



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0013019
(43) 공개일자 2023년01월26일

- (51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) G06F 21/62 (2013.01)
H04L 67/02 (2022.01) H04L 9/40 (2022.01)
- (52) CPC특허분류
G06F 21/606 (2013.01)
G06F 21/6281 (2013.01)
- (21) 출원번호 10-2022-7035597
(22) 출원일자(국제) 2021년05월14일
심사청구일자 없음
- (85) 번역문제출일자 2022년10월13일
(86) 국제출원번호 PCT/US2021/032424
(87) 국제공개번호 WO 2021/236436
국제공개일자 2021년11월25일
- (30) 우선권주장
16/876,549 2020년05월18일 미국(US)

- (71) 출원인
캐피탈 원 서비스즈, 엘엘씨
미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680
- (72) 발명자
루나티, 스테판
미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680, 캐피탈 원 서비스즈, 엘엘씨 내
- (74) 대리인
김동완

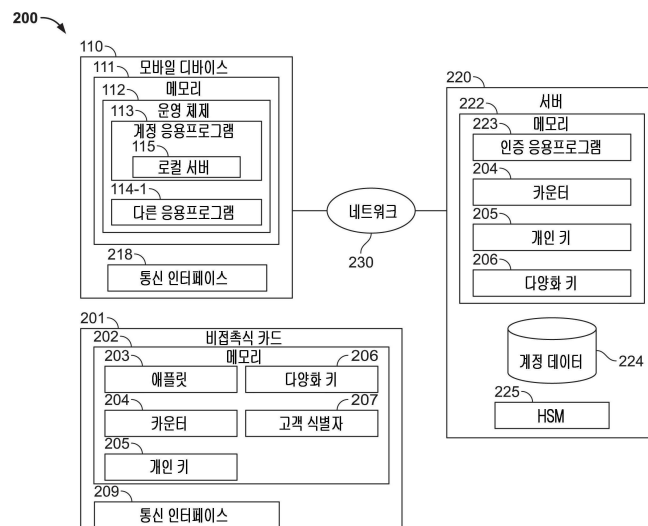
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 모바일 운영 체제에서 응용프로그램 간 통신의 활성화

(57) 요약

모바일 운영 체제에서 응용프로그램 간의 통신을 위한 시스템, 방법 및 컴퓨터 판독 가능 매체가 제공된다. 제1 응용프로그램은 제2 응용프로그램으로부터 데이터에 대한 요청을 수신할 수 있다. 제1 응용프로그램은 제2 응용프로그램에 대한 제1 URL을 생성할 수 있으며 제1 URL의 파라미터는 제1 응용프로그램의 식별자를 포함한다. 모바일 운영 체제는 제1 URL에 액세스하여 제2 응용프로그램을 열 수 있다. 제2 응용 프로그램은 계정에 대한 자격 증명을 검증하고 포트에서 서버를 개시할 수 있습니다. 제2 응용프로그램은 제1 응용프로그램에 대한 제2 URL을 생성할 수 있으며 제2 URL의 파라미터는 포트를 포함한다. 운영 체제는 제1 응용프로그램을 열기 위해 제2 URL에 액세스할 수 있다. 제1 응용프로그램은 제2 URL 내에 명시된 포트를 이용하여 서버와 연결을 설정하고, 서버와의 연결을 통해 제2 응용프로그램으로부터 데이터를 수신할 수 있다.

대표도



(52) CPC특허분류

H04L 63/0823 (2013.01)

H04L 63/0853 (2013.01)

H04L 63/18 (2013.01)

H04L 67/02 (2022.05)

명세서

청구범위

청구항 1

프로세서; 및

명령어를 저장하는 메모리;

를 포함하는 디바이스에 있어서,

상기 명령어는 프로세서에 의해 실행될 때 프로세서가

제2 응용프로그램으로부터 데이터를 수신하도록 명시하는 표시를 프로세서 상에서 실행하는 제1 응용프로그램에 의해 수신하고;

제1 URL의 파라미터는 제1 응용프로그램의 식별자를 포함하며, 제2 응용프로그램으로 향하는 제1 URL을 제1 응용프로그램에 의해 생성하고;

제2 응용프로그램을 열기 위한 제1 URL에 프로세서에서 실행하는 모바일 운영 체제(OS)에 의해 액세스하고;

계정에 대한 인증 자격증명을 제2 응용프로그램에 의해 검증하고;

포트 상의 로컬 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP) 서버를 제2 응용프로그램에 의해 개시하고;

제2 URL의 파라미터는 포트를 포함하며, 제1 응용프로그램으로 향하는 제2 URL을 제2 응용프로그램에 의해 생성하고;

제1 응용프로그램을 열기 위한 제2 URL에 OS에 의해 액세스하고;

제2 URL의 파라미터에 명시된 포트를 사용하여 로컬 TCP/IP 서버와의 연결을 제1 응용프로그램에 의해 설정하고; 및

로컬 TCP/IP 서버와의 연결을 통해 제2 응용프로그램으로부터 데이터를 제1 응용프로그램에 의해 수신;

하도록 유도함을 특징으로 하는 디바이스.

청구항 2

제 1항에 있어서, 명령어를 메모리는 프로세서에 의해 실행될 때 프로세서가

제1 응용프로그램으로부터 연결 설정 요청을 제2 응용프로그램의 로컬 TCP/IP 서버에 의해 수신하고; 및

요청 내에서 제 1 응용프로그램의 식별자를 식별하는 것에 기반하여 연결을 설정하도록 제 2 응용프로그램에 의해 결정;

하도록 유도함을 특징으로 하는 디바이스.

청구항 3

제 2항에 있어서, 요청은 제1 응용프로그램의 인증서를 더욱 포함하고, 명령어를 저장하는 메모리는 프로세서에 의해 실행될 때 프로세서가

제 1 응용프로그램의 인증서를 제 2 응용프로그램에 의해 검증하도록 유도하고,

여기서 제 2 응용프로그램은 제 1 응용프로그램의 인증서를 검증하는 것에 기반하여 연결을 설정하기로 더욱 결정하고, 로컬 TCP/IP 서버는 디바이스 상에서 실행하는 응용프로그램에만 액세스할 수 있음

을 특징으로 하는 디바이스.

청구항 4

제 1항에 있어서, 명령어를 저장하는 메모리는 프로세서에 의해 실행될 때 프로세서가, 제2 응용프로그램이 로컬 TCP/IP 서버를 개시하기 전에

비접촉식 카드로부터 암호화된 데이터를 인증 자격증명을 검증한 후에 제2 응용프로그램에 의해 수신하고;

암호화된 데이터를 인증 서버로 제2 응용프로그램에 의해 전송하고; 및

제2 응용프로그램은 인증 서버로부터 수신된 표시에 적어도 부분적으로 기반하여 로컬 TCP/IP 서버를 개시하며, 인증 서버가 암호화된 데이터를 복호화 하였음을 명시하는 표시를 인증 서버로부터 제2 응용프로그램에 의해 수신;

하도록 유도함을 특징으로 하는 디바이스.

청구항 5

제 1항에 있어서, 명령어를 메모리는 프로세서에 의해 실행될 때 프로세서가

제1 URL의 적어도 일부를 OS의 응용프로그램 프로그래밍 인터페이스(API)를 사용하여 제1 응용프로그램에 의해 검증하고; 및

제2 URL의 적어도 일부를 OS의 API를 사용하여 제2 응용프로그램에 의해 검증;

하도록 유도함을 특징으로 하는 디바이스.

청구항 6

제 1항에 있어서, 명령어를 저장하는 메모리는 프로세서에 의해 실행될 때 프로세서가

제2 응용프로그램으로부터 수신된 데이터가 계정의 하나 이상의 속성을 포함하는지 제1 응용프로그램에 의해 결정하고; 및

계정의 하나 이상의 속성을 제1 응용프로그램 내의 하나 이상의 양식 필드에 제1 응용프로그램에 의해 자동 채우기;

하도록 유도함을 특징으로 하는 디바이스.

청구항 7

제 1항에 있어서, 제1 및 제2 URL은 범용 링크 URL을 포함하고, OS는 제1 및 제2 응용프로그램이 서로 다른 개발자에게 등록된 것에 기반하여 로컬 TCP/IP 서버의 사용 없이 제1 및 제2 응용프로그램 간의 통신을 제한함을 특징으로 하고,

명령어를 저장하는 메모리는 프로세서에 의해 실행될 때 프로세서가

OS의 백그라운드에서 실행할 백그라운드 태스크로서 제2 응용프로그램을 OS의 응용프로그램 프로그래밍 인터페이스를 사용하여 제2 응용프로그램에 의해 등록하고; 및

OS의 백그라운드에서 백그라운드 태스크의 일부로 로컬 TCP/IP 서버를 OS에 의해 실행;

하도록 유도함을 특징으로 하는 디바이스.

청구항 8

컴퓨터-판독가능 프로그램 코드를 포함하는 비-일시적 컴퓨터-판독가능 저장 매체에 있어서,

상기 프로그램 코드는 디바이스의 프로세서에 의해 프로세서가

제2 응용프로그램으로부터 데이터를 수신하도록 명시하는 표시를 프로세서 상에서 실행하는 제1 응용프로그램에 의해 수신하고;

제1 URL의 파라미터는 제1 응용프로그램의 식별자를 포함하며, 제2 응용프로그램으로 향하는 제1 URL을 제1 응용프로그램에 의해 생성하고;

제2 응용프로그램을 열기 위한 제1 URL에 프로세서에서 실행하는 모바일 운영 체제(OS)에 의해 액세스하고;

계정에 대한 인증 자격증명을 제2 응용프로그램에 의해 검증하고;

포트 상의 로컬 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP) 서버를 제2 응용프로그램에 의해 개시하고;

제2 URL의 파라미터는 포트를 포함하며, 제1 응용프로그램으로 향하는 제2 URL을 제2 응용프로그램에 의해 생성하고;

OS에 의해, 제1 응용프로그램을 열기 위한 제2 URL에 액세스하고;

제2 URL의 파라미터에 명시된 포트를 사용하여 로컬 TCP/IP 서버와의 연결을 제1 응용프로그램에 의해 설정하고; 및

로컬 TCP/IP 서버와의 연결을 통해 제2 응용프로그램으로부터 데이터를 제1 응용프로그램에 의해 수신;

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

청구항 9

제 8항에 있어서, 프로세서에 의해 실행될 때 프로세서가

요청은 제1 응용프로그램의 인증서를 포함하며, 제1 응용프로그램으로부터 연결을 설정하기 위한 요청을 제2 응용프로그램의 로컬 TCP/IP 서버에 의해 수신하고;

제1 응용프로그램의 인증서를 제2 응용프로그램에 의해 검증하고; 및

로컬 TCP/IP 서버는 디바이스 상에서 실행되는 응용프로그램에만 액세스 가능하며, 요청 내에서 제 1 응용프로그램의 식별자 식별 및 제 1 응용프로그램의 인증서 검증에 기반하여 연결을 설정하도록 제 2 응용프로그램에 의해 결정;

하도록 유도하는 컴퓨터-판독가능 프로그램 코드를 포함함을 특징으로 하는 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 10

제 9항에 있어서, 프로세서에 의해 실행될 때 프로세서가, 제2 응용프로그램이 로컬 TCP/IP 서버를 개시하기 전에:

비접촉식 카드로부터 암호화된 데이터를 인증 자격증명을 검증한 후에 제2 응용프로그램에 의해 수신하고;

암호화된 데이터를 인증 서버로 제2 응용프로그램에 의해 전송하고; 및

제2 응용프로그램은 인증 서버로부터 수신된 표시에 적어도 부분적으로 기반하여 로컬 TCP/IP 서버를 개시하며, 인증 서버가 암호화된 데이터를 복호화 하였음을 명시하는 표시를 인증 서버로부터 제2 응용프로그램에 의해 수신;

하도록 유도하는 컴퓨터-판독가능 프로그램 코드를 포함함을 특징으로 하는 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 11

제 8항에 있어서, 프로세서에 의해 실행될 때 프로세서가

제1 URL의 적어도 일부를 OS의 응용프로그램 프로그래밍 인터페이스(API)를 사용하여 제1 응용프로그램에 의해 검증하고; 및

제2 URL의 적어도 일부를 OS의 API를 사용하여 제2 응용프로그램에 의해 검증;

하도록 유도하는 컴퓨터-판독가능 프로그램 코드를 포함함을 특징으로 하는 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 12

제 8항에 있어서, 프로세서에 의해 실행될 때 프로세서가

제2 응용프로그램으로부터 수신된 데이터가 계정의 하나 이상의 속성을 포함하는지 제1 응용프로그램에 의해 결정하고; 및

계정의 하나 이상의 속성을 제1 응용프로그램 내의 하나 이상의 양식 필드에 제1 응용프로그램에 의해 자동 채우기;

하도록 유도하는 컴퓨터-판독가능 프로그램 코드를 포함함을 특징으로 하는 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 13

제 8항에 있어서, 프로세서에 의해 실행될 때 프로세서가

OS의 백그라운드에서 실행할 백그라운드 태스크로서 제2 응용프로그램을 OS의 응용프로그램 프로그래밍 인터페이스를 사용하여 제2 응용프로그램에 의해 등록하고; 및

OS의 백그라운드에서 백그라운드 태스크로 로컬 TCP/IP 서버를 OS에 의해 실행;

하도록 유도하는 컴퓨터-판독가능 프로그램 코드를 포함하고,

여기서 제1 및 제2 URL은 범용 링크 URL을 포함하고, OS는 제1 및 제2 응용프로그램이 서로 다른 개발자에게 등록된 것에 기반하여 로컬 TCP/IP 서버의 사용 없이 제1 및 제2 응용프로그램 간의 통신을 제한함

을 특징으로 하는 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 14

제2 응용프로그램으로부터 데이터를 수신하도록 명시하는 표시를 디바이스의 프로세서 상에서 실행하는 제1 응용프로그램에 의해 수신하는 단계;

제1 URL의 파라미터는 제1 응용프로그램의 식별자를 포함하며, 제2 응용프로그램으로 향하는 제1 URL을 제1 응용프로그램에 의해 생성하는 단계;

제2 응용프로그램을 열기 위한 제1 URL에 프로세서에서 실행하는 모바일 운영 체제(OS)에 의해 액세스하는 단계;

계정에 대한 인증 자격증명을 제2 응용프로그램에 의해 검증하는 단계;

포트 상에서 로컬 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP) 서버를 제2 응용프로그램에 의해 개시하는 단계;

제2 URL의 파라미터는 포트를 포함하며, 제1 응용프로그램으로 향하는 제2 URL을 제2 응용프로그램에 의해 생성하는 단계;

제1 응용프로그램을 열기 위한 제2 URL에 OS에 의해 액세스하는 단계;

제2 URL의 파라미터에 명시된 포트를 사용하여 로컬 TCP/IP 서버와 연결을 제1 응용프로그램에 의해 설정하는 단계; 및

로컬 TCP/IP 서버와의 연결을 통해 제2 응용프로그램으로부터 데이터를 제1 응용프로그램에 의해 수신하는 단계;

를 포함하는 방법.

