

명세서

발명의 명칭: 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 방법

기술분야

- [1] 본 개시는 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 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 실제 카드번호가 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. 그러나 아직까지 이에 대한 적절한 방안이 제시되지 못하는 실정이다.

발명의 상세한 설명

기술적 과제

- [7] 본 개시에 개시된 실시예는 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 방법을 제공하는데 그 목적이 있다.
- [8] 본 개시가 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 기술적 과제를 달성하기 위한 본 개시에 일 측면에 따른 사용자가 등록되지 않은 실물 형태의 홀더리스(Holderless) 카드에 의해 수행되는 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 방법은, 카드 태깅을

통해 상기 사용자의 단말로부터 현재 시간 데이터를 수신하는 단계, 상기 카드에 포함된 애플릿(Applet)을 이용하여, 상기 현재 시간 데이터 및 기 저장된 시드 데이터를 기반으로 상기 사용자의 인증을 위한 가상코드를 생성하는 단계 및 상기 가상코드를 상기 사용자 단말을 통해 검증 서버로 송신하여 상기 가상코드에 대한 검증을 요청하는 단계를 포함하고, 상기 카드는, 상기 사용자가 등록되지 않은 상태로 제작되고, 상기 검증이 완료되면 상기 검증 서버 내에 상기 사용자가 기 보유한 모바일 카드와 연결되어 상기 사용자가 등록되는 것이다.

- [10] 또한, 상기 검증 서버가 금융사 서버이고, 상기 카드가 상기 금융사와 연계된 카드제조사에 의해 제작되는 경우, 상기 검증 요청 단계는, 상기 사용자 단말을 통해 상기 검증 서버로 기 저장된 상기 카드의 카드번호 및 상기 카드의 고유값 중 적어도 하나를 더 송신하여 상기 검증을 요청하고, 상기 검증이 완료되면, 상기 검증 서버 내에 상기 시드 데이터, 상기 카드의 카드번호 및 상기 카드의 고유값 중 적어도 하나, 및 상기 사용자 단말에서 생성된 사용자 정보가 매칭되어 저장될 수 있다.
- [11] 또한, 상기 카드의 카드번호, 상기 카드의 고유값 및 상기 시드 데이터는, 상기 검증 서버에 의해 상기 카드제조사의 서버로 전달되어, 상기 카드의 제작 시 IC 칩에 내장되고, 상기 카드의 카드번호는, 상기 금융사의 식별코드를 포함하고, 상기 카드의 고유값은, 상기 카드제조사에 의해 제작되는 카드 별로 순차적으로 부여되는 값일 수 있다.
- [12] 또한, 상기 검증 서버가 카드발급을 대행하는 서비스 서버이고, 상기 카드가 상기 카드발급 대행 서비스의 제공사에 의해 제작되는 경우, 상기 사용자의 등록은, 실물 카드 등록용 어플리케이션 기반의 제1 방식 또는 실물 카드 등록용 인터페이스 기반의 제2 방식에 의해 수행될 수 있다.
- [13] 또한, 상기 사용자 단말은, 상기 서비스 서버에 의해 제공되는 상기 어플리케이션이 구비되고, 상기 제1 방식의 사용자 등록은, 상기 어플리케이션을 통해 상기 모바일 카드의 카드번호가 입력된 후에 상기 카드 태깅을 통해 수행될 수 있다.
- [14] 또한, 상기 제1 방식의 사용자 등록은, 상기 서비스 서버에 의해 상기 가상코드 기반으로 탐색된 상기 카드의 카드번호와 상기 모바일 카드의 카드번호가 매칭되어 수행되고, 상기 카드의 카드번호는, 상기 등록이 완료된 상기 카드를 통해 결제가 요청되는 경우에 결제망을 통해 결제 서버로부터 상기 서비스 서버로 송신되고, 상기 카드의 카드번호에 매칭된 상기 모바일 카드의 카드번호는, 상기 결제망을 통해 상기 서비스 서버로부터 상기 결제 서버로 송신될 수 있다.
- [15] 또한, 상기 제2 방식의 사용자 등록은, 금융사의 어플리케이션에 상기 카드발급 대행 서비스와 연동되는 상기 인터페이스가 생성된 후에 상기 카드 태깅을 통해 수행될 수 있다.

- [16] 또한, 상기 제2 방식의 사용자 등록은, 상기 인터페이스를 통해 상기 서비스 서버로 송신된 상기 가상코드 및 상기 사용자의 고유값을 기반으로 수행되며, 상기 카드의 카드번호는, 상기 등록이 완료된 상기 카드를 통해 결제가 요청되는 경우에 결제망을 통해 결제 서버로부터 상기 서비스 서버로 송신되어 상기 사용자 고유값 추출에 이용되고, 상기 사용자 고유값은, 상기 금융사의 서버로 송신되어 상기 모바일 카드의 카드번호 추출에 이용될 수 있다.
- [17] 또한, 상기 수신 단계는, 상기 카드 태깅 시에 상기 애플릿의 구동을 위한 APDU 명령어와 함께 상기 현재 시간 데이터가 수신되고, 상기 생성 단계는, 상기 APDU 명령어에 따라 상기 애플릿이 구동되어 생성될 수 있다.
- [18] 또한, 상술한 기술적 과제를 달성하기 위한 본 개시에 다른 측면에 따른 사용자가 등록되지 않은 실물 형태의 홀더리스(Holderless) 카드 장치는, 상기 사용자의 단말과 태깅 시에 NFC 기반의 통신을 수행하는 NFC 모듈 및 상기 사용자의 인증을 위한 가상코드를 생성하기 위한 애플릿(Applet)이 포함된 IC 모듈을 포함하고, 상기 IC 모듈은, 상기 사용자 단말과 태깅 시, 상기 NFC 모듈을 통해 상기 사용자 단말로부터 현재 시간 데이터를 수신하고, 상기 애플릿을 제어하여, 상기 현재 시간 데이터 및 기 저장된 시드 데이터를 기반으로 가상코드를 생성하며, 상기 가상코드가 상기 사용자 단말을 통해 검증 서버로 송신되도록 하여, 상기 검증 서버에 상기 가상코드에 대한 검증을 요청하고, 상기 카드 장치는, 상기 사용자가 등록되지 않은 상태로 제작되고, 상기 검증이 완료되면 상기 검증 서버 내에 상기 사용자가 기 보유한 모바일 카드와 연결되어 상기 사용자가 등록되는 것일 수 있다.
- [19] 이 외에도, 본 개시를 구현하기 위한 실행하기 위한 컴퓨터 판독 가능한 기록 매체에 저장된 컴퓨터 프로그램이 더 제공될 수 있다.
- [20] 이 외에도, 본 개시를 구현하기 위한 방법을 실행하기 위한 컴퓨터 프로그램을 기록하는 컴퓨터 판독 가능한 기록 매체가 더 제공될 수 있다.

발명의 효과

- [21] 본 개시의 기술한 과제 해결 수단에 의하면, 금융사가 카드 발급을 연계된 카드제조사를 통해 수행하거나, 외부의 발급대행 서비스를 이용함으로써 실물 카드를 제작하고 배송하는 데 드는 비용을 절감할 수 있다.
- [22] 또한, 카드제조사와 연계하거나 외부 발급대행 서비스를 이용함으로써 카드의 커스터마이징이 가능하고 마케팅에 활용함으로써 실물 카드를 새로운 거래 물품으로 활용할 수 있다.
- [23] 또한, 기존에는 실물 카드를 사용하기 위해 연회비를 지불해야 했지만, 실물 카드를 모바일 카드에 연결하여 사용함으로써 실물 카드에 대한 연회비를 지불할 필요가 없게 된다.
- [24] 본 개시의 효과들은 이상에서 언급된 효과로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수

있을 것이다.

