



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2025년03월04일

(11) 등록번호 10-2776180

(24) 등록일자 2025년02월27일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) H04L 9/32 (2006.01)(52) CPC특허분류
H04L 63/0853 (2013.01)
H04L 63/083 (2013.01)

(21) 출원번호 10-2022-7011540

(22) 출원일자(국제) 2020년11월23일

심사청구일자 2023년11월03일

(85) 번역문제출일자 2022년04월07일

(65) 공개번호 10-2022-0115919

(43) 공개일자 2022년08월19일

(86) 국제출원번호 PCT/US2020/061799

(87) 국제공개번호 WO 2021/133493

국제공개일자 2021년07월01일

(30) 우선권주장
16/725,547 2019년12월23일 미국(US)

(56) 선행기술조사문헌

US10438437 B

US20070118745 A1

EP02579199 A1

WO2005104704 A1

(73) 특허권자

캐피탈 원 서비스즈, 엘엘씨

미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680

(72) 발명자

에드워즈, 사무엘

미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680, 캐피탈 원 서비스즈, 엘엘씨 내

프리블, 제이슨

미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680, 캐피탈 원 서비스즈, 엘엘씨 내

카푸르소, 니콜라스

미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680, 캐피탈 원 서비스즈, 엘엘씨 내

(74) 대리인

김동완

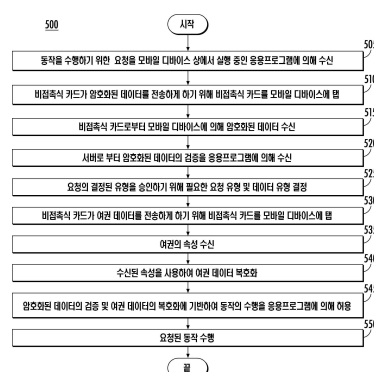
전체 청구항 수 : 총 20 항

심사관 : 천대식

(54) 발명의 명칭 비접촉식 카드에 저장된 여권 데이터 기반의 보안 인증

(57) 요약

계정과 연결된 비접촉식 카드에 저장된 여권 데이터를 기반으로 하는 보안 인증을 위한 시스템, 방법, 제조 물품 및 컴퓨터 판독 가능 매체가 제공된다. 응용프로그램은 동작을 수행하라는 지시를 수신할 수 있다. 응용프로그램은 카드에서 암호화된 데이터를 수신할 수 있다. 응용프로그램은 인증 서버가 개인 키를 기반으로 암호화된 데이터를 검증하였다는 표시를 수신할 수 있다. 응용프로그램은 비접촉식 카드로부터 암호화된 여권 데이터를 수신할 수 있으며 계정과 연관된 여권에 대한 암호화된 여권 데이터를 수신할 수 있다. 응용프로그램은 이미지 데이터 또는 텍스트 입력에 적어도 부분적으로 기반하여 여권의 속성을 결정할 수 있다. 응용프로그램은 여권 속성을 기반으로 암호화된 여권 데이터를 복호화할 수 있다. 응용프로그램은 인증 서버가 암호화된 데이터 및 암호화된 여권 데이터의 복호화를 검증했음을 명시하는 수신된 표시에 기반하여 동작의 수행을 개시할 수 있다.

대표도 - 도5

(52) CPC특허분류

H04L 63/0861 (2013.01)

H04L 63/105 (2013.01)

H04L 9/3247 (2013.01)

명세서

청구범위

청구항 1

디바이스의 프로세서에서 실행되는 응용프로그램에 의해, 응용프로그램의 다수의 기능 중 제1 기능을 이용하여 계정과 관련된 작업을 수행하라는 요청을 수신하는 단계;

응용프로그램에 의해 계정과 연결된 비접촉식 카드로부터 암호화된 데이터를 수신하는 단계;

인증 서버로부터 응용프로그램에 의해, 계정에 대한 제1 권한 레벨 및 인증 서버가 암호화된 데이터를 검증하였음을 명시하는 표시를 수신하는 단계;

응용프로그램에 의해 계정에 대한 제1 권한 수준이 응용프로그램의 제1 기능을 사용하여 작업을 수행하는 데 요구되는 권한 수준을 충족하지 않는다고 결정하는 단계;

요구되는 권한 수준을 충족하지 않는 제1 권한 레벨 및 다수의 규칙 중 제1 규칙에 기반한 응용프로그램에 의해, 응용프로그램의 제1 기능을 사용하여 요청된 작업의 수행을 시작하려면 암호화된 여권 데이터를 사용한 인증이 필요하다고 결정하는 단계;

응용프로그램에 의해 비접촉식 카드로부터 암호화된 여권 데이터 및 암호화된 여권 데이터에 대한 디지털 서명, 계정과 연관된 여권에 대한 암호화된 여권 데이터를 수신하는 단계;

응용프로그램에 의해 암호화된 여권 데이터를 복호화 하는 단계;

응용프로그램에 의해 공개키를 기반으로 암호화된 여권 데이터의 디지털 서명을 검증하는 단계;

암호화된 여권 데이터의 복호화 및 디지털 서명의 유효성 확인을 기반으로 인증 서버에 응용프로그램에 의해, 계정에 대한 첫 번째 권한 레벨의 표시, 디지털 서명의 유효성 확인을 반영하는 표시 및 암호화된 여권 데이터가 복호화 되었음을 명시하는 표시를 전송하는 단계;

응용프로그램이 인증 서버로부터 암호화된 여권 데이터의 복호화에 기반하여 계정에 할당된 제2 권한 레벨은 제1 권한 레벨보다 더 큰 권한을 지니는 제2 권한 레벨을 수신하는 단계; 및

응용프로그램의 제1 기능에 의해, 인증 서버가 암호화된 데이터, 암호화된 여권 데이터의 복호화, 계정의 제2 허용 레벨 및 디지털 서명이 유효함을 확인

했음을 명시하는 수신된 표시에 기반하여 동작의 수행을 시작하는 단계;

를 포함하는 방법.

청구항 2

제 1항에 있어서, 상기 암호화된 데이터는 비접촉식 카드와 연관된 다양화 키 및 고객 식별자에 기반하고, 상기 다양화 키는 비접촉식 카드와 연관된 카운터 값 및 마스터 키에 기반하고, 상기 서버는 다양화된 키, 카운터 값 및 마스터 키를 기반으로 암호화된 데이터를 검증하는 것을 특징으로 하는 방법.

청구항 3

제 1항에 있어서,

응용프로그램에 의해 암호화된 여권 데이터의 업데이트된 버전을 수신하는 단계; 및

비접촉식 카드에 저장하기 위해 암호화된 여권 데이터의 업데이트된 버전을 응용프로그램에 의해 비접촉식 카드로 전송하는 단계;

를 더욱 포함하는 방법.

청구항 4

제 1항에 있어서,

응용프로그램에 의해 여권의 제1 이미지로부터 여권의 적어도 하나의 속성을 추출하는 단계를 더욱 포함하고, 제1 이미지는 여권의 적어도 하나의 속성을 묘사하고, 응용프로그램은 추출된 적어도 하나의 속성에 기반하여 암호화된 데이터를 복호화 함을 특징으로 하는 방법.

청구항 5

제 1항에 있어서, 상기 동작은 (i) 응용프로그램의 다수 페이지 중 첫 번째 페이지에서 제공하는 제1 기능을 이용하여 계정의 속성을 조회하는 단계, (ii) 응용프로그램의 다수 페이지 중 두 번째 페이지에서 제공하는 다수의 기능 중 두 번째 기능을 사용하여 계정의 속성을 수정하는 단계, (iii) 응용프로그램의 다수 페이지 중 세 번째 페이지에서 제공되는 다수 기능 중 세 번째 기능에 액세스하는 단계, 또는 (iv) 응용프로그램의 다수 페이지 중 네 번째 페이지에서 제공하는 다수의 기능 중 제4 기능을 이용하여 비접촉식 카드를 이용한 거래를 처리하는 단계, 중 하나 이상의 단계를 포함함을 특징으로 하는 방법.

청구항 6

제 1항에 있어서, 상기 요구되는 허가 수준은 다수의 규칙 중 두 번째 규칙에 의해 상세화 됨을 특징으로 하는 방법.

청구항 7

제1항에 있어서, 상기 디지털 서명을 검증하는 단계는 공개 키에 기반하여 디지털 서명을 복호화 하는 단계를 포함함을 특징으로 하는 방법.

청구항 8

프로세서에 의해 실행될 때, 프로세서가 수행하도록 하는 명령어를 저장하는 비일시적 컴퓨터 판독가능 저장 매체에 있어서,

상기 명령어는 프로세서가

디바이스의 프로세서에서 실행되는 응용프로그램에 의해, 응용프로그램의 다수의 기능 중 제1 기능을 이용하여 계정과 관련된 작업을 수행하라는 요청을 수신하고;

응용프로그램에 의해 계정과 연결된 비접촉식 카드로부터 암호화된 데이터를 수신하고;

인증 서버로부터 응용프로그램에 의해, 계정에 대한 제1 권한 레벨 및 인증 서버가 암호화된 데이터를 검증하였음을 명시하는 표시를 수신하고;

응용프로그램에 의해 계정에 대한 제1 권한 수준이 응용프로그램의 제1 기능을 사용하여 작업을 수행하는 데 요구되는 권한 수준을 충족하지 않는다고 결정하고;

요구되는 권한 수준을 충족하지 않는 제1 권한 레벨 및 다수의 규칙 중 제1 규칙에 기반한 응용프로그램에 의해, 응용프로그램의 제1 기능을 사용하여 요청된 작업의 수행을 시작하려면 암호화된 여권 데이터를 사용한 인증이 필요하다고 결정하고;

응용프로그램에 의해 비접촉식 카드로부터 암호화된 여권 데이터 및 암호화된 여권 데이터에 대한 디지털 서명,

계정과 연관된 여권에 대한 암호화된 여권 데이터를 수신하고;

응용프로그램에 의해 암호화된 여권 데이터를 복호화 하고;

응용프로그램에 의해 공개키를 기반으로 암호화된 여권 데이터의 디지털 서명을 검증하고;

암호화된 여권 데이터의 복호화 및 디지털 서명의 유효성 확인을 기반으로 인증 서버에 응용프로그램에 의해, 계정에 대한 첫 번째 권한 레벨의 표시, 디지털 서명의 유효성 확인을 반영하는 표시 및 암호화된 여권 데이터가 복호화 되었음을 명시하는 표시를 전송하고;

응용프로그램이 인증 서버로부터 암호화된 여권 데이터의 복호화에 기반하여 계정에 할당된 제2 권한 레벨은 제1 권한 레벨보다 더 큰 권한을 지니는 제2 권한 레벨을 수신하고; 및

응용프로그램의 제1 기능에 의해, 인증 서버가 암호화된 데이터, 암호화된 여권 데이터의 복호화, 계정의 제2 허용 레벨 및 디지털 서명이 유효함을 확인

했음을 명시하는 수신된 표시에 기반하여 동작의 수행을 시작;

하도록 유도하는 비밀시적 컴퓨터 판독가능 저장 매체.

청구항 9

제 8항에 있어서, 상기 암호화된 데이터는 비접촉식 카드와 연관된 다양화 키 및 고객 식별자에 기반하고, 상기 다양화 키는 비접촉식 카드와 연관된 카운터 값 및 마스터 키에 기반하고, 상기 서버는 다양화된 키, 카운터 값 및 마스터 키를 기반으로 암호화된 데이터를 검증하는 것을 특징으로 하는 컴퓨터 판독가능 저장 매체.

청구항 10

제 8항에 있어서, 상기 명령어는 프로세서가

응용프로그램에 의해 암호화된 여권 데이터의 업데이트된 버전을 수신하고; 및

비접촉식 카드에 저장하기 위해 암호화된 여권 데이터의 업데이트된 버전을 응용프로그램에 의해 비접촉식 카드로 전송;

하도록 더욱 유도함을 특징으로 하는 컴퓨터 판독가능 저장 매체.

청구항 11

제 8항에 있어서, 상기 명령어는 프로세서가

응용프로그램에 의해 여권의 제1 이미지로부터 여권의 적어도 하나의 속성을 추출하는 단계를 더욱 유도하고, 제1 이미지는 여권의 적어도 하나의 속성을 묘사하고, 응용프로그램은 추출된 적어도 하나의 속성에 기반하여 암호화된 데이터를 복호화 함을 특징으로 하는 컴퓨터 판독가능 저장 매체.

청구항 12

제 8항에 있어서, 상기 동작은 (i) 응용프로그램의 다수 페이지 중 첫 번째 페이지에서 제공하는 제1 기능을 이용하여 계정의 속성을 조회함, (ii) 응용프로그램의 다수 페이지 중 두 번째 페이지에서 제공하는 다수의 기능 중 두 번째 기능을 사용하여 계정의 속성을 수정함, (iii) 응용프로그램의 다수 페이지 중 세 번째 페이지에서 제공되는 다수 기능 중 세 번째 기능에 액세스함, 또는 (iv) 응용프로그램의 다수 페이지 중 네 번째 페이지에서 제공하는 다수의 기능 중 제4 기능을 이용하여 비접촉식 카드를 이용한 거래를 처리함, 중 하나 이상의 동작을 포함함을 특징으로 하는 컴퓨터 판독가능 저장 매체.

청구항 13

제 8항에 있어서, 상기 요구되는 허가 수준은 다수의 규칙 중 두 번째 규칙에 의해 상세화 됨을 특징으로 하는 컴퓨터 판독가능 저장 매체.

청구항 14

제 8항에 있어서, 상기 디지털 서명을 검증함은 공개 키에 기반하여 디지털 서명을 복호화 함을 포함함을 특징으로 하는 컴퓨터 판독가능 저장 매체.