청구항 15

제 14항에 있어서, 방법은

제1 응용프로그램으로부터 연결 설정 요청을 제2 응용프로그램의 로컬 TCP/IP 서버에 의해 수신하는 단계; 및

요청 내에서 제1 응용프로그램의 식별자를 식별하는 것에 기반하여 연결을 설정하도록 제2 응용프로그램에 의해 결정하는 단계;

를 더욱 포함함을 특징으로 하는 방법.

청구항 16

제 15항에 있어서, 요청은 제1 응용프로그램의 인증서를 더욱 포함하고, 방법은

제 1 응용프로그램의 인증서를 제 2 응용프로그램에 의해 검증하는 단계를 더욱 포함하고,

여기서 제 2 응용프로그램은 제 1 응용프로그램의 인증서를 검증하는 것에 기반하여 연결을 설정하기로 더욱 결정하고, 로컬 TCP/IP 서버는 디바이스에서 실행하는 응용프로그램에만 액세스할 수 있으며, OS는 원격 디바이스로부터 수신된 TCP/IP 서버에 대한 액세스 요청을 거부함

을 특징으로 하는 방법.

청구항 17

제14항에 있어서, 제2 응용프로그램이 로컬 TCP/IP 서버를 개시하기 전에

비접촉식 카드로부터 암호화된 데이터를 인증 자격증명을 검증한 후에 제2 응용프로그램에 의해 수신하는 단계;

암호화된 데이터를 인증 서버로 제2 응용프로그램에 의해 전송하는 단계; 및

제2 응용프로그램은 인증 서버로부터 수신된 표시에 적어도 부분적으로 기초하여 로컬 TCP/IP 서버를 개시하며, 인증 서버가 암호화된 데이터를 복호화 하였음을 명시하는 표시를 인증 서버로부터 제2 응용프로그램에 의해 수신하는 단계;

를 더욱 포함함을 특징으로 하는 방법.

청구항 18

제 14항에 있어서,

제1 URL의 적어도 일부를 OS의 응용프로그램 프로그래밍 인터페이스(API)를 사용하여 제1 응용프로그램에 의해 검증하는 단계; 및

제2 URL의 적어도 일부를 OS의 API를 사용하여 제2 응용프로그램에 의해 검증하는 단계;
를 더욱 포함함을 특징으로 하는 방법.

청구항 19

제 14항에 있어서,

제2 응용프로그램으로부터 수신된 데이터가 계정의 하나 이상의 속성을 포함하는지 제1 응용프로그램에 의해 결정하는 단계; 및

계정의 하나 이상의 속성을 제1 응용프로그램 내의 하나 이상의 양식 필드에 제1 응용프로그램에 의해 자동 채우기하는 단계;

를 더욱 포함함을 특징으로 하는 방법.

청구항 20

제 14항에 있어서, 제1 및 제2 URL은 범용 링크 URL을 포함하고, OS는 제1 및 제2 응용프로그램이 서로 다른 개발자에게 등록된 것에 기반하여 로컬 TCP/IP 서버의 사용 없이 제1 및 제2 응용프로그램 간의 통신을 제한함을 특징으로 하고,

OS의 백그라운드에서 실행할 백그라운드 태스크로서 제2 응용프로그램을 OS의 응용프로그램 프로그래밍 인터페이스를 사용하여 제2 응용프로그램에 의해 등록하는 단계; 및

OS의 백그라운드에서 백그라운드 태스크의 일부로 로컬 TCP/IP 서버를 OS에 의해 실행하는 단계;

를 더욱 포함함을 특징으로 하는 방법.

발명의 설명

기술 분야

[0001] 본 발명은 2020년 5월 18일자로 출원된 미국 비-잠정출원 제16/876,549호 "모바일 운영 체제에서 응용프로그램 간 통신의 활성화"의 우선권을 주장한다. 상기 언급된 특허출원의 내용은 그 전체로 본 발명에 참고문헌으로 통합된다.

[0002] 본 발명의 실시형태는 일반적으로 컴퓨터 플랫폼에 관한 것으로 보다 상세하게는 모바일 운영 체제에서 응용프로그램 간의 통신을 가능하게 하는 것에 관한 것이다.

배경 기술

[0003] 일부 모바일 운영 체제는 동일한 디바이스에서 실행되는 둘 이상의 응용프로그램 간의 통신을 제한한다. 예를 들어 일부 모바일 운영 체제는 제1 응용프로그램이 제2 응용프로그램과 직접 통신하는 것을 방지할 수 있다. 유사하게 일부 모바일 운영 체제는 이러한 응용프로그램 간의 데이터 교환을 제한할 수 있다. 이를 통해 응용프로그램 간의 합법적이고 안전한 통신이 불필요하게 제한될 수 있다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0004] 본 발명에 개시된 실시형태는 모바일 운영 체제에서 응용프로그램 간의 통신을 위한 시스템, 방법, 제조 물품 및 컴퓨터 판독가능 매체를 제공한다. 하나의 예에서 디바이스의 프로세서 상에서 실행되는 제1 응용프로그램은 디바이스 상의 제2 응용프로그램으로부터 데이터에 대한 요청을 수신할 수 있다. 제1 응용프로그램은 제2 응용

프로그램으로 향하는 제1 URL을 생성할 수 있다. 제1 URL의 파라미터는 제1 응용프로그램의 식별자를 포함할 수 있다. 디바이스에서 실행되는 모바일 운영 체제는 제1 URL에 액세스하여 제2 응용프로그램을 열 수 있다.

[0005] 제2 응용프로그램은 계정에 대한 자격증명을 검증하고 디바이스에서 실행하기 위해 포트에서 서버를 개시할 수 있다. 제2 응용프로그램은 제1 응용프로그램으로 향하는 제2 URL을 생성할 수 있으며 제2 URL의 파라미터는 포트를 포함한다. 운영 체제는 제1 응용프로그램을 열기 위해 제2 URL에 액세스할 수 있다. 제1 응용프로그램은 제2 URL에 명시된 포트를 이용하여 서버와 연결을 설정하고 서버와의 연결을 통해 제2 응용프로그램으로부터 데이터를 수신할 수 있다.

도면의 간단한 설명

[0006] 도 1a 내지 도 1f는 모바일 운영 체제에서 응용프로그램 간의 통신을 가능하게 하기 위한 시스템의 실시형태를 도시한다.

도 2a 내지 도 2c는 모바일 운영 체제에서 응용프로그램 간의 통신을 가능하게 하기 위한 시스템의 실시형태를 도시한다.

도 3a 내지 도 3c는 모바일 운영 체제에서 응용프로그램 간의 통신을 가능하게 하는 실시형태를 도시한다.

도 4는 제1 로직 흐름의 실시형태를 도시한다.

도 5는 제2 로직 흐름의 실시형태를 도시한다.

도 6a 내지 도 6b는 예시적인 비접촉식 카드를 도시한다.

도 7은 컴퓨터 시스템의 실시형태를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0007] 본 발명에 개시된 실시형태는 상이한 개발자에게 등록된 응용프로그램 간의 통신을 제한하는 모바일 운영 체제(OS)에서 2개 이상의 응용프로그램 간의 보안 통신을 위한 기술을 제공한다. 일반적으로 디바이스 상에서 실행되는 제1 응용프로그램은 디바이스 상의 제2 응용프로그램에 의해 제공될 수 있는 데이터로부터 이익을 얻을 수 있다. 예를 들어 제1 응용프로그램은 OS에서 판매자에 등록된 판매자 응용프로그램일 수 있고 제2 응용프로그램은 OS에서 금융기관에 등록된 금융기관에서 제공하는 응용프로그램일 수 있다.

[0008] 이러한 실시예에서 판매자 응용프로그램의 사용자는 금융기관 응용프로그램으로부터의 데이터 예를 들어 결제 정보, 신상 정보 등을 판매자 응용프로그램에서 사용하도록 요청할 수 있다. 요청에 응답하여 판매자 응용프로그램은 금융기관 응용프로그램으로 향하는 제1 고유 리소스 로케이터(URL)를 생성할 수 있다. 제1 URL의 파라미터는 판매자 응용프로그램의 식별자를 포함할 수 있다.

[0009] 그 후 판매자 응용프로그램은 제1 URL을 오픈하거나 액세스하도록 모바일 OS에 지시할 수 있다. 이를 통해 모바일 OS는 디바이스에서 금융기관 응용 프로그램을 열도록 한다. 금융기관 응용프로그램은 모바일 디바이스에서 실행되는 응용프로그램에만 액세스할 수 있는 OS 내의 로컬 서버를 개시할 수 있다. 로컬 서버는 포트에서 개시될 수 있으며 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP) 서버 또는 임의의 다른 유형의 서버 예를 들어 하이퍼텍스트 전송 프로토콜(HTTP) 서버일 수 있다.

[0010] 일부 실시형태에서 금융기관 응용프로그램은 서버를 시작하기 전에 금융기관과의 계정에 대한 인증 자격증명을 수신할 수 있다. 추가적으로 및/또는 대안적으로 서버를 시작하기 전에 금융기관 응용프로그램은 계정과 연관된 비접촉식 카드로부터 암호화된 데이터를 수신하고, 인증 서버로 암호화된 데이터를 전송하고, 암호화된 데이터가 검증되었다는 확인을 인증 서버로부터 수신할 수 있다.

[0011] 금융기관 응용프로그램은 판매자 응용프로그램으로 향하는 제2 URL을 생성할 수 있다. 제2 URL은 제1 URL의 파라미터로서 명시된 판매자 응용프로그램의 식별자에 적어도 부분적으로 기반할 수 있다. 제2 URL은 파라미터로서 로컬 서버의 포트를 추가로 명시할 수 있다. 금융기관 응용프로그램은 OS의 백그라운드 태스크로 로컬 서버 및/또는 금융기관 응용프로그램을 추가로 등록할 수 있다. 이는 OS의 포그라운드에서 예를 들어 판매자 응용프로그램과 같은 다른 응용프로그램이 실행됨에 따라 로컬 서버 및/또는 금융기관 응용프로그램이 OS의 백그라운드에서 계속 실행되게 한다. 금융기관 응용프로그램은 제2 URL을 오픈하거나 액세스하도록 모바일 OS에 지시할 수 있다. 이를 통해 OS가 OS의 포그라운드에서 판매자 응용프로그램을 열도록 한다.

- [0012] 일단 열리게 되면 판매자 응용프로그램은 제2 URL에 명시된 로컬 서버의 포트를 식별하고 로컬 인터페이스 예를 들어 로컬 루프백 IP 주소의 명시된 포트에서 로컬 서버와의 연결을 설정할 수 있다. 일부 실시형태에서 판매자 응용프로그램은 연결 설정의 일부로서 서버에 의해 검증될 수 있는 인증서를 제공할 수 있다. 추가적으로 및/또는 대안적으로 판매자 응용프로그램은 연결 설정의 일부로서 서버에 의해 검증될 수 있는 토큰을 제공할 수 있다. 연결이 설정되면 연결을 통해 금융기관 응용프로그램이 판매자 응용프로그램과 데이터를 교환할 수 있으며 그 반대도 가능하다.
- [0013] 예를 들어 금융기관 응용프로그램은 인증된 계정 소유자에 대한 계정 세부 정보 예를 들어 결제 카드 번호, 만료 날짜, 카드 검증 값(CVV), 주소 정보 등을 제공할 수 있다. 그러한 실시예에서 판매자 응용프로그램은 수신된 데이터를 양식에 자동으로 채울 수 있고 이에 따라 사용자는 수신된 데이터를 사용하여 구매 또는 기타 작업을 완료할 수 있다. 보다 일반적으로 연결을 통해 임의의 수와 유형의 데이터를 교환할 수 있다.
- [0014] 유리하게는 모바일 OS는 외부 엔티티에 의한 로컬 서버에 대한 액세스를 제한할 수 있다. 이를 통해 디바이스와 모든 데이터의 보안이 향상된다. 또한 금융기관 응용프로그램으로부터 결제 데이터를 안전하게 수신하여 결제 데이터의 보안을 강화한다. 예를 들어 사용자가 데이터를 수동으로 입력할 필요가 없으므로 데이터 보안이 손상될 수 있다. 또한 일부 실시형태에서 금융기관은 본 발명에 개시된 작업을 수행하는 데 필요한 기능을 포함하는 프레임워크 예를 들어 소프트웨어 개발 키트(SDK)를 제공할 수 있다. 이를 통해 본 발명에 개시된 작업을 수행하는 데 필요한 전체 SDK 및/또는 프레임워크 없이 필요한 기능만 제3자 응용프로그램 예를 들어 판매자 응용프로그램에 통합될 수 있다.
- [0015] 예를 들어 데이터 교환에 사용될 수 있는 하나 이상의 API를 판매자 응용프로그램에 제공함으로써, SDK는 판매자 응용프로그램에서 필요한 기능을 제공하기 위해 판매자 응용프로그램에 금융기관 응용프로그램의 전체 코드 기반을 포함하는 것에 비해 판매자 응용프로그램의 크기를 줄일 수 있게 한다.
- [0016] 본 발명에 사용된 표기법 및 명명법을 일반적으로 참조하여 이어지는 발명의 상세한 설명의 하나 이상의 부분은 컴퓨터 또는 컴퓨터 네트워크 상에서 실행되는 프로그램 절차의 관점에서 제시될 수 있다. 이러한 절차적 설명 및 표현은 해당 분야의 당업자에게 작업 내용을 가장 효과적으로 전달하기 위해 해당 기술 분야의 당업자가 사용한다. 절차는 여기에서 일반적으로 원하는 결과로 이어지는 자체 일관된 작업 시퀀스로 간주된다. 이러한 작업은 물리적 수량의 물리적 조작이 필요한 작업이다.
- [0017] 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, 엘레먼트, 기호, 문자, 용어, 숫자 등으로 지칭하는 것이 편리한 경우가 있다. 그러나 이러한 모든 용어 및 유사한 용어는 적절한 물리적 수량과 관련되어야 하며 해당 수량에 적용되는 편리한 라벨일 뿐이다.
- [0018] 또한 이러한 조작은 일반적으로 인간 작업자가 수행하는 정신적 조작과 관련된 추가 또는 비교와 같은 용어로 참조된다. 그러나 인간 작업자의 그러한 능력은 하나 이상의 실시형태의 일부를 형성하는 본 발명에 설명된 임의의 작업에서 대부분의 경우에 필요하지 않거나 바람직하지 않다. 오히려 이러한 작업은 기계 작업이다. 다양한 실시형태의 동작을 수행하기 위한 유용한 기계는 본 발명의 가르침에 따라 기록된 내부에 저장된 컴퓨터 프로그램에 의해 선택적으로 활성화되거나 형상화된 디지털 컴퓨터를 포함하거나 및/또는 요구되는 목적을 위해 특별히 구성된 디바이스 또는 디지털 컴퓨터를 포함한다. 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.
- [0019] 이제 도면을 참조하며 여기서 유사한 참조 번호는 전체에 걸쳐 유사한 엘레먼트를 나타내기 위해 사용된다. 하기 설명에서는 설명의 목적으로 그에 대한 완전한 이해를 제공하기 위해 다수의 구체적인 세부사항이 제시된다. 그러나 신규한 실시형태는 이러한 특정 세부사항 없이 실시될 수 있음이 명백할 것이다. 다른 예에서 잘 알려진 구조 및 디바이스는 설명을 용이하게 하기 위해 블록도 형태로 표시된다. 의도는 청구범위 내에서 모든 수정, 등가물 및 대안을 포함하는 것이다.
- [0020] 도 1a는 개시된 실시형태와 일치하는 예시적인 시스템(100)의 개략도를 도시한다. 도시된 바와 같이 시스템(100)은 하나 이상의 모바일 컴퓨터 디바이스(110)를 포함한다. 모바일 디바이스(110)는 스마트폰, 태블릿 컴퓨터, 웨어러블 디바이스, 랩톱, 휴대용 게임 디바이스 등과 같이 모바일 운영 체제를 실행하는 임의의 유형의 네트워크 가능 컴퓨터 디바이스를 나타낸다.
- [0021] 모바일 디바이스(110)는 프로세서(101) 및 메모리(111)를 포함할 수 있다. 프로세서(101)는 AMD® Athlon®,

Duron® 및 Opteron® 프로세서; ARM® 응용프로그램, 임베디드 및 보안 프로세서; IBM® 및 Motorola® DragonBall® 및 PowerPC® 프로세서; IBM 및 Sony® Cell 프로세서; Intel® Celeron®, Core®, Core (2) Duo®, Itanium®, Pentium®, Xeon® 및 XScale® 프로세서; 및 유사한 프로세서를 제한 없이 포함하는 임의의 컴퓨터 프로세서일 수 있다. 듀얼 마이크로프로세서, 멀티 코어 프로세서 및 기타 멀티 프로세서 아키텍처가 프로세서(101)로 적용될 수도 있다.

