(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0124913
(43) 공개일자 2024년08월19일

(51) 국제특허분류(Int. Cl.)
G06Q 20/36 (2012.01) *G06Q 20/32* (2012.01)
G06Q 20/34 (2012.01) *G06Q 20/38* (2012.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
G06Q 20/3672 (2020.05)
G06Q 20/3226 (2013.01)
(21) 출원번호 10-2024-7019242
(22) 출원일자(국제) 2022년11월23일
심사청구일자 없음
(85) 번역문제출일자 2024년06월10일
(86) 국제출원번호 PCT/US2022/050885
(87) 국제공개번호 WO 2023/113986
국제공개일자 2023년06월22일
(30) 우선권주장
17/551,670 2021년12월15일 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
프라사드, 자이키스한
미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680, 캐피탈 원 서비시즈, 엘엘씨 내
카탈라 카스텔라, 조세
미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680, 캐피탈 원 서비시즈, 엘엘씨 내
(74) 대리인
김동완

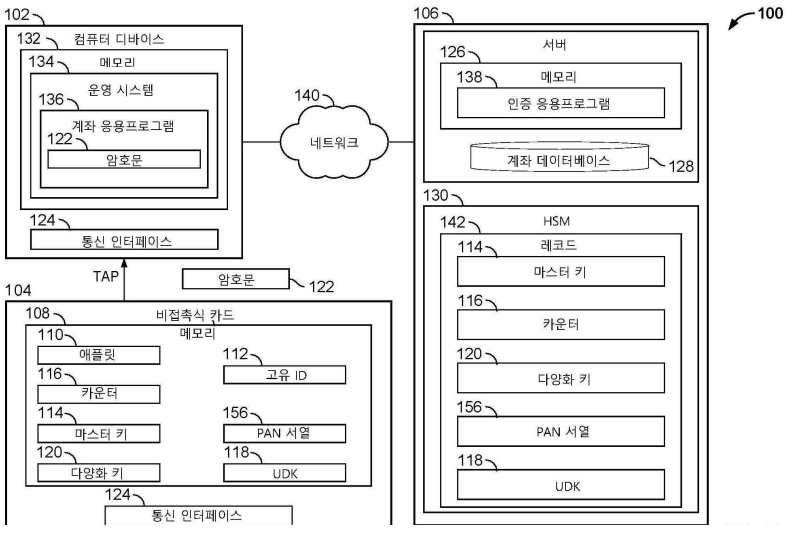
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **비접촉식 카드 인증 기반의 키 복구**

(57) 요 약

비접촉식 카드 암호 기반 키 복구를 위한 시스템, 방법, 장치 및 컴퓨터 판독 가능 매체에 관한 것이다. 서버는 응용프로그램으로부터 디지털 지갑에 대한 개인 키를 복구하라는 요청을 수신할 수 있으며, 요청에는 비접촉식 카드에 의해 생성된 제1 암호가 포함된다. 서버는 비접촉식 카드의 키를 기반으로 제1 암호를 복호화 할 수 있다. 서버는 복호화에 기초하여 비접촉식 카드의 고유 식별자와 디지털 지갑 과 관련된 다양화 인자를 결정할 수 있다. 서버는 고유 식별자와 다양화 인자를 기반으로 개인 키를 생성할 수 있다. 서버는 네트워크를 통해 개인 키를 응용프로그램에 전송할 수 있다.

대 표 도 - 도1a



(52) CPC특허분류
G06Q 20/341 (2013.01)
G06Q 20/343 (2013.01)
G06Q 20/352 (2013.01)
G06Q 20/3674 (2013.01)
G06Q 20/3829 (2013.01)
H04L 9/0819 (2013.01)
H04L 9/0866 (2013.01)
H04L 9/0869 (2013.01)
H04L 9/0897 (2013.01)

명 세 서

청구범위

청구항 1

비접촉식 카드에 의해 생성된 제1 암호를 포함하는, 디지털 지갑의 개인 키를 복구하라는 요청을 응용프로그램으로부터 서버에 의해 수신하는 단계;

비접촉식 카드를 위한 키에 기반하여 제1 암호를 서버에 의해 복호화하는 단계;

비접촉식 카드의 고유 식별자 및 디지털 지갑과 관련된 다양화 인자를 복호화에 기반하여 서버에 의해 결정하는 단계;

고유식별자와 다양화 인자를 기반으로 서버에 의해 개인키를 생성하는 단계; 및

네트워크를 통해 응용프로그램에 서버에 의해 개인 키를 전송하는 단계;

를 포함하는 방법.

청구항 2

제1항에 있어서, 상기 다양화 인자는 비접촉식 카드의 응용프로그램 기본 계정 번호(PAN) 시퀀스 번호를 포함함을 특징으로 하는 방법.

청구항 3

제1항에 있어서, 상기 다양화 인자는 비접촉식 카드의 응용프로그램 거래 카운터(ATC)를 포함함을 특징으로 하는 방법.

청구항 4

제1항에 있어서, 요청을 수신하기 전에,

비접촉식 카드에 의해 생성된 제2 암호를 응용프로그램으로부터 서버에 의해 수신하는 단계;

제2 암호를 서버에 의해 복호화 하는 단계;

제2 암호의 복호화에 기반하여 서버에 의해 개인 키를 생성하는 단계;

개인 키에 기반하여 공개 키를 생성하고, 공개 키에 기반하여 디지털 지갑에 대한 지갑 주소를 서버에 의해 생성하는 단계; 및

개인키, 공개키, 지갑 주소를 응용프로그램에 서버에 의해 전송하는 단계;

를 더욱 포함하는 방법.

청구항 5

제4항에 있어서, 상기 비접촉식 카드의 고유 식별자 및 다양화 인자는 디지털 지갑의 지갑 주소에 기반하여 결정됨을 특징으로 하는 방법.

청구항 6

제5항에 있어서, 제1 암호의 복호화에 기반하여 디지털 지갑의 지갑 주소를 생성하는 단계를 더 포함하는 방법.

청구항 7

제1항에 있어서, 상기 서버는 디지털 지갑과 관련된 설트(salt) 값을 더 결정하고, 서버는 설트 값에 기반하여 개인 키를 더 생성하며,

상기 방법은,

개인 키를 기반으로 한 응용프로그램에 의해 디지털 지갑에 액세스하는 단계를 더 포함함을 특징으로 하는 방법.

청구항 8

디바이스의 프로세서에 의해 실행되는 명령어를 포함하는 비-일시적 컴퓨터 판독가능 저장 매체에 있어서,

상기 프로세서는

비접촉식 카드에 의해 생성된 제1 암호를 포함하는, 디지털 지갑의 개인 키를 복구하라는 요청을 응용프로그램으로부터 수신하고;

비접촉식 카드를 위한 키에 기반하여 제1 암호를 복호화하고;

비접촉식 카드의 고유 식별자 및 디지털 지갑과 관련된 다양화 인자를 복호화에 기반하여 결정하고;

고유식별자와 다양화 인자를 기반으로 개인키를 생성하고; 및

네트워크를 통해 응용프로그램에 개인 키를 전송;

을 유도하는 비-일시적 컴퓨터 판독가능 저장 매체.

청구항 9

제8항에 있어서, 상기 다양화 인자는 비접촉식 카드의 응용프로그램 기본 계정 번호(PAN) 시퀀스 번호 포함함을 특징으로 하는 비-일시적 컴퓨터 판독가능 저장 매체.

청구항 10

제8항 있어서, 상기 다양화 인자는 비접촉식 카드의 응용프로그램 거래 카운터(ATC)를 포함함을 특징으로 하는 비-일시적 컴퓨터 판독가능 저장 매체.

청구항 11

제8항에 있어서, 요청을 수신하기 전에, 상기 프로세서는

비접촉식 카드에 의해 생성된 제2 암호를 응용프로그램으로부터 수신하고;

제2 암호를 복호화 하고;

제2 암호의 복호화에 기반하여 개인 키를 생성하고;

개인 키에 기반하여 공개 키를 생성하고, 공개 키에 기반하여 디지털 지갑에 대한 지갑 주소를 생성하고; 및

개인키, 공개키, 지갑 주소를 응용프로그램에 전송;

하도록 더욱 유도함을 특징으로 하는 비-일시적 컴퓨터 판독가능 저장 매체.

청구항 12

제11항에 있어서, 상기 비접촉식 카드의 고유 식별자 및 다양화 인자는 디지털 지갑의 지갑 주소에 기반하여 결정됨을 특징으로 하는 비-일시적 컴퓨터 판독가능 저장 매체.

청구항 13

제12항에 있어서, 상기 프로세서는 제1 암호의 복호화에 기반하여 디지털 지갑의 지갑 주소를 생성하도록 더욱 유도함을 특징으로 하는 비-일시적 컴퓨터 판독가능 저장 매체.

청구항 14

제8항에 있어서, 상기 프로세서는 디지털 지갑과 관련된 설트(salt) 값을 더 결정하고, 프로세서는 설트 값에 기반하여 개인 키를 더 생성함을 특징으로 하는 비-일시적 컴퓨터 판독가능 저장 매체.

청구항 15

프로세서; 및

프로세서에 의해 실행되는 명령어를 저장한 메모리; 를 포함하는 컴퓨터 장치에 있어서,

상기 프로세서는

비접촉식 카드에 의해 생성된 제1 암호를 포함하는, 디지털 지갑의 개인 키를 복구하라는 요청을 응용프로그램으로부터 수신하고;

비접촉식 카드를 위한 키에 기반하여 제1 암호를 복호화하고;

비접촉식 카드의 고유 식별자 및 디지털 지갑과 관련된 다양화 인자를 복호화에 기반하여 결정하고;

고유식별자와 다양화 인자를 기반으로 개인키를 생성하고; 및

네트워크를 통해 응용프로그램에 개인 키를 전송;

을 유도하는 컴퓨터 장치.

청구항 16

제15항에 있어서, 상기 다양화 인자는 비접촉식 카드의 응용프로그램 기본 계정 번호(PAN) 시퀀스 번호 포함함을 특징으로 하는 컴퓨터 장치.

청구항 17

제15항 있어서, 상기 다양화 인자는 비접촉식 카드의 응용프로그램 거래 카운터(ATC)를 포함함을 특징으로 하는 컴퓨터 장치.

청구항 18

제15항에 있어서, 요청을 수신하기 전에, 상기 프로세서는

비접촉식 카드에 의해 생성된 제2 암호를 응용프로그램으로부터 수신하고;

제2 암호를 복호화 하고;

제2 암호의 복호화에 기반하여 개인 키를 생성하고;

개인 키에 기반하여 공개 키를 생성하고, 공개 키에 기반하여 디지털 지갑에 대한 지갑 주소를 생성하고; 및

개인키, 공개키, 지갑 주소를 응용프로그램에 전송;

하도록 더욱 유도함을 특징으로 하는 컴퓨터 장치.

청구항 19

제18항에 있어서, 상기 비접촉식 카드의 고유 식별자 및 다양화 인자는 디지털 지갑의 지갑 주소에 기반하여 결정되고,

상기 프로세서는 제1 암호의 복호화에 기반하여 디지털 지갑의 지갑 주소를 생성하도록 더욱 유도함을 특징으로 하는 컴퓨터 장치.

청구항 20

제15항에 있어서, 상기 프로세서는 디지털 지갑과 관련된 설트(salt) 값을 더 결정하고, 프로세서는 설트 값에 기반하여 개인 키를 더 생성함을 특징으로 하는 컴퓨터 장치.

발명의 설명

기 술 분 야

[0001] 본 출원은 2021년 12월 15일에 출원된 "비접촉식 카드 인증 기반의 키 복구"라는 발명의 명칭의 미국 특허 출원 일련 번호 제17/551,670호에 대한 우선권을 주장한다. 전술한 출원의 내용은 그 전체가 참조로 본 명세서에 포

함된다.

배 경 기 술

[0002] 디지털 지갑은 수많은 장점을 갖고 있지만 보안 및 개인 정보 보호 문제를 지니고 있다. 가장 일반적인 위험에는 도난, 액세스 키 분실 또는 잃어버린 경우가 있다. 게다가 수탁 지갑은 특정 기관에 묶여 있어 이동성을 허용하지 않는다. 프록시 지갑은 보안 위반 및/또는 도난의 위험이 있어 액세스 키가 손상될 수 있다. 하드웨어 지갑은 복구 시드를 제공할 수 있지만 이러한 시드는 도난 및/또는 기타 유형의 예를 들면 사용자가 시드를 기억할 수 없거나 시드 기록을 찾을 수 없는 경우 손실이 발생하기 쉽다

발명의 내용

과제의 해결 수단

[0003] 비접촉식 카드 인증에 기초한 키 복구를 위한 시스템, 방법, 장치 및 컴퓨터 판독 가능 매체에 관한 것이다. 하나의 측면에서, 방법은 응용프로그램 으로부터 서버에 의해 디지털 지갑에 대한 개인 키를 복구하라는 요청을 수신하는 단계를 포함하며, 요청은 비접촉식 카드에 의해 생성된 제1 암호를 포함하고, 서버에 의해 제1 암호를 복호화한다. 비접촉식 카드에 대한 키에 기초하여 서버에 의한 복호화에 기초하여 비접촉식 카드의 고유 식별자 및 하드웨어 보안 모듈의 디지털 지갑과 관련된 다양화 인자를 결정하고, 서버에 의해 고유한 식별자에 기초하여 생성 식별자와 다양화 인자, 개인 키 및 서버가 네트워크를 통해 응용프로그램에 개인 키를 전송한다.

도면의 간단한 설명

[0004] 임의의 특정 엘레멘트 또는 행위에 대한 설명을 쉽게 식별하기 위해, 참조 번호의 최상위 숫자는 해당 엘레멘트가 처음 소개되는 도면의 번호를 나타낸다.

도 1a는 하나의 실시형태에 따른 주제의 측면을 도시한 것이다.

도 1b는 하나의 실시형태에 따른 주제의 측면을 도시한 것이다.

도 1c는 하나의 실시형태에 따른 주제의 측면을 도시한 것이다.

도 2a는 하나의 실시형태에 따른 주제의 측면을 도시한 것이다.

도 2b는 하나의 실시형태에 따른 주제의 측면을 도시한 것이다.

도 2c는 하나의 실시형태에 따른 주제의 측면을 도시한 것이다.

도 2d는 하나의 실시형태에 따른 주제의 측면을 도시한 것이다.

도 3a는 하나의 실시형태에 따른 주제의 측면을 도시한 것이다.

도 3b는 하나의 실시형태에 따른 주제의 측면을 도시한 것이다.

도 4는 하나의 실시형태에 따른 루틴(400)을 도시한 것이다.

도 5는 하나의 실시형태에 따른 루틴(500)을 도시한 것이다.

도 6는 하나의 실시형태에 따른 루틴(600)을 도시한 것이다.

도 7a는 하나의 실시형태에 따른 비접촉식 카드를 도시한 것이다.

도 7b는 하나의 실시형태에 따른 비접촉식 카드(104)를 도시한 것이다.

도 8은 하나의 실시형태에 따른 데이터 구조(800)를 도시한 것이다.

도 9은 하나의 실시형태에 따른 시스템(900)의 실시형태를 도시한 것이다.

도 10은 하나의 실시형태에 따른 논리 모델(1000)의 실시형태를 도시한 것이다.

도 11은 하나의 실시형태에 따른 논리 모델(1100)의 실시형태를 도시한 것이다.

도 12은 하나의 실시형태에 따른 컴퓨터 아키텍처(1200)를 도시한 것이다.

발명을 실시하기 위한 구체적인 내용

[0005] 본 명세서에 개시된 실시형태는 비접촉식 카드를 사용하여 암호화폐 지갑과 같은 디지털 지갑에 액세스하는 데 사용되는 암호화 키를 안전하게 복구하기 위한 기술을 제공한다. 디지털 지갑을 생성하기 위해 컴퓨터 디바이스는 비접촉식 카드에 지시하여 암호를 생성할 수 있다. 컴퓨터 디바이스에서 실행되는 응용프로그램은 비접촉식 카드와의 무선 통신을 통해 암호를 수신하고 확인을 위해 서버에 암호를 전송할 수 있다. 서버가 암호를 확인하면 서버는 디지털 지갑을 사용하여 액세스하거나 작업을 수행하는 데 필요한 개인 키를 생성할 수 있다. 이에 따라 서버는 개인 키에 대응하는 공개 키를 생성하고 공개 키를 기반으로 디지털 지갑에 대한 지갑 주소를 생성할 수 있다. 그런 다음 서버는 하드웨어 보안 모듈(HSM)에서 개인 키를 생성하는 데 사용되는 암호화 알고리즘에 대한 하나 이상의 입력을 저장할 수 있다. 입력은 비접촉식 카드와 연관된 키, 비접촉식 카드의 고유 식별자 및 다양화 인자 중 하나 이상을 포함할 수 있다.일부 실시형태에서, 키는 HSM에 저장될 수 있는 반면, 고유 식별자 및 다양화 인자는 개인 키를 다양화하기 위해 HSM에 대한 입력으로 제공될 수 있다.예를 들어, 고유 식별자 및 다양화 인자는 HSM에 저장될 필요가 없다.

[0006] 서버는 개인 키, 공개 키 및 지갑 주소를 응용프로그램에 안전하게 전송할 수 있으며, 응용프로그램은 디지털 지갑을 생성하고 개인 키, 공개 키 및 지갑 주소를 저장할 수 있다. 일부 실시형태에서 사용자가 디지털 지갑에 액세스하려고 시도할 때, 비접촉식 카드를 사용한 암호화 확인이 디지털 지갑에 대한 액세스를 인증하는 데 사용될 수 있다. 암호 화폐 검증에 실패할 경우 사용자의 지갑 접근이 제한될 수 있어 지갑의 보안이 향상될 수 있다.

[0007] 디지털 지갑은 개인 키의 난독화 버전을 저장하기 때문에 사용자는 디지털 지갑과의 거래 예를 들면 암호화폐 전송 등을 수행하기 위한 전제 조건으로 개인 키를 분실 또는 잊어버리거나 제공하지 못할 수 있다. 유리하게도 본 명세서내에 개시된 실시형태는 비접촉식 카드를 사용하여 개인 키를 복구하는 보안 솔루션을 제공한다. 일반적으로 개인 키를 복구하기 위해 비접촉식 카드는 서버에서 확인되는 암호를 생성할 수 있다. 서버가 암호를 확인할 수 있는 경우 개인 키를 생성하는 데 사용된 입력이 HSM에 제공될 수 있다. 그런 다음 서버는 개인 키를 다시 생성하고 다시 생성된 개인 키를 요청하는 응용프로그램 및/또는 장치에 하나 이상의 부분으로 전송할 수 있다.

[0008] 유리하게도 본 명세서내에 개시된 실시형태는 비접촉식 카드에 의해 생성된 암호를 사용하여 디지털 지갑에 액세스하는 데 사용되는 개인 키를 복구하는 보안 기술을 제공한다. 암호를 활용함으로써 본 개시 내용의 실시형태는 사기 행위의 위험을 최소화하면서 사용자의 신원을 안전하게 확인할 수 있다. 또한 이렇게 하면 사용자가 서버의 암호화 확인을 용이하게 하는 비접촉식 카드에 액세스할 수 있는 경우에만 개인 키가 복원된다. 더욱이, 디지털 지갑에 접근하거나 개인 키를 복구하기 위한 전제 조건으로 암호화 검증을 요구함으로써 디지털 지갑의 보안이 강화된다.

[0009] 본 명세서에 사용된 표기법 및 명명법을 일반적으로 참조하면, 본 명세서의 상세한 설명은 컴퓨터 또는 컴퓨터 네트워크에서 실행되는 프로그램 절차의 관점에서 제시될 수 있다. 이러한 절차적 설명 및 표현은 당업자가 자신의 작업 내용을 다른 당업자에게 효과적으로 전달하기 위해 사용된다. 여기서 절차는 일반적으로 원하는 결과를 가져오는 일관된 동작 시퀀스로 간주된다. 이러한 작업은 물리량의 물리적 조작이 필요한 작업이다. 반드시 그런 것은 아니지만 일반적으로 이러한 양은 저장, 전송, 결합, 비교 및 기타 조작이 가능한 전기, 자기 또는 광학 신호의 형태를 취한다.

