

명세서

발명의 명칭: 스마트 카드 장치, 인증용가상코드 생성 장치, 이를 이용한 인증용가상코드 생성 방법 및 인증용가상코드 검증 서버 기술분야

- [1] 본 발명은 스마트 카드 장치, 인증용가상코드 생성 장치, 이를 이용한 인증용가상코드 생성 방법 및 인증용가상코드 검증 서버에 관한 것이다.

배경기술

- [2] 코드 형태데이터는 많은 영역에서 이용되고 있다. 결제 시에 이용되는 카드번호, 계좌번호뿐만 아니라 사용자 식별을 위한 IPIN번호, 주민등록번호 등이 코드형태 데이터인인증용가상코드 생성 장치다.
- [3] 그러나 이러한 코드데이터를 이용하는 과정에서 유출되는 사고가 많이 발생한다. 카드번호의 경우, 카드표면에 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 데이터가 유출되지 않도록 하여 보안을 높이는 방안이 필요하다.

발명의 상세한 설명

기술적 과제

- [7] 본 발명이 해결하고자 하는 과제는 스마트 카드 장치, 인증용가상코드 생성 장치, 이를 이용한 인증용가상코드 생성 방법 및 인증용가상코드 검증 서버를 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 인증용가상코드 생성 장치에 의해 수행되는 인증용가상코드 생성 방법은, IC 칩이 내장된 카드 태깅 시, 상기 카드로 시간 데이터를 송신하는 단계, 상기 시간 데이터를 기반으로

생성된 1차 인증용가상코드를 상기 카드로부터 수신하는 단계, 상기 1차 인증용가상코드를 이용하여 2차 인증용가상코드를 생성하는 단계, 상기 1차 인증용가상코드 및 상기 2차 인증용가상코드 중 적어도 하나를 서버로 송신하는 단계 및 상기 서버가 상기 적어도 하나에 대한 검증을 수행하도록 요청하는 단계를 포함한다.

- [10] 본 발명에서, 상기 1차 인증용가상코드는, 복수의 코드를 포함하고, 상기 복수의 코드 중 제1 코드는, 상기 시간 데이터 및 제1 OTP를 기반으로 생성되고, 상기 복수의 코드 중 제2 코드는, 상기 제1 코드에서 상기 카드의 식별 정보인 제1 UID (user identification)를 제외하여 생성될 수 있다.
- [11] 본 발명에서, 상기 2차 인증용가상코드를 생성 단계는, 상기 제1 코드에서 상기 인증용가상코드 생성 장치의 식별 정보인 제2 UID를 제외하여 제3 코드를 생성하고, 상기 제1 코드, 상기 제2 코드 및 상기 제3 코드를 결합하여 상기 2차 인증용가상코드를 생성할 수 있다.
- [12] 본 발명에서, 상기 카드는, 상기 제1 코드 및 상기 제2 코드를 기반으로 검증이 수행되고, 상기 인증용가상코드 생성 장치는, 상기 제1 코드 및 상기 제3 코드를 기반으로 검증이 수행될 수 있다.
- [13] 본 발명에서, 상기 2차 인증용가상코드를 생성 단계는, 상기 1차 인증용가상코드를 기반으로 제2 OTP를 생성하고, 상기 제2 OTP 및 상기 인증용가상코드 생성 장치의 식별 정보인 제2 UID를 기반으로 상기 2차 인증용가상코드를 생성할 수 있다.
- [14] 본 발명에서, 상기 2차 인증용가상코드는, 상기 2차 인증용가상코드에 포함된 상기 제2 OTP 및 검증용 제2 OTP의 비교를 통해 검증되고, 상기 검증용 제2 OTP는, 상기 제2 OTP 생성 시에 이용된 시드 데이터와 동일한 시드 데이터를 기반으로 상기 서버에 의해 생성된 것일 수 있다.
- [15] 본 발명에서, 상기 1차 인증용가상코드는, 오프라인 출입통제 및 온라인 로그인 시 사용자 인증용으로 이용될 수 있다.
- [16] 본 발명에서, 상기 2차 인증용가상코드는, 금융 결제 시 사용자 인증용으로 이용될 수 있다.
- [17] 본 발명에서, 상기 시간 데이터는, APDU(Application Protocol Data Unit) 명령어와 결합된 형태일 수 있다.
- [18] 상술한 과제를 해결하기 위한 본 발명의 다른 면에 따른 스마트 카드 장치는, 카드 태깅을 통해 인증용가상코드 생성 장치로부터 시간 데이터를 수신하는 NFC 모듈 및 상기 수신된 시간 데이터를 기반으로 1차 인증용가상코드를 생성하는 IC 모듈을 포함하고, 상기 1차 인증용 가상코드는 자체적으로 송신되어 사용자 인증에 이용되거나, 2차 인증용 가상코드 생성에 이용되는 것이고, 상기 2차 인증용가상코드는, 상기 1차 인증용가상코드를 이용하여 상기 인증용가상코드 생성 장치에 의해 생성되는 것이고, 상기 1차 인증용가상코드 및 상기 2차 인증용가상코드 중 적어도 하나는, 서버에 의해 검증이 수행되도록

- 상기 인증용가상코드 생성 장치에 의해 상기 서버로 전송된다.
- [19] 상술한 과제를 해결하기 위한 본 발명의 또 다른 면에 따른 인증용가상코드 생성 장치는, IC 칩이 내장된 카드 태깅 시, 상기 카드로 시간 데이터를 송신하고, 상기 시간 데이터를 기반으로 생성된 1차 인증용가상코드를 상기 카드로부터 수신하는 통신부, 상기 1차 인증용가상코드를 이용하여 2차 인증용가상코드를 생성하는 코드생성부 및 상기 통신부를 통해 상기 1차 인증용가상코드 및 상기 2차 인증용가상코드 중 적어도 하나를 서버로 송신하여, 상기 서버가 상기 적어도 하나에 대한 검증을 수행하도록 요청하는 검증요청부를 포함한다.
- [20] 상술한 과제를 해결하기 위한 본 발명의 또 다른 면에 따른 서버에 의해 수행되는 인증용가상코드 검증 방법에 있어서, 인증용가상코드 생성 장치로부터 1차 인증용가상코드 및 2차 인증용가상코드 중 적어도 하나를 수신하는 단계 및 상기 1차 인증용가상코드 및 상기 2차 인증용가상코드 중 적어도 하나에 대한 검증을 수행하는 단계를 포함하고, 상기 2차 인증용가상코드가 복수의 코드를 포함하는 경우, 상기 검증 수행 단계는, 상기 복수의 코드 중 제1 코드 및 제2 코드를 기반으로 카드의 식별 정보인 제1 UID (user identification)를 추출하여 상기 카드에 대한 검증을 수행하고, 상기 복수의 코드 중 상기 제1 코드 및 제3 코드를 기반으로 상기 인증용가상코드 생성 장치의 식별 정보인 제2 UID를 추출하여 상기 인증용가상코드 생성 장치에 대한 검증을 수행한다.
- [21] 본 발명에서, 상기 2차 인증용가상코드가 제2 OTP 및 상기 제2 UID를 포함하는 경우, 상기 검증 수행 단계는, 상기 제2 OTP 생성 시에 이용된 시드 데이터와 동일한 시드 데이터를 기반으로 검증용 제2 OTP를 생성하고, 상기 2차 인증용가상코드에 포함된 상기 제2 OTP 및 상기 검증용 제2 OTP를 비교하고, 상기 제2 OTP 및 상기 검증용 제2 OTP가 동일하면 상기 카드 및 상기 인증용가상코드 생성 장치에 대한 검증을 완료할 수 있다.
- [22] 본 발명에서, 상기 1차 인증용가상코드가 수신된 경우, 상기 검증 수행 단계는, 제1 검증 알고리즘을 이용하여 상기 1차 인증용가상코드를 기반으로 카드의 식별 정보인 제1 UID (user identification)를 추출하여 상기 카드에 대한 검증을 수행할 수 있다.
- [23] 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**
- [24] 본 발명에 따르면, 카드 태깅 시에 인증용가상코드 생성 장치가 스마트 카드 장치로 시간 데이터를 제공함으로써, 별도의 OTP 장치 없이도 NFC 방식을 기초로 획득한 시간 데이터를 이용하여 사용자 인증에 필요한 가상보안코드를 생성할 수 있다.

