

명세서

발명의 명칭: 스마트 카드 장치, 데이터 일치 여부 판단을 통해 가상보안코드를 생성하는 장치 및 그 방법

기술분야

- [1] 본 발명은 스마트 카드 장치, 데이터 일치 여부 판단을 통해 가상보안코드를 생성하는 장치 및 그 방법에 관한 것이다.

배경기술

- [2] 코드형태 데이터는 많은 영역에서 이용되고 있다. 결제 시에 이용되는 카드번호, 계좌 번호뿐만 아니라 사용자 식별을 위한 IPIN번호, 주민등록번호 등이 코드형태 데이터이다.
- [3] 그러나 이러한 코드데이터를 이용하는 과정에서 유출되는 사고가 많이 발생한다. 카드번호의 경우, 카드 표면에 실제카드번호가 그대로 기재되어 있어서 타인에게 시각적으로 유출되며, 마그네틱을 이용한 결제 시에 카드번호가 그대로 POS장치로 전달되면서 유출된다.
- [4] 실제코드가 그대로 유출되지 않도록 하기 위해 가상코드를 이용하고자 하는 시도가 많았으나, 가상코드에 대응되는 실제코드를 탐색하기 위해 사용자를 식별하기 위한 데이터가 필요하였다.
- [5] 그러나 OTP(One Time Password)의 경우, 별도의 OTP생성 장치를 필요로 하여 불편함을 수반하고, 특히 사용자 단말기의 경우 OTP생성에 이용되는 시드 데이터의 유출로 보안상의 취약점 존재한다.
- [6] 따라서 많은 사용자가 소지하고 있는 카드의 카드 데이터를 기반으로 사용자 인증에 필요한 가상 보안 코드를 생성하는 것과 같이 OTP코드를 생성하되, 별도의 OTP생성 장치를 필요로 하지 않고 동시에 시드 데이터의 유출되지 않도록 하여 보안을 높이는 방안이 필요하다. 그러나 아직까지 이에 대한 적절한 방안이 제시되지 못하는 실정이다.

발명의 상세한 설명

기술적 과제

- [7] 본 발명이 해결하고자 하는 과제는 스마트 카드 장치, 데이터 일치 여부 판단을 통해 가상보안코드를 생성하는 장치 및 그 방법을 제공하는 것이다.
- [8] 본 발명이 해결하고자 하는 과제들은 이상에서 언급된 과제로 제한되지 않으며, 언급되지 않은 또 다른 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제 해결 수단

- [9] 상술한 과제를 해결하기 위한 본 발명의 일 면에 따른 가상보안코드 생성 장치에 의해 수행되는 방법은, IC 칩 및 NFC 칩이 내장된 카드 태깅 시, 상기 카드로부터 가상보안코드의 생성에 필요한 시드 데이터 및 칩 고유 값을

수신하는 단계, 상기 수신된 칩 고유 값이 기 저장된 칩 고유 값과 일치하는지의 여부를 판단하는 단계 및 상기 수신된 칩 고유 값이 상기 기 저장된 칩 고유 값과 일치하면, 상기 시드 데이터 및 상기 시드 데이터의 수신 시점에 해당하는 시간 데이터에 기초하여 가상보안코드를 생성하는 단계를 포함한다.

- [10] 본 발명에서, 상기 방법은, 상기 카드 태깅 시, 상기 카드로 명령어 및 유저 키 값을 전송하는 단계 및 상기 유저 키 값의 정상 여부에 따라, 상기 카드로부터 상기 시드 데이터를 수신하는 단계를 포함할 수 있다.
- [11] 본 발명에서, 상기 카드는, 상기 유저 키 값이 기 저장된 유저 키 값과 일치하는지의 여부를 판단하고, 상기 유저 키 값이 상기 기 저장된 유저 키 값과 일치하면, 상기 가상보안코드 생성 장치로 상기 시드 데이터를 전송할 수 있다.
- [12] 본 발명에서, 상기 유저 키 값은, 사용자에게 발급된 카드와 상기 사용자를 맵핑하기 위해 상기 사용자에게 고유하게 할당된 값이고, 상기 유저 키 값은, 상기 명령어에 결합된 형태로 전송될 수 있다.
- [13] 본 발명에서, 상기 카드 발급 시, 상기 카드가 발급될 사용자에게 대해 상기 카드의 카드 번호, 상기 시드 데이터, 상기 유저 키 값 및 상기 칩 고유 값이 할당될 수 있다.
- [14] 본 발명에서, 상기 칩 고유 값은, 상기 사용자가 가상보안코드 생성 장치 내의 애플리케이션에 상기 카드를 등록할 때, 상기 카드 태깅을 통해 상기 카드로부터 수신되어 상기 애플리케이션에 저장되고, 상기 가상보안코드 생성 장치를 통해 서버로 전송되어, 상기 서버에서 사용자 식별 정보와 맵핑되어 저장될 수 있다.
- [15] 본 발명에서, 상기 방법은, 상기 가상보안코드를 서버로 송신하여 사용자 인증을 요청하는 단계를 더 포함하고, 상기 서버는, 상기 가상보안코드를 기반으로 사용자 식별 정보의 저장 위치를 탐색함으로써 상기 사용자 식별 정보를 추출하고, 상기 추출된 사용자 식별 정보를 기반으로 사용자 인증을 수행할 수 있다.
- [16] 본 발명에서, 상기 가상보안코드, 복수의 세부코드를 포함하고, 상기 복수의 세부코드는, 상기 사용자 식별 정보의 저장 위치 탐색의 시작지점을 설정하는 제1 코드 및 기 설정된 탐색방식에 따라, 상기 시작지점으로부터 상기 사용자 식별 정보의 저장위치로의 탐색경로를 설정하는 제2 코드를 포함할 수 있다.
- [17] 상술한 과제를 해결하기 위한 본 발명의 다른 면에 따른 스마트 카드 장치는, 가상보안코드 생성 장치와 태깅 시에 NFC 기반의 통신을 수행하는 NFC 모듈 및 애플릿(Applet)을 통해 가상보안코드 생성을 위한 데이터를 저장하는 IC 모듈을 포함하고, 상기 IC 모듈은, 가상보안코드 생성 장치와 태깅 시, 상기 NFC 모듈을 통해 상기 가상보안코드 생성 장치로 상기 가상보안코드의 생성에 필요한 시드 데이터 및 칩 고유 값을 전송하고, 상기 가상보안코드는, 상기 전송된 칩 고유 값이 상기 가상보안코드 생성 장치에 기 저장된 칩 고유 값과 일치하면, 상기 시드 데이터 및 상기 시드 데이터의 수신 시점에 해당하는 시간 데이터에 기초하여 생성된다.

- [18] 본 발명에서, 상기 IC 모듈은, 가상보안코드 생성 장치와 태깅 시, 상기 NFC 모듈을 통해 상기 가상보안코드 생성 장치로부터 명령어 및 유저 키 값을 수신하고, 상기 수신된 유저 키 값이 기 저장된 유저 키 값과 일치하는지의 여부를 판단하고, 상기 수신된 유저 키 값이 상기 기 저장된 유저 키 값과 일치하면, 상기 가상보안코드 생성 장치로 상기 시드 데이터를 전송할 수 있다.
- [19] 이 외에도, 본 발명을 구현하기 위한 다른 방법, 다른 시스템 및 상기 방법을 실행하기 위한 컴퓨터 프로그램을 기록하는 컴퓨터 판독 가능한 기록 매체가 더 제공될 수 있다.

