(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0116430
(43) 공개일자 2022년08월23일

(51) 국제특허분류(Int. Cl.)
G06Q 30/02 (2012.01) *G06Q 20/32* (2012.01)
G06Q 20/34 (2012.01) *G06Q 20/38* (2012.01)
G06Q 20/40 (2012.01)
(52) CPC특허분류
G06Q 30/0215 (2013.01)
G06Q 20/3278 (2013.01)
(21) 출원번호 10-2022-7014392
(22) 출원일자(국제) 2020년11월24일
심사청구일자 없음
(85) 번역문제출일자 2022년04월28일
(86) 국제출원번호 PCT/US2020/061972
(87) 국제공개번호 WO 2021/133503
국제공개일자 2021년07월01일
(30) 우선권주장
16/727,294 2019년12월26일 미국(US)

(71) 출원인
캐피탈 원 서비시즈, 엘엘씨
미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680
(72) 발명자
오스본, 케빈
미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680, 캐피탈 원 서비시즈, 엘엘씨 내
치구루파티, 스리니바사
미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680, 캐피탈 원 서비시즈, 엘엘씨 내
룰, 제프리
미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680, 캐피탈 원 서비시즈, 엘엘씨 내
(74) 대리인
김동완

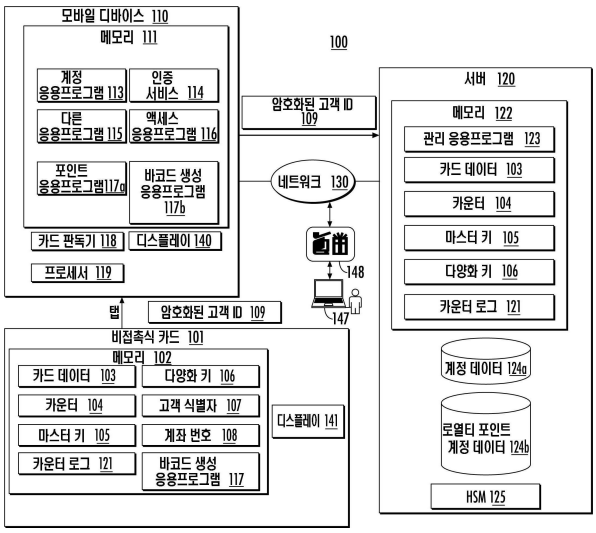
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **다수의 로열티 포인트 계정의 액세스 및 활용**

(57) 요 약

다양한 실시형태는 다수의 로열티 포인트 및 로열티 계정에 액세스, 상환 또는 활용하기 위해 오프라인 및/또는 온라인 검증 또는 인증 프로토콜을 활용하는 것에 일반적으로 관한 것이다. 다양한 로열티 포인트를 활용하는 방법은 사용자가 로열티 포인트 계정 데이터베이스에 대한 액세스를 요청하고 있다고 결정하는 단계; 암호화 알고리즘 및 다양화 키를 기반으로 생성된 암호화된 데이터를 수신하는 단계; 검증은 암호화된 데이터를 포함하는 데이터 조합을 검증하는 것을 포함하고, 여기서 발급자와 연관된 서버는 암호화 알고리즘 및 다양화 키를 기반으로 데이터 조합을 복호화 할 수 있으며, 사용자의 검증을 수신하는 단계; 사용자의 검증을 수신하는 것에 응답하여, 사용자의 로열티 포인트 계정과 연관된 데이터베이스에 액세스하는 단계; 및 로열티 포인트 계정과 연관된 다수의 로열티 포인트의 상환을 승인하는 단계;를 포함한다.

대 표 도



(52) CPC특허분류
G06Q 20/341 (2013.01)
G06Q 20/352 (2013.01)
G06Q 20/3829 (2013.01)
G06Q 20/40975 (2020.05)
G06Q 30/0233 (2013.01)

명 세 서

청구범위

청구항 1

프로세서 회로; 및

명령어를 저장하는 메모리; 를 포함하는 기기에 있어서,

상기 명령어는 프로세서 회로에 의해 실행될 때 프로세서 회로가

다수의 로열티 포인트와 연관된 다수의 계정과 관련된 적어도 하나의 동작을 수행하기 위한 요청을 프로세서 회로 상에서 실행하는 응용프로그램에 의해 개시하고;

암호화된 데이터는 암호화 알고리즘 및 다양화 키를 기반으로 하고, 다양화 키는 마스터 키 및 키운터 값을 기반으로 하며, 비접촉식 카드의 통신 인터페이스로부터 암호화된 데이터를 응용프로그램에 의해 수신하고;

서버가 암호화 알고리즘 및 다양화 키에 기반하여 암호화된 데이터를 검증했다는 표시를 서버로부터 응용프로그램에 의해 수신하고; 및

적어도 하나의 동작은 i) 각각의 계정은 로열티 포인트의 별개의 세트와 연관되고, 적어도 하나의 사용자 및 적어도 2개의 별개의 계정과 연관된 다수의 로열티 식별자를 포함하는 데이터베이스에 액세스하는 단계; 및 ii) 데이터베이스의 적어도 2개의 별개의 계정과 관련하여 다수의 로열티 식별자 중 적어도 하나를 저장하는 단계; 중 적어도 하나를 포함하며, 검증을 수신하는 것에 응답하여, 적어도 하나의 동작을 수행하기 위한 권한을 부여;

하도록 유도하는 기기.

청구항 2

제 1항에 있어서, 명령어를 저장하는 프로세서 회로에 의해 실행될 때 프로세서 회로가:

적어도 2개의 계정 중에서 하나를 선택하고; 및

선택된 계정과 연관된 로열티의 개별 포인트 세트와 관련하여 적어도 하나의 동작을 실행;

하도록 유도함을 특징으로 하는 기기.

청구항 3

제 2항에 있어서, 적어도 하나의 동작은 상환(redemption)동작임을 특징으로 하는 기기.

청구항 4

제 3항에 있어서, 비접촉식 카드로부터 수신된 암호화된 데이터는 컴퓨터 디바이스에 대한 비접촉식 카드의 제1탭에 기반함을 특징으로 하는 기기.

청구항 5

제 4항에 있어서, 암호화된 데이터의 검증은 다수의 계정 중 적어도 하나와 연관된 적어도 하나의 사용자 식별과 결합되는 암호와 관련됨을 특징으로 하는 기기.

청구항 6

제 5항에 있어서, 조합은 논리 연산에 기반함을 특징으로 하는 기기.

청구항 7

제 6항에 있어서, 논리 연산은 배타적 논리합 연산을 포함함을 특징으로 하는 기기.

청구항 8

사용자가 로열티 포인트 계정 데이터베이스에 대한 액세스를 요청하고 있음을 프로세서 회로 상에서 실행하는 응용프로그램에 의해 결정하는 단계;

암호화된 데이터는 암호화 알고리즘 및 다양화 키를 기반으로 생성되고, 다양화 키는 비접촉식 카드의 메모리 내에 저장되고 비접촉식 카드의 메모리 내에 저장된 마스터 키 및 카운터 값을 기반으로 생성되며, 계정과 연관된 비접촉식 카드의 통신 인터페이스로부터 암호화된 데이터를 응용프로그램에 의해 수신하는 단계;

검증은 암호화된 데이터를 포함하는 데이터 조합을 검증하는 것을 포함하고, 서버는 데이터 조합을 검증하기 위하여 서버의 메모리 내에 저장된 암호화 알고리즘 및 다양화 키를 기반으로 데이터 조합을 복호화하기 위한 것이고, 서버의 메모리 내에 저장된 다양화 키는 서버의 메모리 내에 저장된 마스터 키 및 카운터 값을 기반으로 생성되며, 사용자의 검증을 서버로부터 응용프로그램에 의해 수신하는 단계; 및

사용자의 검증을 수신하는 것에 응답하여, 데이터 베이스 내에서 사용자의 로열티 포인트 계정에 대한 액세스를 승인하고 로열티 포인트 계정과 연관된 다수의 로열티 포인트의 상환을 승인하는 단계;

를 포함하는 방법.

청구항 9

제 8항에 있어서,

처리 화로와 연관된 컴퓨터 디바이스로부터 응용프로그램에 의해 서버로 제1 응용프로그램 사용자 자격증명을 전송하는 단계; 및

복호화 이전에, 서버에서, 제1 응용프로그램 사용자 자격증명을 서버에 의해 저장된 제2 응용프로그램 사용자 자격증명과 비교하는 단계;

를 더욱 포함함을 특징으로 하는 방법.

청구항 10

제 9항에 있어서,

데이터 조합은 로열티 식별자 및 암호화된 데이터의 조합을 포함하고,

복호화 전에, 및 제1 응용프로그램 사용자 자격증명과 제2 응용프로그램 사용자 자격증명 사이의 매치를 찾는 것에 응답하여, 사용자와 연관된 로열티 식별자를 암호화된 데이터와 결합하는 단계;

를 더욱 포함함을 특징으로 하는 방법.

청구항 11

제 10항에 있어서, 사용자와 연관된 로열티 식별자를 암호화된 데이터와 결합하는 단계는

서버에서, 수신된 암호화된 데이터 및 로열티 식별자에 대한 동작을 수행하는 단계;

를 포함함을 특징으로 하는 방법.

청구항 12

제 11항에 있어서, 로열티 식별자는 서버에 저장됨을 특징으로 하는 방법.

청구항 13

제 11항에 있어서, 연산은 배타적 논리합 연산임을 특징으로 하는 방법.

청구항 14

제 10항에 있어서,

생성된 바코드는 서버로부터 수신된 토큰을 기반으로 하며,

ⅰ) 비접촉식 카드 및 ⅱ) 컴퓨터 디바이스에서 바코드를 생성하는 단계;

를 더욱 포함함을 특징으로 하는 방법.

청구항 15

제 14항에 있어서, 토큰은 암호화된 데이터와 로열티 식별자의 조합에 기반함을 특징으로 하는 방법.

청구항 16

제 15항에 있어서,

생성된 바코드를 표시하는 단계; 및

스캔 디바이스를 사용하여 생성된 바코드를 스캔하는 단계;

를 더욱 포함함을 특징으로 하는 방법.

청구항 17

제 16항에 있어서,

생성된 바코드의 스캐닝에 응답하여 데이터 조합의 복호화를 수행하는 단계;

를 더욱 포함함을 특징으로 하는 방법.

청구항 18

프로세서 회로가

다수의 로열티 포인트와 연관된 다수의 계정과 관련된 적어도 하나의 동작을 수행하기 위한 요청을 개시하고;

암호화된 데이터는 암호화 알고리즘 및 다양화 키를 기반으로 하고, 다양화 키는 마스터 키 및 키운터 값을 기반으로 하며, 비접촉식 카드로부터 암호화된 데이터를 수신하고;

서버가 암호화 알고리즘 및 다양화 키에 기반하여 암호화된 데이터를 검증했다는 표시를 서버로부터 수신하고;

및

적어도 하나의 동작은 i) 각각의 계정은 로열티 포인트의 별개의 세트와 연관되고, 적어도 하나의 사용자 및 적어도 2개의 별개의 계정과 연관된 다수의 로열티 식별자를 포함하는 데이터베이스에 액세스하는 단계; 및 ii) 데이터베이스의 적어도 2개의 별개의 계정과 관련하여 다수의 로열티 식별자 중 적어도 하나를 저장하는 단계; 중 적어도 하나를 포함하며, 검증을 수신하는 것에 응답하여, 적어도 하나의 동작을 수행하기 위한 권한을 부여;

하도록 유도하는

프로세서 회로에 의해 실행 가능한 컴퓨터 판독가능 프로그램 코드를 저장하는 비일시적 컴퓨터 판독가능 저장 매체.

청구항 19

제 18항에 있어서, 프로세서 회로가

서버로부터 토큰을 수신;

하도록 유도하는

프로세서 회로에 의해 실행가능한 컴퓨터 판독가능 프로그램 코드를 더욱 포함함을 특징으로 하는 컴퓨터 판독가능 저장 매체.

청구항 20

제 19항에 있어서, 프로세서 회로가

서버로부터 수신된 토큰에 기반하여 바코드를 생성;

하도록 유도하는

프로세서 회로에 의해 실행가능한 컴퓨터 판독가능 프로그램 코드를 더욱 포함함을 특징으로 하는 컴퓨터 판독가능 저장 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 2019년 12월 26일자로 출원된 "다수의 로열티 포인트 계정의 액세스 및 활용"이라는 제목의 미국 특허출원 제16/727,294호에 대한 우선권을 주장한다. 앞서 언급한 특허 출원의 내용은 그 전체가 참고 문헌으로 본 명세서에 통합되어 있다.

[0002] 본 발명의 실시형태는 일반적으로 컴퓨터 플랫폼에 관한 것으로 보다 구체적으로는 다양한 인증 프로토콜을 사용하여 다수의 로열티 계정에 액세스하는 것에 관한 것이다.

배 경 기 술

[0003] 많은 카드, 특히 금융 카드 예를 들어 신용 카드를 활성화하려면 카드 소유자가 전화 번호로 전화를 걸거나 웹 사이트를 방문하고 카드 정보를 입력하거나 제공하는 시간 소모적인 프로세스가 필요한다. 또한 칩 기반 금융 카드의 사용이 증가하면서 직접 구매를 위한 이전 기술 예를 들어 마그네틱 스트립 카드에 비해 더 안전한 기능을 제공하지만 계정 액세스는 카드 소유자의 신원 확인 및/또는 거래 완료를 위해 여전히 일반적으로 예를 들어 사용자 이름 및 패스워드와 같은 로그인 자격증명에 의존한다. 그러나 로그인 자격증명이 손상되면 다른 사람이 사용자 계정에 액세스할 수 있다.

[0004] 여러 계정에 효율적으로 액세스하려고 시도할 때 계정 보안 문제가 악화된다. 계정 액세스가 결제, 상환 활동 또는 일반 액세스와 관련이 있는지 여부에 관계없이 단일 인증 자격증명 또는 메커니즘이 손상되면 보안 위험이 가중될 수 있다.

[0005] 따라서 결제 및 환매 거래를 포함한 거래 경쟁 및 계정 접근에 대한 인증 메커니즘을 개선할 필요가 있다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0006] 본 발명에 개시된 실시형태는 결제 트랜잭션을 포함하지만 이에 제한되지 않는 사용자 검증 및/또는 거래 완료를 위해 스테가노그래피로 인코딩된 이미지를 활용하는 시스템, 방법, 제조 물품 및 컴퓨터 판독 가능 매체를 제공한다. 하나 이상의 실시예에 따르면 온라인 프로토콜은 로열티 포인트와 연관된 하나 이상의 계정에 대한 액세스를 제공하는 또는 그렇지 않으면 활용하는 정보의 교환을 개시하기 위해 사용자를 검증 및/또는 인증하는데 사용된다.

[0007] 하나의 실시에 따르면 컴퓨터 시스템에서 실행되는 응용프로그램을 활용하는 컴퓨터 구현 방법은 스테가노그래피로 인코딩된 이미지를 활용하여 사용자의 신원을 검증하고 및/또는 트랜잭션을 승인하기 위해 트랜잭션을 개시할 수 있다. 다양한 실시형태에서 응용프로그램은 사용자 디바이스, 예를 들어 모바일 디바이스에서 비접촉식 카드를 탭 함으로써 시작될 수 있다.

[0008] 방법은 프로세서 회로 상에서 실행하는 응용프로그램에 의해, 사용자가 로열티 포인트 계정 데이터베이스에 대한 액세스를 요청하고 있음을 결정하는 단계: 암호화된 데이터는 암호화 알고리즘 및 다양화 키를 기반으로 생성되고, 비접촉식 카드의 메모리 내에 저장된 다양화 키는 비접촉식 카드의 메모리 내에 저장된 마스터 키 및 카운터 값을 기반으로 생성되며, 계정과 연관된 비접촉식 카드의 통신 인터페이스로부터 암호화된 데이터를 응용프로그램에 의해 수신하는 단계; 검증은 암호화된 데이터를 포함하는 데이터 조합을 검증하는 것을 포함하고, 서버는 데이터 조합을 검증하기 위하여 서버의 메모리 내에 저장된 암호화 알고리즘 및 다양화 키를 기반으로 데이터 조합을 복호화 하기 위한 것이고, 서버의 메모리 내에 저장된 다양화 키는 서버의 메모리 내에 저장된 마스터 키 및 카운터 값을 기반으로 생성되며, 사용자의 검증을 서버로부터 응용프로그램에 의해 수신하는 단계; 및 사용자의 검증을 수신하는 것에 응답하여, 사용자의 로열티 포인트 계정과 연관된 데이터베이스에 액세스하고 로열티 포인트 계정과 연관된 다수의 로열티 포인트의 상환을 승인하는 단계;를 포함할 수 있다.

[0009] 다른 실시예에 따르면 시스템은 온라인 및/또는 오프라인 인증과 스테가노그래피적으로 인코딩된 이미지를 사용하여 사용자를 인증 및/또는 검증하고 및/또는 거래를 승인한다.

[0010] 시스템은 프로세서 회로 및 명령어를 저장하는 메모리를 포함할 수 있으며, 상기 명령어는 프로세서 회로에 의해 실행될 때 프로세서 회로가 다수의 로열티 포인트와 연관된 다수의 계정과 관련된 적어도 하나의 동작을 수행하기 위한 요청을 프로세서 회로 상에서 실행하는 응용프로그램에 의해 개시하고,암호화된 데이터는 암호화 알고리즘 및 다양화 키를 기반으로 생성되고, 비접촉식 카드의 메모리 내에 저장된 다양화 키는 비접촉식 카드의 메모리 내에 저장된 마스터 키와 카운터 값을 기반으로 생성되며, 계정과 연관된 비접촉식 카드의 통신 인터페이스로부터 암호화된 데이터를 응용프로그램에 의해 수신하고,서버는 암호화된 데이터를 검증하기 위하여 서버의 메모리 내에 저장된 암호화 알고리즘 및 다양화 키를 기반으로 암호화된 데이터를 복호화 하기 위한 것이고, 서버의 메모리 내에 저장된 다양화 키는 서버의 메모리 내에 저장된 마스터 키 및 카운터 값을 기반으로 생성되며, 암호화된 데이터의 검증을 서버로부터 응용프로그램에 의해 수신하고; 및 적어도 하나의 동작은 i) 각각의 계정은 로열티 포인트의 별개의 세트와 연관되고, 적어도 하나의 사용자 및 적어도 2개의 별개의 계정과 연관된 다수의 로열티 식별자를 포함하는 데이터베이스에 액세스하는 단계; 및 ii) 데이터베이스의 적어도 2개의 별개의 계정과 관련하여 다수의 로열티 식별자 중 적어도 하나를 저장하는 단계; 중 적어도 하나를 포함하며, 검증을 수신하는 것에 응답하여, 적어도 하나의 동작을 수행하기 위한 권한을 부여,하도록 유도한다.

[0011] 또 다른 실시예에 따르면 사용자와 연관된 카드의 발급자와 연관된 호스트 시스템으로서, 호스트 시스템은 컴퓨터 판독가능 프로그램 코드를 저장하는 비일시적 컴퓨터 판독가능 저장 매체를 포함하며, 상기 컴퓨터 판독가능 프로그램 코드는 프로세서에 의해 실행되어, i) 다수의 로열티 계정과 연관된 적어도 하나의 사용자 계정의 로열티 식별자 및 ii) 암호화 알고리즘 및 다양화 키를 기반으로 생성된 암호화된 데이터;를 포함하는 데이터 조합을 생성시키고, 및 암호화된 데이터를 검증하기 위하여 서버의 메모리 내에 저장된 암호화 알고리즘 및 다양화 키를 기반으로 암호화된 데이터를 복호화하고, 이때 서버의 메모리 내에 저장된 다양화 키는 서버의 메모리

내에 저장된 마스터 키 및 카운터 값을 기반으로 생성 되는 것이다.