도면의 간단한 설명

- [25] 도 1은 본 개시에 따른 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하기 위한 시스템을 개략적으로 나타낸 도면이다.
- [26] 도 2는 본 개시에 따른 홀더리스 카드 장치의 개략적인 구성도이다.
- [27] 도 3은 본 개시에 따른 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 방법의 순서도이다.
- [28] 도 4는 본 개시에 따른 사용자가 등록되지 않은 실물 카드를 모바일 카드에 연결하여 사용자를 등록하는 것을 설명하기 위한 도면이다.
- [29] 도 5는 본 개시에 따른 검증 서버가 금융사 서버인 경우의 등록 프로세스를 설명하기 위한 도면이다.
- [30] 도 6 및 도 7은 본 개시에 따른 검증 서버가 카드발급을 대행하는 서비스 서버인 경우의 등록 프로세스를 설명하기 위한 도면이다.
- [31] 도 8은 본 개시에 따른 컴퓨팅 장치를 나타내는 도면이다.

발명의 실시를 위한 형태

- [32] 본 개시 전체에 걸쳐 동일 참조 부호는 동일 구성요소를 지칭한다. 본 개시가 실시예들의 모든 요소들을 설명하는 것은 아니며, 본 개시가 속하는 기술분야에서 일반적인 내용 또는 실시예들 간에 중복되는 내용은 생략한다. 명세서에서 사용되는 '부, 모듈, 부재, 블록'이라는 용어는 소프트웨어 또는 하드웨어로 구현될 수 있으며, 실시예들에 따라 복수의 '부, 모듈, 부재, 블록'이 하나의 구성요소로 구현되거나, 하나의 '부, 모듈, 부재, 블록'이 복수의 구성요소들을 포함하는 것도 가능하다.
- [33] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 직접적으로 연결되어 있는 경우뿐 아니라, 간접적으로 연결되어 있는 경우를 포함하고, 간접적인 연결은 무선 통신망을 통해 연결되는 것을 포함한다.
- [34] 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.
- [35] 명세서 전체에서, 어떤 부재가 다른 부재 "상에" 위치하고 있다고 할 때, 이는 어떤 부재가 다른 부재에 접해 있는 경우뿐 아니라 두 부재 사이에 또 다른 부재가 존재하는 경우도 포함한다.
- [36] 제 1, 제 2 등의 용어는 하나의 구성요소를 다른 구성요소로부터 구별하기 위해 사용되는 것으로, 구성요소가 전술된 용어들에 의해 제한되는 것은 아니다.
- [37] 단수의 표현은 문맥상 명백하게 예외가 있지 않는 한, 복수의 표현을 포함한다.
- [38] 각 단계들에 있어 식별부호는 설명의 편의를 위하여 사용되는 것으로 식별부호는 각 단계들의 순서를 설명하는 것이 아니며, 각 단계들은 문맥상 명백하게 특정 순서를 기재하지 않는 이상 명기된 순서와 다르게 실시될 수

있다.

- [39] 이하 첨부된 도면들을 참고하여 본 개시의 작용 원리 및 실시예들에 대해 설명한다.
- [40] 이하, 첨부된 도면을 참조하여 본 개시의 실시예를 상세하게 설명한다.
- [41] 설명에 앞서 본 명세서에서 사용하는 용어의 의미를 간략히 설명한다. 그렇지만 용어의 설명은 본 명세서의 이해를 돕기 위한 것이므로, 명시적으로 본 개시를 한정하는 사항으로 기재하지 않은 경우에 본 개시의 기술적 사상을 한정하는 의미로 사용하는 것이 아님을 주의해야 한다.
- [42] 본 명세서에서 "문자"는 코드를 구성하는 구성요소로서, 대문자 알파벳, 소문자 알파벳, 숫자 및 특수문자 등의 전부 또는 일부를 포함한다.
- [43] 본 명세서에서 "코드"는 문자가 나열된 문자열을 의미한다.
- [44] 본 명세서에서 "인증용 가상코드"는 상기 사용자 등록을 위해 임시적으로 생성되는 OTAC(One Time Authentication Code)를 의미할 수 있다.
- [45] 본 명세서에서 "홀더리스(holderless) 카드"는 가상코드를 생성하기 위한 애플릿(Applet)이 탑재된 실물 카드로, 사용자가 할당되지 않은 상태로 제작 및 발급되는 카드를 의미한다. 홀더리스 카드는 사용자가 할당되지 않았지만, 사용자의 등록 절차 이후에 결제에 사용 가능한 실체카드번호가 저장되어 있을 수 있다.
- [46] 본 명세서에서 "가상코드 생성 함수"는 가상코드를 생성하는 함수를 의미한다. 예를 들어, OTP(One Time Password) 등을 포함하며, 이에 한정하는 것은 아니다.
- [47] 본 명세서에서 "세부코드 생성 함수"는 가상코드를 구성하는 각각의 세부코드를 생성하는 함수를 의미한다.
- [48] 본 명세서에서 "세부코드 결합 함수"는 복수의 세부코드를 조합 또는 결합하여 가상코드를 생성하는 함수를 의미한다.
- [49] 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.
- [50] 본 명세서에서 "저장위치"는 사용자에게 의해 카드의 등록이 요청된 시점에 해당하는 트랙 상 지점(카운트)을 의미한다.
- [51] 본 명세서에서 "사용자 등록" 및 "카드 등록"은 사용자가 특정되지 않은 실물 형태의 홀더리스 카드에 사용자를 할당하여 등록을 수행한다는 것으로 동일한 의미로 해석될 수 있다.
- [52] 도 1은 본 개시에 따른 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하기 위한 시스템을 개략적으로 나타낸 도면이다.
- [53] 도 1을 참조하면, 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하기 위한 시스템(1)(이하, 시스템)은 실물 카드(10), 사용자 단말(20) 및 검증 서버(30)를 포함한다. 다만, 몇몇 실시예에서 시스템(1)은 도 1에 도시된 구성요소보다 더 적은 수의 구성요소나 더 많은 수의 구성요소를 포함할 수도

있다.

