(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0052549
(43) 공개일자 2017년05월12일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 12/02* (2006.01)
G06K 19/077 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3278 (2013.01)
G06F 12/0246 (2013.01)
(21) 출원번호 10-2017-0055428(분할)
(22) 출원일자 2017년04월28일
심사청구일자 없음
(62) 원출원 특허 10-2015-0050163
원출원일자 2015년04월09일
심사청구일자 2015년04월09일
(30) 우선권주장
1020140042362 2014년04월09일 대한민국(KR)

(71) 출원인
(주) 아이씨티케이
경기도 성남시 분당구 판교로 323 , 3층, 5층(삼평동, 투썬벤처포럼빌딩)
한양대학교 산학협력단
서울특별시 성동구 왕십리로 222(행당동, 한양대학교내)
(72) 발명자
김동규
서울특별시 동대문구 장한로14길 81, 105동 2103호 (장안동, 삼성래미안1차아파트)
최병덕
서울특별시 강동구 올림픽로62길 9-24
지광현
경기도 구리시 체육관로 69 205동 1603호 (교문동, 하나아파트)
(74) 대리인
특허법인 무한

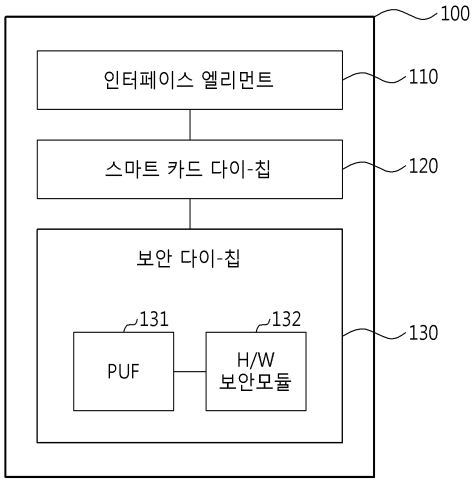
전체 청구항 수 : 총 18 항

(54) 발명의 명칭 **인증 장치 및 방법**

(57) 요 약

기기와 연결되는 인터페이스 엘리먼트와 보안 다이-칩이 하나의 패키지 내에 구현된다. 상기 보안 다이-칩은 보안 인증 기능을 구비하지 못하는 상기 인터페이스 엘리먼트에 보안 인증 기능을 제공할 수 있다. 예시적으로, 상기 보안 다이-칩은 개인 키를 제공하는 PUF 및 상기 개인 키를 이용하여 암호화 및 복호화를 수행하는 하드웨어 와이어된 보안 모듈을 포함할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
G06K 19/077 (2013.01)
H04L 9/0866 (2013.01)

명 세 서

청구범위

청구항 1

기기와 인터페이스 하는 인터페이스 엘리먼트; 및

상기 인터페이스 엘리먼트와 함께 패키지 되며, 상기 패키지 내에서 상기 인터페이스 엘리먼트에 하드웨어-기반 인증을 제공하는 보안 다이-칩

을 포함하는 인증 장치.

청구항 2

제1항에 있어서,

상기 보안 다이-칩은,

개인 키를 제공하는 PUF (Physically Unclonable Function); 및

상기 개인 키를 이용하여 암호화 및 복호화를 수행하는 하드웨어 와이어된 보안 모듈

을 포함하는 인증 장치.

청구항 3

제1항에 있어서,

상기 보안 다이-칩이 상기 기기와 인터페이스 하도록 컨트롤 하는 컨트롤 칩

을 더 포함하는 인증 장치.

청구항 4

제3항에 있어서,

상기 컨트롤 칩은 스마트카드 다이-칩을 포함하는 인증 장치.

청구항 5

제1항에 있어서,

상기 인터페이스 엘리먼트는 SD (Secure Digital)인 인증 장치.

청구항 6

제5항에 있어서,

상기 보안 다이-칩은 상기 SD에 저장되는 데이터를 암호화 하는 인증 장치.

청구항 7

제1항에 있어서,

상기 인터페이스 엘리먼트는 SIM (Subscriber Identity Module)인 인증 장치.

청구항 8

제7항에 있어서,

상기 보안 다이-칩은 상기 기기와 네트워크 연결되는 서버에 대해 상기 기기에 대한 인증을 수행하는 인증 장치.

청구항 9

저장 장치에 있어서,

플래시 메모리;

상기 플래시 메모리로부터의 데이터 독출 및 상기 플래시 메모리에 대한 데이터 프로그램을 컨트롤하는 컨트롤러; 및

상기 컨트롤러가 상기 플래시 메모리에 기록하는 제1 데이터를 암호화 하여 암호화된 제2 데이터를 생성하는 하드웨어-기반 보안 다이-칩

을 포함하고,

상기 컨트롤러는 상기 제2 데이터를 상기 플래시 메모리에 저장하는 저장 장치.

청구항 10

제9항에 있어서,

상기 보안 다이-칩은,

인증 키를 제공하는 PUF (Physically Unclonable Function); 및

상기 인증 키를 이용하여 상기 제1 데이터를 암호화하는 하드웨어 와이어된 보안 모듈

을 포함하는 저장 장치.

청구항 11

제10항에 있어서,

상기 보안 다이-칩이 상기 컨트롤러 및 상기 저장 장치 외부의 기기 중 적어도 하나와 인터페이스하도록 컨트롤하는 스마트카드 다이-칩

을 더 포함하는 저장 장치.

청구항 12

제10항에 있어서,

상기 제1 데이터에 대한 인증된 액세스 요청이 수신되는 경우, 상기 보안 다이-칩은 상기 인증 키를 이용하여 상기 제2 데이터를 상기 제1 데이터로 복호화 하는 저장 장치.

청구항 13

제9항에 있어서,

상기 저장 장치는 SD 카드 및 마이크로 SD 카드 중 어느 하나이고,

상기 저장 장치는 상기 SD 카드 또는 상기 마이크로 SD 카드 규격에 따른 패키지 내에 상기 하드웨어-기반 보안 다이-칩을 포함하는 저장 장치.

청구항 14

저장 장치의 동작 방법에 있어서,

상기 저장 장치에 저장될 제1 데이터가 수신되는 경우, 상기 저장 장치 내에 패키징된 보안 다이-칩의 하드웨어 와이어된 보안 모듈이, 상기 보안 다이-칩 내의 PUF (Physically Unclonable Function)가 제공하는 개인 키를 이용하여 상기 제1 데이터를 암호화하여 제2 데이터를 생성하는 단계; 및

상기 저장 장치의 컨트롤러가 상기 저장 장치의 플래시 메모리에 상기 제2 데이터를 프로그램하는 단계

를 포함하는 저장 장치의 동작 방법.

청구항 15

기기에 연결되는 인터페이스 엘리먼트를 이용한 기기 인증 방법에 있어서,

상기 인터페이스 엘리먼트와 함께 패키징 되는 보안 다이-칩에 포함되는 하드웨어 와이어된 보안 모듈이 상기 보안 다이-칩 내의 PUF (Physically Unclonable Function)가 제공하는 개인 키를 이용하여 전자 서명을 생성하는 단계; 및

상기 기기와 연결 되는 외부 디바이스에 의해 상기 전자 서명이 검증되도록, 상기 인터페이스 엘리먼트 및 상기 기기를 통해 상기 외부 디바이스에 상기 전자 서명을 전송하는 단계

를 포함하는 기기 인증 방법.

청구항 16

제15항에 있어서,

상기 인터페이스 엘리먼트는 SD (Secure Digital) 및 SIM (Subscriber Identity Module) 중 적어도 하나를 포함하는 기기 인증 방법.

청구항 17

기기에 연결되는 인터페이스 엘리먼트를 이용한 보안 통신 방법에 있어서,

외부 기기로부터 공개 키로 암호화되어 상기 인터페이스 엘리먼트를 통해 수신되는 암호화된 세션 키를 수신하는 단계;

상기 인터페이스 엘리먼트와 함께 패키징 되는 보안 다이-칩에 포함되는 하드웨어 와이어된 보안 모듈이 상기 보안 다이-칩 내의 PUF (Physically Unclonable Function)가 제공하는 개인 키를 이용하여 상기 암호화된 세션 키를 복호화 하여 상기 세션 키를 획득하는 단계; 및

상기 하드웨어 와이어된 상기 보안 모듈이 메시지를 상기 세션 키로 암호화 하여 암호화된 메시지를 생성하는 단계; 및

상기 인터페이스 엘리먼트를 통해 상기 암호화된 메시지를 전송하는 단계

를 포함하는 보안 통신 방법.

청구항 18

제17항에 있어서,

상기 인터페이스 엘리먼트는 SD (Secure Digital), SIM (Subscriber Identity Module), 블루투스, USB (Universal Serial Bus), NFC (Near Field Communication) 중 적어도 하나를 포함하는 보안 통신 방법.

발명의 설명

기 술 분 야

[0001] 인증 장치 및 방법에 연관되며, 보다 특정하게는 기기(device), 기기에 저장된 데이터, 및/또는 기기가 송수신하는 데이터를 인증하는 장치 및 방법에 연관된다.

배 경 기 술

[0003] 스마트폰이나 태블릿과 같은 종래의 통신 기기뿐만 아니라 각종 센서, 가전제품, 자동차 등 다양한 사물이 네트워크에 연결되는 IoT (Internet of Things) 환경이 확산될 것으로 예상된다. 이러한 IoT 환경에서 보안 및 인증은 가장 중요한 기술로 인식되고 있다.

