(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06K 17/00 (2006.01)
H04B 5/00 (2006.01)

(45) 공고일자 2006년12월26일
(11) 등록번호 10-0661021
(24) 등록일자 2006년12월18일

(21) 출원번호 10-2006-0012520
(22) 출원일자 2006년02월09일
심사청구일자 2006년02월09일

(65) 공개번호
(43) 공개일자

(73) 특허권자 한국과학기술원
대전 유성구 구성동 373-1

(72) 발명자 박기웅
서울 노원구 월계4동 500-11번지

임상석
광주 광산구 월곡2동 일신아파트 104동 1403호

박영우
경기 성남시 중원구 은행2동 708번지

박규호
충청남도 공주시 장기면 금암리 314-98 번지

(74) 대리인 이원희

심사관 : 김창주

전체 청구항 수 : 총 7 항

(54) ＲＦＩＤ를 이용한 보안 카드의 저전력 인증 장치 및 방법

(57) 요약

본 발명은 보안 카드에 전원 관리 모듈을 구비하여 RFID로부터 수신된 신호를 바탕으로 보안 카드의 가동이 필요한 경우에만 전력이 공급되도록 하여 보안 카드의 연속 사용 시간을 증가시킴과 더불어 복잡한 암호 해독 처리를 지원하는 RFID를 이용한 보안 카드의 저전력 인증 장치 및 방법을 제공한다.

본 발명의 구현을 위한 보안 카드는 RF 안테나에서 발생된 전자기장에 의해 활성화되는 RF 태그; RF 리더로부터의 정보에 따라 보안 카드의 현재 위치가 인증이 필요한 구간인지 아니면 인증과 위치기반서비스가 필요한 구간인지의 여부를 파악하는 RFID LF 송수신기; 상기 RFID LF 송수신기에서 파악된 정보를 해석하여 이로부터 인증만 필요한지 또는 인증과 위치기반서비스가 필요한지의 상태 판단을 통해 인증시 보안 카드의 전원 차단 또는 전원 공급을 제어하는 전원 관리 모듈; 상기 전원 관리 모듈의 상태 판단에 따른 전원 공급시 정해진 인증 프로토콜을 수행하는 중앙처리장치; 및 전원 관리 모듈의 상태 판단에 따른 전원 공급시 상기 중앙처리장치의 제어에 따라 RSA(Rivest Shamir Adleman) 암호화를 행하는 암호 프로세서;를 포함하여 구성된다.

대표도

도 4

특허청구의 범위

청구항 1.

RF 안테나에서 발생되는 전자기장으로 인해 활성화되는 보안 카드; 상기 보안 카드에서 인증요청을 위해 송신되는 신호를 수신하여 무선통신모듈을 통해 인증 서버로 전달하는 RF 리더; 및 상기 보안 카드의 인증을 위한 인증 서버를 포함하는 인증 장치에 있어서,

상기 보안 카드는 상기 RF 안테나에서 발생되는 전자기장으로 활성화된 후, 상기 RF 리더로부터 제공되는 정보에 따른 인증 또는 인증과 위치기반서비스의 필요여부에 따라, 보안 카드의 전원 차단 또는 전원 공급을 제어하는 전원 관리 모듈을 구비하는 것을 특징으로 하는 RFID를 이용한 보안 카드의 저전력 인증 장치.

청구항 2.

제 1 항에 있어서, 상기 보안 카드는

상기 RF 안테나에서 발생된 전자기장에 의해 활성화되는 RF 태그;

상기 RF 리더에서 제공되는 정보로부터 보안 카드의 현재 위치가 인증이 필요한 구간인지 아니면 인증과 위치기반서비스가 필요한 구간인지의 여부를 파악하는 RFID LF 송수신기;

상기 RFID LF 송수신기에서 파악된 정보를 해석하여 이로부터 인증만 필요한지 또는 인증과 위치기반서비스가 필요한지의 상태 판단을 통해 보안 카드의 전원 차단 또는 전원 공급을 제어하는 전원 관리 모듈;

상기 전원 관리 모듈의 상태 판단에 따른 전원 공급시 정해진 인증 프로토콜을 수행하는 중앙처리장치; 및

상기 전원 관리 모듈의 상태 판단에 따른 전원 공급시 상기 중앙처리장치의 제어에 따라 상기 RF 리더측의 무선통신모듈과 무선 통신하는 무선통신모듈;

을 포함하는 것을 특징으로 하는 RFID를 이용한 보안 카드의 저전력 인증 장치.

청구항 3.

제 2 항에 있어서, 상기 무선통신모듈은

지그비 통신모듈인 것을 특징으로 하는 RFID를 이용한 보안 카드의 저전력 인증 장치.

청구항 4.

제 2 항에 있어서, 상기 보안 카드는

상기 전원 관리 모듈의 상태 판단에 따른 전원 공급시 상기 중앙처리장치의 제어에 따라 RSA(Rivest Shamir Adleman) 암호화를 행하는 암호 프로세서를 더 포함하는 것을 특징으로 하는 RFID를 이용한 보안 카드의 저전력 인증 장치.

청구항 5.

전원관리를 위한 전원 관리 모듈을 구비하는 보안 카드; 상기 보안 카드의 인증을 위한 RF 리더 및 인증 서버를 포함하는 시스템에서의 인증 방법에 있어서,

상기 보안 카드의 전원 관리 모듈에서, RF 안테나에서 발생되는 전자기장에 의해 활성화되는 상기 보안 카드의 현재 위치가 인증만 필요한 구간인지 또는 인증과 위치기반서비스가 필요한 구간인지에 대한 정보를 바탕으로 전원 관리를 위한 상태를 판단하는 제1과정; 및

상기 전원 관리 모듈에서, 상기 전원 관리를 위한 상태 판단에 따른 인증 또는 인증과 위치기반서비스의 필요여부에 따라 상기 보안 카드의 전원 차단 또는 전원이 공급되도록 전원의 상태 전이를 행하는 제2과정;

을 포함하여 이루어짐을 특징으로 하는 RFID를 이용한 보안 카드의 저전력 인증 방법.

