(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0007169
(43) 공개일자 2024년01월16일

(51) 국제특허분류(Int. Cl.)
G06Q 20/40 (2012.01) *G06F 3/048* (2021.01)
G06Q 20/32 (2012.01) *G06Q 20/34* (2012.01)
G06Q 20/38 (2012.01) *H04W 4/80* (2018.01)
(52) CPC특허분류
G06Q 20/401 (2023.05)
G06F 3/048 (2021.01)
(21) 출원번호 10-2023-7039474
(22) 출원일자(국제) 2022년03월22일
심사청구일자 없음
(85) 번역문제출일자 2023년11월16일
(86) 국제출원번호 PCT/US2022/021272
(87) 국제공개번호 WO 2022/240484
국제공개일자 2022년11월17일
(30) 우선권주장
17/317,262 2021년05월11일 미국(US)

(71) 출원인
캐피탈 원 서비시즈, 엘엘씨
미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680
(72) 발명자
룰, 제프리
미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680, 캐피탈 원 서비시즈 엘엘씨 내
베르게론, 조지
미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680, 캐피탈 원 서비시즈 엘엘씨 내
(뒷면에 계속)
(74) 대리인
김동완

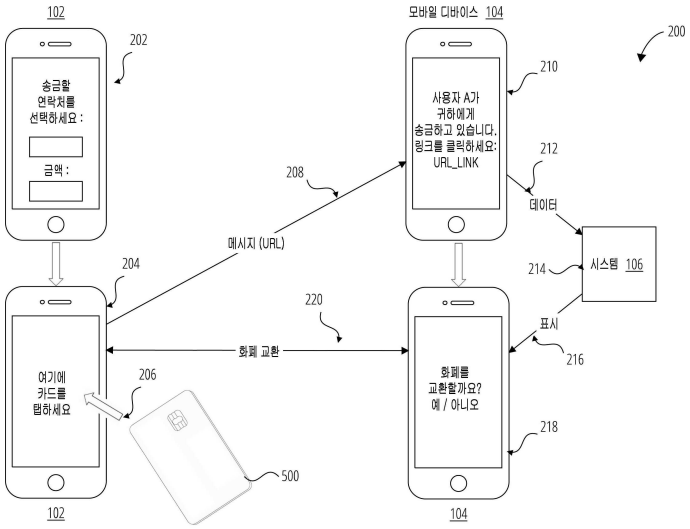
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **화폐 교환을 수행하기 위해 고유 리소스 로케이터의 활성 링크를 활용하는 시스템 및 기술**

(57) 요 약

실시형태는 일반적으로 금전을 교환하기 위해 고유 리소스 로케이터를 활용하는 시스템, 디바이스 및 기술에 관한 것이다.

대 표 도



(52) CPC특허분류
G06Q 20/3278 (2013.01)
G06Q 20/352 (2013.01)
G06Q 20/381 (2013.01)
G06Q 20/3829 (2013.01)
G06Q 20/386 (2023.05)
H04W 4/80 (2018.02)
(72) 발명자
뉴맨, 케이틀린
미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680, 캐피탈 원 서비시즈 엘엘씨 내
하트, 콜린
미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680, 캐피탈 원 서비시즈 엘엘씨 내

명 세 서

청구범위

청구항 1

디스플레이 디바이스;

프로세서; 및

명령어를 포함하는 메모리; 를 포함하는 모바일 디바이스에 있어서,

상기 메모리는 프로세서에 의해 실행될 때 프로세서가

제1 사용자의 제2 모바일 디바이스와 전자 화폐 교환을 수행하기 위한 입력을 수신하고;

디스플레이 디바이스가 모바일 디바이스에 비접촉식 카드를 제공하라는 표시를 제시하게 하고;

제2 사용자의 개인 키로 암호화된 제1 데이터를 비접촉식 카드로부터 수신하고;

고유 리소스 로케이터(URL)은 제2 모바일 디바이스가 제1 데이터로 제2 사용자의 인증을 수행하도록 형상화 되며, 제2 모바일 디바이스에 전달하기 위한 제1 데이터를 포함하는 URL 을 포함하는 메시지를 생성하고;

메시지를 제2 모바일 디바이스에 전달하고; 및

제2 사용자의 인증을 기반으로 전자 화폐 교환을 유발;

하도록 유도함을 특징으로 하는 모바일 디바이스.

청구항 2

제 1항에 있어서, 메모리 및 프로세서에 결합된 입력 디바이스를 포함하고, 입력 디바이스는 연락처 선택, 전자적으로 교환할 표시된 금액 또는 이들의 조합을 포함하는 입력을 수신하도록 형상화 됨을 특징으로 하는 모바일 디바이스.

청구항 3

제 2항에 있어서, URL은 금액을 식별하기 위한 제1 식별자와, 제1 사용자를 식별하기 위한 제2 식별자를 더욱 포함함을 특징으로 하는 모바일 디바이스.

청구항 4

제 1항에 있어서, 프로세서는

비접촉식 카드를 근거리 통신(NFC) 신호를 통해 감지하고;

모바일 디바이스의 통신 범위 내에 진입하는 비접촉식 카드에 기반하여 비접촉식 카드와의 NFC 교환을 개시하고; 및

NFC 교환을 통해 비접촉식 카드로부터 제1 데이터를 수신;

하도록 유도함을 특징으로 하는 모바일 디바이스.

청구항 5

제 1항에 있어서, URL은 활성화될 때 제1 데이터로 제2 사용자의 인증을 수행하기 위해 제2 모바일 디바이스에

서 웹페이지를 실행하도록 형상화 된 링크를 포함함을 특징으로 하는 모바일 디바이스.

청구항 6

제1항에 있어서, 제1 데이터는 비접촉식 카드에 저장된 개인 키로 암호화된 문자열을 포함함을 특징으로 하는 모바일 디바이스.

청구항 7

제 1항에 있어서, 개인 키는 키 쌍의 일부이고, 키 쌍은 비접촉식 카드, 제1 사용자 또는 이들의 조합과 연관된 공개 키를 더욱 포함함을 특징으로 하는 모바일 디바이스.

청구항 8

제 1항에 있어서, 프로세서는 제2 사용자가 성공적으로 인증되었음을 나타내는 결과를 제2 모바일 디바이스로부터 수신하고, 결과에 기반하여 전자 교환을 유도하기 위한 것임을 특징으로 하는 모바일 디바이스.

청구항 9

제 1항에 있어서, 프로세서는 단문 메시지 서비스(SMS) 메시지, 멀티미디어 메시지 서비스(MMS) 메시지 또는 리치 통신 서비스(RCS) 메시지로서 제2 모바일 디바이스에 메시지를 전달하기 위한 것임을 특징으로 하는 모바일 디바이스.

청구항 10

입력 디바이스;

프로세서; 및

명령어를 저장하는 메모리;를 포함하는 모바일 디바이스에 있어서,

상기 명령어는 프로세서에 의해 실행될 때 프로세서가

URL은 모바일 디바이스가 제1 데이터로 제1 사용자의 인증을 수행하도록 형상화 되며, 제2 모바일 디바이스로부터 제1 데이터를 포함하는 고유 리소스 로케이터(URL)를 포함하는 메시지를 수신하고;

URL을 활성화하기 위한 입력을 입력 디바이스를 통해 감지하고;

서버와 통신하여 제1 데이터로 제1 사용자의 인증을 수행하도록 형상화 된 응용프로그램을 입력에 응답하여 실행하고;

제1 사용자가 서버에 의해 인증되었다는 표시를 수신하고; 및

제1 데이터와 제1 사용자가 인증되었다는 표시를 기반으로 화폐 교환을 수행;

하도록 유도함을 특징으로 하는 모바일 디바이스.

청구항 11

제 10항에 있어서, 입력 디바이스는 터치스크린 인터페이스를 포함하고, 터치스크린 인터페이스는 디스플레이 디바이스 상에서 URL의 선택을 감지함을 특징으로 하는 모바일 디바이스.

청구항 12

제 11항에 있어서, URL은 선택될 때 응용프로그램을 실행하는 링크를 포함함을 특징으로 하는 모바일 디바이스.

청구항 13

제 10항에 있어서, 그래픽 사용자 인터페이스(GUI) 디스플레이에 메시지를 표시하도록 형상화 된 디스플레이 디바이스를 포함함을 특징으로 하는 모바일 디바이스.

청구항 14

제 10항에 있어서, 프로세서는 제1 사용자의 인증을 수행하기 위해 서버로 제1 데이터를 전달함을 특징으로 하는 모바일 디바이스.

청구항 15

제 14항에 있어서, URL은 교환할 금액의 제1 식별자, 제1 사용자를 식별하는 제2 식별자를 더욱 포함하고, 프로세서는 제1 식별자와 제2 식별자 중 적어도 하나를 서버에 전달함을 특징으로 하는 모바일 디바이스.

청구항 16

제 15항에 있어서, 프로세서는 금액 및 인증된 제1 사용자에 기반하여 교환의 수행을 유도함을 특징으로 하는 모바일 디바이스.

청구항 17

제 10항에 있어서, 제1 데이터는 제1 사용자와 연관된 암호화된 문자열을 포함하고, 표시는 암호화된 문자열이 제1 사용자와 연관된 개인 키로 성공적으로 복호화 되었음을 나타내는 정보를 포함함을 특징으로 하는 모바일 디바이스.

청구항 18

제 17항에 있어서, 암호화된 문자열은 제1 사용자와 연관된 비접촉식 카드에 저장된 개인 키로 암호화됨을 특징으로 하는 모바일 디바이스.

청구항 19

제10항에 있어서, 프로세서는 단문 메시지 서비스(SMS) 메시지, 멀티미디어 메시지 서비스(MMS) 메시지 또는 리치 통신 서비스(RCS) 메시지로 메시지를 수신하기 위한 것임을 특징으로 하는 모바일 디바이스.

청구항 20

제2 모바일 디바이스의 제2 사용자와의 화폐 교환 요청을 제1 사용자와 연관된 제1 모바일 디바이스의 프로세서에 의해 감지하는 단계;

제1 사용자 디바이스 상에 비접촉식 카드를 탭 하도록 제1 사용자 디바이스와 연관된 제1 사용자에게 요청하는 프롬프트를 디스플레이 디바이스 상에서 유도하는 단계;

제1 사용자와 연관된 개인 키로 암호화된 제1 데이터를 비접촉식 카드로부터 수신하는 단계;

제2 모바일 디바이스가 제1 데이터로 제1 사용자의 인증을 수행하게 하도록 형상화 되고, 제2 사용자 디바이스로 전달하기 위한 제1 데이터를 더욱 포함하는 고유 리소스 로케이터(URL)를 포함하는 텍스트 메시지를 생성하는 단계;

제2 모바일 디바이스에 메시지를 전달하는 단계;

제1 사용자가 인증되었음을 나타내는 표시를 제2 모바일 디바이스로부터 수신하는 단계; 및

금전을 교환하기 위해 제2 모바일 디바이스와 정보를 교환하는 단계;

를 포함하는 컴퓨터 구현 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 2021년 5월 11일자로 출원된 " 화폐 교환을 수행하기 위해 고유 리소스 로케이터의 활성 링크를 활용하는 시스템 및 기술"이라는 제목의 미국 특허출원 제17/317,262호에 대한 우선권을 주장한다. 언급된 특허출원의 내용은 그 전체로 본 발명에 참고문헌으로 포함된다.

배 경 기 술

[0002] 사용자가 다른 사용자와 금전을 교환할 수 있는 전자 결제 시스템 즉 피어-투-피어 결제 트랜잭션에는 여러 유형이 있다. 이론적으로 기존 전자 결제 시스템은 사용자 간 화폐 교환에 편리한 방법을 제공한다. 그러나 기존의 전자 결제 시스템에는 종종 사용자의 불만과 혼란을 야기하고 만족스럽지 못한 교환을 초래하는 몇 가지 단점이 존재한다.

[0003] 기존 전자 결제 시스템의 한 가지 단점은 일반적으로 송금인과 수신인 모두가 가입해야 하는 독립형 시스템이며 사용자가 트랜잭션을 완료하기 위해 다수의 단계를 거쳐야 한다는 점이다. 경우에 따라 송금인, 수신인 또는 모두는 다른 뱅킹 시스템을 통해 결제를 송금 및 수신하기 위해 시스템을 이용하여 계정을 설정하고 민감한 금융 정보를 제공하는 시간 소모적인 프로세스를 거쳐야 할 수도 있다. 사용자는 최초 트랜잭션 이후 전자 결제 시스템을 거의 사용하지 않는 경우가 종종 있다.

[0004] 기존 전자 결제 시스템의 제한적인 특성도 불편을 가중시킨다. 특히 기존 전자 결제 시스템의 독립형 특성으로 인해 일반적으로 사용자는 결제를 전송하거나 수신하기 위해 결제 트랜잭션 전용의 별도 응용프로그램을 열어야 한다. 기존 전자 결제 시스템의 독립형 특성으로 인한 불편함은 사용자가 이러한 시스템을 사용하는 것을 방해할 수 있다. 따라서 기존 전자 결제 시스템 및 방법에는 많은 단점이 존재한다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0005] 실시형태는 디스플레이 디바이스, 프로세서 및 메모리를 지니는 모바일 디바이스를 포함하는 시스템, 디바이스, 기술 및 방법을 포함할 수 있다. 메모리는 프로세서에 의해 실행될 때 프로세서가 제1 사용자의 제2 모바일 디바이스와 전적 화폐 교환을 수행하기 위한 입력을 수신하고,디스플레이 디바이스가 모바일 디바이스에 비접촉식 카드를 제공하라는 표시를 표시하고,제2 사용자의 개인 키로 암호화 된 제1 데이터를 비접촉식 카드로부터 수신하고,제2 모바일 디바이스가 제1 데이터로 제2 사용자의 인증을 수행하게 하도록 형상화 되고, 제2 모바일 디바이스에 전달하기 위한 제1 데이터를 포함하는 고유 리소스 로케이터(URL)를 포함하는 메시지를 생성하고,제2 모바일 디바이스에 메시지를 전달하고 및제2 사용자의 인증을 기반으로 전자 화폐 교환을 유발하도록 유도하는 명령어를 포함할 수 있다.

[0006] 또한 실시형태는 입력 디바이스, 프로세서 및 메모리를 지니는 모바일 디바이스를 포함하는 시스템, 디바이스, 기술 및 방법을 포함한다. 메모리는 프로세서에 의해 실행될 때 프로세서가 모바일 디바이스가 제1 데이터로 제

1 사용자의 인증을 수행하게 하도록 형상화 되고, 제2 모바일 디바이스로부터의 제1 데이터를 포함하는 고유 리소스 로케이터(URL)를 포함하는 메시지를 수신하고, URL을 활성화 하기 위한 입력을 입력 디바이스를 통해 감지하고, 서버와 통신하여 제1 데이터로 제1 사용자의 인증을 수행하도록 형상화 된 응용프로그램을 입력에 응답하여 실행하고, 제1 사용자가 서버에 의해 인증되었다는 표시를 수신하고 및 제1 데이터와 제1 사용자가 인증되었다는 표시를 기반으로 화폐 교환을 수행; 하도록 유도하는 명령어를 포함할 수 있다.

[0007] 또한 실시형태는 시스템, 디바이스, 기술 및 방법을 포함하며 방법은 제2 모바일 디바이스의 제2 사용자와의 화폐 교환 요청을 제1 사용자와 연관된 제1 모바일 디바이스의 프로세서에 의해 감지하는 단계, 제1 사용자 디바이스 상에 비접촉식 카드를 탭 하도록 제1 사용자 디바이스와 연관된 제1 사용자에게 요청하는 프롬프트를 디스플레이 디바이스 상에서 유도하는 단계. 제1 사용자와 연관된 개인 키로 암호화된 제1 데이터를 비접촉식 카드로부터 수신하는 단계, 제2 모바일 디바이스가 제1 데이터로 제1 사용자의 인증을 수행하게 하도록 형상화되고, 제2 사용자 디바이스로 전달하기 위한 제1 데이터를 더욱 포함하는 고유 리소스 로케이터(URL)를 포함하는 텍스트 메시지를 생성하는 단계; 제2 모바일 디바이스에 메시지를 전달하는 단계; 제1 사용자가 인증되었음을 나타내는 표시를 제2 모바일 디바이스로부터 수신하는 단계; 금전을 교환하기 위해 제2 모바일 디바이스와 정보를 교환하는 단계;를 포함하는 컴퓨터 구현 방법을 포함한다.

도면의 간단한 설명

[0008] 도 1은 본 발명에 논의된 실시형태에 따른 시스템(100)의 실시예를 도시한다.

도 2는 하나의 실시형태에 따른 청구 대상의 측면을 도시한다.

도 3은 본 발명에 논의된 실시형태에 따른 루틴(300)을 도시한다.

도 4는 본 발명에 논의된 실시형태에 따른 루틴(400)을 도시한다.

도 5는 실시형태에 따른 비접촉식 카드(500)를 도시한다.

도 6은 실시형태에 따른 트랜잭션 카드 컴포넌트(600)를 도시한다.

도 7은 실시형태에 따른 시퀀스 흐름(700)을 도시한다.

도 8은 실시형태에 따른 키 시스템(800)의 도면이다.

도 9는 실시형태에 따라 암호문을 생성하기 위한 흐름도(900)의 예이다.

도 10은 실시형태에 따른 흐름도(1000)의 실시예를 도시한다.

도 11은 실시형태에 따른 흐름도(1100)의 실시예를 도시한다.

도 12는 하나의 실시형태에 따른 컴퓨터 아키텍처(1200)를 도시한다.

도 13은 하나의 실시형태에 따른 통신 아키텍처(1300)를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0009] 본 발명에 논의된 실시형태는 일반적으로 사용자가 안전하고 효율적인 방식으로 금전을 교환할 수 있게 하는 디바이스, 시스템 및 기술에 관한 것일 수 있다. 예를 들어 자신의 모바일 디바이스를 사용하는 사용자는 자신의 모바일 디바이스를 통해 다른 사용자에게 금전을 보낼 수 있다. 교환은 송금인이 모바일 디바이스의 뱅킹 응용프로그램과 상호 작용함으로써 수행될 수 있다. 상세하게는 뱅킹 응용프로그램은 사용자가 인물이나 연락처를 입력하고 금액을 입력하고 특정 인물이나 연락처에 금전을 보낼 수 있도록 형상화 될 수 있다.

[0010] 송금인의 뱅킹 응용프로그램은 송금인을 식별하는 정보 및 금액을 포함하는 시지를 생성할 수 있다. 메시지는 교환을 개시하기 위해 수신인의 모바일 디바이스로 전송될 수 있다. 어떤 경우에 메시지는 정보가 포함된 고유 리소스 로케이터(URL)를 포함될 수 있다. URL은 송금인을 인증하고 교환을 수행하기 위한 수신인의 모바일 디바이스 상의 뱅킹 응용프로그램을 자동으로 실행하기 위해 수신인에 의해 호출될 수 있다.

[0011] 다음 설명에서 더욱 상세히 설명하는 바와 같이 이러한 기술은 송금인을 인증하기 위해 송금인과 연관된 보안 데이터를 지니는 비접촉식 카드를 활용하기 때문에 이전 솔루션보다 더 안전하고 간소화된다. 보안 데이터는 URL 내에 포함되어 메시지를 통해 수신인의 모바일 디바이스로 전달될 수 있다. 수신인의 모바일 디바이스는 로컬 또는 서버를 통해 원격으로 송금인을 인증한 후 인증 과정의 결과에 따라 교환을 수행할 수 있다.

[0012] 또한 교환은 송금인과 수신인이 수행하는 최소한의 동작으로 발생할 수 있다. 예를 들어 송금인은 연락처를 선택하거나 입력하고 금액을 입력한 후 모바일 디바이스에 비접촉식 카드를 탭 하여 교환을 수행할 수 있다. 수신인은 메시지를 읽고 URL을 활성화하여 화폐 교환을 확인할 수 있다. 교환은 송금인의 모바일 디바이스, 수신인의 모바일 디바이스 및 뱅킹 시스템이나 제3자 시스템에서 수행되는 동작을 기반으로 발생할 수 있다. 세부사항은 다음의 상세한 설명에서 논의된다.