[0004] 이러한 보안 및 인증은 기기(things or devices)의 인증, 기기에 저장된 데이터 보안, 및/또는 기기가 송수신하는 정보의 보호를 포함하는 것으로 이해된다. 그런데, 보안은 성능과 편의성을 저해하는 요소이기도 하므로,

이미 보급된 많은 기기들에는 보안 기능이 부재하거나, 약한(vulnerable) 경우가 많다.

[0005] 한편, PUF (Physically Unclonable Function)는 예측 불가능한 (unpredictable) 디지털 값을 제공할 수 있다. 개개의 PUF들은 정확한 제조 공정이 주어지고, 동일한 공정에서 제조되더라도, 상기 개개의 PUF들이 제공하는 디지털 값은 다르다. PUF는 복제가 불가능한 POWF (Physical One-Way Function practically impossible to be duplicated)로 지칭될 수도 있다.

[0006] 이러한 PUF의 복제 불가능한 특성은 보안 및/또는 인증을 위한 기기의 식별자(identifier)를 생성하는 데에 이용될 수 있다. 이를테면, 디바이스를 다른 디바이스와 구별하기 위한 유니크 키(unique key to distinguish devices from one another)를 제공하기 위해 PUF가 이용될 수 있다.

[0007] 한국 등록특허 10-1139630호(이하 '630 특허)에서 PUF를 구현하는 방법이 제시된 바 있다. '630 특허에서는 반도체의 공정 편차(process variation)를 이용하여 반도체의 전도성 레이어들 사이의 인터-레이어 콘택(inter-layer contact) 또는 비아(via)의 생성 여부가 확률적으로 결정되도록 한 방법이 제시되었다.

발명의 내용

과제의 해결 수단

[0009] 실시예들에 따르면, 인증 기능을 갖추지 않은 기기(device)에서 하드웨어-기반(hardware-based) 인증이 가능하도록 구현한 장치 및 방법이 제공된다. 이러한 장치 및 방법에 의해 기기의 인증, 기기에 저장된 데이터의 보호, 및/또는 기기가 송수신하는 데이터 통신의 보안이 높은 수준으로 구현된다.

[0010] 일측에 따르면, 기기와 인터페이스 하는 인터페이스 엘리먼트; 및 상기 인터페이스 엘리먼트와 함께 패키지 되며, 상기 패키지 내에서 상기 인터페이스 엘리먼트에 하드웨어-기반 인증을 제공하는 보안 다이-칩을 포함하는 인증 장치가 제공된다. 일실시예에 따르면 상기 보안 다이-칩은, 개인 키를 제공하는 PUF (Physically Unclonable Function); 및 상기 개인 키를 이용하여 암호화 및 복호화를 수행하는 하드웨어 와이어된 보안 모듈을 포함한다.

[0011] 일실시예에 따르면 상기 인증 장치는 상기 보안 다이-칩이 상기 기기와 인터페이스 하도록 컨트롤 하는 컨트롤 칩을 더 포함한다. 예시적으로, 그러나 한정되지 않게, 상기 컨트롤 칩은 스마트카드 다이-칩을 포함한다.

[0012] 한편, 상기 인터페이스 엘리먼트는 SD (Secure Digital)일 수 있다. 이 경우, 상기 보안 다이-칩은 상기 SD에 저장되는 데이터를 암호화할 수 있다. 다른 예에서, 상기 인터페이스 엘리먼트는 SIM (Subscriber Identity Module)일 수 있다. 이 경우, 상기 보안 다이-칩은 상기 기기와 네트워크 연결되는 서버에 대해 상기 기기에 대한 인증을 수행할 수 있다.

[0013] 다른 일측에 따르면, 저장 장치에 있어서, 플래시 메모리; 상기 플래시 메모리로부터의 데이터 독출 및 상기 플래시 메모리에 대한 데이터 프로그램을 컨트롤하는 컨트롤러; 및 상기 컨트롤러가 상기 플래시 메모리에 기록하는 제1 데이터를 암호화 하여 암호화된 제2 데이터를 생성하는 하드웨어-기반 보안 다이-칩을 포함하고, 상기 컨트롤러는 상기 제2 데이터를 상기 플래시 메모리에 저장하는 저장 장치가 제공된다. 일실시예에 따르면 상기 보안 다이-칩은, 인증 키를 제공하는 PUF (Physically Unclonable Function); 및 상기 인증 키를 이용하여 상기 제1 데이터를 암호화하는 하드웨어 와이어된 보안 모듈을 포함한다. 예시적으로, 그러나 한정되지 않게, 이 인증 키는 대칭 키 암호화 알고리즘에서 사용되는 키 값일 수 있다.

[0014] 일실시예에 따르면 상기 저장 장치는 상기 보안 다이-칩이 상기 컨트롤러 및 상기 저장장치 외부의 기기와 인터페이스하도록 컨트롤하는 스마트카드 다이-칩을 더 포함할 수 있다.

[0015] 한편, 상기 제1 데이터에 대한 인증된 액세스 요청이 수신되는 경우, 상기 보안 다이-칩은 상기 인증 키를 이용하여 상기 제2 데이터를 다시 상기 제1 데이터로 복호화 할 수 있다.

[0016] 일실시예에 따르면 상기 저장 장치는 SD 카드 및 마이크로 SD 카드 중 어느 하나일 수 있다. 이 경우, 상기 저장 장치는 상기 SD 카드 또는 상기 마이크로 SD 카드 규격에 따른 패키지 내에 상기 하드웨어-기반 보안 다이-칩을 포함할 수 있다.

[0017] 또 다른 일측에 따르면, 저장 장치의 동작 방법에 있어서, 상기 저장 장치에 저장될 제1 데이터가 수신되는 경우, 상기 저장 장치 내에 패키징된 보안 다이-칩의 하드웨어 와이어된 보안 모듈이, 상기 보안 다이-칩 내의

PUF (Physically Unclonable Function)가 제공하는 개인 키를 이용하여 상기 제1 데이터를 암호화하여 제2 데이터를 생성하는 단계; 및 상기 저장 장치의 컨트롤러가 상기 저장 장치의 플래시 메모리에 상기 제2 데이터를 프로그램하는 단계를 포함하는 저장 장치의 동작 방법이 제공된다.

[0018] 또 다른 일측에 따르면, 기기에 연결되는 인터페이스 엘리먼트를 이용한 기기 인증 방법에 있어서, 상기 인터페이스 엘리먼트와 함께 패키징 되는 보안 다이-칩에 포함되는 하드웨어 와이어된 보안 모듈이 상기 보안 다이-칩 내의 PUF (Physically Unclonable Function)가 제공하는 개인 키를 이용하여 전자 서명을 생성하는 단계; 및 상기 기기와 연결 되는 외부 디바이스에 의해 상기 전자 서명이 검증되도록, 상기 인터페이스 엘리먼트 및 상기 기기를 통해 상기 외부 디바이스에 상기 전자 서명을 전송하는 단계를 포함하는 기기 인증 방법이 제공된다. 예시적으로, 그러나 한정되지 않게 상기 인터페이스 엘리먼트는 SD (Secure Digital), SIM (Subscriber Identity Module), RFID, BlueTooth, NFC, 및 USB 중 적어도 하나를 포함한다.

[0019] 또 다른 일측에 따르면, 기기에 연결되는 인터페이스 엘리먼트를 이용한 보안 통신 방법에 있어서, 외부 기기로부터 공개 키로 암호화되어 상기 인터페이스 엘리먼트를 통해 수신되는 암호화된 세션 키를 수신하는 단계; 상기 인터페이스 엘리먼트와 함께 패키징 되는 보안 다이-칩에 포함되는 하드웨어 와이어된 보안 모듈이 상기 보안 다이-칩 내의 PUF (Physically Unclonable Function)가 제공하는 개인 키를 이용하여 상기 암호화된 세션 키를 복호화 하여 상기 세션 키를 획득하는 단계; 상기 하드웨어 와이어된 상기 보안 모듈이 메시지를 상기 세션 키로 암호화 하여 암호화된 메시지를 생성하는 단계; 및 상기 인터페이스 엘리먼트를 통해 상기 암호화된 메시지를 전송하는 단계를 포함하는 보안 통신 방법이 제공된다. 일실시예에 따르면 상기 인터페이스 엘리먼트는 SD (Secure Digital), SIM (Subscriber Identity Module), 블루투스, USB (Universal Serial Bus), NFC (Near Field Communication) 중 적어도 하나를 포함한다.

도면의 간단한 설명

[0021] 도 1은 일실시예에 따른 인증 장치의 블록도를 도시한다.

도 2는 일실시예에 따른 SD 카드를 도시한다.

도 3은 실시예들에 따라 기기와 인터페이스 하는 인증 장치들을 도시한다.

도 4는 실시예들에 따른 인증 장치와 기기의 인터페이스를 설명하기 위한 개념도이다.

도 5는 일실시예에 따른 저장 장치 동작 방법을 도시하는 흐름도이다.

도 6은 일실시예에 따른 기기 인증 방법을 도시하는 흐름도이다.

도 7과 도 8은 일실시예에 따른 보안 통신 방법을 도시하는 흐름도이다.