- [25] 인증용가상코드 생성 장치에 스마트 카드 장치를 태깅할 때, 두 개의 장치 간 데이터가 송수신될 때 해당 데이터의 탈취를 방어하기 위해, 스마트 카드 장치에서 생성된 1차 인증용가상코드를 재가공해 인증용가상코드 생성 장치에서 2차 인증용가상코드를 새롭게 생성할 수 있다.
- [26] 또한, 오프라인 출입통제 또는 온라인 로그인 상황에서는 1차 인증용가상코드 검증을 통해 사용자 인증을 수행하고, 금융 결제 상황에서는 1차 인증용가상코드를 이용하여 생성된 2차 인증용가상코드의 검증을 통해 사용자 인증을 수행함으로써, 상황에 따라 보안 수준을 달리할 수 있다.
- [27] 또한, 스마트 카드 장치가 오프라인 출입통제 상황과 금융 결제 상황 모두에 적용될 수 있기 때문에, 금융카드(개인카드 또는 법인카드)를 회사의 출입카드로도 확장하여 활용할 수 있다.
- [28] 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

- [29] 도 1은 본 발명에 따른 인증용가상코드 기반 사용자 인증 시스템의 구성도이다.
- [30] 도 2는 본 발명에 따른 스마트 카드 장치의 개략적인 구성도이다.
- [31] 도 3은 본 발명에 따른 인증용가상코드 생성 장치의 개략적인 구성도이다.
- [32] 도 4는 본 발명에 따른 인증용가상코드 생성 장치에 의해 수행되는 인증용가상코드 생성 방법의 순서도이다.
- [33] 도 5는 본 발명에 따른 시간 데이터를 설명하기 위한 도면이다.
- [34] 도 6은 본 발명에 따른 1차 인증용가상코드 검증을 설명하기 위한 도면이다.
- [35] 도 7은 본 발명에 따른 2차 인증용가상코드 검증을 설명하기 위한 도면이다.
- [36] 도 8은 본 발명에 따른 스마트 카드 장치에 의해 수행되는 인증용가상코드 생성 방법의 순서도이다.

발명의 실시를 위한 형태

- [37] 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.
- [38] 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.

- [39] 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.
- [40] 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.
- [41] 본 명세서에서 '문자'는 코드를 구성하는 구성요소로서, 대문자알파벳, 소문자알파벳, 숫자 및 특수문자 등의 전부 또는 일부를 포함한다.
- [42] 본 명세서에서 '코드'는 문자가 나열된 문자열을 의미한다.
- [43] 본 명세서에서 'OTP(One Time Password)'는 사용자 인증을 위해 임시적으로 생성되며 단위시간마다 변경되는 랜덤코드로서, 문자로 이루어진 특정한 자릿수의 코드를 포함할 수 있다.
- [44] 본 명세서에서 '인증용가상코드'는 인증용가상코드생성수단에서 생성되는 코드로서, 인증용가상코드검증수단에서 검증되는 코드를 의미한다. 즉, '인증용가상코드'는 검증이 수행될 수 있도록 단위카운트마다 임시적으로 부여된 가상의 코드를 의미한다. 여기서, 인증용가상코드생성수단은 실시예에 따라 스마트 카드 장치가 될 수도 있고, 인증용가상코드 생성 장치가 될 수도 있지만, 이에 제한되지는 않는다.
- [45] 본 명세서에서 '세부코드'는 인증용가상코드에 포함되는 일부코드를 의미한다.
- [46] 본 명세서에서 '단위카운트'는 특정한 시간간격으로 설정되어, 시간간격이 경과됨에 따라 변경되는 것으로 정의된 단위이다. 예를 들어, 1카운트는 특정한 시간간격(예를 들어, 1.5초)으로 설정되어 사용될 수 있다.
- [47] 본 명세서에서 '인증용가상코드생성함수'는 인증용가상코드를 생성하는데 이용되는 함수를 의미한다.
- [48] 본 명세서에서, '사용자'는 스마트 카드 장치를 이용하여 보안이 필요한 특정 공간(오프라인 또는 온라인 공간)에 접근하거나, 또는 스마트 카드 장치를 이용하여 금융 결제를 수행하는 사용자일 수 있지만, 이에 제한되는 것은

아니다.

- [49] 본 명세서에서 "UID(user identification)"는 사용자를 식별하기 위해 사용자별로 중복되지 않게 부여되는 고유한 코드 형태의 값을 의미한다.
- [50] 본 명세서에서 "시간 데이터"는 현재 시점의 시간 데이터를 의미한다. 즉, 인증용가상코드 생성 및 검증에 사용되는 시간 데이터는 모두 동일 시점의 시간 데이터를 의미할 수 있다.
- [51] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세하게 설명한다.
- [52] 도 1은 본 발명에 따른 인증용가상코드 기반 사용자 인증 시스템의 구성도이다.
- [53] 도 2는 본 발명에 따른 스마트 카드 장치의 개략적인 구성도이다.
- [54] 도 3은 본 발명에 따른 인증용가상코드 생성 장치의 개략적인 구성도이다.
- [55] 도 4는 본 발명에 따른 인증용가상코드 생성 장치에 의해 수행되는 인증용가상코드 생성 방법의 순서도이다.
- [56] 도 5는 본 발명에 따른 시간 데이터를 설명하기 위한 도면이다.
- [57] 도 6은 본 발명에 따른 1차 인증용가상코드 검증을 설명하기 위한 도면이다.
- [58] 도 7은 본 발명에 따른 2차 인증용가상코드 검증을 설명하기 위한 도면이다.
- [59] 도 8은 본 발명에 따른 스마트 카드 장치에 의해 수행되는 인증용가상코드 생성 방법의 순서도이다.
- [60] 도 1을 참조하면, 인증용가상코드 기반 사용자 인증 시스템(이하, 시스템)은 관제 서버(100), 스마트 카드 장치(10), 인증용가상코드 생성 장치(20) 및 서버(30)를 포함한다. 여기서, 시스템은 도 1에 도시된 구성요소보다 더 적은 수의 구성요소나 더 많은 구성요소를 포함할 수 있다.
- [61] 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.
- [62] 실시예에 따라, 스마트 카드 장치(10)는 출입통제용 카드일 수 있고, 금융 결제용 카드(예를 들어, 신용카드, 체크카드, 현금카드, 법인카드 등)일 수 있다.
- [63] 구체적으로, 스마트 카드 장치(10)가 출입통제용 출입카드인 경우, 스마트 카드 장치(10)는 사용자가 오프라인 상에서 보안이 필요한 특정 공간으로 출입할 때 사용되거나, 온라인 상에서 특정 웹사이트 또는 앱에 로그인할 때 사용될 수 있다. 스마트 카드 장치(10)가 금융 결제용 카드인 경우, 스마트 카드 장치(10)는 사용자가 금융거래를 진행할 때 사용될 수 있다. 그러나, 카드의 형태, 종류 및 목적은 상술한 바에 제한되지 않는다. 스마트 카드 장치(10)에 대한 상세한 설명은 후술한다.
- [64] 인증용가상코드 생성 장치(20)는 출입통제 장치(예를 들어, 게이트 리더기, 도어락 등)일 수 있고, 사용자가 사용하는 사용자 단말기일 수 있다. 이때, 사용자 단말기는 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 디바이스(wearable device)등을 포함하며 이에 한정되는 것은 아니다. 인증용가상코드 생성 장치(20)에 대한 상세한 설명은 후술한다.

- [65] 서버(30)는 인증용가상코드검증수단으로서, 인증용가상코드 생성 장치(20)로부터 수신된 인증용가상코드에 대한 검증을 수행한다. 그러나, 이에 제한되지 않고, 실시예에 따라 서버(30 대신 인증용가상코드 생성 장치(20)가 인증용가상코드를 검증할 수도 있다.
- [66] 이때, 서버(30)는 인증용가상코드 생성 장치(20)와 통신하는 보안 관련 서버 또는 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.
- [67] 도 1에 도시된 바와 같이, 스마트 카드 장치(10), 인증용가상코드 생성 장치(20) 및 서버(30)는 통신망을 통해 서로 각종 데이터, 신호 또는 정보를 송수신할 수 있다.
- [68] 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.
- [69] 한편, 통신망은 상기에 제시된 통신방식에 한정되는 것은 아니며, 상술한 통신방식 이외에도 기타 널리 공지되었거나 향후 개발될 모든 형태의 통신 방식을 포함할 수 있다.
- [70] 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.
- [71] NFC(Narrow Frequency Communication) 모듈(12)(즉, NFC 칩)은 통신 모듈로서, 인증용가상코드 생성 장치(20)와 각종 데이터를 송수신할 수 있다. 여기서, NFC 모듈(12)은 애플릿(applet) 형태로 형성될 수 있지만, 이제 제한되는 것은 아니다. NFC 모듈(12)은 스마트 카드 장치(10)가 인증용가상코드 생성 장치(20)에 태그(tag)되면, 인증용가상코드 생성 장치(20)로부터 시간 데이터를 수신할 수 있다.
- [72] IC 모듈(14)(즉, IC 칩)은 1차 인증용가상코드 생성할 수 있다. 여기서, IC 모듈(14)은 애플릿(applet) 형태로 형성될 수 있지만, 이제 제한되는 것은 아니다.
- [73] IC 모듈(14)은 수신된 시간 데이터를 이용하여 1차 인증용가상코드를 생성할 수 있다. 구체적으로, IC 모듈(14)은 수신된 시간 데이터뿐만 아니라 메모리(미도시)에 저장된 카드 데이터 및 인증용가상코드생성함수를 이용하여 1차 인증용가상코드를 생성할 수 있다.

