



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0010610
(43) 공개일자 2025년01월21일

(51) 국제특허분류(Int. Cl.)
H04W 12/30 (2021.01) H04L 9/40 (2022.01)
H04W 12/03 (2021.01) H04W 12/06 (2021.01)
H04W 12/47 (2021.01)
(52) CPC특허분류
H04W 12/35 (2021.01)
H04L 63/0853 (2013.01)
(21) 출원번호 10-2024-7038717
(22) 출원일자(국제) 2023년04월24일
심사청구일자 없음
(85) 번역문제출일자 2024년11월21일
(86) 국제출원번호 PCT/US2023/019567
(87) 국제공개번호 WO 2023/229768
국제공개일자 2023년11월30일
(30) 우선권주장
17/664,460 2022년05월23일 미국(US)

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

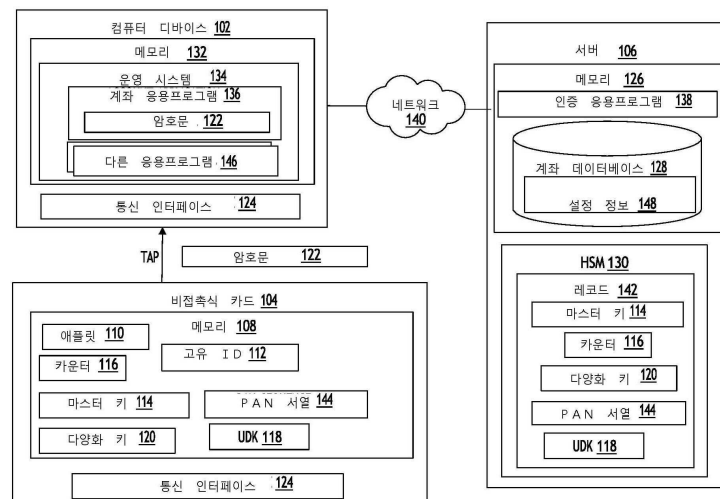
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 비접촉식 카드를 사용한 디바이스에서 응용프로그램의 설정

(57) 요약

비접촉식 카드를 사용하여 디바이스에서 응용프로그램을 구성하기 위한 시스템, 방법, 디바이스 및 컴퓨터 판독 가능 매체. 디바이스에서 실행되는 응용프로그램은 계정과 관련된 비접촉식 카드로부터 암호문을 수신할 수 있다. 응용프로그램은 암호문을 서버로 전송할 수 있다. 응용프로그램은 암호문을 기반으로 계정과 관련된 여러 응용프로그램에 대한 설정 정보를 수신할 수 있다. 응용프로그램은 설정 정보를 기반으로 디바이스에서 각 응용프로그램의 해당 설정을 수정할 수 있다.

대표도 - 도1a



100

(52) CPC특허분류

H04W 12/03 (2021.01)

H04W 12/06 (2021.01)

H04W 12/47 (2021.01)

명세서

청구범위

청구항 1

디바이스에서 실행하는 응용프로그램에 의해, 설정 정보 관련된 비접촉식 카드에서 암호화된 데이터를 수신하는 단계;

응용프로그램에 의해, 암호화된 데이터를 서버에 전송하는 단계;

암호화된 데이터에 근거한 응용프로그램에 의해, 계정과 관련된 다수의 응용프로그램에 대한 설정 정보를 수신하는 단계; 및

설정 정보에 근거하여 디바이스에서 각각의 응용프로그램의 해당 설정을 수정하는 단계;

를 포함하는 방법.

청구항 2

제1항에 있어서, 각각의 응용프로그램의 설정을 수정하기 전,

응용프로그램에 의해, 다수의 응용프로그램 중 제1 응용프로그램이 디바이스에 설치되지 않았음을 확인하는 단계;

응용프로그램에 의해, 제1 응용프로그램을 디바이스에 다운로드하는 단계; 및

디바이스의 운영 체제(OS)에 의해 디바이스에 제1 응용프로그램을 설치하는 단계; 를 더욱 포함함을 특징으로 하는 방법.

청구항 3

제1항에 있어서, 디바이스에 제1 응용프로그램을 설치한 후에,

제1 응용프로그램의 설정 정보를 기반으로 제1 응용프로그램의 설정을 수정하는 단계; 를 더욱 포함하는 방법.

청구항 4

제1항에 있어서, 설정 정보를 수신하는 단계는 서버로부터 다수의 설정 파일을 수신하는 단계; 를 포함함을 특징으로 하는 방법.

청구항 5

제1항에 있어서, 설정 정보를 수신하는 단계는 각각의 응용프로그램에 의해, 서버로부터 해당 푸시 알림을 수신하는 단계를 포함하고, 해당 푸시 알림은 해당 응용프로그램에 대한 해당 설정 정보를 포함하고, 푸시 알림은 백그라운드 알림을 포함함을 특징으로 하는 방법.

청구항 6

제1항에 있어서, 설정 정보를 수신하는 단계는 푸시 알림은 해당 토큰을 포함하고, 푸시 알림은 백그라운드 알림을 포함하며, 각각의 응용프로그램에 의해, 서버로부터 해당 푸시 알림을 수신하는 단계; 각각의 응용프로그램에 의해, 해당 토큰을 서버에 전송하는 단계; 각각의 응용프로그램에 의해, 해당 토큰을 기반으로 해당 설정 정보를 수신하는 단계; 를 포함함을 특징으로 하는 방법.

청구항 7

제1항에 있어서, 설정 정보는 (i) 하나 이상의 서버에 연결하기 위한 정보, (ii) 계정 정보, (iii) 메시지, (iv) 기본 설정 및 (v) 설정. 을 포함함을 특징으로 하는 방법.

청구항 8

디바이스상의 프로세서에 의해 실행되는 명령어를 포함하는 컴퓨터 판독 가능 저장 매체에 있어서,

상기 명령어는 프로세서가

디바이스에서 실행하는 응용프로그램에 의해, 설정 정보 관련된 비접촉식 카드에서 암호화된 데이터를 수신하고;

응용프로그램에 의해, 암호화된 데이터를 서버에 전송하고;

암호화된 데이터에 근거한 응용프로그램에 의해, 계정과 관련된 다수의 응용프로그램에 대한 설정 정보를 수신하고; 및

설정 정보에 근거하여 디바이스에서 각각의 응용프로그램의 해당 설정을 수정;

하도록 유도하는 비-일시적 컴퓨터 판독 가능 저장 매체.

청구항 9

제8항에 있어서, 상기 명령어는 프로세서가

각각의 응용프로그램의 설정을 수정하기 전,

응용프로그램에 의해, 다수의 응용프로그램 중 제1 응용프로그램이 디바이스에 설치되지 않았음을 확인하고;

응용프로그램에 의해, 제1 응용프로그램을 디바이스에 다운로드하고; 및

디바이스의 운영 체제(OS)에 의해 디바이스에 제1 응용프로그램을 설치;

하도록 더욱 유도함을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

청구항 10

제8항에 있어서, 상기 명령어는 프로세서가 디바이스에 제1 응용프로그램을 설치한 후에,

제1 응용프로그램의 설정 정보를 기반으로 제1 응용프로그램의 설정을 수정; 하도록 더욱 유도함을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

청구항 11

제8항에 있어서, 설정 정보의 수신은 서버로부터 다수의 설정 파일을 수신; 을 포함함을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

청구항 12

제8항에 있어서, 설정 정보의 수신은 각각의 응용프로그램에 의해, 서버로부터 해당 푸시 알림을 수신을 포함하고, 해당 푸시 알림은 해당 응용프로그램에 대한 해당 설정 정보를 포함하고, 푸시 알림은 백그라운드 알림을 포함함을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

청구항 13

제8항에 있어서, 설정 정보의 수신은 푸시 알림은 해당 토큰을 포함하고, 푸시 알림은 백그라운드 알림을 포함하며, 각각의 응용프로그램에 의해, 서버로부터 해당 푸시 알림을 수신하고; 각각의 응용프로그램에 의해, 해당 토큰을 서버에 전송하고; 각각의 응용프로그램에 의해, 해당 토큰을 기반으로 해당 설정 정보를 수신; 을 포함함을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

청구항 14

제8항에 있어서, 설정 정보는 (i) 하나 이상의 서버에 연결하기 위한 정보, (ii) 계정 정보, (iii) 메시지, (iv) 기본 설정 및 (v) 설정. 을 포함함을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

청구항 15

프로세서; 및

프로세서에 의해 실행시키는 명령어를 저장한 메모리; 를 포함하는 컴퓨터 기기에 있어서,

상기 명령어는 프로세서가

디바이스에서 실행하는 응용프로그램에 의해, 설정 정보 관련된 비접촉식 카드에서 암호화된 데이터를 수신하고;

응용프로그램에 의해, 암호화된 데이터를 서버에 전송하고;

암호화된 데이터에 근거한 응용프로그램에 의해, 계정과 관련된 다수의 응용프로그램에 대한 설정 정보를 수신하고; 및

설정 정보에 근거하여 디바이스에서 각각의 응용프로그램의 해당 설정을 수정;

하도록 유도하는 컴퓨터 기기.

청구항 16

제15항에 있어서, 상기 명령어는 프로세서가

각각의 응용프로그램의 설정을 수정하기 전,

응용프로그램에 의해, 다수의 응용프로그램 중 제1 응용프로그램이 디바이스에 설치되지 않았음을 확인하고;

응용프로그램에 의해, 제1 응용프로그램을 디바이스에 다운로드하고; 및

디바이스의 운영 체제(OS)에 의해 디바이스에 제1 응용프로그램을 설치;

하도록 더욱 유도함을 특징으로 하는 컴퓨터 기기.

청구항 17

제15항에 있어서, 상기 명령어는 프로세서가 디바이스에 제1 응용프로그램 을 설치한 후에,

제1 응용프로그램의 설정 정보를 기반으로 제1 응용프로그램의 설정을 수정; 하도록 더욱 유도함을 특징으로 하는 컴퓨터 기기.

청구항 18

제15항에 있어서, 설정 정보의 수신은 서버로부터 다수의 설정 파일을 수신; 을 포함함을 특징으로 하는 컴퓨터 기기.

청구항 19

제15항에 있어서, 설정 정보의 수신은 각각의 응용프로그램에 의해, 서버로부터 해당 푸시 알림을 수신을 포함하고, 해당 푸시 알림은 해당 응용프로그램에 대한 해당 설정 정보를 포함하고, 푸시 알림은 백그라운드 알림을 포함함을 특징으로 하는 컴퓨터 기기.

청구항 20

제15항에 있어서, 설정 정보의 수신은 푸시 알림은 해당 토큰을 포함하고, 푸시 알림은 백그라운드 알림을 포함하며, 각각의 응용프로그램에 의해, 서버로부터 해당 푸시 알림을 수신하고; 각각의 응용프로그램에 의해, 해당 토큰을 서버에 전송하고; 각각의 응용프로그램에 의해, 해당 토큰을 기반으로 해당 설정 정보를 수신; 를 포함함을 특징으로 하는 컴퓨터 기기.

발명의 설명

기술 분야

[0001] 본 출원은 2022년 5월 23일에 출원된 " 비접촉식 카드를 사용한 디바이스에서 응용프로그램의 설정" 라는 제목

의 미국 특허 출원 번호 17/664,460호에 대한 우선권을 주장한다. 상기 출원의 내용은 본원에 전체적으로 참조로 통합된다.

배경 기술

[0002]

새로운 기기나 추가 기기를 설정하는 것은 지루하고 시간이 많이 걸리며 오류가 발생하기 쉽다. 예를 들어, 사용자는 다른 기기를 대체하기 위해 새 기기를 구매할 수 있다. 그러나 새 기기에는 다른 기기의 응용프로그램 및/또는 형상화가 포함되지 않는다. 기기를 설정하는 기존 솔루션은 오류에 취약하고 보안 위험이 있으며 악의적인 공격에 취약하다.

발명의 내용

과제의 해결 수단

[0003]

비접촉식 카드를 사용하여 디바이스에서 응용프로그램을 형상화하기 위한 시스템, 방법, 디바이스 및 컴퓨터 판독 가능 매체에 관한 것이다. 하나의 측면에서, 방법은 디바이스에서 실행되는 응용프로그램에 의해 계정과 관련된 비접촉식 카드로부터 암호문을 수신하는 단계, 응용프로그램에 의해 암호문을 서버로 전송하는 단계, 응용프로그램에 의해 암호문을 기반으로 계정과 관련된 다수의 응용프로그램에 대한 설정정보를 수신하는 단계, 설정 정보를 기반으로 디바이스에서 각각의 응용프로그램의 해당 설정을 수정하는 단계를 포함한다.

도면의 간단한 설명

[0004]

특정 엘리먼트 또는 행위에 대한 논의를 쉽게 식별하기 위해 참조 번호의 가장 중요한 숫자 또는 숫자들은 해당 엘리먼트가 처음 도입된 도면 번호를 참조한다.

도 1A는 하나의 실시형태에 따른 청구 대상의 측면을 도시한 것이다.

도 1B는 하나의 실시형태에 따른 청구 대상의 측면을 도시한 것이다.

도 1C는 하나의 실시형태에 따른 청구 대상의 측면을 도시한 것이다.

도 1D는 하나의 실시형태에 따른 청구 대상의 측면을 도시한 것이다.

도 2A는 하나의 실시형태에 따른 청구 대상의 측면을 도시한 것이다.

도 2B는 하나의 실시형태에 따른 청구 대상의 측면을 도시한 것이다.

도 2C는 하나의 실시형태에 따른 청구 대상의 측면을 도시한 것이다.

도 2D는 하나의 실시형태에 따른 청구 대상의 측면을 도시한 것이다.

도 3은 하나의 실시형태에 따른 루틴 300을 도시한 것이다.

도 4는 하나의 실시형태에 따른 루틴 (400)을 도시한 것이다.

도 5는 하나의 실시형태에 따른 루틴 (500)을 도시한 것이다.

도 6A는 하나의 실시형태에 따른 비접촉식 카드 (104)를 도시한 것이다.

도 6B는 하나의 실시형태에 따른 비접촉식 카드 (104)를 도시한 것이다.

도 7은 하나의 실시형태에 따른 데이터 구조 700을 도시한 것이다.

도 8은 하나의 실시형태에 따른 컴퓨터 아키텍처 (800)을 도시한 것이다.

발명을 실시하기 위한 구체적인 내용

[0005]

본 명세서에 공개된 실시예는 비접촉식 카드를 사용하여 스마트폰, 태블릿 또는 기타 컴퓨터 디바이스와 같은 디바이스를 자동으로 설정하는 보안 기술을 제공한다. 디바이스를 설정하는 예로는 디바이스에 응용프로그램을 설치하고, 디바이스에서 응용프로그램을 제거하고, 디바이스에서 응용프로그램을 설정하는 것, 예를 들면 응용프로그램 설정, 응용프로그램 매개변수 등 수정이 있다. 처음에 사용자는 하나 이상의 응용프로그램 및/또는 하나 이상의 응용프로그램에 대한 설정 정보를 등록할 수 있다. 이를 수행하는 데는 계정 데이터베이스에 주어진 디바이스 및/또는 계정에 대한 정보를 저장하는 것이 포함될 수 있다. 등록은 응용프로그램 및/또는 설정 정보

를 비접촉식 카드와 연관시킬 수 있다.

- [0006] 그 후, 사용자는 이전에 등록된 디바이스, 새 디바이스, 기존 디바이스 등을 포함할 수 있는 모든 디바이스에 비접촉식 카드를 탭 할 수 있다. 일부 실시예에서는 카드를 디바이스에 탭 하면 카드가 암호를 생성할 수 있다. 일부 실시예에서는 암호가 균일 자원 로케이터(URL)의 매개변수이다. 디바이스가 URL 및/또는 암호문을 수신하면, 디바이스는 응용프로그램을 시작할 수 있으며, 이는 암호를 검증을 위해 서버로 전송할 수 있다. 서버는 암호문을 해독하는 것에 적어도 부분적으로 기초하여 암호를 검증할 수 있다.
- [0007] 다른 실시예에서 카드를 디바이스에 탭 하면 디바이스가 URL을 기반으로 웹 브라우저를 시작할 수 있다. 이러한 실시예에서 웹 브라우저는 URL과 연관된 페이지에 액세스할 수 있다. 서버는 웹 브라우저가 액세스한 URL의 매개변수로 암호를 식별할 수 있다. 서버는 암호문을 해독하는 것에 적어도 부분적으로 기초하여 암호를 검증할 수 있다.
- [0008] 카드를 디바이스에 탭 하는 것에 반응하여 실행되는 응용프로그램과 관계없이, 암호문을 검증한 후, 서버는 암호문 및/또는 암호문의 매개변수를 사용하여 계정 데이터베이스의 연관된 응용프로그램 및/또는 응용프로그램에 대한 설정 정보를 식별할 수 있다. 그런 다음 서버는 설정 정보를 요청하는 디바이스로 전송할 수 있다. 일부 구현예에서, 서버는 하나 이상의 푸시 알림을 통해 설정 정보를 디바이스로 전송한다. 일부 구현예에서, 설정 정보의 크기가 임계값 크기를 초과하는 경우, 서버는 하나 이상의 토큰을 디바이스로 전송할 수 있다. 그런 다음 디바이스는 토큰을 사용하여 서버에 설정 정보를 요청할 수 있다.
- [0009] 수신되면, 디바이스는 수신된 설정 정보를 각 응용프로그램에 적용할 수 있다. 예를 들어, 설정 정보에는 계정 로그인 자격 증명, 하나 이상의 서버에 연결을 설정하는 서버 정보, 사용자 기본 설정, 설정 등이 포함될 수 있다. 일부 구현예에서, 설정 정보에는 디바이스에 설치되지 않은 하나 이상의 응용프로그램에 대한 정보가 포함될 수 있다. 이러한 실시예에서 이러한 응용프로그램은 설정 정보 수신에 따라 디바이스에 다운로드 되어 설치될 수 있다. 마찬가지로, 설정 정보에는 기존 응용프로그램을 비활성화하거나 설치 해제하기 위한 정보가 포함될 수 있다. 이러한 실시예에서 디바이스는 설정 정보에 따라 이러한 응용프로그램을 비활성화 및/또는 설치 해제할 수 있다. 더욱이, 디바이스는 설정 정보에 따라 일부 응용프로그램이 디바이스에서 활성화 및/또는 재설치되는 것을 방지할 수 있다.
- [0010] 유리하게도, 여기에 공개된 실시예는 비접촉식 카드를 사용하여 디바이스를 자동으로 설정하는 보안 기술을 제공한다. 형상화를 시작하기 위해 암호화 검증을 요구함으로써, 사용자 계정, 응용프로그램, 디바이스 및 데이터의 보안이 개선된다.
- [0011] 더욱이, 그렇게 함으로써, 사용자가 서버와의 암호문 검증을 용이하게 하는 비접촉식 카드에 액세스할 때에만 자동 디바이스 형상화가 수행되도록 보장한다. 또한, 공개된 자동 형상화기능을 제공함으로써, 모든 응용프로그램, 운영 체제 및/또는 디바이스에 통합할 필요 없이 많은 다른 응용프로그램, 운영 체제 및/또는 디바이스를 자동으로 설정할 수 있다.
- [0012] 여기에 사용된 표기법 및 명명법에 대한 일반적인 참조와 함께, 여기에 있는 자세한 설명은 컴퓨터 또는 컴퓨터 네트워크에서 실행되는 프로그램 절차의 관점에서 제시될 수 있다. 이러한 절차 설명 및 표현은 해당 분야의 숙련자들이 해당 분야의 숙련자들에게 자신의 작업의 내용을 효과적으로 전달하기 위해 사용한다.
- [0013] 절차는 본 명세서내에서 그리고 일반적으로 원하는 결과를 이끌어내는 자기 일관성 있는 일련의 작업으로 구성된다. 이러한 작업은 물리적 양의 물리적 조작을 필요로 하는 작업이다. 반드시 그런 것은 아니지만, 일반적으로 이러한 양은 저장, 전송, 결합, 비교 및 기타 조작이 가능한 전기, 자기 또는 광학 신호의 형태를 취한다. 주로 일반적인 사용상의 이유로 이러한 신호를 비트, 값, 엘레먼트, 기호, 문자, 용어, 숫자 또는 이와 유사한 것으로 지칭하는 것이 편리한 경우가 있다. 그러나 이러한 모든 용어와 유사한 용어는 적절한 물리적 양과 연관되어야 하며 해당 양에 적용된 편리한 레이블일 뿐이라는 점에 유의해야 한다.
- [0014] 또한 수행되는 조작은 종종 추가 또는 비교와 같은 용어로 지칭되며, 이는 일반적으로 인간 작업자가 수행하는 정신적 작업과 연관된다. 대부분의 경우 하나 이상의 구체예의 일부를 형성하는 여기에 설명된 작업에서 인간 작업자의 그러한 능력은 필요하거나 바람직하지 않는다. 오히려 이러한 작업은 기계 작업이다. 다양한 실시예의 작업을 수행하는 데 유용한 기계에는 디지털 컴퓨터 또는 유사한 디바이스가 포함된다.
- [0015] 일부 실시예는 "결합" 및 "연결"이라는 표현과 그 파생어를 사용하여 설명될 수 있다. 이러한 용어는 반드시 서로의 동의어로 의도된 것은 아니다. 예를 들어, 일부 실시예는 두 개 이상의 엘레먼트가 서로 직접 물리적 또는 전기적으로 접촉하고 있음을 나타내기 위해 "연결" 및/또는 "결합"이라는 용어를 사용하여 설명될 수 있다.

