(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년01월23일
(11) 등록번호 10-1354388
(24) 등록일자 2014년01월15일

(51) 국제특허분류(Int. Cl.)
G06Q 40/02 (2012.01) *G06Q 20/30* (2012.01)
(21) 출원번호 10-2012-0144216
(22) 출원일자 2012년12월12일
심사청구일자 2012년12월12일
(56) 선행기술조사문헌
KR1020050034058 A*
KR1020120086790 A*
KR1020120086790 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
신한카드 주식회사
서울특별시 중구 소공로 70 (충무로1가)
현대카드 주식회사
서울특별시 영등포구 의사당대로 3 (여의도동)
주식회사 케이비국민카드
서울특별시 종로구 새문안로3길 30 (내수동)
(72) 발명자
박해철
서울특별시 동작구 상도로 346-1 110동 404호(상도동, 상도엠코타운 센트럴파크)
김병수
서울특별시 용산구 새창로8길 157 101동 206호(산천동, 한강타운아파트)
이정진
서울특별시 송파구 백제고분로19길 30-25 (잠실동)
(74) 대리인
이준성

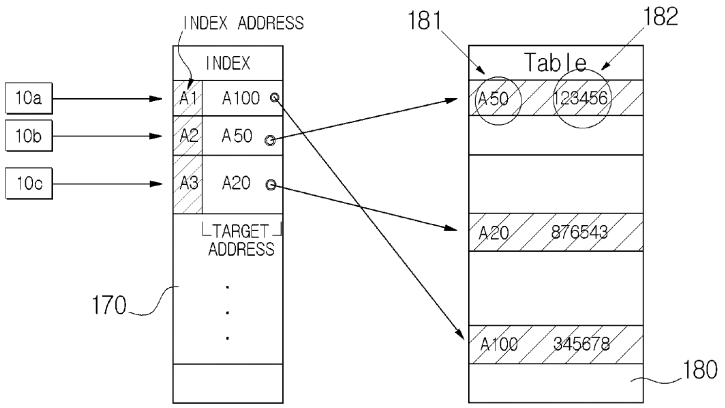
전체 청구항 수 : 총 8 항 심사관 : 이정재

(54) 발명의 명칭 **일회성 카드번호 생성방법**

(57) 요 약

본 발명은 결제 디바이스로 일회성 카드번호를 발급하되, 발급되는 일회성 카드번호가 타인에 의해 유추 또는 예측이 불가한 방식으로 생성함으로써, 보안성이 향상된 신용 결제를 수행할 수 있도록 하는 일회성 카드번호 생성 방법을 개시한다. 이를 위해 본 발명은, 무선 네트워크 접속되는 결제 디바이스로부터 일회성 카드번호가 요청될 때, 결제 디바이스로 일회성 카드번호를 제공하는 카드사 서버를 통해 수행되며, 결제 디바이스가 일회성 카드번호를 요청 시, 일회성 카드번호를 요청하는 순번에 따라 결제 디바이스를 인덱스 테이블에 할당하는 단계, 인덱스 테이블에서 비 순차로 마련되는 타겟 어드레스를 이용하여 일회성 번호가 구비되는 일회성 카드번호 테이블에서 숫자열을 획득하는 단계 및 숫자열 및 공개 상태의 BIN(Bank Identification Number)을 포함하는 일회성 카드번호를 생성하는 단계를 포함할 수 있다.

대 표 도



특허청구의 범위

청구항 1

무선 네트워크 접속되는 결제 디바이스로부터 일회성 카드번호가 요청될 때, 상기 결제 디바이스로 일회성 카드번호를 제공하는 카드사 서버를 통해 수행되며,

상기 결제 디바이스가 상기 일회성 카드번호를 요청 시, 상기 일회성 카드번호를 요청하는 순서에 따라 상기 결제 디바이스를 인덱스 테이블에 할당하는 단계;

상기 인덱스 테이블에서 상기 할당된 결제 디바이스에 대응하여 랜덤(random)하게 지정된 타겟 어드레스를 획득하고, 복수의 일회성 번호가 구비된 카드 번호 테이블에서 상기 획득한 타겟 어드레스를 이용하여 상기 복수의 일회성 번호 중 상기 타겟 어드레스에 대응되는 일회성 번호를 포함하는 숫자열을 획득하는 단계;

상기 획득한 상기 숫자열 및 공개 상태의 BIN(Bank Identification Number)을 포함하는 일회성 카드번호를 생성하는 단계; 및

상기 생성된 일회성 카드번호를 상기 결제 디바이스에 제공하는 단계를 포함하며,

상기 지정된 타겟 어드레스는 상기 인덱스 테이블에 포함된 미리 결정된 복수의 타겟 어드레스 중 적어도 일부를 비 순차로 선택하는 방법에 의해 결정되는 문자열이고,

상기 일회성 번호는 한 쌍의 헥사데시멀(Hexa-decimal) 코드열을 이용하여 미리 결정된 길이의 10진수 숫자열을 생성하는 방법에 의해 결정되는 숫자열이고,

상기 문자열은 적어도 하나의 숫자 또는 문자를 포함하고,

상기 타겟 어드레스에 포함된 문자 또는 숫자의 개수와 상기 일회성 번호에 포함된 숫자의 개수는 서로 상이한 것을 특징으로 하는 일회성 카드번호 생성방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 타겟 어드레스의 값은,

상기 인덱스 테이블의 어드레스 순서에 따르지 않고 불규칙하게 배열되며,

상기 인덱스 테이블에는 동일한 타겟 어드레스 값이 존재하지 않는 것을 특징으로 하는 일회성 카드번호 생성방법.

청구항 5

삭제

청구항 6

제1항에 있어서,

상기 일회성 카드번호는,

BIN(Bank Identification Number), 상기 일회성 번호 및 제휴사에 대응하는 예비 코드를 포함하여 구성되는 것을 특징으로 하는 일회성 카드번호 생성방법.

청구항 7

제6항에 있어서,

상기 예비 코드는,

부가서비스 정보 및 제휴사 카드정보 중 어느 하나를 포함하는 것을 특징으로 하는 일회성 카드번호 생성방법.

청구항 8

제6항에 있어서,

상기 일회성 카드번호는,

상기 BIN과 상기 일회성 번호 사이에 마련되며,

상기 BIN의 데이터 필드 연장을 위한 예비 필드를 더 포함하는 것을 특징으로 하는 일회성 카드번호 생성방법.

청구항 9

삭제

청구항 10

제1항에 있어서,

상기 일회성 번호는,

임의의 숫자열로서, 16진수로 형성되는 제1헥사데시멀 코드열, 및 제2헥사데시멀 코드열을 이용하여 생성하고,

상기 제1헥사데시멀 코드열과 상기 제2헥사데시멀 코드열 각각은 상위 자릿수는 숫자만으로 구성되고 하위 자릿수는 16진수 값을 10진수로 치환하여 생성하는 제1숫자열과 제2숫자열을 생성하며,

상기 제1숫자열을 반분하여 가산한 제1가산값과 상기 제2숫자열을 반분하여 가산한 제2가산값에 대해 재차 가산 후, 상위 3 자릿수를 제거하여 얻는 숫자열인 것을 특징으로 하는 일회성 카드번호 생성방법.

청구항 11

삭제

청구항 12

제1항에 있어서,

상기 일회성 카드번호는,

상기 일회성 카드번호의 검증을 위한 OVC(One time code Verification Code)를 더 포함하며,

상기 OVC는 BIN(Bank Identification Number)과 상기 일회성 번호로 구성되는 일회성 카드번호의 부분 영역, 상기 결제 디바이스에서 상기 일회성 카드번호를 요청한 요청시간 정보 및 실물 카드번호를 SHA(Scure Hash Standard) 알고리즘의 인자로 하여 생성되는 것을 특징으로 하는 일회성 카드번호 생성방법.