[0013] 도 1은 사용자가 모바일 디바이스를 통해 금전을 교환할 수 있게 하는 단계를 포함하여 본 발명에 설명된 동작을 수행하는 시스템(100)의 실시예를 도시한다. 도시된 시스템(100)은 논의 목적으로 제한된 수의 컴포넌트 및 디바이스를 포함한다. 실시형태에서 시스템(100)은 임의의 수의 사용자가 디바이스를 통해 다른 사용자에게 금전을 보낼 수 있도록 형상화 된 임의의 수의 서버, 디바이스, 네트워크 장비 등을 포함한다.

[0014] 도 1에서 시스템(100)은 모바일 디바이스(102), 모바일 디바이스(104) 및 시스템(106)을 포함하며 이들 모두는 네트워크(108) 예를 들어 인터넷을 통해 연결될 수 있다. 모바일 디바이스의 실시예는 셀룰러 전화기, 휴대 정보 단말기, 태블릿 컴퓨터 등을 포함할 수 있으며 셀룰러 프로토콜, 무선 프로토콜 등에 따라 통신하도록 형상화 된다. 예를 들어 모바일 디바이스는 금속 또는 플라스틱과 같은 재료로 만들어진 하우징을 포함할 수 있으며, 하나 이상의 프로세서, 메모리, 저장소, 입력 디바이스 예를 들어 터치스크린 인터페이스, 버튼, 센서, 마이크 등, 출력 디바이스 예를 들어 디스플레이 스피커, 진동 디바이스, 촉각 디바이스 등, 단거리 통신 라디오, 안테나 등과 같은 컴포넌트를 포함할 수 있다.

[0015] 도시된 실시예에서 모바일 디바이스(102)는 네트워크(108)를 통해 모바일 디바이스(104)와 또는 그 반대로 통신할 수 있다. 일부 경우에 모바일 디바이스는 근거리 네트워크, 무선 근거리 네트워크, 광역 네트워크 등과 같은 다른 네트워크를 통해 서로 통신할 수 있다. 또한 모바일 디바이스는 보안 포인트-투-포인트(P2P) 연결 또는 상호 간의 직접 연결을 설정하도록 형상화 될 수 있다. P2P 또는 직접 연결은 블루투스 저 에너지(BLE), Bluetooth, Wireless Fidelity(WiFi), HaLow(IEEE 802.11ah), Z-wave 또는 Zigbee와 같은 프로토콜을 활용하여 설정될 수 있다.

[0016] 실시형태에서 모바일 디바이스는 운영 체제, 응용프로그램 또는 앱과 같은 소프트웨어를 포함한다. 운영 체제는 ANDRIOD®, IOS® 또는 WINDOWS®와 같은 임의의 유형의 운영 체제일 수 있으며 모바일 디바이스의 하드웨어, 소프트웨어 리소스를 관리하고 다른 응용프로그램에 서비스를 제공하도록 형상화 된다. 응용프로그램은 모바일 디바이스에서 작동하고 사용자에게 서비스와 경험을 제공하도록 설계된 소프트웨어 응용프로그램일 수 있다.

[0017] 응용프로그램의 실시예는 이메일 응용프로그램, 메시지 응용프로그램, 전화 응용프로그램, 연락처 데이터베이스, 캘린더 응용프로그램 등과 같은 생산성 응용프로그램을 포함한다. 다른 응용프로그램은 게임 응용프로그램, 지도 응용프로그램, 위치 기반 서비스 등을 포함할 수 있다.

[0018] 또한 본 발명에 논의된 실시형태에서 모바일 디바이스는 하나 이상의 은행 계좌와 연관된 은행 응용프로그램을 포함할 수 있으며 사용자가 상호 간에 금전을 송금 및 수신할 수 있게 하는 단계를 포함하여 사용자에게 뱅킹 서비스를 제공하도록 형상화 된다. 뱅킹 응용프로그램은 예를 들어 계좌 관리, 청구서 지불, 계좌 검토 등과 같은 추가 뱅킹 서비스를 제공하도록 형상화 될 수 있다. 높은 수준에서 뱅킹 응용프로그램은 하나 이상의 그래픽 사용자 인터페이스(GUI) 디스플레이 내에서 사용자에게 정보를 표시하고, 사용자 입력 및 선택을 처리하고, 다른 응용프로그램과 통신하고, 하나 이상의 백-엔드 시스템인 뱅킹 서버 및 서비스와 통신하는 것 등을 위해 형상화 되어 뱅킹 서비스를 제공할 수 있다.

[0019] 또한 모바일 디바이스(102 및 104)는 네트워크(108)를 통해 시스템(106)에 결합될 수 있다. 시스템(106)은 하나 이상의 서버 또는 컴퓨터 디바이스를 포함할 수 있으며 모바일 응용프로그램이 금전을 송금/수신할 수 있도록 하나 이상의 서비스를 제공할 수 있다. 하나의 실시예에서 시스템(106)은 다른 사용자에게 금전을 송금하도록 요청하거나 다른 사용자로부터 금전을 요청하는 사용자를 인증하기 위해 인증 동작을 수행하도록 형상화 된 뱅킹 시스템일 수 있다. 시스템(106)은 일반 은행 서비스, 계좌 관리, 결제 서비스 등과 같은 추가 서비스를 제공할 수도 있다. 실시형태는 이러한 방식으로 제한되지 않는다.

[0020] 일부 경우에 시스템(106)은 모바일 디바이스(102 및 104) 사이의 화폐 교환을 처리하도록 형상화 될 수 있다. 예를 들어 시스템(106)은 송금인의 계좌에서 금전을 전자적으로 공제하고 수신인의 계좌에 금전을 전자적으로 추가할 수 있다. 일부 경우에 송금인은 제1 금융 시스템과 연관될 수 있고 수신인은 제2 금융 시스템과 연관될 수 있다. 뱅킹 시스템은 화폐 교환을 조정하기 위해 상호 간에 데이터를 통신할 수 있다. 다음의 상세한 설명에서 도 2는 시스템(100)을 활용하여 화폐 교환을 수행하기 위한 추가 세부사항을 도시한다.

[0021] 도 2는 제1 모바일 디바이스(102)에서 제2 모바일 디바이스(104)로 금전을 송금하기 위해 시스템(100)에서 수행될 수 있는 시퀀스 다이어그램(200)의 실시예이다. 도 2는 하나의 가능한 시퀀스를 도시하며 일부 실시형태에서 하나 이상의 동작이 다른 동작 이전, 이후 및 동시에 발생할 수 있다. 또한 하기 더욱 상세히 설명되는 바와 같이 사용자는 다른 사용자에게 금전을 요청할 수도 있다.

[0022] 202에서 모바일 디바이스(102)는 사용자가 금전을 송금 또는 요청하는 정보를 입력하도록 하나 이상의 GUI 디스플레이를 표시할 수 있다. 상세하게는 뱅킹 응용프로그램 또는 웹 브라우저와 같은 모바일 응용프로그램을 포함하는 모바일 디바이스(102)는 하나 이상의 GUI 디스플레이를 표시한다. 디스플레이는 사용자가 선택을 하고, 옵션과 메뉴를 탐색하고, 동작을 수행하는 등 상호 작용하도록 형상화 될 수 있다. GUI 디스플레이는 임의의 유형의 입력 엘레멘트 예를 들어 입력 필드, 드롭다운 메뉴, 터치 기반 메뉴 또는 버튼 등으로 형상화 될 수 있으며 모바일 디바이스(102)는 입력 디바이스 예를 들어 버튼, 스크롤 휠, 터치스크린 인터페이스 등에 의해 감지된 사용자 입력을 처리하도록 형상화 된다.

[0023] 도시된 실시예에서 뱅킹 응용프로그램은 사용자가 연락처와 금액을 입력할 수 있는 영역을 제공한다. 텍스트 필드는 자동 완성, 제안과 같은 기능을 포함할 수 있으며 이메일 주소, 전화번호, 사용자 이름 등과 같은 다양한 형식의 연락처를 수락하도록 형상화 될 수 있다. 실시형태는 예시된 특정 GUI 디스플레이에 제한되지 않는다. 디스플레이는 다른 형식일 수 있다. 예를 들어 뱅킹 응용프로그램은 모바일 디바이스(102)의 연락처 데이터베이스로부터의 연락처 목록을 제공할 수 있다.

[0024] 일부 경우에 목록은 사용 빈도, 가까운 연락처, 친구 대 가족 등과 같은 기준에 따라 정렬될 수 있다. 일부 경우에 모바일 응용프로그램은 두 개 이상의 GUI 디스플레이 예를 들어 연락처를 입력하기 위한 제1 GUI 디스플레이 또는 페이지 및 금액을 입력하기 위한 제2 GUI 디스플레이를 제공할 수 있다. 상기 언급된 바와 같이 일부 경우에 사용자는 다른 사용자에게 금전을 요청할 수도 있다. 이러한 경우 유사한 GUI 디스플레이가 사용자에게 표시될 수 있다. 그러나 GUI 디스플레이는 사용자가 금전을 송금하는 것이 아니라 금전을 요청하고 있다는 표시를 제공한다.

[0025] 202에서 사용자는 연락처를 선택하거나 입력하고 송금하거나 요청할 금액을 제공할 수 있다. 모바일 디바이스(102)는 선택된 연락처와 연관된 디바이스 예를 들어 모바일 디바이스(104)를 결정하기 위해 입력을 처리할 수 있다. 모바일 디바이스(102)는 금전을 송금하거나 요청하려는 사용자를 인증하기 위해 인증 동작을 수행하도록 형상화 된다. 도시된 실시예에서 모바일 디바이스(102)는 사용자와 연관된 비접촉식 카드를 활용하여 인증을 수행한다.

[0026] 204에서 뱅킹 응용프로그램을 포함하는 모바일 디바이스(102)는 모바일 디바이스(102)에 카드를 탭 하도록 사용자에게 지시하는 GUI 디스플레이를 표시할 수 있다. 일부 실시예에서 GUI 디스플레이는 특정 표면 예를 들어 모바일 디바이스(102)의 디스플레이 또는 후면에 카드를 탭 하도록 사용자에게 지시할 수 있다. 모바일 디바이스(102)에 카드를 탭 하면 모바일 디바이스(102)와 카드 사이의 데이터 교환이 개시된다. 모바일 디바이스(102)와 비접촉식 카드(500) 모두는 단거리 통신 프로토콜을 활용하여 서로 통신하도록 형상화 된다.

[0027] 예를 들어 비접촉식 카드와 모바일 디바이스(102)는 하나 이상의 근거리 통신(NFC) 교환을 수행할 수 있다. 교환의 일부로서 비접촉식 카드(500)는 사용자를 인증하는 데 사용될 수 있는 정보 및 데이터를 카드(102)에 전달하도록 형상화 될 수 있다. 예를 들어 206에서 500은 500에 저장되고 사용자를 고유하게 식별하는 문자열 예를 들어 문자의 영숫자 시퀀스를 전송할 수 있다. 일부 경우에 비접촉식 카드(500)는 모바일 디바이스(102)에 의해 수행된 요청 또는 판독에 기반하여 문자열을 전송할 수 있다.

[0028] 또한 비접촉식 카드(500)는 비접촉식 카드(500)에 저장된 개인 키를 사용하여 문자열을 암호화하고 모바일 디바이스(102)에 암호화된 문자열로서 문자열을 전송할 수 있다. 개인 키는 키 쌍의 일부일 수 있으며 사용자를 인증하는데 사용되는 공개 키와 연관될 수 있다. 실시형태에서 개인 키는 카드 공급자에 의해 생성되고 이와 연관된 독점 키일 수 있다. 다른 경우에 개인 키는 Europay, Mastercard, Visa(EMV) 표준에 따라 동작을 행하는 것과 연관될 수 있다.

[0029] 206에서 모바일 디바이스(102)는 비접촉식 카드(500)로부터 수신된 정보를 처리하고 선택된 연락처와 연관된 디바이스인 모바일 디바이스(104)에 전송할 메시지를 생성할 수 있다. 실시형태에서 모바일 디바이스(102)는 연락처에 대한 식별자 또는 속성 예를 들어 전화번호, 사용자 이름, 전자 메일 이메일 주소 등을 사용하여 모바일 디바이스에 메시지를 전송하기로 결정할 수 있다. 도시된 실시예에서 모바일 디바이스(102)는 문자 메시지 프로토콜 예를 들어 SMS, MMS, RCS 등에 따라 문자 메시지를 생성한다. 그러나 실시형태에서 예를 들어 이메일, 실

시간 메시지 등과 같은 다른 형식이 활용될 수 있으며 사용자 데이터그램 프로토콜(UDP) 및 전송 제어 프로토콜(TCP)과 같은 프로토콜을 사용한다.

[0030] 메시지는 다른 사용자가 금전을 송금하거나 요청하기를 원한다는 것을 수신인에게 알리는 정보, 비접촉식 카드(500)로부터 수신된 정보 및 사용자 입력 예를 들어 선택한 연락처 및 입력된 금액에 따른 정보를 포함할 수 있다. 실시형태에서 메시지는 활성 링크 또는 활성 URL을 포함할 수도 있다. 활성 URL은 수신인이 화폐 교환을 용이하게 하기 위해 사용될 수 있다. 예를 들어 수신인은 URL을 선택하거나 활성화할 수 있으며 그 후 모바일 응용프로그램은 수신인의 디바이스를 실행하게 된다. 활성 URL은 예를 들어 모바일 디바이스(104)에서 뱅킹 앱이나 웹페이지를 실행하기 위한 딥 링크일 수 있다.

[0031] 실시형태에서 URL에는 비접촉식 카드(500)에 의해 생성된 암호화된 문자열, 수신인의 식별자, 금액의 식별자, 송금인의 식별자 중 하나 이상을 포함하는 정보가 내장될 수 있다. URL은 하나 이상의 운영 체제 및 API에 따른 형식일 수 있다. 예를 들어 메시지는 운영 체제 IOS, ANDROID 및/또는 MICROSOFT에 대한 표준 및 API에 따른 형식의 URL을 포함할 수 있다. 예시적인 형식은 "appam://<문자열> <수신인 식별자> <금액 식별자>" 또는 "https://site.com/<문자열>/<수신인 식별자>/<금액 식별자>"를 포함할 수 있으나 실시형태는 이러한 방식으로 제한되지 않는다.

[0032] 208에서 모바일 디바이스(102)는 모바일 디바이스(104) 즉 연락처와 연관된 디바이스로 메시지를 전송할 수 있다. 메시지는 메시지 유형에 기반하여 하나 이상의 통신 프로토콜에 따라 전송될 수 있다. 210에서 모바일 디바이스(104)는 메시지를 수신하고 디스플레이 디바이스에 메시지를 표시할 수 있다. 언급된 바와 같이 메시지는 모바일 디바이스(104)의 사용자에 의해 선택 가능한 활성 URL을 포함할 수 있다. 모바일 디바이스(104)는 메시지 응용프로그램의 GUI 디스플레이에 메시지를 표시할 수 있다. 사용자는 메시지와 상호 작용하고 URL을 선택하거나 클릭할 수 있다.

[0033] 모바일 디바이스(104)는 사용자가 URL을 선택 및/또는 활성화하는 것을 감지하고 URL 내의 정보에 기반하여 응용프로그램이나 웹페이지를 실행하도록 형상화 된다. 모바일 디바이스(104)는 웹 브라우저에서 뱅킹 응용프로그램 또는 웹페이지와 같은 응용프로그램을 실행할 수 있다. 또한 실시형태에서 응용프로그램을 포함하는 모바일 디바이스(104)는 URL에 내장된 정보를 처리하도록 형상화 된다.

[0034] 예를 들어 응용프로그램은 암호화된 문자열을 처리하고 송금인을 인증하기 위해 시스템(106)으로 API를 통해 암호화된 문자열을 전달할 수 있다. 실시형태에서 응용프로그램은 또한 송금인의 식별자, 수신인의 식별자 및 금액을 포함하는 다른 데이터를 시스템(106)에 전송할 수도 있다.

[0035] 214에서 시스템(106)은 모바일 디바이스(104)로부터 수신된 정보에 기반하여 송금인을 인증할 수 있다. 예를 들어 시스템(106)은 데이터베이스 또는 데이터 저장소로부터 저장된 인증 문자열을 결정하기 위한 조회를 수행하기 위해 송금인의 식별자를 활용할 수 있다. 또한 시스템(106)은 송금인과 연관된 공개 키를 결정하고 문자열을 복호화 하려고 시도할 수도 있다. 그 후 복호화 된 문자열을 인증 문자열과 비교하여 매치하는지 결정하고 송금인을 인증할 수 있다. 시스템(106)이 문자열이 매치한다고 결정하면 송금인이 인증되고 매치하지 않으면 송금인이 인증되지 않는다.

[0036] 216에서 시스템(106)은 송금인이 인증되었는지 여부에 대한 표시 또는 비교 결과를 반송할 수 있다. 인증 동작을 수행하기 위한 API 호출에 대한 결과로 표시가 전달될 수 있다. 218에서 모바일 디바이스(104)는 GUI 디스플레이 내에서 사용자에게 표시를 제시할 수 있다. 일부 경우에 모바일 디바이스(104)는 사용자가 금전을 수락하거나 거절할 수 있는 옵션을 표시할 수 있다. 모바일 디바이스(104)는 교환을 거부하고 동작을 중단하거나 화폐 교환을 위한 추가 동작을 수행하지 않기 위한 사용자 입력을 처리할 수 있다.

[0037] 대안적으로 모바일 디바이스(104)는 화폐 교환을 수락하거나 진행하기 위해 사용자 입력을 처리하고 220에서 교환을 수행하기 위한 추가 동작을 수행할 수 있다. 예를 들어 모바일 디바이스(104)는 금전의 송금을 진행하도록 모바일 디바이스(102)에 표시를 제공하거나 또는 통신할 수 있다. 모바일 디바이스(102)는 수신인과 연관된 계좌로 금전을 전자적으로 교환하라는 표시를 뱅킹 서버와 같은 하나 이상의 백-엔드 서버 및 모바일 디바이스(104)와 통신할 수 있다. 다른 경우에 응용프로그램은 화폐 교환을 진행하라는 표시를 뱅킹 서버와 통신할 수 있다.

[0038] 일부 경우에는 화폐 교환을 위해 모바일 디바이스(102)와 모바일 디바이스(104) 사이에 보안 연결이 설정될 수 있다. 보안 연결은 모바일 디바이스(102 및 104) 사이의 P2P 국소화 된 연결일 수 있다. 모바일 디바이스(102)는 모바일 디바이스(104)에 전자 토큰으로서 금전을 송금할 수 있다. 모바일 디바이스(104)는 토큰을 처리하고

은행 서버와 통신하여 교환의 표시를 제공할 수 있다. 토큰은 교환을 완료하기 위해 뱅킹 서버에서 사용할 수 있는 정보를 포함할 수 있다. 정보는 송금인의 식별자, 수신인의 식별자, 금액 등을 포함할 수 있다. 실시형태는 이러한 방식으로 제한되지 않는다.

[0039] 도 3은 시스템(100)에 의해 수행될 수 있는 예시적인 루틴(300)을 도시한다. 상세하게는 루틴(300)은 모바일 디바이스를 통해 다른 사용자에게 금전을 송금 또는 요청하도록 형상화 된 모바일 디바이스에 의해 수행될 수 있다.

[0040] 블록 302에서 루틴(300)은 제1 사용자와 연관된 제1 모바일 디바이스의 프로세서에 의해 제2 모바일 디바이스의 제2 사용자와의 화폐 교환 요청을 감지하는 단계를 포함한다. 예를 들어 모바일 디바이스는 P2P 교환을 통해 다른 사람에게 금전을 송금하거나 요청할 수 있는 하나 이상의 옵션을 사용자에게 표시할 수 있는 뱅킹 응용프로그램을 포함할 수 있다. 사용자는 금전을 송금하거나 요청할 지 선택하는 입력을 뱅킹 응용프로그램을 통해 제공할 수 있다.

[0041] 또한 사용자는 교환을 위한 추가 정보를 제공할 수 있다. 예를 들어 응용프로그램을 통해 사용자는 금전을 송금하거나 요청할 연락처나 사람 및 교환을 위한 금액을 입력할 수 있다. 모바일 디바이스는 예를 들어 다른 사용자에게 금전을 송금하기 위해 터치스크린 인터페이스를 통해 입력 선택을 수신할 수 있다.