그러나 "결합된"이라는 용어는 두 개 이상의 엘레먼트가 서로 직접 접촉하지 않지만 여전히 서로 협력하거나 상호 작용한다는 것을 의미할 수도 있다.

[0016] 다양한 실시예에는 또한 이러한 작업을 수행하기 위한 디바이스 또는 시스템과 관련이 있다. 이 디바이스는 필요한 목적을 위해 특별히 형성화될 수도 있고, 컴퓨터에 저장된 컴퓨터 프로그램에 의해 선택적으로 활성화되거나 재 형성화되는 컴퓨터를 포함할 수도 있다. 여기에 제시된 절차는 특정 컴퓨터 또는 다른 디바이스와 본질적으로 관련이 없습니다. 다양한 기계는 여기에 제시된 가르침에 따라 작성된 프로그램과 함께 사용될 수 있거나, 필요한 방법 단계를 수행하기 위해 보다 특수화된 디바이스를 설정하는 것이 편리할 수 있다. 이러한 다양한 기계에 필요한 구조는 제공된 설명에서 나타난다.

[0017] 이제 도면을 참조하며 여기서 유사한 참조 번호는 전체에서 유사한 엘레먼트를 나타내는 데 사용된다. 다음 설명에서 설명의 목적을 위해, 이에 대한 철저한 이해를 제공하기 위해 수많은 특정 세부 사항이 제시된다. 그러나 새로운 실시예에는 이러한 특정 세부 사항 없이도 실행될 수 있다. 다른 경우, 구조와 디바이스는 설명을 용이하게 하기 위해 블록 다이어그램 형태로 표시된다. 청구된 청구 대상과 일치하는 모든 수정, 균등물 및 대안을 포함하는 것이 의도이다.

[0018] 도면 및 첨부 설명에서, "a" 및 "b" 및 "c"(및 유사한 지정자)라는 명칭은 임의의 양의 정수를 나타내는 변수가 되도록 의도된 것이다. 따라서, 예를 들어, 구현이 a = 5에 대한 값을 설정하는 경우, 컴포넌트 123-1 내지 123-a (또는 123a)로 도시된 컴포넌트 123의 전체 세트는 컴포넌트 123-1, 123-2, 123-3, 123-4 및 123-5를 포함할 수 있다. 이 맥락에서 구현에는 제한되지 않는다.

[0019] 도면 1A는 공개된 구현예와 일치하는 시스템이라고도 하는 예시적인 컴퓨터 아키텍처 (100)을 묘사한다. 도면 1A-1C에 도시된 컴퓨터 아키텍처 (100)은 특정 토폴로지에서 제한된 수의 엘레먼트를 갖지만, 컴퓨터 아키텍처 (100)은 주어진 구현에 대해 원하는 대로 대체 토폴로지에서 더 많거나 적은 엘레먼트를 포함할 수 있다는 것을 알 수 있다.

[0020] 컴퓨터 아키텍처 (100)은 하나 이상의 컴퓨터 디바이스 (102), 하나 이상의 서버 (106) 및 하나 이상의 비접촉식 카드 (104)를 포함한다. 비접촉식 카드 (104)는 신용 카드, 직불 카드, ATM 카드, 기프트 카드, 지불 카드, 스마트 카드 등과 같은 모든 유형의 카드를 나타낸다. 비접촉식 카드 (104)는 NFC, EMV 표준 또는 무선 통신의 다른 단거리 프로토콜을 통해 컴퓨터 디바이스 (102)의 통신 인터페이스 (124) 본 명세서에서 "카드 리더기", "무선 카드 리더기" 및/또는 "무선 통신 인터페이스"라고도 함과 통신하도록 형성화된 무선 주파수 식별(RFID) 칩과 같은 하나 이상의 통신 인터페이스 (124)를 포함할 수 있다. NFC가 본 명세서에서 예시적인 통신 프로토콜로 사용되지만, 본 공개는 EMV 표준, Bluetooth 및/또는 Wi-Fi와 같은 다른 유형의 무선 통신에도 동일하게 적용할 수 있다.

[0021] 컴퓨터 디바이스 (102)는 스마트폰, 태블릿 컴퓨터, 웨어러블 디바이스, 랩톱, 휴대용 게임 디바이스, 가상화 컴퓨터 시스템, 상인 단말기, POS 시스템, 서버, 데스크톱 컴퓨터 등과 같은 모든 수와 유형의 컴퓨터 디바이스를 나타낸다. 모바일 디바이스는 컴퓨터 디바이스 (102)의 예로 사용될 수 있지만, 공개 내용을 제한하는 것으로 간주되어서는 안 된다. 서버 (106)은 서버, 워크스테이션, 컴퓨터 클러스터, 클라우드 컴퓨터 플랫폼, 가상화 컴퓨터 시스템 등과 같은 모든 유형의 컴퓨터 디바이스를 나타낸다. 명확성을 위해 도시하지는 않았지만, 컴퓨터 디바이스 (102), 비접촉식 카드 (104) 및 서버 (106)은 각각 하나 이상의 프로세서 회로를 포함하여, 예를 들어 프로그램, 코드 및/또는 명령어를 실행한다.

[0022] 도시된 바와 같이, 비접촉식 카드 (104)의 메모리 (108)은 애플릿 (110), 카운터 (116), 하나 이상의 마스터 키 (114), 하나 이상의 다양화 키 (120), 고유 ID (112), 기본 계정 번호(PAN) 시퀀스 번호 (144), 하나 이상의 고유 파생 키(UDK) (118)을 포함한다. 고유 ID (112)는 다른 비접촉식 카드 (104)에 비해 비접촉식 카드 (104)를 고유하게 식별하는 모든 식별자일 수 있다. PAN 시퀀스 (144)는 비접촉식 카드 (104)에 의해 저장된 카운터 값을 포함할 수 있다. 애플릿 (110)은 여기에 설명된 일부 또는 모든 작업을 수행하도록 형성화된 실행 가능한 코드이다. 카운터 (116)은 비접촉식 카드 (104)와 서버 (106) 사이에서 동기화되는 값이다. 카운터 (116)은 비접촉식 카드 (104)와 서버 (106) 및/또는 비접촉식 카드 (104)와 컴퓨터 디바이스 (102)사이에서 데이터가 교환될 때마다 변경되는 숫자를 포함할 수 있다. 카운터 (116), 마스터 키 (114), 다양화 키 (120), UDK (118), PAN 시퀀스 (144) 및/또는 고유 ID (112)는 아래에서 더 자세히 설명하는 바와 같이 시스템 (100)에서 보안을 제공하는 데 사용된다.

[0023] 도시된 바와 같이, 컴퓨터 디바이스 (102)의 메모리 (132)는 운영 체제 (134)의 인스턴스를 포함한다. 운영 체

제의 예로는 Android® OS, iOS®, macOS®, Linux® 및 Windows® 운영 체제가 있다. 도시된 바와 같이, 운영 체제 (134)는 계정 응용프로그램 (136)과 하나 이상의 다른 응용프로그램 (146)을 포함한다. 계정 응용프로그램 (136)은 사용자가 서버 (106)에 의해 저장된 설정 정보 (148)에 따라 디바이스 (102)를 설정하는 것과 같은 다양한 작업을 수행할 수 있도록 한다. 일부 구현예에서 계정 응용프로그램 (136)은 지불 카드 활성화, 계정 잔액 보기, 품목 구매, 지불 처리 등과 같은 다른 계정 관련 작업을 추가로 수행할 수 있다.

[0024] 일부 구현예에서 사용자는 인증 자격 증명을 사용하여 인증하여 계정 응용프로그램 (136)의 특정 기능에 액세스할 수 있다. 예를 들어, 인증 자격 증명에는 사용자 이름 또는 로그인 및 비밀번호, 생체 인증 자격 증명 예를 들면 지문, Face ID 등이 포함될 수 있다. 다른 응용프로그램 (146)은 웹 브라우저, 이메일 클라이언트, 메시징 클라이언트 소셜 미디어 응용프로그램 등과 같은 모든 유형의 응용프로그램 을 나타낸다.

[0025] 도시된 바와 같이, 서버 (106)의 메모리 126은 인증 응용프로그램 (138) 및 계정 데이터베이스 (128)을 포함한다. 계정 데이터베이스 (128)은 일반적으로 계정 소유자 예를 들면 하나 이상의 사용자, 계정 소유자의 하나 이상의 계정 및 계정의 하나 이상의 비접촉식 카드 (104)와 관련된 정보를 포함한다. 예를 들어 도시된 바와 같이, 계정 데이터베이스 (128)은 다수의 계정에 대한 설정 정보 (148)을 포함할 수 있다. 설정 정보 (148)은 컴퓨터 디바이스 (102), 운영 체제 (134), 계정 응용프로그램 (136), 다른 응용프로그램 (146) 및/또는 그 모든 컴포넌트를 형상화하기 위한 모든 데이터를 포함할 수 있다. 예를 들어, 설정 정보 (148)에는 하나 이상의 서버에 연결하기 위한 정보 예를 들면 인터넷 프로토콜(IP) 주소, 포트 등, 계정 정보 예를 들면 로그인/비밀번호, 받은 편지함 내용 예를 들면 메시지, 이메일 등, 기본 설정, 변수 값 및/또는 설정이 포함될 수 있다. 설정 정보 (148)에는 또한 실행 파일, 스크립트 등이 포함되어 주어진 컴퓨터 디바이스 (102)에 설정 정보 (148)의 하나 이상의 부분을 설치 및/또는 설정할 수 있다. 이 맥락에서 실시예는 제한되지 않는다. 설정 정보 (148)은 컴퓨터 디바이스 (102) 및/또는 해당 소프트웨어 컴포넌트의 모든 속성 및/또는 기능을 수정하는 데 사용될 수 있기 때문이다.

[0026] 명시된 바와 같이, 설정 정보 (148)은 컴퓨터 디바이스 (102)를 자동으로 설정하는 데 사용될 수 있다. 달리 말하면, 설정 정보 (148)은 주어진 디바이스 및/또는 계정의 적어도 일부의 "백업"을 나타낼 수 있다. 모든 응용프로그램, 운영 체제 및/또는 매개변수를 포함하며, 모든 디바이스가 백업과 유사한 상태로 복원될 수 있다. 예를 들어, 사용자가 새 스마트폰을 구매하는 경우, 이전 스마트폰의 설정 정보 (148)은 새 스마트폰을 자동으로 설정하는 데 사용될 수 있다. 예를 들어 설정 정보 (148)은 새 스마트폰에 응용프로그램을 설치하는 데 사용될 수 있다. 예를 들면 구매 시 스마트폰에 포함되지 않았지만 이전 스마트폰에 설치되어 설정 정보 (148)의 일부로 등록된 응용프로그램이다, 이전 스마트폰에 설치되지 않은 응용프로그램을 새 스마트폰에서 제거하고 및/또는 설정 정보 (148)에 따라 제한된 응용프로그램을 제거하고, 이전 스마트폰의 설정 및/또는 매개변수를 새 스마트폰에 적용하는 등의 작업을 할 수 있다.

[0027] 다양한 실시예에서 사용자는 처음에 설정 정보 (148)을 서버 (106)에 등록할 수 있다. 예를 들어 사용자는 계정 응용프로그램 (136)의 기능에 액세스하거나, 웹 페이지 또는 기타 리소스에 액세스하여 모든 디바이스 및/또는 계정에 대한 설정 정보 (148)을 등록할 수 있다. 설정 정보 (148)은 계정과 관련된 모든 디바이스 및/또는 계정과 관련된 디바이스의 하위 집합에 특정할 수 있다. 추가적으로 및/또는 대안적으로, 설정 정보 (148)은 계정과 관련된 모든 응용프로그램 및/또는 계정과 관련된 응용프로그램의 하위 집합에 특정할 수 있다. 일부 실시예에서 계정 응용프로그램 (136)은 컴퓨터 디바이스 (102)를 설명하는 정보 예를 들면 설치된 응용프로그램, 형상화 파일 등을 수집할 수 있으며, 이는 설정 정보 (148)로 저장될 수 있다. 다른 실시예에서 사용자는 주어진 디바이스의 다양한 응용프로그램, 설정, 기능 등을 지정하는 입력을 제공할 수 있다.

[0028] 일부 실시예에서 설정 정보 (148)에는 등록할 각 응용프로그램의 패키지 이름, 등록할 운영 체제 (134) 예를 들면 디바이스 식별자, 디바이스 버전, 기본 설정, 설정 등을 설명하는 메타데이터, 등록할 각 응용프로그램을 설명하는 메타데이터, 기본 설정, 로그인 정보, 응용프로그램 ID 또는 디바이스, 응용프로그램, 운영 체제 (134) 및/또는 그 컴포넌트의 다른 속성이 포함된다. 또한 설정 정보 (148)은 계정 데이터베이스 (128)의 계정과 연관될 수 있으며, 이를 통해 서버 (106)은 설정 정보 (148)을 계정과 연관된 하나 이상의 비접촉식 카드 (104)와 추가로 연관시킬 수 있다.

[0029] 예를 들어 사용자는 소셜 미디어 응용프로그램과 이메일 클라이언트를 서버 (106)에 등록할 수 있다. 따라서, 사용자에 대한 설정 정보 (148)에는 소셜 미디어 응용프로그램과 이메일 클라이언트의 각각의 패키지 이름, 미디어 응용프로그램과 이메일 클라이언트가 각각의 서버에 연결하기 위한 연결 정보, 소셜 미디어 응용프로그램과 이메일 응용프로그램의 사용자 ID, 이메일 클라이언트의 이메일 받은 편지함 또는 폴더, 소셜 미디어 응용프

로그래밍의 소셜 미디어 프로필, 소셜 미디어 응용프로그램의 소셜 미디어 메시지, 소셜 미디어 응용프로그램과 이메일 클라이언트의 각각의 버전, 디스플레이 설정 예를 들면 두 응용프로그램 모두에서 다크 모드 활성화, 2개의 응용프로그램 모두에서 푸시 알림 활성화, 운영 체제 (134) 내의 각 응용프로그램에 대한 권한 등이 포함될 수 있다. 실시예는 이 맥락에서 제한되지 않는다. 따라서 이 정보의 표시는 계정에 대한 설정 정보 (148)로 저장될 수 있다.

[0030] 그 후, 사용자는 설정 정보 (148)를 사용하여 컴퓨터 디바이스 (102)를 설정하고자 할 수 있다. 예를 들어, 컴퓨터 디바이스 (102)는 새로운 스마트폰일 수 있으며, 사용자는 소셜 미디어 응용프로그램과 이메일 클라이언트를 설정하고자 할 수 있다. 예를 들면 이메일 클라이언트에서 모든 이메일을 복원하고, 소셜 미디어 응용프로그램에서 소셜 미디어 프로필/설정을 로드한다. 일부 실시예에서 이러한 응용프로그램은 새로운 스마트폰에 설치되지 않을 수 있으므로, 설정 정보 (148)는 컴퓨터 디바이스 (102)에 설치하기 위해 소셜 미디어 응용프로그램 및/또는 이메일 클라이언트를 다운로드하는 데 추가로 사용될 수 있다. 설정 정보 (148)에 기반하여 디바이스의 형상화를 시작하기 위해, 사용자는 비접촉식 카드 (104)를 컴퓨터 디바이스 (102)에 탭 할 수 있다.

[0031] 도 1A에 도시된 실시예에서, 사용자는 비접촉식 카드 (104)를 컴퓨터 디바이스 (102)에 탭 할 수 있다. 또는 그렇지 않으면 비접촉식 카드 (104)를 디바이스 (102)의 통신 인터페이스 (124)의 통신 범위 내로 가져올 수 있다. 그런 다음 애플릿 (110)은 암호문 (122)를 생성할 수 있다. 암호문 (122)는 모든 적합한 암호화 기술을 기반으로 생성될 수 있다. 일부 실시예에서, 암호문 (122)는 비접촉식 카드 (104)의 고유 ID (112)에 기반할 수 있다. 일부 실시예에서, 애플릿 (110)은 암호문 (122)와 암호화되지 않은 식별자 예를 들면 카운터 (116), PAN 시퀀스 (144), 고유 ID (112) 및/또는 기타 고유 식별자를 암호문 (122)를 포함하는 데이터 패키지의 일부로 포함할 수 있다. 적어도 하나의 실시예에서, 데이터 패키지는 NDEF 파일이다.

[0032] 언급된 바와 같이, 컴퓨터 아키텍처 (100)은 데이터를 보호하기 위해 키 다양화를 구현하도록 형상화되며, 이를 본 명세서에서 키 다양화 기술이라고 할 수 있다. 일반적으로 서버 (106) 또는 다른 컴퓨터 디바이스와 비접촉식 카드 (104)는 동일한 마스터 키 (114) (마스터 대칭 키라고도 함)로 프로비저닝 될 수 있다. 보다 구체적으로 각 비접촉식 카드 (104)는 서버 (106)의 하드웨어 보안 모듈(HSM) (130)에 대응하는 쌍을 갖는 고유한 마스터 키 (114)로 프로그래밍 된다. 예를 들어, 비접촉식 카드 (104)가 제조될 때, 고유한 마스터 키 (114)가 비접촉식 카드 (104)의 메모리 (108)에 프로그래밍 될 수 있다. 마찬가지로, 고유한 마스터 키 (114)는 HSM (130)의 레코드 (142)에 저장될 수 있다.