도 9, 도 10 및 도 11은 실시예들에 따른 서비스들을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0022] 이하에서, 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다. 그러나, 권리범위는 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0023] 아래 설명에서 사용되는 용어는, 연관되는 기술 분야에서 일반적이고 보편적인 것으로 선택되었으나, 기술의 발달 및/또는 변화, 관례, 기술자의 선호 등에 따라 다른 용어가 있을 수 있다. 따라서, 아래 설명에서 사용되는 용어는 기술적 사상을 한정하는 것으로 이해되어서는 안 되며, 실시예들을 설명하기 위한 예시적 용어로 이해되어야 한다.

[0024] 또한 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 설명 부분에서 상세한 그 의미를 기재할 것이다. 따라서 아래 설명에서 사용되는 용어는 단순한 용어의 명칭이 아닌 그 용어가 가지는 의미와 명세서 전반에 걸친 내용을 토대로 이해되어야 한다.

[0026] 도 1은 일실시예에 따른 인증 장치의 블록도를 도시한다. 인증 장치(100)는 기기(device)와 인터페이스 하는 인터페이스 엘리먼트(110)을 포함한다. 상기 기기는 이를테면, 스마트폰, 태블릿, 통상적인 컴퓨팅 단말, 사물

인터넷(IoT) 단말, 이동수단(vehicle) 등 유선 및/또는 무선 네트워크를 통해 외부와 연결되는 임의의 장치일 수 있다.

[0027] 예시적으로, 그러나 한정되지 않게 상기 인터페이스 엘리먼트는, SD, micro-SD, SIM, USIM, nano-SIM, NFC, USB, Blurtooth™ 등 중 어느 하나에 대응할 수 있다. 이러한 예에 따른 인터페이스 엘리먼트(110)의 규격이 정해져 있을 수 있다. 이를테면, 외형적 크기(dimension), 단자들의 기능 등 다양한 규격이 표준 또는 산업 표준으로 정해져 있고, 외부와 통신하는 주파수 대역이나 프로토콜도 정해져 있을 수 있다. 인증 장치(100)는 이렇게 정해진 규격에 변경을 가하지 않는 범위에서, 따라서 인터페이스 엘리먼트(110)의 일반적인 동작을 모두 허용하는 범위에서, 인터페이스 엘리먼트(110) 외부 하우징 내에서 하나의 기판으로 함께 패키징 될 수 있다. 따라서, 인증 장치(100)는 외형상으로는 통상의 SD 카드, SIM 칩, NFC 모듈, USB 스틱 등으로 보일 수 있으며, 기능상으로도 일반적인 SD 카드, SIM 칩 등의 기능은 그대로 수행될 수 있다.

[0028] 앞서 설명한 바와 같이, 인터페이스 엘리먼트(110) 및/또는 상기 기기들은 보안/인증 기능을 구비하지 않았거나, 구비하였더라도 보안 공격에 취약한 경우가 많다. 실시예들에 따르면, 이렇게 신뢰할 수 있는 보안/인증 수단을 구비하지 않은 기기 및/또는 인터페이스 엘리먼트에 보안 다이-칩(130)이 하드웨어-기반 보안 인증을 제공한다. 보안/인증은 기기의 인증, 기기에 저장된 데이터의 보호, 및/또는 기기가 송수신하는 데이터 통신의 보안 등을 포함하는 것이다. 그리고 명세서 전반에서, "하드웨어-기반"이라는 용어는 보안 인증에 사용되는 키 값이 물리적인 PUF에 의해 홀드되고, 암호화/복호화 알고리즘의 수행이 소프트웨어 어플리케이션이 아니라 진성 하드웨어 로직(truly hardware logic)인 회로에 의해 수행되는 것으로 이해될 수 있다. 하드웨어 로직에 의해서만 물리적으로 암복호화 알고리즘이 동작하기 때문에, 전용 하드웨어(dedicated HW) 또는 하드웨어 와이어드(hardware-wired) 로직이라고도 할 수 있다.

[0029] 일실시예에 따르면 보안 다이-칩(130)은 인증 장치(110)에만 유니크한 개인 키(private key)를 제공하는 PUF(131)와 상기 개인 키를 이용하여 암호화 및 복호화를 수행하는 하드웨어 와이어된 (하드웨어-기반의) 보안 모듈(132)을 포함한다.

[0030] PUF(131)를 구현하는 실시예에는 여러 가지가 있다. 예시적으로 반도체 제조 공정의 공정 편차(process variation)를 이용하여 구현할 수 있다. 일실시예에 따르면, PUF(131)는 전도성 레이어들 사이에 배치되는 비아(via)들 또는 인터-레이어 컨택(inter-layer contact)들에 의해 구현될 수 있으며, '630 특허의 명세서를 통해 자세한 내용이 제시된 바 있으며, 참고로서 이 명세서에 인용된다.

[0031] 한편, 일실시예에 따르면, PUF(131)는 보안 다이-칩(130), 이를테면 하드웨어 보안 모듈(132)를 구현하기 위한 반도체 일부 내에서 구현될 수 있다. 따라서, 외부에서 관찰하는 경우에는 PUF(131)의 정확한 위치를 식별할 수 없도록 할 수 있다. 비아나 인터-레이어 컨택은 반도체 회로에 무수히 많기 때문에 어떤 부분이 PUF(131)로 이용되는 부분인지 파악하는 것은 어렵고, 이러한 점은 보안 측면에 유리하다.

[0032] 나아가, 일실시예에 따르면 개인 키를 제공하는 PUF(131)는 하나가 아니라 복수 개 구비될 수도 있다. 실제 사용되는 PUF는 이들 중 하나일 수 있으며, 보안 모듈(130)의 와이어링과 동작을 완전히 이해하더라도 어느 PUF가 제공하는 개인 키가 실제로 암호화 복호화에 이용되는 지까지 파악하는 것은 더욱 어렵다. 따라서 이 실시예에 따르면 더욱 높은 수준의 하드웨어-기반 보안이 구현될 수 있다.

[0033] 한편, 일실시예에 따르면 인증 장치(100)는 보안 다이-칩(130)이 외부 기기 및/또는 인터페이스 엘리먼트(110)과 인터페이스 하도록 컨트롤 하는 컨트롤 칩을 더 포함할 수 있다. 예시적으로, 그러나 한정되지 않게, 이러한 칩은 도 1에 도시되는 스마트 카드 다이-칩(120)일 수 있다. 스마트 카드 다이-칩(120)은 하드웨어 칩이기는 하지만, 스마트 카드 내에 저장될 수 있는 소프트웨어 자체가 유출되는 우려, 스마트 카드 펌웨어 업데이트 등의 과정에서 내부 프로그램이 악성 코드에 의해 오염될 수 있는 위험성, 버스 프로빙(bus probing) 등 물리적 공격에 대한 우려 때문에, 그 자체가 보안 인증을 수행하기에 취약점이 있다. 스마트 카드 내부에는 CPU, ROM, RAM 등의 IP (information provider)가 포함되어 있으며 이러한 IP들은 디패키징 후 역공학으로 레이아웃을 분석하는 물리적 공격, 버스 프로빙, 메모리 스캔 공격 등에 약하기 때문이다. 따라서, 상기 실시예에서 스마트 카드 다이-칩(120)은 보안 다이-칩(130)과 외부 기기, 또는 보안 다이-칩(130)과 인터페이스 엘리먼트(110) 사이의 인터페이스를 컨트롤 한다. 인증 장치(100)의 각 구성의 동작 및 다양한 보안 응용은 더 자세하게 후술한다.

[0035] 도 2는 일실시예에 따른 SD 카드를 도시한다. 저장 장치로 알려져 있는 SD 카드(200)는 SD 카드 컨트롤러(230)

및 플래시 메모리(240)을 포함할 수 있다. SD 카드(200)의 규격, 외형, 단자 기능, 컨트롤러(230)와 플래시 메모리(240)에 있어서는 통상의 SD 카드 표준에 의한 것과 동일할 수 있다. 이 실시예에 따르면, 보안 다이-칩(210) 및 스마트 카드 다이-칩(220)이 SD 카드(200) 내에 함께 패키징되어, 하드웨어-기반 보안 인증이 가능하다. 보안 다이-칩(210) 내에는 개인 키를 제공하는 PUF와 상기 개인 키를 이용하여 암호화 및 복호화를 수행하는 하드웨어 와이어된 (하드웨어-기반의) 보안 모듈이 포함될 수 있다.

[0036] 구체적으로 설명하면, 보안 다이-칩(210) 및 스마트 카드 다이-칩(220)이 SD 카드(200) 내에 함께 패키징 됨으로써, 플래시 메모리(240)에 저장되어야 하는 중요한 데이터를 암호화 하여 안전하게 저장할 수 있고(저장되는 데이터 보호), SD 카드(200)가 삽입되는 기기나 SD 카드(200) 자체를 식별/인증할 수 있으며(기기 인증), 및/또는 SD 카드(200)에 저장된 데이터나 SD 카드(200)가 삽입된 기기가 보유하고 있는 데이터를 안전하게 신뢰할 수 있는 기관으로 보내는 통신 보안을 할 수 있다(보안 통신). 저장되는 데이터 보호 과정은 도 5를 참조하여 상세히 설명하며, 기기 인증 과정은 도 6을 참고하여, 그리고 보안 통신 과정은 도 7과 도 8을 참조하여 상세히 설명할 것이다.