[0022] 메모리(111)는 읽기 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 동적 RAM(DRAM), 더블 데이터 레이트 DRAM(DDR), 동기식 DRAM(SDRAM) 정적 RAM(SRAM), 프로그램가능 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, 복수 배열 독립 디스크(RAID) 드라이브와 같은 디바이스 어레이, 고체 상태 메모리 디바이스(예를 들어 USB 메모리, 고체 상태 드라이브(SSD) 및 정보 저장에 적합한 기타 유형의 저장 매체와 같은 하나 이상 고속 메모리 유니트의 형태로 다양한 종류의 컴퓨터 판독가능 저장 매체를 포함할 수 있다.

[0023] 도시된 바와 같이 모바일 디바이스(110)의 메모리(111)는 모바일 운영 체제(OS)(112)의 인스턴스를 포함한다. 예시적인 모바일 운영 체제(112)는 Android® 및 iOS® 모바일 운영 체제를 포함한다. 도시된 바와 같이 OS(112)는 계정 응용프로그램(113) 및 하나 이상의 다른 응용프로그램(114)을 포함한다. 계정 응용프로그램(113)은 결제 카드 활성화, 계좌 잔액 조회, 아이템 구매, 결제 처리 등과 같은 다양한 계정 관련 작업을 사용자가 수행할 수 있게 한다.

[0024] 일부 실시형태에서 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, 페이스 ID 등을 포함할 수 있다. 다른 응용프로그램(114)은 웹 브라우저, 판매자 응용프로그램, 쇼핑 응용프로그램, 배달 서비스 응용프로그램, 승차 공유 응용프로그램, 메시지 응용프로그램, 워드 프로세서 응용프로그램, 소셜 미디어 응용프로그램 등과 같은 임의의 유형의 컴퓨터 응용프로그램을 나타낸다.

[0025] 예를 들어 다른 응용프로그램(114) 중 제1 응용프로그램은 상품, 서비스 또는 임의의 다른 유형의 항목을 구매하기 위해 판매자에 의해 제공되는 판매자 응용프로그램일 수 있다. 다른 예로서 다른 응용프로그램(114) 중 제2 응용프로그램은 사용자가 교통 서비스를 마련하고 비용을 지불할 수 있게 하는 승차 공유 응용프로그램일 수 있다. 또 다른 예로서 다른 응용프로그램(114) 중 제3 응용프로그램은 사용자가 배달을 위해 음식을 구매할 수 있게 하는 배달 서비스 응용프로그램일 수 있다.

[0026] OS(112)에 의해 부과된 제한으로 인해 다른 개발자 또는 엔티티에 등록 또는 할당된 응용프로그램은 통신 및/또는 데이터 교환이 불가능할 수 있다. 예를 들어 그러한 제한이 있는 경우, 개발자인 금융기관에 등록된 계정 응용프로그램(113)은 금융기관이 아닌 다른 엔티티에 등록된 다른 응용프로그램(114)과 통신 및/또는 데이터를 교환할 수 없다. 유사하게 다른 응용프로그램(114) 중 제1 엔티티에 등록된 제1 응용프로그램은 다른 응용프로그램(114) 중 제1 엔티티와 상이한 제2 엔티티에 등록된 다른 응용프로그램과 통신할 수 없다. 응용프로그램 등록은 응용프로그램이 OS(112) 제공자와 연관된 응용프로그램 스토어에 제출될 때 발생할 수 있다.

[0027] 그러나 유리하게는 본 발명에 개시된 실시형태는 상이한 개발자 예를 들어 계정 응용프로그램(113) 및 임의의 다른 응용프로그램(114) 및/또는 다른 응용프로그램(114) 중 임의의 2개에 등록된 응용프로그램 간의 통신 및/또는 데이터 교환을 안전하게 허용하는 기술을 제공한다.

[0028] 도 1b는 응용프로그램(114-1)이 계정 응용프로그램(113)과 통신하기 위한 요청을 수신하는 실시형태를 도시한다. 예를 들어 응용프로그램(114-1)은 판매자에게 등록 또는 할당된 응용프로그램일 수 있다. 이러한 실시예에서 사용자는 응용프로그램(114-1)을 통해 구매할 하나 이상의 아이템을 선택할 수 있다. 체크아웃 프로세스 동안 응용프로그램(114-1)은 계정 응용프로그램(113)을 사용하여 결제 및/또는 개인 정보를 제공하는 옵션을 사용자에게 제공할 수 있다. 그 후 사용자는 옵션을 수락하여 응용프로그램(114-1)이 데이터를 수신하기 위해 계정 응용프로그램(113)과 통신하도록 지시할 수 있다. 요청에 응답하여 응용프로그램(114-1)은 URL(125)을 생성할 수 있다.

[0029] URL(125)은 계정 응용프로그램(113)으로 향할 수 있다. URL(125)은 응용프로그램(114-1)이 URL(125)을 생성했음을 나타내는 파라미터를 더욱 포함할 수 있다. URL(125)은 범용 링크 또는 임의의 유형의 URL일 수 있다. 파라미터는 고유 식별자, 토큰 또는 URL 문자열과 같이 응용프로그램(114-1)을 고유하게 식별하기에 적합한 임의

의 식별자일 수 있다. 예를 들어 URL(125)은 "capitalone:///appid=merchantapp"일 수 있으며 여기서 "capitalone:///" 부분은 디바이스(110) 상의 계정 응용프로그램(113)의 인스턴스로 향하고 "appid=merchantapp"은 URL(125)을 생성하는 응용프로그램(114-1)의 식별자이다. 일부 실시형태에서 파라미터는 응용프로그램(114-1)에 의해 암호화되고 수신 시 계정 응용프로그램(113)에 의해 복호화된다.

[0030] 일부 실시형태에서 응용프로그램(114-1)은 OS(112)의 응용프로그램 프로그래밍 인터페이스(API)를 사용하여 URL(125)이 유효한지 여부를 결정한다. 예를 들어 URL(125)에 의해 타겟팅 된 응용프로그램이 디바이스(110)에 설치되었는지 여부를 표시한다. 예를 들어 OS(112)는 API에 대한 입력으로 제공된 URL이 유효한지 여부를 나타내는 "canOpenURL" API를 제공할 수 있다. 일반적으로 응용프로그램 개발자는 응용프로그램 스토어에 응용프로그램을 제출할 때 OS(112)의 공급자에게 하나 이상의 URL을 등록할 수 있다. 이를 통해 OS가 제공하는 API에 의한 검증을 용이하게 할 수 있다.

[0031] 그러한 실시예에서 응용프로그램(114-1)은 URL(125) 및/또는 계정 응용프로그램(113)으로 향하는 URL(125)의 일부를 API에 제공할 수 있으며 이는 계정 응용프로그램(113)이 디바이스에 설치되고 URL(125)를 사용하여 열릴 수 있음을 나타낸다. 이를 통해 올바른 응용 프로그램이 설치되었는지 확인하고 계정 응용 프로그램(113)으로 위장한 응용 프로그램을 제공하는 제3자의 시도를 저지함으로써 보안이 강화된다. 후자의 경우 제3자 응용프로그램이 API에 대한 입력으로 제공되는 URL에 등록되지 않기 때문에 위장 시도가 좌절될 수 있다.

[0032] 그러한 실시예에서 API가 무효 응답을 반환하는 경우, URL(125)에 액세스하면 계정 응용프로그램(113)을 등록하는 엔티티와 연관된 웹사이트 예를 들어 금융기관의 웹사이트 및/또는 계정 응용프로그램(113)이 다운로드 될 수 있는 응용프로그램 스토어로 향하는 웹 브라우저를 OS(112)가 시작할 수 있게 한다.

[0033] 응용프로그램(114-1) 및/또는 OS(112)는 URL(125)에 액세스하거나 이를 오픈하거나 그렇지 않으면 이를 팔로우할 수 있으며 이에 따라 계정 응용프로그램(113)이 OS(112)의 포그라운드에서 열리게 한다. 도 1c는 계정 응용프로그램(113)이 URL(125)에 대한 액세스에 응답하여 열리는 실시형태를 도시한다. 이에 응답하여 계정 응용프로그램(113)은 계정에 대한 인증 자격증명을 선택적으로 수신할 수 있다. 추가적으로 및/또는 대안적으로 및 도 2a 내지 도 2c를 참조하여 더욱 상세히 논의된 바와 같이 계정 응용프로그램(113)은 비접촉식 카드에 의해 생성된 암호화된 데이터의 검증을 선택적으로 개시할 수 있다. 그 후 계정 응용프로그램(113)은 모바일 디바이스(110) 상에서 실행하기 위해 로컬 서버(115)를 개시할 수 있다. 로컬 서버(115)는 TCP/IP 서버, HTTP 서버, 하이퍼텍스트 전송 프로토콜 보안(HTTPS) 서버, 스트리밍 서버 등과 같은 임의의 유형의 서버일 수 있다.

[0034] 그러나 로컬 응용프로그램 예를 들어 모바일 디바이스(110) 상에서 실행되는 응용프로그램 만이 로컬 서버(115)에 액세스할 수 있다. OS(112)는 예를 들어 네트워크를 통해 외부 소스로부터 로컬 서버(115)에 액세스하려는 시도를 제한할 수 있다. 계정 응용프로그램(113)은 특정 포트 번호에서 로컬 서버(115)를 개시할 수 있다. 계정 응용프로그램(113)은 미리 결정된 포트 번호를 사용하여 포트 번호를 무작위로 생성하는 것과 같은 임의의 실행 가능한 선택 방식에 따라 포트를 선택할 수 있다.

[0035] 도 1d는 계정 응용프로그램(113)이 URL(126)을 생성하는 실시형태를 도시한다. URL(126)은 응용프로그램(114-1)으로 향할 수 있으며 로컬 서버(115)의 포트 번호를 포함할 수 있다. 예를 들어 URL(126)은 "merchantapp:///port=2080"일 수 있으며 여기서 "merchantapp:///" 부분은 응용프로그램(114-1)으로 향하고 "port=2080" 부분은 로컬 서버(115)가 포트 2080 상에서 열려 있음을 나타낸다. 계정 응용프로그램(113)은 URL(125)에 명시된 응용프로그램(114-1)의 식별자에 기반하여 응용프로그램(114-1)으로 향하는 URL(126)의 부분을 결정한다. 일부 실시형태에서 URL(125)과 유사하게 계정 응용프로그램(113)은 URL(126)에 액세스하기 전에 URL(126)이 유효한지 여부를 결정하기 위해 API가 OS(112)에 호출하게 한다.

[0036] 보다 일반적으로 URL(126)은 선택된 포트에서 로컬 서버(115)에 대한 연결을 설정하기에 충분한 임의의 파라미터를 포함할 수 있다. 일부 실시형태에서 계정 응용프로그램(113)은 예를 들어 암호화 키 또는 공개 키를 사용하여 URL(126)의 포트 번호 또는 임의의 추가 파라미터를 암호화할 수 있다. 이러한 실시형태에서 응용프로그램(114-1)은 예를 들어 개인 키와 같은 대응하는 복호화 키를 사용하여 포트 번호 및/또는 추가 파라미터를 복호화할 수 있다. 또한 응용프로그램 간에 교환되는 모든 URL 파라미터가 보안을 강화하기 위해 암호화 될 수 있다.

[0037] 또한 계정 응용프로그램(113)은 로컬 서버(115) 및/또는 계정 응용프로그램(113)을 OS(112)에 백그라운드 태스크로 등록할 수 있다. 이를 통해 OS(112)의 포그라운드에서 다른 응용프로그램이 실행되는 동안 OS(112)의 백그라운드에서 로컬 서버(115) 및/또는 계정 응용프로그램(113)이 계속 실행될 수 있게 한다. 로컬 서버(115)가 개

시되었으나 일부 실시형태에서 계정 응용프로그램(113)은 URL(126)을 생성한 후에 로컬 서버(115)를 개시할 수 있다.

[0038] 도 1e는 로컬 서버(115) 및/또는 계정 응용프로그램(113)이 OS(112)의 백그라운드에서 계속 실행되는 동안 계정 응용프로그램(113) 및/또는 OS(112)가 응용프로그램(114-1)을 열기 위한 URL(126)을 여는 실시형태를 도시한다. URL(126) 수신에 응답하여 응용프로그램(114-1)은 URL(126)의 파라미터로서 명시된 로컬 서버(115)의 포트 번호를 식별할 수 있다.

[0039] 그 후 응용프로그램(114-1)은 명시된 포트에서 예를 들어 로컬 루프백 IP 주소(예를 들어, IPv4의 경우 127.0.0.1, IPv6의 경우 ::1 등), "localhost" 호스트 이름 또는 기타 미리 정의된 로컬 IP 주소에서 로컬 서버(115)와의 연결 설정을 요청할 수 있다. 연결은 로컬 서버(115)에 의해 지원되는 프로토콜 예를 들어 TCP/IP 연결 설정 등을 사용하여 설정될 수 있다. 언급된 바와 같이 URL(126)이 암호화된 데이터를 포함하는 경우, 응용프로그램(114-1)은 URL(126) 내의 암호화된 포트 번호 또는 임의의 다른 관련 파라미터를 복호화 할 수 있다.