청구항 15

프로세서; 및

프로세서를 실행하는 명령어를 저장하는 메모리; 를 포함하는 컴퓨터 기기에 있어서,

상기 프로세서는

디바이스의 프로세서에서 실행되는 응용프로그램에 의해, 응용프로그램의 다수의 기능 중 제1 기능을 이용하여 계정과 관련된 작업을 수행하라는 요청을 수신하고;

응용프로그램에 의해 계정과 연결된 비접촉식 카드로부터 암호화된 데이터를 수신하고;

인증 서버로부터 응용프로그램에 의해, 계정에 대한 제1 권한 레벨 및 인증 서버가 암호화된 데이터를 검증하였음을 명시하는 표시를 수신하고;

응용프로그램에 의해 계정에 대한 제1 권한 수준이 응용프로그램의 제1 기능을 사용하여 작업을 수행하는 데 요구되는 권한 수준을 충족하지 않는다고 결정하고;

요구되는 권한 수준을 충족하지 않는 제1 권한 레벨 및 다수의 규칙 중 제1 규칙에 기반한 응용프로그램에 의해, 응용프로그램의 제1 기능을 사용하여 요청된 작업의 수행을 시작하려면 암호화된 여권 데이터를 사용한 인증이 필요하다고 결정하고;

응용프로그램에 의해 비접촉식 카드로부터 암호화된 여권 데이터 및 암호화된 여권 데이터에 대한 디지털 서명, 계정과 연관된 여권에 대한 암호화된 여권 데이터를 수신하고;

응용프로그램에 의해 암호화된 여권 데이터를 복호화 하고;

응용프로그램에 의해 공개키를 기반으로 암호화된 여권 데이터의 디지털 서명을 검증하고;

암호화된 여권 데이터의 복호화 및 디지털 서명의 유효성 확인을 기반으로 인증 서버에 응용프로그램에 의해, 계정에 대한 첫 번째 권한 레벨의 표시, 디지털 서명의 유효성 확인을 반영하는 표시 및 암호화된 여권 데이터가 복호화 되었음을 명시하는 표시를 전송하고;

응용프로그램이 인증 서버로부터 암호화된 여권 데이터의 복호화에 기반하여 계정에 할당된 제2 권한 레벨은 제1 권한 레벨보다 더 큰 권한을 지니는 제2 권한 레벨을 수신하고; 및

응용프로그램의 제1 기능에 의해, 인증 서버가 암호화된 데이터, 암호화된 여권 데이터의 복호화, 계정의 제2 허용 레벨 및 디지털 서명이 유효함을 확인

했음을 명시하는 수신된 표시에 기반하여 동작의 수행을 시작;

하도록 유도하는 컴퓨터 기기.

청구항 16

제 15항에 있어서, 상기 암호화된 데이터는 비접촉식 카드와 연관된 다양화 키 및 고객 식별자에 기반하고, 상기 다양화 키는 비접촉식 카드와 연관된 카운터 값 및 마스터 키에 기반하고, 상기 서버는 다양화된 키, 카운터

값 및 마스터 키를 기반으로 암호화된 데이터를 검증하는 것을 특징으로 하는 컴퓨터 기기.

청구항 17

제 15항에 있어서, 상기 명령어는 프로세서가

응용프로그램에 의해 암호화된 여권 데이터의 업데이트된 버전을 수신하고; 및

비접촉식 카드에 저장하기 위해 암호화된 여권 데이터의 업데이트된 버전을 응용프로그램에 의해 비접촉식 카드로 전송;

하도록 더욱 유도함을 특징으로 하는 컴퓨터 기기.

청구항 18

제 15항에 있어서, 상기 명령어는 프로세서가

응용프로그램에 의해 여권의 제1 이미지로부터 여권의 적어도 하나의 속성을 추출하는 단계를 더욱 유도하고, 제1 이미지는 여권의 적어도 하나의 속성을 묘사하고, 응용프로그램은 추출된 적어도 하나의 속성에 기반하여 암호화된 데이터를 복호화 함을 특징으로 하는 컴퓨터 기기.

청구항 19

제 15항에 있어서, 상기 동작은 (i) 응용프로그램의 다수 페이지 중 첫 번째 페이지에서 제공하는 제1 기능을 이용하여 계정의 속성을 조회함, (ii) 응용프로그램의 다수 페이지 중 두 번째 페이지에서 제공하는 다수의 기능 중 두 번째 기능을 사용하여 계정의 속성을 수정함, (iii) 응용프로그램의 다수 페이지 중 세 번째 페이지에서 제공되는 다수 기능 중 세 번째 기능에 액세스함, 또는 (iv) 응용프로그램의 다수 페이지 중 네 번째 페이지에서 제공하는 다수의 기능 중 제4 기능을 이용하여 비접촉식 카드를 이용한 거래를 처리함, 중 하나 이상의 동작을 포함함을 특징으로 하는 컴퓨터 기기.

청구항 20

제15항에 있어서, 상기 요구되는 허가 수준은 다수의 규칙 중 두 번째 규칙에 의해 상세화 됨을 특징으로 하고, 상기 디지털 서명을 검증함은 공개 키에 기반하여 디지털 서명을 복호화 함을 포함함을 특징으로 하는 컴퓨터 기기.

발명의 설명

기술 분야

[0001] 본 발명은 2019년 12월 23일자로 출원된 "비접촉식 카드에 저장된 여권 데이터 기반의 보안 인증"이라는 제목의 미국 특허출원 제16/725,547호에 대한 우선권을 주장한다. 상기 언급된 특허출원의 내용은 그 전체로 본 발명에 참조문헌으로 통합된다.

[0002] 본 명세서의 실시형태는 일반적으로 컴퓨터 플랫폼에 관한 것으로, 보다 구체적으로 보안 인증을 위해 여권 데이터를 저장하는 비접촉식 카드를 사용하는 것에 관한 것이다.

배경 기술

[0003] 신원 확인은 현대 컴퓨터 시스템에서 중요한 작업이다. 기존 접근 방식에서는 사용자가 컴퓨터 시스템에 액세스 하거나 전자 거래를 수행하려고 할 때 일회성 암호(OTP)와 같은 추가 정보를 제공해야 할 수 있다. 그러나 이러한 솔루션에는 보안 취약점이 있을 수 있다. 예를 들어 OTP는 가로채서 무단 액세스를 획득하는 데 사용될 수 있다. 또한 시스템마다 신원 확인을 위해 다른 유형의 추가 정보가 필요할 수 있으므로 많은 사용자에게 기존

솔루션을 비실용적으로 만든다.

발명의 내용

과제의 해결 수단

[0004] 본 명세서에 개시된 실시형태는 비접촉식 카드에 저장된 신원 데이터에 기반한 보안 인증을 위한 시스템, 방법, 제조 물품 및 컴퓨터 판독 가능 매체를 제공한다. 하나의 실시예에서 응용프로그램은 계정과 연관된 동작을 수행하도록 명시하는 표시를 수신할 수 있다. 응용프로그램은 계정과 연관된 비접촉식 카드로부터 암호화된 데이터를 수신할 수 있으며 암호화된 데이터는 암호학적 알고리즘, 고객 식별자 및 비접촉식 카드에 대한 개인 키를 기반으로 한다.

[0005] 응용프로그램은 인증 서버로부터 비접촉식 카드에 대한 개인 키에 기반하여 암호화된 데이터를 검증했다는 표시를 인증 서버로부터 수신할 수 있다. 응용프로그램은 비접촉식 카드로부터 암호화된 여권 데이터를 수신할 수 있으며, 계정과 연관된 여권에 대한 암호화된 여권 데이터를 수신할 수 있다. 응용프로그램은 이미지 데이터 또는 텍스트 입력에 적어도 부분적으로 기반하여 여권의 속성을 결정할 수 있다. 응용프로그램은 여권 속성을 기반으로 암호화된 여권 데이터를 복호화할 수 있다. 응용프로그램은 인증 서버가 암호화된 데이터 및 암호화된 여권 데이터의 복호화를 검증했음을 명시하는 수신된 표시에 기반하여 동작의 수행을 개시할 수 있다.

도면의 간단한 설명

[0006] 도 1a 내지 도 1b는 비접촉식 카드에 저장된 여권 데이터에 기반한 보안 인증을 위한 시스템의 실시형태를 도시한다.

도 2a 내지 도 2b는 비접촉식 카드에 저장된 여권 데이터에 기반한 보안 인증을 위한 시스템의 실시형태를 도시한다.

도 3a 내지 도 3b는 비접촉식 카드에 저장된 여권 데이터에 기반하여 보안 인증을 제공하기 위해 컴퓨터 디바이스에 비접촉식 카드를 탭 하는 실시형태를 도시한다.

도 4a 내지 도 4b는 예시적인 비접촉식 카드를 도시한다.

도 5는 제1 논리 흐름의 실시형태를 도시한다.

도 6은 제2 논리 흐름의 실시형태를 도시한다.

도 7은 제3 논리 흐름의 실시형태를 도시한다.

도 8은 컴퓨터 시스템의 실시형태를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0007] 본 발명에 개시된 실시형태는 비접촉식 카드에 저장된 여권 데이터를 사용하여 보안 인증을 위한 기술을 제공한다. 일반적으로 비접촉식 카드는 결제 정보, 여권 정보 및/또는 임의의 다른 이력 정보와 같은 사용자에게 대다수의 상이한 유형의 정보를 저장할 수 있다. 그 후 사용자는 구매, 모바일 디바이스에서 실행되는 응용프로그램을 통한 자금 이체, 응용프로그램을 통한 신용 증가 요청 등과 같은 동작을 수행하려고 시도할 수 있다.

[0008] 응용프로그램은 요청된 동작을 승인하는 데 필요한 인증 데이터 유형을 결정할 수 있다. 예를 들어 규칙은 응용프로그램을 통해 자금을 이체하려면 비접촉식 카드에 저장된 여권 데이터를 기반으로 한 인증이 필요하다고 명시할 수 있다. 따라서 응용프로그램은 해당 여권 데이터를 인증 데이터의 유형으로 결정할 수 있다.

[0009] 사용자는 보안 인증 프로세스를 시작하기 위해 모바일 디바이스에 비접촉식 카드를 탭 할 수 있다. 탭 하면 비접촉식 카드가 암호화된 데이터를 생성하여 응용프로그램에 전송할 수 있다. 암호화된 데이터는 암호화 알고리즘, 고객 식별자 및 비접촉식 카드에 대한 암호화 키를 기반으로 생성될 수 있다. 그 후 응용프로그램은 인증을 위해 인증 서버로 암호화된 데이터를 전송할 수 있다.

[0010] 그 후 서버는 비접촉식 카드에 대한 암호화 키의 로컬 사본을 사용하여 암호화된 데이터를 복호화하여 고객 식별자를 생성함으로써 암호화된 데이터를 인증할 수 있다. 그 후 서버는 암호화된 데이터의 인증 표시를 응용프로그램에 전송할 수 있다.

- [0011] 그 후 응용 프로그램은 여권 데이터의 암호 복호화를 시도할 수 있다. 일부 실시형태에서 여권 데이터는 암호화된 고객 식별자와 함께 응용프로그램으로 비접촉식 카드에 의해 전송된다. 다른 실시형태에서 여권 데이터는 비접촉식 카드의 또 다른 탭에 후속하여 비접촉식 카드에 의해 모바일 디바이스로 개별적으로 전송된다. 여권 데이터를 복호화하기 위해 응용프로그램은 여권의 하나 이상의 속성을 수신할 수 있다. 예를 들어 여권의 하나 이상의 페이지를 묘사하는 이미지가 캡처될 수 있으며 캡처된 이미지에서 속성이 추출될 수 있다.
- [0012] 다른 실시예로서 사용자는 속성을 입력으로 제공할 수 있다. 그 후 응용프로그램은 인증 서버가 여권 데이터의 암호화된 데이터 및 복호화를 검증했음을 명시하는 수신된 표시에 기반하여 동작의 수행을 승인할 수 있다. 예를 들어 사용자는 한 계정에서 다른 계정으로 자금을 이체하기 위해 응용프로그램의 인터페이스에 액세스하도록 허용될 수 있다.
- [0013] 유리하게는 본 발명에 개시된 실시형태는 모든 디바이스 및 관련 데이터의 보안을 개선한다. 예를 들어 응용프로그램 및/또는 데이터에 액세스하기 위해 비접촉식 카드에 의해 생성된 암호화된 데이터의 검증을 요구함으로써 응용프로그램 및/또는 데이터의 보안이 향상된다. 또 다른 실시예로서 구매 및 신용 연장과 같은 동작을 수행하기 전에 암호화된 여권 데이터의 유효성 검사를 요구함으로써 이러한 동작 및 관련 자산의 보안이 향상된다.
- [0014] 본 발명에 사용된 표기법 및 명명법을 일반적으로 참조하여, 다음의 상세한 설명의 하나 이상의 부분은 컴퓨터 또는 컴퓨터 네트워크에서 실행되는 프로그램 절차의 관점에서 제시될 수 있다. 이러한 절차적 설명 및 표현은 해당 분야의 숙련자에게 작업 내용을 가장 효과적으로 전달하기 위해 해당 기술 분야의 숙련자에 의해 사용된다. 여기에서 절차는 일반적으로 원하는 결과로 이어지는 자체 일관된 작업 시퀀스로 간주된다. 이러한 작업은 물리적 수량의 물리적 조작이 필요한 작업이다.
- [0015] 일반적으로 반드시 그런 것은 아니지만 이러한 수량은 저장, 전송, 결합, 비교 및 기타 조작이 가능한 전기, 자기 또는 광학 신호의 형태를 취한다. 주로 일반적인 사용을 위해 이러한 신호를 비트, 값, 요소, 기호, 문자, 용어, 숫자 등으로 지칭하는 것이 때때로 편리한 것으로 판명되었다. 그러나 이러한 모든 용어 및 유사한 용어는 적절한 물리적 수량과 관련되어야 하며 해당 수량에 적용되는 편리한 라벨일 뿐이다.
- [0016] 또한 이러한 조작은 일반적으로 인간 작업자가 수행하는 정신적 동작과 관련된 추가 또는 비교와 같은 용어로 참조된다. 그러나 인간 작업자의 그러한 능력은 하나 이상의 실시형태의 일부를 형성하는 본 명세서에 설명된 임의의 작업에서 대부분의 경우에 필요하지 않거나 바람직하지 않다. 오히려 이러한 작업은 기계 작업이다. 다양한 실시형태의 동작을 수행하기 위한 유용한 기계는 본 명세서의 가르침에 따라 기록된 내부에 저장된 컴퓨터 프로그램에 의해 선택적으로 활성화되거나 형상화된 디지털 컴퓨터를 포함 및/또는 요구되는 목적을 위해 특별히 구성된 디바이스 또는 디지털 컴퓨터를 포함한다.
- [0017] 또한 다양한 실시형태는 이러한 동작을 수행하기 위한 디바이스 또는 시스템에 관한 것이다. 이러한 디바이스는 요구되는 목적을 위해 특별히 제작될 수 있다. 이러한 다양한 기계에 필요한 구조는 주어진 설명에서 명백할 것이다.
- [0018] 이제 도면에 대한 참조가 이루어지며 여기에서 유사한 참조 번호는 전체에 걸쳐 유사한 엘리먼트를 나타내기 위해 사용된다. 하기 설명에서는 설명의 목적으로, 이에 대한 완전한 이해를 제공하기 위해 다수의 특정 세부사항이 제시된다. 그러나 신규한 실시형태는 이러한 특정 세부사항 없이도 실시될 수 있음이 명백할 수 있다. 다른 예에서 잘 알려진 구조 및 디바이스는 설명을 용이하게 하기 위해 블록도 형태로 표시된다. 의도는 청구 범위 내에서 모든 수정, 등가물 및 대안을 포함하는 것이다.
- [0019] 도 1a는 개시된 실시형태와 일치하는 예시적인 시스템(100)의 개략도를 도시한다. 도시된 바와 같이 시스템(100)은 하나 이상의 비접촉식 카드(101), 하나 이상의 모바일 컴퓨터 디바이스(110) 및 인증 서버(120)를 포함한다. 비접촉식 카드(101)는 신용 카드, 직불 카드, ATM 카드, 기프트 카드 등과 같은 임의의 형태의 결제 카드를 나타낸다. 비접촉식 카드(101)는 NFC, EMV 표준, 또는 무선 통신의 다른 단거리 프로토콜을 통해 컴퓨터 디바이스(110)와 통신하도록 구성된 무선 주파수 식별(RFID) 칩과 같은 하나 이상의 통신 인터페이스(133)를 포함할 수 있다. NFC가 예시적인 통신 프로토콜로 사용되었으나 본 발명은 EMV 표준, 블루투스 및/또는 Wi-Fi와 같은 다른 유형의 무선 통신에도 동일하게 적용 가능하다.
- [0020] 모바일 디바이스(110)는 스마트폰, 태블릿 컴퓨터, 웨어러블 디바이스, 랩톱, 휴대용 게임 디바이스 등과 같은 임의의 유형의 네트워크 가능 컴퓨터 디바이스를 나타낸다. 인증 서버(120)는 서버, 워크스테이션, 컴퓨터 클러스터, 클라우드 컴퓨터 플랫폼, 가상화된 컴퓨터 시스템 등과 같은 임의의 유형의 컴퓨터 디바이스를 나타낸다.