발명의 효과

- [20] 본 발명에 따르면, 사용자는 별도의 OTP 장치 없이도 NFC 방식을 기초로 획득한 카드데이터로 사용자 인증에 필요한 가상보안코드를 생성할 수 있다.
- [21] 또한, 스마트 카드 장치는 유저 키 값에 대한 정상 여부를 확인하고, 유저 키 값이 정상인 경우에만 가상보안코드 생성을 위한 시드 데이터를 가상보안코드 생성 장치로 제공하기 때문에, 시드 데이터에 대한 노출을 방지할 수 있다.
- [22] 또한, 가상보안코드 생성 장치는 칩 고유 값에 대한 정상 여부를 확인하고, 칩 고유 값이 정상인 경우에만 가상보안코드를 생성하기 때문에, 카드 복제를 이용한 비정상적인 접근을 막을 수 있다.
- [23] 본 발명의 효과들은 이상에서 언급된 효과로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

- [24] 도 1은 본 발명에 따른 데이터 일치 여부 판단을 통해 가상보안코드를 생성하는 시스템의 구성도이다.
- [25] 도 2는 본 발명에 따른 스마트 카드 장치의 개략적인 구성도이다.
- [26] 도 3은 본 발명에 따른 가상보안코드 생성 장치의 개략적인 구성도이다.
- [27] 도 4는 본 발명에 따른 데이터 일치 여부 판단을 통해 가상보안코드를 생성하는 방법의 순서도이다.
- [28] 도 5는 본 발명에 따른 칩 고유 값 확인을 통해 가상보안코드를 생성하는 것을 설명하기 위한 도면이다.
- [29] 도 6은 본 발명에 따른 유저 키 값 확인을 통해 가상보안코드를 생성하는 것을 설명하기 위한 도면이다.
- [30] 도 7은 본 발명에 따른 칩 고유 값 및 유저 키 값 확인을 통해 가상보안코드를 생성하는 것을 설명하기 위한 도면이다.

발명의 실시를 위한 형태

- [31] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 제한되는 것이 아니라 서로 다른 다양한

형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술 분야의 통상의 기술자에게 본 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.

- [32] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소 외에 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다. 명세서 전체에 걸쳐 동일한 도면 부호는 동일한 구성 요소를 지칭하며, "및/또는"은 언급된 구성요소들의 각각 및 하나 이상의 모든 조합을 포함한다. 비록 "제1", "제2" 등이 다양한 구성요소들을 서술하기 위해서 사용되나, 이들 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 구성요소를 다른 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제1 구성요소는 본 발명의 기술적 사상 내에서 제2 구성요소일 수도 있음은 물론이다.
- [33] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술분야의 통상의 기술자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또한, 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.
- [34] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세하게 설명한다.
- [35] 설명에 앞서 본 명세서에서 사용하는 용어의 의미를 간략히 설명한다. 그렇지만 용어의 설명은 본 명세서의 이해를 돕기 위한 것이므로, 명시적으로 본 발명을 한정하는 사항으로 기재하지 않은 경우에 본 발명의 기술적 사상을 한정하는 의미로 사용하는 것이 아님을 주의해야 한다.
- [36] 본 명세서에서 "문자"는 코드를 구성하는 구성요소로서, 대문자 알파벳, 소문자 알파벳, 숫자 및 특수문자 등의 전부 또는 일부를 포함한다.
- [37] 본 명세서에서 "코드"는 문자가 나열된 문자열을 의미한다.
- [38] 본 명세서에서 "가상보안코드"는 사용자 인증을 위해 임시적으로 생성되며 단위시간마다 변경되는 랜덤코드[일 예로, OTP(One Time Password)]로서, 문자로 이루어진 특정한 자릿수의 코드를 포함할 수 있다. 가상보안코드는 본 발명의 일 실시예에 따라서 서버에 저장된 사용자의 식별 정보를 탐색하는데 이용될 수 있다.
- [39] 또한, 상기 "가상보안코드"는 상기 사용자 인증을 위해 임시적으로 생성되는 인증용 가상코드(OTAC: One Time Authentication Code) 및 상기 인증용 가상코드를 통해 상기 사용자의 1차적 인증이 수행된 후에 추가적으로 2차 인증에 이용되는 랜덤코드[일 예로, OTP(One Time Password)]를 포함할 수도

있다.

- [40] 본 명세서에서 "스마트 카드 장치"는 가상보안코드 생성을 위한 데이터를 제공하는 카드를 의미한다. 또한, 신용카드, 체크카드, 현금카드 등 금융거래를 진행하는 임의의 카드일 수 있으며, 카드의 종류 및 목적에는 제한이 없다.
- [41] 본 명세서에서 "가상보안코드 생성 장치"는 사용자가 사용하는 단말기로서, 어플리케이션을 구동할 수 있는 어플리케이션 프로세서(application processor, AP)를 구비한 임의의 전자기기이다. 사용자 단말기는 휴대가 불가능한 데스크탑(desktop) 컴퓨터 또는 휴대가 가능한 모바일 기기(예를 들어, 스마트폰(smart phone), 태블릿 PC, PDA(personal digital assistant), EDA(enterprise digital assistant), PMP(portable multimedia player), PND(personal navigation device), 웨어러블 디 바이스(wearable device)등을 포함하며 이에 한정되는 것은 아니다.
- [42] 본 명세서에서 "가상보안코드 생성 함수"는 가상보안코드를 생성하는 함수를 의미한다. 예를 들어, OTP(One Time Password) 등을 포함하며, 이에 한정하는 것은 아니다.
- [43] 본 명세서에서 "세부코드 생성 함수"는 가상보안코드를 구성하는 각각의 세부코드를 생성하는 함수를 의미한다.
- [44] 본 명세서에서 "세부코드 결합 함수"는 복수의 세부코드를 조합 또는 결합하여 가상보안코드를 생성하는 함수를 의미한다.
- [45] 본 명세서에서 "UID(user identification)"는 사용자를 식별하기 위해 사용자별로 중복되지 않게 부여되는 고유한 코드 형태의 값을 의미한다.
- [46] 본 명세서에서 "단위카운트"는 특정한 시간간격으로 설정되어, 상기 시간간격이 경과됨에 따라 변경되는 것으로 정의된 단위이다. 예를 들어, 1카운트는 특정한 시간간격(예를 들어, 1.5초)으로 설정되어 사용될 수 있다.
- [47] 본 명세서에서 "저장위치"는 사용자에게 의해 카드의 등록이 요청된 시점에 해당하는 트랙 상 지점(카운트)을 의미한다.
- [48] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세하게 설명한다.
- [49] 도 1은 본 발명에 따른 데이터 일치 여부 판단을 통해 가상보안코드를 생성하는 시스템의 구성도이다.
- [50] 도 2는 본 발명에 따른 스마트 카드 장치의 개략적인 구성도이다.
- [51] 도 3은 본 발명에 따른 가상보안코드 생성 장치의 개략적인 구성도이다.
- [52] 도 4는 본 발명에 따른 데이터 일치 여부 판단을 통해 가상보안코드를 생성하는 방법의 순서도이다.
- [53] 도 5는 본 발명에 따른 칩 고유 값 확인을 통해 가상보안코드를 생성하는 것을 설명하기 위한 도면이다.
- [54] 도 6은 본 발명에 따른 유저 키 값 확인을 통해 가상보안코드를 생성하는 것을 설명하기 위한 도면이다.
- [55] 도 7은 본 발명에 따른 칩 고유 값 및 유저 키 값 확인을 통해 가상보안코드를 생성하는 것을 설명하기 위한 도면이다.