[0038] 도 3은 실시예들에 따라 기기와 인터페이스 하는 인증 장치들을 도시한다. 도 2를 참조하여 먼저 설명한 SD 카드(320)뿐만 아니라, 기기(300)에 삽입되는 USIM 카드(310) 형태로도 인증 장치가 구현될 수 있다. 이렇게 기기에 구비되는 인터페이스, 이를테면 카드 슬롯을 통해 기기에 착탈 가능한 인증 장치는, 이러한 하드웨어-기반 보안 인증 기능을 갖지 않고 제조된 기기에도 하드웨어-기반 보안 인증을 사후적으로 제공할 수 있는 점에서 상업적 가치가 크다. 종래에 이미 보급된 스마트폰이나 태블릿, 나아가 범용 컴퓨터, USB 단자가 있는 자동차 등에도 적용 가능성이 있기 때문이다.

[0039] 차후에 기기(300) 제조 시부터, 인증 장치를 임베드 시키고자 하는 시도가 있을 수도 있을 것이며, 이 경우 임베드되는 보안 엘리먼트(SE)(330)에 인증 장치가 구현될 수도 있다.

[0041] 도 4는 실시예들에 따른 인증 장치와 기기의 인터페이스를 설명하기 위한 개념도이다. 스마트 카드가 포함된 신용 카드(401), USB 스틱(402), SD 카드(403), SIM 칩(404) 등 다양한 형태 내에 하드웨어-기반 인증 장치가 구현되어 있다. 상술한 바와 같이 실시예들에 따른 보안 인증 구현이 통상적인 접촉식 또는 비접촉식 신용 카드, USB, SD 카드, SIM 칩의 기능을 배제시키거나 방해하지 않는다. 하나로 패키징 됨으로써, 이러한 신용카드, USB, SD 카드, SIM 칩에 하드웨어 보안 인증을 더 제공하는 것이며, 따라서 데이터 보호, 기기 인증, 보안 통신 등이 가능해 진다.

[0043] *스마트 카드 다이-칩(410)은 PUF 기반 보안 다이-칩(420)을 지원한다. 예를 들어, 칩 외부로의 인터페이스를 제공할 수 있다. 인터페이스에는 소형 칩에 탑재될 수 있는 USB, SDIO와 같은 접촉 인터페이스나, NFC와 같은 밀착형 통신 인터페이스, Bluetooth 같은 근거리 통신 인터페이스 등이 가능하다. 또한 스마트 카드 다이-칩(410)은 연결 프로그램이나 PUF 기반 보안 다이-칩(420)이 보안 기능을 제공할 수 있도록 하는 다양한 형태의 응용 프로그램을 지원할 수도 있다.

[0044] PUF 기반 보안 다이-칩(420)은 암호화, 복호화 등 인증 기능을 수행하며, 신뢰된 저장 공간 등에 대한 보안(데이터 보안) 기능, 기기 인증, 및 통신 보안 기능을 제공할 수 있다. 앞서 설명한 바와 같이, PUF 기반 보안 다이-칩(420)에는 개인 키를 제공하는 PUF 및 하드웨어 와이어된 보안 모듈이 하나의 칩으로 패키징 되어 있을 수 있다.

[0045] PUF는 복제 불가능한 하드웨어 핑거 프린트로도 이해될 수 있다. 물리적 공격에 의해 그 값을 알아내는 것이 거의 불가능하다. 또한, 상기한 바와 같이 보안 다이-칩 내에서 PUF가 아닌 다른 일반적인 셀과 섞여서 물리적으로 무작위하게 배치되기 때문에, PUF 셀들을 모두 찾아내는 것은 매우 어렵다. 또한, PUF 값은 동작 중에만 값이 판독되므로, 유효한 동작이 유지되도록 하면서도 디패키징 등 물리적 공격을 수행하는 것은 매우 어려운 일이다. 나아가, PUF가 제공하는 바이너리 값들을 읽어냈더라도, 이를 유효한 순서로 그 값을 배열하는 것 또한 조합의 수가 매우 많기 때문에 이를 유효하게 사용하는 것은 더더욱 어렵다.

[0046] 이렇게 PUF를 다른 값을 암호화하는데 사용되는 근원 키 (또는 시드 키)로 사용함으로써, 높은 수준의 보안 인증이 가능해지면서도, PUF 자체는 물리적 공격에도 안전하다(안전한 키 관리). 또한 기기인증에 사용되는 공개

키 쌍의 개인키를 PUF로 구현할 경우 이 값은 키 값이 기기 밖으로 노출되지 않으므로 보안 칩이 탑재되는 모바일 기기의 형태나 종류, 통신 방식과 상관없이 안전한 기기 인증 및 부인 방지를 보장한다(안전한 기기 인증).

[0047] 아울러 HW 기반 보안 모듈은 순수하게 HW로만 제작되며, 부채널 공격 대응 기법이 적용되어 설계 및 제작된다. 하드웨어로 구현되어 있기 때문에 소프트웨어적인 공격, 이를테면 악성 코드에 의한 공격이 유효하지 않으며, FIB(Focused Ion Beam)등의 장비로 하드웨어 회로 자체를 수정하는 것이 가능하더라도, 원래의 동작을 보장하면서 유효한 공격 결과가 나오기는 어렵다. 따라서 보안 칩의 무결성이 보장된다.

[0049] 도 5는 일실시예에 따른 저장 장치 동작 방법을 도시하는 흐름도이다. 도시된 실시예는 데이터 보안에 연관된다. 기기로부터 (또는 외부로부터) 데이터(501)가 스마트 카드 다이-칩으로 수신되면, 이것이 보안 다이-칩으로 전달된다(502). 그러면, 단계(510)에서 보안 다이-칩은 이 데이터를 PUF 값을 이용하여 암호화고, 단계(520)에서 플래시 메모리 등 매체에 이 암호화된 데이터를 저장한다(단계 520). 이 단계에서 저장되는 데이터는 이미 암호화 되어 있는 것이기 때문에, 반드시 PUF 기반 칩의 비휘발성 메모리와 같은 격리된 공간에 저장되지 않고, 액세스가 자유로운 플래시 메모리에 저장되어도 되고, 또한 기기 외부에 보관되어도 된다. 이 경우, 이러한 저장 장치는 데이터를 암호화 시켜서 전달하는 수단이 될 수도 있다.

[0050] 인증된 외부 서버나 장치로부터 암호화된 데이터(503)의 액세스 요청이 수신되는 경우, 이는 암호화된 상태로 전달(504)될 수 있다. 상기 외부 서버나 장치가 단계(510)의 암호화 과정에 이용된 PUF 기반 개인 키에 대응하는 공개 키를 가지고 있다면 이 암호화된 데이터는 복호화 될 수 있을 것이다.

[0052] 도 6은 일실시예에 따른 기기 인증 방법을 도시하는 흐름도이다. 인증 장치(600)에 포함되는 보안 다이-칩이 스마트 카드 다이-칩의 지원으로 기기 인증을 수행하고 있다. 단계(610)에서 보안 다이-칩에 포함되는 하드웨어 와이어된 보안 모듈이 상기 보안 다이-칩 내의 PUF가 제공하는 개인 키를 이용하여 전자 서명을 생성한다.

[0053] 그러면 이 전자 서명(601)이 스마트 카드 다이-칩을 거쳐 외부 인터페이스, 이를테면 블루투스, USB, NFC, SD 카드 인터페이스 등 다양한 방법에 의해 기기로 전송된다. 위 인터페이스들은 비교적 근거리 통신이나 접촉식 통신에 대응하므로, 서비스 제공을 위해 네트워크 또는 인터넷에 연결되기 위해 기기, 이를테면 스마트폰의 통신 기능을 이용하는 것이다. 기기는 제공 받은 전자 서명(602)를, 와이파이나 4G 같은 브로드 밴드 네트워크를 이용하여 서버나 다른 기기로 전송한다(603). 이러한 전자 서명은 단계(620)에서 상기 개인 키에 대응하는 공개 키로 검증될 수 있으며, 이러한 과정을 통해 기기 인증이 가능하다.

[0054] 기기 인증을 이용한 응용 서비스는 굉장히 다양하다. 예를 들어, 전자 결제에서 미리 등록된 사용자의 단말기를 확인하는 데에 활용될 수 있다. 기본적인 단말기 인증뿐만 아니라, 전자 상거래의 활성화를 위한 간편 결제, 자동 결제 등에도 활용될 수 있다. 나아가, 스마트 뱅킹에서 자금 이체를 하는 경우에 공인 인증서를 대체한 전자 서명에 활용 가능하다. 이 응용이 유용한 것은, 소프트웨어 기반의 종래 공인 인증서를 완전한 하드웨어-기반(truly hardware-based) 공인 인증서로 대체 및/또는 보완할 수 있다는 데에 있다. 공인 인증서는 ID와 패스워드로 대변되는 지식 기반 인증을 소유 기반 인증으로 보완한다는 의미를 가지고 있었는데, 이 공인 인증서가 전자 파일 형태로 저장되는 것이다 보니 공인 인증서의 부정한 유출의 문제도 있었다. 그런데, 이 실시예에 따라 완전한 하드웨어-기반 전자 서명이 가능하다면, 굉장히 신뢰 수준이 높은 기기 인증이 가능하다. 또한 금융사 입장에서는 PUF 자체의 복제 불가능성과 유일성에 따라, 전자 서명되어 완료된 트랜잭션에 대해 사용자가 부인을 하는 것을 방지할 수 있는 기대 효과도 있다.