[0033] 또한 주어진 카드 (104)가 제조될 때, UDK (118)은 HSM (130)의 마스터 키 (114) 인덱스에 대한 참조와 다양화 요인을 입력으로 취하는 HSM 기능을 통해 마스터 키 (114)로부터 다양화될 수 있다. 예를 들면 레코드 (142)에 대한 인덱스이다. 일부 실시예에서 다각화 요인은 비접촉식 카드 (104)의 고유 ID (112) 및/또는 PAN 시퀀스 (144)일 수 있다. UDK (118)은 비접촉식 카드 (104) 및 HSM (130)의 레코드 (142)에 저장될 수 있다. 마스터 키 (114) 및 UDK (118)은 비접촉식 카드 (104) 및 서버 (106)을 제외한 모든 당사자에게 비밀로 유지될 수 있으므로 시스템 (100)의 보안을 강화할 수 있다. 레코드 (142)에 저장되어 있는 것으로 묘사되었지만, 일부 실시예에서 카운터 (116) 및/또는 PAN 시퀀스 (144)는 HSM (130)에 저장되지 않는다. 예를 들어 고유 ID (112), 카운터 (116) 및 PAN 시퀀스 (144)는 계정 데이터베이스 (128)에 저장될 수 있다.

[0034] 일부 실시예에서 암호문 (122)를 생성하기 위해 애플릿 (110)은 UDK를 제공할 수 있다. (118), 고유 ID (112), 그리고 암호화 알고리즘에 대한 입력으로 다양화 인자를 통해 다양화 키 (120)을 생성한다. 일부 실시예에서 다양화 인자는 카운터 (116)이다. 다른 실시예에서 PAN 시퀀스 (144)는 다양화 인자이다. 다양화 키 (120)은 다양화 인자 예를 들면 카운터 (116) 및/또는 PAN 시퀀스 (144) 또는 기타 민감한 데이터와 같은 일부 데이터를 암호화하는 데 사용될 수 있다. 애플릿 (110) 및 서버 (106)은 암호문의 복호화 및/또는 검증 처리를 용이하게 하기 위해 동일한 유형의 데이터를 암호화하도록 형상화될 수 있다.

[0035] 언급된 바와 같이, 비접촉식 카드 (104) 및 서버 (106)의 UDK (118)은 키 다양화를 사용하여 보안을 강화하기 위해 카운터 (116)과 함께 사용될 수 있다. 명시된 바와 같이, 카운터 (116)은 비접촉식 카드 (104)와 서버 (106) 사이에서 동기화되는 값을 포함한다. 카운터 (116)은 비접촉식 카드 (104)와 서버 (106) 및/또는 비접촉식 카드 (104)와 컴퓨터 디바이스 (102) 사이에서 데이터가 교환될 때마다 변경되는 숫자를 포함할 수 있다. 데이터를 보낼 준비를 할 때, 예를 들면 서버 (106) 및/또는 디바이스 (102)로 비접촉식 카드 (104)의 애플릿 (110)은 카운터 (116)을 증가시킬 수 있다. 비접촉식 카드 (104)의 애플릿 (110)은 UDK (118), 고유 ID (112) 및 카운터 (116)을 암호화 알고리즘에 대한 입력으로 제공할 수 있으며, 이는 출력으로 다양화 키 (120)을 생성한다. 암호화 알고리즘에는 암호화 알고리즘, 해시 기반 메시지 인증 코드(HMAC) 알고리즘, 암호 기반 메시지

인증 코드(CMAC) 알고리즘 등이 포함될 수 있다.

- [0036] 암호화 알고리즘의 비제한적 예로는 3DES 또는 AES107과 같은 대칭 암호화 알고리즘, HMAC-SHA-256과 같은 대칭 HMAC 알고리즘, AES-CMAC과 같은 대칭 CMAC 알고리즘이 포함될 수 있다. 키 다양화 기술의 예는 2018년 11월 29일에 출원된 미국 특허 출원 16/205,119호에 더 자세히 설명되어 있다. 상기 특허 출원은 본원에 전체적으로 참조로 통합된다. 일부 실시예에서, PAN 시퀀스 (144)는 카운터 (116) 대신 암호화 알고리즘에 대한 입력으로 사용되어 다양화 키 (120)을 생성한다. 예를 들면 UDK (118), 고유 ID (112) 및 PAN 시퀀스 (144)를 암호화 등이다.
- [0037] 애플릿 (110)은 이후 다양화 키 (120)과 암호화 알고리즘에 대한 입력으로의 데이터를 사용하여 일부 데이터 예를 들면 고유 ID (112), 카운터 (116), PAN 시퀀스 (144), 명령 및/또는 기타 데이터를 암호화할 수 있다. 예를 들어, 다양화 키 (120)으로 고유 ID (112)를 암호화하면 암호화된 고유 ID (112), 예를 들면 암호문 (122)이 생성될 수 있다. 설명한 대로, 애플릿 (110)과 서버 (106)은 동일한 데이터를 암호화하도록 형상화될 수 있다.
- [0038] 일부 실시예에서 2 개의 다양화 키 (120)은 예를 들어 암호화 기능에 대한 입력의 하나 이상의 부분을 기반으로 생성될 수 있다. 일부 실시예에서, 2 개의 다양화 키 (120)은 두 개의 서로 다른 마스터 키 (114), 두 개의 서로 다른 UDK (118), 고유 ID (112) 및 카운터 (116) 또는 PAN 시퀀스 (144)을 기반으로 생성된다. 이러한 실시예에서, 메시지 인증 코드(MAC)는 다양화 키 (120) 중 하나를 사용하여 생성되고, MAC은 다양화 키 (120) 중 다른 하나를 사용하여 암호화될 수 있다. MAC은 민감한 데이터, 고유 ID (112), 카운터 (116) 및/또는 PAN 시퀀스 (144)와 같은 MAC 알고리즘에 대한 모든 적합한 데이터 입력을 기반으로 생성될 수 있다. 보다 일반적으로 애플릿 (110) 및 서버 (106)은 동일한 데이터를 기반으로 MAC을 생성하도록 형상화될 수 있다. 일부 실시예에서 암호문 (122)는 NDEF 파일과 같은 데이터 패키지에 포함된다. 계정 응용프로그램 (136)은 컴퓨터 디바이스 (102)의 통신 인터페이스 (124)를 통해 암호문 (122)를 포함하는 데이터 패키지를 읽을 수 있다.
- [0039] 일부 실시예에서 애플릿은 URL의 매개변수로서 암호문 (122)를 포함한다. 예를 들어, URL은 "http://www.example.com/appconfig?param=ABC123&custID=123"일 수 있다. 그러한 예에서, 암호문 (122)는 매개변수 "ABC123"에 대응할 수 있고 고유 ID (112)는 매개변수 "cust ID"에 대응할 수 있다. 운영 체제 (134)가 수신하면 운영 체제 (134)는 URL을 처리하기 위해 응용프로그램을 열 수 있다. 일부 실시예에서 URL은 계정 응용프로그램 (136)에 등록될 수 있으며, 이는 운영 체제 (134)가 계정 응용프로그램 (136)을 시작하고 URL (120)을 계정 응용프로그램 (136)에 대한 입력으로 제공하게 한다. 그러나 다른 실시예에서 운영 체제 (134)는 웹 브라우저를 시작하고 URL을 웹 브라우저에 대한 입력으로 제공할 수 있다. 다른 실시예에서 암호문 (122)는 URL의 매개변수가 아니지만 NDEF 파일과 같은 데이터 패키지에서 URL과 함께 전송된다. 이러한 실시예에서 운영 체제 (134)는 컴퓨터 디바이스 (102)의 통신 인터페이스 (124)를 통해 URL과 암호문 (122)를 포함하는 데이터 패키지를 읽을 수 있다.
- [0040] 도 1A에 도시된 실시예에서, 운영 체제 (134)는 암호문 (122)를 읽은 것에 따라 계정 응용프로그램 (136)을 시작할 수 있다. 언급된 바와 같이, 암호문 (122)는 URL의 매개변수일 수 있다. 이러한 실시예에서, URL은 계정 응용프로그램 (136)과 연관될 수 있다. 그렇게 하면 운영 체제 (134)가 계정 응용프로그램 (136)을 시작한다. 그런 다음 계정 응용프로그램 (136)은 암호문 (122)를 추출하고 암호문 (122)를 검증을 위해 서버 (106)으로 전송할 수 있다.
- [0041] 암호문 (122)가 URL의 매개변수가 아닌 실시형태에서, 운영 체제 (134)는 암호문 (122) 및/또는 암호문 (122)를 포함하는 NDEF 파일을 읽은 것에 따라 계정 응용프로그램 (136)을 시작할 수 있다. 운영 체제 (134)는 암호문 (122)를 계정 응용프로그램 (136)에 제공할 수 있다. 그런 다음 계정 응용프로그램 (136)은 암호문 (122)를 추출하고 확인을 위해 암호문 (122)를 서버 (106)에 전송할 수 있다.
- [0042] 일부 실시형태에서 계정 응용프로그램 (136)(또는 설정 정보 (148)에 따라 컴퓨터 디바이스 (102)를 형상화하기 위한 다른 응용프로그램)은 디바이스에 설치되지 않을 수 있다. 이러한 일부 실시예에서, 운영 체제 (134)는 URL 및/또는 암호문 (122)에 따라 계정 응용프로그램 (136)이 컴퓨터 디바이스 (102)에 다운로드 되어 설치되도록 할 수 있다.
- [0043] 이러한 다른 실시예에서 계정 응용프로그램 (136)의 공개된 기능을 포함하는 응용프로그램 클립 예를 들면 애플 앱 클립, 인스턴트 응용프로그램 예를 들면 Android 인스턴트 응용프로그램 또는 프로그래시브 웹 응용프로그램, 예를 들면 Android 프로그래시브 웹 응용프로그램이 설정 정보 (148)에 따라 컴퓨터 디바이스 (102)에 다운로드 되어 설치될 수 있다. 이러한 실시예에서 설정 정보 (148)이 컴퓨터 디바이스 (102)를 설정하

는 데 사용된 후, 앱 클립, 인스턴트 응용프로그램 및/또는 프로그래시브 웹 응용프로그램이 컴퓨터 디바이스 (102)에서 자동으로 제거될 수 있다.

[0044] 도 1B는 계정 응용프로그램 (136)이 암호문 (122)를 서버 (106)에 전송하는 실시예를 도시한 것이다. 서버 (106)은 서버 (106)에 의해 저장된 마스터 키 (114) 및/또는 UDK (118)의 인스턴스에 따라 적어도 부분적으로 검증을 위해 인증 응용프로그램 (138) 및/또는 HSM (130)에 암호문 (122)를 제공할 수 있다. 일부 실시예에서 인증 응용프로그램 (138) 및/또는 HSM (130)은 서버 (106)에 제공된 암호화되지 않은 고유 ID (112)를 사용하여 UDK (118) (또는 마스터 키 (114)) 및 카운터 (116)을 식별할 수 있다. PAN 시퀀스 (144)가 암호문 (122)를 생성하는 데 사용되는 실시예에서 서버 (106)은 암호화되지 않은 고유 ID를 사용하여 계정 데이터베이스 (128) 및/또는 HSM (130)에서 PAN 시퀀스 (144)를 식별할 수 있다. (112). 일부 실시예에서 인증 응용프로그램 (138)은 UDK (118), 고유 ID (112) 및 카운터 (116)을 HSM (130)의 암호화 기능에 대한 입력으로 제공할 수 있으며, 이는 하나 이상의 다양화 키 (120)을 출력으로 생성한다.

[0045] 다른 구현예에서 서버는 UDK (118), 고유 ID (112) 및 PAN 시퀀스 (144)를 암호화하여 다양화 키 (120)을 생성한다. 그 결과 다양화 키 (120)은 비접촉식 카드 (104)의 다양화 키 (120)에 해당할 수 있으며, 이는 암호문 (122)를 해독하거나 해독된 후 MAC을 확인하는 데 사용될 수 있다. 예를 들어 서버 (106)은 애플릿 (110)과 동일한 데이터, 예를 들어 민감한 데이터, 고유 ID (112), 카운터 (116) 및/또는 PAN 시퀀스 (144)를 기반으로 MAC을 생성할 수 있다. 서버 (106)에서 생성된 MAC이 암호문 (122)의 복호화된 MAC과 일치하는 경우, 서버 (106)은 암호문 (122)를 검증하거나 다른 방식으로 인증할 수 있다.

[0046] 사용된 복호화 기술에 관계없이, 인증 응용프로그램 (138) 및/또는 HSM (130)은 암호문 (122)를 성공적으로 복호화하고 MAC을 검증하여 암호문 (122)를 검증 및/또는 인증할 수 있다. 복호화 및/또는 MAC 검증이 성공한 경우, 인증 응용프로그램 (138)은 계정 데이터베이스 (128)를 참조하여 계정에 대한 설정 정보 (148)를 식별할 수 있다. 일부 실시예에서 인증 응용프로그램 (138)은 서버 (106)에 제공된 암호화되지 않은 고유 ID (112)를 기반으로 설정 정보 (148)에 액세스할 수 있다. 실시예는 이 맥락에서 제한되지 않으며, 모든 적합한 식별자가 계정에 대한 설정 정보 (148)에 액세스하는 데 사용될 수 있다. 서버 (106)은 또한 컴퓨터 디바이스 (102) 예를 들면 계정 응용프로그램 (136) 및/또는 운영 체제 (134)에 서버 (106)이 암호문 (122)를 검증했으며 설정 정보 (148)이 컴퓨터 디바이스 (102)를 설정하는데 사용될 수 있음을 나타내는 응답을 전송할 수 있다.

[0047] 인증 응용프로그램 (138)은 그 후 설정 정보 (148)을 구문 분석하여 여기에 등록된 각 응용프로그램, 운영 체제 및/또는 설정을 식별할 수 있다. 이전 실시예를 계속하면, 설정 정보 (148)에는 소셜 미디어 응용프로그램 및 이메일 클라이언트의 표시가 포함될 수 있다. 아래에서 더 자세히 설명하듯이, 서버 (106)은 설정 정보 (148) 및/또는 그 일부를 컴퓨터 디바이스 (102)로 전송할 수 있다.

[0048] 복호화로 돌아가서, 인증 응용프로그램 (138)이 암호문 (122)를 복호화 할 수 없는 경우 및/또는 MAC을 검증할 수 없는 경우, 인증 응용프로그램 (138)은 암호문 (122)를 검증하지 않는다. 이러한 실시예에서 인증 응용프로그램 (138)은 컴퓨터 디바이스 (102)를 자동으로 형상화하기 위해 설정 정보 (148)에 액세스하지 않기로 결정한다. 인증 응용프로그램 (138)은 복호화 및/또는 검증에 실패했다는 표시와 설정 정보 (148)을 사용하여 컴퓨터 디바이스 (102)를 설정할 수 없다는 표시를 포함하는 응답을 컴퓨터 디바이스 (102)로 전송할 수 있다.

[0049] 도 1C는 인증 응용프로그램 (138)이 계정 데이터베이스 (128)내의 설정 정보 (148)에서 식별된 각 응용프로그램 또는 기타 소프트웨어 컴포넌트에 대해 계정 응용프로그램 (136)에 대한 설정 정보 (148)를 포함하는 푸시 알림 (150)을 전송하는 실시예를 도시한 것이다. 일부 실시예에서 푸시 알림 (150)에는 서버 (106)이 암호문 (122)를 검증했으며 설정 정보 (148)을 사용하여 컴퓨터 디바이스 (102)를 설정할 수 있다는 표시가 포함된다. 단일 푸시 알림으로 전송되는 것으로 묘사되었지만, 일부 실시예에서 서버 (106)은 각 푸시 알림이 설정 정보 (148)의 일부 이상을 포함하는 여러 푸시 알림을 컴퓨터 디바이스 (102)에 전송할 수 있다. 일부 실시예에서, 주어진 푸시 알림은 운영 체제 (134)의 백그라운드에서 수신될 수 있다. 예를 들면 컴퓨터 디바이스 (102)에 표시되도록 출력되지 않지만 해당 응용프로그램 및/또는 운영 체제 (134)에 직접 전송되는 백그라운드 푸시 알림이다. 일부 실시예에서 푸시 알림은 포그라운드 푸시 알림 예를 들면 컴퓨터 디바이스 (102)에 표시되는 알림이다. 일부 실시예에서 설정 정보 (148)에는 하나 이상의 형상화파일이 포함된다.

[0050] 또한 일부 실시예에서 설정 정보 (148) 및/또는 그 일부의 크기는 크기 임계값 예를 들면 1메가바이트, 10메가바이트 등을 초과할 수 있다. 이러한 실시예에서 서버 (106)은 하나 이상의 토큰을 생성하고, 각 토큰을 설정 정보 (148)의 하나 이상의 부분과 연관시키고, 하나 이상의 토큰을 컴퓨터 디바이스 (102)로 전송할 수 있다. 그런 다음 컴퓨터 디바이스 (102)는 토큰을 서버 (106)으로 전송하여 서버 (106)에서 관련 설정 정보 (148) 및/

또는 그 일부를 가져올 수 있다. 예를 들어 토큰을 설정 정보 (148)와 연관시킴으로써, 서버 (106)은 계정 응용 프로그램 (136), 운영 체제 (134) 및/또는 다른 응용프로그램 (146)으로부터 토큰을 수신하는 것에 따라 연관된 설정 정보 (148)를 제공할 수 있다.

[0051] 일부 실시예에서 컴퓨터 디바이스 (102)는 설정 정보 (148) 및/또는 토큰을 비접촉식 카드 (104)로 전송할 수 있다. 그런 다음 비접촉식 카드 (104)는 설정 정보 (148) 및/또는 토큰을 메모리(108)에 저장할 수 있다. 그 후, 컴퓨터 디바이스 (102)는 비접촉식 카드 (104)로부터 설정 정보 (148)를 수신할 수 있다. 예를 들면 비접촉식 카드 (104)를 컴퓨터 디바이스 (102)에 탭 하는 것에 응답하는 NFC를 통해서이다. 이를 통해 컴퓨터 디바이스 (102) 및 그 컴포넌트를 여기에 설명된 대로 설정할 수 있다.

[0052] 또한 도시된 바와 같이 도 1C는 컴퓨터 디바이스 (102)가 계정 응용프로그램 (136) 외에 세 가지 다른 응용프로그램, 예를 들어 다른 응용프로그램 (146-1), 다른 응용프로그램 (146-2) 및 다른 응용프로그램 (146-N)을 포함하는 실시예를 도시한 것이다. 유리하게도, 계정 응용프로그램 (136)은 설정 정보 (148)를 사용하여 컴퓨터 디바이스 (102)에서 이러한 응용프로그램을 설정할 수 있다.

