특 허 법 원

제 5 - 3 부

판 결

사 건	2021허3574 거절결정(특)
원 고	주식회사 A
	대표이사 B
	소송대리인 변리사 박수조
피 고	특허청장
	소송수행자 권오성
변 론 종 결	2022. 4. 5.
판 결 선 고	2022. 5. 12.

주 문

1. 원고의 청구를 기각한다.

2. 소송비용은 원고가 부담한다.

청 구 취 지

특허심판원이 2021. 3. 31. 2020원1775호 사건에 관하여 한 심결을 취소한다.

이 유

1. 기초사실

가. 이 사건 출원발명(을 제1호증)

1) 발명의 명칭 : 무전원 지문인식 카드

2) 출원일/ 출원번호 : 2018. 3. 16./ 제10-2018-31055호

3) 청구범위

【청구항 1】 무전원 지문인식 카드에 있어서, 무전원 지문인식 카드가 리더부에 접근하면서 유도전류를 생성하는 유도전류생성부(이하 '구성요소 1'이라 한다): 상기 생성된 유도전류에 의해 턴온되어 사용자의 생체정보를 센싱하는 생체정보인식센서(이하 '구성요소 2'라 한다); 센싱된 사용자의 생체정보를 프로세싱하는 제어부(이하 '구성요소 3'이라 한다); 및 상기 사용자의 생체정보가 등록된 정보인 경우에 상기 리더부와 태깅되는 NFC칩;을 포함하고(이하 '구성요소 4'라 한다), 상기 제어부는 무전원 지문인식 카드가 리더부에 근접되거나 서로 접촉이 발생되는 경우에도 NFC태깅이 이루어지지 않도록 제어할 수 있고(이하 '구성요소 5'라 한다), 상기 제어부는 상기 사용자의 생체정보를 등록, 대비 및 삭제 중 어느 하나를 수행하고(이하 '구성요소 6'이라 한다), 상기 NFC칩이 상기 리더부와 태깅되는 경우에 설정 장치의 락 또는 언락 기능이 수행되되, 상기 리더부는 상기 사용자의 생체정보가 등록된 정보인 경우에도 상기 락 또는 언락 기능을 블록할 수 있고(이하 '구성요소 7'이라 한다), 상기 생체정보는 지문정보이고(이하 '구성요소 8'이라 한다), 상기 유도전류생성부는 무전원 지문인식 카드의 최외각 테두리를 감는 형태의 코일로 형성되며(이하 '구성요소 9'라 한다), 상기 코일의 내부에는 제어부를 구성하는 칩, 생체정보인식센서 및 NFC칩이 실장되는 PCB가 배치되

고(이하 '구성요소 10'이라 한다), 상기 PCB는 코일의 내부에서 공간을 점유하는 PCB 영역을 형성하고, 상기 코일의 내부에서 상기 PCB영역을 제외한 부분은 빈공간 영역을 형성하고, 상기 PCB영역은 사각의 형태로 이루어지고, 상기 사각을 구성하는 선분 중에서 3개의 선분은 상기 코일과 근접하게 배치되되 상기 코일과 맞닿지 않게 배치되는 것(이하 '구성요소 11'이라 한다)을 특징으로 하는 무전원 지문인식 카드.

【청구항 2~9】 (삭제)

4) 발명의 주요 내용

㉮ 기술분야

본 발명은 지문인식 카드 및 이의 구동 방법에 대한 것으로서, 보다 상세하게는 무전원으로 사용자의 지문을 인식하여 출입 기능 등을 수행하는 무전원 지문인식 카드 및 이의 구동 방법에 대한 것이다(문단번호 [0001]).

㉯ 배경기술

최근 들어 생활이 더욱 윤택해지고 여유로워지면서 보안에 대한 관심이 높아지고 있다. 이러한 가운데 기존의 도어락은 사용자가 외출시 열쇠를 필히 휴대해야 하는 불편함과 열쇠의 복사가 쉽고 열쇠 분실로 인한 불안함이 늘 존재하여 왔다. 불편함과 불안함을 동시에 해소시키기 위하여 디지털 도어락(Digital Door Lock)이 개발되어 사용되고 있다(문단번호 [0002]).

디지털 도어락(digital door lock) 장치는 전기적인 특성을 이용한 전자 카드 시스템 혹은 비밀번호 시스템을 도입하여 사용되고 있으며, 전자 카드를 이용한 도어락의 경우, 전자카드를 도어락에 구비되어 있는 카드 리더기로 상기 전자카드를 읽고, 상기 전자카드에 등록되어 있는 정보를 확인 후 도어를 개폐하도록 제어한다(문단번호 [0003]).

이와 같이, 상기 디지털 도어락은 디지털 신호 감응에 의하여 도어의 잠금 해지가 이루어지도록 하여 방범 및 보안을 목적으로 하는 다양한 기능들을 구비하고 있다. 이에 한국등록특허 제10-1296863호에는 NFC를 이용하여 보안 기능을 강화한 디지털 도어락 시스템을 개시하고 있다. 그러나, 본 특허는 오직 NFC에 저장된 정보를 통해 구동되므로 그 보안에 있어 취약한 부분이 있다(문단번호 [0004]).

이에, 한국등록특허 제10-1792002호에서는 사용자의 지문을 이용하여 보안을 강화한 융합 카드를 제시하고 있다. 그러나, 별도의 전원이나 전원의 충전이 필요하므로 비상시 또는 특수한 경우 융합 카드를 사용하지 못할 가능성을 항상 내포하고 있다(문단번호 [0005]).

㈐ 해결하고자 하는 과제

본 발명은 상기한 종래기술의 문제점을 해결하기 위한 것으로서, 본 발명의 목적은 보안을 극도로 향상하면서 전원도 필요없는 무전원 지문인식 카드 및 이의 구동 방법을 제공한다(문단번호 [0008]).

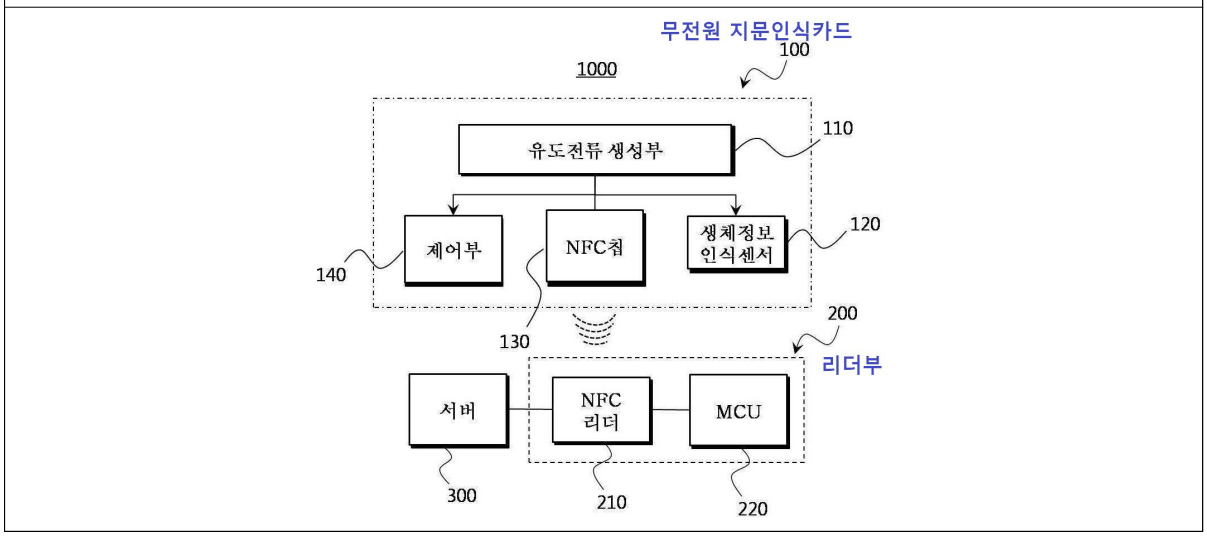
㈑ 발명의 효과

본 발명은 목적 장치의 구동을 위해 NFC칩을 이용하여 편의성을 극대화하면서, 사용자의 지문 등 생체정보를 이용하므로 보안을 강화하고 나아가 인가되는 유도 전류를 이용하므로 편의성을 극대화한다(문단번호 [0019]).

㈒ 발명을 실시하기 위한 구체적인 내용

도면을 참조하면, 본 발명의 일 실시예에 따른 무전원 지문인식 시스템(1000)은 무전원 지문인식 카드(100) 및 리더부(200)를 포함하여 이루어진다. 또한, 무전원 지문인식 시스템(1000)은 서버(300)를 더 포함할 수 있다(문단번호 [0026]).

<도 1> 본 발명의 일 실시예에 따른 무전원 지문인식 시스템의 구성도



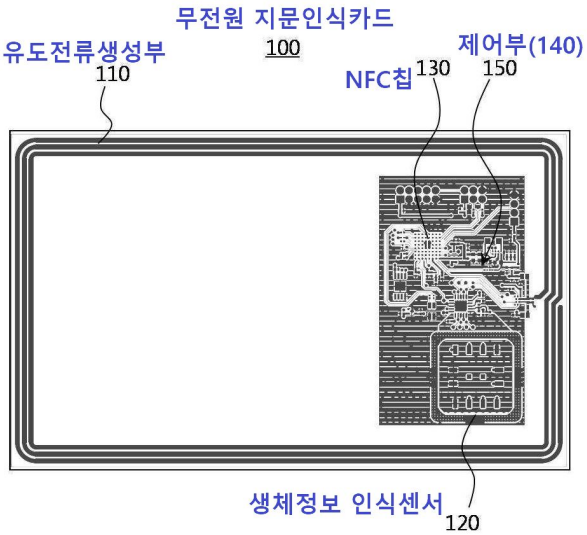
이때, 무전원 지문인식 카드(100)는 유도전류생성부(110), 생체정보인식센서(120), NFC칩(130), 및 제어부(140)를 포함하여 이루어진다(문단번호 [0027]).

유도전류생성부(110)는 본 발명의 일 실시예에 따른 무전원 지문인식카드(100)를 리더부

(200)에 접근시키는 경우에 유도전류를 생성한다. 유도전류생성부(110)는 무전원 지문인식 카드 내의 생체정보인식센서(120)를 구동하기 위한 전원공급을 카드 내의 코일 안테나를 통해 유도 전류를 발생해 이루어진다(문단번호 [0028]).