청구항 6.

제 5 항에 있어서, 상기 제2과정에서 상기 전원 관리를 위한 상태 판단 결과 인증만 필요한 경우,

상기 보안 카드 내의 중앙처리장치에 의해 보안 카드의 인증을 위한 정해진 인증 프로토콜을 수행하는 제1단계; 및

상기 인증 프로토콜 수행 후, 상기 전원 관리 모듈에 의해 보안 카드의 전원이 차단되는 유휴상태로 상태 전이하는 제2단계;

를 포함하는 것을 특징으로 하는 RFID를 이용한 보안 카드의 저전력 인증 방법.

청구항 7.

제 5 항에 있어서, 상기 제2과정에서 상기 전원 관리를 위한 상태 판단 결과 인증과 위치기반서비스가 필요한 경우,

상기 보안 카드 내의 중앙처리장치에 의해 보안 카드의 인증을 위한 정해진 인증 프로토콜을 수행하는 제1단계;

상기 인증 프로토콜 수행 결과, 상기 인증 서버로부터 보안 카드가 인증을 받지 못하면 상기 전원 관리 모듈에 의해 상기 보안 카드의 전원이 차단되는 유휴상태로 전이되는 제2단계;

상기 인증 프로토콜 수행 결과, 인증을 받게 되면 상기 중앙처리장치의 제어에 따라 RSSI(Received Signal Strength Indication) 데이터를 위치기반서비스를 위해 일정 간격으로 전송하는 제3단계; 및

상기 RSSI 데이터 전송 중 상기 보안 카드가 위치인식서비스가 필요한 구간을 벗어나면 위치기반서비스 종료구간으로 상태 전이되어 상기 전원 관리 모듈에 의해 보안 카드의 전원이 차단되는 유휴상태로 전이되는 제4단계;

를 포함하는 것을 특징으로 하는 RFID를 이용한 보안 카드의 저전력 인증 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 RFID(Radio Frequency Identification)를 이용하는 인증 시스템에 관한 것으로, 특히 보안 카드에 전원 관리 모듈을 구비하여 RFID로부터 수신된 신호를 바탕으로 보안 카드의 가동이 필요한 경우에만 전력이 공급되도록 하여 보안 카드의 연속 사용 시간을 증가시킴과 더불어 복잡한 암호 해독 처리를 지원하는 RFID를 이용한 보안 카드의 저전력 인증 장치 및 방법에 관한 것이다.

일반적으로 보안이 중요시 되는 환경에서 허가를 요청하는 사용자가 등록되어 있거나 정당하게 허가받은 사용자인지를 확인하는 인증 시스템이 널리 사용되고 있다. 특히 RFID와 스마트카드와 같은 소형 보안 카드가 개발됨에 따라 인증 시스템을 구축하는데 있어서 RFID와 스마트카드가 널리 사용되고 있다.

RFID는 무선주파수 인식기술로, 무선 주파수를 사용하여 고유한 식별정보를 가지고 있는 태그로부터 비접촉식으로 정보를 독출하거나 기록함으로써 태그가 부착된 물건이나 동물, 사람 등을 인식.추적.관리할 수 있는 기술이다.

RFID시스템은 고유한 식별정보를 지니고 물건이나 동물 등에 부착되는 다수의 RF 태그(Tag 또는 Transponder)와, 상기 RF 태그를 가지고 있는 정보를 읽거나 쓰기 위한 RF 리더로 구성된다.

도 1은 일반적인 RFID시스템의 기본적인 구성을 보여주고 있다.

도시된 바와 같이, RF 태그(5)는 안테나와 IC칩으로 이루어지고, IC칩에는 고주파 신호를 처리하기 위한 RF회로, 제어로직 및 메모리 등이 내장되어 있다. RF 리더(1)는 특정 주파수 대역의 무선 주파수(RF)를 RF 태그(5)로 전송함과 아울러 RF 태그(5)에서 반사되는 고주파수 신호를 수신한다. 상기 RF 리더(1)는 무선 주파수를 송수신하기 위한 안테나와 RF송수신부 그리고 신호 처리를 위한 신호처리부 등으로 이루어진다.

한편, RF 리더(1)는 컴퓨터 등 정보처리장치와 연결될 수 있으며, 상기 정보처리장치는 소정의 미들웨어 또는 응용프로그램을 사용하여 RF 리더(1)에 의해 독출된 정보를 분석.저장한다.

이러한 RFID를 인증 시스템에 이용할 경우 자신이 가지고 있는 RFID 정보를 RFID 리더에 자신의 의사와 관계없이 송신함으로서 보안을 유지하는데 있어 많은 문제점을 노출한다.

이를 이용하여 특정 RFID 카드에 대한 복제가 가능하여 보안성이 낮아지는 단점이 있다. 이러한 문제점을 보완하기 위해 전자기장을 통해 유도되는 전력량을 고려하여 40bit정도의 대칭키를 사용하여 송신시 데이터의 암호화를 시도하나 짧은 키의 길이에 의해 여전히 키의 해킹에 취약하다.

접촉형 스마트카드를 인증시스템에 이용할 경우 카드 내부에 중앙 처리 장치, 메모리를 내장하여 카드 내부에서 특정 암호화 알고리즘의 수행이 가능하므로 RFID 카드에 비해 높은 보안성을 유지시킬 수 있지만 사용시 매번 리더에 삽입해야하는 번거러움 때문에 사용성이 매우 저하되고 비접촉형 스마트카드는 RFID의 키 해킹 취약성 문제점들을 갖고 있다.

이러한 문제를 해결하고자 다음과 같은 방안들이 모색되어지고 있다.

첫 번째로, 보안 카드에 독립적인 전원 공급 장치를 부착하고 암호 프로세서를 장착하여 보다 높은 보안성을 제공하는 것이 가능하게 하는 방법이 있다.

