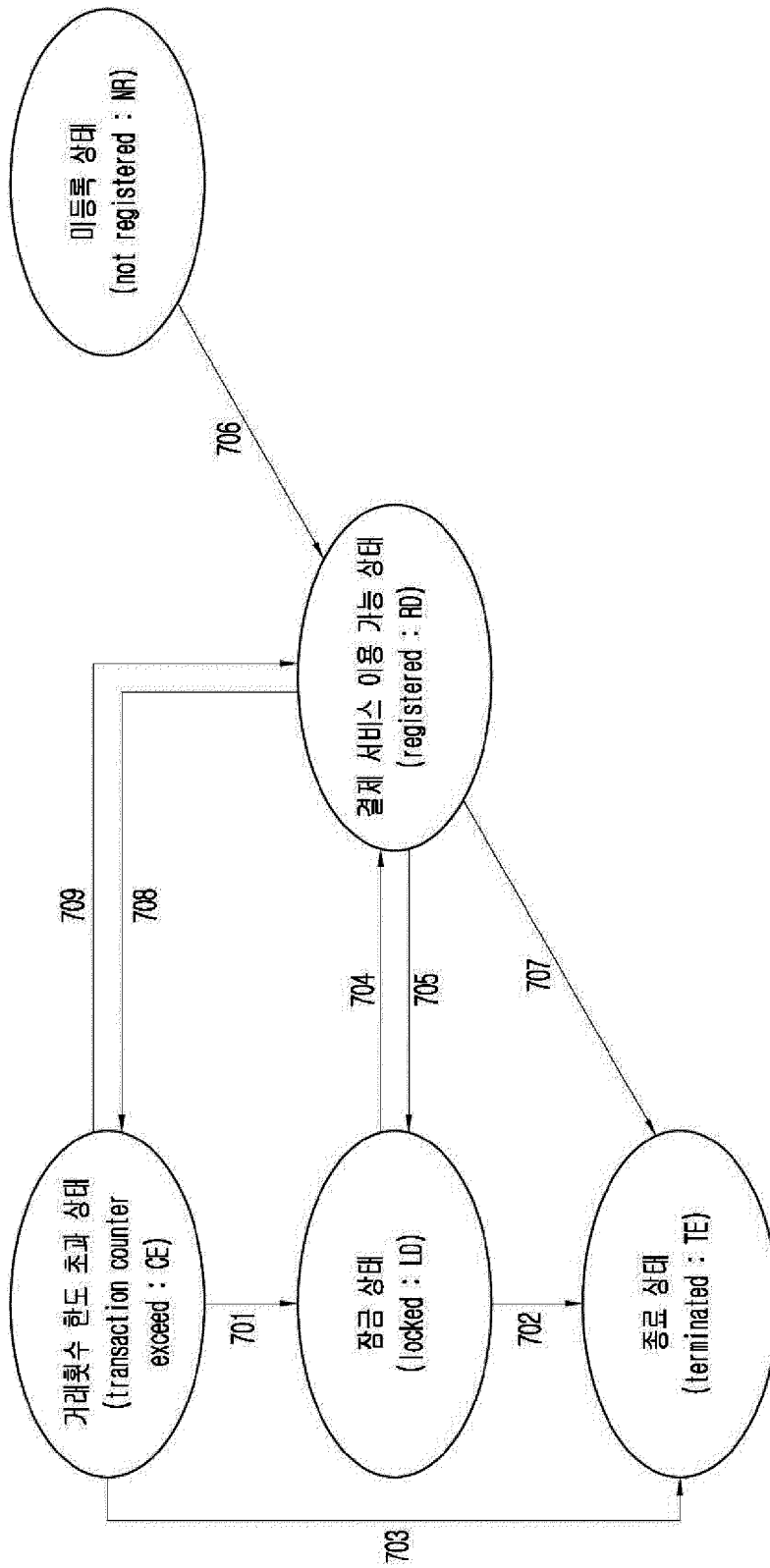


(a)

(b)

(c)

[도7]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2017/004982

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/34(2012.01)i, G06K 19/07(2006.01)i, G06Q 20/32(2012.01)i, G06Q 20/38(2012.01)i, G06Q 20/40(2012.01)i, G06Q 40/02(2012.01)i, G06Q 10/06(2012.01)i, G06Q 10/10(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q 20/34; G06Q 20/24; G06K 19/10; G06Q 20/32; G06K 19/07; G06Q 20/16; G06Q 20/38; G06Q 20/40; G06Q 40/02; G06Q 10/06; G06Q 10/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: first, second, user input, secure element, accumulation, payment data, number, card, payment

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2015-183590 A1 (APPLE INC.) 03 December 2015 See claims 1, 20 and figure 1.	1-14
A	KR 10-2015-0128073 A (KT CORPORATION) 18 November 2015 See paragraph [0062], claims 1, 12 and figure 5.	1-14
A	KR 10-2016-0008444 A (BRILLIANTTS CO., LTD.) 22 January 2016 See claim 1 and figure 1.	1-14
A	KR 10-2015-0123572 A (MOZIDO CORFIRE - KOREA, LTD.) 04 November 2015 See paragraphs [0015], [0017], claims 8, 10 and figures 1-2.	1-14
A	KR 10-2016-0023750 A (LEE, Do-Hun) 03 March 2016 See paragraphs [0056]-[0057], claims 1, 7 and figures 4, 7.	1-14