즉, 리더부(200)와 유도전류생성부(110) 사이에 RF 패스(path)가 연결된다. 이에 초기환경이 셋업되어 전원이 일정하게 생체정보인식센서(120)로 공급된다. 그렇지 않은 경우에는 생체정보인식센서(120)가 턴온되거나 턴오프되는 것이 반복될 수 있기 때문이다(문단번호 [0029]).

<도 2> 도 1에서의 무전원 지문인식 카드의 레이아웃을 더욱 구체적으로 도시한 도면



이때, 도 2에 도시한 바와 같이, 유도전류생성부(110)는 무전원 지문인식 카드(100)의 최외각 테두리를 감는 형태의 코일로 형성될 수 있다(문단번호 [0030]).

유도전류생성부(110)가 발생시킨 유도 전류에 의해 턴온된 생체정보인식센서(120)는 사용자의 생체정보를 센싱하게 된다. 더욱 상세하게, 사용자의 생체정보는 지문 정보일 수 있으며, 생체정보인식센서(120)는 지문센서일 수 있다(문단번호 [0031]).

이때, 제어부(140)는 사용자의 생체정보가 등록된 정보인 경우에 NFC칩(130)이 리더부(200)의 NFC리더(210)에 태깅되는 것이 가능하도록 제어한다. 더욱 상세하게 도 3에 도시한 바와 같이 제어부(140)는 생체정보관리모듈(141), NFC태깅제어모듈(142), 및 전원제어모듈(143)를 포함하여 이루어진다(문단번호 [0032]).

생체정보관리모듈(141)은 생체정보인식센서(120)를 동작시켜 지문 등의 생체정보를 프로세

싱하여 이를 등록, 매칭, 및 삭제한다. 또한, NFC태깅모듈(142)는 센싱된 사용자의 생체정보가 등록된 정보인 경우에 NFC칩(130)이 NFC리더(210)에 태깅이 가능하도록 제어한다(문단번호 [0033]).

더욱 상세하게, 본 발명의 일 실시예에 따른 무전원 지문인식 카드(100)가 리더부(210)에 근접되거나 서로 접촉이 발생되는 경우에도 NFC태깅이 이루어지지 않도록 제어할 수 있다. 즉, NFC태깅제어모듈(142)는 지문인식에 의해 등록된 사용자인 경우에만 NFC태깅이 가능하도록 제어한다. 전원제어모듈(143)은 발생된 유도전류를 이용하여 후술할 인디케이터(미도시) 등의 출력을 제어한다(문단번호 [0034]).

이때, 등록된 지문의 인식 후 NFC태깅이 이루어지면 리더부(200)의 MCU(220)는 설정된 장치가 구동되도록 한다. 이 경우 설정 장치는 도어일 수 있고, 그 구체적 구동은 도어의 락 또는 언락일 수 있다. 한편, MCU(220)는 서버(300)로부터 전송받은 정보에 따라 등록된 지문의 인식 후 NFC태깅이 이루어지는 경우에도 도어가 락 또는 언락 되지 않도록 제어할 수 있다. 예를 들어, 일정 등급 이상 사용자의 회의가 개최되는 경우에는 그 이전에는 일반 사용자가 지문인식 및 NFC태깅으로 도어의 언락이 가능했더라도 도어가 열리는 것을 방지해야 되는 경우를 상정할 수 있다(문단번호 [0035]).

본 발명의 일 실시예에 따른 무전원 지문인식 시스템의 구동 방법은 무전원 지문인식 카드를 리더부에 근접시켜 유도전류를 생성하는 제1단계(S10), 생성된 유도전류에 따라 생체정보센서를 턴온하여 사용자의 지문을 감지하는 제2단계(S20), 제어부가 상기 감지된 지문이 등록된 지문인지 확인하는 제3단계(S30), 감지된 지문이 등록된 지문인 경우 NFC태깅을 활성화하는 제4단계(S40), 및 NFC태깅에 의해 설정 장치의 락 또는 언락 기능을 수행하는 제5단계(S50)를 포함하여 이루어진다(문단번호 [0040]).

이때, 제4단계(S40)에서 지문이 등록된 지문이 아닌 경우에는 NFC태깅이 수행되지 않으므로 도어의 언락 또는 락이 수행되지 않게 된다(문단번호 [0041]).

나. 선행발명들

1) 선행발명 1(을 제2호증)

2017. 5. 11. 공개된 공개특허공보 제10-2017-50055호에 게재된 '근거리 무선 통신을 사용하는 휴대용 생체 인증 장치 및 단말 장치'에 관한 것으로, 그 주요 내용은 다음과 같다.

㉮ **기술분야**

본 개시의 기술적 사상은 휴대용 생체 인증 장치 및 단말 장치에 관한 것으로서, 근거리 무선 통신을 사용하는 휴대용 생체 인증 장치 및 단말 장치에 관한 것이다(문단번호 [0001]).

㉯ **배경기술**

전자 장치는 지불, 뱅킹(banking) 등과 같은 기능을 지원하기 위하여 개인 인증을 필요로 할 수 있다. 개인 인증은 고도의 정확성 및 보안성을 요구하며, 개인 인증을 위한 다양한 방법들 중 하나로서, 사용자의 지문, 홍채, 지정맥, 목소리, 등과 같은 사용자의 생체 정보를 사용하는 생체 인증이 사용되고 있다(문단번호 [0002]).

생체 인증은 높은 편의성을 제공할 수 있다. 즉, 생체 인증을 통해서 사용자는 개인 인증을 위한 카드 또는 열쇠 등을 휴대할 필요가 없으며, 비밀번호 등을 기억할 필요가 없다. 또한, 위조 및 변조가 용이하지 아니한 생체 정보의 특성에 기인하여, 생체 인증은 높은 보안성을 제공할 수도 있다. 생체 정보는 생체 센서를 통해서 취득될 수 있고, 생체 센서를 내장하지 아니하는 전자 장치, 예컨대 생체 센서를 내장하지 아니하는 모바일 폰은 생체 인증을 통한 개인 인증의 구현이 제한적일 수 있다(문단번호 [0003]).

㉰ **해결하려는 과제**

본 개시의 기술적 사상은 휴대용 생체 인증 장치 및 단말 시스템에 관한 것으로서, 근거리 무선 통신을 통해서 생체 정보를 제공하는 휴대용 생체 인증 장치 및 근거리 무선 통신을 통해서 휴대용 생체 인증 장치에 전력을 공급하는 단말 장치를 제공한다(문단번호 [0004]).

㉱ **발명의 효과**

본 개시의 기술적 사상에 따른 휴대용 생체 인증 장치는, 단말 장치로부터 근거리 무선

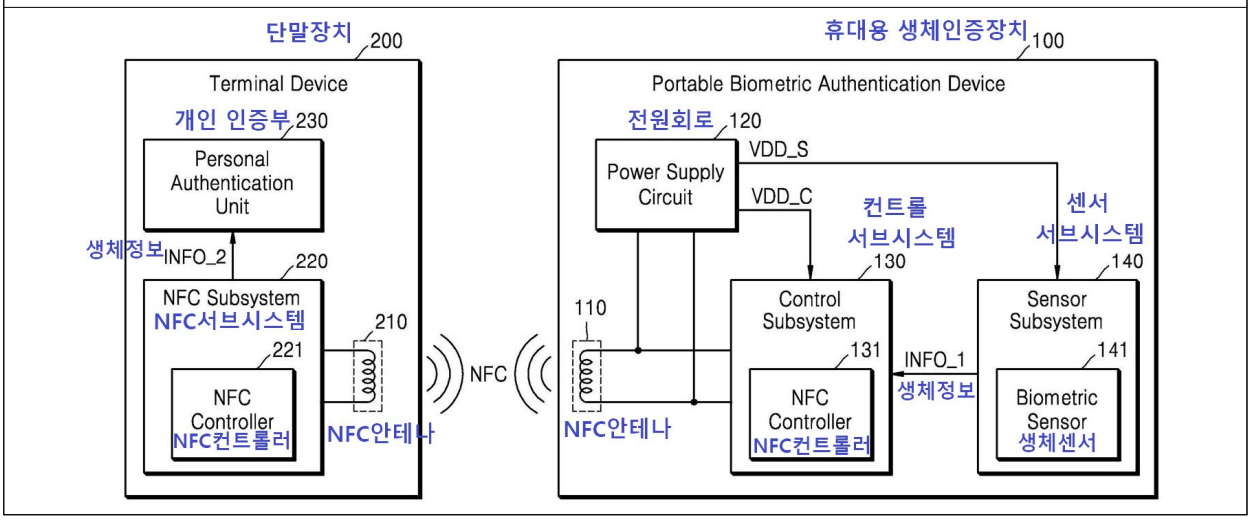
통신을 통해서 전력을 공급받음으로써 충전이나 단말 장치와의 전기적 연결 등이 생략될 수 있고, 이에 따라 사용자에게 높은 편의성을 제공할 수 있다(문단번호 [0007]).

또한, 본 개시의 기술적 사상에 따른 휴대용 생체 인증 장치 및 단말 장치는, 근거리 무선 통신의 근접성 및 보안성에 기인하여 높은 보안성을 가지는 개인 인증을 실현할 수 있다(문단번호 [0008]).

㈐ 발명을 실시하기 위한 구체적인 내용

도 1은 본 개시의 예시적 실시예에 따른 휴대용 생체 인증 장치(100) 및 단말 장치(200)의 블록도를 나타내는 도면이다. 휴대용 생체 인증 장치(100) 및 단말 장치(200)는 근거리 무선 통신(near field communication; NFC)을 통해서 서로 통신할 수 있고, 휴대용 생체 인증 장치(100)는 사용자로부터 생체 정보를 취득하여 단말장치(200)에 제공할 수 있고, 단말 장치(200)는 수신된 생체 정보에 기초하여 개인 인증을 수행할 수 있다(문단번호 [0014]).