- [56] 도 1을 참조하면, 데이터 일치 여부 판단을 통해 가상보안코드를 생성하는 시스템(이하, 시스템)은 스마트 카드 장치(10), 가상보안코드 생성 장치(20) 및 서버(30)를 포함한다. 여기서, 시스템은 도 1에 도시된 구성요소보다 더 적은 수의 구성요소나 더 많은 구성요소를 포함할 수 있다.
- [57] 스마트 카드 장치(10)는 사용자가 사용하는 실물카드를 의미한다. 실시예에 따라, 스마트 카드 장치(10)의 표면에는 카드 또는 사용자를 식별할 만한 정보 중 일부만 표시될 수 있고 또는 어떠한 정보도 표시되지 않을 수 있다.
- [58] 가상보안코드 생성 장치(20)는 스마트 카드 장치(10)로부터 수신되어 획득되는 카드 데이터를 기반으로 사용자 인증을 위한 가상보안코드를 생성한다.
- [59] 보다 구체적으로, 가상보안코드 생성 장치(20) 내의 프로그램 또는 애플리케이션은 스마트 카드 장치(10)로부터 획득한 시드 데이터를 기반으로 가상보안코드를 생성한다. 이를 위해 상기 프로그램 또는 애플리케이션은 OTP함수를 포함할 수 있다.
- [60] 스마트 카드 장치(10)의 시드 데이터는 해당 스마트 카드 장치(10)의 사용자 식별 정보[UID (User ID)]를 포함할 수 있다. 여기서, 사용자 식별 정보는 사용자로부터 입력된 정보 또는 사용자의 로그인(Log-in) 정보를 기반으로 생성될 수 있다. 구체적으로, 사용자가 프로그램 또는 애플리케이션에 로그인하여 서버(30)로 카드 발급을 신청하면, 서버는 해당 사용자의 로그인 정보에 기초한 사용자 식별 정보와 해당 사용자에게 발급할 카드와 관련한 데이터를 맵핑한다. 이렇게 맵핑된 정보는 서버(30)에 저장될 수 있다.
- [61] 그러나, 본 발명의 사용자 식별 정보는 이에 제한되는 것은 아니며, 스마트 카드 장치(10)의 일련번호와 같이 사용자에게 의해 설정된 것인 아닌 스마트 카드 장치(10) 제작 시 디폴트로 설정된 특정 고유 정보가 특정 사용자에게 대하여 맵핑됨으로써 사용자 정보로 설정되거나 또는 이용될 수도 있다. 또한, 상기 사용자 식별 정보는, 비단 UID 뿐만 아니라, 주민등록번호, 은행계좌번호, 신용카드번호와 같은 개인 정보를 포함할 수도 있다.
- [62] 전술한 바와 같이 가상보안코드 생성 장치(20)는 스마트 카드 장치(10)로부터 획득된 시드 데이터를 기반으로 가상보안코드를 생성한다. 이때, 상기 가상보안코드는 OTP(One Tim Password) 함수에 의해 생성될 수 있는데, 이러한 경우 가상보안코드는 시드 데이터와 가상보안코드 생성을 요청받은 시점 또는 시드 데이터를 획득한 시점의 시간 데이터를 기반으로 생성된다.
- [63] 구체적으로, 상기 가상보안코드는 가상보안코드 생성 장치(20)에 구비된 가상보안코드 생성 함수에 의해 생성되며, 특히 상기 가상보안코드는 적어도 하나 또는 복수의 세부코드를 포함할 수 있는데, 이에 대해서는 자세히 후술하도록 한다.
- [64] 한편, 서버(30)는 가상보안코드 생성 장치(20)로부터 수신된 가상보안코드를 기초로 사용자 인증을 수행한다. 이때, 서버(30)는 가상보안코드 생성 장치(20)와 통신하는 금융사 서버일 수 있으나 이에 한정하는 것은 아니다. 또한 도 1을

참조하면, 서버(30)는 하나의 서버로 구성된 것으로 표시되어 있지만, 복수의 서버가 서로 연계된 시스템 형태로 구성될 수도 있다.

- [65] 한편, 본 발명의 일 실시예로 서버(30)는 상기 수신된 가상보안코드가 정상적으로 생성된 것인지 또는 중복하여 이용된 것인지 여부를 검증하는 과정을 더 수행할 수도 있다.
- [66] 도 1에 도시된 바와 같이, 스마트 카드 장치(10), 가상보안코드 생성 장치(20) 및 서버(30)는 통신망을 통해 서로 각종 데이터, 신호 또는 정보를 송수신할 수 있다.
- [67] 여기서, 통신망은 다양한 형태의 통신망이 이용될 수 있으며, 예컨대, WLAN(Wireless LAN), 와이파이(Wi-Fi), 와이브로(Wibro), 와이맥스(Wimax), HSDPA(High Speed Downlink Packet Access) 등의 무선 통신방식 또는 이더넷(Ethernet), xDSL(ADSL, VDSL), HFC(Hybrid Fiber Coax), FTTC(Fiber to The Curb), FTTH(Fiber To The Home) 등의 유선 통신방식이 이용될 수 있다.
- [68] 한편, 통신망은 상기에 제시된 통신방식에 한정되는 것은 아니며, 상술한 통신방식 이외에도 기타 널리 공지되었거나 향후 개발될 모든 형태의 통신방식을 포함할 수 있다.
- [69] 도 2를 참조하면, 스마트 카드 장치(10)는 NFC 모듈(12) 및 IC 모듈(14)을 포함할 수 있다. 여기서, 스마트 카드 장치(10)는 도 2에 도시된 구성요소보다 더 적은 수의 구성요소나 더 많은 구성요소를 포함할 수 있다.
- [70] NFC(Narrow Frequency Communication) 모듈(12)(즉, NFC 칩)은 통신 모듈로서, 가상보안코드 생성 장치(20)와 태깅 시에 NFC 기반의 통신을 수행할 수 있다.
- [71] IC 모듈(14)(즉, IC 칩)은 애플릿(Applet)을 통해 가상보안코드 생성을 위한 데이터를 저장할 수 있다.
- [72] IC 모듈(14)은 PCB판 내에 실장되어 IC방식의 카드리더기의 단자와 접촉하여 데이터 교환을 수행하도록 한다. IC 모듈(14)은 집적회로(Integrated circuit; IC)를 포함하는 부품, 시스템 온칩(System on chip; SoC) 등 임의의 형태를 포함한다. 예를 들어, IC칩은 본 발명에 따라 ISO 14443 NXP Mifare Classic 타입일 수 있으나, 이에 한정하는 것은 아니다.
- [73] 또한, 도면에 도시되지는 않았으나, 스마트 카드 장치(10)는 카드 데이터를 저장한 메모리(미도시)를 포함할 수 있다. 여기서, 카드 데이터는 가상보안코드 생성을 위해 필요한 데이터를 모두 포함할 수 있다. 보다 상세하게, 카드 데이터는 해당 스마트 카드의 발급을 신청한 사용자의 사용자 식별 정보와 상기 사용자에게 발급된 카드의 카드 식별 정보를 포함할 수 있다.
- [74] 애플릿은 스마트 카드 장치(10)에 카드 데이터를 저장한다. 이때, 본 발명의 일 실시예로 스마트 카드 장치(10)의 애플릿은 카드 데이터를 NDEF(NFC Data Exchange Format)에 기반하여 상기 메모리의 저장 영역에 저장할 수 있다. 즉, 스마트 카드 장치(10)와 가상보안코드 생성 장치(20)가 상호 간에 NFC를 통해 정보 교환이 가능하도록, 상기 카드 데이터는 표준화된 NDEF형식으로 스마트 카드 장치(10) 내에 저장된다.

