(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년09월26일
(11) 등록번호 10-1778755
(24) 등록일자 2017년09월08일

(51) 국제특허분류(Int. Cl.)
G06Q 20/20 (2012.01) *G06Q 20/32* (2012.01)
G06Q 20/38 (2012.01) *H04B 5/02* (2006.01)
(52) CPC특허분류
G06Q 20/20 (2013.01)
G06Q 20/32 (2013.01)
(21) 출원번호 10-2016-7029349(분할)
(22) 출원일자(국제) 2013년04월09일
심사청구일자 2016년10월20일
(85) 번역문제출일자 2016년10월20일
(65) 공개번호 10-2016-0127155
(43) 공개일자 2016년11월02일
(62) 원출원 특허 10-2015-7021234
원출원일자(국제) 2013년04월09일
심사청구일자 2015년08월06일
(86) 국제출원번호 PCT/US2013/035865
(87) 국제공개번호 WO 2013/158419
국제공개일자 2013년10월24일
(30) 우선권주장
61/635,277 2012년04월18일 미국(US)
(56) 선행기술조사문헌
KR100822160 B1
KR1020080102439 A
US20110078079 A1

(73) 특허권자
구글 인코포레이티드
미국 캘리포니아 마운틴 뷰 엠피시어터 파크웨이 1600 (우:94043)
(72) 발명자
주스티 사렐 코버스
미국 캘리포니아 94043 마운틴 뷰 앰피시어터 파크웨이 1600 구글 인코포레이티드 내
(74) 대리인
박장원

전체 청구항 수 : 총 27 항 심사관 : 이재근

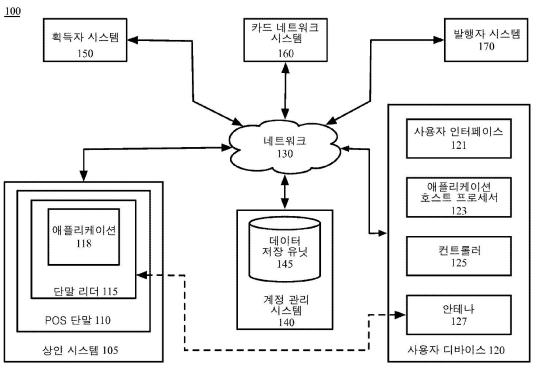
(54) 발명의 명칭 **보안 요소를 갖지 않는 지불 거래들의 처리**

(57) 요 약

사용자는 사용자 디바이스 상에 상주하는 보안 요소에 액세스하는 것 없이 사용자 디바이스로부터의 지불 정보를 단말 리더(terminal reader)에 송신함으로써 상인 시스템과 무선 지불 거래를 수행한다. 사용자는 상인 시스템의 단말 리더의 무선 주파수 필드(radio frequency field)에서 사용자 디바이스를 태핑(tapping)한다. 단말 리더

(뒷면에 계속)

대 표 도



및 사용자 디바이스는 통신 채널을 설정하고 단말 리더는 지불 처리 응답에 대한 요청을 포함하는 신호를 송신한다. 신호는 사용자 디바이스에 의해 수신되고 컨트롤러(controller)에 의해 애플리케이션 호스트 프로세서(application host processor)에 의해 이해가능한 요청으로 변환한다. 컨트롤러는 요청을 애플리케이션 호스트 프로세서에 송신하며, 여기서 요청은 처리되고, 응답은 컨트롤러에 송신된 다음 단말 리더에 송신된다. 애플리케이션 호스트 프로세서에 의해 생성되는 응답은 지불 응답으로 상인 시스템에 의해 식별가능하다.

(52) CPC특허분류
G06Q 20/38 (2013.01)
H04B 5/02 (2013.01)

명 세 서

청구범위

청구항 1

컴퓨터에 의해 구현되는, 보안 메모리들에 액세스(access)하지 않고 지불 거래들을 처리하는 방법으로서,

이동 컴퓨팅 디바이스에 의해 그리고 상인 시스템 컴퓨팅 디바이스(merchant system computing device)로부터, 지불 거래를 처리하기 위해 지불 계정 정보(payment account information)에 대한 요청을 수신하는 단계와;

상기 이동 컴퓨팅 디바이스에 의해, 상기 지불 계정 정보에 대한 상기 요청을 비-보안 요소 프로세서(non-secure element processor)에 의해 이해 가능한 요청으로 변환함으로써 상기 지불 계정 정보에 대한 상기 요청을 처리하는 단계 - 상기 비-보안 요소 프로세서는 복수의 지불 제공자(payment provider)들 중 어느 지불 제공자에 대한 금융 계정 정보(financial account information)를 이용하여 상기 지불 거래들을 처리할 수 있게 함 - 와;

상기 이동 컴퓨팅 디바이스의 상기 비-보안 요소 프로세서에 의해, 보안 요소 프로세서에 의해 생성된 응답과 구별 불가능한(indistinguishable) 상기 지불 계정 정보에 대한 상기 요청의 응답을 생성하는 단계 - 상기 응답은 지불 계정 식별자(payment account identifier)를 포함하고, 상기 비-보안 요소 프로세서에 의해 상기 응답을 생성하는 것은 상기 이동 컴퓨팅 디바이스로 하여금 복수의 지불 제공자들 중 어느 지불 제공자에 대한 금융 계정 정보를 이용해서 지불 거래들을 처리하게 함 - 와; 그리고

상기 이동 컴퓨팅 디바이스에 의해, 상기 지불 계정 정보에 대한 상기 요청의 상기 응답을 상기 상인 시스템 컴퓨팅 디바이스에 송신하는 단계를 포함하는 컴퓨터에 의해 구현되는 방법.

청구항 2

제 1항에 있어서,

상기 지불 계정 식별자는 상기 이동 컴퓨팅 디바이스에 의해 생성되는 것을 특징으로 하는 컴퓨터에 의해 구현되는 방법.

청구항 3

제 1항에 있어서,

상기 지불 계정 식별자는 계정 관리 시스템에 의해 생성되고 상기 이동 컴퓨팅 디바이스에 송신되며, 상기 계정 관리 시스템은 계정을 유지하고, 이 계정은 상기 이동 컴퓨팅 디바이스와 관련된 사용자에 대한 신용 카드 계정, 인출 계정, 저장 값 계정, 기프트 카드(gift card) 계정, 및 은행 계정 중 적어도 하나에 대한 정보를 포함하는 것을 특징으로 하는 컴퓨터에 의해 구현되는 방법.

청구항 4

제 1항에 있어서,

상기 지불 계정 식별자는 제한된 사용 횟수에 대해서만 유효한 것을 특징으로 하는 컴퓨터에 의해 구현되는 방법.

청구항 5

제 1항에 있어서,

상기 지불 계정 식별자는 지리적 제한 및 시간 제한 중 적어도 하나와 관련된 것을 특징으로 하는 컴퓨터에 의해 구현되는 방법.

청구항 6

제 1항에 있어서,

상기 지불 계정 식별자는 신용 카드 계정, 인출 계정, 저장 값 계정, 기프트 카드 계정, 및 은행 계정 번호 중 하나를 포함하는 것을 특징으로 하는 컴퓨터에 의해 구현되는 방법.

청구항 7

제 1항에 있어서,

상기 지불 계정 식별자는 상기 이동 컴퓨팅 디바이스 상의 디지털 지갑 애플리케이션으로부터 검색되는 것을 특징으로 하는 컴퓨터에 의해 구현되는 방법.

청구항 8

제 1항에 있어서,

지불 처리 응답에 대한 상기 요청은 근거리 통신(NFC; near field communication) 프로토콜을 사용하여 수신되는 것을 특징으로 하는 컴퓨터에 의해 구현되는 방법.

청구항 9

제 2항에 있어서,

상기 이동 컴퓨팅 디바이스에 의해, 지불 요청의 처리 동안 지불 계정 식별자의 검증(verification)을 위해 계정 관리 시스템에 상기 지불 계정 식별자를 통신하는 단계를 더 포함하는 것을 특징으로 하는 컴퓨터에 의해 구현되는 방법.

청구항 10

제 2항에 있어서,

상기 이동 컴퓨팅 디바이스에 상주하는 상기 비-보안 요소 프로세서는 지불 요청의 처리 동안 계정 관리 시스템에 의해 복제될 수 있는 방식을 사용하여 지불 계정 번호를 생성하는 것을 특징으로 하는 컴퓨터에 의해 구현되는 방법.

청구항 11

제 1항에 있어서,

상기 이동 컴퓨팅 디바이스는 상기 상인 시스템 컴퓨팅 디바이스로부터 수신된 지불 계정 정보에 대한 상기 요청을 상기 비-보안 요소 프로세서에 의해 이해 가능한 요청을 포함하는 바이트들로 변환하는 것을 특징으로 하는 컴퓨터에 의해 구현되는 방법.

청구항 12

컴퓨터 판독가능 프로그램 명령들이 수록된 비-일시적 컴퓨터 판독가능 매체로서, 상기 컴퓨터 판독가능 프로그램 명령들은 이동 컴퓨팅 디바이스에 의해 실행될 때 상기 이동 컴퓨팅 디바이스가 보안 메모리들에 액세스하지 않고 지불 거래들을 처리하게 하며, 상기 컴퓨터 판독가능 프로그램 명령들은:

상인 컴퓨팅 디바이스로부터, 지불 거래를 처리하기 위한 지불 계정 정보에 대한 요청을 수신하기 위한 컴퓨터 판독가능 프로그램 명령들과;

상기 지불 계정 정보에 대한 상기 요청을 비-보안 요소 프로세서에 의해 이해 가능한 요청으로 변환함으로써 상기 지불 계정 정보에 대한 요청을 처리하기 위한 컴퓨터 판독가능 프로그램 명령들 - 상기 비-보안 요소 프로세서는 복수의 지불 제공자들 중 어느 지불 제공자에 대한 금융 계정 정보를 이용하여 상기 지불 거래들을 처리할 수 있게 함 - 과;

보안 요소 프로세서에 의해 생성된 응답과 구별 불가능한 상기 지불 계정 정보에 대한 상기 요청의 응답을 생성하기 위한 컴퓨터 판독가능 프로그램 명령들 - 상기 응답은 지불 계정 식별자를 포함함 - 과; 그리고

상기 지불 계정 정보에 대한 상기 요청의 상기 응답을 상기 상인 컴퓨팅 디바이스에 송신하는 컴퓨터 판독가능 프로그램 명령들을 포함하는 것을 특징으로 하는 비-일시적 컴퓨터 판독가능 매체.

청구항 13

제 12항에 있어서,

상기 지불 계정 식별자는 상기 이동 컴퓨팅 디바이스에 의해 생성되는 프록시 계정 번호를 포함하는 것을 특징으로 하는 비-일시적 컴퓨터 판독가능 매체.

청구항 14

제 12항에 있어서,

상기 지불 계정 식별자는 계정 관리 시스템에 의해 생성되고 상기 이동 컴퓨팅 디바이스에 송신되는 프록시 계정 번호를 포함하며, 상기 계정 관리 시스템은 계정을 유지하고, 이 계정은 상기 이동 컴퓨팅 디바이스에 관련된 사용자에 대한 신용 카드 계정, 인출 계정, 저장 값 계정, 기프트 카드 계정, 및 은행 계정 번호 중 하나에 대한 정보를 포함하는 것을 특징으로 하는 비-일시적 컴퓨터 판독가능 매체.

청구항 15

제 12항에 있어서,

상기 지불 계정 식별자는 제한된 사용 횟수에 대해서만 유효한 프록시 계정 번호를 포함하는 것을 특징으로 하는 비-일시적 컴퓨터 판독가능 매체.

청구항 16

제 12항에 있어서,

상기 지불 계정 식별자는 지리적 제한 및 시간 제한 중 적어도 하나와 관련되는 프록시 계정 번호를 포함하는 것을 특징으로 하는 비-일시적 컴퓨터 판독가능 매체.

청구항 17

지불 거래들을 처리하는 이동 컴퓨팅 디바이스로서,

저장 디바이스;

상기 저장 디바이스에 통신가능하게 결합된 컨트롤러; 그리고

상기 저장 디바이스 및 상기 컨트롤러에 통신가능하게 결합된 프로세서를 포함하며,

상기 이동 컴퓨팅 디바이스의 상기 컨트롤러는 상기 저장 디바이스에 저장된 애플리케이션 코드 명령들을 실행하고, 상기 애플리케이션 코드 명령들은 상기 이동 컴퓨팅 디바이스로 하여금:

상인 시스템 컴퓨팅 디바이스로부터 지불 거래를 처리하기 위한 지불 계정 정보에 대한 요청을 수신하고; 그리고

상기 지불 계정 정보에 대한 상기 요청을 상기 프로세서에 의해 이해 가능한 요청으로 변환함으로써 상기 지불 계정 정보에 대한 상기 요청을 처리 - 상기 프로세서는 상기 이동 컴퓨팅 디바이스로 하여금 복수의 지불 제공자들 중 어느 지불 제공자에 대한 금융 계정 정보를 이용하여 상기 지불 거래들을 처리하도록 함 - 하게 하며; 그리고

상기 이동 컴퓨팅 디바이스의 상기 프로세서는 상기 저장 디바이스에 저장된 애플리케이션 코드 명령들을 실행하고, 상기 애플리케이션 코드 명령들은 상기 이동 컴퓨팅 디바이스로 하여금:

보안 요소 프로세서에 의해 생성된 응답과 구별 불가능한 상기 지불 계정 정보에 대한 상기 요청의 응답을 생성하게 하고, 상기 응답은 지불 계정 식별자를 포함하고, 상기 프로세서에 의해 상기 응답을 생성하는 것은 상기 이동 컴퓨팅 디바이스로 하여금 복수의 지불 제공자들 중 어느 지불 제공자에 대한 금융 계정 정보를 사용하여 지불 거래들을 처리하게 하는 것을 특징으로 하는 이동 컴퓨팅 디바이스.

청구항 18

제 17항에 있어서,

상기 지불 계정 식별자는 비-보안 요소 프로세서에 의해 생성되는 것을 특징으로 하는 이동 컴퓨팅 디바이스.

청구항 19

청구항 17에 있어서,

상기 지불 계정 식별자는 상기 이동 컴퓨팅 디바이스 상의 디지털 지갑 애플리케이션으로부터 검색되는 것을 특징으로 하는 이동 컴퓨팅 디바이스.

