(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(45) 공고일자 2007년06월15일
(11) 등록번호 10-0728637
(24) 등록일자 2007년06월08일

(21) 출원번호 10-2005-0083564
(22) 출원일자 2005년09월08일
심사청구일자 2005년09월08일

(65) 공개번호 10-2007-0028849
(43) 공개일자 2007년03월13일

(73) 특허권자 (주)한창시스템
경기도 안산시 단원구 신길동 1058-2

에스케이 텔레콤주식회사
서울 중구 을지로2가 11번지

(72) 발명자 천성록
경기 광명시 하안3동 110번지 고층주공아파트 1213동 1304호

전재식
서울 송파구 신천동 미성아파트 5동 408호

권오현
서울 강남구 대치동 316번지 은마아파트 20-1009

이주식
서울 강남구 대치동 미도아파트 206동 1006호

(74) 대리인 김성남

(56) 선행기술조사문헌
Near Field Communication Interface and Protocol-2, S2C Interface for NFC, PHILIPS (2005.01.21)
Standard ECMA-352 (2003.12.)

심사관 : 양종필

전체 청구항 수 : 총 26 항

(54) 플러그-인 형태로 여러 가지 보안 모듈들을 지원하는 보안ＮＦＣ 통신 장치 및 방법

(57) 요약

본 발명은 플러그-인 형태로 여러 가지 보안 모듈들을 지원하는 보안 NFC 통신 장치 및 방법에 관한 것으로서, 상기 보안 NFC 통신 장치에서는, 프로토콜 매칭부가 플러그-인 형태로 삽입되는 보안 모듈의 칩 종류를 확인하여 칩 확인 신호를 생성하고, 상기 칩 확인 신호에 따라 NFC 통신부에서 입출력되는 S2C 프로토콜에 따른 신호들을 상기 보안 모듈로 입출력되는 신호들의 프로토콜과 매칭시킨다.

대표도

도 2

특허청구의 범위

청구항 1.

보안 모듈이 삽입되는 플러그-인 소켓;

S2C 프로토콜에 따른 신호들을 이용하여 비접촉식의 근거리 통신 방식으로 외부와 통신하는 NFC 통신부; 및

상기 삽입되는 보안 모듈의 칩 종류를 확인하여 칩 확인 신호를 생성하고, 상기 칩 확인 신호에 따라 상기NFC 통신부에서 입출력되는 상기 S2C 프로토콜에 따른 신호들을 상기 보안 모듈로 입출력되는 신호들의 프로토콜과 매칭시키는 프로토콜 매칭부

를 포함하는 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 2.

제1항에 있어서, 상기 보안 모듈은,

ISO 프로토콜에 따른 칩 또는 상기S2C 프로토콜에 따른 칩 중 어느 하나를 가지는 모듈인 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 3.

제2항에 있어서, 상기 ISO 프로토콜에 따른 칩은 비접촉식 스마트카드의 칩인 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 4.

제1항에 있어서, 상기 플러그-인 소켓은 접촉식 스마트카드의 칩 규격에 대응되는 소켓인 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 5.

제1항에 있어서, 상기 보안 모듈은,

입력 신호에 응답하여 사용자 식별을 위한 사용자 ID, 또는 서비스를 이용하기 위한 충전 금액을 인증 정보로서 출력하는 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 6.

제1항에 있어서, 상기 보안 모듈은,

입력 신호에 응답하여 인증을 수행하고, 상기 인증의 성공 시에 상기 입력 신호에 포함된 개인 정보를 저장하는 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 7.

제6항에 있어서, 상기 보안 NFC 통신 장치는 이동 통신 단말기에 탑재되고, 상기 보안 모듈로의 입력 신호는 상기 보안 NFC 통신 장치를 탑재한 다른 이동 통신 단말기와의 상기 비접촉식의 근거리 통신 방식으로 수신되는 정보로부터 생성된 신호인 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 8.

제7항에 있어서, 상기 개인 정보는 상기 다른 이동 통신 단말기의 보안 모듈에서 관리되는 전자 명함, 사진, 동영상, 또는 전화 번호 리스트인 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 9.

제1항에 있어서, 상기 프로토콜 매칭부는,

상기 보안 모듈로 요청 신호를 전송하고, 이에 응답하여 수신되는 응답 신호에 따라 상기 칩 확인 신호를 생성하는 칩 확인부를 포함하는 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 10.

제9항에 있어서, 상기 칩 확인부는,

상기 보안 모듈이 상기S2C 프로토콜에 따른 칩을 가지는 모듈인지를 먼저 확인하여, 상기 보안 모듈이 상기S2C 프로토콜에 따른 칩을 가지는 모듈이 아니라면 상기 보안 모듈이 상기ISO 프로토콜에 따른 칩을 가지는 모듈인지를 확인하는 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 11.

제10항에 있어서, 상기 칩 확인부는,

상기 보안 모듈로 상기S2C 프로토콜에 따른 일정 요청 신호를 송신한 후 일정 시간 내에 상기S2C 프로토콜에 따른 일정 응답 신호가 수신되는 경우에 상기 보안 모듈이 상기 S2C 프로토콜에 따른 칩을 가지는 모듈을 나타내는 상기 칩 확인 신호를 생성하는 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 12.

제11항에 있어서, 상기 칩 확인부는,

상기S2C 프로토콜에 따른 일정 응답 신호가 수신되지 않으면, 상기 보안 모듈로 상기ISO 프로토콜에 따른 일정 요청 신호를 송신한 후 일정 시간 내에 상기ISO 프로토콜에 따른 일정 응답 신호가 수신되는 경우에 상기 보안 모듈이 상기 ISO 프로토콜에 따른 칩을 가지는 모듈을 나타내는 상기 칩 확인 신호를 생성하는 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 13.

제9항에 있어서, 상기 프로토콜 매칭부는,

상기NFC 통신부에서 입출력되는 상기 S2C 프로토콜에 따른 신호들을 상기 칩 확인 신호에 따라 선택적으로 상기 보안 모듈로 바이패스시키거나 변환 처리를 위한 신호들로서 출력하는 선택부; 및

상기 선택부에서 출력되는 상기 변환 처리를 위한 S2C 프로토콜에 따른 신호들과 상기 보안 모듈로 입출력되는 신호들 사이에서 서로 호환되도록 프로토콜 변환을 수행하는 프로토콜 변환부

를 더 포함하는 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 14.

제13항에 있어서, 상기 프로토콜 변환부는,

상기 S2C 프로토콜에 따른 밀러 코드화된 신호들과 ISO 프로토콜에 따른 맨체스터 코드화된 신호들 사이에서 서로 호환되도록 프로토콜 변환을 수행하는 신호 변환부; 및

상기 신호 변환부와 상기 보안 모듈 사이에서 상기 보안 모듈로 전달되는 아날로그 신호가 상기 신호 변환부로 전달되는 아날로그 신호보다 크도록 파형 정형하는 파형 정형부

를 포함하는 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 15.

제14항에 있어서, 상기 파형 정형부는,

상기 신호 변환부와 연결된 제1 단자와 제2 단자 사이에 연결된 제1 저항;

상기 신호 변환부와 연결된 제2 단자와 제1 노드 사이에 연결된 제1 커패시터;

상기 제1 노드와 접지 사이에 연결된 제2 저항;

상기 제1 노드와 상기 접지 사이에 연결된 제2 커패시터;

상기 제1 노드와 제2 노드 사이에 연결된 제1 다이오드;

상기 제2 노드와 상기 접지 사이에 연결된 제2 다이오드;

상기 보안 모듈에 연결된 제1 단자와 제2 단자 사이에 연결된 제3 커패시터;

상기 보안 모듈에 연결된 제1 단자와 상기 제2 노드 사이에 연결된 제4 커패시터; 및

상기 신호 변환부와 연결된 제3 단자와 상기 보안 모듈에 연결된 제1 단자 사이에 연결된 인덕터

를 포함하는 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 16.

제15항에 있어서, 상기 신호 변환부는,

상기 프로토콜 변환된 신호들을 상기 보안 모듈로 입출력시키는 경우에, 상기 보안 모듈에 연결된 제2 단자에 접지를 공급하는 것을 특징으로 하는 보안 NFC 통신 장치.

청구항 17.

플러그-인 형태로 소켓에 삽입된 보안 모듈을 이용하여 통신하는 방법에 있어서,

S2C 프로토콜에 따른 신호들을 이용하여 외부와 NFC통신하는 단계;

상기 보안 모듈의 칩 종류를 확인하여 칩 확인 신호를 생성하는 단계; 및

상기 칩 확인 신호에 따라 상기 S2C 프로토콜에 따른 신호들을 상기 보안 모듈로 입출력되는 신호들의 프로토콜과 매칭시키는 단계

를 포함하는 것을 특징으로 하는 보안 NFC 통신 방법.