- [0021] 도시된 바와 같이 비접촉식 카드의 메모리(102)는 애플릿(103), 카운터(104), 마스터 키(105), 다양화 키(106), 고유 고객 식별자(ID)(107) 및 여권 데이터(108)를 포함한다. 애플릿(103)은 본 발명에 개시된 동작을 수행하도록 형상화된 실행 가능한 코드이다. 카운터(104), 마스터 키(105), 다양화 키(106) 및 고객 ID(107)는 하기 더욱 상세히 설명하는 바와 같이 시스템(100)에서 보안을 제공하기 위해 사용된다. 여권 데이터(108)는 비접촉식 카드(101)와 연관된 사용자의 전자 여권을 나타낸다.
- [0022] 여권 데이터(108)는 임의의 수 및 유형의 데이터를 포함할 수 있다. 예를 들어 여권 데이터(108)는 예를 들어 이름, 생년월일, 여권 번호, 여권 발급일, 여권 유효기한, 발급 국가 등과 같은 여권 및/또는 사용자의 상이한 속성을 설명하는 텍스트 데이터를 포함할 수 있을 뿐만 아니라 여권 자체의 하나 이상의 이미지, 여권에 포함된 사용자의 이미지 등과 같은 이미지 데이터를 포함할 수 있다.
- [0023] 일부 실시형태에서 여권 데이터(108)는 암호화된다. 예를 들어 여권 데이터(108)는 여권의 하나 이상의 속성에 기반하여 암호화될 수 있다. 하나 이상의 속성은 여권 번호, 여권 발행 일자 및/또는 여권 만료 일자를 포함할 수 있다.
- [0024] 도시된 바와 같이, 모바일 디바이스(110)의 메모리(111)는 운영 체제(OS)(112)의 인스턴스를 포함한다. 예시적인 운영 체제(112)는 Android® OS, iOS®, macOS®, Linux® 및 Windows® 운영 체제를 포함한다. 도시된 바와 같이 OS(112)는 계정 응용프로그램(113)을 포함한다. 계정 응용프로그램(113)은 사용자가 계정 잔고 보기, 아이템 구매, 지불 처리 등과 같은 다양한 계정 관련 동작을 수행할 수 있게 한다. 계정 응용프로그램(113)은 계정 응용프로그램(113) 및/또는 다른 응용프로그램(114)에 의해 제공되는 상이한 기능에 대한 액세스 권한을 추가로 제어할 수 있다.
- [0025] 일반적으로 사용자는 계정 응용프로그램(113)의 특정 기능에 액세스하기 위해 인증 자격증명을 사용하여 인증할 수 있다. 예를 들어 인증 자격증명은 사용자 이름(또는 로그인) 및 패스워드, 생체 인증 자격증명(예를 들어 지문, 얼굴 ID 등)을 포함할 수 있다.
- [0026] 다양한 실시형태에 따르면 사용자는 동작을 요청 및/또는 시도할 수 있다. 동작은 비접촉식 카드(101)를 사용하여 구매하고 계정 응용프로그램(113)의 특정 기능에 액세스하고 계정 응용프로그램(113)을 사용하여 다양한 계정 관련 동작을 수행하고 및/또는 다른 응용프로그램(114) 또는 그 기능에 액세스하는 것과 같은 임의의 유형의 동작을 포함할 수 있다.
- [0027] 다른 응용프로그램(114)은 웹 브라우저, 메시지 응용프로그램, 워드 프로세서 응용프로그램, 소셜 미디어 응용프로그램 등과 같은 임의의 유형의 컴퓨터 응용프로그램을 나타낸다. 예를 들어 사용자는 계정 응용프로그램(113)을 사용하여 자신의 계정에서 다른 계정으로 자금을 이체하기를 원할 수 있다. 본 발명에서 참조 예로서 특정 동작의 사용은 본 발명을 제한하지 않는다. 본 발명은 다른 유형의 동작에도 동일하게 적용 가능하기 때문이다.
- [0028] 요청된 동작을 승인하기 위해(예를 들어 상기 자금 이체의 예) 시스템(100)은 사용자의 신원을 인증 및/또는 검증해야 한다. 사용자의 신원을 인증하기 위해 본 발명에 개시된 실시형태는 비접촉식 카드(101)를 활용할 수 있다. 보다 구체적으로 사용자가 동작을 수행하도록 또는 그렇지 않으면 제한된 리소스에 액세스하도록 요청하면 계정 응용프로그램(113)은 사용자에게 비접촉식 카드(101)를 디바이스(110)에 탭 하도록 지시하는 알림을 출력할 수 있다.
- [0029] 일반적으로 비접촉식 카드(101)가 디바이스(110)의 통신 인터페이스(118)의 통신 범위 내로 잔압허몬 비접촉식 카드(101)의 애플릿(103)은 암호화된 데이터를 예를 들어 암호화된 고객 ID(132)를 요청된 동작을 승인하기 위해 필요한 인증 프로세스의 일부로 생성할 수 있다.
- [0030] 비접촉식 카드(101)와 모바일 디바이스(110) 간의 NFC 데이터 전송을 가능하게 하기 위해 비접촉식 카드(101)가 모바일 디바이스(110)의 통신 인터페이스(118)에 충분히 가까울 때 계정 응용프로그램(113)은 비접촉식 카드(101)와 통신할 수 있다. 통신 인터페이스(118)는 예를 들어 NFC, 블루투스, RFID 등을 통해 비접촉식 카드(101)의 통신 인터페이스(133)로부터 판독 및/또는 통신하도록 형상화될 수 있다. 따라서 예시적인 통신 인터페이스(118)는 NFC 통신 모듈, 블루투스 통신 모듈 및/또는 RFID 통신 모듈을 포함한다.
- [0031] 언급된 바와 같이 시스템(100)은 데이터를 보호하기 위해 키 다양화를 구현하도록 형상화되며 이는 본 발명에서 키 다양화 기술로 지칭될 수 있다. 일반적으로 서버(120) 또는 다른 컴퓨터 디바이스 및 비접촉식 카드(101)에는 마스터 대칭 키라고도 하는 동일한 마스터 키(105)가 제공될 수 있다.

- [0032] 보다 구체적으로 각각의 비접촉식 카드(101)는 서버(120)에서 대응하는 쌍을 지니는 별개의 마스터 키(105)로 프로그램 된다. 예를 들어 비접촉식 카드(101)가 제조될 때, 고유한 마스터 키(105)는 고유 마스터 키가 비접촉식 카드(101)의 메모리(102) 내에 프로그래밍 될 수 있다. 유사하게, 고유 마스터 키(105)는 서버(120) 및/또는 하드웨어 보안 모듈(HSM)(125)과 같은 다른 보안 위치에 저장된 계정 데이터(124) 내의 비접촉식 카드(101)와 연관된 고객의 기록에 저장될 수 있다.
- [0033] 마스터 키는 비접촉식 카드(101) 및 서버(120) 이외의 모든 당사자들로부터 비밀로 유지될 수 있으며 이에 의해 시스템(100)의 보안이 강화된다. 일부 실시형태에서 비접촉식 카드(101)의 애플릿(103)은 마스터 키(105)를 사용하여 및 암호화 알고리즘의 입력으로 데이터를 사용하여 데이터(예를 들어 고객 ID(107) 및/또는 여권 데이터(108))를 암호화 및/또는 복호화 할 수 있다. 예를 들어 마스터 키(105)로 고객 ID(107)를 암호화 함으로써 암호화된 고객 ID(132)가 생성될 수 있다. 유사하게 인증 서버(120)는 대응하는 마스터 키(105)를 사용하여 비접촉식 카드(101)와 관련된 데이터를 암호화 및/또는 복호화 할 수 있다.
- [0034] 다른 실시형태에서 비접촉식 카드(101) 및 서버(120)의 마스터 키(105)는 키 다양화를 사용하여 보안을 강화하기 위해 카운터(104)와 함께 사용될 수 있다. 카운터(104)는 비접촉식 카드(101)와 서버(120) 사이에서 동기화된 값을 포함할 수 있다. 값(104)은 비접촉식 카드(101)와 서버(120) 및/또는 비접촉식 카드(101) 및/또는 모바일 디바이스(110) 사이에서 데이터가 교환될 때마다 변경되는 숫자를 포함할 수 있다.
- [0035] 예를 들어 서버(120) 및/또는 모바일 디바이스(110)로 데이터를 전송할 준비를 할 때 비접촉식 카드(101)는 카운터 값(104)을 증가시킬 수 있다. 그 후 비접촉식 카드(101)는 마스터 키(105) 및 카운터 값(104)을 출력으로 다양화 키(106)를 생성하는 암호화 알고리즘에 대한 입력으로 제공할 수 있다. 암호화 알고리즘은 암호화 알고리즘, 해시 기반 메시지 인증 코드(HMAC) 알고리즘, 암호 기반 메시지 인증 코드(CMAC) 알고리즘 등을 포함할 수 있다. 암호화 알고리즘의 비제한적인 예는 3DES 또는 AES128과 같은 대칭 암호화 알고리즘; HMAC-SHA-256과 같은 대칭 HMAC 알고리즘; 및 AES-CMAC와 같은 대칭 CMAC 알고리즘이 있다.
- [0036] 주요 다양화 기술의 예는 2018년 11월 29일자로 출원된 미국 특허출원 제16/205,119호에 더 자세히 설명되어 있다. 상기 특허 출원은 그 전체로 본 발명에 참고문헌으로 통합된다.
- [0037] 키 다양화 예를 계속하면, 비접촉식 카드(101)는 다양화 키(106) 및 암호화 알고리즘에 대한 입력으로 데이터를 사용하여 데이터 예를 들어 고객 ID(107) 및/또는 여권 데이터(108)와 같은 임의의 다른 데이터를 암호화할 수 있다. 예를 들어 다양화 키(106)로 고객 ID(107)를 암호화하면 암호화된 고객 ID(132)가 생성될 수 있다.
- [0038] 사용된 암호화 기술에 관계없이 비접촉식 카드(101)는 암호화된 데이터 예를 들어 암호화된 고객 ID(132)를 모바일 디바이스(110)의 계정 응용프로그램(113)에 예를 들어 NFC 연결, 블루투스 연결 등을 통해 전송할 수 있다. 모바일 디바이스(110)의 계정 응용프로그램(113)은 암호화된 고객 ID(132)를 네트워크(130)를 통해 서버(120)로 전송할 수 있다. 적어도 하나의 실시형태에서 비접촉식 카드(101)는 암호화된 데이터와 함께 카운터 값(104)을 전송한다. 이러한 실시형태에서 비접촉식 카드(101)는 암호화된 카운터 값(104) 또는 암호화되지 않은 카운터 값(104)을 전송할 수 있다.
- [0039] 일단 수신되면 인증 응용프로그램(123)은 암호화된 고객 ID(132)를 인증할 수 있다. 예를 들어 인증 응용프로그램(123)은 인증 서버(120)의 메모리(122)에 저장된 마스터 키(105)의 사본을 사용하여 암호화된 고객 ID(132)의 복호화를 시도할 수 있다. 다른 실시예에서 인증 응용프로그램(123)은 출력으로 다양화 키(106)를 생성하는 암호화 알고리즘에 대한 입력으로 마스터 키(105) 및 카운터 값(104)을 제공할 수 있다. 결과적인 다양화 키(106)는 비접촉식 카드(101)의 다양화 키(106)에 대응할 수 있으며 이는 암호화된 고객 ID(132)를 복호화 하는데 사용될 수 있다.
- [0040] 사용된 복호화 기술에 관계없이 인증 응용프로그램(123)은 암호화된 고객 ID(132)를 성공적으로 복호화함으로써 암호화된 고객 ID(132)를 검증할 수 있다. 예를 들어 결과적인 고객 ID(107)를 계정 데이터(124)에 저장된 고객 ID와 비교함으로써 및/또는 키(105 및/또는 106)를 사용한 복호화가 성공했다는 표시에 기반한다. 키(105, 106)가 메모리(122)에 저장되는 것으로 도시되어 있으나 키(105, 106)는 보안 요소 및/또는 HSM(125)과 같은 다른 곳에 저장될 수 있다.
- [0041] 그러한 실시형태에서 보안 요소 및/또는 HSM(125)은 키(105 및/또는 106) 및 암호화 기능을 사용하여 암호화된 고객 ID(132)를 복호화 할 수 있다. 유사하게 보안 요소 및/또는 HSM(125)은 전술한 바와 같이 마스터 키(105) 및 카운터 값(104)에 기반하여 다양화 키(106)를 생성할 수 있다.