이 방법의 단점은 인증 절차를 거치기 위해 보안 카드는 인증 시스템이 요구하는 응답을 처리하기 위해 항상 대기 상태로 있어야 한다. 대기 상태로 있어야 함은 보안 카드에 전원이 연속적으로 공급이 되어야 함을 의미하고 사용자가 주기적으로 전원 공급 장치를 교체 또는 충전을 해주어야 하므로 사용성이 떨어진다.

두 번째 방법으로는 용량이 큰 전원 공급 장치를 부착하여 연속 대기 시간을 늘리는 방법이 있다. 이 방법의 단점은 착용성이 떨어지고 미관에 좋지 않다.

세 번째로, 장치에 다소 넓은 태양열발전 패널을 부착시켜 전원을 공급해 주어 연속 대기 시간을 늘리는 방법이 있다.

이 방법에서는 미관에 안 좋은 다소 넓은 태양열발전 패널을 각 사용자가 가지고 있어야 하고, 다수의 인증 시스템이 건물 내에 위치하고 있다는 것을 감안하면 실직적인 충전이 어렵다는 단점이 있다.

한편, 종래 RFID를 이용한 인증 기술의 일예로, 국제공개번호 제 WO2003/081934 호에 따른 인증장치, 방법 및 시스템을 들 수 있다.

이는 보안 카드의 사용자의 의사와 관계없이 독출장치의 요구에 따라 자신의 사용자 식별 아이디를 무조건적으로 방사하도록 되어 있어 보안성이 매우 떨어지는 단점이 있다.

또한, "Next Generation PC 2005 pp172-178, October 2005년"에 게재된 "An Interoperable Authentication System using ZigBee-enabled Tiny Portable Device and PKI"에는 보다 높은 보안 카드의 제작을 위하여 자체 전력을 이용한 프로세서를 장착하고, 인증 프로토콜을 실행하여 인증을 받는 절차를 수행하도록 되어 있으나, 이는 전력 문제를 고려하지 않아 연속대기시간이 매우 짧은 단점이 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 이러한 점을 감안한 것으로, 본 발명의 목적은 RFID와 보안 카드의 전원 관리 모듈에 의하여 보안 카드의 전원을 제어하여 보안 카드의 사용 시간을 증대시킬 수 있도록 한 RFID를 이용한 보안 카드의 저전력 인증 장치 및 방법을 제공함에 있다.

본 발명의 다른 목적은 자체 전원으로 작동하는 중앙처리장치와 암호 프로세서를 이용하여 복잡한 암호 해독이 가능토록 함으로써 보안성이 높은 RFID를 이용한 보안 카드의 저전력 인증 장치 및 방법을 제공함에 있다.

발명의 구성

상기 본 발명의 목적을 달성하기 위한 본 발명에 따른 RFID를 이용한 보안 카드의 저전력 인증 장치는, RF 안테나에서 발생되는 전자기장으로 인해 활성화되는 보안 카드; 상기 보안 카드에서 인증요청을 위해 송신되는 신호를 수신하여 무선통신모듈을 통해 인증 서버로 전달하는 RF 리더; 및 상기 보안 카드의 인증을 위한 인증 서버를 포함하는 인증 장치에 있어서, 상기 보안 카드는 상기 RF 안테나에서 발생되는 전자기장으로 활성화된 후, 상기 RF 리더로부터 제공되는 정보에 따른 인증 또는 인증과 위치기반서비스의 필요여부에 따라, 보안 카드의 전원 차단 또는 전원 공급을 제어하는 전원 관리 모듈을 구비하는 것을 특징으로 한다.

상기 보안 카드는 상기 RF 안테나에서 발생된 전자기장에 의해 활성화되는 RF 태그; 상기 RF 리더에서 제공되는 정보로부터 보안 카드의 현재 위치가 인증이 필요한 구간인지 아니면 인증과 위치기반서비스가 필요한 구간인지의 여부를 파악하는 RFID LF 송수신기; 상기 RFID LF 송수신기에서 파악된 정보를 해석하여 이로부터 인증만 필요한지 또는 인증과 위치기반서비스가 필요한지의 상태 판단을 통해 보안 카드의 전원 차단 또는 전원 공급을 제어하는 전원 관리 모듈; 상기 전원 관리 모듈의 상태 판단에 따른 전원 공급시 정해진 인증 프로토콜을 수행하는 중앙처리장치; 및 상기 전원 관리 모듈의 상태 판단에 따른 전원 공급시 상기 중앙처리장치의 제어에 따라 상기 RF 리더측의 무선통신모듈과 무선 통신하는 무선통신모듈;을 포함하는 것을 특징으로 한다.

상기 목적을 달성하기 위한 본 발명에 따른 RFID를 이용한 보안 카드의 저전력 인증 방법은, 전원관리를 위한 전원 관리 모듈을 구비하는 보안 카드; 상기 보안 카드의 인증을 위한 RF 리더 및 인증 서버를 포함하는 시스템에서의 인증 방법에 있어서, 상기 보안 카드의 전원 관리 모듈에서, RF 안테나에서 발생되는 전자기장에 의해 활성화되는 상기 보안 카드의 현재 위치가 인증만 필요한 구간인지 또는 인증과 위치기반서비스가 필요한 구간인지에 대한 정보를 바탕으로 전원 관리를 위한 상태를 판단하는 제1과정; 및 상기 전원 관리 모듈에서, 상기 전원 관리를 위한 상태 판단에 따른 인증 또는 인증과 위치기반서비스의 필요여부에 따라 인증시 상기 보안 카드의 전원 차단 또는 전원이 공급되도록 전원의 상태 전이를 행하는 제2과정;을 포함하여 이루어짐을 특징으로 한다.