청구항 18.

제17항에 있어서, 상기 보안 모듈은,

ISO 프로토콜에 따른 칩 또는 상기S2C 프로토콜에 따른 칩 중 어느 하나를 가지는 모듈인 것을 특징으로 하는 보안 NFC 통신 방법.

청구항 19.

제18항에 있어서, 상기 ISO 프로토콜에 따른 칩은 비접촉식 스마트카드의 칩인 것을 특징으로 하는 보안 NFC 통신 방법.

청구항 20.

제17항에 있어서, 상기 플러그-인 소켓은 접촉식 스마트카드의 칩 규격에 대응되는 소켓인 것을 특징으로 하는 보안 NFC 통신 방법.

청구항 21.

제17항에 있어서, 상기 NFC 통신은 인증을 위한 리더와 이루어지는 것을 특징으로 하는 보안 NFC 통신 방법.

청구항 22.

제17항에 있어서, 상기 NFC 통신은 개인 정보를 관리하는 이동 통신 단말기들 간에 이루어지는 것을 특징으로 하는 보안 NFC 통신 방법.

청구항 23.

제17항에 있어서,

상기 보안 모듈이 상기S2C 프로토콜에 따른 칩을 가지는 모듈인지를 먼저 확인하는 단계;

상기 보안 모듈이 상기S2C 프로토콜에 따른 칩을 가지는 모듈이라면 상기 S2C 프로토콜에 따른 신호들을 상기 보안 모듈로 바이패스시키는 단계;

상기 보안 모듈이 상기 ISO 프로토콜에 따른 칩을 가지는 모듈인지를 확인하는 단계; 및

상기 보안 모듈이 상기 ISO 프로토콜에 따른 칩을 가지는 모듈이라면 상기 S2C 프로토콜에 따른 신호들과 상기 보안 모듈로 입출력되는 신호들 사이에서 프로토콜 변환하는 단계

를 더 포함하는 것을 특징으로 하는 보안 NFC 통신 방법.

청구항 24.

제23항에 있어서,

상기 보안 모듈로 상기S2C 프로토콜에 따른 일정 요청 신호를 송신한 후 일정 시간 내에 상기S2C 프로토콜에 따른 일정 응답 신호가 수신되는 경우에 상기 보안 모듈이 상기 S2C 프로토콜에 따른 칩을 가지는 모듈을 가지는 것으로 확인하는 단계

를 더 포함하는 것을 특징으로 하는 보안 NFC 통신 방법.

청구항 25.

제24항에 있어서,

상기S2C 프로토콜에 따른 일정 응답 신호가 수신되지 않으면, 상기 보안 모듈로 상기ISO 프로토콜에 따른 일정 요청 신호를 송신한 후 일정 시간 내에 상기ISO 프로토콜에 따른 일정 응답 신호가 수신되는 경우에 상기 보안 모듈이 상기 ISO 프로토콜에 따른 칩을 가지는 모듈을 가지는 것으로 확인하는 단계

를 더 포함하는 것을 특징으로 하는 보안 NFC 통신 방법.

청구항 26.

제 17항 내지 제 25항 중 어느 한 항의 방법을 실행하기 위한 프로그램이 기록되어 있는 것을 특징으로 하는 컴퓨터에서 판독 가능한 기록매체.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 NFC(Near Field Communication: 근거리 무선 통신)에 관한 것으로, 더욱 상세하게는 S2C(SigIn-SigOut-Connection) 인터페이스에 따른 보안 모듈이나 접촉식/비접촉식 스마트카드 등과 같은 일반적인 보안 모듈들을 플러그-인 형태로 지원할 수 있는 NFC 통신 장치 및 방법에 관한 것이다.

도 1은 종래의 보안 NFC 통신 장치(100)의 블록도이다. 도 1을 참조하면, 상기 보안 NFC 통신 장치(100)는 NFC 통신부(110) 및 보안 모듈(120)을 포함한다.

상기 NFC 통신부는(110)는 이동 통신 단말기 등의 호스트 프로세서의 제어를 받을 수 있고, 상기 보안 모듈(120)과 S2C 인터페이스에 따른 신호들(SigIn, SigOut)을 통하여 통신한다. 상기 보안 모듈(120)은 SIM(Subscriber Identity Module)과 같은 것으로서, 사용자 식별을 위한 인증 정보를 저장할 수 있다. 상기 S2C 인터페이스는 상기 NFC 통신부(110)와 상기 보안 모듈(120) 간의 통신을 위하여 필립스(Philips)에서 개발되었다.

상기 보안 NFC 통신 장치(100)는 휴대 단말기, 예를 들어, 이동 통신 단말기 등에 탑재될 수 있다. 상기 보안 NFC 통신 장치(100)는 교통 카드, 스마트카드 등의 기능을 수행할 수 있다.

예를 들어, 보안 게이트를 통과하려는 사용자는 상기 보안 게이트에 설치된 출입자 인증을 위한 본체에 상기 보안 NFC 통신 장치(100)가 탑재된 휴대 단말기를 가까이 접근시킴으로써, 상기 보안 NFC 통신 장치(100)의 안테나(111)을 통하여 인증 정보를 상기 출입자 인증을 위한 본체에 전송할 수 있다. 이에 따라, 상기 출입자 인증을 위한 본체가 인증에 성공하면, 사용자는 보안 게이트를 통과할 수 있다.

또한, 충전 금액을 인증하는 일정 리더(reader)에 상기 보안 NFC 통신 장치(100)가 탑재된 휴대 단말기를 가까이 접근시킴으로써, 리더의 인증 성공에 따라 사용자로 하여금 교통 수단을 이용하게 하거나 쇼핑 결제 등을 할 수 있도록 할 수 있다.

아직까지 상기 종래의 보안 NFC 통신 장치(100)에서는 상기 NFC 통신부(110)와 S2C 인터페이스에 따라 통신하는 보안 모듈(120) 만을 지원한다. 이에 따라 상기 보안 모듈(120)로서ISO 7816 프로토콜에 따른 접촉식 또는 ISO 14443프로토콜에 따른 비접촉식 스마트카드 등과 같은 다른 보안 인증 모듈을 사용하는 경우에, 상기 NFC 통신부(110)와의 인터페이스 규격이 맞지 않아 사용되는 보안 인증 모듈들에 대한 데이터(예를 들어, 인증 정보 등) 호환성이 없으므로 사용자에게 데이터 관리의 불편을 주는 문제점이 있다.

또한, 상기 NFC 통신부(110)에 의하여 외부로부터 인증 정보 등 일정 데이터를 수신하여 상기 보안 모듈(120)에서 관리되도록 하려는 시도가 있으나 매우 미흡한 실정이고, 더욱이 이동 통신 단말기들 간(peer-to-peer) 데이터 송수신을 지원하지 못하므로, 이동 통신 단말기에서 관리되는 전자 명함과 같은 개인 정보의 관리가 어려운 문제점이 있다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명은 상술한 문제점을 해결하기 위한 것으로서, 본 발명의 목적은, NFC 통신의 S2C 프로토콜뿐만 아니라 일반적인 접촉식/비접촉식 스마트카드 등의 ISO 프로토콜에 따른 보안 인증 모듈들이 플러그-인(plug-in) 형태로 소켓에 삽입되어 NFC 통신에서 호환될 수 있도록 하기 위하여, S2C 프로토콜을 따르지 않는 보안 인증 모듈에 대해서는 프로토콜 변환을 수행하는 보안 NFC 통신 장치를 제공하는 데 있다.

본 발명의 다른 목적은, 플러그-인 형태로 소켓에 삽입되는 보안 인증 모듈들을 지원하기 위하여, 보안 인증 모듈의 종류를 확인하고, 그에 따라 S2C 프로토콜을 따르지 않는 보안 인증 모듈에 대해서는 프로토콜 변환을 수행하는 보안 NFC 통신 방법을 제공하는 데 있다.

발명의 구성

상기와 같은 본 발명의 목적을 달성하기 위한 본 발명에 따른 보안 NFC 통신 장치는, 보안 모듈이 삽입되는 플러그-인 소켓; S2C 프로토콜에 따른 신호들을 이용하여 비접촉식의 근거리 통신 방식으로 외부와 통신하는 NFC 통신부; 및 상기 삽입되는 보안 모듈의 칩 종류를 확인하여 칩 확인 신호를 생성하고, 상기 칩 확인 신호에 따라 상기NFC 통신부에서 입출력되는 상기 S2C 프로토콜에 따른 신호들을 상기 보안 모듈로 입출력되는 신호들의 프로토콜과 매칭시키는 프로토콜 매칭부를 포함한다.