- [0042] 그러나 인증 응용프로그램(123)이 암호화된 고객 ID(132)를 복호화 하여 예상 결과(예를 들어 비접촉식 카드(101)와 관련된 계정의 고객 ID(107))를 생성할 수 없는 경우, 인증 응용프로그램(123)은 암호화된 고객을 검증하지 않는다. 이러한 예에서 인증 응용프로그램(123)은 실패한 검증의 표시를 계정 응용프로그램(113)에 전송한다. 이와 같이 계정 응용프로그램(113)은 계정의 보안을 유지하기 위해 요청된 동작의 수행을 거부할 수 있다.
- [0043] 도 1b는 인증 응용프로그램(123)이 암호화된 고객 ID(132)를 복호화 하여 암호화된 데이터를 검증 또는 인증의 하나의 실시형태를 도시한다. 도시된 바와 같이 인증 응용프로그램(123)은 인증 응용프로그램(123)이 암호화된 고객 ID(132)를 성공적으로 복호화 하였음 나타내는 검증(134)을 모바일 디바이스(110)에 전송한다. 검증(134)수신에 응답하여 계정 응용프로그램(113)은 필요하다면 어떤 추가 인증 단계가 필요한 지 결정하기 위해 규칙(115)을 참조할 수 있다. 규칙(115)은 일반적으로 다수의 상이한 인증 규칙 및/또는 상이한 요청된 동작에 대한 임계 값을 지정할 수 있다. 규칙은 요청된 동작 유형을 기반으로 할 수 있다. 예를 들어 자금 이체를 위해 규칙(115)은 여권 데이터(108)와 같은 추가 데이터 요소에 기반한 추가 인증을 요구할 수 있다.
- [0044] 그러한 실시예에서 계정 응용프로그램(113)은 사용자가 비접촉식 카드(101)를 모바일 디바이스(110)에 탭 한다는 것을 명시하는 표시를 출력할 수 있다. 그 후 계정 응용프로그램(113)은 비접촉식 카드(101)에 여권 데이터(108)를 전송하도록 지시할 수 있다. 비접촉식 카드(101)는 여권 데이터(108)를 계정 응용프로그램(113)으로 전송할 수 있다. 언급된 바와 같이 일부 실시형태에서 여권 데이터(108)는 암호화될 수 있다. 여권 데이터(108)는 사용자 여권의 여권 번호, 사용자 여권 발행 일자 및/또는 사용자 여권 만료 일자와 같은 여권의 하나 이상의 속성을 사용하여 암호화될 수 있다. 비접촉식 카드(101)의 개별 탭에서 수신되는 것으로 도시되어 있으나 일부 실시형태에서 여권 데이터(108)는 모바일 디바이스(110)에 대한 비접촉식 카드(101)의 단일 탭 예를 들어 도 1a에 도시된 탭에서 암호화된 사용자 ID(132)와 함께 전송된다.
- [0045] 그 후 계정 응용프로그램(113)은 암호화된 여권 데이터(108)를 복호화 하기 위한 여권 속성을 수신할 수 있다. 예를 들어 사용자는 계정 응용프로그램(113)의 그래픽 사용자 인터페이스(GUI)를 통해 여권 번호, 만료 일자 및/또는 발행 일자를 제공할 수 있다. 다른 실시형태에서 모바일 디바이스(110)의 카메라(119)는 여권의 물리적 버전의 하나 이상의 페이지의 하나 이상의 이미지를 캡처하는 데 사용될 수 있다. 하나 이상의 페이지는 암호화된 여권 데이터(108)를 복호화 하는 데 필요한 속성을 나타낼 수 있다. 따라서 계정 응용프로그램(113)은 예를 들어 컴퓨터 비전, 광학 문자 인식(OCR) 등을 사용하여 캡처된 이미지에서 여권 번호, 유효기한 및/또는 발급 날짜를 추출할 수 있다.
- [0046] 도 1b에 도시된 실시형태에서 계정 응용프로그램(113)은 수신된 여권 속성을 사용하여 암호화된 여권 데이터(108)를 복호화 한다. 암호 복호화가 성공하면 계정 응용프로그램(113)은 요청된 동작의 수행을 허용할 수 있다. 예를 들어 여권 데이터(108)를 복호화 할 때, 계정 응용프로그램(113)은 사용자가 원하는 자금 이체를 개시할 수 있도록 하는 GUI를 표시할 수 있다. 그렇지 않으면 계정 응용프로그램(113)은 예를 들어 자금 이체를 위한 GUI에 대한 액세스를 차단하고 실패한 암호 복호화에 기반하여 요청된 동작을 수행할 수 없다는 알림을 출력함으로써 요청된 동작의 수행을 제한할 수 있다.
- [0047] 일부 실시형태에서 인증 서버(120)는 암호화된 여권 데이터(108)를 복호화 한다. 예를 들어 도 2a는 인증 서버(120)가 여권 데이터(108)를 복호화 하는 데 사용되는 실시형태를 도시하는 개략도(200)이다. 도시된 바와 같이 사용자는 요청된 동작으로 진행하기 위해 모바일 디바이스(110)에 비접촉식 카드(101)를 탭 한다. 언급된 바와 같이 사용자는 비접촉식 카드(101)를 디바이스(110)에 탭 하기 전에 비접촉식 카드(101)와 연관된 계정에 액세스하기 위해 인증 자격증명을 제공할 수 있다.
- [0048] 예를 들어 요청된 동작은 계정 세부사항에 액세스하기 위해 인증 자격증명을 제공한 후 계정 응용프로그램(113)에서 계정 정보를 업데이트하는 것일 수 있다. 탭에 응답하여 애플릿(103)은 암호화된 고객 ID(201)를 생성하고 이는 암호화된 여권 데이터(108)와 함께 계정 응용프로그램(113)에 전송된다. 일반적으로 암호화된 고객 ID(201)는 암호화된 고객 ID(132)의 생성과 관련하여 전송한 바와 같이 예를 들어 마스터 키(105) 및/또는 다양화 키(106)로 고객 ID(107)를 암호화함으로써 애플릿(103)에 의해 생성된다.
- [0049] 암호화된 고객 ID(201) 및 암호화된 여권 데이터(108)를 수신하는 것에 응답하여 계정 응용프로그램(113)은 암호화된 여권 데이터(108)를 복호화 하는 데 필요한 여권 속성 예를 들어 여권 번호, 만료 일자 및/또는 발행 일자를 수신할 수 있다. 예를 들어 사용자는 계정 응용프로그램(113)의 GUI에서 입력으로 여권 속성을 제공할 수 있다. 다른 예로서 물리적 여권의 이미지가 캡처 될 수 있으며 계정 응용프로그램(113)은 예를 들어 이미지에서 관련 필드와 값을 식별함으로써 캡처 된 이미지로부터 여권 속성을 추출할 수 있다. 일단 수신되면 계정 응용프로그램(113)은 수신된 여권 속성을 암호화된 고객 ID(201) 및 여권 데이터(108)와 함께 여권 속성(202)으로서

인증 서버(120)에 전송할 수 있다.

- [0050] 일단 수신되면 인증 응용프로그램(123)은 상기 설명된 바와 같이 마스터 키(105) 및/또는 다양화 키(106)를 사용하여 암호화된 고객 ID(201)를 복호화 하려고 시도할 수 있다. 암호 복호화 시도가 계정과 관련된 고객 ID(107)를 생성하면 인증 응용프로그램(123)은 여권 속성(202)을 사용하여 여권 데이터(108)의 암호 복호화를 시도할 수 있다.
- [0051] 암호화된 고객 ID(201) 및 여권 데이터(108)의 복호화가 성공하면, 도 2b에 반영된 바와 같이 인증 응용프로그램(123)은 검증(204)을 계정 응용프로그램(113)에 전송할 수 있다. 계정 응용프로그램(113)은 암호화된 고객 ID(201) 및 암호화된 여권 데이터(108)가 인증 서버(120)에 의해 검증(또는 인증)되었음을 명시하는 검증(204)의 수신에 기반하여 요청된 동작을 허용할 수 있다. 예를 들어 계정 응용프로그램(113)은 사용자가 자신의 계정 세부사항을 수정할 수 있게 하는 GUI를 노출 및/또는 활성화할 수 있다.
- [0052] 암호화된 고객 ID(201) 및 암호화된 여권 데이터(108)의 복호화 시도 중 하나가 성공하지 못한 경우, 인증 응용프로그램(123)은 실패한 암호 복호화의 표시를 계정 응용프로그램(113)에 전송할 수 있으며, 이는 요청된 동작의 수행을 거부할 수 있다. 예를 들어 계정 응용프로그램(113)은 사용자가 자신의 계정 세부사항을 수정할 수 있게 하는 GUI에 대한 액세스를 제한 및/또는 그 요소를 비활성화할 수 있다.
- [0053] 일부 실시형태에서 여권 속성을 사용하여 암호화된 여권 데이터(108)는 마스터 키(104) 및/또는 다양화 키(106)에 기반하여 애플릿(103)에 의해 추가로 암호화될 수 있다. 따라서 이러한 실시형태에서 인증 응용프로그램(123)은 전술한 바와 같이 키(105 및/또는 106)를 사용하여 여권 데이터(108)를 초기에 복호화한다. 초기 복호화가 성공하면 인증 응용프로그램(123)은 여권 속성(202)을 사용하여 여권 데이터(108)의 복호화를 시도할 수 있다. 여권 속성(202)을 사용하는 여권 데이터(108)의 복호화가 성공하면 인증 응용프로그램(123)은 요청된 동작을 승인하는 계정 응용프로그램(113)에 검증(204)을 전송할 수 있다.
- [0054] 여권 데이터(108)를 복호화 하는 엔티티에 관계없이 적어도 하나의 실시형태에서 비접촉식 카드(101)의 애플릿(103)은 키(105 및/또는 106)를 사용하여 여권 데이터(108)에 대한 디지털 서명(도시되지 않음)을 생성할 수 있다. 디지털 서명은 여권 데이터(108)에 서명할 수 있다. 그 후 비접촉식 카드(101)는 여권 데이터(108)와 함께 디지털 서명을 계정 응용프로그램(113)에 전송할 수 있고, 계정 응용프로그램(113)은 차례로 디지털 서명을 인증 서버(120)에 전송한다. 또한 인증 응용프로그램(123)은 비접촉식 카드(101)와 연관되고 서버(120)에 의해 저장된 공개 키를 사용하여 디지털 서명을 복호화 함으로써 디지털 서명을 검증할 수 있다.
- [0055] 전자 서명이 검증되면 인증 응용프로그램(123)은 성공적인 전자 서명 검증의 표시를 계정 응용프로그램(113)으로 전송할 수 있고 이는 전자 서명의 검증에 기반한 동작의 수행을 허용할 수 있다. 전자 서명이 검증되지 않은 경우, 계정 응용프로그램(113)은 동작의 수행을 제한할 수 있다.
- [0056] 여권 데이터(108)를 복호화하는 엔티티에 관계없이 일부 실시형태에서 계정 응용프로그램(113)은 동작을 수행하는 데 필요한 규칙(115)에 의해 명시된 액세스 권한의 수준을 결정할 수 있다. 예를 들어 규칙(115)은 사용자가 요청된 동작 예를 들어 자금 이체를 수행하기 위해 "높은" 보안 수준을 지닐 것을 요구할 수 있다. 그러나 사용자의 계정 응용프로그램(113)에 국소적으로 저장되고 및/또는 서버(120)로부터 수신될 수 있는 계정 데이터(124)()는 사용자가 "중간" 수준의 보안을 지닌다는 것을 명시할 수 있다.
- [0057] 이러한 실시형태에서 계정 응용프로그램(113)은 업데이트된 권한 수준에 대한 요청을 서버(120)에 전송할 수 있다. 응답으로 인증 응용프로그램(123)은 암호화된 고객 ID 및 여권 데이터(108)의 복호화에 기반하여 사용자의 권한 수준을 "높음"으로 업데이트하기로 결정할 수 있다. 이러한 실시형태에서 인증 응용프로그램(123)은 업데이트된 권한 수준을 계정 응용프로그램(113)에 전송할 수 있으며, 이는 규칙(115)에 의해 요구되는 권한 수준을 충족시키는 업데이트된 권한 수준에 기반하여 요청된 동작을 허용한다.
- [0058] 또한 일부 실시형태에서 사용자는 새로운 및/또는 업데이트된 여권을 취득할 수 있다. 이러한 실시형태에서 계정 응용프로그램(113)은 예를 들어 인증 서버(120)로부터 여권 데이터(108)의 신규 및/또는 업데이트된 버전을 수신할 수 있다. 이러한 실시형태에서 계정 응용프로그램(113)은 서버(120)로부터 수신된 업데이트된 여권 데이터를 비접촉식 카드(101)에 전송할 수 있으며 애플릿(103)은 수신된 데이터를 메모리(102) 내에 저장할 수 있다.
- [0059] 도 3a는 비접촉식 카드(101)에 저장된 여권 데이터(108)에 기반하여 보안 인증을 제공하기 위해 비접촉식 카드(101)를 탭 하는 예시적인 실시형태를 도시하는 개략도(300)이다. 도시된 바와 같이 계정 응용프로그램(113)은 동작을 수행하기 위한 요청을 수신할 수 있다. 예를 들어 요청은 한 계정에서 다른 계정으로 자금을 이체하는

것일 수 있다. 계정 응용프로그램(113)은 요청된 자금 이체를 승인하기 위해 어떤 유형의 데이터가 필요한지를 결정하기 위해 규칙(115)을 참조할 수 있다.

[0060] 예를 들어 규칙(115)은 암호화된 고객 ID의 검증 및 여권 데이터(108)에 기반한 검증을 자금 이체가 요구하도록 명시할 수 있다. 적어도 하나의 실시형태에서 규칙(115)에 의해 명시된 데이터의 유형은 자금 이체와 같은 요청된 동작의 유형에 기반한다. 일반적으로 규칙(115)은 상이한 유형의 거래에 대해 상이한 수준의 보안을 명시할 수 있다. 예를 들어 더 높은 위험 동작에 대해 여권 데이터(108)의 검증을 요구하지만 더 낮은 위험 동작에 대해서는 여권 데이터(108)의 검증을 요구하지 않는다.

[0061] 이에 응답하여 계정 응용프로그램(113)은 디바이스(110)에 비접촉식 카드(101)를 탭 하라는 표시를 출력할 수 있다. 사용자가 모바일 디바이스(110)에 대해 비접촉식 카드(101)를 탭 하면 비접촉식 카드(101)의 애플릿(103)은 예를 들어 암호화된 고객 ID(132 및/또는 201)를 생성하기 위해 고객 ID(107)를 암호화한다. 그 후 애플릿(103)은 예를 들어 NFC를 통해 모바일 디바이스(110)에 암호화된 고객 ID(107) 및 암호화된 여권 데이터(108)를 전송할 수 있다.