[0040] 일부 실시형태에서 응용프로그램(114-1)은 로컬 서버(115-1)에 대한 연결 요청의 일부로서 토큰 및/또는 디지털 인증서 또는 서명을 제공한다. 로컬 서버(115)는 토큰이 유효한지 및/또는 예상되는지 여부를 결정할 수 있다. 예를 들어 토큰은 URL(125)의 파라미터로서 수신된 토큰과 매치할 수 있는 응용프로그램(114-1)을 식별한다. 유사하게 로컬 서버(115)는 응용프로그램(114-1)과 연관된 공개 키를 사용하여 인증서를 검증할 수 있다. 토큰 및/또는 인증서가 검증되면 로컬 서버(115)는 응용프로그램(114-1)과의 연결을 설정할 수 있다. 그렇지 않으면 로컬 서버(115)는 연결 요청을 거부할 수 있다.

[0041] 도 1e는 응용프로그램(114-1)과 로컬 서버(115) 사이의 연결이 설정된 및 로컬 서버(115)가 OS(112)에서 백그라운드 태스크로서 계속 실행되는 실시형태를 도시한다. 도시된 바와 같이 계정 응용프로그램(113)은 데이터(117)를 포함할 수 있다. 데이터(117)는 임의의 유형의 데이터일 수 있다. 예를 들어 데이터(117)는 가상 계좌 번호일 수 있는 결제 카드 번호, 유효기한, CVV, 주소, 이름, 성 또는 계정 응용프로그램(113)이 있는 계정의 임의의 다른 속성을 포함할 수 있다. 로컬 서버(115)가 OS(112)의 백그라운드에서 실행되고 응용프로그램(114-1)이 OS(112)의 포그라운드에서 실행되는 동안 로컬 서버(115)는 응용프로그램(114-1)에 데이터(117)를 제공할 수 있다.

[0042] 도 1f는 응용프로그램(114-1)이 로컬 서버(115)로부터 데이터(117)를 수신하는 실시형태를 도시한다. 응용프로그램(114-1)은 데이터(117)를 식별하고 데이터(117)가 사용자 및/또는 연관된 계정의 하나 이상의 속성을 포함하는지 결정할 수 있다. 그 후 응용프로그램(114-1)은 데이터(117)를 하나 이상의 양식 필드에 자동 채울 수 있으며 이를 통해 사용자는 로컬 서버(115)로부터 안전하게 수신된 데이터를 사용하여 체크아웃을 완료할 수 있다. 언급된 바와 같이 이를 통해 데이터(117)가 동일한 디바이스(110) 상의 응용프로그램 간에 안전하게 전송될 수 있다.

[0043] 또한 응용프로그램(114-1)은 최소 세트의 요구사항 예를 들어 API, 최소 SDK 등 만을 요구함으로써 로컬 서버(115)로부터 임의의 양의 데이터를 수신할 수 있다. 그렇지 않으면 응용프로그램(114-1)의 크기는 개시된 기능을 지원하기 위해 훨씬 더 커질 것이다. 또한 본 발명에 개시된 실시형태는 응용프로그램이 상이한 개발자에게 등록되더라도 응용프로그램(114-1 및 113)이 데이터를 교환할 수 있게 한다.

[0044] 도 2a는 개시된 실시형태와 일치하는 예시적인 시스템(200)의 개략도를 도시한다. 도시된 바와 같이 시스템(200)은 하나 이상의 비접촉식 카드(201), 하나 이상의 모바일 컴퓨터 디바이스(110) 및 인증 서버(220)를 포함한다. 비접촉식 카드(201)는 신용 카드, 직불 카드, ATM 카드, 기프트 카드 등과 같은 임의의 유형의 결제 카드를 나타낸다.

[0045] 비접촉식 카드(201)는 NFC, EMV 표준 또는 무선 통신의 다른 단거리 프로토콜을 통해 컴퓨터 디바이스(110)와 통신하도록 형상화된 무선 주파수 식별(RFID) 칩과 같은 하나 이상의 통신 인터페이스(209)를 포함할 수 있다. NFC가 예시적인 통신 프로토콜로 사용되었으나 본 발명은 EMV 표준, 블루투스 및/또는 Wi-Fi와 같은 다른 유형의 통신에도 동일하게 적용 가능하다. 인증 서버(220)는 서버, 워크스테이션, 컴퓨터 클러스터, 클라우드 컴퓨터 플랫폼, 가상화 컴퓨터 시스템 등과 같은 임의의 유형의 컴퓨터 디바이스를 나타낸다.

[0046] 도시된 바와 같이 비접촉식 카드의 메모리(202)는 애플릿(203), 카운터(204), 개인 키(205), 다양화 키(206) 및 고유 고객 식별자(ID)(207)를 포함한다. 애플릿(203)은 본 발명에 개시된 동작을 수행하도록 형상화된 실행 코드이다. 카운터(204), 개인 키(205), 다양화 키(206) 및 고객 ID(207)는 하기 더욱 상세히 설명되는 바와 같이 시스템(200)에서 보안을 제공하기 위해 사용된다.

- [0047] 언급된 바와 같이 비접촉식 카드(201)는 로컬 서버(115) 및 모바일 디바이스(110)의 보안을 강화하는데 사용될 수 있다. 예를 들어 디바이스(110)의 사용자는 응용프로그램(114-1)에서 계정 응용프로그램(113)으로부터의 데이터를 사용하기를 원할 수 있다. 따라서 도 2a는 계정 응용프로그램(114-1)이 계정 응용프로그램(113)으로 향하는 URL(125)을 생성하고 액세스 하는 실시형태를 도시한다. 그 후 OS(112)는 사용자의 계정에 대한 인증 자격 증명을 수신할 수 있는 계정 응용프로그램(113)을 열 수 있다. 그 후 계정 응용프로그램(113)은 비접촉식 카드(201)를 디바이스(110)에 탭하도록 사용자에게 지시할 수 있다.
- [0048] 일반적으로 비접촉식 카드(201)가 디바이스(110)의 통신 인터페이스(218) 예를 들어 카드 판독기/작성기의 통신 범위 내에 진입하면 비접촉식 카드(201)의 애플릿(203)은 비접촉식 카드(201)를 활성화 하기 위해 필요한 인증 프로세스의 일부로서 암호화된 데이터를 생성할 수 있다. 비접촉식 카드(201)와 모바일 디바이스(110) 사이의 NFC 데이터 전송을 가능하게 하기 위해, 비접촉식 카드(201)가 모바일 디바이스(110)의 통신 인터페이스(218)에 충분히 근접할 때 계정 응용프로그램(113)은 비접촉식 카드(201)와 통신할 수 있다.
- [0049] 통신 인터페이스(218)는 예를 들어 NFC, 블루투스, RFID 등을 통해 비접촉식 카드(201)의 통신 인터페이스(209)로부터 판독 및/또는 통신하도록 형상화될 수 있다. 따라서 예시적인 통신 인터페이스(218)는 NFC 통신 모듈, 블루투스 통신 모듈 및/또는 RFID 통신 모듈을 포함한다.
- [0050] 언급된 바와 같이 시스템(100)은 데이터를 보호하기 위해 키 다양화를 구현하도록 형상화 되며 이는 여기에서 키 다양화 기술로 지칭될 수 있다. 일반적으로 서버(220) 또는 다른 컴퓨터 디바이스 및 비접촉식 카드(201)는 마스터 키 또는 마스터 대칭 키라고도 하는 동일한 개인 키(205)를 제공받을 수 있다. 보다 상세하게는 각각의 비접촉식 카드(201)는 서버(220)에서 또는 서버(220)에 의해 관리되는 대응하는 쌍을 지니는 고유한 개인 키(205)로 프로그래밍 된다. 예를 들어 비접촉식 카드(201)가 제조될 때 고유한 개인 키(205)가 비접촉식 카드(201)의 메모리(202) 내에 저장될 수 있다.
- [0051] 유사하게 고유 개인 키(205)는 서버(220)의 계정 데이터(224) 내의 비접촉식 카드(201)와 연관된 고객의 기록 또는 프로파일로 저장될 수 있거나 및/또는 하드웨어 보안 모듈(HSM)(225)와 같은 다른 보안 위치에 저장될 수 있다. 개인 키(205)는 비접촉식 카드(201) 및 서버(220) 이외의 모든 당사자들로부터 비밀로 유지될 수 있으며 이에 의해 시스템(100)의 보안을 강화할 수 있다.
- [0052] 일부 실시형태에서 비접촉식 카드(201)의 애플릿(203)은 암호화 알고리즘에 대한 입력으로 개인 키(205) 및 데이터를 사용하여 데이터 예를 들어 고객 ID(207)를 암호화 및/또는 복호화 할 수 있다. 예를 들어 개인 키(205)로 고객 ID(207)를 암호화하면 암호화된 고객 ID가 생성될 수 있다. 유사하게 인증 서버(220)는 대응하는 개인 키(205)를 사용하여 비접촉식 카드(201)와 관련된 데이터를 암호화 및/또는 복호화 할 수 있다.
- [0053] 일부 실시형태에서 비접촉식 카드(201) 및 서버(220)의 카운터(204) 및/또는 개인 키(205)는 키 다양화를 사용하여 보안을 강화하기 위해 카운터(204)와 함께 사용될 수 있다. 카운터(204)는 주어진 비접촉식 카드(201)와 서버(220) 사이에서 동기화된 값을 포함한다. 카운터 값(204)은 비접촉식 카드(201)와 서버(220) 및/또는 비접촉식 카드(201)와 모바일 디바이스(110) 사이에서 데이터가 교환될 때마다 변경되는 숫자를 포함할 수 있다. (예를 들어 서버(220) 및/또는 모바일 디바이스(110)로 데이터를 전송할 준비를 할 때, 비접촉식 카드(201)의 애플릿(203)은 카운터 값(204)을 증가시킬 수 있다.
- [0054] 그 후 비접촉식 카드(201)는 출력으로 다양화 키(206)를 생성하는 암호화 알고리즘에 대한 입력으로 개인 키(205) 및 카운터 값(204)을 제공할 수 있다. 암호화 알고리즘은 암호화 알고리즘, 해시 기반 메시지 인증 코드(HMAC) 알고리즘, 암호 기반 메시지 인증 코드(CMAC) 알고리즘 등을 포함할 수 있다. 암호화 알고리즘의 비제한적인 예는 3DES 또는 AES128과 같은 대칭 암호화 알고리즘; HMAC-SHA-256과 같은 대칭 HMAC 알고리즘; 및 AES-CMAC와 같은 대칭 CMAC 알고리즘이 있다. 주요 다양화 기술의 예는 2018년 11월 29일자로 출원된 미국 특허출원 제16/205,119호에 더욱 상세히 개시되어 있다. 상기 언급된 특허출원은 그 전체로 본 발명에 참고문헌으로 통합된다.
- [0055] 키 다양화 예를 계속하면 비접촉식 카드(201)는 암호화 알고리즘에 대한 입력으로 다양화 키(206) 및 데이터를 사용하여 데이터 예를 들어 고객 ID(207) 및/또는 임의의 다른 데이터를 암호화할 수 있다. 예를 들어 다양화 키(206)로 고객 ID(207)를 암호화하면 암호화된 고객 ID(208)가 생성될 수 있다. 일단 생성되면 애플릿(203)은 암호화된 고객 ID(208)를 예를 들어 NFC를 통해 모바일 디바이스(110)로 전송할 수 있다. 그 후 계정 응용프로그램(113)은 암호화된 고객 ID(208)를 네트워크(230)를 통해 인증 서버(220)로 전송할 수 있다.
- [0056] 그 후 인증 응용프로그램(223)은 암호화된 데이터를 인증하려고 시도할 수 있다. 예를 들어 인증 응용프로그램

(223)은 서버(220)에 의해 저장된 개인 키(205)의 사본을 사용하여 암호화된 고객 ID(208)의 복호화를 시도할 수 있다. 다른 실시예에서 인증 응용프로그램(223)은 개인 키(205) 및 출력으로 다양화 키(206)를 생성하는 암호화 알고리즘에 대한 입력으로 카운터 값(204)을 제공할 수 있다. 생성된 다양화 키(206)는 암호화된 고객 ID(208)를 복호화하는데 사용될 수 있는 비접촉식 카드(201)의 다양화 키(206)에 대응할 수 있다. 따라서 인증 응용프로그램(223)은 암호화된 데이터를 성공적으로 복호화하여 암호화된 고객 ID(208)를 검증할 수 있다.

[0057] 예를 들어 언급된 바와 같이 고객 ID(207)는 암호화된 고객 ID(208)를 생성하는데 사용될 수 있다. 이러한 실시예에서 인증 응용프로그램(223)은 인증 서버(220)의 개인 키(205)를 사용하여 암호화된 고객 ID(208)를 복호화할 수 있다. 암호 복호화의 결과가 계정 데이터(224) 내의 계정과 연관된 고객 ID(207)를 산출하는 경우, 인증 응용프로그램(223)은 암호화된 고객 ID(208)를 검증한다. 인증 응용프로그램(223)이 암호화된 고객 ID(208)를 복호화 하여 예상 결과 예를 들어 비접촉식 카드(201)와 연관된 계정의 고객 ID(207)를 산출할 수 없는 경우, 인증 응용프로그램(223)은 암호화된 고객 ID(208)를 검증하지 않는다. 실패한 검증으로 인해 인증 응용프로그램(223)은 계정 응용프로그램(113)에 오류를 반송할 수 있으며 이는 로컬 서버(115)의 개시를 억제할 수 있다.

[0058] 사용된 복호화 기술에 관계없이 인증 응용프로그램(223)은 암호화된 고객 ID(208)를 성공적으로 복호화 함으로써, 예를 들어 결과 고객 ID(208)를 계정 데이터(224) 내에 저장된 고객 ID와 비교하여 맞/또는 키(205 및/또는 206)를 사용한 복호화가 성공했다는 표시에 기반하여 암호화된 고객 ID(207)를 검증할 수 있다. 키(205, 206)가 메모리(222) 내에 저장되는 것으로 도시되어 있으나 키(205, 206)는 보안 요소 및/또는 HSM(225)과 같은 다른 곳에 저장될 수 있다. 그러한 실시형태에서 보안 요소 및/또는 HSM(225)은 키(205 및/또는 206) 및 암호화 기능을 사용하여 암호화된 고객 ID(207)를 복호화할 수 있다. 유사하게 보안 요소 및/또는 HSM(225)은 전술한 바와 같이 개인 키(205) 및 카운터 값(204)에 기반하여 다양화 키(206)를 생성할 수 있다.