청구항 13

삭제

청구항 14

제12항에 있어서,

상기 인자는 UUID(Universally unique identifier)를 더 포함하는 것을 특징으로 하는 일회성 카드번호 생성방법.

명 세 서

기 술 분 야

[0001] 본 발명은 일회성 카드번호 생성방법에 관한 것으로, 더욱 상세하게는 모바일 환경에서 스마트폰 및 휴대폰과 같은 결제 디바이스가 일회성 카드번호를 이용하여 결제를 진행하도록 하되, 일회성 카드번호가 타인에 의해 예측이 불가한 방식으로 생성되도록 함으로써 모바일 결제의 보안성을 향상시키는 일회성 카드번호 생성방법에 관한 것이다.

배 경 기 술

[0002] 현금은 결제에 필요한 금액에 비례하여 그 부피가 증가하는 측면이 있으나, 신용카드는 사용이 간편하면서도 결제 금액에 관계없이 한 장의 플라스틱 카드 형태의 미디어를 카드 리더기에 근접, 또는 접촉함으로써 결제를 진행 가능한 편리함이 있다.

[0003] 신용카드는 플라스틱, 또는 금속 재질의 몸체에 양각 또는 음각으로 16자리의 숫자열이 새겨지고, 숫자열에는 BIN(Bank Identification Number), 카드 번호 및 CVC(Card Validation Code) 값을 포함하고 있으며, 현재, 카드번호와 유효기간 만으로도 신용 결제가 가능한 경우가 많다. 따라서, 카드번호나 유효기간 정보는 타인에게 노출되지 않도록 관리될 필요가 있으나, 신용카드와 접촉 또는 근접하는 카드 리더기에서 카드번호나 유효기간 정보를 판독 가능하며, 카드 리더기에서 중계 서버(예컨대 VAN(Value Added Netwokr) 서버)를 경유하여 카드사 서버로 향하는 결제 프로세스 중에서 해커나 타인에 의해 카드번호가 노출될 위험성이 있다.

[0004] 이러한 문제에 대해 한국 공개특허 10-2001-0112546은 신용카드 리더기 - 중계 서버 - 카드사 서버로 이어지는 기존의 결제 프로세스에 임시 신용카드 번호 생성 서버를 부가하여 임시 카드번호를 이용토록 하는 신용카드를 이용한 전자 상거래 시스템을 제안한 바 있다.

[0005] 10-2001-0112546은 사용자 단말기(퍼스널 컴퓨터)에서 임시 신용카드 번호 생성 서버로 임시 신용카드 번호를 요청 시, 임시 신용카드 번호 생성 서버가 임시 카드번호와 유효기간을 설정하고, 이를 카드사 서버로 통보하며, 통보된 임시 카드번호를 사용자 단말기로 제공함으로써 사용자 단말기가 임시 카드번호를 이용하여 전자 상거래를 진행할 수 있도록 한다.

[0006] 그러나, 10-2001-0112546은 카드 리더기 - 중계 서버 - 카드사 서버로 이어지는 기존의 결제 프로세스에 임시 신용카드 번호를 발급하기 위한 별도의 임시 신용카드 번호 생성 서버를 부가해야 하고, 임시로 생성된 임시 신용카드 번호의 유효성을 신용카드사 서버에서 검증해야 하므로 결제 프로세스가 길어지고 복잡해질 수 있다. 또한, 10-2001-0112546에서는 임시 신용카드 번호를 생성하는 방법이 구체화되지 않았는데, 이런 경우, 통상 순차로 생성되는 숫자열을 사용자 단말기에 할당하는 방법이 주로 이용되는 바, 생성되는 임시 신용카드 번호는 해커, 또는 타인에 의해 유추될 우려가 존재한다.

발명의 내용

해결하려는 과제

[0007] 본 발명의 목적은 타인에 의해 순번 예측, 및 알고리즘 예측이 어려운 일회성 카드번호를 생성하고 이를 이용하여 보안성이 향상된 신용 결제를 수행할 수 있도록 하는 카드번호 생성방법을 제공함에 있다.

과제의 해결 수단

[0008] 상기한 목적은 본 발명에 따라, 무선 네트워크 접속되는 결제 디바이스로부터 일회성 카드번호가 요청될 때, 상기 결제 디바이스로 일회성 카드번호를 제공하는 카드사 서버를 통해 수행되며, 상기 결제 디바이스가 상기 일회성 카드번호를 요청 시, 상기 일회성 카드번호를 요청하는 순번에 따라 상기 결제 디바이스를 인덱스 테이블에 할당하는 단계, 상기 인덱스 테이블에서 비 순차로 마련되는 타겟 어드레스를 이용하여 일회성 번호가 구비되는 일회성 카드번호 테이블에서 상기 숫자열을 획득하는 단계 및 상기 숫자열 및 공개 상태의 BIN(Bank Identification Number)을 포함하는 일회성 카드번호를 생성하는 단계에 의해 달성된다.

발명의 효과

[0009] 본 발명에 따르면, 결제 디바이스로 일회성 카드번호를 발급하되, 발급되는 일회성 카드번호가 타인에 의해 유추 또는 예측이 불가한 방식으로 생성함으로써, 보안성이 향상된 신용 결제를 수행할 수 있도록 한다.

도면의 간단한 설명

[0010] 도 1은 본 발명의 일 실시예에 따라 일회성 카드번호를 생성하는 방법에 대한 개념도를 도시한다.

도 2 내지 도 5는 일회성 카드번호의 구조에 대한 참조도면을 도시한다.

도 6은 일회성 카드번호를 생성하는 카드사 서버의 일 예에 대한 블록개념도를 도시한다.

도 7과 도 8은 OVC 검증방법의 일 예에 대한 참조도면을 도시한다.

도 9는 일회성 번호 생성방법의 일 예에 대한 참조도면을 도시한다.

도 10은 OVC를 생성하는 일 예에 대한 참조도면을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0011] 본 명세서에서 언급되는 결제 디바이스는, 모바일 환경에서 비용 결제가 가능한 장치를 의미할 수 있다. 모바일 환경에서 비용 결제가 가능한 장치로서, 모바일 폰(Mobile Phone), 스마트 폰(Smart Phone), 노트북 및 PDA(Personal Digital Assistant)와 같은 장치가 있으나, 이 외에도 무선 통신이 가능하고, USIM(Universal Subscriber Identity Module) 칩 또는 금융사에서 신용카드 결제를 대체하는 금융 칩 및 기타 금융 거래를 위한 전자 칩을 장착 가능한 장치를 지칭할 수도 있다.

[0012] 본 명세서에서 언급되는 "신용카드" 는 신용카드 자체는 물론이고, 신용카드를 대신하여 카드 리더기로 카드번호 또는 카드번호에 준하거나, 카드번호를 대체하는 정보를 전송하는 휴대단말기 그 자체를 의미할 수도 있다. 즉, 본 명세서에서 신용카드의 의미는 자기식 신용카드, 전자 신용카드는 물론, 모바일 환경에서 비용 결제가 가능한 휴대단말기를 지칭할 수 있는 것이며, 굳이 카드 형태의 매체에 그 의미가 한정되지는 않는다.

[0013] 본 명세서에서 언급되는 중계 서버는 카드 리더기와 카드사 서버 사이에 마련되는 서버를 의미할 수 있다. 또는 중계 서버는, 카드사 서버나 VAN 서버에 네트워크 접속되는 POS(Point Of Sales system) 서버를 의미할 수도 있다. 또는, 중계 서버는, 카드 리더기에서 결제 데이터를 카드사 서버로 전송 시, 각 카드사를 대행하여 매출 전표를 수집 관리하고, 카드 리더기에서 전송된 결제 데이터에서 카드사 정보를 파악하여 결제 데이터를 해당 카드사 서버로 제공하는 VAN(Value Added Network) 서버일 수 있다.