[0062] 도 3b의 개략도(310)에 도시된 바와 같이 계정 응용프로그램(113)은 사용자가 카메라(119)를 사용하여 물리적 여권의 하나 이상의 페이지의 사진을 찍도록 명시하는 표시를 출력할 수 있다. 그 후 사용자는 여권의 이미지를 캡처할 수 있다. 그 후 계정 응용프로그램(113)은 캡처된 이미지를 처리하여 여권 번호, 발행 일자 및 만료 일자 와 같은 여권의 하나 이상의 속성을 추출할 수 있다.

[0063] 언급된 바와 같이 일부 실시형태에서 계정 응용프로그램(113)은 이미지로부터 추출된 속성을 사용하여 암호화된 여권 데이터(108)를 복호화 할 수 있다. 도 3a 내지 도 3b의 실시형태와 같은 다른 실시형태에서 인증 응용프로그램(123)은 계정 응용프로그램(113)에 의해 추출된 속성을 사용하여 암호화된 여권 데이터(108)를 복호화 할 수 있다. 따라서 계정 응용프로그램(113)은 암호화된 고객 ID(107), 암호화된 여권 데이터(108) 및 여권의 추출된 속성을 인증 응용프로그램(123)에 제공한다.

[0064] 그 후 인증 응용프로그램(123)은 마스터 키(105) 및/또는 비접촉식 카드(101)와 연관된 다양화 키(106)를 사용하여 암호화된 고객 ID(107) 및/또는 암호화된 여권 데이터(108)를 복호화 하려고 시도할 수 있다. 인증 응용프로그램(123)이 예상된 결과 예를 들어 계정의 고객 ID(107)를 생성하기 위해 암호화된 고객 ID(107)를 복호화할 수 없는 경우, 인증 응용프로그램(123)은 암호화된 고객 ID(107)를 검증하지 않는다. 인증 응용프로그램(123)이 예상된 결과 예를 들어 계정의 고객 ID(107)를 생성하기 위해 암호화된 고객 ID(107)를 성공적으로 복호화 한 경우, 인증 응용프로그램(123)은 암호화된 고객 ID(107)를 검증하고 계정 응용프로그램(113)으로부터 수신된 속성을 사용하여 여권 데이터(108)의 복호화를 시도한다.

[0065] 인증 응용프로그램(123)이 여권 데이터(108)를 성공적으로 복호화 하면 계정 응용프로그램(123)은 암호화된 고객 ID(107) 및 암호화된 여권 데이터(108)의 검증 표시를 계정 응용프로그램(113)에 전송한다. 그 후 계정 응용프로그램(113)은 검증 수신에 응답하여 요청된 동작의 수행을 허용한다.

[0066] 그러나 인증 응용프로그램(123)이 암호화된 고객 ID(107) 및/또는 암호화된 여권 데이터(108)를 복호화 할 수 없는 경우, 인증 응용프로그램(123)은 실패한 암호 복호화의 표시를 계정 응용프로그램(113)에 전송한다. 그 후 계정 응용프로그램(113) 예를 들어 도 3b에 표시된 "다음" 버튼을 비활성화하여 요청된 동작의 성능을 제한할 수 있다.

[0067] 언급된 바와 같이, 일부 실시형태에서 규칙(115)은 연관된 동작을 수행하는 데 필요한 권한 수준을 명시한다. 예를 들어 계정 세부사항을 업데이트하기 위해 규칙(115)은 0.0-10.0의 척도에서 2.0 이상의 권한 수준을 요구할 수 있다. 따라서 이러한 실시형태에서 계정 응용프로그램(113)은 사용자의 현재 권한 수준을 인증 응용프로그램(123)으로 전송할 수 있다. 현재 허용 수준은 계정 응용프로그램(113)에 의해 국소적으로 저장될 수 있으며 예를 들어 계정 데이터(124)가 모바일 디바이스(110)의 메모리(111) 내에 저장되는 경우 및/또는 인증 응용프로그램(123)으로부터 수신될 수 있다. 예를 들어 사용자가 인증 자격증명을 사용하여 계정 응용프로그램(113)에 로그인 할 때이다.

[0068] 이러한 실시예에서 사용자의 현재 권한 수준은 1.5일 수 있다. 따라서 계정 응용프로그램(113)은 사용자의 현재 권한 수준이 필요한 권한 수준을 충족하지 않는다는 것을 명시하는 표시를 인증 응용프로그램(123)에 전송할 수 있다. 그 후 인증 응용프로그램(123)은 사용자의 권한 수준을 증가시킬지 여부를 결정할 수 있다. 예를 들어 인증 응용프로그램(123)이 암호화된 고객 ID(107) 및 암호화된 여권 데이터(108)를 성공적으로 복호화 하는 것에 기반하여 인증 응용프로그램(123)은 사용자의 권한 수준을 3.0으로 증가시킬 수 있다.

- [0069] 인증 응용프로그램(123)은 새로운 권한 수준의 표시를 계정 응용프로그램(113)으로 검증과 함께 전송할 수 있다. 그 후 계정 응용프로그램(113)은 인증 서버(123)로부터 검증을 수신하는 것에 응답하여 및 규칙(115) 내에 명시된 권한 수준을 초과하는 업데이트된 권한 수준에 기반하여 요청된 동작의 수행을 허용할 수 있다.
- [0070] 도 4a는 신용 카드, 직불 카드 및/또는 기프트 카드와 같은 결제 카드를 포함할 수 있는 비접촉식 카드(101)를 도시한다. 도시된 바와 같이 비접촉식 카드(101)는 카드(101)의 전면 또는 후면에 표시된 서비스 공급자(405)에 의해 발행될 수 있다. 일부 실시예에서 비접촉식 카드(101)는 결제 카드와 관련되지 않으며 신분증을 제한없이 포함한다. 일부 실시예에서 결제 카드는 이중 인터페이스 비접촉식 결제 카드를 포함할 수 있다.
- [0071] 비접촉식 카드(101)는 플라스틱, 금속 및 기타 재료로 구성된 단일 층 또는 하나 이상의 적층된 층을 포함할 수 있는 기판(410)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.
- [0072] 일부 실시예에서 비접촉식 카드(101)는 ISO/IEC 7810 표준의 ID-1 형식을 준수하는 물리적 특성을 지닐 수 있고, 그렇지 않으면 비접촉식 카드는 ISO/IEC 14443 표준을 준수할 수 있다. 그러나, 본 발명에 따른 비접촉식 카드(101)는 상이한 특성을 지닐 수 있으며 본 발명은 비접촉식 카드가 결제 카드에서 구현될 필요가 없다는 것으로 이해된다.
- [0073] 또한 비접촉식 카드(101)는 카드의 전면 및/또는 후면에 표시된 식별 정보(415) 및 접촉 패드(420)를 포함할 수 있다. 접촉 패드(420)는 모바일 디바이스(40), 사용자 디바이스, 스마트폰, 랩톱, 데스크톱 또는 태블릿 컴퓨터. 비접촉식 카드(101)는 또한 처리 회로, 안테나 및 도 4a에 도시되지 않은 다른 컴포넌트를 포함할 수 있다. 이들 컴포넌트는 접촉 패드(420) 후면에 또는 기판(410) 상의 다른 곳에 위치될 수 있다. 또한 비접촉식 카드(101)는 카드의 후면에 위치될 수 있는 자기 스트립 또는 테이프를 포함할 수 있다(도 4a에 도시되지 않음).
- [0074] 도 4b에 도시된 바와 같이 비접촉식 카드(101)의 접촉 패드(420)는 마이크로프로세서(430) 및 메모리(102)를 포함하여 정보를 저장 및 처리하기 위한 처리 회로(425)를 포함할 수 있다. 처리 회로(425)는 본 발명에 개시된 기능을 수행하기 위해 필요한 프로세서, 메모리, 오류 및 패리티/CRC 검사기, 데이터 인코더, 충돌 방지 알고리즘, 컨트롤러, 명령 디코더, 보안 프리미티브 및 변조 방지 하드웨어를 포함하는 추가 컴포넌트를 포함할 수 있다.
- [0075] 메모리(102)는 읽기 전용 메모리, 1회 쓰기 다회 읽기 메모리 또는 읽기/쓰기 메모리 예를 들어 RAM, ROM 및 EEPROM일 수 있으며 비접촉식 카드(101)는 이들 메모리 중 하나 이상을 포함할 수 있다. 읽기 전용 메모리는 공장에서 읽기 전용 또는 1회성 프로그래밍 가능으로 프로그래밍 될 수 있다. 일회성 프로그래밍 기능은 한 번 쓰고 여러 번 읽을 수 있는 기회를 제공한다. 1회 쓰기 다회 읽기 메모리는 메모리 칩이 공장에서 출고된 후 특정 시점에 프로그래밍 될 수 있다. 메모리는 한 번 프로그래밍 되면 다시 쓸 수 없지만 여러 번 읽을 수 있다. 읽기/쓰기 메모리는 출고 후 여러 번 프로그래밍 및 재프로그래밍 될 수 있다. 읽기/쓰기 메모리는 출고 후 여러 번 읽을 수도 있다.
- [0076] 메모리(102)는 하나 이상의 애플릿(103), 카운터(104), 마스터 키(105), 다양화 키(106), 하나 이상의 고객(또는 사용자) ID(107) 및 여권 데이터(108)를 저장하도록 형상화 될 수 있다. 하나 이상의 애플릿(103)은 Java® 카드 애플릿과 같이 하나 이상의 비접촉식 카드 상에서 실행하도록 형상화 된 하나 이상의 소프트웨어 응용프로그램을 포함할 수 있다. 그러나 애플릿(103)은 자바 카드 애플릿으로 제한되지 않으며 비접촉식 카드 또는 제한된 메모리를 지니는 다른 디바이스에서 작동 가능한 임의의 소프트웨어 응용프로그램일 수 있는 것으로 이해된다.
- [0077] 고객 ID(107)는 비접촉식 카드(101)의 사용자에게 할당된 고유한 영숫자 식별자를 포함할 수 있으며 식별자는 비접촉식 카드의 사용자를 다른 비접촉식 카드 사용자와 구별할 수 있다. 일부 실시예에서 고객 ID(107)는 고객 및 그 고객에게 할당된 계정 모두를 식별할 수 있으며 고객의 계정과 연관된 비접촉식 카드를 추가로 식별할 수 있다.
- [0078] 일부 실시예에서 애플릿(103)은 고객 ID(107)를 암호화하기 위해 키(105 및/또는 106)를 지니는 암호화 알고리즘에 대한 입력으로 고객 ID(107)를 사용할 수 있다. 유사하게 애플릿(103)은 여권 데이터를 암호화하기 위해 키(105 및/또는 106)를 지니는 암호화 알고리즘에 대한 입력으로 여권(108)의 하나 이상의 속성에 기반하여 암호화 및/또는 암호화되지 않을 수 있는 여권 데이터(108)를 사용할 수 있다.

- [0079] 기술한 실시형태의 프로세서 및 메모리 요소는 접촉 패드를 참조하여 설명되었으나 본 발명은 이에 제한되지 않는다. 이들 요소는 패드(420) 외부에 구현되거나 패드로부터 완전히 분리될 수 있거나 접촉 패드(420) 내에 위치한 프로세서(430) 및 메모리(102) 요소에 더하여 추가 요소로서 구현될 수 있는 것으로 이해된다.
- [0080] 일부 실시예에서 비접촉식 카드(101)는 하나 이상의 안테나(455)를 포함할 수 있다. 하나 이상의 안테나(455)는 비접촉식 카드(101) 내에 및 접촉 패드(420)의 처리 회로(425) 주위에 배치될 수 있다. 예를 들어 하나 이상의 안테나(455)는 처리 회로(425)와 통합될 수 있으며 하나 이상의 안테나(455)는 외부 부스터 코일과 함께 사용될 수 있다. 다른 예로서 하나 이상의 안테나(455)는 접촉 패드(420) 및 처리 회로(425)의 외부에 있을 수 있다.
- [0081] 하나의 실시형태에서 비접촉식 카드(101)의 코일은 공심 변압기의 2차로서 작용할 수 있다. 단말은 전력 또는 진폭 변조를 차단함으로써 비접촉식 카드(101)와 통신할 수 있다. 비접촉식 카드(101)는 하나 이상의 커패시터를 통해 기능적으로 유지될 수 있는 비접촉식 카드의 전원 연결의 갭을 사용하여 단말기에서 전송된 데이터를 추론할 수 있다. 비접촉식 카드(101)는 비접촉식 카드의 코일 또는 부하 변조에 대한 부하를 전환함으로써 다시 통신할 수 있다. 부하 변조는 간섭을 통해 터미널 코일에서 감지될 수 있다. 보다 일반적으로 안테나(455), 처리 회로(425) 및/또는 메모리(102)를 사용하여, 비접촉식 카드(101)는 NFC, 블루투스 및/또는 Wi-Fi 통신을 통해 통신하기 위한 통신 인터페이스를 제공한다.
- [0082] 상기 설명된 바와 같이 비접촉식 카드(101)는 스마트 카드 또는 JavaCard와 같은 제한된 메모리를 지니는 다른 디바이스에서 작동 가능한 소프트웨어 플랫폼에 구축될 수 있으며 하나 이상의 응용프로그램 또는 애플릿이 안전하게 실행될 수 있다. 애플릿은 다양한 모바일 응용프로그램 기반 사용 사례에서 다중요인 인증(MFA)을 위한 일회용 암호(OTP)를 제공하기 위해 비접촉식 카드에 추가될 수 있다. 애플릿은 모바일 NFC 판독기(예를 들어 디바이스(110)의 통신 인터페이스(118))와 같은 판독기로부터의 근거리장 데이터 교환 요청과 같은 하나 이상의 요청에 응답하고 NDEF 텍스트 태그로 인코딩된 암호화 보안 OTP를 포함하는 NDEF 메시지를 생성하도록 형성될 수 있다.
- [0083] 개시된 실시형태에 대한 동작은 도면을 참조하여 더욱 설명될 수 있다. 일부 도면에는 논리 흐름이 포함될 수 있다. 본 발명에 개시된 그러한 도면은 특정 논리 흐름을 포함할 수 있으나 논리 흐름은 단지 본 발명에 개시된 바와 같은 일반적인 기능이 구현될 수 있는 방법의 하나의 예를 제공한다는 것으로 이해된다. 또한 달리 표시되지 않는 한 주어진 논리 흐름이 반드시 제시된 순서대로 실행될 필요는 없다. 또한 주어진 논리 흐름은 하드웨어 요소, 프로세서에 의해 실행되는 소프트웨어 요소 또는 이들의 임의의 조합에 의해 구현될 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다.
- [0084] 도 5는 논리 흐름(500)의 실시형태를 도시한다. 논리 흐름(500)은 본 발명에 개시된 하나 이상의 실시형태에 의해 실행되는 동작의 일부 또는 전부를 나타낼 수 있다. 예를 들어 논리 흐름(500)은 비접촉식 카드(101)에 저장된 여권 데이터에 기반하여 보안 인증을 제공하기 위해 비접촉식 카드(101)를 사용하는 동작의 일부 또는 전부를 포함할 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다.
- [0085] 도시된 바와 같이 논리 흐름(500)은 계정 응용프로그램(113)이 동작을 수행하기 위한 요청을 수신하는 블록 505에서 시작한다. 언급된 바와 같이 요청된 동작은 계정 응용프로그램(113)의 사용자, 외부 소스(예를 들어 다른 응용프로그램(114) 중 하나) 또는 임의의 다른 소스로부터의 입력에 기반하여 수신될 수 있다. 요청은 예를 들어 그리고 비제한적으로 계정 응용프로그램(113)의 사용, 다른 응용프로그램(114)의 사용, 비접촉식 카드(101)와 연관된 계정과 관련된 동작 및/또는 트랜잭션과 관련될 수 있다.
- [0086] 보다 일반적으로 요청은 계정 응용프로그램(113)에서 계정에 액세스하는 데 필요한 인증 자격증명을 사용자가 제공한 후에 수신될 수 있다. 블록 510에서 사용자는 모바일 디바이스(110)에 비접촉식 카드(101)를 탭 하여 비접촉식 카드(101)의 애플릿(103)이 고객 ID(107)를 암호화 하고 암호화된 고객 ID를 모바일 디바이스(110)로 전송하게 한다.
- [0087] 블록 515에서 계정 응용프로그램(113)은 비접촉식 카드(101)로부터 암호화된 고객 ID를 수신할 수 있다. 그 후 계정 응용프로그램(113)은 비접촉식 카드(101)로부터 수신된 암호화된 고객 ID를 인증 서버(120)에 전송할 수 있다. 서버(120)는 본 발명에 개시된 바와 같이 암호화된 고객 ID의 복호화를 시도할 수 있다. 블록 520에서 계정 응용프로그램(113)은 암호화된 고객 ID(132)를 복호화 함으로써 암호화된 고객 ID가 검증되었다는 표시를 서버(120)로부터 수신한다.
- [0088] 블록 525에서 계정 응용프로그램(113)은 요청의 유형을 결정하고 이는 동작의 유형을 승인하는 데 필요한 규칙