청구항 20

제 17항에 있어서,

상기 이동 컴퓨팅 디바이스의 상기 프로세서는 상기 이동 컴퓨팅 디바이스로 하여금 지불 요청의 처리 동안 계정 관리 시스템에 의해 복제될 수 있는 방식을 사용하여 지불 계정 식별자를 생성하게 하는 상기 저장 디바이스에 저장된 컴퓨터 실행 가능 명령들을 실행하도록 더 구성되는 것을 특징으로 하는 이동 컴퓨팅 디바이스.

청구항 21

제 17항에 있어서,

상기 지불 계정 식별자는 계정 관리 시스템에 의해 생성되고 상기 이동 컴퓨팅 디바이스에 송신되며, 상기 계정 관리 시스템은 계정을 유지하고, 이 계정은 상기 이동 컴퓨팅 디바이스에 관련된 사용자에 대한 신용 카드 계정, 인출 계정, 저장 값 계정, 기프트 카드 계정, 및 은행 계정 번호 중 하나에 대한 정보를 포함하는 것을 특징으로 하는 이동 컴퓨팅 디바이스.

청구항 22

제 17항에 있어서,

상기 지불 계정 식별자는 제한된 사용 횟수에 대해서만 유효한 것을 특징으로 하는 이동 컴퓨팅 디바이스.

청구항 23

제 17항에 있어서,

상기 지불 계정 식별자는 지리적 제한 및 시간 제한 중 적어도 하나와 관련되는 것을 특징으로 하는 이동 컴퓨팅 디바이스.

청구항 24

제 17항에 있어서,

상기 이동 컴퓨팅 디바이스의 상기 프로세서는 상기 이동 컴퓨팅 디바이스로 하여금 지불 계정 식별자의 검증을 위해 계정 관리 시스템에 상기 지불 계정 식별자를 통신하게 하는 상기 저장 디바이스에 저장된 컴퓨터 실행 가능 명령들을 실행하도록 더 구성되며, 상기 계정 관리 시스템에 대한 통신은 상기 이동 컴퓨팅 디바이스에 의해 상기 상인 시스템 컴퓨팅 디바이스에 송신된 상기 지불 계정 정보에 대한 상기 요청의 상기 응답을 포함하는 것을 특징으로 하는 이동 컴퓨팅 디바이스.

청구항 25

제 17항에 있어서,

상기 이동 컴퓨팅 디바이스의 상기 프로세서는 지불 요청의 처리 동안 계정 관리 시스템에 의해 복제될 수 있는 방식을 사용하여 상기 지불 계정 식별자를 생성하는 것을 특징으로 하는 이동 컴퓨팅 디바이스.

청구항 26

제 17항에 있어서,

상기 컨트롤러는 근거리 통신 컨트롤러를 포함하는 것을 특징으로 하는 이동 컴퓨팅 디바이스.

청구항 27

제 17항에 있어서,

상기 컨트롤러는 블루투스(Bluetooth) 컨트롤러를 포함하는 것을 특징으로 하는 이동 컴퓨팅 디바이스.

청구항 28

삭제

청구항 29

삭제

발명의 설명

기 술 분 야

[0001] 본 특허 출원은 2012년 4월 18일 출원되고 발명의 명칭이 "Processing a Contactless Payment Transaction Without a Secure Element"인 미국 특허 출원 제61/635,277호에 대한 우선권을 주장한다. 상기 식별된 출원의 전체 내용들은 이로써 본 명세서에 참고문헌으로 통합된다.

[0002] 본 발명은 일반적으로 지불 거래(payment transaction)에 관한 것으로, 특히 사용자 디바이스의 보안 요소에 액세스하는 것 없이 사용자 컴퓨팅 디바이스를 통해 이루어지는 지불 거래에 관한 것이다.

배 경 기 술

[0003] 현재의 근거리 무선 통신("NFC"; near field communication) 시스템들은 금융 거래들, 교통 티켓팅(transit ticketing), 식별 및 인증, 물리적 보안 액세스, 및 다른 기능들을 위한 보안 동작 환경을 제공하기 위해 통신 디바이스들 상에 설치된 "보안 요소(secure element)"로 통상 지칭되는 하드웨어(hardware) 구성요소에 의존한다. 보안 요소는 일반적으로 쉽게 변경할 수 없는 마이크로프로세서(microprocessor), 메모리(memory), 및 운영 체제를 갖는 그 자체의 동작 환경을 포함한다. NFC 컨트롤러(controller)는 상인의 판매 시점 관리("POS"; point of sale) 시스템으로부터 지불 요청 메시지를 수신하고 메시지를 처리를 위한 보안 요소에 송신한다. 전형적인 NFC 컨트롤러는 보안 요소를 포함한다. 신뢰받는 서비스 관리자("TSM"; trusted service manager), 또는 다른 형태의 보안 서비스 제공자는 다른 것들 가운데서, 보안 요소에 애플리케이션들(applications) 및 데이터(data)를 설치하고, 프로비저닝(provisioning)하고, 개인화할 수 있다. 보안 요소는 전형적으로 제조 시에 설치되는 하나 이상의 액세스 키들(access keys)을 갖는다. 대응하는 키는 보안 요소를 갖는 디바이스가 최종 사용자에게 소유되는 동안, TSM이 보안 요소의 설치, 프로비저닝, 및 개인화를 위해 보안 요소에 암호 보안 채널을 설정할 수 있도록, TSM에 의해 공유된다. 이러한 방식으로, 보안 요소는 디바이스 내의 호스트 CPU가 손상되었을지라도 보안을 유지할 수 있다.

[0004] 현재의 NFC 시스템들이 갖는 하나의 결핍은 보안 요소와 TSM 사이에 밀착 결합이 존재한다는 것이다. 현재의 배치들에 대해, 하나의 TSM만이 특정 보안 요소의 키들에 액세스할 수 있다. 따라서, 최종 사용자는 하나의 TSM에 의해서만 공급되는 보안 요소 피처들(features)을 프로비저닝하는 것을 선택할 수 있다. 디바이스의 제조자는 전형적으로 이러한 TSM을 선택한다. 예를 들어, 스마트폰(smart phone) 제조자는 최종 사용자보다는 스마트폰을 구매하는, 스프린트(Sprint) 또는 버라이즌(Verizon)과 같은, 이동 통신망 사업자("MNO"; mobile network operator)로부터의 안내 하에 스마트폰들에 대한 TSM을 선택할 수 있다. 따라서, 최종 사용자에게 이용가능한 TSM 피처들은 최종 사용자의 관심에 있지 않을 수 있다. 일 예로서, MNO는 마스터카드(MasterCard) 또는 뱅크 오브 아메리카(Bank of America)와 같은, 단 하나의 지불 제공자와 영업 관계를 가질 수 있다. 그러한 TSM은 보안 요소가 하나의 지불 제공자만으로부터의 지불 명령들로 프로비저닝되는 것을 허용할 수 있다. 따라서, 최종 사용자는 비자(VISA)와 같은, 다른 지불 제공자들로부터의 서비스들에 액세스할 수 없을 것이다.

발명의 내용

과제의 해결 수단

[0005] 본 명세서에 설명된 임의의 대표적인 측면들에서, 보안 요소에 액세스하는 것 없이 지불 거래를 처리하는 방법

은 사용자 디바이스와 통신 채널을 가능하게 하는 단말 리더(terminal reader)를 포함한다. 사용자는 단말 리더의 무선 주파수 필드에서 사용자 디바이스를 태핑(tapping)한다. 단말 리더 및 사용자 디바이스는 통신 채널을 설정하고, 단말 리더는 지불 처리 응답에 대한 요청을 포함하는 신호를 송신한다. 신호는 사용자 디바이스에 의해 수신되고 컨트롤러에 의해 애플리케이션 호스트 프로세서(application host processor)에 의해 이해가능한 요청으로 변환된다. 컨트롤러는 요청을 애플리케이션 호스트 프로세서에 송신하며, 여기서 요청은 처리되고 응답은 컨트롤러에 송신된 다음 단말 리더에 송신된다. 애플리케이션 호스트 프로세서에 의해 생성되는 응답은 상인 시스템에 의해 지불 응답으로 식별가능하고 종래의 보안 요소에 의해 생성되는 응답과 구별할 수 없고 이 응답과 동일한 기능성을 제공한다.

[0006] 대표적인 실시예들의 이러한 및 다른 측면들, 목적들, 피처들, 및 장점들은 예시된 대표적인 실시예들의 이하의 상세한 설명을 고려하면 당해 기술에서 통상의 기술자들에게 분명해질 것이다.

도면의 간단한 설명

[0007] 도 1은 대표적인 실시예들에 따른 지불 처리 시스템을 도시하는 블록도이다.

도 2는 대표적인 실시예들에 따른 보안 요소에 액세스하는 것 없이 지불을 처리하는 방법을 도시하는 블록 흐름도이다.

도 3은 대표적인 실시예들에 따른 지불 처리 응답을 처리하는 방법을 도시하는 블록 흐름도이다.

도 4는 대표적인 실시예들에 따른 지불 정보에 대한 요청을 처리하는 방법을 도시하는 블록 흐름도이다.

도 5는 대표적인 실시예들에 따른 지불을 처리하는 방법을 도시하는 블록 흐름도이다.

도 6은 임의의 대표적인 실시예들에 따른 컴퓨터 머신(machine) 및 모듈(module)을 도시하는 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0008] **개요**

[0009] 본 명세서에 설명된 대표적인 실시예들은 사용자 디바이스의 보안 요소에 액세스하는 것 없이 지불 거래의 처리를 가능하게 하는 방법들 및 시스템들을 제공한다. 대표적인 실시예에서, 사용자는 사용자 디바이스로부터의 지불 정보를 단말 리더(terminal reader)에 송신함으로써 상인 시스템과 무선 지불 거래를 행하고 있다. 사용자 디바이스 상에 상주하는 보안 요소는 제조 시에 TSM에 밀착 결합될 수 있음으로써, 사용자가 보안 요소 상에 프로비저닝(provisioning)되지 않은 지불 계정에 대한 지불 명령들을 제공하는 것을 방지한다. 대표적인 실시예에서, 사용자 디바이스는 보안 요소에 액세스하는 것 없이 지불 정보를 송신할 수 있는 애플리케이션 호스트 프로세서(application host processor)를 포함한다.

[0010] 사용자는 단말 리더의 무선 주파수 필드에서 사용자 디바이스를 태핑(tapping)한다. 단말 리더 및 사용자 디바이스는 통신 채널을 설정하고 단말 리더는 지불 처리 응답에 대한 요청을 포함하는 신호를 송신한다. 신호는 사용자 디바이스에 의해 수신되고 컨트롤러에 의해 애플리케이션 호스트 프로세서에 의해 이해가능한 요청으로 변환된다. 컨트롤러는 요청을 요청이 처리되고 응답이 생성되는 애플리케이션 호스트 프로세서에 송신한다. 애플리케이션 호스트 프로세서에 의해 생성되는 응답은 상인 시스템에 의해 지불 응답으로 식별가능하고 보안 요소에 의해 생성되는 응답과 구별할 수 없다. 응답은 애플리케이션 호스트 프로세서에 의해 컨트롤러에 송신되며, 여기서 응답은 단말 리더에 송신을 위한 신호로 변환된다. 신호는 그것이 수신되는 단말 리더에 송신되고 상인 시스템에 송신된다. 상인 시스템 상에 상주하는 애플리케이션은 신호를 처리하고 그것을 상인 시스템에 의해 이해가능한 응답으로 변환한다. 상인 시스템은 응답을 판독하며, 이는 사용자 디바이스가 지불 거래로 진행할 수 있다는 긍정 표시를 포함한다.

[0011] 상인 시스템은 지불 정보에 대한 요청을 생성하고 요청을 단말 리더에 송신한다. 단말 리더는 단말 리더와 사용자 디바이스 사이에 설정된 통신 채널을 통해 송신가능한 신호의 형태로 요청을 송신한다. 신호는 사용자 디바이스에 의해 수신되고 컨트롤러에 의해 애플리케이션 호스트 프로세서에 의해 이해가능한 요청으로 변환된다. 컨트롤러는 요청을 요청이 처리되고 응답이 생성되는 애플리케이션 호스트 프로세서에 송신한다. 응답은 거래에 사용할 지불 계정 번호를 포함한다. 지불 계정 번호는 사용자와 연관되는 금융 계정과 연관된 번호, 예를 들어, 신용 계정 번호, 인출 계정 번호, 저장 값 계정 번호, 기프트 카드 계정 번호, 쿠폰, 로열티 계정 번호, 보상 계정 번호, 또는 은행 계정 번호를 포함할 수 있다. 응답은 또는 그 대신에 계정 관리 시스템 또는 애플리케이션 호스트 프로세서에 의해 생성되는 프록시 계정 번호를 포함할 수도 있다. 프록시 계정 번호는 사용자의 실제

금융 계정 정보가 검색될 수 있는 계정 관리 시스템에 지불 거래를 라우팅(routing)하는 정보를 포함한다. 프록시 계정 번호들은 시간, 지리적 및 / 또는 값 제한들을 가질 수 있다. 프록시 계정 번호들은 그들이 사용될 수 있는 횟수에 관한 제한들을 가질 수도 있다.

[0012] 지불 계정 정보를 포함하는 응답은 애플리케이션 호스트 프로세서에 의해 컨트롤러에 송신되며, 여기서 응답은 단말 리더에 송신을 위한 신호로 변환된다. 신호는 그것이 수신되는 단말 리더에 송신되고 상인 시스템에 송신된다. 상인 시스템 상에 상주하는 애플리케이션은 신호를 처리하고 그것을 상인 시스템에 의해 이해가능한 응답으로 변환한다. 상인 시스템은 지불 계정 정보를 판독하고 지불을 처리한다.

[0013] 본 발명의 창의적인 기능성은 프로그램 흐름을 예시하는 도면들과 함께 판독되는, 이하의 설명에서 더 상세히 설명될 것이다.

[0014] **대표적인 시스템 아키텍처들(System Architectures)**

[0015] 이제 유사한 번호들이 도면들에 걸쳐 유사한(반드시 동일한 것은 아닌) 요소들을 지시하는 도면들을 참조하여, 대표적인 실시예들이 상세히 설명된다.

[0016] 도 1은 임의의 대표적인 실시예들에 따른 지불 처리 시스템을 도시하는 블록도이다. 도 1에 도시된 바와 같이, 대표적인 동작 환경(100)은 하나 이상의 네트워크들(networks)(130)을 통해 서로 통신하도록 구성되는 상인 시스템(merchant system)(105), 사용자 디바이스 시스템(120), 계정 관리 시스템(140), 획득자 시스템(150), 카드 네트워크 시스템(card network system)(160), 및 발행자 시스템(issuer system)(170)을 포함한다. 일부 대표적인 실시예들에서, 이러한 시스템들(시스템들(105, 120, 140, 150, 160, 및 170)을 포함함) 중 2개 이상은 동일한 시스템에 통합된다.