<도 1> 본 개시의 예시적 실시예에 따른 휴대용 생체 인증 장치(100) 및 단말 장치(200)의 블록도를 나타내는 도면



도 1을 참조하면, 휴대용 생체 인증 장치(100)는 NFC 안테나(110), 전원 회로(120), 컨트롤 서브시스템(130) 및 센서 서브시스템(140)을 포함할 수 있다. NFC 안테나(110)는 컨트롤 서브시스템(130)(또는 NFC 컨트롤러(131))로부터 수신된 신호에 따라 전자기장을 발생시킬 수도 있고, 단말 장치(200)에서 발생된 전자기장에 응답하여 신호를 발생시킬 수도 있다. NFC 안테나(110)는 복수의 수동 소자들을 포함하는 안테나 모듈일 수 있고, 복수의 수동 소자들은 NFC 안테나(110)의 공진 주파수를 결정하거나 임피던스(impedance)를 변환할 수 있다(문

단번호 [0017]).

전원 회로(120)는 NFC 안테나(110)와 연결될 수 있고, NFC 안테나(110)에 유도된 전자기장으로부터 전력을 생성할 수 있다. 예를 들면, 전원 회로(120)는 NFC 안테나(110)에 유도된 전자기장으로부터 전류를 인출할 수 있고, 인출된 전류로부터 적어도 하나의 전원 전압들을 생성할 수 있다. 예를 들면, 도 1에 도시된 바와 같이, 전원 회로(120)는 컨트롤 서브시스템(130)에 전압(VDD_C)을 제공할 수 있고, 센서 서브시스템(140)에 전압(VDD_S)을 제공할 수 있다. 컨트롤 서브시스템(130) 및 센서 서브시스템(140)은 전원 회로(120)로부터 제공된 전압들(VDD_C, VDD_S)에 각각 기초하여 동작할 수 있다. 비록 도 1에서 컨트롤 서브시스템(130) 및 센서 서브시스템(140)은 상이한 전압들(VDD_C, VDD_S)을 전원 회로(120)로부터 제공받는 것으로 도시되었으나, 본 개시의 예시적 실시예에 따라 컨트롤 서브시스템(130) 및 센서 서브시스템(140)은 동일한 전압을 전원 회로(120)로부터 제공받을 수 있다(문단번호 [0018]).

컨트롤 서브시스템(130)은 NFC 컨트롤러(131)를 포함할 수 있고, NFC 컨트롤러(131)는 NFC 안테나(110)를 통해 서 데이터를 송수신하는 동작을 제어할 수 있다. 예를 들면, NFC 컨트롤러(131)는 NFC 안테나(110)를 통해서, 단말 장치(200)로부터 생체 정보 요청을 수신할 수도 있고, 센서 서브시스템(140)으로부터 제공된 생체 정보(INFO_1)를 단말 장치(200)에 전송할 수도 있다. NFC 컨트롤러(131)는 전원 회로(120)로부터 제공된 전압(VDD_C)에 기초하여 동작할 수 있다(문단번호 [0019]).

센서 서브시스템(140)은 생체 센서(141)를 포함할 수 있고, 컨트롤 서브시스템(130)에 생체 정보(INFO_1)를 제공할 수 있다. 생체 센서(141)는 사용자로부터 생체 정보를 취득할 수 있다. 예를 들면, 생체 센서(141)는 사용자의 지문, 홍채, 지정맥, 목소리 등을 감지할 수 있고, 전기적 신호로 변환할 수 있다. 생체 센서(141)는 전원 회로(120)로부터 제공된 전압(VDD_S)에 기초하여 동작할 수 있다(문단번호 [0020]).

휴대용 생체 인증 장치(100)에 포함된 컨트롤 서브시스템(130) 및 센서 서브시스템(140)은, 전원 회로(120)가 단말 장치(200)에 의해서 NFC 안테나(110)에 유도된 전자기장으로부터 생성된 전력에 의해서 동작할 수 있다. 이에 따라 휴대용 생체 인증 장치(100)에서 배터리 또는 외부로 노출된 단자 등이 생략될 수 있고, 휴대용 생체 인증 장치(100)는 감소된 폼 펙터(form factor)를 가질 수 있다. 단순한 구조 및 감소된 폼 팩터에 기인하여, 휴대용 생체 인증 장치(100)는 다양한 형태로 구현될 수 있다. 예를 들면, 휴대용 생체 인증 장치(100)는,

도 2를 참조하여 후술되는 바와 같이 단말 장치(200)의 커버 또는 케이스에 내장될 수도 있고, 도 16을 참조하여 후술되는 바와 같이 카드에 내장될 수도 있다. 결과적으로, 본 개시의 예시적 실시예에 따른 휴대용 생체 인증 장치(100)는 고도의 정확성 및 보안성을 제공할 뿐만 아니라, 높은 편의성을 제공할 수 있다(문단번호 [0021]).

단말 장치(200)는 근거리 무선 통신을 통해서 휴대용 생체 인증 장치(100)와 통신함으로써 개인 인증을 수행하는 전자 장치일 수 있다. 예를 들면, 단말 장치(200)는 비제한적인 예시로서, 데스크탑 컴퓨터(desktop computer), 서버 시스템(server system), 스마트 TV(smart TV), 전자 게이트(electric gate), POS 시스템(point of sale system) 등일 수 있다. 또한, 단말 장치(200)는, 비제한적인 예시로서, 랩탑 컴퓨터(laptop computer), 태블릿 PC(tablet PC), 모바일 폰(mobile phone), 스마트 폰(smart phone), e-리더(e-reader), PDA(personal digital assistant), EDA(enterprise digital assistant), 디지털 스틸 카메라(digital still camera), 디지털 비디오 카메라(digital video camera), PMP(portable multimedia player), PND(personal navigation device 또는 portable navigation device), 휴대형 게임 콘솔(handheld game console) 등과 같은 휴대용 전자 장치일 수 있다(문단번호 [0022]).

도 1을 참조하면, 단말 장치(200)는 NFC 안테나(210), NFC 서브시스템(220) 및 개인 인증부(230)를 포함할 수 있다. NFC 안테나(210)는 NFC 서브시스템(220)(또는 NFC 컨트롤러(221))로부터 수신된 신호에 따라 전자기장을 발생시킬 수도 있고, 휴대용 생체 인증 장치(100)에서 발생된 전자기장에 응답하여 신호를 발생시킬 수도 있다. 휴대용 생체 인증 장치(100)의 NFC 안테나(110)와 유사하게, NFC 안테나(210)는 복수의 수동 소자들을 포함하는 안테나 모듈일 수 있고, 복수의 수동 소자들은 NFC 안테나(210)의 공진 주파수를 결정하거나 임피던스를 변환할 수 있다(문단번호 [0023]).

NFC 서브시스템(220)은 NFC 컨트롤러(221)를 포함할 수 있고, NFC 컨트롤러(221)는 NFC 안테나(210)를 통해서 데이터를 송수신하는 동작을 제어할 수 있다. 예를 들면, NFC 컨트롤러(221)는 NFC 안테나(210)를 통해서, 휴대용 생체 인증 장치(100)에 생체 정보 요청을 전송할 수 있고, 휴대용 생체 인증 장치(100)로부터 생체 정보를 수신할 수 있다. 또한, NFC 컨트롤러(221)는 NFC 안테나(210)를 통해서 생성되는 전자기장이 휴대용 생체 인증 장치(100)가 동작하기에 충분한 크기의 전력을 공급하도록 NFC 안테나(210)를 제어할 수 있다(문단번호 [0024]).

개인 인증부(230)는 NFC 서브시스템(220)으로부터 생체 정보(INFO_2)를 제공받을 수 있고, 생체 정보(INFO_2)에 기초하여 개인 인증을 수행할 수 있다. 예를 들면, 개인 인증부(230)는 생체 정보(INFO_2)가 미리 등록된 사용자의 생체 정보와 일치하는지 여부를 판단할 수 있고, 판단 결과에 따라 개인 인증의 성공 여부를 결정할 수 있다. 본 개시의 예시적 실시예에 따라, 개인 인증부(230)는 스테이트 머신에 따라 동작하는 전용 하드웨어 로직일 수도 있고, 메모리 장치에 저장된 프로그램을 수행하는 프로세서일 수도 있다(문단번호 [0025]).

도 5는 본 개시의 예시적 실시예에 따라, 도 3 및 도 4의 휴대용 생체 인증 장치(100a) 및 단말 장치(200a) 사이의 동작을 시간의 흐름에 따라 나타내는 도면이다. 구체적으로, 도 5는 단말 장치(200a)가 보안 기능의 요청을 수신하고 보안 기능을 착수할 때까지 휴대용 생체 인증 장치(100a) 및 단말 장치(200a) 사이의 동작을 시간의 흐름에 따라 나타내는 도면이다. 이하에서, 도 5는 도 3 및 도 4를 참조하여 설명될 것이다(문단번호 [0043]).

단계 S100에서, 단말 장치(200a)는 보안 기능 요청의 발생 여부를 체크할 수 있다. 보안 기능은 개인 인증이 필요한 동작을 지칭할 수 있고, 예컨대 지불, 뱅킹 등을 포함할 수 있다. 단말 장치(200a)는 사용자로부터 보안 기능의 요청을 수신할 수 있다(문단번호 [0044]).

단계 S110에서, 단말 장치(200a) 및 휴대용 생체 인증 장치(100a)는 암호화된 NFC 채널을 형성하는 동작을 수행할 수 있다. 암호화된 NFC 채널이 형성됨으로써, 단말 장치(200a) 및 휴대용 생체 인증 장치(100a) 사이에 이동하는 데이터는 보안이 유지될 수 있다. 단계 S110에 대한 상세한 내용은 도 6을 참조하여 후술될 것이다(문단번호 [0045]).

단계 S120에서, 단말 장치(200a) 및 휴대용 생체 인증 장치(100a)는 휴대용 생체 인증 장치(100a)를 인증하는 동작을 수행할 수 있다. 그 다음에, 단계 S130에서, 단말 장치(200a) 및 휴대용 생체 인증 장치(100a)는 단말 장치(200a)를 인증하는 동작을 수행할 수 있다. 단말 장치(200a) 및 휴대용 생체 인증 장치(100a) 상호간에 인증하는 동작을 통해서, 휴대용 생체 인증 장치(100a)를 사용하는 개인 인증의 보안이 더욱 강화될 수 있다. 단계 S120 및 단계 S130에 대한 상세한 내용은 도 8 및 도 9를 참조하여 후술될 것이다(문단번호 [0046]).

