(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0077170
(43) 공개일자 2017년07월05일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01) *G06Q 20/32* (2012.01)
(52) CPC특허분류
G06Q 20/385 (2013.01)
G06Q 20/3227 (2013.01)
(21) 출원번호 10-2017-7014112
(22) 출원일자(국제) 2015년10월26일
심사청구일자 없음
(85) 번역문제출일자 2017년05월24일
(86) 국제출원번호 PCT/GB2015/053200
(87) 국제공개번호 WO 2016/063089
국제공개일자 2016년04월28일
(30) 우선권주장
1419016.9 2014년10월24일 영국(GB)

(71) 출원인
비자 유럽 리미티드
영국, 런던 더블류2 6티티, 셸던 스퀘어 1
(72) 발명자
설리번, 브라이언
영국, 그레이터 런던 더블유2 6티티, 런던, 셸던 스퀘어 1
(74) 대리인
한양특허법인

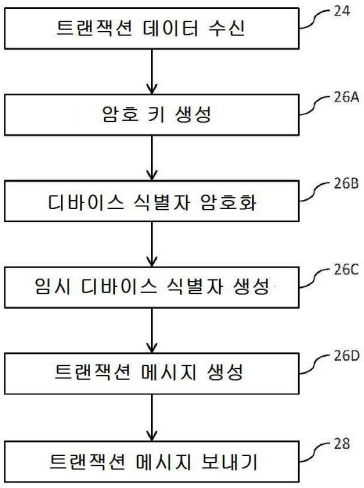
전체 청구항 수 : 총 44 항

(54) 발명의 명칭 **트랜잭션 메시징**

(57) 요 약

트랜잭션 디바이스 식별자를 갖는 트랜잭션 디바이스로부터 트랜잭션 메시지를 전송하는 방법이 제공된다 상기 방법은: 트랜잭션 디바이스에서, 트랜잭션 디바이스 식별자를 암호화하는 단계; 상기 트랜잭션 디바이스에서, 트랜잭션 시스템에 대한 트랜잭션 메시지를 생성하는 단계 - 상기 트랜잭션 메시지는, 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함함 - ; 및 트랜잭션 처리 시스템에 상기 트랜잭션 메시지를 보내는 단계를 포함한다. 상기 트랜잭션 메시지를 생성하는 단계는, 상기 트랜잭션 디바이스를 식별하지 않는 상기 트랜잭션 메시지의 상기 제 1 데이터 필드에 데이터를 제공하는 단계 및 상기 트랜잭션 메시지의 상기 제 2 데이터 필드에 암호화된 상기 트랜잭션 디바이스 식별자를 제공하는 단계를 포함한다.

대 표 도



(52) CPC특허분류
G06Q 20/3278 (2013.01)
G06Q 20/3825 (2013.01)

명 세 서

청구범위

청구항 1

트랜잭션 디바이스 식별자(transaction device indentifier)를 갖는 트랜잭션 디바이스로부터 트랜잭션 메시지를 전송하는 방법으로서, 상기 방법은:

트랜잭션 디바이스에서, 트랜잭션 디바이스 식별자를 암호화하는 단계;

상기 트랜잭션 디바이스에서, 트랜잭션 시스템에 대한 트랜잭션 메시지를 생성하는 단계 - 상기 트랜잭션 메시지는, 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함함 - ; 및

트랜잭션 처리 시스템에 상기 트랜잭션 메시지를 보내는 단계를 포함하고,

상기 트랜잭션 메시지를 생성하는 단계는, 상기 트랜잭션 디바이스를 식별하지 않는 데이터를 상기 트랜잭션 메시지의 상기 제 1 데이터 필드에 제공하는 단계 및 상기 트랜잭션 메시지의 상기 제 2 데이터 필드에 암호화된 상기 트랜잭션 디바이스 식별자를 제공하는 단계를 포함하는, 트랜잭션 메시지를 전송하는 방법.

청구항 2

청구항 1에 있어서, 상기 트랜잭션 메시지는 제 3 데이터 필드를 포함하며,

상기 트랜잭션 메시지를 생성하는 단계는, 상기 제 3 데이터 필드에 트랜잭션 디바이스 식별자의 암호화와 관련된 암호 키를 적어도 부분적으로 식별하는 데이터를 제공하는 단계를 더 포함하는, 트랜잭션 메시지를 전송하는 방법.

청구항 3

청구항 2에 있어서, 상기 암호 키는 적어도 부분적으로 추가 데이터를 사용하여 생성되고, 상기 추가 데이터는 상기 트랜잭션 디바이스 식별자가 아닌, 트랜잭션 메시지를 전송하는 방법.

청구항 4

청구항 3에 있어서, 상기 암호 키는, 상기 트랜잭션 디바이스 식별자와 고유하게 관련된 값을 추가로 사용하여 생성되는, 트랜잭션 메시지를 전송하는 방법.

청구항 5

청구항 1 내지 청구항 4 중 어느 한 항에 있어서, 상기 트랜잭션 디바이스에서, 추가 데이터를 적어도 부분적으로 사용하며 임시 트랜잭션 디바이스 식별자를 생성하는 단계를 더 포함하고, 상기 추가 데이터는 상기 트랜잭션 디바이스 식별자가 아니며, 상기 제 1 필드에 제공된 상기 데이터는 상기 임시 트랜잭션 디바이스 식별자인, 트랜잭션 메시지를 전송하는 방법.