[0010] 주로 일반적인 사용법으로 인해 이러한 신호를 비트, 값, 요소, 기호, 문자, 용어, 숫자 등으로 참조하는 것이 편리한 경우가 있다. 그러나 이러한 용어 및 유사한 용어는 모두 적절한 물리적 수량과 연관되어야 하며 해당 수량에 적용되는 편리한 라벨일 뿐이라는 점에 유의해야 한다. 또한 수행되는 조작은 종종 추가 또는 비교와 같은 용어로 지칭되며, 이는 일반적으로 인간 조작자에 의해 수행되는 정신적 작업과 연관되어 있다. 하나 이상의 실시형태의 일부를 형성하는 본 명세서에 설명된 작업 중 대부분의 경우 인간 조작자의 그러한 능력은 필요하지 않거나 바람직하지 않는다. 오히려 작업은 기계 작업이다. 다양한 실시형태의 동작을 수행하는 데 유용한 기계에는 디지털 컴퓨터 또는 유사한 장치가 포함된다.

[0011] 일부 실시형태는 "결합된" 및 "연결된"이라는 표현과 그 파생어를 사용하여 설명될 수 있다. 이러한 용어는 반드시 서로 동의어로 사용되는 것은 아니다. 예를 들어, 일부 실시형태는 2개 이상의 요소가 서로 직접적인 물리적 또는 전기적 접촉을 이루고 있음을 나타내기 위해 "연결된" 및/또는 "결합된"이라는 용어를 사용하여 설명될 수 있다. 그러나 "결합된"이라는 용어는 둘 이상의 요소가 서로 직접 접촉하지 않지만 여전히 서로 협력하거나

상호 작용한다는 것을 의미할 수도 있다.

[0012] 다양한 실시형태는 또한 이들 동작을 수행하기 위한 장치 또는 시스템에 관한 것이다. 이 장치는 필요한 목적을 위해 특별히 형상화될 수 있거나 컴퓨터에 저장된 컴퓨터 프로그램에 의해 선택적으로 활성화되거나 재구성되는 컴퓨터로 형상화될 수 있다. 본 명세서내에 제시된 절차는 본질적으로 특정 컴퓨터나 기타 장치와 관련이 없다. 다양한 기계는 본 명세서의 교시 내용에 따라 작성된 프로그램과 함께 사용될 수 있으며, 필요한 방법 단계를 수행하기 위해 보다 특수한 장치를 구성하는 것이 편리할 수도 있다. 이러한 다양한 기계에 필요한 구조는 주어진 설명에서 나타낸다.

[0013] 이제 도면을 참조하며, 여기서 유사한 참조 번호는 전체적으로 유사한 요소를 지칭하는 데 사용된다. 다음의 설명에서는, 설명의 목적으로, 이에 대한 철저한 이해를 제공하기 위해 다양한 특정 세부 사항이 제시된다. 그러나, 신규한 실시형태는 이러한 특정 세부사항 없이도 실행될 수 있다. 다른 경우에, 구조 및 장치는 설명을 용이하게 하기 위해 블록도 형식으로 표시된다. 이는 청구된 주제와 일치하는 모든 수정, 등가물 및 대안을 포괄하는 것이다.

[0014] 도면 및 첨부된 설명에서, 지정 "a", "b" 및 "c" 및 유사한 지정자는 임의의 양의 정수를 나타내는 변수로 의도된다. 따라서, 예를 들어, 구현이 a = 5에 대한 값을 설정하는 경우, 컴포넌트 123-1 내지 123-a 또는 123a로 도시된 완전한 컴포넌트 세트(123)는 컴포넌트 123-1, 123-2, 123-1을 포함할 수 있다. 3, 123-4, 123-5. 실시형태는 이러한 맥락으로 제한되지 않는다.

[0015]

[0016] 도 1a는 개시된 실시형태에 따른 시스템이라고도 불리는 예시적인 컴퓨터 아키텍처 (100)를 도시한다. 도 1a 내지 도 1c에 도시된 컴퓨터 아키텍처(100)는 특정 토폴로지에서 제한된 수의 요소를 갖지만, 컴퓨터 아키텍처(100)는 주어진 구현에 대해 원하는 대로 대체 토폴로지에서 더 많거나 더 적은 요소를 포함할 수 있다는 것이 이해될 수 있다.

[0017] 컴퓨터 아키텍처(100)는 하나 이상의 컴퓨터 디바이스(102), 하나 이상의 서버(106) 및 하나 이상의 비접촉식 카드(104)를 포함한다. 비접촉식 카드(104)는 신용 카드, 직불 카드, ATM 카드, 기프트 카드, 결제 카드, 스마트 카드 등이다. 비접촉식 카드(104)는 통신 인터페이스(124) 또한 본 명세서에서 "카드 판독기", "무선 카드 판독기"와 통신하도록 구성된 무선 주파수 식별(RFID) 칩과 및/또는 NFC, EMV 표준, 또는 무선 통신의 다른 단거리 프로토콜을 통한 컴퓨터 디바이스 (102)의 "무선 통신 인터페이스" 같은 하나 이상의 통신 인터페이스(124)를 포함할 수 있다. NFC가 본 명세서에서 예시적인 통신 프로토콜로 사용되었지만, 본 개시 내용은 EMV 표준, 블루투스 및/또는 Wi-Fi와 같은 다른 유형의 무선 통신에도 동일하게 적용 가능하다.

[0018] 컴퓨터 디바이스(102)는 스마트폰, 태블릿 컴퓨터, 웨어러블 장치, 랩톱, 휴대용 게임 장치, 가상화 컴퓨터 시스템, 판매자 단말기, POS 시스템, 서버, 데스크톱 컴퓨터 등. 모바일 장치는 컴퓨터 디바이스(102)의 예로서 사용될 수 있지만, 본 개시를 제한하는 것으로 간주되어서는 안 된다. 서버(106)는 서버, 워크스테이션, 컴퓨터 클러스터, 클라우드 컴퓨터 플랫폼, 가상화 컴퓨터 시스템 등과 같은 임의 유형의 컴퓨터 디바이스를 대표한다.명확성을 위해 도시되지는 않았지만, 컴퓨터 디바이스(102), 비접촉식 카드(104) 및 서버(106) 각각은 예를 들어 프로그램, 코드 및/또는 명령을 실행하기 위한 하나 이상의 프로세서 회로를 포함한다.

[0019] 도시된 바와 같이, 비접촉식 카드(104)의 메모리(108)는 애플릿(110), 카운터(116), 하나 이상의 마스터 키(114), 하나 이상의 다양화 키(120), 고유 ID(112), 기본 계정 번호(PAN) 시퀀스(156) 하나 이상의 고유 파생 키(UDK)(118)를 포함한다. 고유 ID(112)는 다른 비접촉식 카드(104)에 대해 비접촉식 카드(104)를 고유하게 식별 하는 임의의 식별자일 수 있다. PAN 시퀀스(156)는 비접촉식 카드(104)에 의해 저장된 카운터 값을 포함할 수 있다. 애플릿(110)은 일부 또는 전부를 수행하도록 구성된 실행 가능한 코드이다. 여기에 설명된 작업 중 하나이다. 카운터(116)는 비접촉식 카드(104)와 서버(106) 사이에서 동기화되는 값이다. 카운터(116)는 비접촉식 카드(104)와 서버(106) 및/또는 비접촉식 카드(104)와 컴퓨터 디바이스 (102) 사이에서 데이터가 교환될 때마다 변경되는 숫자를 포함할 수 있다. 카운터 (116), 마스터 키(114), 다양화 키(120), UDK(118), PAN 시퀀스(156) 및/또는 고유 ID(112)는 아래에서 더 자세히 설명되는 것처럼 시스템(100)에 보안을 제공하는 데 사용된다.

[0020] 도시된 바와 같이, 컴퓨터 디바이스(102)의 메모리(132)는 운영 체제(134)의 인스턴스를 포함한다. 예시적인 운영 체제는 Android® OS, iOS®, macOS®, Linux® 및 Windows® 운영 체제를 포함한다. 도시 된 바와 같이, 운영 체제 (134)는 계정 응용프로그램(136)을 포함한다. 계정 응용프로그램(136)은 사용자가 디지털 지갑 관리, 지갑을 사용한 거래 처리, 블록체인 및/또는 암호화폐 거래 처리, 결제 카드 활성화, 계정 잔액 보기, 품목 구

매, 결제 처리 등과 같은 다양한 계정 관련 작업을 수행할 수 있게 해준다. 일부 실시형태에서 사용자는 계정 응용프로그램(136)의 특정 기능에 액세스하기 위해 인증 자격 증명을 사용하여 인증할 수 있다. 예를 들어, 인증 자격 증명에는 사용자 이름 또는 로그인 및 비밀번호, 생체 인식 자격 증명 예를 들면 지문, Face ID 등이 포함될 수 있다. 도시 된 바와 같이, 서버(106)의 메모리(126)는 인증 응용프로그램(138) 및 계정 데이터베이스(128)를 포함한다. 계정 데이터베이스 (128)는 일반적으로 계정 소유자 예를 들어, 한 명 이상의 사용자, 하나 이상의 계정 계정 보유자 및 계정의 하나 이상의 비접촉식 카드(104)와 관련된 정보를 포함한다

[0021] 언급된 바와 같이, 계정 응용프로그램(136)은 디지털 지갑을 생성, 관리, 액세스 또는 달리 사용하는 데 사용될 수 있다. 디지털 지갑을 사용하면 한 당사자가 다른 당사자와 전자 거래를 할 수 있다. 일부 실시형태에서, 디지털 지갑은 암호화폐에 대한 개인 키 및/또는 공개 키를 저장하는 암호화폐 지갑이다. 암호화폐는 비트코인, 이더리움 등과 같은 모든 유형의 암호화폐일 수 있다. 디지털 지갑을 만들기 위해 사용자는 인증 자격 증명을 사용하여 계정을 인증할 수 있다. 그러면 계정 응용프로그램(136)은 사용자에게 비접촉식 카드(104)를 컴퓨터 디바이스 (102)에 탭 하라고 지시할 수 있다.

[0022] 도 1a에 도시된 실시형태에서, 사용자는 비접촉식 카드(104)를 컴퓨터 디바이스 (102)에 탭 할 수 있다(또는 그렇지 않으면 비접촉식 카드(104)를 장치(102)의 통신 인터페이스(124)의 통신 범위 내로 가져올 수 있다). 그러면 계정 응용프로그램 (136)은 애플릿(110)에 암호(122)를 생성하도록 지시할 수 있다. 암호122)는 임의의 적절한 암호 기법에 기초하여 생성될 수 있다. 일부 실시형태에서 암호(122)는 비접촉식 카드(104)의 고유 ID(112)에 기초할 수 있다. 일부 실시형태에서 애플릿(110)은 암호(122)를 포함하는 데이터 패키지의 일부로서 암호(122) 및 암호화되지 않은 식별자 예를 들어, 카운터(116), PAN 시퀀스(156), 고유 ID(112) 및/또는 임의의 다른 고유 식별자를 포함할 수 있다. 적어도 일 실시형태에서 데이터 패키지는 NDEF 파일이다.

[0023] 언급된 바와 같이, 컴퓨터 아키텍처(100)는 데이터를 보호하기 위해 키 다양화를 구현하도록 구성되며, 이는 본 명세서에서 키 다양화 기술로 지칭될 수 있다. 일반적으로, 서버(106)(또는 다른 컴퓨터 디바이스) 및 비접촉식 카드(104)에는 동일한 마스터 키(114)(마스터 대칭 키라고도 함)가 제공될 수 있다. 보다 구체적으로, 각각의 비접촉식 카드(104)는 서버(106)의 하드웨어 보안 모듈(HSM) (130)에 대응하는 쌍을 갖는 별개의 마스터 키(114)로 프로그래밍 된다.

[0024] 예를 들어, 비접촉식 카드(104)가 제조될 때, 고유 마스터 키(114)는 비접촉식 카드(104)의 메모리(108)에 프로그래밍 될 수 있다. 마찬가지로, 고유 마스터 키(114)는 HSM(130)의 레코드(142)에 저장될 수 있다.

[0025] 또한, 주어진 카드(104)가 제조될 때, UDK(118)는 다양화 인자 및 HSM(130)의 마스터 키(114) 인덱스 예를 들어, 레코드 (142)에 대한 색인에 대한 참조를 입력으로 취하는 HSM 기능을 통해 마스터 키(114)로부터 다양화될 수 있다. 일부 실시형태에서, 다양화 인자는 비접촉식 카드(104)의 고유 ID(112) 및 PAN 시퀀스 (156)일 수 있다. UDK(118)는 비접촉식 카드(104) 및 HSM(130)의 레코드(142)에 저장될 수 있다. 마스터 키(114) 및 UDK(118)는 비접촉식 카드(104) 및 서버(106) 이외의 모든 당사자로부터 비밀로 유지될 수 있으며, 그에 따라 시스템(100)의 보안을 강화한다. 레코드(142)에 저장되는 것으로 도시되어 있지만, 일부 실시형태에서는 카운터(116) 및 /또는 PAN 시퀀스(156)는 HSM(130)에 저장되지 않는다. 예를 들어, 고유 ID(112), 카운터(116) 및 PAN 시퀀스(156)는 계정 데이터베이스(128)에 저장될 수 있다.

[0026] 일부 실시형태에서, 암호(122)를 생성하기 위해, 애플릿(110)은 UDK(118), 고유 ID(112) 및 암호화 알고리즘에 대한 입력으로서 다양화 인자를 제공하여 다양화 키(120)를 생성할 수 있다. 요소는 카운터 (116)이다. 다른 실시형태에서, PAN 시퀀스(156)는 다양화 인자이다. 그러면 다양화된 키(120)는 다양화 인자 예를 들어, 카운터(116) 및/또는 PAN 시퀀스(156)또는 다른 민감한 데이터와 같은 일부 데이터를 암호화하는 데 사용될 수 있다. 애플릿(110)과 서버(106)는 암호의 복호화 및/또는 검증 처리를 용이하게 하기 위해 동일한 유형의 데이터를 암호화하도록 형상화될 수 있다.

[0027] 언급된 바와 같이, 비접촉식 카드(104) 및 서버(106)의 UDK(118)는 키 다양화를 사용하여 보안을 강화하기 위해 카운터(116)와 함께 사용될 수 있다. 언급된 바와 같이, 카운터(116)는 비접촉식 카드(104)와 서버(106) 사이에서 동기화되는 값을 포함한다. 카운터(116)는 비접촉식 카드(104)와 서버(106)(및/또는 비접촉식 카드(104)와 컴퓨터 디바이스(102)) 사이에서 데이터가 교환될 때마다 변경되는 숫자를 포함할 수 있다. 예를 들어, 서버(106) 및/또는 장치(102)로 데이터 전송을 준비할 때, 비접촉식 카드(104)의 애플릿(110)은 카운터(116)를 증가시킬 수 있다.

[0028] 비접촉식 카드(104)의 애플릿(110)은 UDK(118), 고유 ID(112) 및 카운터(116)를 암호화 알고리즘에 대한 입력으

로 제공할 수 있으며, 이는 출력으로서 다양화 키(120)를 생성한다. 암호 알고리즘에는 암호화 알고리즘, 해시 기반 메시지 인증 코드(HMAC) 알고리즘, Cipher-기반 메시지인증 코드(CMAC) 알고리즘 등이 포함될 수 있다. 암호화 알고리즘의 비제한적인 예에는 3DES 또는 AES107과 같은 대칭 암호화 알고리즘; HMAC-SHA-256과 같은 대칭 HMAC 알고리즘; AES-CMAC와 같은 대칭 CMAC 알고리즘이 있다. 주요 다양화 기술의 예는 2018년 11월 29일에 출원된 미국 특허 출원 제16/205,119호에 더 자세히 설명되어 있다. 전술한 특허 출원은 그 전체가 참조로서 본 명세서에 포함된다. 일부 실시형태에서, PAN 시퀀스(156)는 예를 들어 UDK(118), 고유 ID(112) 및 PAN 시퀀스(156)를 암호화함으로써 다양화 키(120)를 생성하기 위해 카운터(116) 대신 암호화 알고리즘에 대한 입력으로 사용된다.

[0029] 그러면 애플릿(110)은 다양화된 키(120) 및 데이터를 애플릿(110)에 대한 입력으로 사용하여 일부 데이터(예를 들어, 고유 ID(112), 카운터(116), PAN 시퀀스(156), 명령 및/또는 기타 데이터)를 암호화할 수 있다. 암호화 알고리즘. 예를 들어, 다양화된 키(120)로 고유 ID(112)를 암호화하면 암호화된 고유 ID(112) 예를 들어, 암호(122)가 생성될 수 있다. 언급한 바와 같이, 애플릿(110)과 서버(106)는 동일한 데이터를 암호화하도록 형상화될 수 있다.

[0030] 일부 실시형태에서, 예를 들어 암호화 기능에 대한 입력의 하나 이상의 부분에 기초하여 두 개의 다양화 키(120)가 생성될 수 있다. 일부 실시형태에서, 2개의 다양화 키(120)는 2개의 별개의 마스터 키(114), 2개의 별개의 UDK(118), 고유 ID(112) 및 카운터(116)(또는 PAN 시퀀스(156))에 기초하여 생성된다. 이러한 실시형태에서, 메시지 인증 코드(MAC)는 다양화된 키(120) 중 하나를 사용하여 생성되고, MAC는 다양화된 키(120) 중 다른 하나를 사용하여 암호화될 수 있다. MAC는 민감한 데이터, 고유 ID(112), 카운터(116) 및/또는 PAN 시퀀스(156)와 같은 MAC 알고리즘에 입력된 임의의 적절한 데이터에 기초하여 생성될 수 있다.

[0031] 더 일반적으로, 애플릿(110)과 서버(106)는 동일한 데이터에 기초하여 MAC를 생성하도록 형상화될 수 있다. 일부 실시형태에서, 암호(122)는 NDEF 파일과 같은 데이터 패키지에 포함된다. 그러면 계정 응용프로그램(136)은 컴퓨터 디바이스 (102)의 통신 인터페이스(124)를 통해 암호(122)를 포함하는 데이터 패키지를 판독할 수 있다.

[0032] 도 1b는 계정 응용프로그램(136)이 암호(122)를 서버(106)에 전송하는 실시형태를 도시한다. 서버(106)는 서버(106)에 의해 저장된 마스터 키(114) 및/또는 UDK(118)의 인스턴스에 적어도 부분적으로 기초한 검증을 위해 인증 응용프로그램 (138) 및/또는 HSM(130)에 암호(122)를 제공할 수 있다. 일부 실시형태에서, 인증 응용프로그램(138) 및/또는 HSM(130)은 서버(106)에 제공된 암호화되지 않은 고유 ID(112)를 사용하여 UDK(118)(또는 마스터 키(114)) 및 카운터(116)를 식별할 수 있다. PAN 시퀀스(156)가 암호(122)를 생성하는 데 사용되는 예에서, 서버(106)는 암호화되지 않은 고유 ID(112)를 사용하여 계정 데이터베이스(128) 및/또는 HSM(130)에서 PAN 시퀀스(156)를 식별할 수 있다.

[0033] 일부 실시예에서, 인증 응용프로그램(138)은 출력으로 하나 이상의 다양화 키(120)를 생성하는 HSM(130)의 암호화 기능에 대한 입력으로 UDK(118), 고유 ID(112) 및 카운터(116)를 제공할 수 있다. 다른 실시형태에서, 서버는 UDK(118), 고유 ID(112) 및 PAN 시퀀스(156)를 암호화하여 다양화 키(120)를 생성한다. 결과적인 다양화 키(120)는 암호를 복호화하는 데 사용될 수 있는 비접촉식 카드(104)의 다양화 키(120)에 대응할 수 있다. 암호(122) 및/또는 일단 복호화된 MAC를 검증한다. 예를 들어, 서버(106)는 애플릿(110)과 동일한 데이터, 예를 들어 민감 데이터, 고유 ID(112), 카운터(116) 및/또는 PAN 시퀀스(156)에 기초하여 MAC를 생성할 수 있다. 서버(106)에 의해 생성된 MAC가 암호(122)의 복호화된 MAC와 일치하는 경우, 서버(106)는 암호(122)를 검증하거나 인증할 수 있다.

[0034] 사용된 복호화 기술에 관계없이, 인증 응용프로그램(138) 및/또는 HSM (130)은 암호(122)를 성공적으로 복호화하고 MAC를 검증함으로써 암호(122)를 검증 또는 인증할 수 있다. 복호화 및/또는 MAC 검증이 성공하면 인증 응용프로그램 (138) 및/또는 HSM(130)은 사용자를 위한 디지털 지갑(144)을 생성할 수 있다. 일반적으로 디지털 지갑(144)을 생성하기 위해 개인 키(146)가 생성될 수 있다. 일부 실시형태에서, 임의의 길이의 개인 키(146)를 생성하기 위해 SHA-2 알고리즘 또는 임의의 다른 적합한 알고리즘과 같은 암호화(Or 해시) 알고리즘에 대한 입력으로 난수가 제공된다. 다른 실시형태에서, 비접촉식 카드(104)의 고유 ID(112)와 PAN 시퀀스(156)는 연결되어 해시 알고리즘에 대한 입력으로 제공되어 개인 키(146)를 생성한다. 다른 실시형태에서, 비접촉식 카드(104)의 고유 ID(112)와 PAN 시퀀스(156)는 카운터(116)는 연결되어 해시 알고리즘에 대한 입력으로 제공되어 개인 키(146)를 생성한다.