(115)에 명시된 검증 데이터 유형을 결정하는 데 사용될 수 있다. 예를 들어 여권 데이터(108)는 규칙(115)에 의해 요구되는 검증 데이터로서 명시될 수 있다. 블록 530)에서 사용자는 비접촉식 카드(101)를 모바일 디바이스(110)에 탭 한다. 이를 통해 비접촉식 카드(101)의 애플릿(103)이 여권 데이터(108)를 모바일 디바이스(110)로 전송하게 한다. 그 후 계정 응용프로그램(110)은 비접촉식 카드(101)로부터 여권 데이터(108)를 수신할 수 있다. 그러나 언급된 바와 같이 일부 실시형태에서 여권 데이터(108)는 블록 510에서 탭에 응답하여 블록 515에서 수신될 수 있다.

[0089] 블록 535에서 계정 응용프로그램(113)은 여권 속성을 수신할 수 있다. 예를 들어 사용자는 계정 응용프로그램(113)에 대한 입력으로 여권 속성을 제공할 수 있다. 다른 실시예로서 계정 응용프로그램(113)은 여권 속성을 포함하는 여권 페이지의 이미지를 캡처하도록 사용자에게 지시할 수 있다. 그 후 계정 응용프로그램(113)은 예를 들어 캡처된 이미지에서 각각의 여권 속성과 연관된 값을 식별함으로써 캡처된 이미지로부터 속성을 추출할 수 있다. 블록 540에서 계정 응용프로그램(113)은 블록 535에서 수신된 속성을 사용하여 여권 데이터(108)를 성공적으로 복호화 할 수 있다.

[0090] 그러나 언급된 바와 같이 일부 실시형태에서 계정 응용프로그램(113)은 암호 복호화를 위해 여권 데이터(108) 및 추출된 속성을 인증 응용프로그램(123)에 전송한다. 이러한 실시형태에서 계정 응용프로그램(113)은 비접촉식 카드(101)에 의해 생성된 암호화된 고객 ID와 함께 여권 데이터(108) 및 추출된 속성을 전송할 수 있다. 그 후 인증 응용프로그램(123)은 고객 ID 및 여권 데이터(108)의 암호 복호화를 시도하고 복호화 시도가 성공했는지 실패했는지 여부를 계정 응용프로그램(113)에 통보 할 수 있다.

[0091] 블록 545에서 계정 응용프로그램(113)은 서버(120)에 의한 암호화된 고객 ID의 검증 및 암호화된 여권 데이터(108)의 복호화에 기반하여 요청된 동작의 수행을 허용한다. 블록 550에서 예를 들어 사용자 및/또는 계정 응용프로그램(113)에 의해 요청된 동작이 수행될 수 있다.

[0092] 도 6은 논리 흐름(600)의 실시형태를 도시한다. 논리 흐름(600)은 여기에 설명된 하나 이상의 실시형태에 의해 실행되는 동작의 일부 또는 전부를 나타낼 수 있다. 예를 들어 논리 흐름(600)은 비접촉식 카드(101)에 저장된 여권 데이터(108)를 복호화 하기 위해 여권 속성을 수신하기 위한 동작의 일부 또는 전부를 포함할 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다.

[0093] 도시된 바와 같이 논리 흐름(600)은 계정 응용프로그램(113)이 여권 속성을 명시하는 사용자로부터 텍스트-기반 입력을 선택적으로 수신하는 블록 610에서 시작한다. 명시된 바와 같이 여권 속성에는 여권 번호, 여권 발급 날짜 및 여권 유효기한이 포함될 수 있다. 그러나 해당 인물의 이름 또는 기타 정보와 같은 다른 데이터가 여권 데이터(108)의 암호화/복호화를 위해 사용될 수 있다. 보다 일반적으로 계정 응용프로그램(113)은 필요한 속성 및/또는 속성 유형을 알고 있을 수 있다. 블록 620에서 계정 응용프로그램(113)은 여권 데이터(108)에 상응하는 물리적 여권의 페이지를 묘사하는 이미지를 캡처하라는 명령을 사용자에게 출력한다. 블록 630에서 계정 응용프로그램(113)은 모바일 디바이스(110)의 카메라(119)에 의해 캡처된 이미지를 수신한다.

[0094] 블록 640에서 계정 응용프로그램(113)은 캡처된 이미지로부터 속성을 추출한다. 예를 들어 계정 응용프로그램(113)은 속성을 추출하기 위해 하나 이상의 이미지 처리 알고리즘을 적용할 수 있다. 일반적으로 계정 응용프로그램(113)은 필수 여권 속성을 식별하도록 프로그래밍 되어 이미지를 처리하여 필수 속성을 식별하고 각 속성과 연관된 값을 추출할 수 있다. 예를 들어 이미지에서 텍스트를 인식함으로써 계정 응용프로그램(113)은 이미지의 텍스트 내에서 "여권 번호" 또는 그 일부 변형을 식별할 수 있다.

[0095] 그 후 계정 응용프로그램(113)은 식별된 문구와 연관된 값 예를 들어 숫자 및/또는 영숫자 값을 추출할 수 있다. 예를 들어 계정 응용프로그램(113)은 여권의 레이아웃을 설명하는 정보로 프로그래밍 될 수 있다. 따라서 계정 응용프로그램(113)은 이미지 내에서 관련 속성 이름을 추출할 위치 및 이미지 내에서 관련 값을 추출할 위치를 결정할 수 있다.

[0096] 도 7은 논리 흐름(700)의 실시형태를 도시한다. 논리 흐름(700)은 본 발명에 개시된 하나 이상의 실시형태에 의해 실행되는 동작의 일부 또는 전부를 나타낼 수 있다. 예를 들어 논리 흐름(700)은 비접촉식 카드(101)에 저장된 여권 데이터(108)를 사용하여 요청된 동작을 승인하는 동작의 일부 또는 전부를 포함할 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다.

[0097] 도시된 바와 같이 논리 흐름(700)은 계정 응용프로그램(113)이 계정과 연관된 인증 자격증명을 수신하는 블록 705에서 시작한다. 블록 710에서 계정 응용프로그램(113)은 계정 및/또는 계정과 연관된 사용자의 현재 권한 수준을 결정한다. 블록 720에서 계정 응용프로그램(113)은 규칙(115)이 사용자의 현재 권한 수준을 초과하는 권한

수준을 명시한다고 결정한다. 규칙(115)에 의해 명시된 권한 수준은 사용자에게 의해 수행되도록 요청된 동작 예를 들어 논리 흐름(500)의 블록 505에서 요청된 동작에 대한 것일 수 있다.

[0098] 블록 730에서 계정 응용프로그램(113)은 계정 응용프로그램(113)이 여권 데이터(108)를 복호화 하였음을 명시하는 표시를 인증 응용프로그램(123)에 예를 들어 논리 흐름(500)의 블록 540에서 전송한다. 블록 740에서 인증 응용프로그램(123)은 사용자의 권한 수준을 업데이트한다. 인증 응용프로그램(123)은 여권 데이터(108)가 복호화 되었음을 명시하는 표시 및 인증 응용프로그램(123)이 비접촉식 카드(101)에 의해 생성된 암호화된 데이터를 검증하였다고 결정하는 표시에 기반하여 권한 수준을 업데이트할 수 있다.

[0099] 예를 들어 인증 응용프로그램(123)은 논리 흐름(500)의 블록 520에서 암호화된 고객 ID(107)를 검증하는 것에 응답하여 타이머를 설정할 수 있다. 인증 응용프로그램(123)이 타이머가 시간 임계치를 초과하기 전에 블록 730에서 표시를 수신하면 인증 응용프로그램(123)은 권한 수준을 업데이트하고 업데이트된 권한 수준을 계정 응용프로그램(113)에 전송하기로 결정할 수 있다.

[0100] 블록 750에서 계정 응용프로그램(113)은 서버(120)로부터 업데이트된 권한 수준을 수신한다. 블록 760에서 계정 응용프로그램(113)은 블록 750에서 수신된 업데이트된 권한 수준이 규칙(115)에 의해 동작에 대해 명시된 권한 수준을 충족하거나 초과한다고 결정한다. 이에 응답하여 계정 응용프로그램(113)은 동작의 수행을 허용할 수 있다.

[0101] 도 8은 이전에 설명된 바와 같은 다양한 실시형태를 구현하기에 적합할 수 있는 컴퓨터 시스템(802)을 포함하는 예시적인 컴퓨터 아키텍처(800)의 실시형태를 도시한다. 다양한 실시형태에서 컴퓨터 아키텍처(800)는 전자 디바이스를 포함하거나 전자 디바이스의 일부로서 구현될 수 있다. 일부 실시형태에서 컴퓨터 아키텍처(800)는 예를 들어 시스템(100)의 하나 이상의 컴포넌트를 구현하는 시스템을 나타낼 수 있다.

[0102] 일부 실시형태에서 컴퓨터 시스템(802)은 예를 들어 시스템(100)의 비접촉식 카드(101), 모바일 디바이스(110) 및 인증 서버(120)를 대표할 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다. 보다 일반적으로 컴퓨터 아키텍처(800)는 도 1 내지 도 7을 참조하여 본 명세서에 설명된 모든 로직, 응용프로그램, 시스템, 방법, 디바이스 및 기능을 구현하도록 형상화 된다.

[0103] 본 발명에서 사용된 용어 "시스템", "컴포넌트" 및 "모듈"은 하드웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어 또는 실행 중인 소프트웨어인 컴퓨터 관련 엔티티를 의미한다. 예를 들어 컴포넌트는 컴퓨터 프로세서, 컴퓨터 프로세서, 하드 디스크 드라이브, 다중 저장 드라이브(광학 및/또는 자기 저장 매체), 객체, 실행 파일, 실행 스레드, 프로그램 및/또는 컴퓨터. 예를 들어 서버에서 실행되는 응용 프로그램과 서버 모두 컴포넌트가 될 수 있다.

[0104] 하나 이상의 컴포넌트는 프로세스 및/또는 실행 스레드 내에 상주할 수 있으며 컴포넌트는 하나의 컴퓨터에 국한되거나 두 개 이상의 컴퓨터에 분산될 수 있다. 또한 컴포넌트들은 동작을 협력하기 위해 다양한 유형의 통신 매체에 의해 서로 통신 가능하게 결합될 수 있다. 협력에는 정보의 단방향 또는 양방향 교환이 포함될 수 있다. 예를 들어 컴포넌트는 통신 매체를 통해 통신되는 신호의 형태로 정보를 전달할 수 있다. 정보는 다양한 신호 라인에 할당된 신호로 구현될 수 있다. 이러한 할당에서 각 메시지는 신호이다. 그러나 다른 실시형태는 대안적으로 데이터 메시지를 사용할 수 있다. 이러한 데이터 메시지는 다양한 연결을 통해 전송될 수 있다. 예시적인 연결은 병렬 인터페이스, 직렬 인터페이스 및 버스 인터페이스를 포함한다.

[0105] 컴퓨터 시스템(802)은 하나 이상의 프로세서, 멀티 코어 프로세서, 코프로세서, 메모리 유니트, 칩셋, 컨트롤러, 주변 디바이스, 인터페이스, 발전기, 타이밍 디바이스, 비디오 카드, 오디오 카드, 멀티미디어 입력/출력(I/O) 컴포넌트, 전원 공급 디바이스 등 과 같은 다양한 공통 컴퓨터 엘리먼트를 포함한다. 그러나, 실시형태는 컴퓨터 시스템(802)에 의한 구현으로 제한되지 않는다.