도면의 간단한 설명

[0012] 도 1은 결제 프로토콜에 따라 사용자를 검증 또는 인증하기 위한 시스템의 실시형태를 도시한다.

도 2는 인증 프로토콜을 활용하여 사용자를 검증하기 위해 탭 하는 적어도 하나의 실시형태를 도시한다.

도 3은 도 2의 탭 및 검증에 기반하여 바코드를 생성하는 적어도 하나의 실시형태를 도시한다.

도 4a 내지 도 4b는 예시적인 비접촉식 카드를 도시한다.

도 5는 제1 논리 흐름의 실시형태를 도시한다.

도 6은 제2 논리 흐름의 실시형태를 도시한다.

도 7은 컴퓨터 아키텍처의 실시형태를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0013] 본 발명의 측면은 인증된 카드소유자 액세스를 제공하기 위한 시스템, 방법 및/또는 기술을 포함한다. 일반적으로 다양한 실시형태는 온라인 인증 프로토콜을 활용하고 바코드를 생성함으로써 하나 이상의 로열티 포인트 계정에 액세스하거나 그렇지 않으면 활용하는 것에 관한 것이며, 여기서 바코드는 결제 트랜잭션을 포함하는 하나 이상의 거래를 완료하기 위해 사용될 수 있다. 다양한 실시형태에서 바코드는 온라인 인증 프로토콜에 따라 생성되지만, 보안을 더욱 강화하기 위해 단일 트랜잭션에 대해서만 유효하고, 단일 트랜잭션과 연관된 응용프로그램의 부적절한 사용을 방지하기 위해 만료된다. 개시된 실시형태와 일치하여 시스템 및 방법은 하나 이상의 컴퓨터 디바이스, 프로세서, 웹 서버, 계정 서버 및/또는 비접촉식 디바이스(예를 들어 무선 주파수 식별(RFID) 카드)를 활용할 수 있다.

[0014] 본 발명의 다양한 실시형태는 온라인 기술과 같은 동적 인증 기술에 의해 제공되는 강화된 보안의 이점을 이용하는 것을 포함하여, 사용자를 검증하고 결제 트랜잭션과 같은 거래를 완료하는 측면에서 또한 거래를 완료하기 위해 바코드를 활용하는 측면에서(이는 편의성과 추가 보안 모두를 제공한다) 하나 이상의 이점을 제공한다.

[0015] 다양한 실시형태에서 온라인 기술을 활용하면 예를 들어 엔터테인먼트 응용프로그램과 관련된 운송 응용프로그램과 같이 하나 이상의 응용 프로그램의 목적이 구별되는 경우에도 하나 이상의 응용 프로그램에서 사용자를 인증하거나 검증하기 위한 단일 방법을 제공함으로써 휴대 전화와 같은 컴퓨터 디바이스의 효율성이 향상된다.

[0016] 따라서 다양한 실시형태에서 인증 프로토콜은 상이한 응용프로그램 및 목적에 걸쳐 사용자를 효율적이고 더 안전하게 인증하는 데 사용될 수 있으며 그 후 결제를 포함하거나 포함하지 않을 수 있는 거래 및 동작을 포함하는 하나 이상의 상이한 응용프로그램과 연관된 트랜잭션을 완료하기 위해 검증의 결과로서 생성된 바코드를 활용할 수 있다.

[0017] 도 1은 개시된 실시형태와 일치하는 예시적인 시스템(100)의 개략도를 도시한다. 도시된 바와 같이 시스템(100)은 하나 이상의 비접촉식 카드(101), 하나 이상의 모바일 디바이스(110) 및 서버(120)를 포함한다. 비접촉식 카드(101)는 신용 카드, 직불 카드, ATM 카드, 로열티 계정 카드, 기프트 카드 등과 같은 임의의 유형의 결제 카드를 나타낸다. 다양한 실시형태에서 비접촉식 카드(101) 또는 카드(101)는 가상 결제 카드이다.

[0018] 비접촉식 카드(101)는 NFC, EMV 표준, 또는 무선 통신의 다른 단거리 프로토콜을 통해 모바일 디바이스(110)와 통신하도록 구성된 무선 주파수 식별(RFID) 칩과 같은 하나 이상의 칩을 포함할 수 있다(나타내지 않음). NFC가 예시적인 통신 프로토콜로서 사용되었으나 본 발명은 EMV 표준, 블루투스 및/또는 Wi-Fi에 따른 다른 적절한 통신 프로토콜과 같은 다른 유형의 무선 통신에도 동일하게 적용 가능하다.

[0019] 모바일 디바이스(110)는 스마트폰, 태블릿 컴퓨터, 웨어러블 디바이스, 랩톱, 휴대용 게임 디바이스 등과 같은 임의의 유형의 네트워크 가능 컴퓨터 디바이스를 나타낸다. 서버(120)는 서버, 워크스테이션, 컴퓨터 클러스터, 클라우드 컴퓨터 플랫폼, 가상화 컴퓨터 시스템 등과 같은 임의의 유형의 컴퓨터 디바이스를 나타낸다.

[0020] 도시된 바와 같이 비접촉식 카드의 메모리(102)는 카드 데이터(103), 카운터(104), 마스터 키(105), 다양화 키(106), 고유 고객 식별자(107) 및 계좌 번호의 데이터 저장소(108)를 포함한다. 카드 데이터(103)는 비접촉식 카드(101)를 사용하여 결제를 처리하는 데 사용되는 정보와 같은 계정 관련 정보를 일반적으로 포함한다. 예를 들어 카드 데이터(103)는 계좌 번호, 유효기한, 청구 주소 및 카드 검증 값(CVV)을 포함할 수 있다. 계좌 번호

는 주 계좌 번호(PAN), 가상 계좌 번호 및/또는 PAN을 기반으로 생성된 토큰과 같은 모든 유형의 계좌 번호일 수 있다. 다른 유형의 계좌 번호가 고려되며 계좌 번호 또는 다른 유형의 카드 데이터(103)의 사용이 본 발명을 제한하는 것으로 간주되어서는 안 된다.

[0021] 카드 데이터(103)는 이름, 청구서 수신 주소, 배송 주소 및 기타 계정 관련 정보를 더욱 포함할 수 있다. 계좌 번호(108)는 관련 유효기한 및 CVV 값과 함께 1회용 가상 계좌 번호를 저장한다. 예를 들어 계좌 번호(108)는 수천 개의 일회용 가상 계좌 번호, 만료 날짜 및 CVV 값을 포함할 수 있다.

[0022] 도시된 바와 같이 모바일 디바이스(110)의 메모리(111)는 운영 체제(OS)(112)의 인스턴스를 포함하고 프로세서(119)는 운영 체제(OS)(112)의 응용프로그램과 연관된 하나 이상의 동작을 실행하고 및/또는 메모리(111)와 연관된 비교 연산 및 실행 명령을 포함하는 프로세서 활동과 연관된 임의의 적절한 연산을 수행할 수 있다. 예시적인 운영 체제(112)는 Android® OS, iOS®, Linux® 및 Windows® 운영 체제를 포함한다. 도시된 바와 같이 OS(112)는 계정 응용프로그램(113), 인증 또는 검증 응용프로그램 또는 서비스(114)(이하 편의상 "인증 응용프로그램"이라 함), 하나 이상의 다른 응용프로그램(115) 및/또는 하나 이상의 액세스 응용프로그램)116)을 포함하는 하나 이상의 응용프로그램을 포함한다.

[0023] 계정 응용프로그램(113)은 사용자가 계정 잔액 보기, 항목 구매 및 결제 처리와 같은 다양한 계정 관련 동작을 수행할 수 있도록 한다. 처음에, 사용자는 계정 응용프로그램(113)에 액세스하기 위해 인증 자격증명을 사용하여 인증할 수 있다. 예를 들어 인증 자격증명은 사용자 이름 및 패스워드, 생체 인증 자격증명 등을 포함할 수 있다.

[0024] 인증 응용프로그램(114)은 응용프로그램과 연관된 결제를 완료하는 것을 포함하여 트랜잭션, 서비스 또는 접근성 요청에 대해 사용자가 인증을 요구할 때를 결정하도록 일반적으로 형상화 된다. 예를 들어 인증 응용프로그램(114)은 사용자가 특정 응용프로그램에 대한 액세스 및/또는 액세스 응용프로그램(116)과 같이 그와 연관된 거래 또는 결제를 완료할 것을 요구한다고 결정할 수 있다.

[0025] 액세스 응용프로그램(116)은 운송 서비스(예를 들어 대중 교통), 은행 계좌, 건강 보험 계좌, 금융 계좌와 같은 사용자 계정과 연관된 특정 서비스의 하나 이상의 기능에 대한 액세스를 허용하도록 형상화 된 응용프로그램 또는 계정 잔액, 중개 정보 또는 기타 적절한 금융 데이터가 포함된 금융 응용프로그램, 서비스 응용프로그램(소매 서비스, 배달 서비스, 엔터테인먼트 서비스, 게임 서비스 등) 및 사용자 인증이 필요할 수 있는 기타 적절한 응용프로그램 이거나 이를 포함할 수 있다.

[0026] 다양한 실시형태에서 액세스 응용프로그램(116)은 예를 들어 결제를 하거나 받기 위한 신용 또는 은행 계좌와 같은 결제 기능과 연관될 수 있으며 및/또는 인증 거래는 예를 들어 신용 카드 또는 직불 카드 활성화와 같이 인증 또는 검증을 위한 비-결제 기능을 여전히 포함할 수 있다. 다양한 실시형태에서 액세스 응용프로그램(116)은 소매 또는 상품/서비스 제공 응용프로그램이고, 액세스 응용프로그램(116)과 관련된 하나 이상의 기능은 액세스 응용프로그램(116)과 관련하여 제공되는 상품 또는 서비스와 관련하여 결제를 완료하는 것을 포함한다. 여기서 아래에서 논의되는 바와 같이 온라인 인증 프로토콜에 따라 생성된 바코드를 스캔하여 거래 또는 이와 관련된 결제를 완료할 수 있다. 다양한 실시형태에서 인증 응용프로그램(114)은 별도의 API 인터페이스 및 액세스 응용프로그램(116)에 대한 액세스를 활용하는 인증 프로토콜을 용이하게 할 수 있다.

[0027] 인증 응용프로그램(114)은 암호화 기술, EMV 표준 또는 EMV 표준을 준수하는 인증 프로토콜을 활용하는 임의의 검증 프로세스 중 하나 이상을 포함하는 임의의 적절한 프로토콜을 활용하여 사용자를 검증하도록 형상화 될 수 있다. 다양한 실시형태에서 인증 응용프로그램(114)은 사용자의 인증이 발생할 때 비접촉식 카드(101) 및 모바일 디바이스와 통신할 수 있는 발급자와 연관된 서버(120) 및 비접촉식 카드(101)와 연관된 카운터(104)를 동기화 하도록 형상화 된다.

[0028] 다양한 실시형태에서 인증 응용프로그램(114)은 서버(120) 및/또는 비접촉식 카드(101)와 협력하여 카운터(104)와 관련된 비-결제 트랜잭션에 대한 승인을 로그 할 수 있다. 로그는 서버(120)의 메모리(122) 또는 비접촉식 카드(101)의 메모리(102) 내에 위치한 카운터 로그(121)일 수 있다. 로그는 카운터(104) 및 서버(120) 또는 비접촉식 카드(101)의 총계와 무관하게 결제 트랜잭션과 비-결제 트랜잭션인 거래의 거래 집계를 별도로 보관할 수 있다. 비접촉식 카드(101)와 통신하는 서버(120) 및/또는 인증 응용프로그램(114)은 사기 방지 조치를 위해 그 안에 포함된 정보를 활용할 수 있다.

[0029] 예를 들어 인증 응용프로그램(114) 및/또는 서버(120)는 비-결제 트랜잭션과 결제 트랜잭션 사이에 또는 그 반대의 경우 비-결제 트랜잭션의 임계 수가 너무 적거나(또는 너무 많으면) 결제 트랜잭션을 거부할 수 있다. 다

양한 실시형태에서 예를 들어 비-결제 및 결제 트랜잭션 사이의 카운트와 같이 구별 정보를 포함하는 카운터 로그(121)는 온라인 검증 프로토콜 동안 다른 적절한 목적으로 사용될 수 있다.

[0030] 다양한 실시형태에서 인증 응용프로그램(114)은 계정 응용프로그램(113)과 연관된다. 예를 들어 인증 응용프로그램(114)은 계정 응용프로그램(113)과 함께 모바일 디바이스(110) 상에 설치될 수 있으며 사용자는 설치 후에 인증 응용프로그램(114)을 활성화하도록 프롬프트 된다. 보다 일반적으로 계정 응용프로그램(113)이 열릴 때마다 계정 응용프로그램(113)은 인증 응용프로그램(114)이 OS(112)에 대한 기본 인증 응용프로그램으로 활성화되어 있는지 여부를 결정할 수 있다. 인증 응용프로그램(114)이 기본 인증 응용프로그램으로서 활성화 되지 않은 경우, 계정 응용프로그램(113)은 OS(112)에 대한 기본 인증 응용프로그램으로서 인증 응용프로그램(114)을 활성화하고 및/또는 인증 응용프로그램(114)의 하나 이상의 기능을 활성화하도록 사용자에게 프롬프트 할 수 있다.

[0031] OS(112)에 대한 디폴트 인증 응용프로그램으로서 활성화되면, 인증 응용프로그램(114)은 승인 응용프로그램이 인증을 필요로 하는 때를 프로그래밍 방식으로 식별할 수 있으며 결제가 검증 또는 승인과 연관되지 않더라도 검증을 가능하게 하기 위해 결제 프로토콜을 활용할 수 있다. 다양한 실시형태에서 인증 또는 검증 프로토콜(예를 들어 온라인 검증 기술 또는 프로토콜과 연관된 적어도 하나의 동작)을 개시하기 위해, 인증 응용프로그램(114)은 인증 응용프로그램(114) 또는 그와 연관된 하나 이상의 동작을 개시하기 위해 모바일 디바이스(110)에 비접촉식 카드(101)를 탭 하도록 사용자에게 프롬프트 할 수 있다.

[0032] 일반적으로 본 발명에 개시된 다양한 실시형태에서 온라인 검증 또는 인증 프로토콜은 다음 동작 중 하나 이상을 포함할 수 있다: 인증 응용프로그램은 사용자의 신원을 검증하기 위해 트랜잭션을 개시할 수 있으며 여기서 인증 응용프로그램은 예를 들어 액세스 응용프로그램(116)과 같은 응용프로그램 전체 또는 일부를 개시할 수 있고 및/또는 비접촉식 카드(101)를 모바일 디바이스(110)와 같은 컴퓨터 디바이스 상에 탭 하도록 사용자를 프롬프트 함으로써 응용프로그램(116)의 기능에 액세스하기 위해 및/또는 그와 연관된 거래를 완료하기 위하여 스캔될 수 있는 바코드를 생성할 수 있다.

[0033] 거래는 카드 판독기(118)와 비접촉식 카드(101) 사이의 NFC 통신을 수반할 수 있으며, 여기서 비접촉식 카드(101)는 최신 버전의 응용프로그램 트랜잭션 카운터(ATC)를 포함하는 하나 이상의 입력을 모바일 디바이스(110)에 제공할 수 있다. 또한 비접촉식 카드(101) 또는 그와 관련된 임의의 적절한 컴포넌트를 포함하는 모바일 디바이스(110)는 다수의 입력을 기반으로 적절한 암호를 생성할 수 있고, 그 후 비접촉식 카드(101) 또는 그와 관련된 임의의 적절한 컴포넌트를 포함하는 모바일 디바이스(110)는 비접촉식 카드(101)의 발급자(예를 들어 발급자와 연관된 서버(120))에 암호 및 ATC를 전송한다.

[0034] 그 후 사용자는 사용자를 검증하거나 승인하는 발급자로부터 응답을 수신함으로써 검증되고 응용프로그램(116)과 연관된 하나 이상의 기능에 대한 액세스를 수신할 수 있으며, 여기서 수신된 응답은 암호 수신에 대한 응답으로 발급자 (예를 들어 서버 120)에 의해 수행된 적어도 하나의 암호화 동작에 기반한다. 예를 들어 서버(120)가 암호를 복호화 할 수 있다면, 서버는 암호가 검증되었다는 표시를 모바일 디바이스(110)에 전송할 수 있다.

[0035] 다양한 실시형태에서 일단 사용자가 검증되면 서버(120)는 모바일 디바이스(110) 및 비접촉식 카드(101) 중 어느 하나와 연관된 바코드 생성 응용프로그램(117b)에 인증 토큰을 (임의의 적절한 토큰 생성 기술을 사용하여) 전송할 수 있으며, 여기서 바코드 생성 응용프로그램(117b)은 모바일 디바이스(110) 및/또는 비접촉식 카드(101) 중 하나의 디스플레이(140, 141)가 임의의 적절한 스캐닝 디바이스에 의해 스캔 될 수 있는 바코드를 디스플레이 하게 할 수 있다.

[0036] 인증 토큰은 액세스 응용프로그램(116)과 관련된 결제 트랜잭션을 완료하는 것을 포함하여 액세스 응용프로그램(116)의 하나 이상의 기능에 대한 액세스를 허용하도록 형상화 될 수 있으며, 다양한 실시형태에서 거래와 관련된 보안을 강화하기 위해 서버(120)는 액세스 응용프로그램(116)과 연관된 단일 트랜잭션을 승인하도록 인증 토큰을 형상화 할 수 있으며, 그 후 토큰/바코드가 온라인 또는 오프라인 다른 검증없이 액세스 응용프로그램(116)과 관련된 다른 동작을 승인하지 않도록 할 수 있다.

[0037] 다양한 실시형태에서 비접촉식 카드(101)가 가상 결제 카드인 경우, 인증 응용프로그램(114)은 모바일 디바이스(110) 상에 구현된 디지털 지갑에 액세스 함으로써 비접촉식 카드(101)와 연관된 정보를 검색할 수 있으며, 여기서 디지털 지갑은 가상 결제 카드를 포함한다.

[0038] 도시된 바와 같이 서버(120)는 계정 데이터(124a) 데이터 저장소 및 메모리(122)를 더욱 포함한다. 계정 데이터(124a)는 다수의 사용자 및/또는 계정에 대한 계정 관련 데이터를 포함한다. 계정 데이터(124a)는 적어도 마스

터 키(105), 응용프로그램 트랜잭션 카운터("ATC")(104)와 같은 카운터(104), 고객 ID(107), 연관된 비접촉식 카드(101), 계정 소유자 이름, 계정 청구 주소, 하나 이상의 배송 주소, 하나 이상의 가상 카드 번호 및 각 계정에 대한 이력 정보를 포함할 수 있다. 메모리(122)는 관리 응용프로그램(123) 및 계정 데이터(124a)로부터의 하나 이상의 계정에 대한 카드 데이터(103), 카운터(104), 마스터 키(105) 및 다양화 키(106)의 인스턴스를 포함한다. 시스템은 하나 이상의 로열티 계정(124b)을 더욱 포함할 수 있다.