상기 프로토콜 매칭부는, 상기 보안 모듈로 요청 신호를 전송하고, 이에 응답하여 수신되는 응답 신호에 따라 상기 칩 확인 신호를 생성하는 칩 확인부; 상기NFC 통신부에서 입출력되는 상기 S2C 프로토콜에 따른 신호들을 상기 칩 확인 신호에 따라 선택적으로 상기 보안 모듈로 바이패스시키거나 변환 처리를 위한 신호들로서 출력하는 선택부; 및 상기 선택부에서 출력되는 상기 변환 처리를 위한 S2C 프로토콜에 따른 신호들과 상기 보안 모듈로 입출력되는 신호들 사이에서 서로 호환되도록 프로토콜 변환을 수행하는 프로토콜 변환부를 포함한다.

상기와 같은 본 발명의 다른 목적을 달성하기 위한 본 발명에 따른 보안 NFC 통신 방법은, 플러그-인 형태로 소켓에 삽입된 보안 모듈을 이용하여 통신하는 방법에 있어서, S2C 프로토콜에 따른 신호들을 이용하여 외부와 NFC통신하는 단계; 상기 보안 모듈의 칩 종류를 확인하여 칩 확인 신호를 생성하는 단계; 및 상기 칩 확인 신호에 따라 상기 S2C 프로토콜에 따른 신호들을 상기 보안 모듈로 입출력되는 신호들의 프로토콜과 매칭시키는 단계를 포함한다.

상기 보안 NFC 통신 방법은, 상기 보안 모듈이 상기S2C 프로토콜에 따른 칩을 가지는 모듈인지를 먼저 확인하는 단계; 상기 보안 모듈이 상기S2C 프로토콜에 따른 칩을 가지는 모듈이라면 상기 S2C 프로토콜에 따른 신호들을 상기 보안 모듈로 바이패스시키는 단계; 상기 보안 모듈이 상기 ISO 프로토콜에 따른 칩을 가지는 모듈인지를 확인하는 단계; 및 상기 보안 모듈이 상기 ISO 프로토콜에 따른 칩을 가지는 모듈이라면 상기 S2C 프로토콜에 따른 신호들과 상기 보안 모듈로 입출력되는 신호들 사이에서 프로토콜 변환하는 단계를 더 포함한다.

이하 첨부 도면들 및 첨부 도면들에 기재된 내용들을 참조하여 본 발명의 바람직한 실시예를 상세하게 설명하지만, 본 발명이 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조부호는 동일한 부재를 나타낸다.

도 2는 본 발명의 일실시예에 따른 보안 NFC 통신 장치(200)의 블록도이다. 도 2를 참조하면, 상기 NFC 통신 장치(200)는 NFC 통신부(210), 프로토콜 매칭부(220), 보안 모듈(230) 및 상기 보안 모듈(230)을 삽입하기 위한 플러그-인(plug-in) 소켓(240)을 포함한다.

상기 보안 NFC 통신 장치(200)는 휴대 단말기, 예를 들어, 이동 통신 단말기 등에 탑재될 수 있다. 상기 보안 NFC 통신 장치(200)는 도 9와 같이, 리더(reader)와의 통신으로 교통 카드, 스마트카드 등의 기능을 수행할 수 있다. 또한, 본 발명에서는 도 10과 같이, 상기 보안 NFC 통신 장치(200)를 탑재한 피어들, 즉, 이동 통신 단말기들 간에 개인 정보를 주고 받도록 제안되었다.

특히, 종래의 보안 NFC 통신 프로세서가 S2C 인터페이스에 따라 통신하는 특정 보안 인증 모듈과의 통신 만을 지원한 것과는 달리, 본 발명에서는 상기 보안 모듈(230)로서 NFC 통신의 S2C 프로토콜뿐만 아니라 일반적인 ISO 7816 프로토콜에 따른 접촉식 또는 ISO 14443프로토콜에 따른 비접촉식 스마트카드 등의 ISO 프로토콜에 따른 보안 인증 칩을 가지는 모듈들이 플러그-인(plug-in) 형태로 상기 소켓(240)에 삽입되어 NFC 통신에서 호환될 수 있도록 하기 위하여, 상기 프로토콜 매칭부(220)가 S2C 프로토콜을 따르지 않는 보안 인증 모듈에 대해서는 프로토콜 변환을 수행한다.

상기 NFC 통신부(210)는 S2C 프로토콜에 따른 신호들(SigIn, SigOut)을 이용하여 외부의 리더나 상대방 단말기 내의 NFC 통신 장치와 비접촉식의 근거리 통신을 인터페이스하는 NFC 통신 프로세서이다. 상기 NFC 통신부(210)는 상기 보안 NFC 통신 장치(200)를 탑재한 이동 통신 단말기 등의 호스트 프로세서의 제어를 받아 동작할 수 있다.

상기 NFC 통신부(210)는 S2C 프로토콜에 따른 기저 대역의 제1 신호(SigIn)를 상기 프로토콜 매칭부(220)로부터 받아 처리하여, 상기 제1 신호(SigIn)에 대응되는 RF(Radio Frequency) 형태의 정보를 생성한다. 상기 NFC 통신부(210)는 상기 생성한 정보를 비접촉식의 근거리 통신 방식, 즉 NFC 방식으로 안테나(211)를 통하여 리더 또는 상대방 단말기로 송신한다.

상기 NFC 통신부(210)는 안테나(211)를 통하여 상기 NFC 방식으로 리더 또는 상대방 단말기로부터 일정 RF 정보를 수신할 수 있다. 상기 NFC 통신부(210)는 상기 수신된 RF 정보를 처리하여 S2C 프로토콜에 따른 기저 대역의 제2 신호(SigOut)를 생성하여 상기 프로토콜 매칭부(220)로 송신할 수 있다.

상기 프로토콜 매칭부(220)는 상기 보안 모듈(230)의 칩 종류를 나타내는 칩 확인 신호(CIS)에 따라 상기 NFC 통신부(210)와 상기 보안 모듈(230) 사이에서 상호간에 입출력되는 신호의 프로토콜을 매칭시킨다. 예를 들어, 상기 칩 확인 신호(CIS)에 따라 상기 보안 모듈(230)의 칩이 상기 S2C 프로토콜에 따른 칩을 나타내는 경우에는, 상기 프로토콜 매칭부(220)는 상기NFC 통신부(210)의 두 입출력 단자들과 상기 보안 모듈(230)의 두 입출력 단자들을 서로 연결시켜, 상기 NFC 통신부(210)에서 입출력되는 상기 S2C 프로토콜에 따른 신호들(SigIn, SigOut)을 상기 보안 모듈(230)로 바이패스

(bypass)시키고, 상기 보안 모듈(230)에서 입출력되는 신호들을 상기NFC 통신부(210)로 바이패스시킨다. 또한, 상기 칩 확인 신호(CIS)에 따라 상기 보안 모듈(230)의 칩이 ISO 14443프로토콜에 따른 비접촉식 스마트카드의 보안 인증 칩 등을 나타내는 경우에는, 상기 프로토콜 매칭부(220)는 상기NFC 통신부(210)와 상기 보안 모듈(230) 사이에서, 상기NFC 통신부(210)에서 입출력되는 상기 S2C 프로토콜에 따른 신호들(SigIn, SigOut)을 상기 보안 모듈(230)로 입출력되는 ISO 프로토콜에 따른 신호들(LA-LB)로 변환하고, 상기 보안 모듈(230)에서 입출력되는 ISO 프로토콜에 따른 신호들(LA-LB)을 상기NFC 통신부(210)로 입출력되는 ISO 프로토콜에 따른 신호들(SigIn, SigOut)로 변환한다. 상기 칩 확인 신호(CIS)의 생성에 대해서는 아래에서 자세히 설명된다.

상기 보안 모듈(230)은 플러그-인 형태로 소켓(240)에 삽입되고, NFC 통신의 S2C 프로토콜을 따르는 보안 인증 칩, 또는 일반적인 ISO 7816 프로토콜에 따른 접촉식 또는 ISO 14443프로토콜에 따른 비접촉식 스마트카드 코아 칩 등과 같은 다양한 인증 칩을 가지는 모듈일 수 있다. 특히, 상기 보안 모듈(230)이 ISO 14443프로토콜에 따른 비접촉식 스마트카드 코아 칩을 가지는 경우에, 그 칩에 입출력되는 신호들(LA-LB)에 따라 동작하여, 내부에 저장된 인증 정보 등을 (LA-LB) 단자로 출력할 수 있다. 상기 플러그-인 소켓(240)에 삽입되는 상기 보안 모듈(230)의 칩 외형은 도 3과 같이, ISO 7816 프로토콜에 따른 접촉식 스마트카드 코아 칩을 가지는 모듈을 따를 수 있고, 이때 칩의 내부 회로와 연결된8개의 외부 핀(pin)들을 가질 수 있다. 이에 따라, 상기 보안 모듈(230)이 삽입되는 소켓(240)으로서 ISO 7816 프로토콜에 따른 접촉식 스마트카드의 칩 규격에 대응되는 플러그-인 소켓이 이용된다.