[0106] 도 8에 도시된 바와 같이, 컴퓨터 시스템(802)은 프로세서(804), 시스템 메모리(806) 및 시스템 버스(808)를 포함한다. 프로세서(804)는 AMD® Athlon®, Duron® 및 Opteron® 프로세서; ARM® 응용프로그램, 임베디드 및 보안 프로세서; IBM® 및 Motorola® DragonBall® 및 PowerPC® 프로세서; IBM 및 Sony® Cell 프로세서; Intel® Celeron®, Core®, Core (2) Duo®, Itanium®, Pentium®, Xeon® 및 XScale® 프로세서; 및 유사한 프로세서를 제한없이 포함하는 임의의 다양한 상업적으로 이용가능한 컴퓨터 프로세서일 수 있다. 듀얼 마이크로프로세서, 멀티 코어 프로세서 및 기타 멀티 프로세서 아키텍처가 프로세서(804)로 사용될 수도 있다.

[0107] 시스템 버스(808)는 프로세서(804)에 대한 시스템 메모리(806)를 포함하지만 이에 국한되지 않는 시스템 컴포넌트를 위한 인터페이스를 제공한다. 시스템 버스(808)는 임의의 다양한 상업적으로 이용 가능한 버스 아키텍처를

사용하여 메모리 버스(메모리 컨트롤러가 있거나 없는), 주변기기 버스 및 로컬 버스에 추가로 상호 연결될 수 있는 여러 유형의 버스 구조 중 임의의 것일 수 있다. 인터페이스 어댑터는 슬롯 아키텍처를 통해 시스템 버스(808)에 연결할 수 있다. 슬롯 아키텍처의 예에는 가속 그래픽 포트(AGP), 카드 버스, (확장) 산업 표준 아키텍처((E)ISA), 마이크로 채널 아키텍처(MCA), NuBus, 주변 디바이스 컴포넌트 상호 연결(확장)(PCI(X)), PCI Express, 개인용 컴퓨터 메모리 카드 국제 협회(PCMCIA)가 제한없이 포함될 수 있다.

[0108] 시스템 메모리(806)는 읽기 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 동적 RAM(DRAM), 더블 데이터-레이트(DDR) RAM, 동기식 DRAM(SDRAM), 정적 RAM(SRAM), 프로그램 가능 ROM(PROM), 지울 수 있는 프로그램 가능 ROM(EPROM), 전기적으로 지울 수 있는 프로그램 가능 ROM(EEPROM), 플래시 메모리(예를 들어 하나 이상의 플래시 어레이), 강유전성 폴리머 메모리, 오보닉 메모리, 상 변화 또는 강유전성 메모리와 같은 폴리머 메모리, 실리콘-옥사이드-니트라이드-옥사이드-실리콘(SONOS) 메모리, 자기 또는 광학 카드, 독수 배열 독립 디스크(RAID) 드라이브, 고체 상태 메모리 디바이스(예를 들어 USB 메모리, 고체 상태 드라이브(SSD) 및 정보 저장에 적합한 기타 유형의 저장 매체)와 같은 하나 이상의 고속 메모리 유닛의 형태로 다양한 유형의 컴퓨터 판독 가능 저장 매체를 포함할 수 있다.

[0109] 도 8에 도시된 예시된 실시형태에서 시스템 메모리(806)는 비휘발성 메모리(810) 및/또는 휘발성 메모리(812)를 포함할 수 있다. 기본 입/출력 시스템(BIOS)은 비휘발성 메모리(810) 내에 저장될 수 있다.

[0110] 컴퓨터 시스템(802)은 내부(또는 외부) 하드 디스크 드라이브(HDD)(814), 이동식 자기 디스크(818)로부터 읽거나 쓰기 위한 자기 플로피 디스크 드라이브(FDD)(816), 이동식 광 디스크(822)(예를 들어 CD-ROM 또는 DVD)로부터 읽거나 쓰기 위한 광 디스크 드라이브(820)를 포함하는 하나 이상의 저속 메모리 유닛의 형태로 다양한 유형의 컴퓨터 판독 가능 저장 매체를 포함할 수 있다. HDD(814), FDD(816) 및 광 디스크 드라이브(820)는 각각 HDD 인터페이스(824), FDD 인터페이스(826) 및 광 드라이브 인터페이스(828)에 의해 시스템 버스(808)에 연결될 수 있다.

[0111] 외부 드라이브 구현을 위한 HDD 인터페이스(824)는 범용 직렬 버스(USB) 및 IEEE 1394 인터페이스 기술 중 적어도 하나 또는 모두를 포함할 수 있다. 컴퓨터 시스템(802)은 일반적으로 도 1 내지 7을 참조하여 본 명세서에 설명된 모든 로직, 시스템, 방법, 디바이스 및 기능을 구현하도록 형상화 된다.

[0112] 드라이브 및 관련 컴퓨터 판독 가능 매체는 데이터, 데이터 구조, 컴퓨터 판독 가능 명령어, 컴퓨터 실행 가능 명령어 등의 휘발성 및/또는 비휘발성 저장 디바이스를 제공한다. 예를 들어 운영 체제(830), 하나 이상의 응용 프로그램 프로그램(832), 다른 프로그램 모듈(834) 및 프로그램 데이터(836)를 포함하는 다수의 프로그램 모듈이 드라이브 및 메모리 유닛(810, 812)에 저장될 수 있다.

[0113] 하나의 실시형태에서 하나 이상의 어플리케이션 프로그램(832), 다른 프로그램 모듈(834) 및 프로그램 데이터(836)는 예를 들어 시스템(100)의 다양한 응용프로그램 및/또는 컴포넌트, 예를 들어 애플릿(103), 카운터(104), 마스터 키(105), 다양화 키(106), 고객 ID(107), 여권 데이터(108), 암호화된 고객 ID(132), 운영 체제(112), 계정 응용프로그램(113), 다른 응용프로그램(114), 인증 응용프로그램(123), 계정 데이터(124), 암호화된 고객 ID(201) 및/또는 여권 속성(202)을 포함할 수 있다.

[0114] 사용자는 하나 이상의 유무선 입력 디바이스, 예를 들어 키보드(838) 및 마우스(840)와 같은 포인팅 디바이스를 통해 명령어 및 정보를 컴퓨터 시스템(802)에 입력할 수 있다. 다른 입력 디바이스는 마이크, 적외선(IR) 리모콘, 무선 주파수(RF) 리모콘, 게임 패드, 스타일러스 펜, 카드 판독기, 동글, 지문 판독기, 장갑, 그래픽 태블릿, 조이스틱, 키보드, 망막 판독기, 터치 스크린(예를 들어 정전식, 감압식 등), 트랙볼, 트랙패드, 센서, 스타일러스 등을 포함할 수 있다.

[0115] 이들 및 다른 입력 디바이스는 종종 시스템 버스(808)에 연결된 입력 디바이스 인터페이스(842)를 통해 프로세서(804)에 연결되지만 병렬 포트, IEEE 1394 직렬 포트, 게임 포트, USB 포트, IR 인터페이스 등과 같은 다른 인터페이스에 의해 연결될 수도 있다.

[0116] 모니터(844) 또는 다른 유형의 디스플레이 디바이스 또한 비디오 어댑터(846)와 같은 인터페이스를 통해 시스템 버스(808)에 연결된다. 모니터(844)는 컴퓨터 시스템(802)의 내부 또는 외부에 있을 수 있다. 모니터(844) 외에 컴퓨터에는 일반적으로 스피커, 프린터 등과 같은 기타 주변 출력 디바이스가 포함된다.

[0117] 컴퓨터 시스템(802)은 원격 컴퓨터(848)와 같은 하나 이상의 원격 컴퓨터에 대한 유선 및/또는 무선 통신을 통한 논리적 연결을 사용하여 네트워크 환경에서 동작할 수 있다. 원격 컴퓨터(848)는 워크스테이션, 서버 컴퓨터, 라우터, 개인용 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서 기반 엔터테인먼트 기기, 피어 디바이스 또

는 기타 공통 네트워크 노드를 포함하며 일반적으로 컴퓨터 시스템(802)과 관련하여 설명된 많은 또는 모든 요소를 포함하지만 간결함을 위해 메모리/저장 디바이스(850)가 도시되어 있다.

- [0118] 도시된 논리적 연결은 근거리 네트워크(LAN)(852) 및/또는 광역 네트워크(WAN)(854)와 같은 더 큰 네트워크에 대한 유무선 연결을 포함한다. 이러한 LAN 및 WAN 네트워크 환경은 사무실과 회사에서 흔히 볼 수 있으며 인터넷과 같은 글로벌 통신 네트워크에 연결할 수 있는 인트라넷과 같은 전기업적 컴퓨터 네트워크를 용이하게 한다. 실시형태에서 도 1의 네트워크(130)는 LAN(852) 및 WAN(854) 중 하나 이상이다.
- [0119] LAN 네트워크 환경에서 사용될 때, 컴퓨터 시스템(802)은 유선 및/또는 무선 통신 네트워크 인터페이스 또는 어댑터(856)를 통해 LAN(852)에 연결된다. 어댑터(856)는 LAN(852)으로의 유선 및/또는 무선 통신을 용이하게 할 수 있으며 이는 또한 어댑터(856)의 무선 기능과 통신하기 위해 그 위에 배치된 무선 액세스 포인트를 포함한다.
- [0120] WAN 네트워크 환경에서 사용될 때, 컴퓨터 시스템(802)은 모뎀(858)을 포함할 수 있거나, WAN(854) 상의 통신 서버에 연결되거나 인터넷과 같이 WAN(854)을 통한 통신을 설정하기 위한 다른 수단을 지닐 수 있다. 내부 또는 외부 및 유선 및/또는 무선 디바이스일 수 있는 모뎀(858)은 입력 디바이스 인터페이스(842)를 통해 시스템 버스(808)에 연결된다. 네트워크 환경에서 컴퓨터 시스템(802) 또는 그 일부와 관련하여 도시된 프로그램 모듈은 원격 메모리/저장 디바이스(850) 내에 저장될 수 있다. 도시된 네트워크 연결은 예시적이며 컴퓨터 사이의 통신 링크를 설정하는 다른 수단이 사용될 수 있는 것으로 이해된다.
- [0121] 컴퓨터 시스템(802)은 무선 통신(예를 들어 IEEE 802.16 무선 변조 기술)에서 동작 가능하게 배치된 무선 디바이스와 같은 IEEE 802 표준 패밀리를 사용하여 유선 및 무선 디바이스 또는 엔티티와 통신하도록 작동 가능하다. 여기에는 최소한 Wi-Fi(또는 Wireless Fidelity), WiMax 및 Bluetooth™ 무선 기술 등이 포함된다. 따라서, 통신은 기존 네트워크에서와 같이 미리 정의된 구조이거나 단순히 두 개 이상의 디바이스 간의 임시 통신일 수 있다. Wi-Fi 네트워크는 IEEE 802.11x(a, b, g, n 등)라는 무선 기술을 사용하여 안전하고 안정적이며 빠른 무선 연결을 제공한다. Wi-Fi 네트워크는 컴퓨터를 상호 간에 연결하고 인터넷에 연결하고 IEEE 802.3 관련 미디어 및 기능을 사용하는 유선 네트워크에 연결하는 데 사용할 수 있다.
- [0122] 다양한 실시형태는 하드웨어 엘리먼트, 소프트웨어 엘리먼트, 또는 양자의 조합을 사용하여 구현될 수 있다. 하드웨어 엘리먼트의 예에는 프로세서, 마이크로프로세서, 회로, 회로 엘리먼트 (예를 들어 트랜지스터, 레지스터, 커패시터, 인덕터 등), 집적 회로, 주문형 집적 회로(ASIC), 프로그래밍 가능한 논리 디바이스(PLD), 디지털 신호 프로세서(DSP), 필드 프로그램 가능 게이트 어레이(FPGA), 논리 게이트, 레지스터, 반도체 디바이스, 칩, 마이크로칩, 칩셋 등이 포함될 수 있다.
- [0123] 소프트웨어의 예에는 소프트웨어 컴포넌트, 프로그램, 응용 프로그램, 컴퓨터 프로그램, 어플리케이션 프로그램, 시스템 프로그램, 기계 프로그램, 운영 체제 소프트웨어, 미들웨어, 펌웨어, 소프트웨어 모듈, 루틴, 서브루틴, 기능, 방법, 절차, 소프트웨어 인터페이스, 어플리케이션 프로그램 인터페이스(API), 명령어 세트, 컴퓨팅 코드, 컴퓨터 코드, 코드 세그먼트, 컴퓨터 코드 세그먼트, 단어, 값, 기호 또는 이들의 조합이 포함될 수 있다. 실시형태가 하드웨어 요소 및/또는 소프트웨어 엘리먼트를 사용하여 구현되는지 여부를 결정하는 것은 원하는 연산 속도, 전력 수준, 열 허용 오차, 처리 주기 예산, 입력 데이터 속도, 출력 데이터 속도, 메모리 리소스, 데이터 버스 속도 및 기타 설계 또는 성능 제약과 같은 임의의 수의 요인에 따라 달라질 수 있다.
- [0124] 적어도 하나의 실시형태의 하나 이상의 측면은 프로세서 내의 다양한 로직을 나타내는 머신 판독가능 매체에 저장된 대표적인 명령어에 의해 구현될 수 있으며 이는 머신에 의해 판독될 때 머신이 본 명세서에 설명된 기술을 수행하게 하는 로직을 제조하게 한다. "IP 코어"로 알려진 그러한 표현은 유형의 기계 판독 가능 매체에 저장될 수 있으며 로직 또는 프로세서를 만드는 제조 기계에 로드하기 위해 다양한 고객 또는 제조 시설에 제공될 수 있다.
- [0125] 일부 실시형태는 예를 들어 기계에 의해 실행되는 경우 기계가 실시형태에 따른 방법 및/또는 동작을 수행하게 할 수 있는 명령어 또는 명령어 세트를 저장할 수 있는 기계 판독가능 매체 또는 물품을 사용하여 구현될 수 있다. 그러한 기계는 예를 들어 임의의 적절한 처리 플랫폼, 컴퓨터 플랫폼, 컴퓨터 디바이스, 처리 디바이스, 컴퓨터 시스템, 처리 시스템, 컴퓨터, 프로세서 등을 포함할 수 있으며 하드웨어 및/또는 소프트웨어의 임의의 적절한 조합을 사용하여 구현될 수 있다.
- [0126] 기계 판독가능 매체 또는 물품은 예를 들어 임의의 적합한 유형의 메모리 유니트, 메모리 디바이스, 메모리 물품, 메모리 매체, 저장 디바이스, 저장 물품, 저장 매체 및/또는 저장 유니트, 예를 들어 메모리, 이동식 또는