- [74] 여기서, 카드 데이터는 해당 스마트 카드 장치(10)의 발급을 신청한 사용자의 사용자 식별 정보와 카드 식별 정보를 포함할 수 있다. 여기서, 상기 카드 식별 정보는, 상기 스마트 카드 장치(10)의 식별 정보인 제1 UID (user identification), 시크릿(secret), 카드번호, 시리얼넘버를 포함할 수 있으며, 이에 제한되지 않고 카드 관련 정보는 모두 포함할 수 있다. 여기서, 상기 사용자 식별 정보는 주민등록번호를 포함할 수 있으며, 이에 제한되지 않고 사용자 관련한 개인 정보는 모두 포함할 수 있다.
- [75] IC 모듈(14)에는 사용자 식별 정보 및 카드 식별 정보 이외에도 스마트 카드 장치(10)를 발급하고 관리하는 회사(예를 들어, 카드 제작 회사, 금융사, 보안 회사, 온라인 웹 또는 앱 서비스 회사 등)의 URL 주소 등이 저장될 수 있다. 예를 들어, 스마트 카드 장치(10)의 IC 모듈(14)에 특정 금융사의 URL 주소가 저장된 경우에는, 인증용가상코드 생성 장치(20)에 해당 스마트 카드 장치(10)가 태그되면, 인증용가상코드 생성 장치(20)는 상기 URL 주소를 획득할 수 있다. 이때 URL 주소는 해당 금융사의 프로그램 또는 어플리케이션의 설치 정보 또는 실행 정보에 관한 것일 수 있다.
- [76] 즉, IC 모듈(14)에는 사용자 식별 정보 및 카드 식별 정보 이외에도 다양한 정보가 저장된다. 이러한, 다양한 정보는 인증용가상코드 생성 장치(20)에 스마트 카드 장치(10)가 태그되면, 인증용가상코드 생성 장치(20)는 스마트 카드 장치(10)로부터 해당 정보를 수신하게 된다.
- [77] 스마트 카드 장치(10)는 스마트 카드 장치(10)의 전반적인 동작을 제어하는 프로세서(미도시)를 더 포함할 수 있다. 프로세서(미도시)는 위에서 살펴본 구성요소들을 통해 입력 또는 출력되는 신호, 데이터, 정보 등을 처리하거나 저장된 응용 프로그램을 구동할 수 있다. 여기서 프로세서(미도시)가 IC 모듈(14)과 구별되는 구성으로 설명하였지만, 실시예에 따라 IC 모듈(14)이 프로세서(미도시) 역할을 수행할 수 있다.
- [78] 도 3을 참조하면, 인증용가상코드 생성 장치(20)는 통신부(22), 메모리(24) 및 프로세서(26)를 포함할 수 있다. 여기서, 인증용가상코드 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 인증용가상코드 생성 장치(20)에 태그되면, 상기 통신망을 통해 상기 스마트 카드 장치(10)로 시간 데이터를 송신하고, 상기 시간 데이터를 기반으로 생성된 1차 인증용가상코드를 상기 스마트 카드 장치(10)로부터 수신할 수 있다. 이외에도, 두 장치는 태그 시에 다양한 데이터들을 서로 송수신할 수 있다.
- [80] 메모리(24)는 인증용가상코드 생성 장치(20)의 다양한 기능을 지원하는 데이터를 저장할 수 있다. 메모리(24)는 인증용가상코드 생성 장치(20)에서 구동되는 다수의 응용 프로그램(application program 또는 어플리케이션(application)), 인증용가상코드 생성 장치(20)의 동작을 위한 적어도

하나의 프로세서, 데이터들, 명령어들을 저장할 수 있다. 이러한 응용 프로그램 중 적어도 일부는, 인증용가상코드 생성 장치(20)의 기본적인 기능을 위하여 존재할 수 있다.

- [81] 프로세서(26)는 상기 응용 프로그램과 관련된 동작 외에도, 통상적으로 인증용가상코드 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, 인증용가상코드 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(164)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)에서 생성된 1차 인증용가상코드를 이용하여 2차 인증용가상코드를 생성할 수 있다.
- [85] 검증요청부(264)는 통신부(22)를 통해 상기 1차 인증용가상코드 및 상기 2차 인증용가상코드 중 적어도 하나를 서버로 송신하여, 상기 서버가 상기 적어도 하나에 대한 검증을 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, 인증용가상코드 생성 장치(20)에 의해 수행되는 인증용가상코드 기반 사용자 인증 방법에 대해 상세히 설명하도록 한다.
- [88] 도 4를 참조하면, 인증용가상코드 생성 장치(20)의 통신부(22)는 IC 칩이 내장된 카드 태깅 시, 상기 스마트 카드 장치(10)로 시간 데이터를 송신할 수 있다(S110).
- [89] 스마트 카드 장치(10)는 자체적으로 시간 데이터를 획득할 수 없기 때문에, 태깅을 통해 인증용가상코드 생성 장치(20)로부터 시간 데이터를 제공받을 수 있다.
- [90] 이때, 상기 시간 데이터는, APDU(Application Protocol Data Unit) 명령어와 결합된 형태일 수 있다. 도 5를 참조하면, 시간 데이터는 APDU 명령어 뒤에 결합된 형태로 스마트 카드 장치(10)로 전달될 수 있다. 그러나 결합 형태는 이에 제한되는 것은 아니다.

- [91] 인증용가상코드 생성 장치(20)의 통신부(22)는 상기 시간 데이터를 기반으로 생성된 1차 인증용가상코드를 상기 스마트 카드 장치(10)로부터 수신할 수 있다(S120).
- [92] 즉, 스마트 카드 장치(10)는 시간 데이터를 수신하여, 수신된 시간 데이터와 카드 내에 저장되어 있던 카드 데이터(예를 들어, 시크릿, 제1 UID)를 함께 이용하여 1차 인증용가상코드를 생성하고, 이를 인증용가상코드 생성 장치(20)로 전달할 수 있다.
- [93] 상기 1차 인증용가상코드는, 제1 코드 및 제2 코드를 포함할 수 있다. 여기서, 제1 코드 및 제2 코드는 상기 1차 인증용가상코드의 세부코드이며, 1차 인증용가상코드는 제1 코드 및 제2 코드 이외에도 더 많은 수의 세부코드를 포함할 수 있다.
- [94] 상기 1차 인증용가상코드의 제1 코드는 상기 시간 데이터 및 제1 OTP를 기반으로 생성될 수 있다. 먼저, 스마트 카드 장치(10)는 제1 인증용가상코드생성함수를 이용하여 카드 내에 저장되어 있던 시크릿 값과 상기 시간 데이터를 시드 데이터로 하여 제1 OTP를 생성할 수 있다. 이때, 시드 데이터는 실시예에 따라 시크릿 값 및 시간 데이터 이외의 값을 더 이용할 수도 있다.
- [95] 그런 다음, 스마트 카드 장치(10)는 제1 인증용가상코드생성함수를 이용하여 상기 수신된 시간 데이터에 생성된 제1 OTP를 더하여 제1 코드를 생성할 수 있다.
- [96] 스마트 카드 장치(10)는 제1 인증용가상코드생성함수를 이용하여 상기 제1 코드에서 상기 카드의 식별 정보인 제1 UID (user identification)를 제외하여 상기 제2 코드를 생성할 수 있다. 여기서, 제1 UID는 스마트 카드 장치(10)에 저장된 데이터로서 스마트 카드 장치(10)를 식별할 수 있는 고유 값이다.
- [97] 제1 코드 = 시간 데이터 + 제1 OTP
- [98] 제2 코드 = 제1 코드 - 제1 UID
- [99] 스마트 카드 장치(10)는 생성된 세부코드(제1 코드 및 제2 코드)를 조합하여 1차 인증용가상코드를 생성할 수 있다. 일 실시예로, 스마트 카드 장치(10)는 제1 인증용가상코드생성함수를 이용하여 복수의 세부코드를 특정한 규칙에 따라 결합함으로써 상기 1차 인증용가상코드를 생성할 수 있다. 상기 제1 인증용가상코드생성함수는 복수의 세부코드를 조합하는 규칙(즉, 세부코드결합함수)을 포함할 수 있다.
- [100] 복수의 세부코드를 결합하여 하나의 인증용가상코드를 생성하는 방식으로는 다양한 방식이 적용될 수 있다. 상기 세부코드결합함수의 일 예로, 스마트 카드 장치(10)는 M자리의 제1 코드와 N자리의 제2 코드를 번갈아 배치하는 방식으로 인증용가상코드를 생성할 수 있다. 또한, 다른 일 예로, 세부코드결합함수는 제1 코드 뒤에 제2 코드를 결합하는 함수일 수 있다. 인증용가상코드에 포함되는 세부코드가 늘어남에 따라 세부코드결합함수도 다양하게 생성될 수 있다.