[0017] 각각의 네트워크(130)는 네트워크 시스템들(시스템들(105, 120, 140, 150, 160, 및 170)을 포함함)이 데이터를 전달하고 교환할 수 있는 유선 또는 무선 전기통신 수단을 포함한다. 예를 들어, 각각의 네트워크(130)는 광저장장치 영역 네트워크(SAN; storage area network), 개인 영역 네트워크(PAN; personal area network), 도시권 영역 네트워크(MAN; metropolitan area network), 로컬 영역 네트워크(LAN; local area network), 광역 네트워크(WAN; wide area network), 무선 로컬 영역 네트워크(WLAN; wireless local area network), 가상 사설망(VPN; virtual private network), 인트라넷(intranet), 인터넷(Internet), 이동 전화 네트워크(mobile telephone network), 카드 네트워크, 블루투스(Bluetooth), 근거리 통신망 네트워크(NFC; near field communication network), 임의의 형태의 표준화 무선 주파수, 또는 그것의 임의의 조합, 또는 신호들, 데이터, 및/또는 메시지들(일반적으로 데이터로 지칭됨)의 전달을 용이하게 하는 임의의 다른 적절한 아키텍처 또는 시스템으로 구현될 수 있거나, 이들의 일부일 수 있다. 본 명세서에 걸쳐, 용어들 "데이터(data)" 및 "정보(information)"는 텍스트(text), 이미지들(images), 오디오(audio), 비디오(video), 또는 컴퓨터 기반 환경에 존재할 수 있는 임의의 다른 형태의 정보를 언급하기 위해 본 명세서에서 교환가능하게 사용된다는 점이 이해되어야 한다.

[0018] 대표적인 실시예에서, NFC 통신 프로토콜들(protocols)은 ISO/IEC 14443 타입 A 및/또는 B 기술(이하 "ISO 14443"), 마이페어(MIFARE) 기술(이하 "MIFARE"), 및/또는 ISO/IEC 18092 기술(이하 "ISO 18092")을 포함하지만, 이들에 제한되지 않는다. ISO 14443은 리더와 아주 근접하여 동작하는 사용자 디바이스들에 대한 통신 프로토콜이다. ISO 14443 통신 프로토콜은 신용 카드 지불들, 직불 카드 지불들, 및 다른 형태들의 금융 카드 지불들을 포함하지만, 이들에 제한되지 않는 보안 카드 지불들에 이용된다. MIFARE는 ISO 14443에 기초한 독점 디바이스 표준들에 따르는 사용자 디바이스들에 대한 통신 프로토콜이다. MIFARE 프로토콜은 기프트 카드들(gift cards), 교통 카드들(transit cards), 티켓들(tickets), 액세스 카드들(access cards), 로열티 카드들(loyalty cards), 및 다른 형태들의 저장 값 카드 거래들을 포함하지만 이들에 제한되지 않는 저장된 기능 거래들에 이용된다. MIFARE 프로토콜은 제한된 부가 가치 서비스들에 사용될 수도 있다. ISO 18092는 더 높은 비트 레이트들(bit rates)로 동작하는 사용자 디바이스들에 대한 통신 프로토콜이며, 디바이스들 사이에서 리치 통신(richer communication)을 허용한다. ISO 18092 통신 프로토콜은 피어 투 피어(peer-to-peer) 통신, 부가 가치 서비스들(쿠폰들, 로열티 카드들, 체크인들(check-ins), 멤버십 카드들, 기프트 카드들, 및 다른 형태들의 부가 가치 서비스들을 포함하지만, 이들에 제한되지 않음), 및 다른 형태들의 리치 통신에 이용된다. 임의의 적절한 NFC 통신 프로토콜은 본 명세서에 설명된 방법들 및 기능성을 구현하기 위해 사용자 디바이스(120)와 단말 리더(115) 사이의 NFC 통신에 사용될 수 있다.

[0019] 대표적인 실시예에서, 각각의 네트워크 시스템(시스템들(105, 120, 140, 150, 160, 및 170)을 포함함)은 네트워

크(130)를 통해 데이터를 송신하고 수신할 수 있는 통신 모듈을 갖는 디바이스를 포함한다. 예를 들어, 각각의 네트워크 시스템(시스템들(105, 120, 140, 150, 160, 및 170)을 포함함)은 서버(server), 개인용 컴퓨터, 이동 디바이스(예를 들어, 노트북 컴퓨터(notebook computer), 태블릿 컴퓨터(tablet computer), 넷북 컴퓨터(netbook computer), 개인 휴대 정보 단말기(PDA; personal digital assistant), 비디오 게임 디바이스, GPS 위치 입력 디바이스(GPS locator device), 휴대 전화(cellular phone), 스마트폰(Smartphone), 또는 다른 이동 디바이스), 하나 이상의 프로세서들이 그 안에 내장되고/되거나 그것에 결합된 텔레비전(television), 또는 네트워크(130)를 통해 통신하는 웹 브라우저(web browser) 또는 다른 애플리케이션을 포함하거나 이들에 결합되는 다른 적절한 기술을 포함할 수 있다. 도 1에 도시된 대표적인 실시예에서, 네트워크 시스템들(시스템들(105, 120, 140, 150, 160, 및 170)을 포함함)은 상인들, 사용자들 또는 소비자들, 계정 관리 시스템 운영자, 획득자 시스템 운영자, 카드 네트워크 시스템 운영자, 및 발행자 시스템 운영자 각각에 의해 동작된다.

[0020] 상인 시스템(105)은 사용자에 의해 개시된 구매 거래를 처리할 수 있는 적어도 하나의 판매 시점 관리("POS"; point of sale) 단말(110)을 포함한다. 대표적인 실시예에서, 상인은 온라인(online) 가게를 운영하고 사용자는 웹 사이트 상의 링크(link) 또는 "체크아웃(check out)" 버튼을 클릭(click)함으로써 구매를 하는 요구를 표시한다. 일부 대표적인 실시예들에서, 사용자 디바이스(120)는 POS 단말(110)의 기능들을 수행하도록 구성된다. 이러한 예에서, 사용자는 POS 단말(110)과 상호 작용하는 것 없이 사용자 디바이스(120)를 통해 거래를 스캔하고/하거나 지불한다. 대표적인 상인 시스템(105)은 애플리케이션(118)을 통해 사용자 디바이스 시스템(120) 및 상인 POS 단말(110)과 통신할 수 있는 적어도 하나의 단말 리더(115)를 포함한다. 애플리케이션(118)은 일부 대표적인 실시예들에 따른 POS 단말(110) 또는 상인 시스템(105)(도 1에 도시되지 않음)의 통합 부분, 단말 리더(115)(도시됨)의 통합 부분, 또는 독립형 하드웨어 디바이스(도시되지 않음)일 수 있다.

[0021] 대표적인 실시예에서, 단말 리더(115)는 NFC 통신 방법을 사용하여 사용자 디바이스(120)와 통신할 수 있다. 다른 대표적인 실시예에서, 단말 리더(115)는 블루투스 통신 방법을 사용하여 사용자 디바이스(120)와 통신할 수 있다. 또 다른 실시예에서, 단말 리더(115)는 Wi-Fi 통신 방법을 사용하여 사용자 디바이스(120)와 통신할 수 있다. 일부 대표적인 실시예들에서, 사용자는 QR 코드 또는 바 코드(bar code)를 스캔하거나 사용자 디바이스(120) 상의 URL 링크를 클릭하며, 이는 사용자 디바이스(120)를 온라인 상인 시스템(105)에 일시적으로 연관시킨다. POS 단말(110)은 사용자 및/또는 사용자 디바이스(120)에 링크하기 위해 온라인 상인 시스템(105)에 질의한다. 대표적인 실시예에서, 단말 리더(115)는 QR 코드, 통일 상품 코드("UPC"; universal product code), 국제 거래 단위 번호("GTIN"; global trade item number), 재고 보관 단위("SKU"; stock keeping unit), 일본 물품 번호("JAN"; Japanese article number), 국제 제품 코드("WPC"; world product code), 국제 표준 도서 번호("ISBN"; International Standard Book Number), 유럽 물품 번호("EAN"; European Article Number) 등을 제한 없이 포함하는, 임의의 수의 바코드 포맷들(formats)을 판독하도록 구성될 수 있다. 다른 대표적인 실시예들에 따르면, 단말 리더(115)는 CPU를 갖는 전자 필드 생성기(eletronic field generator), 레이저 스캐너(laser scanner), 전하 결합 소자("CCD"; charged-coupled device) 리더, 카메라 기반 리더, 전방향 바 코드 스캐너, 카메라, RFID 리더, 또는 상인 시스템(105)에서 제품 식별자 정보를 판독할 수 있는 임의의 다른 디바이스일 수 있다.

[0023] *대표적인 실시예에서, 사용자 디바이스(120)는 개인용 컴퓨터, 이동 디바이스(예를 들어, 노트북, 컴퓨터, 태블릿 컴퓨터, 넷북 컴퓨터, 개인 휴대 정보 단말기(PDA), 비디오 게임 디바이스, GPS 위치 입력 디바이스, 휴대 전화, 스마트폰 또는 다른 이동 디바이스), 하나 이상의 프로세서들이 그 안에 내장되고/되거나 그것에 결합된 텔레비전, 또는 디바이스(120)와 단말 리더(115)와 같은, 다른 디바이스 사이에서 전자, 자기, 또는 무선 주파수 필드를 통해 통신할 수 있는 다른 적절한 기술일 수 있다. 대표적인 실시예에서, 사용자 디바이스(120)는 특정 기능을 수행할 수 있는 저장 용량/메모리 및 하나 이상의 애플리케이션들(예시되지 않음)과 같은, 처리 능력들을 갖는다. 대표적인 실시예에서, 사용자 디바이스(120)는 운영 체제(예시되지 않음) 및 사용자 인터페이스(user interface)(121)를 포함한다. 일부 대표적인 실시예들에서, 사용자 디바이스(120)는 사용자 인터페이스(121) 없이 오디오 포트(audio port) 또는 보조 데이터 포트를 통해 통신하는 운영 체제(예시되지 않음)를 포함한다.

[0024] 또한, 사용자 디바이스(120)는 컨트롤러(125)를 포함한다. 대표적인 실시예에서, 컨트롤러(125)는 NFC 컨트롤러이다. 일부 대표적인 실시예들에서, 컨트롤러(125)는 블루투스 링크 컨트롤러(Bluetooth link controller)이다. 블루투스 링크 컨트롤러는 데이터를 송신하고 수신가능할 수 있어, 인증 및 암호 기능들을 수행하고, 사용자 디바이스(120)가 어떻게 단말 리더(115)로부터의 송신들을 리스닝(listening)할지를 지시하거나 사용자 디바이스(120)를 블루투스 특정 절차들에 따라 다양한 절전 모드들로 구성한다. 다른 대표적인 실시예에서, 컨트롤러

(125)는 유사한 기능들을 수행할 수 있는 Wi-Fi 컨트롤러 또는 NFC 컨트롤러이다.

[0025] 사용자 디바이스(120)는 안테나(antenna)(127)를 통해 단말 리더(115)와 통신한다. 대표적인 실시예에서, 사용자 디바이스 애플리케이션이 활성화되고 우선순위화되었다면, 컨트롤러(125)는 거래에 대한 사용자 디바이스(120)의 준비의 상태를 통지받는다. 컨트롤러(125)는 안테나(127)를 통해 무선 신호를 출력하거나, 디바이스 리더(115)로부터의 무선 신호들을 리스닝한다. 사용자 디바이스(120)와 단말 리더(115) 사이에 보안 통신 채널을 설정하면, 리더(115)는 사용자 디바이스(120)로부터 지불 처리 응답을 요청한다.

[0026] 대표적인 컨트롤러(125)는 안테나(127)를 통해 송신되는 단말 리더(115)로부터의 전파(radio wave) 통신 신호를 수신한다. 컨트롤러(125)는 신호를 판독가능 바이트들(bytes)로 변환한다. 대표적인 실시예에서, 바이트들은 지불 처리 응답에 대한 요청 또는 지불 카드 정보에 대한 요청과 같은, 디지털 정보를 포함한다. 컨트롤러(125)는 요청을 애플리케이션 호스트 프로세서(123)에 송신한다.

[0027] 대표적인 사용자 디바이스(120)는 보안 요소 또는 보안 메모리(도시되지 않음)를 포함할 수 있으며, 이는 이동식 스마트 칩 또는 보안 디지털("SD"; secure digital) 카드 내에 존재할 수 있거나 디바이스(120) 상의 고정된 칩 내에 내장될 수 있다. 임의의 대표적인 실시예들에서, 가입자 식별 모듈("SIM"; Subscriber Identity Module) 카드들은 보안 요소, 예를 들어 NFC SIM 카드를 호스팅가능할 수 있다. 보안 요소(도시되지 않음)는 보안 요소(도시되지 않음) 내에 저장된 정보를 보호하는 동안, 사용자 디바이스(120) 상에 상주하고 디바이스 사용자에 의해 액세스가능한 소프트웨어 애플리케이션이 보안 요소 내의 임의의 기능들과 안전하게 상호 작용하는 것을 허용한다. 대표적인 실시예에서, 보안 요소(도시되지 않음)는 암호 프로세서들 및 랜덤 생성기들(random generators)과 같은, 스마트 카드의 전형적인 구성요소들을 포함한다. 대표적인 실시예에서, 보안 요소(도시되지 않음)는 자바카드 오픈 플랫폼("JCOP"; JavaCard Open Platform) 운영 체제와 같은, 스마트 카드 운영 체제에 의해 제어되는 매우 안전한 시스템 온 칩(system on a chip) 내의 스마트 MX 타입 NFC 컨트롤러를 포함한다. 다른 대표적인 실시예에서, 보안 요소(도시되지 않음)는 비-EMV 타입 비접촉 스마트 카드를 선택적 구현으로서 포함하도록 구성된다. 보안 요소(도시되지 않음)는 사용자 디바이스(120) 내의 애플리케이션과 통신한다. 대표적인 실시예에서, 보안 요소(도시되지 않음)는 암호화된 사용자 정보를 저장하고 신뢰된 애플리케이션들만이 저장된 정보에 액세스하는 것을 허용할 수 있다. 대표적인 실시예에서, 컨트롤러(125)는 보안 요소에서의 복호화 및 설치를 위한 보안 키 암호화 애플리케이션과 상호 작용한다.