[0056] 도 7과 도 8은 일실시예에 따른 보안 통신 방법을 도시하는 흐름도이다. 인증 장치에 포함되는 보안 다이-칩이 스마트 카드 다이-칩의 지원으로 보안 통신을 수행하고 있다. 도 7은 보안 통신을 위한 세션 키의 수신 과정을, 도 8은 이 세션 키를 이용한 데이터의 보안 전송을 제시한다. 도 7을 참고하면, 단계(710)에서 인증 장치(700)와 보안 통신할 서버 또는 다른 기기가 상기 인증 장치(700)가 가지고 있는 개인 키에 상응하는 공개 키로 통신에 사용될 세션 키를 암호화 한다. 그리고 이렇게 암호화된 세션 키(701)가 와이드 밴드를 통해 기기에 전송되고, 기기는 이를 인증 장치(700)에 전달한다(702). 이 전달 시에 인증 장치(700)에 포함되는 스마트 카드 다이-칩이 가지는 인터페이스, 이를테면 블루투스, SD 카드 슬롯, NFC, USB 등이 이용될 수 있다. 스마트 카드 다이-칩이 암호화된 세션 키(703)을 보안 다이-칩에 전달하면, 단계(720)에서 PUF가 제공하는 개인 키를

통해 이 세션 키의 복호화가 수행된다. 이로써 인증 장치(700)은 보안 통신에 이용되는 세션 키를 획득한다.

[0058] 도 8을 참고하면, 기기가 보안 통신을 통해 전송하고자 하는 메시지(801)이 인터페이스들을 이용하여 스마트 카드 다이-칩에 전달되고, 다시 보안 다이-칩에 전달된다(802). 그러면, 단계(810)에서 인증 장치(800)의 보안 다이-칩은 위에서 획득된 세션 키를 이용하여 메시지(802)의 암호화를 수행한다. 암호화된 메시지(803)는 스마트 카드 다이-칩에 전달되고, 이는 다시 인터페이스를 통해 기기에 전달된다(804). 기기는 다시 와이드 밴드 통신을 통해 서버 또는 다른 기기에 이 암호화된 메시지(805)를 전달하고, 단계(820)에서 세션 키를 이용한 메시지의 복호화가 수행된다. 예를 들었던 바와 같이 스마트 카드 다이-칩이 기기와 연결되는 인터페이스에는, 제한적이지 않고 예시적으로, SD, SIM, 블루투스, USB, NFC 등이 있다. 도시된 실시예는 중요한 장점을 제공한다. 바로 개방된 통신구간의 보호이다. 이미 언급한 바와 같이, IoT, M2M 환경에서는 기기 간에 주고 받는 메시지를 부정한 주체가 청취하는 위협이 존재하는데 이러한 실시예에 의해 해당 위협이 방지된다. 또한, IoT 기기, 특히 소형 센서 등의 기기는 탈취나 분실의 우려도 있으므로, 그에 따른 물리적 공격, 이를테면 부채널 공격이 있을 수도 있는데, PUF 및 하드웨어 보안 모듈을 포함하는 보안 다이-칩은 이러한 위협에도 강인하다. 따라서, IoT의 활성화에 있어서 이러한 하드웨어 보안이 중요한 역할을 할 수 있을 것이다.

[0060] 도 9, 도 10 및 도 11은 실시예들에 따른 서비스들을 도시한다. 먼저 도 9는 상술한 바와 같이, 종래의 인터페이스 엘리먼트들(910)이 각자 자신의 인터페이스(마이크로-SD카드 슬롯 921, USIM 슬롯 922, USB 포트 923, NFC 통신 인터페이스 924)를 이용해 기기(920)에 연결되는 것을 볼 수 있다. 상술한 실시예, 이를테면 도 1이나 도 2를 참조하여 설명한 구현에 따라, 이러한 통상의 인터페이스 엘리먼트들(910) 내에 PUF 기반 보안 다이-칩을 임베드 한다. 그리고 스마트 카드 다이-칩과 같은 지원 칩으로 이를 인터페이스 엘리먼트(910)와 연동 시킴으로써, 하드웨어-기반의 보안 인증 수단이 없던 기기(920) 및 인터페이스 엘리먼트들(910)이 하드웨어-기반 보안 인증 수단을 갖게 된다. 다시 말해, 종래의 마이크로-SD 카드(901), USIM 칩(902), USB 저장매체(903), NFC 기능이 있는 카드(904)가 휴대가능하고 및/또는 기기에 탈부착 가능한 하드웨어-기반 보안 엘리먼트(SE: Secure Element)가 되는 것이다. 이러한 응용을 보면 기기(920)에 임베드 되지 않고 사용자가 휴대하면서, 보안 인증이 필요할 때에만 선택적으로 해당 SE를 기기에 인터페이스 시킴으로써, 데이터 보호, 기기 인증 및 서버(930)와의 보안 통신 등을 수행할 수 있다. 이를 더 응용하면, 자동차(Vehicle)이나 다른 접속 분야에도 적용 가능하다.

[0062] 도 10은 자동차 스마트 키(1000)에 상기 실시예들에 따른 스마트 카드 다이-칩(1010)과 PUF 기반 보안 다이-칩(1020)을 하나의 칩으로 패키징 한 것을 도시한다. 스마트 카드 다이-칩(1010)이 가지고 있는 인터페이스 및/또는 Bluetooth, UHF RFID 등 스마트 키 자체의 인터페이스(1030)을 통해 자동차(1040)와 연결이 이루어 진다. 그러면, 스마트 키(1000) 및/또는 이 스마트 키와 연결된 자동차(1040)의 기기 인증이 가능하고, 이에 따라 선별적인 서비스 제공이 가능하다. 예를 들어, 자동차 회사에서 제공하는 원격 문열림, 시동 제어 등 자동차 관리 유료 서비스(1051)을 제공하는 데에 기기를 인증하는 것이 가능하고, 자동차와 자동차, 자동차와 인프라 등 V2X 통신을 이용한 자율 주행/ 스마트 주행에서 기기를 인증하는 응용(1052)도 가능하다. 나아가, 스마트 하이웨이 서비스에 연결되어(1053), 스마트 톨링이나 맞춤 정보 제공을 위한 기기 인증도 가능할 것이다.

[0064] 도 11은 와이파이 AP의 인증을 위해 실시예들이 이용되는 응용을 제시한다. 최근 스마트폰과 같은 모바일 단말에 위협이 되는 보안 공격 중 하나가, 정상적인 WiFi AP (Access Point)인 것으로 가장하여, 단말이 이에 연결되면 보안 공격을 하는 사례가 소개되고 있다. 이 경우, WiFi AP(1121)에 상기 실시예에 따른 하드웨어 기반 SE(1120)이 탑재되어 기기 인증을 할 수 있으면, 부정한 보안 공격을 방지할 수 있다. 또한, 단말(1111)쪽에 상기 실시예에 따른 하드웨어 기반 SE(1110)가 연결 됨으로써 기기 인증, 보안 통신 및 데이터 보호 등 상술한 서비스가 가능하다. 개인용 가정용 응용뿐만 아니라, 사무 행정용, 군사용, 산업용에 이르기까지 이러한 패러다임에 의한 기기-기기 연결은 M2M 또는 IoT에서 이슈로 제기되는 보안 위협을 해결하는 값싸고 신뢰성 높은 해결책이 될 것이다.

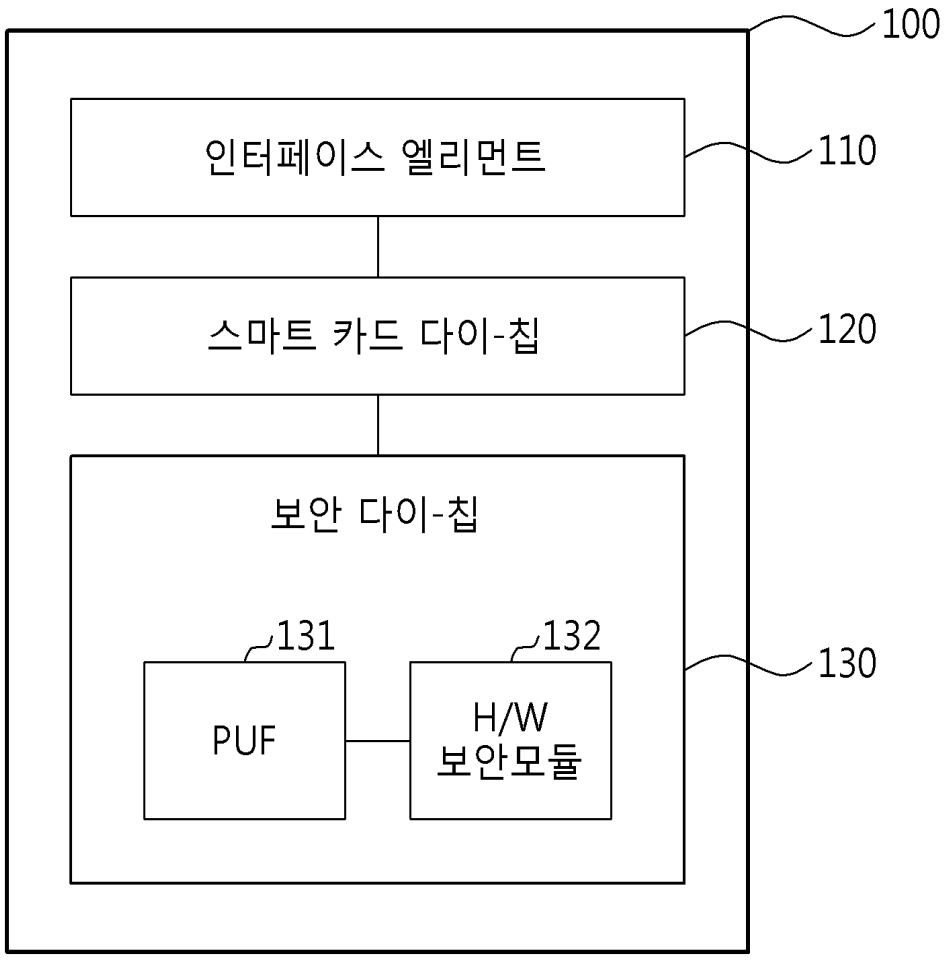
[0066] 이상에서, 실시예들이 비록 한정된 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면