- [101] 이렇게 생성된 1차 인증용가상코드는 인증용가상코드 생성 장치(20)로 송신된다.
- [102] 인증용가상코드 생성 장치(20)의 코드생성부(262)는 상기 1차 인증용가상코드를 이용하여 2차 인증용가상코드를 생성할 수 있다(S130).
- [103] 단계 S130 이전에, 인증용가상코드 생성 장치(20)의 코드생성부(262)는 상기 스마트 카드 장치(10)의 종류에 따라 2차 인증용가상코드를 생성할지의 여부를 먼저 판단할 수 있다. 보다 상세하게, 코드생성부(262)는 1차 인증용가상코드와 함께 수신된 카드 데이터를 기반으로 상기 판단 동작을 수행할 수 있다(실시예에 따라, 카드 데이터는 태깅 시에 수신될 수도 있다). 즉, 코드생성부(262)는 상기 카드 데이터를 기반으로 상기 스마트 카드 장치(10)가 출입통제용 카드인지 금융 결제용 카드인지를 판단할 수 있다. 그리고, 상기 스마트 카드 장치(10)가 출입통제용 카드인 것으로 확인되면 2차 인증용가상코드를 생성하지 않고, 상기 카드 데이터를 기반으로 상기 스마트 카드 장치(10)가 금융 결제용 카드인 것으로 확인되면 2차 인증용가상코드를 생성할 수 있다.
- [104] 실시예에 따라, 인증용가상코드 생성 장치(20)의 종류에 따라 2차 인증용가상코드 생성 여부가 결정될 수 있다. 구체적으로, 인증용가상코드 생성 장치(20)가 출입통제 장치인 경우에는 상기 판단 동작 없이 2차 인증용가상코드를 생성하지 않을 수 있다. 인증용가상코드 생성 장치(20)가 사용자 단말인 경우에는 코드생성부(262)는 상기 스마트 카드 장치(10)의 종류에 따라 2차 인증용가상코드를 생성할지의 여부를 판단할 수 있다. 보다 상세하게, 코드생성부(262)는 1차 인증용가상코드와 함께 수신된 카드 데이터를 기반으로 상기 판단 동작을 수행할 수 있다(실시예에 따라, 카드 데이터는 태깅 시에 수신될 수도 있다). 즉, 코드생성부(262)는 상기 카드 데이터를 기반으로 상기 스마트 카드 장치(10)가 출입통제용 카드인 것으로 확인되면 2차 인증용가상코드를 생성하지 않고, 상기 카드 데이터를 기반으로 상기 스마트 카드 장치(10)가 금융 결제용 카드인 것으로 확인되면 2차 인증용가상코드를 생성할 수 있다.
- [105] 상기에서는 코드생성부(262)가 상기 판단 동작을 수행하는 것으로 설명하였지만, 이에 제한되지 않고 프로세서(260)의 다른 구성요소가 상기 판단 동작을 수행할 수도 있다.
- [106] 상기 과정을 통해 2차 인증용가상코드를 생성하는 것으로 결정되면, 단계 S130에서, 코드생성부(262)는 상기 1차 인증용가상코드를 이용하여 2차 인증용가상코드를 생성할 수 있다. 이때, 2차 인증용가상코드를 생성하기 위해서, 우선 서버(30)에서 1차 인증용가상코드에 대한 검증이 수행되어야 한다. 서버(30)는 검증을 통해 1차 인증용가상코드에 포함된 복수의 세부코드(제1 코드 및 제2 코드)를 추출하고, 이를 인증용가상코드 생성 장치(20)로 전달할 수 있다.
- [107] 상기에서는 2차 인증용가상코드 생성을 위한 1차 인증용가상코드에 대한

검증을 서버(30)에서 수행하는 것으로 설명하였지만, 실시예에 따라 서버(30)가 아닌 인증용가상코드 생성 장치(20)가 해당 검증을 수행할 수도 있다.

인증용가상코드를 검증하는 방법에 대한 설명은 후술한다.

- [108] 본 명세서에서 2차 인증용가상코드를 생성하는 방식은 OTP 연산을 한번 수행하는 방식과 두번 수행하는 방식으로 구분될 수 있다.
- [109] OTP 연산을 한번 수행하는 방식(제1 방식)은 스마트 카드 장치(10)에서 1차 인증용가상코드가 생성될 때만 OTP 연산이 수행되며, 2차 인증용가상코드의 코드길이가 길어지게 된다.
- [110] 상기 제1 방식에서, 코드생성부(262)는 제2 인증용가상코드생성함수를 이용하여 수신된 제1 코드에서 상기 인증용가상코드 생성 장치(20)의 식별 정보인 제2 UID를 제외하여 제3 코드를 생성할 수 있다. 여기서, 제2 UID는 인증용가상코드 생성 장치(20)에 저장된 데이터로서 인증용가상코드 생성 장치(20)를 식별할 수 있는 고유 값이다.
- [111] 제3 코드 = 제1 코드 - 제2 UID
- [112] 그런 다음, 코드생성부(262)는 제2 인증용가상코드생성함수를 이용하여 스마트 카드 장치(10)에서 생성된 제1 코드, 스마트 카드 장치(10)에서 생성된 제2 코드 및 인증용가상코드 생성 장치(20)에서 생성된 제3 코드를 결합하여 2차 인증용가상코드를 생성할 수 있다.
- [113] 코드생성부(262)는 생성된 복수의 세부코드(제1 코드, 제2 코드 및 제3 코드)를 조합하여 2차 인증용가상코드를 생성할 수 있다. 일 실시예로, 코드생성부(262)는 제2 인증용가상코드생성함수를 이용하여 복수의 세부코드를 특정한 규칙에 따라 결합함으로써 상기 2차 인증용가상코드를 생성할 수 있다. 상기 제2 인증용가상코드생성함수는 복수의 세부코드를 조합하는 규칙(즉, 세부코드결합함수)을 포함할 수 있다. 복수의 세부코드를 결합하여 하나의 인증용가상코드를 생성하는 방식으로는 상술한 방식들이 적용될 수 있다.
- [114] 상기 제1 방식에서, 1차 인증용가상코드에 포함된 제1 코드 및 제2 코드와 2차 인증용가상코드에 포함된 제1 코드 및 제2 코드는 모두 스마트 카드 장치(10)에서 생성된 것으로 동일한 코드를 의미한다. 제3 코드가 스마트 인증 장치(20)에서 새롭게 생성되어 상기 제1 코드 및 제2 코드와 결합되어 2차 인증용가상코드가 생성되는 것이다.
- [115] OTP 연산을 두번 수행하는 방식(제2 방식)은 스마트 카드 장치(10)에서 1차 인증용가상코드가 생성될 때 OTP 연산이 수행되고 이후에 인증용가상코드 생성 장치(20)에서 2차 인증용가상코드가 생성될 때 OTP 연산이 또 한번 수행되며, 2차 인증용가상코드의 코드길이에 변화가 없다(즉, 1차 인증용가상코드의 길이와 동일)
- [116] 상기 제2 방식에서, 코드생성부(262)는 상기 1차 인증용가상코드를 기반으로 제2 OTP를 생성하고, 상기 제2 OTP 및 상기 인증용가상코드 생성 장치의 식별 정보인 제2 UID를 기반으로 상기 2차 인증용가상코드를 생성할 수 있다. 여기서,

제2 UID는 인증용가상코드 생성 장치(20)에 저장된 데이터로서 인증용가상코드 생성 장치(20)를 식별할 수 있는 고유 값이다.