[0028] 대표적인 사용자 디바이스(120)에서, 지불 요청은 보안 요소(도시되지 않음)에 의하는 대신에, 애플리케이션 호스트 프로세서(123)에 의해 처리된다. 대표적인 애플리케이션 호스트 프로세서(123)는 이동식 스마트 칩 또는 보안 디지털("SD") 카드 내에 존재할 수 있거나 이는 디바이스(120) 상의 고정된 칩 내에 내장될 수 있다. 애플리케이션 호스트 프로세서는 본 명세서에 설명된 기능성을 수행하는 그 위에 실행하는 애플리케이션들(도시되지 않음)을 포함할 수 있다. 대표적인 실시예에서, 사용자 디바이스(120)는 사용자의 실제 계정 정보를 송신하는 것 없이, 지불 계정 정보를 프록시(proxy) 또는 가상 계정 식별자의 형태로 상인 시스템(105)에 전달한다. 사용자의 실제 계정 정보는 사용자 디바이스(120) 상에 상주하는 보안 요소(도시되지 않음) 내에 대신에 계정 관리 시스템(140)에 의해 유지된다.

[0029] 대표적인 상인 시스템(105) 및 사용자 디바이스(120)는 계정 관리 시스템(140)과 통신한다. 계정 관리 시스템(140)은 사용자에 대한 하나 이상의 지불 계정들의 저장을 가능하게 한다. 대표적인 실시예에서, 사용자는 하나 이상의 지불 계정들, 예를 들어, 신용 카드 계정들, 인출 계정들, 은행 계정들, 기프트 카드 계정들, 쿠폰들, 저장 값 계정들, 로열티 계정들, 보상 계정들, 및 계정 관리 시스템(140)과 구매를 할 수 있는 다른 형태들의 지불 계정들을 등록한다. 예를 들어, 사용자는 계정 관리 시스템(140)으로 디지털 지갑 계정을 생성할 수 있다. 지불 계정들은 계정 관리 시스템(140)에 의해 유지되는 사용자의 디지털 지갑 계정과 연관될 수 있다. 사용자는 지불 계정들을 추가하거나, 변경하거나, 제거하기 위해 언제든지 디지털 지갑 계정에 액세스할 수 있다. 대표적인 실시예에서, 사용자의 디지털 지갑 정보는 사용자의 사용자 디바이스(120)에 송신되어, 계정 관리 시스템(140)에 액세스하는 것 없이 사용자의 지불 계정의 사용을 가능하게 한다. 일부 대표적인 실시예들에서, 계정 관리 시스템(140)은 제한된 사용 프록시 계정 정보를 사용자 디바이스(120)에 송신하여 지불 처리 동안 계정 관리 시스템(140)에 라우팅(routing)되는 지불 거래 동안 지불 계정들의 사용을 가능하게 한다. 예를 들어, 프록시 계정 번호는 지불 인가 요청을 계정 관리 시스템(140)에 라우팅하여 프록시 계정에 대한 발행자 시스템(170)으로서 동작할 수 있다. 다른 대표적인 실시예에서, 사용자 디바이스(120)는 지불 거래가 계정 관리 시스템(140)에 라우팅될 수 있게 하는 제한된 사용 프록시 계정 번호들을 생성하는 애플리케이션(도시되지 않음)을 포함할 수 있다. 일부 대표적인 실시예들에서, 애플리케이션 호스트 프로세서(123)는 이러한 기능을 수행한다.

[0030] 대표적인 계정 관리 시스템(140)은 계정 관리 시스템(140)에 의해 액세스가능한 데이터 저장 유닛(145)을 포함한다. 대표적인 데이터 저장 유닛(145)은 사용자의 지불 계정 정보를 저장할 수 있는 하나 이상의 유형의(tangible) 컴퓨터 판독가능 저장 디바이스들을 포함할 수 있다. 사용자는 상인 시스템(105)으로부터 구매를 요청할 수 있다. 대표적인 실시예에서, 구매는 단말 리더(115)와의 사용자 디바이스(120)의 무선 "탭(tap)"에 의해 개시된다. 상인 시스템(105)은 지불을 처리하기 위해 획득자 시스템(150)(예를 들어 체이스(Chase), 페이먼트테크(PaymentTech), 또는 다른 제3자 지불 처리 회사들), 카드 네트워크 시스템(160)(예를 들어 비자, 마스터카드, 아메리칸 익스프레스(American Express), 디스커버(Discover), 또는 다른 카드 처리 네트워크들), 및 발행자 시스템(170)(예를 들어 시티뱅크(Citibank), 캐피탈 원(CapitalOne), 뱅크 오브 아메리카, 및 지불을 인가하는 다른 금융 기관들)과 상호 작용한다. 일부 대표적인 실시예들에서, 사용자 디바이스(120)에 의해 단말 리더(115)에 송신되는 지불 카드 정보는 계정 관리 시스템(140)에 의해 유지되는 사용자 계정에 지불 거래를 링크하는 프록시 계정 번호 또는 토큰(token) 계정 번호이다. 지불 거래는 사용자의 정확한 지불 카드 정보의 식별을 위해 계정 관리 시스템(140)에 라우팅된다.

[0031] 대표적인 동작 환경(100)의 구성요소들은 이하 도 2 내지 도 5에 예시된 대표적인 방법들을 참조하여 설명된다. 도 2 내지 도 5의 대표적인 방법들은 다른 시스템들에 의해 그리고 다른 환경들에서 수행될 수도 있다.

[0032] **대표적인 시스템 프로세스들**

[0033] 도 2는 대표적인 실시예들에 따른 보안 요소에 액세스하는 것 없이 지불을 처리하는 방법을 도시하는 블록 흐름도이다. 방법(200)은 도 1에 예시된 구성요소들을 참조하여 설명된다.

[0034] 블록(205)에서, 사용자는 단말 리더(115)와 근접한 사용자 디바이스(120)를 태핑한다. 대표적인 실시예에서, 단말 리더(115)는 사용자 디바이스(120)의 존재를 위해 폴링하는(polling) 무선 주파수("RF"; radio frequency) 또는 다른 필드를 생성하고, 사용자는 디바이스(120)를 단말 리더(115)의 필드 내에 설치함으로써 사용자 디바이스(120)를 "태핑"한다. 일부 대표적인 실시예들에서, 상인은 단말 리더(115) 상의 애플리케이션(118)을 사용하여 사용자 디바이스(120)의 존재를 위해 폴링하는 RF 필드 또는 다른 필드를 활성화한다. 임의의 대표적인 실시예들에서, 본 명세서의 도 2 내지 도 5에 설명된 시스템들 및 방법들은 사용자 디바이스(120)가 태핑되는 동안 수행된다.

[0035] 블록(210)에서, 사용자 디바이스(120) 및 단말 리더(115)는 통신 채널을 설정한다. 대표적인 실시예에서, 통신 채널은 NFC 통신 채널이다. 일부 대표적인 실시예들에서, 통신 채널은 블루투스 통신 채널이다. 또 다른 대표적인 실시예에서, 통신 채널은 Wi-Fi 통신 채널이다. 따라서, 지불 거래는 사용자 디바이스(120)와 단말 리더(115) 사이에서 무선 또는 "비접촉" 통신을 통해 수행될 수 있다.

[0036] 대표적인 실시예에서, 단말 리더(115)는 통신 채널을 설정하기 위해 사용자 디바이스(120)로부터 프로토콜들 및 특성들을 요청한다. 예를 들어, 단말 리더(115)는 사용자 디바이스(120)로부터 통신 프로토콜들(예를 들어 ISO/IEC 14443, MIFARE, 및/또는 ISO/IEC 18092)의 식별, 이용가능한 애플리케이션들의 리스트, 및 보안 프로토콜들을 요청할 수 있다.

[0037] 블록(215)에서, 단말 리더(115)는 지불 처리 응답을 요청하는 신호를 사용자 디바이스(120)에 송신한다. 대표적인 실시예에서, 지불 처리 응답은 금융 지불 거래로 진행하기 위한 요청이다. 대표적인 실시예에서, 지불 처리 응답은 사용자 디바이스(120)가 금융 거래를 수행할 수 있는 것을 단말 리더(115)에 표시한다. 보안 요소를 수반하는 전형적인 무선 지불 거래에서, 사용자 디바이스(120)는 보안 요소에 의해 생성되는 메시지로 단말 리더(115)의 요청에 응답한다. 이러한 메시지는 지불 처리 응답을 포함하기 위해 단말 리더(115)에 의해 이해가능하다. 대표적인 실시예에서, 지불 처리 응답은 보안 요소가 아닌, 사용자 디바이스(120)에 상주하는 애플리케이션 호스트 프로세서(123)에 의해 생성된다. 지불 처리 응답은 보안 요소에 의해 생성되는 응답과 동일한 방식으로 단말 리더(115)에 의해 이해가능하다.

[0038] 블록(220)에서, 사용자 디바이스(120)는 단말 리더(115)에 의해 송신되는 신호를 수신한다. 대표적인 실시예에서, 신호는 안테나(127)에 의해 수신되고 컨트롤러(125)에 송신된다. 대표적인 실시예에서, 탭은 NFC 탭이고 컨트롤러(125)는 NFC 컨트롤러이다.

[0039] 블록(225)에서, 컨트롤러(125)는 지불 처리 응답을 위해 신호를 판독가능 요청으로 변환한다. 대표적인 실시예에서, 신호는 지불 처리 응답을 위해 판독가능 요청을 포함하는 바이트들로 변환된다.

[0040] 블록(230)에서, 컨트롤러(125)는 지불 처리 응답에 대한 요청을 애플리케이션 호스트 프로세서(123)에

송신한다. 대표적인 실시예에서, 애플리케이션 호스트 프로세서(123)는 지불 거래 동안 보안 요소와 유사한 방식으로 기능한다.

[0041] 블록(235)에서, 지불 처리 응답에 대한 요청이 처리된다. 지불 처리 응답에 대한 요청을 처리하는 방법은 이하 도 3에 설명된 방법들을 참조하여 더 상세히 설명된다.

[0042] 도 3은 도 2의 블록(235)에 참조된 바와 같이, 대표적인 실시예들에 따른 지불 처리 응답을 처리하는 방법을 도시하는 블록 흐름도이다. 방법(235)은 도 1에 예시된 구성요소들을 참조하여 설명된다.

[0043] 블록(310)에서, 애플리케이션 호스트 프로세서(123)는 지불 처리 응답에 대한 요청을 수신한다. 대표적인 실시예에서, 요청은 애플리케이션 호스트 프로세서(123)에 의해 수신되기 전에 직렬 연결들을 통해 송신된다. 일부 대표적인 실시예들에서, 요청은 컨트롤러(125)로부터 애플리케이션 호스트 프로세서(123)로 직접 송신된다.

[0044] 블록(320)에서, 애플리케이션 호스트 프로세서(123)는 지불 처리 응답을 생성한다. 대표적인 실시예에서, 지불 처리 응답은 사용자 디바이스(120)가 지불 거래를 완료할 수 있다는 것을 표시하는 단말 리더(115)에 의해 이해가능한 언어를 포함한다. 대표적인 실시예에서, 지불 처리 응답은 종래의 보안 요소 또는 보안 메모리에 의해 생성되는 지불 처리 응답으로서 동일한 언어 및/또는 정보를 포함한다. 대표적인 실시예에서, 지불 처리 응답은 사용자 식별가능 데이터, 개인 식별자들, 계정 식별자들, 지불 네트워크 구성 데이터, 상인 특정 데이터, 및/또는 보안 데이터를 포함하며, 이들 중 어느 것은 사용자의 계정 상에 수행되는 거래들의 시퀀스(sequence)를 검증하기 위해 사용될 수 있다.

[0045] 블록(330)에서, 애플리케이션 호스트 프로세서(123)는 지불 처리 응답을 컨트롤러(125)에 송신한다. 대표적인 실시예에서, 지불 처리 응답은 컨트롤러(125)에 의해 수신되기 전에 직렬 연결들을 통해 송신된다. 일부 대표적인 실시예들에서, 지불 처리 응답은 컨트롤러(125)에 직접 송신된다.

[0046] 블록(340)에서, 컨트롤러(125)는 지불 처리 응답을 수신한다. 대표적인 실시예에서, 지불 처리 응답은 컨트롤러(125)에 의해 송신가능 신호로 변환될 바이트들을 포함한다.

[0047] 블록(350)에서, 컨트롤러(125)는 지불 처리 응답을 단말 리더(115)에 송신한다. 대표적인 실시예에서, 지불 처리 응답은 안테나(127)에 의해 단말 리더(115)에 송신되는 신호이다.

[0048] 블록(360)에서, 단말 리더(115)는 지불 처리 응답을 수신한다. 대표적인 실시예에서, 단말 리더(115)는 사용자 디바이스에 의해 송신되는 신호를 수신한다.

[0049] 블록(370)에서, 단말 리더는 지불 처리 응답을 상인 시스템(105)에 송신한다. 대표적인 실시예에서, 지불 처리 응답은 상인 시스템(105)에 상주하는 POS 단말(110)에 송신된다.

[0050] 블록(380)에서, 상인 시스템(105)은 지불 처리 응답을 수신한다. 대표적인 실시예에서, 상인 시스템 상에 상주하는 애플리케이션(118)은 신호를 상인 시스템(105)에 의해 이해가능한 언어로 변환한다. 대표적인 실시예에서, 상인 시스템(105)은 사용자 디바이스(120)가 지불 거래를 수행할 수 있다는 긍정 응답을 포함하기 위해 지불 처리 응답을 이해한다.

[0051] 그 다음, 방법(235)은 도 2의 블록(240)으로 진행한다.

[0052] 도 2로 돌아가면, 블록(240)에서, 지불 계정 정보에 대한 요청이 처리된다. 지불 계정 정보를 처리하는 방법은 이하 도 4에 설명된 방법들을 참조하여 더 상세히 설명된다.

[0053] 도 4는 도 2의 블록(240)에 참조된 바와 같이, 대표적인 실시예들에 따른 지불 정보에 대한 요청을 처리하는 방법을 도시하는 블록 흐름도이다. 방법(240)은 도 1에 예시된 구성요소들을 참조하여 설명된다.