[0035] 다른 실시형태에서, 마스터 키(114), 고유 ID(112) 및 비접촉식 카드(104)의 카운터(116)는 연결되어 해시 알고리즘에 대한 입력으로 제공되어 개인 키(146)를 생성한다. 개인 키(146)를 생성하는 데 사용되는 경우, 비접촉

식 카드(104)의 제1 마스터 키(114)는 암호(122)를 생성하는 데 사용될 수 있고, 비접촉식 카드(104)의 제2 마스터 키(114)는 개인 키(146)를 생성하는 데 사용될 수 있다. 제1 및 제2 마스터 키(114)는 별개의 키이다. 다른 실시형태에서, 다양화 키(120) 중 하나, 고유 ID(112), 및 비접촉식 카드(104)의 카운터(116)가 연결되어 해시 알고리즘에 대한 입력으로 제공되어 개인 키(146)를 생성한다. 다른 실시형태에서, UDK(118), 고유 ID(112) 및 비접촉식 카드(104)의 카운터(116) 중 하나가 연결되어 해시 알고리즘에 대한 입력으로 제공되어 개인 키(146)를 생성한다. 키(146)에 따르면, 일부 실시형태에서는 개인 키(146)를 생성하기 위해 해시 알고리즘에 대한 입력에 설트 예를 들면 무작위 데이터가 포함된다.

[0036] 그 후, 개인 키(146)는 대응하는 공개 키(148)를 생성하는 데 사용될 수 있다. 일부 실시형태에서, 공개 키(148)는 타원 곡선 디지털 서명 알고리즘 (ECDSA)을 사용하여 개인 키(146)에 기초하여 생성될 수 있다. 일부 실시형태에서, 공개 키(148)는 예를 들어 해시 알고리즘을 사용하여 연결(또는 압축)될 수 있다. 일부 실시형태에서, 공개 키(148)를 생성하기 위해 설트가 사용된다. 예를 들어 공개 키(148)를 해싱함으로써 공개 키(148)에 기초하여 디지털 지갑(144)에 대한 지갑 주소(150)가 생성될 수 있다. HSM(130)에 저장되는 것으로 도시되어 있지만, 일부 실시형태에서 디지털 지갑(144)은 HSM(130)에 영구적으로 저장되지 않는다. 대신, 본 명세서에 더 자세히 설명된 바와 같이, 개인 키(146)를 재생성 하는 데 사용되는 요소는 HSM (130) 및/또는 계정 데이터베이스(128)에 저장될 수 있다. 예를 들어, 고유 ID(112) 및 카운터(116)는 HSM(130) 및/또는 계정 데이터베이스(128)에 저장될 수 있다.

[0037] 다른 실시예에서, 고유 ID(112) 및 PAN 시퀀스(156)는 HSM(130) 및/또는 계정 데이터베이스(128)에 저장될 수 있다. 일부 실시형태에서, 개인 키(146) 및/또는 공개 키(148)는 예를 들어 계층적 결정론적 키를 생성하기 위해 더욱 다양화될 수 있다. 예를 들어, 개인 키(146)는 카운터(116), 고유 ID(112), 설트 값(154), 또는 임의의 다른 미리 결정된 시드 값으로 다양화될 수 있다. 그렇게 하면 개인 키(146) 가 다양화될 수 있다. 유사하게, 공개 키(148)는 카운터(116), 고유 ID(112), 설트 값(154), 또는 임의의 다른 미리 결정된 시드 값으로 다양화되어 다양한 공개 키 (148)를 생성할 수 있다. 즉, 개인 키(146) 및/또는 공개 키(148)를 다양화하는 데 사용되는 임의의 시드 값은 계정 데이터베이스(128) 및/또는 HSM(130)의 복구 레코드(152)에 저장될 수 있다.

[0038] 보다 일반적으로 개인 키(146) 및/또는 공개 키(148)는 시드 값을 여러 번 사용하여 다양화될 수 있으며, 이에 따라 다양한 개인 키(146) 및/또는 다양한 공개 (148)의 트리 또는 계층 구조가 생성된다. 이러한 실시형태에서, 트리 또는 계층 구조의 하나 이상의 경로는 서로 다른 다양화 키를 지정하는 데 사용될 수 있다. 보다 일반적으로, 트리의 각 노드는 다양한 공개 키 및/또는 다양한 하위 키에 대응할 수 있다. 트리 노드의 개인 키와 공개 키가 주어지면 트리의 모든 하위 노드의 다양한 개인 키와 공개 키가 파생될 수 있다. 또한 트리의 각 리프 노드는 다양한 공개 키 및/또는 다양한 하위 키에 대응할 수 있다. 일부 실시형태에서, 경로는 통화, 통화 금액, 거래에 대한 제1 지갑 주소 예를 들면 송신 지갑 주소, 거래에 대한 제2 지갑 주소 예를 들면 수신자 지갑 주소와 같은 거래에 대한 속성 또는 다른 속성을 지정하는 데 추가로 사용된다. 이러한 속성은 트리의 특정 노드에 저장될 수 있다.

[0039] 복호화로 돌아가서, 인증 응용프로그램(138)이 암호(122)를 복호화 할 수 없는 경우 및/또는 MAC를 확인할 수 없는 경우 인증 응용프로그램(138)은 암호(122)를 검증 하지 않는다. 인증 응용프로그램(138)은 디지털 지갑 생성을 자제하기로 결정한다. 인증 응용프로그램(138)은 실패한 복호화 및/또는 검증의 표시를 컴퓨터 디바이스(102)에 전송할 수 있다.

[0040] 도 1c는 인증 응용프로그램(138)이 디지털 지갑(144)을 컴퓨터 디바이스(102)로 전송하는 실시형태를 도시한다. 도시된 바와 같이, 계정 응용프로그램(136)은 디지털 지갑(144)을 명확성을 위해 도시되지 않은 메모리(132) 및/또는 비휘발성 저장소에 저장할 수 있다. 디지털 지갑에는 개인 키(146), 공개 키(148) 및 지갑 주소(150)가 포함된다. 계정 응용프로그램(136)은 개인 키(146), 공개 키(148) 및/또는 지갑 주소(150)를 해시 또는 암호화하거나, 달리 난독화 할 수 있다.

[0041] 계정 응용프로그램(136)은 사용자 이름 및/또는 비밀번호, 생체인식 자격 증명 등과 같은 인증 제어를 통해 디지털 지갑(144)을 보호할 수 있다. 추가적으로 및/또는 대안으로, 계정 응용프로그램(136)은 비접촉식 암호 복호화 및/또는 인증을 요구할 수 있다. 카드(104)를 사용하여 디지털 지갑(144)에 액세스한다. 예를 들어, 비접촉식 카드(104)는 본 명세서에 설명된 바와 같이 서버(106)에 의해 확인되는 암호를 생성한다. 게다가, 일부 실시형태에서, 계정 응용프로그램(136)은 디지털 지갑(144)에 액세스하고/하거나 디지털 지갑(144)을 사용하여 작업을 수행하기 위해 개인 키(146)를 제공하도록 사용자에게 요구할 수 있다. 보다 일반적으로, 계정 응용프로그램(136)은 디지털 지갑(144)에 액세스하거나 사용하거나 관리하기 위한 인터페이스의 다양한 기능을 제공할 수

있다.

[0042] 일부 실시형태에서, 디지털 지갑(144)은 클라우드 기반 지갑, 예를 들어 서버(106) 또는 클라우드 기반 지갑 서비스를 클라이언트에 제공하는 다른 컴퓨터 시스템에 저장될 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다. 클라우드 기반 지갑은 예를 들어 계정 응용프로그램(136)을 통해 디지털 지갑(144)에 액세스하거나 다른 방식으로 사용하기 위한 인터페이스를 제공할 수 있다.

[0043] 도시된 바와 같이, 서버(106)는 디지털 지갑(144)의 생성에 기초하여 계정 데이터베이스(128)에 복구 기록(152)을 생성한다. 복구 레코드(152)는 개인 키(146) 를 생성하기 위해 고유 ID(112), 다양화 인자(158)(예를 들어, 카운터(116) 및/또는 PAN 시퀀스(156)) 및 임의의 설트(154)(사용된 경우)를 포함한다. 일부 실시형태 에서 복구 레코드(152)는 지갑(144)의 지갑 주소(150)에 기초하여 인덱싱 될 수 있다. 다른 실시형태에서 복구 레코드(152)는 비접촉식 카드(104)의 키를 저장하는 HSM(130)의 레코드(142)에 기초하여 인덱싱 될 수 있다. 다른 실시형태에서, 복구 기록(152)은 비접촉식 카드(104)의 고유 ID(112)에 기초하여 인덱싱 된다. 그런 다음 복구 레코드(152)는 예를 들어 고유 ID(112), 다양화 인자(158) 및/또는 설트(154) 및 적절한 알고리즘에 기초하여 개인 키(146)를 재생성 하는 데 사용될 수 있다. 다양화 키(120), UDK(118) 또는 마스터 키(114)가 개인 키(146)를 생성하는 데 사용되는 실시형태에서, 보안을 향상시키기 위해 다양화된 키(120), UDK(118) 또는 마스터 키(114)는 복구 레코드(152)에 저장되지 않는 것이 유리 한다.이러한 실시형태에서, HSM(130)은 개인 키(146)를 재생성하는 데 사용되는 마스터 키(114), UDK(118) 및/또는 다양화 키(120)를 저장할 수 있다. 고유 ID (112), 다양화 인자(158) 및/또는 설트(154)는 계정 데이터베이스(128)에 저장될 수 있다.

[0044] 도 2a는 사용자가 개인 키(146) 복구를 요청하는 실시형태를 도시하는 개략도 (200)이다. 도시된 바와 같이, 개인 키(146)를 복구하기 위해, 계정 응용프로그램 (136)은 사용자에게 비접촉식 카드(104)를 컴퓨터 디바이스(102)에 탭 하라고 지시할 수 있으며, 이는 비접촉식 카드(104)가 암호(208)를 생성하게 한다. 암호(208)는 암호(122)를 참조하여 전술한 바와 같이 생성될 수 있다. 예를 들어, 애플릿(110)은 카운터(116)를 증가시키고 하나 이상의 UDK(118), 고유 ID(112) 및 카운터(116)를 암호화하여 하나 이상의 다양화 키(120)를 생성할 수 있다. 하나 이상의 다양화 키(120)는 일부 데이터에 기초하여 MAC를 생성하고 MAC 및/또는 데이터를 암호화하는 데 사용될 수 있다. 일부 실시형태에서, MAC는 지갑 주소(150) 및 다양화 키(120) 중 하나에 기초하여 생성된다. 이러한 실시형태에서, 지갑 주소(150) 및 MAC는 암호화(208)를 생성하기 위해 다양화 키(120) 중 다른 하나를 사용하여 암호화된다. 다른 실시예로서, 공개 키(148)는 MAC을 생성하는 데 사용될 수 있고, 공개 키(148)는 MAC으로 암호화할 수 있다.

[0045] 도 2b는 계정 응용프로그램(136)이 검증을 위해 서버(106)에 암호(208)를 전송하는 실시형태를 도시한다. 일반적으로, 서버(106)는 카운터(116)를 증가시키고 UDK (118), 고유 ID(112) 및 비접촉식 카드(104)의 카운터(116)를 암호화하여 비접촉식 카드(104)에 의해 생성된 키에 대응하는 하나 이상의 다양화 키(120)를 생성할 수 있다. 하나 이상의 다양화된 키(120)는 암호(208)를 복호화하고 및/또는 MAC를 검증하는 데 사용될 수 있다.

[0046] 서버(106)가 암호(208)를 복호화하고/하거나 MAC를 검증할 수 있는 경우, 서버(106)는 복구 기록(152)에 기초하여 개인 키(146)를 재생성 할 수 있다.

[0047] 지갑 주소(150)가 암호(208)로 암호화되는 실시형태에서, 복구 기록(152)은 지갑 주소(150)에 기초하여 인덱싱(예를 들어, 검색)될 수 있고, 서버(106)는 복호화된 지갑 주소(150)를 사용하여 복구 기록(152)에 액세스할 수 있다.

[0048] 공개 키(148)가 암호(208)로 암호화되는 실시형태에서, 서버(106)는 공개 키(148)를 사용하여 지갑 주소(150)를 재생성하고, 재생성 된 지갑 주소(150)를 사용하여 계정 데이터베이스(128)를 인덱싱할 수 있다.

[0049] 다른 실시형태에서, 계정 데이터베이스(128)는 복구 기록(152)을 식별하기 위해 고유 ID(112)를 사용하여 인덱싱된다. 이러한 실시형태에서, 고유 ID(112)는 암호(208)에 포함된 고유 ID(112)의 암호화되지 않은 버전에 기초하여 결정된다.

[0050] 서버(106)가 복구 레코드(152)를 식별하면, 복구 레코드(152)는 개인 키(146)를 재생성 하는 데 사용될 수 있다. 예를 들어, 복구 레코드(152)의 고유 ID(112), 다양화 인자(158) 및 설트(154)사용된 경우는 개인 키(146)를 초기에 생성하는 데 사용되는 HSM(130)의 기능에 대한 입력으로 제공될 수 있다. 그렇게 하면 개인 키(146)이 다시 생성된다.

[0051] 일부 실시형태에서, 서버(106)는 마스터 키(114) 또는 UDK(118)에 기초하여 개인 키(146)를 추가로 재생성한다. 예를 들어 서버(106)는 비접촉식 카드(104)의 마스터 키(114) 및 복구 데이터를 제공할 수 있다. 개인 키

(146)를 생성하는 데 사용되는 HSM(130) 기능에 대한 입력으로 레코드(152)(예: 고유 ID(112), 다양화 요소(158) 및 임의의 설트(154))를 기록한다. 그렇게 하면 개인 키(146)가 재생성 된다. 또 다른 실시예로서, 서버(106)는 비접촉식 카드(104)의 UDK(118) 및 복구 기록(152)의 데이터 예를 들어, 고유 ID(112), 다양화 인자(158) 및 임의의 설트(154)를 제공할 수 있다. 개인 키(146)를 생성하는 데 사용되는 HSM(130)의 기능에 대한 입력으로 사용된다. 그렇게 하면 개인 키(146)도 다시 생성된다.

[0052] 일부 실시형태에서, UDK(118), 고유 ID(112), 다양화 인자(158) 및 임의의 설트 (154)는 개인 키(146)를 생성하는 데 사용되는 다양화된 키(120)를 생성하기 위해 HSM(130)의 기능에 입력된다. 다양화 인자(158) 및 임의의 설트(154)가 개인 키 (146)를 재생성하기 위해 HSM(130)의 기능에 대한 입력으로 제공될 수 있다.

[0053] 반면에 HSM(130)이 암호(122)를 복호화할 수 없고 및/또는 MAC를 검증할 수 없는 경우 HSM(130)은 암호(122)를 검증하지 않는다. 이러한 실시예에서 인증 응용프로그램 (138)은 개인 키(146)를 복구하지 않기로 결정한다. 인증 응용프로그램(138)은 실패한 암호 복호화 및/또는 MAC 검증의 표시를 컴퓨터 디바이스(102)에 전송할 수 있다. 이러한 실시형태에서, 사용자는 복구 기록(152)을 사용하여 개인 키(146)를 복구하는 것이 제한된다.

[0054] 도 2c는 HSM(130)이 복구 레코드(152)에 기초하여 개인 키(146)를 재생성하고 개인 키(146)를 계정 응용프로그램(136)으로 전송하는 실시형태를 묘사한다.일부 실시형태에서 서버(106)는 하나 이상의 데이터 부분으로 개인 키(146)를 전송할 수 있다. 보다 일반적으로, 서버(106)는 컴퓨터 디바이스(102)와의 보안 연결을 사용하여 개인 키(146)를 전송할 수 있다.그러면 컴퓨터 디바이스(102)는 개인 키(146)를 표시하여 사용자가 개인 키(146)를 복구할 수 있게 한다.그런 다음 사용자는 개인 키(146)를 사용하여 디지털 지갑(144) 및/또는 디지털 지갑(144)과 연관된 임의의 암호화폐를 사용하여 하나 이상의 작업을 수행할 수 있다.예를 들어, 개인 키(146)는 블록체인(906)에서 트랜잭션을 생성하는 데 사용될 수 있다.

[0055] 일부 실시형태에서, 개인 키(146)는 컴퓨터 디바이스(102)로 전송되지 않는다. 예를 들어, 클라우드 기반 지갑 실시형태에서, 개인 키(146)는 거래 또는 다른 유형의 데이터에 서명하는 데 사용될 수 있다. 이러한 실시예에서, 사용자는 계정 인증 자격증명을 사용하여 계정 응용프로그램(136)에서 자신의 계정을 인증하고 의도된 거래 예를 들면 구매, 암호화폐 전송 등의 세부정보를 제공할 수 있다. 계정 응용프로그램(136)은 거래 세부사항을 서버(106)에 제공할 수 있다. 일부 실시형태에서, 계정 응용프로그램(136)은 거래 세부사항을 암호 및/또는 암호를 포함하는 데이터 패키지로 제공한다. 암호는 암호(122) 및/또는 암호(208)와 유사할 수 있다. 그런 다음 서버(106)는 복구 레코드(152) 예를 들어 고유 ID(112), 카운터(116), PAN 시퀀스(156) 및/또는 설트(154)로부터 키를 다양화하는 데 사용되는 데이터를 검색할 수 있다. 복구 레코드(152)로부터의 데이터는 복구 레코드 및 마스터 키(114) 및/또는 UDK(118)로부터의 데이터를 사용하여 거래에 대한 디지털 서명을 생성하는 HSM(130)에 제공될 수 있다. 이를 통해 거래에 필요한 서명이 생성된다. 예를 들어, 유효한 서명을 생성함으로써 거래는 공개 키(148)를 사용하여 검증될 수 있다. 이러한 실시예에서, 검증된 거래를 반영하기 위해 거래가 블록체인에 추가될 수 있다.

[0056] 도 3a는 예를 들어 개인 키(146)를 복구하기 위해 비접촉식 카드(104)가 컴퓨터 디바이스(102)에 탭핑 되는 실시형태를 도시하는 개략도(300a)이다. 언급된 바와 같이, 비접촉식 카드(104)가 컴퓨터 디바이스(102)에 탭 될 때, 애플릿(110)은 암호 예를 들어, 암호(122) 및/또는 암호(208)를 생성할 수 있다. 암호 및 임의의 다른 데이터(예를 들어, 암호화되지 않은 고유 ID(112))는 컴퓨터 디바이스(102)에 의해 판독되는 NDEF 파일과 같은 데이터 패키지에 포함될 수 있다. 그 후 컴퓨터 디바이스(102)는 본 명세서에 설명된 바와 같이 확인 예를 들어, 복호화 및/또는 MAC 확인을 위해 서버(106)에 암호를 전송할 수 있다.

[0057] 도 3b는 서버(106)가 도 3a에서 생성된 암호를 검증한 실시형태를 도시하는 개략도(300b)이다. 검증에 기초하여, 서버(106)는 복구 기록(152)에 기초하여 개인 키(146)를 재생성 할 수 있다. 그 후, 서버(106)는 개인 키(146)를 계정 응용프로그램(136)으로 전송할 수 있다. 도시된 바와 같이, 계정 응용프로그램 (136)은 개인 키(146)를 문자열로서 디스플레이 상에 표시할 수 있다. 일부 실시형태에서 개인 키(146)를 나타내기 위해 매트릭스 코드(302)가 생성될 수 있다. 그렇게 하면 매트릭스 코드(302)가 스캔 되어 개인 키(146)를 결정할 수 있게 된다.

[0058] 개시된 실시형태에 대한 동작은 다음 도면을 참조하여 더 설명될 수 있다. 일부 그림에는 논리 흐름이 포함될 수 있다. 여기에 제시된 이러한 도면은 특정 논리 흐름을 포함할 수 있지만, 논리 흐름은 단지 여기에 설명된 일반적인 기능이 구현될 수 있는 방법의 예를 제공한다는 것이 이해될 수 있다. 또한, 주어진 논리 흐름은 달리 명시되지 않는 한 반드시 제시된 순서대로 실행될 필요는 없다. 더욱이, 일부 실시형태에서는 논리 흐름에 예시된 모든 행위가 요구되지 않을 수도 있다. 또한, 주어진 논리 흐름은 하드웨어 요소, 프로세서에 의해 실행되는

소프트웨어 요소, 또는 이들의 임의의 조합에 의해 구현될 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다.