단계 S140에서, 휴대용 생체 인증 장치(100a)는 센서 서브시스템(140a)를 활성화하는 동작을 수행할 수 있다. 예를 들면, NFC 컨트롤러(131a)는, 단계 S130에서 단말 장치(200a)의 인증이 성공한 경우, 센서 서브시스템(140a)를 활성화할 수 있다. NFC 컨트롤러(131a)는, 예컨대 센서 서브시스템(140a)에 전압(VDD_S)가 공급되도록 전원 회로(120a)를 제어하거나 센서

서브시스템(140a)의 인에이블 입력 신호를 비활성화할 수 있다(문단번호 [0047]).

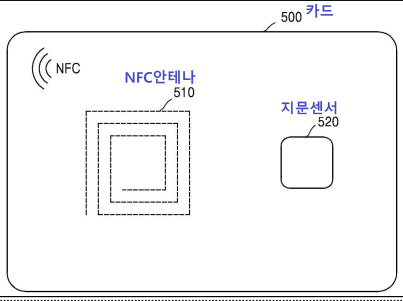
단계 S150에서, 단말 장치(200a)는 휴대용 생체 인증 장치(100a)에 지문 영상의 취득을 요청할 수 있다. 단계 S160에서, 휴대용 생체 인증 장치(100a)(예컨대, 지문 센서(141a))는 사용자의 지문으로부터 지문 영상을 취득할 수 있다. 단계 S170에서, 휴대용 생체 인증 장치(100a)(예컨대, 암호화 처리부(132a))는 취득된 지문 영상을 압축할 수 있다. 단계 S180에서, 휴대용 생체 인증 장치(100a)(예컨대, NFC 컨트롤러(131a))는 암호화 처리된 지문 영상을 단말 장치(200a)에 전송할 수 있다(문단번호 [0048]).

단계 S190에서, 단말 장치(200a)는 개인 인증의 성공 여부를 판단할 수 있다. 예를 들면, 단말 장치(200a)(예컨대, 암호화 처리부(222a))는 휴대용 생체 인증 장치(100a)로부터 수신된 암호화 처리된 지문 영상을 복호화 처리할 수 있다. 그 다음에, 단말 장치(200a)(예컨대, 개인 인증부(230a))는 복호화 처리된 지문 영상을 등록된 사용자의 지문 영상과 비교할 수 있다. 2개의 지문 영상들이 상이한 경우, 단말 장치(200a)는 휴대용 생체 인증 장치(100a)에 지문 영상을 다시 요청할 수 있다. 다른 한편으로, 복호화 처리된 지문 영상 및 등록된 사용자의 지문 영상이 일치하는 경우, 단계 S200에서 단말 장치(200a)는 보안 기능을 수행할 수 있다(문단번호 [0049]).

도 16은 본 개시의 예시적 실시예에 따른 카드(500)를 나타내는 도면이다. 본 개시의 예시적 실시예에 따라 휴대용 생체 인증 장치는, 단순한 구조 및 작은 폭 펙터에 기인하여 카드(500)로서 구현될 수 있다. 즉, 도 16에 도시된 바와 같이, 카드(500)는 NFC 안테나(510) 및 지문 센서(520)를 포함할 수 있다(문단번호 [0111]).

카드(500)는 신용카드, 직불카드와 같이 독립적인 지불 수단으로서 사용될 수도 있고, 본 개시의 예시적 실시예에 따른 근거리 무선 통신 및 지문 영상을 이용한 개인 인증 장치로서 사용될 수도 있다(문단번호 [0112]).

<도 16> 본 개시의 예시적 실시예에 따른 카드를 나타내는 도면



2) 선행발명 2(을 제3호증)

2017. 11. 21. 공고된 등록특허공보 제10-1792002호에 게재된 '지문인식과 연동되어 NFC모듈 근거리 무선통신을 작동시키는 융합카드의 인증처리 알고리즘'에 관한 것으로, 그 주요 내용은 다음과 같다.

㉮ **기술분야**

본 발명은 지문인식과 연동되어 NFC모듈 근거리 무선통신을 작동시키는 융합카드의 인증처리 알고리즘에 관한 것이다. 특히 손가락지문을 인증하여 사용할 수 있는 인증카드로서, 인증카드를 분실하더라도 본인의 인체정보가 아니면 사용할 수 없도록 창안된 지문인식과 연동되어 NFC모듈 근거리 무선 통신을 작동시키는 융합카드의 인증처리 알고리즘에 관한 것이다(문단번호 [0001]).

㉯ **배경기술**

현금 결제카드를 이용하여 사람마다 고유한 생체정보를 획득하고, 그것을 인식함으로써 본인인증을 한다는 것, 즉 지문과 지정맥 인식을 이용한 융합 인증카드에 적용되는 생체 인증기술의 요점이다(문단번호 [0002]).

지문인식의 경우에는 지문 겉면이 쉽게 위조 및 복사가 가능하다는 문제점이 있었다. 또한 습기나 이물질이 손가락에 묻어 있는 경우나 손가락 피부의 훼손과 변형이 있는 경우 등, 잦은 인증 오류가 지적되었다. 지문인식의 오인식률은 약 5%에 이르는 것으로 알려졌다. 예컨대 100명 중 5명 정도의 지문을 인식하지 못한다는 것이다(문단번호 [0003]).

한편, 홍체 인식기술에서는 거리와 각도에 따른 오류 문제가 지적되었다. 또한 대상자가 컬러 콘텐트렌즈를 착용했다거나 라식, 라섹 수술을 받았을 경우에 인증에 실패한다는 문제점이 있었다. 특히 인증에 소요되는 시간이 길었다(문단번호 [0004]).

카드에 있어서 NFC(Near Field Communication)방식은 비접촉의 근거리 통신으로 보안에 유리하여 스마트폰에 적용되면서 활성화되었고, NFC 통신은 NFC 리더기와 NFC 태그(Tag) 사이에서 무선으로 이뤄지고, 그리고 NFC 태그는 정보를 저장하고 있는 NFC칩과 루프안테나(Loop Antenna)로 구성이 되어 있다(문단번호 [0005]).

위와 같은 생체인식 기술보다 내위조성, 오인식률(False Acceptance Rate), 오거절률(False

Reject Rate), 등록실패율(Failure to Enroll Rate), 인증시간 등 모든 면에서 우수한 생체정보로서 지정맥 인증기술이 알려졌다. 지정맥 인증기술은 근적외선을 손가락에 투과시켜 정맥 패턴을 인식하는 기술이다. 혈관내부를 인증하기 때문에 위변조가 불가능하며, 죽은 사람의 지정맥 패턴은 활용할 수 없다는 장점도 있다(문단번호 [0009]).

그러나, 상기 지문인식에 의한 카드결제방법 및 그 카드에 관한 기술은 카드에 가압발광에 의하여 지문데이터를 생성 출력하는 지문인식소자를 구비함으로써 카드사용자의 진성확인 작업이 신뢰성을 가지고, 카드의 보안성이 향상되도록 하였으나, 이러한 종래 기술은 카드이용장비(1)를 이용하였기 때문에 별도의 신분 확인장치을 구비하지 않고도 카드이용장비(1)에서 카드사용자의 진성유무를 확인할 수 있으며, 카드이용장비(1)를 통한 진성확인과정에 있어 별도의 지문인식등과 같은 작업을 수행하지 않더라도 편리성이 향상되는 장점은 있었으나, 결국 지문을 확인할 수 있는 카드이용장비(1)를 구축하지 않을 경우에는 결제카드에 지문패턴이 내장되어 있더라도 카드를 사용할 수 없었고, 이를 활용할 수 있는 시스템을 별도로 개발해야만 하는 것이어서, 이의 기술은 사장되어 있는 실정이다(문단번호 [0019]).

그리고, 지문인증에는 오인식의 가능성과, 지문 하나만의 오인식률을 커버할 수 없었던 문제점이 있었던 것이다(문단번호 [0020]).

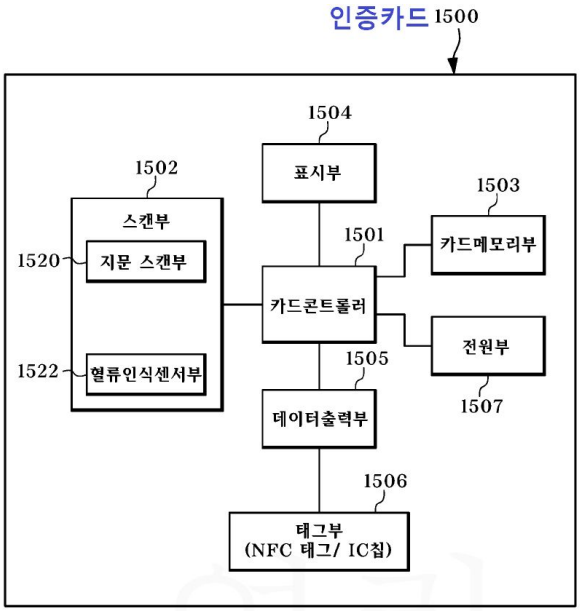
㈐ 해결하려는 과제

본 발명의 목적은 인증카드 자체에 지문의 데이터를 탑재하고, 인증카드 자체에서 사용자의 지문인식시에 혈류 감지를 한 후가 아니면, 이를 사용할 수 없도록 하여 현금의 출금 또는 카드결제 등과 같은 작업을 이행함에 있어 카드사용자의 진성확인의 보안성과 신뢰성을 높일 수 있도록 하고, 지문인식 자체도 정확성과 간편성을 추구하는데 그 목적이 있다. 즉, 실리콘 등의 위변조로 인하여 온도 또는/및 혈류감지가 안되는 경우에는 이의 인증을 차단하는 인증 시스템을 제공하는데 그 목적이 있다(문단번호 [0021]).

더구나, 통상 육안으로 카드의 소지자를 구분할 수 없는 문제점을 해소하기 위하여 카드 메모리부(스마트 칩)에 본인의 사진을 등록시키고, 지문이 일치될 경우에 액정디스플레이에 이를 표출시켜 본인 인증을 할 수 있는 방안을 제공하는데 그 목적이 있다(문단번호 [0022]).