[0054] 블록(410)에서, 상인 시스템(105)은 지불 계정 정보에 대한 요청을 생성하여 단말 리더(115)에 송신한다. 대표적인 실시예에서, 지불 처리 응답에 대한 요청은 지불 계정 정보에 대한 요청을 포함하고 블록들(410 내지 490) 및 블록(240 내지 265)에 설명된 방법들은 요구되지 않는다.

[0055] 블록(420)에서, 단말 리더(115)는 상인 시스템(105)에 의해 송신되는 지불 계정 정보에 대한 요청을 수신한다. 대표적인 실시예에서, 상인 시스템(105) 상에 상주하는 애플리케이션(118)은 지불 처리 응답을 판독하고 지불 계정 정보에 요청을 응답으로 생성한다. 대표적인 실시예에서, 요청은 통신 채널을 통해 사용자 디바이스(120)에 송신될 수 있는 신호로 변환되고 애플리케이션 호스트 프로세서(123)에 의해 이해가능한 바이트들로 변환된다.

[0056] 블록(430)에서, 단말 리더(115)는 지불 계정 정보에 대한 요청을 포함하는 신호를 사용자 디바이스(120)에 송신한다. 대표적인 실시예에서, 지불 계정 정보에 대한 요청은 계정 번호, 만료 날짜, 및 보안 코드와 같은, 지불 거래를 완료하기 위해 정보에 대한 요청을 포함한다.

[0057] 블록(440)에서, 사용자 디바이스(120)는 단말 리더(115)에 의해 송신되는 신호를 수신한다. 대표적인 실시예에서, 신호는 안테나(127)에 의해 수신되고 컨트롤러(125)에 송신된다.

[0058] 블록(450)에서, 컨트롤러(125)는 신호를 지불 계정 정보에 대한 판독가능 요청으로 변환한다. 대표적인 실시예에서, 신호는 지불 계정 정보에 대한 판독가능 요청을 포함하는 바이트들로 변환된다.

[0059] 블록(460)에서, 컨트롤러(125)는 지불 계정 정보에 대한 요청을 애플리케이션 호스트 프로세서(123)에 송신한다. 대표적인 실시예에서, 애플리케이션 호스트 프로세서(123)는 지불 거래 동안 보안 요소와 유사한 방식으로 기능한다.

[0060] 블록(470)에서, 애플리케이션 호스트 프로세서(123)는 지불 계정 정보에 대한 요청을 수신한다. 대표적인 실시예에서, 요청은 애플리케이션 호스트 프로세서(123)에 의해 수신되기 전에 직렬 연결들을 통해 송신된다. 일부 대표적인 실시예들에서, 요청은 컨트롤러(125)로부터 애플리케이션 호스트 프로세서(123)로 직접 송신된다.

[0061] 블록(480)에서, 애플리케이션 호스트 프로세서(123)는 지불 거래에 사용될 지불 계정 정보를 생성한다. 대표적인 실시예에서, 사용자는 하나 이상의 지불 계정들, 예를 들어, 신용 카드 계정들, 인출 계정들, 은행 계정들, 기프트 카드 계정들, 쿠폰들, 저장 값 계정들, 로열티 계정들, 보상 계정들, 및 계정 관리 시스템(140)과 구매를 할 수 있는 다른 형태들의 지불 계정들을 등록한다. 예를 들어, 사용자는 계정 관리 시스템(140)으로 디지털 지갑 계정을 생성할 수 있으며, 이는 지불 계정들을 사용자 및/또는 사용자의 사용자 디바이스(120)와 연관시킨다. 디지털 지갑 계정 정보는 계정 관리 시스템(140)에 저장될 수 있고 사용자의 사용자 디바이스(120)에 국부적으로 저장될 수도 있다.

[0062] 대표적인 실시예에서, 사용자의 디지털 지갑 정보는 사용자의 사용자 디바이스(120)에 송신되었고, 애플리케이션 호스트 프로세서(123)는 사용자의 디지털 지갑 계정에 저장된 사용자의 지불 계정들에 액세스함으로써 지불 계정 정보를 생성한다. 이러한 실시예에서, 애플리케이션 호스트 프로세서(123)는 지불 거래에서 사용하기 위한 특정 지불 계정을 선택할 수 있다.

[0063] 일부 대표적인 실시예들에서, 계정 관리 시스템(140)은 하나 이상의 제한된 사용 프록시 계정 번호들을 사용자 디바이스(120)에 송신한다. 애플리케이션 호스트 프로세서(123)는 송신된 제한된 사용 프록시 계정 번호들에 액세스하고 거래에 사용하기 위한 특정 프록시 계정 번호를 선택함으로써 지불 계정 정보를 생성한다. 대표적인 실시예에서, 계정 관리 시스템(140)은 제한된 사용 프록시 계정 번호를 주기적으로 생성하고 현재 번호로 사용자의 사용자 디바이스(120)를 업데이트(update)할 수 있다. 일부 대표적인 실시예들에서, 사용자의 사용자 디바이스(120)는 제한된 사용 프록시 계정 번호에 대한 요청을 계정 관리 시스템(140)에 전달할 수 있고, 계정 관리 시스템(140)은 이에 응답하여, 지불 거래에서의 사용을 위해 제한된 사용 프록시 계정 번호를 사용자의 사용자 디바이스(120)에 전달할 수 있다. 또 다른 대표적인 실시예에서, 애플리케이션 호스트 프로세서(123)는 프록시 계정 번호를 국부적으로 생성한다. 애플리케이션 호스트 프로세서(123)는 계정 관리 시스템(140)이 상인 시스템(105)으로부터 지불 요청을 수신할 때, 계정 관리 시스템(140)에 의한 검증을 위해 생성된 제한된 사용 프록시 계정 번호를 계정 관리 시스템(140)에 전달할 수 있다. 일부 대표적인 실시예들에서, 애플리케이션 호스트 프로세서는 계정 관리 시스템(140)이 상인 시스템(105)으로부터 지불 요청을 수신할 때, 계정 관리 시스템(140)이 생성된 제한된 사용 프록시 계정 번호를 검증하는 것을 허용하기 위해, 계정 관리 시스템(140)에 의해 복제될 수 있는 방식을 사용하여 제한된 사용 프록시 계정 번호를 생성할 수 있다.

[0064] 프록시 계정 번호들은 시간 또는 지리적 제한들을 가질 수 있다. 예를 들어, 프록시 계정 번호는 제한된 양의 시간 동안만 유효할 수 있거나 그것은 특정 지리적 위치에서만 유효할 수 있다. 제한된 사용 프록시 계정 번호는 시간 기준, 시간 지속 기간, 사용자 디바이스(120)의 지리적 위치, 및/또는 사용자 디바이스(120)의 지리적 위치에 기초한 지리적 영역으로 스탬핑(stamping)되거나, 그 안에서 인코딩(encoding)되었거나, 그렇지 않으면 이들을 포함할 수 있다. 이러한 피처들은 제한된 사용 프록시 계정 번호가 시간의 특정 기간 후에 또는 특정 지리적 위치의 외부에서 사용될 때 만료되는 것을 허용할 수 있다. 프록시 계정 번호들은 그들이 사용될 수 있는 횟수에 관한 제한들을 가질 수도 있다. 예를 들어, 각각의 프록시 계정 번호는 단일 사용에 대해서만 유효할 수 있다.

[0065] 블록(490)에서, 애플리케이션 호스트 프로세서(123)는 지불 계정 정보를 컨트롤러(125)에 송신한다. 대표적인

실시예에서, 지불 계정 정보는 컨트롤러(125)에 의해 수신되기 전에 직렬 연결들을 통해 송신된다. 일부 대표적인 실시예들에서, 지불 처리 응답은 컨트롤러(125)에 직접 송신된다.

[0066] 그 다음, 방법(240)은 도 2의 블록(245)으로 진행한다.

[0067] 도 2로 돌아가면, 블록(250)에서, 컨트롤러(125)는 지불 계정 정보를 수신한다. 대표적인 실시예에서, 지불 계정 정보는 컨트롤러(125)에 의해 송신가능한 신호로 변화될 바이트들을 포함한다.

[0068] 블록(250)에서, 컨트롤러(125)는 지불 계정 정보를 단말 리더(115)에 송신한다. 대표적인 실시예에서, 지불 계정 정보는 안테나(127)에 의해 단말 리더(115)에 송신되는 신호이다.

[0069] 블록(255)에서, 단말 리더(115)는 지불 계정 정보를 수신한다. 대표적인 실시예에서, 단말 리더(115)는 사용자 디바이스(120)에 의해 송신되는 신호를 수신한다.

[0070] 블록(260)에서, 단말 리더는 지불 처리 응답을 상인 시스템(105)에 송신한다. 대표적인 실시예에서, 지불 처리 응답은 상인 시스템(105)에 상주하는 POS 단말(110)에 송신된다.

[0072] *블록(265)에서, 상인 시스템(105)은 지불 계정 정보를 수신한다. 대표적인 실시예에서, 상인 시스템(105) 상에 상주하는 애플리케이션(118)은 신호를 상인 시스템(105)에 의해 이해가능한 언어로 변환한다. 대표적인 실시예에서, 사용자는 개인 식별 번호("PIN"; personal identification number)를 상인 시스템(105)으로 입력하도록 유도될 수 있다.

[0073] 블록(270)에서, 지불이 처리된다. 지불을 처리하는 방법들은 이하 도 5에 설명된 방법들을 참조하여 더 상세히 설명된다.

[0074] 도 5는 도 2의 블록(270)에 참조된 바와 같이, 대표적인 실시예들에 따른 지불을 처리하는 방법을 도시하는 블록 흐름도이다. 방법(270)은 도 1에 예시된 구성요소들을 참조하여 설명된다.

[0075] 블록(505)에서, 상인 시스템(105)은 사용자 디바이스(120)에 의해 제공되는 지불 계정 정보를 사용하여 지불을 요청하는 지불 요청 메시지를 생성하고 지불 요청을 획득자 시스템(150)에 제출한다. 대표적인 실시예에서, 상인의 POS 단말(110)은 요청을 네트워크(130)를 통해 획득자 시스템(150)에 제출한다.

[0076] 블록(510)에서, 획득자 시스템(150)은 지불 요청을 수신하고 그것을 카드 네트워크 시스템(160)에 제출한다.

[0077] 블록(515)에서, 카드 네트워크 시스템(160)은 거래에 대해 지불하기 위해 사용되는 지불 계정 정보가 클래식 계정 번호인지를 판단한다. 대표적인 실시예에서, 카드 네트워크 시스템(160)은 지불 계정 정보 내의 일련의 번호들 또는 라우팅 정보를 사용하여 이러한 판단을 자동으로 형성한다. 일부 대표적인 실시예들에서, 카드 네트워크 시스템(160)은 계정 관리 시스템(140)에 의해 카드 네트워크 시스템(160)에 제공되는 저장된 계정 식별 정보의 리스트를 검토한다.

[0078] 계정 번호가 클래식 계정 번호이면, 지불은 블록(520)에서, 전통적인 지불 처리 방법들에 따라 처리된다. 대표적인 실시예에서, 계정 번호는 계정 관리 시스템(140)에 의한 처리 없이 그것이 발행자 시스템에 라우팅될 수 있으면(예를 들어, 사용자 디바이스(120)가 사용자의 실제 신용 카드 계정 번호, 직불 카드 계정 번호, 저장 값 계정 번호, 기프트 카드 계정 번호, 또는 은행 계정 번호를 상인 시스템(105)에 송신했다면), 클래식 지불 계정이다.

[0079] 블록(515)으로 돌아가면, 계정 번호가 클래식 계정 번호가 아니면, 발행자 시스템(170)은 계정 관리 시스템(140)이다(예를 들어, 프록시 계정 정보가 거래에 사용된 경우). 그 다음, 카드 네트워크 시스템(160)은 블록(525)에서, 지불 요청을 계정 관리 시스템(140)에 전송한다.

[0080] 일부 대표적인 실시예들에서, 지불 계정 정보는 계정 번호들 또는 다른 인디시아(indicia)의 블록과 같은, 저장된 계정 식별 정보의 리스트에 대응하는 식별자를 포함할 수 있으며, 이는 발행자 시스템(170) 또는 계정 관리 시스템(140)을 식별한다. 이러한 식별자에 기초하여, 지불은 식별자가 종래의 발행자 시스템(170)에 대응하면, 블록(520)에서 전통적인 지불 처리 방법들에 따라 처리되거나, 지불은 식별자가 계정 관리 시스템(140)에 대응하면, 블록(525)에서 계정 관리 시스템(140)에 전송된다.

[0081] 일부 대표적인 실시예들에서, 블록들(515 및 525)을 참조하여 설명된 방법들은 카드 네트워크 시스템(160) 대신에, 획득자 시스템(150) 또는 발행자 시스템(170)에 의해 수행될 수 있다.

[0082] 블록(530)에서, 계정 관리 시스템(140)은 카드 네트워크 시스템(160)으로부터 지불 요청을 수신한다.

[0083] 블록(535)에서, 계정 관리 시스템(140)은 프록시 계정 정보와 연관된 사용자를 식별한다. 대표적인 실시예에서, 계정 관리 시스템(140)은 각각의 사용자에 대해 생성된 프록시 계정 정보의 리스트를 포함하고 이러한 정보를 사용자의 디지털 지갑 계정에 매핑(mapping)할 수 있다. 일부 대표적인 실시예들, 해시(hash) 함수와 같은, 단방향 알고리즘은 사용자의 디지털 지갑 계정을 프록시 계정 정보로 식별하거나 연관시키기 위해 사용될 수 있다. 또 다른 대표적인 실시예에서, 하드웨어 보안 모듈("HSM"; hardware security module)은 각각의 사용자에 대해 생성된 프록시 계정 정보의 리스트와 같은, 보안 데이터를 저장하기 위해 사용될 수 있다. HSM은 각각의 사용자에 대해 생성된 프록시 계정 정보의 리스트를 사용자의 디지털 지갑 계정에 매핑하기 위해 보안 네트워크를 통해 계정 관리 시스템(140)에 의해 접촉될 수 있다.

[0084] 대표적인 실시예에서, 계정 관리 시스템(140)은 프록시 계정 정보에 대한 제한 규칙들이 위반된 것을 검증한다. 예를 들어, 계정 관리 시스템(140)은 프록시가 시간/지리적 제한 또는 사용들의 수에 관한 제한을 위반한 것을 확인한다.