[0059] 도 2b는 인증 응용프로그램(223)이 암호화된 고객 ID(208)를 검증하는 실시형태를 도시한다. 도시된 바와 같이 인증 응용프로그램(223)은 계정 응용프로그램(113)에 검증(210)의 표시를 반송할 수 있다. 계정에 대한 검증(210) 및/또는 인증 자격증명의 수신에 기반하여, 계정 응용프로그램(113)은 로컬 서버(115)를 개시하도록 결정할 수 있다. 도 2c는 계정 응용프로그램(113)이 디바이스(110) 상에서 로컬 서버(115)를 개시한 실시형태를 도시한다.

[0060] 계정 응용프로그램(113)은 URL이 요청 응용프로그램(114-1)으로 향하는 로컬 서버(115)의 포트 번호를 포함하는 URL을 생성할 수 있다. 그 후 URL은 요청 응용프로그램(114-1)을 열어 응용프로그램(114-1)이 OS(112)의 백그라운드에서 실행되는 로컬 서버(115)와 연결을 설정할 수 있게 한다. 그 후 응용프로그램(114-1)은 계정 응용프로그램(113) 및/또는 서버(115)로부터 데이터를 수신할 수 있다.

[0061] 도 3a는 모바일 운영 체제에서 응용프로그램 간의 통신을 가능하게 하는 예시적인 실시형태를 도시하는 개략도(300)이다. 도시된 바와 같이 도 3a는 예시적인 응용프로그램(114)을 실행하는 모바일 디바이스(110)를 포함한다. 예를 들어 응용프로그램(114)은 사용자가 주문을 하고 결제 정보 또는 주문을 제공할 수 있게 하는 응용프로그램일 수 있다. 도시된 바와 같이 응용프로그램(114)의 그래픽 사용자 인터페이스(GUI)는 필드(301-305)를 지니는 결제 양식을 포함하며 여기서 필드(301)는 이름 필드, 필드(302)는 계좌 번호 필드, 필드(303)는 유효기한 필드, 필드(304)는 CVV 필드, 필드(305)는 주소 필드이다. 도시된 바와 같이 응용프로그램(114)은 다른 응용프로그램 예를 들어 계정 응용프로그램(113)으로부터의 데이터를 사용하여 체크아웃을 완료하기 위해 알림(309)를 선택하도록 명시하는 알림(309)을 출력할 수 있다.

[0062] 도 3b는 사용자가 알림(309)을 선택하는 실시형태를 도시한 개략도(310)이다. 이를 통해 응용프로그램(114)이 계정 응용프로그램(113)에 대한 URL(125)을 생성할 수 있으며 여기서 URL(125)은 응용프로그램(114)의 식별자를 파라미터로 포함한다. 일단 열리면 URL(125)은 계정 응용프로그램(113)이 OS(112)의 포그라운드에서 열리도록 한다. 도 3b에 도시된 바와 같이 계정 응용프로그램(113)은 인증을 진행하기 위해 비접촉식 카드(201)를 모바일 디바이스(110)에 탭 하도록 명시하는 알림(306)을 출력할 수 있다.

[0063] 언급된 바와 같이 계정 응용프로그램(113)은 카드(201)의 탭 이전 및/또는 이후에 인증 자격증명을 제공하도록 사용자에게 지시할 수 있다(도시되지 않음). 비접촉식 카드(201)가 모바일 디바이스(110)에 탭 되면 상기 개시된 바와 같은 암호화된 데이터 예를 들어 암호화된 고객 ID(208)를 생성하기 위한 표시를 계정 응용프로그램(113)은 통신 인터페이스(218)를 통해 비접촉식 카드(201)에 전송하고 계정 응용프로그램(113)에 암호화된 데이터를 전송한다.

[0064] 일단 수신되면 계정 응용프로그램(113)은 암호화된 데이터를 서버(220)에 전송할 수 있고 여기서 인증 응용프로그램

그램(223)은 상기 개시된 바와 같이 키 다양화를 사용하여 암호화된 데이터를 검증한다. 그 후 인증 응용프로그램(223)은 검증의 표시를 계정 응용프로그램(113)에 전송할 수 있다. 또한 인증 응용프로그램(223)은 계정 데이터(224)로부터의 암호화된 데이터 예를 들어 계정 소유자 이름, 청구 주소, 배송 주소 등의 검증에 기반하여 임의의 유형의 데이터를 계정 응용프로그램(113)으로 전송할 수 있다.

[0065] 서버(220)가 암호화된 데이터를 검증했다고 명시하는 표시를 계정 응용프로그램(113)이 표시를 수신하면 계정 응용프로그램(113)은 디바이스(110)에서 로컬 서버(115)를 개시할 수 있다. 그 후 계정 응용프로그램(113)은 요청 응용프로그램(114)으로 향하는 URL(126)을 생성할 수 있으며 여기서 URL(126)의 파라미터는 로컬 서버(115)의 포트 번호를 포함한다. 그러면 응용프로그램(114)은 상기 개시된 바와 같이 로컬 서버(115)에 연결하고 관련 데이터 예를 들어 이름, 주소, 결제 카드 정보, 유효기한 및 CVV를 요청할 수 있다.

[0066] 도 3c는 응용프로그램(114)이 로컬 서버(115)로부터 요청된 데이터를 수신하는 실시형태를 나타내는 개략도(320)이다. 도시된 바와 같이 응용프로그램(114)은 사용자의 이름을 이름 필드(201)에, 계좌 번호를 계좌 번호 필드(302)에, 유효기한을 유효기한 필드(303)에, CVV를 CVV 필드(304)에 및 주소를 주소 필드(305)에 자동 채울 수 있다. 그 후 사용자는 버튼(311)을 사용하여 구매를 완료할 수 있다. 또한 필드(301-305)에 채워진 데이터는 응용프로그램(114)과 연관된 사용자 프로파일 내에 저장될 수 있다.

[0067] 개시된 실시형태에 대한 동작은 다음 도면을 참조하여 추가로 설명될 수 있다. 일부 도면에는 로직 흐름이 포함될 수 있다. 본 발명에 제시된 그러한 도면은 특정 로직 흐름을 포함할 수 있으나 로직 흐름은 단지 본 발명에 개시된 바와 같은 일반적인 기능이 구현될 수 있는 방법의 일례를 제공하는 것으로 이해된다. 또한 주어진 로직 흐름은 달리 명시되지 않는 한 반드시 제시된 순서대로 실행될 필요는 없다. 또한 주어진 로직 흐름은 하드웨어 요소, 프로세서에 의해 실행되는 소프트웨어 요소 또는 이들의 임의의 조합에 의해 구현될 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다.

[0068] 도 4는 로직 흐름(400)의 실시형태를 도시한다. 로직 흐름(400)은 본 발명에 개시된 하나 이상의 실시형태에 의해 실행되는 동작의 일부 또는 전부를 나타낼 수 있다. 예를 들어 로직 흐름(400)은 모바일 운영 체제에서 응용프로그램 간의 통신을 가능하게 하는 동작의 일부 또는 전부를 포함할 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다.

[0069] 도시된 바와 같이 로직 흐름(400)은 디바이스(110)가 OS(112)의 포그라운드에서 제1 응용프로그램을 출력하는 블록 405에서 시작한다. 예를 들어 제1 응용프로그램은 승차 공유 응용프로그램일 수 있는 응용프로그램(114-1)일 수 있다. 블록 410에서 제1 응용프로그램은 제2 응용프로그램으로부터 데이터를 수신하도록 명시하는 표시를 수신할 수 있다. 제2 응용프로그램은 계정 응용프로그램(113)일 수 있다. 예를 들어 승차 공유 응용프로그램을 사용하여 운송 서비스를 주문하려고 시도하는 동안, 사용자는 계정 응용프로그램(113)으로부터 결제 데이터를 가져오도록 명시할 수 있다. 블록 415에서 제1 응용프로그램은 제2 응용프로그램으로 향하는 제1 URL을 생성한다. 제1 URL은 파라미터로 제1 응용프로그램의 고유 식별자를 포함할 수 있다.

[0070] 블록 420에서 OS(112)는 제1 URL에 액세스 할 수 있게 하여 이에 따라 OS(112)의 포그라운드에서 제2 응용프로그램 예를 들어 계정 응용프로그램(113)을 연다. 블록 425에서 제2 응용프로그램은 비접촉식 카드(201)로부터 계정에 대한 인증 자격증명 및/또는 암호화된 데이터를 선택적으로 수신할 수 있다. 예를 들어 사용자는 생체 자격증명을 제공하고 비접촉식 카드(201)를 디바이스(110)에 탭 할 수 있으며 이는 카드(201)가 암호화된 데이터를 생성하고 전송하게 한다. 블록 430에서 제2 응용프로그램은 인증 서버(220)로부터 암호화된 데이터의 검증을 수신한다. 블록 435에서 제2 응용프로그램은 명시된 포트에서 모바일 디바이스(110) 상의 로컬 서버(115)를 생성한다.

[0071] 블록 440에서 제2 응용프로그램은 제2 URL을 생성한다. 제2 URL은 제1 응용프로그램으로 향할 수 있다. 제2 URL의 파라미터는 로컬 서버(115)의 포트 번호를 포함할 수 있다. 블록 445에서 제2 응용프로그램은 로컬 서버(115) 및/또는 제2 응용프로그램을 OS(112)에 백그라운드 태스크로서 등록함으로써 로컬 서버(115)가 및/또는 제2 응용프로그램이 OS(112)의 백그라운드에서 일정 시간 동안 실행될 수 있게 한다. 블록 450에서 제2 URL은 OS(112)의 포그라운드에서 제1 응용프로그램을 열기 위해 액세스 되고 로컬 서버(115) 및/또는 제2 응용프로그램이 OS(112)의 백그라운드에서 계속 실행된다.

[0072] 블록 455에서 제1 응용프로그램은 로컬 서버(115)와의 연결을 설정한다. 블록 460에서 제1 응용프로그램은 로컬 서버(115)로부터 데이터를 요청하고 수신한다. 블록 465에서 제1 응용프로그램은 수신된 데이터를 처리한다. 예를 들어 데이터는 계정 응용프로그램(113)으로부터의 결제 정보일 수 있으며 승차 공유 응용프로그램(114)은 결

제 정보를 결제 양식에 자동 채울 수 있다. 그 후 사용자는 자동 채우기 된 결제 정보를 사용하여 승차 공유 응용프로그램에서 운송 요청을 완료할 수 있다.

[0073] 도 5는 로직 흐름(500)의 실시형태를 도시한다. 로직 흐름(500)은 본 발명에 개시된 하나 이상의 실시형태에 의해 실행되는 동작의 일부 또는 전부를 나타낼 수 있다. 예를 들어 로직 흐름(500)은 비접촉식 카드(201)에 의해 생성된 암호화된 데이터의 검증에 기반하여 모바일 운영 체제에서 응용프로그램 사이의 통신을 가능하게 하는 동작의 일부 또는 전부를 포함할 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다.

[0074] 도시된 바와 같이 로직 흐름(500)은 블록 505에서 시작하며 여기서 사용자는 비접촉식 카드(201)가 암호화된 데이터 예를 들어 암호화된 고객 ID(208)를 생성 및 전송하게 하기 위해 비접촉식 카드(201)를 모바일 디바이스(110)에 탭 한다. 블록 510에서 비접촉식 카드(201)의 애플릿(203)은 비접촉식 카드의 메모리(202) 내에 저장된 카운터 값(204) 및 마스터 키(205)를 암호화함으로써 다양화 키(206)를 생성한다. 일부 실시형태에서 애플릿(203)은 암호화 이전에 카운터(204)를 증가시킬 수 있다. 블록 515에서 비접촉식 카드(201)는 다양화 키(206) 및 암호화 알고리즘을 사용하여 데이터 예를 들어 고객 식별자(207)를 암호화하여 암호화된 데이터 예를 들어 암호화된 고객 ID(208)를 생성한다.

[0075] 블록 520에서 비접촉식 카드(201)는 예를 들어 NFC를 사용하여 모바일 디바이스(110)의 계정 응용프로그램(113)에 암호화된 데이터를 전송할 수 있다. 블록 525에서 모바일 디바이스(110)의 계정 응용프로그램(113)은 비접촉식 카드(201)로부터 수신된 데이터를 서버(220)의 인증 응용프로그램(223)으로 전송할 수 있다. 블록 530에서 서버(220)의 인증 응용프로그램(223)은 암호화 알고리즘에 대한 입력으로 마스터 키(205) 및 카운터 값(204)을 사용하여 다양화 키(206)를 생성할 수 있다. 하나의 실시형태에서 인증 응용프로그램(223)은 비접촉식 카드(201)의 메모리 내에 있는 카운터 값(204)과 동기화하기 위해 서버(220)의 카운터 값(204)을 증가시킨다.

[0076] 블록 535에서 인증 응용프로그램(223)은 다양화 키(206)를 사용하여 모바일 디바이스(110)를 통해 비접촉식 카드(201)로부터 수신된 암호화된 고객 ID(208)를 복호화 한다. 이를 통해 적어도 고객 ID(207)를 산출할 수 있다. 고객 ID(207)를 산출함으로써 인증 응용프로그램(223)은 블록 540에서 비접촉식 카드(201)로부터 수신된 데이터를 검증할 수 있다.

[0077] 예를 들어 인증 응용프로그램(223)은 고객 ID(207)를 계정 데이터(224)의 연관된 계정에 대한 고객 식별자와 비교하고 매치에 기반하여 데이터를 검증할 수 있다. 블록 545에서 인증 응용프로그램(223)은 암호화된 데이터가 검증되었음을 명시하는 표시를 계정 응용프로그램(113)에 전송할 수 있다. 블록 550에서 계정 응용프로그램(113)은 블록 545에서 서버로부터 표시를 수신하는 것에 응답하여 로컬 서버(115)를 개시할 수 있다.

[0078] 도 6a는 신용 카드, 직불 카드 및/또는 기프트 카드와 같은 결제 카드를 포함할 수 있는 비접촉식 카드(201)를 도시한다. 도시된 바와 같이 비접촉식 카드(201)는 카드(201)의 전면 또는 후면 상에 표시된 서비스 공급자(602)에 의해 발행될 수 있다. 일부 실시예에서 비접촉식 카드(201)는 결제 카드와 관련되지 않으며 신분증을 제한없이 포함할 수 있다.

[0079] 일부 실시예에서 지불 카드는 이중 인터페이스 비접촉식 결제 카드를 포함할 수 있다. 비접촉식 카드(201)는 플라스틱, 금속 및 기타 재료로 구성된 단일 층 또는 하나 이상의 적층된 층을 포함할 수 있는 기판(610)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.

[0080] 일부 실시예에서 비접촉식 카드(201)는 ISO/IEC 7810 표준의 ID-1 형식을 준수하는 물리적 특성을 지닐 수 있으며 그렇지 않으면 비접촉식 카드는 ISO/IEC 14443 표준을 준수할 수 있다. 그러나 본 발명에 따른 비접촉식 카드(201)는 상이한 특성을 지닐 수 있으며 본 발명은 비접촉식 카드가 결제 카드 내에서 구현될 필요가 없는 것으로 이해된다.