㈑ 발명을 실시하기 위한 구체적인 내용

<도 8> 본 발명의 다른 실시예로서 융합 인증카드의 주요구성을 나타낸 블록구성도



도 8에 도시된 바와 같이 인증카드(1500)는 사람의 손가락에 의하여 지문데이터를 생성 출력하는 지문스캔부(1520)와, 손가락이 접촉될 경우 발생되는 고객의 손가락의 혈류의 흐름을 인식하는 혈류를 통해 카드콘트롤러(1501)를 활성화시키는 혈류감지센서(1522)를 포함하는 스캔부(1502)가 형성되고, 스캔부(1502)로부터 지문데이터를 읽어 들여 카드메모리부(1503)에 저장된 진성확인을 위한 지문데이터와의 일치 여부를 판단하는 카드콘트롤러(1501)와, 카드콘트롤러(1501)에서 출력되는 신호를 NFC 태그(1506a)나 IC칩(1506b)과 같은 태그부(1506)에 기록하는 데이터출력부(1505)로 이루어져 있고, 이의 작동여부를 표시하는 표시부(1504)가 형성되어 있다(문단번호 [0043]).

여기서 카드메모리부(1503)에 저장되는 지문데이터는 인증카드(1500)를 초기 발급할 때 금융기관 및 카드 발급기관에 별도로 구비된 스캔장비(미도시)를 통해 지문을 스캔하여 취득한 지문데이터를 저장할 수 있다(문단번호 [0044]).

또한, 인증카드(1500)의 작동을 위한 전원을 생성하여 저장하는 전원부(1507)로써 태양전지 패널(1507a)이 인증카드(1500)의 전면에 형성된다(문단번호 [0045]).

카드콘트롤러(1501)는 태그부(1506)에 기록하는 신호 즉, 카드정보는 스캔부(1502)로부터 입력된 지데이터와 카드메모리부(1503)에 저장된 지문데이터가 일치할 경우 송출하여 기록한 후 1회 터치하여 카드정보를 사용한 후에는 태그부(1506)를 초기화하여 카드정보가 상실

되도록 하는 것이 바람직하다(문단번호 [0046]).

도 21에 도시된 바와 같이 본 발명의 일 실시예에 따른 융합 인증카드의 처리를 위해 먼저, 전원(1703)을 ON한다(S1700)(문단번호 [0133]).

전원이 ON되면, 우선 스마트칩으로 형성된 카드메모리부에 고유의 지문이나 사진, 기본정보가 등록되어 있는지 여부를 판단한다(S1700a)(문단번호 [0134]).

상기 정보들이 등록되어 있지 않는 경우에는 스마트칩으로 형성된 카드메모리부(1720)에 지문 또는 증명사진을 스캔하여 등록하거나 주민등록번호(또는 이름, 법인명 등) 등 기본정보를 등록한다(S1710)(문단번호 [0135]).

다음은 도 28에서 보는 바와 같이, LCD지문카드의 지문 인증과 LCD 표시 및 NFC 근거리 무선 통신을 하는 수순에 대하여 설명한다(문단번호 [0189]).

혈류감지 여부를 판별한다(S111). 혈류감지 되었을 경우 지문스캔모듈에서 지문 이미지를 스캔한다(S112)(문단번호 [0190]~[0191]).

스캔한 지문 이미지와 사용자의 지문이미지를 비교하여 인증 여부를 판별한다(S113). 지문인증이 되었을 경우 우 LCD화면을 투명해지도록 하여 증명사진이 표출된다(S114). 지문 인증이 되었을 경우 NFC 근거리 무선 통신을 가능하게 활성시킨다(S115)(문단번호 [0192]~[0194]).

상기와 같이, 혈류를 감지할 수 있도록 된 지문모듈센서모듈에서 지문 인증이 되었을 경우 NFC 근거리 무선 통신을 가능하게 되고, 이어서 본인임을 인증하는 지문 인증이 되었을 경우 LCD화면에 증명사진을 표출됨으로써, 카드를 분실하더라도 지문에 의하여 또는 얼굴사진에 의하여 진위성을 판달할 수 있는 카드를 제공할 수 있는 것이다(문단번호 [0198]).

다음은 메인컨트롤러(U3)에 대하여 설명한다(문단번호 [0221]).

상기 메인컨트롤러(U3)의 --(중략)-- 상기와 같은 구성은 지문스캔모듈(U4)에서 지문을 스캔하여 미리 저장된 이미지와 비교하여 같을 경우 NFC모듈(U5)을 이용하여 NFC통신(근거리 무선 통신)을 사용할 수 있게 한다(문단번호 [0222]).

3) 선행발명 3(을 제4호증)

2016. 1. 18. 공개된 공개특허공보 제10-2016-5863호에 게재된 '태그 리더와 개인 인증 기능이 구비된 휴대용 인증 장치를 사용한 보안 장치'에 관한 것으로, 그 주요

내용은 다음과 같다.

㉮ **기술분야**

본 발명은 휴대용 인증 장치를 사용한 보안 장치에 관한 것으로, 보다 상세하게는 출입문이나 개폐가 요구되는 동작대상물에 NFC 또는 RFID 태그를 부착하고, 사용자가 태그 리더기능과 개인인증기능을 갖춘 휴대용 인증장치를 휴대하도록 하여 다양한 개인 인증기능을 손쉽게 부가할 수 있는 태그 리더와 개인인증 기능이 구비된 휴대용 인증 장치를 사용한 보안 장치에 관한 것이다(문단번호 [0001]).

㉯ **배경기술**

그러나 기존의 출입문 제어 장치(ACU, Access Control Unit)와 디지털 도어락은 장치 자체에서 비밀번호 인식, 내부 구성이 복잡하고 고가의 비용이 드는 지문 인식기, 얼굴 인식기, 홍채 인식기, 음성 인식기, RFID 리더기, NFC 카드 리더기를 구비하고 출입 인증을 확인하여 잠금장치의 개폐를 제어하였으나, 내부 구성이 복잡하고 고가의 비용이 드는 문제가 있었다(문단번호 [0008]).

도 1은 종래의 출입문 통제 시스템의 구성도이고, 도 2는 출입 인증수단으로 RFID 리더/NFC 리더 또는 생체 인식기(지문, 얼굴, 홍채, 음성 인식기)를 구비하는 종래의 도어락 시스템 구성도이다(문단번호 [0009]).

종래 보안장치의 전형적인 구조인 태그리더기가 출입문이나 개폐가 요구되는 동작대상물에 부착되고 태그를 사용자가 휴대하여 사용하던 구조는 태그리더기가 개폐가 요구되는 동작대상물에 부착되어 있어 있을 뿐 아니라 그 기능이 고정되어 있어 기능자체를 바꾸기 위해서는 고가의 태그리더기 자체를 바꾸어야 하는 문제점이 있었다(문단번호 [0010]).

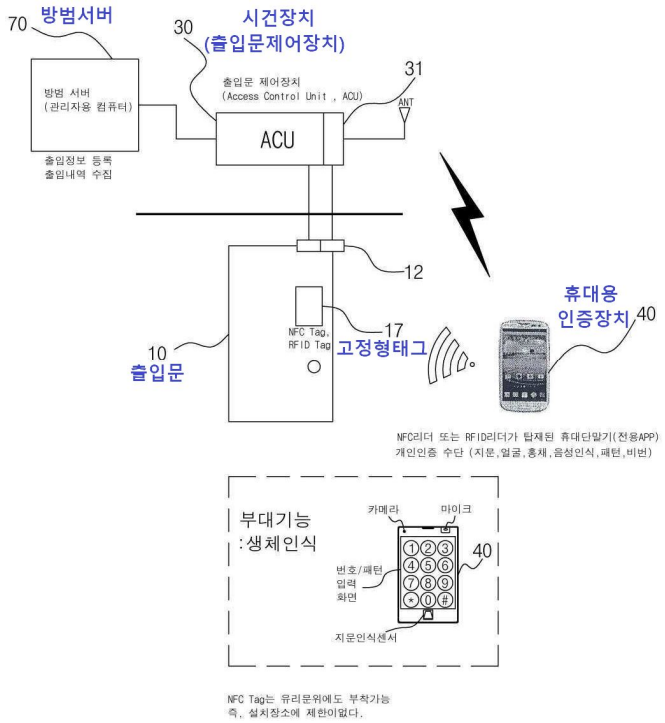
㉰ **해결하려는 과제**

상기 문제점을 해결하기 위한 본 발명은 출입문 또는 개폐가 요구되는 동작대상물에 NFC 또는 RFID 태그(tag)를 부착하고, 사용자가 태그 리더기능과 개인인증기능을 갖춘 휴대용 인증장치를 휴대하도록 하여 다양한 개인인증 기능을 손쉽게 부가할 수 있는 보안장치에 관한 것이다(문단번호 [0012]).

또한 본 발명은 상기 휴대용 인증장치가 갖는 유연성을 활용하여 다양한 접근레벨을 부가할 수 있는 보안장치를 제한하는 것에 관한 것이다(문단번호 [0013]).

㉱ **발명을 실시하기 위한 구체적인 내용**

<도 3> 태그 리더(RFID 리더기, NFC 태그 리더기)와 개인 인증 기능이 구비된 휴대용 인증 장치를 사용한 보안 장치와 관련된 본 발명에 따른 출입문 통제 시스템 구성도



도 3을 참조하면, 출입문(10)에 RFID 태그 또는 NFC 태그를 나타내는 고정형 태그, 또는 RFID 태그가 부착된 RFID 카드 또는 NFC 태그가 부착된 NFC 카드가 설치된다(문단번호 [0045]).

휴대용 인증장치(40)는 노트북/타블렛PC, 핸드헬드 컴퓨터, 이동통신 단말기, 스마트폰, 휴대 단말기 중 어느 하나의 단말기를 사용하며, 상기 휴대 단말기는 이동통신 모뎀(LTE/CDMA/GSM) 또는 Wi-Fi, Bluetooth, ZigBee, NFC, RFID 중 어느 하나의 근거리 무선 통신을 지원하는 근거리 무선 통신부를 구비한다(문단번호 [0046]).

휴대용 인증 장치(40)가 RFID 태그 또는 NFC 태그 인식 후에 사용자에 따라 출입권한등급(Access Level)을 검사하여 추가적으로 비밀번호 또는 패턴 비밀번호, 지문 인식, 얼굴 인식, 홍채 인식, 음성 인식 정보의 개인 인증 정보가 입력되며, 개인 인증 수단을 구비한다(문단번호 [0047]).