일반적으로 ISO 7816 프로토콜에 따른 접촉식 스마트카드 코아 칩에서는, 1, 2, 3, 5, 7번이 이용되고 있고, 본 발명에서는 4 및 8번을 상기 보안 모듈(230)로서 삽입될 수 있는 NFC 통신의 S2C 프로토콜을 따르는 보안 인증 칩의 입출력 신호(SigIn, SigOut) 핀들, 또는 일반적인 ISO 14443프로토콜에 따른 비접촉식 스마트카드 코아 칩의 입출력 신호(LA-LB) 핀들로서 이용한다. 또한, 6번 핀은 비접촉식 칩인지를 검출할 수 있도록 하는 비접촉 알림 검출 신호(CLAD: Contactless Appearance Detection) 핀으로 이용될 수 있다.

도 4는 도 2의 보안 모듈(230)의 구체적인 구성을 나타내는 일례이다. 도 4를 참조하면, 상기 보안 모듈(230)은 CPU(Central Processing Unit: 중앙 처리부)(231), ROM(Read Only Memory)(232), RAM(Random Access Memory)(233) 및 EEPROM(Electrically Erasable ROM)(234)를 포함할 수 있다. 상기 CPU(231)는 상기 보안 모듈(230)의 전반적인 제어를 담당한다. 상기 ROM(232)은 상기 보안 모듈(230)의 동작을 위한 전반적인 시스템 프로그램을 저장하고, 상기 RAM(233)은 내부 데이터의 연산 시 필요한 임시 데이터를 저장한다. 상기 EEPROM(234)은 외부의 카드 리더나 다른 단말기와 송수신하기 위한 인증 정보 등을 저장한다.

도 2에서, 상기 프로토콜 매칭부(220)는 선택부(221), 칩 확인부(222), 및 프로토콜 변환부(223)를 포함한다.

상기 칩 확인부(222)는 상기 보안 모듈(230)로 요청 신호를 전송하고, 이에 응답하여 수신되는 응답 신호에 따라 상기 칩 확인 신호(CIS)를 생성한다. 상기 칩 확인 신호(CIS)에 따라 상기 보안 모듈(230)이 상기 S2C 프로토콜에 따른 칩을 가지는 모듈을 나타낼 때에는, 상기 선택부(221)는 상기NFC 통신부(210)에서 입출력되는 상기 S2C 프로토콜에 따른 신호들(SigIn, SigOut)을 상기 보안 모듈(230)로 바이패스시킨다. 상기 칩 확인 신호(CIS)에 따라 상기 보안 모듈(230)이 상기 ISO 프로토콜에 따른 칩을 가지는 모듈을 나타낼 때에는, 상기 선택부(221)는 상기NFC 통신부(210)에서 입출력되는 상기 S2C 프로토콜에 따른 신호들(SigIn, SigOut)을 상기 프로토콜 변환부(223)에 프로토콜 변환 처리를 위한 신호들로서 출력한다. 이에 따라, 상기 프로토콜 변환부(223)는 상기 칩 확인 신호(CIS)에 따라 상기 보안 모듈(230)이 상기 ISO 프로토콜에 따른 칩을 가지는 모듈을 나타낼 때, 상기 선택부(221)에서 출력되는 상기 변환 처리를 위한 S2C 프로토콜에 따른 신호들(SigIn, SigOut)과 상기 보안 모듈(230)로 입출력되는 신호들(LA-LB) 사이에서 서로 호환되도록 프로토콜 변환을 수행한다.

상기 프로토콜 변환부(223)가 프로토콜 변환 처리를 할 때, 도 2의 상기 프로토콜 변환부(223)와 상기 보안 모듈(230)로서 삽입된 상기 ISO 프로토콜에 따른 칩의 관계를 나타내는 구체적인 블록도가 도 5에 도시되어 있다. 도 5를 참조하면, 상기 프로토콜 변환부(223)는 신호 변환부(223-1) 및 파형 정형부(223-2)를 포함한다.

상기 신호 변환부(223-1)는 상기 S2C 프로토콜에 따른 밀러(Miller) 코드화된 신호들과 ISO 프로토콜에 따른 맨체스터(Manchester) 코드화된 신호들 사이에서 서로 호환되도록 프로토콜 변환을 수행한다.

예를 들어, 상기NFC 통신부(210)로부터의 상기 S2C 프로토콜에 따른 신호(SigOut)는 도 6의 아래 그림과 같이 밀러(Miller) 방식에 따라 코드화된 디지털 형태이고, 상기 신호 변환부(223-1)로부터 생성되어 상기 파형 정형부(223-2)로 출력되는 아날로그 신호(LAA-LBB)는 도 6의 위 그림과 같이 맨체스터(Manchester) 방식에 따라 변조되어 코드화된 신호 형태를 가진다. 도 6에서와 같이, 상기 신호 변환부(223-1)에서는 상기 밀러 방식에 따른 신호(SigOut)가 그 논리 상태

에 따라 일정 주파수의 피크-피크(peak-to-peak) 레벨을 가지는 아날로그 신호로 변환된다. 즉, 논리 하이(high) 상태의 디지털 신호는 큰 피크-피크 레벨을 가지는 아날로그 신호로 변환하고, 논리 로우(low) 상태의 디지털 신호는 작은 피크-피크 레벨을 가지는 아날로그 신호로 변환한다. 밀러 방식에 따른 디지털 코드는 도 6과 같이, 일정 주기 동안 중 초기 부분에 논리 로우 상태를 가지는 신호를 데이터 '0'으로 보고, 일정 주기 동안 중 중간 부분에 논리 로우 상태를 가지는 신호를 데이터 '1'로보는 코드화 방식을 가진다. 맨체스터 방식에 따른 신호는 도 6과 같이, 밀러 방식의 디지털 값을 서브 캐리어(subcarrier) 형태로 변조한 코드화 방식을 가진다.

상기 파형 정형부(223-2)는 상기 신호 변환부(223-1)와 상기 보안 모듈(230) 사이에서 상기 보안 모듈(230)로 전달되는 아날로그 신호(LA-LB)가 상기 신호 변환부(223-1)로 전달되는 아날로그 신호(LAA-LBB)보다 크도록 파형 정형한다.

마찬가지로, 상기 보안 모듈(230)로부터 출력되는 아날로그 신호(LA-LB)는 도 7의 아래 그림과 같이 맨체스터(Manchester) 방식에 따라 변조되어 코드화된 신호 형태를 가지고, 상기 아날로그 신호(LA-LB)는 상기 파형 정형부(223-2)에서 (LAA-LBB)로 파형 정형된 후, 상기 신호 변환부(223-1)에서 상기 S2C 프로토콜에 따라 밀러 방식으로 코드화된 신호(SigIn)로 변환된다.

도 5에서, 상기 파형 정형부(223-2)는 제1 저항(R1), 제2 저항(R2), 제1 다이오드(diode)(D1), 제2 다이오드(D2), 제1 커패시터(C1), 제2 커패시터(C2), 제3 커패시터(C3), 제4 커패시터(C4) 및 인덕터(inductor)(L1)를 포함한다. 도 5의 상기 파형 정형부(223-2)를 나타내는 회로는 단지 일례일 뿐, 파형 정형을 위한 여러 가지 다양한 회로가 이용될 수 있다. 상기 제1 저항(R1)은 상기 신호 변환부(223-1)와 연결된 제1 단자(LS)와 제2 단자(LAA) 사이에 연결된다. 상기 제1 커패시터(C1)는 상기 신호 변환부(223-1)와 연결된 제2 단자(LAA)와 제1 노드(ND1) 사이에 연결된다. 상기 제2 저항(R2)은 상기 제1 노드(ND1)와 접지(GND) 사이에 연결된다. 상기 제2 커패시터(C2)는 상기 제1 노드(ND1)와 상기 접지(GND) 사이에 연결된다. 상기 제1 다이오드(D1)는 상기 제1 노드(ND1)와 제2 노드(ND2) 사이에 연결된다. 상기 제2 다이오드(D2)는 상기 제2 노드(ND2)와 상기 접지(GND) 사이에 연결된다. 상기 제3 커패시터(C3)는 상기 보안 모듈(230)에 연결된 제1 단자(LA)와 제2 단자(LB) 사이에 연결된다. 상기 제4 커패시터(C4)는 상기 보안 모듈(230)에 연결된 제1 단자(LA)와 상기 제2 노드(ND2) 사이에 연결된다. 상기 인덕터(L1)는 상기 신호 변환부(223-1)와 연결된 제3 단자(LBB)와 상기 보안 모듈(230)에 연결된 제1 단자(LA) 사이에 연결된다.