상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

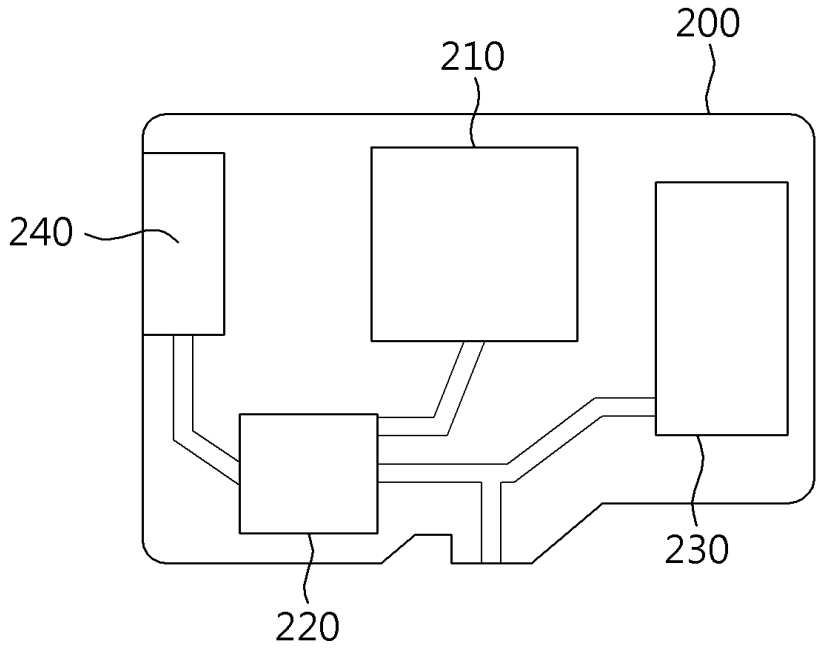
[0067] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