[0014] 본 명세서에서 언급되는 카드 리더기는, 기존의 MS(Magnetic Strip) 신용카드에서 트랙 2 정보를 읽어내는 종류의 카드 리더기, 기존의 전자 신용카드에 내장되는 IC 칩과 접촉(또는 근접)하여 트랙 2 정보를 읽어내는 종류의 카드 리더기 및 휴대폰이나 스마트폰 같은 휴대단말기와 근거리 무선통신을 수행하여 이들 휴대단말기로부터 트랙 2 정보를 얻는 형태의 것이 존재할 수 있다.

[0015] 따라서, 카드 리더기는 자기식 신용카드와 접촉하여 ISO/IEC 7813 규격의 트랙 2 정보를 획득하는 장치, 전자 신용카드 또는 USIM 칩이나 금융 칩을 내장하는 휴대단말기 중 어느 하나와 접촉 또는 근접하여 본 발명에 따른 일회성 카드정보를 읽어내고, 이를 중계 서버를 통해 카드사 서버로 전송할 수 있는 장치를 의미할 수 있다.

[0016] 본 명세서에서 결제 디바이스는 카드 리더기와 근거리 무선통신을 수행할 수 있다. 이때, 결제 디바이스는 NFC(Near Field Communication) 기능의 칩을 휴대단말기 내에 별도로 내장하거나 또는 USIM 칩과 일체로 형성하는 것을 구비할 수 있다.

[0017] 이하, 도면을 참조하여 본 발명을 상세히 설명하도록 한다.

[0018] 도 1은 본 발명의 일 실시예에 따라 일회성 카드번호를 생성하는 방법에 대한 개념도를 도시한다.

[0019] 도 1을 참조하면, 실시예에 따른 일회성 카드번호를 생성하는 방법은, 카드사 서버에서 수행되며, 결제 디바이스(10a, 10b 및 10c)에서 카드사 서버에 접속하면, 카드사 서버는 결제 디바이스(10a, 10b 및 10c)를 인덱스 테이블(170)에 마련되는 인덱스(Index) 어드레스에 대응시킬 수 있다. 결제 디바이스(10a, 10b 및 10c)에 대응하는 인덱스 어드레스는, 결제 디바이스(10a, 10b 및 10c)가 카드사 서버에 접속하여 일회성 카드번호를 요청하는 순번에 따라 대응할 수 있다. 예컨대, 인덱스 테이블(170)은 결제 디바이스(10a, 10b 및 10c)에서 카드사 서버로 접속하는 순번에 따라 인덱스 테이블(170)의 인덱스 어드레스를 순차로 대응시킬 수 있는 것이다.

[0020] 인덱스 테이블(170)에서 인덱스 어드레스는 시작번지를 기준으로 단조 증가하는 형태로 어드레스가 부여될 수 있다. 인덱스 테이블(170)의 어드레스 그 자체는 불규칙하지 않다. 그러나, 인덱스 테이블(170)의 각 어드레스에 대응하는 저장영역에 마련되는 타겟 어드레스는 불규칙적이며, 이는 인덱스 테이블(170)과 결제 디바이스

(10a, 10b 및 10c)의 어드레스가 순차로 매칭된다 하더라도, 각 결제 디바이스(10a, 10b 및 10c)에 할당되는 타겟 어드레스 값이 상이하므로 타인에 의해 예측이 어렵게 된다.

[0021] 카드사 서버는 결제 디바이스(10a, 10b 및 10c)를 인덱스 테이블(170)에 대응시킨 후, 인덱스 어드레스의 데이터로서 포함되는 타겟 어드레스를 참조할 수 있다. 타겟 어드레스는 카드번호 테이블(180)에 대한 어드레스를 나타낸다.

[0022] 인덱스 테이블(170)에는 카드번호 테이블(180)에 대한 타겟 어드레스가 포함되며, 인덱스 테이블(170)에 포함되는 타겟 어드레스는 동일한 것이 중복하여 존재하지 않는다. 즉, 인덱스 테이블(170)에는 동일하지 않으며, 서로 다른 타겟 어드레스가 마련되며, 타겟 어드레스는 인덱스 테이블(170)의 어드레스 배열 순서에 따르지 않고 그 위치는 불규칙하게 마련될 수 있다.

[0023] 예컨대, 인덱스 테이블(170)의 인덱스 어드레스의 데이터로서, 타겟 어드레스가 A(Address)100, A50 및 A20번지가 순서대로 마련될 수 있다. 인덱스 테이블(170)에서 첫 번째 인덱스 어드레스의 데이터는 A100 번 어드레스 값을 가질 수 있다. A100번 어드레스는 일회성 카드번호 테이블(180)의 타겟 어드레스를 지칭하며, 두 번째 인덱스 어드레스의 데이터는 일회성 카드번호 테이블(180)의 A50 번 어드레스를 타겟 어드레스로서 지정하고 있다. 이처럼, 인덱스 테이블(170)에는 비 순차이며, 불규칙한 타겟 어드레스가 배열될 수 있다.

[0024] 따라서, 카드사 서버가 인덱스 테이블(170)에서 첫 번째, 인덱스 어드레스를 선택한 후, 두 번째 인덱스 어드레스를 선택하는 경우, 두 번째로 선택되는 인덱스 어드레스의 데이터로 기록된 타겟 어드레스의 값(예컨대 A50)은 타인(또는 금융 전산망 직원)에 의한 예측이 매우 곤란한 측면이 있다. 이는 인덱스 테이블(170)에 마련되는 타겟 어드레스 값의 저장 방식이 어떤 패턴을 갖지 않고, 불규칙한데 따른다.

[0025] 인덱스 테이블(170)에서 결제 디바이스(10a, 10b 및 10c)에 대응하는 타겟 어드레스가 선택된 후, 카드사 서버는 일회성 카드번호 테이블(180)의 타겟 어드레스에 억세스한다. 억세스한 타겟 어드레스에는 인덱스 테이블(170)의 인덱스 어드레스 및 일회성 번호(OTN : One Time Number)가 마련될 수 있다. 예컨대, 결제 디바이스(10a)가 인덱스 테이블(170)의 첫 번째 인덱스 어드레스에 대응된 후, A100을 타겟 어드레스로 지정받는다면, 카드사 서버는 일회성 카드번호 테이블(180)에서 A100 어드레스에 대응하는 일회성 번호로서 "345678"을 선택하고, 일회성 번호 "345678"을 포함하는 일회성 카드번호를 생성할 수 있다.

[0026] 이때, 카드사 서버는 결제 디바이스(10a, 10b 및 10c)의 식별자, 예컨대, 전화번호, ESN(Electrical Serial Number), UUID(Universal Unique Identifier) 또는 MAC ADDRESS를 참조하여 결제 디바이스(10a, 10b 및 10c)에 대응하는 실물 카드번호를 조회하며, 실물 카드번호에 포함되는 BIN(Bank Identification Number)을 추출하고, BIN + 일회성 번호(OTN : One Time Number) + OVC(One time code Verification Code) 및 예비 코드를 포함하는 일회성 카드번호를 생성하고, 생성된 일회성 카드번호를 결제 디바이스(10a, 10b 및 10c)로 제공할 수 있다.

[0027] 일회성 카드번호는 고정 필드를 구비하거나, 또는 가변 필드로 구현될 수 있다. 이는 도 2 내지 도 5를 함께 참조하여 설명하도록 한다.

[0028] 먼저, 도 2를 참조하면, 일회성 카드번호의 기본 구조로서, 6 디지트(Digit)의 BIN, 1 디지트의 제1 예비 필드, 6 디지트의 일회성 번호(OTN), 3 디지트의 OVC, 1 디지트의 제2 예비 필드 및 4 디지트의 예비 코드를 포함하여 구성될 수 있다.