- [75] 상기 IC 모듈(14)은, 가상보안코드 생성 장치(20)와 태깅 시, 상기 NFC 모듈(12)을 통해 상기 가상보안코드 생성 장치(20)로 상기 가상보안코드의 생성에 필요한 데이터를 전송할 수 있다. 이때, 전송되는 데이터는 시드 데이터 및 칩 고유 값일 수 있지만, 이에 제한되는 것은 아니다. 여기서, 칩 고유 값은, IC 칩의 고유 값일 수도 있고, NFC 칩의 고유 값일 수도 있다.
- [76] 상기 가상보안코드는, 상기 전송된 칩 고유 값이 상기 가상보안코드 생성 장치(20)에 기 저장된 칩 고유 값과 일치하면, 상기 시드 데이터 및 상기 시드 데이터의 수신 시점(또는 가상보안코드 생성 요청 시점)에 해당하는 시간 데이터에 기초하여 생성될 수 있다. 이에 대한 상세한 설명은 후술하도록 한다.
- [77] 또한, 상기 IC 모듈(14)은, 가상보안코드 생성 장치(20)와 태깅 시, 상기 NFC 모듈(12)을 통해 상기 가상보안코드 생성 장치(20)로부터 명령어 및 유저 키 값을 수신하고, 상기 수신된 유저 키 값이 기 저장된 유저 키 값과 일치하는지의 여부를 판단하고, 상기 수신된 유저 키 값이 상기 기 저장된 유저 키 값과 일치하면, 상기 가상보안코드 생성 장치(20)로 상기 시드 데이터를 전송할 수 있다. 이에 대한 상세한 설명은 후술하도록 한다.
- [78] 도 3을 참조하면, 가상보안코드 생성 장치(20)는 통신부(22), 메모리(24) 및 프로세서(26)를 포함할 수 있다. 여기서, 가상보안코드 생성 장치(20)는 도 3에 도시된 구성요소보다 더 적은 수의 구성요소나 더 많은 구성요소를 포함할 수 있다.
- [79] 통신부(22)는 상기 스마트 카드 장치(10)가 가상보안코드 생성 장치(20)에 태깅되면, 상기 통신망을 통해 상기 스마트 카드 장치(10)로 칩 고유 값 리턴을 요청하는 명령어 및 유저 키 값을 전송할 수 있고, 상기 스마트 카드 장치(10)로부터 시드 데이터 및 칩 고유 값을 수신할 수 있다. 이외에도, 두 장치는 태깅 시에 다양한 데이터들을 서로 송수신할 수 있다.
- [80] 메모리(24)는 가상보안코드 생성 장치(20)의 다양한 기능을 지원하는 데이터를 저장할 수 있다. 메모리(24)는 가상보안코드 생성 장치(20)에서 구동되는 다수의 응용 프로그램(application program 또는 애플리케이션(application)), 가상보안코드 생성 장치(20)의 동작을 위한 적어도 하나의 프로세스, 데이터들, 명령어들을 저장할 수 있다. 이러한 응용 프로그램 중 적어도 일부는, 가상보안코드 생성 장치(20)의 기본적인 기능을 위하여 존재할 수 있다.
- [81] 프로세서(26)는 상기 응용 프로그램과 관련된 동작 외에도, 통상적으로 가상보안코드 생성 장치(20)의 전반적인 동작을 제어할 수 있다. 프로세서(26)는 위에서 살펴본 구성요소들을 통해 입력 또는 출력되는 신호, 데이터, 정보 등을 처리하거나 메모리(24)에 저장된 응용 프로그램을 구동함으로써, 상기 스마트 카드 장치(10) 또는 서버(30)에 적절한 정보 또는 기능을 제공 또는 처리할 수 있다.
- [82] 또한, 프로세서(26)는 메모리(24)에 저장된 응용 프로그램을 구동하기 위하여, 도 3과 함께 살펴본 구성요소들 중 적어도 일부를 제어할 수 있다. 나아가,

프로세서(26)는 상기 응용 프로그램의 구동을 위하여, 가상보안코드 생성 장치(20)에 포함된 구성요소들 중 적어도 둘 이상을 서로 조합하여 동작 시킬 수 있다.

- [83] 도 3을 참조하면, 프로세서(26)는 코드생성부(262) 및 검증요청부(264)를 포함할 수 있다. 여기서, 프로세서(26)는 도 3에 도시된 구성요소보다 더 적은 수의 구성요소나 더 많은 구성요소를 포함할 수 있다.
- [84] 코드생성부(262)는 스마트 카드 장치(10)로부터 수신된 시드 데이터 및 시간 데이터를 이용하여 가상보안코드를 생성할 수 있다.
- [85] 검증요청부(264)는 통신부(22)를 통해 상기 가상보안코드를 서버(30)로 송신하여, 상기 서버(30)가 상기 가상보안코드에 대한 검증 및 사용자 인증을 수행하도록 요청할 수 있다.
- [86] 도 3에 도시하지는 않았지만, 프로세서(26)는 코드생성부(262) 및 검증요청부(264) 이외에도, 다양한 연산 동작 및 판단 동작 등을 수행하는 구성요소들을 더 포함할 수 있다.
- [87] 이하에서는 도 4 내지 도 7을 참조하여, 가상보안코드 생성 장치(20)가 가상보안코드를 생성하는 방법에 대해 설명하도록 한다.
- [88] 도 4를 참조하면, 가상보안코드 생성 장치(20)는 IC 칩 및 NFC 칩이 내장된 카드 태깅 시, 상기 카드로부터 가상보안코드의 생성에 필요한 시드 데이터 및 칩 고유 값을 수신할 수 있다(S110). 여기서, 카드는 상기에서 설명한 스마트 카드 장치(10)를 의미할 수 있다.
- [89] 가상보안코드 생성 장치(20)는 상기 수신된 칩 고유 값이 기 저장된 칩 고유 값과 일치하는지의 여부를 판단할 수 있다(S120).
- [90] 가상보안코드 생성 장치(20)는 상기 수신된 칩 고유 값이 상기 기 저장된 칩 고유 값과 일치하면, 상기 시드 데이터 및 상기 시드 데이터의 수신 시점에 해당하는 시간 데이터에 기초하여 가상보안코드를 생성할 수 있다(S130).
- [91] 여기서, 칩 고유 값은 IC 칩의 고유 값일 수도 있고, NFC 칩의 고유 값일 수도 있지만, 이하에서는 칩 고유 값이 IC 칩의 고유 값인 것으로 가정하여 설명하도록 한다.
- [92] 가상보안코드 생성 장치(20)가 수신된 칩 고유 값과 장치 내에 기 저장되어 있던 칩 고유 값이 일치하는지를 확인한 후 두 값이 일치하는 경우에만 가상보안코드를 생성하는 것은, 카드의 칩 데이터를 복제하여 결제를 요청하는 비정상적인 접근을 막기 위함이다. 즉, 해커는 카드 내의 칩 데이터를 복제하여 사용할 수는 있어도 칩 제작 시에 부여된 칩 자체의 고유 값을 알 수는 없으므로, 가상보안코드 생성 장치(20)는 수신된 칩 고유 값이 정상적인 값인지를 확인한 후에 결제를 위한 가상보안코드를 생성하게 된다. 이와 관련하여 도 5를 참조하여 보다 상세하게 설명하도록 한다.
- [93] 도 5를 참조하면, 스마트 카드 장치(10)가 가상보안코드 생성 장치(20)에 태깅되면, 가상보안코드 생성 장치(20)는 스마트 카드 장치(10)로 명령어를