상기 제2과정에서 상기 전원 관리를 위한 상태 판단 결과 인증만 필요한 경우, 상기 보안 카드 내의 중앙처리장치에 의해 보안 카드의 인증을 위한 정해진 인증 프로토콜을 수행하는 제1단계; 및 상기 인증 프로토콜 수행 후, 상기 전원 관리 모듈에 의해 보안 카드의 전원이 차단되는 유휴상태로 상태 전이하는 제2단계;를 포함하는 것을 특징으로 한다.

상기 제2과정에서 상기 전원 관리를 위한 상태 판단 결과 인증과 위치기반서비스가 필요한 경우, 상기 보안 카드 내의 중앙처리장치에 의해 보안 카드의 인증을 위한 정해진 인증 프로토콜을 수행하는 제1단계; 상기 인증 프로토콜 수행 결과, 상기 인증 서버로부터 보안 카드가 인증을 받지 못하면 상기 전원 관리 모듈에 의해 상기 보안 카드의 전원이 차단되는 유휴상태로 전이되는 제2단계; 상기 인증 프로토콜 수행 결과, 인증을 받게 되면 상기 중앙처리장치의 제어에 따라 RSSI 데

이터를 위치기반서비스를 위해 일정 간격으로 전송하는 제3단계; 및 상기 RSSI 데이터 전송 중 상기 보안 카드가 위치인식 서비스가 필요한 구간을 벗어나면 위치기반서비스 종료구간으로 상태 전이되어 상기 전원 관리 모듈에 의해 보안 카드의 전원이 차단되는 유휴상태로 전이되는 제4단계;를 포함하는 것을 특징으로 한다.

이하, 본 발명의 바람직한 실시 예를 첨부된 도면을 참조하여 보다 상세하게 설명한다. 단, 하기 실시 예는 본 발명을 예시하는 것일 뿐 본 발명의 내용이 하기 실시 예에 한정되는 것은 아니다.

도 2는 본 발명에 따른 인증 장치에서 사용자의 보안 카드와 인증 장치와의 관계를 나타낸 도로, 본 발명의 인증 장치(100)는 RF 안테나(101), RF 리더(102), 지그비 송수신기(103), 인증 서버(104), 인증서 데이터베이스(105)로 구성된다.

이와 같은 시스템에서 사용자는 보안 카드(106)를 이용하여 인증을 받게 된다.

사용자가 소지하고 있는 보안 카드(106)와 RF 리더(102)의 RF 안테나(101) 사이의 거리가 가까워지게 되면, RF 안테나(101)에서 발생한 전자기장으로 보안 카드(106)가 작동하게 된다.

보안 카드(106)는 자신의 고유한 사용자 식별 아이디를 RF 리더(102)측의 지그비 송수신기(103)로 전송하게 되며, 지그비 송수신기(103)는 사용자 보안 카드(106)로 요청(이하, challenge라 칭함) 메시지를 보낸다. 사용자 보안 카드는(106)은 수신된 challenge 메시지를 개인 키로 암호화 하여 지그비 송수신기(103)로 응답한다.

이때, 지그비 송수신기(103)는 이전에 수신된 식별 아이디를 인증 서버(104)로 전송하게 되며, 인증 서버(104)는 수신된 식별 아이디에 해당하는 공개키를 얻기 위하여 쿼리를 인증서 데이터베이스(105)로 보낸다.

쿼리를 수신한 인증서 데이터베이스(105)는 보안 카드(106)에 해당하는 인증서를 인증 서버(104)로 전송하게 된다. 인증 서버(104)는 수신된 인증서에서 공개키를 추출하고 그것의 폐지여부를 확인한다.

공개키가 유효할 경우 사용자 보안 카드(106)가 암호화하여 전송하였던 응답 메시지를 해독하여 처음 송신하였던 challenge 메시지와의 동일여부를 검사하여 인증 여부를 결정한다.

이러한 연산에서 보안 카드(106)와 지그비 송수신기(103) 사이의 메시지 전송은 무선통신 수단인 지그비가 될 수 있고, 블루투스(Bluetooth), WLAN 등의 다른 무선 신호일 수 있다.

도 3은 상기 보안 카드(106)에 대한 상세 구성도를 도시한 것으로, 보안 카드(106)는 RF 태그(200), RFID LF(Low Frequency) 송수신기(201), 전원 관리 모듈(202), 중앙처리장치(203), 암호 프로세서(204), 지그비 통신 모듈(205)로 구성되어 있다. 여기서, 상기 RFID LF 송수신기(201)는 RF 태그(200) 내에 구성되는 것이 아니라 보안 카드(106) 내에 상기 RF 태그(200)와는 별도로 구성된다.

상기 RF 안테나(101)와 보안 카드(106) 사이의 거리가 가까워지면 RF 태그(200)에는 RF 안테나(101)에서 발생된 전자기장으로 인해 전력이 발생되고, RFID LF 송수신기(201)에 신호를 인가하게 된다.

RFID LF 송수신기(201)에서는 인가된 신호에 따라 전원 관리 모듈(202)에 신호를 전송하게 되며, 전원 관리 모듈(202)은 RFID LF 송수신기(201)로부터 인가되는 신호를 분석하여 분석결과에 따라 중앙처리장치(203), 암호 프로세서(204), 지그비 통신 모듈(205)에 전원을 인가하여 인증 연산이 수행될 수 있도록 하며, 위치 기반 서비스(LBS : Location Based Service)가 필요한 구간일 경우 중앙처리장치(203)에서 RSSI(Received Signal Strength Indication) 값을 송신하게 된다.

도 4는 상기 전원 관리 모듈(202)의 상태도를 나타낸 것이다.

전원 관리 모듈(202)은 평상시에는 보안 카드(106)의 전원이 차단되는 유휴 상태(300)에 있게 된다.

사용자가 소지한 보안 카드(106)가 RF 안테나(101)와 가까워지면 RFID LF 송수신기(201)에서는 RF 리더(102)로부터 현재의 위치가 인증이 필요한 구간인지, 인증과 위치 기반 서비스(LBS)가 필요한 구간인지에 대한 정보를 얻는다.