[0029] BIN(Bank Identificaiton Number)은 카드사를 나타내는 코드로서, 6 디지트 내지 10 디지트로 구성될 수 있다.

[0030] 일회성 번호(OTN)는 일회성 카드번호 테이블(180)에서 획득된 번호로서, 6 디지트로 구성되거나, 또는 6 디지트 이상의 필드 길이로 형성될 수 있다. 일회성 번호는 결제 디바이스(10a, 10b 및 10c)에서 인덱스 테이블(170)에 대응된 후, 인덱스 테이블(170)에서 할당받은 타겟 어드레스를 참조하여 일회성 카드번호 테이블(180)에서 채번된 번호에 대응한다. 일회성 번호(OTN)는 일회성 카드번호 테이블(180)의 어드레스 순서에 따라 단조 증가하거나, 또는 단조 감소하지 않는다.

[0031] 예컨대, 일회성 카드번호 테이블(180)의 타겟 어드레스가 A10, A11, A12, A13, A14가 순차로 존재한다고 가정할 때, 각 타겟 어드레스(A11, A12, A13, A14)에 대응하는 일회성 카드번호는,

[0032] 111111, 111112, 111113, 111114, 111115 와 같이 단조 증가하거나,

[0033] 111115, 111114, 111113, 111112, 111111 과 같이 단조 감소하거나,

[0034] 111111, 111114, 111117, 111120, 111123 과 같이 일정한 규칙(+ 3인 규칙)에 따라 단조 증가하는 형태로는 마련되지 않음을 의미한다.

[0035] 즉, 일회성 카드번호 테이블(180)에 마련되는 일회성 번호는 단조 증가, 단조 감소, 및 일정한 규칙에 따른 단조 증가나 단조 감소되는 번호 열을 구비하지 않음을 의미한다. 또한, 일회성 카드번호는 1차 선형함수나, 2차 함수에 의해 일정한 패턴을 갖는 형태로 생성되지 않는 것이 바람직하다.

[0036] OVC(One time code Verfication Code)는 일회성 번호(OTN)에 대한 검증 값으로서, OVC는 결제 디바이스(10a, 10b 및 10c)에서 일회성 번호를 포함하는 일회성 카드번호를 요청 시, 결제 디바이스(10a, 10b 및 10c)가 일회성 카드번호를 요청하는 시간에 따른 시간정보, 결제 디바이스(10a, 10b 및 10c)의 식별자(예컨대, UUID, MAC ADDRESS, 폰 번호) 실물 신용카드 번호 중 일 영역 및 순번 증가 값을 SHA 알고리즘의 입력값으로 하여 생성할 수 있다. 여기서, 순번 증가 값은, 매번 OVC를 생성할 때마다, +1씩 증가하는 값으로서, 시작 값은 시스템 설계자에 의해 임의로 설정될 수 있음은 물론이다. SHA 알고리즘은 입력 값이 다를 경우, 동일한 결과 값을 도출하지 않는 특징을 이용한 것이다. SHA 알고리즘은, 입력 값으로, 동일한 입력 값을 넣지 않는 경우, 절대 동일한 결과 값을 산출하지 않는 특징이 있다.

[0037] 예비 코드는 부가 서비스, 또는 제휴사 카드정보가 포함될 수 있다.

[0038] 이는, 일회성 카드번호(OTN)가 카드 정보 그 자체가 아니고, 다만 실물 카드번호에 대응하는 임의의 숫자열인데 따른 것으로, 별도의 제휴 카드정보나 부가 서비스에 대한 정보를 표현하고자 할 때, 4 디지트의 예비 코드가 요구될 수 있다.

[0039] 부가 서비스는 포인트 적립 카드, OK 캐쉬 백(OK Cash Back) 카드와 같이 포인트나 금액을 보전하는 형태의 부가 서비스를 제공하는 종류의 카드, 및 해당 카드의 서비스 종류를 예비 코드에 표현할 수 있는 것이다. 또한, 신용카드 사용자가 결제 비용의 일부를 되돌려 받는 형태를 갖는 제휴 카드에 대한 정보도 예비 코드에 기록될 수 있다.

[0040] OVC와 예비 코드 사이에는 제2 예비 필드가 마련될 수 있다. 제2 예비 필드는 부가 서비스 또는 제휴 카드정보를 나타내는데 더 많은 디지트가 요구되는 경우, 4 디지트인 예비 코드를 5 디지트로 사용할 수 있도록 한다. 즉, 예비 코드의 디지트가 4 디지트에서 5 디지트로 증가할 수 있다. 예비 코드 및 제2 예비 필드에 대한 설명은 이하의 설명에서 동일하게 적용되며, 중복되는 설명을 따로 부연하지는 않는다.

[0041] 다음으로, 도 3을 참조하면, BIN 과 일회성 번호(OTN) 사이에 마련되는 예비 필드에 의해 BIN의 필드가 확장되는 일 예를 도시한다.

[0042] 도 3에 도시된 바와 같이, 예비 필드는 BIN의 필드를 연장하는데 이용될 수 있으며, 6 디지트의 필드 길이를 갖는 BIN이 7 디지트의 필드 길이를 갖도록 할 수 있다. 6 디지트에서 7 디지트로 필드 길이가 연장되면, BIN을 통해 표현 가능한 카드사 및 카드사에 부속되는 신용카드의 종류는 대폭 증가할 수 있다. 추후 각 신용카드사에서 출시되는 다양한 종류의 신용카드는 예비 필드를 이용하여 표현할 수 있는 것이다.

[0043] 다음으로, 도 4는 일회성 번호(OTN)의 필드 길이를 연장하는 일 예를 도시한다.

[0044] 도 4를 참조하면, 일회성 번호(OTN)를 검증하기 위한 OVC를 제외하고, OVC에 할당되었던 필드를 일회성 번호(OTN)에 할당함으로써, OTN의 자릿수를 증가시킬 수 있다. 일회성 번호(OTN)의 자릿수를 증가시키면, 한 번에 생성 가능한 일회성 번호의 수가 증가할 수 있다. 도 4에서, 일회성 번호는 10 디지트의 필드 길이를 가질 수 있으며, 예비 필드는 생략될 수 있다.

[0045] 다음으로, 도 5는 예비 필드는 유지하고, 일회성 번호(OTN)의 필드 길이는 증가시킨 일 예를 도시한다.

[0046] 도 5를 참조하면, 일회성 카드번호는 6디지트의 필드 길이를 갖는 BIN, 1 디지트의 필드 길이를 갖는 예비 필드, 9 디지트의 필드 길이를 갖는 일회성 번호(OTN) 및 4 디지트의 필드 길이를 갖는 예비 코드로 구성될 수 있다.

[0047] BIN을 6디지트로 설정 시, BIN은 예비 필드에 의해 1 디지트의 필드 길이가 연장될 수 있으므로, 최소 6 디지트, 최대 7 디지트의 필드 길이로 설정될 수 있다. 일회성 번호(OTN)는 9 디지트의 필드 길이를 가질 수 있으며, OVC는 생략되고, 예비 코드는 4 디지트로 구성될 수 있다.

[0048] 여기서, 도 2 내지 도 5에 예시된 예비 코드는 모두 4 디지트로 구성된 것을 예시하고 있으나, 예비 코드는 2

디지트 내지 5 디지트 범위일 수 있다.

[0049] 도 6은 일회성 카드번호를 생성하는 카드사 서버의 일 예에 대한 블록개념도를 도시한다.

[0050] 도 6을 참조하면, 카드사 서버는, 인덱스 테이블(170), 일회성 카드번호 테이블(180), OTC 생성모듈(110), OTC 암호화 모듈(120), OVC 검증모듈(130), 데이터 베이스(150) 및 유효성 판단모듈(140)을 포함하여 구성될 수 있다.