청구항 6

청구항 3 내지 청구항 5 중 어느 한 항에 있어서, 트랜잭션 처리 시스템으로부터 상기 추가 데이터를 수신하는 단계를 포함하는, 트랜잭션 메시지를 전송하는 방법.

청구항 7

청구항 3 내지 청구항 6 중 어느 한 항에 있어서, 주어진 트랜잭션에 있어서, 상기 추가 데이터의 적어도 일부가 상기 트랜잭션에 특정되는, 트랜잭션 메시지를 전송하는 방법.

청구항 8

청구항 1 내지 청구항 7 중 어느 한 항에 있어서, 상기 트랜잭션 디바이스 식별자는 금융 수단(financial

instrument)의 주 계좌 번호를 표시하는 데이터를 포함하는, 트랜잭션 메시지를 전송하는 방법.

청구항 9

청구항 1 내지 청구항 8 중 어느 한 항에 있어서, 상기 트랜잭션 메시지는 지불 처리를 위한 EMV 기준에 따라 포맷되는(formatted), 트랜잭션 메시지를 전송하는 방법.

청구항 10

트랜잭션 메시지를 처리하는 방법으로서, 상기 방법은: 트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지를 수신하는 단계 - 상기 트랜잭션 메시지는, 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함함 - ;

보조 데이터 필드 내의 데이터를 복호화해서 복호화된 데이터를 생성하는 단계;

상기 제 1 데이터 필드의 데이터 대신 상기 트랜잭션 디바이스 식별자를 형성하도록 상기 복호화된 데이터의 적어도 일부를 사용하여 상기 트랜잭션 메시지를 처리하는 단계를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 11

청구항 10에 있어서, 상기 처리하는 단계는 상기 제 1 데이터 필드의 데이터가 상기 복호화된 데이터로 교체된, 변경된 트랜잭션 메시지를 트랜잭션 처리 시스템의 제 2 부에 보내는 단계를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 12

청구항 11에 있어서, 상기 제 1 데이터 필드의 상기 데이터와 상기 복호화된 데이터 사이의 관련성을 저장하는 단계를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 13

청구항 13에 있어서,

상기 트랜잭션 처리 시스템의 상기 제 2 부로부터 응답 메시지를 수신하는 단계 - 상기 응답 메시지는 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 데이터 필드를 포함하고, 상기 데이터 필드는 상기 복호화된 데이터를 포함함 - ;

상기 복호화된 데이터를 상기 제 1 데이터 필드의 상기 데이터로 교체하도록 상기 응답 메시지를 변경하는 단계; 및

상기 트랜잭션 처리 시스템의 상기 제 1 부에 변경된 상기 응답 메시지를 전송하는 단계를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 14

청구항 10 내지 청구항 13 중 어느 한 항에 있어서, 상기 트랜잭션 메시지는 제 3 데이터 필드를 포함하며, 상기 제 2 데이터 필드 내의 상기 데이터의 암호화와 관련된 암호 키를 적어도 부분적으로 식별하는 데이터가 상기 제 3 데이터 필드에 제공되는, 트랜잭션 메시지를 처리하는 방법.

청구항 15

청구항 14에 있어서, 상기 트랜잭션 메시지는 추가 트랜잭션 데이터를 홀드하도록 구성되는 하나 이상의 추가 데이터 필드를 포함하며, 상기 방법은, 상기 제 3 데이터 필드의 데이터를 사용하여 상기 추가 트랜잭션 데이터를 검증하는 단계를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 16

청구항 10 내지 청구항 13 중 어느 한 항에 있어서, 상기 트랜잭션 메시지는 추가 트랜잭션 데이터를 홀드하도록 구성되는 하나 이상의 추가 데이터 필드를 포함하며, 상기 방법은, 상기 추가 트랜잭션 데이터로부터 상기 제 2 데이터 필드 내의 데이터를 복호화하는데 사용되는 암호 키를 생성하는 단계를 포함하는, 트랜잭션 메시지

를 처리하는 방법.

청구항 17

청구항 15 또는 청구항 16에 있어서, 상기 추가 트랜잭션 데이터를 검증하기 위하여 상기 복호화된 데이터와 고유하게 관련된 값을 추가로 사용하는 단계를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 18

청구항 10 내지 청구항 17 중 어느 한 항에 있어서, 상기 트랜잭션 디바이스 식별자는 금융 수단의 주 계좌 번호를 표시하는 데이터를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 19

청구항 10 내지 청구항 18 중 어느 한 항에 있어서, 상기 트랜잭션 메시지는 지불 처리에 대한 EMV 기준에 따라 포맷되는, 트랜잭션 메시지를 처리하는 방법.

청구항 20

트랜잭션 메시지를 전송하는 방법으로서, 상기 방법은:

암호화 함수에 대한 입력으로서, 적어도, 트랜잭션 디바이스 식별자 및 상기 트랜잭션 디바이스 식별자가 아닌 추가 데이터를 사용하여 적어도 하나의 암호화 데이터 요소를, 트랜잭션 디바이스에서, 생성하는 단계;

트랜잭션 메시지를 트랜잭션 처리 시스템에 보내지게끔 하는 단계 - 상기 트랜잭션 메시지는 적어도, 상기 추가 데이터 및 상기 적어도 하나의 암호화 데이터 요소를 포함함 - 를 포함하는, 트랜잭션 메시지를 전송하는 방법.