개인 인증 수단은 휴대용 인증 장치(40) 또는 시건 장치(예, 출입문 제어 장치(ACU,

Access Control Unit)(30)에 비밀번호 또는 패턴 비밀번호 인식기, 지문 인식기, 얼굴 인식기, 홍채 인식기, 음성 인식기 중 어느 하나를 구비할 수 있다(문단번호 [0048]).

시건 장치(30)는 비밀번호 또는 패턴 비밀번호 인식, 지문 인식, 얼굴 인식, 홍채 인식, 음성 인식기를 구비하지 않는다. 예를 들면, 휴대용 인증장치(40)로 사용되는 스마트폰은 비밀번호 또는 패턴 비밀번호 인식, 지문 인식, 얼굴 인식, 홍채 인식, 음성 인식 중 어느 하나를 사용하여 추가적인 개인 인증 기능을 한다(문단번호 [0049]).

휴대용 인증장치(40)는 비밀번호 데이터 또는 패턴 비밀번호 데이터, 지문인식 센서를 사용한 지문 인식 데이터, 카메라를 사용한 얼굴 인식 데이터 또는 홍채 인식 데이터, 마이크를 사용한 음성 인식 데이터 중 어느 하나의 인식 정보를 사용하여 개인 인증을 한다. 휴대용 인증 장치(40)는 휴대용 인증장치 ID와 인식 정보를 단말기 자체 DB와 비교하거나 또는 근거리 무선통신을 통해 시건 장치(30) 또는 보안서버(방범서버)(70)로 전송하여 시건 장치(30)의 출입권한등급을 확인하거나 또는 보안서버(70)에서 기 저장된 DB의 생체인식정보와 비교하여 개인 인증을 확인한다. 개인 인증이 확인되면, 휴대용 인증장치(40)는 시건 장치(30)로 개폐제어신호(lock/unlock)를 전송하고, 상기 시건장치(30)를 작동하여 도어 개폐를 제어되도록 한다(문단번호 [0050]).

시건 장치(30)는 보안 서버(방범 서버)(70)와 연결되어 사용될 수 있다(문단번호 [0051]).

보안 서버(70)는 최초 접근권한 등록 시 개별적으로 허가된 사용자의 휴대용 인증 장치(40)에게 출입 가능한 출입 가능한 고정형 태그 ID(예, NFC Tag ID)와 출입권한등급(Access Level) 정보가 부여된다(문단번호 [0052]).

개인 인증 수단은 구축 방식에 따라 시건 장치(30) 또는 휴대용 인증 장치(40)에 출입권한등급(Access Level) 테이블 정보를 저장한다(문단번호 [0053]).

예를 들면, 출입권한등급(Access Level)은 회장의 경우 출입문에 부착된 RFID 태그 또는 NFC 태그가 인식되면 출입문, 회사의 금고, 기밀 서류 보관실 모든 잠금 장치를 개폐할 수 있다. 회사의 금고와 기밀 서류 보관실은 접근 권한 허가된 사장, 그룹 이사, 담당 부장만이 NFC 태그 인식 후에 추가적인 개인 인증(지문, 얼굴, 홍채, 음성 인식 정보)을 받은 후에 출입문의 접근이 허가된다. 이때, 부장과 과장, 사원의 경우 허가된 구역의 출입문에 접근 레벨을 가지며, 통제 구역의 회사의 금고와 기밀 서류 보관실을 액세스할 수 없다(문단번호 [0054]).

다. 이 사건 심결의 경위

1) 특허청 심사관은 2019. 5. 22. 이 사건 출원발명에 대하여 '청구항 전항은 이 발명이 속하는 기술분야에서 통상의 지식을 가진 사람(이하 '통상의 기술자'라 한다)이 선행발명 1 내지 3에 의하여 쉽게 발명할 수 있는 것이므로 특허법 제29조 제2항에 따라 진보성이 부정되어 특허를 받을 수 없다.'라는 취지의 의견제출통지를 하였다.

2) 이에 원고는 2019. 10. 22. 보정서를 제출하였고, 2020. 4. 27. 재심사 청구를 구하는 취지의 보정서를 제출하였으나, 특허청 심사관은 2020. 6. 11. 이 사건 출원발명에 대해 '청구항 제1항에 기재된 발명은 선행발명 1 내지 3에 의하여 진보성이 부정되어 특허법 제29조 제2항에 따라 특허를 받을 수 없다.'라는 취지의 이유를 들어 거절결정(이하 '원결정'이라 한다)을 하였다.

3) 그러자 원고는 2020. 7. 13. 특허심판원 2020원1775호로 원결정에 대한 불복심판청구를 하였고, 특허심판원은 2021. 3. 31. '이 사건 출원발명은 통상의 기술자가 선행발명 1 내지 3 및 주지관용기술에 의하여 쉽게 발명할 수 있는 것이므로 특허법 제29조 제2항의 규정에 의해 특허를 받을 수 없는 것이어서, 원결정은 적법하다'라는 이유로 원고의 위 심판청구를 기각하는 심결(이하 '이 사건 심결'이라 한다)을 하였다.

【인정 근거】 다툼 없는 사실, 갑 제1 내지 5호증, 을 제1 내지 4호증의 각 기재, 변론 전체의 취지

2. 당사자 주장의 요지

가. 원고의 주장 요지

이 사건 출원발명의 핵심은 당초 출입권한이 있는 자도 후발적으로 출입권한이 없도록 제어할 수 있는 것인데, 선행발명 3에는 그에 대응하는 구성이 전혀 없는 등 선

행발명 1 내지 3 등에 의하여 이 사건 출원발명의 진보성이 부정되지 않는다. 따라서 그와 달리 판단한 이 사건 심결은 위법하므로 취소되어야 한다.

나. 피고의 주장

이 사건 출원발명은 통상의 기술자가 선행발명 1에 선행발명 2 내지 3을 결합하거나 주지관용기술에 의하여 쉽게 발명할 수 있는 것이어서 진보성이 부정된다. 따라서 그와 같이 판단한 이 사건 심결은 정당하다.

3. 이 사건 심결의 위법 여부에 대한 판단

가. 이 사건 출원발명과 선행발명 1의 구성요소 대비

구성요소	이 사건 출원발명	선행발명 1
1	무전원 지문인식 카드에 있어서, 무전원 지문인식 카드가 리더부에 접근하면서 유도전류를 생성하는 유도전류생성부	휴대용 생체 인증 장치(100)는 NFC 안테나(110), 전원 회로(120), 컨트롤 서브시스템(130) 및 센서 서브시스템(140)을 포함할 수 있다(문단번호 [0017]). 예를 들면, 휴대용 생체 인증 장치(100)는, 도 2를 참조하여 후술되는 바와 같이 단말 장치(200)의 커버 또는 케이스에 내장될 수도 있고, 도 16을 참조하여 후술되는 바와 같이 카드에 내장될 수도 있다(문단번호 [0021]). 전원 회로(120)는 NFC 안테나(110)와 연결될 수 있고, NFC 안테나(110)에 유도된 전자기장으로부터 전력을 생성할 수 있다(문단번호 [0018]). 센서 서브시스템(140)은 생체 센서(141)를 포함할 수 있고, 컨트롤 서브시스템(130)
2	상기 생성된 유도전류에 의해 턴온되어 사용자의 생체정보를 센싱하는 생체정보 인식센서	

		에 생체 정보(INFO_1)를 제공할 수 있다. 생체 센서(141)는 사용자로부터 생체 정보를 취득할 수 있다. 예를 들면, 생체 센서(141)는 사용자의 지문, 홍채, 지정맥, 목소리 등을 감지할 수 있고, 전기적 신호로 변환할 수 있다. 생체 센서(141)는 전원 회로(120)로부터 제공된 전압(VDD_S)에 기초하여 동작할 수 있다(문단번호 [0020]).
3	센싱된 사용자의 생체정보를 프로세싱하는 제어부	컨트롤 서브시스템(130)은 NFC 컨트롤러(131)를 포함할 수 있고, NFC 컨트롤러(131)는 NFC 안테나(110)를 통해서 데이터를 송수신하는 동작을 제어할 수 있다. 예를 들면, NFC 컨트롤러(131)는 NFC 안테나(110)를 통해서, 단말 장치(200)로부터 생체 정보 요청을 수신할 수도 있고, 센서 서브시스템(140)으로부터 제공된 생체 정보(INFO_1)를 단말 장치(200)에 전송할 수도 있다. NFC 컨트롤러(131)는 전원 회로(120)로부터 제공된 전압(VDD_C)에 기초하여 동작할 수 있다(문단번호 [0019]).
4	상기 사용자의 생체정보가 등록된 정보인 경우에 상기 리더부와 태깅되는 NFC칩;을 포함하고	
5	상기 제어부는 무전원 지문인식 카드가 리더부에 근접되거나 서로 접촉이 발생되는 경우에도 NFC태깅이 이루어지지 않도록 제어할 수 있고	
6	상기 제어부는 상기 사용자의 생체정보를 등록, 대비 및 삭제 중 어느 하나를 수행하고	센서 서브시스템(140)은 생체 센서(141)를 포함할 수 있고, 컨트롤 서브시스템(130)에 생체 정보(INFO_1)를 제공할 수 있다. 생체 센서(141)는 사용자로부터 생체 정보를 취득할 수 있다. 예를 들면, 생체 센서(141)는 사용자의 지문, 홍채, 지정맥, 목소리 등을 감지할 수 있고, 전기적 신호로 변환할 수 있다. 생체 센서(141)는 전원