전송한다(S51). 여기서, 명령어는 칩 고유 값 반환을 요청하는 명령어일 수 있다. 스마트 카드 장치(10)는 상기 명령어에 대한 응답으로 칩 고유 값을 가상보안코드 생성 장치(20)로 전송한다(S52). 가상보안코드 생성 장치(20)는 수신된 칩 고유 값과 기 저장된 칩 고유 값의 일치 여부를 판단한다(S53). 판단 결과 두 개의 칩 고유 값이 일치하면, 가상보안코드 생성 장치(20)는 스마트 카드 장치(10)로부터 수신된 시드 데이터와, 상기 시드 데이터의 수신 시점(또는, 가상보안코드 생성 요청 시점)에 획득된 시간 데이터를 이용하여 가상보안코드를 생성한다(S54).

[94] 한편, 도 4에 도시하지는 않았지만, 본 발명의 가상보안코드 생성 장치에 의해 수행되는 가상보안코드 생성 방법은 상기 카드 태깅 시, 상기 카드로 명령어 및 유저 키 값을 전송하는 단계 및 상기 유저 키 값의 정상 여부에 따라, 상기 카드로부터 상기 시드 데이터를 수신하는 단계를 더 포함할 수 있다. 여기서, 카드는 상기에서 설명한 스마트 카드 장치(10)를 의미할 수 있다.

[95] 즉, 상기 카드는, 상기 유저 키 값이 기 저장된 유저 키 값과 일치하는지의 여부를 판단하고, 상기 유저 키 값이 상기 기 저장된 유저 키 값과 일치하면, 상기 가상보안코드 생성 장치(20)로 상기 시드 데이터를 전송할 수 있다.

[96] 여기서, 상기 유저 키 값은, 사용자에게 발급된 카드와 상기 사용자를 맵핑하기 위해 상기 사용자에게 고유하게 할당된 값이다. 즉, 사용자가 상기 애플리케이션에 가입하여 카드 발급을 신청하면, 서버(30)는 해당 사용자에게 발급할 카드에 대해 유저 키 값을 설정함으로써, 상기 카드와 상기 사용자를 맵핑할 수 있다.

[97] 상기 유저 키 값은 카드로 전송될 때, 상기 명령어에 결합된 형태로 전송될 수 있다. 보다 상세하게, 상기 유저 키 값은, APDU(Application Protocol Data Unit) 명령어 뒤에 결합된 형태로 스마트 카드 장치(10)로 전달될 수 있다. 그러나 결합 형태는 이에 제한되는 것은 아니다.

[98] 스마트 카드 장치(10)가 수신된 유저 키 값과 장치 내에 기 저장되어 있던 유저 키 값이 일치하는지를 확인한 후 두 값이 일치하는 경우에만 시드 데이터를 전송하는 것은, 사용자가 아닌 사람에게 시드 데이터가 노출되지 않도록 하기 위함이다. 이와 관련하여 도 6을 참조하여 보다 상세하게 설명하도록 한다.

[99] 도 6을 참조하면, 가상보안코드 생성 장치(20)는 스마트 카드 장치(10)로 명령어에 결합된 형태의 유저 키 값을 전송한다(S61). 스마트 카드 장치(10)는 수신된 유저 키 값이 기 저장된 유저 키 값과 일치하는지 판단한다(S62). 판단 결과, 두 개의 유저 키 값이 일치하면, 스마트 카드 장치(10)는 가상보안코드 생성 장치(20)로 시드 데이터를 전송한다(S63). 가상보안코드 생성 장치(20)는 수신된 시드 데이터와, 시드 데이터가 수신된 시점에 획득된 시간 데이터를 이용하여 가상보안코드를 생성한다(S64).

[100] 정리하면 본 발명은 가상보안코드 생성 장치(20)에 스마트 카드 장치(10)가 태깅되면, 스마트 카드 장치(10) 및 가상보안코드 생성 장치(20) 각각에서 데이터

일치 여부 판단 과정이 수행되고, 두 개의 판단 결과가 모두 정상인 경우에만 가상보안코드가 생성되기 때문에, 가상보안코드를 생성함에 있어서 보안성을 강화할 수 있다.

- [101] 도 7을 참조하면, 가상보안코드 생성 장치(20)는 스마트 카드 장치(10)로 칩 고유 값 반환 요청 명령어를 전송하되, 이때, 해당 명령어에는 유저 키 값이 결합되어 함께 전송된다(S71). 스마트 카드 장치(10)는 수신된 유저 키 값에 대한 정상 여부를 확인한다(S72). 수신된 유저 키 값이 기 저장된 유저 키 값과 일치하면, 가상보안코드 생성 장치(20)로 시드 데이터와 함께, 상기 명령어에 대한 응답으로 칩 고유 값을 전송한다(S73). 가상보안코드 생성 장치(20)는 수신된 칩 고유 값에 대한 정상 여부를 확인한다(S74). 수신된 칩 고유 값이 기 저장된 칩 고유 값과 일치하면, 상기 수신된 시드 데이터와, 시드 데이터 수신 시점(가상보안코드 생성 요청 시점)의 시간 데이터를 이용하여 가상보안코드를 생성한다(S75).
- [102] 이때, 수신된 유저 키 값이 기 저장된 유저 키 값과 일치하지 않으면, 스마트 카드 장치(10)는 가상보안코드 생성 장치(20)로 시드 데이터를 전송하지 않을 수 있다. 실시예에 따라, 시드 데이터 전송 여부와 상관 없이, 스마트 카드 장치(10)는 상기 명령어에 대한 응답으로 칩 고유 값을 가상보안코드 생성 장치(20)로 전송할 수 있으나, 시드 데이터가 전송되지 않았기 때문에 가상보안코드를 생성할 수는 없다.
- [103] 또한, 상기에는 유저 키 값이 칩 고유 값 반환 요청 명령어에 결합되어 함께 전송되는 것으로 설명하였지만, 실시예에 따라 칩 고유 값 반환 요청 명령어와 상기 유저 키 값이 결합되는 명령어가 상이할 수 있다. 즉, 카드가 태깅되면, 가상보안코드 생성 장치(20)는 스마트 카드 장치(10)로 칩 고유 값 반환 요청 명령어와, 유저 키 값이 결합된 명령어를 각각 전송할 수 있다.
- [104] 이하에서는, 본 발명의 일 실시예인 가상보안코드를 생성하는 구체적인 방법에 대하여 설명한다.
- [105] 코드생성부(262)는 하나 또는 복수의 세부코드를 생성하는 역할을 수행한다. 세부코드는 가상보안코드를 구성하는 일부 코드를 의미하는데, 가상보안코드는 세부코드만으로 구성될 수도 있으며, 또는 OTP함수에 의해 생성된 제1 가상보안코드에 하나 또는 복수의 세부코드를 결합하여 최종 가상보안코드(OTAC)의 형태로 형성될 수도 있다.
- [106] 가상보안코드 생성 장치(20)는 가상보안코드를 생성하는 가상보안코드 생성 함수를 포함하고, 가상보안코드 생성 함수는 하나 이상의 세부코드를 생성하는 세부코드 생성 함수와, 상기 세부코드를 결합하여 가상보안코드를 생성하는 세부코드 결합 함수(즉, 복수의 세부코드를 조합하는 규칙)를 포함한다.
- [107] 즉, 가상보안코드가 복수의 세부코드를 포함하는 경우, 가상보안코드 생성 함수는 복수의 세부코드 생성 함수를 이용하여 복수의 세부코드를 생성하고, 상기 세부코드 결합 함수를 통해 상기 복수의 세부코드를 기 설정된 조합으로

결합하여 가상보안코드를 생성한다.