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family


Date of the actual completion of the international search

15 SEPTEMBER 2017 (15.09.2017)

Date of mailing of the international search report

15 SEPTEMBER 2017 (15.09.2017)

Name and mailing address of the ISA/KR

 Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2017/004982

Patent document cited in search report	Publication date	Patent family member	Publication date
WO 2015-183590 A1	03/12/2015	CN 106255984 A	21/12/2016
		EP 3149682 A1	05/04/2017
		KR 10-2016-0137613 A	30/11/2016
		US 2015-0348007 A1	03/12/2015
		US 2016-0203467 A1	14/07/2016
		US 9299072 B2	29/03/2016
KR 10-2015-0128073 A	18/11/2015	KR 10-1602465 B1	10/03/2016
		US 2015-0324766 A1	12/11/2015
KR 10-2016-0008444 A	22/01/2016	CN 106489157 A	08/03/2017
		CN 106489158 A	08/03/2017
		CN 106537419 A	22/03/2017
		EP 3171298 A1	24/05/2017
		EP 3171299 A1	24/05/2017
		JP 2017-522211 A	10/08/2017
		JP 2017-522680 A	10/08/2017
		JP 2017-524219 A	24/08/2017
		KR 10-1598371 B1	29/02/2016
		KR 10-1613855 B1	20/04/2016
		KR 10-2016-0008451 A	22/01/2016
		KR 10-2016-0008452 A	22/01/2016
		KR 10-2016-0008474 A	22/01/2016
		US 2017-0206444 A1	20/07/2017
		US 2017-0213119 A1	27/07/2017
		US 2017-0213120 A1	27/07/2017
		WO 2016-010320 A1	21/01/2016
WO 2016-010324 A1	21/01/2016		
WO 2016-010325 A1	21/01/2016		
WO 2016-010327 A1	21/01/2016		
KR 10-2015-0123572 A	04/11/2015	KR 10-1623636 B1	23/05/2016
		US 2017-0132629 A1	11/05/2017
		WO 2015-163739 A1	29/10/2015
KR 10-2016-0023750 A	03/03/2016	WO 2017-138789 A1	17/08/2017

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06Q 20/34(2012.01)i, G06K 19/07(2006.01)i, G06Q 20/32(2012.01)i, G06Q 20/38(2012.01)i, G06Q 20/40(2012.01)i, G06Q 40/02(2012.01)i, G06Q 10/06(2012.01)i, G06Q 10/10(2012.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06Q 20/34; G06Q 20/24; G06K 19/10; G06Q 20/32; G06K 19/07; G06Q 20/16; G06Q 20/38; G06Q 20/40; G06Q 40/02; G06Q 10/06; G06Q 10/10

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 제1, 제2, 사용자입력, 시큐어엘리먼트, 누적, 결제데이터, 횡수, 카드, 결제

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	WO 2015-183590 A1 (APPLE INC.) 2015.12.03 청구항 1,20 및 도면 1 참조.	1-14
A	KR 10-2015-0128073 A (주식회사 케이티) 2015.11.18 단락 [0062], 청구항 1,12 및 도면 5 참조.	1-14
A	KR 10-2016-0008444 A (브릴리언츠 주식회사) 2016.01.22 청구항 1 및 도면 1 참조.	1-14
A	KR 10-2015-0123572 A (모지도코화이어코리아 유한회사) 2015.11.04 단락 [0015],[0017], 청구항 8,10 및 도면 1-2 참조.	1-14
A	KR 10-2016-0023750 A (이도훈) 2016.03.03 단락 [0056]-[0057], 청구항 1,7 및 도면 4,7 참조.	1-14

추가 문헌이 C(계속)에 기재되어 있습니다.

대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2017년 09월 15일 (15.09.2017)

국제조사보고서 발송일

2017년 09월 15일 (15.09.2017)

ISA/KR의 명칭 및 우편주소



대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-481-8578

심사관

장기정

전화번호 +82-42-481-8364



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
WO 2015-183590 A1	2015/12/03	CN 106255984 A EP 3149682 A1 KR 10-2016-0137613 A US 2015-0348007 A1 US 2016-0203467 A1 US 9299072 B2	2016/12/21 2017/04/05 2016/11/30 2015/12/03 2016/07/14 2016/03/29
KR 10-2015-0128073 A	2015/11/18	KR 10-1602465 B1 US 2015-0324766 A1	2016/03/10 2015/11/12
KR 10-2016-0008444 A	2016/01/22	CN 106489157 A CN 106489158 A CN 106537419 A EP 3171298 A1 EP 3171299 A1 JP 2017-522211 A JP 2017-522680 A JP 2017-524219 A KR 10-1598371 B1 KR 10-1613855 B1 KR 10-2016-0008451 A KR 10-2016-0008452 A KR 10-2016-0008474 A US 2017-0206444 A1 US 2017-0213119 A1 US 2017-0213120 A1 WO 2016-010320 A1 WO 2016-010324 A1 WO 2016-010325 A1 WO 2016-010327 A1	2017/03/08 2017/03/08 2017/03/22 2017/05/24 2017/05/24 2017/08/10 2017/08/10 2017/08/24 2016/02/29 2016/04/20 2016/01/22 2016/01/22 2016/01/22 2017/07/20 2017/07/27 2017/07/27 2016/01/21 2016/01/21 2016/01/21 2016/01/21
KR 10-2015-0123572 A	2015/11/04	KR 10-1623636 B1 US 2017-0132629 A1 WO 2015-163739 A1	2016/05/23 2017/05/11 2015/10/29
KR 10-2016-0023750 A	2016/03/03	WO 2017-138789 A1	2017/08/17