[0053] 도 1D는 계정 응용프로그램 (136)이 서버 (106)으로부터 수신한 설정 정보 (148)의 하나 이상의 부분을 사용하여 컴퓨터 디바이스 (102)를 설정하는 실시예를 도시한 것이다. 언급된 바와 같이, 계정 응용프로그램 (136)은 서버 (106)이 암호문 (122)를 검증했으며 설정 정보 (148)를 사용하여 컴퓨터 디바이스 (102)를 설정할 수 있다는 것을 나타내는 서버 (106)의 응답에 따라 설정 정보 (148)의 사용을 조건화 할 수 있다. 도시된 바와 같이 계정 응용프로그램 (136)은 설정 정보 (148)-1을 사용하여 다른 응용프로그램 (146-1)을 형상화하고 설정 정보 (148-N)을 사용하여 다른 응용프로그램 (146-N)을 설정한다. 일부 실시예에서 계정 응용프로그램 (136)은 설정 정보 (148)를 구문 분석하여 설정 정보 (148-1) 내지 (148)-N을 생성할 수 있다.

[0054] 다른 실시예에서 서버 (106)은 컴퓨터 디바이스 (102)에서 형상화되는 각 응용프로그램 또는 다른 엔터티에 대해 하나의 파일인 여러 파일을 포함하도록 설정 정보 (148)를 생성한다. 따라서 이러한 실시예에서 설정 정보 (148-1) 내지 (148)-N은 서버 (106)에 의해 생성된다. 일부 실시예에서 설정 정보 (148)의 적어도 일부는 계정 응용프로그램 (136)과 연관되어 있으므로 계정 응용프로그램 (136)을 설정하는 데 사용된다. 예를 들면 사용자 프로필, 설정 등을 로드 등이다.

[0055] 일부 실시예에서 계정 응용프로그램 (136)은 설정 정보 (148)를 각 응용프로그램 및/또는 운영 체제 (134)와 연관된 위치에 해당 형상화파일로 저장(또는 쓰기)한다. 예를 들어, 계정 응용프로그램 (136)은 설정 정보 (148-1)을 다른 응용프로그램 (146-1)에 대한 형상화파일로 저장할 수 있다. 예를 들면 파일 이름과 함께 및/또는 응용프로그램 (146-1)에 대한 설정 정보를 저장하는 파일과 연관된 파일 위치에 저장한다. 또 다른 실시예로서, 계정 응용프로그램 (136)은 설정 정보 (148)의 일부를 사용하여 운영 체제 (134)의 하나 이상의 파일, 레지스트리 설정 또는 기타 매개변수를 저장 및/또는 수정할 수 있다. 이러한 일부 실시예에서, 계정 응용프로그램 (136)은 설정 정보 (148)를 운영 체제 (134)에 제공할 수 있으며, 여기서 운영 체제 (134)는 설정 정보 (148)를 사용하여 운영 체제 (134)를 수정할 수 있다. 일부 구현예에서, 설정 정보 (148)를 사용하면 새로운 설정 정보가 컴퓨터 디바이스 (102)에 기록되고, 컴퓨터 디바이스 (102)의 일부 기존 설정 정보가 수정되고 예를 들면 값, 설정 등을 변경하여, 컴퓨터 디바이스 (102)의 다른 기존 설정 정보가 수정되지 않은 상태로 유지될 수 있다.

[0056] 또한 계정 응용프로그램 (136)은 설정 정보 (148-3)를 사용하여 응용프로그램 (146-3)이 컴퓨터 디바이스 (102)에 설치되지 않았음을 판별한다. 이러한 실시예에서, 계정 응용프로그램 (136)은 설정 정보 (148-3)를 들면 응용프로그램 (146-3)의 패키지 이름을 사용하여 인터넷에서 응용프로그램 (146-3)을 다운로드한다. 그런 다음, 계정 응용프로그램 (136)은 설정 정보 (148-3)를 사용하여 여기에 설명된 대로 응용프로그램 (146-3)을 설정할 수 있다.

[0057] 마찬가지로 계정 응용프로그램 (136)은 설정 정보 (148)를 사용하여 다른 응용프로그램 (146)-2가 설정 정보 (148)에 등록되지 않았음을 판별한다. 일부 실시예에서, 계정 응용프로그램 (136)은 설정 정보 (148)를 기반으로 다른 응용프로그램 (146-2)가 제한된 응용프로그램임을 판별한다. 예를 들어 기업은 기업 디바이스에서 소셜 미디어 응용프로그램의 사용을 제한할 수 있다. 따라서, 설정 정보 (148)에 따라, 계정 응용프로그램 (136)은 컴퓨터 디바이스 (102)가 다른 응용프로그램 (146-2)를 설치 해제하거나 다른 방식으로 비활성화하도록 한다.

[0058] 일부 구현예에서 계정 응용프로그램 (136)은 사용자가 다른 응용프로그램 (146-2)를 재-설치하거나 다른 방식으로 활성화하는 것을 영구적으로 제한할 수 있다. 예를 들면 운영 체제 (134)를 설정하여 다른 응용프로그램

(146)-2가 컴퓨터 디바이스 (102)에 설치 및/또는 활성화되는 것을 제한할 수 있다.

- [0059] 일부 실시예에서 계정 응용프로그램 (136)은 컴퓨터 디바이스 (102)를 형상화하기 위한 추가 권한이 필요할 수 있다. 예를 들어, 계정 응용프로그램 (136)은 컴퓨터 디바이스 (102)의 저장 매체에 들면 명확성을 위해 도시되지 않은 비휘발성 및/또는 휘발성 메모리)에 액세스해야 할 수 있다. 예를 들어, 저장 매체를 읽고, 쓰고, 또는 다른 방식으로 액세스하기 위해서이다. 이러한 실시예에서 계정 응용프로그램 (136) 및/또는 운영 체제 (134)는 계정 응용프로그램 (136)에 저장 매체에 대한 액세스를 허용하도록 요청할 수 있으며, 이는 사용자에게 의해 승인될 수 있고, 차례로 운영 체제 (134)에 의해 승인될 수 있다.
- [0060] 따라서 설정 정보 (148)을 사용하여 컴퓨터 디바이스 (102)를 설정함으로써, 컴퓨터 디바이스 (102)는 모든 연관된 응용프로그램, 설정 및/또는 기능을 포함하도록 자동으로 형상화될 수 있다. 예를 들어 설정 정보 (148)로 이메일 클라이언트를 설정함으로써, 사용자는 이메일을 보고 새로운 이메일을 받고 이메일 서버에 연결하고 새로운 이메일을 보낼 수 있다. 실시예는 이 맥락에서 제한되지 않는다. 또한, 설정 정보 (148)을 사용하여 컴퓨터 디바이스 (102)를 형상화하기 전에, 사용자는 이메일을 보고, 이메일을 받고, 이메일 서버에 연결하거나, 이메일 클라이언트로 이메일을 보낼 수 없다. 이메일 클라이언트를 수동으로 설정하여야 한다.
- [0061] 도 2A는 컴퓨터 디바이스 (102)의 자동 형상화의 적어도 일부를 수행하기 위해 웹 브라우저 206을 사용하는 실시예를 설명하는 개략도 (200)이다. 도 2A에 도시된 예에서, 비접촉식 카드 (104)는 비접촉식 카드 (104)를 컴퓨터 디바이스 (102)에 탭하는 것에 반응하여 암호문 (204)가 있는 URL을 생성한다. 암호문 (204)가 있는 URL에는 암호문 (122)를 참조하여 위에서 설명한 대로 생성된 암호문과 다른 관련 정보 예를 들면 암호화되지 않은 식별자가 포함될 수 있다. 보다 일반적으로, 암호문 (204)가 있는 URL은 도 1A-1D를 참조하여 위에서 설명한 대로 생성될 수 있다.
- [0062] 운영 체제 (134) (명확성을 위해 그림으로 표시하지 않음)에 의해 관독되면 운영 체제 (134)는 웹 브라우저 206 예를 들면 다른 응용프로그램 (146) 중 하나를 시작하고 암호문 (204)가 있는 URL을 웹 브라우저 206에 제공할 수 있다. 그렇게 하면 웹 브라우저 206이 암호문 (204)또는 그 일부가 있는 URL에 액세스할 수 있다. 일부 실시예에서 암호문 (204)가 있는 URL은 컴퓨터 디바이스 (102)를 자동으로 형상화하기 위한 형상화페이지로 이동한다. 실시예는 이 맥락에서 제한되지 않는다.
- [0063] 도 2B는 웹 브라우저 206이 암호문 (204)를 포함하는 URL에 액세스하는 실시예를 도시한 것이다. 예를 들어 암호문 (204)를 포함하는 하이퍼텍스트 전송 프로토콜 (HTTP) 요청에 기반한다. 도시된 바와 같이, 인증 응용프로그램 (138)은 HTTP 요청에 기반하여 암호문 (204)를 포함하는 URL을 수신할 수 있다. 그런 다음 인증 응용프로그램 (138)은 확인을 위해 암호문 (204)를 포함하는 URL에서 암호문을 추출할 수 있다. 예를 들어, 서버 (106)은 암호문을 해독하고/하거나 위에 설명된 대로 암호문에 포함된 MAC을 확인하여 암호문을 확인할 수 있다.
- [0064] 서버 (106)이 암호문을 검증하는 것 예를 들면 암호문 (204)를 사용하여 URL의 암호문을 해독하고/하거나 MAC을 검증하는 것에 따라, 서버 (106)은 계정 데이터베이스 (128)을 참조하여 연관된 설정 정보 (148)을 식별할 수 있다.
- [0065] 서버 (106)은 검증에 따라 컴퓨터 디바이스 (102), 예를 들면 웹 브라우저 206 및/또는 운영 체제 (134)에 서버 (106)이 암호문 (122)를 검증했고 설정 정보 (148)을 사용하여 컴퓨터 디바이스 (102)를 설정할 수 있음을 나타내는 응답을 추가로 전송할 수 있다. 일부 실시예에서, 인증 응용프로그램 (138)은 암호문 (204)를 사용하여 URL에서 서버 (106)에 제공된 암호화되지 않은 고유 ID (112)를 기반으로 설정 정보 (148)에 액세스할 수 있다. 실시예는 이 맥락에서 제한되지 않는다. 계정에 대한 설정 정보 (148)에 액세스에 모든 적절한 식별자를 사용할 수 있다.
- [0066] 반면에 서버 (106)이 암호문을 해독하고/하거나 MAC을 검증할 수 없는 경우, 서버 (106)은 암호문을 검증하지 않는다. 이러한 실시예에서, 인증 응용프로그램 (138)은 컴퓨터 디바이스 (102)를 자동으로 형상화하기 위해 설정 정보 (148)에 액세스하지 않기로 결정한다. 인증 응용프로그램 (138)은 실패한 암호 해독 및/또는 검증의 표시를 컴퓨터 디바이스 (102)에 전송할 수 있다.
- [0067] 도 2C는 서버 (106)이 URL의 암호문 부분을 암호문 (204)로 검증하는 실시예를 도시한 것이다. 설명한 바와 같이, 서버 (106)이 암호를 검증하면, 서버 (106)은 비접촉식 카드 (104)와 연관된 계정에 대한 설정 정보 (148)에 액세스한다. 그런 다음 서버 (106)은 설정 정보 (148)에 표시된 다수의 다른 응용프로그램을 식별할 수 있다. 식별된 각 응용프로그램에 대해, 서버 (106)은 관련 설정 정보 (148) 및/또는 그 일부를 포함하는 각각의 푸시 알림을 생성할 수 있다.

- [0068] 도시된 바와 같이 서버 (106)은 푸시 알림 (208), 푸시 알림 (210), 푸시 알림 (212)를 컴퓨터 디바이스 (102)로 전송한다. 도시된 바와 같이, 푸시 알림 (208)은 설정 정보 (148-1)을 포함하고, 푸시 알림 (210)은 설정 정보 (148-2)를 포함하고, 푸시 알림 (212)는 설정 정보 (148-N)을 포함한다. 이러한 실시예에서, 각각의 푸시 알림과 그 안의 각각의 설정 정보 인스턴스는 디바이스에서 실행되는 각각의 응용프로그램과 연관될 수 있다. 일부 실시예에서, 푸시 알림은 또한 운영 체제 (134)로 전송되는 푸시 알림을 포함할 수 있으며, 여기에는 운영 체제 (134)에 적용 가능한 설정 정보 (148) 예를 들면 블루 라이트 필터 활성화, 방해 금지 기능 등이 포함될 수 있다. 일부 실시예에서, 푸시 알림 (208, 210 및/또는 212)는 서버 (106)이 암호문 (122)를 검증했고 설정 정보 (148)을 사용하여 컴퓨터 디바이스 (102)를 설정할 수 있다는 각각의 표시를 포함한다.
- [0069] 일부 실시예에서 푸시 알림 (208, 210 및/또는 212)는 운영 체제 (134)의 백그라운드에서 수신될 수 있다. 예를 들면 컴퓨터 디바이스 (102)에 표시되도록 출력되지 않지만 해당 응용프로그램 및/또는 운영 체제 (134)에 직접 전송되는 백그라운드 푸시 알림 일 수 있다. 일부 실시예에서, 푸시 알림 (208, 210 및/또는 212)는 포그라운드 푸시 알림 예를 들면 컴퓨터 디바이스 (102)에 표시되는 알림이다. 일부 실시예에서 설정 정보 (148)에는 하나 이상의 형상화파일이 포함된다. 또한, 일부 실시예에서 설정 정보 (148-1) 내지 (148-N)의 크기는 크기 임계값을 초과할 수 있다. 이러한 실시예에서, 서버 (106)은 하나 이상의 토큰을 생성하고, 각각의 푸시 알림 (208, 210 및 212)에 해당 토큰을 포함할 수 있다. 각각의 응용프로그램은 수신되면, 수신된 토큰을 서버 (106)에 제공하여 서버 (106)에서 관련 설정 정보 (148) 및/또는 그 일부를 끌어올 수 있다.
- [0070] 도 2D는 푸시 알림 (208, 210 및 212)가 각각 다른 응용프로그램 (146-1, 146-2 및 146-N)에 의해 수신되는 실시예를 도시한 것이다. 일반적으로, 수신되면, 다른 응용프로그램 (146-1, 146-2 및 146-N)은 각각 형상화를 위해 설정 정보 (148-1, 148-2 및 148-N)을 사용할 수 있다. 예를 들어 다른 응용프로그램 (146-1)은 설정 정보 (148-1)에 따라 형상화될 수 있고, 다른 응용프로그램 (146-2)는 설정 정보 (148-2)에 따라 형상화될 수 있으며, 다른 응용프로그램 (146-N)은 설정 정보 (148-N)에 따라 형상화될 수 있다. 일부 실시예에서 다른 응용프로그램 (146-1, 146-2 및 146-N) 및/또는 운영 체제 (134)는 서버 (106)이 암호문 (122)를 검증했고 설정 정보 (148)을 사용하여 컴퓨터 디바이스 (102)를 설정할 수 있다는 서버 (106) 으로부터 표시를 수신하는 것에 따라 설정 정보 (148)의 사용을 조건화 할 수 있다.
- [0071] 일부 실시예에서 설정 정보 (148)은 각 응용프로그램 및/또는 운영 체제 (134)와 연관된 위치에 해당 형상화파일로 저장된다. 예를 들어, 다른 응용프로그램 (146-1)은 설정 정보 (148-1)을 다른 응용프로그램 (146-1)에 대한 형상화파일 예를 들면 파일 이름 및/또는 응용프로그램 (146-1)에 대한 설정 정보를 저장하는 파일과 연관된 파일 위치로 저장할 수 있다. 또 다른 실시예로서, 다른 응용프로그램 (146-1)은 설정 정보 (148-1)의 일부를 사용하여 운영 체제 (134)의 하나 이상의 파일, 레지스트리 설정 또는 기타 매개변수를 저장 및/또는 수정하여 다른 응용프로그램 (146-1)을 설정할 수 있다. 이러한 일부 실시예에서, 다른 응용프로그램 (146-1)은 설정 정보 (148-1)을 운영 체제 (134)에 제공할 수 있으며, 운영 체제 (134)는 설정 정보 (148)을 사용하여 운영 체제 (134)를 수정할 수 있다. 마찬가지로 응용프로그램 (146-2)는 설정 정보 (148-2)를 다른 응용프로그램 (146-2)에 대한 형상화파일로 저장할 수 있고, 응용프로그램 (146-N)은 설정 정보 (148-N)을 다른 응용프로그램 (146-N)에 대한 형상화파일로 저장할 수 있다.
- [0072] 일부 실시예에서 설정 정보 (148-1) 내지 (148-N)을 사용하면 새로운 설정 정보가 컴퓨터 디바이스 (102)에 기록될 수 있고, 컴퓨터 디바이스 (102)의 일부 기존 설정 정보가 수정될 수 있으며 예를 들면 값, 설정 등을 변경함으로써, 컴퓨터 디바이스 (102)의 다른 기존 설정 정보가 수정되지 않은 상태로 유지될 수 있다.
- [0073] 도 1A-도 1D에 도시된 실시예와 유사하게 설정 정보 (148)은 컴퓨터 디바이스 (102)에서 응용프로그램을 설치 및/또는 제거하는 데 사용될 수 있다. 예를 들어, 운영 체제 (134)는 푸시 알림 210을 수신하고 응용프로그램 (146-2)가 컴퓨터 디바이스 (102)에 설치되지 않았음을 확인할 수 있다. 이러한 실시예에서, 운영 체제 (134)는 응용프로그램 스토어, 인터넷 등 예서와 같이 컴퓨터 디바이스 (102)에 응용프로그램 (146-2)를 다운로드하여 설치할 수 있다. 마찬가지로, 설정 정보 (148-N)이 응용프로그램 (146-N)이 디바이스에 설치되도록 허용되지 않았거나 설정 정보 (148)에 등록되지 않았음을 지칭하는 경우, 설정 정보 (148-N)은 응용프로그램 (146-N)이 컴퓨터 디바이스 (102)에서 응용프로그램 (146-N)의 제거 및/또는 비활성화를 시작하도록 할 수 있다.
- [0074] 유리하게 설정 정보 (148)은 컴퓨터 디바이스 (102)를 자동으로 설정 및/또는 복원하는 데 사용된다. 암호문의 검증을 요구함으로써 컴퓨터 디바이스 (102)의 형상화가 안전한 방식으로 완료된다. 보다 일반적으로, 사용자는 백업을 빠르게 복원하고, 새로운 디바이스를 형상화하고, 설정 정보 (148)을 한 디바이스에서 다른 디바이스로 적용할 수 있다. 실시예는 이러한 맥락에 제한되지 않는다.