청구항 21

청구항 20에 있어서, 상기 적어도 하나의 암호화 데이터 요소는 상기 트랜잭션 디바이스 식별자의 암호화된 버전을 포함하는, 트랜잭션 메시지를 전송하는 방법.

청구항 22

청구항 21에 있어서,

적어도 상기 추가 데이터를 사용하여 암호 키를 생성하는 단계; 및

상기 암호 키를 사용하여 상기 트랜잭션 디바이스 식별자의 암호화된 버전을 생성하는 단계를 포함하는, 트랜잭션 메시지를 전송하는 방법.

청구항 23

청구항 22에 있어서, 상기 암호 키를 생성하도록 상기 트랜잭션 디바이스 식별자와 고유하게 관련된 값을 추가로 사용하는 단계를 포함하는, 트랜잭션 메시지를 전송하는 방법.

청구항 24

청구항 23에 있어서, 상기 적어도 하나의 암호화 데이터 요소는 상기 암호 키를 적어도 부분적으로 식별하는 데이터를 더 포함하는, 트랜잭션 메시지를 전송하는 방법.

청구항 25

청구항 20 내지 청구항 24 중 어느 한 항에 있어서, 상기 트랜잭션 디바이스 식별자는 금융 수단의 주 계좌 번호를 표시하는 데이터를 포함하는, 트랜잭션 메시지를 전송하는 방법.

청구항 26

트랜잭션 메시지를 처리하는 방법으로서, 상기 방법은:

트랜잭션 처리 시스템의 제 1 부로부터, 트랜잭션 메시지를 수신하는 단계 - 상기 트랜잭션 메시지는 제 1 트랜잭션 디바이스 식별자 및 적어도 2개의 암호화 데이터 요소를 포함함 - ; 및

암호 키를 결정하도록 제 1 암호화 데이터 요소를 사용하는 단계;

제 2 암호화 데이터 요소를 복호화하여 제 2 트랜잭션 디바이스 식별자를 결정하는 단계; 및

상기 제 2 트랜잭션 디바이스 식별자를 기초로 트랜잭션 메시지를 처리하는 단계를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 27

청구항 26에 있어서, 상기 처리하는 단계는 트랜잭션 처리 시스템의 제 2 부에 상기 제 1 트랜잭션 디바이스 식별자가 상기 제 2 트랜잭션 디바이스 식별자로 교체된, 변경된 트랜잭션 메시지를 보내는 단계를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 28

청구항 26에 있어서, 상기 제 1 트랜잭션 디바이스 식별자와 상기 제 2 트랜잭션 디바이스 식별자 사이의 관련성을 저장하는 단계를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 29

청구항 28에 있어서,

상기 트랜잭션 처리 시스템의 상기 제 2 부로부터 응답 메시지를 수신하는 단계 - 상기 응답 메시지는 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 데이터 필드를 포함하고, 상기 데이터 필드는 상기 제 2 트랜잭션 디바이스 식별자를 포함함 - ;

상기 제 2 트랜잭션 디바이스 식별자를 상기 제 1 트랜잭션 디바이스 식별자로 교체하도록 상기 응답 메시지를 변경하는 단계; 및

상기 트랜잭션 처리 시스템의 상기 제 1 부에 변경된 상기 응답 메시지를 보내는 단계를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 30

청구항 26 내지 청구항 29 중 어느 한 항에 있어서, 상기 트랜잭션 메시지는 추가 데이터를 홀드하도록 구성되는 하나 이상의 추가 데이터 필드를 포함하며, 상기 방법은 상기 제 1 암호화 데이터 요소를 사용하여 상기 추가 데이터를 검증하는 단계를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 31

청구항 30에 있어서, 상기 추가 데이터를 검증하도록 상기 제 2 트랜잭션 디바이스 식별자와 고유하게 관련된 값을 추가로 사용하는 단계를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 32

청구항 26 내지 청구항 31 중 어느 한 항에 있어서, 상기 트랜잭션 디바이스 식별자는 금융 수단의 주 계좌 번호를 표시하는 데이터를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 33

트랜잭션 메시지를 처리하는 방법으로서, 상기 방법은:

트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지를 수신하는 단계 - 상기 트랜잭션 메시지는 제 1 트랜잭션 디바이스 식별자, 암호화 데이터 요소 및 추가 데이터를 포함함 - ;

적어도 상기 추가 데이터를 사용하여 암호 키를 생성하는 단계;

상기 암호 키를 사용하여 상기 암호화 데이터 요소를 복호화하여 제 2 트랜잭션 디바이스 식별자를 결정하는 단계; 및

상기 제 2 트랜잭션 디바이스 식별자를 기초로 상기 트랜잭션 메시지를 처리하는 단계를 포함하는, 트랜잭션 메시지를 처리하는 방법.

청구항 34

트랜잭션 디바이스로부터 트랜잭션 메시지를 전송하는데 사용하기 위한 장치로서, 상기 장치는:

트랜잭션 디바이스 식별자를 암호화하고;

적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함하는 트랜잭션 메시지를 생성하며;

상기 트랜잭션 처리 시스템에 상기 트랜잭션 메시지를 보내도록 구성되고,

상기 장치는, 상기 트랜잭션 디바이스를 식별하지 않는 데이터가 상기 제 1 데이터 필드에 제공되며, 암호화된 상기 트랜잭션 디바이스 식별자가 상기 제 2 데이터 필드에 제공되도록, 상기 트랜잭션 메시지를 생성하도록 배열되는, 트랜잭션 메시지를 전송하는데 사용하기 위한 장치.