[0039] 시스템(100)은 데이터를 보호하기 위해 키 다양화를 구현하도록 형상화 되며, 이는 본 발명에서 키 다양화 기술로 지칭될 수 있다. 시스템(100)은 온라인 인증 프로토콜을 구현할 수 있다.

[0040] 다양한 실시형태에서 인증 응용프로그램(114)은 사용자 프로파일과 연관된 제1 응용프로그램 사용자 자격증명을 사용자로부터 수신한다. 제1 응용프로그램 사용자 자격증명은 생체 인식 데이터, 사용자 인식과 관련된 확립된 제스처, 사용자 이름 및 패스워드 조합 등을 포함할 수 있다. 프로세서(119)는 제1 응용프로그램 사용자 자격증명을 저장된 제2 응용프로그램 사용자 자격증명과 비교한다. 저장된 제2 응용프로그램 사용자 자격증명은 사용자 신원과 연관될 수 있으며 모바일 디바이스(110)의 메모리(111) 또는 서버(120)의 메모리(122) 내에 저장될 수 있다.

[0041] 다양한 실시형태에서 저장된 제2 응용프로그램 사용자 자격증명은 서버(120)에 유지되고 제1 매치는 서버(120)에 의해 수행된다. 다양한 실시형태에서 제1 응용프로그램 사용자 자격증명과 저장된 제2 응용프로그램 사용자 자격증명 사이의 제1 매치를 결정할 때, 인증 응용프로그램(114)은 액세스 응용프로그램(116)과 연관된 사용자 계정의 하나 이상의 제1 레벨 사용자 계정 옵션에 대한 액세스를 사용자에게 허용할 수 있다. 사용자 계정은 금융 계정, 건강 보험 계정 및/또는 서비스 공급자와 연관 다른 계정 예를 들어 대중 교통 계정, 엔터테인먼트 계정 등 일 수 있다.

[0042] 일단 제1 매치가 결정되면, 사용자는 바코드 생성 없이 그리고 결제의 완료와 같은 트랜잭션 완료 없이 액세스 응용프로그램(116)과 연관된 특정 제1 레벨 사용자 계정 옵션에 액세스할 수 있다. 사용자 계정의 제1 레벨 사용자 계정 옵션은 계좌 잔고 표시, 최근 거래 표시 등을 포함할 수 있다. 더 많은 액세스 및/또는 특정 계정 기능, 즉 결제 트랜잭션 실행과 같은 제2 레벨 사용자 계정 옵션을 실행하려면 온라인 인증 프로토콜을 완전히 완료하는 것, 프로토콜의 성공적인 완료에 대한 응답으로 인증 토큰을 생성하는 것, 인증 토큰을 활용하여 스캔을 위한 바코드를 생성하는 것과 같은 제2 레벨 인증이 필요할 수 있다. 여기서 스캔은 액세스 응용프로그램(116)과 연관된 트랜잭션 예를 들어 결제를 완료한다.

[0043] 일반적으로 서버(120) 또는 다른 컴퓨터 디바이스 및 비접촉식 카드(101)에는 동일한 마스터 키(105)(마스터 대칭 키라고도 함)가 제공될 수 있다. 보다 구체적으로 각각의 비접촉식 카드(101)는 서버(120)에서 대응하는 쌍을 지니는 별개의 마스터 키(105)로 프로그래밍 된다. 예를 들어 비접촉식 카드(101)가 제조될 때, 고유 마스터 키(105)는 비접촉식 카드(101)의 메모리(102) 내로 프로그래밍 될 수 있다. 유사하게 고유 마스터 키(105)는 서버(120)의 계정 데이터(124a) 내에서 비접촉식 카드(101)와 연관된 고객의 기록에 저장될 수 있다(및/또는 다른 보안 위치에 저장된다). 마스터 키는 비접촉식 카드(101) 및 서버(120) 이외의 모든 당사자로부터 비밀로 유지될 수 있으므로 시스템(100)의 보안이 강화된다.

[0044] 마스터 키(105)는 키 다양화를 사용하여 보안을 강화하기 위해 카운터(104)와 함께 사용될 수 있다. 카운터(104)는 비접촉식 카드(101)와 서버(120) 사이에서 동기화된 값을 포함할 수 있다. 카운터 값(104)은 비접촉식 카드(101)와 서버(120)(및/또는 비접촉식 카드(101) 및/또는 모바일 디바이스(110)) 사이에 데이터가 교환될 때마다 변화하는 숫자를 포함할 수 있다.

[0045] 비접촉식 카드(101)와 모바일 디바이스(110) 사이의 NFC 데이터 전송을 가능하게 하기 위해, 비접촉식 카드(101)가 모바일 디바이스(110)의 카드 판독기(118)에 충분히 가까울 때(예를 들어 NFC 범위 내) 계정 응용프로그램(113)은 비접촉식 카드(101)와 통신할 수 있다. 카드 판독기(118)는 NFC 기능을 가진 디지털 판독기, 예를 들어 NFC 판독기일 수 있으며 비접촉식 카드(101)로부터 판독 및/또는 (예를 들어 NFC, 블루투스, RFID 등을 통해) 그와 통신하도록 형상화 될 수 있다. 따라서 예시적인 카드 판독기(118)는 NFC 통신 모듈, 블루투스 통신 모듈 및/또는 RFID 통신 모듈을 포함한다.

[0046] 예를 들어 사용자는 액세스 응용프로그램(116)에 액세스하기 위해 승인 또는 검증을 요구할 수 있다. 인증 응용프로그램(114)을 포함하는 시스템(100)의 하나 이상의 컴포넌트는 액세스 응용프로그램(116) 또는 액세스 응용프로그램(116)의 사용자에 의한 액세스를 위해 추구된 특정 측면이 결제를 하는 것을 포함하거나 포함하지 않는지 사용자를 검증 또는 인증하기 위한 하나 이상의 결제 프로토콜을 활용하기 위해 액세스 응용프로그램(116)과

의 통신 예를 들어 API 호출 또는 다른 적절한 메커니즘을 개시할 수 있다.

[0047] 다양한 실시형태에서 하나 이상의 프로토콜은 본 발명의 다른 곳에서 논의된 온라인 기술을 포함할 수 있다. 인증 응용프로그램(114)은 사용자가 비접촉식 카드(101)를 모바일 디바이스(110)에 탭 할 수 있도록 프롬프트를 제공할 수 있으며, 이에 따라 비접촉식 카드(101)를 모바일 디바이스(110)의 카드 판독기(118)에 충분히 가깝게 하여 NFC 데이터 전송을 가능하게 할 수 있다. 다양한 실시형태에서 모바일 디바이스(110)는 API 호출을 통해 카드 판독기(118)를 트리거 할 수 있다. 추가적으로 및/또는 선택적으로 모바일 디바이스(110)는 카드 판독기(118)를 주기적으로 폴링 하는 것에 기반하여 카드 판독기(118)를 트리거 할 수 있다. 보다 일반적으로 모바일 디바이스(110)는 임의의 실행 가능한 방법을 사용하여 통신에 참여하도록 카드 판독기(118)를 트리거 할 수 있다.

[0048] 다양한 실시형태에서 비접촉식 카드(101), 카드 판독기(118) 및 모바일 디바이스(110)와 관련된 임의의 통신을 개시하기 전에 및/또는 비접촉식 카드(101)와 카드 판독기(118) 사이의 통신을 설정한 직후, 인증 응용프로그램(114)은 카드 활성화 및/또는 온라인 인증 프로토콜 시작을 위한 전제 조건으로서 제1 응용프로그램 사용자 자격증명을 수신할 수 있다. 사용자는 인증 응용프로그램으로부터 자격증명을 입력하라는 프롬프트를 수신한 후 제1 응용프로그램 사용자 자격증명을 제공할 수 있다.

[0049] 상기 언급한 바와 같이 제1 응용프로그램 사용자 자격증명은 생체 인식 데이터, 사용자 인식과 연관된 확립된 제스처, 사용자 이름 및 패스워드 조합, 안면 인식 등을 포함할 수 있다. 상기 언급한 바와 같이 다양한 실시형태에서 인증 응용프로그램(114)은 제1 응용프로그램 사용자 자격증명을 프로세서(119)에 전달한다. 프로세서(119)는 제1 응용프로그램 사용자 자격증명을 저장된 제2 응용프로그램 사용자 자격증명과 비교한다. 저장된 제2 응용프로그램 사용자 자격증명은 모바일 디바이스(110)와 연관된 메모리(111), 비접촉식 카드(101)와 연관된 메모리(102) 및/또는 서버(120)와 연관된 메모리(122) 내에 위치될 수 있다.

[0050] 다양한 실시형태에서 제1 응용프로그램 사용자 자격증명이 서버(120)에 제공되고, 서버(120)는 제1 응용프로그램 사용자 자격증명을 저장된 제2 응용프로그램 사용자 자격증명과 비교한다. 다양한 실시형태에서 상기 언급된 바와 같이 프로세서(119)는 비교 결과를 예를 들어 매치를 위해 인증 응용프로그램(114)에 전달한다.

[0051] 다양한 실시형태에서 제1 매치는 ⅰ) 액세스 응용프로그램(116)에 액세스하기 위해 사용자를 검증 또는 인증하기 위한 온라인 검증 프로토콜의 나머지의 개시 및/또는 ii) 액세스 응용프로그램(116)과 연관된 사용자 계정의 제1 레벨 사용자 계정 옵션 예를 들어 계정 잔고 및/또는 최근 거래의 표시에 대한 사용자 액세스 허용; 및/또는 iii) 액세스 응용프로그램(116)과 연관된 하나 이상의 기능에 액세스 하기 위해 및/또는 예를 들어 결제 트랜잭션과 같이 그와 연관된 거래를 완료하기 위해 스캔될 수 있는 바코드의 생성을 위해 바코드 생성 응용프로그램(117b)에 제공되는 인증 토큰의 생성; 중 하나 이상을 개시하거나 이에 대한 전제조건으로서 기능할 수 있다.

[0052] 이와 같이 다양한 실시형태에서 검증 인증 응용프로그램은 제1 매치를 찾는 것에 응답하여 사용자 신원을 검증하기 위해 온라인 검증 프로세스와 연관된 추가 동작을 개시한다.

[0053] 다양한 실시형태에서 시스템(100)은 바코드 생성 응용프로그램(117b)과 연관되어 생성된 바코드를 활용하거나 활용하지 않을 수 있는 온라인 검증 프로토콜에 기반하여 액세스 응용프로그램(116) 및/또는 소매업자(148)와 연관된 로열티 포인트를 활용하는 로열티 포인트 응용프로그램(117a)을 포함한다. 로열티 포인트 응용프로그램(117a)은 로열티 포인트 잔액 보기, 제품, 상품 및/또는 서비스에 대한 로열티 포인트 상환, 다른 계정으로 로열티 포인트 이전과 같은 로열티 포인트에 관련한 임의의 수 및 임의의 유형의 동작을 사용자가 수행하게 할 수 있다.

[0054] 사용자가 로열티 포인트 응용프로그램(117a)에서 동작을 수행하도록 요청할 때 사용자는 비접촉식 카드(101)를 사용하여 자신의 신원을 검증해야 할 수 있다. 본 발명에 더욱 자세히 설명된 바와 같이 요청된 동작은 비접촉식 카드(101)에 의해 생성된 암호화된 데이터를 검증하는 서버(120), 응용프로그램 사용자 자격증명의 매치 및/또는 바코드 생성 응용프로그램(117b)에 의해 생성된 바코드 사용에 기반하여 승인될 수 있다.

[0055] 다양한 실시형태에서 저장된 제2 응용프로그램 사용자 자격증명에 대한 제1 응용프로그램 사용자 자격증명의 제1 매치는 예를 들어 액세스 응용프로그램(116)과 같은 응용프로그램에 대한 제1 레벨 액세스를 허용할 수도 있고 허용하지 않을 수도 있다. 그러나 제1 매치는 어떠한 경우에도 온라인 인증 프로토콜 중 적어도 하나를 개시하기 위한 전제 조건으로 작용할 수 있다. 제1 레벨 액세스가 초기에 허용되지 않은 다양한 실시형태에서 적어도 하나의 온라인 및/또는 오프라인 프로토콜의 성공적인 완료는 제1 레벨 액세스를 허용하는 결과를 낳는다.

[0056] 다양한 실시형태에서 액세스 응용프로그램(116)에 대한 제2 레벨 액세스는 온라인 및/또는 오프라인 검증 프로

토콜 중 적어도 하나의 완료 및 이러한 프로토콜 중 하나의 완료의 결과로 생성된 바코드의 스캔 즉시 허용되며, 여기서 제2 레벨 액세스는 액세스 응용프로그램(116)과 관련하여 결제 트랜잭션을 완료하는 것을 의미할 수 있다.

[0057] 다양한 실시형태에서 임의의 다른 전제조건과 무관하게, 비접촉식 카드(101)의 모바일 디바이스(110) 상의 제1 탭은 온라인 및 오프라인 검증 프로토콜을 개시하고, 제2 탭인 후속 탭은 온라인 및 오프라인 검증 프로토콜 중 다른 하나를 개시한다.

[0058] 다양한 실시형태에서 하나 이상의 전제조건이 적용되거나 발생하는지에 상관없이, 모바일 디바이스(110)와 비접촉식 카드(101) 사이에 통신이 설정된 후, 비접촉식 카드(101)는 메시지 인증 코드(MAC) 암호를 생성한다. 다양한 실시형태에서 이것은 비접촉식 카드(101)가 계정 응용프로그램(113)에 의해 판독될 때 발생할 수 있다. 특히 이것은 근거리 데이터 교환(NDEF) 태그의 NFC 판독과 같은 판독 시에 발생할 수 있으며, 이는 NFC 데이터 교환 형식에 따라 생성될 수 있다. 예를 들어 계정 응용프로그램(113) 및/또는 카드 판독기(118)와 같은 판독기는 NDEF 생성 애플릿의 애플릿 ID와 함께 애플릿 선택 메시지와 같은 메시지를 전송할 수 있다. 다양한 실시형태에서 생성된 암호는 EMV 표준과 일치하는 인증 요청 암호(ARQC)일 수 있다.

[0059] 다양한 실시형태에서 선택의 확인 시에 파일 읽기 메시지가 뒤따르는 파일 선택 메시지의 시퀀스가 전송될 수 있다. 예를 들어 시퀀스는 "기능 파일 선택", "기능 파일 읽기" 및 "NDEF 파일 선택"을 포함할 수 있다. 이러한 시점에서 비접촉식 카드(101)에 의해 유지되는 카운터 값(104)은 업데이트되거나 증가될 수 있고, "NDEF 파일 읽기"가 뒤따를 수 있다. 이때 헤더와 공유 비밀을 포함할 수 있는 메시지가 생성될 수 있다. 그 후 세션 키가 생성될 수 있다. MAC 암호는 헤더와 공유 비밀을 포함할 수 있는 메시지로부터 생성될 수 있다. 그 후 MAC 암호는 랜덤 데이터의 하나 이상의 블록과 연결될 수 있고 MAC 암호 및 난수(RND)는 세션 키로 암호화될 수 있다.

[0060] 그 후 암호문과 헤더는 연결되어 ASCII 16진수로 인코딩되고 "NDEF 파일 읽기" 메시지에 대해 응답하여 NDEF 메시지 형식으로 반환될 수 있다. 다양한 실시형태에서 MAC 암호는 NDEF 태그로서 전송될 수 있으며 다른 실시들에서 MAC 암호는 (예를 들어 포맷된 문자열로서 균일 자원 표시자와 함께 포함될 수 있다. 그 후 비접촉식 카드(101)는 MAC 암호를 모바일 디바이스(110)에 전송할 수 있으며 모바일 디바이스는 아래에서 설명되는 바와 같이 검증을 위해 서버(120)로 MAC 암호를 전달할 수 있다. 그러나 다양한 실시형태에서 모바일 디바이스(110)는 MAC 암호를 검증할 수 있다.

[0061] 보다 일반적으로 예를 들어 서버(120) 및/또는 모바일 디바이스(110)로 데이터를 전송할 준비를 할 때, 비접촉식 카드(101)는 카운터 값(104)을 증가시킬 수 있다. 그 후 비접촉식 카드(101)는 출력으로 다양화 키(106)를 생성하는 암호화 알고리즘에 대한 입력으로 마스터 키(105) 및 카운터 값(104)을 제공할 수 있다. 암호화 알고리즘은 암호화 알고리즘, 해시 기반 메시지 인증 코드(HMAC) 알고리즘, 암호 기반 메시지 인증 코드(CMAC) 알고리즘 등을 포함할 수 있다. 암호화 알고리즘의 비제한적인 실시예는 3DES 또는 AES128과 같은 대칭 암호화 알고리즘; HMAC-SHA-256과 같은 대칭 HMAC 알고리즘; AES-CMAC와 같은 대칭 CMAC 알고리즘; 및/또는 ISO/IEC 1833 및/또는 ISO/IEC 7816의 적용 가능한 버전과 일치하는 기타 알고리즘 또는 기술을 포함할 수 있다.

[0062] 그 다음, 비접촉식 카드(101)는 다양화 키(106)를 사용하여 예를 들어 고객 식별자(107) 및 임의의 다른 데이터와 같은 데이터를 암호화할 수 있다. 그 후 비접촉식 카드(101)는 예를 들어 암호화된 고객 ID(109)와 같은 암호화된 데이터를 예를 들어 NFC 연결, 블루투스 연결 등을 통해 모바일 디바이스(110)의 계정 응용프로그램(113)에 전송할 수 있다.

[0063] 모바일 디바이스(110)의 계정 응용프로그램(113)은 암호화된 데이터를 네트워크(130)를 통해 서버(120)로 전송할 수 있다. 적어도 다양한 실시형태에서 비접촉식 카드(101)는 암호화된 데이터와 함께 카운터 값(104)을 전송한다. 이러한 실시형태에서 비접촉식 카드(101)는 암호화된 카운터 값(104) 또는 암호화되지 않은 카운터 값(104)을 전송할 수 있다.

[0064] 암호화된 고객 ID(109)를 수신하면 서버(120)의 관리 응용프로그램(123)은 암호화에 대한 입력으로 카운터 값(104) 및 암호화를 위한 키로 마스터 키(105)를 사용하여 동일한 대칭 암호화를 수행할 수 있다. 언급된 바와 같이 카운터 값(104)은 모바일 디바이스(110)로부터 수신된 데이터 또는 비접촉식 카드(101)에 대한 키 다양화를 구현하기 위해 서버(120)에 의해 유지되는 카운터 값(104)에 명시될 수 있다. 암호화의 출력은 비접촉식 카드(101)에 의해 생성된 다양화 키 값(106)과 동일할 수 있다.

[0065] 그 후 관리 응용프로그램(123)은 비접촉식 카드(101)에 의해 전송된 데이터 예를 들어 적어도 고객 식별자(107)를 나타내는 다양화 키(106)를 사용하여 네트워크(130)를 통해 수신된 암호화된 고객 ID(109)를 복호화 할 수

있다. 이를 통해 예를 들어 계정에 대한 계정 데이터(124a) 내의 고객 ID와 복호화된 고객 ID(107)를 비교함으로써 관리 응용프로그램(123)이 모바일 디바이스(110)를 통해 비접촉식 카드(101)에 의해 전송된 데이터를 검증하게 한다. 일단 검증되면 관리 응용프로그램(123)은 성공적인 검증의 표시를 모바일 디바이스(110)에 전송할 수 있다.