[0042] 하나의 실시예에서 입력 선택은 모바일 디바이스에 저장된 연락처 목록에서 연락처를 선택하는 단계를 포함할 수 있다. 다른 경우에 사용자는 물리적 키보드 또는 가상 키보드와 같은 키보드를 사용하여 필드에 연락처를 입력할 수 있다. 다른 경우에 사용자는 전화번호, 이메일 주소, 사용자 이름 등과 같은 다른 식별 정보를 제공할 수 있다. 실시형태는 이들 실시예로 제한되지 않을 수 있다.

[0043] 화폐 교환을 위해 사용자는 제2 모바일 디바이스와 제2의 사용자에게 인증되어야 한다. 패스워드 제공, 생체 분석 수행, 문자 메시지로 코드 전송 등을 포함하는 일반적인 인증 방법이 활용될 수 있다. 그러나 본 발명에 설명된 실시형태는 비접촉식 카드를 활용하여 추가적인 보안을 제공할 수 있다. 도시된 루틴(300)에서 제1 사용자는 제1 사용자와 연관된 비접촉식 카드를 활용하여 인증된다. 비접촉식 카드를 사용하여 사용자를 인증하는 것은 사용자가 카드를 소유하고 비접촉식 카드가 사용자에게 고유한 토큰이나 문자열을 포함하고 있음을 보장함으로써 다른 기술에 비해 이점을 제공한다.

[0044] 더욱 상세히 논의되는 바와 같이 토큰 또는 문자열은 제3자 예를 들어 뱅킹 시스템 또는 기타 제3자 인증 시스템을 통해 사용자를 인증하는 데 사용될 수 있다. 일부 경우에 제2 사용자는 로컬 인증 문자열 및 제1 사용자와 연관된 공개 키를 활용하여 제1 사용자를 인증할 수 있다.

[0045] 비접촉식 카드로 수행된 인증 동작은 모바일 디바이스가 비접촉식 카드와 정보를 교환하는 단계를 포함하며 이는 사용자가 모바일 디바이스의 통신 범위 예를 들어 10cm 이내의 NFC 통신 범위 내에 비접촉식 카드를 가져가는 것에 의해 개시될 수 있다. 블록 304에서 루틴(300)은 제1 모바일 디바이스와 연관된 제1 사용자에게 제1 모바일 디바이스 상에 비접촉식 카드를 탭 하도록 요청하라는 프롬프트를 디스플레이 디바이스에서 유도하는 단계를 포함한다. 비접촉식 카드가 모바일 디바이스의 충분한 범위 내에 진입하면 디바이스와 카드 사이에 연결이 설정될 수 있고 모바일 디바이스는 카드와 데이터를 교환하도록 형상화 될 수 있으며 카드는 모바일 디바이스와 데이터를 교환하도록 형상화 될 수 있다.

[0046] 모바일 디바이스에 카드를 탭 하도록 사용자에게 지시하면 카드가 통신 범위 내에 있게 된다. 그러나 다른 실시형태는 비접촉식 카드를 모바일 디바이스에 가까이 가져오라고 사용자에게 지시하는 단계를 포함할 수 있으며 모바일 디바이스는 카드가 통신 범위 내에 있을 때 표시 예를 들어 메시지 또는 아이콘 표시, LED 조명 등을 제공할 수 있다.

[0047] 블록 306에서 루틴(300)은 비접촉식 카드로부터 데이터를 수신하는 단계를 포함한다. 데이터는 개인 키 예를 들어 독점 개인 키 또는 EMV 기반 개인 키를 사용하여 비접촉식 카드에 의해 암호화될 수 있으며 이는 제1 사용자와 연관되고 비접촉식 카드에 안전하게 저장된다. 어떤 경우에 비접촉식 카드는 하나 이상의 NFC 데이터 교환 형식(NDEF) 메시지를 통해 모바일 디바이스에 데이터를 전달할 수 있다. 암호화된 데이터는 비접촉식 카드에도 안전하게 저장되는 토큰 또는 문자열과 같이 제1 사용자를 식별하는 정보를 포함할 수 있다. 모바일 디바이스는 교환이 완료될 때 사용자에게 표시를 제공할 수 있으며 메시지가 제2 모바일 디바이스로 전송된다.

[0048] 실시형태에서 모바일 디바이스는 화폐 교환에 대한 표시를 생성하여 제2 사용자와 연관된 제2 모바일 디바이스로 전송할 수 있다. 예를 들어 블록 308에서 루틴(300)은 교환 정보, 고유 리소스 로케이터(URL) 및 비접촉식 카드로부터의 데이터를 지니는 텍스트를 포함하는 텍스트 메시지를 생성하는 단계를 포함한다. 문자는 송금인과

금액을 표시할 수 있다. URL은 수신인이 활성화할 때 수신 모바일 디바이스가 응용프로그램을 실행하고 비접촉식 카드의 데이터를 사용하여 제1 사용자의 인증을 수행하게 하는 활성 URL 또는 딥 링크일 수 있다.

[0049] 실시형태에서 모바일 디바이스는 메시지를 생성하고 메시지 및/또는 URL에 데이터를 내장 시킬 수 있다. 예를 들어 암호화된 문자열을 지니는 데이터는 파라미터로 URL에 통함 될 수 있다. 따라서 URL이 활성화되면 암호화된 문자열은 실행된 응용프로그램에 전달된다. 일부 경우에 모바일 디바이스는 송금인을 식별하는 식별자, 수신인을 식별하는 식별자 및 교환할 특정 금액을 포함하는 추가 정보를 URL에 포함할 수 있다. 또한 식별자와 지정된 금액은 실행된 응용프로그램에 파라미터로 전달될 수 있으며 교환을 처리하기 위해 응용프로그램에 의해 사용될 수 있다.

[0050] 블록 310에서 루틴(300)은 메시지를 제2 모바일 디바이스에 전달하는 단계를 포함한다. 메시지는 문자 메시지일 수 있으며 연관된 전화번호에 기반하여 제2 모바일 디바이스에 전달될 수 있다. 문자 메시지는 SMS, MMS, RCS 등 모든 유형의 메시지 프로토콜에 따라 전송될 수 있다. 일부 경우에 메시지, 이메일, 채팅 응용프로그램 등을 전송하는 데 다른 매체가 사용될 수도 있다. 실시형태는 이러한 방식으로 제한되지 않는다.

[0051] 실시형태에서 제2 모바일 디바이스는 메시지를 수신하고 메시지를 처리할 수 있다. 예를 들어 제2 모바일 디바이스는 GUI 디스플레이의 디스플레이 디바이스에서 제2 사용자에게 메시지를 표시할 수 있다. 제2 사용자에 의해 URL이 활성화되면 제2 모바일 디바이스는 제1 사용자 인증을 포함하는 추가 동작을 수행할 수 있다. 일부 경우에 인증은 제2 모바일 디바이스에 의해 로컬로 수행될 수도 있으며 다른 경우에 제2 모바일 디바이스는 제1 사용자를 인증하기 위해 뱅킹 시스템 또는 다른 제3자 시스템을 활용할 수 있다. 제 2 모바일 디바이스는 인증 동작의 결과를 판단하고 그 결과를 제 1 모바일 디바이스에게 제공할 수 있다.

[0052] 블록 312에서 루틴(300)은 제1 사용자가 인증되었는지 여부를 나타내는 표시를 제2 모바일 디바이스로부터 수신하는 단계를 포함한다. 표시는 문자 메시지 또는 다른 통신 매체를 통해 제2 모바일 디바이스로부터 수신될 수 있다. 표시는 인증 결과 및 제2 사용자의 화폐 교환 수락 여부에 대한 표시를 포함할 수 있다.

[0053] 제1 사용자가 인증되지 않거나 제2 사용자가 교환을 거부하는 경우, 제1 및 제2 모바일 디바이스는 교환 동작을 중단할 수 있다. 대안적으로 제1 사용자가 인증되고 제2 사용자가 교환을 수락하는 경우, 디바이스는 화폐 교환을 위한 동작을 계속 수행할 수 있다. 블록 314에서 루틴(300)은 화폐를 교환하기 위해 제2 모바일 디바이스와 정보를 교환하는 단계를 포함한다.

[0054] 어떤 경우에는 예를 들어 제1 및 제2 모바일 디바이스가 서로 멀리 떨어져 있을 때 또는 예를 들어 국소화 P2P 연결을 형성할 수 없는 경우, 모바일 디바이스는 뱅킹 시스템을 통해 화폐 교환을 수행할 수 있다. 예를 들어 송금인과 수신인은 동일한 은행 및 뱅킹 시스템에 계좌를 보유할 수 있다. 각각의 디바이스에 있는 뱅킹 응용프로그램은 뱅킹 시스템과 직접 통신하도록 형상화 될 수도 있다. 이러한 실시 예에서 제2 모바일 디바이스는 제1 사용자가 인증되고 제2 사용자가 교환을 수락하는 경우 교환이 수락되었음을 나타내는 표시를 뱅킹 시스템에 전달할 수 있다.

[0055] 표시는 API 통신을 통해 제2 모바일 디바이스의 뱅킹 응용프로그램에서 뱅킹 시스템으로 전송될 수 있다. 그 후 뱅킹 시스템은 송금인의 계좌에서 금전을 공제하고 그 금전을 받는 사람의 계좌에 추가함으로써 트랜잭션을 전자적으로 수행할 수 있다. 일부 경우에 제1 모바일 디바이스는 제1 사용자가 인증되고 제2 사용자가 교환을 승인한다는 표시를 수신함에 따라 화폐 교환을 개시하고 유도할 수 있다.

[0056] 유사하게 제1 모바일 디바이스는 교환을 유도하기 위해 제1 모바일 상의 뱅킹 응용프로그램을 통해 뱅킹 시스템과 통신할 수 있다. 그 후 뱅킹 시스템은 상기 논의된 바와 같이 교환을 수행할 수 있으며 예를 들어 송금인의 계좌에서 금전을 전자적으로 공제하고 그 금전을 수신인의 계좌에 추가하는 것이다.

[0057] 실시형태에서 제1 사용자와 제2 사용자는 서로 다른 뱅킹 시스템을 보유하는 서로 다른 은행을 활용할 수 있으며 뱅킹 시스템은 교환을 수행하기 위해 서로 통신할 수 있다. 예를 들어 제1 사용자는 제1 사용자의 뱅킹 시스템을 식별하기 위한 식별자를 제2 모바일 디바이스에 제공할 수 있다. 교환이 승인되면 제2 모바일 디바이스는 제2 사용자와 연관된 뱅킹 시스템에 정보를 전달할 수 있다.

[0058] 그 후 제2 사용자의 뱅킹 시스템은 교환을 수행하기 위해 제1 사용자의 뱅킹 시스템과 통신할 수 있다. 다른 경우에 제2 모바일 디바이스는 제2 사용자의 뱅킹 시스템을 식별하기 위한 정보를 제1 모바일 디바이스에 전달할 수 있으며 제1 모바일 디바이스는 제1 사용자의 뱅킹 시스템과 통신함으로써 교환을 개시할 수 있다.

[0059] 일부 실시형태에서 뱅킹 응용프로그램은 제3자 뱅킹 응용프로그램 예를 들어 뱅킹 시스템에 의해 직접 운영되지

않는 응용프로그램일 수 있다. 제3자 뱅킹 응용프로그램은 제3자 뱅킹 응용프로그램과 함께 작동하도록 형상화된 하나 이상의 뱅킹 계좌를 지니는 단계를 포함하여 각각의 모바일 디바이스에 형상화 될 수 있다. 교환이 승인되면 송금인과 수신인의 각 디바이스에 있는 제3자 응용프로그램이 해당 은행과 통신하여 교환을 수행할 수 있다.

[0060] 일부 경우에는 제3자 시스템을 포함한 제3자 응용프로그램이 송금인의 뱅킹 시스템과 통신하여 송금인의 계좌에서 금전을 공제할 수 있다. 제3자 시스템은 수수료나 이자를 받기 위해 일정 기간 동안 금전을 보관한 후 수신인의 계좌로 금전을 보낼 수 있다. 실시형태는 이러한 방식으로 제한되지 않는다.

[0061] 실시형태에서 제1 및 제2 모바일 디바이스는 금전을 교환하기 위해 P2P 보안 연결을 통해 데이터를 전달할 수 있다. 예를 들어 제1 사용자가 인증되고 제2 사용자가 교환을 승인하는 경우, 제2 모바일 디바이스는 P2P 연결을 설정하기 위해 제1 모바일 디바이스와 통신할 수 있다. 연결은 BLE, Bluetooth, ZigBee, Wi-Fi 등과 같은 특정 P2P 프로토콜에 따라 설정될 수 있다. 연결이 설정되면 제1 및/또는 제2 모바일 디바이스는 메시지 전달에 의해 화폐 교환을 개시할 수 있다.

[0062] 예를 들어 제2 모바일 디바이스는 금전을 교환하기 위한 데이터 또는 토큰에 대한 요청을 제1 모바일 디바이스에 전달할 수 있다. 제1 모바일 디바이스는 토큰 또는 교환할 금액의 표시를 지니는 보안 정보를 포함할 수 있는 데이터를 제2 모바일 디바이스로 전송할 수 있다. 제2 모바일 디바이스는 제1 사용자와 제2 사용자의 뱅킹 계좌 간의 교환을 수행하기 위해 뱅킹 시스템과 통신할 수 있다. 어떤 경우에 데이터는 송금인의 식별자, 수신인의 식별자, 송금인의 은행 계좌 정보 등을 포함할 수도 있다. 데이터는 안전하게 전송되고 암호화될 수 있다.

[0063] 도 4는 시스템(100)에 의해 수행될 수 있는 예시적인 루틴(400)을 도시한다. 상세하게는 루틴(400)은 다른 모바일 디바이스로부터 통신을 수신하는 모바일 디바이스에 의해 수행될 수 있으며 통신은 다른 사용자가 금전을 송금하거나 요청하기 원한다는 것을 나타낸다.

[0064] 블록 402에서 루틴(400)은 사용자가 금전을 송금하거나 요청하기 원한다는 것을 나타내는 텍스트와 데이터를 포함하는 고유 리소스 로케이터(URL)를 포함하는 메시지를 제1 사용자와 연관된 제1 모바일 디바이스에 의해 수신하는 단계를 포함한다. 문자를 통해 메시지의 송금인과 금액을 식별할 수 있다. 실시형태에서 메시지는 SMS, MMS, RCS 또는 다른 프로토콜과 같은 통신 프로토콜을 통해 제2 사용자와 연관된 제2 모바일 디바이스로부터 수신될 수 있다.

[0065] 실시형태에서 URL은 수신인에 의해 활성화될 때 제2 모바일 디바이스가 응용프로그램을 실행하고 제1 모바일 디바이스 및 비접촉식 카드로부터 수신된 데이터를 사용하여 제2 사용자의 인증을 수행하게 하는 활성 URL 또는 딥 링크일 수 있다. 실시형태에서 데이터는 토큰 또는 암호화된 문자열을 포함할 수 있으며 URL에 내장될 수 있다. 데이터는 실행될 때 제2 사용자의 인증을 수행하기 위해 응용프로그램에 의해 사용될 수 있는 파라미터로서 응용프로그램에 전달될 수 있다. 제1 사용자와 제2 사용자의 식별자, 교환할 금액과 같은 다른 정보 또한 URL에 포함될 수 있다.

[0066] 블록 404에서 루틴(400)은 URL을 활성화하기 위한 입력을 제1 모바일 디바이스에 의해 감지하는 단계를 포함한다. 예를 들어 제1 모바일 디바이스는 터치스크린 인터페이스와 같은 입력 디바이스를 포함할 수 있으며 사용자는 URL을 선택하거나 "클릭"할 수 있다. 실시형태는 이러한 실시예로 한정되지 않으며 예를 들어 버튼, 음성 명령어 경우에 마이크 등과 같은 다른 입력 디바이스를 통해 제공될 수도 있다.

[0067] 블록 406에서 루틴(400)은 입력에 응답하여 제1 모바일 디바이스에 의해 응용프로그램을 실행하는 단계를 포함하며 응용프로그램은 서버와 통신하여 데이터로 제2 사용자의 인증을 수행하도록 형상화 된다. 언급한 바와 같이 URL은 위치를 가리키거나 응용프로그램을 실행하기 위해 운영 체제에 의해 처리되는 명령어를 제공하는 딥 링크일 수 있다.

[0068] 예를 들어 URL은 시작할 특정 응용프로그램을 나타내거나 웹 브라우저에서 실행할 웹사이트를 가리킬 수 있다. 어떤 경우에는 URL은 표시를 포함하거나 응용 프로그램을 실행하기 위한 랜딩 지점이나 위치를 명시할 수 있다. 따라서 응용프로그램이나 웹 브라우저는 예를 들어 송금인/요청 이름, 연락처 정보, 금액 등 화폐 교환을 위한 정보를 표시하는 GUI 디스플레이를 열 수 있다.

[0069] 실시형태에서 URL은 토큰 또는 암호화된 문자열, 송금인을 식별하는 식별자, 수신인을 식별하는 식별자 및 응용프로그램이 실행될 때 파라미터로 응용프로그램에 전달될 수 있는 금액 표시와 같은 데이터를 포함할 수 있다.

[0070] 실시형태에서 실행된 응용프로그램을 포함하는 제1 모바일 디바이스는 URL이 활성화될 때 제2 사용자를 인증하

기 위해 인증 동작을 개시할 수 있다. 상세하게는 실행된 응용프로그램은 사용자를 인증하기 위해 URL에 포함된 정보 예를 들어 토큰 또는 암호화된 문자열을 활용할 수 있다. 일부 경우에 응용프로그램은 암호화된 문자열을 복호화 하고 복호화 된 문자열을 인증된 문자열과 비교함으로써 로컬로 인증 동작을 수행할 수 있다. 일부 경우에 제1 모바일 디바이스는 보안 통신 내에서 뱅킹 시스템으로부터 인증된 문자열을 우선 수득할 수 있다.

[0071] 도시된 실시예에서 응용프로그램을 포함하는 제2 모바일 디바이스는 암호화된 문자열을 뱅킹 시스템의 서버 또는 제3자 시스템으로 전송하여 인증 동작을 수행할 수 있다. 응용프로그램은 암호화된 문자열을 포함하는 데이터를 API 통신을 통해 서버로 전송할 수 있다. 서버는 제2 사용자와 연관된 공개 키에 기반하여 암호화된 문자열을 복호화 하고 복호화 된 문자열을 뱅킹 시스템에 저장된 인증된 문자열과 비교할 수 있다. 문자열이 매치하면 제2 사용자가 인증될 수 있으며 매치하지 않으면 인증될 수 없다.

[0072] 블록 408에서 루틴(400)은 제2 사용자가 서버에 의해 인증되었는지 여부에 대한 표시를 제1 모바일 디바이스에 의해 수신하는 단계를 포함한다. 표시는 API 통신에 대한 응답으로 응용프로그램에 반송될 수 있다. 일부 경우에 GUI 디스플레이는 제2 사용자를 인증하기 위해 인증 동작이 수행되고 있다는 표시와 결정되면 인증 동작의 결과를 표시할 수 있다. 사용자가 인증되지 않는 경우 교환 동작이 중단될 수 있다. 사용자가 인증되면 응용프로그램은 자금 교환을 진행할 것인지 확인하도록 제1 사용자에게 요청할 수 있다.

[0073] 제2 사용자가 인증되고 제1 사용자가 트랜잭션을 확인하는 것에 응답하여 블록 410에서 루틴(400)은 제1 모바일 디바이스에 의해 화폐 교환을 수행하는 단계를 포함한다. 도 3에서 전술한 바와 같이 제1 모바일 디바이스는 화폐 교환을 수행하기 위해 하나 이상의 뱅킹 시스템과 통신할 수 있다. 다른 경우에 제1 모바일 디바이스는 인증이 성공했으며 제1 사용자가 교환을 승인했다는 표시를 제2 모바일 디바이스인 송금인의 디바이스에 전송할 수 있다. 제2 모바일 디바이스는 교환을 수행하기 위해 하나 이상의 뱅킹 시스템과 통신할 수 있다. 심지어 다른 경우에 P2P 연결이 제1 모바일 디바이스와 제2 모바일 디바이스 사이에 설정될 수 있으며 교환을 수행하기 위해 디바이스 사이에서 데이터가 교환될 수 있다.