청구항 35

트랜잭션 메시지를 처리하는 장치로서, 상기 장치는:

트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지 - 상기 트랜잭션 메시지는 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함함 - 를 수신하고;

복호화된 데이터를 생성하도록 보조 데이터 필드 내의 데이터를 복호화하며;

상기 제 1 데이터 필드의 상기 데이터 대신 상기 트랜잭션 디바이스 식별자를 형성하도록 상기 복호화된 데이터의 적어도 일부를 사용하여 상기 트랜잭션 메시지를 처리하도록 구성되는, 트랜잭션 메시지를 처리하는 장치.

청구항 36

트랜잭션 디바이스로부터 트랜잭션 메시지를 전송하는데 사용하기 위한 장치로서, 상기 장치는:

암호화 함수에 대한 입력으로서 적어도 트랜잭션 디바이스 식별자 및 추가 데이터를 사용하여 적어도 하나의 암호화 데이터 요소를 생성하고;

트랜잭션 메시지 - 상기 트랜잭션 메시지는, 적어도, 상기 추가 데이터 및 상기 적어도 하나의 암호화 데이터 요소를 포함함 - 를 트랜잭션 처리 시스템에 보내지게끔 하도록 구성되는, 트랜잭션 메시지를 전송하는데 사용하기 위한 장치.

청구항 37

트랜잭션 메시지를 처리하는 장치로서, 상기 장치는:

트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지 - 상기 트랜잭션 메시지는 제 1 트랜잭션 디바이스 식별자 및 적어도 2개의 암호화 데이터 요소를 포함함 - 를 수신하고;

암호 키로서 제 1 암호화 데이터 요소를 사용하여 제 2 암호화 데이터 요소를 복호화하여 제 2 트랜잭션 디바이스 식별자를 결정하며;

상기 제 2 트랜잭션 디바이스 식별자를 기초로 상기 트랜잭션 메시지를 처리하도록 구성되는, 트랜잭션 메시지를 처리하는 장치.

청구항 38

트랜잭션 메시지를 처리하는 장치로서, 상기 장치는:

트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지 - 상기 트랜잭션 메시지는 제 1 트랜잭션 디바이스 식별자, 암호화 데이터 요소 및 추가 데이터를 포함함 - 를 수신하고;

적어도 상기 추가 데이터를 사용하여 암호 키를 생성하고;

상기 암호 키를 사용하여 상기 암호화 데이터 요소를 복호화하여 제 2 트랜잭션 디바이스 식별자를 결정하며;

상기 제 2 트랜잭션 디바이스 식별자를 기초로 상기 트랜잭션 메시지를 처리하도록 구성되는, 트랜잭션 메시지

를 처리하는 장치.

청구항 39

트랜잭션 디바이스로부터 트랜잭션 메시지를 전송하는데 사용하기 위한 컴퓨터 프로그램으로서, 상기 컴퓨터 프로그램은:

트랜잭션 디바이스 식별자를 암호화하고;

적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함하는 트랜잭션 메시지를 생성하며;

트랜잭션 처리 시스템에 상기 트랜잭션 메시지를 보내도록 구성되고,

상기 트랜잭션 메시지를 생성하는 것은 상기 트랜잭션 디바이스를 식별하지 않는 상기 트랜잭션 메시지의 제 1 데이터 필드에 데이터를 제공하는 것 및 상기 트랜잭션 메시지의 상기 제 2 데이터 필드에 암호화된 상기 트랜잭션 디바이스 식별자를 제공하는 것을 포함하는, 트랜잭션 디바이스로부터 트랜잭션 메시지를 전송하는데 사용하기 위한 컴퓨터 프로그램.

청구항 40

트랜잭션 메시지를 처리하기 위한 컴퓨터 프로그램으로서, 상기 컴퓨터 프로그램은:

트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지 - 상기 트랜잭션 메시지는 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함하고, 상기 제 1 데이터 필드는 제 1 트랜잭션 디바이스 식별자를 포함함 - 를 수신하고;

복호화된 데이터를 생성하도록 보조 데이터 필드 내의 데이터를 복호화하고;

상기 제 1 데이터 필드의 데이터 대신 상기 트랜잭션 디바이스 식별자를 형성하도록 상기 복호화된 데이터의 적어도 일부를 사용하여 상기 트랜잭션 메시지를 처리하도록 구성되는, 트랜잭션 메시지를 처리하기 위한 컴퓨터 프로그램.

청구항 41

트랜잭션 디바이스로부터 트랜잭션 메시지를 전송하는데 사용하기 위한 컴퓨터 프로그램으로서, 상기 컴퓨터 프로그램은:

암호화 함수에 대한 입력으로서 적어도 트랜잭션 디바이스 식별자 및 추가 데이터를 사용하여 적어도 하나의 암호화 데이터 요소를 생성하고;

트랜잭션 메시지 - 상기 트랜잭션 메시지는 적어도, 상기 추가 데이터 및 상기 적어도 하나의 암호화 데이터 요소를 포함함 - 를 트랜잭션 처리 시스템에 보내지게끔 하도록 구성되는, 트랜잭션 메시지를 전송하는데 사용하기 위한 컴퓨터 프로그램.