- [108] 일 실시예로, 코드생성부(262)는 스마트 카드 장치(10)가 태깅됨에 따라 획득된 시드 데이터를 기반으로 세부코드 생성 함수에 의해 상기 가상보안코드를 생성할 수 있다.
- [109] 복수의 세부코드 간에는 서버(30)가 사용자 식별 정보의 저장공간을 탐색하기 위해 이용되는 상관관계를 가진다. 즉, 서버(30)는 탐색 알고리즘(저장공간탐색알고리즘)을 구비하고, 상기 탐색 알고리즘은 가상보안코드 생성 장치(20)로부터 수신된 가상보안코드에 포함된 복수의 세부코드를 추출하고, 상기 복수의 세부코드의 상관관계를 기반으로 사용자에게 부여된 사용자 식별 정보[UID(User identification)]의 저장공간을 탐색한다. 상기 복수의 세부코드가 가지는 상관 관계에 대한 일 실시예로, 서버(30)에 포함된 탐색알고리즘은 복수의 세부코드 중 하나 이상의 세부코드에 대응하는 경유지점으로부터 상기 복수의 세부코드 간의 상관 관계를 기반으로 연산하여 상기 사용자 식별 정보의 저장위치를 탐색할 수 있다. 이때, 상기 경유지점은 하나 또는 복수일 수 있으며 개수 및 순서에 제한은 없다.
- [110] 또한, 복수의 세부코드의 일 실시예로, 복수의 세부코드는 제1코드 및 제2코드를 포함할 수 있고, 코드생성부(262)는 세부코드 생성 함수로 제1함수와 제2함수를 포함하여, 제1코드 및 제2코드를 생성한다. 제1코드와 제2코드는 서버(30) 내에서 사용자 식별 정보(UID)의 저장공간을 탐색하기 위한 상관관계를 가지나, 가상보안코드 생성 장치(20)는 보안성을 높이기 위해 제1코드를 생성하는 제1함수와 제2코드를 생성하는 제2함수를 세부코드 생성 함수로 포함할 뿐, 제1코드와 제2코드의 상관관계에 대한 데이터를 포함하지 않을 수 있다.
- [111] 제1코드와 제2코드의 상관관계의 구체적인 예로, 제1코드와 제2코드는 사용자 식별 정보(UID)의 저장공간을 탐색하기 위한 각각의 역할을 수행할 수 있다. 즉, 제1코드는 상기 경유지점에 대한 정보를 포함하고, 제2코드는 상기 경유지점으로부터 사용자 식별 정보의 저장공간에 도달할 수 있는 연산에 필요한 정보를 포함할 수 있다.
- [112] 한편, 본 발명의 일 실시예로 제1코드는 제1카운트를 기반으로 생성되며, 제2코드는 제2카운트를 기반으로 생성될 수 있다. 이때, 제1카운트는 서버(30)에서 가상보안코드 생성 함수가 구동된 최초시점으로부터 가상보안코드가 생성된 시점까지 경과된 단위 카운트의 개수이고, 제2카운트는 사용자의 사용자 식별 정보(UID)가 서버(30)에 등록된 시점 또는 사용자의 스마트 카드 장치(10)가 발급된 후 가상보안코드 생성 장치(20)를 통해 서버(30)에 등록된 시점으로부터 경과된 단위 카운트 개수를 포함할 수 있다.
- [113] 즉, 제1코드를 생성하는 제1함수는 제1카운트에 대응되는 특정한 코드값을 제공하는 함수이고, 제2코드를 생성하는 제2함수는 제2카운트에 대응되는 특정한 코드값을 제공하는 함수이다.

- [114] 이를 통해, 가상보안코드의 생성시기 및 사용자와 무관하게, 동일한 가상 보안 코드가 중복되어 생성되지 않도록 할 수 있다. 예를 들어, 제1코드는 서버(300) 내에서 제1함수가 구동되는 초기시점으로부터 각 카운트마다 매칭된 코드 중에서 어느 하나의 코드값[예를 들어, 가상보안코드의 생성이 요청된 시점(또는 카운트)에 대응되는 코드값]으로 설정되고, 가상보안코드 생성 장치(20)는 동일한 사용자에서 가상보안코드의 생성 시기마다 다른 코드값을 가지는 제1코드를 생성한다.
- [115] 또한, 동일한 시점의 경우에도 가상보안코드 생성 장치(20)마다 항상 상이한 제2카운트 값을 가지게 되어, 가상보안코드 생성 장치(20)는 사용자마다 동일 시점에 항상 상이한 제2코드를 생성한다. 즉, 제1코드는 각 카운트마다 상이한 코드값이 되고, 제2코드는 동일시점에 각 사용자의 가상보안코드 생성 장치(20)에 설치된 앱카드 애플리케이션마다 상이한 코드값을 가지게 되어서, 결과적으로 제1코드와 제2코드가 결합된 가상보안코드(OTAC)는 사용자 및 가상보안코드 생성요청시기와 관계없이 항상 동일하지 않거나 또는 중복되지 않는 코드값으로 출력되는 것이다.
- [116] 또한, 다른 일실시예로, 상기 가상보안코드 생성 함수는, M 개 문자로 N 자리의 상기 제1코드 또는 상기 제2코드를 생성할 수 있고, 이 경우 상기 가상보안코드 생성 함수는 상이한 MN 개의 코드가 단위카운트마다 순차적으로 변경되는 제1코드 또는 제2코드를 각각 제공하는 제1함수 및 제2함수를 포함한다. 즉, 제1함수 또는 제2함수는 MN 개의 코드가 카운트 증가에 따라 중복되지 않게 생성하는 함수로서, 특정한 시점에 대응하는 카운트에 MN 개의 코드 중에 특정한 하나를 제1코드 또는 제2코드로 생성한다. 이를 통해, 가상보안코드 생성 장치(20)는 MN 카운트(즉, MN 개의 카운트에 대응하는 시간길이) 내에 동일한 제1코드 또는 제2코드를 중복 생성하지 않고, 단위카운트마다 새로운 세부코드(즉, 제1코드 또는 제2코드)를 생성하여, 단위카운트마다 새로운 가상보안코드(OTAC)를 생성한다.
- [117] 구체적으로, 상기 가상보안코드 생성 함수는, M 개 문자로 N 자리의 상기 제1코드 또는 상기 제2코드를 생성함에 따라 MN 개의 코드를 제1코드 또는 제2코드로 이용하는 경우, 제1코드 또는 제2코드를 세부코드 생성 함수가 구동되는 초기시점으로부터 각 카운트마다 매칭한다.
- [118] 예를 들어, 단위카운트를 1초로 설정하는 경우, 세부코드 생성 함수가 최초 구동된 시점에서부터 매초에 상이한 MN 개의 코드를 매칭한다. 그리고, 특정한 세부코드 생성 함수를 이용하는 주기 또는 가상보안코드 생성 장치(20) 내에 가상보안코드의 생성을 위한 프로그램 또는 애플리케이션의 사용주기를 MN 카운트에 해당하는 시간 길이(예를 들어, 1카운트가 1초인 경우, MN 초)보다 짧은 시간길이를 설정하면, 제1코드 또는 제2코드는 사용주기 동안에는 서로 동일한 코드로 중복 생성되지 않는다. 즉, 시간이 흐름에 따라 카운트가 증가할 때, 사용자가 특정시점에 가상보안코드를 생성하는 경우, 가상보안코드 생성

장치(20)는 특정시점에 대응되는 카운트에 매칭된 코드값을 제1코드 또는 제2코드로 생성할 수 있는 것이다.