[0074] 도 5는 비접촉식 카드(500)의 예시적인 형상화를 도시하며 이는 비접촉식 카드(500)의 전면 또는 후면에 서비스 공급자 표식(502)으로 표시된 서비스 공급자에 의해 발급된 비접촉식 카드, 신용 카드, 직불 카드 또는 기프트 카드와 같은 결제 카드를 포함할 수 있다. 일부 실시예에서 비접촉식 카드(500)는 결제 카드와 연관이 없으며 제한 없이 신분증을 포함할 수 있다. 일부 실시예에서 트랜잭션 카드는 이중 인터페이스 비접촉식 결제 카드, 리워드 카드 등을 포함할 수 있다.

[0075] 비접촉식 카드(500)는 플라스틱, 금속 및 기타 재료로 구성된 단일 층 또는 하나 이상의 적층된 층을 포함할 수 있는 기판(508)을 포함할 수 있다. 예시적인 기판 재료는 폴리염화비닐, 폴리염화비닐 아세테이트, 아크릴로니트릴 부타디엔 스티렌, 폴리카보네이트, 폴리에스테르, 양극성 산화 티타늄, 팔라듐, 금, 탄소, 종이 및 생분해성 물질을 포함한다.

[0076] 일부 실시예에서 비접촉식 카드(500)는 ISO/IEC 7816 표준의 ID-1 형식을 준수하는 물리적 특성을 지닐 수 있으며 그렇지 않으면 트랜잭션 카드는 ISO/IEC 14443 표준을 준수할 수 있다. 다만 본 발명에 따른 비접촉식 카드(500)는 서로 상이한 특성을 지닐 수 있으며 본 발명에서는 트랜잭션 카드가 결제 카드 내에 구현될 필요가 없는 것으로 이해된다.

[0077] 또한 비접촉식 카드(500)는 카드의 전면 및/또는 후면에 표시된 식별 정보(506) 및 접촉 패드(504)를 포함할 수 있다. 접촉 패드(504)는 하나 이상의 패드를 포함할 수 있으며 트랜잭션 카드를 통해 ATM, 사용자 디바이스, 스마트폰, 노트북, 데스크톱 또는 태블릿 컴퓨터와 같은 다른 클라이언트 디바이스와 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. 또한 비접촉식 카드(500)는 도 6에서 더욱 설명되는 바와 같이 처리 회로, 안테나 및 다른 컴포넌트를 포함할 수 있다.

[0078] 이러한 컴포넌트는 접촉 패드(504) 후면 또는 기판(508) 상의 다른 곳에 위치할 수 있다. 또한 비접촉식 카드(500)는 카드 후면에 위치할 수 있는 자기 스트립 또는 테이프를 포함할 수 있다(도 5에는 나타내지 않음). 비접촉식 카드(500)는 NFC 프로토콜을 통해 통신할 수 있는 안테나와 결합된 근거리 통신(NFC) 디바이스를 또한 포함할 수 있다. 실시형태는 이러한 방식으로 제한되지 않는다.

[0079] 도 5에 도시된 바와 같이 비접촉식 카드(500)의 접촉 패드(504)는 프로세서(602), 메모리(604) 및 하나 이상의 인터페이스(606)를 포함하여 정보를 저장, 처리 및 전달하기 위한 처리 회로(616)를 포함할 수 있다. 처리 회로(616)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.

[0080] 메모리(604)는 읽기 전용 메모리, 1회 쓰기 다회 읽기 메모리 또는 읽기/쓰기 메모리 예를 들어 RAM, ROM, EEPROM일 수 있으며 비접촉식 카드(500)는 이들 메모리 중 하나 이상을 포함할 수 있다. 읽기 전용 메모리는 공장에서 읽기 전용 또는 일회성 프로그래밍 가능으로 프로그래밍할 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. 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(604)는 데이터를 암호화하기 위해 프로세서(602)에 의해 실행되는 암호화 알고리즘을 활용하는 암호화된 메모리일 수 있다.

[0081] 메모리(604)는 하나 이상의 애플릿(608), 하나 이상의 카운터(610), 토큰 또는 문자열과 같은 고객 식별자(614) 및 가상 계좌 번호일 수 있는 계좌 번호(612)를 저장하도록 형상화 될 수 있다. 하나 이상의 애플릿(608)은 Java® 카드 애플릿과 같이 하나 이상의 비접촉식 카드에서 실행되도록 형상화 된 하나 이상의 소프트웨어 응용 프로그램을 포함할 수 있다. 그러나 애플릿(608)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.

[0082] 하나 이상의 카운터(610)는 정수를 저장하기에 충분한 숫자 카운터를 포함할 수 있다. 고객 식별자(614)는 비접촉식 카드(500)의 사용자에게 할당된 고유 영숫자 식별자, 토큰 또는 문자열을 포함할 수 있으며 식별자는 비접촉식 카드의 사용자를 다른 비접촉식 카드 사용자와 구별할 수 있다.

[0083] 일부 실시예에서 고객 식별자(614)는 고객과 그 고객에게 할당된 계정을 모두 식별할 수 있으며 고객의 계정과 연관된 비접촉식 카드(500)를 추가로 식별할 수 있다. 일부 경우에 메모리(604)는 고객 식별자(614) 및 고객을 식별하는 데 사용될 수 있는 하나 이상의 토큰 또는 추가 문자열을 포함할 수 있다. 언급된 바와 같이 계좌 번호(612)는 비접촉식 카드(500)와 연관된 수천 개의 일회용 가상 계좌 번호를 포함할 수 있다. 비접촉식 카드(500)의 애플릿(608)은 계좌 번호를 관리하도록 형상화 될 수 있다. 예를 들어 계좌 번호(612)를 선택하면 선택된 계좌 번호(612)를 사용된 것으로 표시하고 자동 채우기 서비스에 의한 자동 채우기를 위해 계좌 번호(612)를 모바일 디바이스에 전송한다.

[0084] 전술한 실시형태의 프로세서(602) 및 메모리 엘레멘트는 접촉 패드(504)를 참조하여 설명되었으나 본 발명은 이에 제한되지 않는다. 이들 엘레멘트는 접촉 패드(504) 외부에 구현되거나 접촉 패드와 완전히 떨어져 구현될 수 있거나 접촉 패드(504) 내에 위치하는 프로세서(602) 및 메모리(604) 엘레멘트에 추가하는 추가 엘레멘트로서 구현될 수 있는 것으로 이해된다.

[0085] 일부 실시예에서 비접촉식 카드(500)는 하나 이상의 안테나(618)를 포함할 수 있다. 하나 이상의 안테나(618)는 비접촉식 카드(500) 내에 그리고 접촉 패드(504)의 처리 회로(616) 주위에 배치될 수 있다. 예를 들어 하나 이상의 안테나(618)는 처리 회로(616)와 통합될 수 있으며 하나 이상의 안테나(618)는 외부 부스터 코일과 함께 사용될 수 있다. 다른 실시예로서 하나 이상의 안테나(618)는 접촉 패드(504) 및 처리 회로(616) 외부에 있을 수 있다.

[0086] 실시형태에서 비접촉식 카드(500)의 코일은 공심 변압기의 2차 역할을 할 수 있다. 단말은 전력 차단 또는 진폭 변조를 통해 비접촉식 카드(500)와 통신할 수 있다. 비접촉식 카드(101)는 하나 이상의 커패시터를 통해 기능적으로 유지될 수 있는 비접촉식 카드의 전원 연결의 갭을 이용하여 단말기에서 전송되는 데이터를 추론할 수 있다. 비접촉식 카드(500)는 비접촉식 카드 코일의 부하를 전환하거나 부하 변조를 통해 다시 통신할 수 있다. 간섭을 통해 단말기 코일에서 부하 변조가 감지될 수 있다. 보다 일반적으로 안테나(618), 프로세서(602) 및/또는 메모리(604)를 사용하여 비접촉식 카드(101)는 NFC, Bluetooth 및/또는 Wi-Fi 통신을 통해 통신하기 위한 통신 인터페이스를 제공한다.

[0087] 상기 설명된 바와 같이 비접촉식 카드(500)는 스마트 카드 또는 JavaCard와 같은 제한된 메모리를 지니는 다른 디바이스 상에서 작동 가능한 소프트웨어 플랫폼 상에 구축될 수 있으며 하나 이상의 응용프로그램 또는 애플릿이 안전하게 실행될 수 있다. 애플릿(608)은 다양한 모바일 응용프로그램 기반 사용 사례에서 다중 요인 인증(MFA)을 위한 일회성 패스워드(OTP)를 제공하기 위해 비접촉식 카드에 추가될 수 있다. 애플릿(608)은 모바일 NFC 판독기 예를 들어 모바일 디바이스 또는 POS 단말기와 같은 판독기로부터의 근거리 데이터 교환 요청과 같

은 하나 이상의 요청에 응답하고 NDEF 텍스트 태그로 인코딩된 암호화 보안 OTP를 포함하는 NDEF 메시지를 생성하도록 형상화 될 수 있다.

[0088] NDEF OTP의 한 가지 예는 NDEF 짧은 레코드 레이아웃(SR=1)이다. 이러한 실시예에서 하나 이상의 애플릿(608)은 OTP를 NDEF 유형 4 잘 알려진 유형의 텍스트 태그로서 인코딩하도록 형상화 될 수 있다. 일부 실시예에서 NDEF 메시지는 하나 이상의 레코드를 포함할 수 있다. 애플릿(608)은 OTP 레코드에 더하여 하나 이상의 정적 태그 레코드를 추가하도록 형상화 될 수 있다.

[0089] 일부 실시예에서 하나 이상의 애플릿(608)은 RFID 태그를 에뮬레이트 하도록 형상화 될 수 있다. RFID 태그는 하나 이상의 다형성 태그를 포함할 수 있다. 일부 예에서 태그가 판독될 때마다 비접촉식 카드의 진위를 나타낼 수 있는 상이한 암호화 데이터가 제공된다. 하나 이상의 애플릿(608)에 기반하여 태그의 NFC 판독이 처리될 수 있으며 데이터가 뱅킹 시스템의 서버와 같은 서버로 전송되고 데이터가 서버에서 검증될 수 있다.

[0090] 일부 실시예에서 비접촉식 카드(500) 및 서버는 카드가 적절하게 식별될 수 있도록 특정 데이터를 포함할 수 있다. 비접촉식 카드(500)는 하나 이상의 고유 식별자 예를 들어 토큰 또는 문자열을 포함할 수 있다(도시되지 않음). 판독 동작이 발생할 때마다 카운터(610)는 증가하도록 형상화 될 수 있다. 일부 실시예에서 비접촉식 카드(500)로부터의 데이터가 예를 들어 모바일 디바이스에 의해 판독될 때마다 카운터(610)는 검증을 위해 서버로 전송되고 카운터(610)가 서버의 카운터와 동일한지 여부를 검증의 일부로 결정한다.

[0091] 하나 이상의 카운터(610)는 재생 공격을 방지하도록 형상화 될 수 있다. 예를 들어 암호문이 획득되어 재생된 경우 카운터(610)가 판독되거나 사용되거나 다른 방식으로 전달되면 해당 암호문은 즉시 거부된다. 카운터(610)가 사용되지 않은 경우 이는 재생될 수 있다. 일부 실시예에서 카드에서 증가되는 카운터는 트랜잭션에 대해 증가되는 카운터와 상이하다. 비접촉식 카드(500) 상의 애플릿(608) 사이에 통신이 없기 때문에 비접촉식 카드(101)는 응용프로그램 트랜잭션 카운터(610)를 결정할 수 없다.

[0092] 일부 실시예에서 카운터(610)는 동기화되지 않을 수 있다. 일부 예에서 비스듬히 판독하는 것과 같이 트랜잭션을 개시하는 우발적인 판독을 설명하기 위해 카운터(610)는 증가할 수 있지만 응용프로그램은 카운터(610)을 처리하지 않는다. 일부 실시예에서 모바일 디바이스가 깨어나면 NFC가 활성화될 수 있으며 디바이스(110)는 사용 가능한 태그를 판독하도록 형상화 될 수 있으나 판독에 응답하여 어떠한 동작도 수행되지 않는다.

[0093] 카운터(610)을 동기화 상태로 유지하기 위해 모바일 디바이스(110)가 깨어나는 때를 감지하고 감지로 인한 판독이 카운터(610)를 앞으로 이동시킴을 나타내는 뱅킹 시스템의 서버와 동기화하도록 형상화 된 백그라운드 응용프로그램과 같은 응용프로그램이 실행될 수 있다. 다른 실시예에서는 잘못된 동기화의 윈도우를 허용하기 위해 해시된 일회성 패스워드가 활용될 수 있다.

[0094] 예를 들어 10의 임계값 내에 있으면 카운터(610)는 앞으로 이동하도록 형상화 될 수 있다. 그러나 다른 임계값 예를 들어 10 또는 1200 이내에 있는 경우 재동기화 수행 요청이 처리될 수 있으며 이러한 요청은 사용자가 사용자의 디바이스를 통해 한번 이상 탭 하거나 제스처 하거나 다른 방식으로 표시하도록 하나 이상의 응용프로그램을 통해 요청한다. 카운터(610)가 적절한 순서로 증가하면 사용자가 그렇게 했음을 알 수 있다.

[0095] 카운터(610), 마스터 키 및 다양화된 키를 참조하여 본 발명에 설명된 키 다양화 기술은 키 다양화 기술의 암호화 및/또는 복호화의 일례이다. 이러한 예시적인 키 다양화 기술은 본 발명을 제한하는 것으로 간주되어서는 안된다. 본 발명은 다른 유형의 키 다양화 기술에도 동일하게 적용 가능하기 때문이다.

[0096] 비접촉식 카드(500)의 생성 프로세스 동안, 2개의 암호화 키가 카드마다 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(500)의 하드웨어에 의해 구현된다. 키 다양화 프로세스를 사용함으로써 하나 이상의 키가 피를 필요로 하는 각각의 엔티티에 대해 고유한 식별 정보를 기반으로 마스터 키에서 파생될 수 있다.

[0097] 일부 실시예에서 취약성에 취약할 수 있는 3DES 알고리즘의 결함을 극복하기 위해 세션 당 고유 키와 같은 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 동작할 때마다 메시지 인증 코드(MAC) 생성과 암호화 수행을 위해 서로 다른 키가 사용될 수 있다. 이로 인해 삼중 암호화 계층이 생성된다. 세션 키가 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.

[0098] 또한 각 카드의 증분은 고유할 수 있으며 개인화에 의해 할당되거나 일부 식별 정보에 의해 알고리즘적으로 할당될 수 있다. 예를 들어 홀수 카드는 2만큼 증가할 수 있으며 짝수 카드는 5만큼 증가할 수 있다. 일부 실시예에서 증분은 순차적인 판독에서도 상이할 수 있으므로 하나의 카드는 1, 3, 5, 2, 2 … 반복 만큼 순차적으로 증가할 수 있다. 특정 시퀀스 또는 알고리즘 시퀀스는 개인화 시에 정의되거나 고유 식별자에서 파생된 하나 이상의 프로세스에서 정의될 수 있다. 이로 인해 재생 공격자는 적은 수의 카드 인스턴스로부터 일반화하기가 더 어렵게 된다.

[0099] 인증 메시지는 16진수 ASCII 형식의 텍스트 NDEF 레코드 내용으로 전달될 수 있다. 다른 실시예에서 NDEF 레코드는 16진수 형식으로 인코딩 될 수 있다.

[0100] 도 7은 본 발명의 하나 이상의 실시형태에 따라 데이터 교환을 제공하기 위한 예시적인 시퀀스를 예시하는 타이밍도이다. 시퀀스 흐름(700)은 응용프로그램(702) 및 프로세서(704)를 포함할 수 있는 비접촉식 카드(500) 및 모바일 디바이스를 포함할 수 있다.

[0101] 라인 708에서 응용프로그램(702)은 예를 들어 비접촉식 카드(500) 근처에 근접한 후 비접촉식 카드(500)와 통신한다. 응용프로그램(702)과 비접촉식 카드(500) 사이의 통신은 응용프로그램(702)과 비접촉식 카드(500) 사이의 NFC 데이터 전송을 가능하게 하기 위해 모바일 디바이스의 카드 판독기(나타내지 않음)에 충분히 근접한 비접촉식 카드(500)를 수반할 수 있다.

[0102] 라인 706에서 모바일 디바이스와 비접촉식 카드(500) 사이에 통신이 설정된 후, 비접촉식 카드(500)는 메시지 인증 코드(MAC) 암호문을 생성한다. 일부 실시예에서 이는 비접촉식 카드(500)가 응용프로그램(702)에 의해 판독될 때 발생할 수 있다. 특히 이는 NFC 데이터 교환 형식에 따라 생성될 수 있는 근거리 데이터 교환(NDEF) 태그의 NFC 판독과 같은 판독 시에 발생할 수 있다. 예를 들어 응용프로그램(702)과 같은 판독기 응용프로그램은 NDEF 생성 애플릿의 애플릿 ID와 함께 애플릿 선택 메시지와 같은 메시지를 전송할 수 있다. 선택이 확인되면 일련의 파일 선택 메시지와 파일 판독 메시지가 전송될 수 있다.

[0103] 예를 들어 시퀀스는 "기능 파일 선택", "기능 파일 판독" 및 "NDEF 파일 선택"을 포함할 수 있다. 이때, 비접촉식 카드(500)에 의해 유지되는 카운터 값이 업데이트되거나 증가될 수 있으며 이어서 "NDEF 파일 읽기"가 이어질 수 있다. 이러한 시점에서 헤더와 토큰 또는 문자열과 같은 공유 비밀을 포함하는 메시지가 생성될 수 있다. 그 후 세션 키가 생성될 수 있다. MAC 암호문은 헤더와 공유 비밀을 포함할 수 있는 메시지로부터 생성될 수 있다. 그 후 MAC 암호문은 하나 이상의 무작위 데이터 블록과 연결될 수 있으며 MAC 암호문 및 난수(RND)는 세션 키로 암호화될 수 있다. 그 후 암호문과 헤더는 연결되고 ASCII 16진수로 인코딩되어 "NDEF 파일 판독" 메시지에 대한 응답으로 NDEF 메시지 형식으로 반환할 수 있다.

[0104] 일부 실시예에서 MAC 암호문은 NDEF 태그로서 전송될 수 있으며 다른 실시예에서 MAC 암호문은 예를 들어 포맷된 문자열로서 고유 리소스 표시자와 함께 포함될 수 있다. 일부 실시예에서 응용프로그램(702)은 MAC 암호문을 생성하라는 명령어를 포함하는 요청을 비접촉식 카드(500)에 전송하도록 형상화 될 수 있다.

[0105] 라인 710에서 비접촉식 카드(500)는 MAC 암호문을 응용프로그램(702)에 전송한다. 일부 실시예에서 MAC 암호문의 전송은 NFC를 통해 발생하지만 본 발명은 이에 제한되지 않는다. 다른 실시예에서 이러한 통신은 블루투스, Wi-Fi 또는 기타 무선 데이터 통신 수단을 통해 발생할 수 있다. 라인 712에서 응용프로그램(702)은 MAC 암호문을 프로세서(704)에 전달한다.

[0106] 라인 714에서 프로세서(704)는 응용프로그램(122)으로부터의 명령어에 따라 MAC 암호문을 검증한다. 예를 들어 MAC 암호문은 하기 설명된 바와 같이 검증될 수 있다. 일부 실시예에서 MAC 암호문의 검증은 모바일 디바이스와 데이터 통신하는 뱅킹 시스템의 서버와 같은 모바일 디바이스 이외의 디바이스에 의해 수행될 수 있다. 예를 들어 프로세서(704)는 MAC 암호문을 검증할 수 있는 뱅킹 시스템의 서버로의 전송을 위해 MAC 암호문을 출력할 수 있다. 일부 실시예에서 MAC 암호문은 검증 목적의 디지털 서명으로 기능할 수 있다. 디지털 서명 알고리즘 및 RSA 알고리즘과 같은 공개 키 비대칭 알고리즘 또는 영지식 프로토콜과 같은 다른 디지털 서명 알고리즘을 사용하여 이러한 검증을 수행할 수 있다.

[0107] 도 8은 본 발명의 하나 이상의 실시형태를 구현하도록 형상화 된 시스템(800)의 다이어그램을 도시한다. 하기 설명된 바와 같이 비접촉식 카드 생성 과정에서 두 개의 암호화 키가 각 카드에 고유하게 할당될 수 있다. 암호화 키는 데이터의 암호화 및 암호문 복호화 모두에 사용될 수 있는 대칭 키를 포함할 수 있다. 트리플 DES(3DES) 알고리즘은 EMV에서 사용될 수 있으며 비접촉식 카드의 하드웨어로 구현된다. 키 다양화 프로세스를 사용하면 키를 필요로 하는 각각의 엔티티에 대해 고유하게 식별 가능한 정보를 기반으로 마스터 키로부터 하나

이상의 키가 파생될 수 있다.