상기 RF 리더(102)는 RFID LF 송수신기(201)로 현재 환경에 대한 정보를 전해주며, RFID LF 송수신기(201)는 RF 리더(102)로부터 받은 정보를 전원 관리 모듈(202)로 전해주게 된다.

이에 따라 전원 관리 모듈(202)에서는 입력된 신호에 따라 상태 판단(301)을 행하게 된다.

즉, 입력된 신호를 해석하여 보안 카드(106)의 인증만 필요한 경우, 중앙처리장치(203)의 기 정해진 인증 프로토콜을 구동(302)시키게 된다. 인증 프로토콜의 연산이 끝나면 보안 카드(106)의 전원이 차단되는 유휴상태(300)로 돌아가게 된다.

유휴상태(300)로의 전환은 상기 중앙처리장치(203)로부터의 인증이 종료되었음을 알리는 신호에 따라 행해지게 된다.

반면, 상태 판단(301) 상태에서 인증 연산과 위치 기반 서비스가 필요한 구간일 경우에는 중앙처리장치(203)의 기 정해진 인증 프로토콜을 구동(303)시키고, 인증 프로토콜의 연산이 끝나 인증을 받게 되면 중앙처리장치(203)가 위치 기반 서비스(LBS)를 위해 RSSI 데이터를 일정 간격으로 전송하게 된다.

만약, 인증을 받지 못할 경우에는 인증 프로토콜 구동(303) 후, 보안 카드(106)의 전원이 차단되는 유휴상태(300)로 돌아가게 된다.

보안 카드(106)를 소지한 사용자가 위치 인식 서비스(LBS)가 필요한 구간을 벗어날 경우에는 위치 기반 서비스 종료구간(304)으로 상태가 전환되어 보안 카드(106)의 전원이 차단되면 전원 관리 모듈(202)은 유휴상태(300)로 전이된다.

상기 인증 프로토콜(302),(303)에 대한 상세 동작을 도 5 및 도 6에 나타내었다.

도 5는 위치 기반 서비스(LBS)가 필요 없는 구역의 인증에 대한 프로토콜 상세 설명을 위한 도이다.

보안 카드(106)의 전원 관리 모듈(202)은 RFID LF 송수신기(201)로부터 신호를 받아 상태 판단(301)을 하여 위치 기반 서비스(LBS)가 필요없는 구역임을 인지하고, 중앙처리장치(203)에 의한 인증 프로토콜 구동(302) 상태로 들어가게 되며, 도 5에 도시된 프로토콜이 가동되게 된다.

보안 카드(106)의 중앙처리장치(203)는 RF 태그(200) 내의 도시하지 않은 메모리에 기록되어 있는 사용자 식별 아이디(400)를 지그비 통신 모듈(205)을 통해 RF 리더(102)를 거쳐 인증 장치(100)로 송신하게 된다.

이를 수신한 인증 장치(100)는 무작위 생성된 데이터(challenge) 메시지(401)를 보안 카드(106)로 전송한다.

보안 카드(106)에서는 사용자 식별 아이디(400)의 전송 실패에 대비하기 위하여 사용자 식별 아이디 전송(400) 후, 도시하지 않은 타이머를 가동하여 일정 시간 초과시까지 challenge 메시지(401) 수신이 없으면 재전송(403)을 수행한다. 인증 장치(100)에서는 challenge 메시지(401)의 소실을 대비하여 타이머를 사용하여 일정 시간 초과시 재전송(405)을 수행한다.

지그비 통신 모듈(205)을 통해 challenge 메시지(401)를 수신한 보안 카드(106)는 중앙처리장치(203)의 제어에 따라 개인 키를 이용하여 암호 프로세서(204)에서 RSA(Rivest Shamir Adleman) 암호화(406)를 한 후, 응답(respnse) 메시지(407)를 인증 장치(100)로 전송한다.

응답 메세지(407)를 수신한 인증 장치(100)는 이전에 수신한 사용자 식별 아이디(400)를 인증서 데이터베이스(105)로 전송하여 해당하는 공개 키를 검색하고, 보안 카드(106)의 개인키로 암호화(406)된 응답 메시지(407) 데이터를 공개 키로 해독(410)하여 처음에 송신한 challenge(401)와 데이터가 일치하는지 비교한다.

일치할시 억셉트(이하, accept라 칭함) 메시지(411)를 보안 카드(106)로 전송하여 인증여부를 알려준다.

도 6은 위치 기반 서비스(LBS)가 필요한 구역의 인증에 대한 프로토콜 상세 설명을 위한 도이다.

보안 카드(106)의 전원 관리 모듈(202)은 RFID LF 송수신기(201)로부터 신호를 받아 상태 판단(301)을 하여 위치 기반 서비스(LBS)가 필요한 구역임을 인지하고, 중앙처리장치(203)에 의한 인증 프로토콜 구동(303) 상태로 들어가게 되며, 도 6에 도시된 인증 프로토콜이 가동되게 된다.

보안 카드(106)의 중앙처리장치(203)는 RF 태그(200) 내의 도시하지 않은 메모리에 기록되어 있는 사용자 식별 아이디(500)를 지그비 통신 모듈(205)을 RF 리더(102)를 거쳐 통해 인증 장치(100)로 송신하게 된다.

이를 수신한 인증 장치(100)는 무작위 생성된 데이터(challenge) 메시지(501)을 보안 카드(106)로 전송한다.

보안 카드(106)에서는 사용자 식별 아이디의 전송(500) 실패를 대비하기 위하여 전송(500) 후, 타이머를 가동하여 일정 시간 초과시까지 challenge 메시지(501) 수신이 없으면 재전송(503)을 수행하여 인증을 재시도한다.

인증 장치(100)에서는 challenge 메시지(501)의 소실을 대비하여 타이머를 사용하여 일정 시간 초과시 재전송(505)을 수행한다.