- [54] 실물 카드(10)는 사용자가 특정(등록)되지 않은 상태로 제작 및 발급되는 홀더리스(holderless) 카드로서, 이후 가상코드 검증을 통해 사용자 등록이 완료되면 사용자가 이미 보유하여 사용하고 있는 모바일 카드와 연결될 수 있다. 본 명세서에서, “실물 카드” 및 “홀더리스 카드”는 동일 의미로 해석될 수 있다.
- [55] 실물 카드(10)는 사용자가 특정되지 않기 때문에 제작 시에 사용자 관련 정보가 내장되지 않는다. 실시예에 따라, 실물 카드(10)의 표면에는 어떠한 정보도 표시되지 않을 수 있다.
- [56] 실물 카드(10)는 인증용 가상코드를 생성하기 위한 애플릿(Applet)을 포함하고, 애플릿을 이용하여 사용자 단말(20)로부터 수신된 데이터와 내장된 데이터를 기반으로 인증용 가상코드(이하, 가상코드)를 생성할 수 있다. 본 개시에서, 실물 카드(10)는 애플릿을 포함하여 카드 등록을 위한 다양한 연산처리를 수행하는 카드 장치일 수 있다.
- [57] 사용자 단말(20)은 실물 카드(10)와 태깅 시 실물 카드(10)로 현재 시간 데이터를 송신할 수 있다.
- [58] 사용자 단말(20)은 실물 카드(10)로부터 가상코드를 전달받아, 가상코드와 함께 사용자 정보를 검증 서버(30)로 송신할 수 있다.
- [59] 검증 서버(30)는 사용자 단말(20)로부터 수신된 가상코드를 검증하여 수신된 가상코드가 현시점에 정상적으로 생성된 것으로 판단되면, 실물 카드(10)에 대한 사용자 등록을 완료할 수 있다. 이로써, 사용자의 실물 카드(10)는 사용자가 이미 사용하고 있던 모바일 카드와 연결되어, 이후 실물 카드(10)를 이용하여 결제가 요청되면 실물 카드(10)와 연결된 모바일 카드로 결제가 진행될 수 있다.
- [60] 도 1을 참조하면, 검증 서버(30)는 하나의 서버로 구성된 것으로 표시되어 있지만, 복수의 서버가 서로 연계된 시스템 형태로 구성될 수도 있다.
- [61] 도 1에 도시된 바와 같이, 실물 카드(10), 사용자 단말(20) 및 검증 서버(30)는 통신망을 통해 서로 각종 데이터, 신호 또는 정보를 송수신할 수 있다.
- [62] 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.
- [63] 한편, 통신망은 상기에 제시된 통신방식에 한정되는 것은 아니며, 상술한 통신방식 이외에도 기타 널리 공지되었거나 향후 개발될 모든 형태의 통신방식을 포함할 수 있다.
- [64] 도 2는 본 개시에 따른 홀더리스 카드 장치의 개략적인 구성도이다. 도 2의 홀더리스 카드 장치(100)는 도 1을 참조하여 설명한 실물 카드(10)를 의미한다. 즉, 홀더리스 카드 장치(10)는 사용자가 등록되지 않은 상태로 제작되고, 가상코드 검증이 완료되면 검증 서버(30) 내에 사용자가 기 보유한 모바일

- 카드와 연결되어 사용자가 등록되는 실물 카드(10)를 의미할 수 있다.
- [65] 도 2를 참조하면, 홀더리스 카드 장치(100)는 NFC 모듈(120) 및 IC 모듈(140)을 포함할 수 있다. 다만, 몇몇 실시예에서 홀더리스 카드 장치(100)는 도 2에 도시된 구성요소보다 더 적은 수의 구성요소나 더 많은 수의 구성요소를 포함할 수도 있다.
- [66] NFC(Narrow Frequency Communication) 모듈(120)(즉, NFC 칩)은 통신 모듈로서, 사용자 단말(20)과 태깅 시에 NFC 기반의 통신을 수행할 수 있다.
- [67] IC 모듈(140)(즉, IC 칩)은 사용자의 인증을 위한 가상코드를 생성하기 위한 애플릿(Applet)을 포함할 수 있다. IC 모듈이 애플릿을 포함하는 것으로 설명하였지만, IC 모듈(140)이 애플릿 자체일 수 있다.
- [68] 보다 상세하게, IC 모듈(140)은 EMV 애플릿 및 OTAC 애플릿을 포함할 수 있다. EMV 애플릿에는 실물 카드(10)의 카드번호 및 실물 카드(10)의 고유값이 내장되고, OTAC 애플릿에는 가상코드(OTAC) 생성을 위한 시드 데이터가 내장될 수 있다.
- [69] IC 모듈(140)은 사용자 단말(20)과 태깅 시, 상기 NFC 모듈(120)을 통해 상기 사용자 단말(20)로부터 현재 시간 데이터를 수신하고, 상기 애플릿(구체적으로, OTAC 애플릿)을 이용(제어)하여, 상기 현재 시간 데이터 및 기 저장된 시드 데이터를 기반으로 가상코드를 생성하고, NFC 모듈(120)을 통해 상기 가상코드를 상기 사용자 단말(20)로 송신할 수 있다. 사용자 단말(20)은 상기 가상코드를 검증 서버(30)로 송신하여 상기 가상코드에 대한 검증을 요청할 수 있다.
- [70] 도 2에는 홀더리스 카드 장치(100)가 NFC 모듈(120)만 포함하는 것으로 도시하였지만, 홀더리스 카드 장치(100)는 별도의 통신 모듈을 더 구비하여 사용자 단말(20)과 통신을 수행할 수 있다. 즉, 별도의 통신 모듈을 통해 사용자 단말(20)로 가상코드를 송신할 수 있다. 여기서, 별도의 통신 모듈은 무선 통신 모듈 및 근거리 통신 모듈을 포함할 수 있다.
- [71] 무선 통신 모듈은 와이파이(Wifi) 모듈, 와이브로(Wireless broadband) 모듈 외에도, GSM(global System for Mobile Communication), CDMA(Code Division Multiple Access), WCDMA(Wideband Code Division Multiple Access), UMTS(universal mobile telecommunications system), TDMA(Time Division Multiple Access), LTE(Long Term Evolution), 4G, 5G, 6G 등 다양한 무선 통신 방식을 지원하는 무선 통신 모듈을 포함할 수 있다.
- [72] 근거리 통신 모듈은 근거리 통신(Short range communication)을 위한 것으로서, 블루투스(Bluetooth™), RFID(Radio Frequency Identification), 적외선 통신(Infrared Data Association; IrDA), UWB(Ultra Wideband), ZigBee, NFC(Near Field Communication), Wi-Fi(Wireless-Fidelity), Wi-Fi Direct, Wireless USB(Wireless Universal Serial Bus) 기술 중 적어도 하나를 이용하여, 근거리 통신을 지원할 수 있다.

- [73] IC 모듈(140)은 PCB판 내에 실장되어 IC 방식의 카드리더기의 단자와 접촉하여 데이터 교환을 수행하도록 한다. IC 모듈(140)은 집적회로(Integrated circuit; IC)를 포함하는 부품, 시스템 온칩(System on chip; SoC) 등 임의의 형태를 포함한다. 예를 들어, IC 칩은 본 개시에 따라 ISO 14443 NXP Mifare Classic 타입일 수 있으나, 이에 한정하는 것은 아니다.
- [74] 도 3은 본 개시에 따른 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 방법의 순서도이다. 도 4는 본 개시에 따른 사용자가 등록되지 않은 실물 카드를 모바일 카드에 연결하여 사용자를 등록하는 것을 설명하기 위한 도면이다. 도 3의 방법은 홀더리스 카드에 의해 수행될 수 있다. 이하에서는 도 3의 방법을 도 1에 개시된 실물 카드(10)가 수행하는 것으로 설명하지만, 이는 홀더리스 카드 장치(100)에 의해 수행되는 것으로도 이해될 수 있다.
- [75] 본 개시는 사용자가 이미 금융사 어플리케이션(앱)에 등록하여 사용하고 있는 모바일 카드에 실물 카드(10)를 연결하여 실물 카드(10)를 오프라인 결제에 사용하길 원하는 경우에 실물 카드(10)(홀더리스 카드)의 사용자 등록을 수행할 수 있다. 본 개시에서 실물 카드(10)는 금융사가 사용자에게 배송해주는 것이 아니라 사용자가 직접 구매하여 획득될 수 있다.
- [76] 도 3을 참조하면, 실물 카드(10)는 카드 태깅을 통해 사용자의 단말(20)(이하, 사용자 단말)로부터 현재 시간 데이터를 수신할 수 있다(S110).
- [77] 실물 카드(10)는 상기 카드에 포함된 애플릿(Applet)을 이용하여, 현재 시간 데이터 및 실물 카드에 기 저장된 시드 데이터를 기반으로 사용자의 인증을 위한 가상코드를 생성할 수 있다(S120). 이때, 각 카드에서 생성되는 가상코드는 카드 내에 저장된 시드 데이터에 의해 카드 간에 절대 중복되지 않게 생성될 수 있다.
- [78] 실물 카드(10)는 가상코드를 사용자 단말(20)을 통해 검증 서버(30)로 송신하여 가상코드에 대한 검증을 요청할 수 있다(S130).
- [79] 실물 카드(10)는 상기 카드 태깅 시에 사용자 단말(20)로부터 상기 애플릿의 구동을 위한 APDU 명령어와 함께 상기 현재 시간 데이터를 수신할 수 있다.
- [80] 즉, 실물 카드(10)는 카드 태깅을 통해 사용자 단말(20)로부터 APDU 명령어 및 현재 시간 데이터를 수신하면, APDU 명령어를 기반으로 애플릿을 구동시킬 수 있다. 그리고, 구동된 애플릿을 이용하여 수신된 현재 시간 데이터와 카드 내에 이미 저장되어 있던 가상코드 생성을 위한 시드 데이터를 기반으로 가상코드를 생성할 수 있다. 이렇게 생성된 가상코드는 사용자 단말(20)로 송신될 수 있다.
- [81] 사용자 단말(20)은 금융서비스 어플리케이션에 로그인되어 있는 사용자 정보와 수신된 가상코드 중 적어도 하나를 검증 서버(30)로 송신할 수 있다. 여기서, 사용자 정보는 사용자의 로그인 정보 및 사용자가 실물 카드(10)와 연결하기를 원하는 모바일 카드 정보를 포함할 수 있다. 여기서, 금융서비스 어플리케이션은 금융사가 자체적으로 구축한 어플리케이션일 수 있고, 외부 서버로부터 제공받은 어플리케이션일 수 있다.
- [82] 검증 서버(30)는 가상코드가 현시점에 정상적으로 생성된 것으로 판단되면,