- [0075] 공개된 실시예에 대한 동작은 다음 도면을 참조하여 추가로 설명될 수 있다. 일부 도면에는 논리 흐름이 포함될 수 있다. 여기에 제시된 이러한 도면에는 특정 논리 흐름이 포함될 수 있지만, 논리 흐름은 여기에 설명된 일반적인 기능을 구현할 수 있는 방법의 예를 제공할 뿐임을 알 수 있다. 또한, 주어진 논리 흐름은 달리 표시되지 않는 한 반드시 제시된 순서대로 실행될 필요는 없습니다. 더욱이, 논리 흐름에 설명된 모든 행위가 일부 실시예에서 요구되는 것은 아니다. 또한 주어진 논리 흐름은 하드웨어 요소, 프로세서에 의해 실행되는 소프트웨어 요소 또는 이들의 임의의 조합에 의해 구현될 수 있다. 실시예는 이러한 맥락에 제한되지 않는다.
- [0076] 도 3은 논리 흐름 또는 루틴 300의 실시예를 도시한 것이다. 논리 흐름 300은 여기에 설명된 하나 이상의 실시예에 의해 실행되는 일부 또는 모든 동작을 나타낼 수 있다. 예를 들어, 논리 흐름 300은 설정 정보와 비접촉식 카드를 사용하여 디바이스를 자동으로 설정하는 일부 또는 모든 동작을 포함할 수 있다. 실시예는 이 맥락에서 제한되지 않는다.
- [0077] 블록 302에서 루틴 300은 컴퓨터 디바이스 (102)에서 실행되는 계정 응용프로그램 (136)에 의해 계정과 연관된 비접촉식 카드 (104)로부터 암호문 예를 들면 암호문 (122) 및/또는 암호문 (204)가 있는 URL의 암호문을 수신한다. 블록 304에서 루틴 300은 계정 응용프로그램 (136)을 통해 암호문을 서버 (106)으로 전송한다. 블록 306에서 루틴 300은 서버가 암호문을 검증하는 것을 기반으로 계정 응용프로그램 (136)을 통해 계정과 관련된 다수의 응용프로그램에 대한 설정 정보 (148)을 수신한다. 서버 (106)은 설정 정보 (148)과 함께 서버 (106)이 암호문 (122)를 검증했으며 설정 정보 (148)을 사용하여 컴퓨터 디바이스 (102)를 설정할 수 있음을 지칭하는 표시를 포함할 수 있다. 응용 프로그램에는 다른 응용 프로그램 (146), 운영 체제 (134) 및/또는 계정 응용 프로그램 (136)이 포함될 수 있다. 블록 308에서 루틴 300은 설정 정보 (148)을 기반으로 컴퓨터 디바이스 (102)의 각 응용 프로그램의 해당 형상화를 수정한다.
- [0078] 도 4는 논리 흐름 또는 루틴 (400)의 실시예를 설명한다. 논리 흐름 (400)은 여기에 설명된 하나 이상의 실시예에 의해 실행되는 일부 또는 모든 작업을 나타낼 수 있다. 예를 들어, 논리 흐름 (400)은 설정 정보와 비접촉식 카드를 사용하여 디바이스를 자동으로 설정하는 일부 또는 모든 작업을 포함할 수 있다. 실시예는 이 맥락에서 제한되지 않는다.
- [0079] 블록 402에서 루틴 (400)은 서버 (106)에 계정 및/또는 컴퓨터 디바이스 (102)와 연관된 각 응용프로그램에 대한 다수의 응용프로그램 및 설정 정보를 등록한다. 그렇게 하면 설정 정보 (148)이 계정 데이터베이스 (128)의 계정과 연관된 적어도 하나의 항목에 저장될 수 있다. 블록 404에서 루틴 (400)은 컴퓨터 디바이스 (102)에 의해 계정과 연관된 비접촉식 카드 (104)로부터 암호문 예를 들면 암호문 (122) 및/또는 암호문 (204)가 있는 URL의 암호문을 수신한다. 블록 406에서 루틴 (400)은 컴퓨터 디바이스 (102)를 통해 암호문을 서버 (106)으로 전송한다. 블록 408에서 루틴 (400)은 컴퓨터 디바이스 (102)가 서버 (106)으로부터 수신한 응답을 기반으로 서버 (106)이 암호문을 검증했으며 설정 정보 (148)을 사용하여 컴퓨터 디바이스 (102)를 설정할 수 있는지 확인한다. 블록 410에서 루틴 (400)은 컴퓨터 디바이스 (102)가 서버 (106)이 암호문을 검증한 것을 기반으로 계정과 관련된 여러 응용프로그램에 대한 설정 정보 (148)을 수신한다. 응용프로그램에는 다른 응용프로그램 (146), 운영 체제 (134) 및/또는 계정 응용프로그램 (136)이 포함될 수 있다.
- [0080] 블록 412에서 루틴 (400)은 컴퓨터 디바이스 (102)에 제1 응용프로그램예를 들면 다른 응용프로그램 중 하나 (146))이 컴퓨터 디바이스 (102)에 설치되지 않았다는 결정에 따라 디바이스에 제1 응용프로그램을 다운로드한다. 블록 414에서 루틴 (400)은 컴퓨터 디바이스 (102)에 의해 디바이스에 제1 응용프로그램을 설치한다. 블록 416에서 루틴 (400)은 설정 정보 (148)에 따라 컴퓨터 디바이스 (102)에서 제2 응용프로그램예를 들면 다른 응용프로그램 중 하나 (146))을 설치 해제한다. 예를 들어, 설정 정보 (148)은 제2 응용프로그램을 설치 해제하거나 비활성화하도록 지정할 수 있다. 블록 418에서 루틴 (400)은 컴퓨터 디바이스 (102)에 의해 설정 정보 (148)에 따라 각 응용프로그램의 해당 형상화를 수정한다.
- [0081] 도 5는 논리 흐름 또는 루틴 (500)의 실시예를 설명한다. 논리 흐름 (500)은 여기에 설명된 하나 이상의 실시예에 의해 실행되는 일부 또는 모든 작업을 나타낼 수 있다. 예를 들어, 논리 흐름 (500)은 설정 정보와 비접촉식 카드를 사용하여 디바이스를 자동으로 설정하는 일부 또는 모든 작업을 포함할 수 있다. 이 실시예는 이 맥락에서 제한되지 않는다.
- [0082] 블록 502에서 루틴 (500)은 서버에 다수의 응용프로그램과 각 응용프로그램에 대한 설정 정보를 계정에 등록한다. 그렇게 하면 설정 정보 (148)이 계정 데이터베이스 (128)의 계정과 관련된 항목에 저장될 수 있다. 블록 504에서 루틴 (500)은 컴퓨터 디바이스 (102)를 통해 계정과 관련된 비접촉식 카드 (104)에서 암호문 (204)가

포함된 URL을 수신한다.

- [0083] 블록 506에서 루틴 (500)은 컴퓨터 디바이스 (102)에 의해 암호문 (204)가 있는 URL에 기반한 웹 브라우저를 시작한다. 블록 508에서 루틴 (500)은 웹 브라우저 206에 의해 적어도 암호문을 서버 (106)에 전송한다. 예를 들어 암호문 (204)가 있는 URL과 연관된 웹 페이지에 액세스한다. 블록 510에서 루틴 (500)은 웹 브라우저 206에 의해 서버로부터 수신된 응답에 따라 서버가 암호문 (204)가 있는 URL에서 암호문을 검증했으며 설정 정보 (148)를 사용하여 컴퓨터 디바이스 (102)를 설정할 수 있음을 확인한다.
- [0084] 블록 512에서 루틴 (500)은 컴퓨터 디바이스 (102)가 서버에 의한 암호문 검증을 기반으로 계정과 관련된 다수의 응용프로그램에 대한 설정 정보 (148)를 수신한다. 응용프로그램에는 다른 응용프로그램 (146), 운영 체제 (134) 및/또는 계정 응용프로그램 (136)이 포함될 수 있다. 블록 514에서 루틴 (500)은 컴퓨터 디바이스 (102)에 제1 응용프로그램이 설치되지 않았다는 결정에 따라 컴퓨터 디바이스 (102)에 제1 응용프로그램을 다운로드한다. 블록 516에서 루틴 (500)은 컴퓨터 디바이스 (102)에 의해 컴퓨터 디바이스 (102)에 제1 응용프로그램을 설치한다. 블록 518에서 루틴 (500)은 설정 정보 (148)에 따라 컴퓨터 디바이스 (102)에서 제2 응용프로그램에를 들면 다른 응용프로그램 중 하나 (146)을 설치 해제한다. 예를 들어, 설정 정보 (148)은 제2 응용프로그램을 설치 해제하거나 비활성화하도록 지정할 수 있다. 블록 520에서 루틴 (500)은 컴퓨터 디바이스 (102)에 의해 설정 정보 (148)에 따라 각 응용프로그램의 해당 형상화를 수정한다.
- [0085] 도 6A는 비접촉식 카드 (104)의 예시 형상화를 도시한 개략도 (600)으로, 여기에는 서비스 제공자가 발급한 신용 카드, 직불 카드 또는 상품권과 같은 지불 카드가 포함될 수 있으며, 비접촉식 카드 (104)의 앞면 또는 뒷면에 서비스 제공자 표시 602로 표시된다.
- [0086] 일부 실시예에서 비접촉식 카드 (104)는 지불 카드와 관련이 없으며, 제한 없이 신분증을 포함할 수 있다. 일부 실시예에서 거래 카드는 듀얼 인터페이스 비접촉식 지불 카드, 보상 카드 등을 포함할 수 있다. 비접촉식 카드 (104)는 기관 (604)를 포함할 수 있으며, 기관은 플라스틱, 금속 및 기타 재료로 형상화된 단일 층 또는 하나 이상의 적층 층을 포함할 수 있다. 예시적인 기관 재료에는 폴리염화비닐, 폴리염화비닐 아세테이트, 아크릴로니트릴 부타디엔 스티렌, 폴리카보네이트, 폴리에스터, 양극산화 티타늄, 팔라듐, 금, 탄소, 종이 및 생분해성 재료가 포함된다. 일부 실시예에서 비접촉식 카드 (104)는 ISO/IEC 7816 표준의 ID-1 형식을 준수하는 물리적 특성을 가질 수 있으며, 거래 카드는 그렇지 않으면 ISO/IEC 14443 표준을 준수할 수 있다. 그러나 본 공개에 따른 비접촉식 카드 (104)는 다른 특성을 가질 수 있으며, 본 공개는 거래 카드가 지불 카드에 구현될 것을 요구하지 않는다는 것이 이해된다.
- [0087] 비접촉식 카드 (104)는 또한 카드의 앞면 및/또는 뒷면에 표시된 식별 정보 606과 접촉 패드 (608)를 포함할 수 있다. 접촉 패드 (608)은 하나 이상의 패드를 포함할 수 있으며, 거래 카드를 통해 ATM, 사용자 디바이스, 스마트폰, 랩톱, 데스크톱 또는 태블릿 컴퓨터와 같은 다른 클라이언트 디바이스와 접촉을 설정하도록 형상화될 수 있다. 접촉 패드는 ISO/IEC 7(816) 표준과 같은 하나 이상의 표준에 따라 설계될 수 있으며, EMV 프로토콜에 따라 통신을 가능하게 할 수 있다. 비접촉식 카드 (104)는 또한 도 6B에서 추가로 논의될 바와 같이 처리 회로, 안테나 및 기타 컴포넌트를 포함할 수 있다. 이러한 컴포넌트는 접촉 패드 (608) 뒤 또는 기관 (604)의 다른 곳, 예를 들어, 기관(604)의 다른 층 내에 있고, 접촉 패드 (608)과 전기적으로 및 물리적으로 결합될 수 있다. 비접촉식 카드 (104)는 또한 카드 뒷면에 위치할 수 있는 자기 스트립 또는 테이프를 포함할 수 있다. 도 6A에 도시되지 않음. 비접촉식 카드 (104)는 또한 NFC 프로토콜을 통해 통신할 수 있는 안테나와 결합된 근거리 무선 통신(NFC) 디바이스를 포함할 수 있다. 실시예는 이러한 방식으로 제한되지 않는다.
- [0088] 도 6A에 도시된 바와 같이, 6B, 비접촉식 카드 (104)의 접촉 패드 (608)은 프로세서 (612), 메모리 (108) 및 하나 이상의 통신 인터페이스 (124)를 포함하여 정보를 저장, 처리 및 통신하기 위한 처리 회로망 (610)을 포함할 수 있다. 처리 회로망 (610)은 여기에 설명된 기능을 수행하는 데 필요한 프로세서, 메모리, 오류 및 패리티/CRC 검사기, 데이터 인코더, 충돌 방지 알고리즘, 컨트롤러, 명령 디코더, 보안 기본 요소 및 변조 방지 하드웨어를 포함한 추가 컴포넌트를 포함할 수 있다는 것이 이해된다.
- [0089] 메모리 (108)은 읽기 전용 메모리, 한 번 쓰기-다중 읽기 메모리 또는 읽기/쓰기 메모리, 예를 들어 RAM, ROM 및 EEPROM일 수 있으며, 비접촉식 카드 (104)는 이러한 메모리 중 하나 이상을 포함할 수 있다. 읽기 전용 메모리는 읽기 전용 또는 일회성 프로그래밍으로 공장에서 프로그래밍 될 수 있다. 일회성 프로그래밍은 한 번 쓰고 여러 번 읽을 수 있는 기회를 제공한다. 한 번 쓰기/다중 읽기 메모리는 메모리 칩이 공장을 떠난 후의 시점에 프로그래밍 될 수 있다. 메모리가 프로그래밍 되면 다시 쓸 수 없지만 여러 번 읽을 수 있다. 읽기/쓰기 메모리는 공장을 떠난 후 여러 번 프로그래밍 되고 다시 프로그래밍 될 수 있다. 읽기/쓰기 메모리는 또한 공장을 떠

난 후 여러 번 읽을 수 있다. 어떤 경우에는 메모리 (108)이 프로세서 (612)가 암호화된 데이터를 실행하기 위해 실행하는 암호화 알고리즘을 활용하는 암호화된 메모리일 수 있다. 메모리 (108)은 하나 이상의 애플릿 (110), 하나 이상의 카운터 (116), 고유 ID (112), 마스터 키 (114), UDK (118), 다양화 키 (120), PAN 시퀀스 (144) 및 설정 정보 (148)를 저장하도록 형상화될 수 있다. 설정 정보 (148)은 서버 (106)에서 생성된 하나 이상의 토큰을 포함할 수 있다.

[0090] 하나 이상의 애플릿 (110)은 Java® 카드 애플릿과 같은 하나 이상의 비접촉식 카드 (104)에서 실행되도록 형상화된 하나 이상의 소프트웨어 응용프로그램을 포함할 수 있다. 그러나 애플릿 (110)은 Java 카드 애플릿에 국한되지 않으며, 대신 비접촉식 카드 또는 제한된 메모리를 갖는 다른 디바이스에서 작동할 수 있는 모든 소프트웨어 응용프로그램일 수 있다. 하나 이상의 카운터 (116)은 정수를 저장하기에 충분한 숫자 카운터를 포함할 수 있다. 고유 ID (112)는 비접촉식 카드 (104)에 할당된 고유한 영숫자 식별자를 포함할 수 있으며, 식별자는 비접촉식 카드 (104)를 다른 비접촉식 카드 (104)와 구별할 수 있다. 일부 실시예에서, 고유 ID (112)는 고객과 해당 고객에게 할당된 계정을 모두 식별할 수 있다.

[0091] 상기 실시예의 프로세서 (612) 및 메모리 요소는 접촉 패드 (608)를 참조하여 설명하지만, 본 공개는 이에 한정되지 않는다. 이러한 요소는 접촉 패드 (608) 외부에 구현되거나 접촉 패드 (608)과 완전히 분리되거나 접촉 패드 (608) 내부에 위치한 프로세서 (612) 및 메모리 (108) 요소에 더하여 추가 요소로 구현될 수 있다는 것이 이해된다.

[0092] 일부 실시예에서 비접촉식 카드 (104)는 하나 이상의 안테나(들) 614를 포함할 수 있다. 하나 이상의 안테나(들) 614는 비접촉식 카드 (104) 내부와 접촉 패드 (608)의 처리 회로망 610 주위에 배치될 수 있다. 예를 들어, 하나 이상의 안테나(들) 614는 처리 회로망 610과 일체형일 수 있고, 하나 이상의 안테나(들) 614는 외부 부스터 코일과 함께 사용될 수 있다. 또 다른 실시예로서, 하나 이상의 안테나(들) 614는 접촉 패드 (608) 및 처리 회로망 610 외부에 있을 수 있다.

[0093] 실시예에서 비접촉식 카드 (104)의 코일은 공심 변압기의 2차로 작용할 수 있다. 단말기는 전력을 차단하거나 진폭 변조를 통해 비접촉식 카드 (104)와 통신할 수 있다. 비접촉식 카드 (104)는 비접촉식 카드 (104)의 전원 연결의 갭을 사용하여 단말기에서 전송된 데이터를 추론할 수 있으며, 이는 하나 이상의 커패시터를 통해 기능적으로 유지될 수 있다. 비접촉식 카드 (104)는 비접촉식 카드 (104)의 코일에 부하를 전환하거나 부하 변조를 통해 다시 통신할 수 있다. 부하 변조는 간섭을 통해 단말기의 코일에서 감지될 수 있다. 보다 일반적으로, 안테나(들) 614, 프로세서 (612) 및/또는 메모리 (108)를 사용하여 비접촉식 카드 (104)는 NFC, 블루투스 및/또는 Wi-Fi 통신을 통해 통신하기 위한 통신 인터페이스를 제공한다.

[0094] 위에서 설명한 바와 같이, 비접촉식 카드 (104)는 JavaCard와 같이 메모리가 제한된 스마트 카드 또는 기타 디바이스에서 작동할 수 있는 소프트웨어 플랫폼에 구축될 수 있으며, 하나 이상의 응용프로그램 또는 애플릿이 안전하게 실행될 수 있다. 애플릿 (110)은 다양한 모바일 응용프로그램 기반 사용 사례에서 다중 인증(MFA)을 위한 일회용 비밀번호(OTP)를 제공하기 위해 비접촉식 카드에 추가될 수 있다. 애플릿 (110)은 모바일 NFC 리더 예를 들면 모바일 컴퓨터 디바이스 (102) 또는 POS 단말기)와 같은 리더의 근거리 데이터 교환 요청과 같은 하나 이상의 요청에 응답하고 NDEF 텍스트 태그로 인코딩된 암호화적으로 안전한 OTP를 포함하는 NDEF 메시지를 생성하도록 형상화될 수 있다. NDEF 메시지에는 암호문 (122) 또는 암호문 (204)이 있는 URL과 같은 암호문과 다른 데이터가 포함될 수 있다.

[0095] NDEF OTP의 한 예는 NDEF 단축 레코드 레이아웃(SR=1)이다. 이러한 실시예에서 하나 이상의 애플릿 (110)은 OTP를 NDEF 유형 4 잘 알려진 유형 텍스트 태그로 인코딩하도록 형상화될 수 있다. 일부 실시예에서, NDEF 메시지는 하나 이상의 레코드를 포함할 수 있다. 애플릿 (110)은 OTP 레코드 외에도 하나 이상의 정적 태그 레코드를 추가하도록 형상화될 수 있다.

[0096] 일부 실시예에서, 하나 이상의 애플릿 (110)은 RFID 태그를 에뮬레이션 하도록 형상화될 수 있다. RFID 태그는 하나 이상의 다형성 태그를 포함할 수 있다. 일부 실시예에서, 태그가 읽힐 때마다 비접촉식 카드의 진위성을 나타낼 수 있는 다른 암호화 데이터가 제공된다. 하나 이상의 애플릿 (110)을 기반으로, 태그의 NFC 판독이 처리될 수 있고, 데이터는 은행 시스템의 서버와 같은 서버로 전송될 수 있으며, 데이터는 서버에서 검증될 수 있다.