[0108] 마스터 키 관리와 관련하여 하나 이상의 애플릿이 발행되는 포트폴리오의 각 부분에 대해 두 개의 발급자 마스터 키(802, 826)가 필요할 수 있다. 예를 들어 제1 마스터 키(802)는 발급자 암호화 생성/인증 키(Iss-Key-Auth)를 포함할 수 있으며 제2 마스터 키(826)는 발급자 데이터 암호화 키(Iss-Key-DEK)를 포함할 수 있다. 본 발명에 더욱 설명되는 바와 같이 2개의 발급자 마스터 키(802, 826)는 각 카드에 대해 고유한 카드 마스터 키(808, 820)로 다양화된다. 일부 실시예에서 백오피스 데이터로서 네트워크 프로파일 레코드 ID (pNPR)(522) 및 유도 키 인덱스(pDKI)(824)가 인증을 위한 암호화 프로세스에서 사용할 발급자 마스터 키(802, 826)를 식별하는 데 사용될 수 있다.

[0109] 인증을 수행하는 시스템은 인증 시 비접촉식 카드에 대한 pNPR(822) 및 pDKI(824) 값을 검색하도록 형상화 될 수 있다.

[0110] 일부 실시예에서 솔루션의 보안을 높이기 위해 세션 당 고유 키와 같은 세션 키가 파생될 수 있으나 마스터 키를 사용하는 대신에 상기 설명된 바와 같이 고유 카드-파생 키와 카운터가 다양화 데이터로 사용될 수 있다. 예를 들어 카드가 동작할 때마다 메시지 인증 코드(MAC) 생성과 암호화 수행에 상이한 키가 사용될 수 있다. 세션 키 생성과 관련하여 하나 이상의 애플릿에서 암호문을 생성하고 데이터를 암호화하는 데 사용되는 키는 카드 고유 키 Card-Key-Auth(808) 및 Card-Key-Dek(820)를 기반으로 하는 세션 키를 포함할 수 있다.

[0111] 세션 키 Aut-Session-Key(832) 및 DEK-Session-Key(810)는 하나 이상의 애플릿에 의해 생성될 수 있으며 하나 이상의 알고리즘과 함께 응용프로그램 트랜잭션 카운터(pATC)(804)를 사용하여 파생될 수 있다. 데이터를 하나 이상의 알고리즘에 맞추려면 4바이트 pATC(804)의 하위 2바이트 만이 사용된다. 일부 실시예에서 4바이트 세션 키 파생 방법은 다음을 포함할 수 있다. F1 := PATC(하위 2바이트) || 'F0' || '00' || PATC(4바이트) F1 := PATC(하위 2바이트) || '0F' || '00' || PATC(4바이트) SK :={(ALG (MK) [F1]) || ALG (MK) [F2] }, 여기서 ALG는 3DES ECB를 포함할 수 있으며 MK는 카드 고유 파생 마스터 키를 포함할 수 있다.

[0112] 본 발명에 설명된 바와 같이 하나 이상의 MAC 세션 키는 pATC(804) 카운터의 하위 2바이트를 사용하여 파생될 수 있다. 비접촉식 카드를 탭 할 때마다 pATC(804)는 업데이트 하도록 형상화 되며 카드 마스터 키 Card-Key-AUTH(704) 및 Card-Key-DEK(820)은 세션 키 Aut-Session-Key(832) 및 DEK-Session-KEY(810)로 더욱 다양화 된다. pATC(804)는 개인화 또는 애플릿 초기화 시간에 0으로 초기화될 수 있다. 일부 실시예에서 pATC 카운터(804)는 개인화 시 또는 그 이전에 초기화될 수 있으며 각각의 NDEF 판독에서 1씩 증가하도록 형상화 될 수 있다.

[0113] 또한 각 카드의 업데이트는 고유할 수 있으며 개인화를 통해 할당되거나 pUID 또는 기타 식별 정보에 의해 알고리즘적으로 할당될 수 있다. 예를 들어 홀수 카드는 2만큼 증가 또는 감소할 수 있고 짝수 카드는 5만큼 증가 또는 감소할 수 있다. 일부 실시예에서 업데이트는 순차적 판독에서도 상이할 수 있으므로 하나의 카드가 1, 3, 5, 2, 2 … 반복 만큼 순차적으로 증가할 수 있다. 특정 시퀀스 또는 알고리즘 시퀀스는 개인화 시 정의되거나 고유 식별자에서 파생된 하나 이상의 프로세스에서 정의될 수 있다. 이로 인해 재생 공격자는 적은 수의 카드 인스턴스로부터 일반화하기가 더 어렵게 된다.

[0114] 인증 메시지는 16진수 ASCII 형식의 텍스트 NDEF 레코드 내용으로 전달될 수 있다. 일부 실시예에서는 인증 데이터 및 인증 데이터의 MAC에 이어지는 8바이트 난수만을 포함할 수 있다. 일부 실시예에서 난수는 암호문 A 앞에 올 수 있고 하나의 블록 길이일 수 있다. 다른 실시예에서는 난수의 길이에 제한이 없을 수 있다.

[0115] 추가 실시예에서 전체 데이터 즉, 난수 + 암호문은 블록 크기의 배수일 수 있다. 이러한 실시예에서 MAC 알고리즘에 의해 생성된 블록과 매치하도록 추가 8바이트 블록이 추가될 수 있다. 또 다른 실시예로서 적용된 알고리즘이 16바이트 블록을 사용하는 경우 해당 블록 크기의 배수가 사용될 수 있으며 출력이 해당 블록 크기의 배수로 자동 또는 수동으로 패딩 될 수 있다.

[0116] MAC는 기능 키 AUT-Session-Key(832)에 의해 수행될 수 있다. 암호문 내에 명시된 데이터는 EMV ARQC 검증 방법과 관련시키기 위해 javacard.signature 방법: ALG_DES_MAC8_ISO9797_1_M2_ALG3으로 처리될 수 있다. 이러한 연산에 사용되는 키는 상기 설명된 바와 같이 세션 키 AUT-Session-Key(832)를 포함할 수 있다. 상기 설명된 바와 같이 카운터의 하위 2바이트는 하나 이상의 MAC 세션 키에 대해 다양화하는 데 사용될 수 있다. 하기 설명되는 바와 같이 AUT-Session-키(832)는 MAC 데이터(806)에 사용될 수 있으며 결과 데이터 또는 암호문 An(814) 및 난수 RND는 DEK-세션 키(810)를 사용하여 암호화되어 메시지 내에서 전송된 암호문 B 또는 출력(818)을 생성할 수 있다.

[0117] 일부 실시예에서 하나 이상의 HSM 명령은 이진, 32 16진수의 최종 16 바이트가 MAC 인증 데이터가 뒤따르는 난수의 IV가 0인 CBC 모드를 사용하는 3DES 대칭 암호화를 포함할 수 있도록 복호화를 위해 처리될 수 있다. 이러한 암호화에 사용되는 키는 Card-Key-DEK(820)에서 파생된 세션 키 DEK-Session-Key(810)를 포함할 수 있다. 이러한 경우에 세션 키 파생을 위한 ATC 값은 카운터 pATC(804)의 최하위 바이트이다.

[0118] 아래 형식은 이진 버전 예시적인 실시형태를 나타낸다. 또한 일부 실시예에서 제1 바이트는 ASCII 'A'로 설정될 수 있다.??

[0119]

메시지 형식				
1	2	4	8	8
0x43 (메시지 유형 'A')	버전	pATC	RND	암호문 A (MAC)
암호문 A (MAC)	8 바이트			
MAC 의				
2	8	4	4	18 바이트 입력 데이터
버전	pUID	pATC	공유 비밀	

[0120]

메시지 형식				
1	2	4	16	
0x43 (메시지 유형 'A')	버전	pATC	암호문 B	
암호문 A (MAC)	8 바이트			
MAC 의				
2	8	4	4	18 바이트 입력 데이터
버전	pUID	pATC	공유 비밀	
암호문 B	16			
대칭 암호화				
8	8			
RND	암호문 A			

[0121] 또 다른 예시적인 형식을 하기 나타내었다. 이러한 실시예에서 태그는 16진수 형식으로 인코딩 될 수 있다.

[0122]

메시지 형식				
2	8	4	8	8
버전	pUID	pATC	RND	암호문 A (MAC)
8 바이트				
8	8	4	4	18 바이트 입력 데이터
pUID	pUID	pATC	공유 비밀	

메시지 형식			
2	8	4	16
버전	pUID	pATC	암호문 B
8 바이트			

8		4	4	18 바이트 입력 데이터
pUID	pUID	pATC	공유 비밀	

암호문 B	16		
대칭 암호화			

8	8		
RND	암호문 A		

[0123]

[0124] 수신된 메시지의 UID 필드는 마스터 키 Iss-Key-AUTH(500) 및 Iss-Key-DEK(826)로부터 특정 카드에 대한 카드 마스터 키 Card-Key-Auth(808) 및 Card-Key-DEK(820)를 파생시키기 위해 추출될 수 있다. 카드 마스터 키 Card-Key-Auth(704) 및 Card-Key-DEK(820)를 사용하면 수신된 메시지의 카운터(pATC) 필드를 사용하여 특정 카드에 대한 세션 키 Aut-Session-Key(832) 및 DEK-Session-Key(810)를 파생시킬 수 있다.

[0125] 암호문 B(818)는 DEK-Session-KEY를 사용하여 복호화 될 수 있으며 이는 암호문 An(814) 및 RND를 생성하고 RND는 폐기될 수 있다. UID 필드는 비접촉식 카드의 공유 비밀을 조회하기 위해 사용될 수 있으며 이는 메시지의 Ver, UID 및 pATC 필드와 함께 MAC'과 같은 MAC 출력을 생성하기 위해 재-생성된 Aut-Session-Key를 사용하여 암호화 MAC을 통해 처리될 수 있다. MAC'이 암호문 An(814)과 동일한 경우 이는 메시지 복호화 및 MAC 검사가 모두 통과되었음을 나타낸다. 그 후 pATC를 판독하여 유효한지 결정할 수 있다.

[0126] 인증 세션 중에 하나 이상의 응용프로그램에 의해 하나 이상의 암호문이 생성될 수 있다. 예를 들어 하나 이상의 암호문은 Aut-Session-Key(832)와 같은 하나 이상의 세션 키를 통해 방법 2 패딩과 함께 ISO 9797-1 알고리즘 3을 사용하여 3DES MAC로 생성될 수 있다. 입력 데이터(806)는 다음 형식을 취할 수 있다: 버전(2), pUID(8), pATC(4), 공유 비밀(4). 일부 실시예에서 괄호 안의 숫자는 바이트 길이를 포함할 수 있다. 일부 실시예에서 공유 비밀은 하나 이상의 보안 프로세스를 통해 난수가 예측 불가능함을 보장하도록 형상화 될 수 있는 하나 이상의 난수 생성기에 의해 생성될 수 있다.

[0127] 일부 실시예에서 공유 비밀은 인증 서비스에 의해 알려진 개인화 시에 카드에 주입된 무작위 4-바이트 이진 수를 포함할 수 있다. 인증 세션 중에는 공유 비밀이 하나 이상의 애플릿에서 모바일 응용프로그램으로 제공되지 않을 수 있다. 방법 2 패딩은 입력 데이터 끝에 필수 0x'80' 바이트를 추가하고 최대 8바이트 경계까지 결과 데이터 끝에 추가할 수 있는 0x'00' 바이트를 추가하는 단계를 포함할 수 있다. 결과 암호문은 8바이트 길이로 형상화 될 수 있다.

[0128] 일부 실시예에서 MAC 암호문으로 공유되지 않은 난수를 제1 블록으로 암호화하는 것의 한 가지 이점은 대칭 암호화 알고리즘의 블록 체인(CBC) 모드를 사용하는 동안 초기화 벡터로 작동한다는 것이다. 이를 통해 고정 또는 동적 IV를 미리 설정하지 않고도 블록 간 "스크램블링"이 가능하다.

[0129] MAC 암호문 내에 포함된 데이터의 일부로 응용프로그램 트랜잭션 카운터(pATC)를 포함시킴으로써 인증 서비스는 일반 데이터에 전달된 값이 변조되었는지 여부를 결정하도록 형상화 될 수 있다. 또한 하나 이상의 암호문에 버전을 포함함으로써 공격자가 암호화 솔루션의 강도를 낮추려는 시도로 응용 프로그램 버전을 의도적으로 허위로 표시하는 것이 어렵게 된다. 일부 실시예에서 pATC는 0에서 시작하여 하나 이상의 응용프로그램이 인증 데이터를 생성할 때마다 1씩 업데이트될 수 있다. 인증 서비스는 인증 세션 중에 사용된 pATC를 추적하도록 형상화 될 수 있다.

[0130] 일부 실시예에서 인증 데이터가 인증 서비스에 의해 수신된 이전 값 이하의 pATC를 사용하는 경우, 이는 이전 메시지를 재생하려는 시도로 해석될 수 있으며 인증된 메시지가 거부될 수 있다. 일부 실시예에서 pATC가 수신된 이전 값보다 큰 경우, 이는 허용 가능한 범위 또는 임계값 내에 있는지 결정하기 위해 평가될 수 있으며 범

위 또는 임계값을 초과하거나 벗어나면 검증은 실패하거나 신뢰할 수 없는 것으로 간주될 수 있다. MAC 동작(812)에서 데이터(806)는 암호화되는 MAC 출력인 암호문 A(814)를 생성하기 위해 Aut-Session-Key(832)를 사용하여 MAC를 통해 처리된다.

[0131] 카드의 키를 노출시키는 무차별 대입 공격에 대한 추가적인 보호를 제공하기 위해 MAC 암호문(814)을 암호화하는 것이 바람직하다. 일부 실시예에서 암호문 내에 포함될 데이터 또는 암호문 An(814)은 난수(8), 암호문(8)을 포함할 수 있다. 일부 실시예에서 괄호 안의 숫자는 바이트 길이를 포함할 수 있다. 일부 실시예에서 난수는 하나 이상의 보안 프로세스를 통해 난수가 예측 불가능함을 보장하도록 형상화 될 수 있는 하나 이상의 난수 생성기에 의해 생성될 수 있다. 이러한 데이터를 암호화하는 데 사용되는 키는 세션 키로 형상화 될 수 있다.

[0132] 예를 들어 세션 키는 DEK-Session-Key(810)를 포함할 수 있다. 암호화 동작(816)에서 데이터 또는 암호문 An(814) 및 RND는 DEK-Session-Key(706)를 사용하여 처리되어 암호화된 데이터, 암호문 B(818)를 생성할 수 있다. 공격자가 모든 암호문에 대해 공격을 실행해야 함을 보장하기 위해 데이터(814)는 암호문 블록 체인 모드에서 3DES를 사용하여 암호화된다. 비제한적인 실시예로서 고급 암호화 표준(AES)과 같은 다른 알고리즘이 사용될 수 있다. 일부 실시예에서 0x'0000000000000000'의 초기화 벡터가 사용될 수 있다.

[0133] 이러한 데이터를 암호화하는 데 사용되는 키를 무차별 대입하려는 공격자는 올바른 키가 언제 사용되었는지 확인할 수 없다. 올바르게 복호화 된 데이터는 무작위 출현으로 인해 잘못 복호화 된 데이터와 구별할 수 없기 때문이다.

[0134] 인증 서비스가 하나 이상의 애플릿에 의해 제공된 하나 이상의 암호문을 검증하기 위해서는 다음 데이터가 하나 이상의 애플릿에서 모바일 디바이스로 명확하게 인증 세션 동안 전달되어야 한다: 향후 접근 방식 변경을 가능하게 하는 사용된 암호화 접근 방식과 암호문의 검증을 위한 메시지 형식을 결정하기 위한 버전 번호; 암호화 자산을 검색하고 카드 키를 파생하기 위한 pUID; 및 암호문에 사용ehls 세션 키를 파생하기 위한 pATC이다.

[0135] 도 9는 암호문을 생성하는 방법(900)을 도시한다. 예를 들어 블록 902에서 네트워크 프로파일 레코드 ID(pNPR) 및 파생 키 인덱스(pDKI)는 인증을 위한 암호화 프로세스에 사용할 발급자 마스터 키를 식별하는 데 사용될 수 있다. 일부 실시예에서 방법은 인증 시 비접촉식 카드에 대한 pNPR 및 pDKI의 값을 검색하기 위해 인증을 수행하는 단계를 포함할 수 있다.

[0136] 블록 904에서 발급자 마스터 키는 카드의 고유 ID 번호(pUID) 및 하나 이상의 애플릿 예를 들어 결제 애플릿의 PAN 시퀀스 번호(PSN)와 결합하여 다양화될 수 있다.

[0137] 블록 906에서 MAC 암호문을 생성하는 데 사용될 수 있는 세션 키를 생성하기 위해 발급자 마스터 키를 다양화함으로써 Card-Key-Auth 및 고유 카드 키인 Card-Key-DEK가 생성될 수 있다.

[0138] 블록 908에서 하나 이상의 애플릿에서 암호문을 생성하고 데이터를 암호화하는 데 사용되는 키는 카드 고유 키 Card-Key-Auth 및 Card-Key-DEK에 기반한 블록 1230의 세션 키를 포함할 수 있다. 일부 실시예에서 이들 세션 키는 하나 이상의 애플릿에 의해 생성되고 pATC를 사용하여 파생될 수 있으며 그 결과로 세션 키 Aut-Session-Key 및 DEK-Session-Key가 생성된다.

[0139] 도 10은 하나의 실시예에 따른 키 다양화를 설명하는 예시적인 프로세스(1000)를 도시한다. 초기에는 송금인과 수신인에게 서로 다른 두 개의 마스터 키가 제공될 수 있다. 예를 들어 제1 마스터 키는 데이터 암호화 마스터 키를 포함할 수 있으며 제2 마스터 키는 데이터 무결성 마스터 키를 포함할 수 있다. 송금인은 블록 1002에서 업데이트될 수 있는 카운터 값과 수신인과의 공유를 보장할 수 있는 보호될 데이터와 같은 다른 데이터를 지닌다.

[0140] 블록 1004에서 카운터 값은 데이터 암호화 파생 세션 키를 생성하기 위해 데이터 암호화 마스터 키를 사용하여 송금인에 의해 암호화될 수 있으며 카운터 값은 데이터 무결성 파생 세션 키를 생성하기 위해 데이터 무결성 마스터 키를 사용하여 송금인에 의해 또한 암호화될 수 있다. 일부 실시예에서 전체 카운터 값 또는 카운터 값의 일부가 두 암호화 동안 사용될 수 있다.

[0141] 일부 실시예에서는 카운터 값이 암호화되지 않을 수 있다. 이러한 실시예에서 카운터는 송금인과 수신인 사이에 암호화 없이 일반 형식으로 전송될 수 있다.

[0142] 블록 1006에서 보호될 데이터는 데이터 무결성 세션 키 및 암호화 MAC 알고리즘을 사용하여 송금인에 의해 암호화 MAC 동작으로 처리된다. 일반 텍스트 및 공유 비밀을 포함하는 보호된 데이터는 세션 키 AUT-Session-Key의

하나를 사용하여 MAC를 생성하는 데 사용될 수 있다.

[0143] 블록 1008에서 보호될 데이터는 대칭 암호화 알고리즘과 함께 데이터 암호화 파생 세션 키를 사용하여 송금인에 의해 암호화될 수 있다. 일부 실시예에서 MAC는 동일한 양의 무작위 데이터 예를 들어 각 8바이트 길이와 결합된 후 제2 세션 키 DEK-Session-Key를 사용하여 암호화된다.

[0144] 블록 1010에서 암호문의 검증을 위해 추가 비밀 정보 예를 들어 공유 비밀, 마스터 키 등을 식별하는 데 충분한 정보와 함께 암호화된 MAC가 발신자로부터 수신자에게 전송된다.

[0145] 블록 1012에서 수신자는 수신된 카운터 값을 사용하여 상기 설명된 바와 같이 두 개의 마스터 키로부터 두 개의 파생 세션 키를 독립적으로 파생시킨다.