실물 카드(10)를 모바일 카드에 연결하여 상기 실물 카드(10)에 대한 사용자 등록을 완료할 수 있다.

- [83] 도 3을 참조하면, 실물 카드(10)는 사용자가 등록되지 않은 상태로 제작 및 발급되고, 사용자가 이를 구매하여 자신이 금융사 어플리케이션에 등록하여 사용 중인 모바일 카드에 연결하여 카드 등록을 수행할 수 있다. 보다 상세하게, 사용자는 자신의 사용자 단말(20)에 금융서비스 어플리케이션을 설치하여 해당 어플리케이션을 통해 자신이 이미 사용하고 있는 모바일 카드를 실물 카드(10)와 연결할 수 있다. 구체적으로, 검증 서버(30)가 실물 카드(10)에서 생성된 가상코드에 대한 검증을 완료하면, 해당 실물 카드(10)는 모바일 카드에 연결되어, 모바일 카드의 사용자가 실물 카드(10)의 사용자로 등록이 완료될 수 있다. 여기서, 금융서비스 어플리케이션이 금융사가 자체적으로 구축한 어플리케이션인 경우, 상기 사용자 등록은 금융사가 제공하는 하나의 어플리케이션을 이용하여 수행될 수 있고, 금융서비스 어플리케이션이 외부 서버로부터 제공받은 어플리케이션일인 경우, 상기 사용자 등록은 금융사가 제공하는 어플리케이션과 외부 서비스사가 제공하는 어플리케이션, 두 개의 어플리케이션을 이용하여 수행될 수 있다.
- [84] 이하에서는 가상코드 생성 장치로서의 역할을 수행하는 실물 카드(10)가 가상코드를 생성하는 방법에 대해서 구체적으로 설명하도록 한다.
- [85] 실물 카드(10)에 포함된 OTAC 애플릿은 하나 또는 복수의 세부코드를 생성할 수 있다. 세부코드는 가상코드를 구성하는 일부 코드를 의미하는데, 가상코드는 세부코드만으로 구성될 수도 있으며, 또는 OTP함수에 의해 생성된 제1 가상보안코드에 하나 또는 복수의 세부코드를 결합하여 최종 가상코드(OTAC)의 형태로 형성될 수도 있다.
- [86] OTAC 애플릿은 가상코드를 생성하는 가상코드 생성 함수를 포함하고, 가상코드 생성 함수는 하나 이상의 세부코드를 생성하는 세부코드 생성 함수와, 상기 세부코드를 결합하여 가상코드를 생성하는 세부코드 결합 함수(즉, 복수의 세부코드를 조합하는 규칙)를 포함한다.
- [87] 즉, 가상코드가 복수의 세부코드를 포함하는 경우, 가상코드 생성 함수는 복수의 세부코드 생성 함수를 이용하여 복수의 세부코드를 생성하고, 상기 세부코드 결합 함수를 통해 상기 복수의 세부코드를 기 설정된 조합으로 결합하여 가상보안코드를 생성한다.
- [88] 복수의 세부코드 간에는 검증 서버(30)가 사용자 또는 카드를 식별할 수 있는 정보의 저장공간을 탐색하기 위해 이용되는 상관관계를 가진다. 즉, 검증 서버(30)는 탐색 알고리즘(저장공간탐색알고리즘)을 구비하고, 상기 탐색 알고리즘은 가상코드에 포함된 복수의 세부코드를 추출하고, 상기 복수의 세부코드의 상관관계를 기반으로 사용자 또는 카드에 부여된 식별 정보의 저장공간을 탐색한다. 상기 복수의 세부코드가 가지는 상관관계에 대한 일 실시예로, 검증 서버(30)에 포함된 탐색 알고리즘은 복수의 세부코드 중 하나

이상의 세부코드에 대응하는 경유지점으로부터 상기 복수의 세부코드 간의 상관관계를 기반으로 연산하여 상기 사용자 또는 카드의 식별 정보의 저장위치를 탐색할 수 있다. 이때, 상기 경유지점은 하나 또는 복수일 수 있으며 개수 및 순서에 제한은 없다.