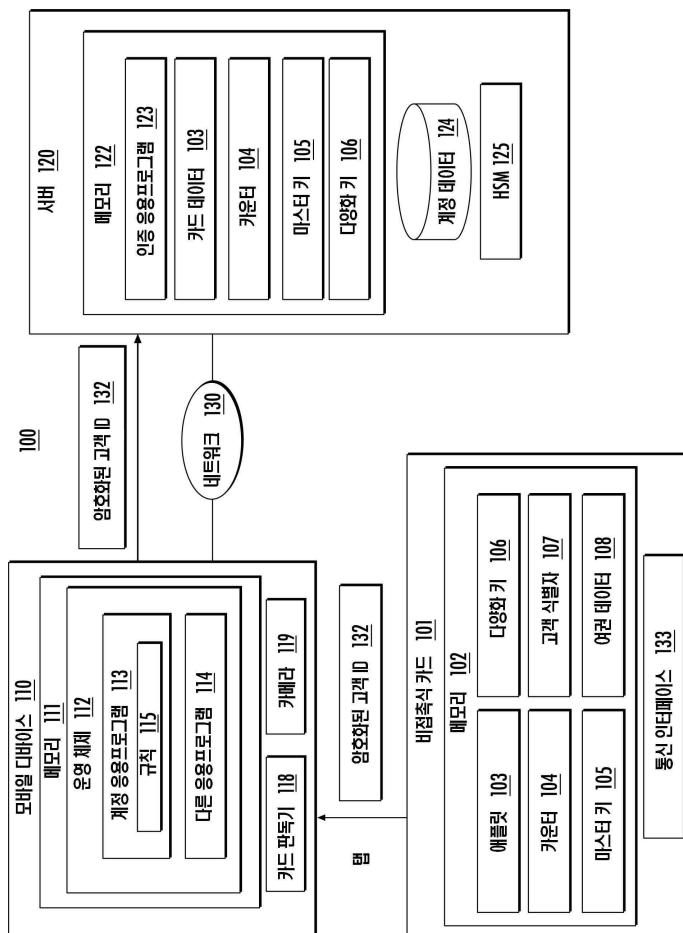
비이동식 매체, 지울 수 있거나 지울 수 없는 매체, 쓰기 가능 또는 다시 쓰기 가능 매체, 디지털 또는 아날로그 매체, 하드 디스크, 플로피 디스크, 콤팩트 디스크 읽기 전용 메모리(CD-ROM), 기록 가능 콤팩트 디스크(CD-R), 재기록 가능 콤팩트 디스크CD-RW(Compact Disk Rewriteable), 광 디스크, 자기 매체, 광자기 매체, 이동식 메모리 카드 또는 디스크, 다양한 유형의 지지털 다목적 디스크(DVD), 테이프, 카세트 등을 포함할 수 있다.

[0127] 명령어는 소스 코드, 컴파일된 코드, 해석된 코드, 실행 가능한 코드, 정적 코드, 동적 코드, 암호화된 코드 등과 같은 임의의 적절한 유형의 코드를 포함할 수 있으며, 적절한 상위 수준, 하위 수준, 개체-지향, 시각적, 컴파일된 및/또는 해석된 프로그래밍 언어를 사용하여 구현된다.

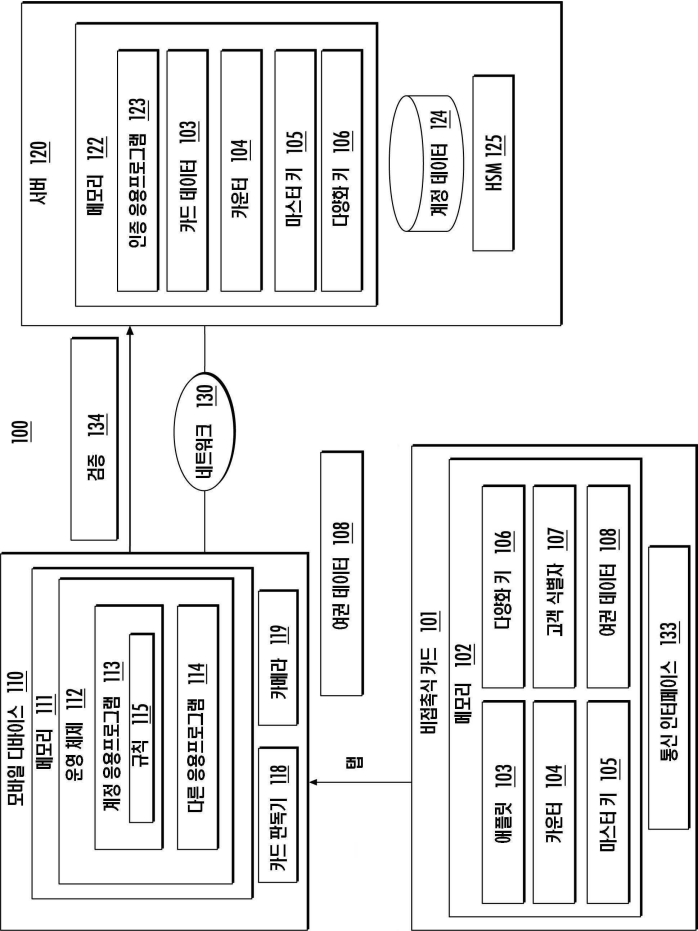
[0128] 예시적인 실시형태의 기술한 설명은 예시 및 설명의 목적으로 제시되었다. 이는 본 발명을 개시된 정확한 형태로 철저하게 제한하거나 제한하려는 의도가 아니다. 본 발명에 비추어 많은 수정 및 변형이 가능하다. 본 발명의 범위는 이러한 상세한 설명이 아니라 여기에 첨부된 청구범위에 의해 제한되는 것으로 의도된다. 본 발명에 대한 우선권을 주장하는 미래의 특허 출원은 개시된 주제를 다른 방식으로 청구할 수 있으며 일반적으로 여기에 서 다양하게 개시되거나 달리 입증된 바와 같이 하나 이상의 제한의 임의의 세트를 포함할 수 있다.

도면

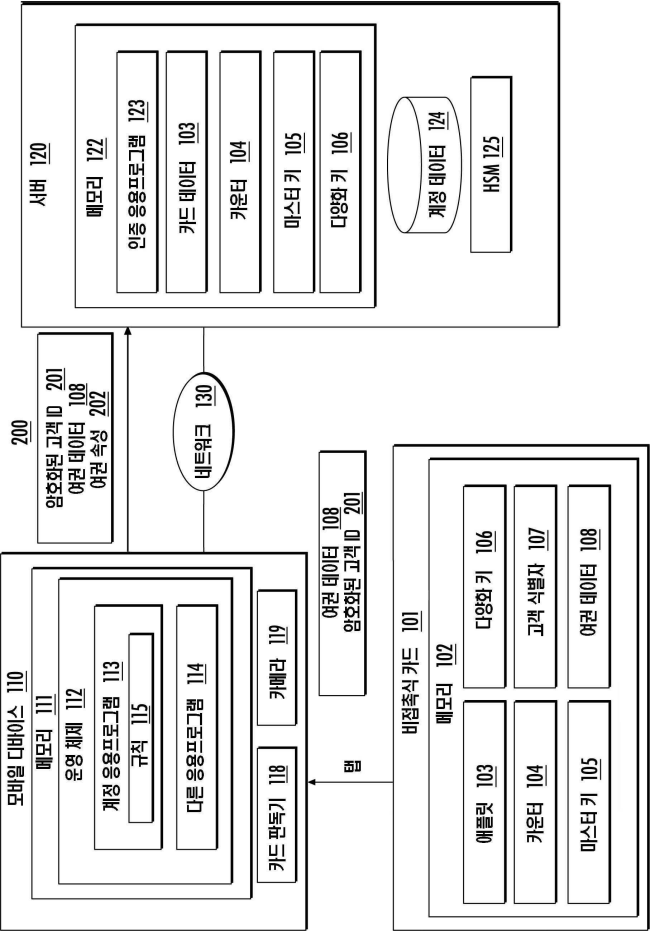
도면1a



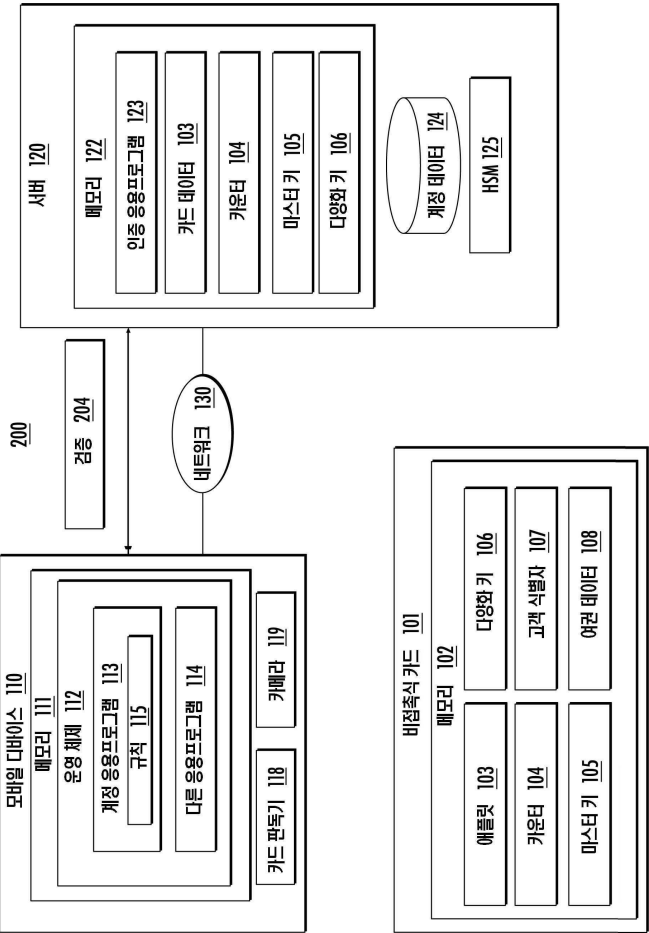
도면1b



도면2a



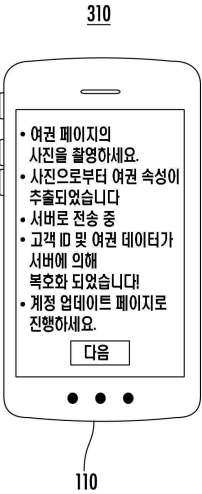
도면2b



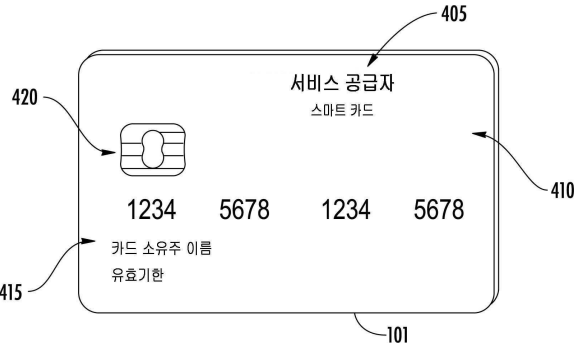
도면3a



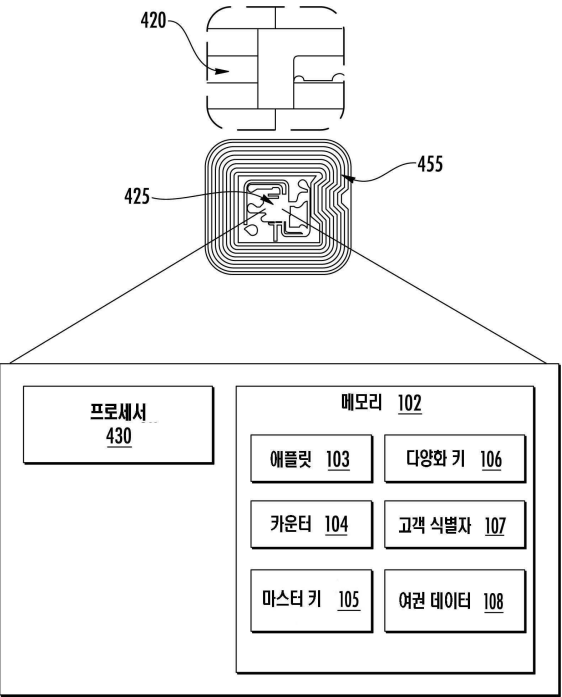
도면3b



도면4a



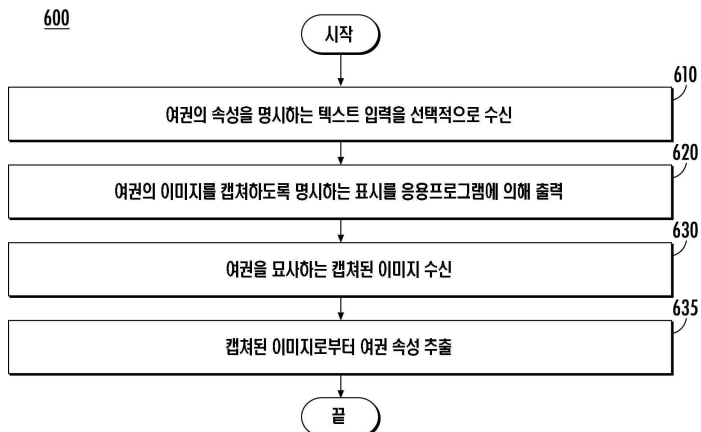
도면4b



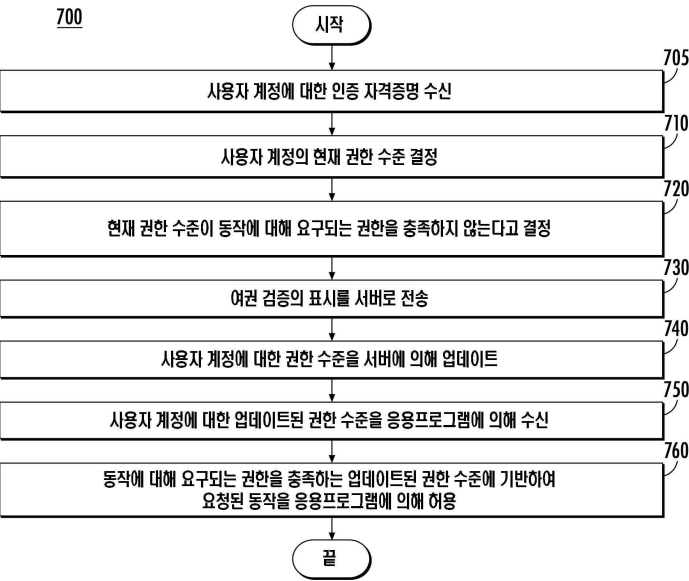
도면5



도면6



도면7



도면8