[0066] 카운터(104) 예를 들어 ATC가 실시예로서 사용되었으나 비접촉식 카드(101), 모바일 디바이스(110) 및/또는 서버(120) 사이의 통신을 보안하기 위해 다른 데이터가 사용될 수 있다. 예를 들어 카운터(104)는 새로운 다양화 키(106)가 필요한 때마다 생성되는 랜덤 넌스, 비접촉식 카드(101) 및 서버(120)로부터 전송된 카운터 값의 전체 값, 비접촉식 카드(101) 및 서버(120)로부터 전송된 카운터 값의 일부, 비접촉식 카드(101)와 서버(120)에 의해 독립적으로 유지되지만 둘 사이에 전송되지 않는 카운터, 비접촉식 카드(101)와 서버(120) 간에 교환되는 일회용 패스코드 및 데이터의 암호화 해시로 대체될 수 있다. 다양한 실시형태에서 다양화 키(106)의 하나 이상의 부분은 다수의 다양화 키(106)를 생성하기 위해 당사자에 의해 사용될 수 있다.

[0067] 도시된 바와 같이 서버(120)는 하나 이상의 하드웨어 보안 모듈(HSM)(125)을 포함할 수 있다. 예를 들어 하나 이상의 HSM(125)은 본 발명에 개시된 바와 같이 하나 이상의 암호화 동작을 수행하도록 형상화 될 수 있다. 다양한 실시형태에서 하나 이상의 HSM(125)은 하나 이상의 암호화 동작을 수행하도록 형상화 되는 특수 목적 보안 디바이스로서 형상화 될 수 있다. HSM(125)은 키가 HSM(125) 외부에서 노출되지 않고 대신 HSM(125) 내에서 유지되도록 형상화 될 수 있다. 예를 들어 하나 이상의 HSM(125)은 키 유도, 복호화 및 MAC 동작 중 적어도 하나를 수행하도록 형상화 될 수 있다. 하나 이상의 HSM(125)은 서버(120) 내에 포함될 수 있거나 서버(120)와 데이터 통신할 수 있다.

[0068] 언급된 바와 같이 키 다양화 기술은 비접촉식 카드(101)를 사용하여 보안 동작을 수행하는 데 사용될 수 있다. 예를 들어 관리 응용프로그램(123)이 키 다양화를 사용하여 암호화된 고객 ID(109)를 검증하면, 관리 응용프로그램(123)은 인증 응용프로그램(114) 또는 계정 응용프로그램(113), 포인트 응용프로그램(117A), 액세스 응용프로그램(116) 등과 같은 디바이스(110)의 임의의 다른 컴포넌트에 메시지를 전송할 수 있다. 이는 사용자가 검증 및/또는 인증되었음을 표시하고, 인증 응용프로그램(114)은 결과적으로 액세스 응용프로그램(116)에 대한 사용자 액세스를 허가할 수 있다.

[0069] 다양한 실시형태에서 전송된 출력은 승인 응답 암호(ARPC)를 포함할 수 있다. 일반적으로, 암호화된 고객 ID(109)의 확인에 기반하여 사용자가 확인 및/또는 인증되었음을 나타내는 메시지를 수신하면, 모바일 디바이스(110)의 수신 컴포넌트는 임의의 수의 동작을 허가할 수 있다. 예를 들어 포인트 응용프로그램(117A)은, 예를 들어 로열티 포인트를 보고, 로열티 포인트를 상환하는 등의 로열티 계정에 대한 액세스를 허가할 수 있다.

[0070] 상기 논의를 포함하여 본 발명에 개시된 하나 이상의 실시형태에 고유한 바와 같이 서버(120)는 온라인 인증 또는 검증에 사용될 수 있으며 비-결제 목적을 위해 EMV 결제 프로토콜을 활용하는 동작을 수행하는 것을 포함하여 EMV 표준과 일치하게 동작하도록 형상화 될 수 있다. 호스트 서버(또는 시스템)(120)는 사용자와 연관된 카드의 발급자와 연관될 수 있고, 호스트 시스템은 프로세서에 의해 실행가능한 컴퓨터 판독가능 프로그램 코드를 저장하는 비일시적 컴퓨터 판독가능 저장 매체를 포함하고, 여기서 프로세서 및 저장 매체는 도 8에 일반적으로 설명된 것을 포함하여 하나 이상의 하드웨어 또는 소프트웨어 컴포넌트를 포함할 수 있다.

[0071] 호스트 시스템은 액세스 응용프로그램(116) 및/또는 비접촉식 카드(101)와 관련된 거래 데이터를 수신하도록 형상화 될 수 있다. 트랜잭션 데이터의 수신은 예를 들어 모바일 디바이스(110) 및 사용자(또는 다른 적절한 컴퓨터 디바이스)와 연관된 인증 응용프로그램(114)(또는 모바일 디바이스(110)의 다른 적절한 컴포넌트 또는 응용프로그램)에 의해 본 발명에 개시된 바와 같이 용이하게 될 수 있다. 여기서 인증 응용프로그램(114)은 하나 이상의 다른 컴포넌트 예를 들어 비접촉식 카드(101) 및 카드 판독기(118)와 인증 또는 검증 트랜잭션을 개시할 수 있다.

[0072] 트랜잭션 데이터는 인증 응용프로그램(114)으로부터 서버(120)에 의해 수신된다. 트랜잭션 데이터는 ⅰ) 카운터(예를 들어 ATC) 및 트랜잭션의 하나 이상의 입력 및 카드와 연관된 대칭 키에 기반한 암호를 포함할 수 있다. 다양한 실시형태에서 암호는 승인 요청 암호(ARQC)이다.

[0073] 다양한 실시형태에서 일단 서버(120)가 거래 데이터를 수신하면, 관리 응용프로그램(123)은 예를 들어 인증 응용프로그램(114), 계정 응용프로그램(113), 포인트 응용프로그램(117a) 등과 같은 모바일 디바이스(110)의 적절한 컴포넌트에 수신된 암호에 기반하여 사용자의 신원을 검증하는 응답을 예를 들어 발급자로부터 전송할 수 있다. 검증 응답의 수신에 응답하여 인증 응용프로그램(114)은 결과로서 액세스 응용프로그램(116)의 관련 부분

또는 특징에 대한 액세스를 허용할 수 있고 및/또는 액세스 응용프로그램(116)과 연관된 거래를 완료하는 데 유용한 바코드의 생성을 용이하게 할 수 있다.

[0074] 다양한 실시형태에서 응답은 비접촉식 카드(101) 및/또는 모바일 디바이스(110)와 연관된 바코드 생성 응용프로그램(117b)에 제공된 인증 토큰을 포함할 수 있으며, 이는 바코드 생성 응용프로그램(117b)에 의해 사용되어 디스플레이(140) 및/또는 디스플레이(141) 상에 바코드를 표시할 수 있다. 여기서 바코드는 예를 들어 결제 트랜잭션과 같은 액세스 응용프로그램(116)과 연관된 거래를 완료하기 위해 및/또는 액세스 응용프로그램(116)과 연관된 기능에 대한 액세스를 제공하기 위해 인증 토큰을 복호화 할 수 있는 적절한 스캐닝 디바이스에 의해 스캔될 수 있다.

[0075] 또한 액세스 응용프로그램(116)은 모바일 디바이스(110) 상의 다른 응용프로그램, 예를 들어 계정 응용프로그램(113) 및/또는 포인트 응용프로그램(117a)의 관련 부분 또는 특징에 대한 액세스를 허가할 수 있다. 유사하게 계정 응용프로그램(113) 및/또는 포인트 응용프로그램(117a)은 검증 응답을 수신하여 포인트 응용프로그램(117a)의 로열티 포인트 계정에 액세스하고, 로열티 포인트를 사용하여 트랜잭션을 승인하는 것과 같은 응용프로그램의 관련 부분 또는 기능에 대한 액세스를 허가할 수 있다.

[0076] 다양한 실시형태에서 관리 컴포넌트(123)는 바코드의 단일 스캔이 발생하면 비활성화되도록 인증 토큰을 형상화할 수 있으며, 여기서 스캔은 액세스 응용프로그램(116)과 연관된 기능에 대한 액세스를 허용하고 및/또는 이와 연관된 트랜잭션을 완료한다. 이는 차례로 액세스 응용프로그램(116)의 측면에 액세스하기 위한 바코드의 무단 후속 사용을 금지할 수 있다. 다양한 실시형태에서 생성된 바코드는 인증 프로토콜이 발생했다면 사용자가 어떤 선택을 하기로 결정했는지에 따라 예를 들어 다중 액세스 응용프로그램(116)과 같은 하나 이상의 응용프로그램에 사용될 수 있다.

[0077] 다양한 실시형태에서 관리 응용프로그램(123)은 전체 트랜잭션 데이터의 일부로서 사용자 또는 인증 응용프로그램(114)으로부터 명령을 수신하여 액세스 응용프로그램(116)과 연관된 트랜잭션에 제한을 둘 수 있다. 예를 들어 결제 트랜잭션 에 대한 금전적 제한이며 여기서 관리 응용프로그램(123)은 제한을 구현하기 위해 승인 토큰(및 확장하여 후속하여 생성된 바코드)을 형상화 한다. 다양한 실시형태에서 승인 토큰은 지출될 수 있는 금액에 대해 미리 규정된 사용자 제한이 있거나 없는 액세스 응용프로그램(116)과 관련하여 결제 트랜잭션을 승인하는 결제 토큰일 수 있다.

[0078] 따라서, 다양한 실시형태에서 본 발명에 개략된 바와 같이 생성된 바코드는 모바일 디바이스(110) 및/또는 비접촉식 카드(101)의 표면 중 하나에 디스플레이되는 동적 바코드일 수 있으며, 다음 특징 중 적어도 하나를 지닌다:

[0079] ⅰ) 바코드는 1회 사용 후 비활성화되도록 형상화 될 수 있다.

[0080] ⅱ) 바코드는 단일 또는 다중 사용 사례를 포함하여 하나 이상의 액세스 응용프로그램(116)에 활용될 수 있다(인증 토큰과 연관된 인증 프로토콜이 발생하는 경우). 예를 들어 단일 사용 사례에서 바코드가 생성되고 스캔이 발생하기 전이라면 인증 응용프로그램(114)은 사용자가 다른 액세스 응용프로그램(116)에 액세스하고 다시 실행할 프로토콜 없이 바코드를 활용하도록 허가할 수 있다. 예를 들어 바코드 생성 후 후속 트랜잭션이 발생하지 않았음을 보장하기 위해 인증 응용프로그램(114)에 의해 카운터 로그(121)가 활용될 수 있으며, 이는 사용자가 바코드의 사용을 다른 액세스 응용프로그램(116)으로 전환하고 및/또는 원래 선택된 것과 별개로 원래 선택된 액세스 응용프로그램(116)의 다른 기능에 액세스하는 것을 차례로 허가할 수 있다;

[0081] ⅲ) 바코드는 검증 프로토콜이 발생하면 다중 스캔 및 상이한 액세스 응용프로그램(116)에 대해 활성 상태를 유지하도록 형상화 될 수 있다. 및/또는

[0082] ⅳ) 승인 토큰(그리고 확장하여 바코드)은 액세스 응용프로그램(116)과 연관된 트랜잭션과 관련하여 예를 들어 액세스 응용프로그램(116)과 관련하여 완료될 결제 트랜잭션에 금전적 제한을 두는 것과 같이 (사용자에 의해 또는 다른 방식으로) 미리 규정된 제한과 연관되도록 형상화 될 수 있다.

[0083] 다양한 실시형태에서 현재 단락에서 개시된 특징은 상기 개시된 온라인 프로토콜과 관련하여 생성된 바코드뿐만 아니라 본 발명에 개시된 임의의 다른 프로토콜과 관련하여 적용된다는 점에 유의한다.

[0084] 다양한 실시형태에서 서버(120)는 사기 방지 조치를 수행하기 위해 카운터 로그(121)를 활용할 수 있다. 다양한 실시형태에서 카운터 로그(121)는 하나 이상의 비-결제 트랜잭션과 연관된 카운터 값과 연관된 타임 스탬프를 포함할 수 있다. 다양한 실시형태에서 카운터 로그(121)는 하나 이상의 결제 트랜잭션과 연관된 카운터 값과 연

관된 타임스탬프를 포함할 수 있다.

[0085] 다양한 실시형태에서 특정 트랜잭션과 관련된 ATC의 카운터 값, 예를 들어 결제 트랜잭션인지 비-결제 트랜잭션인지 여부 또한 로그 될 수 있다. 관리 응용프로그램(123)은 비-결제 트랜잭션 사이에서 발생하는 결제 트랜잭션의 일반적인 수를 비교하도록 형상화 될 수 있다. 비-결제 트랜잭션 후의 결제 트랜잭션 수가 특정 임계 값을 초과하면 관리 응용프로그램(123)은 결제 트랜잭션을 거부할 수 있다. 그렇지 않으면 거래가 완료될 수 있다. 예를 들어 사용자가 비-결제 및 결제 프로토콜에 대해 결제 프로토콜을 사용할 수 있다고 가정하기 때문에 비-결제 트랜잭션 이후 과도하게 많은 수의 결제 트랜잭션은 사기로 간주될 수 있다.

[0086] 다양한 실시형태에서 그 반대가 구현될 수 있다. 임계 값을 초과하는 결제 트랜잭션 후에 수행되는 다수의 비-결제 트랜잭션은 검증 또는 인증이 발생할 때 관리 응용프로그램(123)이 특정 비-결제 트랜잭션을 거부하도록 할 수 있다. 다양한 실시형태에서 최소 또는 최대 임계 값을 초과하는 관점에서 예를 들어 결제 또는 비-결제와 같은 임의의 트랜잭션 사이의 시간과 관련된 임계 값은 관리 응용프로그램(123)이 인증 또는 검증 동작을 거부하게 할 수 있다. 임의의 다른 적절한 방식으로 사기 방지 조치를 수행하는 것을 포함하여 임의의 다른 적절한 동작을 수행하는 데 카운터 로그(121)가 사용될 수 있다.

[0087] 다양한 실시형태에서 사기 방지 조치는 바코드와 연관된 인증 토큰이 유효한 경우에도 응용프로그램을 거부하도록 모바일 디바이스의 적절한 컴포넌트, 예를 들어 인증 응용프로그램(114)에 지시함으로써 유효한 인증 토큰을 무시할 수 있다.

[0088] 도 2는 기능 액세스 및/또는 액세스 응용프로그램(116)과 관련된 트랜잭션 완료를 위한 바코드를 생성하기 위해 온라인 검증 및/또는 인증 프로토콜을 개시하기 위해 탭 하는 예시적인 실시형태를 도시하는 개략도(200)이다. 모바일 디바이스(110) 상의 승인 응용프로그램(114)의 그래픽 사용자 인터페이스(GUi)는 액세스 응용프로그램(116)과 같은 다른 응용프로그램에 대한 인증 또는 검증을 개시하도록 비접촉식 카드를 탭 하라는 프롬프트(206)를 포함할 수 있다. 여기서 (완료되면) 인증 응용프로그램(114)에 의해 액세스 응용프로그램(116)으로 검증 또는 인증을 전달하기 위해 별도의 API 인터페이스가 제공될 수 있다.

[0089] 다양한 실시형태에서 액세스 응용프로그램(116)은 탭 프롬프트(206)를 수신하기 위한 전제조건으로서 또는 탭이 발생한 후 임의의 추가적인 온라인 검증 동작 이전에, 비교를 위해 사용자 자격증명을 입력하기 위한 프롬프트(202)를 제공한다. 예를 들어 도 1을 참고하여 개시된 것과 같음. 이는 액세스 응용프로그램(116)에 관련된 제1 레벨 및/또는 제2 레벨 정보 액세스에 대한 것이다. 다양한 실시형태에서 인증 응용프로그램(114)은 액세스 응용프로그램(116) 및 /또는 예를 들어 다른 응용프로그램(116)과 같은 다른 응용프로그램과 관련하여 사용자 자격증명을 입력하기 위한 프롬프트(202)에 대한 인터페이스를 제공한다.

[0090] 다양한 실시형태에서 비접촉식 카드(101)가 모바일 디바이스(110)에 탭 되면 인증 응용프로그램(114)은 카드 판독기(118)를 통해(예를 들어 NFC, 블루투스, RFID 등을 통해) 표시를 비접촉식 카드(101)에 전송한다. 다양한 실시형태에서 표시는 도 1과 관련하여 개시된 바와 같이 하나 이상의 암호화 기술을 수행하도록 명시할 수 있다. 다양한 실시형태에서 온라인 인증 기술이 사용되며 인증 응용프로그램(114)은 서버(120)로부터 트랜잭션 데이터를 수신한다.

[0091] 다양한 실시형태에서 비접촉식 카드(101)와 모바일 디바이스(110) 사이에서 데이터를 전송하라는 프롬프트는 EMV 프로토콜 또는 표준과 일치하는 임의의 적절한 프로토콜을 통해 인증 응용프로그램(114)에 데이터를 전송하도록 명시할 수 있으며, 여기서 다양한 실시형태에서 인증 응용프로그램(114)은 EMV 프로토콜 또는 표준과 일치하는 프로토콜을 통해 비접촉식 카드(101)로부터 임의의 적절한 데이터를 직접 수신한다.

[0092] 도 3은 (바코드를 생성하기 위해) 온라인 검증 및/또는 인증 프로토콜을 개시하기 위한 탭 이후, 예를 들어 기능 액세스 및/또는 액세스 응용프로그램(116)과 관련된 트랜잭션 완료를 위한 탭이 발생한 후, 생성된 바코드의 예시적인 실시형태를 도시하는 개략도(300)이다. 다양한 실시형태에서 임의의 적절한 스캐닝 디바이스에 의한 스캐닝에 적합한 바코드(307)가 모바일 디바이스의 디스플레이 상에 생성된다.

[0093] 다양한 실시형태에서 서버의 관리 응용프로그램(123) 및/또는 모바일 디바이스(110)의 인증 응용프로그램(114)은 모바일 디바이스(110)(도 3에 도시됨) 및/또는 비접촉식 카드(101)와 연관된 바코드 생성 응용프로그램(117b)에 인증 토큰을 제공할 수 있다. 또한 바코드 생성 응용프로그램(117b)는 액세스 응용프로그램(116)의 하나 이상의 기능에 대한 액세스를 허용하기 위한(및/또는 그와 관련된 트랜잭션을 완료하기 위한) 단일 사용 바코드(307) 및/또는 액세스 응용프로그램(116)의 하나 이상의 기능에 대한 액세스를 허용하기 위한(및/또는 그와 관련된 트랜잭션을 완료하기 위한) 반복 사용 바코드를 생성하기 위해 인증 토큰을 사용할 수 있다.

[0094] 다른 예로서 바코드(307)는 포인트 응용프로그램(117a)의 로열티 계정에 대한 액세스를 승인하고 및/또는 포인트 응용프로그램(117a)의 로열티 계정과 연관된 동작을 수행하는 데 사용될 수 있다.