지그비 통신 모듈(205)를 통해 challenge 메시지(501)를 수신한 보안 카드(106)는 중앙처리장치(203)의 제어에 따라 개인 키를 이용하여 암호 프로세서(204)에서 RSA(Rivest Shamir Adleman) 암호화(506)를 한 후, 응답(respnse) 메시지(507)를 인증 장치(100)로 전송한다.

응답 메세지(507)를 수신한 인증 장치(100)는 이전에 수신한 사용자 식별 아이디(500)를 인증서 데이터베이스(105)로 전송하여 해당하는 공개 키를 검색하고, 응답 메시지(507) 데이터를 공개 키로 해독하여 처음에 송신한 challenge 메시지(501)와 데이터가 일치하는지 비교(510)한다. 일치할시 accept 메시지(511)를 보안 카드(106)로 전송하여 인증여부를 알려준다.

상기 응답 메시지(507)를 받은 인증 장치(100)는 accept 메시지(511)를 전송하게 되고, accept 메시지(511)의 소실을 대비하여 시간 초과시 재전송(512,513)을 수행한다.

accept 메시지(511)를 받은 보안 카드(106)는 일정 간격으로 위치 인식을 위한 RSSI값(515,516)을 일정 주기로 전송하게 된다.

상술한 바와 같이, 본 발명의 바람직한 실시 예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 또는 변형하여 실시할 수 있다.

발명의 효과

이상에서 살펴본 바와 같이, 본 발명은 종래의 인증 방식에서 수반되는 단점들, 즉 RFID에서는 사용자의 의사와 관계없이 ID정보가 유출이 되어 복제의 위험성과 스마트 카드 형태의 인증 시스템에서 발생되는 보안의 취약성을 해결할 수 있고, RFID기반 전원 관리 기법과 RFID와 독립적인 중앙처리장치와 암호 프로세서, 지그비 통신 모듈을 통해 연속 사용 시간을 높이고 1024비트 이상의 암호화 알고리즘의 수행이 가능하여 보안성 증대는 물론 사용성을 높일 수 있다.

도면의 간단한 설명

도 1은 일반적인 RFID시스템의 기본적인 구성을 나타낸 도.

도 2는 본 발명에 따른 인증 시스템에서 사용자의 보안 카드와 RFID 장비 및 인증 서버의 관계를 나타낸도.

도 3은 본 발명에 따른 보안 카드의 전원 관리를 위한 모듈 연결 배치도.

도 4는 본 발명에 따른 전원 관리 모듈의 상태 전이 알고리즘을 나타내는 상태 전이 다이어그램.

도 5는 본 발명에 따른 위치 기반 서비스가 필요 없는 공간 및 디바이스에 대한 프로토콜 다이어그램.

도 6은 본 발명에 따른 위치 기반 서비스가 필요한 공간 및 디바이스에 대한 프로토콜 다이어그램.