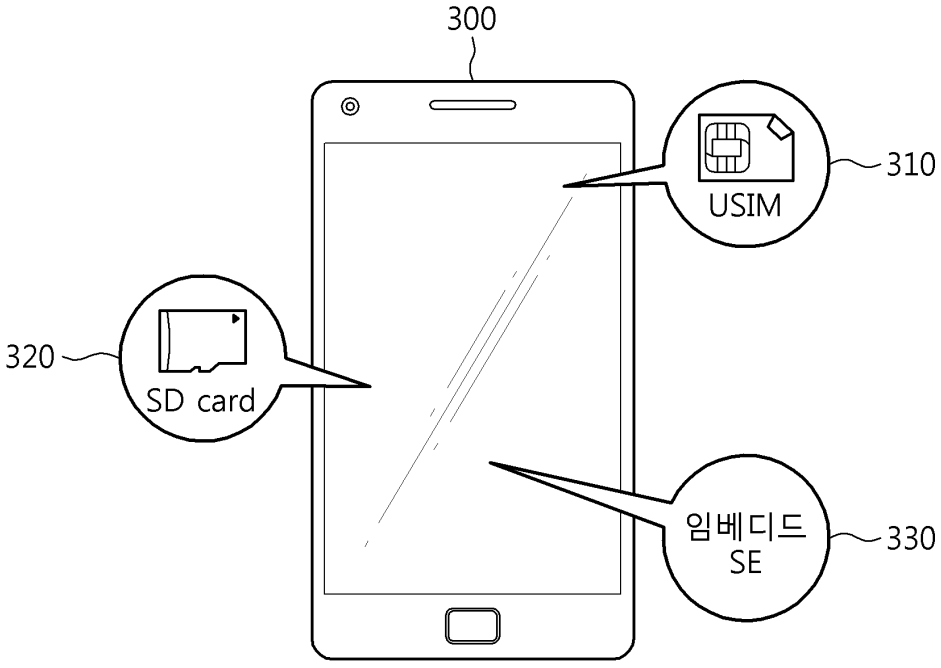
도면1



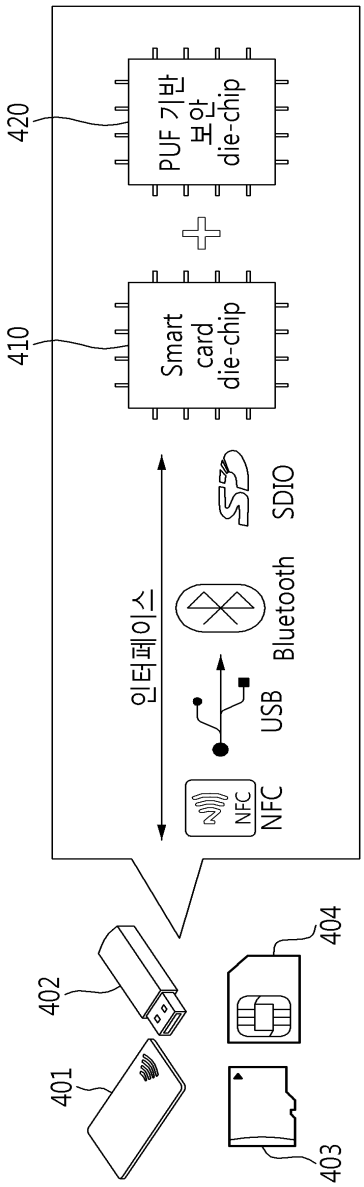
도면2



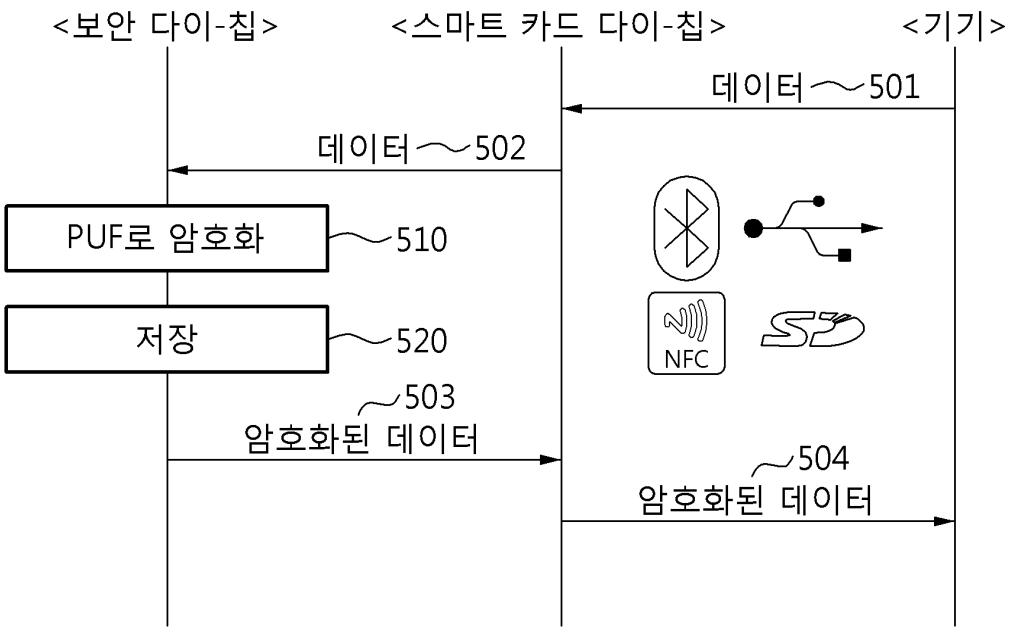
도면3



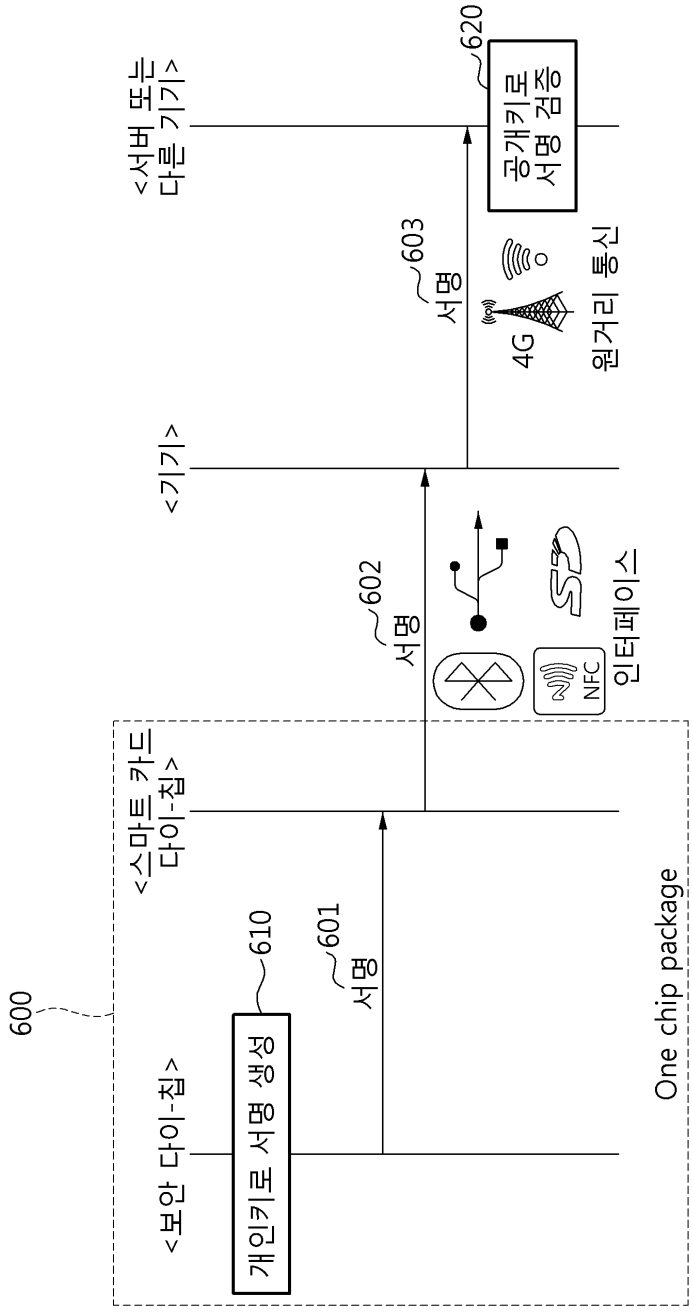
도면4


420
PUF 기반 보안 die-chip
410
Smart card die-chip
인터페이스
SDIO
Bluetooth
USB
NFC
NFC
402
401
404
403

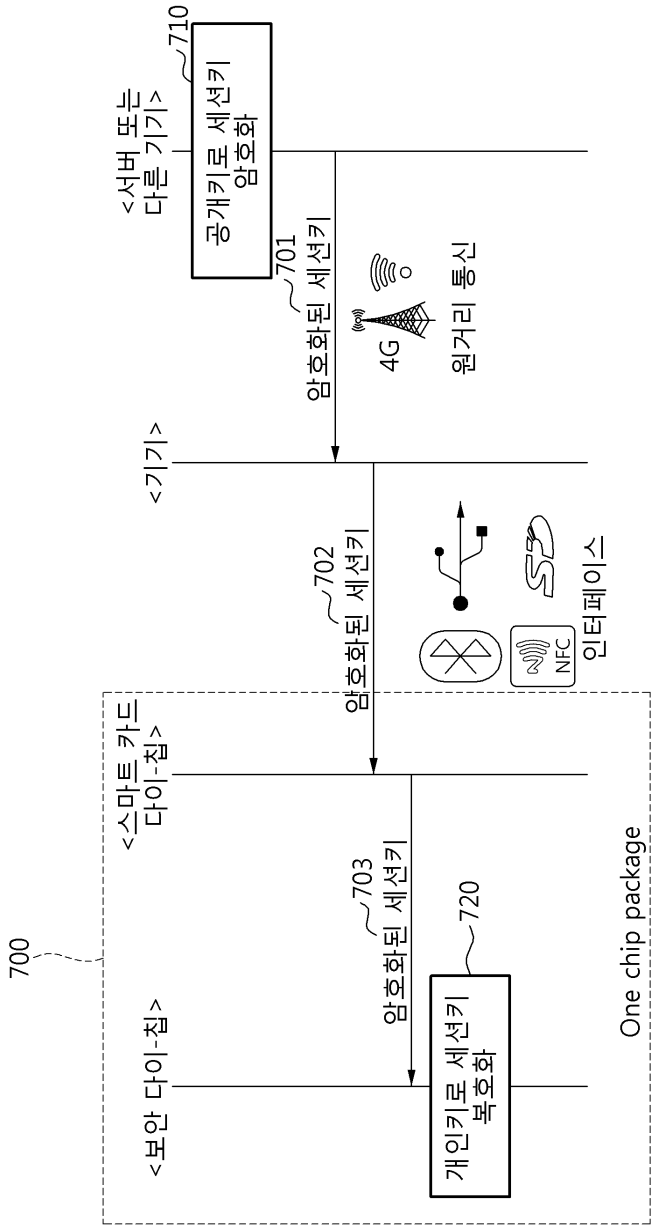
도면5


<보안 다이-칩>
<스마트 카드 다이-칩>
<기기>
데이터 501
데이터 502
PUF로 암호화
510
저장
520
503
암호화된 데이터
504
암호화된 데이터
NFC

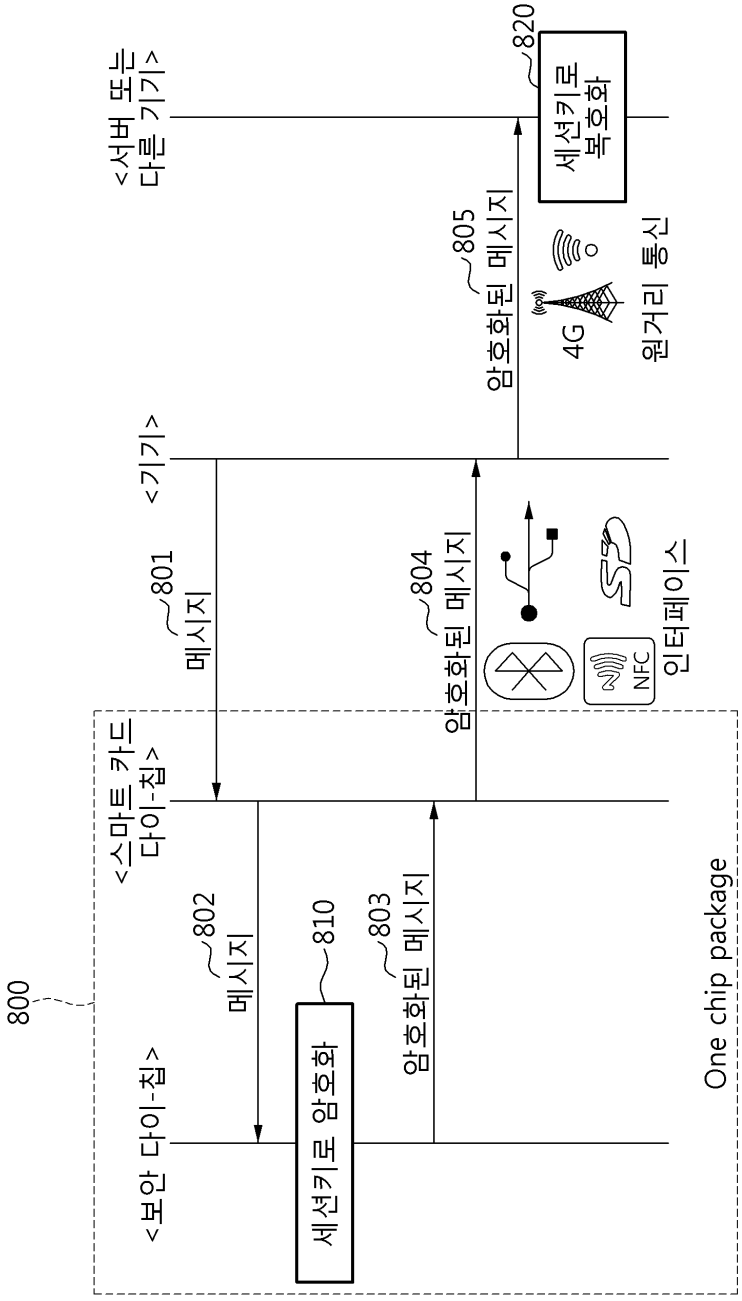
도면6


600
One chip package
<보안 다이-칩>
개인키로 서명 생성
610
601
서명
<스마트 카드 다이-칩>
602
서명
인터페이스
NFC
<기기>
603
서명
4G
원거리 통신
<서버 또는 다른 기기>
620
공개키로 서명 검증

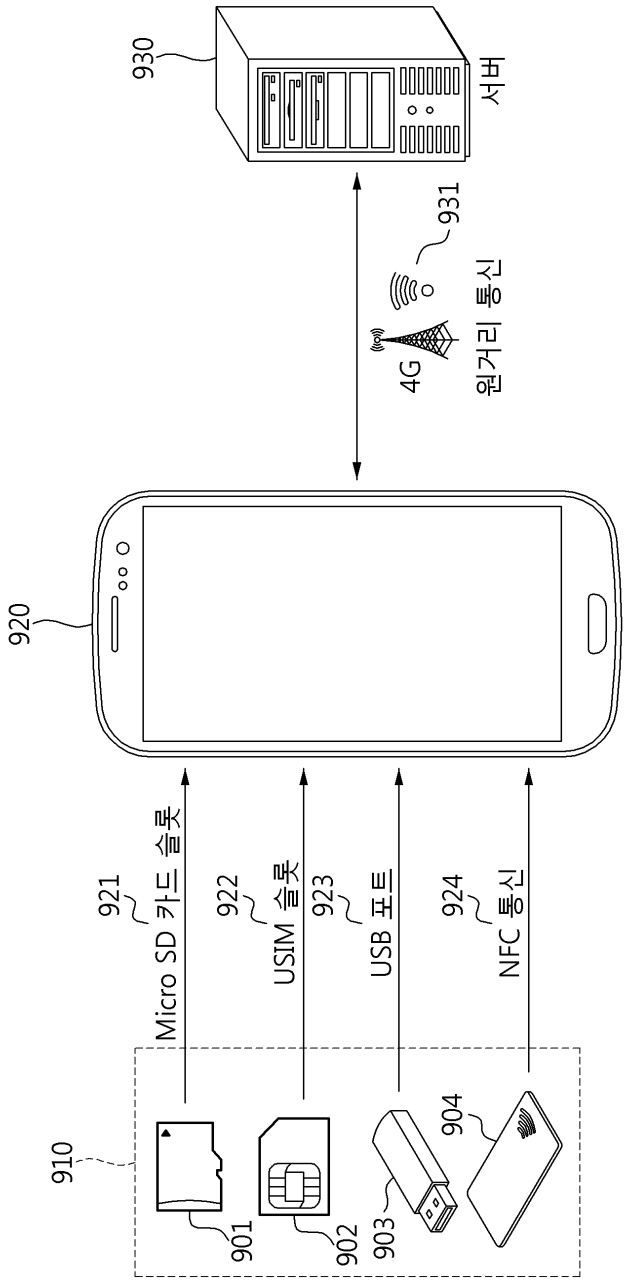
도면7


700
<보안 다이-칩>
<스마트 카드 다이-칩>
<기기>
<서버 또는 다른 기기>
710
공개키로 세션키 암호화
701
암호화된 세션키
4G
원거리 통신
702
암호화된 세션키
NFC
인터페이스
703
암호화된 세션키
720
개인키로 세션키 복호화
One chip package