청구항 42

트랜잭션 메시지를 처리하기 위한 컴퓨터 프로그램으로서, 상기 컴퓨터 프로그램은:

트랜잭션 처리 시스템의 제 1 부로부터, 트랜잭션 메시지 - 상기 트랜잭션 메시지는 제 1 트랜잭션 디바이스 식별자 및 적어도 2개의 암호화 데이터 요소를 포함함 - 를 수신하고;

암호 키로서 제 1 암호화 데이터 요소를 사용하여 제 2 암호화 데이터 요소를 복호화하여 제 2 트랜잭션 디바이스 식별자를 결정하며;

상기 제 2 트랜잭션 디바이스 식별자를 기초로 상기 트랜잭션 메시지를 처리하도록 구성되는, 트랜잭션 메시지를 처리하기 위한 컴퓨터 프로그램.

청구항 43

트랜잭션 메시지를 처리하는 컴퓨터 프로그램으로서, 상기 컴퓨터 프로그램은:

트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지 - 상기 트랜잭션 메시지는 제 1 트랜잭션 디바이스 식

별자, 암호화 데이터 요소 및 추가 데이터를 포함함 - 를 수신하고;

적어도 상기 추가 데이터를 사용하여 암호 키를 생성하고;

상기 암호 키를 사용하여 상기 암호화 데이터 요소를 복호화하여 제 2 트랜잭션 디바이스 식별자를 결정하며;

상기 제 2 트랜잭션 디바이스 식별자를 기초로 상기 트랜잭션 메시지를 처리하도록 구성되는, 트랜잭션 메시지를 처리하는 컴퓨터 프로그램.

청구항 44

트랜잭션 메시지를 전송하는 방법으로서, 상기 방법은:

트랜잭션 디바이스에서, 트랜잭션 디바이스 식별자를 암호화하는 단계;

상기 트랜잭션 디바이스에서, 임시 트랜잭션 디바이스 식별자를 생성하는 단계;

트랜잭션 메시지를 트랜잭션 처리 시스템에 보내지게끔 하는 단계 - 상기 트랜잭션 메시지는 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함하고, 상기 임시 트랜잭션 디바이스 식별자는 상기 제 1 데이터 필드에 제공되며, 암호화된 상기 트랜잭션 디바이스 식별자는 상기 제 2 데이터 필드에 제공됨 - 를 포함하는, 트랜잭션 메시지를 전송하는 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 트랜잭션 메시지를 전송하고 처리하기 위한 시스템 및 방법에 관한 것이며, 구체적으로 식별자가 암호화되는 트랜잭션 메시지를 전송하는데 사용될 수 있는 메시지 및 방법에 관한 것이다.

배 경 기 술

[0002] 스마트카드, 액세스 카드, 포브(fob), 지불 카드와 같은 금융 수단과 같은 스마트 디바이스 및 최신형 휴대 전화 및 기타 휴대 가능한 전자 기기는 트랜잭션을 수행하도록 점점 더 사용된다. 트랜잭션은 다수의 기능을 포함할 수 있다. 일반적인 형태로, 적절한 스마트 디바이스를 소지한 사용자는 보안 도어를 통한 액세스에 대해 승인될 수 있다. 대안적으로 또는 이에 더하여, 이러한 사용자는 재화 및 용역에 대한 대가를 지불하는 것, 대중교통 또는 이벤트에 접근하기 위한 티켓 발권(ticketing)에 있어서 스마트 디바이스를 사용하는 것을 가능하게 할 수 있다.

[0003] 적절한 스마트 디바이스는 프로세서 및 메모리를 갖는다. 이들은 보안 요소에 결합될 수 있고, 이 보안 요소는 오직 한정된 방식으로 통신할 수 있는 일종의 변형 억제(tamper resistant) 하드웨어이다.

[0004] 사용 중에, 스마트 디바이스는 예컨대 도어 락, 포인트 오브 세일 디바이스(point of sale device) 또는 개찰구와 같은 트랜잭션 처리 시스템의 단말에 주어진다. 스마트 디바이스는 단말과 통신한다. 이러한 통신은 예컨대 근접장 통신(NFC)을 사용하는 무접점(contactless)이 되고 또는 디바이스와 단말 사이의 접촉을 통한 것이 될 수 있다. 스마트 디바이스는, 단말과 단독으로 소통할 수 있되, 더 빈번하게, 스마트 디바이스에 의해 제공된 데이터는 적절한 수신자에게 트랜잭션 처리 시스템을 통해 전송된다. 이러한 수신인은 스마트 디바이스를 인증하며 예컨대 단말이 도어 또는 베리어(barrier)를 열도록 명령함으로써 또는 데이터를 스마트 디바이스에 제공함으로써 응답할 수 있다.

[0005] 스마트 디바이스가 이런 방식으로 사용될 수 있도록, 스마트 디바이스에는 디바이스 식별자가 제공된다. 이는 디바이스를 고유하게 식별하여 액세스가 승인되는지 또는 지불이 행해졌는 지를 트랜잭션 처리 시스템이 결정하는 것을 가능하게 할 수 있는 숫자 또는 영숫자 스트링이 될 수 있다. 지불에 사용된 적절한 디바이스 식별자의 예시는 주 계좌 번호 또는 PAN이며, 이것은 지불이 행해지도록 신용카드 또는 직불 카드 상에 사용된다.

발명의 내용

해결하려는 과제

[0006] 보안을 증대하기 위해, 트랜잭션 동안 디바이스 식별자를 변경하거나 감추기 위한(obscure) 방법이 제안되어 왔다. 이러한 제안된 시스템은 악의를 가진 제 3자가 스마트 디바이스인 척하거나 이것을 흉내내는 것을 어렵게

하나, 이러한 시스템은 여전히, 제 3 자가 디바이스로부터 전달된 데이터를 사용하는 사용자의 움직임 또는 활동을 추적할 수 있는 위험을 미연에 방지하지 않는다.