<도면의 주요 부분에 대한 부호의 설명>

101 : RF 안테나 102 : RF 리더

103 : 지그비 송수신기 104 : 인증 서버

105 : 인증서 데이터베이스 106 : 보안 카드

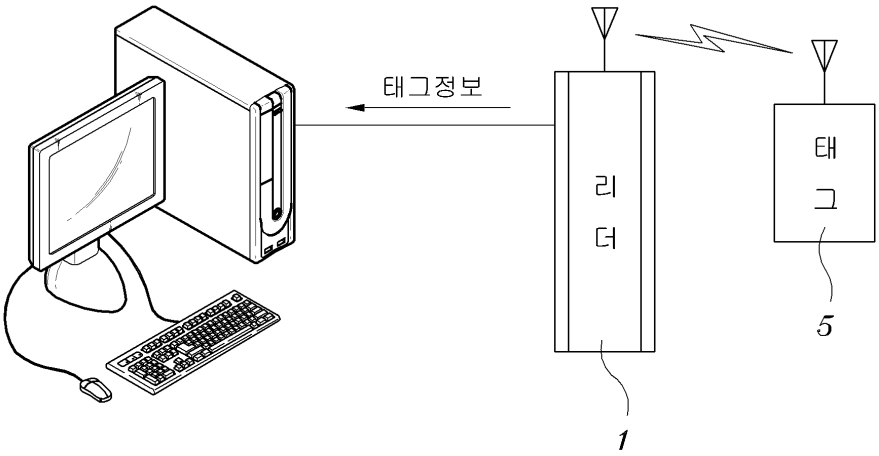
200 : RF 태그 201 : RFID LF 송수신기

203 : 중앙처리장치 204 : 암호 프로세서

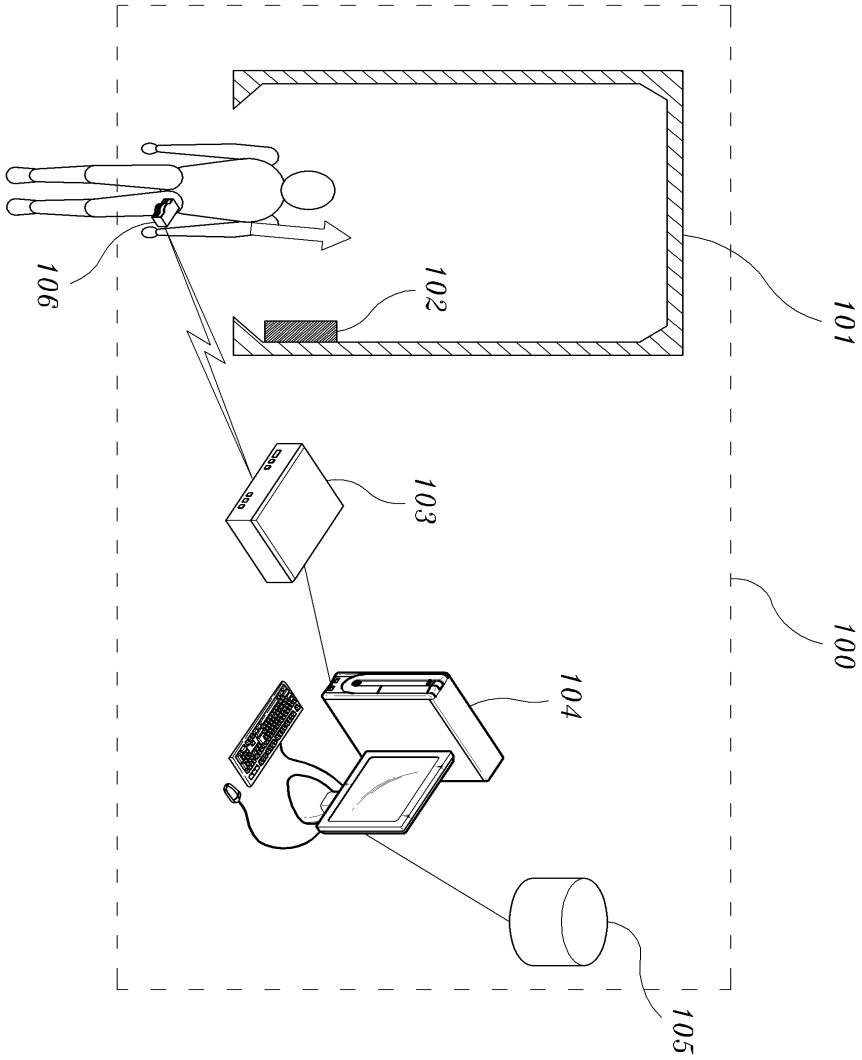
205 : 지그비 통신 모듈

도면

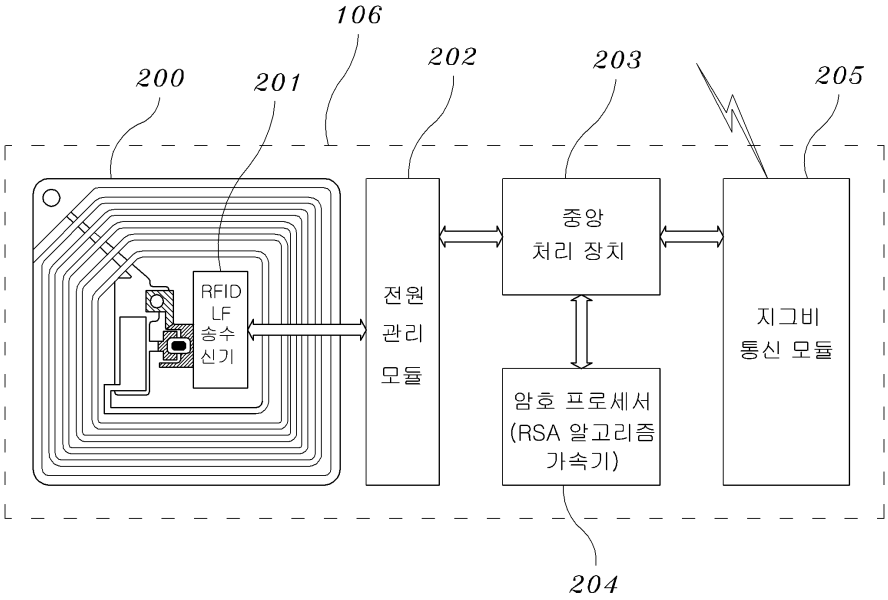
도면1



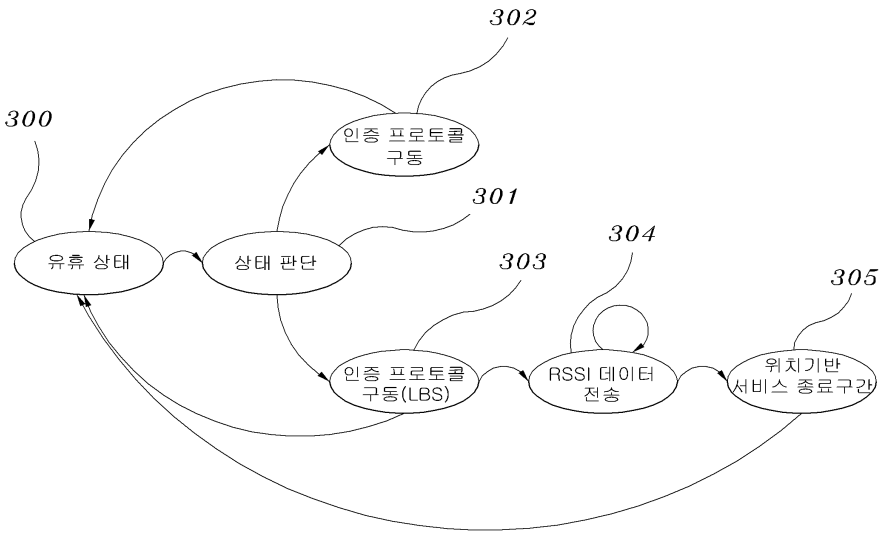
도면2


106
102
101
103
100
104
105

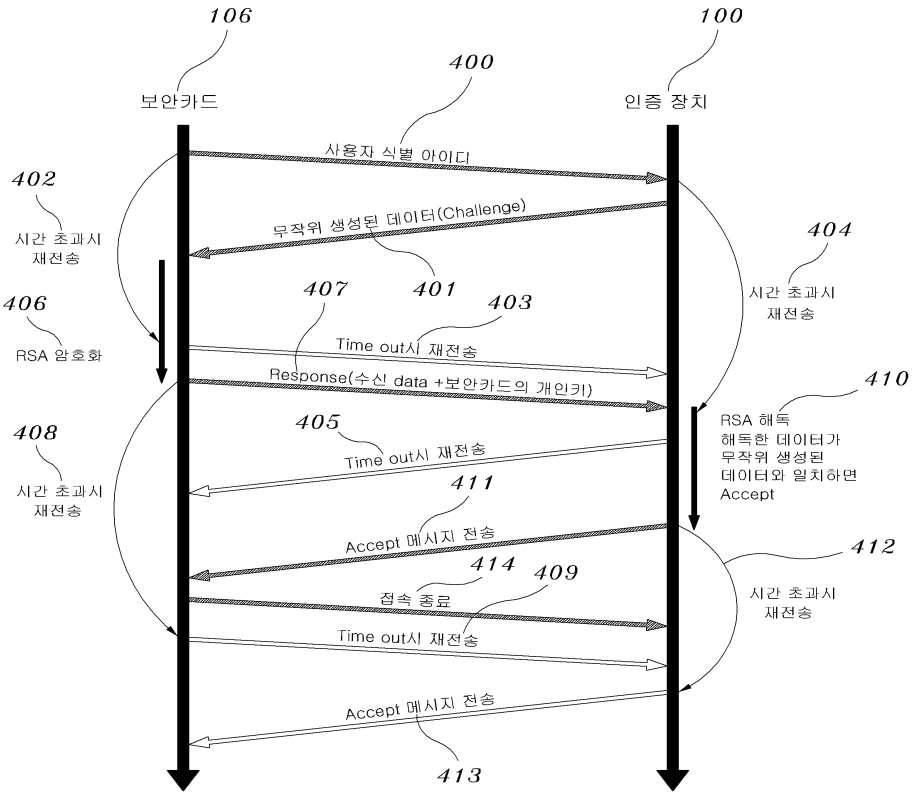
도면3


106
200
201
202
203
205
RFID
LF
송수
신기
전원
관리
모듈
중앙
처리 장치
지그비
통신 모듈
암호 프로세서
(RSA 알고리즘
가속기)
204

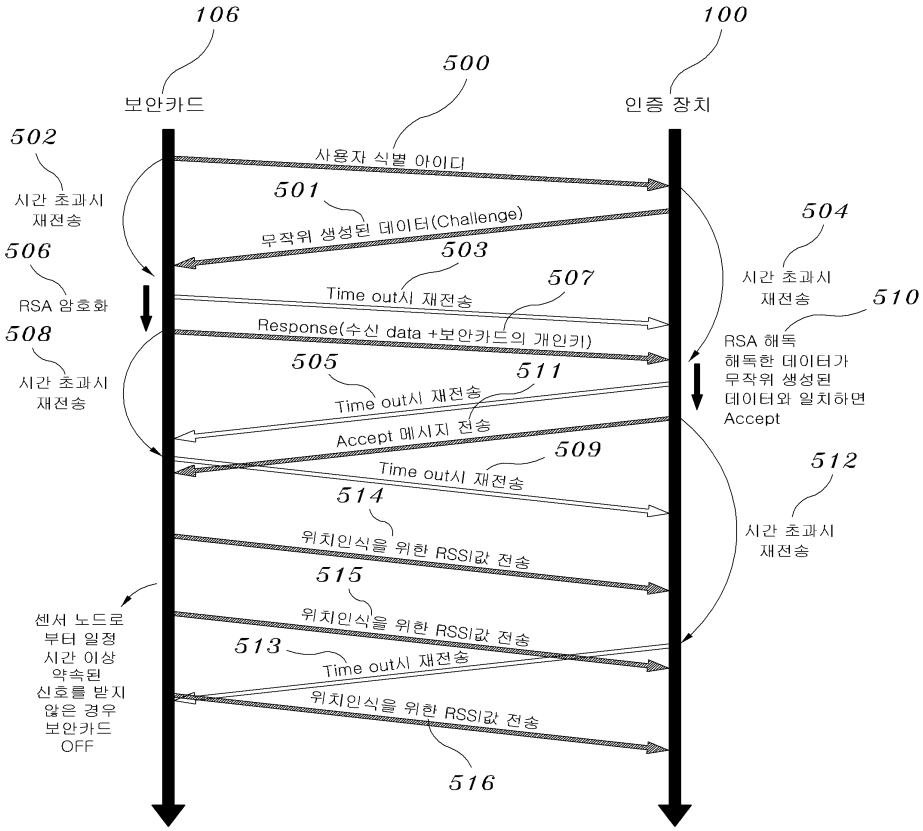
도면4


300
302
301
303
304
305
유휴 상태
상태 판단
인증 프로토콜 구동
인증 프로토콜 구동(LBS)
RSSI 데이터 전송
위치기반 서비스 종료구간

도면5


106
보안카드
100
인증 장치
400