이때, 상기 프로토콜 변환된 신호들을 상기 보안 모듈(230)로 입출력시키는 경우에, 상기 파형 정형부(223-2)의 동작을 위하여, 상기 신호 변환부(223-1)는 스위치(SW)를 턴온(turn-on)시켜 상기 보안 모듈(230)에 연결된 제2 단자(LB)에 접지(GND)를 공급한다.

따라서, 상기 파형 정형부(223-2)의 상기 제1 다이오드(D1) 및 상기 제2 다이오드(D2)의 일반적인 다이오드 동작과 R-C 필터(R2, C2) 형태의 회로 동작에 의하여, 상기 보안 모듈(230)과 연결된 단자들의 신호(LA-LB)는, 상기 파형 정형부(223-2)에서 작아지면서 상기 신호 변환부(223-1)로 출력되고, 상기 신호 변환부(223-1)로부터의 신호(LAA-LBB)는 상기 파형 정형부(223-2)에서 커지면서 상기 보안 모듈(230)로 출력된다. 예를 들어, 상기 신호 변환부(223-1)로 전달되는 신호(LAA-LBB)는 3V(Volt) 정도의 피크-피크(peak-to-peak)를 가지고, 상기 보안 모듈(230)로 전달되는 신호(LA-LB)는 12~13V 정도의 피크-피크를 가진다.

이하, 도 8의 흐름도를 참조하여 상기 프로토콜 매칭부(220)의 동작을 좀더 자세히 설명한다.

먼저, 상기 프로토콜 매칭부(220)에 파워가 공급되면, 일정 전압이 상기 보안 모듈(230)로 전달되어 상기 보안 모듈(230)도 동작 상태로 된다(도 8의 S810). 이와 같은 초기 상태에서, 상기 칩 확인부(222)는 상기 보안 모듈(230)이 상기S2C 프로토콜에 따른 칩을 가지는 것으로 먼저 가정하고, 상기 보안 모듈(230)의 SigOut(또는 LA) 단자로 상기S2C 프로토콜에 따른 일정 요청 신호(REQA: Request A)(예를 들어, 16진수에서 0x26)를 송신한다(도 8의 S820). 상기 보안 모듈(230)로 일정 요청 신호(REQA)가 송신된 후, 상기 칩 확인부(222)는 일정 시간(예를 들어, 5msec) 내에 상기 보안 모듈(230)의 SigIn 단자(또는 LB 단자)로부터 상기S2C 프로토콜에 따른 일정 응답 신호(ATQA: Answer to Request A)(예를 들어, 16진수에서 0403)가 수신되는 지를 판단한다(도 8의 S830). 상기 일정 응답 신호(ATQA)가 수신되면, 상기 칩 확인부(222)는 상기 보안 모듈(230)이 상기 S2C 프로토콜에 따른 칩을 가지는 모듈을 나타내는 상기 칩 확인 신호(CIS)를 생성한다. 이때, 상기 칩 확인 신호(CIS)는 논리 로우 상태로 출력될 수 있다. 상기 칩 확인 신호(CIS) 가 논리 로우 상태로 출력되는 경우에, 상기 선택부(221)는 상기 NFC 통신부(210)와 상기 보안 모듈(230)로서 삽입된 상기 S2C 프로토콜에 따른 칩을 직접 연결시켜, 상기NFC 통신부(210)에서 입출력되는 상기 S2C 프로토콜에 따른 신호들(SigIn, SigOut)을 상기 보안 모듈(230)로 바이패스시킨다(도 8의 S840).

반면, S830 단계에서, 상기S2C 프로토콜에 따른 일정 응답 신호가 수신되지 않으면, 상기 칩 확인부(222)는 상기 보안 모듈(230)이 상기ISO 프로토콜에 따른 칩을 가지는 것으로 가정하고, 상기 보안 모듈(230)의 (LA-LB) 단자(또는, SigIn, SigOut 단자)로 상기ISO 프로토콜에 따른 일정 요청 신호(REQA)(예를 들어, 16진수에서 0x26)를 송신한다(도 8의 S850). 이때, 상기 보안 모듈(230)로 일정 요청 신호(REQA)가 송신된 후, 상기 칩 확인부(222)는 일정 시간(예를 들어, 5msec) 내에 상기 보안 모듈(230)의 (LA-LB) 단자(또는, SigIn, SigOut 단자)로부터 상기ISO 프로토콜에 따른 일정 응답 신호(ATQA)(예를 들어, 16진수에서 0403)가 수신되는 지를 판단한다(도 8의 S860). 상기 일정 응답 신호(ATQA)가 수신되면, 상기 칩 확인부(222)는 상기 보안 모듈(230)이 상기 ISO 프로토콜에 따른 칩을 가지는 모듈을 나타내는 상기 칩 확인 신호(CIS)를 생성한다. 이때, 상기 칩 확인 신호(CIS)는 논리 하이 상태로 출력될 수 있다. 상기 칩 확인 신호(CIS) 가 논리 하이 상태로 출력되는 경우에, 상기 NFC 통신부(210)와 상기 보안 모듈(230)로서 삽입된 상기 ISO 프로토콜에 따른 칩 사이에서, 상기NFC 통신부(210)에서 입출력되는 상기 S2C 프로토콜에 따른 신호들(SigIn, SigOut)과 상기 보안 모듈(230)에서 입출력되는 상기 ISO 프로토콜에 따른 신호들(LA-LB)이 서로 호환되도록 하기 위한 프로토콜 변환을 위하여, 상기 선택부(221)는 상기 변환 처리를 위한 S2C 프로토콜에 따른 신호들(SigIn, SigOut)을 상기 프로토콜 변환부(223)로 출력시킨다. 이에 따라, 상기 프로토콜 변환부(223)는 상기 변환 처리를 위한 S2C 프로토콜에 따른 신호들(SigIn, SigOut)과 상기 보안 모듈(230)로 입출력되는 신호들(LA-LB) 사이에서 서로 호환되도록 프로토콜 변환을 수행한다(도 8의 S870).

위와 같이, 칩 확인부(222)는 상기 보안 모듈(230)이 상기S2C 프로토콜에 따른 칩을 가지는 모듈인지를 먼저 확인한다. 상기 보안 모듈(230)의 (SigIn, SigOut) 또는 (LA, LB) 단자를 통하여 상기S2C 프로토콜에 따른 일정 요청 신호(REQA)를 전송하고 일정 응답 신호(ATQA)를 수신할 때에는 밀러 방식에 따른 디지털의 3~5V 피크-피크를 가지지만, 상기 보안 모듈(230)로 상기 ISO 프로토콜에 따른 일정 요청 신호(REQA)를 전송하고 일정 응답 신호(ATQA)를 수신할 때에는 맨체스터 방식에 따른 아날로그의 12~13V 피크-피크를 가지기 때문이다. 이와 같이, 상기 보안 모듈(230)이 저전압, 즉, S2C 프로토콜에 따라 동작하는 지를 먼저 확인함으로써, 상기 보안 모듈(230)에 고전압인가로 인한 회로의 손상을 방지할 수 있다.

한편, 본 발명에 따른 도 2와 같은 상기 보안 NFC 통신 장치(200)는 도 9와 같이, 이동통신 단말기에 탑재되어 리더(reader)와 통신할 수 있다.

예를 들어, 보안 게이트를 통과하려는 사용자는 상기 보안 게이트에 설치된 출입자 인증을 위한 본체, 즉, 상기 리더에 상기 보안 NFC 통신 장치(200)가 탑재된 이동 통신 단말기를 가까이 접근시킴으로써, 상기 보안 NFC 통신 장치(200)의 안테나(211)을 통하여 인증 정보를 상기 출입자 인증을 위한 리더에 전송할 수 있다. 즉, 상기 보안 NFC 통신 장치(200)의 안테나(211)를 통하여 리더에서 인증을 위하여 요청되는 정보가 수신되면, 상기 수신된 신호를 기반으로 한 정보가 상기 NFC 통신부(210) 및 상기 프로토콜 매칭부(220)를 통하여 상기 보안 모듈(230)로 전달될 수 있다. 이때, 상기 보안 모듈(230)은 CPU(231)의 제어에 따라 EEPROM(234)에 저장된 인증 정보, 예를 들어, 사용자 식별을 위한 사용자 ID(Identification)를 추출하고, 상기 추출된 인증 정보는 상기 프로토콜 매칭부(220) 및 상기 NFC 통신부(210)를 통하여 상기 리더로 전송될 수 있다. 이에 따라, 상기 리더에서 해당 인증에 성공하면, 사용자는 보안 게이트를 통과할 수 있다.