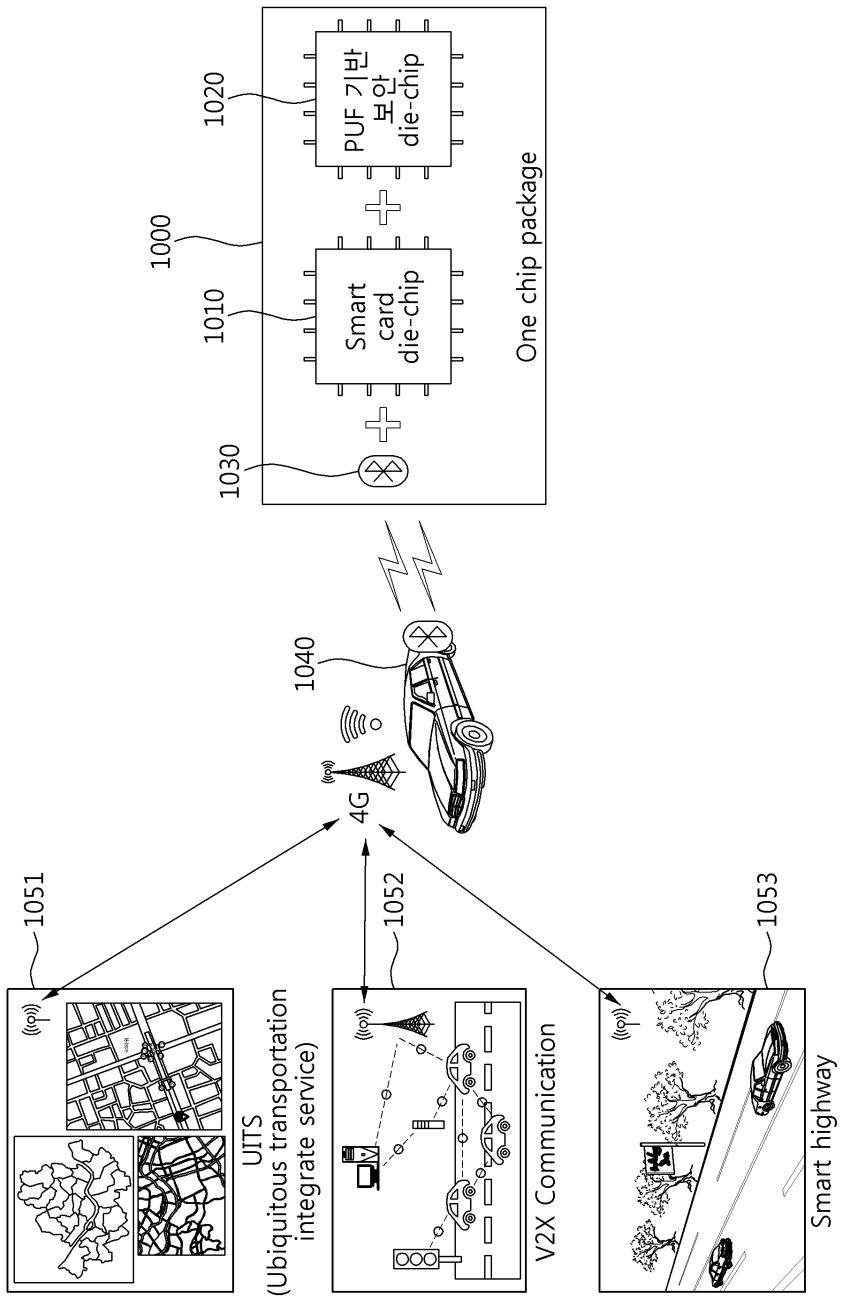
도면8


800
<보안 다이-칩>
<스마트 카드 다이-칩>
<기기>
<서버 또는 다른 기기>
802 메시지
801 메시지
803 암호화된 메시지
804 암호화된 메시지
805 암호화된 메시지
810 세션키로 암호화
820 세션키로 복호화
4G
원거리 통신
NFC
인터페이스
One chip package

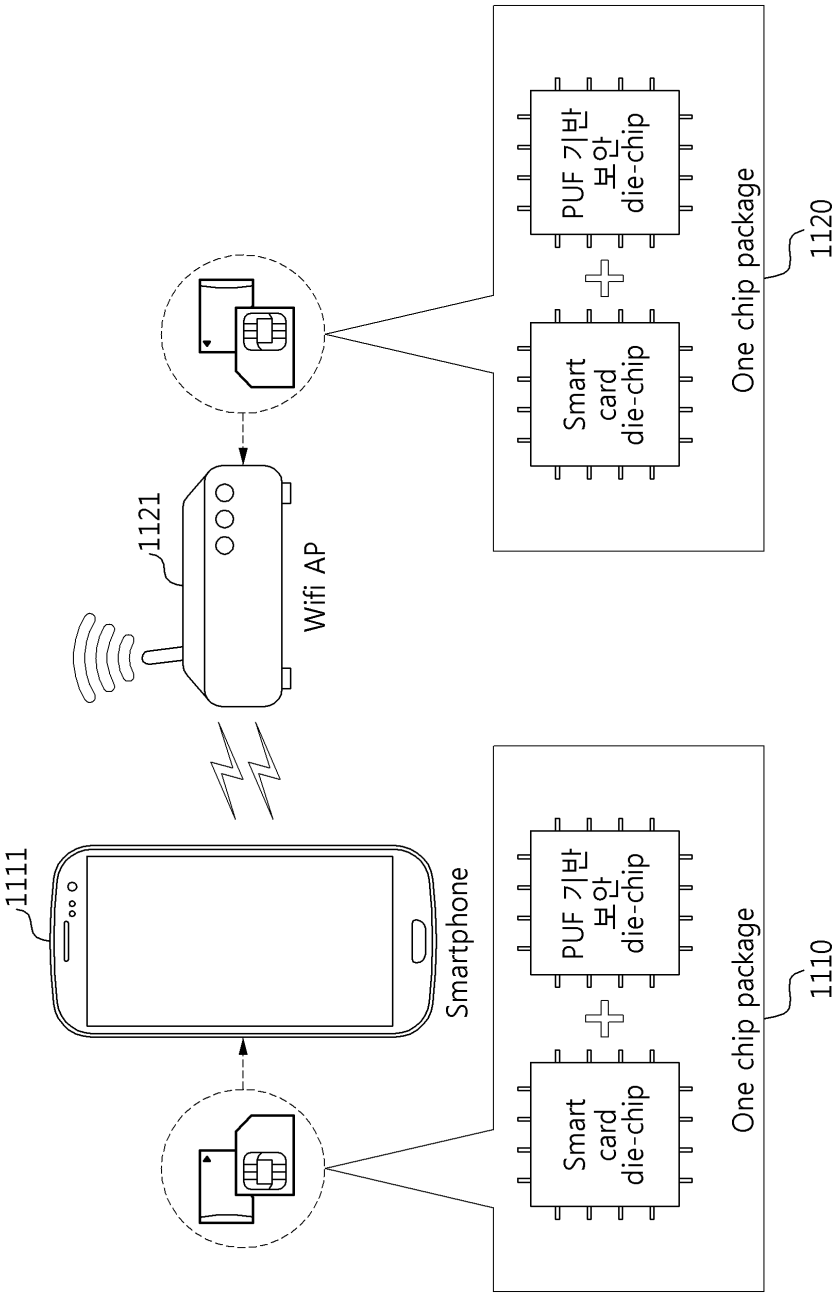
도면9


930
서버
931
원거리 통신
4G
920
921
Micro SD 카드 슬롯
922
USIM 슬롯
923
USB 포트
924
NFC 통신
910
901
902
903
904

도면10


1020
PUF 기반 보안 die-chip
1000
1010
Smart card die-chip
One chip package
1030
1040
4G
1051
1052
1053
UITS
(Ubiquitous transportation integrate service)
V2X Communication
Smart highway

도면11


PUF 기반
보안
die-chip
Smart
card
die-chip
One chip package
1120
1121
Wifi AP
1111
Smartphone
PUF 기반
보안
die-chip
Smart
card
die-chip
One chip package
1110