사용자 식별 아이디
402
시간 초과시 재전송
무작위 생성된 데이터(Challenge)
401
404
시간 초과시 재전송
406
RSA 암호화
407
403
Time out시 재전송
Response(수신 data +보안카드의 개인키)
410
RSA 해독
해독한 데이터가 무작위 생성된 데이터와 일치하면 Accept
408
시간 초과시 재전송
405
Time out시 재전송
411
Accept 메시지 전송
412
414
409
접속 종료
시간 초과시 재전송
Time out시 재전송
Accept 메시지 전송
413

도면6


106
보안카드
500
100
인증 장치
502
시간 초과시
재전송
사용자 식별 아이디
501
무작위 생성된 데이터(Challenge)
504
시간 초과시
재전송
506
RSA 암호화
503
Time out시 재전송
507
510
Response(수신 data +보안카드의 개인키)
RSA 해독
해독한 데이터가
무작위 생성된
데이터와 일치하면
Accept
508
시간 초과시
재전송
505
Time out시 재전송
511
Accept 메시지 전송
509
Time out시 재전송
512
시간 초과시
재전송
514
위치인식을 위한 RSSI값 전송
515
위치인식을 위한 RSSI값 전송
513
Time out시 재전송
위치인식을 위한 RSSI값 전송
516
센서 노드로
부터 일정
시간 이상
약속된
신호를 받지
않은 경우
보안카드
OFF