또한, 교통 수단을 이용하거나 쇼핑 결제 등을 위한 일정 리더가 사용되는 경우에, 위와 같은 방법으로 상기 보안 NFC 통신 장치(200)가 탑재된 이동 통신 단말기를 그 리더에 가까이 접근시킴으로써, 리더의 충전 금액 등에 대한 인증 성공에 따라 사용자로 하여금 해당 결제 등을 할 수 있게 할 수 있다.

또한, 본 발명에 따른 도 2와 같은 상기 보안 NFC 통신 장치(200)는 도 10과 같이, 서로 다른 이동통신 단말기들에 탑재되어 단말기들 상호 간(peer-to-peer) 에 통신이 이루어질 수 있도록 할 수 있다.

예를 들어, 오늘날 대부분의 사용자는 이동통신 단말기에 전자 명함, 사진, 동영상, 또는 전화 번호 리스트 등을 저장하여 사용한다. 그러나, 단말기의 교체시 마다 이와 같은 개인 정보는 새로 입력되거나 다운로드 되어야만, 사용자는 새로운 교체 단말기에서 이전 단말기와 같이 위와 같은 개인 정보를 이용할 수 있다.

그러나, 본 발명에서는 이동통신 단말기에 탑재되는 상기 보안 NFC 통신 장치(200)의 보안 모듈(230)에서 위와 같은 개인 정보가 관리될 수 있다. 상기 보안 모듈(230)에 상기 개인 정보가 관리되는 경우에, 상기 이동통신 단말기들 간의 통신으로 상대방 단말기로의 개인 정보의 이동이 가능하다.

예를 들어, 상기 보안 NFC 통신 장치(200)가 탑재된 이동 통신 단말기들을 서로 가까이 접근시킴으로써, 개인 정보를 송신하려는 어느 하나의 단말기에서는 상기 보안 NFC 통신 장치(200)의 안테나(211)을 통하여 인증 정보와 함께 개인 정보

를 상대방 단말기로 전송할 수 있다. 상기 상대방 단말기는 상기 보안 NFC 통신 장치(200)의 안테나(211)를 통하여 상기 인증 정보와 개인 정보가 수신되면, 상기 수신된 신호들을 기반으로 한 정보가 상기 NFC 통신부(210) 및 상기 프로토콜 매칭부(220)를 통하여 상기 보안 모듈(230)로 전달될 수 있다. 이때, 상기 보안 모듈(230)은 CPU(231)의 제어에 따라 일정 인증을 수행할 수 있고, 상기 인증의 성공 시에 상기 수신된 신호들에 포함된 개인 정보를 EEPROM(234)에 저장하여 관리할 수 있다.

위에서 기술한 바와 같이, 본 발명에 따른 가치 보안 NFC 통신 장치(200)에서는, 프로토콜 매칭부(220)가 플러그-인 형태로 삽입되는 보안 모듈(230)의 칩 종류를 확인하여 칩 확인 신호(CIS)를 생성하고, 상기 칩 확인 신호(CIS)에 따라 NFC 통신부(210)에서 입출력되는 S2C 프로토콜에 따른 신호들(SigIn, SigOut)을 상기 보안 모듈(230)로 입출력되는 신호들(LA-LB)의 프로토콜과 매칭시킨다.

본 발명에 따른 보안 NFC 통신 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 매체는 프로그램 명령, 데이터 구조 등을 지정하는 신호를 전송하는 반송파를 포함하는 광 또는 금속선, 도파관 등의 전송 매체일 수도 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

발명의 효과

상술한 바와 같이 본 발명에 따른 보안 NFC 통신 장치에서는, NFC 통신의 S2C 프로토콜에 따른 신호를 선택적으로 다른 보안 인증 모듈의 프로토콜에 맞는 신호로 변환하므로, 플러그-인 형태로 소켓에 삽입되는 S2C 프로토콜에 따른 보안 인증 모듈뿐만 아니라 일반적인 접촉식/비접촉식 스마트카드 등과 같은 다양한 보안 인증 모듈들을 지원하여, 여러 형태의 보안 인증 모듈들에서 관리되는 사용자의 인증 정보가 용이하게 호환될 수 있는 효과가 있다.

또한, 이동 통신 단말기 등과 같은 포터블 장치들, 즉, 피어들 간 데이터 통신이 자유로우므로, 전자 명함, 사진, 동영상, 등록 전화 번호 등과 같은 개인 정보들이 용이하게 관리될 수 있는 효과가 있다.

도면의 간단한 설명

도 1은 종래의 보안 NFC 통신 장치의 블록도이다.

도 2는 본 발명의 일실시예에 따른 보안 NFC 통신 장치의 블록도이다.

도 3은 플러그-인 소켓에 삽입되는 보안 모듈의 칩 외형을 설명하기 위한 도면이다.

도 4는 도 2의 보안 모듈의 구체적인 구성을 나타내는 일례이다.

도 5는 도 2의 프로토콜 변환부와 ISO 칩의 관계를 나타내는 구체적인 블록도이다.

도 6은 NFC 통신부로부터의 S2C 방식에 따른 신호가 ISO 방식에 따른 신호로 변환되어 보안 모듈로 출력되는 과정을 설명하기 위한 각 신호의 파형을 나타내는 일례이다.

도 7은 보안 모듈로부터의 ISO 방식에 따른 신호가 S2C 방식에 따른 신호로 변환되어NFC 통신부로 출력되는 과정을 설명하기 위한 각 신호의 파형을 나타내는 일례이다.

도 8은 도 2의 프로토콜 매칭부의 동작 설명을 위한 흐름도이다.

도 9는 본 발명에 따른 보안 NFC 통신 장치를 탑재한 이동통신 단말기와 리더 간의 통신 응용 관계를 설명하기 위한 도면이다.

도 10은 본 발명에 따른 보안 NFC 통신 장치를 탑재한 이동통신 단말기들 간의 통신 응용 관계를 설명하기 위한 도면이다.