[0095] 도 4a는 신용 카드, 직불 카드 및/또는 기프트 카드와 같은 결제 카드를 포함할 수 있는 비접촉식 카드(101)를 도시한다. 도시된 바와 같이 비접촉식 카드(101)는 카드(101)의 전면 또는 후면에 표시된 서비스 공급자(405)에 의해 발행될 수 있다. 다양한 실시형태에서 비접촉식 카드(101)는 결제 카드와 관련이 없으며 신분증을 제한 없이 포함할 수 있다. 다양한 실시형태에서 결제 카드는 이중 인터페이스 비접촉식 결제 카드를 포함할 수 있다. 비접촉식 카드(101)는 기판(410)을 포함할 수 있으며, 기판(410)은 단일 층, 또는 플라스틱, 금속 및 기타 재료로 구성된 하나 이상의 적층된 층을 포함할 수 있다.

[0096] 예시적인 기판 재료는 폴리염화비닐, 폴리염화비닐 아세테이트, 아크릴로니트릴 부타디엔 스티렌, 폴리카보네이트, 폴리에스테르, 양극성 산화된 티타늄, 팔라듐, 금, 탄소, 종이 및 생분해성 재료를 포함한다. 다양한 실시형태에서 비접촉식 카드(101)는 ISO/IEC 7810 표준의 ID-1 형식을 준수하는 물리적 특성을 지닐 수 있고 그렇지 않으면 비접촉식 카드는 ISO/IEC 14443 표준을 준수할 수 있다. 그러나 본 발명에 따른 비접촉식 카드(101)는 상이한 특성을 지닐 수 있으며 본 발명은 비접촉식 카드가 결제 카드 내에서 구현될 필요가 없는 것으로 이해된다.

[0097] 또한 비접촉식 카드(101)는 카드의 전면 및/또는 후면에 표시된 식별 정보(415) 및 접촉 패드(420)를 포함할 수 있다. 접촉 패드(420)는 모바일 디바이스(110), 사용자 디바이스, 스마트폰, 랩톱, 데스크톱 또는 태블릿 컴퓨터와 같은 다른 통신 디바이스와 접촉을 설정하도록 형상화 될 수 있다. 또한 비접촉식 카드(101)는 처리 회로, 안테나 및 도 4a에 도시되지 않은 다른 컴포넌트를 포함할 수 있다. 이러한 컴포넌트는 접촉 패드(420) 후면에 또는 기판(410)의 다른 곳에 위치할 수 있다. 또한 비접촉식 카드(101)는 카드의 후면에 위치될 수 있는 자기 스트립 또는 테이프를 포함할 수 있다(도 4a에 도시되지 않음).

[0098] 비접촉식 카드(101)는 도 1 내지 도 3 및 도 5 내지 도7b를 참조하여 개시된 바와 같이 생성될 수 있는 바코드(417)를 표시할 수 있는 디스플레이 인터페이스(416)를 포함할 수 있다. 여기서 응용프로그램의 기능에 대한 액세스를 허용하기 위해 및/또는 결제 트랜잭션과 같은 응용프로그램과 연관된 트랜잭션의 완료를 촉진하기 위해 바코드(417)가 임의의 적절한 스캐닝 디바이스에 의해 스캔 및 복호화 될 수 있다.

[0099] 도 4b에 도시된 바와 같이 비접촉식 카드(101)의 접촉 패드(420)는 마이크로프로세서(430) 및 메모리(102)를 포함하여 정보를 저장 및 처리하기 위한 처리 회로(425)를 포함할 수 있다. 처리 회로(425)는 본 발명에 개시된 기능을 수행하기 위해 필요한 프로세서, 메모리, 오류 및 패리티/CRC 검사기, 데이터 인코더, 충돌 방지 알고리즘, 컨트롤러, 명령 디코더, 보안 프리미티브 및 변조 방지 하드웨어를 포함하는 추가 컴포넌트를 포함할 수 있다.

[0100] 메모리(102)는 읽기 전용 메모리, 1회 쓰기 다회 읽기 메모리 또는 읽기/쓰기 메모리, 예를 들어 RAM, ROM 및 EEPROM일 수 있으며 비접촉식 카드(101)는 이들 메모리 중 하나 이상을 포함할 수 있다. 읽기 전용 메모리는 공장에서 읽기 전용 또는 1회 프로그래밍 가능으로 프로그래밍 될 수 있다. 일회성 프로그래밍 기능은 한 번 쓰고 여러 번 읽을 수 있는 기회를 제공한다. 1회 쓰기/다회 읽기 메모리는 메모리 칩이 공장에서 출고된 후 특정 시점에 프로그래밍 될 수 있다. 메모리는 한 번 프로그래밍 되면 다시 쓸 수 없지만 여러 번 읽을 수 있다. 읽기/쓰기 메모리는 출고 후 여러 번 프로그래밍 및 재프로그래밍 될 수 있다. 읽기/쓰기 메모리는 출고 후 여러 번 읽을 수도 있다.

[0101] 메모리(102)는 하나 이상의 애플릿(440), 하나 이상의 카운터(104), 고객 식별자(107) 및 가상 계좌 번호(108)를 저장하도록 형상화 될 수 있다. 하나 이상의 애플릿(440)은 Java® 카드 애플릿과 같이 하나 이상의 비접촉식 카드에서 실행하도록 형상화 된 하나 이상의 소프트웨어 응용프로그램을 포함할 수 있다. 그러나 애플릿(440)은 자바 카드 애플릿으로 제한되지 않으며 대신 비접촉식 카드 또는 제한된 메모리를 지니는 다른 디바이스 상에서 작동 가능한 임의의 소프트웨어 응용프로그램일 수 있는 것으로 이해된다.

[0102] 하나 이상의 카운터(104)는 정수를 저장하기에 충분한 숫자 카운터를 포함할 수 있다. 고객 식별자(107)는 비접촉식 카드(101)의 사용자에게 할당된 고유한 영숫자 식별자를 포함할 수 있고, 식별자는 비접촉식 카드의 사용자를 다른 비접촉식 카드 사용자와 구별할 수 있다. 다양한 실시형태에서 고객 식별자(107)는 고객과 그 고객에게 할당된 계정 모두를 식별할 수 있고 고객의 계정과 연관된 비접촉식 카드를 추가로 식별할 수 있다.

[0103] 언급된 바와 같이 계좌 번호(108)는 비접촉식 카드(101)와 연관된 수천 개의 일회용 가상 계좌 번호를 포함할 수 있다. 비접촉식 카드(101)의 애플릿(440)은 계좌 번호(108)를 관리하도록 형상화 될 수 있다. 메모리(102)는

예를 들어 도 4a에 나타난 바와 같은 바코드(417)를 생성할 수 있는 바코드 생성 응용프로그램(117b)를 포함하도록 형상화 될 수 있다. 바코드는 임의의 적절한 스캐닝 디바이스에 의해 및 본 발명에 개시된 임의의 적절한 목적을 위해 스캔 및 복호화될 수 있다.

[0104] 전술한 실시형태의 프로세서 및 메모리 엘레멘트는 접촉 패드를 참조하여 설명되었으나 본 발명은 이에 제한되지 않는다. 이들 엘레멘트는 패드(420) 외부에 구현되거나 패드로부터 완전히 분리될 수 있거나 접촉 패드(420) 내에 위치된 프로세서(430) 및 메모리(102) 엘레멘트에 더하여 추가 엘레멘트 로서 구현될 수 있는 것으로 이해된다.

[0105] 다양한 실시형태에서 비접촉식 카드(101)는 하나 이상의 안테나(455)를 포함할 수 있다. 하나 이상의 안테나(455)는 비접촉식 카드(101) 내에 그리고 접촉 패드(420)의 처리 회로(425) 주위에 배치될 수 있다. 예를 들어 하나 이상의 안테나는 455는 처리 회로(425)와 통합될 수 있고 하나 이상의 안테나(455)는 외부 부스터 코일과 함께 사용될 수 있다. 다른 예로서 하나 이상의 안테나(455)는 접촉 패드(420) 및 처리 회로(425)의 외부에 있을 수 있다.

[0106] 하나의 실시형태에서 비접촉식 카드(101)의 코일은 공심 변압기의 2차로서 작용할 수 있다. 단말은 전력 또는 진폭 변조를 차단함으로써 비접촉식 카드(101)와 통신할 수 있다. 비접촉식 카드(101)는 하나 이상의 커패시터를 통해 기능적으로 유지될 수 있는 비접촉식 카드의 전원 연결의 갭을 사용하여 단말기에서 전송된 데이터를 추론할 수 있다. 비접촉식 카드(101)는 비접촉식 카드의 코일 또는 부하 변조에 대한 부하를 전환함으로써 다시 통신할 수 있다. 부하 변조는 간섭을 통해 터미널 코일에서 감지될 수 있다. 보다 일반적으로 안테나(455), 처리 회로(425) 및/또는 메모리(102)를 사용하여 비접촉식 카드(101)는 NFC, 블루투스 및/또는 Wi-Fi 통신을 통해 통신하기 위한 통신 인터페이스를 제공한다.

[0107] 위에서 설명된 바와 같이 비접촉식 카드(101)는 스마트 카드 또는 JavaCard와 같은 제한된 메모리를 지니는 다른 디바이스에서 작동 가능한 소프트웨어 플랫폼에 구축될 수 있으며, 하나 이상의 응용프로그램 또는 애플릿이 안전하게 실행될 수 있다. 애플릿(440)은 다양한 모바일 응용프로그램 기반 사용 사례에서 다중 요인 인증(MFA)을 위한 일회용 패스워드(OTP)를 제공하기 위해 비접촉식 카드에 추가될 수 있다. 애플릿(440)은 (예를 들어 모바일 디바이스(110)의) 모바일 NFC 판독기와 같은 판독기로부터의 근거리 데이터 교환 요청과 같은 하나 이상의 요청에 응답하고 NDEF 텍스트 태그로 인코딩된 암호학적으로 안전한 OTP를 포함하는 NDEF 메시지를 생성하도록 형상화 될 수 있다.

[0108] NDEF OTP의 하나의 실시예는 NDEF 숏-레코드 레이아웃(SR=1)이다. 그러한 실시예에서 하나 이상의 애플릿(440)은 OTP를 NDEF 유형 4 잘 알려진 유형 텍스트 태그로서 인코딩하도록 형상화 될 수 있다. 다양한 실시형태에서 NDEF 메시지는 하나 이상의 레코드를 포함할 수 있다. 애플릿(440)은 OTP 레코드에 추가하여 하나 이상의 정적 태그 레코드를 추가하도록 형상화 될 수 있다.

[0109] 다양한 실시형태에서 하나 이상의 애플릿(440)은 RFID 태그를 에뮬레이트 하도록 형상화 될 수 있다. RFID 태그는 하나 이상의 다형성 태그를 포함할 수 있다. 다양한 실시형태에서 태그가 판독될 때마다 비접촉식 카드의 진위를 나타낼 수 있는 상이한 암호화 데이터가 제시된다. 하나 이상의 응용프로그램에 기반하여 태그의 NFC 판독이 처리될 수 있으며 데이터가 서버(120)와 같은 서버로 전송될 수 있고 데이터가 서버에서 검증될 수 있다.

[0110] 다양한 실시형태에서 비접촉식 카드(101) 및 서버(120)는 카드가 적절하게 식별될 수 있도록 특정 데이터를 포함할 수 있다. 비접촉식 카드(101)는 하나 이상의 고유 식별자를 포함할 수 있다(도시되지 않음). 판독 동작이 발생할 때마다 카운터(104)는 증가하도록 형상화 될 수 있다. 다양한 실시형태에서 (예를 들어 모바일 디바이스(110)에 의해) 비접촉식 카드(101)로부터의 데이터가 판독될 때마다, 카운터(104)는 검증을 위해 서버로 전송되고 카운터 값(104)이 동일한지 여부를 (검증의 일부로서)결정한다.

[0111] 하나 이상의 카운터(104)는 리플레이 공격을 방지하도록 형상화 될 수 있다. 예를 들어 암호가 획득되어 리플레이 된 경우, 카운터(104)가 읽히거나 사용되었거나 다른 방식으로 전달된 경우 해당 암호는 즉시 거부된다. 카운터(104)가 사용되지 않았다면 리플레이 될 수 있다. 다양한 실시형태에서 카드 상에서 증가되는 카운터는 트랜잭션을 위해 증가되는 카운터와 상이하다. 비접촉식 카드(101)는 비접촉식 카드(101) 상에서 애플릿(440) 사이에 통신이 없기 때문에 응용프로그램 트랜잭션 카운터(104)를 결정할 수 없다. 다양한 실시형태에서 비접촉식 카드(101)는 거래 애플릿일 수 있는 제1 애플릿(440-1) 및 제2 애플릿(440-2)을 포함할 수 있다. 각각의 애플릿(440-1, 440-2)은 각각의 카운터(104)를 포함할 수 있다.

[0112] 다양한 실시형태에서 카운터(104)는 동기화되지 않을 수 있다. 다양한 실시형태에서 비스듬히 읽기와 같이 트랜

잭션을 개시하는 우발적인 읽기를 설명하기 위해, 카운터(104)는 증가할 수 있지만 응용프로그램은 카운터(104)를 처리하지 않는다. 다양한 실시형태에서 모바일 디바이스(110)가 깨어날 때, NFC는 활성화되고 디바이스(110)는 이용 가능한 태그를 판독하도록 형상화 될 수 있지만 판독에 응답하여 어떠한 조치도 취해지지 않는다.

[0113] 카운터(104)를 동기화 상태로 유지하기 위해 백그라운드 응용프로그램과 같은 응용프로그램이 실행될 수 있다. 이는 모바일 디바이스(110)가 깨어났을 때를 감지하고 감지로 인해 발생한 읽기가 카운터(104)를 앞으로 이동시킨다는 것을 나타내는 서버(120)와 동기화하도록 형상화 될 수 있다. 다른 실시예에서 동기화 오류의 윈도우가 허용될 수 있도록 해시된 일회용 패스워드가 활용될 수 있다.

[0114] 예를 들어 임계값 10 내에 있으면 카운터(104)는 앞으로 이동하도록 형상화 될 수 있다. 그러나 다른 임계값 내, 예를 들어 10 또는 1000 이내인 경우 재동기화를 수행하기 위한 요청이 처리될 수 있으며 이는 사용자가 탭, 제스처 또는 사용자의 디바이스를 통해 한 번 이상 표시하는 하나 이상의 응용프로그램을 통해 요청한다. 카운터(104)가 적절한 순서로 증가한다면, 사용자가 그렇게 했다는 것을 알 수 있다.

[0115] 카운터(104), 마스터 키(105) 및 다양화 키(106)를 참조하여 본 발명에 설명된 키 다양화 기술은 키 다양화 기술의 암호화 및/또는 복호화의 일례이다. 이 예시적인 키 다양화 기술은 본 발명을 제한하는 것으로 간주되어서는 안 되며 그 이유는 본 발명이 다른 유형의 키 다양화 기술에도 동일하게 적용가능하기 때문이다.

[0116] 비접촉식 카드(101)의 생성 프로세스 동안, 2개의 암호화 키가 카드당 고유하게 할당될 수 있다. 암호화 키는 데이터의 암호화 및 복호화 모두에 사용될 수 있는 대칭 키를 포함할 수 있다. 트리플 DES(3DES) 알고리즘은 EMV에 의해 사용될 수 있으며 비접촉식 카드(101)의 하드웨어에 의해 구현된다. 키 다양화 프로세스를 사용함으로써 하나 이상의 키가 키를 필요로 하는 각각의 엔티티에 대해 고유하게 식별 가능한 정보를 기반으로 마스터 키로부터 파생될 수 있다.

[0117] 다양한 실시형태에서 취약성에 취약할 수 있는 3DES 알고리즘의 결함을 극복하기 위해 (세션당 고유 키와 같이) 세션 키가 파생될 수 있으나 마스터 키를 사용하는 것 대신에 고유 카드-파생 키 및 카운터가 다양화 데이터로 사용될 수 있다. 예를 들어 비접촉식 카드(101)가 동작에 사용될 때마다, 메시지 인증 코드(MAC)를 생성하고 암호화를 수행하기 위해 다른 키가 사용될 수 있다. 그 결과 3중 암호화 계층이 생성된다. 세션 키는 하나 이상의 애플릿에 의해 생성될 수 있으며 EMV 4.3 Book 2 A1.3.1 공통 세션 키 파생에 정의된 바와 같은 하나 이상의 알고리즘과 함께 응용프로그램 트랜잭션 카운터를 사용하여 파생될 수 있다.

[0118] 또한 각 카드의 증분은 고유할 수 있으며 개인화에 의해 할당되거나 일부 식별 정보에 의해 알고리즘적으로 할당된다. 예를 들어 홀수 번호의 카드는 2만큼 증가할 수 있고 짝수 번호의 카드는 5만큼 증가할 수 있다. 다양한 실시형태에서 증가는 또한 순차 읽기에서 변할 수 있으므로, 하나의 카드는 1, 3, 5, 2, 2, … 반복 만큼 순서대로 증가할 수 있다. 특정 시퀀스 또는 알고리즘 시퀀스는 개인화 시 또는 고유 식별자에서 파생된 하나 이상의 프로세스로부터 정의될 수 있다. 이것은 리플레이 공격자가 소수의 카드 인스턴스에서 일반화하는 것을 더 어렵게 만들 수 있다.

[0119] 인증 메시지는 16진법 ASCII 형식의 텍스트 NDEF 레코드의 내용으로 전달될 수 있다. 다른 예에서 NDEF 레코드는 16진법 형식으로 인코딩될 수 있다.

[0120] 도 5는 논리 흐름(500)의 실시형태를 도시한다. 논리 흐름(500)은 본 발명에 개시된 하나 이상의 실시형태에 의해 실행되는 동작의 일부 또는 전부를 나타낼 수 있다. 예를 들어 논리 흐름(500)은 로열티 포인트와 연관된 하나 이상의 계정에 액세스하고 및/또는 그렇지 않으면 로열티 포인트를 활용하기 위해 온라인 인증 기술을 활용하여 사용자를 검증 또는 인증하기 위한 동작의 일부 또는 전부를 포함할 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다.

[0121] 도시된 바와 같이 논리 흐름(500)은 인증 응용프로그램(114), OS(112), 관리 응용프로그램(123) 및/또는 임의의 다른 적절한 응용프로그램 중 적어도 하나가 사용자의 신원을 검증하고 액세스 응용프로그램(116)과 연관된 기능에 액세스하기 위한 바코드를 생성하기 위한 트랜잭션을 개시한다. 다양한 실시형태에서 검증은 모바일 디바이스(110) 상의 비접촉식 카드(101)를 탭 함으로써 시작될 수 있다.

[0122] 다양한 실시형태에서 액세스 응용프로그램(116)은 탭 프롬프트를 수신하기 위한 전제조건으로 또는 탭이 발생한 직후 그러나 임의의 추가 온라인 검증 동작 이전에 프롬프트를 제공한다. 프롬프트는 액세스 응용프로그램(116)과 관련하여 제1 레벨 및/또는 제2 레벨 정보 액세스에 대한 비교를 위한 사용자 자격증명을 입력하기 위한 것이다. 여기서 제1 레벨 기능의 특성은 본 발명의 다른 곳에서 개시된다.