- [119] 또한, 복수의 세부코드를 결합하여 하나의 가상보안코드(OTAC)를 생성하는 방식으로는 다양한 방식이 적용될 수 있다. 상기 세부코드 결합 함수의 일 예로, 세부코드 결합 함수는 M자리의 제1코드와 N자리의 제2코드를 번갈아 배치하는 방식으로 가상보안코드를 생성할 수 있다.
- [120] 또한, 다른 일 예로, 세부코드결합함수는 제1코드 뒤에 제2코드를 결합하는 방식으로 가상보안코드를 생성할 수도 있다. 가상보안코드에 포함되는 세부코드의 개수가 늘어남에 따라 이에 따른 가상보안코드도 중복되지 않게 다양하게 생성될 수 있다. 코드생성부(262)는 하나 이상의 세부코드를 조합하여 가상보안코드를 생성하는 역할을 수행한다.
- [121] 한편, 본 발명의 가상보안코드 생성 장치에 의해 수행되는 가상보안코드 생성 방법은 상기 가상보안코드를 서버로 송신하여 사용자 인증을 요청하는 단계를 더 포함할 수 있다.
- [122] 상기 서버(30)는, 상기 가상보안코드를 기반으로 사용자 식별 정보의 저장 위치를 탐색함으로써 상기 사용자 식별 정보를 추출하고, 상기 추출된 사용자 식별 정보를 기반으로 사용자 인증을 수행할 수 있다.
- [123] 여기서, 상기 가상보안코드, 복수의 세부코드를 포함하고, 상기 복수의 세부코드는, 상기 사용자 식별 정보의 저장 위치 탐색의 시작지점을 설정하는 제1 코드 및 기 설정된 탐색방식에 따라, 상기 시작지점으로부터 상기 사용자 식별 정보의 저장위치로의 탐색경로를 설정하는 제2 코드를 포함할 수 있다.
- [124] 이하에서는, 서버(30)에서의 가상보안코드를 검증하고, 상기 검증된 가상보안코드를 기반으로 사용자를 인증하는 방법에 대하여 설명한다.
- [125] 본 발명의 일 실시예로, 서버(30)가 상기 가상보안코드 생성 장치(20)로부터 상기 가상보안코드를 수신하면, 상기 가상보안코드를 수신한 시간 데이터 및 상기 가상보안코드의 시간 데이터를 비교하여 상기 가상보안코드를 검증할 수 있다.
- [126] 구체적으로, 서버(30)에서 가상보안코드 생성 장치(20)를 통해 전달된 가상보안코드가 정상적으로 생성된 것인지를 검증한다. 즉, 서버(30)는 가상보안코드를 수신한 후 서버(30)에 저장된 정보(즉, 가상보안코드 생성 함수 및 시드 데이터)를 바탕으로 상기 수신한 가상보안코드가 금융 거래 요청 시점에 정상적으로 생성된 것인지를 확인하여 가상보안코드의 정상 여부를 판단한다. 예를 들어, 서버(30)(예를 들어, 금융사서버)는 가상보안코드 생성 함수(즉, OTP함수)를 가상보안코드를 수신한 카운트로부터 특정범위 내의 카운트를 입력하여 산출된 OTP번호 중에 가상보안코드와 일치하는 값이 있는지 여부를 확인한다. 서버(30)는 가상보안코드에 가상보안코드 생성 함수의 역함수를 적용하여 가상보안코드가 생성된 시점에 상응하는 카운트를 찾아낸다. 가상보안코드의 전송시간이나 딜레이에 의해 가상보안코드 생성 장치(20)에서

가상보안코드가 생성된 시점과 서버(30)가 가상보안코드를 수신한 시점의 차이가 존재함에 따라 서버(30)가 가상보안코드를 수신한 카운트와 가상보안코드에 해당하는 OTP번호를 생성한 카운트가 일치하지 않을 수도 있으므로, 서버(30)는 가상보안코드를 수신한 카운트로부터 오차범위를 허용한다.

- [127] 한편, 본 발명의 일 실시예로 서버(30)는 상기 가상보안코드를 기반으로 사용자 식별 정보의 저장 위치를 탐색하여 상기 사용자 식별 정보를 추출하고, 상기 추출한 사용자 식별 정보를 기반으로 사용자 인증을 수행할 수 있다.
- [128] 이때, 상술한 바와 같이 상기 가상보안코드는 복수의 세부코드를 포함하는데, 복수의 세부코드는, 사용자 식별 정보의 저장 위치 탐색의 시작지점을 설정하는 제1코드와 기 설정된 탐색방식에 따라, 상기 시작지점으로부터 상기 사용자 식별 정보의 저장위치로의 탐색경로를 설정하는 제2코드로 구성될 수 있다.
- [129] 한편, 제1코드 및 제2코드의 구체적인 예로, 제1코드에 대응되는 코드값(제1코드값)은 가상보안코드 생성 함수 구동시점을 기준으로 현재시점에 대응되는 카운트에서 OTP코드에 제1가상보안코드값을 더한 값일 수 있다. 제1코드값은 실제코드 탐색 과정에서 경유지점의 역할을 한다. 제2코드에 대응되는 코드값(제2코드값)은 상기 제1코드값에서 사용자 식별 정보(예를 들어, UID)의 저장 위치값을 뺀 값일 수 있다. 제2코드값은 경유지점(제1코드값)으로부터 사용자 식별 정보의 저장 위치값까지의 카운트이다.
- [130] 즉, 가상보안코드 생성 장치(20)가 생성하는 제1코드 및 제2코드의 일 실시예는 다음과 같다.
- [131] 제1코드 = 현재시점 카운트 + OTP코드(제1가상보안코드)
- [132] 제2코드 = 제1코드 - 실제코드의 저장위치값
- [133] 상술한 바와 같이 최종 가상보안코드는 OTP함수에 의해 생성된 제1가상보안코드, 제1코드 및 제2 코드로 구성될 수 있다. 이때 제1가상보안코드는 OTP함수에 의해 생성되는 코드로서, 매 시점 다르게 생성되는 코드이다. 따라서, 세부코드는 가상보안코드의 생성시점에 따라 다르게 생성되므로 중복되어 생성되는 것을 방지할 수 있고, 보안성을 강화시키는 효과가 있다.
- [134] 제1코드 및 제2코드의 구체적인 다른 예로, 제1코드에 대응되는 코드값(제1코드값)은 OTP코드값에 사용자 식별정보(UID)를 더한 값이고, 제2코드에 대응되는 코드값(제2코드값)은 OTP코드값일 수 있다. 이때, 사용자 식별 정보(UID)의 값은 사용자 또는 가상보안코드 생성 장치(20)에 대하여 특정 시점(예를 들어, 카드 제조시점, 카드 등록시점 등)에 부여되어, 각 사용자 또는 가상보안코드 생성 장치(20)를 식별할 수 있는 코드값이다.
- [135] 즉, 가상보안코드 생성 장치(20)가 생성하는 제1코드의 다른 실시예는 다음과 같다. 이때, 가상보안코드는 제1 가상보안코드와 제1 코드를 기초로 생성된다.
- [136] 제1코드 = OTP코드(제1가상보안코드) + UID