<도면의 주요 부분에 대한 부호의 설명>

200: 보안 NFC 통신 장치

210: NFC 통신부

220: 프로토콜 매칭부

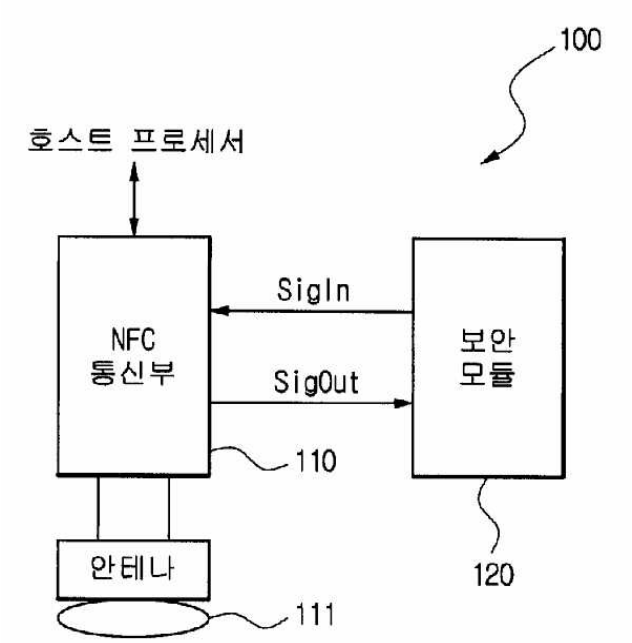
222: 칩확인부

223: 프로토콜 변환부

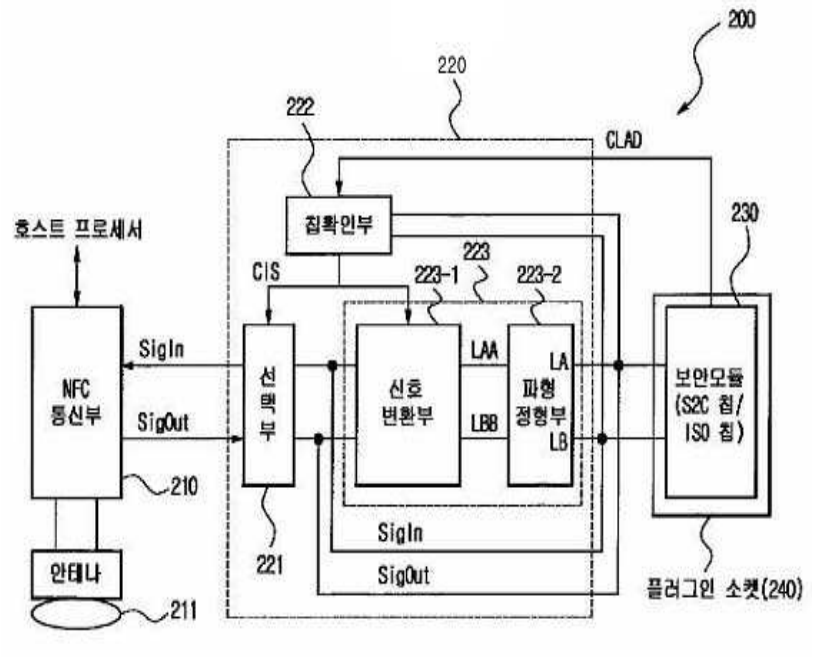
230: 보안 모듈

도면

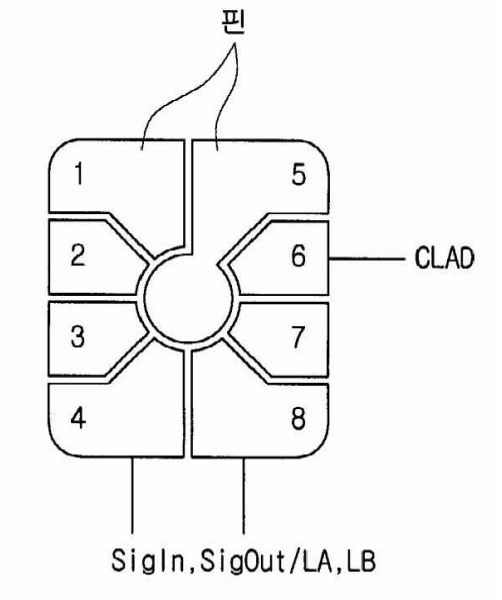
도면1



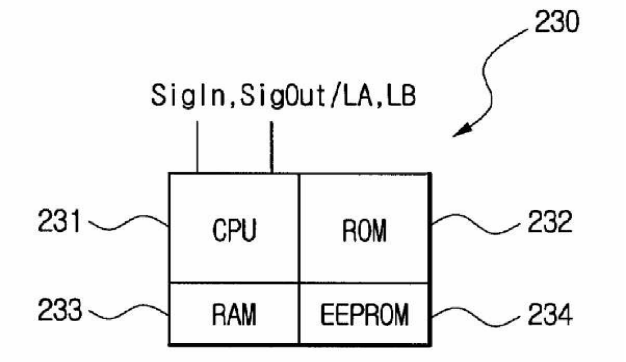
도면2


200
220
222
CLAD
230
칩확인부
호스트 프로세서
CIS
223
223-1
223-2
NFC
통신부
SigIn
SigOut
선택부
신호
변환부
LAA
LBB
LA
파형
정형부
LB
보안모듈
(S2C 칩/
ISO 칩)
210
221
SigIn
SigOut
안테나
211
플러그인 소켓(240)

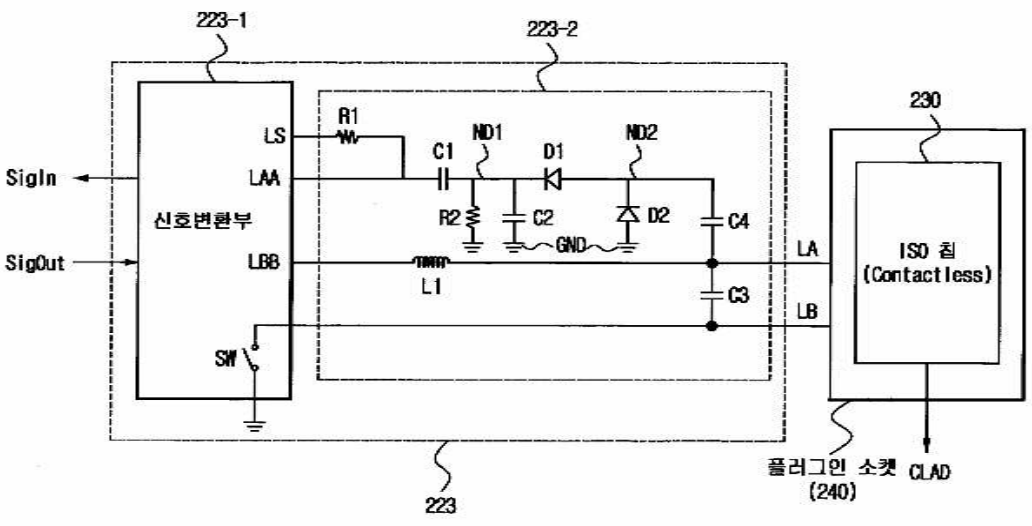
도면3


핀
1
2
3
4
5
6
7
8
CLAD
SigIn,SigOut/LA,LB

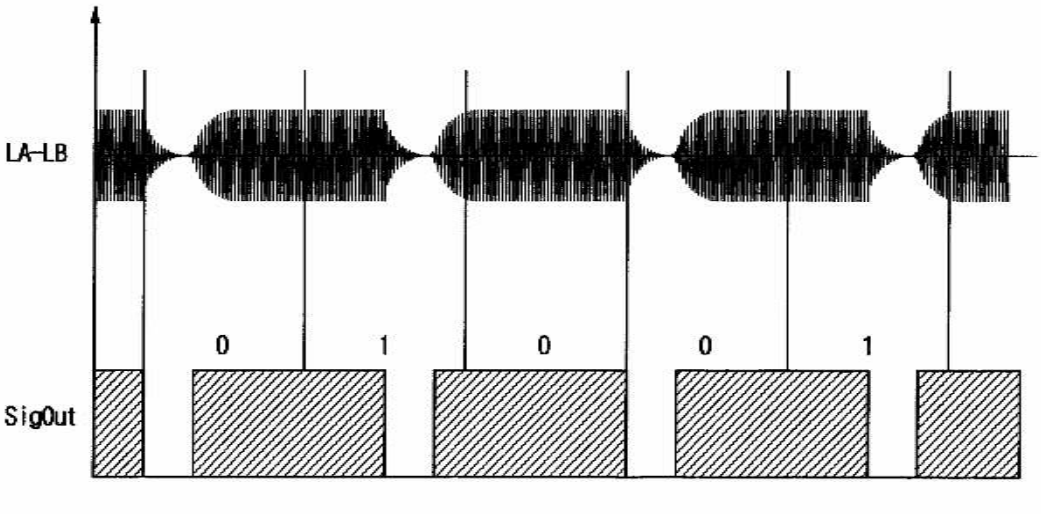
도면4


230
SigIn,SigOut/LA,LB
231
CPU
ROM
232
233
RAM
EEPROM
234

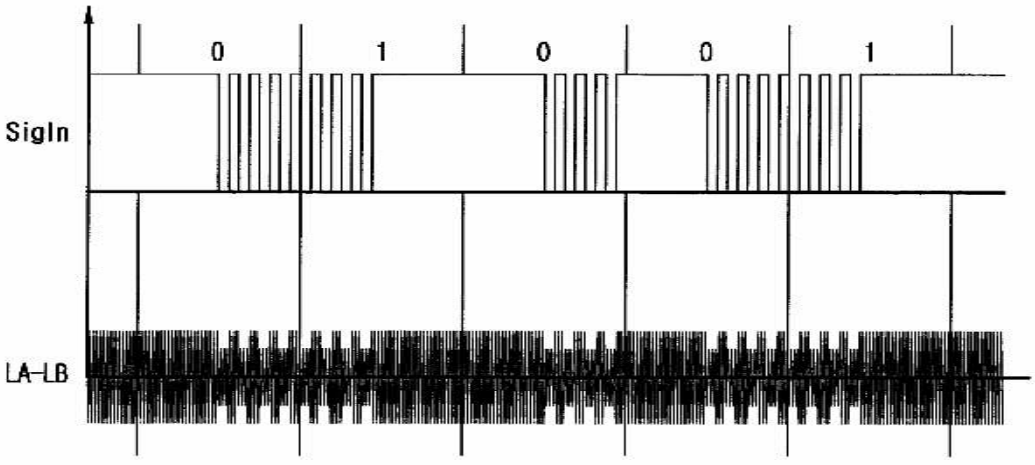
도면5


223-1
223-2
230
SigIn
SigOut
LS
LAA
LBB
SW
신호변환부
R1
C1
ND1
D1
ND2
R2
C2
D2
C4
GND
L1
C3
LA
LB
ISO 칩
(Contactless)
223
플러그인 소켓
(240)
CLAD