과제의 해결 수단

[0007] 적어도 하나의 실시예에 있어서, 방법, 디바이스, 시스템 및 소프트웨어는 트랜잭션 메시지를 전송하고 및/또는 처리하기 위한 기능을 지원하거나 구현하기 위해 제공된다.

[0008] 이것은 각 독립항에 언급된 특징의 조합에 의해 성취된다. 따라서, 독립항은 다양한 실시예의 추가 상세한 구현을 규정한다.

[0009] 본 발명의 제 1 측면에 있어서, 트랜잭션 메시지를 전송하는 방법이 제공되고, 상기 방법은: 트랜잭션 디바이스에서, 트랜잭션 디바이스 식별자를 암호화하는 단계; 상기 트랜잭션 디바이스에서, 임시 트랜잭션 디바이스 식별자를 생성하는 단계; 트랜잭션 메시지가 트랜잭션 처리 시스템에 보내지게끔 하는 단계 - 상기 트랜잭션 메시지는 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함함 - 를 포함하고, 임시 트랜잭션 디바이스 식별자는 제 1 데이터 필드에 제공되며 암호화된 트랜잭션 디바이스 식별자는 제 2 데이터 필드에 제공된다.

[0010] 임시 트랜잭션 디바이스 식별자는 추가 데이터를 적어도 부분적으로 사용하여 생성될 수 있고, 상기 추가 데이터는 트랜잭션 디바이스 식별자가 아니다. 게다가, 트랜잭션 메시지는 제 3 데이터 필드를 포함할 수 있으며, 트랜잭션 디바이스 식별자의 암호화와 관련된 암호 키를 적어도 부분적으로 식별하는 데이터는 제 3 데이터 필드에 제공될 수 있다. 암호 키는 추가 데이터를 적어도 부분적으로 사용하여 생성될 수 있고, 이러한 추가 데이터는 트랜잭션 디바이스 식별자가 아니다. 암호 키는 또한 트랜잭션 디바이스 식별자와 고유하게 관련된 값을 추가로 사용하여 생성될 수 있다.

[0011] 상기 방법은, 트랜잭션 처리 시스템으로부터 추가 데이터를 수신하는 단계를 포함할 수 있다. 주어진 트랜잭션에 있어서, 추가 데이터의 적어도 일부는 트랜잭션에 특정할 수 있다.

[0012] 실시예에서, 트랜잭션 디바이스 식별자는 금융 수단의 주 계좌 번호를 표시하는 데이터를 포함할 수 있다.

[0013] 본 발명의 제 2 측면에 있어서, 트랜잭션 메시지를 처리하는 방법이 제공되고, 상기 방법은: 트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지를 수신하는 단계 - 상기 트랜잭션 메시지는, 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함하고, 상기 제 1 데이터 필드는 제 1 트랜잭션 디바이스 식별자를 포함함 - ; 제 2 트랜잭션 디바이스 식별자를 식별하도록 상기 보조 데이터 필드 내의 데이터를 복호화하는 단계; 제 2 트랜잭션 디바이스 식별자를 기초로 트랜잭션 메시지를 처리하는 단계를 포함한다.

[0014] 상기 처리하는 단계는 제 1 트랜잭션 디바이스 식별자가 제 2 트랜잭션 디바이스 식별자로 교체된, 변경된 트랜잭션 메시지를 트랜잭션 처리 시스템의 제 2 부에 보내는 단계를 포함할 수 있다. 상기 방법은 또한 제 1 트랜잭션 디바이스 식별자와 제 2 트랜잭션 디바이스 식별자 사이의 관련성을 저장하는 단계를 더 포함할 수 있다.

[0015] 상기 방법은: 상기 트랜잭션 처리 시스템의 상기 제 2 부로부터 응답 메시지를 수신하는 단계 - 상기 응답 메시지는 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 데이터 필드를 포함하고, 상기 데이터 필드는 제 2 트랜잭션 디바이스 식별자를 포함함 - ; 상기 제 2 트랜잭션 디바이스 식별자를 상기 제 1 트랜잭션 디바이스 식별자로 교체하도록 상기 응답 메시지를 변경하는 단계; 및 상기 트랜잭션 처리 시스템의 상기 제 1 부에 변경된 상기 응답 메시지를 전송하는 단계를 포함할 수 있다.

[0016] 상기 트랜잭션 메시지는 제 3 데이터 필드를 포함하며, 제 2 데이터 필드 내의 데이터의 암호화와 관련된 암호 키를 적어도 부분적으로 식별하는 데이터는 제 3 데이터 필드에 제공될 수 있다. 또한, 트랜잭션 메시지는 추가 트랜잭션 데이터를 홀드하도록 구성된 하나 이상의 추가 데이터 필드를 포함할 수 있으며 상기 방법은 제 3 데이터 필드의 데이터를 사용하여 추가 트랜잭션 데이터를 검증하는 단계를 포함할 수 있다.