[0081] 또한 비접촉식 카드(201)는 카드의 전면 및/또는 후면에 표시된 식별 정보(615) 및 접촉 패드(620)를 포함할 수 있다. 접촉 패드(620)는 모바일 디바이스(110), 사용자 디바이스, 스마트폰, 랩톱, 데스크톱 또는 태블릿 컴퓨터와 같은 다른 통신 디바이스와 접촉을 설정하도록 형상화 된다. 또한 비접촉식 카드(201)는 처리 회로, 안테나 및 도 6a에 도시되지 않은 다른 컴포넌트를 포함할 수 있다. 이들 컴포넌트는 접촉 패드(620) 후면에 또는 기판(610) 상의 다른 곳에 위치할 수 있다. 비접촉식 카드(201)는 또한 카드의 후면에 위치될 수 있는 자기 스트립 또는 테이프를 포함할 수 있다(도 6a에 도시되지 않음).

[0082] 도 6b에 도시된 바와 같이 비접촉식 카드(201)의 접촉 패드(620)는 마이크로프로세서(630) 및 메모리(202)를 포함하는 정보를 저장 및 처리하기 위한 처리 회로(625)를 포함할 수 있다. 처리 회로(625)는 본 발명에 개시된

기능을 수행하기 위한 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.

[0083] 메모리(202)는 읽기 전용 메모리, 1회 쓰기 다회 읽기 메모리 또는 읽기/쓰기 메모리, 예를 들어 RAM, ROM 및 EEPROM일 수 있으며 비접촉식 카드(201)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 출고된 후 특정 시점에 프로그래밍 될 수 있다. 메모리는 한 번 프로그램 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 후에도 여러 번 읽을 수 있다.

[0084] 메모리(202)는 하나 이상의 애플릿(203), 카운터 값(204), 개인 키(205), 다양화 키(206) 및 하나 이상의 고객 ID(207)를 저장하도록 형상화될 수 있다. 하나 이상의 애플릿(203)은 Java® 카드 애플릿과 같이 하나 이상의 비접촉식 카드에서 실행되도록 형상화된 하나 이상의 소프트웨어 응용프로그램을 포함할 수 있다. 그러나 애플릿(203)은 자바 카드 애플릿으로 제한되지 않으며 그 대신 비접촉식 카드 또는 제한된 메모리를 지니는 다른 디바이스 상에서 작동 가능한 임의의 소프트웨어 응용프로그램일 수 있는 것으로 이해된다. 고객 ID(207)는 비접촉식 카드(201)의 사용자에게 할당된 고유한 영숫자 식별자를 포함할 수 있으며 식별자는 비접촉식 카드의 사용자를 다른 비접촉식 카드 사용자와 구별할 수 있다.

[0085] 일부 실시예에서 고객 ID(207)는 고객 및 그 고객에게 할당된 계정 모두를 식별할 수 있고 고객의 계정과 연관된 비접촉식 카드를 추가로 식별할 수 있다. 일부 실시형태에서 애플릿(203)은 암호화 알고리즘에 대한 입력으로 고객 ID(207)를 키(205 및/또는 206)와 함께 사용하여 고객 ID(207)를 암호화할 수 있다. 유사하게 애플릿(203)은 암호화된 고객 ID(207)를 파라미터로 포함하는 URL을 구성할 수 있다.

[0086] 전술한 실시형태의 프로세서 및 메모리 엘리먼트는 접촉 패드를 참조하여 설명되었으나 본 발명은 이에 제한되지 않는다. 이들 엘리먼트는 패드(620) 외부에 구현되거나 패드로부터 완전히 분리될 수 있거나, 접촉 패드(620) 내에 위치한 프로세서(630) 및 메모리(202) 엘리먼트 이외에 추가 엘리먼트로서 구현될 수 있는 것으로 이해된다.

[0087] 일부 실시예에서 비접촉식 카드(201)는 하나 이상의 안테나(655)를 포함할 수 있다. 하나 이상의 안테나(655)는 비접촉식 카드(201) 내에 그리고 접촉 패드(620)의 처리 회로(625) 주위에 배치될 수 있다. 예를 들어 하나 이상의 안테나는(655)는 처리 회로(625)와 통합될 수 있고 하나 이상의 안테나(655)는 외부 부스터 코일과 함께 사용될 수 있다. 다른 예에서 하나 이상의 안테나(655)는 접촉 패드(620) 및 처리 회로(625)의 외부에 있을 수 있다.

[0088] 하나의 실시형태에서 비접촉식 카드(201)의 코일은 공심 변압기의 2차로서 작용할 수 있다. 단말은 전력 또는 진폭 변조를 차단함으로써 비접촉식 카드(201)와 통신할 수 있다. 비접촉식 카드(201)는 하나 이상의 커패시터를 통해 기능적으로 유지될 수 있는 비접촉식 카드의 전원 연결의 갭을 사용하여 단말기에서 전송된 데이터를 추론할 수 있다. 비접촉식 카드(201)는 비접촉식 카드의 코일 또는 부하 변조에 대한 부하를 전환함으로써 다시 통신할 수 있다. 부하 변조는 간섭을 통해 단말 코일에서 감지될 수 있다. 보다 일반적으로 안테나(655), 처리 회로(625) 및/또는 메모리(202)를 사용하여 비접촉식 카드(201)는 NFC, 블루투스 및/또는 Wi-Fi 통신을 통해 통신하기 위한 통신 인터페이스를 제공한다.

[0089] 위에서 설명된 바와 같이 비접촉식 카드(201)는 스마트 카드 또는 JavaCard와 같은 제한된 메모리를 지니는 다른 디바이스 상에서 작동 가능한 소프트웨어 플랫폼에 구축될 수 있으며 하나 이상의 응용프로그램 또는 애플릿이 안전하게 실행될 수 있다. 다양한 모바일 응용프로그램 기반 사용 사례에서 다중 요인 인증(MFA)을 위한 일회용 암호(OTP)를 제공하기 위해 애플릿을 비접촉식 카드에 추가할 수 있다. 애플릿은 모바일 NFC 판독기 예를 들어 디바이스(110)의 통신 인터페이스(218)와 같은 판독기로부터의 근거리 데이터 교환 요청과 같은 하나 이상의 요청에 응답하고 NDEF 텍스트 태그로 인코딩된 암호화 보안 OTP 예를 들어 암호화된 고객 ID를 포함하는 NDEF 메시지를 생성하도록 형상화 될 수 있다.

[0090] 도 7은 상기 개시된 바와 같은 다양한 실시형태를 구현하기에 적합할 수 있는 컴퓨터 시스템(702)을 포함하는 예시적인 컴퓨터 아키텍처(700)의 실시형태를 도시한다. 다양한 실시형태에서 컴퓨터 아키텍처(700)는 전자 디바이스를 포함하거나 전자 디바이스의 일부로서 구현될 수 있다. 일부 실시형태에서 컴퓨터 아키텍처(700)는 예를 들어 시스템(100 및/또는 200)의 하나 이상의 컴포넌트를 구현하는 시스템을 대표할 수 있다. 일부 실시형태

에서 컴퓨터 시스템(702)은 예를 들어 비접촉식 카드(201), 모바일 디바이스(110) 및 인증 서버(220)를 대표할 수 있다. 실시형태는 이러한 맥락으로 제한되지 않는다. 보다 일반적으로 컴퓨터 아키텍처(700)는 도 1 내지 도 6b를 참조하여 본 발명에 개시된 모든 로직, 응용프로그램, 시스템, 방법, 기기 및 기능을 구현하도록 형성된다.

[0091] 본 발명에서 사용된 "시스템" 및 "컴포넌트" 및 "모듈"은 하드웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어 또는 실행 중인 소프트웨어인 컴퓨터 관련 엔티티를 의미한다. 예를 들어 컴포넌트는 컴퓨터 프로세서 상에서 실행 중인 프로세스, 컴퓨터 프로세서, 하드 디스크 드라이브, 다중 저장 드라이브(광학 및/또는 자기 저장 매체), 개체, 실행 파일, 실행 스레드, 프로그램 및/또는 컴퓨터일 수 있으나 이에 제한되지 않는다. 예를 들어 서버에서 실행되는 응용프로그램과 서버 모두 컴포넌트가 될 수 있다.

[0092] 하나 이상의 컴포넌트는 프로세스 및/또는 실행 스레드 내에 상주할 수 있으며 컴포넌트는 하나의 컴퓨터에 국한되거나 2 이상의 컴퓨터 간에 분산될 수 있다. 또한 컴포넌트는 동작을 조정하기 위해 다양한 유형의 통신 매체에 의해 서로 통신 가능하게 결합될 수 있다. 조정에는 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 데이터 메시지를 대안적으로 사용할 수 있다. 이러한 데이터 메시지는 다양한 연결을 통해 전송될 수 있다. 예시적인 연결은 병렬 인터페이스, 직렬 인터페이스 및 버스 인터페이스를 포함한다.

[0093] 컴퓨터 시스템(702)은 하나 이상의 프로세서, 멀티 코어 프로세서, 코프로세서, 메모리 유니트, 칩셋, 컨트롤러, 주변기기, 인터페이스, 발진기, 타이밍 디바이스, 비디오 카드, 오디오 카드, 멀티미디어 입력/출력(I/O) 컴포넌트, 전원 공급 디바이스 등과 같은 다양한 공통 컴퓨터 엘리먼트를 포함한다. 그러나 실시형태는 컴퓨터 시스템(702)에 의한 구현으로 제한되지 않는다.

[0094] 도 7에 도시된 바와 같이 컴퓨터 시스템(702)은 프로세서(704), 시스템 메모리(706) 및 시스템 버스(708)를 포함한다. 프로세서(704)는 AMD® Athlon®, Duron® 및 Opteron® 프로세서; ARM® 응용프로그램, 임베디드 및 보안 프로세서; IBM® 및 Motorola® DragonBall® 및 PowerPC® 프로세서; IBM 및 Sony® Cell 프로세서; Intel® Celeron®, Core®, Core (2) Duo®, Itanium®, Pentium®, Xeon® 및 XScale® 프로세서; 및 유사한 프로세서를 제한 없이 포함하는 임의의 다양한 상업적으로 이용 가능한 컴퓨터 프로세서일 수 있다. 듀얼 마이크로프로세서, 멀티 코어 프로세서 및 기타 멀티 프로세서 아키텍처가 프로세서(704)로 사용될 수도 있다.

[0095] 시스템 버스(708)는 프로세서(704)에 대한 시스템 메모리(706)를 포함하지만 이에 한정되지 않는 시스템 컴포넌트에 대한 인터페이스를 제공한다. 시스템 버스(708)는 다양한 상업적으로 이용 가능한 버스 아키텍처를 사용하여 메모리 컨트롤러 존재 또는 부재 하에 메모리 버스, 주변기기 버스 및 로컬 버스에 더욱 상호연결될 수 있는 여러 유형의 버스 구조 중 임의의 것일 수 있다. 인터페이스 어댑터는 슬롯 아키텍처를 통해 시스템 버스(708)에 연결할 수 있다. 슬롯 아키텍처의 예에는 가속 그래픽 포트(AGP), 카드 버스, (확장) 산업 표준 아키텍처((E)ISA), 마이크로 채널 아키텍처(MCA), NuBus, 주변기기 컴포넌트 상호연결(확장)(PCI(X)), PCI 익스프레스, 개인용 컴퓨터 메모리 카드 국제 협회(PCMCIA) 등이 포함될 수 있으나 이에 한정되지 않는다.

[0096] 시스템 메모리(706)는 읽기 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 동적 RAM(DRAM), 더블 데이터 레이트 DRAM(DDRDRAM), 동기식 DRAM(SDRAM), 정적 RAM(SRAM), 프로그래밍 가능한 ROM(PROM), 지울 수 있는 프로그래밍 가능한 ROM(EPROM), 전기적으로 지울 수 있는 프로그래밍 가능한 ROM(EEPROM), 플래시 메모리(예를 들어 하나 또는 더 많은 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, 복수 배열 독립 디스크(RAID) 드라이브, USD 메모리, 고체 상태 드라이브(SSD)와 같은 고체 상태 메모리 디바이스 및 정보 저장에 적합한 다른 유형의 저장 매체와 같은 하나 이상의 고속 메모리 유니트의 형태로 다양한 유형의 컴퓨터 관독가능 저장 매체를 포함할 수 있다.

[0097] 도 7에 도시된 예시된 실시형태에서 시스템 메모리(706)는 비휘발성 메모리(710) 및/또는 휘발성 메모리(712)를 포함할 수 있다. 기본 입/출력 시스템(BIOS)은 비휘발성 메모리(710) 내에 저장될 수 있다.

[0098] 컴퓨터 시스템(702)은 내부(또는 외부) 하드 디스크 드라이브(HDD)(714), 이동식 자기 디스크(718)로부터 읽거나 이에 쓰기 위한 자기 플로피 디스크 드라이브(FDD)(716), 이동식 광 디스크(722)(예를 들어 CD-ROM 또는 DVD)로부터 읽거나 이에 쓰기 위한 광 디스크 드라이브(720)를 포함하는 하나 이상의 저속 메모리 유니트의 형태로 다양한 유형의 컴퓨터 관독 가능 저장 매체를 포함할 수 있다. HDD(714), FDD(716) 및 광 디스크 드라이브

(720)는 각각 HDD 인터페이스(724), FDD 인터페이스(726) 및 광 드라이브 인터페이스(728)에 의해 시스템 버스(708)에 연결될 수 있다. 외부 드라이브 구현을 위한 HDD 인터페이스(724)는 범용 직렬 버스(USB) 및 IEEE 1394 인터페이스 기술 중 적어도 하나 또는 모두를 포함할 수 있다. 컴퓨터 시스템(702)은 일반적으로 도 1 내지 도 6b를 참조하여 본 발명에 개시된 모든 로직, 시스템, 방법, 디바이스 및 기능을 구현하도록 형성된다.

[0099] 드라이브 및 관련 컴퓨터 판독가능 매체는 데이터, 데이터 구조, 컴퓨터 판독 가능 명령어, 컴퓨터 실행 가능 명령어 등의 휘발성 및/또는 비휘발성 저장소를 제공한다. 예를 들어 운영 체제(730), 하나 이상의 응용프로그램 프로그램(732), 다른 프로그램 모듈(734) 및 프로그램 데이터(736)를 포함하는 다수의 프로그램 모듈이 드라이브 및 메모리 유닛(710, 712) 내에 저장될 수 있다. 하나의 실시형태에서 하나 이상의 어플리케이션 프로그램(2032), 다른 프로그램 모듈(734) 및 프로그램 데이터(736)는 예를 들어 시스템(100, 200)의 다양한 응용프로그램 및/또는 컴포넌트를 포함할 수 있다. 예를 들어 애플릿(203), 카운터(204), 개인 키(205), 다양화 키(206), 고객 ID(207), 운영 체제(112), 계정 응용프로그램(113), 기타 응용프로그램(114), 인증 응용프로그램(223), 계정 데이터(224) 및/또는 암호화된 고객 ID(208)를 포함할 수 있다.