[0059] 도 4는 논리 흐름 또는 루틴(400)의 실시형태를 도시한다. 논리 흐름(400)은 여기에 설명된 하나 이상의 실시형태에 의해 실행되는 동작 중 일부 또는 전부를 나타낼 수 있다. 예를 들어, 논리 흐름(400)은 디지털 지갑을 생성하기 위한 동작의 일부 또는 전부를 포함할 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다.

[0060] 블록(402)에서 서버(106)는 컴퓨터 디바이스(102)에서 실행되는 계정 응용프로그램 (136)으로부터 디지털 지갑을 생성하라는 요청을 수신할 수 있다. 요청은 비접촉식 카드(104)에 의해 생성되어 컴퓨터 디바이스(102)로 전송되는 암호를 포함할 수 있다. 블록(404)에서 서버는 마스터 키(114), UDK(118) 및 카운터(116)에 기초하여 하나 이상의 다양화 키(120)를 생성함으로써 암호를 복호화할 수 있다. 서버(106)는 또한 암호를 검증할 수 있는데, 예를 들어 서버(106)에 의해 생성된 MAC가 복호화된 암호의 MAC와 일치하는지 결정할 수 있다.

[0061] 블록 (406)에서, 서버(106)는 블록 404에서의 성공적인 암호 복호화 및/또는 암호 검증에 기초하여 개인 키(146)를 생성한다. 개인 키(146)는 HSM(130)의 암호화 기능에 대한 입력에 기초할 수 있다. 입력은 고유 ID(112) 및 다양화 인자(158) 예를 들어, 비접촉식 카드(104)의 카운터(116) 및/또는 PAN 시퀀스(156)를 포함할 수 있다. 일부 실시형태에서, 입력은 마스터 키(114), UDK(118) 및/또는 다양화 키(120)를 더 포함할 수 있다. 블록 (408)에서, 서버(106)는 개인 키(146)에 기초하여 공개 키(148)를 생성할 수 있다. 서버는 공개 키(148)에 기초하여 디지털 지갑(144)에 대한 지갑 주소(150)를 추가로 생성할 수 있다. 블록 (410)에서, 서버는 응용프로그램에 개인 키(146), 공개 키(148) 및 지갑 주소(150)를 전송할 수 있다. 블록 412에서, 서버(106)는 계정 데이터베이스(128) 예를 들어 고유 ID(112) 및 다양화 인자(158)에 개인 키를 생성하는 데 사용되는 하나 이상의 입력을 저장한다.

[0062] 도 5는 논리 흐름 또는 루틴(500)의 실시형태를 도시한다. 논리 흐름(500)은 여기에 설명된 하나 이상의 실시형태에 의해 실행되는 동작 중 일부 또는 전부를 나타낼 수 있다. 예를 들어, 논리 흐름(500)은 디지털 지갑에 액세스하기 위한 동작 중 일부 또는 전부를 포함할 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다.

[0063] 블록(502)에서, 루틴(500)은 서버(106)에 의해 컴퓨터 디바이스(102)에서 실행되는 계정 응용프로그램(136)으로부터 디지털 지갑(144)에 액세스하라는 요청을 수신하며, 이 요청은 암호를 포함한다.블록(504)에서, 서버(106)는 마스터 키(114), UDK(118) 및 카운터(116)에 기초하여 하나 이상의 다양화 키(120)를 생성함으로써 암호를 복호화할 수 있다.서버(106)는 또한 암호를 검증할 수 있는데, 예를 들어 서버(106)에 의해 생성된 MAC가 복호화된 암호의 MAC와 일치하는지 결정할 수 있다. 블록 506에서, 서버는 성공적인 복호화 및 검증에 기초하여 인증을 생성할 수 있다. 승인은 일반적으로 디지털 지갑(144)에 대한 요청된 액세스가 허용된다는 것을 나타낼 수 있다. 블록 508에서, 서버는 인증을 계정 응용프로그램(136)에 전송한다. 승인은 계정 응용프로그램(136)이 디지털 지갑(144)에 대한 요청된 액세스를 허용하게 할 수 있다. 그러나 일부 실시형태에서는 디지털 지갑(144)에 액세스하기 위해 개인 키(146)가 더 필요하다.

[0064] 도 6은 논리 흐름 또는 루틴(600)의 실시형태를 도시한다. 논리 흐름(600)은 여기에 설명된 하나 이상의 실시형태에 의해 실행되는 동작 중 일부 또는 전부를 나타낼 수 있다. 예를 들어, 논리 흐름(600)은 디지털 지갑에 대한 개인 키를 복구하기 위한 동작 중 일부 또는 전부를 포함할 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다.

[0065] 블록(602)에서, 루틴(600)은 서버(106)에 의해 계정 응용프로그램(136)으로부터 디지털 지갑(144)에 대한 개인 키(146)를 복구하라는 요청을 수신한다.

[0066] 요청은 키 다양화에 기초하여(예를 들어, 마스터 키(114), UDK(118) 및 하나 이상의 다양화된 키(120)에 기초함) 비접촉식 카드(104)에 의해 생성된 암호를 포함할 수 있다. 블록(604)에서, 서버(106)는 마스터 키(114), UDK(118) 및 카운터(116)에 기초하여 하나 이상의 다양화 키(120)를 생성함으로써 암호를 복호화할 수 있다. 서버(106)는 암호를 추가로 검증할 수 있는데, 예를 들어 MAC가 서버(106)에 의해 생성된 서버는 복호화된 암호의 MAC와 일치한다.

[0067] 블록(606)에서, 서버(106)는 복호화 및 검증에 기초하여 계정 데이터베이스(128) 내에서 비접촉식 카드(104)의 고유 ID(112) 및 다양화 인자(158) 예를 들어, 카운터(116) 및/또는 PAN 시퀀스(156)를 결정할 수 있다. 블록(608)에서 서버(106) 는 고유 ID(112), 다양화 인자(158) 및 임의의 설트(154)를 기반으로 개인 키(146) 를 재생성 한다. 일부 실시형태에서, 서버(106)는 마스터 키(114), 고유 ID(112), 다양화 인자(158) 및 임의의 설트(154)에 기초하여 개인 키(146)를 재생성 한다. 일부 실시형태에서, 서버(106)는 UDK(118), 고유 ID(112), 다

양화 인자(158) 및 임의의 설트(154)를 기반으로 개인 키(146)를 재생성 한다. 일부 실시형태에서, 서버(106)는 다양화 키(120), 고유 ID(112), 다양화 인자(158) 및 임의의 설트 (154)에 기초하여 개인 키(146)를 재생성 한다. 블록(610)에서, 서버(106)는 재생성 된 개인 키(146)를 네트워크를 통해 계정 응용프로그램(136)으로 전송한다.

[0068] 도 7a는 전면 또는 비접촉식 카드 뒷면(104)에 서비스 제공자 표시(702)로서 디스플레이 되는 바와 같이 서비스 제공자에 의해 발행된 신용 카드, 직불 카드 또는 기프트 카드와 같은 지불 카드를 포함할 수 있는 비접촉식 카드(104)의 예시적인 구성을 도시하는 개략도(700)이다. 일부 실시예에서, 비접촉식 카드 (104)는 결제 카드와 관련이 없으며, 신분증을 포함할 수 있지만 이에 국한되지는 않는다. 일부 실시예에서, 거래 카드는 듀얼 인터페이스 비접촉식 지불 카드, 보상 카드 등을 포함할 수 있다. 비접촉식 카드(104)는 플라스틱, 금속 및 기타 재료로 구성된 단일 층 또는 하나 이상의 적층 층을 포함할 수 있는 기판(704)을 포함할 수 있다. 예시적인 기판 재료에는 폴리염화비닐, 폴리염화비닐 아세테이트, 아크릴로니트릴 부타디엔 스티렌, 폴리카보네이트, 폴리에스테르, 양극산화 티타늄, 팔라듐, 금, 탄소, 종이 및 생분해성 재료가 포함된다. 일부 실시예에서, 비접촉식 카드(104)는 ISO/IEC 7816 표준의 ID-1 형식을 준수하는 물리적 특성을 가질 수 있고, 거래 카드는 ISO/IEC 14443 표준을 준수할 수 있다. 그러나, 본 발명에 따른 비접촉식 카드(104)는 다른 특성을 가질 수 있으며, 본 개시는 거래 카드가 결제 카드에 구현될 것을 요구하지 않는다는 것이 이해된다.

[0069] 비접촉식 카드(104)는 또한 카드의 앞면 및/또는 뒷면에 표시된 식별 정보(706) 및 접촉 패드(708)를 포함할 수 있다.접촉 패드(708)는 하나 이상의 패드를 포함할 수 있고, 거래 카드를 통해 ATM, 사용자 장치, 스마트폰, 랩톱, 데스크톱 또는 태블릿 컴퓨터와 같은 다른 클라이언트 장치와 접촉을 설정하도록 형상화될 수 있다. 접촉 패드는 ISO/IEC 7816 표준과 같은 하나 이상의 표준에 따라 설계될 수 있으며 EMV 프로토콜에 따른 통신을 가능하게 한다. 비접촉식 카드(104)는 또한 도 7b에서 더 설명되는 바와 같이 처리 회로, 안테나 및 기타 컴포넌트를 포함할 수 있다. 이러한 컴포넌트는 접촉 패드(708) 뒤에 위치하거나 기판(704)의 다른 곳에 위치할 수 있다. 기판(704)의 다른 층 내에 접촉 패드(708)와 전기적 및 물리적으로 결합될 수 있다. 비접촉식 카드(104)는 또한 카드의 뒷면에 위치할 수 있는 자기 스트립 또는 테이프를 포함할 수 있다. 도 7a에는 도시되지 않음. 비접촉식 카드(104)는 또한 NFC 프로토콜을 통해 통신할 수 있는 안테나와 결합된 근거리 무선통신(NFC) 장치를 포함할 수 있다. 실시형태는 이러한 방식으로 제한되지 않는다.

[0070] 도 7b에 도시된 바와 같이, 비접촉식 카드(104)의 접촉 패드(708)는 프로세서(712), 메모리(108) 및 하나 이상의 통신 인터페이스(124)를 포함하여 정보를 저장, 처리 및 통신하기 위한 처리 회로(710)를 포함할 수 있다. 처리 회로(710)는 여기에 설명된 기능을 수행하는 데 필요한 프로세서, 메모리, 오류 및 패리티/CRC 체커, 데이터 인코더, 충돌 방지 알고리즘, 컨트롤러, 명령 디코더, 보안 프리미티브 및 변조 방지 하드웨어를 포함한 추가 컴포넌트를 포함할 수 있다는 것이 이해된다.

[0071] 메모리(108)는 읽기 전용 메모리, 1회 기록 다중 메모리 또는 읽기/쓰기 메모리, 예를 들어 RAM, ROM 및 EEPROM일 수 있고, 비접촉식 카드(104)는 이들 메모리 중 하나 이상을 포함할 수 있다. 읽기 전용 메모리는 공장에서 읽기 전용 또는 일회성 프로그래밍이 가능하도록 프로그래밍할 수 있다. 일회성 프로그래밍 기능은 한 번 쓰고 여러 번 읽을 수 있는 기회를 제공한다. 1회 쓰기/다중 읽기 메모리는 메모리 칩이 공장에서 출고된 후 특정 시점에 프로그래밍 될 수 있다. 메모리가 프로그래밍 되면 다시 쓸 수는 없지만 여러 번 읽을 수는 있다. 읽기/쓰기 메모리는 공장에서 출고된 후에도 여러 번 프로그래밍 되고 다시 프로그래밍 될 수 있다. 읽기/쓰기 메모리는 공장에서 출고된 후에도 여러 번 읽을 수도 있다. 일부 경우에, 메모리 (108)는 데이터를 암호화하기 위해 프로세서(712)에 의해 실행되는 암호화 알고리즘을 활용하는 암호화된 메모리일 수 있다.

[0072] 메모리(108)는 하나 이상의 애플릿(110), 하나 이상의 카운터(116), 고유 ID(112), 마스터 키(114), UDK(118), 다양화 키(120) 및 PAN 시퀀스(156)를 저장하도록 형상화될 수 있다. 하나 이상의 애플릿(110)은 Java® 카드 애플릿과 같은 하나 이상의 비접촉식 카드(104)에서 실행되도록 구성된 하나 이상의 소프트웨어 응용프로그램을 포함할 수 있다. 그러나 애플릿(110)은 자바 카드 애플릿으로 제한되지 않고, 대신 비접촉식 카드 또는 제한된 메모리를 갖는 다른 장치에서 작동할 수 있는 임의의 소프트웨어 응용프로그램일 수 있다는 것이 이해된다.

[0073] 하나 이상의 카운터(116)는 정수를 저장하기에 충분한 숫자 카운터를 포함할 수 있다. 고유 ID(112)는 비접촉식 카드(104)에 할당된 고유 영숫자 식별자를 포함할 수 있고, 식별자는 비접촉식 카드(104)를 다른 비접촉식 카드(104)와 구별할 수 있다. 일부 실시예에서 고유 ID(112)는 고객과 해당 고객에게 할당된 계정을 모두 식별할 수 있다.

[0074] 전술한 실시형태의 프로세서(712) 및 메모리 소자는 접촉 패드(708)를 참조하여 설명되었으나, 본 발명은 이에

제한되지 않는다. 이들 요소는 접촉 패드(708) 외부에 구현되거나 접촉 패드와 완전히 별개로 구현될 수 있거나, 접촉 패드(708) 내에 위치하는 프로세서(712) 및 메모리(108) 요소에 추가하는 추가 요소로서 구현될 수 있다는 것이 이해된다.

[0075] 일부 실시예에서, 비접촉식 카드(104)는 하나 이상의 안테나(들)(714)를 포함할 수 있다. 하나 이상의 안테나(714)는 비접촉식 카드(104) 내에 그리고 접촉 패드(708)의 처리 회로(710) 주위에 배치될 수 있다. 예를 들어, 하나 이상의 안테나(714)는 처리 회로(710)와 통합될 수 있고 하나 이상의 안테나(714)는 외부 부스터 코일과 함께 사용될 수 있다. 다른 실시예로서, 하나 이상의 안테나(714)는 접촉 패드(708) 및 처리 회로(710) 외부에 있을 수 있다.

[0076] 하나의 실시형태에서, 비접촉식 카드(104)의 코일은 공심 변압기의 2차 역할을 할 수 있다. 단말은 전력을 차단하거나 진폭 변조를 통해 비접촉식 카드(104)와 통신할 수 있다. 비접촉식 카드(104)는 하나 이상의 커패시터를 통해 기능적으로 유지될 수 있는 비접촉식 카드(104)의 전원 연결의 틈을 이용하여 단말기에서 전송된 데이터를 추론할 수 있다. 비접촉식 카드(104)는 비접촉식 카드(104) 코일의 부하를 전환 또는 부하 변조를 수행함으로써 다시 통신할 수 있다. 간섭을 통해 단말기 코일에서 부하 변조가 감지될 수 있다. 보다 일반적으로, 안테나(714), 프로세서 (712) 및/또는 메모리(108)를 사용하여, 비접촉식 카드(104)는 NFC, Bluetooth 및/또는 Wi-Fi 통신을 통해 통신하기 위한 통신 인터페이스를 제공한다.

[0077] 위에서 설명된 바와 같이, 비접촉식 카드(104)는 스마트 카드 또는 JavaCard와 같은 제한된 메모리를 갖는 다른 장치에서 동작할 수 있는 소프트웨어 플랫폼 상에 구축될 수 있으며, 하나 이상의 응용프로그램 또는 애플릿이 안전하게 실행될 수 있다. 애플릿(110)은 다양한 모바일 응용프로그램 기반 사용 사례에서 다중 요소 인증(MFA)을 위한 일회용 비밀번호(OTP)를 제공하기 위해 비접촉식 카드에 추가될 수 있다. 애플릿(110)은 모바일 NFC 리더 예를 들어, 모바일 컴퓨터 디바이스(102) 또는 POS 단말기와 같은 리더로부터의 근거리 데이터 교환 요청과 같은 하나 이상의 요청에 응답하도록 형상화될 수 있으며, NDEF 텍스트 태그로 인코딩 된 암호화된 보안 OTP로 구성된 NDEF 메시지를 생성한다. NDEF 메시지는 암호(122) 또는 암호(208)와 같은 암호 및 기타 데이터를 포함할 수 있다.

[0078] NDEF OTP의 한 예는 NDEF 짧은 레코드 레이아웃(SR=1)이다. 이러한 실시예에서, 하나 이상의 애플릿(110)은 OTP를 NDEF 유형 4 잘 알려진 유형의 텍스트 태그로서 인코딩하도록 형상화될 수 있다. 일부 실시예에서, NDEF 메시지는 하나 이상의 레코드를 포함할 수 있다. 애플릿(110)은 OTP 레코드 외에 하나 이상의 정적 태그 레코드를 추가하도록 형상화될 수 있다.

[0079] 일부 실시예에서, 하나 이상의 애플릿(110)은 RFID 태그를 에뮬레이트 하도록 형상화될 수 있다. RFID 태그는 하나 이상의 다형성 태그를 포함할 수 있다. 일부 실시예에서, 태그가 판독될 때마다 비접촉식 카드의 진위 여부를 나타낼 수 있는 서로 다른 암호화 데이터가 제공된다. 하나 이상의 애플릿(110)을 기반으로 태그의 NFC 판독이 처리될 수 있고, 데이터는 은행 시스템의 서버와 같은 서버로 전송될 수 있으며, 서버에서 데이터의 유효성이 검증될 수 있다.

[0080] 일부 실시예에서, 비접촉식 카드(104) 및 서버는 카드가 적절하게 식별될 수 있도록 특정 데이터를 포함할 수 있다. 비접촉식 카드(104)는 하나 이상의 고유 식별자 도시되지 않으나 포함할 수 있다. 읽기 동작이 발생할 때마다, 카운터(116)는 증가하도록 형상화될 수 있다. 일부 실시예에서, 비접촉식 카드(104)로부터 데이터가 판독될 때마다 예를 들어, 모바일 장치에 의해 카운터(116)는 검증을 위해 서버로 전송되고 카운터(116)가 검증의 일부로서 서버의 카운터와 동일한지 여부를 결정한다.

[0081] 하나 이상의 카운터(116)는 재생 공격을 방지하도록 형상화될 수 있다. 예를 들어, 암호가 획득되어 재생된 경우, 카운터(116)가 판독 또는 사용되거나 다른 방식으로 전달되면 해당 암호는 즉시 거부된다. 카운터(116)가 사용되지 않은 경우, 재생될 수 있다. 일부 실시예에서, 비접촉식 카드(104) 상에서 증가되는 카운터는 거래에 대해 증가되는 카운터와 다르다. 비접촉식 카드(104) 상의 애플릿(110) 사이에 통신이 없기 때문에 비접촉식 카드(104)는 응용프로그램 거래 카운터(116)를 결정할 수 없다. 일부 실시예에서, 비접촉식 카드(104)는 거래 애플릿일 수 있는 제1 애플릿(440-1) 및 제2 애플릿(440-2)을 포함할 수 있다. 각각의 애플릿(440-1 및 440-2)은 각각의 카운터(116)를 포함할 수 있다.

[0082] 일부 실시예에서, 카운터(116)는 동기화되지 않을 수 있다. 일부 실시예에서, 특정 각도에서 읽기와 같이 트랜잭션을 시작하는 우발적인 읽기를 설명하기 위해 카운터(116)는 증가할 수 있지만 응용프로그램은 카운터(116)를 처리하지 않는다. 일부 실시예에서, 장치(102)가 깨어날 때 NFC는 활성화되고 컴퓨터 디바이스(102)는 이용

가능한 태그를 판독하도록 형상화될 수 있지만, 판독에 응답하여 어떠한 조치도 취해지지 않는다.

[0083] 카운터(116)를 동기화 상태로 유지하기 위해, 컴퓨터 디바이스(102)가 깨어나는 때를 검출하고 뱅킹 시스템의 서버와 동기화하여 판독이 완료되었음을 나타내는 백그라운드 응용프로그램과 같은 응용프로그램이 실행될 수 있다. 감지로 인해 발생한 다음 카운터(116)를 앞으로 이동시킨다. 다른 실시예에서는 동기화 오류 창이 허용될 수 있도록 해시된 일회용 비밀번호가 활용될 수 있다. 예를 들어, 임계값 10 내에 있으면 카운터(116)는 앞으로 이동하도록 형상화될 수 있다. 그러나 다른 임계값 (예: 10 또는 600) 내에 있는 경우, 재동기화 수행 요청이 처리될 수 있으며, 이 요청은 하나 이상의 응용프로그램을 통해 사용자가 사용자 장치를 통해 한 번 이상 탭하거나 몸짓 또는 다른 방식으로 표시하는 요청이다. 카운터(116)가 적절한 순서로 증가하면, 사용자가 그렇게 했다는 것을 아는 것이 가능하다.