[0097] 일부 실시예에서 비접촉식 카드 (104) 및 서버는 카드가 적절하게 식별될 수 있도록 특정 데이터를 포함할 수 있다. 비접촉식 카드 (104)는 하나 이상의 고유 식별자(그룹에 표시되지 않음)를 포함할 수 있다. 읽기 작업이

발생할 때마다 카운터 (116)은 증가하도록 형상화될 수 있다. 일부 실시예에서, 비접촉식 카드 (104)의 데이터가 읽힐 때마다 예를 들면 모바일 기기에 의해, 카운터 (116)은 검증을 위해 서버로 전송되고 카운터 (116)이 서버의 카운터와 동일 한지 검증의 일부로 여부를 판별한다.

[0098] 하나 이상의 카운터 (116)은 재생 공격을 방지하도록 형상화될 수 있다. 예를 들어, 암호문이 획득되어 재생된 경우, 카운터 (116)이 읽히거나 사용되거나 다른 방식으로 전달된 경우 해당 암호문은 즉시 거부된다. 카운터 (116)이 사용되지 않은 경우 재생될 수 있다. 일부 실시예에서, 비접촉식 카드 (104)에서 증가되는 카운터는 거래에 대해 증가되는 카운터와 다르다. 비접촉식 카드 (104)는 비접촉식 카드 (104)의 애플릿 (110) 간에 통신이 없기 때문에 응용프로그램 거래 카운터 (116)을 결정할 수 없다. 일부 실시예에서, 비접촉식 카드 (104)는 거래 애플릿일 수 있는 제1 애플릿 440-1과 제2 애플릿 440-2를 포함할 수 있다. 각 애플릿 440-1 및 440-2는 각각의 카운터 (116)을 포함할 수 있다.

[0099] 일부 실시예에서 카운터 (116)은 동기화되지 않을 수 있다. 일부 실시예에서, 각도에서 읽는 것과 같이 거래를 시작하는 우발적인 읽기를 설명하기 위해 카운터 (116)은 증가할 수 있지만 응용프로그램은 카운터 (116)을 처리하지 않는다. 일부 실시예에서, 모바일 디바이스 10이 깨어날 때 NFC가 활성화되고 컴퓨터 디바이스 (102)는 사용 가능한 태그를 읽도록 형상화될 수 있지만 읽기에 대한 응답으로 아무런 조치도 취하지 않는다.

[0100] 카운터 (116)을 동기화 상태로 유지하기 위해 백그라운드 응용프로그램과 같은 응용프로그램이 실행될 수 있으며, 이는 컴퓨터 디바이스 (102)가 깨어날 때 감지하고 감지로 인해 발생한 읽기를 나타내는 बैंक 시스템의 서버와 동기화하여 카운터 (116)을 앞으로 이동하도록 형상화될 수 있다. 다른 실시예에서, 해시된 일회용 비밀번호가 사용되어 오동작 창이 허용될 수 있다. 예를 들어, 임계값이 10 이내이면 카운터 (116)은 앞으로 이동하도록 형상화될 수 있다. 그러나 다른 임계값 숫자, 예를 들어 10 또는 1000 이내이면 재동기화를 수행하기 위한 요청이 처리될 수 있으며, 이는 하나 이상의 응용프로그램을 통해 사용자가 사용자의 디바이스를 통해 한 번 이상 탭, 제스처 또는 기타 방식으로 표시하도록 요청한다. 카운터 (116)이 적절한 순서로 증가하면 사용자가 그렇게 했다는 것을 알 수 있다.

[0101] 카운터 (116), 마스터 키 (114), UDK (118) 및 다양화 키 (120)을 참조하여 여기에 설명된 키 다양화 기술은 키 다양화 기술의 암호화 및/또는 복호화의 한 예이다. 이 예시 키 다양화 기술은 공개를 제한하는 것으로 간주되어서는 안 되며, 공개는 다른 유형의 키 다양화 기술에도 동일하게 적용 가능하다.

[0102] 비접촉식 카드 (104)의 생성 프로세스 동안 두 개의 암호화 키가 카드당 고유하게 할당될 수 있다. 암호화 키는 데이터의 암호화와 복호화에 모두 사용될 수 있는 대칭 키를 포함할 수 있다. EMV에서 트리플 DES(3DES) 알고리즘을 사용할 수 있으며, 비접촉식 카드 (104)의 하드웨어로 구현된다. 키 다양화 프로세스를 사용하여, 키가 필요한 각 엔터티에 대한 고유 식별 정보를 기반으로 마스터 키에서 하나 이상의 키를 파생할 수 있다.

[0103] 일부 실시예에서 취약성에 취약할 수 있는 3DES 알고리즘의 결함을 극복하기 위해, 세션 키를 파생할 수 있지만 예를 들면 세션당 고유 키, 마스터 키를 사용하는 대신, 고유한 카드 파생 키, 예를 들면 UDK (118)와 카운터를 다양화 데이터로 사용할 수 있다. 예를 들어, 비접촉식 카드 (104)를 작동에 사용할 때마다 메시지 인증 코드 (MAC)를 생성하고 암호화를 수행하는 데 다른 키를 사용할 수 있다. 이는 3중 계층의 암호화를 초래한다. 세션 키는 하나 이상의 애플릿에서 생성될 수 있으며 하나 이상의 알고리즘 (EMV 4.3 Book 2 A1.3.1 공통 세션 키 도출에 정의됨)을 사용하여 응용프로그램 트랜잭션 카운터를 사용하여 도출될 수 있다.

[0104] 또한 각 카드에 대한 증가는 고유할 수 있으며, 개인화에 의해 할당되거나, 일부 식별 정보에 의해 알고리즘적으로 할당될 수 있다. 예를 들어, 홀수 카드는 2씩 증가하고 짝수 카드는 5씩 증가할 수 있다. 일부 실시예에서, 증가는 순차적 읽기에서 달라질 수 있으며, 한 카드가 1, 3, 5, 2, 2, ... 반복되는 순서대로 증가할 수 있다. 특정 시퀀스 또는 알고리즘 시퀀스는 개인화 시점에 정의되거나, 고유 식별자에서 파생된 하나 이상의 프로세스에서 정의될 수 있다. 이는 재생 공격자가 소수의 카드 인스턴스에서 일반화하기 어렵게 만들 수 있다. 인증 메시지는 16진수 ASCII 형식의 텍스트 NDEF 레코드의 내용으로 전달될 수 있다. 다른 실시예에서, NDEF 레코드는 16진수 형식으로 인코딩 될 수 있다.

[0105] 도 7은 예시 실시예에 따른 NDEF 단축 레코드 레이아웃(SR=1) 데이터 구조 700을 도시한 것이다. 하나 이상의 애플릿 (110)은 OTP를 NDEF 유형 4 잘 알려진 유형 텍스트 태그로 인코딩하도록 형상화될 수 있다. 일부 실시예에서, NDEF 메시지는 하나 이상의 레코드를 포함할 수 있다. 애플릿은 OTP 레코드 외에도 하나 이상의 정적 태그 레코드를 추가하도록 형상화될 수 있다. 예시적 태그는 다음을 포함되되, 이에 국한되지 않는다. 태그 유형: 잘 알려진 유형, 텍스트, 인코딩 영어(en); 애플릿 ID: D27(600)00(850)101; 기능: 읽기 전용 액세스; 인코딩:

인증 메시지는 ASCII 16진수로 인코딩 될 수 있다; 유형-길이-값(TLV) 데이터는 NDEF 메시지를 생성하는 데 사용될 수 있는 개인화 매개변수로 제공될 수 있다. 실시예에서, 인증 템플릿은 실제 동적 인증 데이터를 제공하기 위한 잘 알려진 인덱스가 있는 제1 레코드를 포함할 수 있다. 데이터 구조 700은 암호문 (122) 또는 암호문 (204)가 포함된 URL과 같은 암호문과 애플릿 (110)에서 제공하는 다른 데이터를 포함할 수 있다.

[0106] 도 8은 이전에 설명된 다양한 실시예를 구현하는 데 적합한 예시적인 컴퓨터 아키텍처 (800)의 실시예를 설명한다. 한 실시예에서, 컴퓨터 아키텍처 (800)은 컴퓨터 아키텍처 (100) 및/또는 (200)을 포함하거나 그 일부로 구현될 수 있다. 일부 실시예에서, 컴퓨터 시스템 (800)은 예를 들어 비접촉식 카드 (104), 컴퓨터 디바이스 (102) 및/또는 서버 (106)을 나타낼 수 있다. 실시예는 이 맥락에서 제한되지 않는다. 보다 일반적으로, 컴퓨터 아키텍처 (800)은 도 1A-7을 참조하여 여기에 설명된 모든 논리, 응용프로그램, 시스템, 방법, 디바이스 및 기능을 구현하도록 형상화된다.

[0107] 본 출원에서 사용되는 용어 "시스템" 및 "컴포넌트"는 하드웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어 또는 실행 중인 소프트웨어인 컴퓨터 관련 엔티티를 지칭하도록 의도되며, 이러한 예는 예시적인 컴퓨터 컴퓨터 아키텍처 (800)에서 제공된다. 예를 들어, 컴포넌트는 프로세서에서 실행되는 프로세스, 프로세서, 하드 디스크 드라이브, 여러 저장 드라이브 (광학 및/또는 자기 저장 매체), 객체, 실행 파일, 실행 스레드, 프로그램 및/또는 컴퓨터일 수 있지만 이에 국한되지 않는다. 예를 들어, 서버에서 실행되는 응용프로그램과 서버는 모두 컴포넌트가 될 수 있다. 하나 이상의 컴포넌트는 프로세스 및/또는 실행 스레드 내에 상주할 수 있으며, 컴포넌트는 하나의 컴퓨터에 로컬화되거나 2 대 이상의 컴퓨터에 분산될 수 있다.

[0108] 또한 컴포넌트는 다양한 유형의 통신 매체를 통해 서로 통신적으로 결합되어 작업을 조정할 수 있다. 조정에는 단방향 또는 양방향 정보 교환이 포함될 수 있다. 예를 들어, 컴포넌트는 통신 매체를 통해 통신되는 신호의 형태로 정보를 통신할 수 있다. 정보는 다양한 신호 라인에 할당된 신호로 구현될 수 있다. 이러한 할당에서 각 메시지는 신호이다. 그러나 추가 실시예에서는 대안적으로 데이터 메시지를 사용할 수 있다. 이러한 데이터 메시지는 다양한 연결을 통해 전송될 수 있다. 대표적인 연결에는 병렬 인터페이스, 직렬 인터페이스 및 버스 인터페이스가 포함된다.

[0109] 컴퓨터 아키텍처 (800)에는 하나 이상의 프로세서, 멀티코어 프로세서, 코프로세서, 메모리 디바이스, 칩셋, 컨트롤러, 주변 디바이스, 인터페이스, 발진기, 타이밍 디바이스, 비디오 카드, 오디오 카드, 멀티미디어 입출력 (I/O) 컴포넌트, 전원 공급 디바이스 등과 같은 다양한 공통 컴퓨터 요소가 포함된다. 그러나 실시예는 컴퓨터 컴퓨터 아키텍처 (800)에 의한 구현으로 제한되지 않는다.

[0110] 도 1에 도시된 바와 같이, 컴퓨터 아키텍처 (800)은 프로세서 (802), 시스템 메모리 804 및 시스템 버스 (806)를 포함하는 컴퓨터 (812)를 포함한다. 프로세서 (802)는 다양한 상업적으로 이용 가능한 프로세서 중 하나일 수 있다. 컴퓨터 (812)는 컴퓨터 디바이스 (102) 및/또는 서버 (106)을 나타낼 수 있다.

[0111] 시스템 버스 (806)은 시스템 메모리 804를 포함하되 이에 국한되지 않는 시스템 컴포넌트에 대한 프로세서 (802)에 대한 인터페이스를 제공한다. 시스템 버스 (806)은 다양한 유형의 버스 구조 중 하나일 수 있으며, 이는 다양한 상업적으로 이용 가능한 버스 아키텍처를 사용하여 메모리 버스(메모리 컨트롤러가 있거나 없음), 주변 디바이스 버스 및 로컬 버스에 추가로 상호 연결할 수 있다. 인터페이스 어댑터는 슬롯 아키텍처를 통해 시스템 버스 (806)에 연결할 수 있다. 예시 슬롯 아키텍처는 제한 없이 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) 등을 포함할 수 있다.

[0112] 컴퓨터 아키텍처 (800)은 다양한 제조품을 포함하거나 구현할 수 있다. 제조품에는 논리를 저장하기 위한 컴퓨터 판독 가능 저장 매체가 포함될 수 있다.

[0113] 컴퓨터 판독 가능 저장 매체의 예로는 휘발성 메모리 또는 비휘발성 메모리, 이동식 또는 비이동식 메모리, 지울 수 있거나 지울 수 없는 메모리, 쓰기 가능 또는 다시 쓰기 가능한 메모리 등을 포함하여 전자 데이터를 저장할 수 있는 모든 유형의 매체가 포함될 수 있다. 논리의 예로는 소스 코드, 컴파일된 코드, 해석된 코드, 실행 가능한 코드, 정적 코드, 동적 코드, 객체 지향 코드, 시각적 코드 등과 같은 모든 적합한 유형의 코드를 사용하여 구현된 실행 가능한 컴퓨터 프로그램 명령어가 포함될 수 있다. 실시예는 또한 적어도 부분적으로 비일시적 컴퓨터 판독 가능 매체에 포함된 명령어로 구현될 수 있으며, 이는 하나 이상의 프로세서가 읽고 실행하여 여기에 설명된 작업을 수행할 수 있다.

[0114] 시스템 메모리 (804)는 읽기 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 동적 RAM(DRAM), 이중 데이터 속도

DRAM(DDRAM), 동기 DRAM(SDRAM), 정적 RAM(SRAM), 프로그래밍 가능 ROM(PROM), 지울 수 있는 프로그래밍 가능 ROM(EPROM), 전기적으로 지울 수 있는 프로그래밍 가능 ROM(EEPROM), 플래시 메모리, 강유전체 폴리머 메모리, 오보닉 메모리, 상변화 또는 강유전체 메모리와 같은 폴리머 메모리, 실리콘 산화물-질화물-산화물-실리콘(SONOS) 메모리, 자기 또는 광학 카드, RAID(Redundant Array of Independent Disks) 드라이브와 같은 디바이스 어레이, 솔리드 스테이트 메모리 디바이스예를 들면 USB 메모리, 솔리드 스테이트 드라이브(SSD) 및 정보를 저장하는 데 적합한 다른 유형의 저장 매체와 같은 하나 이상의 고속 메모리 유닛 형태의 다양한 유형의 컴퓨터 판독 가능 저장 매체를 포함할 수 있다. 도 8에 도시된 실시예에서, 시스템 메모리 804는 비휘발성 808 및/또는 휘발성(810)을 포함한다. 기본 입출력 시스템(BIOS)은 비휘발성 808에 저장될 수 있다.

[0115] 컴퓨터(812)는 내부(또는 외부) 하드 디스크 드라이브(814), 이동식 자기 디스크 818에서 읽거나 쓰기 위한 자기 디스크 드라이브(816), 이동식 광 디스크(822)예를 들면 CD-ROM 또는 DVD)에서 읽거나 쓰기 위한 광 디스크 드라이브(820)을 포함하여 하나 이상의 저속 메모리 유닛의 형태로 다양한 유형의 컴퓨터 판독 가능 저장 매체를 포함할 수 있다. 하드 디스크 드라이브(814), 자기 디스크 드라이브(816) 및 광 디스크 드라이브(820)은 각각 HDD 인터페이스(824), FDD 인터페이스(826) 및 광 디스크 드라이브 인터페이스(828)에 의해 시스템 버스(806)에 연결될 수 있다. 외부 드라이브 구현을 위한 HDD 인터페이스(824)는 유니버설 시리얼 버스(USB) 및 IEEE 1394 인터페이스 기술 중 하나 이상 또는 둘 다를 포함할 수 있다.

[0116] 드라이브 및 관련 컴퓨터 판독 가능 매체는 데이터, 데이터 구조, 컴퓨터 실행 가능 명령어 등의 휘발성 및/또는 비휘발성 저장소를 제공한다. 예를 들어, 다수의 프로그램 모듈이 드라이브 및 비휘발성(808), 및 휘발성(810)에 저장될 수 있으며, 여기에는 운영 체제(830), 하나 이상의 응용프로그램(832), 다른 프로그램 모듈(834) 및 프로그램 데이터(836)이 포함된다. 한 구현예에서, 하나 이상의 응용프로그램(832), 다른 프로그램 모듈(834) 및 프로그램 데이터(836)은 예를 들어 시스템(100)의 다양한 응용프로그램 및/또는 컴포넌트를 포함할 수 있다.

[0117] 사용자는 하나 이상의 유선/무선 입력 디바이스, 예를 들어 키보드(838) 및 마우스(840)과 같은 포인팅 디바이스를 통해 컴퓨터(812)에 명령 및 정보를 입력할 수 있다. 다른 입력 디바이스에는 마이크, 적외선(IR) 리모컨, 무선 주파수(RF) 리모컨, 게임 패드, 스타일러스 펜, 카드 리더기, 동글, 지문 리더기, 장갑, 그래픽 태블릿, 조이스틱, 키보드, 레티나 리더기, 터치 스크린이 포함될 수 있다. 예를 들면 정전식, 저장식 등, 트랙볼, 트랙 패드, 센서, 스타일러스 등이다. 이러한 입력 디바이스와 기타 입력 디바이스는 종종 시스템 버스(806)에 결합된 입력 디바이스 인터페이스(842)를 통해 프로세서(802)에 연결되지만 병렬 포트, IEEE 1394 직렬 포트, 게임 포트, USB 포트, IR 인터페이스 등과 같은 다른 인터페이스로 연결될 수 있다.

[0118] 모니터(844) 또는 기타 유형의 디스플레이 디바이스도 비디오 어댑터(846)와 같은 인터페이스를 통해 시스템 버스(806)에 연결된다. 모니터(844)는 컴퓨터(812)의 내부 또는 외부에 있을 수 있다. 모니터(844) 외에도 컴퓨터는 일반적으로 스피커, 프린터 등과 같은 다른 주변 출력 디바이스를 포함한다.

[0119] 컴퓨터(812)는 유선 및/또는 무선 통신을 통한 논리적 연결을 사용하여 하나 이상의 원격 컴퓨터 예를 들면 원격 컴퓨터(848)에 네트워크 환경에서 작동할 수 있다. 원격 컴퓨터(848)은 워크스테이션, 서버 컴퓨터, 라우터, 개인용 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서 기반 엔터테인먼트 기기, 피어 디바이스 또는 기타 공통 네트워크 노드일 수 있으며, 일반적으로 컴퓨터(812)와 관련하여 설명된 많은 엘레먼트 또는 모든 엘레먼트를 포함하지만, 간결성을 위해 메모리 및/또는 저장 디바이스(850)만 설명되어 있다. 묘사된 논리적 연결에는 로컬 영역 네트워크(852) 및/또는 더 큰 네트워크 예를 들면 광역 네트워크(854)에 대한 유선/무선 연결이 포함된다. 이러한 LAN 및 WAN 네트워킹 환경은 사무실과 회사에서 흔히 볼 수 있으며, 인트라넷과 같은 기업 전체 컴퓨터 네트워크를 용이하게 하며, 이 모두는 글로벌 통신 네트워크 예를 들면 인터넷에 연결될 수 있다.