[0085] 블록(540)에서, 계정 관리 시스템(140)은 사용자의 저장된 지불 계정 정보를 식별한다. 대표적인 실시예에서, 사용자의 디지털 지갑 계정은 사용자에 의해 정의되는 규칙들(또는 사용자가 디폴트(default) 규칙들을 수정하지 않았다면, 디폴트 규칙들)을 포함한다. 사용자가 지불 규칙들을 정의했다면, 계정 관리 시스템(140)은 지불 계정들을 거래에 적용하는 순서를 결정하기 위해 사용자 정의 규칙들을 우선 적용한다. 대표적인 실시예에서, 계정 관리 시스템(140)은 사용자 정의 규칙들을 우선 적용한다.

[0086] 블록(545)에서, 계정 관리 시스템(140)은 새로운 지불 요청을 생성하여 카드 네트워크 시스템(160)을 통해 선택된 지불 계정의 발행자 시스템(170)에 송신한다. 일부 대표적인 실시예들에서, 계정 관리 시스템(140)은 지불 계정의 발행자 시스템(170)이다. 이러한 실시예에서, 계정 관리 시스템(140)은 충분한 자금들이 거래에 이용가능한지를 판단하고 거래를 적절히 승인/부정할 것이다.

[0087] 블록(550)에서, 발행자(170)는 계정 관리 시스템(140)으로부터 새로운 지불 요청을 수신한다.

[0088] 블록(555)에서, 발행자(170)는 거래를 승인하거나 거절한다. 거래가 거절되면, 블록(557)에서 계정 관리 시스템(140)은 거절된 거래를 통지받는다. 계정 관리 시스템(140)은 상인 시스템(105)에 거절된 거래를 통지한다.

[0089] 거래가 승인되면, 발행자 시스템(170)은 블록(560)에서, 인가 메시지를 카드 네트워크 시스템(160)을 통해 계정 관리 시스템(140)에 송신한다. 계정 관리 시스템(140)이 지불 계정의 발행자 시스템(170)이면(블록(515) 참조), 계정 관리 시스템(140)은 거래에 대한 인가를 언급한다.

[0090] 블록(565)에서, 계정 관리 시스템(140)은 인가 메시지를 수신하고 초기 지불 요청의 승인을 카드 네트워크 시스템(160)에 송신한다.

[0091] 블록(570)에서, 인가 메시지는 획득자 시스템(150)을 통해 상인 시스템(105)에 송신된다.

[0092] 대표적인 실시예에서, 그 후 단말 리더(115)와 사용자 디바이스(120) 사이의 통신 채널이 종결된다. 대표적인 실시예에서, 초기 통신 채널은 단말 리더(115)와 사용자 디바이스(120) 사이에서 통신 채널을 종결하는 요청이 전달될 때, 또는 임의의 적절한 시간 후에 종결될 수 있다.

[0093] **다른 대표적인 실시예들**

[0094] 도 6은 임의의 대표적인 실시예들에 따른 컴퓨팅 머신(2000) 및 모듈(2050)을 도시한다. 컴퓨팅 머신(2000)은 본 명세서에 제시된 다양한 컴퓨터들, 서버들, 이동 디바이스들, 임베디드 시스템들(embedded systems), 또는 컴퓨팅 시스템들 중 임의의 것에 대응할 수 있다. 모듈(2050)은 다양한 방법들을 수행하고 본 명세서에 제시된 기능들을 처리할 시에 컴퓨팅 머신(2000)을 용이하게 하도록 구성된 하나 이상의 하드웨어 또는 소프트웨어 요소들을 포함할 수 있다. 컴퓨팅 머신(2000)은 프로세서(processor)(2010), 시스템 버스(system bus)(2020), 시스템 메모리(2030), 저장 매체(2040), 입력/출력 인터페이스(2060), 및 네트워크(2080)와 통신하는 네트워크 인터페이스(2070)와 같은 다양한 내부 또는 부착 구성요소들을 포함할 수 있다.

[0095] 컴퓨팅 머신(2000)은 종래의 컴퓨터 시스템, 임베디드 컨트롤러, 랩톱(laptop), 서버, 이동 디바이스, 스마트폰, 셋톱박스(set-top box), 키오스크(kiosk), 차량 정보 시스템, 텔레비전에 연관된 하나 보다 많은 프로세서들, 맞춤형 머신, 임의의 다른 하드웨어 플랫폼, 또는 그것의 임의의 조합 또는 다수로 구현될 수 있다. 컴퓨팅 머신(2000)은 데이터 네트워크 또는 버스 시스템을 통해 상호연결된된 다수의 컴퓨팅 머신들을 사용하여 기능하도록 구성된 분산 시스템일 수 있다.

[0096] 프로세서(2010)는 본 명세서에 설명된 동작들 및 기능성을 수행하는 코드 또는 명령들을 실행하고, 요청 흐름 및 어드레스(address) 매핑들을 관리하고, 계산들을 수행하고 커맨드들(commands)을 생성하도록 구성될 수 있다. 프로세서(2010)는 컴퓨팅 머신(2000)에서 구성요소들의 동작을 감시하고 제어하도록 구성될 수 있다. 프로세서(2010)는 범용 프로세서, 프로세서 코어(processor core), 멀티프로세서, 재구성가능 프로세서, 마이크로컨트롤러(microcontroller), 디지털 신호 프로세서("DSP"; digital signal processor), 주문형 반도체("ASIC"; application specific integrated circuit), 그래픽 처리 유닛("GPU"; graphics processing unit), 필드 프로그램가능 게이트 어레이("FPGA"; field programmable gate array), 프로그램가능 논리 소자("PLD"; programmable logic device), 컨트롤러, 상태 머신(state machine), 게이트 로직(gated logic), 이산 하드웨어 구성요소들, 임의의 다른 처리 유닛, 또는 그것의 임의의 조합 또는 다수일 수 있다. 프로세서(2010)는 단일 처리 유닛, 다수의 처리 유닛들, 단일 처리 코어, 다수의 처리 코어들, 특수 목적 처리 코어들, 코프로세서들(co-processors), 또는 그것의 임의의 조합일 수 있다. 임의의 실시예들에 따르면, 프로세서(2010)는 컴퓨팅 머신(2000)의 다른 구성요소들과 함께 하나 이상의 다른 컴퓨팅 머신들 내에 실행하는 가상화 컴퓨팅 머신일 수 있다.

[0097] 시스템 메모리(2030)는 판독 전용 메모리("ROM"; read-only memory), 프로그램가능 판독 전용 메모리("PROM"; programmable read-only memory), 소거가능 프로그램가능 판독 전용 메모리("EPROM"; erasable programmable read-only memory), 플래시 메모리(flash memory), 또는 인가 전력을 갖거나 갖지 않고 프로그램 명령들 또는 데이터를 저장할 수 있는 임의의 다른 디바이스와 같은 비휘발성 메모리들을 포함할 수 있다. 시스템 메모리(2030)는 랜덤 액세스 메모리("RAM"; random access memory), 정적 랜덤 액세스 메모리("SRAM"; static random access memory), 동적 랜덤 액세스 메모리("DRAM"; dynamic random access memory), 및 동기식 동적 랜덤 액세스 메모리("SDRAM"; synchronous dynamic random access memory)와 같은 휘발성 메모리들을 포함할 수도 있다. 다른 타입들의 RAM은 시스템 메모리(2030)를 구현하기 위해 사용될 수도 있다. 시스템 메모리(2030)는 단일 메모리 모듈 또는 다수의 메모리 모듈들을 사용하여 구현될 수 있다. 시스템 메모리(2030)는 컴퓨팅 머신(2000)의 일부인 것으로 도시되지만, 당해 기술에서 통상의 기술자는 시스템 메모리(2030)가 대상 기술의 범위로부터 벗어나는 것 없이 컴퓨팅 머신(2000)으로부터 분리될 수 있는 것을 인식할 것이다. 또한, 시스템 메모리(2030)는 저장 매체(2040)와 같은 비휘발성 저장 디바이스를 포함하거나, 이와 함께 동작할 수 있다는 점이 이해되어야 한다.

[0098] 저장 매체(2040)는 하드 디스크(hark disk), 플로피 디스크(floppy disk), 시디롬("CD-ROM"; compact disc read only memory), 디비디("DVD"; digital versatile disc), 블루 레이 디스크(Blu-ray disc), 자기 테이프(magnetic tape), 플래시 메모리, 다른 비휘발성 메모리 디바이스, 고체 상태 드라이브("SSD"; solid state drive), 임의의 자기 저장 디바이스, 임의의 광 저장 디바이스, 임의의 전기 저장 디바이스, 임의의 반도체 저장 디바이스, 임의의 물리 기반 저장 디바이스, 임의의 다른 데이터 저장 디바이스, 또는 그것의 임의의 조합 또는 다수를 포함할 수 있다. 저장 매체(2040)는 하나 이상의 운영 체제들, 애플리케이션 프로그램들 및 모듈(2050)과 같은 프로그램 모듈들, 데이터, 또는 임의의 다른 정보를 저장할 수 있다. 저장 매체(2040)는 컴퓨팅 머신(2000)의 일부이거나, 이에 연결될 수 있다. 저장 매체(2040)는 서버들, 데이터베이스 서버들(database servers), 클라우드 저장장치(cloud storage), 네트워크 부착 저장장치 등과 같은 컴퓨팅 머신(2000)과 통신하는 하나 이상의 다른 컴퓨팅 머신들의 일부일 수도 있다.

[0099] 모듈(2050)은 다양한 방법들을 수행하고 본 명세서에 제공된 기능들을 처리하면서 컴퓨팅 머신(2000)을 용이하게 하도록 구성된 하나 이상의 하드웨어 또는 소프트웨어 요소들을 포함할 수 있다. 모듈(2050)은 시스템 메모리(2030), 저장 매체(2040), 또는 양자와 공동으로 소프트웨어 또는 펌웨어(firmware)로 저장된 명령들의 하나 이상의 시퀀스들을 포함할 수 있다. 따라서, 저장 매체(2040)는 명령들 또는 코드가 프로세서(2010)에 의한 실행을 위해 저장될 수 있는 머신 또는 컴퓨터 판독가능 매체의 예들을 제시할 수 있다. 머신 또는 컴퓨터 판독가능 매체는 일반적으로 명령들을 프로세서(2010)에 제공하기 위해 사용되는 임의의 매체 또는 매체들을 지칭할 수 있다. 모듈(2050)과 연관된 그러한 머신 또는 컴퓨터 판독가능 매체는 컴퓨터 소프트웨어 제품을 포함할 수 있다. 모듈(2050)을 포함하는 컴퓨터 소프트웨어 제품은 모듈(2050)을 네트워크(2080), 임의의 신호 베어링 매체(signal-bearing medium), 또는 임의의 다른 통신 또는 전송 기술을 통해 컴퓨팅 머신(2000)에 전달하는 하나 이상의 프로세서들 또는 방법들과 연관될 수도 있다는 점이 이해되어야 한다. 모듈(2050)은 FPGA 또는 다른 PLD에 대한 마이크로코드(microcode) 또는 구성 정보와 같은 하드웨어 회로들을 구성하는 하드웨어 회로들 또는 정보를 포함할 수 있다.

[0100] 입력/출력("I/O"; input/output) 인터페이스(2060)는 하나 이상의 외부 디바이스들에 결합하고, 하나 이상의 외

부 디바이스들로부터 데이터를 수신하고, 데이터를 하나 이상의 외부 디바이스들에 송신하도록 구성될 수 있다. 그러한 외부 디바이스들은 다양한 내부 디바이스들과 함께 주변 디바이스들로 공지될 수도 있다. I/O 인터페이스(2060)는 다양한 주변 디바이스들을 컴퓨팅 머신(2000) 또는 프로세서(2010)에 동작가능하게 결합하는 전기 및 물리 연결들 양자를 포함할 수 있다. I/O 인터페이스(2060)는 주변 디바이스들, 컴퓨팅 머신(2000), 또는 프로세서(2010) 사이에서 데이터, 어드레스들, 및 제어 신호들을 전달하도록 구성될 수 있다. I/O 인터페이스(2060)는 소형 컴퓨터 시스템 인터페이스("SCSI"; small computer system interface), 직렬 부착 SCSI("SAS"; serial-attached SCSI), 파이버 채널(fiber channel), 주변 구성요소 상호연결("PCI"; peripheral component interconnect), PCI 익스프레스(PCIe; PCI express), 직렬 버스, 병렬 버스, 고급 기술 부착("ATA"; advanced technology attached), 직렬 ATA("SATA"; serial ATA), 범용 직렬 버스("USB"; universal serial bus), 선더볼트(Thunderbolt), 파이어와이어(FireWire), 다양한 비디오 버스들 등과 같은, 임의의 표준 인터페이스를 구현하도록 구성될 수 있다. I/O 인터페이스(2060)는 하나의 인터페이스 또는 버스 기술만을 구현하도록 구성될 수 있다. 대안적으로, I/O 인터페이스(2060)는 다수의 인터페이스들 또는 버스 기술들을 구현하도록 구성될 수 있다. I/O 인터페이스(2060)는 시스템 버스(2020)의 일부, 모두로서, 또는 이 버스와 함께 동작하도록 구성될 수 있다. I/O 인터페이스(2060)는 하나 이상의 외부 디바이스들, 내부 디바이스들, 컴퓨팅 머신(2000), 또는 프로세서(2010) 사이에서 송신들을 버퍼링(buffering)하는 하나 이상의 버퍼들을 포함할 수 있다.

[0101] I/O 인터페이스(2060)는 컴퓨팅 머신(2000)을 마우스들, 터치스크린들(touch-screens), 스캐너들, 생체 인식 리더들, 전자 디지타이저들(electronic digitizers), 센서들(sensors), 수신기들, 터치패드들(touchpads), 트랙볼들(trackballs), 카메라들(cameras), 마이크로폰들(microphones), 키보드들(keyboards), 임의의 다른 포인팅 디바이스들(pointing devices), 또는 그것의 임의의 조합들을 포함하는 다양한 입력 디바이스들에 결합할 수 있다. I/O 인터페이스(2060)는 컴퓨팅 머신(2000)을 비디오 디스플레이들(video displays), 스피커들(speakers), 프린터들(printers), 프로젝터들(projectors), 촉각 피드백 디바이스들(tactile feedback devices), 자동화 컨트롤, 로봇 구성요소들, 액추에이터들(actuators), 모터들(motors), 팬들(fans), 솔레노이드들(solenoids), 밸브들(valves), 펌프들(pumps), 송신기들, 신호 이미터들(signal emitters), 라이트들(lights) 등을 포함하는 다양한 출력 디바이스들에 결합할 수 있다.