[0084] 카운터(116), 마스터 키(114), UDK(118) 및 다양화된 키(120)를 참조하여 본 명세서에 설명된 키 다양화 기술은 키 다양화 기술의 암호화 및/또는 복호화의 하나의 실시예이다. 상기 예시적인 주요 다양화 기술은 본 개시를 제한하는 것으로 간주되어서는 안 된다. 왜냐하면 본 개시는 다른 유형의 주요 다각화 기술에도 동일하게 적용 가능하기 때문이다.

[0085] 비접촉식 카드(104)의 생성 프로세스 동안, 2개의 암호화 키가 카드마다 고유하게 할당될 수 있다. 암호화 키는 데이터의 암호화 및 암호 복호화 모두에 사용될 수 있는 대칭 키를 포함할 수 있다. 트리플DES 알고리즘은 EMV에 의해 사용될 수 있으며 이는 비접촉식 카드(104)의 하드웨어에 의해 구현된다. 키 다양화 프로세스 를 사용하면 키가 필요한 각 엔터티에 대해 고유하게 식별 가능한 정보를 기반으로 마스터 키에서 하나 이상의 키가 파생될 수 있다.

[0086] 일부 실시예에서, 취약성에 취약할 수 있는 3DES 알고리즘의 결함을 극복하기 위해 예를 들면 세션당 고유 키인 세션 키가 파생될 수 있지만 마스터 키를 사용하는 대신 예를 들어 UDK (118)의 고유 카드 파생 키 및 카운터는 다양화 데이터로 사용될 수 있다. 예를 들어, 비접촉식 카드(104)가 동작할 때마다 메시지 인증 코드(MAC) 생성과 암호화 수행을 위해 서로 다른 키가 사용될 수 있다.

[0087] 이로 인해 삼중 암호화 계층이 생성된다. 세션 키는 하나 이상의 애플릿에 의해 생성될 수 있으며 하나 이상의 알고리즘(EMV 4.3 Book 2 A1.3.1 공통 세션 키 파생에 정의됨)과 함께 응용프로그램 트랜잭션 카운터를 사용하여 파생될 수 있다.

[0088] 또한, 각 카드에 대한 증분은 고유할 수 있으며, 개인화에 의해 할당되거나 일부 식별 정보에 의해 알고리즘적으로 할당될 수 있다. 예를 들어, 홀수 카드는 2만큼 증가할 수 있고 짝수 카드는 5만큼 증가할 수 있다. 일부 실시예에서, 증분은 순차적 읽기에서도 달라질 수 있으므로, 하나의 카드는 1, 3, 5, 2, 2 … 반복하여 만큼 순차적으로 증가할 수 있다. 특정 시퀀스 또는 알고리즘 시퀀스는 개인화 시 정의되거나 고유 식별자에서 파생된 하나 이상의 프로세스에서 정의될 수 있다. 이로 인해 리플레이 공격자가 적은 수의 카드 인스턴스를 일반화하기가 더 어려워질 수 있다. 인증 메시지는 16진수 ASCII 형식의 텍스트 NDEF 레코드의 내용으로 전달될 수 있다. 다른 실시예에서 NDEF 레코드는 16진수 형식으로 인코딩 될 수 있다.

[0089] 도 8은 예시적인 실시형태에 따른 NDEF 쇼트 레코드 레이아웃(SR=1) 데이터 구조 (800)를 도시한다. 하나 이상의 애플릿(110)은 OTP를 NDEF 유형 4 잘 알려진 유형의 텍스트 태그로 인코딩하도록 형상화될 수 있다. 일부 실시예에서, NDEF 메시지는 하나 이상의 레코드를 포함할 수 있다. OTP 레코드 외에 하나 이상의 정적 태그 레코드를 추가하도록 애플릿을 구성할 수 있다. 예시적인 태그에는 태그 유형: 잘 알려진 유형, 텍스트, 인코딩 영어(en); 애플릿 ID: D2760000850101; 기능: 읽기 전용 액세스; 인코딩: 인증 메시지는 ASCII 16진수로 인코딩될 수 있다. 유형 길이 값(TLV) 데이터는 NDEF 메시지를 생성하는 데 사용될 수 있는 개인화 매개변수로 제공될 수 있다. 하나의 실시형태에서 인증 템플릿은 실제 동적 인증 데이터를 제공하기 위한 잘 알려진 인덱스를 갖는 제1 레코드를 포함할 수 있다. 데이터 구조(800)는 암호(122) 또는 암호(208)와 같은 암호 및 애플릿(110)에 의해 제공되는 임의의 다른 데이터를 포함할 수 있다.

[0090] 도 9는 개시된 실시형태에 따른 예시적인 시스템(900)의 개략도를 도시한다. 시스템(900)은 네트워크(902)를 통해 블록체인(906)에 액세스할 수 있는 시스템을 포함할 수 있다.

[0091] 시스템(900)은 블록체인(906)을 사용하여 평판이 좋지 않은 상호 작용 기록을 생성할 수 있다. 또한 블록체인(906)은 복수의 컴퓨터 시스템에 분산될 수 있어 블록체인(906)에 저장된 기록의 유효성에 대한 신뢰를 장려한다. 이러한 방식으로 개시된 시스템은 적어도 종래 시스템의 위에 언급된 기술 문제에 대한 혁신적인 기술 솔루션을 제공한다.

[0092] 사용자 시스템(904)은 컴퓨터 디바이스(102)를 포함할 수 있다. 사용자 시스템 (904)은 개시된 실시형태에 따라 디지털 지갑(144)을 사용하여 거래를 처리하도록 형상화될 수 있다. 사용자 시스템(904)은 서버, 워크스테이션, 데스크탑 또는 모바일 장치 예를 들어, 랩톱, 태블릿, 패블릿, 스마트폰, 스마트 워치 또는 유사한 모바일 컴퓨터 디바이스와 같은 컴퓨터 디바이스를 포함할 수 있다. 도 12와 관련하여 아래에 설명된 바와 같이, 사용자 시스템(904)은 디스플레이 및 입력/출력 인터페이스로 형상화될 수 있다. 사용자 시스템(904)은 디스플레이 및 입력/출력 인터페이스를 사용하여 사용자 (미도시)와 상호작용하도록 형상화될 수 있다.

[0093] 회원 시스템(908)은 개시된 실시형태에 따라 거래를 처리하도록 형상화될 수 있다.

[0094] 구성원 시스템(908)은 서버, 워크스테이션, 데스크톱 컴퓨터 또는 특수 목적 컴퓨터 디바이스와 같은 하나 이상의 컴퓨터 디바이스를 포함할 수 있다. 구성원 시스템 (908)은 독립형 일 수도 있고, 더 큰 시스템의 일부일 수 있는 하위 시스템의 일부일 수도 있다. 예를 들어, 회원 시스템(908)은 상업 기관과 연관될 수 있다. 회원 시스템(908)은 공중 네트워크 또는 전용 사설 네트워크를 통해 금융 기관의 다른 시스템과 원격 위치하여 통신하는 분산 서버를 포함할 수 있다.

[0095] 회원 시스템(908)은 디지털 지갑(144)의 암호화폐를 사용하여 거래를 처리하라는 요청을 수신하도록 형상화될 수 있다. 일부 실시형태에서, 구성원 시스템(908)은 다른 구성원 시스템(908) 및/또는 사용자 시스템(904)과 같은 시스템(900)의 다른 요소로부터 요청을 수신하도록 형상화될 수 있다. 회원 시스템(908)은 거래 요청을 처리하기 위해 블록체인(906)과 상호작용하도록 형상화될 수 있다.

[0096] 회원 시스템(908)은 개시된 실시형태에 따라 블록체인(906)에 메시지를 저장하도록 형상화될 수 있다. 일부 측면에서, 구성원 시스템(908)은 메시지를 포함하는 블록을 블록체인(906)에 추가하도록 형상화될 수 있다. 다양한 양상에서, 구성원 시스템 (908)은 승인된 시스템에 메시지를 제공하도록 형상화될 수 있다. 승인된 시스템은 메시지를 포함하는 블록을 블록체인(906)에 추가하도록 형상화될 수 있다. 도 10에 도시된 바와 같이, 메시지는 거래 기록을 포함할 수 있다.

[0097] 블록체인(906)은 개시된 실시형태에 따라 분산된 데이터 구조를 포함할 수 있다. 블록체인(906)은 개인 블록체인일 수 있다. 예를 들어, 승인된 시스템은 블록체인 (906)의 복사본을 저장할 수 있다. 이러한 승인된 시스템은 블록체인 (906)에 블록을 추가하고 해당 블록을 다른 승인된 시스템에 게시하도록 형상화될 수 있다. 승인된 시스템은 블록체인(906)에 게시하기 위해 다른 시스템으로부터 메시지를 수신하도록 형상화될 수 있다. 이러한 다른 시스템은 블록체인(906)에 대한 읽기 전용 액세스를 가질 수 있다. 일부 실시형태에서, 하나 이상의 구성원 시스템 (908)은 승인된 시스템이다. 일부 실시형태에서, 하나 이상의 사용자 시스템(904)은 승인된 시스템이다. 도 9와 관련하여 자세히 설명된 바와 같이, 블록체인(906)은 회원 시스템으로부터의 메시지를 저장하도록 형상화될 수 있으며, 메시지에는 트랜잭션이 포함된다.

[0098] 네트워크(902)는 도 9의 컴포넌트들 사이의 통신을 제공하도록 형상화될 수 있다.

[0099] 예를 들어, 네트워크(902)는 통신을 제공하고, 정보를 교환하고 및/또는 정보 교환을 용이하게 하는 임의 유형의 네트워크 인프라 포함일 수 있다. 예를 들어, 인터넷, 근거리 통신망, 또는 다음을 가능하게 하는 기타 적절한 연결이 있다. 인증 시스템(900)은 인증 시스템(900)의 컴포넌트 간에 정보를 보내고 받는다.

[0100] 도 10은 개시된 실시형태에 따른 예시적인 블록체인(906)의 논리 모델(1000)을 도시한다. 블록체인(906)은 다양한 시스템 예를 들면 구성원 시스템(908) 또는 기타 시스템에 의해 유지되는 많은 블록체인을 포함할 수 있다. 이러한 예시적인 블록체인은 블록 (1006a) 내지 블록 (1006d)와 같은 블록을 포함할 수 있다. 블록은 메시지 예를 들면 메시지 1008a 내지 메시지 1008d를 포함할 수 있다. 일반적으로, 블록은 각 블록을 고유하게 식별하는 헤더(1002a 내지 1002d)와 같은 헤더를 포함할 수 있다. 헤더(1002a 내지 1002d)는 해시 함수에 의해 생성된 해시 값을 포함할 수 있다.

[0101] 해시 함수는 임의 크기의 입력 데이터를 고정 크기의 해시 값에 매핑하는 데 사용할 수 있는 함수이다. 예를 들어 헤더에는 이전 블록의 해시 값, 블록 내 임의의 메시지를 기반으로 생성된 해시 값 예를 들면 머클 루트, 타임스탬프 중 적어도 하나가 포함될 수 있다. 개시된 실시형태에 따라, 시스템(900)은 블록체인(906)에 추가된 블록이 작업 증명 조건 및 디지털 서명 조건 중 적어도 하나를 만족하도록 요구할 수 있다. 예를 들어 헤더(1002a 내지 1002d)는 헤더가 작업 증명 조건 (1004a 내지 1004d)을 만족시키는 것을 보장하기 위해 선택된 넌스를 포함할 수 있다. 비제한적인 실시예로서 작업 증명 조건(1004a 내지 1004d)은 헤더의 해시가 미리 결정된 값 범위 내에 속하도록 요구할 수 있다. 추가적인 실시예로서, 헤더는 공인 시스템의 암호화 키 예를 들면 개인키(146)로 디지털 서명될 수 있으며, 디지털 서명은 헤더에 포함될 수 있다. 이 디지털 서명은 시스템(900)의

구성원이 사용할 수 있는 키를 사용하여 검증될 수 있다.

[0102] 도 11은 개시된 실시형태에 따른, 블록체인 예를 들어, 블록체인(906)의 요소에 저장된 메시지(1008b)의 논리 모델(1100)을 도시한다. 일부 실시형태에서 메시지 (1008b)는 인덱스 정보(1102)를 포함할 수 있다. 특정 실시예에서, 색인 정보 (1102)는 사용자를 식별하는 정보를 포함할 수 있다. 예를 들어, 색인 정보 (1102) 는 사용자의 성명, 이메일 주소, 전화번호 또는 기타 민감하지 않은 개인 정보 중 적어도 하나일 수 있다. 다양한 측면에서, 인덱스 정보(1102)는 프라이빗 블록체인의 이전 블록에 대한 하나 이상의 참조를 포함할 수 있다. 예를 들어, 인덱스 정보(1102)는 동일한 사용자와 관련된 하나 이상의 이전 블록에 대한 하나 이상의 참조를 포함할 수 있다. 참조에는 비제한적인 예로서 동일한 사용자와 관련된 블록체인의 이전 블록의 해시가 포함될 수 있다. 일부 실시예에서, 인덱스 정보(1102)는 당업자에게 알려진 방법에 따라 난독화 되거나 암호화될 수 있다. 예를 들어, 인덱스 정보(1102)는 개인 키(146)와 같은 암호화 키로 암호화될 수 있다. 추가적인 실시예로서, 색인 정보(1102)는 사용자의 성명, 이메일 주소, 전화번호 또는 기타 민감하지 않은 개인 정보 중 적어도 하나의 해시를 포함할 수 있다.

[0103] 메시지(1008b)는 개시된 실시형태에 따라 추가 정보(1104)를 포함할 수 있다. 추가 정보(1104)는 거래 세부사항, 예를 들어 하나의 디지털 지갑(144)에서 다른 디지털 지갑(144)으로 전송되는 암호화폐의 양을 포함할 수 있다. 다양한 측면에서, 추가 정보(1104)는 당업자에게 알려진 방법에 따라 난독화 또는 암호화될 수 있다. 예를 들어, 루트 시스템 정보(1104)는 개인 키(146)와 같은 암호화 키로 암호화될 수 있다.

[0104] 메시지(1008b)는 개시된 실시형태에 따라 인증 레코드(1106)를 포함할 수 있다. 일부 측면에서, 인증 레코드(1106)는 거래의 후속 감사를 가능하게 하는 정보를 포함할 수 있다. 예를 들어, 인증 기록(1106)은 회원 시스템(908), 회원 시스템 (908)과 연관된 상업 기관, 인증 기록(1106)의 목적 예를 들어, 거래 세부사항 중 적어도 하나를 식별할 수 있다. 일부 실시예에서 인증 레코드 (1106)는 당업자에게 알려진 방법에 따라 난독화 또는 암호화될 수 있다. 예를 들어 인증 레코드(1106) 는 개인 키(146)와 같은 암호화 키로 암호화될 수 있다.

[0105] 개시된 실시형태에 따라, 개인 키(146)와 같은 암호화 키는 블록의 메시지 요소를 암호화하는 데 사용될 수 있다. 일부 측면에서, 이러한 암호화 키는 인증 시스템 (900)의 구성원 예를 들어 구성원 시스템(908)과 연관될 수 있다. 다양한 측면에서 암호화 키 중 적어도 일부는 승인된 시스템과 연관될 수 있다. 공개 키(148) 와 같은 대응 암호화 키는 개시된 실시형태에 따라 암호화된 메시지 요소를 복호화 하는 데 이용될 수 있다. 예를 들어, 블록의 메시지 요소가 대칭 키로 암호화된 경우 동일한 대칭 키를 사용하여 암호화된 요소를 복호화 할 수 있다. 다른 실시예 로서, 블록 내의 메시지 요소가 개인 키(146)로 암호화된 경우 해당 공개 키(148) 는 암호화된 요소를 복호화 하는 데 사용될 수 있다. 일부 측면에서, 해당 암호화 키는 인증 시스템 예를 들어, 회원 시스템(908)의 구성원이 사용할 수 있다.

[0106] 도 12는 이전에 설명된 다양한 실시형태를 구현하는 데 적합한 예시적인 컴퓨터 아키텍처(1200)의 실시형태를 도시한다. 하나의 실시형태에서, 컴퓨터 아키텍처 (1200)는 컴퓨터 아키텍처(100)를 포함하거나 그 일부로서 구현될 수 있다.

[0107] 본 출원에 사용된 용어 "시스템" 및 "컴포넌트"는 하드웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어 또는 실행 중인 소프트웨어 등 컴퓨터 관련 엔터티를 나타내도록 의도되었으며, 그 예는 다음과 같다. 예시적인 컴퓨터 컴퓨터 아키텍처(1200)에 의해 제공된다. 예를 들어, 컴포넌트는 프로세서에서 실행되는 프로세스, 프로세서, 하드 디스크 드라이브, 다중 저장 드라이브, 광학 및/또는 자기 저장 매체, 개체, 실행 파일, 실행 스레드, 프로그램 및/또는 컴퓨터를 들 수 있다.

[0108] 예를 들어 서버에서 실행되는 응용프로그램과 서버 모두 컴포넌트가 될 수 있다. 하나 이상의 컴포넌트는 프로세스 및/또는 실행 스레드 내에 상주할 수 있으며, 컴포넌트는 한 컴퓨터에 지역화 또는 두 대 이상의 컴퓨터 간에 배포될 수 있다. 또한, 컴포넌트들은 동작을 조정하기 위해 다양한 유형의 통신 매체에 의해 서로 통신 가능하게 결합될 수 있다. 조정에는 단방향 또는 양방향 정보 교환이 포함될 수 있다. 예를 들어, 컴포넌트는 통신 매체를 통해 전달되는 신호 형태로 정보를 전달할 수 있다. 상기 정보는 다양한 신호 라인에 할당된 신호로 구현될 수 있다. 이러한 할당에서 각 메시지는 신호이다. 그러나 추가 실시형태는 대안적으로 데이터 메시지를 이용할 수도 있다. 이러한 데이터 메시지는 다양한 연결을 통해 전송될 수 있다. 연결의 예로는 병렬 인터페이스, 직렬 인터페이스 및 버스 인터페이스가 있다.

[0109] 컴퓨터 아키텍처(1200)는 하나 이상의 프로세서, 멀티 코어 프로세서, 보조 프로세서, 메모리 유닛, 칩셋, 컨트롤러, 주변 장치, 인터페이스, 발진기, 타이밍 장치, 비디오 카드, 오디오 카드와 같은 다양한 공통 컴퓨터 요

소를 포함한다. , 멀티미디어 입/출력(I/O) 컴포넌트, 전원 공급 장치 등이 있다. 그러나 실시형태는 컴퓨터 컴퓨터 아키텍처(1200)에 의한 구현으로 제한되지 않는다.

[0110] 도 12에 도시된 바와 같이, 컴퓨터 아키텍처(1200)는 프로세서(1202), 시스템 메모리(1204) 및 시스템 버스(1206)를 포함하는 컴퓨터(1212)를 포함한다. 프로세서(1202)는 상업적으로 이용 가능한 다양한 프로세서 중 임의의 것일 수 있다. 컴퓨터(1212)는 컴퓨터 디바이스(102) 및/또는 서버(106)를 대표할 수 있다.

[0111] 시스템 버스(1206)는 프로세서(1202)에 대한 시스템 메모리(1204)를 포함하지만 이에 제한되지 않는 시스템 컴포넌트에 대한 인터페이스를 제공한다. 시스템 버스(1206)는 상업적으로 이용 가능한 다양한 버스 아키텍처 중 하나를 사용하여 메모리 버스(메모리 컨트롤러가 있거나 없음), 주변 버스 및 로컬 버스에 추가로 상호 연결될 수 있는 여러 유형의 버스 구조 중 하나일 수 있다. 인터페이스 어댑터는 슬롯 아키텍처를 통해 시스템 버스(1206)에 연결될 수 있다. 예시적인 슬롯 아키텍처에는 AGP(가속 그래픽 포트), 카드 버스, (확장) 산업 표준 아키텍처 ((E)ISA), 마이크로 채널 아키텍처(MCA), NuBus, 주변 장치 컴포넌트 상호 연결 (확장)(PCI(X)) PCI 익스프레스, 개인용 컴퓨터 메모리 카드 국제 협회 (PCMCIA) 이 포함될 수 있지만 이에 국한되지는 않는다.