[0120] 로컬 영역 네트워크(852) 네트워킹 환경에서 사용될 때, 컴퓨터(812)는 유선 및/또는 무선 통신 네트워크 인터페이스 또는 네트워크 어댑터(856)을 통해 로컬 영역 네트워크(852)에 연결된다. 네트워크 어댑터(856)은 로컬 영역 네트워크(852)에 대한 유선 및/또는 무선 통신을 용이하게 할 수 있으며, 여기에는 네트워크 어댑터(856)의 무선 기능과 통신하기 위해 배치된 무선 액세스 포인트도 포함될 수 있다.

[0121] 광역 네트워크(854) 네트워킹 환경에서 사용될 때, 컴퓨터(812)는 모뎀(858)을 포함할 수 있거나, 광역 네트워크(854)의 통신 서버에 연결되거나, 인터넷을 통한 것과 같이 광역 네트워크(854)를 통해 통신을 설정하기 위한 다른 수단을 갖는다. 모뎀 858은 내부 또는 외부 및 유선 및/또는 무선 디바이스일 수 있으며, 입력 디바이스 인터페이스(842)를 통해 시스템 버스(806)에 연결된다. 네트워크 환경에서 컴퓨터(812)와 관련하여 묘사된 프로그램 모듈 또는 그 일부는 원격 메모리 및/또는 저장 디바이스(850)에 저장될 수 있다. 표시된 네트

워크 연결은 예시적이며 컴퓨터 간에 통신 링크를 설정하는 다른 수단을 사용할 수 있다.

- [0122] 컴퓨터 (812)는 IEEE 802 표준 계열을 사용하여 유선 및 무선 디바이스 또는 엔터티와 통신할 수 있다. 여기에는 무선 통신 예를 들면 IEEE 802.11 무선 변조 기술에 작동적으로 배치된 무선 디바이스와 같은 디바이스가 포함된다. 여기에는 최소한 Wi-Fi 또는 무선 Fidelity, WiMax 및 블루투스 무선 기술이 포함된다. 따라서 통신은 기존 네트워크와 마찬가지로 미리 정의된 구조이거나 최소한 두 디바이스 간의 임시 통신일 수 있다. Wi-Fi 네트워크는 IEEE 802.11(a, b, g, n, ac, ax 등)이라는 무선 기술을 사용하여 안전하고 안정적이며 빠른 무선 연결을 제공한다. Wi-Fi 네트워크는 컴퓨터를 서로 연결하고, 인터넷에 연결하고, 유선 네트워크 IEEE 802.3 관련 미디어 및 기능 사용에 연결하는 데 사용할 수 있다.
- [0123] 도 1A 내지 도12를 참조하여 이전에 설명된 바와 같이 디바이스의 다양한 엘리먼트는 다양한 하드웨어 엘리먼트, 소프트웨어 엘리먼트 또는 둘의 조합을 포함할 수 있다. 하드웨어 엘리먼트의 예로는 디바이스, 논리 디바이스, 컴포넌트, 프로세서, 마이크로프로세서, 회로, 프로세서, 회로 엘리먼트, 예를 들면 트랜지스터, 저항기, 커패시터, 인덕터 등, 집적 회로, 응용프로그램 특정 집적 회로(ASIC), 프로그래밍 가능 논리 디바이스(PLD), 디지털 신호 프로세서(DSP), 현장 프로그래밍 가능 게이트 어레이(FPGA), 메모리 디바이스, 논리 게이트, 레지스터, 반도체 디바이스, 칩, 마이크로칩, 칩셋 등이 있다.
- [0124] 소프트웨어 엘리먼트의 예로는 소프트웨어 컴포넌트, 프로그램, 응용프로그램, 컴퓨터 프로그램, 응용프로그램 프로그램, 시스템 프로그램, 소프트웨어 개발 프로그램, 머신 프로그램, 운영 체제 소프트웨어, 미들웨어, 펌웨어, 소프트웨어 모듈, 루틴, 서브루틴, 함수, 방법, 프로시저, 소프트웨어 인터페이스, 응용프로그램 프로그램 인터페이스(API), 명령어 세트, 컴퓨터 코드, 컴퓨터 코드, 코드 세그먼트, 컴퓨터 코드 세그먼트, 단어, 값, 기호 또는 이들의 조합이 포함될 수 있다.
- [0125] 그러나 구현이 하드웨어 및/또는 소프트웨어 엘리먼트를 사용하여 구현되는지 여부를 결정하는 것은 원하는 계산 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 제약 조건과 같은 여러 요인에 따라 달라질 수 있으며, 이는 주어진 구현에 대해 원하는 대로이다.
- [0126] 적어도 하나의 실시예의 하나 이상의 측면은 프로세서 내의 다양한 논리를 나타내는 기계 판독 가능 매체에 저장된 대표적 명령어에 의해 구현될 수 있으며, 기계가 이를 읽으면 기계가 여기에 설명된 기술을 수행하는 논리를 제작하게 된다. IP 코어"로 알려진 이러한 표현은 유형의 기계 판독 가능 매체에 저장되어 다양한 고객 또는 제조 시설에 공급되어 논리 또는 프로세서를 만드는 제조 기계에 로드 될 수 있다. 일부 실시예는 예를 들어 기계가 실행하는 경우 기계가 실시예에 따라 방법 및/또는 작업을 수행하게 할 수 있는 명령어 또는 명령어 세트를 저장할 수 있는 기계 판독 가능 매체 또는 제품을 사용하여 구현될 수 있다. 이러한 기계는 예를 들어 모든 적합한 처리 플랫폼, 컴퓨터 플랫폼, 컴퓨터 디바이스, 처리 디바이스, 컴퓨터 시스템, 처리 시스템, 컴퓨터, 프로세서 또는 이와 유사한 것을 포함할 수 있으며, 하드웨어 및/또는 소프트웨어의 모든 적합한 조합을 사용하여 구현될 수 있다.
- [0127] 기계 판독 매체 또는 물품에는 예를 들어, 메모리, 이동식 또는 이동식 불가 매체, 지울 수 있는 또는 지울 수 없는 매체, 쓰기 가능 또는 다시 쓰기 가능한 매체, 디지털 또는 아날로그 매체, 하드 디스크, 플로피 디스크, 콤팩트 디스크 리드 온리 메모리(CD-ROM), 콤팩트 디스크 레코더블 (CD-R), 콤팩트 디스크 리라이트어블(CD-RW), 광 디스크, 자기 매체, 자기 광 매체, 이동식 메모리 카드 또는 디스크, 다양한 유형의 디지털 별세타일 디스크(DVD), 테이프, 카세트 또는 이와 유사한 것과 같은 모든 적합한 유형의 메모리 유닛, 메모리 디바이스, 메모리 물품, 메모리 매체, 저장 디바이스, 저장 물품, 저장 매체 및/또는 저장 유닛이 포함될 수 있다.
- [0128] 지침에는 소스 코드, 컴파일 된 코드, 해석된 코드, 실행 가능한 코드, 정적 코드, 동적 코드, 암호화된 코드 등과 같은 모든 적합한 유형의 코드가 포함될 수 있으며, 모든 적합한 고급, 저수준, 객체 지향, 시각적, 컴파일 된 및/또는 해석된 프로그래밍 언어를 사용하여 구현된다.
- [0129] 상기 설명된 디바이스의 컴포넌트 및 특징은 이산 회로, 응용프로그램 특정 집적 회로(ASIC), 논리 게이트 및/또는 단일 칩 아키텍처의 임의의 조합을 사용하여 구현될 수 있다. 또한 디바이스의 특징은 마이크로컨트롤러, 프로그래밍 가능 논리 어레이 및/또는 마이크로프로세서 또는 상기의 임의의 조합을 사용하여 구현될 수 있다 (적절한 경우). 하드웨어, 펌웨어 및/또는 소프트웨어 엘리먼트는 본 명세서내에서 "논리" 또는 "회로"로 집합적으로 또는 개별적으로 지칭될 수 있음에 유의한다.
- [0130] 상기 설명된 블록 다이어그램에 표시된 예시적인 디바이스는 많은 잠재적 구현의 하나의 기능적으로 설명적인

예를 나타낼 수 있음을 알 수 있을 것이다. 따라서 첨부 도면에 묘사된 블록 기능의 분할, 생략 또는 포함은 이러한 기능을 구현하기 위한 하드웨어 컴포넌트, 회로, 소프트웨어 및/또는 요소가 반드시 실시예에서 분할, 생략 또는 포함될 것이라는 것을 의미하지 않는다. 적어도 하나의 컴퓨터 판독 가능 저장 매체에는 실행 시 시스템이 여기에 설명된 컴퓨터 구현 방법을 수행하도록 하는 명령어가 포함될 수 있다.

[0131] 일부 실시예는 "한 실시예" 또는 "구체예" 라는 표현과 그 파생어를 사용하여 설명될 수 있다. 이러한 용어는 실시예와 관련하여 설명된 특정 기능, 구조 또는 특성이 적어도 하나의 실시예에 포함된다는 것을 의미한다. 명세서의 다양한 곳에 "한 실시예에서"라는 문구가 나타나는 것은 반드시 모두 동일한 실시예를 언급하는 것은 아니다. 게다가, 달리 언급되지 않는 한, 위에 설명된 기능은 어떤 조합이던 함께 사용할 수 있는 것으로 인식된다. 따라서 별도로 논의된 기능은 기능이 서로 호환되지 않는다는 점에 유의하지 않는 한 서로 조합하여 사용될 수 있다.

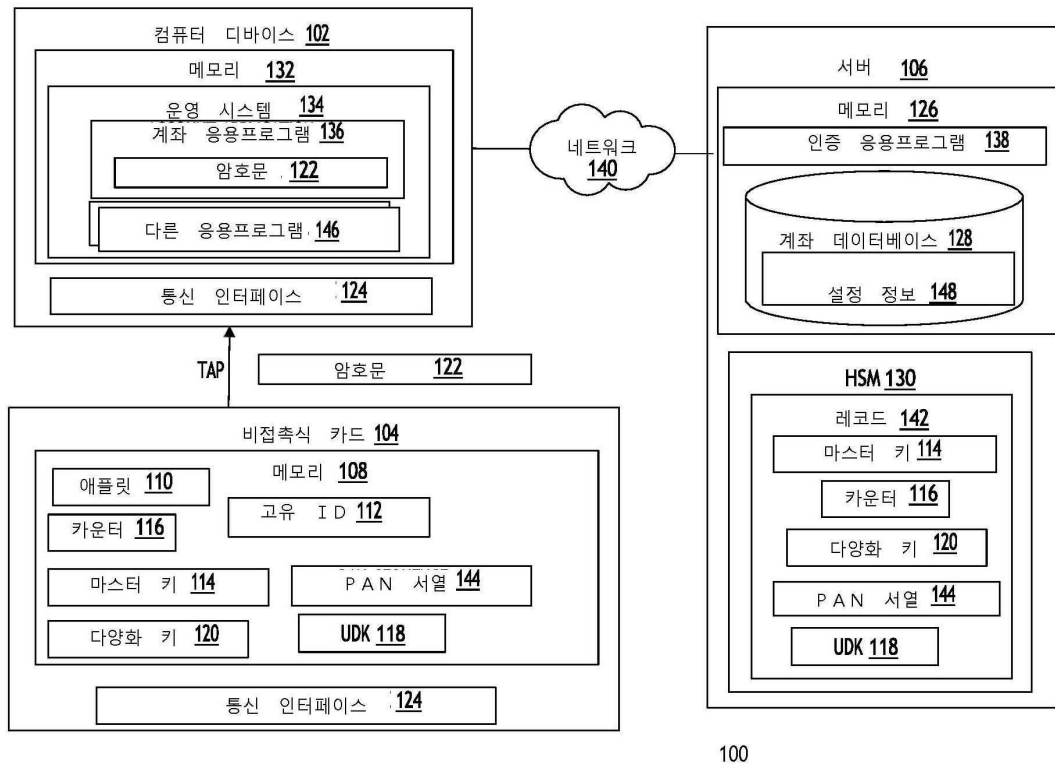
[0132] 발명의 초록은 독자가 기술 공개의 본질을 빠르게 파악할 수 있도록 제공되었음을 강조한다. 이는 청구항의 범위 또는 의미를 해석하거나 제한하는 데 사용되지 않을 것이라는 이해를 바탕으로 제출된다. 또한, 앞서 언급한 상세한 설명에서 다양한 특징이 공개를 간소화하기 위해 단일 구체예에 함께 그룹화되어 있음을 알 수 있다. 이 공개 방법은 청구된 구체예가 각 청구항에 명시적으로 언급된 것보다 더 많은 특징을 필요로 한다는 의도를 반영하는 것으로 해석되어서는 안 된다. 오히려 다음 청구항에서 반영하듯이 창의적인 주제는 단일 공개된 구체예의 모든 특징보다 적다. 따라서 다음 청구항은 상세한 설명에 통합되며 각 청구항은 별도의 구체예로서 독립적으로 존재한다. 첨부된 청구항에서 용어 "포함하는" 및 "본 명세서내에서"는 각각 용어 "포함하는" 및 "여기서"의 일반 영어 동등어로 사용된다. 또한, "제1", "제2", "세 번째" 등의 용어는 단순히 레이블로 사용되며, 해당 객체에 수치적 요구 사항을 부과하려는 것이 아니다.

[0133] 위에서 설명한 것은 공개된 아키텍처의 예를 포함한다. 물론, 모든 상상할 수 있는 컴포넌트 및/또는 방법론의 조합을 설명하는 것은 불가능하지만, 해당 분야의 통상의 기술자는 많은 추가 조합 및 순열이 가능하다는 것을 인식할 수 있다. 따라서, 새로운 아키텍처는 첨부된 청구항의 정신 및 범위 내에 있는 모든 이러한 변경, 수정 및 변형을 포괄하도록 의도된다.

[0134] 예시적 실시예에 대한 상기 설명은 예시 및 설명의 목적으로 제시되었습니다. 이는 포괄적이거나 본 공개를 공개된 정확한 형태로 제한하려는 것이 아닙니다. 이 공개에 비추어 많은 수정 및 변형이 가능하다. 본 공개의 범위는 이 자세한 설명이 아니라 여기에 첨부된 청구항에 의해 제한되도록 의도된다. 이 출원에 우선권을 주장하는 후속 출원은 다른 방식으로 공개된 주제를 장할 수 있으며, 일반적으로 여기에 다양하게 공개되거나 다른 방식으로 입증된 하나 이상의 제한 사항을 포함할 수 있다.