[0102] 컴퓨팅 머신(2000)은 네트워크(2080)에 걸친 하나 이상의 다른 시스템들 또는 컴퓨팅 머신들에 네트워크 인터페이스(2070)를 통한 논리 연결들을 사용하는 네트워킹 환경에서 동작할 수 있다. 네트워크(2080)는 광역 네트워크들(WAN; wide area networks), 로컬 영역 네트워크들(LAN; local area networks), 인트라넷들, 인터넷, 무선 액세스 네트워크들, 유선 네트워크들, 이동 네트워크들, 전화 네트워크들, 광 네트워크들, 또는 그것의 조합들을 포함할 수 있다. 네트워크(2080)는 임의의 토폴로지(topology)의 패킷(packet) 교환, 회선 교환일 수 있고, 임의의 통신 프로토콜을 사용할 수 있다. 네트워크(2080) 내의 통신 링크들은 광섬유 케이블들(fiber optic cables), 자유 공간 옵틱스(free-space optics), 도파관들(waveguides), 전기 도체들, 무선 링크들, 안테나들, 무선 주파수 통신들 등과 같은 다양한 디지털(digital) 또는 아날로그(analog) 통신 매체를 수반할 수 있다.

[0103] 프로세서(2010)는 시스템 버스(2020)를 통해 본 명세서에 논의된 컴퓨팅 머신(2000)의 다른 요소들 또는 다양한 주변 장치들에 연결될 수 있다. 시스템 버스(2020)는 프로세서(2010) 내부에, 프로세서(2010) 외부에, 또는 양자에 있을 수 있다는 점이 이해되어야 한다. 일부 실시예들에 따르면, 본 명세서에 논의된 프로세서(2010), 컴퓨팅 머신(2000)의 다른 요소들, 또는 다양한 주변 장치들 중 어느 것은 시스템 온 칩("SOC"; system on chip), 시스템 온 패키지("SOP"; system on package), 또는 ASIC 디바이스와 같은 단일 디바이스에 통합될 수 있다.

[0104] 본 명세서에 논의된 시스템들이 사용자들에 관한 개인 정보를 수집하거나, 개인 정보를 이용할 수 있는 상황들에서, 사용자들에게는 프로그램들 또는 피처들이 사용자 정보(예를 들어, 사용자의 소셜 네트워크(social network), 소셜 동작들 또는 활동들, 직업, 사용자의 선호도들, 또는 사용자의 현재 위치에 관한 정보)를 수집하는지를 제어하거나, 사용자에게 더 관련될 수 있는 콘텐츠 서버로부터 콘텐츠를 수신하는지 및/또는 어떻게 수신하는지를 제어할 기회가 제공될 수 있다. 게다가, 임의의 데이터는 그것이 저장되거나 사용되기 전에 하나 이상의 방식들로 처리될 수 있어, 개인적으로 식별가능한 정보가 제거된다. 예를 들어, 사용자의 신분은 개인적으로 식별가능한 정보가 사용자에 대해 결정될 수 있도록 처리될 수 있거나, 사용자의 지리적 위치는 위치 정보가 획득되는 곳(예를 들어 도시, ZIP 코드, 또는 상태 레벨)에 일반화될 수 있어, 사용자의 특정 위치가 결정될 수 없다. 따라서, 사용자는 정보가 사용자에 관하여 수집되고 콘텐츠 서버에 의해 어떻게 사용되는지에 대해 제어할 수 있다.

[0105] 실시예들은 본 명세서에 설명되고 예시되는 기능들을 구체화하는 컴퓨터 프로그램을 포함할 수 있으며, 여기서 컴퓨터 프로그램은 머신 판독가능 매체에 저장된 명령들을 포함하는 컴퓨터 시스템 및 명령들을 실행하는 프로

세서로 구현된다. 그러나, 컴퓨터 프로그래밍으로 실시예들을 구현하는 많은 상이한 방식들이 있을 수 있고, 실시예들이 임의의 한 세트의 컴퓨터 프로그램 명령들에 제한되는 것으로 해석되지 않아야 한다는 점이 분명해야 한다. 게다가, 숙련된 프로그래머는 본 출원 본문 내의 첨부된 흐름도들 및 연관된 설명에 기초하여 개시된 실시예들의 일 실시예를 구현하기 위해 그러한 컴퓨터 프로그램을 기록할 것이다. 따라서, 실시예들을 제조하고 사용하는 법의 적절한 이해에 필요한 특정 세트의 프로그램 코드 명령들의 개시가 고려되지 않는다. 게다가, 당해 기술에서 통상의 기술자들은 본 명세서에 설명된 실시예들의 하나 이상의 측면들이 하나 이상의 컴퓨팅 시스템들에 구현될 수 있는 바와 같이, 하드웨어, 소프트웨어, 또는 그것의 조합에 의해 수행될 수 있는 것을 이해할 것이다. 더욱이, 컴퓨터에 의해 수행되는 동작에 대한 임의의 참조는 하나보다 더 많은 컴퓨터가 동작을 수행할 수 있으므로 단일 컴퓨터에 의해 수행되는 것으로 해석되지 않아야 한다.

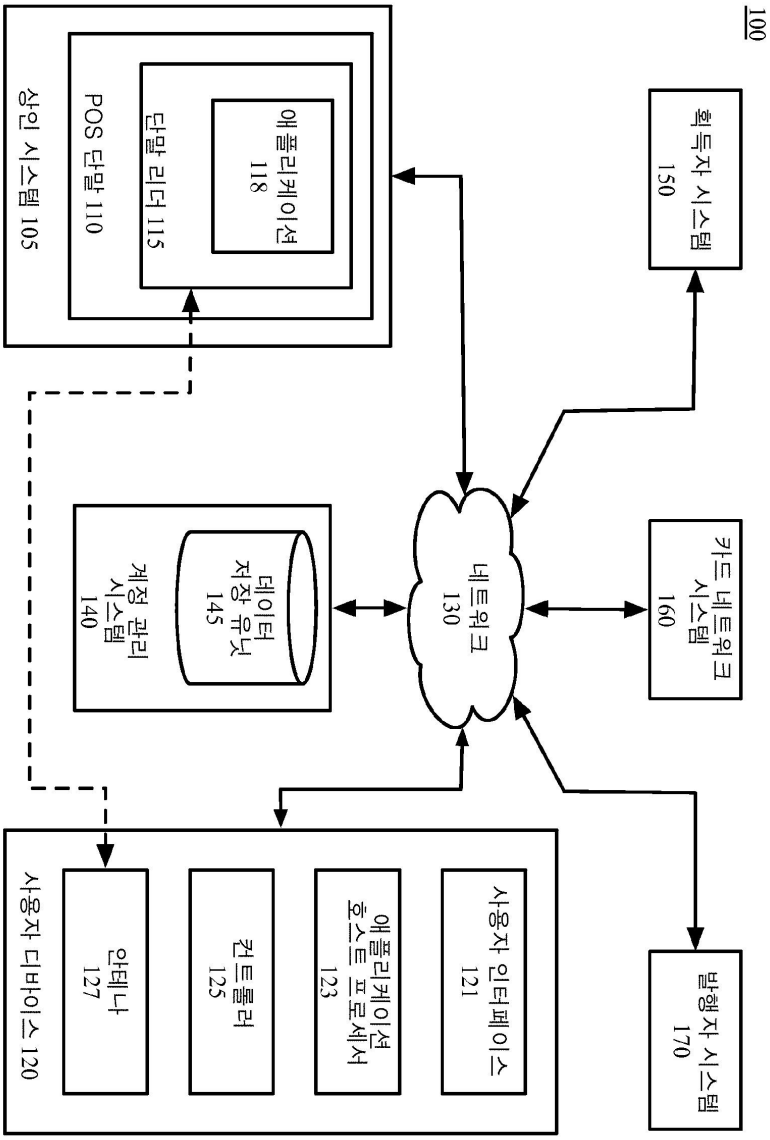
[0106] 본 명세서에 설명된 대표적인 실시예들은 본 명세서에 설명된 방법들 및 처리 기능들을 수행하는 컴퓨터 하드웨어 및 소프트웨어와 함께 사용될 수 있다. 본 명세서에 설명된 시스템들, 방법들, 및 절차들은 프로그램가능 컴퓨터, 컴퓨터 실행가능 소프트웨어, 또는 디지털 회로조직으로 구체화될 수 있다. 소프트웨어는 컴퓨터 판독가능 매체 상에 저장될 수 있다. 예를 들어, 컴퓨터 판독가능 매체는 플로피 디스크, RAM, ROM, 하드 디스크, 이동식 매체, 플래시 메모리, 메모리 스틱(memory stick), 광 매체, 자기 광 매체, CD-ROM 등을 포함할 수 있다. 디지털 회로조직은 집적 회로들, 게이트 어레이들(gate arrays), 형성 블록 로직(building block logic), 필드 프로그램가능 게이트 어레이들(FPGA; field programmable gate arrays) 등을 포함할 수 있다.

[0107] 이전에 제공된 실시예들에 설명된 대표적인 시스템들, 방법들, 및 동작들은 예시적이고, 대안적인 실시예들에서, 임의의 동작들은 상이한 순서로, 서로 병렬로 수행되고/되거나, 전적으로 생략되고/되거나, 상이한 대표적인 실시예들 사이에서 조합될 수 있고/있거나, 어떤 부가 동작들은 다양한 실시예들의 범위 및 사상으로부터 벗어나는 것 없이 수행될 수 있다. 따라서, 그러한 대안적인 실시예들은 본 명세서에 청구된 본 발명에 포함된다.

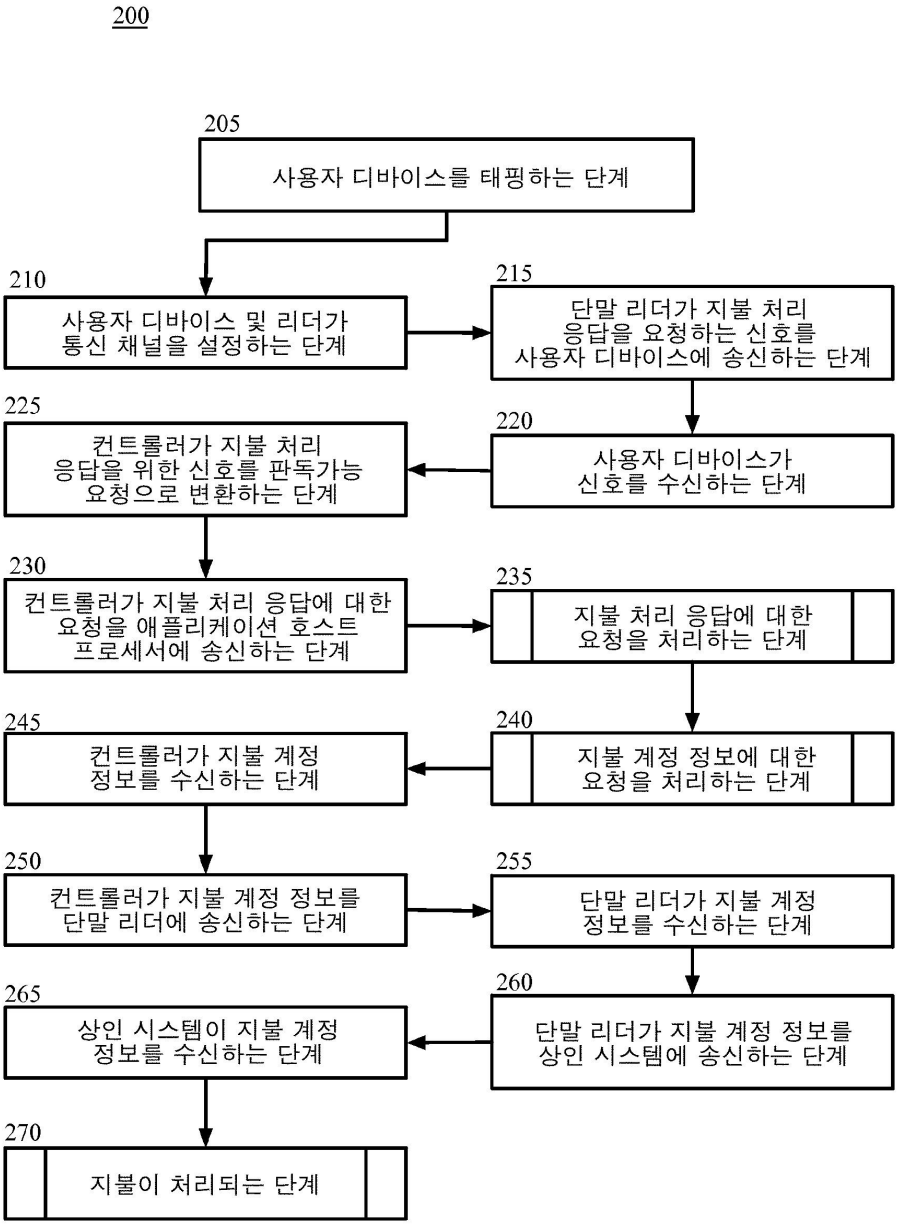
[0108] 특정 실시예들이 위에서 상세히 설명되었지만, 설명은 예시의 목적들만을 위한 것이다. 따라서, 상술된 많은 측면들은 다르게 명시적으로 언급되지 않으면 요구되거나 본질적인 요소들로 의도되지 않는다는 점이 이해되어야 한다. 대표적인 실시예들의 개시된 측면들의 수정들, 및 이 측면들에 대응하는 균등 구성요소들 또는 동작들은 상술된 것들에 더하여, 이하의 특허청구범위에 정의된 실시예들의 사상 및 범위로부터 벗어나는 것 없이, 본 발명의 이득을 갖는 당해 기술에서 통상의 기술자에 의해 이루어질 수 있으며, 그 범위는 그러한 수정들 및 균등 구조들을 망라하도록 가장 넓은 해석에 부합되어야 한다.