[0112] 컴퓨터 아키텍처(1200)는 다양한 제조 물품을 포함하거나 구현할 수 있다. 제조품은 로직을 저장하기 위한 컴퓨터 판독 가능 저장 매체를 포함할 수 있다. 컴퓨터 판독 가능 저장 매체의 예에는 휘발성 메모리 또는 비휘발성 메모리, 제거 가능 또는 비분리 가능 메모리, 지울 수 있거나 지울 수 없는 메모리, 쓰기 가능 또는 재쓰기 가능 메모리를 포함하여 전자 데이터를 저장할 수 있는 모든 유형의 매체가 포함될 수 있다.로직의 예에는 소스 코드, 컴파일 코드, 해석된 코드, 실행 가능한 코드, 정적 코드, 동적 코드, 객체 지향 코드, 시각적 코드 등과 같은 임의의 적합한 유형의 코드를 사용하여 구현된 실행 가능한 컴퓨터 프로그램 명령이 포함될 수 있다. 실시형태는 또한 비일시적 컴퓨터 판독 가능 매체에 포함된 명령으로서 적어도 부분적으로 구현될 수 있으며, 이는 본 명세서에 설명된 동작의 수행을 가능하게 하기 위해 하나 이상의 프로세서에 의해 판독 및 실행될 수 있다.

[0113] 시스템 메모리(1204)는 읽기 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 동적 RAM(DRAM), 이중 데이터 속도 DRAM(DDRAM), 동기식 DRAM(SDRAM), 정적 RAM(SRAM), 프로그래밍 가능 ROM(PROM), 삭제 가능 프로그래밍 가능 ROM(EPROM), 전기적으로 삭제 가능 프로그래밍 가능 ROM(EEPROM), 플래시 메모리, 폴리머 강유전성 폴리머 메모리, 오보닉 메모리, 상 변화 또는 강유전성 메모리, 실리콘-산화물-질화물-산화물-실리콘(SONOS) 메모리, 자기 또는 광학 카드, 복수 배열 독립 디스크(RAID) 드라이브와 같은 장치 배열 , 솔리드 스테이트 메모리 장치 예를 들면 USB 메모리, 솔리드 스테이트 드라이브(SSD) 및 정보 저장에 적합한 기타 유형의 저장 매체 등이다. 도 12에 도시된 바와 같이 시스템 메모리(1204)는 비휘발성(1208) 및/또는 휘발성(1210)을 포함할 수 있다. 기본 입/출력 시스템(BIOS)은 비휘발성(1208)에 저장될 수 있다.

[0114] 컴퓨터(1212)는 내부 또는 외부 하드 디스크 드라이브(1214), 자기 디스크 드라이브(1216)를 포함하여 하나 이상의 저속 메모리 유닛 형태의 다양한 유형의 컴퓨터 판독 가능 저장 매체를 포함할 수 있다. 이동식 자기 디스크(1218) 및 이동식 광 디스크(1222) 예를 들어 CD-ROM 또는 DVD로부터 읽거나 쓰기 위한 광 디스크 드라이브(1220)에 연결된다.

[0115] 하드 디스크 드라이브(1214), 자기 디스크 드라이브(1216) 및 광 디스크 드라이브 (1220)는 각각 HDD 인터페이스(1224), FDD 인터페이스(1226) 및 광 디스크 드라이브 인터페이스(1228)에 의해 시스템 버스(1206)에 연결될 수 있다. 외부 드라이브 구현을 위한 HDD 인터페이스(1224)는 범용 직열 버스(USB) 및 IEEE 1394 인터페이스 기술 중 적어도 하나 또는 둘 다를 포함할 수 있다. 드라이브 및 관련 컴퓨터 판독 가능 매체는 데이터, 데이터 구조, 컴퓨터 실행 가능 명령 등의 휘발성 및/또는 비휘발성 저장 장치를 제공한다. 예를 들어, 운영 체제(1230), 하나 이상의 응용프로그램(1232), 기타 프로그램 모듈(1234) 및 프로그램 데이터(1236)를 포함하는 다수의 프로그램 모듈이 드라이브 및 비휘발성(1208) 및 휘발성(1210)에 저장될 수 있다. 하나의 실시형태에서 하나 이상의 응용프로그램(1232), 다른 프로그램 모듈(1234) 및 프로그램 데이터(1236)는 예를 들어 시스템(100)의 다양한 응용프로그램 및/또는 컴포넌트를 포함할 수 있다.

[0116] 사용자는 하나 이상의 유무선 입력 장치, 예를 들어 키보드(1238) 및 마우스 (1240)와 같은 포인팅 장치를 통해 컴퓨터(1212)에 명령 및 정보를 입력할 수 있다. 빨간색(IR) 리모컨, 무선 주파수(RF) 리모컨, 게임 패드, 스타일러스 펜, 카드 리더기, 동글, 지문 인식기, 장갑, 그래픽 태블릿, 조이스틱, 키보드, 레티나 리더기, 예를 들면 정전식, 저항막 등 터치 스크린, 트랙볼, 트랙 패드, 센서, 스타일러스 등을 들 수 있다. 이들 및 기타 입력 장치는 종종 시스템 버스(1206)에 연결되어 있지만 병렬 포트, IEEE 1394 직렬 포트, 게임 포트, USB 포트와 같은 포트, IR 인터페이스 등과 같은 다른 인터페이스에 의해 연결될 수 있는 입력 장치 인터페이스(1242)를 통해 프로세서(1202)에 연결된다.

[0117] 모니터(1244) 또는 다른 유형의 디스플레이 장치도 비디오 어댑터(1246)와 같은 인터페이스를 통해 시스템 버스(1206)에 연결된다. 모니터(1244)는 컴퓨터(1212)의 내부 또는 외부에 있을 수 있다. 일반적으로 컴퓨터에는 스피커, 프린터 등과 같은 기타 주변 출력 장치가 포함된다.

[0118] 컴퓨터(1212)는 원격 컴퓨터(들)(1248)과 같은 하나 이상의 원격 컴퓨터에 대한 유선 및/또는 무선 통신을 통한 논리적 연결을 사용하여 네트워크 환경에서 작동할 수 있다. 원격 컴퓨터(1248)은 워크스테이션, 서버 컴퓨터, 라우터, 개인용 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서 기반 엔터테인먼트 기기, 피어 장치 또는 기타 공통 네트워크 노드일 수 있다. 일반적으로 컴퓨터(1212)와 관련하여 설명된 많은 또는 모든 요소를 포함하지만, 간결성을 위해 메모리 및/또는 저장 장치(1250)만 도시된다. 도시된 논리적 연결은 근거리 통신망(1252) 및/또는 더 큰 네트워크, 예를 들어 광역 통신망(1254)에 대한 유선/무선 연결을 포함한다. 이러한 LAN 및 WAN 네트워크 환경은 사무실과 회사에서 일반적이며 전사적 컴퓨터 네트워크를 용이하게 한다. 인트라넷과 같은 모든 것들은 인터넷과 같은 글로벌 통신 네트워크에 연결될 수 있다.

[0119] 근거리 통신망(1252) 네트워크 환경에서 사용되는 경우, 컴퓨터(1212)는 유무선 통신 네트워크 인터페이스 또는 네트워크 어댑터(1256)를 통해 근거리 통신망 (1252)에 연결된다. 네트워크 어댑터(1256)는 네트워크 어댑터(1256)의 무선 기능과 통신하기 위해 배치된 무선 액세스 포인트를 또한 포함할 수 있는 근거리 통신망 (1252)에 대한 유선 및/또는 무선 통신을 용이하게 할 수 있다. 광역네트워크(1254) 네트워크 환경에서 사용될 때, 컴퓨터(1212)는 모뎀(1258)을 포함할 수 있거나 광역 네트워크(1254) 상의 통신 서버에 연결되거나 인터넷과 같은 광역 네트워크(1254)를 통해 통신을 설정하기 위한 다른 수단이 있다. 내부 또는 외부일 수 있고 유선 및/또는 무선 장치일 수 있는 모뎀(1258)은 입력 장치 인터페이스(1242)를 통해 시스템 버스(1206)에 연결된다. 네트워크 환경에서, 컴퓨터(1212)와 관련하여 도시된 프로그램 모듈 또는 그 일부는 원격 메모리 및/또는 저장 장치(1250)에 저장될 수 있다. 도시된 네트워크 연결은 예시적이며 컴퓨터 사이에 통신 링크를 설정하는 다른 수단이 사용될 수 있다는 것이 이해될 것이다.

[0120] 컴퓨터(1212)는 무선 통신 예를 들어, IEEE 802.11 무선 변조 기술에서 작동 가능하게 배치된 무선 장치와 같은 IEEE 802 계열 표준을 사용하여 유선 및 무선 장치 또는 개체와 통신하도록 작동 가능한다. 여기에는 특히 Wi-Fi 또는 무선 피델리티, WiMax 및 Bluetooth™ 무선 기술이 포함된다. 따라서, 통신은 기존 네트워크와 같이 미리 정의된 구조이거나 단순히 적어도 두 장치 간의 임시 통신일 수 있다. Wi-Fi 네트워크는 IEEE 802.11(a, b, g, n, ac, ax 등)이라는 무선 기술을 사용하여 안전하고 안정적이며 빠른 무선 연결을 제공한다. Wi-Fi 네트워크는 컴퓨터를 서로 연결하고, 인터넷에 연결하고, 유선 네트워크 IEEE 802.3 관련 미디어 및 기능을 사용에 연결하는 데 사용할 수 있다.

[0121] 장치의 다양한 엘레멘트는 도 1 및 도 2를 참조하여 이전에 설명된 바와 같다. 도 1a 내지 도12에 나타난 다양한 하드웨어 엘레멘트, 소프트웨어 엘레멘트 또는 이 둘의 조합을 포함할 수 있다.

[0122]]

[0123] 하드웨어 엘레멘트의 예에는 장치, 논리 장치, 부품, 프로세서, 마이크로프로세서, 회로, 프로세서, 회로 요소(예: 트랜지스터, 저항기, 커패시터, 인덕터 등), 집적 회로, 주문형 집적 회로(ASIC), 프로그래밍 가능 논리 장치(PLD), 디지털 신호 프로세서(DSP), 필드 프로그래밍 가능 게이트 어레이 (FPGA), 메모리 장치, 논리 게이트, 레지스터, 반도체 장치, 칩, 마이크로칩, 칩셋 등이다.

[0124] 소프트웨어 엘레멘트의 예로는 소프트웨어 컴포넌트, 프로그램, 응용프로그램, 컴퓨터 프로그램, 응용프로그램 프로그램, 시스템 프로그램, 소프트웨어 개발 프로그램, 기계 프로그램, 운영 체제 소프트웨어, 미들웨어, 펌웨어, 소프트웨어 모듈, 루틴, 서브루틴, 기능, 방법, 절차, 소프트웨어 인터페이스, 응용 프로그램 인터페이스(API), 명령어 세트, 컴퓨터 코드, 컴퓨터 코드, 코드 세그먼트, 컴퓨터 코드 세그먼트, 단어, 값, 기호 또는 이들의 조합 등이다.

[0125] 그러나 실시형태가 하드웨어 엘레멘트 및/또는 소프트웨어 엘레멘트를 사용하여 주어진 구현에 대해 원하는 대로 구현되는지 여부를 결정하는 것은 원하는 계산 속도, 전력 레벨, 내열성, 처리 주기 예산, 입력 데이터 속도, 출력 데이터 속도, 메모리 리소스, 데이터 버스 속도 및 기타 설계 또는 성능 제약에 달려 있다.

[0126] 적어도 하나의 실시형태의 하나 이상의 측면은 프로세서 내의 다양한 로직을 나타내는 기계 판독 가능 매체에 저장된 대표적인 명령어에 의해 구현될 수 있다.

[0127] 이는 기계에 의해 판독될 때 기계가 본 명세서에 설명된 기술을 수행하기 위한 논리를 제작하게 한다. "IP

코어"로 알려진 이러한 표현은 유형의 기계 판독 가능 매체에 저장될 수 있으며 다양한 고객이나 제조 시설에 제공되어 로직이나 프로세서를 만드는 제조 기계에 로드 될 수 있다. 일부 실시형태는 예를 들어 기계에 의해 실행될 경우 기계가 다음에 따른 방법 및/또는 동작을 수행하게 할 수 있는 명령어 또는 명령어 세트를 저장할 수 있는 기계 판독 가능 매체 또는 물품을 사용하여 구현될 수 있다. 실시형태에서 이러한 기계는 예를 들어 임의의 적합한 처리 플랫폼, 컴퓨터 플랫폼, 컴퓨터 디바이스, 처리 장치, 컴퓨터 시스템, 처리 시스템, 컴퓨터, 프로세서 등을 포함할 수 있고 하드웨어 및/또는 하드웨어 및/또는 소프트웨어 임의의 적합한 조합을 사용하여 구현될 수 있다.

[0128] 기계 판독 가능 매체 또는 물품은 예를 들어 임의의 적합한 유형의 메모리 유닛, 메모리 장치, 메모리 물품, 메모리 매체, 저장 장치, 저장 물품, 저장 매체 및/또는 저장 유닛, 예를 들어 메모리, 착탈식 또는 저장 장치를 포함할 수 있다. 이동식이 아닌 미디어, 지울 수 있거나 지울 수 없는 미디어, 쓰기 가능하거나 다시 쓰기 가능한 미디어, 디지털 또는 아날로그 미디어, 하드 디스크, 플로피 디스크, 컴팩트 디스크 읽기 전용 메모리(CD-ROM), 컴팩트 디스크 기록 가능(CD-R),컴팩트 디스크 재작성 (CD-RW), 광 디스크, 자기 매체, 광자기 매체, 이동식 메모리 카드 또는 디스크, 다양한 유형의 디지털 벌세타일 디스크(DVD), 테이프, 카세트 등을 들 수 있다. 명령어에는 소스 코드, 컴파일된 코드, 해석된 코드, 실행 가능 코드, 정적 코드, 동적 코드, 암호화된 코드 등과 같은 임의의 적합한 유형의 코드가 포함될 수 있다. 적절한 상위 수준, 하위 수준, 객체 지향, 시각적, 컴파일 및/또는 해석된 프로그래밍 언어를 사용하여 구현된다.

[0129] 위에서 설명된 장치의 컴포넌트 및 특징은 개별 회로, 주문형 집적 회로(ASIC), 논리 게이트 및/또는 단일 칩 아키텍처의 임의의 조합을 사용하여 구현될 수 있다. 또한, 장치의 특징은 마이크로컨트롤러, 프로그래밍 가능한 논리 어레이 및/또는 마이크로프로세서 또는 적절하게 적절한 경우 전술한 것의 임의의 조합을 사용하여 구현될 수 있다. 하드웨어, 펌웨어 및/또는 소프트웨어 요소는 본 명세서에서 집합적으로 또는 개별적으로 "로직" 또는 "회로"로 지칭될 수 있다는 점에 유의한다.

[0130] 전술한 블록도에 도시된 예시적인 장치는 많은 잠재적인 구현 중 기능적으로 설명하는 하나의 예를 나타낼 수 있다는 것이 이해될 것이다. 따라서, 첨부 도면에 도시된 블록 기능의 분할, 생략 또는 포함은 이러한 기능을 구현하기 위한 하드웨어 컴포넌트, 회로, 소프트웨어 및/또는 요소가 실시형태에서 반드시 분할, 생략 또는 포함될 것임을 의미하지 않는다.

[0131] 적어도 하나의 컴퓨터 판독 가능 저장 매체는 실행될 때 시스템이 여기에 설명된 임의의 컴퓨터 구현 방법을 수행하게 하는 명령어를 포함할 수 있다.

[0132] 일부 실시형태는 "하나의 실시형태" 또는 "실시형태"라는 표현과 그 파생어를 사용하여 설명될 수 있다. 이러한 용어들은 실시형태와 관련하여 설명된 특정한 특징, 구조, 특성이 적어도 하나의 실시형태에 포함된다는 것을 의미한다.

[0133] 본 명세서의 여러 곳에서 "일 실시형태에서"라는 문구가 등장한다고 해서 반드시 모두 동일한 실시형태를 지칭하는 것은 아니다. 또한 달리 명시하지 않는 한 위에서 설명한 기능은 어떤 조합으로도 함께 사용할 수 있는 것으로 인식된다. 따라서, 별도로 논의된 임의의 특징은 특징이 서로 호환되지 않는다고 언급되지 않는 한 서로 조합하여 사용될 수 있다.

[0134] 본 발명의 요약은 독자가 기술 개시의 성격을 신속하게 확인할 수 있도록 제공된다는 점을 강조한다. 이는 청구범위의 범위 또는 의미를 해석하거나 제한하는 데 사용되지 않는다는 점을 이해하여 제출된다. 또한, 전술한 상세한 설명에서 개시 내용을 간소화할 목적으로 다양한 특징들이 단일 실시형태로 함께 그룹화되어 있음을 알 수 있다. 이러한 개시 방법은 청구된 실시형태가 각 청구범위에 명시적으로 인용된 것보다 더 많은 특징을 요구한다는 의도를 반영하는 것으로 해석되어서는 안 된다. 오히려, 다음의 청구범위가 반영하는 바와 같이, 본 발명의 주제는 개시된 단일 실시형태의 모든 특징보다 적다. 따라서 다음의 청구범위는 상세한 설명에 포함되며, 각 청구범위는 그 자체로 별도의 실시형태다.

[0135] 첨부된 청구범위에서, "포함하는" 및 "~에서"라는 용어는 각각 "포함하는" 및 "여기서"라는 각각의 용어에 대한 일반 영어 등가물로 사용된다. 더욱이, "첫 번째", "두 번째", "세 번째" 등의 용어는 단지 라벨로만 사용되며 해당 개체에 수치적 요구 사항을 부과하려는 의도는 없다.

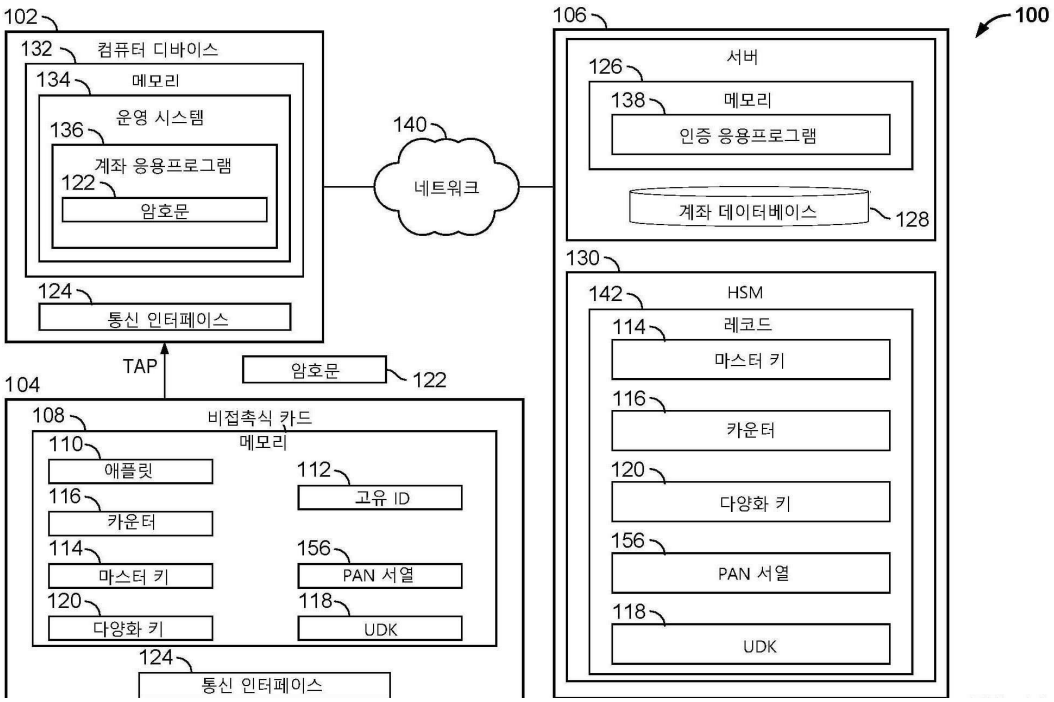
[0136] 상기에 설명된 것은 개시된 아키텍처의 실시예를 포함한다. 물론, 컴포넌트 및/또는 방법론의 가능한 모든 조합을 설명하는 것은 불가능하지만, 당업자는 많은 추가 조합 및 순열이 가능하다는 것을 인식할 수 있다. 따라서, 신규 아키텍처는 첨부된 청구범위의 사상 및 범위 내에 속하는 모든 변경, 수정 및 변형을 포괄하도록

의도된다. 예시적인 실시형태에 대한 전술한 설명은 예시 및 설명의 목적으로 제시되었다. 이는 개시된 정확한 형태로 본 개시를 철저하게 제한하거나 제한하려는 의도가 아니다. 본 개시에 비추어 많은 수정 및 변경이 가능하다.