[0100] 사용자는 하나 이상의 유선/무선 입력 디바이스, 예를 들어 키보드(738) 및 마우스(740)와 같은 포인팅 디바이스를 통해 명령어 및 정보를 컴퓨터 시스템(702)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. 이들 및 다른 입력 디바이스는 종종 시스템 버스(708)에 연결된 입력 디바이스 인터페이스(742)를 통해 프로세서(704)에 연결되지만 병렬 포트, IEEE 1394 직렬 포트, 게임 포트, USB 포트, IR 인터페이스 등과 같은 다른 인터페이스에 의해 연결될 수도 있다.

[0101] 모니터(744) 또는 다른 유형의 디스플레이 디바이스 또한 비디오 어댑터(746)와 같은 인터페이스를 통해 시스템 버스(708)에 연결된다. 모니터(744)는 컴퓨터 시스템(702)의 내부 또는 외부에 있을 수 있다. 모니터(744) 외에 컴퓨터에는 일반적으로 스피커, 프린터 등과 같은 기타 주변 출력 디바이스가 포함된다.

[0102] 컴퓨터 시스템(702)은 원격 컴퓨터(748)와 같은 하나 이상의 원격 컴퓨터에 대한 유선 및/또는 무선 통신을 통한 논리적 연결을 사용하여 네트워크 환경에서 동작할 수 있다. 원격 컴퓨터(748)는 워크스테이션, 서버 컴퓨터, 라우터, 개인용 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서 기반 엔터테인먼트 기기, 피어 디바이스 또는 기타 공통 네트워크 노드를 포함하며 일반적으로 컴퓨터 시스템(702)과 관련하여 설명된 많은 또는 모든 엘리먼트를 포함하지만 간결함을 위해 메모리/저장 디바이스(750)만이 도시되어 있다.

[0103] 도시된 논리적 연결은 근거리 네트워크(LAN)(752) 및/또는 더 큰 네트워크, 예를 들어 광역 네트워크(WAN)(754)에 대한 유무선 연결을 포함한다. 이러한 LAN 및 WAN 네트워크 환경은 사무실과 회사에서 일반적이며, 인터넷과 같은 글로벌 통신 네트워크에 연결할 수 있는 인트라넷과 같은 전기업적 컴퓨터 네트워크를 용이하게 한다. 실시형태에서 도 2의 네트워크(230)는 LAN(752) 및 WAN(754) 중 하나 이상이다.

[0104] LAN 네트워크 환경에서 사용될 때, 컴퓨터 시스템(702)은 유선 및/또는 무선 통신 네트워크 인터페이스 또는 어댑터(756)를 통해 LAN(752)에 연결된다. 어댑터(756)는 LAN(752)으로의 유선 및/또는 무선 통신을 용이하게 할 수 있으며 이는 또한 어댑터(756)의 무선 기능과 통신하기 위해 그 위에 배치된 무선 액세스 포인트를 포함한다.

[0105] WAN 네트워크 환경에서 사용될 때, 컴퓨터 시스템(702)은 모뎀(758)을 포함할 수 있거나 WAN(754) 상의 통신 서버에 연결되거나 인터넷과 같이 WAN(754)을 통한 통신을 설정하기 위한 다른 수단을 지닐 수 있다. 내부 또는 외부 및 유선 및/또는 무선 디바이스일 수 있는 모뎀(758)은 입력 디바이스 인터페이스(742)를 통해 시스템 버스(708)에 연결된다. 네트워크 환경에서 컴퓨터 시스템(702) 또는 그 일부와 관련하여 도시된 프로그램 모듈은 원격 메모리/저장 디바이스(750)에 저장될 수 있다. 도시된 네트워크 연결은 예시적이며 컴퓨터 사이에 통신 링크를 설정하는 다른 수단이 사용될 수 있는 것으로 이해된다.

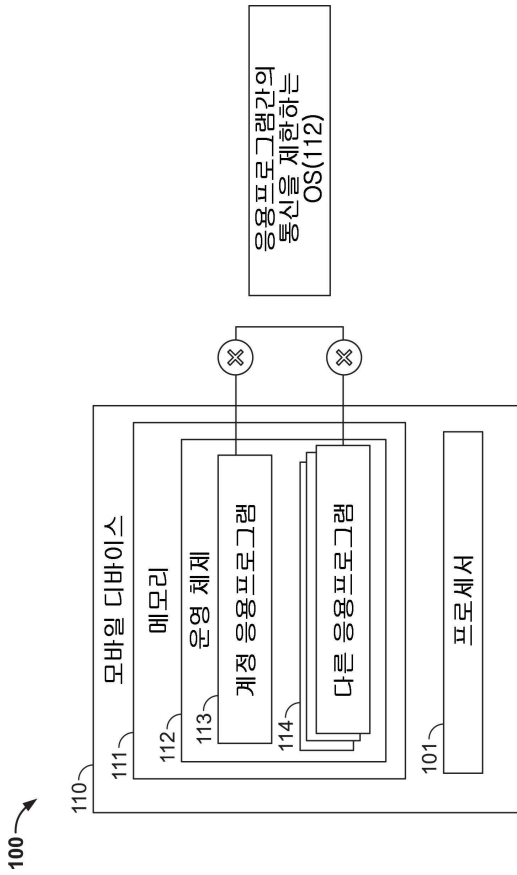
[0106] 컴퓨터 시스템(702)은 무선 통신 예를 들어 IEEE 802.16 무선 변조 기술에서 작동 가능하게 배치된 무선 디바이스와 같은 IEEE 802 계열 표준을 사용하여 유선 및 무선 디바이스 또는 엔티티와 통신하도록 작동 가능하다. 여기에는 최소한 Wi-Fi(또는 Wireless Fidelity), WiMax 및 Bluetooth™ 무선 기술 등이 포함된다. 따라서 통신은 기존 네트워크에서와 같이 미리 정의된 구조이거나 단순히 2 이상의 디바이스 간의 임시 통신일 수 있다. Wi-Fi 네트워크는 IEEE 802.11x(a, b, g, n 등)라는 무선 기술을 사용하여 안전하고 안정적이며 빠른 무선 연결을 제공한다. Wi-Fi 네트워크는 컴퓨터를 상호간에 연결하고 인터넷에 연결하고 IEEE 802.3 관련 미디어 및 기

능을 사용하는 유선 네트워크에 연결하는 데 사용할 수 있다.

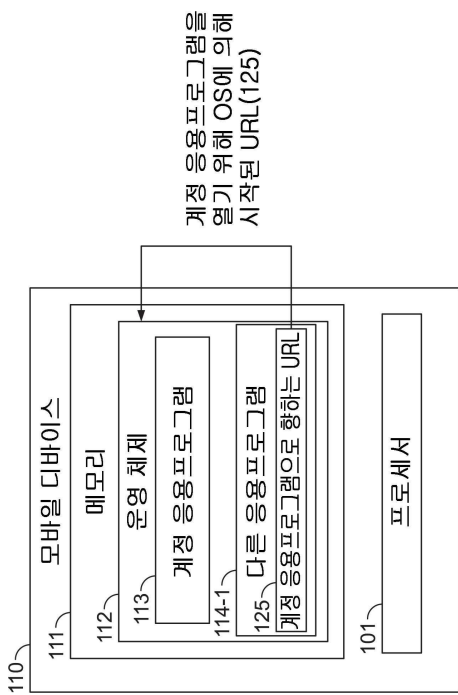
- [0107] 다양한 실시형태는 하드웨어 엘리먼트, 소프트웨어 엘리먼트 또는 이들의 조합을 사용하여 구현될 수 있다. 하드웨어 엘리먼트의 예로는 프로세서, 마이크로프로세서, 회로, 회로 엘리먼트 예를 들어 트랜지스터, 레지스터, 커패시터, 인덕터 등, 집적 회로, 주문형 집적 회로(ASIC), 프로그램 가능 논리 디바이스(PLD), 디지털 신호 프로세서(DSP), 필드 프로그램가능 게이트 어레이(FPGA), 논리 게이트, 레지스터, 반도체 디바이스, 칩, 마이크로 칩, 칩셋 등을 포함할 수 있다. 소프트웨어의 예에는 소프트웨어 컴포넌트, 프로그램, 응용프로그램, 컴퓨터 프로그램, 어플리케이션 프로그램, 시스템 프로그램, 기계 프로그램, 운영 체제 소프트웨어, 미들웨어, 펌웨어, 소프트웨어 모듈, 루틴, 서브루틴, 기능, 방법, 절차, 소프트웨어 인터페이스, 어플리케이션 프로그램 인터페이스(API), 명령어 세트, 컴퓨팅 코드, 컴퓨터 코드, 코드 세그먼트, 컴퓨터 코드 세그먼트, 단어, 값, 기호 또는 이들의 조합을 포함할 수 있다.
- [0108] 실시형태가 하드웨어 엘리먼트 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 엘리먼트에 따라 상이할 수 있다.
- [0109] 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 발명에 설명된 기술을 수행하기 위한 로직을 제조하게 한다. "IP 코어"로 알려진 이러한 표현은 유형적이고 기계 판독 가능 매체에 저장될 수 있으며 다양한 고객 또는 제조 시설에 공급되어 로직 또는 프로세서를 만드는 제조 기계에 로드될 수 있다.
- [0110] 일부 실시형태는 예를 들어 기계에 의해 실행되는 경우 기계가 본 실시형태에 따른 방법 및/또는 동작을 수행할 수 있게 하는 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 적절한 조합을 사용하여 구현될 수 있다.
- [0111] 기계 판독 가능 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 있는 또는 지울 수 없는 매체, 기록 가능 또는 재기록 가능 매체, 디지털 또는 아날로그 매체, 하드 디스크, 플로피 디스크, 읽기 전용 메모리 콤팩트 디스크(CD-ROM), 기록 가능 콤팩트 디스크(CD-R), 재기록 가능 콤팩트 디스크(CD-RW), 광 디스크, 자기 매체, 광자기 매체, 이동식 메모리 카드 또는 디스크, 다양한 유형의 디지털 다목적 디스크(DVD), 테이프, 카세트 등을 포함할 수 있다.
- [0112] 명령어는 소스 코드, 컴파일된 코드, 해석된 코드, 실행 가능한 코드, 정적 코드, 동적 코드, 암호화된 코드 등과 같은 임의의 적절한 유형의 코드를 포함할 수 있으며 적절한 상위 수준, 하위 수준, 개체-지향, 시각적, 컴파일 및/또는 해석된 프로그래밍 언어를 사용하여 구현된다.
- [0113] 예시적인 실시형태의 기술한 설명은 예시 및 설명의 목적으로 제시되었다. 이는 본 발명의 내용을 개시된 정확한 형태로 철저히 제한하거나 한정하려는 의도가 아니다. 본 발명에 비추어 많은 수정 및 변형이 가능하다. 본 발명의 범위는 이러한 발명의 상세한 설명이 아니라 여기에 첨부된 청구범위에 의해 제한되는 것으로 의도된다. 본 발명에 대한 우선권을 주장하는 향후 제출되는 출원은 개시된 주제를 다른 방식으로 청구할 수 있으며 본 발명에 다양하게 개시되거나 달리 입증된 바와 같이 하나 이상의 제한의 임의의 세트를 일반적으로 포함할 수 있다.