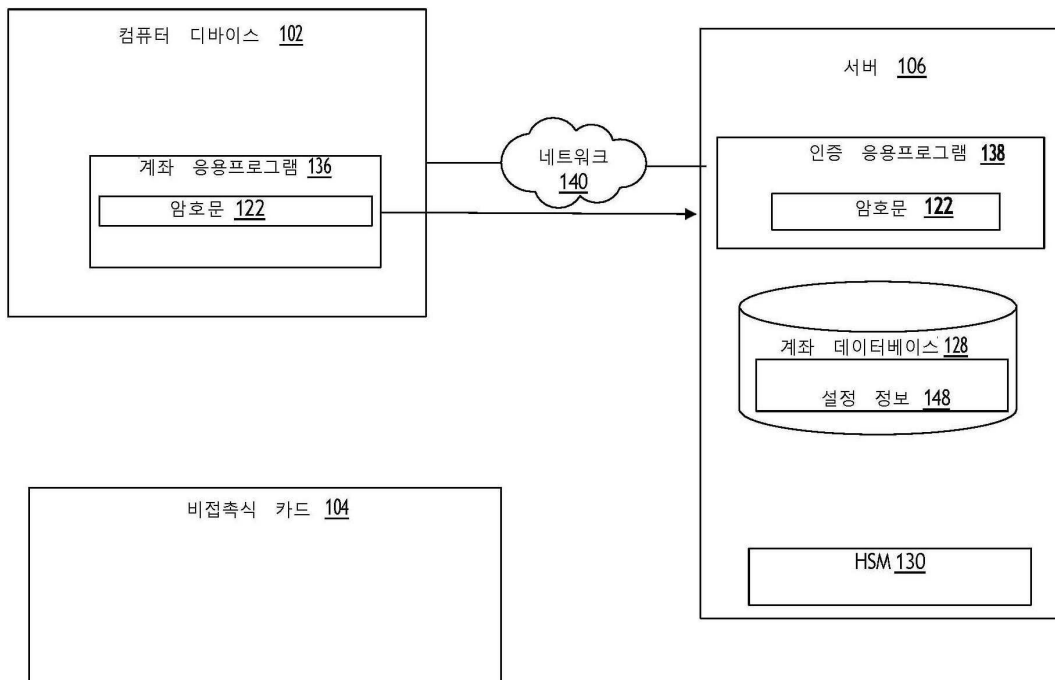
도면

도면1a

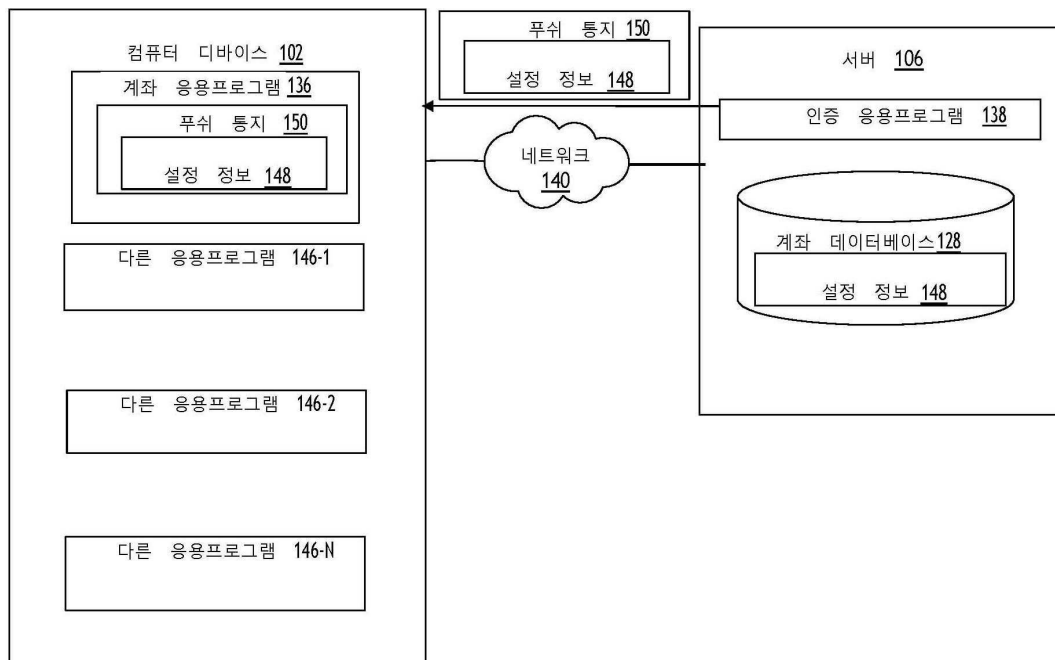


100

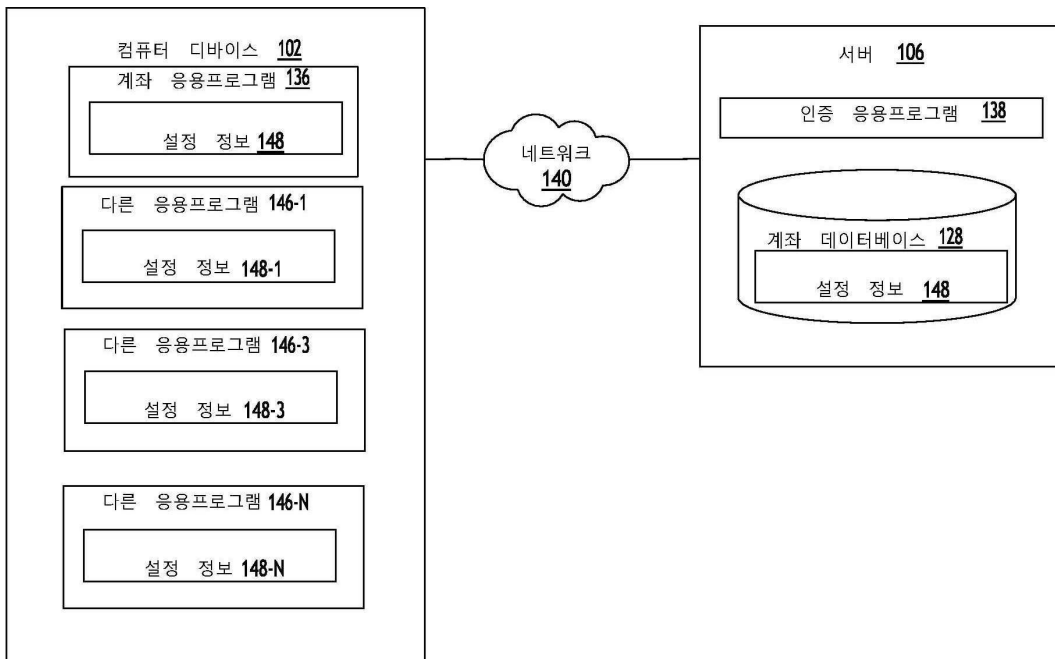
도면1b



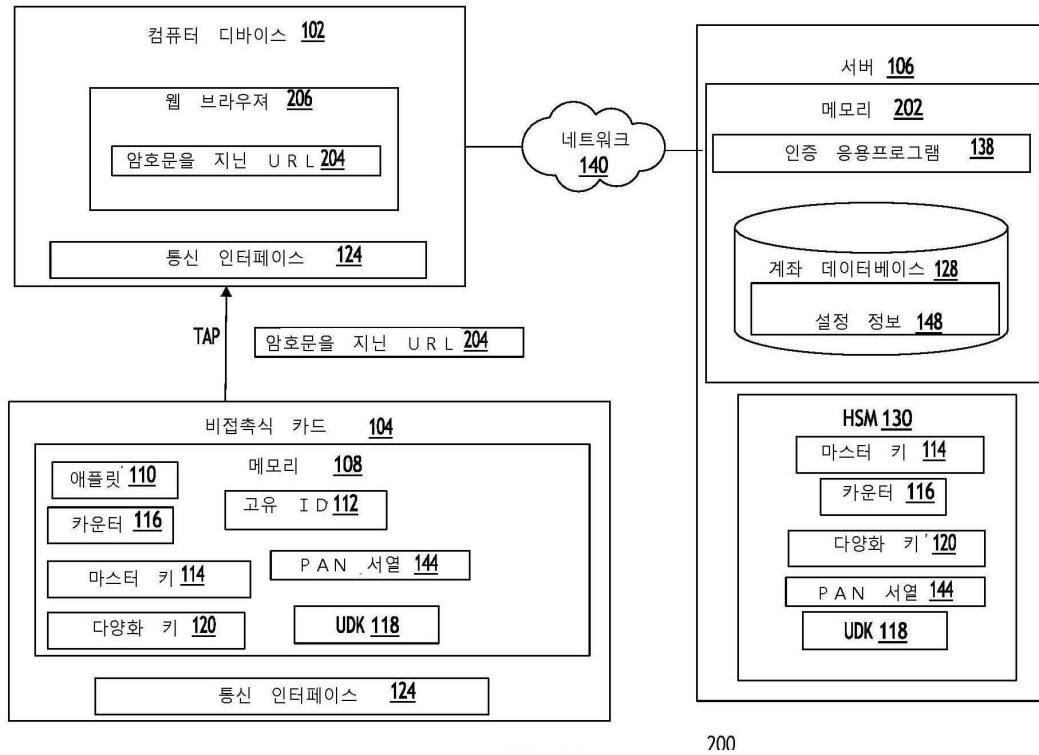
도면1c



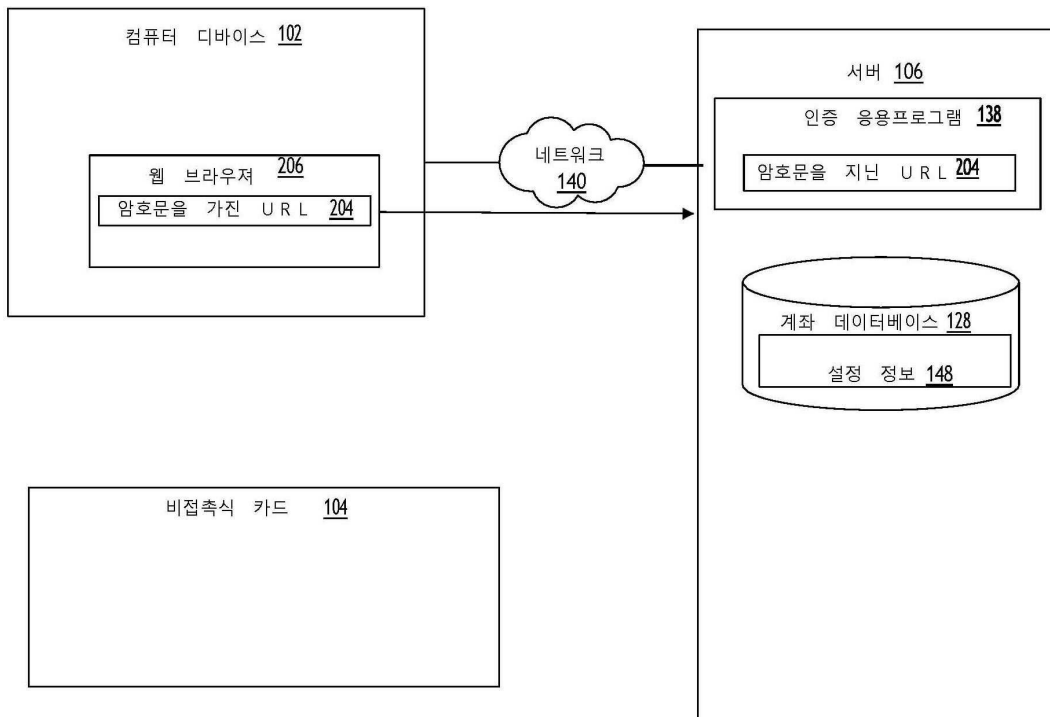
도면1d



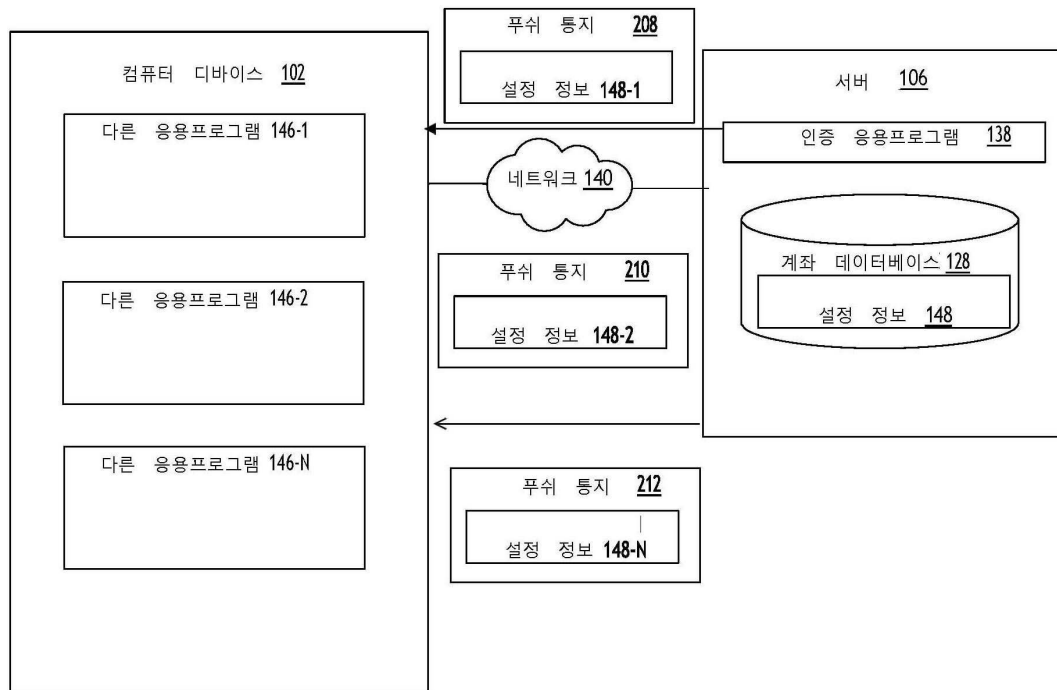
도면2a



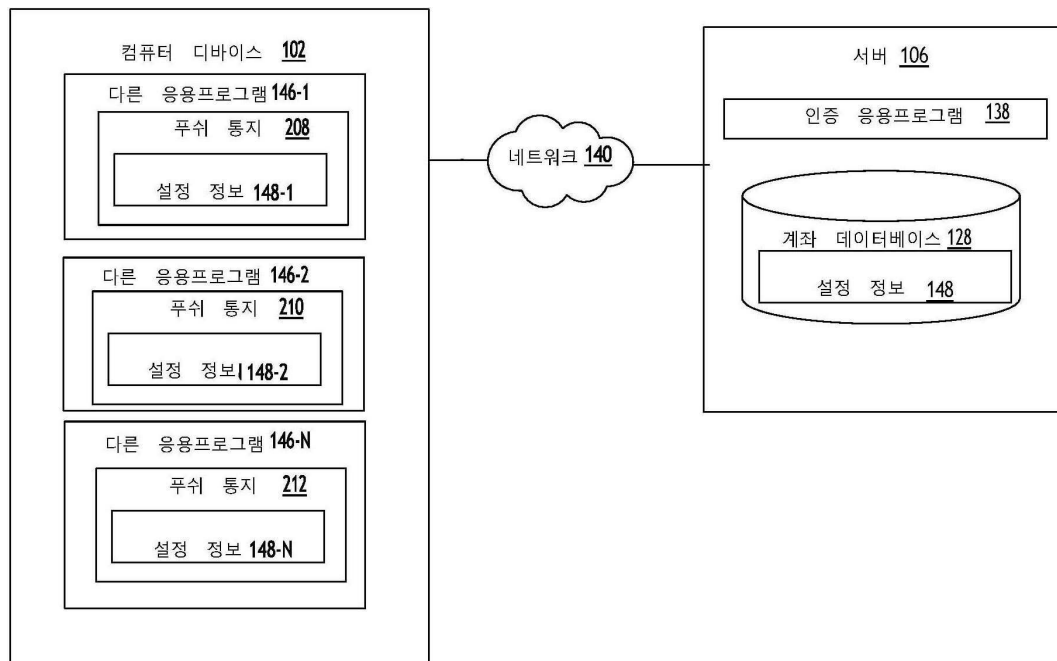
도면2b



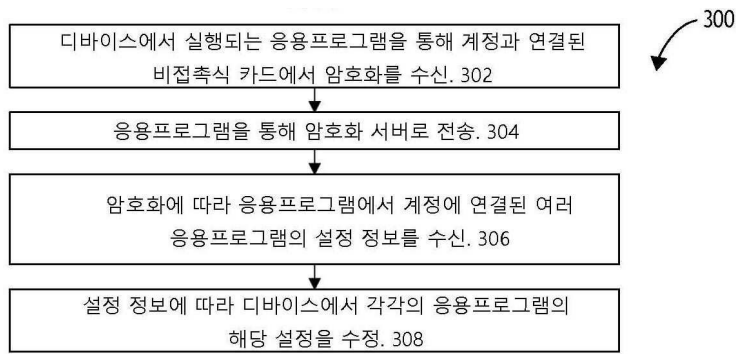
도면2c



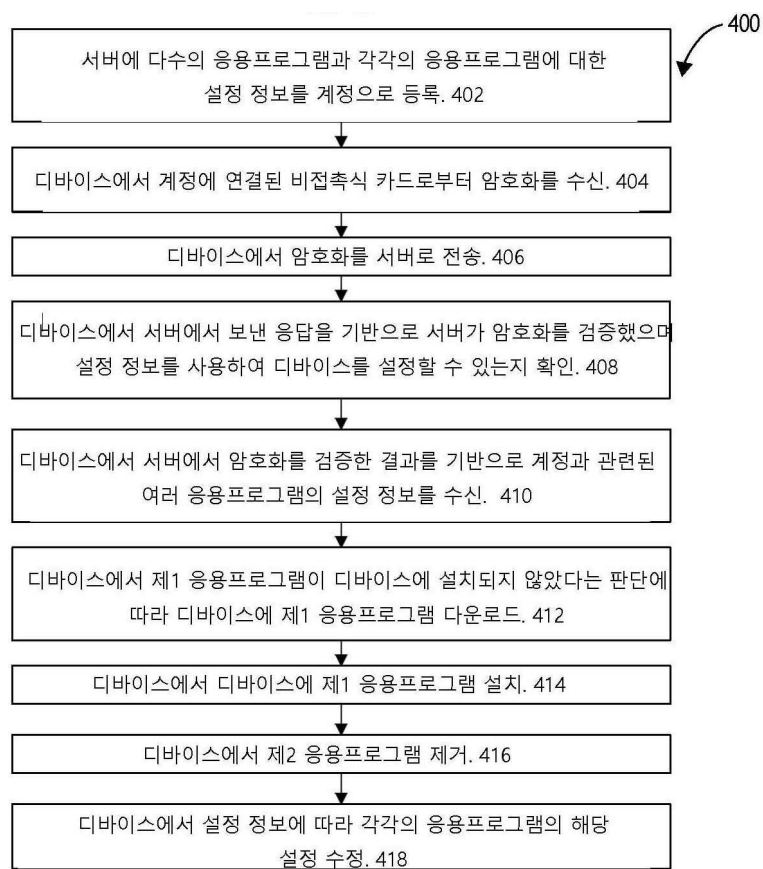
도면2d



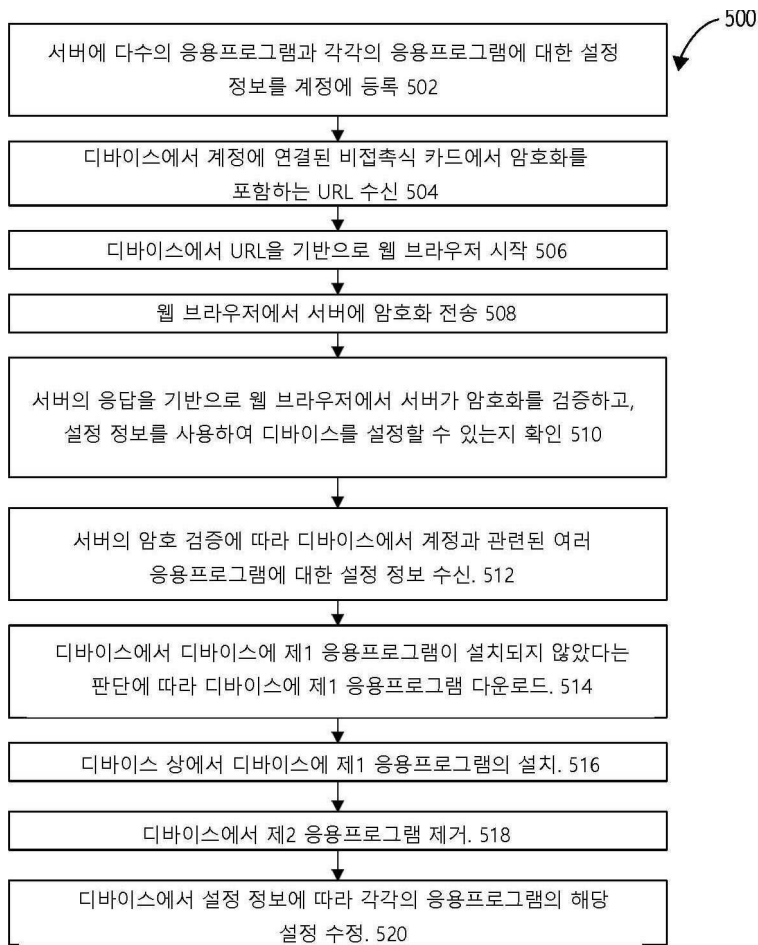
도면3



도면4



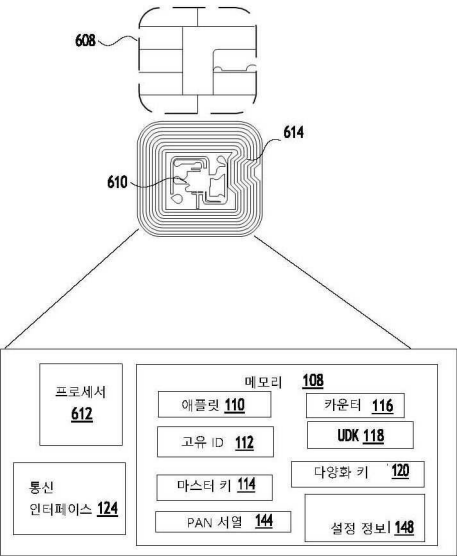
도면5



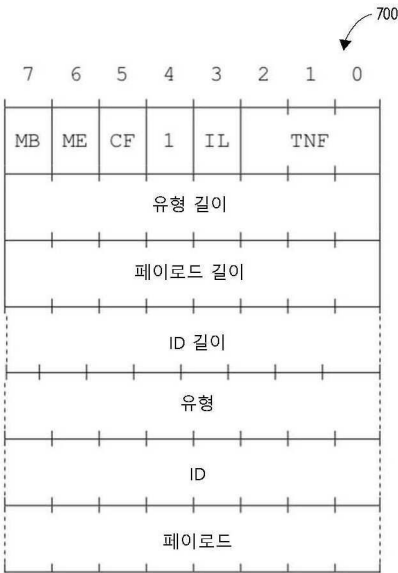
도면6a



도면6b



도면7



도면8