[0051] OTC 생성모듈(110)은 결제 디바이스(10)가 카드사 서버로 일회성 카드번호를 요청 시, 결제 디바이스(10)를 인덱스 테이블(170)의 인덱스 어드레스에 대응시키고, 인덱스 어드레스의 데이터인 타겟 어드레스를 따라 일회성 카드번호 테이블(180)에 억세스한다. OTC 생성모듈(110)은 일회성 카드번호 테이블(180)에 억세스 후, 일회성 카드번호 테이블(180)에서 타겟 어드레스에 대응하는 일회성 번호(OTN)를 획득하며, 획득한 OTN에 BIN, 예비 필드, OVC 및 예비 코드를 부가하여 하나의 일회성 카드번호를 생성할 수 있다. 이때, OTC 생성모듈(110)은 결제 디바이스(10)의 식별자, 결제 디바이스(10)에서 OTC를 요청한 시간에 대한 시간정보, 실물 카드번호의 부분 영역(예컨대, BIN, OTC)을 이용하여 OVC를 생성할 수 있다. 생성된 OVC는 일회성 카드번호(OTC)에 포함되며, OVC가 포함된 일회성 카드번호는 결제 디바이스(10)로 제공될 수 있다.

[0052] 이때, OVC는 데이터베이스(150)에 기록될 수 있다. 또는, OVC는 데이터베이스(150)에 기록되지 않고, OVC를 생성하는데 소요되는 인자, 예컨대, 결제 디바이스(10)에서 일회성 카드번호를 요청한 시간에 대한 시간정보, 결제 디바이스(10)의 식별자, 실물 카드번호에 대한 부분 영역에 대한 정보만을 구비할 수도 있다.

[0053] 데이터베이스(150)에는 결제 디바이스(10)의 등록정보가 마련될 수 있다. 결제 디바이스(10)의 등록정보는 결제 디바이스(10)의 식별자, 예컨대, 결제 디바이스(10)의 전화번호, ESN, UUID, MAC ADDRESS와 같은 식별자 정보를 포함할 수 있으며, 식별자는 결제 디바이스(10)에서 이용할 실물 카드정보(예컨대, 카드 번호, 카드 소지자 정보, ATC(Application Transaction Count), 신용카드의 결제 한도)가 마련될 수 있다.

[0054] 또한, 데이터베이스(150)에는 OVC, 또는 OVC를 생성하는데 필요한 인자를 구비할 수 있다. OVC에 대한 상세한 설명은 추후 OVC 검증모듈에 대한 설명에서 상술하도록 한다.

[0055] OTC 암호화 모듈(120)은 일회성 카드정보를 AES(Advanced Encryption Standard), RSA(Rivest Shamir Adleman), DES(Data Encryption Standard), TDES(Triple DES), ARIA(Academy Research Institute Agency) 알고리즘에 의해 암호화할 수 있다.

[0056] OTC 암호화 모듈(120)은 일회성 카드번호(OTC) 전체에 대해 암호화를 수행하기보다는, 일회성 번호(OTN)에 대해 수행될 수 있다. 그러나, 일회성 번호(OTN) 자체가 인덱스 테이블(170)과 일회성 카드번호 테이블(180)에 의해 생성되므로, 굳이 암호화 과정이 필수적으로 요구되는 것은 아니다. 즉, OTC에 대한 암호화는 선택적이다.

[0057] OVC 검증모듈(130)은 일회성 카드번호(OTC)를 결제 디바이스(10)로 전송한 후, 결제 디바이스(10) - 카드 리더기 - 중계 서버 - 카드사 서버로 이어지는 결제 프로세스에서 중계 서버가 리턴한 승인요청 메시지에 포함되는 일회성 카드번호(OTC)를 이용하여 OVC를 검증할 수 있다.

[0058] 중계 서버를 통해 리턴되는 승인요청 메시지는 카드 리더기에서 작성되는 것으로, 카드 리더기는 승인요청 메시지에 일회성 카드번호를 결합하며, 일회성 카드번호에는 OVC 정보가 포함된다.

[0059] OVC 검증모듈(130)은 중계 서버를 통해 리턴하는 일회성 카드번호에서 OVC를 획득하고, 획득한 OVC가 올바른 값인가를 검증한다. OVC 검증모듈(130)은 아래의 각 호 중 어느 하나에 따라 OVC 값을 검증할 수 있다.

[0060] 1) OVC 검증모듈(130)은 카드사 서버에서 결제 디바이스(10)로 일회성 카드번호를 전송할 때 생성되는 OVC 값의 생성인자, 예컨대,

[0061] - 결제 디바이스(10)에서 일회성 카드번호를 요청한 시간에 대한 시간정보,

[0062] - 결제 디바이스의 식별자,

[0063] - 실물 카드번호에 대한 부분 영역 정보를 저장해둘 수 있다.

[0064] 이 상태에서, 결제 디바이스(10)로 전송된 일회성 카드번호가 중계 서버를 통해 리턴하면, 중계 서버가 리턴한 일회성 카드번호에서 OVC를 추출하고,

[0065] 일회성 카드번호에서 추출되는 일회성 번호(OTN)를 참조하여 데이터베이스(150)에 저장된 OVC 값의 생성인자를

검색할 수 있다.

[0066] 즉, 카드사 서버는, 일회성 번호(OTN)을 이용하여 데이터베이스(150)에 저장된 OVC 생성인자를 조회할 수 있다.

[0067] 이후, 카드사 서버는, OVC 생성인자를 이용하여 OVC를 생성하며, 생성된 OVC가 중계 서버를 통해 리턴한 일회성 카드번호에 포함되는 OVC와 동일한가를 비교하여 중계 서버를 통해 리턴한 일회성 카드번호를 검증할 수 있다.

[0068] 다른 한편으로 카드사 서버는,

[0069] 2) 데이터베이스(150)에 OVC 값을 저장해두고, 중계 서버를 통해 리턴하는 일회성 카드번호(OTN)에서 추출된 OVC 값과 비교하여 OVC 값을 검증할 수 있다.

[0070] 이 경우, 카드사 서버에서 결제 디바이스(10)로 일회성 카드번호를 전송할 때, OTC 생성모듈(110)이 데이터베이스(150)에 OVC의 사본을 저장해둘 수 있다.

[0071] 유효성 판단모듈(140)은 데이터베이스(150)에 저장된 계정정보를 참조하여 사용 가능한 신용카드인가를 판단하며, 이때, 승인요청 메시지에 포함되는 결제 비용이 결제 한도(예컨대 일일 사용한도)를 넘지 않는가를 판단한다. 판단 결과 결제 한도를 충족하고 유효한 신용카드인 경우 중계 서버로 승인 여부를 통보할 수 있다.

[0072] 도 7과 도 8은 OVC 검증방법의 일 예에 대한 참조도면을 도시한다.

[0073] 먼저, 도 7을 참조하면, 결제 디바이스(10)에서 카드사 서버(100)로 일회성 카드번호(OTC)가 요청되면, 카드사 서버(100)는 도 1을 통해 설명된 방식에 따라, 일회성 번호 및 일회성 번호를 포함하는 일회성 카드번호를 생성하고, 생성된 일회성 카드번호를 결제 디바이스(10)로 제공한다.

[0074] 결제 디바이스(10)는 실물 카드번호에 대응하는 일회성 카드번호를 카드 리더기(50)로 제공하여 결제를 요청하며, 카드 리더기(50)는 일회성 카드번호, 가맹점 정보 및 결제 비용정보를 포함하는 승인요청 메시지를 작성하고, 작성된 승인요청 메시지를 중계 서버(200)로 전송하여 결제를 요청할 수 있다. 중계 서버(200)는 카드 리더기(50)에서 전송된 승인요청 메시지에 포함되는 일회성 카드번호의 정보 중 BIN 을 참조하여 어느 카드사 서버로 승인요청 메시지를 전송해야 하는가를 판단할 수 있다. 판단 결과에 따라, 중계 서버(200)가 승인요청 메시지를 전송해야 할 대상이 카드사 서버(100)인 경우, 승인요청 메시지는 카드사 서버(100)로 전송될 수 있다.