[0123] 다양한 실시형태에서 사용자 자격증명은 사용자 프로파일과 연관되고 모바일 디바이스(110)에 의해 제공되는 인터페이스에 입력되며, 언급된 바와 같이 제1 응용프로그램 사용자 자격증명은 생체 인식 데이터, 사용자 인식과 연관된 확립된 제스처, 사용자 이름 및 패스워드 조합 등을 포함할 수 있다. 제1 응용프로그램 사용자 자격증명은 인증 응용프로그램(114)에 의해 서버(120)의 관리 응용프로그램(123)으로 전송될 수 있으며, 여기서 제1 응용프로그램 사용자 자격증명은 저장된 제2 자격증명과 비교된다.

[0124] 블록 510에서 다양한 실시형태에 따라 모바일 디바이스(110)와 비접촉식 카드(101) 사이의 통신이 개시되고, 여기서 통신은 카드 판독기(118)를 활용하고 통신은 NFC 프로토콜에 기반한다. 다양한 실시형태에서 통신은 매치를 초래하는 제1 레벨 비교에 관한 조건이고, 다양한 실시형태에서 서버(120)에서 비교를 위해 제1 응용프로그램 자격증명을 전송하는 대신에 모바일 디바이스(110)와 비접촉식 디바이스 사이에서 비교가 수행되며 저장된 제2 자격증명은 비접촉식 카드의 메모리(102) 내에 저장된다.

[0125] 다양한 실시형태에서 사용자 자격증명에 대한 비교가 생략되고, 모바일 디바이스(110) 상의 비접촉식 카드(101)의 탭은 예를 들어 액세스 응용프로그램(116)과 같이 인증을 필요로 하는 응용프로그램을 선택하기 위한 프롬프트를 개시한다. 또한 비접촉식 카드(101)와 모바일 디바이스(110) 간의 NFC 통신은 단순히 판매 또는 구매를 완료하는 것 이외의 목적을 위한 검증 또는 인증을 포함하는 목적 외로 EMV 표준과 일치하는 결제 프로토콜을 사용하여 사용자의 온라인 검증 또는 인증을 개시하는 것을 시작한다.

[0126] 다양한 실시형태에서 위에서 언급한 바와 같이 사용자는 비접촉식 카드(101)가 암호화된 데이터(예를 들어 암호화된 고객 ID(109))를 생성 및 전송하게 하기 위해 모바일 디바이스(110)에 대해 비접촉식 카드(101)를 탭한다. 비접촉식 카드(101)는 암호화된 데이터를 생성하라는 표시를 수신하는 것에 응답하여 메모리(102)의 카운터 값(104)을 증가시킬 수 있다.

[0127] 다양한 실시형태에서 블록 515에서 비접촉식 카드(101)는 카운터 값(104) 및 메모리(102)의 마스터 키(105) 및 암호화 알고리즘을 사용하여 다양화 키(106)를 생성한다. 블록 520)에서 비접촉식 카드(101)는 다양화 키(106) 및 암호화 알고리즘을 사용하여 데이터(예를 들어 고객 식별자(107))를 암호화하여 암호화된 데이터(예를 들어 암호화된 고객 ID(109))를 생성한다.

[0128] 블록 525에서 비접촉식 카드(101)는 예를 들어 NFC를 사용하여 모바일 디바이스(110)의 계정 응용프로그램(113)에 암호화된 데이터를 전송할 수 있다. 적어도 하나의 실시형태에서 비접촉식 카드(101)는 암호화된 데이터와 함께 카운터 값(104)의 표시를 더욱 포함한다. 블록 530에서 모바일 디바이스(110)의 계정 응용프로그램(113)은 비접촉식 카드(101)로부터 수신된 데이터를 서버(120)의 관리 응용프로그램(123)으로 전송할 수 있다. 블록 535에서 서버(120)의 관리 응용프로그램(123)은 마스터 키(105) 및 카운터 값(104)을 암호화 알고리즘에 대한 입력으로 사용하여 다양화 키(106)를 생성할 수 있다.

[0129] 일 실시형태에서 관리 응용프로그램(123)은 비접촉식 카드(101)에 의해 제공된 카운터 값(104)을 사용한다. 다른 실시형태에서 관리 응용프로그램(123)은 메모리(122) 내의 카운터 값(104)의 상태를 비접촉식 카드(101)의 메모리(102) 내에 있는 카운터 값(104)과 동기화하기 위해 메모리(122) 내의 카운터 값(104)을 증가시킨다.

[0130] 블록 540에서 관리 응용프로그램(123)은 다양화 키(106) 및 암호화 알고리즘을 사용하여 모바일 디바이스(110)를 통해 비접촉식 카드(101)로부터 수신된 암호화된 데이터를 복호화 한다. 이를 통해 적어도 고객 식별자(107)가 생성될 수 있다. 고객 식별자(107)를 생성함으로써 관리 응용프로그램(123)은 블록 545에서 비접촉식 카드(101)로부터 수신된 데이터를 검증할 수 있다. 예를 들어 관리 응용프로그램(123)은 고객 식별자(107)를 계정 데이터(124a)의 관련 계정에 대한 고객 식별자와 비교하고 매치에 기반하여 데이터를 검증할 수 있다. 이는 관리 응용프로그램(123)이 검증의 표시를 모바일 디바이스(110)로 전송하게 할 수 있다.

[0131] 블록 550에서 블록 540 및 545의 복호화 및 검증에 응답하여, 관리 응용프로그램(123)은 하나 이상의 로열티 포인트 계정(124b)에 대한 액세스를 제공할 수 있으며 소매업자(148)와 연관된 로열티 포인트를 포함하여 이와 연관된 하나 이상의 로열티 포인트의 상환을 허가할 수 있다. 서버(120)에 저장되는 것으로 도시되어 있으나 포인트 응용프로그램(117a)은 로열티 포인트 계정(124b)의 인스턴스를 포함할 수 있다.

[0132] 다양한 실시형태에서 복호화 이전에, 관리 응용프로그램(123)은 비접촉식 카드(101) 및/또는 모바일 디바이스(110) 중 하나의 바코드 생성 응용프로그램(117b)에 전송될 수 있는 인증 토큰을 생성할 수 있으며, 여기서 바코드는 디스플레이(140) 및/또는 디스플레이(141)에 의해 디스플레이될 수 있다. 여기서 인증 토큰은 도 1의 다양한 컴포넌트와 관련하여 위에서 개략된 바와 같이 하나 이상의 제한 및 조건을 부과할 수 있으며 로열티 포인트 계정(124b)과 연관된 임의의 로열티 포인트의 암호 복호화 및 활용을 가능하게 하기 위해 임의의 적절한 스

캐닝 디바이스에 의해 바코드가 스캔될 수 있다.

[0133] 다양한 실시형태에서 바코드 생성 응용프로그램(117)은 바코드 생성을 위한 임의의 적절한 기술을 사용하여 바코드를 생성할 수 있으며 생성된 바코드는 모바일 디바이스의 디스플레이(140) 및/또는 비접촉식 카드(101)의 디스플레이(141)에 표시될 수 있다.

[0134] 도 6은 논리 흐름(600)의 실시형태를 도시한다. 논리 흐름(600)은 본 발명에 개시된 하나 이상의 실시형태에 의해 실행되는 동작의 일부 또는 전부를 나타낼 수 있다. 예를 들어 논리 흐름(600)은 액세스 응용프로그램(116)과 연관된 트랜잭션을 승인하기 위해 도 5와 연관하여 생성된 바코드를 활용하는 것을 포함할 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다.

[0135] 도시된 바와 같이 도 5의 하나 이상의 동작이 완료된 후 논리 흐름(600)이 시작되며, 다양한 실시형태에서 흐름은 도 5의 블록 530에서 시작한다. 블록 605에서 시스템(100)의 임의의 적절한 컴포넌트는 사용자가 로열티 포인트 계정 데이터베이스에 대한 액세스를 요청하고 있음을 프로세서 회로에서 실행 중인 응용프로그램에 의해 결정할 수 있다.

[0136] 블록 610에서 본 발명에 논의된 바와 같은 임의의 적절한 기술을 활용하여, 시스템(100)의 임의의 적절한 컴포넌트는 응용프로그램에 의해 그리고 처리 회로와 연관된 컴퓨터 디바이스로부터 서버(120)로 제1 응용프로그램 사용자 자격증명을 전송할 수 있다. 블록 615에서 시스템(100)의 임의의 적절한 컴포넌트는 서버에서 제1 응용프로그램 사용자 자격증명을 저장된 제2 응용프로그램 사용자 자격증명과 비교할 수 있으며 저장된 제2 응용프로그램 사용자 자격증명은 서버에 저장되어 있다.

[0137] 블록 620에서 제1 및 제2 자격증명의 매치에 응답하여 시스템(100)의 임의의 적절한 컴포넌트는 응용프로그램에 의해 계정과 연관된 비접촉식 카드의 통신 인터페이스로부터 암호화된 데이터를 수신할 수 있으며, 암호화된 데이터는 암호화 알고리즘 및 다양화 키를 기반으로 생성된다. 다양화 키는 비접촉식 카드의 메모리에 저장되고 비접촉식 카드의 메모리 내에 저장된 마스터 키 및 카운터 값을 기반으로 생성된다.

[0138] 블록 625에서 제1 자격증명과 제2 자격증명의 매치에 응답하여, 시스템(100)의 임의의 적절한 컴포넌트는 사용자와 연관된 로열티 식별자를 암호화된 데이터와 조합할 수 있고, 여기서 데이터 조합은 로열티 식별자와 암호화된 데이터의 조합을 포함한다. 조합(및/또는 본 발명에 개시된 임의의 다른 조합 동작)은 논리적 동작에 기반할 수 있다. 논리 연산은 배타적 OR 연산일 수 있다. 블록 630에서 시스템(100)의 임의의 적절한 컴포넌트는 수신된 암호화된 데이터 및 로열티 식별자에 대한 동작을 서버에서 수행할 수 있다.

[0139] 블록 635에서 시스템(100)의 임의의 적절한 컴포넌트는 ⅰ) 비접촉식 카드 및 ii) 컴퓨터 디바이스에서 바코드를 생성할 수 있으며, 여기서 생성된 바코드는 서버로부터 수신되고 암호화된 데이터 및 로열티 식별자를 활용하는 토큰에 기반한다. 블록 640에서 시스템(100)의 임의의 적절한 컴포넌트는 생성된 바코드를 표시할 수 있다.

[0140] 블록 645에서 시스템(100)의 임의의 적절한 컴포넌트는 생성된 바코드의 스캔에 기반하여 서버로부터 응용프로그램에 의해 암호화된 데이터의 검증을 수신할 수 있다. 서버는 암호화된 데이터를 검증하기 위해 서버의 메모리 내에 저장된 암호화 알고리즘 및 다양화 키를 기반으로 암호화된 데이터를 복호화 한다. 서버의 메모리 내에 저장된 다양화 키는 서버의 메모리 내에 저장된 마스터 키 및 카운터 값을 개반으로 생성된다.

[0141] 블록 650)에서 시스템(100)의 임의의 적절한 컴포넌트는 검증 수신에 응답하여 적어도 하나의 동작을 수행하기 위한 권한을 부여할 수 있으며, 여기서 적어도 하나의 동작은 ⅰ) 각각의 계정은 로열티 포인트의 개별 세트와 연관되며 적어도 한 명의 사용자 및 적어도 2개의 개별 계정과 연관된 다수의 로열티 식별자를 지니는 데이터베이스에 액세스 하는 단계 및 ii) 데이터베이스의 적어도 2개의 개별 계정과 관련하여 다수의 로열티 식별자 중 적어도 하나를 저장하는 단계 중 적어도 하나를 포함한다.

[0142] 다양한 실시형태에서 비접촉식 카드(101)는 하나 이상의 컴퓨터 키오스크 또는 단말기와 같은 디바이스에 탭 하여 신원을 검증하여 커피와 같은 구매에 응답하는 트랜잭션 항목을 수신할 수 있다. 비접촉식 카드(101)를 사용함으로써, 로열티 프로그램에서 신원을 증명하는 안전한 방법이 확립될 수 있다. 예를 들어 리워드, 쿠폰, 제안 등을 얻기 위해 신원을 안전하게 증명하거나 혜택을 수령하는 것은 단순히 바 카드를 스캔하는 것과는 다른 방식으로 설정된다.

[0143] 예를 들어 하나 이상의 탭 제스처를 처리하도록 형상화 될 수 있는 비접촉식 카드(101)와 디바이스 사이에 암호화된 트랜잭션이 발생할 수 있다. 위에서 설명된 바와 같이 하나 이상의 응용프로그램은 사용자의 신원을 검증

하고 사용자가 예를 들어 하나 이상의 탭 제스처를 통해 그에 대해 행동하거나 응답하게 하도록 형상화 될 수 있다. 다양한 실시형태에서 데이터, 예를 들어 보너스 포인트, 로열티 포인트, 리워드 포인트, 건강 관리 정보 등이 비접촉식 카드에 다시 기록될 수 있다.

[0144] 다양한 실시형태에서 비접촉식 카드(101)는 모바일 디바이스(110)와 같은 디바이스에 탭 될 수 있다. 위에서 설명된 바와 같이 사용자의 신원은 신원의 검증을 기반으로 사용자에게 원하는 혜택을 부여할 수 있는 하나 이상의 응용프로그램에 의해 검증될 수 있다.

[0145] 다양한 실시형태에서 예시적인 인증 통신 프로토콜은 트랜잭션 카드와 판매 시점 관리(POS) 디바이스 사이에서 일반적으로 수행되는 EMV 표준의 오프라인 동적 데이터 인증 프로토콜을 일부 수정하여 모방할 수 있다. 예를 들어 예시적인 인증 프로토콜은 그 자체로 카드 발급사/결제 프로세서와의 결제 트랜잭션을 완료하는 데 사용되지 않기 때문에 일부 데이터 값이 필요하지 않으며 카드 발급사/결제 프로세서에 대한 실시간 온라인 연결 없이 인증이 수행될 수 있다. 당업계에 공지된 바와 같이 판매 시점(POS) 시스템은 트랜잭션 값을 포함하는 트랜잭션을 카드 발급자에게 제출한다. 카드 발급사가 거래 금액을 인식하는지 여부에 따라 발급사의 거래 승인 여부가 결정될 수 있다.

[0146] 한편 본 발명의 특정 실시형태에서 모바일 디바이스에서 발생하는 거래는 POS 시스템과 관련된 트랜잭션 값이 부족하다. 따라서 다양한 실시형태에서 더미 트랜잭션 값(즉, 카드 발급자가 인식할 수 있고 활성화가 발생하도록 허용하기에 충분한 값)이 예시적인 인증 통신 프로토콜의 일부로서 전달될 수 있다. POS 기반 트랜잭션은 트랜잭션 시도 횟수(예를 들어 트랜잭션 카운터)에 따라 거래를 거부할 수도 있다. 시도 횟수가 버퍼 값을 초과하면 트랜잭션을 수락하기 전에 추가 검증을 필요로 하는 완곡한 거절이 발생할 수 있다. 일부 구현에서 트랜잭션 카운터에 대한 버퍼 값은 적법한 트랜잭션이 거절하는 것을 피하기 위해 수정될 수 있다.

[0147] 다양한 실시형태에서 비접촉식 카드(101)는 수신 디바이스에 따라 정보를 선택적으로 전달할 수 있다. 일단 탭되면 비접촉식 카드(101)는 탭이 향하는 디바이스를 인식할 수 있으며 이러한 인식에 기반하여 비접촉식 카드는 해당 디바이스에 대한 적절한 데이터를 제공할 수 있다. 이는 유리하게도 비접촉식 카드가 결제 또는 카드 인증과 같은 즉각적인 조치 또는 거래를 완료하는 데 필요한 정보만을 전송할 수 있게 한다.

[0148] 데이터 전송을 제한하고 불필요한 데이터 전송을 방지함으로써 효율성과 데이터 보안을 모두 향상시킬 수 있다. 정보의 인식 및 선택적 통신은 카드 활성화, 잔액 이체, 계정 액세스 시도, 상거래 및 단계적 사기 감소를 포함한 다양한 시나리오에 적용될 수 있다.

[0149] 비접촉식 카드(101)의 탭이 Apple의 iOS® 운영 체제를 실행하는 디바이스(예를 들어 iPhone, iPod 또는 iPad)로 향하는 경우 비접촉식 카드는 iOS® 운영 체제를 인식하고 이 디바이스와 통신하는 데 적절한 데이터를 전송할 수 있다. 예를 들어 비접촉식 카드(101)는 예를 들어 NFC를 통해 NDEF 태그를 사용하여 카드를 인증하는 데 필요한 암호화된 신원 정보를 제공할 수 있다.

[0150] 유사하게 비접촉식 카드 탭이 Android® 운영 체제를 실행하는 디바이스(예를 들어 Android® 스마트폰 또는 태블릿)로 향하는 경우 비접촉식 카드는 Android® 운영 체제를 인식하고 예를 들어 본 발명에 개시된 방법에 의한 인증에 필요한 암호화된 식별 정보와 같이 이 디바이스와 통신하는데 적절한 데이터를 전송할 수 있다.

[0151] 다른 예로서 비접촉식 카드 탭은 키오스크, 금전 등록기, 결제 스테이션 또는 다른 단말기를 제한 없이 포함하는 POS 디바이스로 향할 수 있다. 탭을 수행하면 비접촉식 카드(101)는 POS 디바이스를 인식하고 동작이나 트랜잭션에 필요한 정보만을 전송할 수 있다. 예를 들어 상거래를 완료하는 데 사용되는 POS 디바이스를 인식하면 비접촉식 카드(101)는 EMV 표준에 따라 거래를 완료하는 데 필요한 결제 정보를 전달할 수 있다.

[0152] 다양한 실시형태에서 트랜잭션에 참여하는 POS 디바이스는 비접촉식 카드에 의해 제공될 추가 정보, 예를 들어 디바이스-특정 정보, 위치-특정 정보 및 트랜잭션-특정 정보를 요구하거나 명시할 수 있다. 예를 들어 POS 디바이스가 비접촉식 카드로부터 데이터 통신을 수신하면 POS 디바이스는 비접촉식 카드를 인식하고 동작 또는 트랜잭션을 완료하는 데 필요한 추가 정보를 요청할 수 있다.

[0153] 다양한 실시형태에서 POS 디바이스는 특정 비접촉식 카드에 익숙하거나 특정 비접촉식 카드 트랜잭션을 수행하는 데 익숙한 승인된 판매자 또는 다른 엔티티와 제휴할 수 있다. 그러나 개시된 방법의 수행을 위해 그러한 제휴가 필요하지 않은 것으로 이해된다.

[0154] 쇼핑 상점, 식료품점, 편의점 등과 같은 다양한 실시형태에서 비접촉식 카드(101)는 응용프로그램을 열 필요 없이 모바일 디바이스에 탭 되어 하나 이상의 구매를 커버하기 위한 리워드 포인트, 로열티 포인트, 쿠폰, 제안

등에서 하나 이상을 활용하려는 욕구 또는 의도를 나타낼 수 있다. 따라서 구매 이면의 의도가 제공된다.

[0155] 다양한 실시형태에서 하나 이상의 응용프로그램은 그것이 비접촉식 카드(101)의 하나 이상의 탭 제스처를 통해 시작되었다고 결정하도록 형상화 될 수 있다. 즉 시작은 오후 3시 51분에 발생하였으며 사용자의 신원을 검증하기 위한 트랜잭션은 3시 36분에 처리되거나 발생하였다.