- [117] 코드생성부(262)는 제2 인증용가상코드생성함수를 이용하여 상기 시간 데이터 및 시크릿 값뿐만 아니라 상기 1차 인증용가상코드를 추가 시드 데이터로 더 활용하여 상기 제2 OTP를 생성할 수 있다.
- [118] 그런 다음, 코드생성부(262)는 제2 인증용가상코드생성함수를 이용하여 스마트 카드 장치(10)에서 생성된 제1 코드에 포함된 상기 시간 데이터(시간 데이터는 2차 인증용가상코드 생성 요청 시점일 수 있다)에 상기 생성된 제2 OTP를 더하여 제1 코드를 생성할 수 있다. 코드생성부(262)는 제2 인증용가상코드생성함수를 이용하여 상기 제1 코드에서 상기 인증용가상코드 생성 장치(20)의 식별 정보인 제2 UID (user identification)를 제외하여 제2 코드를 생성할 수 있다. 여기서 제2 UID는 인증용가상코드 생성 장치(20)에 저장된 데이터로서 인증용가상코드 생성 장치(20)를 식별할 수 있는 고유 값이다.
- [119] 제1 코드 = 시간 데이터 + 제2 OTP
- [120] 제2 코드 = 제1 코드 - 제2 UID
- [121] 여기서, 시간 데이터는 현재 시점의 시간 데이터로서, 상기 1차 인증용가상코드를 생성할 때 사용되는 시간 데이터와 상기 2차 인증용가상코드를 생성할 때 사용되는 시간 데이터는 동일할 수 있다. 즉, 제1 OTP와 제2 OTP는 동일 시점에 생성되는 것이기 때문에 동일한 현재 시간 데이터를 이용할 수 있다.
- [122] 코드생성부(262)는 생성된 세부코드(제1 코드 및 제2 코드)를 조합하여 2차 인증용가상코드를 생성할 수 있다. 일 실시예로, 코드생성부(262)는 제2 인증용가상코드생성함수를 이용하여 복수의 세부코드를 특정한 규칙에 따라 결합함으로써 상기 2차 인증용가상코드를 생성할 수 있다. 상기 제2 인증용가상코드생성함수는 복수의 세부코드를 조합하는 규칙(즉, 세부코드결합함수)을 포함할 수 있다. 복수의 세부코드를 결합하여 하나의 인증용가상코드를 생성하는 방식으로는 상술한 방식들이 적용될 수 있다.
- [123] 상기 제2 방식에서, 1차 인증용가상코드에 포함된 제1 코드 및 제2 코드와 2차 인증용가상코드에 포함된 제1 코드 및 제2 코드는 각각 스마트 카드 장치(10)와 인증용가상코드 생성 장치(20)에서 생성된 것으로 각각 상이한 코드이다. 즉, 1차 인증용가상코드에 포함된 제1 코드 및 제2 코드는 제1 OTP 및 제1 UID를 이용하여 생성된 것이고, 2차 인증용가상코드에 포함된 제1 코드 및 제2 코드는 제2 OTP 및 제2 UID를 이용하여 생성된 것이므로 각각 상이하다.
- [124] 상술한 제1 인증용가상코드생성함수와 제2 인증용가상코드생성함수는 각각 스마트 카드 장치(10)와 인증용가상코드 생성 장치(20)에 저장되지만, 구동된 최초시점은 동일할 수 있다. 즉, 사용자가 스마트 카드 장치(10)를 발급받아 인증용가상코드 생성 장치(20)에 최초 태깅을 통해 서버(30)에 상기 스마트 카드 장치(10)에 대한 사용자 등록을 완료하면, 스마트 카드 장치(10)와

- 인증용가상코드 생성 장치(20) 각각에 저장된 제1 인증용가상코드생성함수와 제2 인증용가상코드생성함수가 구동을 시작할 수 있다. 즉, 제1 인증용가상코드생성함수와 제2 인증용가상코드생성함수는 동일할 수 있다.
- [125] 이와 같이 사용자 등록이 완료되면, 서버에는 스마트 카드 장치(10)의 식별 정보인 제1 UID 및 인증용가상코드 생성 장치(20)의 식별 정보인 제2 UID 중 적어도 하나가 저장될 수 있다. 즉, 서버(30)는 사용자 등록 시에 검증 알고리즘 내에서 사용자에게 할당되는 영역에 상기 제1 UID 및 상기 제2 UID 중 적어도 하나를 저장할 수 있다. 실시예에 따라, 서버(30)는 하나의 영역에 상기 제1 UID를 저장하고 제2 UID를 상기 제1 UID에 매칭하여 저장할 수 있다. 실시예에 따라, 서버(30)는 하나의 영역에 상기 제2 UID를 저장하고 제1 UID를 상기 제2 UID에 매칭하여 저장할 수 있다. 실시예에 따라, 서버(30)는 두 개의 영역 각각에 상기 제1 UID 및 상기 제2 UID를 저장할 수 있다.
- [126] 또한, 사용자 등록 시에, 서버(30)는 상기 제1 UID 및 상기 제2 UID 뿐만 아니라 상기 스마트 카드 장치(10)와 관련된 상기 카드 데이터 및 상기 인증용가상코드 생성 장치(20)와 관련된 단말 데이터를 함께 저장할 수 있다.
- [127] 인증용가상코드 생성 장치(20)의 통신부(22)는 상기 1차 인증용가상코드 및 상기 2차 인증용가상코드 중 적어도 하나를 서버로 송신할 수 있다(S140).
- [128] 인증용가상코드 생성 장치(20)의 검증요청부(264)는 상기 서버(30)가 상기 적어도 하나에 대한 검증을 수행하도록 요청할 수 있다(S150).
- [129] 실시예에 따라, 스마트 카드 장치(10)가 출입통제용 출입카드인 경우, 즉, 사용자가 스마트 카드 장치(10)를 이용하여 오프라인 상에서 보안이 필요한 특정 공간으로 출입하거나, 온라인 상에서 특정 웹사이트 또는 앱에 로그인하는 경우, 서버(30)는 상기 1차 인증용가상코드에 대한 검증 요청을 수신할 수 있다. 구체적으로, 스마트 카드 장치(10)에서 생성된 1차 인증용가상코드는 자체적으로 서버(30)로 송신되어 사용자 인증에 이용될 수 있다.
- [130] 도 6을 참조하면, 인증용가상코드 생성 장치(20)(보다 상세하게, 검증요청부(264))는 스마트 카드 장치(10)에서 생성된 1차 인증용가상코드를 서버(30)로 송신하여 검증을 요청할 수 있다. 서버(30)는 검증 알고리즘을 기반으로 1차 인증용가상코드에 대한 검증을 수행하여 검증 결과를 인증용가상코드 생성 장치(20)로 송신할 수 있다.
- [131] 이때, 인증용가상코드 생성 장치(20)는 1차 인증용가상코드를 서버(30)로 바로 전달하여 검증 요청을 할 수도 있지만, 사용자가 1차 인증용가상코드를 시각적으로 확인하거나 복사하여 다른 프로그램 또는 웹페이지에 입력하거나 붙여넣을 수 있도록 디스플레이부(미도시)에 출력할 수 있다. 인증용가상코드 생성 장치(20)는 사용자에게 의해 입력되거나 붙여넣어진 1차 인증용가상코드를 서버(30)로 송신하여 검증 요청을 할 수 있다.
- [132] 인증용가상코드 생성 장치(20)는 검증 결과에 따라 오프라인 출입통제 및 온라인 로그인 시 사용자 인증을 수행할 수 있다. 즉, 1차 인증용가상코드가 정상

코드이면, 사용자가 상기 보안이 필요한 특정 공간으로 출입하는 것을 허용하거나 상기 특정 웹사이트 또는 앱에 로그인하는 것을 허용할 수 있다.