- [89] 또한, 복수의 세부코드의 일 실시예로, 복수의 세부코드는 제1코드 및 제2코드를 포함할 수 있고, OTAC 애플릿은 세부코드 생성 함수로 제1함수와 제2함수를 포함하여, 제1코드 및 제2코드를 생성한다. 제1코드와 제2코드는 검증 서버(30) 내에서 사용자 또는 카드의 식별 정보의 저장공간을 탐색하기 위한 상관관계를 가지나, OTAC 애플릿은 보안성을 높이기 위해 제1코드를 생성하는 제1함수와 제2코드를 생성하는 제2함수를 세부코드 생성 함수로 포함할 뿐, 제1코드와 제2코드의 상관관계에 대한 데이터를 포함하지 않을 수 있다.
- [90] 제1코드와 제2코드의 상관관계의 구체적인 예로, 제1코드와 제2코드는 상기 식별 정보의 저장공간을 탐색하기 위한 각각의 역할을 수행할 수 있다. 즉, 제1코드는 상기 경유지점에 대한 정보를 포함하고, 제2코드는 상기 경유지점으로부터 상기 식별 정보의 저장공간에 도달할 수 있는 연산에 필요한 정보를 포함할 수 있다.
- [91] 한편, 본 개시의 일 실시예로 제1코드는 제1카운트를 기반으로 생성되며, 제2코드는 제2카운트를 기반으로 생성될 수 있다. 이때, 제1카운트는 검증 서버(30)에서 가상코드 생성 함수가 구동된 최초시점으로부터 가상코드가 생성된 시점까지 경과된 단위 카운트의 개수이고, 제2카운트는 사용자 또는 카드의 식별 정보가 검증 서버(30)에 등록된 시점으로부터 경과된 단위 카운트 개수를 포함할 수 있다.
- [92] 즉, 제1코드를 생성하는 제1함수는 제1카운트에 대응되는 특정한 코드값을 제공하는 함수이고, 제2코드를 생성하는 제2함수는 제2카운트에 대응되는 특정한 코드값을 제공하는 함수이다.
- [93] 이하에서는, 가상코드 검증 장치로서의 역할을 수행하는 검증 서버(30)가 가상코드를 검증하는 방법에 대하여 구체적으로 설명하도록 한다.
- [94] 본 개시의 일 실시예로, 검증 서버(30)가 상기 사용자 단말(20)로부터 상기 가상코드를 수신하면, 상기 가상코드를 수신한 시간 데이터 및 상기 가상코드의 시간 데이터를 비교하여 상기 가상코드를 검증할 수 있다.
- [95] 구체적으로, 검증 서버(30)에서 가상코드가 정상적으로 생성된 것인지를 검증한다. 즉, 검증 서버(30)는 가상코드를 수신한 후 검증 서버(30)에 저장된 정보(즉, 가상코드 생성 함수 및 시드 데이터)를 바탕으로 상기 수신한 가상코드가 현 시점에 정상적으로 생성된 것인지를 확인하여 가상코드의 정상여부를 판단한다. 예를 들어, 검증 서버(30)는 가상코드 생성 함수(즉, OTP함수)를 가상코드를 수신한 카운트로부터 특정범위 내의 카운트를 입력하여 산출된 OTP번호 중에 가상코드와 일치하는 값이 있는지 여부를

확인한다. 검증 서버(30)는 가상코드에 가상코드 생성 함수의 역함수를 적용하여 가상코드가 생성된 시점에 상응하는 카운트를 찾아낸다. 가상코드의 전송시간이나 딜레이에 의해 가상코드가 생성된 시점과 검증 서버(30)가 가상코드를 수신한 시점의 차이가 존재함에 따라 검증 서버(30)가 가상코드를 수신한 카운트와 가상코드에 해당하는 OTP번호를 생성한 카운트가 일치하지 않을 수도 있으므로, 검증 서버(30)는 가상코드를 수신한 카운트로부터 오차범위를 허용한다.

- [96] 한편, 본 개시의 일 실시예로 검증 서버(30)는 상기 가상코드를 기반으로 사용자 또는 카드의 식별 정보의 저장 위치를 탐색하여 상기 사용자 또는 카드의 식별 정보를 추출하고, 상기 추출한 식별 정보를 기반으로 사용자 인증을 수행할 수 있다.
- [97] 도 5는 본 개시에 따른 검증 서버가 금융사 서버인 경우의 등록 프로세스를 설명하기 위한 도면이다. 이하에서는 도 5를 참조하여, 금융사에서 자체적으로 실물 카드(10)를 제작하고 발급하는 경우의 사용자 등록 프로세스를 설명하도록 한다.
- [98] 이러한 경우, 검증 서버(30)는 금융사 서버(31)가 되고, 상기 실물 카드(10)가 상기 금융사와 연계된 카드제조사에 의해 제작된다.
- [99] S130에서, 실물 카드(10)는 사용자 단말(20)을 통해 상기 검증 서버(30)로 상기 가상코드뿐만 실물 카드(10) 내에 기 저장되어 있던 실물 카드(10)의 카드번호 및 실물 카드(10)의 고유값 중 적어도 하나를 더 송신할 수 있다.
- [100] 그리고, 가상코드에 대한 검증이 완료되면, 검증 서버(30) 내에 상기 시드 데이터, 상기 실물 카드(10)의 카드번호 및 상기 실물 카드(10)의 고유값 중 적어도 하나, 및 상기 사용자 단말(20)에서 생성된 사용자 정보가 매칭되어 저장될 수 있다.
- [101] 보다 상세하게, 검증이 완료되면 검증 서버(30)는 가상코드 내에 포함된 시드 데이터를 추출하여, 추출된 시드 데이터와, 실물 카드(10)의 카드번호 및 실물 카드(10)의 고유값 중 적어도 하나, 그리고 사용자 정보를 매칭하여 해당 실물 카드(10)에 대한 사용자 등록을 완료할 수 있다. 여기서, 사용자 정보는 금융사 어플리케이션에 로그인된 사용자의 로그인 정보 및 사용자가 보유한 모바일 카드의 정보(모바일 카드번호)를 포함할 수 있다.
- [102] 실물 카드(10)의 카드번호, 실물 카드(10)의 고유값 및 상기 시드 데이터는, 상기 검증 서버(30)에 의해 상기 카드제조사의 서버로 전달되어, 상기 실물 카드(10)의 제작 시 IC 칩(EMV 애플릿 및 OTAC 애플릿)에 내장된다. 즉, 검증 서버(30)에는 실물 카드(10)의 카드번호, 실물 카드(10)의 고유값 및 실물 카드(10)의 시드 데이터가 이미 저장되어 있을 수 있다.
- [103] 여기서, 실물 카드(10)의 카드번호는 상기 금융사의 식별코드(예를 들어, BIN)를 포함하고, 실물 카드(10)의 고유값은 상기 카드제조사에 의해 제작되는 카드 별로 순차적으로 부여되는 값일 수 있다. 카드제조사는 가상코드(OTAC)

- 서버를 금융사시스템 내 WAS 서버에 설치하고, 실물 카드 제작 시에 가상코드(OTAC) 서버에서 제공한 상기 고유값을 순차적으로 입력할 수 있다.
- [104] 실시예에 따라, 실물 카드(10)가 사용자 단말(20)을 통해 가상코드, 실물 카드(10)의 카드번호 및 실물 카드(10)의 고유값을 검증 서버(30)로 송신하는 경우, 검증 서버(30)는 가상코드에 대한 검증 완료 후, 가상코드로부터 추출된 시드 데이터와 실물 카드(10)의 카드번호 및 실물 카드(10)의 고유값과 사용자 정보를 매칭하여 저장할 수 있다.
- [105] 실시예에 따라, 실물 카드(10)가 사용자 단말(20)을 통해 가상코드 및 실물 카드(10)의 카드번호를 검증 서버(30)로 송신하는 경우, 검증 서버(30)는 가상코드에 대한 검증 완료 후, 가상코드로부터 추출된 시드 데이터와 실물 카드(10)의 카드번호와 사용자 정보를 매칭하여 저장할 수 있다.
- [106] 실시예에 따라, 실물 카드(10)가 사용자 단말(20)을 통해 가상코드 및 실물 카드(10)의 고유값을 검증 서버(30)로 송신하는 경우, 검증 서버(30)는 가상코드에 대한 검증 완료 후, 가상코드로부터 추출된 시드 데이터와 실물 카드(10)의 고유값과 사용자 정보를 매칭하여 저장할 수 있다.
- [107] 실시예에 따라, 실물 카드(10)가 사용자 단말(20)을 통해 가상코드, 실물 카드(10)의 카드번호 및 실물 카드(10)의 고유값 중 제1정보(예를 들어, 카드번호)를 검증 서버(30)로 송신하는 경우, 검증 서버(30)는 가상코드에 대한 검증 완료 후, 가상코드로부터 시드 데이터를 추출하고, 카드번호 및 실물 카드(10)의 고유값 중 수신된 제1정보(예를 들어, 카드번호)로부터 제2정보(예를 들어, 고유값)를 추출하고, 추출된 시드 데이터와 추출된 제2정보(예를 들어, 고유값), 수신된 제1정보(예를 들어, 카드번호), 수신된 사용자 정보를 매칭하여 저장할 수 있다.
- [108] 도 5를 참조하면, 실물 카드(10)와 사용자 단말(20) 간에 태깅이 되면, 사용자 단말(20)은 실물 카드(10)로 현재 시간 데이터를 송신할 수 있다(S21). 실물 카드(10)는 수신된 현재 시간 데이터와 기 저장된 시드 데이터를 기반으로 가상코드를 생성할 수 있다(S22). 실물 카드(10)는 생성된 가상코드와, 기 저장된 실물 카드(10)의 카드번호 및 고유값 중 적어도 하나를 사용자 단말(20)로 송신할 수 있다(S23). 사용자 단말(20)은 수신된 가상코드, 실물 카드(10)의 카드번호 및 고유값 중 적어도 하나와 함께, 사용자 정보를 금융사 서버(31)로 송신한다(S24). 금융사 서버(31)는 가상코드가 현재점에 정상적으로 생성된 코드인지를 판단하는 검증을 수행할 수 있다(S25). 금융사 서버(31)는 가상코드가 정상적인 코드인 것으로 판단되면(검증이 완료되면), 시드 데이터, 카드의 카드번호 및 고유값 중 적어도 하나, 사용자 정보를 매칭하여 상기 실물 카드(10)에 대한 사용자 등록을 완료할 수 있다(S26).
- [109] 이에 따라, 금융사 서버(31) 내에서 상기 실물 카드(10)와 상기 모바일 카드가 연결되어, 이후 사용자가 실물 카드(10)를 이용하여 오프라인 결제를 요청하면, 실물 카드(10)와 연결된 모바일 카드를 이용하여 결제가 진행될 수 있다. 여기서,