		회로(120)로부터 제공된 전압(VDD_S)에 기초하여 동작할 수 있다(문단번호 [0020]).
7	상기 NFC칩이 상기 리더부와 태깅되는 경우에 설정 장치의 락 또는 언락 기능이 수행되되, 상기 리더부는 상기 사용자의 생체정보가 등록된 정보인 경우에도 상기 락 또는 언락 기능을 블록할 수 있고	복호화 처리된 지문 영상 및 등록된 사용자의 지문 영상이 일치하는 경우, 단계 S200에서 단말 장치(200a)는 보안 기능을 수행할 수 있다(문단번호 [0049]).
8	상기 생체정보는 지문정보이고	센서 서브시스템(140)은 생체 센서(141)를 포함할 수 있고, 컨트롤 서브시스템(130)에 생체 정보(INFO_1)를 제공할 수 있다. 생체 센서(141)는 사용자로부터 생체 정보를 취득할 수 있다. 예를 들면, 생체 센서(141)는 사용자의 지문, 홍채, 지정맥, 목소리 등을 감지할 수 있고, 전기적 신호로 변환할 수 있다(문단번호 [0020]).
9	상기 유도전류생성부는 무전원 지문인식 카드의 최외각 테두리를 감는 형태의 코일로 형성되며	전원 회로(120)는 NFC 안테나(110)와 연결될 수 있고, NFC 안테나(110)에 유도된 전자기장으로부터 전력을 생성할 수 있다(문단번호 [0018]). 본 개시의 예시적 실시예에 따라 휴대용 생체 인증 장치는, 단순한 구조 및 작은 폭 펙터에 기인하여 카드(500)로서 구현될 수 있다. 즉, 도 16에 도시된 바와 같이, 카드(500)는 NFC 안테나(510) 및 지문 센서(520)를 포함할 수 있다(문단번호 [0111]).
10	상기 코일의 내부에는 제어부를 구성하는 칩, 생체정보인식센서 및 NFC칩이 실장되는 PCB가 배치되고	
11	상기 PCB는 코일의 내부에서 공간을 점유하는 PCB영역을 형성하고, 상기 코일의 내부에서 상기 PCB영역을 제외한 부분은 빈공간 영역을 형성하고, 상기 PCB영역은 사각의 형태로 이루어지고, 상기 사각을 구성하는 선분 중에서 3개의 선분은 상기 코일과 근접하게 배치되되 상기 코일과 맞닿지 않게 배치되는 것을 특징으로 하	

	는 무전원 지문인식 카드.	

나. 공통점 및 차이점

1) 구성요소 1 및 2

이 사건 출원발명의 구성요소 1, 2와 선행발명 1의 대응 구성요소는 모두 지문을 인식할 수 있는 카드로서 유도전류를 생성할 수 있고, 사용자의 지문과 같은 생체정보를 감지하는 센서를 가진다는 점에서 동일한 구성이다.

2) 구성요소 3 내지 5

이 사건 출원발명의 구성요소 3과 선행발명 1의 대응 구성요소는 모두 사용자의 생체정보를 처리하는 제어부 구성이라는 점에서 동일하다.

이 사건 출원발명의 구성요소 4와 선행발명 1의 대응 구성요소는 NFC칩[NFC 안테나(110)][1]을 포함하고 있으나, 구성요소 4는 사용자의 생체정보가 등록된 정보인 경우에 리더부와 태깅되는 반면, 선행발명 1에는 이러한 점이 명시되어 있지 않다(이하 '차이점 1'이라 한다).

또한, 이 사건 출원발명의 구성요소 5에서 카드가 리더부에 근접되거나 접촉되어도 태깅이 이루어지지 않도록 제어되는 구성이 선행발명 1에는 나타나 있지 않다(이하 '차이점 2'라 한다).

3) 구성요소 6

이 사건 출원발명의 구성요소 6과 선행발명 1의 대응 구성요소는 모두 사용자의 생체정보를 등록할 수 있다는 점에서 동일하다(또한, 선행발명 2에서 카드메모리부에

1) 이하 '[ ]'에 기재한 부분은 이 사건 출원발명의 구성요소에 대응하는 선행발명들의 대응 구성요소를 의미한다.

고유의 지문 등의 정보가 등록되어 있는지 여부를 판단하고, 지문을 등록하는 구성(선행발명 2의 문단번호 [0134], [0135])과도 동일하다).

4) 구성요소 7

이 사건 출원발명의 구성요소 7과 선행발명 1의 대응 구성요소는 NFC칩이 리더부와 태깅되면 락 또는 언락 기능[단말 장치의 보안 기능]이 수행된다는 점에서 동일하나, 구성요소 7은 사용자의 생체정보가 등록된 정보인 경우에도 락 또는 언락 기능이 블록될 수 있는 반면, 선행발명 1에는 이러한 점이 나타나 있지 않다(이하 '차이점 3'이라 한다).

5) 구성요소 8

이 사건 출원발명의 구성요소 8과 선행발명 1의 대응 구성요소는 모두 생체정보가 지문정보라는 점에서 동일한 구성이다.

6) 구성요소 9 내지 11

이 사건 출원발명의 구성요소 9 내지 11과 선행발명 1의 대응 구성요소는 카드에 유도전류생성부[전원 회로(120)], 생체정보인식센서[지문 센서(520)], NFC칩[NFC 안테나(510)]과 같은 구성요소들이 형성된 점에서 동일하나, 이러한 구성요소들이 카드 내에서 배치되는 구체적인 형태에서 차이가 있다(이하 '차이점 4'라 한다).

다. 차이점에 대한 검토

1) 차이점 1

차이점 1은 이 사건 출원발명의 구성요소 4에서 사용자의 생체정보가 등록된 정보인 경우에 리더부와 태깅되는 구성에 관한 것인데, 선행발명 2에도 아래 기재와 같이 사용자의 생체정보인 지문이 인증된 경우에 NFC 통신이 가능하도록 하는 구성(문

단번호 [0192]~[0194], [0222])이 동일하게 나타나 있고, 선행발명 2도 선행발명 1과 마찬가지로 사용자의 지문인식과 NFC 태그를 이용하여 인증장치의 보안성을 향상시키고자 한다는 점에서 차이가 없으며, 선행발명 1, 2의 기술적 관련성과 그 목적·구성 등에 비추어 선행발명 2의 위와 같은 구성을 선행발명 1에 적용하는데 특별한 어려움이 없어 보인다. 따라서 차이점 1은 통상의 기술자가 선행발명 1에 선행발명 2를 결합하여 쉽게 극복할 수 있는 것으로 판단된다.

<선행발명 2>
스캔한 지문 이미지와 사용자의 지문이미지를 비교하여 인증 여부를 판별한다(S113). 지문 인증이 되었을 경우 우 LCD화면을 투명해지도록 하여 증명사진이 표출된다(S114). 지문 인증이 되었을 경우 NFC 근거리 무선 통신을 가능하게 활성시킨다(S115)(문단번호 [0192]~[0194]).
상기 메인컨트롤러(U3)의 --(중략)-- 상기와 같은 구성은 지문스캔모듈(U4)에서 지문을 스캔하여 미리 저장된 이미지와 비교하여 같을 경우 NFC모듈(U5)을 이용하여 NFC통신(근거리 무선 통신)을 사용할 수 있게 한다(문단번호 [0222]).

2) 차이점 2

차이점 2에 관한 이 사건 출원발명의 구성요소 5에서 '카드가 리더부에 근접되거나 접촉되어도 태깅이 이루어지지 않도록 제어'되는 구성이 어떠한 기술적 의미를 가지는지에 대하여 이 사건 출원발명의 '발명을 실시하기 위한 구체적 내용'(이하 '발명의 설명'이라 한다) 부분에 의하면, "본 발명의 일 실시예에 따른 무전원 지문인식 카드(100)가 리더부(210)에 근접되거나 서로 접촉이 발생되는 경우에도 NFC태깅이 이루어지지 않도록 제어할 수 있다. 즉, NFC태깅제어모듈(142)는 지문인식에 의해 등록된 사용자인 경우에만 NFC태깅이 가능하도록 제어한다."(문단번호 [0034])라고 기재되어 있

다. 즉, 이 사건 출원발명의 구성요소 5('카드가 리더부에 근접되거나 접촉되어도 태깅이 이루어지지 않음')는 구성요소 4('사용자의 생체정보가 등록된 경우에만 카드의 태깅이 가능함')와 실질적으로 동일한 의미를 가지는 것이라고 할 것이다. 이러한 사정들과 함께, 앞서 본 증거들에 의하여 인정할 수 있는 선행발명 1, 2의 기술분야 및 그 목적, 선행발명 1의 내용 등을 종합해 보면, 구성요소 5에 관한 차이점 2는 구성요소 4에 관한 차이점 1과 동일하게 통상의 기술자가 선행발명 1에 선행발명 2를 결합하여 쉽게 극복할 수 있다고 봄이 타당하다.

3) 차이점 3

차이점 3은 구성요소 7에서 사용자의 생체정보가 등록된 경우에도 락 또는 언락 기능이 블록될 수 있는 구성에 관한 것인데, 이러한 차이점은 앞서 본 증거들과 을 제5 내지 10호증의 각 기재에 변론 전체의 취지를 보태어 보면 인정할 수 있는 아래의 사정 및 선행발명 1, 3의 기술분야와 그 목적, 이 사건 출원발명 출원일 당시의 기술수준, 해당 기술분야의 발전경향, 해당 업계의 요구 등을 종합해 보면, 통상의 기술자가 선행발명 1에 선행발명 3을 결합하여 쉽게 극복할 수 있다고 볼 것이다.

가) 구성요소 7에 관한 이 사건 출원발명의 발명의 설명에서는 "등록된 지문의 인식 후 NFC태깅이 이루어지는 경우에도 도어가 락 또는 언락 되지 않도록 제어할 수 있다. 예를 들어, 일정 등급 이상 사용자의 회의가 개최되는 경우에는 그 이전에는 일반 사용자가 지문인식 및 NFC태깅으로 도어의 언락이 가능했더라도 도어가 열리는 것을 방지해야 되는 경우를 상정할 수 있다."(문단번호 [0035])라고 기재되어 있어, 구성요소 7은 '필요에 따라 등록된 사용자라도 그 출입을 제한할 수 있다'라는 의미를 가진 것으로 볼 수 있다.

나) 선행발명 3의 아래와 같은 기재에 의하면, 선행발명 3에는 사용자의 '직위'에 따라 출입권한등급이 부여되어 출입을 제한하는 구성이 나타나 있다.