- [133] 실시예에 따라, 스마트 카드 장치(10)가 금융 결제용 카드인 경우, 즉, 사용자가 스마트 카드 장치(10)를 이용하여 금융거래를 진행하는 경우, 서버(30)는 상기 2차 인증용가상코드에 대한 검증 요청을 수신할 수 있다. 즉, 스마트 카드 장치(10)에서 생성된 1차 인증용가상코드는 인증용가상코드 생성 장치(20)로 송신되어 2차 인증용가상코드 생성에 이용될 수 있다.
- [134] 도 7을 참조하면, 인증용가상코드 생성 장치(20)(보다 상세하게, 코드생성부(262))는 스마트 카드 장치(10)에서 생성된 1차 인증용가상코드를 이용하여 2차 인증용가상코드를 생성할 수 있다. 인증용가상코드 생성 장치(20)(보다 상세하게, 검증요청부(264))는 생성된 2차 인증용가상코드를 서버(30)로 송신하여 검증을 요청할 수 있다. 서버(30)는 검증 알고리즘을 기반으로 2차 인증용가상코드에 대한 검증을 수행하여 검증 결과를 인증용가상코드 생성 장치(20)로 송신할 수 있다.
- [135] 이때, 인증용가상코드 생성 장치(20)는 2차 인증용가상코드 생성을 위한 시드 데이터를 획득하기 위해 서버(30)로 1차 인증용가상코드에 대한 검증 요청을 할 수 있다. 서버(30)는 검증 알고리즘을 기반으로 1차 인증용가상코드로부터 제1 코드, 제2 코드, 시간 데이터, 시크릿 값, 제1 UID 중 적어도 하나를 추출하여 인증용가상코드 생성 장치(20)로 전달할 수 있다. 인증용가상코드 생성 장치(20)는 제1 코드, 제2 코드, 시간 데이터, 시크릿 값, 제1 UID, 1차 인증용가상코드 중 적어도 하나를 시드 데이터로 하여 2차 인증용가상코드를 생성할 수 있다. 상술한 바와 같이, 2차 인증용가상코드 생성을 위한 1차 인증용가상코드에 대한 검증은 서버(30)에서 수행할 수도 있지만, 실시예에 따라 인증용가상코드 생성 장치(20)가 직접 해당 검증을 수행할 수도 있다.
- [136] 인증용가상코드 생성 장치(20)는 검증 결과에 따라 금융 결제 시 사용자 인증을 수행할 수 있다. 즉, 2차 인증용가상코드가 정상 코드이면, 사용자가 금융거래를 진행하도록 할 수 있다.
- [137] 이하에서는, 인증용가상코드에 대한 검증 방법을 구체적으로 설명하도록 한다.
- [138] 실시예에 따라, 서버(30)가 1차 인증용가상코드에 대한 검증 요청을 수신한 경우, 제1 인증용가상코드생성함수에 대응하는 검증 알고리즘을 이용하여 상기 1차 인증용가상코드를 기반으로 제1 UID가 저장된 영역을 탐색하여 제1 UID를 추출할 수 있다.
- [139] 이때 상술한 바와 같이 상기 1차 인증용가상코드는 복수의 세부코드를 포함하는데, 복수의 세부코드는, 제1 UID의 저장 영역 탐색의 시작지점을 설정하는 제1 코드와 특정한 탐색방식에 따라 상기 시작지점으로부터 상기 제1 UID의 저장 영역으로의 탐색경로를 설정하는 제2 코드로 구성될 수 있다.
- [140] 제1 코드와 제2 코드는 인증용가상코드검증수단을 구비하는 서버(30) 내에서 1차 인증용가상코드를 검증하기 위한 상관관계를 가지나

인증용가상코드생성수단을 구비하는 스마트 카드 장치(10)는 보안성을 높이기 위해 제1 코드를 생성하는 제1 함수와 제2 코드를 생성하는 제2 함수를 세부코드생성함수로 포함할 뿐, 제1 코드와 제2 코드의 상관관계에 대한 데이터를 포함하지 않을 수 있다.

- [141] 또한, 일 실시예로, 1차 인증용가상코드가 제1 코드 및 제2 코드의 특정한 규칙에 따른 조합으로 생성되는 경우, 제1 코드와 제2 코드는 검증 알고리즘 내의 실체값(제1 UID)의 저장 영역을 탐색하기 위한 각각의 역할을 수행할 수 있다. 예를 들어, 제1 코드는 저장위치탐색의 시작지점을 설정하고, 제2 코드는 특정한 탐색방식에 따라 상기 시작지점으로부터 상기 제1 UID의 저장 영역으로의 탐색경로를 설정한다. 따라서 이후, 스마트 카드 장치(10)에서 단위카운트마다 정상적으로 생성된 인증용가상코드가 제공되면, 서버(30)는 제1 코드에 대응하는 시작지점으로부터 제2 코드에 상응하는 탐색경로에 따라 이동한 지점을 제1 UID가 저장된 영역으로 판단한다.
- [142] 구체적으로, 서버(30)는 검증 알고리즘을 이용하여 1차 인증용가상코드에 포함된 복수의 세부코드를 추출할 수 있다. 상기 1차 인증용가상코드는 복수의 세부코드를 특정한 규칙에 따라 결합하여 생성되는 것이다. 서버(30)는 1차 인증용가상코드 생성 시 사용된 세부코드결합함수와 동일한 함수를 적용하여 1차 인증용가상코드에서 복수의 세부코드를 추출할 수 있다. 예를 들어, 두 개의 세부코드(즉, 제1 코드 및 제2 코드)가 결합된 1차 인증용가상코드가 생성된 경우, 서버(30)는 1차 인증용가상코드의 문자배열에서 세부코드결합함수를 적용하여 제1 코드 및 제2 코드를 분리해낼 수 있다. 이때, 세부코드 간에는 상관관계를 포함할 수 있다.
- [143] 1차 인증용가상코드가 제1 코드 및 제2 코드를 포함하는 경우, 세부코드 간에 상관관계를 가지는 일 실시예로, 서버(30)는 제1 코드에 대응하는 탐색의 시작지점을 결정하고, 상기 탐색시작지점으로부터 제2 코드에 상응하는 탐색경로에 따라 이동한 지점에 대응하는 값을 제1 UID로 간주할 수 있다.
- [144] 또한, 다른 일 실시예로, 스마트 카드 장치(10)가 단위카운트마다 새로운 1차 인증용가상코드를 제공함에 따라, 서버(30)는 각 카운트마다 변경되는 제1 코드 및 제2 코드를 기반으로 시작지점과 탐색경로를 설정하여 제1 UID를 탐색할 수 있다.
- [145] 또한, 일 실시예로, 서버(30)는 상관관계를 가지는 복수의 세부코드를 이용하여 제1 UID를 찾기 위해, 검증 알고리즘을 포함할 수 있다. 검증 알고리즘은 1차 인증용가상코드에 포함되는 각각의 세부코드 적용 시에 제1 UID 탐색이 가능하도록 하는 알고리즘이다. 예를 들어, 1차 인증용가상코드로부터 제1 UID의 탐색의 시작지점을 결정하는 제1 코드와 시작지점으로부터의 저장 영역의 방향을 제시하는 제2 코드를 포함하는 경우, 검증 알고리즘은 제1 코드에 대응되는 지점에서 제2 코드에 대응되는 방향을 지시할 때, 해당 위치에 제1 UID가 배치되도록 조절하는 알고리즘이다. 검증 알고리즘을 이용함에 따라,

서버(30)는 1차 인증용가상코드에 포함된 제1 코드와 제2 코드가 변경되어도 제1 UID를 찾을 수 있다.

- [146] 또한, 일 실시예로, 상기 1차 인증용가상코드가 상기 시간 데이터에 제1 OTP를 더한 제1 코드와, 상기 제1 코드에서 제1 UID를 제외한 제2 코드가 결합되어 생성된 경우, 서버(30)는 상기 제1 코드 값에서 상기 제2 코드 값을 빼서 실제값(즉, 제1 UID)을 추출할 수 있다.
- [147] 또한, 일 실시예로, 서버(30)는 상기 저장 영역을 탐색하여 추출된 제1 UID와 상기 제1 코드 값에서 상기 제2 코드 값을 빼서 추출된 제1 UID를 비교하여, 두 값이 동일하면 상기 1차 인증용가상코드가 정상적인 코드인 것으로 판단할 수 있다. 그러나, 이러한 비교 과정 없이도, 서버(30)는 각각의 값만으로도 해당 1차 인증용가상코드가 정상적인 코드인지를 판단할 수 있다(예를 들어, 추출된 값이 서버(30)의 DB 내 저장된 정보와 일치하는지의 여부를 통해 판단).
- [148] 실시예에 따라, 서버(30)가 2차 인증용가상코드에 대한 검증 요청을 수신한 경우, 제2 인증용가상코드생성함수에 대응하는 검증 알고리즘을 이용하여 상기 2차 인증용가상코드를 기반으로 제1 UID가 저장된 영역 및 제2 UID가 저장된 영역 중 적어도 하나를 탐색하여 제1 UID 및 제2 UID 중 적어도 하나를 추출할 수 있다.
- [149] 상기 제1 방식에서, 상기 2차 인증용가상코드는 상술한 바와 같이 제1 코드, 제2 코드 및 제3 코드를 결합하여 생성된다. 서버(30)는 제2 인증용가상코드생성함수에 대응하는 검증 알고리즘을 이용하여 상기 2차 인증용가상코드를 기반으로 제1 UID가 저장된 영역을 탐색하여 제1 UID를 추출하고, 제2 UID가 저장된 영역을 탐색하여 제2 UID를 추출할 수 있다.
- [150] 서버(30)는 검증 알고리즘을 이용하여 2차 인증용가상코드에 포함된 복수의 세부코드를 추출할 수 있다. 상기 2차 인증용가상코드는 복수의 세부코드를 특정한 규칙에 따라 결합하여 생성되는 것이다. 서버(30)는 2차 인증용가상코드 생성 시 사용된 세부코드결합함수와 동일한 함수를 적용하여 2차 인증용가상코드에서 복수의 세부코드를 추출할 수 있다. 예를 들어, 세 개의 세부코드(즉, 제1 코드, 제2 코드 및 제3 코드)가 결합된 2차 인증용가상코드가 생성된 경우, 서버(30)는 2차 인증용가상코드의 문자배열에서 세부코드결합함수를 적용하여 제1 코드, 제2 코드 및 제3 코드를 분리해낼 수 있다. 이때, 세부코드 간에는 상관관계를 포함할 수 있다.
- [151] 2차 인증용가상코드가 제1 코드, 제2 코드 및 제3 코드를 포함하는 경우, 세부코드 간에 상관관계를 가지는 일 실시예로, 서버(30)는 제1 코드에 대응하는 탐색의 시작지점을 결정하고, 상기 탐색시작지점으로부터 제2 코드에 상응하는 탐색경로에 따라 이동한 지점에 대응하는 값을 제1 UID로 간주할 수 있다. 그리고, 제1 코드에 대응하는 탐색의 시작지점을 결정하고, 상기 시작지점으로부터 제3 코드에 상응하는 탐색경로에 따라 이동한 지점에 대응하는 값을 제2 UID로 간주할 수 있다.