실물 카드(10)와 모바일 카드는 금융사 서버(31) 내에서 실물 카드번호와 모바일 카드번호가 매칭되어 저장됨으로써 연결될 수 있다.

- [110] 도 6 및 도 7은 본 개시에 따른 검증 서버가 카드발급을 대행하는 서비스 서버인 경우의 등록 프로세스를 설명하기 위한 도면이다. 이하에서는 도 6 및 도 7을 참조하여, 금융사가 외부에서 제작한 실물 카드(10)를 이용하는 경우의 사용자 등록 프로세스를 설명하도록 한다. 이렇게 금융사가 자체적으로 제작하지 않고 외부에서 제작한 실물 카드를 이용하는 이유는, 현재 오프라인에서 사용 가능한 실물 카드의 발급 장수가 줄어들고 있고, 실물 카드와 모바일카드/모바일결제가 공존하는 추세이므로, 금융사는 관련 비용(실물 카드 제작 및 배송 비용)을 절감하면서 실물 카드를 사용자에게 발급할 수 있는 서비스를 필요로 하기 때문이다.
- [111] 이렇게 카드발급을 대행하는 서비스 제공사에서 제작한 실물 카드(10)를 이용하는 경우, 검증 서버(30)는 카드발급을 대행하는 서비스 서버(32)(이하, 서비스 서버)가 되고, 상기 실물 카드(10)가 상기 카드발급 대행 서비스의 제공사에 의해 제작된다.
- [112] 이렇게 서비스 제공사에서 제작한 실물 카드(10)를 이용하는 경우, 사용자 등록은 실물 카드 등록용 어플리케이션 기반의 제1 방식 또는 실물 카드 등록용 인터페이스 기반의 제2 방식에 의해 수행될 수 있다.
- [113] - 제1 방식에 의해 수행되는 경우 사용자 등록 방식
- [114] 사용자 단말(20)은 상기 서비스 서버(32)가 제공하는 상기 등록용 어플리케이션이 구비될 수 있다.
- [115] 제1 방식의 사용자 등록은 상기 등록용 어플리케이션을 통해 상기 사용자가 기 보유한 모바일 카드의 카드번호가 입력된 후에, 상기 실물 카드(10) 및 사용자 단말(20) 간의 태깅을 통해 수행될 수 있다.
- [116] 여기서, 제1 방식의 사용자 등록은, 상기 서비스 서버(32)에 의해 상기 가상코드 기반으로 탐색된 상기 실물 카드(10)의 카드번호와 상기 모바일 카드의 카드번호가 매칭되어 수행될 수 있다.
- [117] 이후, 사용자가 상기 등록이 완료된 상기 실물 카드(10)를 이용하여 결제를 요청하는 경우, 상기 실물 카드(10)의 카드번호가 결제망을 통해 결제 서버(미도시)로부터 상기 서비스 서버(32)로 송신되고, 상기 실물 카드(10)의 카드번호에 매칭된 상기 모바일 카드의 카드번호는 상기 결제망을 통해 상기 서비스 서버(32)로부터 상기 결제 서버로 송신될 수 있다.
- [118] 이때, 서비스 서버(32)는 실물 카드(10)(실물 카드번호)를 이용한 결제 건수, 실물 카드(10)를 카드발급 대행 서비스를 통해서 발급받아서 사용하는 사용자 수에 따라 금융사에게 과금을 청구할 수 있다.
- [119] 도 6을 참조하면, 서비스 서버(32)는 등록용 어플리케이션을 사용자 단말(20)로 제공할 수 있다(S31). 사용자 단말(20)은 등록용 어플리케이션을 설치할 수 있다(S32). 사용자는 등록용 어플리케이션을 통해 자신이 사용하고 있는 모바일

카드의 카드번호를 입력할 수 있다(S33). 그런 다음 실물 카드(10)와 사용자 단말(20) 간에 태깅이 되면, 사용자 단말(20)은 실물 카드(10)로 현재 시간 데이터를 송신할 수 있다(S34). 실물 카드(10)는 수신된 현재 시간 데이터와 기 저장된 시드 데이터를 기반으로 가상코드를 생성할 수 있다(S35). 실물 카드(10)는 생성된 가상코드를 사용자 단말(20)로 송신할 수 있다(S36). 사용자 단말(20)은 가상코드와 사용자가 입력한 모바일 카드의 카드번호를 서비스 서버(32)로 송신할 수 있다(S37). 서비스 서버(32)는 가상코드를 기반으로 실물 카드(10)의 카드번호를 탐색할 수 있다(S38). 구체적으로, 발급 대행 서버(32)는 가상코드에 포함된 시드 데이터를 추출하고, 서버 내에 상기 시드 데이터에 매칭되어 저장된 실물 카드번호를 탐색할 수 있다. 서비스 서버(32)는 탐색된 실물 카드의 카드번호를 모바일 카드의 카드번호와 매칭하여 사용자 등록을 완료할 수 있다(S39).