- [137] 이하에서는, 사용자가 카드 발급을 신청하고, 발급된 카드를 서버에 등록하는 방법에 대해 설명하도록 한다.
- [138] 사용자의 요청에 따라 카드 발급 시, 상기 카드가 발급될 상기 사용자에게 대해 상기 카드의 카드 번호, 상기 시드 데이터, 상기 유저 키 값 및 상기 칩 고유 값이 할당될 수 있다.
- [139] 보다 구체적으로, 사용자는 가상보안코드 생성 장치(20)에 내의 애플리케이션을 통해 카드 발급을 신청한다. 서버(30)는 카드 발급 신청을 수신하면, 사용자에게 발급할 카드의 카드 번호, 시드 데이터 및 유저 키 값을 할당하여 상기 사용자의 사용자 식별 정보와 맵핑하여 저장한다. 즉, 카드 번호, 시드 데이터 및 유저 키 값은 서버에서 설정되는 값이다.
- [140] 서버(30)는 카드 발급 대행사로 카드 발급을 요청하면서, 상기 카드 번호, 상기 시드 데이터 및 상기 유저 키 값을 전달한다.
- [141] 카드 발급 대행사는 발급될 카드에 수신된 상기 카드 번호, 상기 시드 데이터 및 상기 유저 키 값을 주입하여 카드 발급을 완료한다. 이때, 카드 발급 대행사는 서버(30)로 칩 고유 값을 전달하고, 서버(30)는 전달된 칩 고유 값을 상기 사용자 식별 정보에 추가적으로 맵핑하여 저장한다. 이때, 칩 고유 값은 카드 내에 포함된 칩이 제작될 때 칩에 부여된 값으로, 서버(30)가 설정한 값이 아니기 때문에, 서버(30)는 카드 발급 대행사로부터 해당 값을 따로 제공받아야 한다.
- [142] 이후 사용자는 가상보안코드 생성 장치(20) 내의 애플리케이션을 통해 발급받은 카드의 등록을 요청한다. 서버(30)는 요청에 따라 상기 사용자의 식별 정보에 맵핑되어 저장된 데이터들 중 유저 키 값 및 칩 고유 값을 상기 가상보안코드 생성 장치(20)로 전달한다. 가상보안코드 생성 장치(20)는 수신된 유저 키 값 및 칩 고유 값을 저장하고, 이후 가상보안코드 생성 시에 사용할 수 있다. 그러나 이에 제한되지 않고, 카드 등록 시에 유저 키 값 및 칩 고유 값뿐만 아니라 다른 데이터도 서버(30)로부터 전달되어 가상보안코드 생성 장치(20)에 저장될 수 있다.
- [143] 이렇게 사용자로부터 카드 등록이 요청되면, 서버(30)는 등록이 요청된 시점에 해당 사용자 또는 가상보안코드 생성 장치(20)에 대한 가상보안코드 생성 함수의 구동을 시작하고, 등록이 요청된 시점에 해당하는 카운트(지점)에 사용자 식별 정보를 저장할 수 있다. 이에 따라, 서버(30)는 이후 가상보안코드 생성 장치(20)로부터 수신되는 가상보안코드로부터 사용자 식별 정보를 탐색함으로써 사용자 인증을 수행할 수 있게 된다.
- [144] 상기에서는, 칩 고유 값이 카드 등록 전에, 카드 발급 대행사로부터 전달받아 서버(30)에 저장되는 것으로 설명하였지만, 실시예에 따라, 칩 고유 값은 카드 등록 시에 스마트 카드 장치(10)를 통해 전달되어 서버(30)에 저장될 수도 있다.
- [145] 상기 칩 고유 값은, 상기 사용자가 가상보안코드 생성 장치(20) 내의 애플리케이션에 상기 카드를 등록할 때, 상기 카드 태깅을 통해 상기 카드로부터 수신되어 상기 애플리케이션에 저장되고, 상기 가상보안코드 생성 장치(20)를

통해 서버(30)로 전송되어, 상기 서버(30)에서 사용자 식별 정보와 맵핑되어 저장될 수 있다.

- [146] 이상에서 기술한 본 발명의 일 실시예에 따른 방법은, 하드웨어인 컴퓨터와 결합되어 실행되기 위해 프로그램으로 구현되어 컴퓨터 판독 가능한 기록 매체에 저장될 수 있다.
- [147] 상기 기술한 프로그램은, 상기 컴퓨터가 프로그램을 읽어 들여 프로그램으로 구현된 상기 방법들을 실행시키기 위하여, 상기 컴퓨터의 프로세서(CPU)가 상기 컴퓨터의 장치 인터페이스를 통해 읽힐 수 있는 C, C++, JAVA, 기계어 등의 컴퓨터 언어로 코드화된 코드(Code)를 포함할 수 있다. 이러한 코드는 상기 방법들을 실행하는 필요한 기능들을 정의한 함수 등과 관련된 기능적인 코드(Functional Code)를 포함할 수 있고, 상기 기능들을 상기 컴퓨터의 프로세서가 소정의 절차대로 실행시키는데 필요한 실행 절차 관련 제어 코드를 포함할 수 있다. 또한, 이러한 코드는 상기 기능들을 상기 컴퓨터의 프로세서가 실행시키는데 필요한 추가 정보나 미디어가 상기 컴퓨터의 내부 또는 외부 메모리의 어느 위치(주소 번지)에서 참조되어야 하는지에 대한 메모리 참조관련 코드를 더 포함할 수 있다. 또한, 상기 컴퓨터의 프로세서가 상기 기능들을 실행시키기 위하여 원격(Remote)에 있는 어떠한 다른 컴퓨터나 서버 등과 통신이 필요한 경우, 코드는 상기 컴퓨터의 통신 모듈을 이용하여 원격에 있는 어떠한 다른 컴퓨터나 서버 등과 어떻게 통신해야 하는지, 통신 시 어떠한 정보나 미디어를 송수신해야 하는지 등에 대한 통신 관련 코드를 더 포함할 수 있다.
- [148] 본 발명의 실시예와 관련하여 설명된 방법 또는 알고리즘의 단계들은 하드웨어로 직접 구현되거나, 하드웨어에 의해 실행되는 소프트웨어 모듈로 구현되거나, 또는 이들의 결합에 의해 구현될 수 있다. 소프트웨어 모듈은 RAM(Random Access Memory), ROM(Read Only Memory), EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM), 플래시 메모리(Flash Memory), 하드 디스크, 착탈형 디스크, CD-ROM, 또는 본 발명이 속하는 기술 분야에서 잘 알려진 임의의 형태의 컴퓨터 판독가능 기록매체에 상주할 수도 있다.
- [149] 이상, 첨부된 도면을 참조로 하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야의 통상의 기술자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며, 제한적이 아닌 것으로 이해해야만 한다.