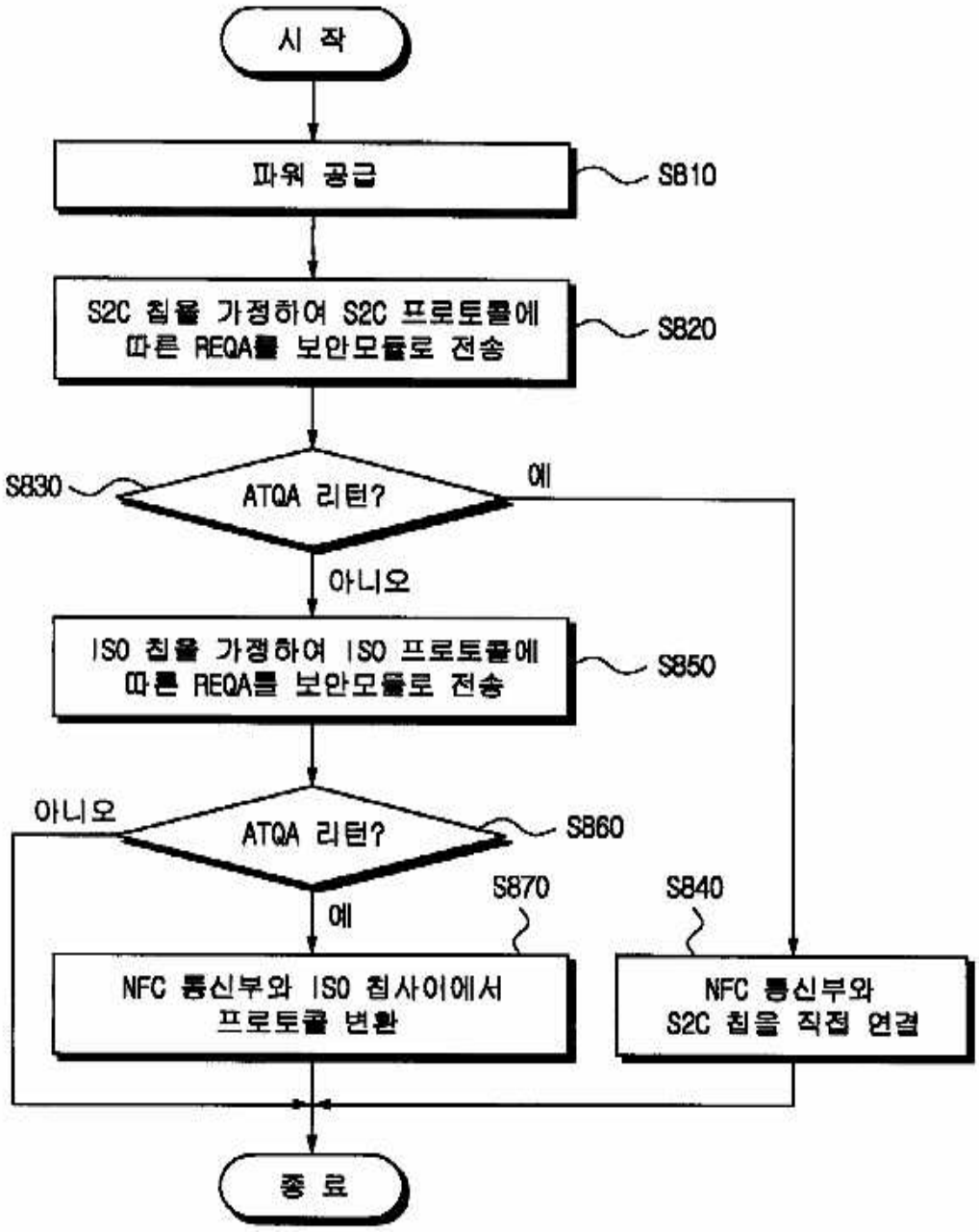
도면6


LA-LB
SigOut
0
1
0
0
1

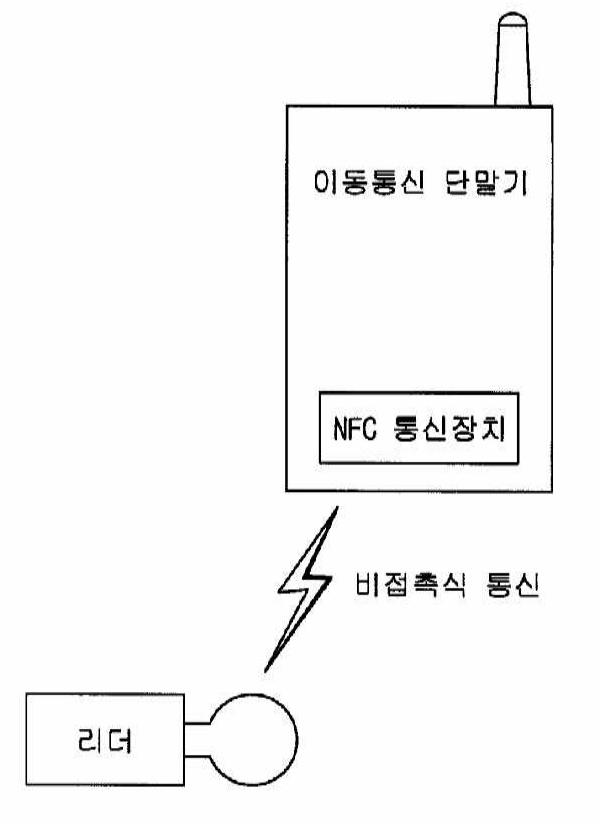
도면7


SigIn
LA-LB
0
1
0
0
1

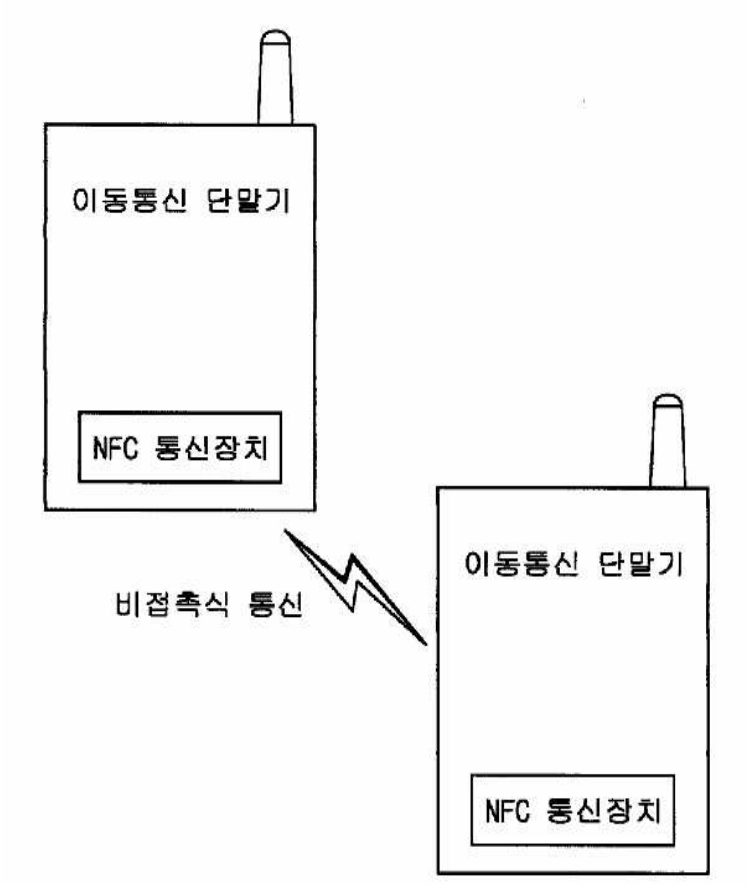
도면8


시 작
파워 공급
S810
S2C 칩을 가정하여 S2C 프로토콜에 따른 REQA를 보안모듈로 전송
S820
S830
ATQA 리턴?
예
아니오
ISO 칩을 가정하여 ISO 프로토콜에 따른 REQA를 보안모듈로 전송
S850
아니오
ATQA 리턴?
S860
예
S870
S840
NFC 통신부와 ISO 칩사이에서 프로토콜 변환
NFC 통신부와 S2C 칩을 직접 연결
종 료

도면9


이동통신 단말기
NFC 통신장치
비접촉식 통신
리더

도면10


이동통신 단말기
NFC 통신장치
비접촉식 통신
이동통신 단말기
NFC 통신장치