[0017] 트랜잭션 메시지는 추가 트랜잭션 데이터를 홀드하도록 구성된 하나 이상의 추가 데이터 필드를 포함할 수 있으며 상기 방법은 추가 트랜잭션 데이터로부터 제 2 데이터 필드 내의 데이터를 복호화하는데 사용되는 암호 키를 생성하는 단계를 포함할 수 있다. 상기 방법은, 추가 트랜잭션 데이터를 검증하기 위하여 제 2 트랜잭션 디바이스 식별자와 고유하게 관련된 값을 추가로 사용하는 단계를 포함할 수 있다.

[0018] 실시예에서, 트랜잭션 디바이스 식별자는 금융 수단의 주 계좌 번호를 표시하는 데이터를 포함할 수 있다.

[0019] 본 발명의 제 3 측면에 있어서, 트랜잭션 메시지를 전송하는 방법이 제공되고, 상기 방법은: 암호화 함수에 대한 입력으로서, 적어도, 트랜잭션 디바이스 식별자 및 상기 트랜잭션 디바이스 식별자가 아닌 추가 데이터를 사용하여 적어도 하나의 암호화 데이터 요소를, 트랜잭션 디바이스에서, 생성하는 단계; 트랜잭션 메시지를 트랜잭션 처리 시스템에 보내지게끔 하는 단계 - 상기 트랜잭션 메시지는 적어도, 상기 추가 데이터 및 상기 적어도 하나의 암호화 데이터 요소를 포함함 - 를 포함한다.

[0020] 적어도 하나의 암호화 데이터 요소는 트랜잭션 디바이스 식별자의 암호화된 버전을 포함할 수 있다. 더욱이, 상기 방법은: 적어도 추가 데이터를 사용하는 암호 키를 생성하는 단계 및 암호 키를 사용하여 트랜잭션 디바이스 식별자의 암호화된 버전을 생성하는 단계를 포함할 수 있다. 또한, 상기 방법은, 암호 키를 생성하도록 트랜잭션 디바이스 식별자와 고유하게 관련된 값을 추가로 사용하는 단계를 포함할 수 있다. 적어도 하나의 암호화 데이터 요소는 암호 키를 적어도 부분적으로 식별하는 데이터를 더 포함할 수 있다.

[0021] 실시예에서, 트랜잭션 디바이스 식별자는 금융 수단의 주 계좌 번호를 표시하는 데이터를 포함할 수 있다.

[0022] 본 발명의 제 4 측면에 있어서, 트랜잭션 메시지를 처리하는 방법이 제공되며, 상기 방법은: 트랜잭션 처리 시스템의 제 1 부로부터, 트랜잭션 메시지를 수신하는 단계 - 상기 트랜잭션 메시지는 제 1 트랜잭션 디바이스 식별자 및 적어도 2개의 암호화 데이터 요소를 포함함 - ; 및 암호 키를 결정하도록 제 1 암호화 데이터 요소를 사용하는 단계; 제 2 암호화 데이터 요소를 복호화하여 제 2 트랜잭션 디바이스 식별자를 결정하는 단계; 및 상기 제 2 트랜잭션 디바이스 식별자를 기초로 트랜잭션 메시지를 처리하는 단계를 포함한다.

[0023] 상기 처리하는 단계는 트랜잭션 처리 시스템의 제 2 부에 상기 제 1 트랜잭션 디바이스 식별자가 상기 제 2 트랜잭션 디바이스 식별자로 교체된, 변경된 트랜잭션 메시지를 보내는 단계를 포함할 수 있다. 상기 방법은 또한 상기 제 1 트랜잭션 디바이스 식별자와 상기 제 2 트랜잭션 디바이스 식별자 사이의 관련성을 저장하는 단계를 포함할 수 있다.

[0024] 상기 방법은: 상기 트랜잭션 처리 시스템의 상기 제 2 부로부터 응답 메시지를 수신하는 단계 - 상기 응답 메시지는 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 데이터 필드를 포함하고, 상기 데이터 필드는 상기 제 2 트랜잭션 디바이스 식별자를 포함함 - ; 상기 제 2 트랜잭션 디바이스 식별자를 상기 제 1 트랜잭션 디바이스 식별자로 교체하도록 상기 응답 메시지를 변경하는 단계; 및 상기 트랜잭션 처리 시스템의 상기 제 1 부에 변경된 상기 응답 메시지를 보내는 단계를 포함한다.

[0025] 상기 트랜잭션 메시지는 추가 데이터를 홀드하도록 구성되는 하나 이상의 추가 데이터 필드를 포함하며, 상기 방법은 상기 제 1 암호화 데이터 요소를 사용하여 상기 추가 데이터를 검증하는 단계를 포함할 수 있다. 상기 방법은 또한 상기 추가 데이터를 검증하도록 상기 제 2 트랜잭션 디바이스 식별자와 고유하게 관련된 값을 추가로 사용하는 단계를 포함할 수 있다.

[0026] 실시예에서, 트랜잭션 디바이스 식별자는 금융 수단의 주 계좌 번호를 표시하는 데이터를 포함할 수 있다.

[0027] 본 발명의 제 5 측면에 있어서, 트랜잭션 메시지를 처리하는 방법이 제공되고, 상기 방법은: 트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지를 수신하는 단계 - 상기 트랜잭션 메시지는 제 1 트랜잭션 디바이스 식별자, 암호화 데이터 요소 및 추가 데이터를 포함함 - ; 적어도 상기 추가 데이터를 사용하여 암호 키를 생성하는 단계; 상기 암호 키를 사용하여 상기 암호화 데이터 요소를 복호화하여 제 2 트랜잭션 디바이스 식별자를 결정하는 단계; 및 상기 제 2 트랜잭션 디바이스 식별자를 기초로 상기 트랜잭션 메시지를 처리하는 단계를 포함한다.