- [152] 또한, 다른 일 실시예로, 인증용가상코드 생성 장치(20)가 단위카운트마다 새로운 2차 인증용가상코드를 제공함에 따라, 서버(30)는 각 카운트마다 변경되는 제1 코드, 제2 코드 및 제3 코드를 기반으로 시작지점과 탐색경로를 설정하여 제1 UID 및 제2 UID를 탐색할 수 있다.
- [153] 또한, 일 실시예로, 서버(30)는 상관관계를 가지는 복수의 세부코드를 이용하여 제1 UID 및 제2 UID를 찾기 위해, 검증 알고리즘을 포함할 수 있다. 검증 알고리즘은 2차 인증용가상코드에 포함되는 각각의 세부코드 적용 시에 제1 UID 탐색 및 제2 UID 탐색이 가능하도록 하는 알고리즘이다. 예를 들어, 2차 인증용가상코드로부터 제1 UID 및 제2 UID의 탐색의 시작지점을 결정하는 제1 코드와 시작지점으로부터의 제1 UID 저장 영역의 방향을 제시하는 제2 코드와 시작지점으로부터의 제2 UID 저장 영역의 방향을 제시하는 제3 코드를 포함하는 경우, 검증 알고리즘은 제1 코드에 대응되는 지점에서 제2 코드에 대응되는 방향을 지시할 때 해당 위치에 제1 UID가 배치되도록 조절하고, 제1 코드에 대응되는 지점에서 제3 코드에 대응되는 방향을 지시할 때, 해당 위치에 제2 UID가 배치되도록 조절하는 알고리즘이다. 검증 알고리즘을 이용함에 따라, 서버(30)는 2차 인증용가상코드에 포함된 제1 코드, 제2 코드 및 제3 코드가 변경되어도 제1 UID 및 제2 UID를 찾을 수 있다.
- [154] 또한, 일 실시예로, 상기 2차 인증용가상코드가 상기 시간 데이터에 제1 OTP를 더한 제1 코드와, 상기 제1 코드에서 제1 UID를 제외한 제2 코드와 상기 제1 코드에서 제2 UID를 제외한 제3 코드가 결합되어 생성된 경우, 서버(30)는 상기 제1 코드 값에서 상기 제2 코드 값을 빼서 실제값(즉, 제1 UID)을 추출하고, 상기 제1 코드 값에서 상기 제3 코드 값을 빼서 실제값(즉, 제2 UID)을 추출할 수 있다.
- [155] 즉, 상기 서버(30)는 상기 제1 코드 및 상기 제2 코드를 기반으로 상기 제1 UID를 추출하여 상기 스마트 카드 장치(10)에 대한 검증을 수행하고, 상기 제1 코드 및 상기 제3 코드를 기반으로 상기 제2 UID를 추출하여 상기 인증용가상코드 생성 장치(20)에 대한 검증을 수행할 수 있다.
- [156] 또한, 일 실시예로, 서버(30)는 상기 저장 영역을 탐색하여 추출된 제1 UID와 상기 제1 코드 값에서 상기 제2 코드 값을 빼서 추출된 제1 UID를 비교하여, 두 값이 동일하면 상기 2차 인증용가상코드에 대한 1차 검증을 완료하고(즉, 상기 스마트 카드 장치에 대한 검증), 상기 저장 영역을 탐색하여 추출된 제2 UID와 상기 제1 코드 값에서 상기 제3 코드 값을 빼서 추출된 제2 UID를 비교하여, 두 값이 동일하면 상기 2차 인증용가상코드에 대한 2차 검증을 완료하여(즉, 상기 인증용가상코드 생성 장치에 대한 검증), 상기 2차 인증용가상코드가 정상적인 코드인 것으로 판단할 수 있다. 그러나, 이러한 비교 과정 없이도, 서버(30)는 각각의 값만으로도 해당 2차 인증용가상코드가 정상적인 코드인지를 판단할 수 있다(예를 들어, 추출된 값이 서버(30)의 DB 내 저장된 정보와 일치하는지의 여부를 통해 판단).
- [157] 상기 제2 방식에서, 상기 2차 인증용가상코드는 상술한 바와 같이 1차

인증용가상코드를 기반으로 생성된 제2 OTP 및 상기 제2 UID를 기반으로 생성된 제1 코드 및 제2 코드를 결합하여 생성된다. 서버(30)는 수신된 상기 2차 인증용가상코드에 포함된 상기 제2 OTP 및 검증용 제2 OTP의 비교를 통해 상기 2차 인증용가상코드의 검증을 수행할 수 있다. 여기서, 상기 검증용 제2 OTP는, 상기 제2 OTP 생성 시에 이용된 시드 데이터와 동일한 시드 데이터를 기반으로 상기 서버(30)에 의해 생성될 수 있다.

- [158] 구체적으로, 서버(30)는 상기 2차 인증용가상코드에서 상기 제1 코드와 상기 제2 코드를 분리하고, 분리된 상기 제1 코드와 상기 제2 코드를 기반으로 상기 제2 UID를 탐색하여, 함께 저장되어 있었던 카드 데이터(예를 들어, 시크릿 값)을 확인할 수 있다. 여기서, 세부코드를 분리하고 세부코드를 이용하여 실제값을 탐색하는 방법은 상술한 바와 같다.
- [159] 그런 다음, 서버(30)는 탐색된 제2 UID에 매칭되어 있는 제1 UID를 탐색할 수 있다.
- [160] 서버(30)는 이렇게 제2 UID를 통해 추출된 값들, 즉 시크릿 값 및 제1 UID와, 현재 시간 데이터를 이용하여 1차 인증용가상코드를 생성하고, 생성된 1차 인증용가상코드와 상기 시크릿 값 및 시간 데이터를 시드 데이터로 하여 검증용 제2 OTP를 생성할 수 있다.
- [161] 이렇게 생성된 검증용 제2 OTP와 상기 제2 인증용가상코드에 포함된 제2 OTP를 비교했을 때, 두 값이 동일하면 서버(30)는 상기 제2 인증용가상코드가 정상적인 코드인 것으로 판단할 수 있다. 즉, 상기 제2 OTP와 상기 검증용 제2 OTP가 동일하면, 시드 데이터로 사용된 값(1차 인증용가상코드와 상기 시크릿 값 및 시간 데이터)들이 전부 동일하고, 또한 1차 인증용가상코드가 동일하면 해당 값으로 생성되는 2차 인증용가상코드도 동일한 것이므로, 상기 스마트 카드 장치(10) 및 상기 인증용가상코드 생성 장치(20)가 정상적인 것으로 검증될 수 있는 것이다.
- [162] 이하에서는, 도 8을 참조하여, 스마트 카드 장치(10)에 의해 수행되는 인증용가상코드 기반 사용자 인증 방법에 대해 상세히 설명하도록 한다.
- [163] 도 8을 참조하면, 스마트 카드 장치(10)는 카드 태깅을 통해 인증용가상코드 생성 장치로부터 시간 데이터를 수신하고(S210), 상기 수신된 시간 데이터를 기반으로 1차 인증용가상코드를 생성할 수 있다(S220).
- [164] 스마트 카드 장치(10)가 1차 인증용가상코드를 생성하는 것과, 사용자 인증용 장치(20)가 2차 인증용가상코드를 생성하는 것과, 서버(30)가 1차 인증용가상코드 및 2차 인증용가상코드 중 적어도 하나에 대한 검증을 수행하는 것은 상기 도 1 내지 도 7을 참조하여 설명한 바와 중복되므로 상세한 설명은 생략하도록 한다.
- [165] 한편, 본 발명의 스마트 카드 장치(10)는 금융 결제용 및 출입통제용의 기능을 함께 수행할 수 있다. 즉, 스마트 카드 장치(10)가 회사의 법인 카드이거나 또는 직원의 개인 카드인 경우 각 사용자는 해당 카드를 이용하여 회사의 출입카드로

사용할 수 있다.