[0146] 블록 1014에서 데이터 암호화 파생 세션 키는 대칭 복호화 동작과 함께 사용되어 보호된 데이터를 복호화한다. 그 후 교환된 데이터에 대한 추가 처리가 발생한다. 일부 실시예에서는 MAC을 추출한 후 MAC을 재현하여 매치시키는 것이 바람직하다. 예를 들어 암호문을 검증할 때 적절하게 생성된 세션 키를 사용하여 암호문을 복호화 할 수 있다. 보호된 데이터는 검증을 위해 재구성 될 수 있다. 적절하게 생성된 세션 키를 사용하여 MAC 동작을 수행하여 그것이 복호화 된 MAC과 매치하는지 확인할 수 있다. MAC 동작은 비가역적인 프로세스이므로 검증하는 유일한 방법은 소스 데이터로부터 다시 생성하는 것이다.

[0147] 블록 1016에서 데이터 무결성 파생 세션 키는 암호화 MAC 동작과 함께 사용되어 보호된 데이터가 수정되지 않았는지 검증한다.

[0148] 본 발명에 설명된 방법의 일부 실시예는 다음 조건이 충족될 때 성공적인 인증이 결정되는 시기를 유리하게 확인할 수 있다. 첫째, MAC을 검증하는 기능은 파생된 세션 키가 적절했음을 나타낸다. MAC는 복호화가 성공적이고 적절한 MAC 값을 산출한 경우에만 정확할 수 있다. 성공적인 복호화는 올바르게 파생된 암호화 키가 암호화된 MAC을 복호화 하는 데 사용되었음을 나타낼 수 있다. 파생된 세션 키는 송금인 예를 들어 전송 디바이스와 수신인 예를 들어 수신 디바이스 만이 알고 있는 마스터 키를 사용하여 생성되므로 원래 MAC을 생성하고 MAC을 암호화한 비접촉식 카드가 참으로 진본임을 신뢰할 수 있다. 또한 제1 세션 키와 제2 세션 키를 파생시키는데 사용된 카운터 값은 유효한 것으로 나타나 인증 동작을 수행하는데 사용될 수 있다.

[0149] 그 후 두 개의 파생된 세션 키는 폐기될 수 있고 데이터 교환의 다음 반복은 블록 1002로 돌아가서 카운터 값을 업데이트 하고 새로운 세션 키 세트가 블록 1010에서 생성될 수 있다. 일부 실시예에서 결합된 랜덤 데이터는 폐기될 수 있다.

[0150] 도 11은 예시적인 실시형태에 따른 카드 활성화 방법(1000)을 도시한다. 예를 들어 카드 활성화는 카드, 디바이스 및 하나 이상의 서버를 포함하는 시스템에 의해 완료될 수 있다. 비접촉식 카드, 디바이스 및 하나 이상의 서버는 비접촉식 카드(500), 모바일 디바이스 및 서버와 같이 이전에 설명된 동일하거나 유사한 컴포넌트를 참조할 수 있다.

[0151] 블록에서 카드는 데이터를 동적으로 생성하도록 형상화 될 수 있다. 일부 실시예에서 이러한 데이터는 카드에서 디바이스로 전송될 수 있는 계좌 번호, 카드 식별자, 카드 검증 값 또는 전화번호와 같은 정보를 포함할 수 있다. 일부 실시예에서 데이터의 하나 이상의 부분은 본 발명에 개시된 시스템 및 방법을 통해 암호화될 수 있다.

[0152] 블록 1104에서 동적으로 생성된 데이터의 하나 이상의 부분은 NFC 또는 다른 무선 통신을 통해 디바이스의 응용프로그램으로 전달될 수 있다. 예를 들어 디바이스에 근접한 카드를 탭 하면 디바이스의 응용프로그램이 비접촉식 카드와 연관된 데이터의 하나 이상의 부분을 판독할 수 있다. 일부 실시예에서 디바이스가 카드 활성화를 지원하는 응용프로그램을 포함하지 않는 경우 카드를 탭 하면 카드를 활성화하기 위해 관련 응용프로그램을 다운로드 하도록 소프트웨어 응용프로그램 스토어로 디바이스를 안내하거나 고객에게 프롬프트 할 수 있다.

[0153] 일부 실시예에서 사용자는 디바이스의 표면을 향해 카드를 충분히 제스처나 배치하거나 배향 시키도록 프롬프트 될 수 있다. 예를 들어 디바이스의 표면 위에 근처에 또는 근접하게 비스듬하게 배치되거나 평평하게 배치되도록 할 수 있다. 카드의 충분한 제스처, 배치 및/또는 배향에 응답하여 디바이스는 카드로부터 수신된 데이터의 하나 이상의 암호화된 부분을 하나 이상의 서버로 전송할 수 있다.

[0154] 블록 1106에서 데이터의 하나 이상의 부분이 카드 발급자 서버와 같은 하나 이상의 서버로 전달될 수 있다. 예를 들어 카드 활성화를 위해 데이터의 하나 이상의 암호화된 부분이 디바이스에서 카드 발급자 서버로 전송될 수 있다.

[0155] 블록 1108에서 하나 이상의 서버는 본 발명에 개시된 시스템 및 방법을 통해 데이터의 하나 이상의 암호화된 부분을 복호화 할 수 있다. 예를 들어 하나 이상의 서버는 디바이스로부터 암호화된 데이터를 수신할 수 있으며 수신된 데이터를 하나 이상의 서버에 액세스 가능한 기록 데이터와 비교하기 위해 이를 복호화 할 수 있다. 하나 이상의 서버에 의한 데이터의 하나 이상의 복호화 된 부분의 비교 결과가 성공적인 매치를 산출하는 경우 카드가 활성화될 수 있다. 하나 이상의 서버에 의한 데이터의 하나 이상의 복호화 된 부분의 비교 결과가 실패한 매치를 산출하는 경우 하나 이상의 프로세스가 발생할 수 있다.

[0156] 예를 들어 실패한 매치의 결정에 응답하여 사용자는 카드를 다시 탭 하거나, 스와이프 하거나, 웨이브 제스처하도록 프롬프트 될 수 있다. 이러한 경우에 사용자가 카드를 활성화하도록 허용되는 시도 횟수를 포함하는 미리 결정된 임계값이 있을 수 있다. 대안적으로 사용자는 카드 검증 시도가 실패했음을 나타내는 자신의 디바이스 상의 메시지와 같은 통지를 수신하고 카드 활성화에 대한 지원을 위해 관련 서비스에 전화, 이메일 또는 문자를 전송하거나 카드 검증 시도가 실패했음을 나타내는 자신의 디바이스 상의 전화 통화와 같은 또 다른 통지를 수신하고 카드 활성화에 대한 지원을 위해 관련 서비스에 전화, 이메일 또는 문자를 전송하거나 카드 검증 시도가 실패했음을 나타내는 이메일과 같은 또 다른 통지를 수신하고 카드 활성화에 대한 지원을 위해 관련 서비스에 전화, 이메일 또는 문자를 전송할 수 있다.

[0157] 블록 1110에서 하나 이상의 서버는 카드의 성공적인 활성화에 기반하여 반송 메시지를 전송할 수 있다. 예를 들어 디바이스는 하나 이상의 서버에 의한 카드의 성공적인 활성화를 나타내는 출력을 하나 이상의 서버로부터 수신하도록 형상화 될 수 있다. 디바이스는 카드의 성공적인 활성화를 나타내는 메시지를 표시하도록 형상화 될 수 있다. 카드가 활성화되면 사기 사용을 방지하기 위해 동적 데이터 생성을 중단시키도록 카드가 형상화 될 수 있다. 이러한 방식으로 카드는 추후 활성화되지 않을 수 있으며 하나 이상의 서버는 카드가 이미 활성화되었음이 통보된다.

[0158] 도 12는 상기 설명된 바와 같은 다양한 실시형태를 구현하는데 적합한 예시적인 컴퓨터 아키텍처(1200)의 실시형태를 도시한다. 하나의 실시형태에서 컴퓨터 아키텍처(1200)는 본 발명에 설명된 하나 이상의 시스템 또는 디바이스를 포함하거나 그 일부로서 구현될 수 있다.

[0159] 본 발명에서 사용된 "시스템" 및 "컴포넌트"라는 용어는 하드웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어 또는 실행 중인 소프트웨어 등 컴퓨터 관련 엔티티를 의미하며 그 예는 예시적인 컴퓨터 컴퓨터 아키텍처(1200)에 의해 제공된다. 예를 들어 컴포넌트는 프로세서 상에서 실행 중인 프로세스, 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 ㅇ낳는다. 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 국소화 되거나 2 이상의 컴퓨터 간에 분산될 수 있다.

[0160] 또한, 컴포넌트는 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. 정보는 다양한 신호 라인에 할당된 신호로 구현될 수 있다. 이러한 할당에서 각 메시지는 신호이다. 그러나 추가 실시형태는 데이터 메시지를 대안적으로 적용할 수도 있다. 이러한 데이터 메시지는 다양한 연결을 통해 전송될 수 있다. 예시적인 연결은 병렬 인터페이스, 직렬 인터페이스 및 버스 인터페이스를 포함한다.

[0161] 컴퓨팅 컴퓨터 아키텍처(1200)는 하나 이상의 프로세서, 멀티-코어 프로세서, 코-프로세서, 메모리 유니트, 칩셋, 컨트롤러, 주변기기, 인터페이스, 발진기, 타이밍 디바이스, 비디오 카드, 오디오 카드, 멀티미디어 입력/출력(I/O) 컴포넌트, 전원 공급 장치 등과 같은 다양한 공통 컴퓨터 엘레멘트를 포함한다. 그러나 실시형태는 컴퓨팅 컴퓨터 아키텍처(1200)에 의한 구현으로 제한되지 않는다.

[0162] 도 12에 도시된 바와 같이 컴퓨팅 컴퓨터 아키텍처(1200)는 프로세서(1212), 시스템 메모리(1204) 및 시스템 버스(1206)를 포함한다. 프로세서(1212)는 상업적으로 이용 가능한 다양한 프로세서 중 임의의 것일 수 있다.

[0163] 시스템 버스(1206)는 프로세서(1212)에 대한 시스템 메모리(1204)를 포함하지만 이에 제한되지 않는 시스템 컴포넌트에 대한 인터페이스를 제공한다. 시스템 버스(1206)는 메모리 컨트롤러가 있거나 없는 메모리 버스, 주변기기 버스 및 다양한 상업적으로 이용 가능한 버스 아키텍처를 사용하는 로컬 버스에 더욱 상호 연결될 수 있는 다양한 유형의 버스 구조 중 임의의 것일 수 있다.

[0164] 인터페이스 어댑터는 슬롯 아키텍처를 통해 시스템 버스(1206)에 연결될 수 있다. 예시적인 슬롯 아키텍처는 가

속 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) 등을 포함할 수 있으나 이에 제한되지 않는다.

[0165] 컴퓨터 아키텍처(1200)는 다양한 제조 물품을 포함하거나 구현할 수 있다. 제조 물품은 로직을 저장하기 위한 컴퓨터 판독 가능 저장 매체를 포함할 수 있다. 컴퓨터 판독 가능 저장 매체의 예는 휘발성 메모리 또는 비휘발성 메모리, 이동식 또는 비이동식 메모리, 지울 수 있는 또는 지울 수 없는 메모리, 기록 가능 또는 재기록 가능 메모리 등을 포함하여 전자 데이터를 저장할 수 있는 모든 유형의 매체를 포함할 수 있다.

[0166] 로직의 예에는 소스 코드, 컴파일 된 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 명령어를 포함할 수 있다. 또한 실시형태는 비일시적 컴퓨터 판독 가능 매체에 포함된 명령어로서 적어도 부분적으로 구현될 수 있으며 이는 본 발명에 설명된 동작의 수행을 가능하게 하기 위해 하나 이상의 프로세서에 의해 판독 및 실행될 수 있다.

[0167] 시스템 메모리(1204)는 읽기 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 동적 RAM(DRAM), 더블 데이터 레이트 DRAM(DDRAM), 동기식 DRAM(SDRAM), 정적 RAM(SRAM), 프로그래밍 가능 ROM(PROM), 지울 수 있는 프로그래밍 가능 ROM(EPROM), 전기적으로 지울 수 있는 프로그래밍 가능 ROM(EEPROM), 플래시 메모리, 강유전성 폴리머 메모리, 오보닉 메모리, 상 변화 또는 강유전성 메모리와 같은 폴리머 메모리, 실리콘-옥사이드-니트라이드-옥사이드-실리콘(SONOS) 메모리, 자기 또는 광학 카드, 복수 배열 독립 디스크(RAID) 드라이브, 예를 들어 UDS 메모리, 고체 상태 드라이브(SSD)와 같은 고체 상태 메모리 디바이스 및 정보 저장에 적합한 임의의 유형의 저장 매체와 같은 하나 이상의 고속 메모리 유니트의 형태로 다양한 유형의 컴퓨터 판독 가능 저장 매체를 포함할 수 있다.

[0168] 도 12에 도시된 예시된 실시형태에서 시스템 메모리(1204)는 비휘발성(1208) 및/또는 휘발성(1210) 메모리를 포함할 수 있다. 기본 입력/출력 시스템(BIOS)은 비휘발성(1208) 메모리 내에 저장될 수 있다.

[0169] 컴퓨터(1202)는 내부(또는 외부) 하드 디스크 드라이브(1230), 이동식 자기 디스크(1220)로부터 읽거나 이에 쓰기 위한 자기 디스크 드라이브(1216), 이동식 광 디스크(1232) 예를 들어 CD-ROM 또는 DVD로부터 읽거나 이에 쓰기 위한 광 디스크 드라이브(1228)를 포함하는 하나 이상의 저속 메모리 유니트의 형태로 다양한 유형의 컴퓨터 판독 가능 저장 매체를 포함할 수 있다. 하드 디스크 드라이브(1230), 자기 디스크 드라이브(1216) 및 광 디스크 드라이브(1228)는 각각 HDD 인터페이스(1214), FDD 인터페이스(1218) 및 광 디스크 드라이브 인터페이스(1234)에 의해 시스템 버스(1206)에 연결될 수 있다. 외부 드라이브 구현을 위한 HDD 인터페이스(1214)는 범용 직렬 버스(USB) 및 IEEE 1394 인터페이스 기술 중 적어도 하나 또는 모두를 포함할 수 있다.

[0170] 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(1222), 하나 이상의 응용프로그램(1242), 기타 프로그램 모듈(1224) 및 프로그램 데이터(1226)를 포함하는 다수의 프로그램 모듈이 드라이브 및 비휘발성(1208) 및 휘발성(1210) 메모리에 저장될 수 있다. 하나의 실시형태에서 하나 이상의 응용프로그램(1242), 다른 프로그램 모듈(1224) 및 프로그램 데이터(1226)는 예를 들어 본 발명에 논의된 시스템의 다양한 응용프로그램 및/또는 컴포넌트를 포함할 수 있다.

[0171] 사용자는 하나 이상의 유선/무선 입력 디바이스 예를 들어 키보드(1250) 및 마우스(1252)와 같은 포인팅 디바이스를 통해 컴퓨터(1202)에 명령어 및 정보를 입력할 수 있다. 다른 입력 디바이스는 마이크, 적외선(IR) 리모콘, 무선 주파수(RF) 리모콘, 게임 패드, 스타일러스 펜, 카드 리더기, 동글, 지문 판독기, 글로브, 그래픽 태블릿, 조이스틱, 키보드, 망막 판독기, 터치 스크린 예를 들어 정전식, 감압식, 트랙볼, 트랙 패드, 센서, 스타일러스 등을 을 포함할 수 있다. 이들 및 다른 입력 디바이스는 시스템 버스(1206)에 결합된 입력 디바이스 인터페이스(1236)를 통해 프로세서(1212)에 종종 연결되지만 병렬 포트, IEEE 1394 직렬 포트, 게임 포트, USB 포트, IR 인터페이스 등과 같은 다른 인터페이스에 의해 연결될 수 있다.

[0172] 모니터(1244) 또는 다른 유형의 디스플레이 디바이스 또한 비디오 어댑터(1246)와 같은 인터페이스를 통해 시스템 버스(1206)에 연결된다. 모니터(1244)는 컴퓨터(1202)의 내부 또는 외부에 있을 수 있다. 모니터(1244)에 더하여 컴퓨터는 일반적으로 스피커, 프린터 등과 같은 기타 주변 출력 디바이스를 포함한다.

[0173] 컴퓨터(1202)는 원격 컴퓨터(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, 라

우터, 개인용 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서 기반 엔터테인먼트 기기, 피어 디바이스 또는 기타 공통 네트워크 노드일 수 있으며 컴퓨터(1202)와 관련하여 설명된 많은 또는 모든 엘레멘트를 일반적으로 포함하지만 간결성을 위해 단지 메모리 및/또는 저장 디바이스(1258) 만이 도시되어 있다. 도시된 논리적 연결은 근거리 네트워크(1256) 및/또는 더 큰 네트워크 예를 들어 광역 네트워크(1254)에 대한 유선/무선 연결을 포함한다. 이러한 LAN 및 WAN 네트워크 환경은 사무실과 회사에서 일반적이며 인트라넷과 같은 전 기업적 컴퓨터 네트워크를 용이하게 한다. 이들 모두는 인터넷과 같은 글로벌 통신 네트워크에 연결될 수 있다.

[0174] 근거리 네트워크(1256) 네트워크 환경에서 사용될 때 컴퓨터(1202)는 유선 및/또는 무선 통신 네트워크 인터페이스 또는 네트워크 어댑터(1238)를 통해 근거리 네트워크(1256)에 연결된다. 네트워크 어댑터(1238)는 근거리 네트워크(1256)에 대한 유선 및/또는 무선 통신을 용이하게 할 수 있으며 이는 네트워크 어댑터(1238)의 무선 기능과 통신하기 위해 그 위에 배치된 무선 액세스 포인트를 또한 포함할 수 있다.

[0175] 광역 네트워크(1254) 네트워크 환경에서 사용되는 경우 컴퓨터(1202)는 모뎀(1240)을 포함할 수 있거나 광역 네트워크(1254) 상의 통신 서버에 연결되거나 인터넷에 의한 방법과 같이 광역 네트워크(1254)를 통해 통신을 설정하기 위한 다른 수단을 지닌다. 내부 또는 외부일 수 있고 유선 및/또는 무선 디바이스일 수 있는 모뎀(1240)은 입력 디바이스 인터페이스(1236)를 통해 시스템 버스(1206)에 연결된다. 네트워크 환경에서 컴퓨터(1202) 또는 그 일부와 관련하여 도시된 프로그램 모듈은 원격 메모리 및/또는 저장 디바이스(1258) 내에 저장될 수 있다. 도시된 네트워크 연결은 예시적이며 컴퓨터 사이에 통신 링크를 설정하는 다른 수단이 사용될 수 있는 것으로 이해된다.

[0176] 컴퓨터(1202)는 무선 통신 예를 들어 IEEE 802.11 무선 변조 기술에서 작동 가능하게 배치된 무선 디바이스와 같은 IEEE 802 계열 표준을 사용하여 유선 및 무선 디바이스 또는 엔티티와 통신하도록 작동 가능한다. 여기에는 특히 Wi-Fi 또는 Wireless Fidelity, WiMax 및 Bluetooth™ 무선 기술이 포함된다. 따라서 통신은 기존 네트워크와 같이 미리 정의된 구조이거나 단순히 적어도 두 디바이스 간의 임시 통신일 수 있다. Wi-Fi 네트워크는 IEEE 802.11(a, b, g, n 등)이라는 무선 기술을 사용하여 안전하고 안정적이며 빠른 무선 연결을 제공한다. Wi-Fi 네트워크는 컴퓨터를 상호간에 연결하고 인터넷에 연결하고 IEEE 802.3 관련 미디어 및 기능을 사용하는 유선 네트워크에 연결하는 데 사용할 수 있다.

[0177] 본 발명에서 이전에 설명된 바와 같은 디바이스의 다양한 엘레멘트는 다양한 하드웨어 엘레멘트, 소프트웨어 엘레멘트 또는 이들의 조합을 포함할 수 있다. 하드웨어 엘레멘트의 예는 디바이스, 로직 디바이스, 컴포넌트, 프로세서, 마이크로프로세서, 회로, 프로세서, 회로 엘레멘트 예를 들어 트랜지스터, 레지스터, 커패시터, 인덕터 등, 집적 회로, 주문형 집적 회로(ASIC), 프로그래밍 가능 논리 디바이스(PLD), 디지털 신호 프로세서(DSP), 필드 프로그래밍 가능 게이트 어레이(FPGA), 메모리 유니트, 로직 게이트, 레지스터, 반도체 디바이스, 칩, 마이크로칩, 칩셋 등을 포함할 수 있다.