도면

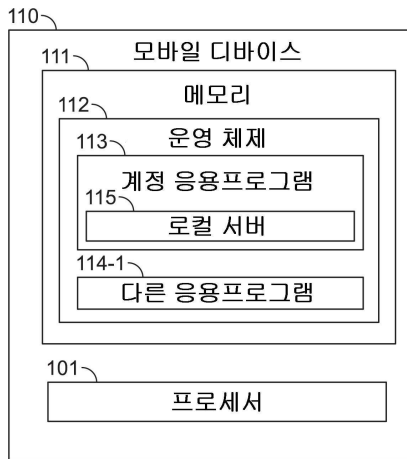
도면1a



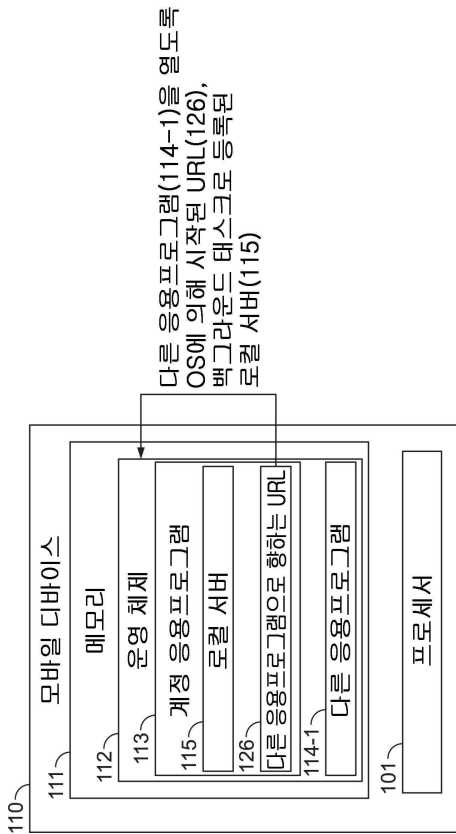
도면1b



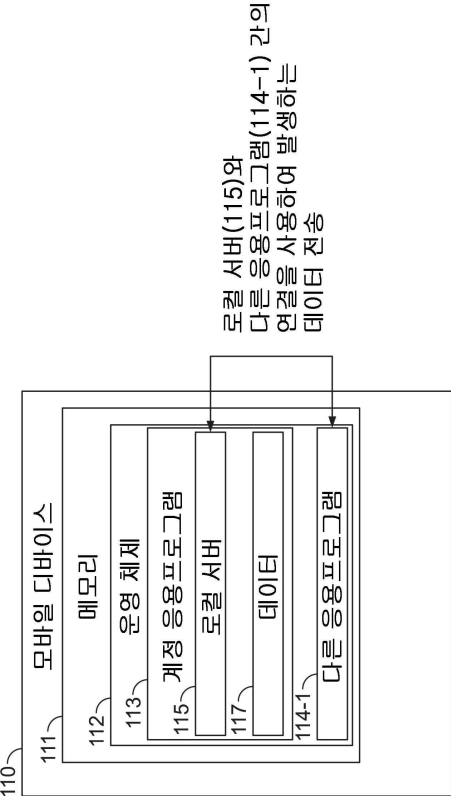
도면 1c



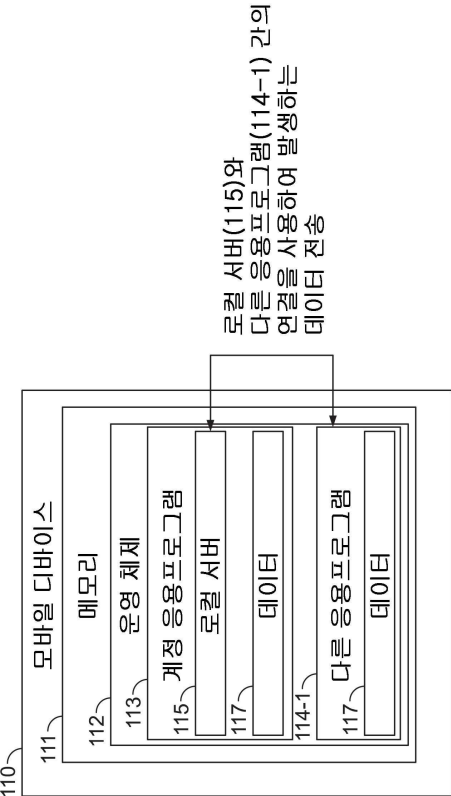
도면 1d



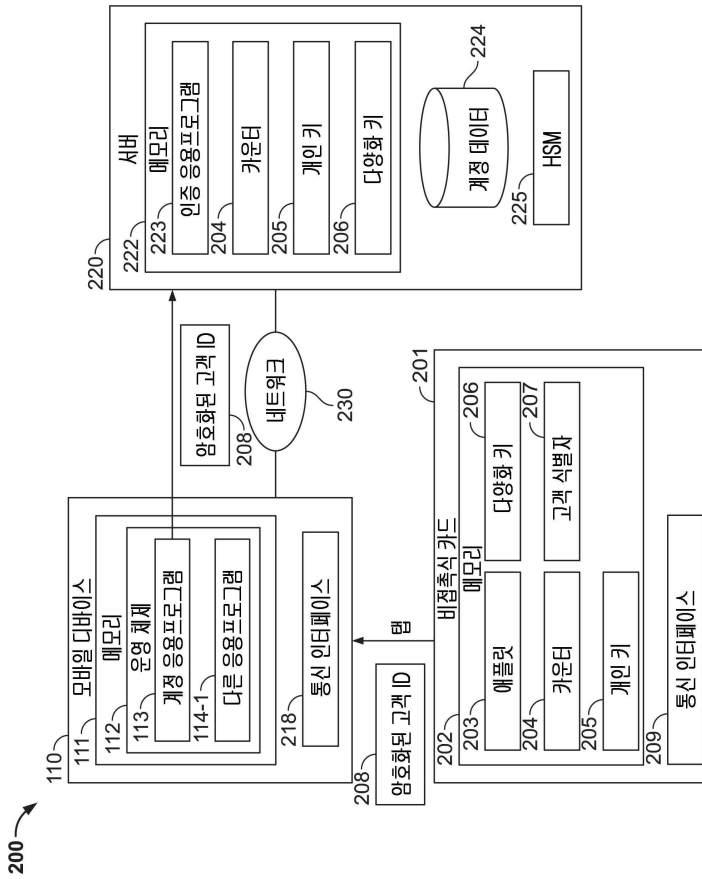
도면1e



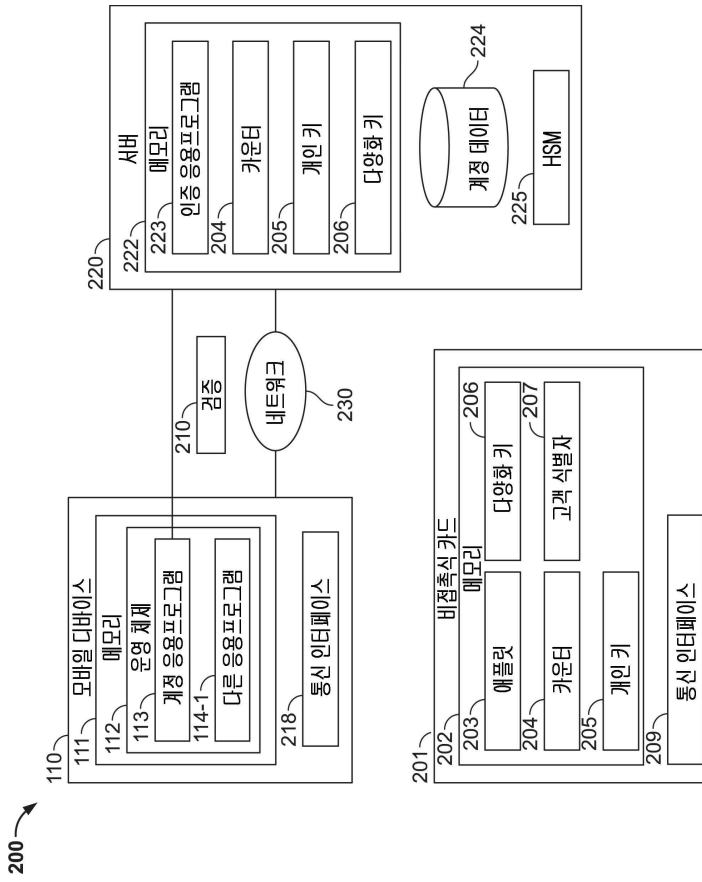
도면1f



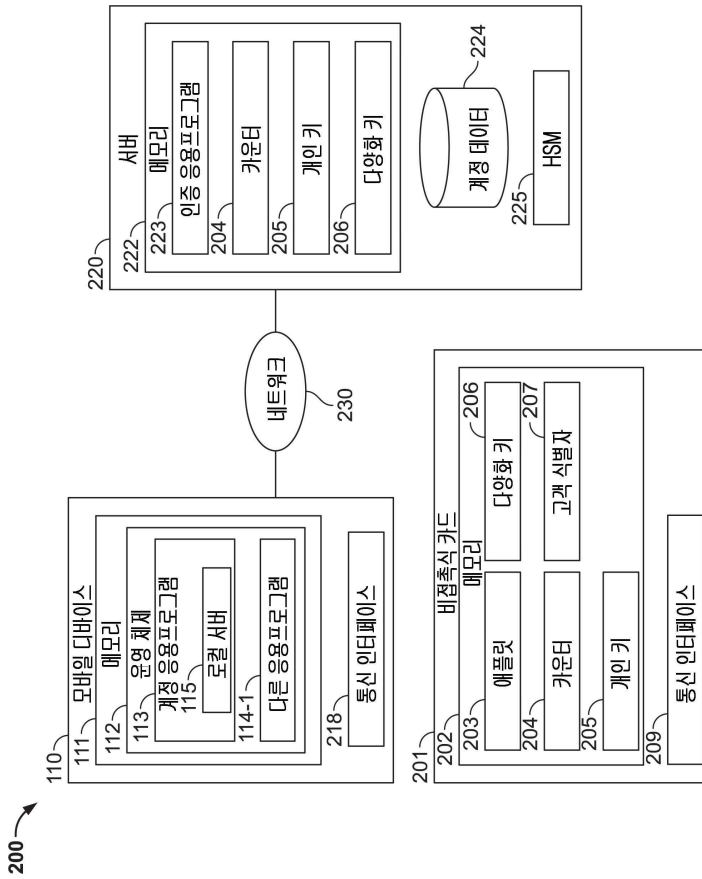
도면2a



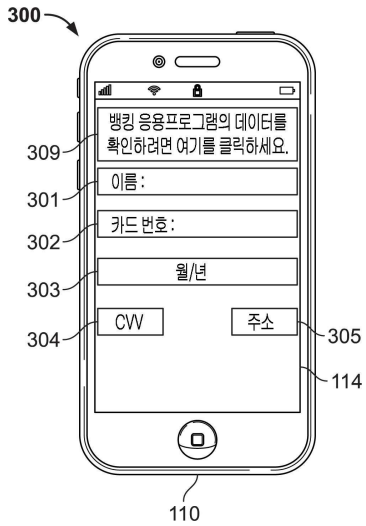
도면2b



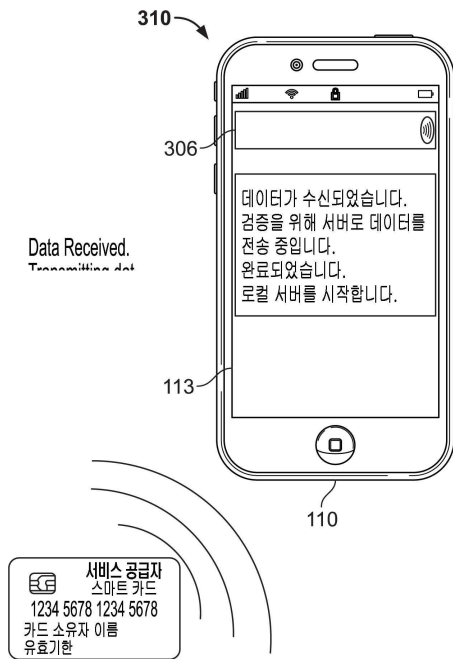
도면2c



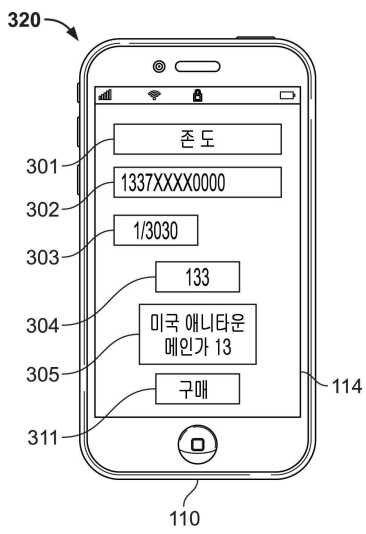
도면3a



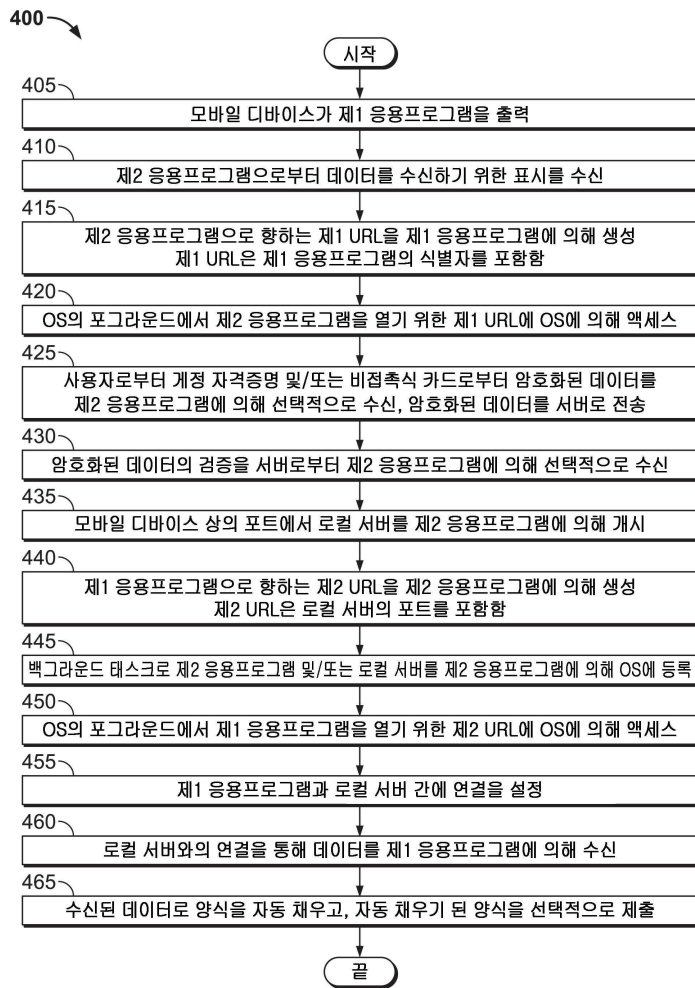
도면3b



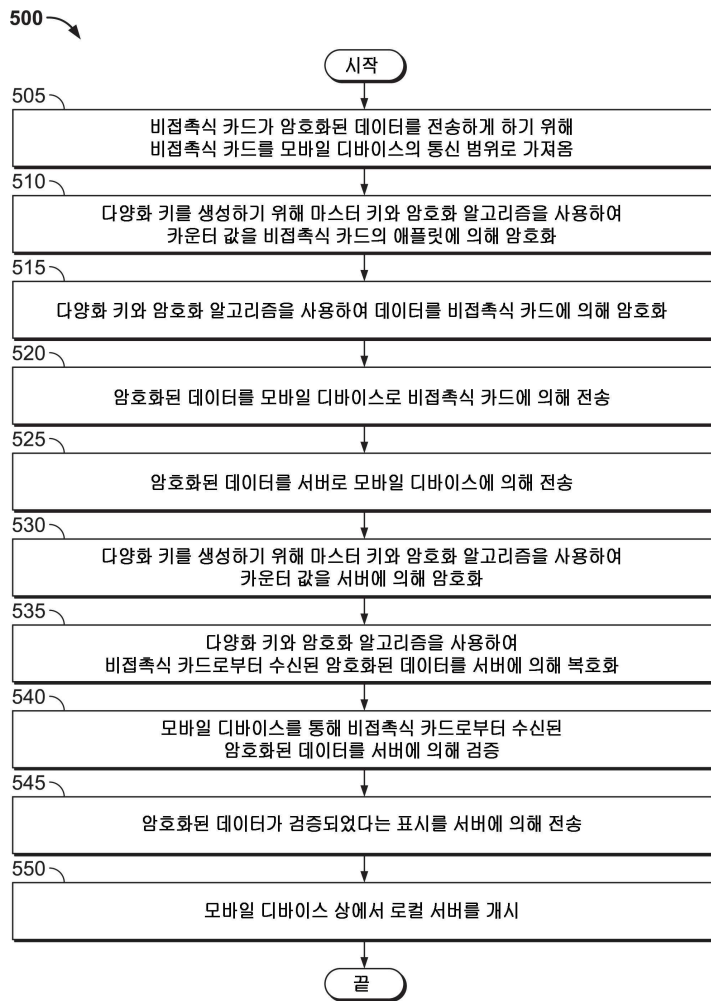
도면3c



도면4



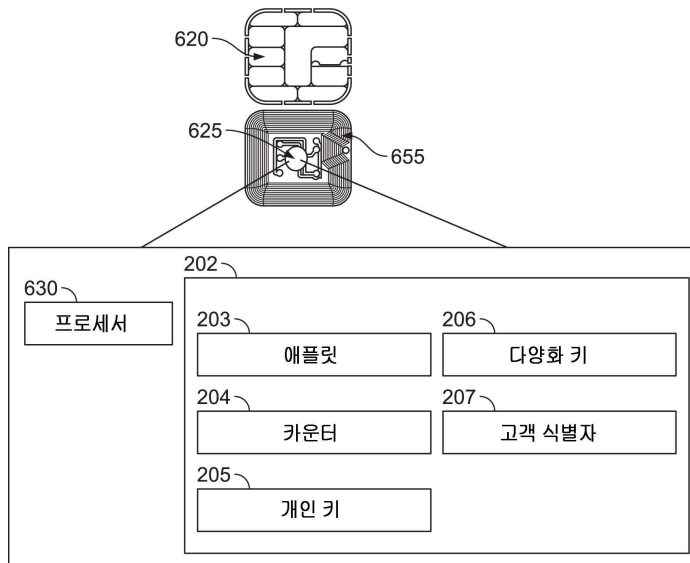
도면5



도면6a



도면6b



도면7