[0075] 카드사 서버(100)는 승인요청 메시지를 수신 후, 승인요청 메시지에 포함되는 일회성 카드번호를 획득하며, 일회성 카드번호에 포함되는 OVC를 추출할 수 있다. 카드사 서버(100)는 중계 서버(200)를 통해 리턴한 일회성 카드번호에 포함되는 일회성 번호(OTN)을 이용하여 카드사 서버(100)에서 결제 디바이스(10)로 전송되었던 일회성 카드번호가 어느 것인가를 판단하며, 일회성 카드번호를 결제 디바이스(10)로 전송할 때, 생성했던 OVC의 OVC 생성인자를 데이터베이스(150)에서 조회할 수 있다. 이후, 카드사 서버(100)는 OVC 생성인자를 이용하여 OVC를 생성하며, 생성된 OVC가 중계 서버(200)를 통해 리턴한 OVC와 동일한 것인가를 비교하여 중계 서버(200)를 통해 리턴한 일회성 카드번호를 검증할 수 있다.

[0076] 다음으로, 도 8을 참조하면, 결제 디바이스(10)에서 카드사 서버(100)로 일회성 카드번호(OTC)가 요청되면, 카드사 서버(100)는 도 1을 통해 설명된 방식에 따라, 일회성 번호 및 일회성 번호를 포함하는 일회성 카드번호를 생성하고, 생성된 일회성 카드번호를 결제 디바이스(10)로 제공한다. 이후, 결제 디바이스(10)에서 카드 리더기(50)로 일회성 카드번호가 제공되고, 카드 리더기(50)에서 일회성 카드번호, 가맹점 정보 및 결제 비용에 대한 정보를 포함하는 승인요청 메시지를 작성하고 중계 서버(200)를 통해 카드사 서버(100)로 리턴할 수 있다.

[0077] 카드사 서버(100)는 중계 서버(200)를 통해 리턴한 일회성 카드번호에서 일회성 번호를 추출하고, 데이터베이스(150)에 추출된 일회성 번호를 조회할 수 있다. 데이터베이스(150)에는 일회성 번호와 OVC가 매칭되어 저장되는 OVC 매칭정보가 마련될 수 있으며, 카드사 서버(100)는 OVC 매칭정보를 이용하여 중계 서버(200)를 통해 리턴한 OVC를 검증할 수 있는 것이다.

[0078] 도 9는 일회성 번호 생성방법의 일 예에 대한 참조도면을 도시한다.

[0079] 도 9를 참조하면, 일회성 번호는, 16진수로 구성되는 한 쌍의 헥사데시멀(HEXA-decimal) 코드열을 이용하여 카드사 서버에서 생성할 수 있다.

[0080] 일회성 번호를 생성하기 위해 아래의 각 호에 따른 헥사데시멀 코드열이 존재한다고 가정한다.

[0081] 3) A9B6735BCB964F3D - 제1헥사데시멀 코드열

[0082] 4) 1234567890ABCDEF - 제2헥사데시멀 코드열

[0083] 3)의 제1헥사데시멀 코드열과 제2헥사데시멀 코드열은 각각 16진수의 숫자열로서, A 내지 F의 16진수 기호를 포함하고 있다.

[0084] 16진수 기호(A 내지 F)를 10진수로 표현하기 위해,

[0085] A -> 1 / B -> 2 / C -> 3 / D -> 4 / E -> 5 / F -> 6 로 치환하는 치환룰에 따라 치환한다고 가정하면,

[0086] 제1헥사데시멀 코드열은, 상위 자릿수는 숫자열로 채우고, 하위 자릿수는 치환 값으로 기입하여 제1숫자열을 생성할 수 있다. 예컨대, 제1헥사데시멀 코드열은,

[0087] A9B6735BCB964F3D -> 9673596431223264 (제1숫자열)로 변환될 수 있고, 제2헥사데시멀 코드열은,

[0088] 1234567890ABCDEF -> 1234567890123456(제2숫자열)으로 변환될 수 있다.

[0089] 여기서, 제1숫자열과 제2숫자열은 각각 같은 자릿수로 반분될 수 있다. 예컨대,

[0090] 5) 제1숫자열 : 96735964 / 31223264

[0091] 6) 제2숫자열 : 12345678 / 90123456

[0092] 제1숫자열을 자릿수에 따라 반분한 96735964 / 31223264을 가산하면 127959228과 같은 제1가산값이 생성된다.

[0093] 제2숫자열을 자릿수에 따라 반분한 12345678 / 90123456을 가산하면 102469134와 같은 제2가산값이 생성된다.

[0094] 이후, 제1가산값과 제2가산값을 재차 가산하면, "230428362"가 생성되며, 생성된 값에서 상위 자릿수 3개를 제거하면, 6 자릿수의 "428362"가 남는다. 남은 6 자릿수의 "428362"가 일회성 번호(OTN)이며,

[0095] 여기에 BIN, 예비 필드, OVC 및 예비 코드를 부가한 것이 일회성 카드번호(OTC)가 된다.

[0096] 상기한 과정에 따라 생성된 OTN은 일회성 카드번호 테이블(180)의 저장영역에 비 순차로, 불규칙하게 배열된다. 따라서, 일회성 카드번호 테이블(180)에 불규칙하게 배열된 일회성 번호(OTN)는 첫 번째 발급되는 일회성 번호와 두 번째 발급되는 일회성 번호 사이에 아무런 연관성도, 어떠한 알고리즘도 유추될 근거가 없는 바, 타인에 의한 예측은 불가능하다.

[0097] 도 10은 OVC를 생성하는 일 예에 대한 참조도면을 도시한다.

[0098] 도 10을 참조하면, OVC는 SHA2(Secure Hash Algorithm 2) 알고리즘(EX : SHA-256 알고리즘)의 인자로서,

[0099] 5) OTC 부분 영역,

[0100] 6) 생성시간,

[0101] 7) 실물 카드번호, 및

[0102] 8) UUID를 이용하여 생성할 수 있다.

[0103] 여기서, OTC 부분 영역은, OTC의 BIN, OTN에 대응하는 영역을 의미하며, 부분 영역의 데이터가 SHA-2 알고리즘의 입력 값으로 이용될 수 있다.

[0104] 여기서, 생성시간은, 결제 디바이스(10)에서 카드사 서버(100)로 일회성 카드번호를 요청한 시간을 의미할 수 있다.

[0105] 여기서, 실물 카드번호는, 실물 신용카드에 양각 또는 음각으로 새겨지는 16자리의 카드번호 전체, 또는 일부를 의미할 수 있다.

[0106] 여기서, UUID는 결제 디바이스(10)에 대한 식별자로서, 이 외에도, MAC ADDRESS, 전화번호, 및 ESN(Electrical Serial Number) 값이 UUID 대신 이용될 수도 있다. 여기서, 결제 디바이스(10)의 식별자인 UUID는 SHA 알고리즘의 입력 값으로 이용되지 않을 수 있다. 이 경우, OVC를 생성하는데 쓰이는 입력 값은 부분 영역, 생성시간,

실물 카드번호일 수 있다.

[0107] OVC 생성을 위해, 카드사 서버(100)는,

[0108] 5) + 6) + 7) + 8) 을 가산하거나,

[0109] 또는 5) + 6) + 7) 을 가산한 값을 SHA 알고리즘에 대한 입력 값으로 할 수 있다. 이후, SHS 알고리즘에서 생성되는 값의 상위 8 디지트를 숫자로 치환하고, 치환된 숫자를 포함하는 SHA 알고리즘의 결과 값 중에서 상위 3 자릿수만을 취해 OVC로 이용할 수 있다. 여기서, 치환 규칙은, 전술한 도 9를 통해 설명된 바와 같이, A -> 1 / B -> 2 / C -> 3 / D -> 4 / E -> 5 / F -> 6 로 치환하는 치환 룰에 따라 치환할 수 있다.