[0178] 소프트웨어 엘레멘트의 예는 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, 응용프로그램 프로그램 인터페이스(API), 명령어 세트, 컴퓨팅 코드, 컴퓨터 코드, 코드 세그먼트, 컴퓨터 코드 세그먼트, 단어, 값, 기호 또는 이들의 조합을 포함할 수 있다.

[0179] 그러나 실시형태가 하드웨어 엘레멘트 및/또는 소프트웨어 엘레멘트를 사용하여 구현되는지 여부를 결정하는 것은 원하는 연산 속도, 전력 수준, 내열성, 처리 주기 예산, 입력 데이터 속도, 출력 데이터 속도, 특정 구현에 필요한 메모리 리소스, 데이터 버스 속도 및 기타 설계 또는 성능 제약과 같은 임의의 수의 요인에 따라 상이할 수 있다.

[0180] 상기 설명된 디바이스의 컴포넌트 및 특징은 개별 회로, 주문형 집적 회로(ASIC), 로직 게이트 및/또는 단일 칩 아키텍처의 임의의 조합을 사용하여 구현될 수 있다. 또한 디바이스의 특징은 마이크로컨트롤러, 프로그래밍 가능 논리 어레이 및/또는 마이크로프로세서 또는 적절하게 적절한 경우 전술한 것의 임의의 조합을 사용하여 구현될 수 있다. 하드웨어, 펌웨어 및/또는 소프트웨어 엘레멘트는 본 발명에서 집합적으로 또는 개별적으로 "로직" 또는 "회로"로 지칭될 수 있음에 유의한다.

[0181] 도 13은 상기 설명된 다양한 실시형태를 구현하는 데 적합한 예시적인 통신 아키텍처(1300)를 도시하는 블록도이다. 통신 아키텍처(1300)는 송신기, 수신기, 트랜시버, 라디오, 네트워크 인터페이스, 기저대역 프로세서, 안테나, 증폭기, 필터, 전원 공급 디바이스 등과 같은 다양한 공통 통신 엘레멘트를 포함한다. 그러나 실시형태는

본 발명에서 논의된 시스템 및 디바이스와 일치할 수 있는 통신 아키텍처(1300)에 의한 구현으로 제한되지 않는다.

[0182] 도 13에 도시된 바와 같이 통신 아키텍처(1300)는 하나 이상의 클라이언트(1302) 및 서버(1304)를 포함한다. 서버(1304)는 본 발명에 논의된 하나 이상의 기능 및 실시형태를 구현할 수 있다. 클라이언트(1302) 및 서버(1304)는 쿠키 및/또는 관련 맥락 정보와 같이 각각의 클라이언트(1302) 및 서버(1304)에 로컬인 정보를 저장하기 위해 적용될 수 있는 하나 이상의 각각의 클라이언트 데이터 저장소(1306) 및 서버 데이터 저장소(1308)에 작동 가능하게 연결된다.

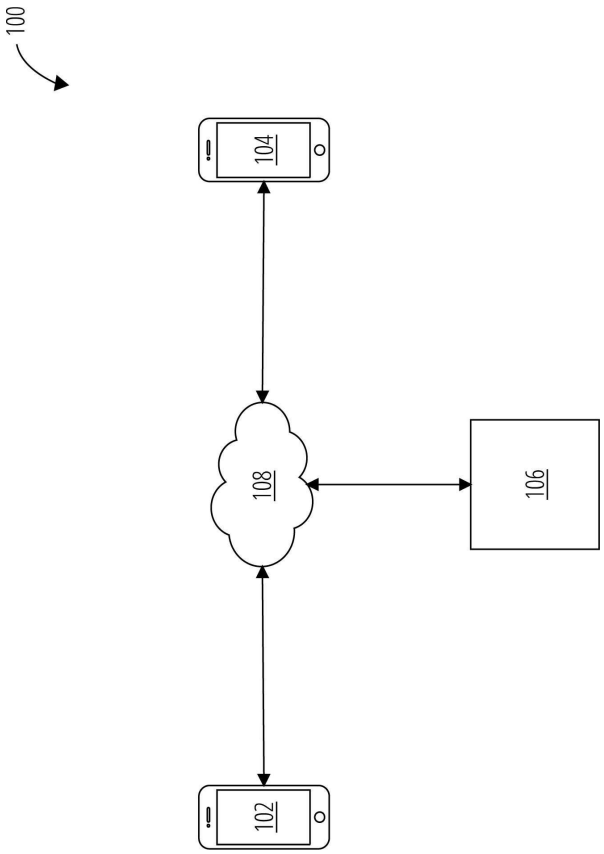
[0183] 클라이언트(1302) 및 서버(1304)는 통신 프레임워크(1310)를 사용하여 서로 간에 정보를 전달할 수 있다. 통신 프레임워크(1310)는 임의의 잘 알려진 통신 기술 및 프로토콜을 구현할 수 있다. 통신 프레임워크(1310)는 예를 들어 인터넷과 같은 공공 네트워크, 기업 인트라넷과 같은 사설 네트워크 등과 같은 패킷 교환 네트워크, 예를 들어 공중 교환 전화 네트워크와 같은 회선 교환 네트워크 또는 적절한 게이트웨이 및 변환기를 포함하여 패킷 교환 네트워크와 회선 교환 네트워크의 조합으로 구현될 수 있다.

[0184] 통신 프레임워크(1310)는 통신 네트워크를 수용하고 통신하고 연결하도록 구성된 다양한 네트워크 인터페이스를 구현할 수 있다. 네트워크 인터페이스는 입출력(I/O) 인터페이스의 특수한 형태로 간주될 수 있다. 네트워크 인터페이스는 직접 연결, 이더넷 예를 들어 씩, 씬, 브위스트 페어 10/100/1200 Base T 등, 토큰 링, 무선 네트워크 인터페이스, 셀룰러 네트워크 인터페이스, IEEE 802.11a-x 네트워크 인터페이스, IEEE 802.16 네트워크 인터페이스, IEEE 802.20 네트워크 인터페이스 등을 제한 없이 포함하는 연결 프로토콜을 적용할 수 있다. 또한 다중 네트워크 인터페이스가 다양한 통신 네트워크 유형에 참여하기 위해 사용될 수 있다.

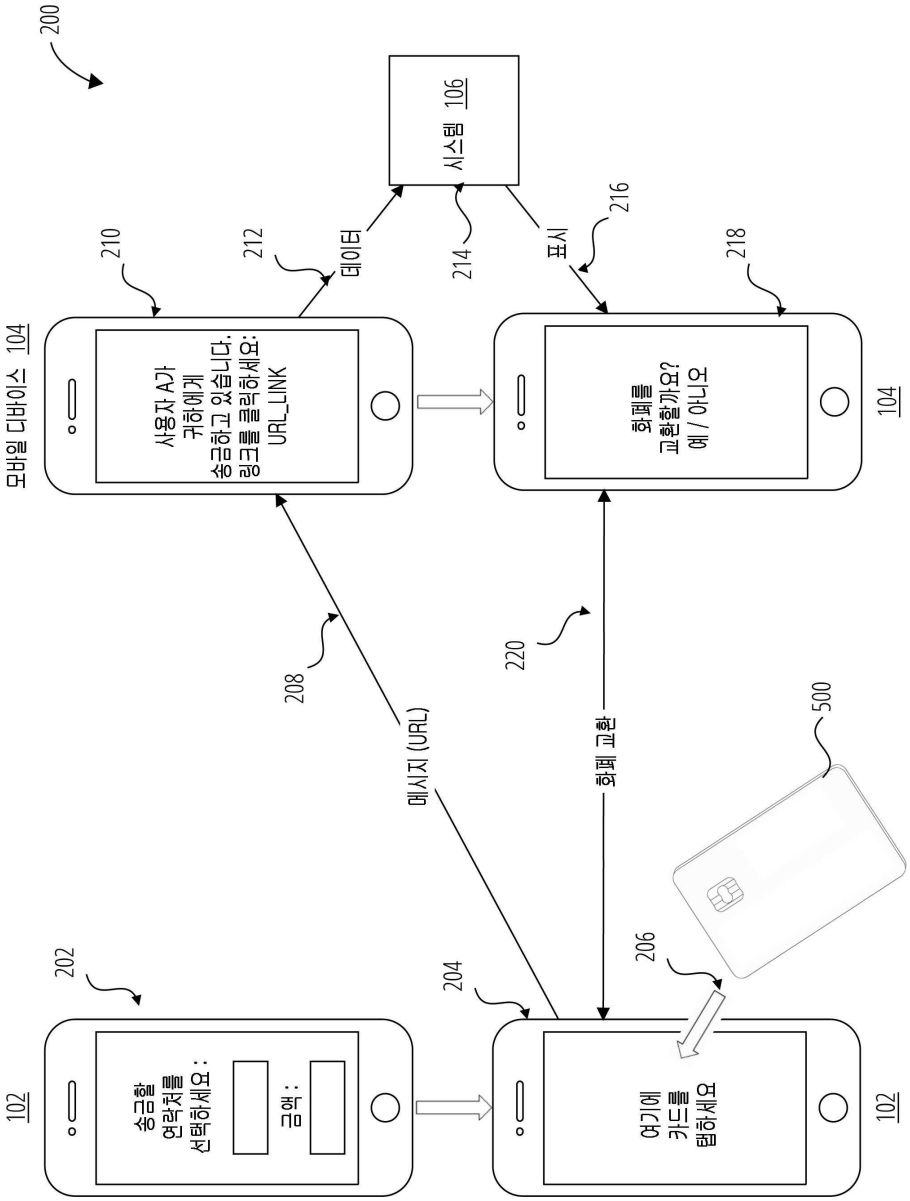
[0185] 예를 들어 브로드캐스트, 멀티캐스트 및 유니캐스트 네트워크를 통한 통신을 허용하기 위해 다중 네트워크 인터페이스가 적용될 수 있다. 처리 요구 사항이 더 큰 속도와 용량을 요구한다면 분산 네트워크 컨트롤러 아키텍처는 클라이언트(1302)와 서버(1304)에 의해 요구되는 통신 대역폭을 풀링하고 로드 밸런싱하고 그렇지 않으면 증가시키기 위해 유사하게 적용될 수 있다. 통신 네트워크는 직접 상호 연결, 보안 사용자정의 연결, 개인 네트워크 예를 들어 기업 인트라넷, 공용 네트워크 예를 들어 인터넷), 개인 영역 네트워크(PAN), 근거리 테트워크(LAN), 도시 영역 네트워크(MAN), 인터넷상의 노드 로서의 운영 임무(OMNI), 광역 네트워크(WAN), 무선 네트워크, 셀룰러 네트워크 및 기타 통신 네트워크를 제한 없이 포함하는 유선 및/또는 무선 네트워크 중 어느 하나 또는 이들의 조합일 수 있다.

도면

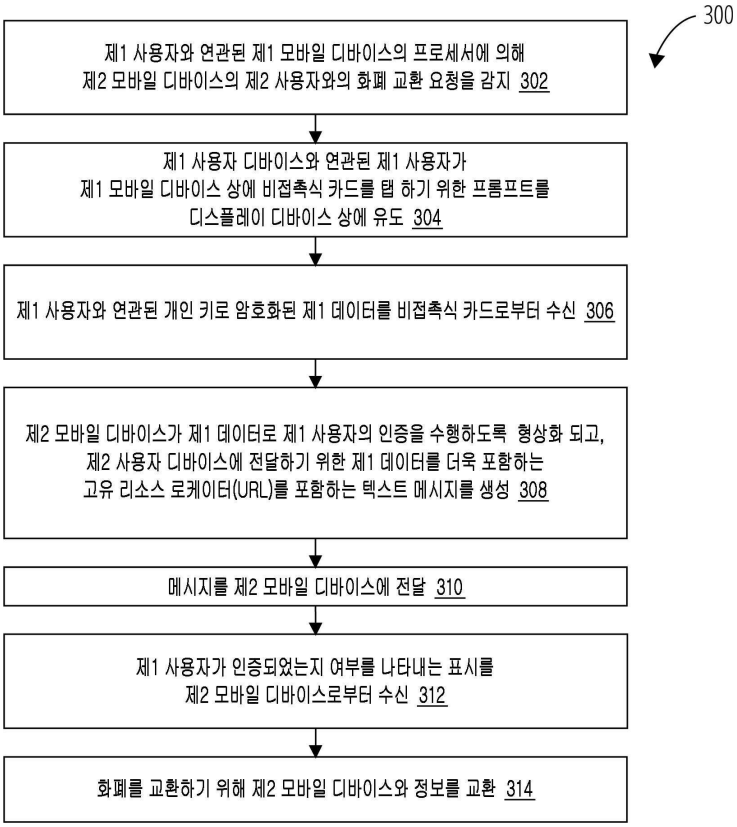
도면1



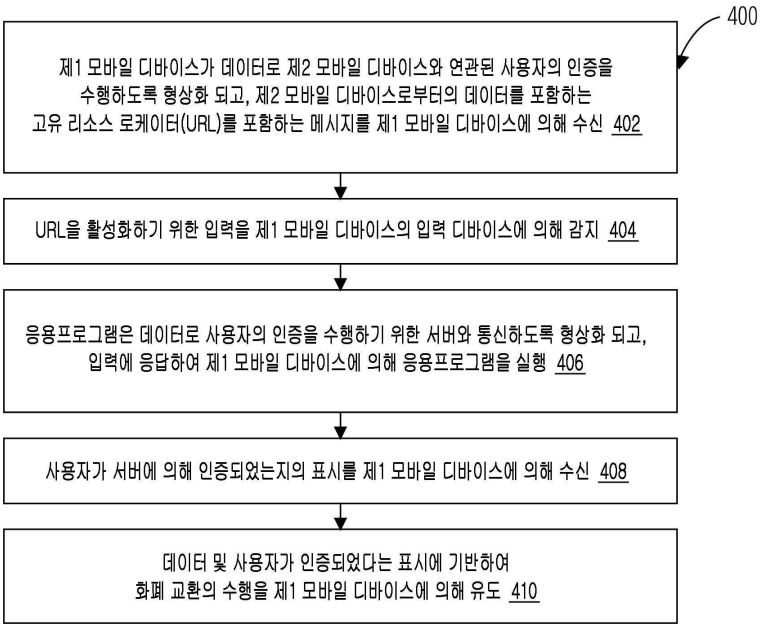
도면2


200
시스템 106
210
212
데이터
214
표시
216
218
모바일 디바이스 104
사용자 A가
귀하에게
송금하고 있습니다.
링크를 클릭하세요:
URL_LINK
화폐를
교환할까요?
예 / 아니오
104
208
메시지 (URL)
220
화폐 교환
500
202
204
206
송금할
연락처를
선택하세요:
금액:
여기에
카드를
탭하세요
102
102

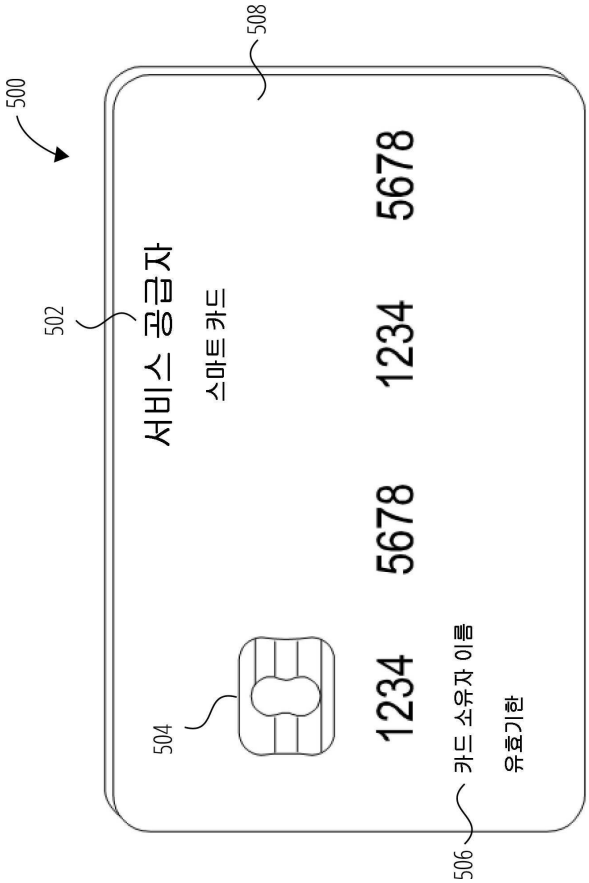
도면3


300
제1 사용자와 연관된 제1 모바일 디바이스의 프로세서에 의해
제2 모바일 디바이스의 제2 사용자와의 화폐 교환 요청을 감지 302
제1 사용자 디바이스와 연관된 제1 사용자가
제1 모바일 디바이스 상에 비접촉식 카드를 탭 하기 위한 프롬프트를
디스플레이 디바이스 상에 유도 304
제1 사용자와 연관된 개인 키로 암호화된 제1 데이터를 비접촉식 카드로부터 수신 306
제2 모바일 디바이스가 제1 데이터로 제1 사용자의 인증을 수행하도록 형상화 되고,
제2 사용자 디바이스에 전달하기 위한 제1 데이터를 더욱 포함하는
고유 리소스 로케이터(URL)를 포함하는 텍스트 메시지를 생성 308
메시지를 제2 모바일 디바이스에 전달 310
제1 사용자가 인증되었는지 여부를 나타내는 표시를
제2 모바일 디바이스로부터 수신 312
화폐를 교환하기 위해 제2 모바일 디바이스와 정보를 교환 314

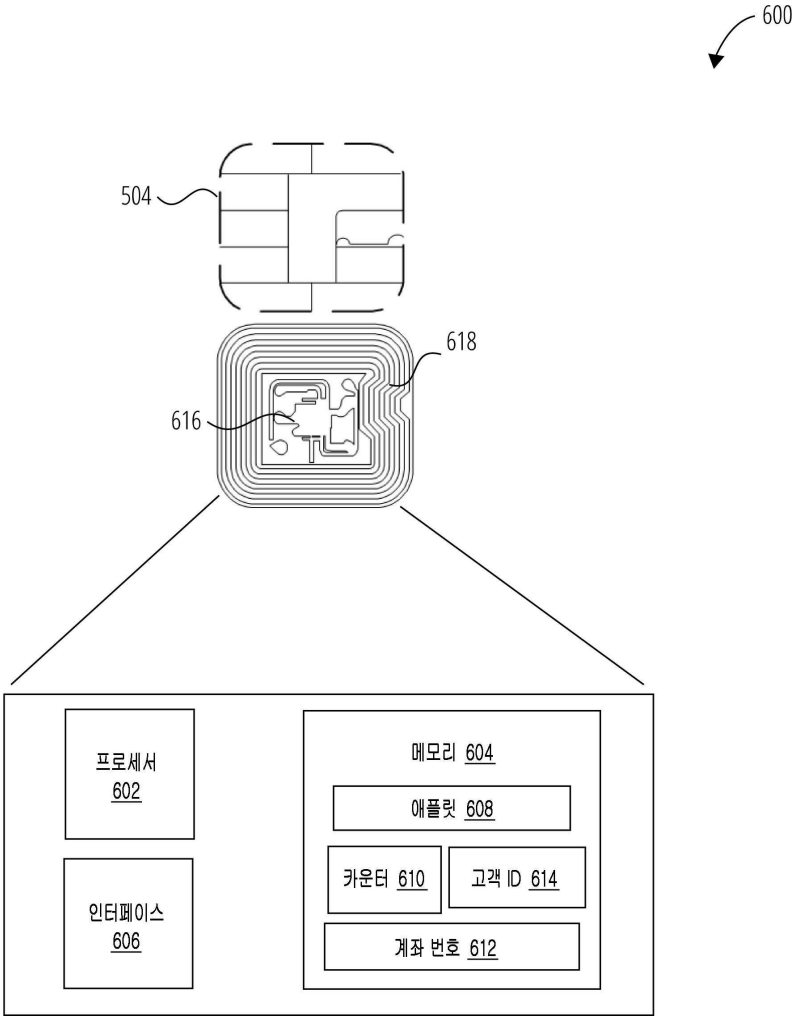
도면4


400
제1 모바일 디바이스가 데이터로 제2 모바일 디바이스와 연관된 사용자의 인증을
수행하도록 형상화 되고, 제2 모바일 디바이스로부터의 데이터를 포함하는
고유 리소스 로케이터(URL)를 포함하는 메시지를 제1 모바일 디바이스에 의해 수신 402
URL을 활성화하기 위한 입력을 제1 모바일 디바이스의 입력 디바이스에 의해 감지 404
응용프로그램은 데이터로 사용자의 인증을 수행하기 위한 서버와 통신하도록 형상화 되고,
입력에 응답하여 제1 모바일 디바이스에 의해 응용프로그램을 실행 406
사용자가 서버에 의해 인증되었는지의 표시를 제1 모바일 디바이스에 의해 수신 408
데이터 및 사용자가 인증되었다는 표시에 기반하여
화폐 교환의 수행을 제1 모바일 디바이스에 의해 유도 410