도면

도면1

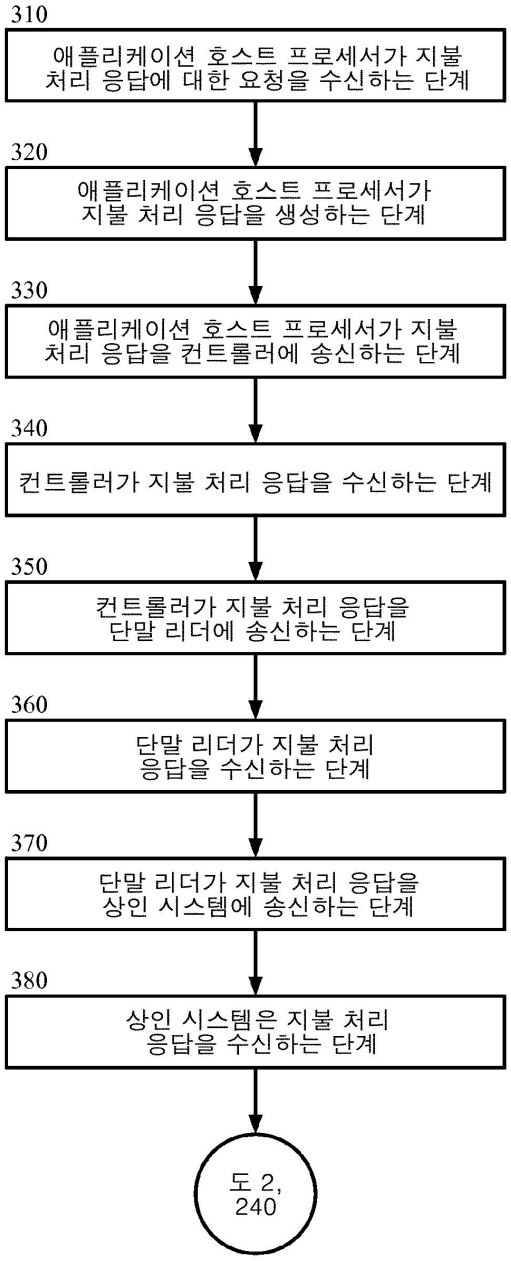

100
상인 시스템 105
POS 단말 110
단말 리더 115
애플리케이션 118
획득자 시스템 150
네트워크 130
계정 관리 시스템 140
데이터 저장 유닛 145
카드 네트워크 시스템 160
사용자 디바이스 120
인테나 127
컨트롤러 125
애플리케이션 호스트 프로세서 123
사용자 인터페이스 121
발행자 시스템 170

도면2


200
205
사용자 디바이스를 태핑하는 단계
210
사용자 디바이스 및 리더가 통신 채널을 설정하는 단계
215
단말 리더가 지불 처리 응답을 요청하는 신호를 사용자 디바이스에 송신하는 단계
220
사용자 디바이스가 신호를 수신하는 단계
225
컨트롤러가 지불 처리 응답을 위한 신호를 판독가능 요청으로 변환하는 단계
230
컨트롤러가 지불 처리 응답에 대한 요청을 애플리케이션 호스트 프로세서에 송신하는 단계
235
지불 처리 응답에 대한 요청을 처리하는 단계
240
지불 계정 정보에 대한 요청을 처리하는 단계
245
컨트롤러가 지불 계정 정보를 수신하는 단계
250
컨트롤러가 지불 계정 정보를 단말 리더에 송신하는 단계
255
단말 리더가 지불 계정 정보를 수신하는 단계
260
단말 리더가 지불 계정 정보를 상인 시스템에 송신하는 단계
265
상인 시스템이 지불 계정 정보를 수신하는 단계
270
지불이 처리되는 단계

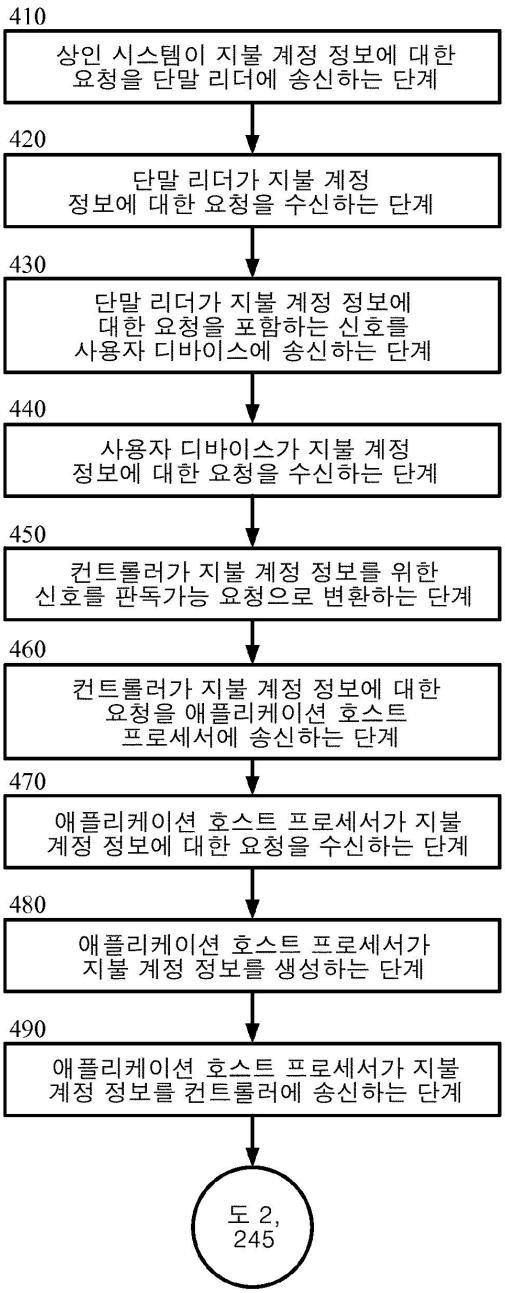
도면3

235

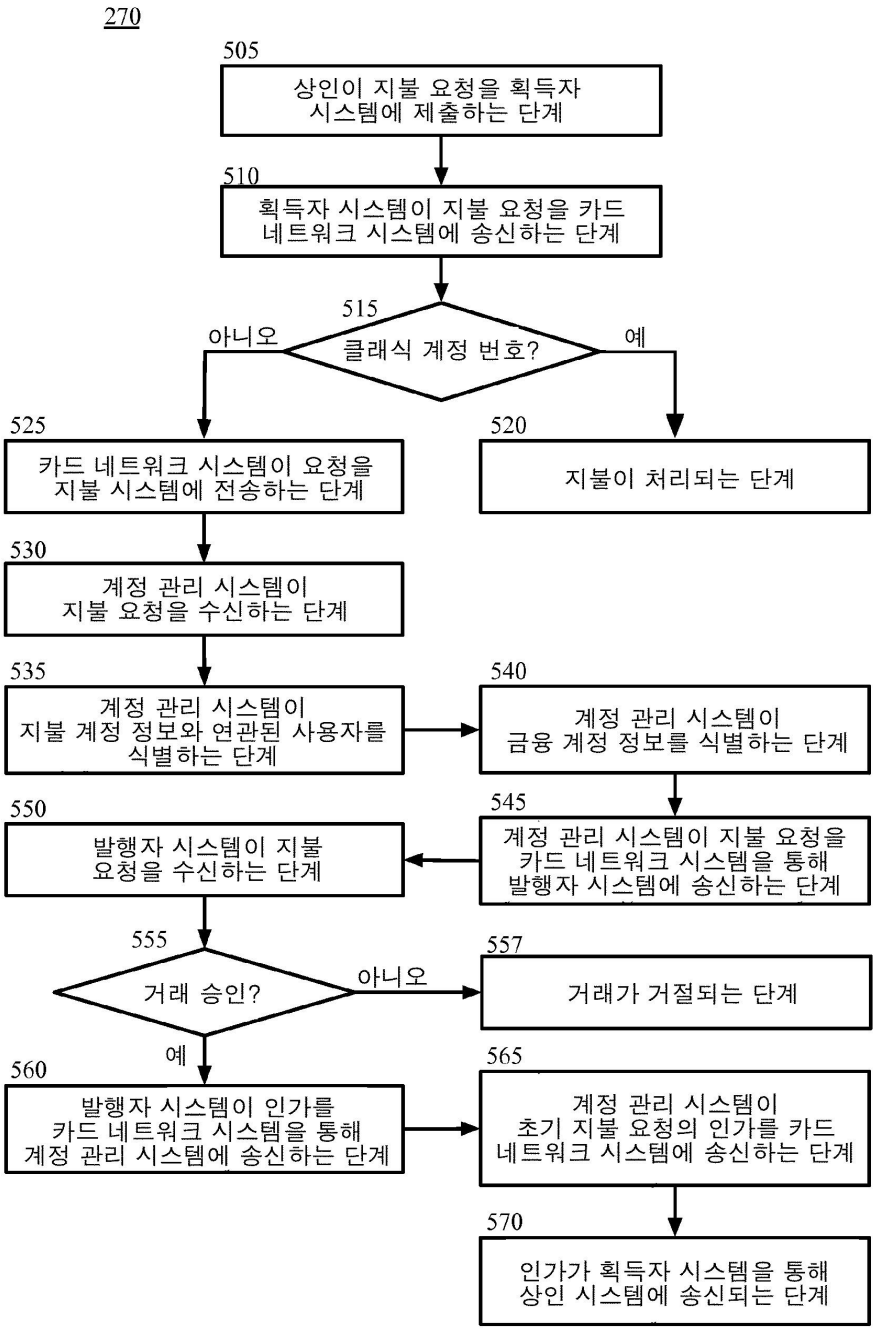

310
애플리케이션 호스트 프로세서가 지불 처리 응답에 대한 요청을 수신하는 단계
320
애플리케이션 호스트 프로세서가 지불 처리 응답을 생성하는 단계
330
애플리케이션 호스트 프로세서가 지불 처리 응답을 컨트롤러에 송신하는 단계
340
컨트롤러가 지불 처리 응답을 수신하는 단계
350
컨트롤러가 지불 처리 응답을 단말 리더에 송신하는 단계
360
단말 리더가 지불 처리 응답을 수신하는 단계
370
단말 리더가 지불 처리 응답을 상인 시스템에 송신하는 단계
380
상인 시스템은 지불 처리 응답을 수신하는 단계
도 2, 240

도면4

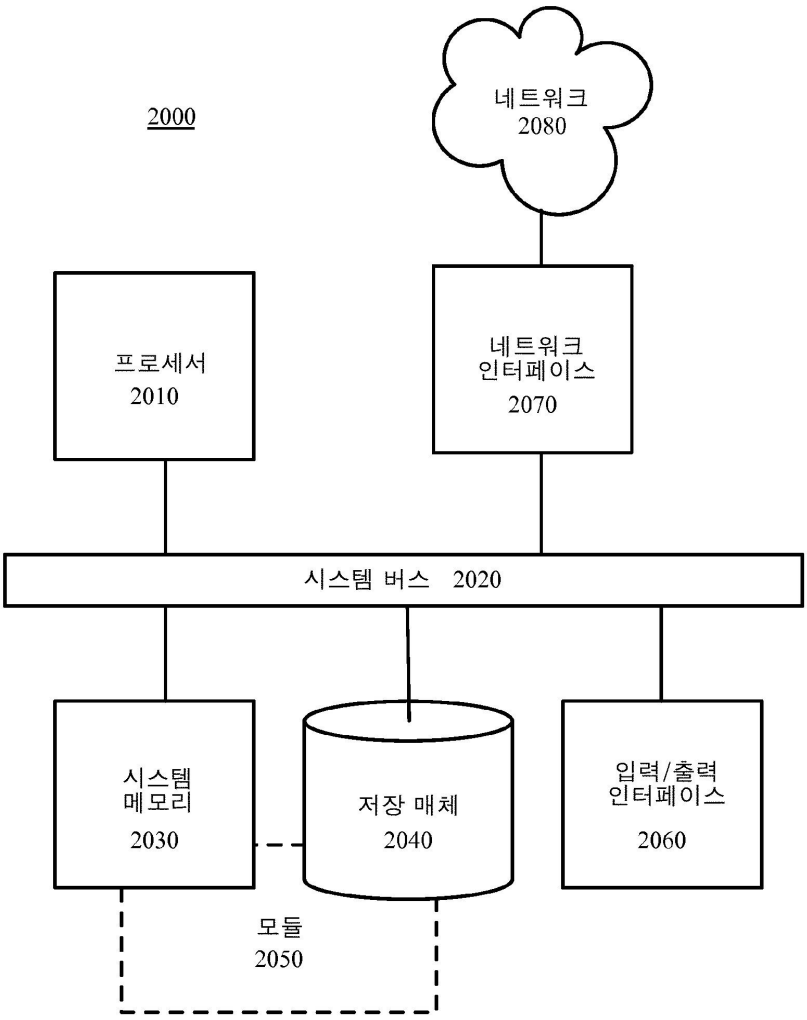
240


410
상인 시스템이 지불 계정 정보에 대한 요청을 단말 리더에 송신하는 단계
420
단말 리더가 지불 계정 정보에 대한 요청을 수신하는 단계
430
단말 리더가 지불 계정 정보에 대한 요청을 포함하는 신호를 사용자 디바이스에 송신하는 단계
440
사용자 디바이스가 지불 계정 정보에 대한 요청을 수신하는 단계
450
컨트롤러가 지불 계정 정보를 위한 신호를 판독가능 요청으로 변환하는 단계
460
컨트롤러가 지불 계정 정보에 대한 요청을 애플리케이션 호스트 프로세서에 송신하는 단계
470
애플리케이션 호스트 프로세서가 지불 계정 정보에 대한 요청을 수신하는 단계
480
애플리케이션 호스트 프로세서가 지불 계정 정보를 생성하는 단계
490
애플리케이션 호스트 프로세서가 지불 계정 정보를 컨트롤러에 송신하는 단계
도 2, 245

도면5


270
505
상인이 지불 요청을 획득자 시스템에 제출하는 단계
510
획득자 시스템이 지불 요청을 카드 네트워크 시스템에 송신하는 단계
515
클래식 계정 번호?
아니오
예
525
카드 네트워크 시스템이 요청을 지불 시스템에 전송하는 단계
520
지불이 처리되는 단계
530
계정 관리 시스템이 지불 요청을 수신하는 단계
535
계정 관리 시스템이 지불 계정 정보와 연관된 사용자를 식별하는 단계
540
계정 관리 시스템이 금융 계정 정보를 식별하는 단계
545
계정 관리 시스템이 지불 요청을 카드 네트워크 시스템을 통해 발행자 시스템에 송신하는 단계
550
발행자 시스템이 지불 요청을 수신하는 단계
555
거래 승인?
아니오
557
거래가 거절되는 단계
예
560
발행자 시스템이 인가를 카드 네트워크 시스템을 통해 계정 관리 시스템에 송신하는 단계
565
계정 관리 시스템이 초기 지불 요청의 인가를 카드 네트워크 시스템에 송신하는 단계
570
인가가 획득자 시스템을 통해 상인 시스템에 송신되는 단계

도면6



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 12(12줄)

【변경전】

상기 보안 요소 프로세서

【변경후】

보안 요소 프로세서