[0156] 다양한 실시형태에서 하나 이상의 응용프로그램은 하나 이상의 탭 제스처에 응답하여 하나 이상의 동작을 제어하도록 형상화 될 수 있다. 예를 들어 하나 이상의 동작은 리워드 수집, 포인트 수집, 가장 중요한 구매 결정, 가장 저렴한 구매 결정 및/또는 실시간으로 다른 동작으로 재형상화 하는 것을 포함할 수 있다.

[0157] 다양한 실시형태에서 생체 인식/제스처 인증으로서 탭 행동에 대해 데이터가 수집될 수 있다. 예를 들어 암호학적으로 안전하고 가로채기 쉽지 않은 고유 식별자가 하나 이상의 백-엔드 서비스로 전송될 수 있다. 고유 식별자는 개인에 대한 2차 정보를 조회하도록 형상화 될 수 있다. 2차 정보는 사용자에 대한 개인 식별 정보를 포함할 수 있다. 다양한 실시형태에서 2차 정보는 비접촉식 카드 내에 저장될 수 있다.

[0158] 다양한 실시형태에서 디바이스는 청구서를 분할하거나 다수의 개인 간의 결제를 확인하는 응용프로그램을 포함할 수 있다. 예를 들어 각 개인은 비접촉식 카드를 소지하고 동일한 발급 금융 기관의 고객일 수 있지만 반드시 필요한 것은 아니다. 이러한 각각의 개인은 구매를 분할하기 위하여 응용프로그램을 통해 그들의 기기에서 푸시 알림을 받을 수 있다. 결제를 표시하기 위해 하나의 카드 탭만 수락하는 대신 다른 비접촉식 카드를 사용할 수 있다. 다양한 실시형태에서 카드를 탭 하는 개인으로부터 하나 이상의 결제 요청을 개시하기 위한 정보를 제공하기 위하여, 상이한 금융 기관을 가진 개인은 비접촉식 카드(101)를 소유할 수 있다.

[0159] 다양한 실시형태에서 본 발명은 비접촉식 카드의 탭에 관한 것이다. 그러나 본 개시는 탭으로 제한되지 않으며 본 발명은 예를 들어 카드의 웨이브 또는 다른 움직임과 같은 다른 제스처를 포함하는 것으로 이해된다.

[0160] 도 7은 앞서 설명된 바와 같은 다양한 실시형태를 구현하는데 적합할 수 있는 컴퓨터 시스템(702)을 포함하는 예시적인 컴퓨터 아키텍처(700)의 실시형태를 도시한다. 다양한 실시형태에서 컴퓨터 아키텍처(700)는 전자 디바이스를 포함하거나 전자 디바이스의 일부로서 구현될 수 있다. 다양한 실시형태에서 컴퓨터 아키텍처(700)는 예를 들어 시스템(100)의 하나 이상의 컴포넌트를 구현하는 시스템을 나타낼 수 있다. 다양한 실시형태에서 컴퓨터 시스템(702)은 예를 들어 시스템(100)의 모바일 디바이스(110) 및 서버(120)를 나타낼 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다. 보다 일반적으로 컴퓨터 아키텍처(700)는 도 1 내지 도 6을 참조하여 본 발명에 설명된 모든 로직, 응용프로그램, 시스템, 방법, 디바이스 및 기능을 구현하도록 형상화 된다.

[0161] 본 발명에서 사용된 용어 "시스템", "컴포넌트" 및 "모듈"은 하드웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어 또는 실행 중인 소프트웨어인 컴퓨터 관련 엔티티를 의미한다. 예를 들어 컴포넌트는 컴퓨터 프로세서 상에서 실행 중인 프로세스, 컴퓨터 프로세서, 하드 디스크 드라이브, (광학 및/또는 자기 저장 매체의) 다중 저장 드라이브, 개체, 실행 파일, 실행 스레드, 프로그램 및/또는 컴퓨터일 수 있으나 이에 제한되지 않는다.

[0162] 예를 들어 서버에서 실행되는 응용프로그램과 서버 모두 컴포넌트가 될 수 있다. 하나 이상의 컴포넌트는 프로세스 및/또는 실행 스레드 내에 상주할 수 있으며 컴포넌트는 하나의 컴퓨터에 국한되거나 2 이상의 컴퓨터에 분산될 수 있다. 또한 컴포넌트들은 동작을 협력하기 위해 다양한 유형의 통신 매체에 의해 서로 통신 가능하게 결합될 수 있다. 협력에는 정보의 단방향 또는 양방향 교환이 포함될 수 있다.

[0163] 예를 들어 컴포넌트는 통신 매체를 통해 통신되는 신호의 형태로 정보를 전달할 수 있다. 정보는 다양한 신호 라인에 할당된 신호로 구현될 수 있다. 이러한 할당에서 각 메시지는 신호이다. 그러나 다른 실시형태는 대안적으로 데이터 메시지를 사용할 수 있다. 이러한 데이터 메시지는 다양한 연결을 통해 전송될 수 있다. 예시적인 연결은 병렬 인터페이스, 직렬 인터페이스 및 버스 인터페이스를 포함한다.

[0164] 컴퓨터 시스템(702)은 하나 이상의 프로세서, 멀티코어 프로세서, 코프로세서, 처리 메모리 유니트, 칩셋, 컨트롤러, 주변기기, 인터페이스, 발진기, 타이밍 디바이스, 비디오 카드, 오디오 카드, 멀티미디어 입/출력(I/O) 컴포넌트, 전원 공급 디바이스 등과 같은 다양한 공통 컴퓨터 엘레멘트를 포함한다. 그러나 실시형태는 컴퓨터 시스템(702)에 의한 구현으로 제한되지 않는다.

[0165] 도 7에 도시된 바와 같이 컴퓨터 시스템(702)은 프로세서(704), 시스템 메모리(706) 및 시스템 버스(708)를 포함한다. 프로세서(704)는 AMD® Athlon®, Duron® 및 Opteron® 프로세서; ARM® 응용프로그램, 임베디드 및 보안 프로세서; IBM® 및 Motorola® DragonBall® 및 PowerPC® 프로세서; IBM 및 Sony® Cell 프로세서; Intel® Celeron®, Core®, Core (2) Duo®, Itanium®, Pentium®, Xeon® 및 XScale® 프로세서; 및 유사한

프로세서를 제한 없이 포함하는 임의의 다양한 상업적으로 이용 가능한 컴퓨터 프로세서 또는 컴퓨터 프로세스 회로일 수 있다. 듀얼 마이크로프로세서, 멀티 코어 프로세서 및 기타 멀티 프로세서 아키텍처가 프로세서(704)로 사용될 수도 있다.

[0166] 프로세서(704)는 시스템 메모리(706)에 포함된 연관된 메모리 명령어에 의해 형상화 될 수 있어서, 명령어가 프로세서(예를 들어 프로세서 회로)(704) 상에서 재실행될 때, 프로세서는 도 5 내지 도 7b의 어느 하나와 연관된 하나 이상의 동작 및/또는 본 발명에 개시된 바와 같은 임의의 다른 동작 또는 기술을 수행할 수 있다.

[0167] 시스템 버스(708)는 프로세서(704)에 대한 시스템 메모리(706)를 포함하지만 이에 국한되지 않는 시스템 컴포넌트에 대한 인터페이스를 제공한다. 시스템 버스(708)는 (메모리 컨트롤러 존재 또느 부재 하에) 메모리 버스, 주변기기 버스 및 상업적으로 이용 가능한 다양한 버스 아키텍처를 사용하는 로컬 버스에 더욱 상호 연결될 수 있는 다양한 유형의 버스 구조 중 하나 일 수 있다. 인터페이스 어댑터는 슬롯 아키텍처를 통해 시스템 버스(708)에 연결할 수 있다. 슬롯 아키텍처의 예에는 가속 그래픽 포트(AGP), 카드 버스, (확장) 산업 표준 아키텍처((E)ISA), 마이크로 채널 아키텍처(MCA), NuBus, 주변기기 컴포넌트 상호 연결(확장)(PCI(X)), PCI Express, 개인용 컴퓨터 메모리 카드 국제 협회(PCMCIA) 등이 포함될 수 있으나 이에 국한되지 않는다.

[0168] 시스템 메모리(706)는 읽기 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 동적 RAM(DRAM), 더블 데이터-레이트 DRAM)DDRRAM), 동기식 DRAM(SDRAM), 정적 RAM(SRAM), 프로그램 가능 ROM(PROM), 지울 수 있는 프로그램 가능 ROM(EPROM), 전기적으로 지울 수 있는 프로그램 가능 ROM(EEPROM), 플래시 메모리(예를 들어 하나 이상의 플래시 어레이), 강유전성 폴리머 메모리, 오보닉 메모리, 상 변화 또는 강유전성 메모리와 같은 폴리머 메모리, 실리콘-옥사이드-니트라이드-옥사이드-실리콘(SONOS) 메모리, 자기 또는 광학 카드, 다수 배열 독립 디스크(RAID) 드라이브, 고체 상태 메모리 디바이스(예를 들어 USB 메모리, 고체 상태 드라이브(SSD) 및 정보 저장에 적합한 기타 유형의 저장 매체)과 같은 하나 이상의 고속 메모리 유니트의 형태로 다양한 유형의 컴퓨터 판독가능 저장 매체를 포함할 수 있다.

[0169] 도 7에 도시된 예시된 실시형태에서 시스템 메모리(706)는 비휘발성 메모리(710) 및/또는 휘발성 메모리(712)를 포함할 수 있다. 기본 입/출력 시스템(BIOS)은 비휘발성 메모리(710) 내에 저장될 수 있다.

[0170] 컴퓨터 시스템(702)은 내부(또는 외부) 하드 디스크 드라이브(HDD)(714), 이동식 자기 디스크(718)로부터 읽거나 쓰기 위한 자기 플로피 디스크 드라이브(FDD)(716), 이동식 광 디스크(722)(예를 들어 CD-ROM 또는 DVD)로부터 읽거나 쓰기 위한 광학 디스크 드라이브(720)를 포함하는 하나 이상의 저속 메모리 유니트의 형태로 다양한 유형의 컴퓨터 판독 가능 저장 매체를 포함할 수 있다. HDD(714), FDD(716) 및 광 디스크 드라이브(720)는 각각 HDD 인터페이스(724), FDD 인터페이스(726) 및 광 드라이브 인터페이스(728)에 의해 시스템 버스(708)에 연결될 수 있다.

[0171] 외부 드라이브 구현을 위한 HDD 인터페이스(724)는 범용 직렬 버스(USB) 및 IEEE 1394 인터페이스 기술 중 적어도 하나 또는 모두를 포함할 수 있다. 컴퓨터 시스템(702)은 일반적으로 도 1 내지 도 6을 참조하여 본 발명에 설명된 모든 로직, 시스템, 방법, 디바이스 및 기능을 구현하도록 형상화 된다.

[0172] 드라이브 및 관련 컴퓨터 판독 가능 매체는 데이터, 데이터 구조, 컴퓨터 실행 가능 명령어 등의 휘발성 및/또는 비휘발성 저장 디바이스를 제공한다. 예를 들어 운영 체제(730), 하나 이상의 어플리케이션 프로그램(732), 다른 프로그램 모듈(734) 및 프로그램 데이터(736)를 포함하는 다수의 프로그램 모듈이 드라이브 및 메모리 유니트(710, 712) 내에 저장될 수 있다. 다양한 실시형태에서 하나 이상의 어플리케이션 프로그램(732), 다른 프로그램 모듈(734) 및 프로그램 데이터(736)는 예를 들어 시스템(100)의 다양한 응용프로그램 및/또는 컴포넌트, 예를 들어 운영 체제(112), 계정 응용프로그램(113), 인증 응용프로그램(114), 다른 응용프로그램(115), 액세스 응용프로그램(116) 및 관리 응용프로그램(123을 포함할 수 있다.

[0173] 사용자는 하나 이상의 유선/무선 입력 디바이스, 예를 들어 키보드(738) 및 마우스(740)와 같은 포인팅 디바이스를 통해 명령 및 정보를 컴퓨터 시스템(702)에 입력할 수 있다. 다른 입력 장치는 마이크, 적외선(IR) 리모콘, 무선 주파수(RF) 리모콘, 게임 패드, 스타일러스 펜, 카드 판독기, 동글, 지문 판독기, 장갑, 그래픽 태블릿, 조이스틱, 키보드, 망막 판독기, 터치 스크린(예를 들어 적전식, 감압식 등), 트랙볼, 트랙패드, 센서, 스타일러스 등을 포함할 수 있다. 이들 및 다른 입력 디바이스는 종종 시스템 버스(708)에 연결된 입력 디바이스 인터페이스(742)를 통해 프로세서(704)에 연결되지만 병렬 포트, IEEE 1394 직렬 포트, 게임 포트, USB 포트, IR 인터페이스 등과 같은 다른 인터페이스에 의해 연결될 수 있다.

[0174] 모니터(744) 또는 다른 유형의 디스플레이 디바이스도 비디오 어댑터(746)와 같은 인터페이스를 통해 시스템 버

스(708)에 연결된다. 모니터(744)는 컴퓨터 시스템(702)의 내부 또는 외부에 있을 수 있다. 모니터(744) 외에 컴퓨터에는 일반적으로 스피커, 프린터 등과 같은 기타 주변 출력 디바이스가 포함된다.

[0175] 컴퓨터 시스템(702)은 원격 컴퓨터(748)와 같은 하나 이상의 원격 컴퓨터에 대한 유선 및/또는 무선 통신을 통한 논리적 연결을 사용하여 네트워크 환경에서 동작할 수 있다. 원격 컴퓨터(748)는 워크스테이션, 서버 컴퓨터, 라우터, 개인용 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서 기반 엔터테인먼트 기기, 피어 디바이스 또는 기타 공통 네트워크 노드를 포함하며 일반적으로 컴퓨터 시스템(702)과 관련하여 설명된 많은 또는 모든 요소를 포함하지만 간결함을 위해 메모리/저장 디바이스(750)가 도시되어 있다.

[0176] 도시된 논리적 연결은 근거리 네트워크(LAN)(752) 및/또는 더 큰 네트워크, 예를 들어 광역 네트워크(WAN)(754)에 대한 유무선 연결을 포함한다. 이러한 LAN 및 WAN 네트워크 환경은 사무실과 회사에서 일반적이며 인트라넷과 같은 전기업적 컴퓨터 네트워크를 용이하게 한다. 이들 모두는 예를 들어 인터넷과 같은 글로벌 통신 네트워크에 연결할 수 있다. 실시형태에서 도 1의 네트워크(130)는 LAN(752) 및 WAN(754) 중 하나 이상이다.

[0177] LAN 네트워크 환경에서 사용될 때, 컴퓨터 시스템(702)은 유선 및/또는 무선 통신 네트워크 인터페이스 또는 어댑터(756)를 통해 LAN(752)에 연결된다. 어댑터(756)는 LAN(752)에 대한 유선 및/또는 무선 통신을 용이하게 할 수 있으며 이는 또한 어댑터(756)의 무선 기능과 통신하기 위해 그 위에 배치된 무선 액세스 포인트를 포함한다.

[0178] WAN 네트워크 환경에서 사용될 때, 컴퓨터 시스템(702)은 모뎀(758)을 포함할 수 있거나, WAN(754) 상의 통신 서버에 연결되거나, 인터넷과 같이 WAN(754)을 통한 통신을 설정하기 위한 다른 수단을 가질 수 있다. 내부 또는 외부 및 유선 및/또는 무선 디바이스일 수 있는 모뎀(758)은 입력 디바이스 인터페이스(742)를 통해 시스템 버스(708)에 연결된다. 네트워크 환경에서 컴퓨터 시스템(702)과 관련하여 도시된 프로그램 모듈 또는 그의 일부는 원격 메모리/저장 디바이스 내에 저장될 수 있다. 도시된 네트워크 연결은 예시적이며 컴퓨터 사이의 통신 링크를 설정하는 다른 수단이 사용될 수 있는 것으로 이해된다.

[0179] 컴퓨터 시스템(702)은 무선 통신(예를 들어 IEEE 802.16 무선 변조 기술)에서 작동 가능하게 배치된 무선 디바이스와 같은 IEEE 802 표준 패밀리를 사용하여 유선 및 무선 디바이스 또는 엔티티와 통신하도록 작동 가능하다. 여기에는 최소한 Wi-Fi(또는 Wireless Fidelity), WiMax 및 Bluetooth™ 무선 기술 등이 포함된다. 따라서 통신은 기존 네트워크 에서와 같이 미리 정의된 구조이거나 단순히 두 개 이상의 디바이스 간의 임시 통신일 수 있다. Wi-Fi 네트워크는 IEEE 802.11x(a, b, g, n 등)라는 무선 기술을 사용하여 안전하고 안정적이며 빠른 무선 연결을 제공한다. Wi-Fi 네트워크는 컴퓨터를 상호간에 연결하고 인터넷에 연결하고 유선 네트워크(IEEE 802.3 관련 미디어 및 기능 사용)에 연결하는 데 사용할 수 있다.

[0180] 다양한 실시형태는 하드웨어 엘레멘트, 소프트웨어 엘레멘트 또는 양자의 조합을 사용하여 구현될 수 있다. 하드웨어 엘레멘트의 예에는 프로세서, 마이크로프로세서, 회로, 회로 엘레멘트(예를 들어 트랜지스터, 레지스터, 커패시터, 인덕터 등), 집적 회로, 주문형 집적 회로(ASIC), 프로그램 가능 논리 디바이스(PLD), 디지털 신호 프로세서(DSP), 필드 프로그램가능 게이트 어레이(FPGA), 논리 게이트, 레지스터, 반도체 디바이스, 칩, 마이크로칩, 칩셋 등이 포함될 수 있다.

[0181] 소프트웨어의 예에는 소프트웨어 컴포넌트, 프로그램, 응용프로그램, 컴퓨터 프로그램, 어플리케이션 프로그램, 시스템 프로그램, 기계 프로그램, 운영 체제 소프트웨어, 미들웨어, 펌웨어, 소프트웨어 모듈, 루틴, 서브루틴, 기능, 방법, 절차, 소프트웨어 인터페이스, 응용프로그램 프로그램 인터페이스(API), 명령어 세트, 컴퓨터 코드, 컴퓨터 코드, 코드 세그먼트, 컴퓨터 코드 세그먼트, 단어, 값, 기호 또는 이들의 조합이 포함될 수 있다.

[0182] 실시형태가 하드웨어 엘레멘트 및/또는 소프트웨어 엘레멘트를 사용하여 구현되는지 여부를 결정하는 것은 원하는 연산 속도, 전력 수준, 열 허용 오차, 처리 주기 예산, 입력 데이터 속도, 출력 데이터 속도, 메모리 리소스, 데이터 버스 속도 및 기타 설계 또는 성능 제약과 같은 임의의 수의 요인에 따라 달라질 수 있다..

[0183] 적어도 다양한 실시형태의 하나 이상의 측면은 프로세서 내의 다양한 로직을 나타내는 머신 판독가능 매체에 저장된 대표적인 명령어에 의해 구현될 수 있으며 이는 머신에 의해 판독될 때 머신이 본 발명에 설명된 기술을 수행하도록 로직을 제조하게 한다. "IP 코어"로 알려진 그러한 표현은 유형의 기계 판독 가능 매체에 저장될 수 있으며 로직 또는 프로세서를 만드는 제조 기계에 로드하기 위해 다양한 고객 또는 제조 시설에 제공될 수 있다.