- [120] 이에 따라, 이후 사용자가 실물 카드(10)를 이용하여 오프라인 결제를 요청하면, 서비스 서버(32)는 결제망을 통해 결제 서버(미도시)로부터 실물 카드의 카드번호를 수신할 수 있다. 서비스 서버(20)는 수신된 실물 카드의 카드번호(실물 카드번호)에 매칭된 모바일 카드의 카드번호(모바일 카드번호)를 결제망을 통해 상기 결제 서버로 제공하여, 결제 서버가 모바일 카드번호를 이용하여 결제를 진행하도록 할 수 있다.
- [121] - 제2 방식에 의해 수행되는 경우 사용자 등록 방식
- [122] 사용자 단말(20)에 설치된 금융사 어플리케이션에 상기 카드발급 대행 서비스와 연동되는 등록용 인터페이스가 생성되고, 이후 사용자 단말(20)에 실물 카드(10)가 태깅되면 상기 등록용 인터페이스를 통해 제2 방식의 사용자 등록이 수행될 수 있다. 이때, 등록용 인터페이스는, 상기 서비스 서버(32)의 SDK 및 API 연동을 통해 생성될 수 있다.
- [123] 여기서, 제2 방식의 사용자 등록은, 상기 등록용 인터페이스를 통해 상기 서비스 서버(32)로 송신된 상기 가상코드 및 사용자의 고유값을 기반으로 수행될 수 있다.
- [124] 이후, 사용자가 상기 등록이 완료된 실물 카드(10)를 이용하여 결제를 요청하는 경우, 실물 카드(10)의 카드번호(실물 카드번호)가 결제망을 통해 결제 서버(미도시)로부터 서비스 서버(32)로 송신되면, 서비스 서버(32)는 수신된 실물 카드번호를 이용하여 상기 사용자의 고유값을 추출할 수 있다. 서비스 서버(32)는 추출된 사용자의 고유값 및 금융사 정보를 기반으로 금융사 서버로 상기 사용자의 고유값을 송신할 수 있다. 금융사 서버는 사용자의 고유값을 이용하여 사용자에게 발급한 모바일 카드의 카드번호(모바일 카드번호)를 탐색하여 결제를 수행할 수 있다. 여기서, 사용자의 고유값은 실물 카드(10)와의 연결이 요청된 특정 모바일 카드에 대한 사용자의 식별정보를 의미할 수 있다.
- [125] 이때, 서비스 서버(32)는 실물 카드(10)를 이용한 결제 건수, 실물 카드(10)를 카드발급 대행 서비스를 통해서 발급받아서 사용하는 사용자 수에 따라

금융사에게 과금을 청구할 수 있다.

- [126] 도 7을 참조하면, 사용자 단말(20)에 설치된 금융사 어플리케이션에 서비스 서버(32)와 연동되는 등록용 인터페이스가 생성될 수 있다(S41). 이때, 등록용 인터페이스는 사용자가 금융사 어플리케이션에 등록된 모바일 카드 중에서 실제 카드(10)와의 연결을 원하는 특정 모바일 카드를 선택했을 때 생성될 수 있다. 그런 다음, 실물 카드(10)와 사용자 단말(20) 간에 태깅이 되면, 사용자 단말(20)은 실물 카드(10)로 현재 시간 데이터를 송신할 수 있다(S42). 실물 카드(10)는 수신된 현재 시간 데이터와 기 저장된 시드 데이터를 기반으로 가상코드를 생성할 수 있다(S43). 실물 카드(10)는 생성된 가상코드를 사용자 단말(20)로 송신할 수 있다(S44). 사용자 단말(20)은 가상코드와 사용자의 고유값을 서비스 서버(32)로 송신할 수 있다(S45). 여기서, 사용자의 고유값은 상기 특정 모바일 카드에 대한 사용자 식별정보를 의미할 수 있다. 서비스 서버(32)는 가상코드를 기반으로 실물 카드(10)의 카드번호(실물 카드번호)를 탐색할 수 있다(S46). 구체적으로, 서비스 서버(32)는 가상코드에 포함된 시드 데이터를 추출하고, 서버 내에 상기 시드 데이터에 매칭되어 저장된 실물 카드번호를 탐색할 수 있다. 서비스 서버(32)는 탐색된 실물 카드의 카드번호를 상기 사용자의 고유값과 매칭하여 사용자 등록을 완료할 수 있다(S47).
- [127] 이에 따라, 이후 사용자가 실물 카드(10)를 이용하여 오프라인 결제를 요청하면, 서비스 서버(32)는 결제망을 통해 결제 서버(미도시)로부터 실물 카드의 카드번호를 수신할 수 있다. 서비스 서버(20)은 수신된 실물 카드의 카드번호(실물 카드번호)에 매칭된 사용자의 고유값과 금융사 정보를 이용하여 해당 금융사 서버로 사용자의 고유값을 송신할 수 있다. 금융사 서버는 수신된 사용자의 고유값을 이용하여 해당 실제 카드(10)와 연결된 모바일 카드의 카드번호를 탐색하여 결제를 진행할 수 있다.
- [128] 도 3, 도 5 내지 도 7은 단계들을 순차적으로 실행하는 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 3, 도 5 내지 도 7에 기재된 순서를 변경하여 실행하거나 병렬적으로 실행하는 것으로 다양하게 수정 및 변형하여 적용 가능할 것이므로, 도 3, 도 5 내지 도 7은 시계열적인 순서로 한정되는 것은 아니다.
- [129] 한편, 상술한 설명에서, 도 3, 도 5 내지 도 7에 기재된 단계들은 본 개시의 구현예에 따라서, 추가적인 단계들로 더 분할되거나, 더 적은 단계들로 조합될 수 있다. 또한, 일부 단계는 필요에 따라 생략될 수도 있고, 단계 간의 순서가 변경될 수도 있다.
- [130]
- [131] 도 8은 본 개시에 따른 컴퓨팅 장치를 나타내는 도면이다. 컴퓨팅 장치(TN100)는 본 명세서에서 기술된 장치(예, 사용자 단말(20), 검증 서버(30))

등)일 수 있다.

- [132] 컴퓨팅 장치(TN100)는 적어도 하나의 프로세서(TN110), 송수신 장치(TN120), 및 메모리(TN130)를 포함할 수 있다. 또한, 컴퓨팅 장치(TN100)는 저장 장치(TN140), 입력 인터페이스 장치(TN150), 출력 인터페이스 장치(TN160) 등을 더 포함할 수 있다. 컴퓨팅 장치(TN100)에 포함된 구성 요소들은 버스(bus)(TN170)에 의해 연결되어 서로 통신을 수행할 수 있다.
- [133] 프로세서(TN110)는 메모리(TN130) 및 저장 장치(TN140) 중에서 적어도 하나에 저장된 프로그램 명령(program command)을 실행할 수 있다. 프로세서(TN110)는 중앙 처리 장치(CPU: central processing unit), 그래픽 처리 장치(GPU: graphics processing unit), 또는 본 발명의 실시예에 따른 방법들이 수행되는 전용의 프로세서를 의미할 수 있다. 프로세서(TN110)는 본 발명의 실시예와 관련하여 기술된 절차, 기능, 및 방법 등을 구현하도록 구성될 수 있다. 프로세서(TN110)는 컴퓨팅 장치(TN100)의 각 구성 요소를 제어할 수 있다.
- [134] 메모리(TN130) 및 저장 장치(TN140) 각각은 프로세서(TN110)의 동작과 관련된 다양한 정보를 저장할 수 있다. 메모리(TN130) 및 저장 장치(TN140) 각각은 휘발성 저장 매체 및 비휘발성 저장 매체 중에서 적어도 하나로 구성될 수 있다. 예를 들어, 메모리(TN130)는 읽기 전용 메모리(ROM: read only memory) 및 랜덤 액세스 메모리(RAM: random access memory) 중에서 적어도 하나로 구성될 수 있다.
- [135] 송수신 장치(TN120)는 유선 신호 또는 무선 신호를 송신 또는 수신할 수 있다. 송수신 장치(TN120)는 네트워크에 연결되어 통신을 수행할 수 있다.
- [136]
- [137] 한편, 개시된 실시예들은 컴퓨터에 의해 실행 가능한 명령어를 저장하는 기록매체의 형태로 구현될 수 있다. 명령어는 프로그램 코드의 형태로 저장될 수 있으며, 프로세서에 의해 실행되었을 때, 프로그램 모듈을 생성하여 개시된 실시예들의 동작을 수행할 수 있다. 기록매체는 컴퓨터로 읽을 수 있는 기록매체로 구현될 수 있다.
- [138] 컴퓨터가 읽을 수 있는 기록매체로는 컴퓨터에 의하여 해독될 수 있는 명령어가 저장된 모든 종류의 기록 매체를 포함한다. 예를 들어, ROM(Read Only Memory), RAM(Random Access Memory), 자기 테이프, 자기 디스크, 플래쉬 메모리, 광 데이터 저장장치 등이 있을 수 있다.
- [139] 이상에서와 같이 첨부된 도면을 참조하여 개시된 실시예들을 설명하였다. 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자는 본 개시의 기술적 사상이나 필수적인 특징을 변경하지 않고도, 개시된 실시예들과 다른 형태로 본 개시가 실시될 수 있음을 이해할 것이다. 개시된 실시예들은 예시적인 것이며, 한정적으로 해석되어서는 안 된다.