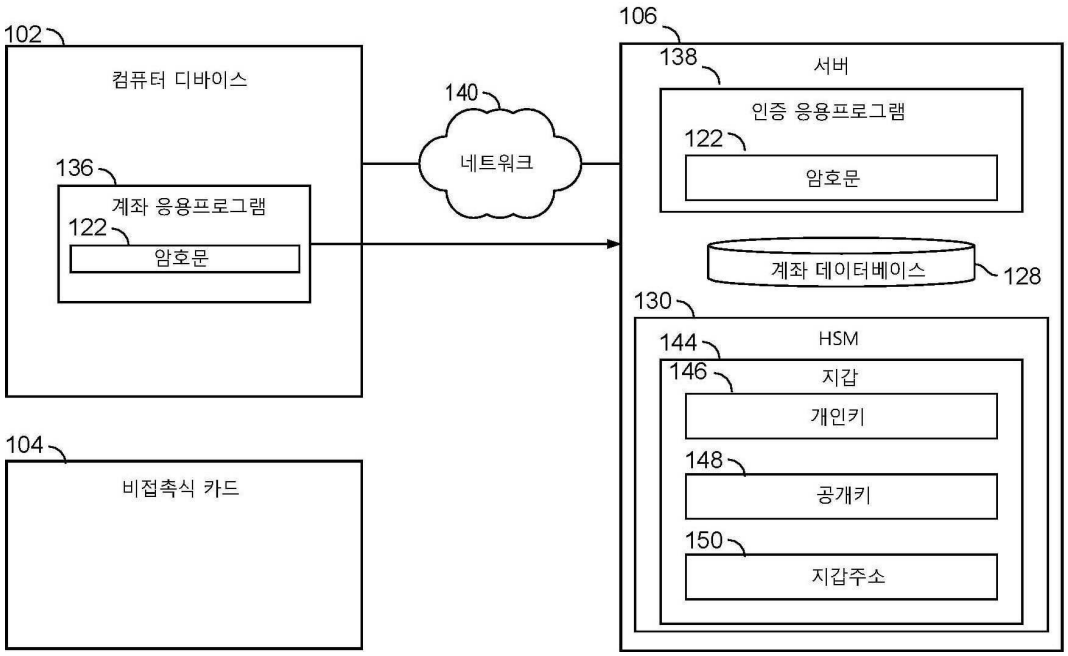
[0137] 본 발명의 범위는 이러한 상세한 설명이 아니라 여기에 첨부된 청구범위에 의해 제한되도록 의도된다. 본 출원에 대한 우선권을 주장하는 장래 출원 출원은 공개된 주제를 다른 방식으로 주장할 수 있으며, 일반적으로 본 문서에 다양하게 공개되거나 설명된 하나 이상의 제한사항 세트를 포함할 수 있다.

도면

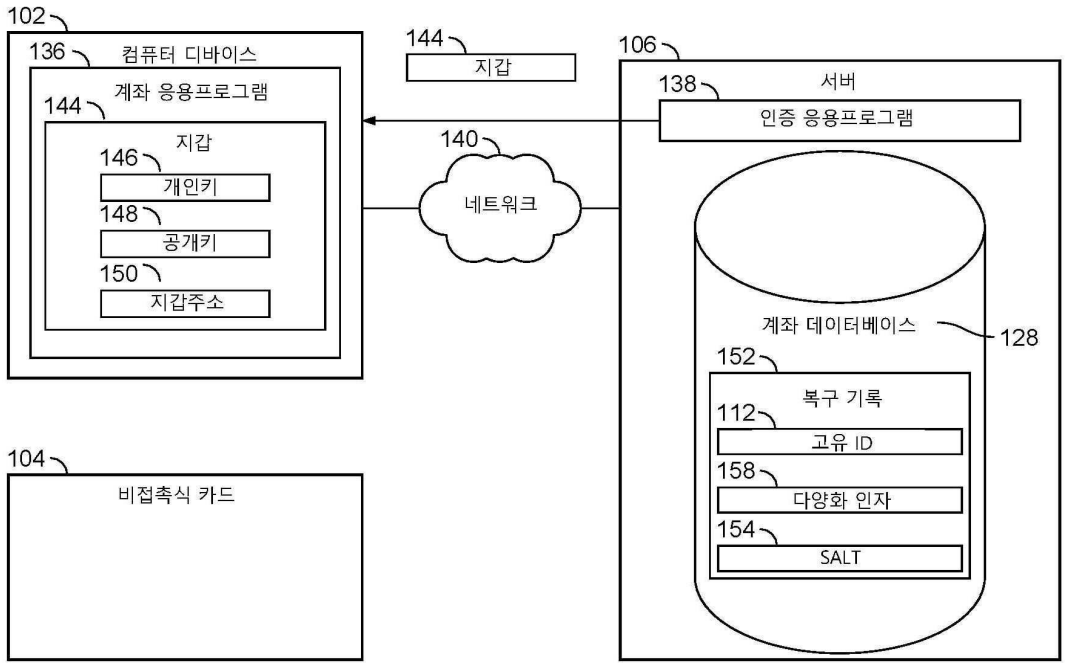
도면1a



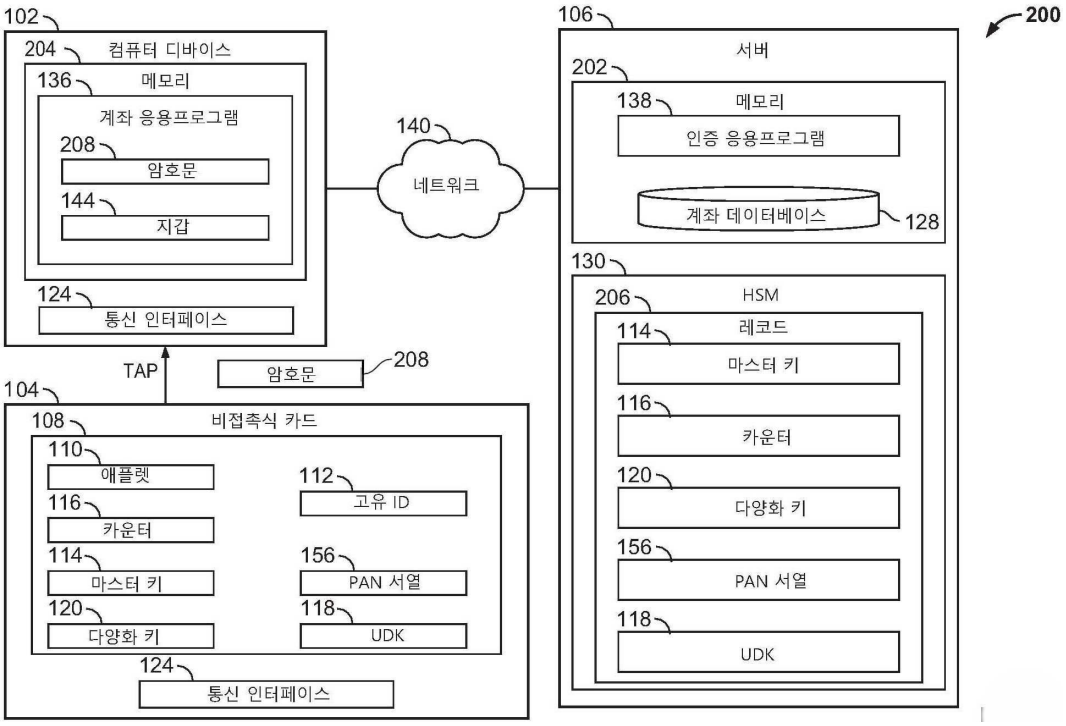
도면1b


102
컴퓨터 디바이스
136
계좌 응용프로그램
122
암호문
140
네트워크
106
138
서버
인증 응용프로그램
122
암호문
계좌 데이터베이스
128
130
HSM
144
지갑
146
개인키
148
공개키
150
지갑주소
104
비접촉식 카드

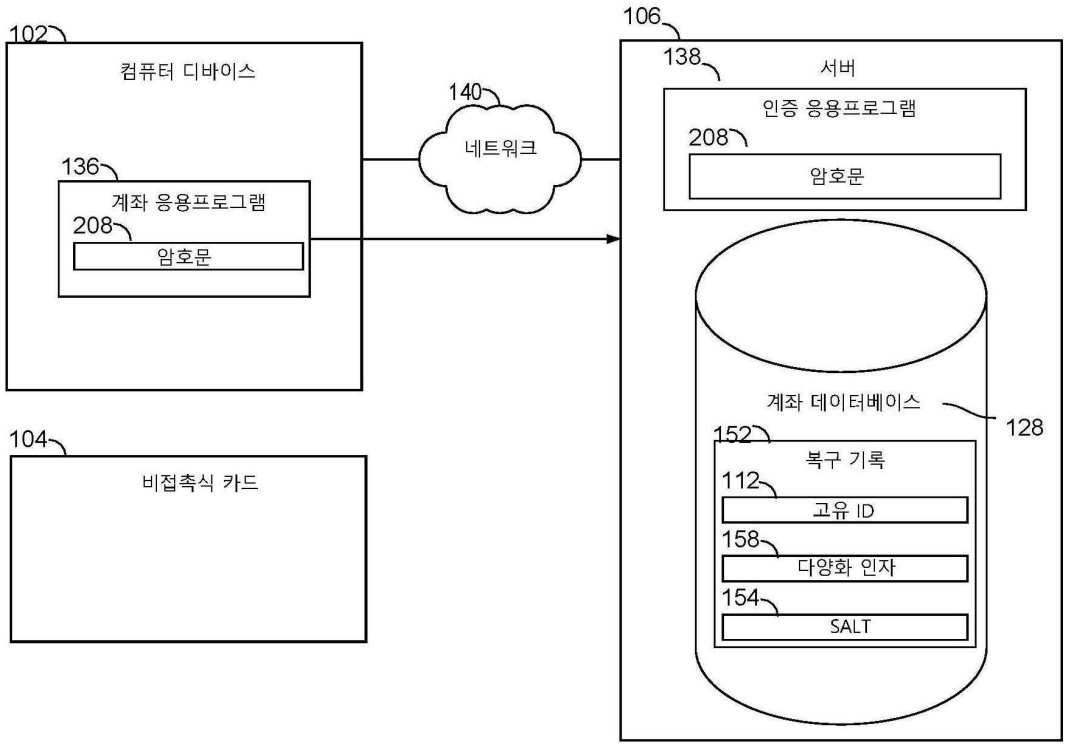
도면1c


102
136
컴퓨터 디바이스
계좌 응용프로그램
144
지갑
146
개인키
148
공개키
150
지갑주소
144
지갑
140
네트워크
106
138
서버
인증 응용프로그램
계좌 데이터베이스
128
152
복구 기록
112
고유 ID
158
다양화 인자
154
SALT
104
비접촉식 카드

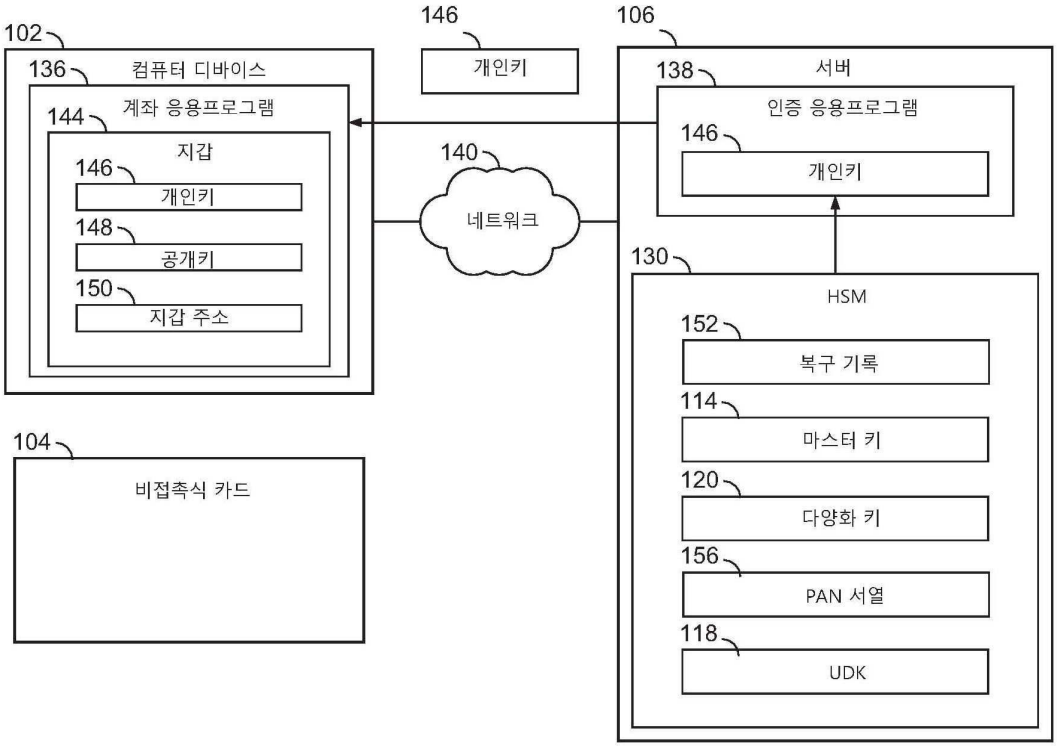
도면2a


102
204
컴퓨터 디바이스
136
메모리
계좌 응용프로그램
208
암호문
144
지갑
124
통신 인터페이스
TAP
암호문
208
104
비접촉식 카드
108
110
애플렛
112
고유 ID
116
카운터
114
마스터 키
156
PAN 서열
120
다양화 키
118
UDK
124
통신 인터페이스
140
네트워크
106
서버
202
138
메모리
인증 응용프로그램
계좌 데이터베이스
128
130
HSM
206
레코드
114
마스터 키
116
카운터
120
다양화 키
156
PAN 서열
118
UDK
200

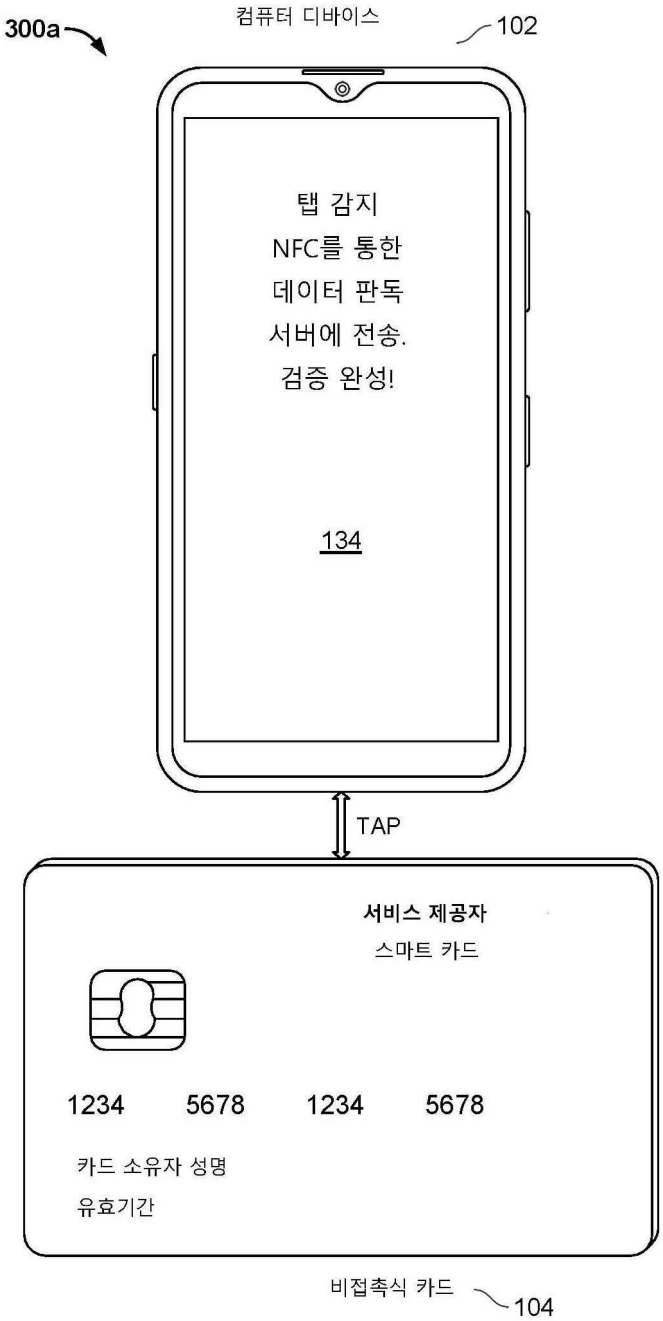
도면2b


102
컴퓨터 디바이스
136
계좌 응용프로그램
208
암호문
104
비접촉식 카드
140
네트워크
106
138
서버
인증 응용프로그램
208
암호문
계좌 데이터베이스
128
152
복구 기록
112
고유 ID
158
다양화 인자
154
SALT

도면2c


102
136
컴퓨터 디바이스
144
계좌 응용프로그램
지갑
146
개인키
148
공개키
150
지갑 주소
104
비접촉식 카드
146
개인키
140
네트워크
106
서버
138
인증 응용프로그램
146
개인키
130
HSM
152
복구 기록
114
마스터 키
120
다양화 키
156
PAN 서열
118
UDK

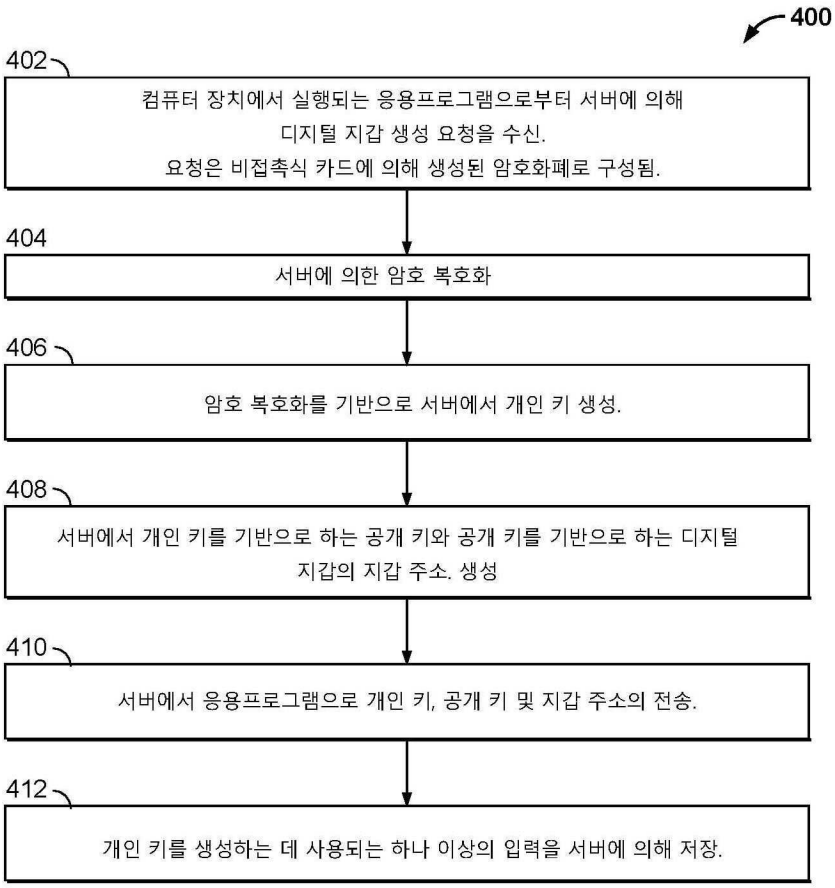
도면3a


300a
컴퓨터 디바이스
102
탭 감지
NFC를 통한
데이터 판독
서버에 전송.
검증 완성!
134
TAP
서비스 제공자
스마트 카드
1234 5678 1234 5678
카드 소유자 성명
유효기간
비접촉식 카드
104