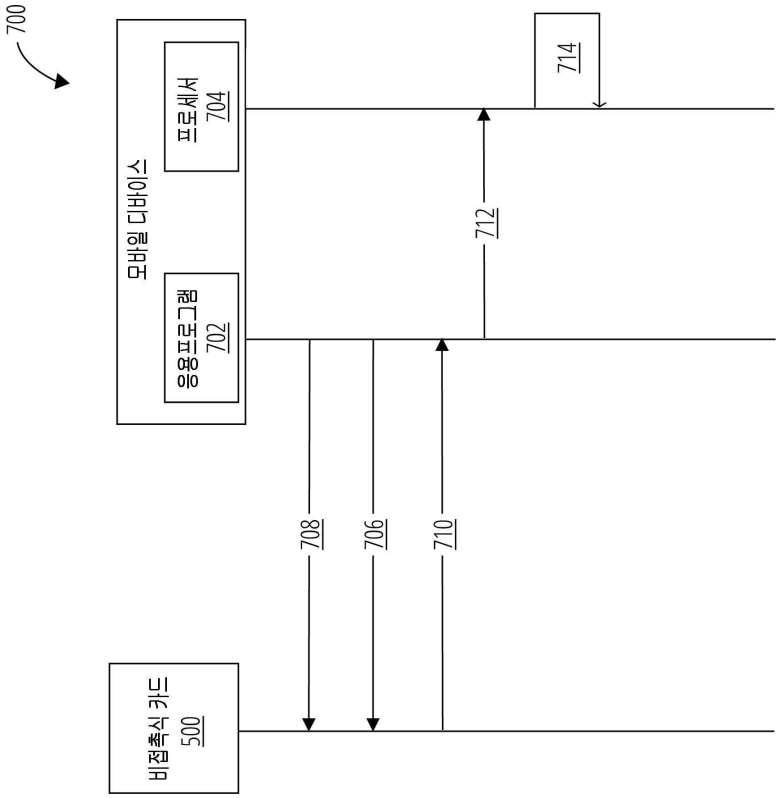
도면5


500
502
서비스 공급자
스마트 카드
504
1234 5678 1234 5678
508
506
카드 소유자 이름
유효기한

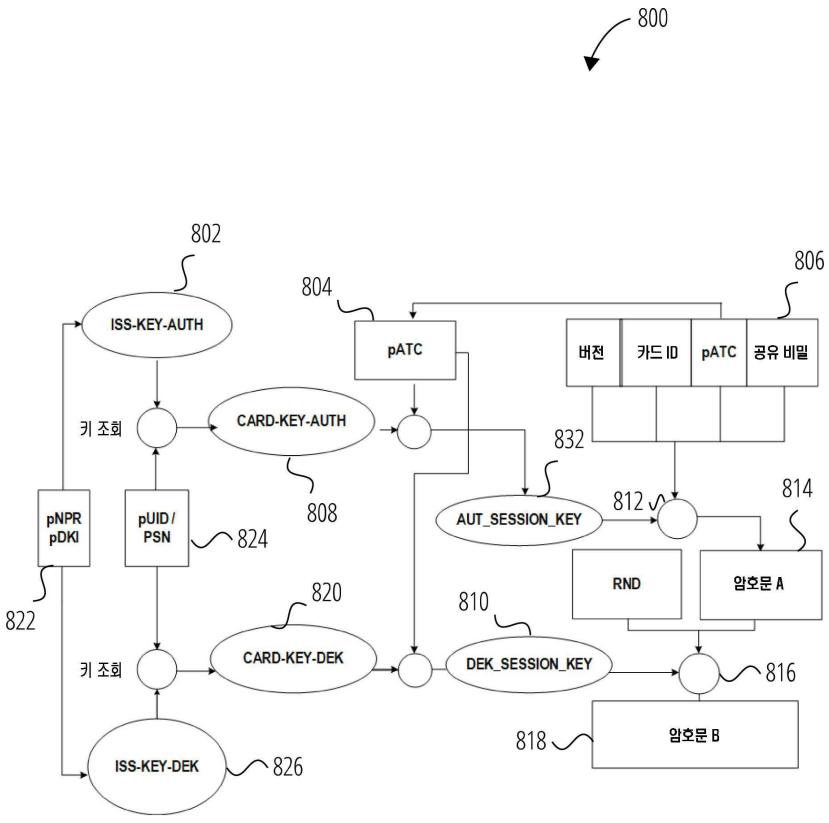
도면6


600
504
618
616
프로세서
602
인터페이스
606
메모리 604
애플릿 608
카운터 610
고객 ID 614
계좌 번호 612

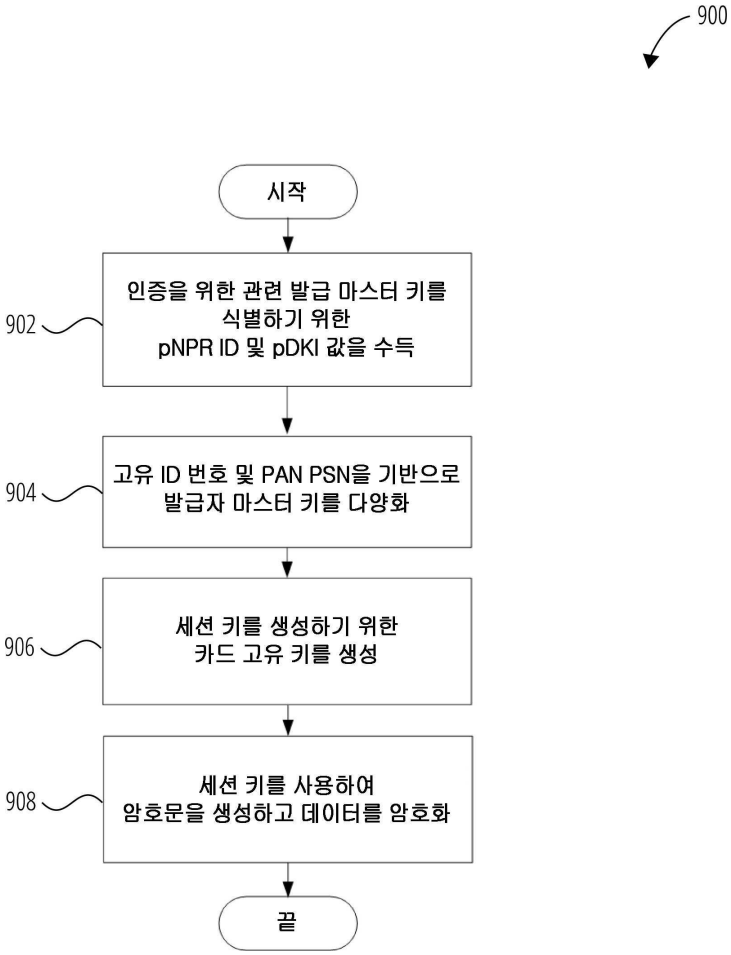
도면7


700
모바일 디바이스
프로세서
704
응용프로그램
702
714
712
708
706
710
비접촉식 카드
500

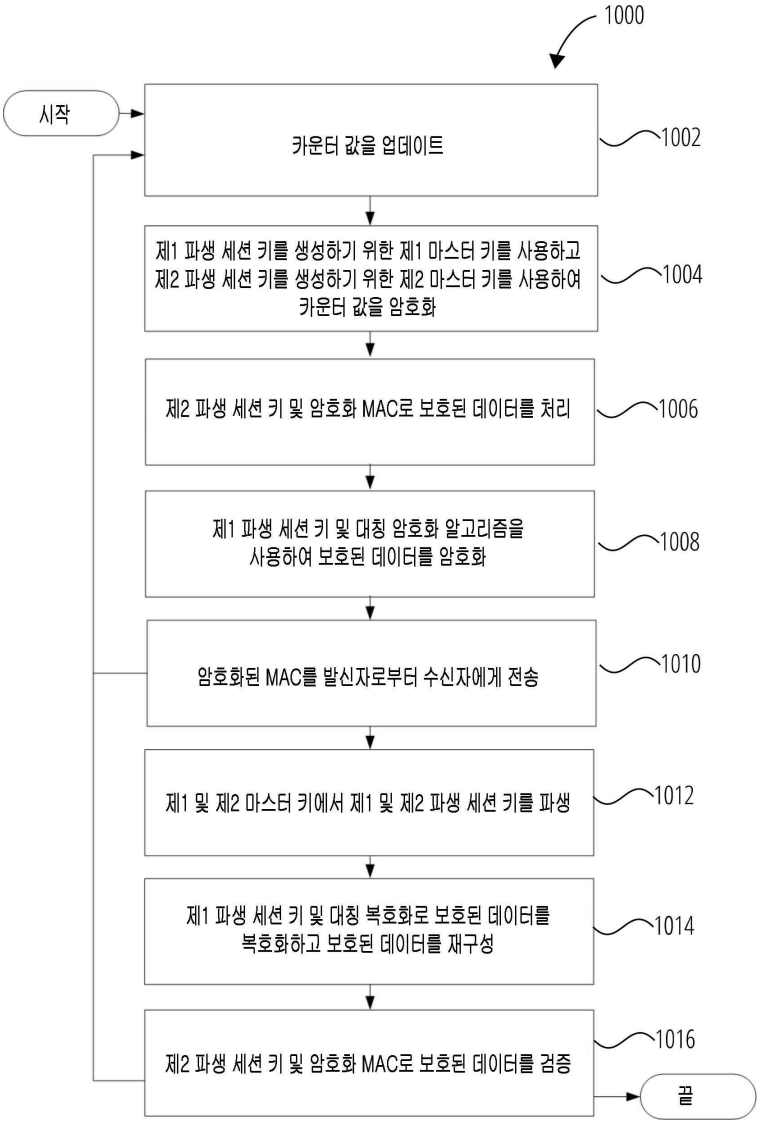
도면8


800
802
ISS-KEY-AUTH
804
pATC
806
버전
카드 ID
pATC
공유 비밀
키 조회
CARD-KEY-AUTH
808
832
AUT_SESSION_KEY
812
814
RND
암호문 A
pNPR
pDKI
822
pUID /
PSN
824
820
CARD-KEY-DEK
810
DEK_SESSION_KEY
816
키 조회
818
암호문 B
ISS-KEY-DEK
826

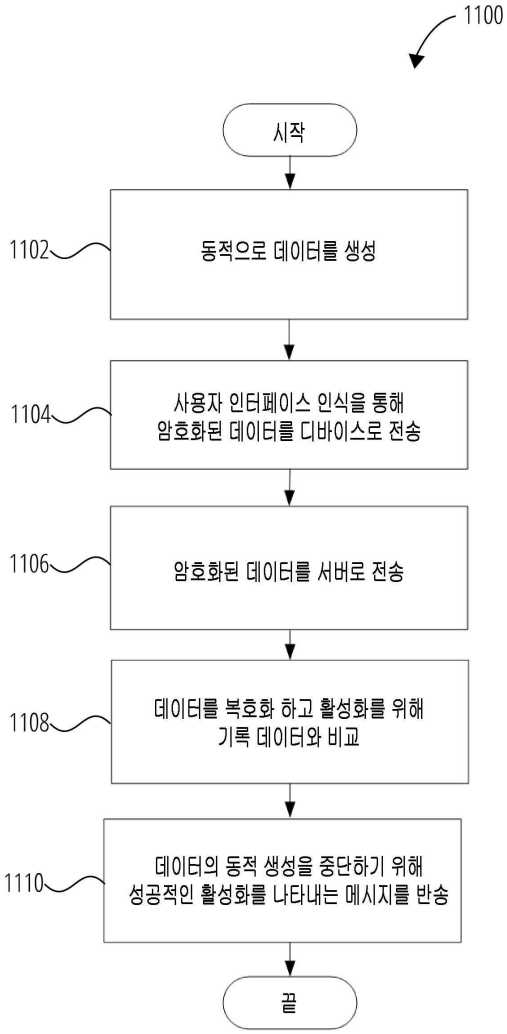
도면9


900
시작
902
인증을 위한 관련 발급 마스터 키를 식별하기 위한 pNPR ID 및 pDKI 값을 수득
904
고유 ID 번호 및 PAN PSN을 기반으로 발급자 마스터 키를 다양화
906
세션 키를 생성하기 위한 카드 고유 키를 생성
908
세션 키를 사용하여 암호문을 생성하고 데이터를 암호화
끝

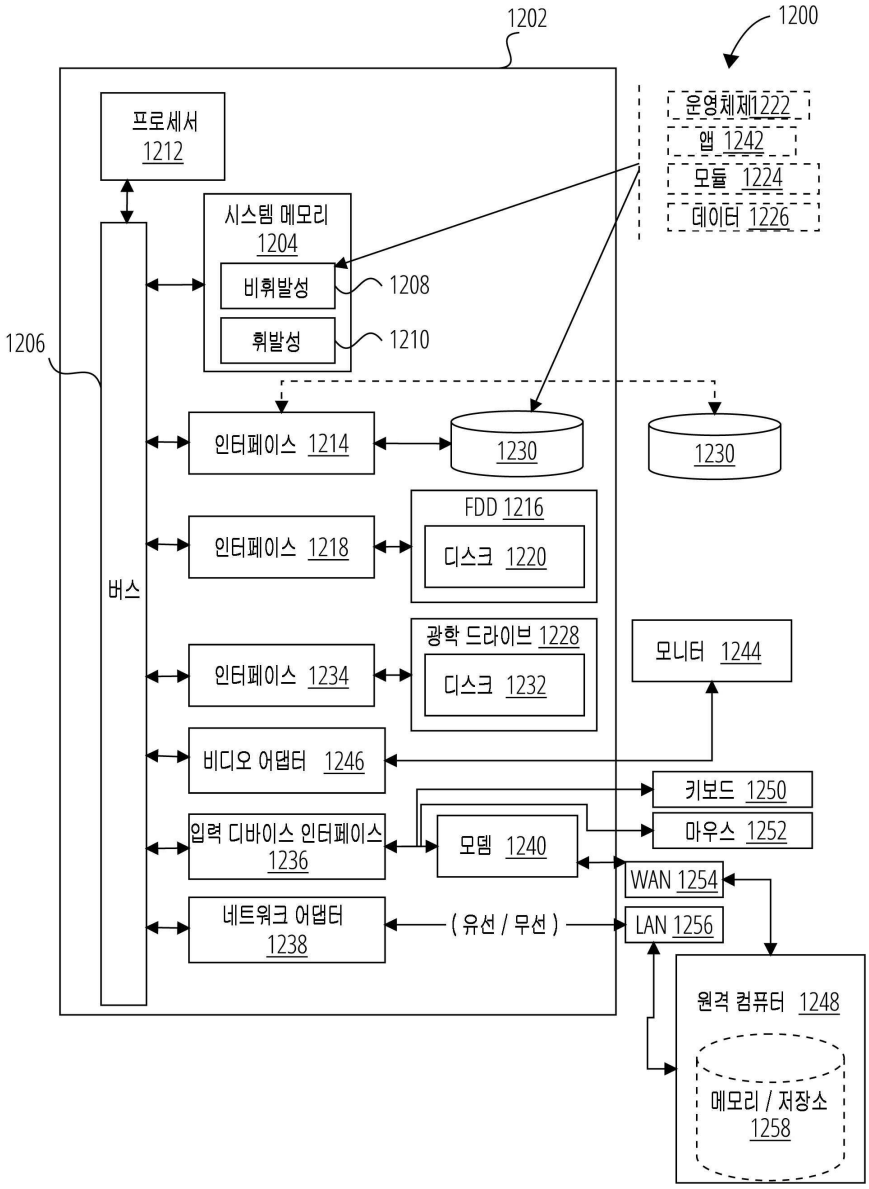
도면10


1000
시작
카운터 값을 업데이트
1002
제1 파생 세션 키를 생성하기 위한 제1 마스터 키를 사용하고
제2 파생 세션 키를 생성하기 위한 제2 마스터 키를 사용하여
카운터 값을 암호화
1004
제2 파생 세션 키 및 암호화 MAC로 보호된 데이터를 처리
1006
제1 파생 세션 키 및 대칭 암호화 알고리즘을
사용하여 보호된 데이터를 암호화
1008
암호화된 MAC를 발신자로부터 수신자에게 전송
1010
제1 및 제2 마스터 키에서 제1 및 제2 파생 세션 키를 파생
1012
제1 파생 세션 키 및 대칭 복호화로 보호된 데이터를
복호화하고 보호된 데이터를 재구성
1014
제2 파생 세션 키 및 암호화 MAC로 보호된 데이터를 검증
1016
끝

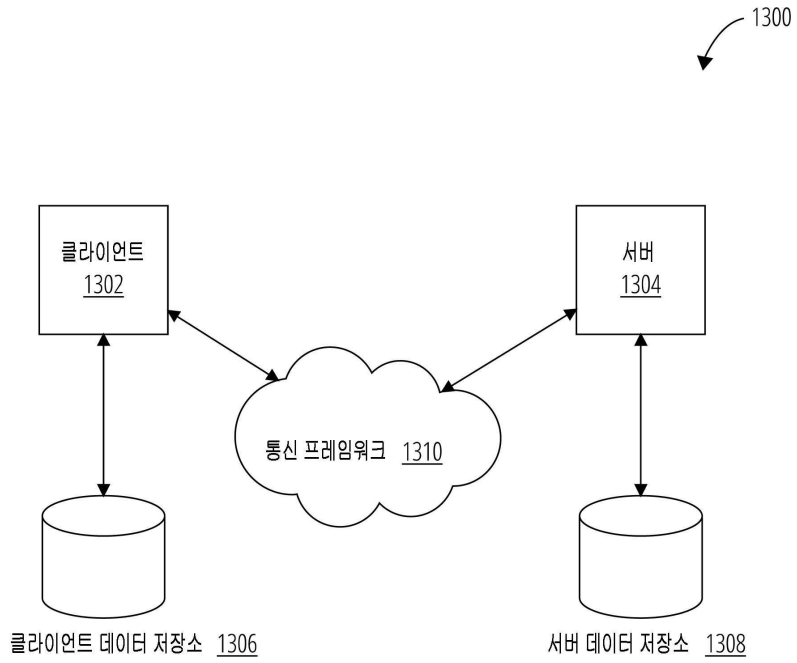
도면11


1100
시작
1102
동적으로 데이터를 생성
1104
사용자 인터페이스 인식을 통해
암호화된 데이터를 디바이스로 전송
1106
암호화된 데이터를 서버로 전송
1108
데이터를 복호화 하고 활성화를 위해
기록 데이터와 비교
1110
데이터의 동적 생성을 중단하기 위해
성공적인 활성화를 나타내는 메시지를 반송
끝

도면12


1202
1200
프로세서 1212
운영체제1222
앱 1242
모듈 1224
데이터 1226
시스템 메모리 1204
비휘발성
휘발성
1208
1210
1206
인터페이스 1214
1230
1230
FDD 1216
인터페이스 1218
디스크 1220
버스
광학 드라이브 1228
모니터 1244
인터페이스 1234
디스크 1232
비디오 어댑터 1246
키보드 1250
마우스 1252
입력 디바이스 인터페이스 1236
모뎀 1240
WAN 1254
네트워크 어댑터 1238
(유선 / 무선)
LAN 1256
원격 컴퓨터 1248
메모리 / 저장소 1258

도면13


1300
클라이언트
1302
서버
1304
통신 프레임워크 1310
클라이언트 데이터 저장소 1306
서버 데이터 저장소 1308