<선행발명 3>
개인 인증 수단은 구축 방식에 따라 시건 장치(30) 또는 휴대용 인증 장치(40)에 출입권한등급(Access Level) 테이블 정보를 저장한다(문단번호 [0053]).
예를 들면, 출입권한등급(Access Level)은 회장의 경우 출입문에 부착된 RFID 태그 또는 NFC 태그가 인식되면 출입문, 회사의 금고, 기밀 서류 보관실 모든 잠금 장치를 개폐할 수 있다. 회사의 금고와 기밀 서류 보관실은 접근 권한 허가된 사장, 그룹 이사, 담당 부장만이 NFC 태그 인식 후에 추가적인 개인 인증(지문, 얼굴, 홍채, 음성 인식 정보)을 받은 후에 출입문의 접근이 허가된다. 이때, 부장과 과장, 사원의 경우 허가된 구역의 출입문에 접근 레벨을 가지며, 통제 구역의 회사의 금고와 기밀 서류 보관실을 액세스할 수 없다(문단번호 [0054]).

다) 구성요소 7에서 '필요'에 따라 출입을 제한하는 것과 선행발명 3에서 '직위'에 따라 출입을 제한하는 것은 모두 특정 장소에 대한 출입권한의 부여정책 내지 그 부여 방식 등에 대한 것으로 평가할 수 있고, 이는 해당 기술 분야의 통상의 기술자가 개별적·구체적 사정에 따라 임의로 선택하여 적용할 수 있는 정도로 판단되는 이상, 구성요소 7과 선행발명 3의 대응 구성요소에 실질적인 차이가 있다고 보기는 어렵다.

라) 선행발명 1의 휴대용 생체 인증 장치는 높은 보안성과 편의성을 제공하려는 것으로(문단번호 [0008], [0021]), 선행발명 3의 위 구성도 직위에 따라 출입 권한을 조정할 수 있는 것이어서 보안성과 편의성을 가진다고 볼 수 있다. 또한, 선행발명 1은 아래에 기재된 바와 같이 필요에 따라 데이터나 프로그램이 변경되거나 갱신될 수 있는 것이다. 그러므로 선행발명 1에 선행발명 3의 위 구성을 적용하여 출입권한의 부여에 관한 사용자 데이터나 출입 프로그램을 변경하는 것이 예정되어 있거나 내재되어 있다고 볼 여지가 많아, 선행발명 1에 선행발명 3을 적용하는데 특별한 어려움이 없어

보인다.

<선행발명 1>
휴대용 생체 인증 장치(100b)는 근거리 무선 통신을 통해서 단말 장치(예컨대, 도 11의 단말 장치(200b))로부터 수신된 데이터에 기초하여 소프트웨어 또는 프로그램을 갱신할 수 있다(문단번호 [0075]).
비휘발성 메모리 장치(150b)에 저장된 데이터는 근거리 무선 통신을 통해서 수신되는 데이터로서 갱신될 수 있고, 이에 따라 컨트롤 서브시스템(130b) 및/또는 센서 서브시스템(140b)의 동작은 변경될 수 있다. 즉, 휴대용 생체 인증 장치(100b)의 소프트웨어가 갱신될 수 있다(문단번호 [0078]).
도 11은 본 개시의 예시적 실시예에 따라 도 10의 휴대용 생체 인증 장치(100b)의 소프트웨어 갱신 동작을 나타내는 도면이다. 단계 S300에서, 단말 장치(200b)는 소프트웨어(SW) 갱신 요청의 발생 여부를 체크할 수 있다. 예를 들면, 사용자로부터 소프트웨어 갱신 요청이 단말 장치(200b)에 입력되거나, 갱신 프로그램으로부터 소프트웨어 갱신 요청이 발생할 수 있다. 단계 S310에서, 단말 장치(200b)는 소프트웨어 갱신 요청 및 바이너리 데이터를 휴대용 생체 인증 장치(100b)에 전송할 수 있다. 바이너리 데이터는 컨트롤 서브시스템(130b) 및/또는 센서 서브시스템(140b)의 동작을 정의하는 프로그램 또는 파라미터에 대응하는 데이터일 수 있다. 단계 S320에서, 휴대용 생체 인증 장치(100b)에서 비휘발성 메모리 장치(150b)에 바이너리 데이터를 기입하는 동작이 수행될 수 있다. 예를 들면, NFC 컨트롤러(131b)는 소프트웨어 업데이트 요청에 응답하여 바이너리 데이터를 비휘발성 메모리 장치(150b)에 기입하는 동작을 제어할 수 있고, 이에 따라 컨트롤 서브시스템(130b) 및 /또는 센서 서브시스템(140b)의 동작은 변경될 수 있다(문단번호 [0081]~[0084]).

4) 차이점 4

차이점 4는 구성요소 9 내지 11에서 카드 내의 코일과 PCB(인쇄회로기판)가 어떠한 위치 또는 영역에 배치되는지에 대한 구체적인 형태에 관한 것인데, 구성요소 9 내지 11에 기재된 배치 형태의 기술적 의미에 대하여는 이 사건 출원발명의 발명의 설명 부분에 별다른 기재가 없고, 이러한 배치 형태는 주지관용의 기술(을 제5 내지 8호

증)에 해당하는 것으로 인정할 수 있으므로, 통상의 기술자가 별다른 어려움 없이 정할 수 있는 것이라고 판단된다.

라. 원고의 주장에 대한 판단

1) 원고는, '이 사건 출원발명은 당초 출입권한이 있는 자도 후발적으로 출입권한이 없도록 제어할 수 있는 구성을 가진 반면, 선행발명 3에는 이러한 구성이 전혀 나타나 있지 아니하므로, 선행발명 3 등을 토대로 이 사건 출원발명의 진보성을 부정한 이 사건 심결은 위법하다'라는 취지로 주장한다.

2) 살피건대, 특허발명의 보호범위는 특허청구 범위에 기재된 사항에 의하여 정하여지는 것이 원칙이고, 다만 그 기재만으로 특허발명의 기술적 구성을 알 수 없거나 알 수는 있더라도 기술적 범위를 확정할 수 없는 경우에는 명세서의 다른 기재에 의한 보충을 할 수는 있으나, 그 경우에도 명세서의 다른 기재에 의하여 특허청구 범위의 확장 해석은 허용되지 아니함은 물론 특허청구 범위의 기재만으로 기술적 범위가 명백한 경우에는 명세서의 다른 기재에 의하여 특허청구 범위의 기재를 제한 해석할 수 없다(대법원 2011. 2. 10. 선고 2010후2377 판결 등 참조).

앞서 인정한 사실과 증거들에 의하면, 이 사건 출원발명 명세서의 '청구범위'에 기재된 청구항 1항에는 "상기 NFC칩이 상기 리더부와 태깅되는 경우에 설정 장치의 락 또는 언락 기능이 수행되되, 상기 리더부는 상기 사용자의 생체정보가 등록된 정보인 경우에도 상기 락 또는 언락 기능을 블록할 수 있고(이하 '쟁점 청구항'[2]이라 한다)"라고 기재되어 있을 뿐, 그 시점 등 제어방식에 관하여 한정되어 있지 않으며, 다만 위 명세서의 '발명의 설명'에서 "한편, MCU(220)는 서버(300)로부터 전송받은 정보

2) 앞서 본 '구성요소 7' 부분이다.

에 따라 등록된 지문의 인식 후 NFC태깅이 이루어지는 경우에도 도어가 락 또는 언락되지 않도록 제어할 수 있다. 예를 들어, 일정 등급 이상 사용자의 회의가 개최되는 경우에는 그 이전에는 일반 사용자가 지문인식 및 NFC태깅으로 도어의 언락이 가능했더라도 도어가 열리는 것을 방지해야 되는 경우를 상정할 수 있다."라고(문단번호 [0035], 이하 '쟁점 발명의 설명'이라 한다) 기재되어 있는 사실을 인정할 수 있다.

위와 같은 사실을 이 사건 출원발명의 목적, 위 명세서에 기재된 제어부의 기능, 위 명세서의 나머지 내용들 및 위 법리와 종합해 볼 때, 원고가 이 법원에서 제출한 증거들과 그 주장의 사정들을 모두 고려하더라도, 쟁점 청구항에서 리더부가 등록된 생체정보라도 그에 대한 락 또는 언락이 되지 않도록 제어할 수 있는 시기나 방법 등을 한정하고 있지 않은 이상, 쟁점 청구항을 원고의 이 부분 주장처럼 당초 출입권한이 있는 자도 후발적으로 출입권한이 없도록 제어하는 의미로 제한하여 해석하기는 어렵고, 쟁점 발명의 설명은 이 사건 출원발명의 실시예의 하나로 볼 수 있어 그와 같은 내용만으로 쟁점 청구항의 의미를 원고의 이 부분 주장처럼 제한하여 해석할 수 있는 근거가 된다고 볼 수도 없다.

설령, 그와 달리 쟁점 청구항을 당초 출입권한이 있는 자도 후발적으로 출입권한이 없도록 제어하는 것으로 제한하여 해석할 수 있다고 가정하더라도, 선행발명 3에도 출입권한등급에 따라 일정 장소에의 출입제한 여부가 가능한 구성이 개시되어 있고[3], 이는 승진이나 퇴직 등 후발적으로 발생한 사유에 따라 출입권한에 변동이 발생하는 것을 예정한 것으로 해석할 수 있는 이상, 그 구성 및 작용효과가 쟁점 청구항과 실질

3) 회사의 금고와 기밀 서류 보관실은 접근 권한 허가된 사장, 그룹 이사, 담당 부장만이 NFC 태그 인식 후에 추가적인 개인 인증(지문, 얼굴, 홍채, 음성 인식 정보)을 받은 후에 출입문의 접근이 허가된다. 이때, 부장, 과장, 사원인 경우 허가된 구역의 출입문에 접근 레벨을 가지며, 통제구역의 회사의 금고와 기밀 서류 보관실을 액세스할 수 없다(문단번호 [0054]).

적으로 동일하다고 판단된다.

따라서 그와 다른 전제에 기초한 원고의 이 부분 주장은 어느 모로 보나 받아들일 수 없다.

마. 소결

앞서 살핀 바에 따르면 이 사건 출원발명은 통상의 기술자가 선행발명 1에 선행발명 2 내지 3을 결합하거나 주지관용의 기술을 더하여 쉽게 발명할 수 있는 것이므로 그 진보성이 부정된다고 봄이 타당하다. 따라서 위와 결론을 같이한 이 사건 심결에는 원고가 주장하는 위법이 없다.

4. 결론

그렇다면 이 사건 심결의 취소를 구하는 원고의 이 사건 청구는 이유 없으므로, 이를 기각하기로 하여 주문과 같이 판결한다.

재판장 판사 우성엽

판사 임영우

판사 김동규