[0184] 다양한 실시형태는 예를 들어 기계에 의해 실행되는 경우 기계가 실시형태에 따른 방법 및/또는 동작을 수행하게 할 수 있는 명령어 또는 명령어 세트를 저장할 수 있는 기계 판독가능 매체 또는 물품을 사용하여 구현될 수

있다. 그러한 기계는 예를 들어 임의의 적절한 처리 플랫폼, 컴퓨터 플랫폼, 컴퓨터 디바이스, 처리 디바이스, 컴퓨터 시스템, 처리 시스템, 컴퓨터, 프로세서 등을 포함할 수 있으며 하드웨어 및/또는 소프트웨어의 임의의 적절한 조합을 사용하여 구현될 수 있다.

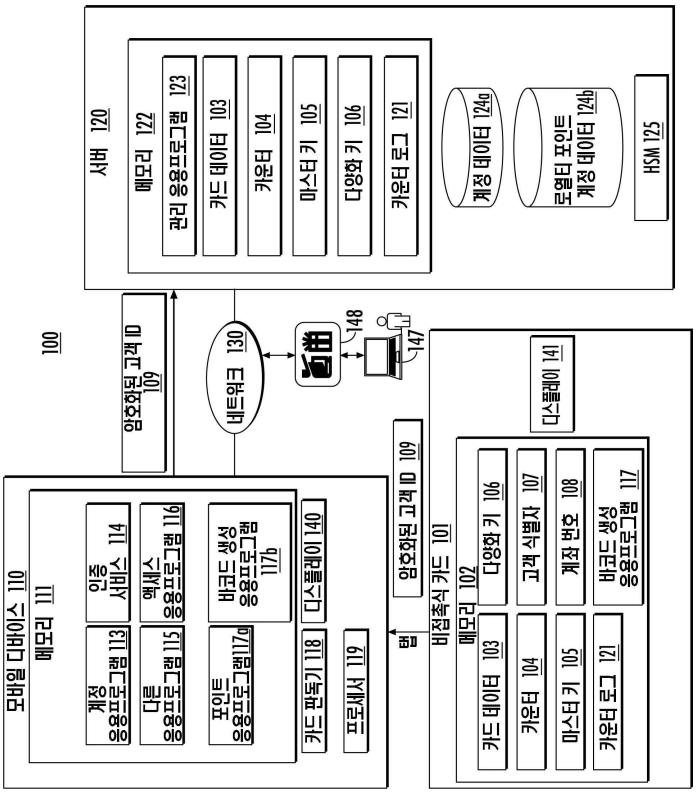
[0185] 기계 판독가능 매체 또는 물품은 예를 들어 임의의 적합한 유형의 메모리 유니트, 메모리 디바이스, 메모리 물품, 메모리 매체, 저장 디바이스, 저장 물품, 저장 매체 및/또는 저장 유니트, 예를 들어 메모리, 이동식 또는 비이동식 매체, 지울 수 있거나 지울 수 없는 매체, 기록 가능 또는 재기록 가능 매체, 디지털 또는 아날로그 매체, 하드 디스크, 플로피 디스크, 읽기 전용 메모리 컴팩트 디스크(CD-ROM), 기록 가능 컴팩트 디스크(CD-R), 재리록 가능 컴팩트 디스크(CD-RW), 광 디스크, 자기 매체, 광자기 매체, 이동식 메모리 카드 또는 디스크, 다양한 유형의 디지털 다목적 디스크(DVD), 테이프, 카세트 등을 포함할 수 있다

[0186] 명령어는 소스 코드, 컴파일된 코드, 해석된 코드, 실행 가능한 코드, 정적 코드, 동적 코드, 암호화된 코드 등과 같은 임의의 적절한 유형의 코드를 포함할 수 있으며, 적절한 상위 수준, 하위 수준 개체-지향, 시각적, 컴파일 및/또는 해석 프로그래밍 언어를 사용하여 구현된다.

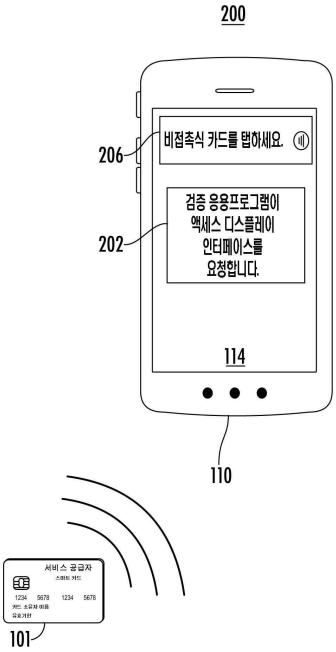
[0187] 예시적인 실시형태의 전술한 설명은 예시 및 설명의 목적으로 제시되었다. 이는 본 발명을 개시된 정확한 형태로 철저하게 제한하거나 제한하려는 의도가 아니다. 본 개시 내용에 비추어 많은 수정 및 변형이 가능하다. 본 발명의 범위는 이러한 상세한 설명이 아니라 여기에 첨부된 청구범위에 의해 제한되는 것으로 의도된다. 본 출원에 대한 우선권을 주장하는 미래의 특허 출원은 개시된 주제를 다른 방식으로 청구할 수 있으며 일반적으로 여기에서 다양하게 개시되거나 달리 입증된 바와 같이 하나 이상의 제한의 임의의 세트를 포함할 수 있다.

도면

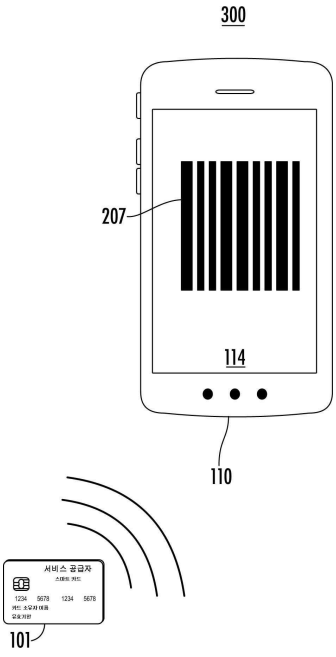
도면1



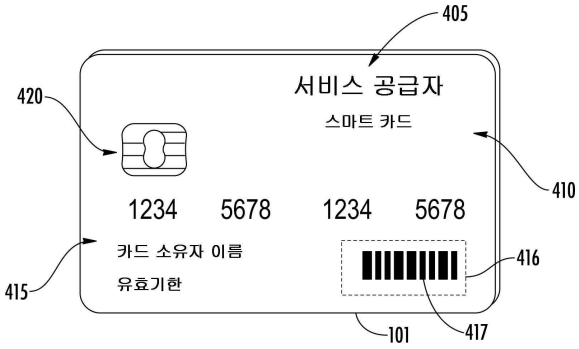
도면2


200
비접촉식 카드를 탭하세요.
206
검증 응용프로그램이
엑세스 디스플레이
인터페이스를
요청합니다.
202
114
110
서비스 공급자
101

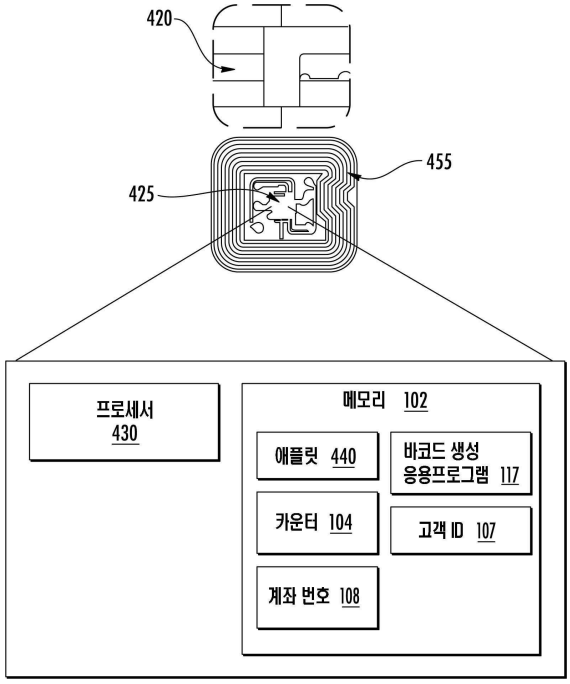
도면3


300
207
114
110
서비스 공급자
101

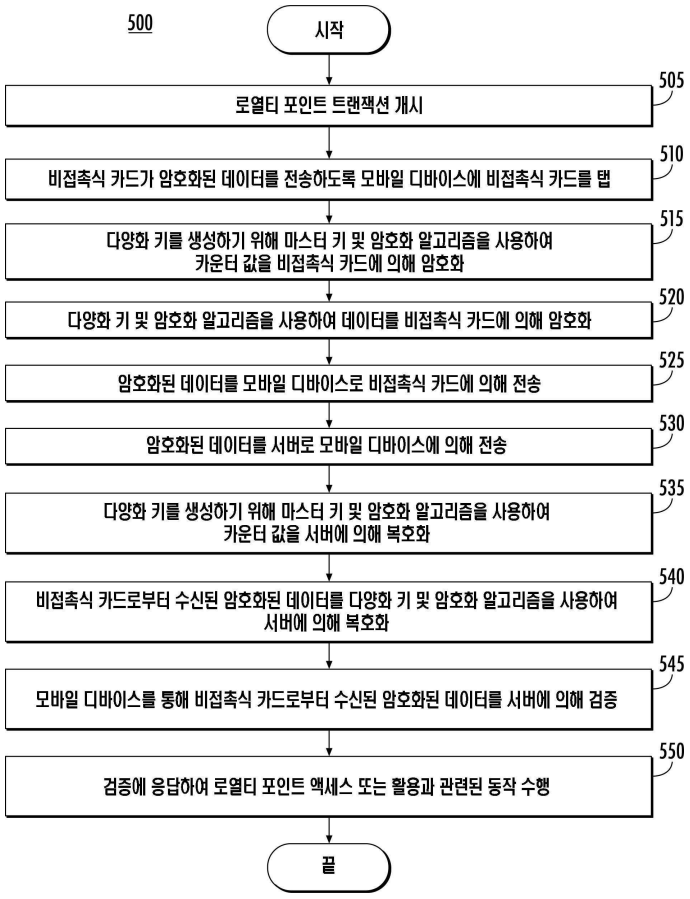
도면4a


405
서비스 공급자
스마트 카드
420
410
1234 5678 1234 5678
카드 소유자 이름
유효기한
415
416
417
101

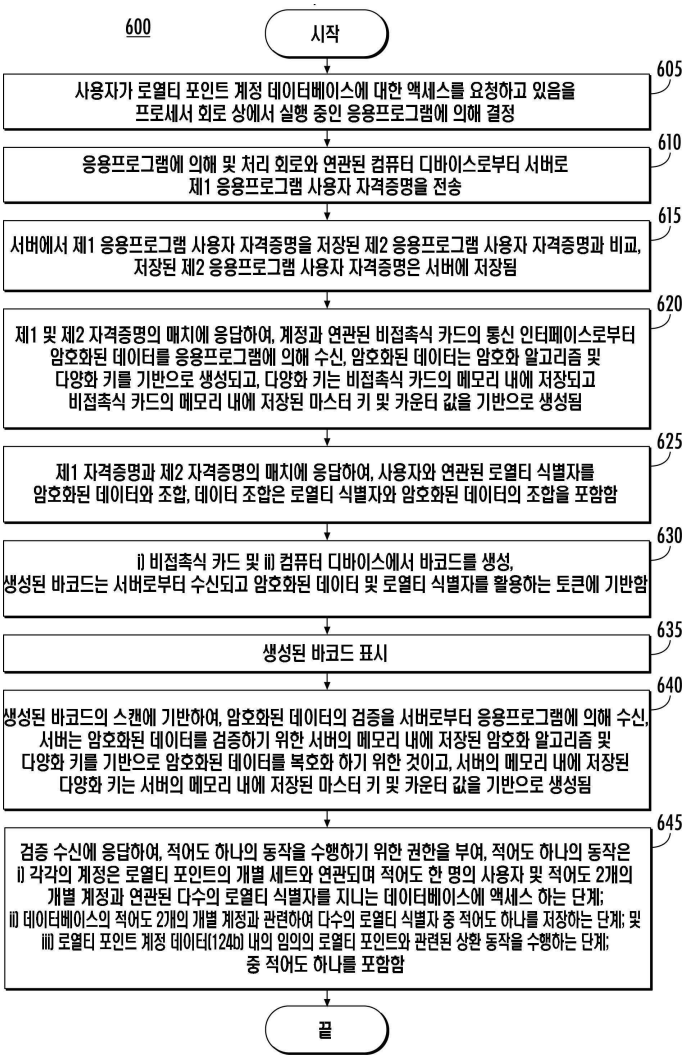
도면4b


420
455
425
프로세서
430
메모리 102
애플릿 440
바코드 생성
응용프로그램 117
카운터 104
고객 ID 107
계좌 번호 108

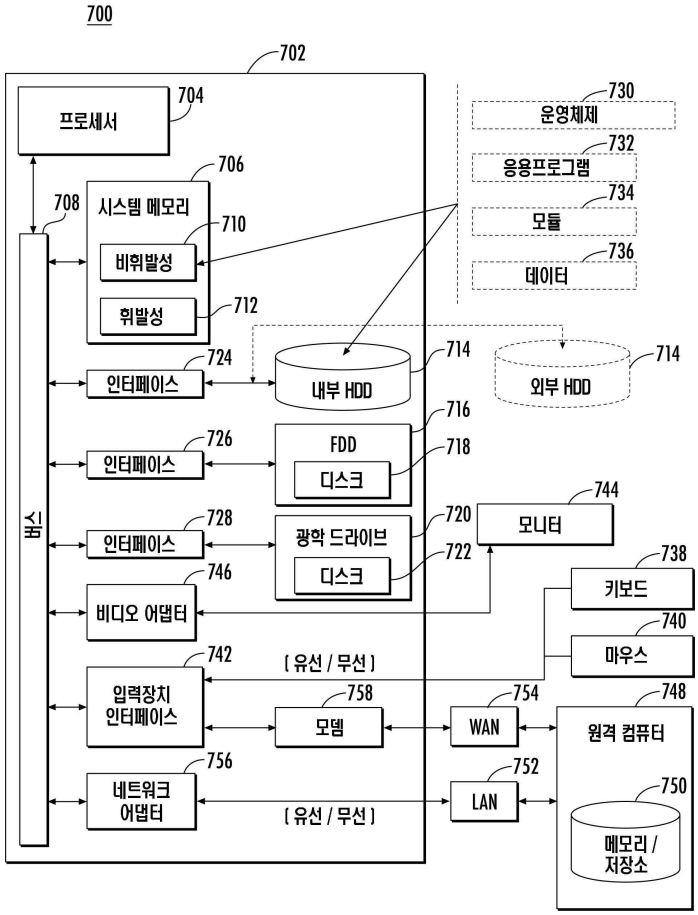
도면5


500
시작
505
로열티 포인트 트랜잭션 개시
510
비접촉식 카드가 암호화된 데이터를 전송하도록 모바일 디바이스에 비접촉식 카드를 탭
515
다양화 키를 생성하기 위해 마스터 키 및 암호화 알고리즘을 사용하여
카운터 값을 비접촉식 카드에 의해 암호화
520
다양화 키 및 암호화 알고리즘을 사용하여 데이터를 비접촉식 카드에 의해 암호화
525
암호화된 데이터를 모바일 디바이스로 비접촉식 카드에 의해 전송
530
암호화된 데이터를 서버로 모바일 디바이스에 의해 전송
535
다양화 키를 생성하기 위해 마스터 키 및 암호화 알고리즘을 사용하여
카운터 값을 서버에 의해 복호화
540
비접촉식 카드로부터 수신된 암호화된 데이터를 다양화 키 및 암호화 알고리즘을 사용하여
서버에 의해 복호화
545
모바일 디바이스를 통해 비접촉식 카드로부터 수신된 암호화된 데이터를 서버에 의해 검증
550
검증에 응답하여 로열티 포인트 액세스 또는 활용과 관련된 동작 수행
끝

도면6


600
시작
605
사용자가 로열티 포인트 계정 데이터베이스에 대한 액세스를 요청하고 있음을 프로세서 회로 상에서 실행 중인 응용프로그램에 의해 결정
610
응용프로그램에 의해 및 처리 회로와 연관된 컴퓨터 디바이스로부터 서버로 제1 응용프로그램 사용자 자격증명을 전송
615
서버에서 제1 응용프로그램 사용자 자격증명을 저장된 제2 응용프로그램 사용자 자격증명과 비교, 저장된 제2 응용프로그램 사용자 자격증명은 서버에 저장됨
620
제1 및 제2 자격증명의 매치에 응답하여, 계정과 연관된 비접촉식 카드의 통신 인터페이스로부터 암호화된 데이터를 응용프로그램에 의해 수신, 암호화된 데이터는 암호화 알고리즘 및 다양화 키를 기반으로 생성되고, 다양화 키는 비접촉식 카드의 메모리 내에 저장되고 비접촉식 카드의 메모리 내에 저장된 마스터 키 및 카운터 값을 기반으로 생성됨
625
제1 자격증명과 제2 자격증명의 매치에 응답하여, 사용자와 연관된 로열티 식별자를 암호화된 데이터와 조합, 데이터 조합은 로열티 식별자와 암호화된 데이터의 조합을 포함함
630
i) 비접촉식 카드 및 ii) 컴퓨터 디바이스에서 바코드를 생성, 생성된 바코드는 서버로부터 수신되고 암호화된 데이터 및 로열티 식별자를 활용하는 토큰에 기반함
635
생성된 바코드 표시
640
생성된 바코드의 스캔에 기반하여, 암호화된 데이터의 검증을 서버로부터 응용프로그램에 의해 수신, 서버는 암호화된 데이터를 검증하기 위한 서버의 메모리 내에 저장된 암호화 알고리즘 및 다양화 키를 기반으로 암호화된 데이터를 복호화 하기 위한 것이고, 서버의 메모리 내에 저장된 다양화 키는 서버의 메모리 내에 저장된 마스터 키 및 카운터 값을 기반으로 생성됨
645
검증 수신에 응답하여, 적어도 하나의 동작을 수행하기 위한 권한을 부여, 적어도 하나의 동작은 i) 각각의 계정은 로열티 포인트의 개별 세트와 연관되며 적어도 한 명의 사용자 및 적어도 2개의 개별 계정과 연관된 다수의 로열티 식별자를 지니는 데이터베이스에 액세스 하는 단계; iii) 데이터베이스의 적어도 2개의 개별 계정과 관련하여 다수의 로열티 식별자 중 적어도 하나를 저장하는 단계; 및 iii) 로열티 포인트 계정 데이터(124b) 내의 임의의 로열티 포인트와 관련된 상환 동작을 수행하는 단계; 중 적어도 하나를 포함함
끝

도면7


700
702
프로세서
704
706
시스템 메모리
708
710
비휘발성
휘발성
712
730
운영체제
732
응용프로그램
734
모듈
736
데이터
714
내부 HDD
714
외부 HDD
716
FDD
718
디스크
720
광학 드라이브
722
디스크
724
인터페이스
726
인터페이스
728
인터페이스
744
모니터
738
키보드
740
마우스
746
비디오 어댑터
742
입력장치 인터페이스
[유선 / 무선]
758
모뎀
754
WAN
748
원격 컴퓨터
752
LAN
750
메모리 / 저장소
756
네트워크 어댑터
[유선 / 무선]
버스