청구범위

- [청구항 1] 사용자가 등록되지 않은 실물 형태의 홀더리스(Holderless) 카드에 의해 수행되는 방법에 있어서,
카드 태깅을 통해 상기 사용자의 단말로부터 현재 시간 데이터를 수신하는 단계;
상기 카드에 포함된 애플릿(Applet)을 이용하여, 상기 현재 시간 데이터 및 기 저장된 시드 데이터를 기반으로 상기 사용자의 인증을 위한 가상코드를 생성하는 단계; 및
상기 가상코드를 상기 사용자 단말을 통해 검증 서버로 송신하여 상기 가상코드에 대한 검증을 요청하는 단계;를 포함하고,
상기 카드는, 상기 사용자가 등록되지 않은 상태로 제작되고, 상기 검증이 완료되면 상기 검증 서버 내에 상기 사용자가 기 보유한 모바일 카드와 연결되어 상기 사용자가 등록되는 것인,
인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 방법.
- [청구항 2] 제1항에 있어서,
상기 검증 서버가 금융사 서버이고, 상기 카드가 상기 금융사와 연계된 카드제조사에 의해 제작되는 경우,
상기 검증 요청 단계는,
상기 사용자 단말을 통해 상기 검증 서버로 기 저장된 상기 카드의 카드번호 및 상기 카드의 고유값 중 적어도 하나를 더 송신하여 상기 검증을 요청하고,
상기 검증이 완료되면, 상기 검증 서버 내에 상기 시드 데이터, 상기 카드의 카드번호 및 상기 카드의 고유값 중 적어도 하나, 및 상기 사용자 단말에서 생성된 사용자 정보가 매칭되어 저장되는,
인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 방법.
- [청구항 3] 제2항에 있어서,
상기 카드의 카드번호, 상기 카드의 고유값 및 상기 시드 데이터는, 상기 검증 서버에 의해 상기 카드제조사의 서버로 전달되어, 상기 카드의 제작 시 IC 칩에 내장되고,
상기 카드의 카드번호는, 상기 금융사의 식별코드를 포함하고,
상기 카드의 고유값은, 상기 카드제조사에 의해 제작되는 카드 별로 순차적으로 부여되는 값인,
인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 방법.
- [청구항 4] 제1항에 있어서,
상기 검증 서버가 카드발급을 대행하는 서비스 서버이고, 상기 카드가 상기 카드발급 대행 서비스의 제공사에 의해 제작되는 경우,
상기 사용자의 등록은, 실물 카드 등록용 어플리케이션 기반의 제1 방식

- 또는 실물 카드 등록용 인터페이스 기반의 제2 방식에 의해 수행되는, 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 방법
- [청구항 5] 제4항에 있어서,
상기 사용자 단말은, 상기 서비스 서버에 의해 제공되는 상기 어플리케이션이 구비되고,
상기 제1 방식의 사용자 등록은, 상기 어플리케이션을 통해 상기 모바일 카드의 카드번호가 입력된 후에 상기 카드 태깅을 통해 수행되는, 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 방법.
- [청구항 6] 제5항에 있어서,
상기 제1 방식의 사용자 등록은, 상기 서비스 서버에 의해 상기 가상코드 기반으로 탐색된 상기 카드의 카드번호와 상기 모바일 카드의 카드번호가 매칭되어 수행되고,
상기 카드의 카드번호는, 상기 등록이 완료된 상기 카드를 통해 결제가 요청되는 경우에 결제망을 통해 결제 서버로부터 상기 서비스 서버로 송신되고,
상기 카드의 카드번호에 매칭된 상기 모바일 카드의 카드번호는, 상기 결제망을 통해 상기 서비스 서버로부터 상기 결제 서버로 송신되는, 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 방법.
- [청구항 7] 제4항에 있어서,
상기 제2 방식의 사용자 등록은, 금융사의 어플리케이션에 상기 카드발급 대행 서비스와 연동되는 상기 인터페이스가 생성된 후에 상기 카드 태깅을 통해 수행되는, 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 방법.
- [청구항 8] 제7항에 있어서,
상기 제2 방식의 사용자 등록은, 상기 인터페이스를 통해 상기 서비스 서버로 송신된 상기 가상코드 및 상기 사용자의 고유값을 기반으로 수행되며,
상기 카드의 카드번호는, 상기 등록이 완료된 상기 카드를 통해 결제가 요청되는 경우에 결제망을 통해 결제 서버로부터 상기 서비스 서버로 송신되어 상기 사용자 고유값 추출에 이용되고,
상기 사용자 고유값은, 상기 금융사의 서버로 송신되어 상기 모바일 카드의 카드번호 추출에 이용되는, 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 방법.
- [청구항 9] 제1항에 있어서,
상기 수신 단계는, 상기 카드 태깅 시에 상기 애플릿의 구동을 위한 APDU 명령어와 함께 상기 현재 시간 데이터가 수신되고,
상기 생성 단계는, 상기 APDU 명령어에 따라 상기 애플릿이 구동되어 생성되는,

- 인증용 가상코드를 이용하여 홀더리스 카드에 사용자를 등록하는 방법.
- [청구항 10] 컴퓨터와 결합되어, 제1항의 방법을 실행하기 위해 컴퓨터 판독 가능한 기록 매체에 저장된 프로그램.
- [청구항 11] 사용자가 등록되지 않은 실물 형태의 홀더리스(Holderless) 카드 장치에 있어서,
 상기 사용자의 단말과 태깅 시에 NFC 기반의 통신을 수행하는 NFC 모듈;
 및
 상기 사용자의 인증을 위한 가상코드를 생성하기 위한 애플릿(Applet)이 포함된 IC 모듈;을 포함하고,
 상기 IC 모듈은,
 상기 사용자 단말과 태깅 시, 상기 NFC 모듈을 통해 상기 사용자 단말로부터 현재 시간 데이터를 수신하고,
 상기 애플릿을 제어하여, 상기 현재 시간 데이터 및 기 저장된 시드 데이터를 기반으로 가상코드를 생성하며,
 상기 가상코드가 상기 사용자 단말을 통해 검증 서버로 송신되도록 하여,
 상기 검증 서버에 상기 가상코드에 대한 검증을 요청하고,
 상기 카드 장치는, 상기 사용자가 등록되지 않은 상태로 제작되고, 상기 검증이 완료되면 상기 검증 서버 내에 상기 사용자가 기 보유한 모바일 카드와 연결되어 상기 사용자가 등록되는 것인,
 실물 형태의 홀더리스 카드 장치.