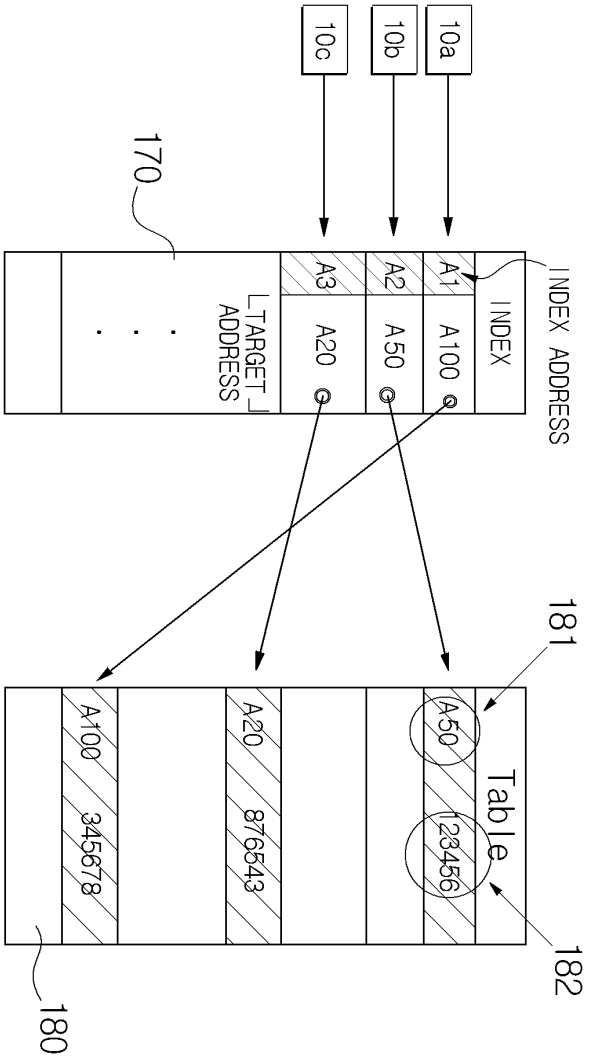
부호의 설명

[0110] 10 : 결제 디바이스 50 : 카드 리더기

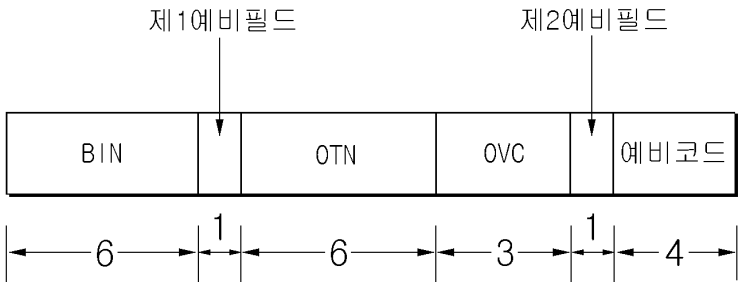
100 : 카드사 서버 200 : 중계 서버

도면

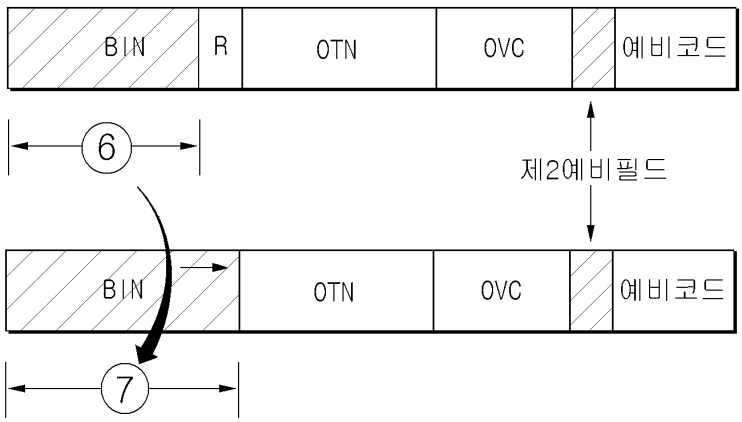
도면1



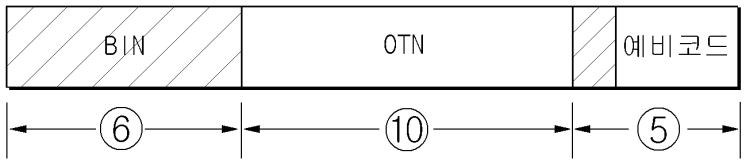
도면2



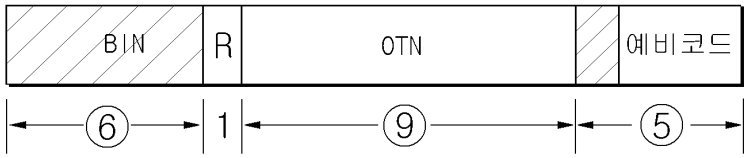
도면3



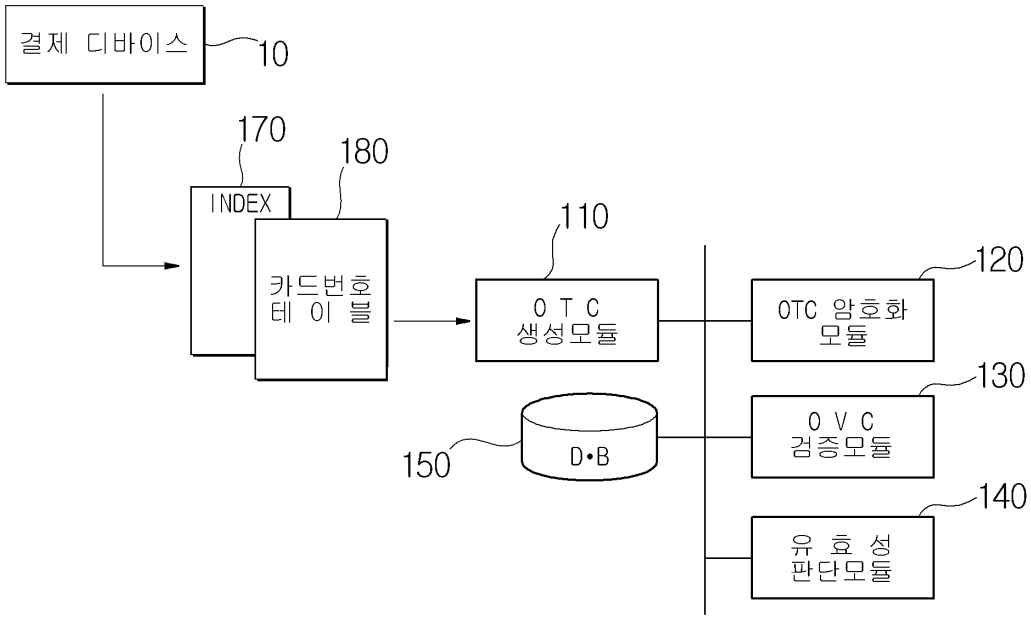
도면4



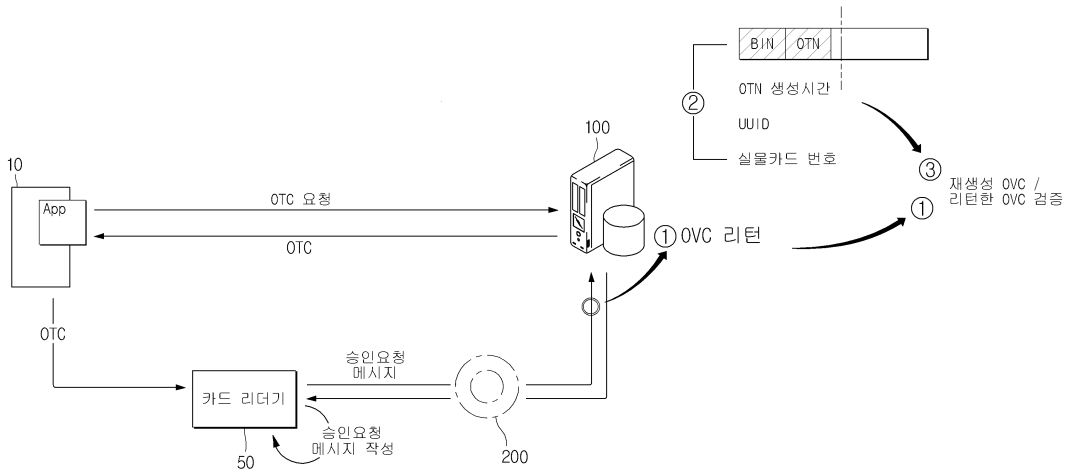
도면5



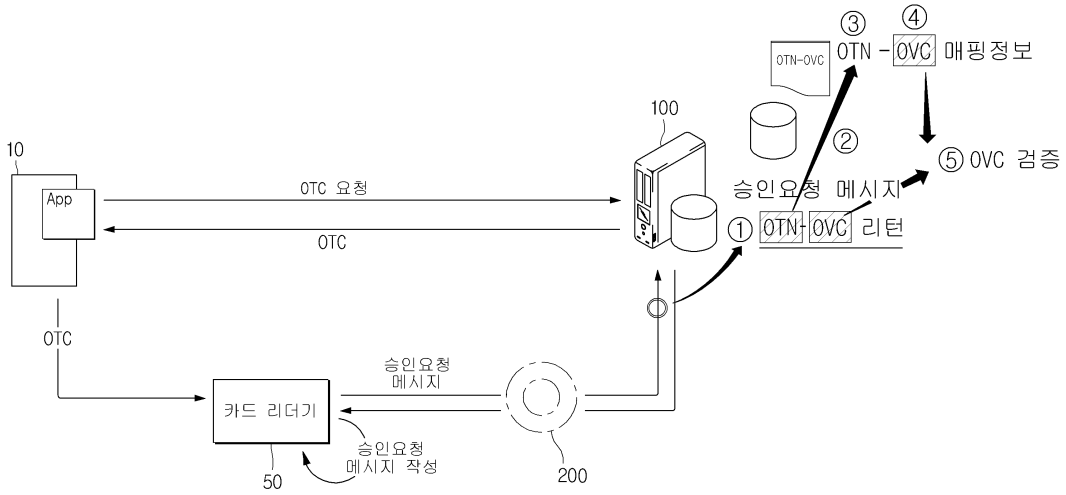
도면6


결제 디바이스
10
170
180
INDEX
카드번호
테 이 블
110
O T C
생성모듈
120
OTC 암호화
모듈
130
O V C
검증모듈
150
D•B
140
유 효 성
판단모듈

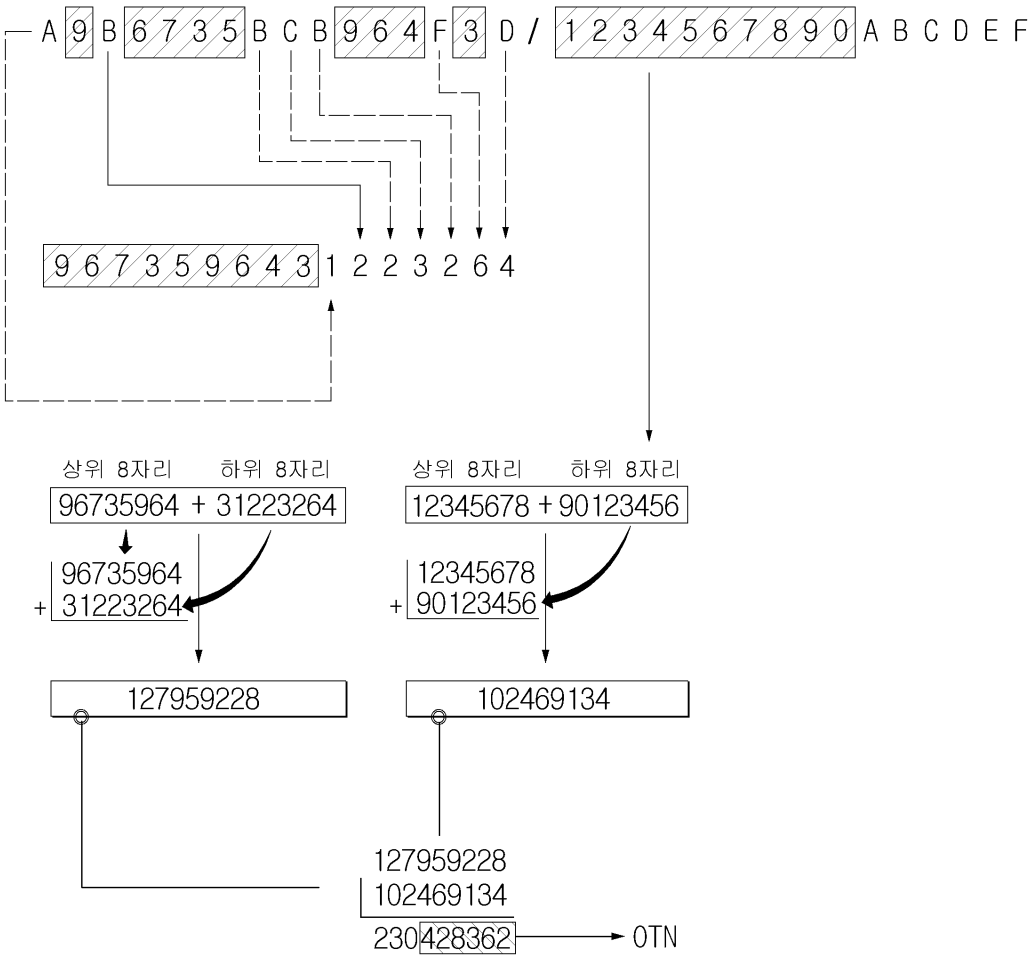
도면7


BIN
OTN
OTN 생성시간
UUID
실물카드 번호
②
③
재생성 OVC /
리턴한 OVC 검증
①
100
10
App
OTC 요청
OTC
① OVC 리턴
OTC
승인요청
메시지
카드 리더기
승인요청
메시지 작성
50
200

도면8


10
App
OTC 요청
OTC
OTC
100
③
④
OTN-OVC
OTN - OVC 매핑정보
②
⑤ OVC 검증
승인요청 메시지
① OTN-OVC 리턴
승인요청
메시지
카드 리더기
승인요청
메시지 작성
50
200

도면9


A 9 B 6 7 3 5 B C B 9 6 4 F 3 D / 1 2 3 4 5 6 7 8 9 0 A B C D E F
9 6 7 3 5 9 6 4 3 1 2 2 3 2 6 4
상위 8자리 하위 8자리
96735964 + 31223264
96735964
+ 31223264
127959228
상위 8자리 하위 8자리
12345678 + 90123456
12345678
+ 90123456
102469134
127959228
102469134
230428362
OTN

도면10

No	Name	길이	내 용
1	OTC	16	[BIN + OTN] : 부분 영역
2	생성시간	14	앱의 요청을 받은 시간
3	실물 카드번호	16	고객이 등록한 카드번호
4	UUID	32	앱에 할당된 UUID