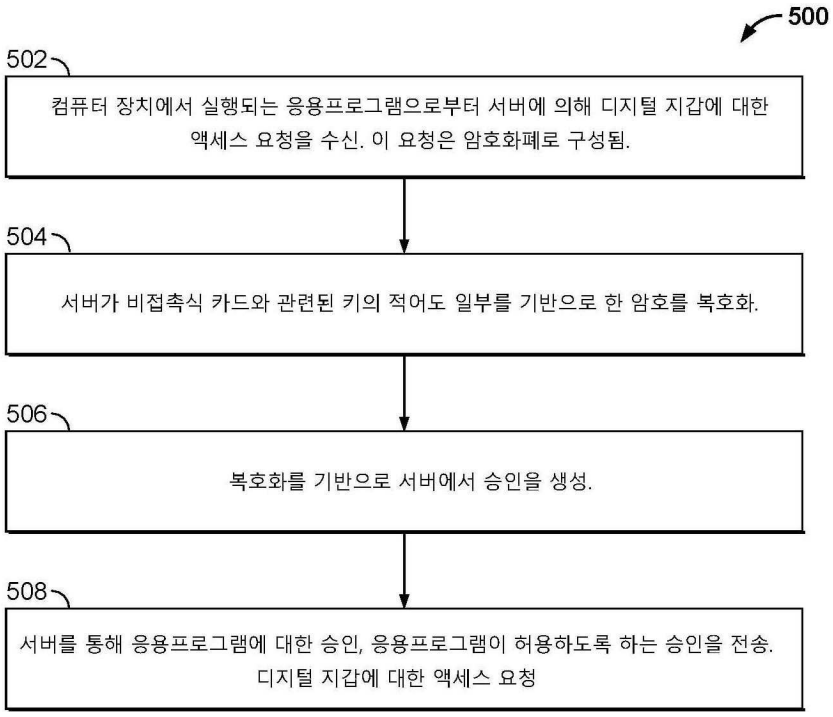
도면3b


300b
컴퓨터 디바이스
102
여기에 너의 개인키 있음
ABCDEFG...12334
스캔 코드:
302
134

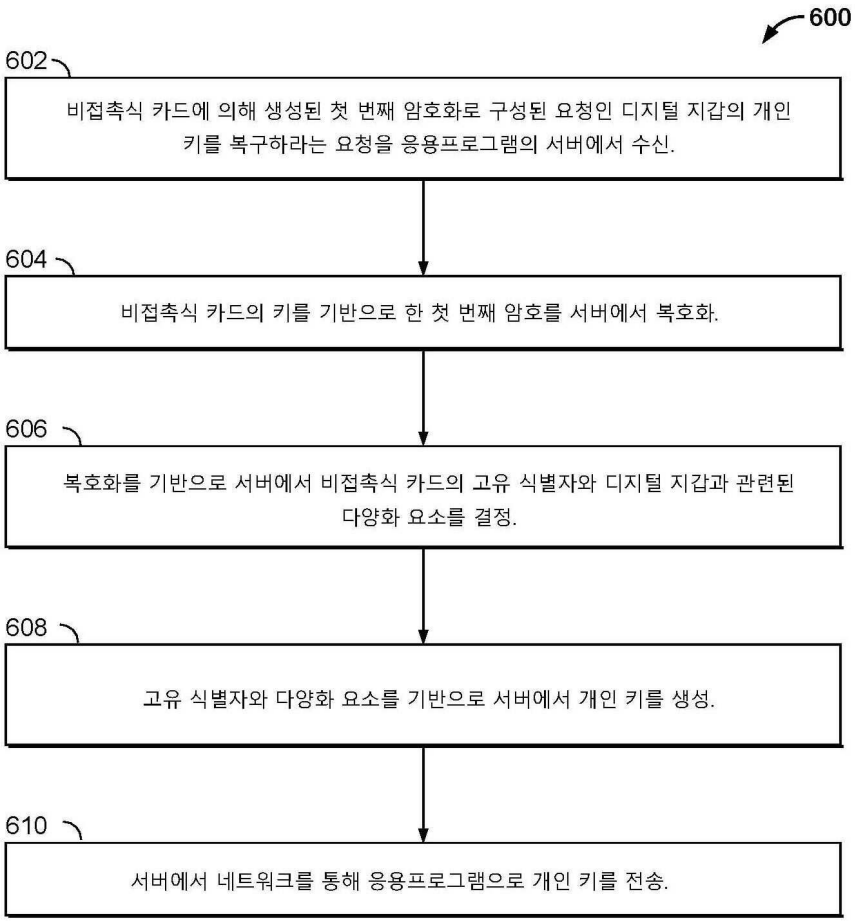
도면4


400
402
컴퓨터 장치에서 실행되는 응용프로그램으로부터 서버에 의해 디지털 지갑 생성 요청을 수신.
요청은 비접촉식 카드에 의해 생성된 암호화폐로 구성됨.
404
서버에 의한 암호 복호화
406
암호 복호화를 기반으로 서버에서 개인 키 생성.
408
서버에서 개인 키를 기반으로 하는 공개 키와 공개 키를 기반으로 하는 디지털 지갑의 지갑 주소. 생성
410
서버에서 응용프로그램으로 개인 키, 공개 키 및 지갑 주소의 전송.
412
개인 키를 생성하는 데 사용되는 하나 이상의 입력을 서버에 의해 저장.

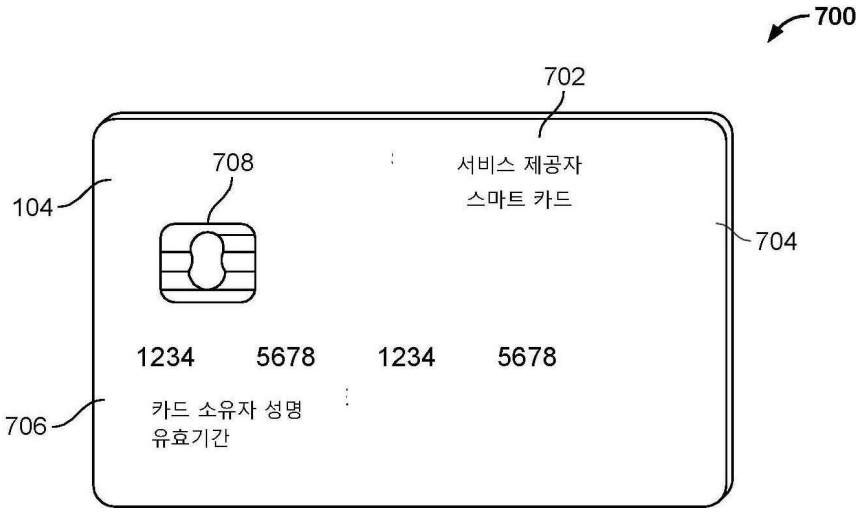
도면5


500
502
컴퓨터 장치에서 실행되는 응용프로그램으로부터 서버에 의해 디지털 지갑에 대한 액세스 요청을 수신. 이 요청은 암호화폐로 구성됨.
504
서버가 비접촉식 카드와 관련된 키의 적어도 일부를 기반으로 한 암호를 복호화.
506
복호화를 기반으로 서버에서 승인을 생성.
508
서버를 통해 응용프로그램에 대한 승인, 응용프로그램이 허용하도록 하는 승인을 전송. 디지털 지갑에 대한 액세스 요청

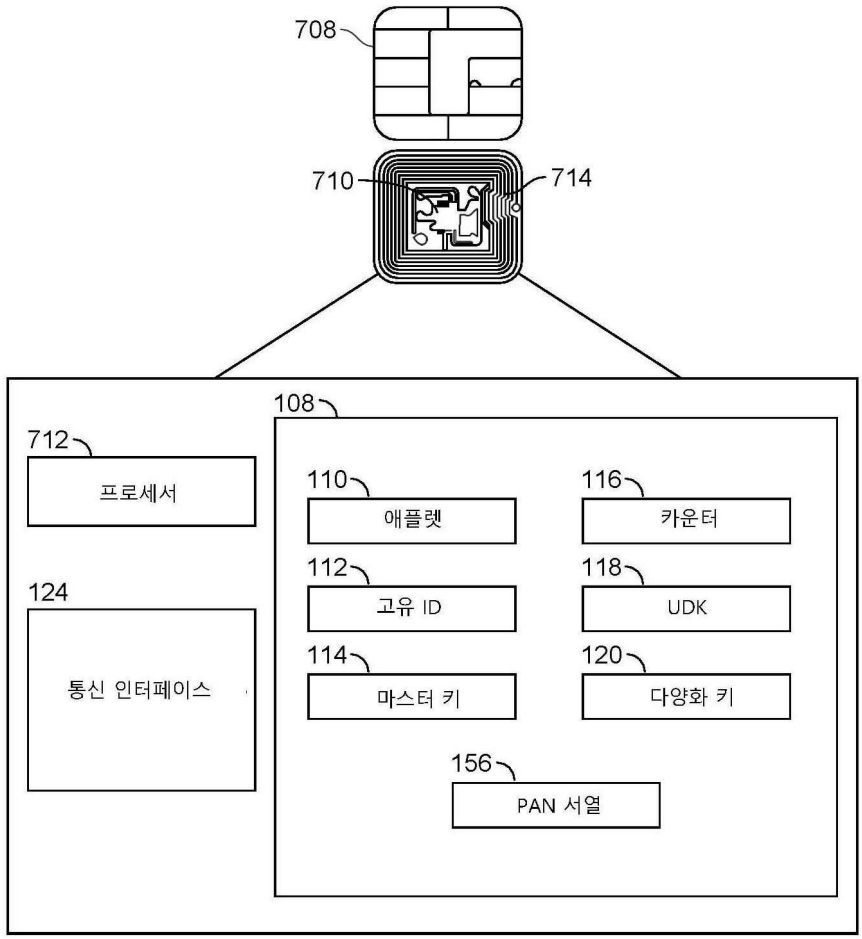
도면6


600
602
비접촉식 카드에 의해 생성된 첫 번째 암호화로 구성된 요청인 디지털 지갑의 개인 키를 복구하라는 요청을 응용프로그램의 서버에서 수신.
604
비접촉식 카드의 키를 기반으로 한 첫 번째 암호를 서버에서 복호화.
606
복호화를 기반으로 서버에서 비접촉식 카드의 고유 식별자와 디지털 지갑과 관련된 다양화 요소를 결정.
608
고유 식별자와 다양화 요소를 기반으로 서버에서 개인 키를 생성.
610
서버에서 네트워크를 통해 응용프로그램으로 개인 키를 전송.

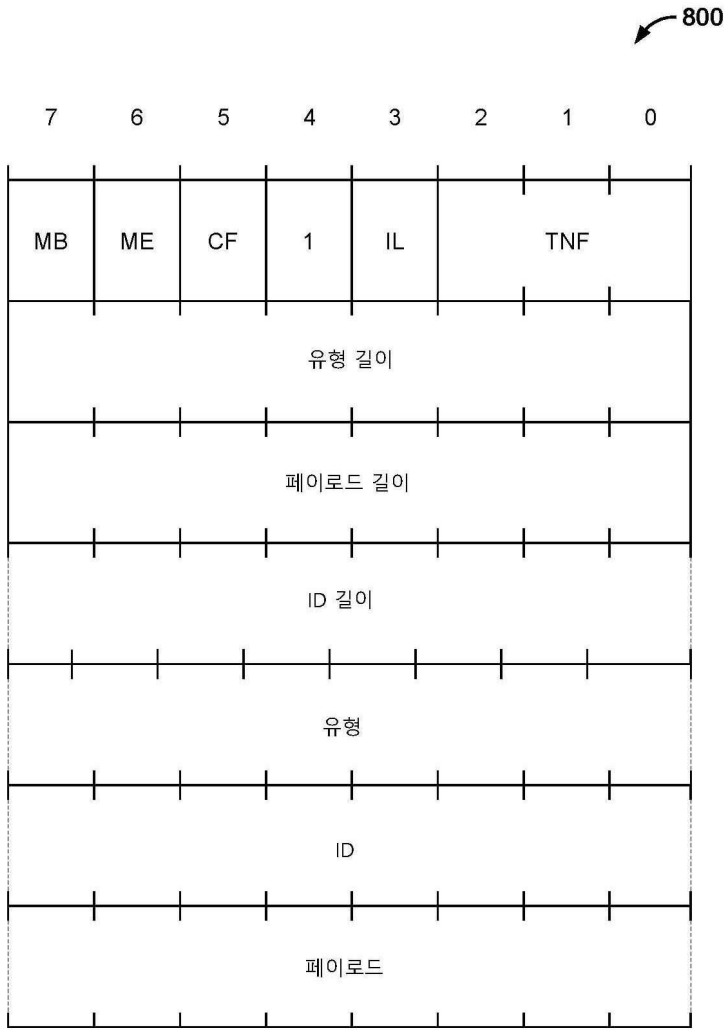
도면7a


700
702
서비스 제공자
스마트 카드
708
104
704
1234 5678 1234 5678
706
카드 소유자 성명
유효기간

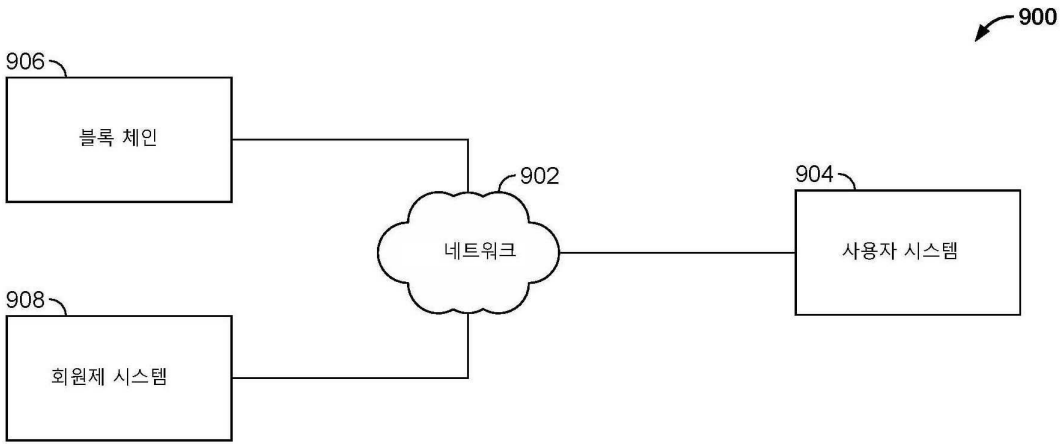
도면7b


708
710
714
108
712
프로세서
110
애플렛
116
카운터
112
고유 ID
118
UDK
124
통신 인터페이스
114
마스터 키
120
다양화 키
156
PAN 서열

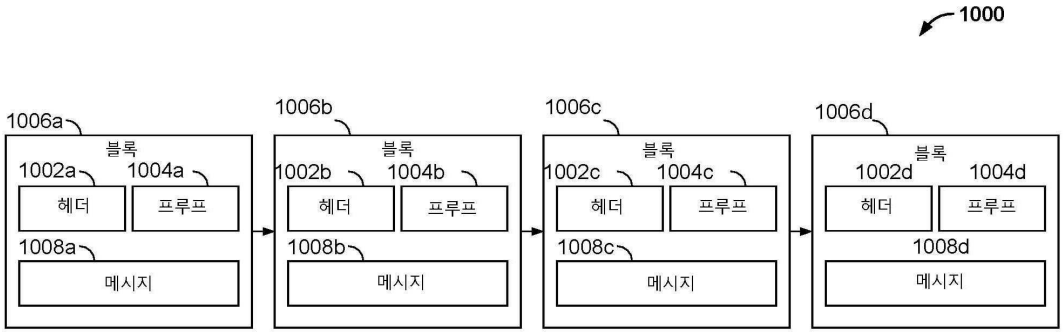
도면8


800
7
6
5
4
3
2
1
0
MB
ME
CF
1
IL
TNF
유형 길이
페이로드 길이
ID 길이
유형
ID
페이로드

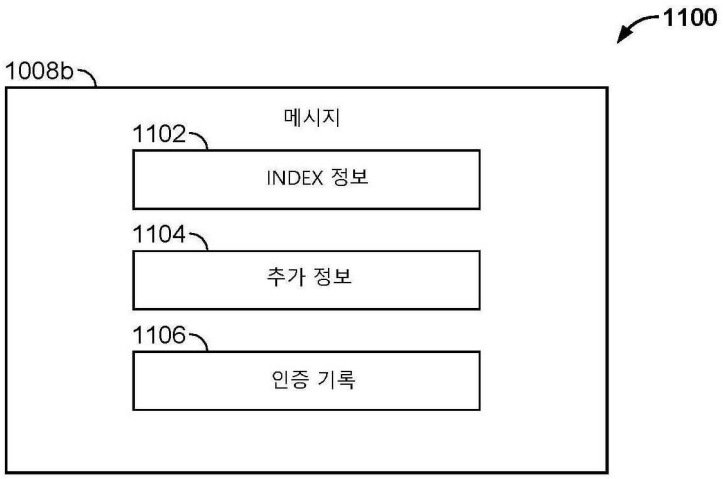
도면9


900
906
블록 체인
902
네트워크
904
사용자 시스템
908
회원제 시스템

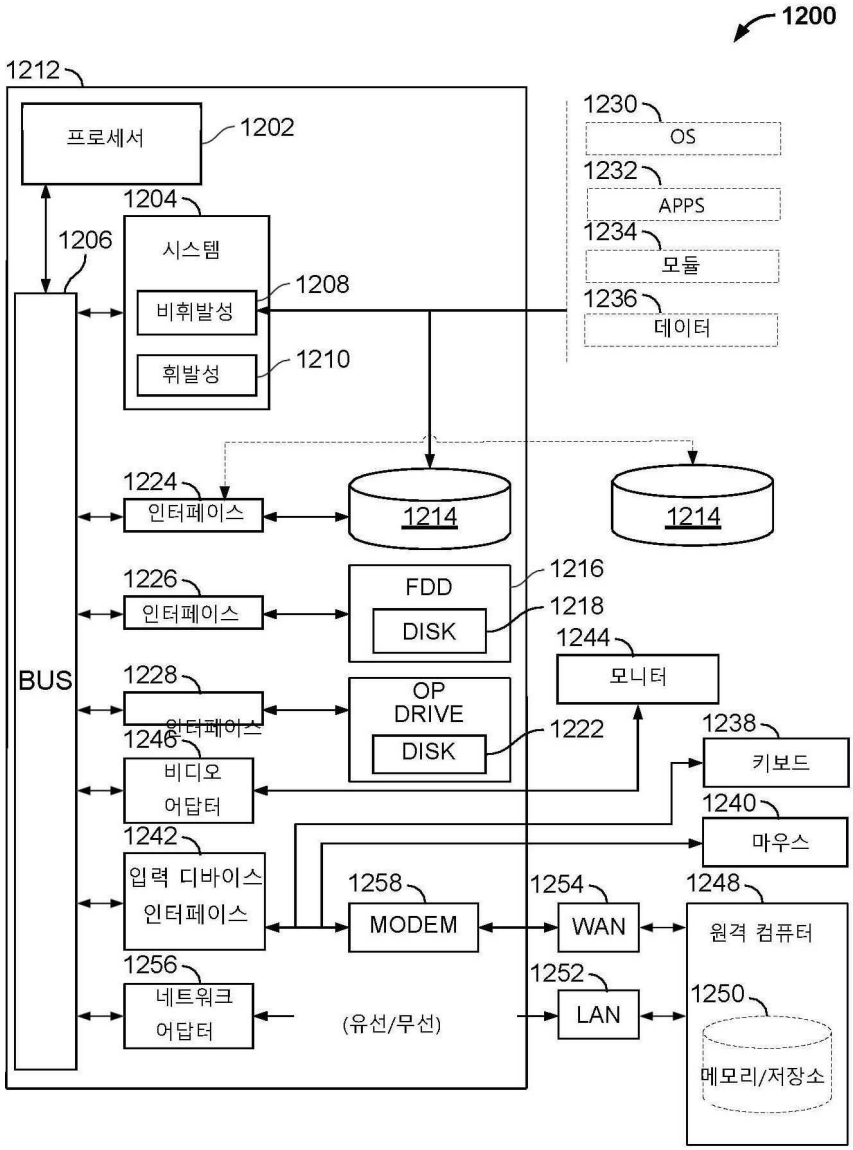
도면10


1000
1006a
블록
1002a
1004a
헤더
프루프
1008a
메시지
1006b
블록
1002b
1004b
헤더
프루프
1008b
메시지
1006c
블록
1002c
1004c
헤더
프루프
1008c
메시지
1006d
블록
1002d
1004d
헤더
프루프
1008d
메시지

도면11


1100
1008b
메시지
1102
INDEX 정보
1104
추가 정보
1106
인증 기록

도면12


1200
1212
프로세서
1202
1204
시스템
1206
1208
비휘발성
휘발성
1210
1230
OS
1232
APPS
1234
모듈
1236
데이터
1224
인터페이스
1214
1214
1226
인터페이스
FDD
DISK
1216
1218
1244
모니터
BUS
1228
OP
DRIVE
DISK
1222
1238
키보드
1246
비디오
어답터
1240
마우스
1242
입력 디바이스
인터페이스
1258
MODEM
1254
WAN
1248
원격 컴퓨터
1256
네트워크
어답터
(유선/무선)
1252
LAN
1250
메모리/저장소