- [166] 도 4 및 도 8에 도시된 단계들은 순차적으로 실행되는 것으로 기재하고 있으나, 이는 본 실시예의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 실시예가 속하는 기술분야에서 통상의 지식을 가진 자라면 본 실시예의 본질적인 특성에서 벗어나지 않는 범위에서 도 4 및 도 8에 기재된 단계들의 순서를 변경하여 실행하거나, 하나 이상의 단계를 병렬적으로 실행하는 것으로 다양하게 수정 및 변형하여 적용 가능할 것이므로, 도 4 및 도 8에 기재된 단계들은 시계열적인 순서로 한정되는 것은 아니다.
- [167] 이상에서 기술한 본 발명은 상기 인증용가상코드 생성 방법을 실행하기 위한 컴퓨터 프로그램을 기록하는 컴퓨터 판독 가능한 기록 매체를 더 제공할 수 있다.
- [168] 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 범위)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.
- [169] 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.
- [170] 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.

청구범위

- [청구항 1] 인증용가상코드 생성 장치에 의해 수행되는 방법에 있어서,
IC 칩이 내장된 카드 태깅 시, 상기 카드로 시간 데이터를 송신하는 단계;
상기 시간 데이터를 기반으로 생성된 1차 인증용가상코드를 상기
카드로부터 수신하는 단계;
상기 1차 인증용가상코드를 이용하여 2차 인증용가상코드를 생성하는
단계;
상기 1차 인증용가상코드 및 상기 2차 인증용가상코드 중 적어도 하나를
서버로 송신하는 단계; 및
상기 서버가 상기 적어도 하나에 대한 검증을 수행하도록 요청하는
단계;를 포함하는, 인증용가상코드 생성 방법.
- [청구항 2] 제1 항에 있어서,
상기 1차 인증용가상코드는, 복수의 코드를 포함하고,
상기 복수의 코드 중 제1 코드는, 상기 시간 데이터 및 제1 OTP를
기반으로 생성되고,
상기 복수의 코드 중 제2 코드는, 상기 제1 코드에서 상기 카드의 식별
정보인 제1 UID (user identification)를 제외하여 생성되는,
인증용가상코드 생성 방법.
- [청구항 3] 제2 항에 있어서,
상기 2차 인증용가상코드를 생성 단계는,
상기 제1 코드에서 상기 인증용가상코드 생성 장치의 식별 정보인 제2
UID를 제외하여 제3 코드를 생성하고,
상기 제1 코드, 상기 제2 코드 및 상기 제3 코드를 결합하여 상기 2차
인증용가상코드를 생성하는, 인증용가상코드 생성 방법.
- [청구항 4] 제3 항에 있어서,
상기 카드는, 상기 제1 코드 및 상기 제2 코드를 기반으로 검증이
수행되고,
상기 인증용가상코드 생성 장치는, 상기 제1 코드 및 상기 제3 코드를
기반으로 검증이 수행되는, 인증용가상코드 생성 방법.
- [청구항 5] 제2 항에 있어서,
상기 2차 인증용가상코드를 생성 단계는,
상기 1차 인증용가상코드를 기반으로 제2 OTP를 생성하고,
상기 제2 OTP 및 상기 인증용가상코드 생성 장치의 식별 정보인 제2
UID를 기반으로 상기 2차 인증용가상코드를 생성하는, 인증용가상코드
생성 방법.
- [청구항 6] 제5 항에 있어서,
상기 2차 인증용가상코드는,

- 상기 2차 인증용가상코드에 포함된 상기 제2 OTP 및 검증용 제2 OTP의 비교를 통해 검증되고,
 상기 검증용 제2 OTP는,
 상기 제2 OTP 생성 시에 이용된 시드 데이터와 동일한 시드 데이터를 기반으로 상기 서버에 의해 생성된 것인, 인증용가상코드 생성 방법.
- [청구항 7] 제1 항에 있어서,
 상기 1차 인증용가상코드는,
 오프라인 출입통제 및 온라인 로그인 시 사용자 인증용으로 이용되는, 인증용가상코드 생성 방법.
- [청구항 8] 제1 항에 있어서,
 상기 2차 인증용가상코드는,
 금융 결제 시 사용자 인증용으로 이용되는, 인증용가상코드 생성 방법.
- [청구항 9] 제1 항에 있어서,
 상기 시간 데이터는,
 APDU(Application Protocol Data Unit) 명령어와 결합된 형태인,
 인증용가상코드 생성 방법.
- [청구항 10] 컴퓨터와 결합되어, 제1 항 내지 제9 항 중 어느 하나의 방법을 실행하기 위해 컴퓨터 판독 가능한 기록 매체에 저장된 프로그램.
- [청구항 11] 카드 태깅을 통해 인증용가상코드 생성 장치로부터 시간 데이터를 수신하는 NFC 모듈; 및
 상기 수신된 시간 데이터를 기반으로 1차 인증용가상코드를 생성하는 IC 모듈;을 포함하고,
 상기 1차 인증용 가상코드는 자체적으로 송신되어 사용자 인증에 이용되거나, 2차 인증용 가상코드 생성에 이용되는 것이고,
 상기 2차 인증용가상코드는, 상기 1차 인증용가상코드를 이용하여 상기 인증용가상코드 생성 장치에 의해 생성되는 것이고,
 상기 1차 인증용가상코드 및 상기 2차 인증용가상코드 중 적어도 하나는, 서버에 의해 검증이 수행되도록 상기 인증용가상코드 생성 장치에 의해 상기 서버로 전송되는, 스마트 카드 장치.
- [청구항 12] IC 칩이 내장된 카드 태깅 시, 상기 카드로 시간 데이터를 송신하고, 상기 시간 데이터를 기반으로 생성된 1차 인증용가상코드를 상기 카드로부터 수신하는 통신부;
 상기 1차 인증용가상코드를 이용하여 2차 인증용가상코드를 생성하는 코드생성부; 및
 상기 통신부를 통해 상기 1차 인증용가상코드 및 상기 2차 인증용가상코드 중 적어도 하나를 서버로 송신하여, 상기 서버가 상기 적어도 하나에 대한 검증을 수행하도록 요청하는 검증요청부;를 포함하는, 인증용가상코드 생성 장치.

- [청구항 13] 서버에 의해 수행되는 방법에 있어서,
 인증용가상코드 생성 장치로부터 1차 인증용가상코드 및 2차
 인증용가상코드 중 적어도 하나를 수신하는 단계; 및
 상기 1차 인증용가상코드 및 상기 2차 인증용가상코드 중 적어도 하나에
 대한 검증을 수행하는 단계;를 포함하고,
 상기 2차 인증용가상코드가 복수의 코드를 포함하는 경우, 상기 검증
 수행 단계는,
 상기 복수의 코드 중 제1 코드 및 제2 코드를 기반으로 카드의 식별
 정보인 제1 UID (user identification)를 추출하여 상기 카드에 대한 검증을
 수행하고,
 상기 복수의 코드 중 상기 제1 코드 및 제3 코드를 기반으로 상기
 인증용가상코드 생성 장치의 식별 정보인 제2 UID를 추출하여 상기
 인증용가상코드 생성 장치에 대한 검증을 수행하는, 인증용가상코드
 검증 서버.
- [청구항 14] 제13 항에 있어서,
 상기 2차 인증용가상코드가 제2 OTP 및 상기 제2 UID를 포함하는 경우,
 상기 검증 수행 단계는,
 상기 제2 OTP 생성 시에 이용된 시드 데이터와 동일한 시드 데이터를
 기반으로 검증용 제2 OTP를 생성하고,
 상기 2차 인증용가상코드에 포함된 상기 제2 OTP 및 상기 검증용 제2
 OTP를 비교하고,
 상기 제2 OTP 및 상기 검증용 제2 OTP가 동일하면 상기 카드 및 상기
 인증용가상코드 생성 장치에 대한 검증을 완료하는, 인증용가상코드
 검증 서버.
- [청구항 15] 제13 항에 있어서,
 상기 1차 인증용가상코드가 수신된 경우,
 상기 검증 수행 단계는,
 제1 검증 알고리즘을 이용하여 상기 1차 인증용가상코드를 기반으로
 카드의 식별 정보인 제1 UID (user identification)를 추출하여 상기 카드에
 대한 검증을 수행하는, 인증용가상코드 검증 서버.