[0028] 본 발명의 제 6 측면에 있어서, 트랜잭션 디바이스로부터 트랜잭션 메시지를 전송하는데 사용하기 위한 장치가 제공되고, 상기 장치는: 임시 트랜잭션 디바이스 식별자를 생성하고; 트랜잭션 메시지가 트랜잭션 처리 시스템으로 보내지게끔 하고, 상기 트랜잭션 메시지는 적어도, 트랜잭션 디바이스 식별자를 구성하도록 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성된 제 2 데이터 필드를 포함하고, 상기 임시 트랜잭션 디바이스 식별자는 제 1 데이터 필드에서 제공되며 암호화된 트랜잭션 디바이스는 제 2 데이터 필드에 제공된다.

[0029] 본 발명의 제 7 측면에 있어서, 트랜잭션 메시지를 처리하는 장치가 제공되고, 상기 장치는: 트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지 - 상기 트랜잭션 메시지는 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함하고, 제 1 데이터 필드는 제 1 트랜잭션 디바이스 식별자를 포함함 - 를 수신하고; 제 2 트랜잭션 디바이스 식별자를 식별하도록 보조 데이터 필드 내에서 데이터를 복호화하며; 제 2 트랜잭션 디바이스 식별자를 기초로 트랜잭션 메시지

를 처리하도록 구성된다.

[0030] 본 발명의 제 8 측면에 있어서, 트랜잭션 디바이스로부터 트랜잭션 메시지를 전송하는데 사용하기 위한 장치가 제공되고, 상기 장치는: 암호화 함수에 대한 입력으로서 적어도 트랜잭션 디바이스 식별자 및 추가 데이터를 사용하여 적어도 하나의 암호화 데이터 요소를 생성하고; 트랜잭션 메시지 - 상기 트랜잭션 메시지는, 적어도, 상기 추가 데이터 및 상기 적어도 하나의 암호화 데이터 요소를 포함함 - 가 트랜잭션 처리 시스템에 보내지게끔 하도록 구성된다.

[0031] 본 발명의 제 9 측면에 있어서, 트랜잭션 메시지를 처리하는 장치가 제공되고, 상기 장치는: 트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지 - 상기 트랜잭션 메시지는 제 1 트랜잭션 디바이스 식별자 및 적어도 2개의 암호화 데이터 요소를 포함함 - 를 수신하고; 암호 키로서 제 1 암호화 데이터 요소를 사용하여 제 2 암호화 데이터 요소를 복호화하여 제 2 트랜잭션 디바이스 식별자를 결정하며; 상기 제 2 트랜잭션 디바이스 식별자를 기초로 상기 트랜잭션 메시지를 처리하도록 구성된다.

[0032] 본 발명의 제 10 측면에 있어서, 트랜잭션 메시지를 처리하는 장치가 제공되고, 상기 장치는: 트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지 - 상기 트랜잭션 메시지는 제 1 트랜잭션 디바이스 식별자, 암호화 데이터 요소 및 추가 데이터를 포함함 - 를 수신하고; 적어도 상기 추가 데이터를 사용하여 암호 키를 생성하고; 상기 암호 키를 사용하여 상기 암호화 데이터 요소를 복호화하여 제 2 트랜잭션 디바이스 식별자를 결정하며; 상기 제 2 트랜잭션 디바이스 식별자를 기초로 상기 트랜잭션 메시지를 처리하도록 구성된다.

[0033] 본 발명의 제 11 측면에 있어서, 트랜잭션 디바이스로부터 트랜잭션 메시지를 전송하는데 사용하기 위한 컴퓨터 프로그램으로서, 상기 컴퓨터 프로그램은: 트랜잭션 디바이스 식별자를 암호화하고; 임시 트랜잭션 디바이스 식별자를 생성하고; 트랜잭션 메시지 - 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함 - 가 트랜잭션 처리 시스템으로 보내지게끔 하도록 구성되고, 임시 트랜잭션 디바이스 식별자는 제 1 데이터 필드에 제공되며 암호화된 트랜잭션 디바이스 식별자는 제 2 데이터 필드에 제공된다.

[0034] 본 발명의 제 12 측면에 있어서, 트랜잭션 메시지를 처리하기 위한 컴퓨터 프로그램으로서, 상기 컴퓨터 프로그램은: 트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지 - 상기 트랜잭션 메시지는 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함하고, 상기 제 1 데이터 필드는 제 1 트랜잭션 디바이스 식별자를 포함함 - 를 수신하고; 제 2 트랜잭션 디바이스 식별자를 식별하도록 상기 보조 데이터 필드 내에서 데이터를 복호화하고; 상기 제 2 트랜잭션 디바이스 식별자를 기초로 트랜잭션 메시지를 처리하도록 구성된다.

[0035] 본 발명의 제 13 측면에 있어서, 트랜잭션 디바이스로부터 트랜잭션 메시지를 전송하는데 사용하기 위한 컴퓨터 프로그램이 제공되고, 상기 컴퓨터 프로그램은: 암호화 함수에 대한 입력으로서 적어도 트랜잭션 디바이스 식별자 및 추가 데이터를 사용하여 적어도 하나의 암호화 데이터 요소를 생성하고; 트랜잭션 메시지 - 상기 트랜잭션 메시지는 적어도, 상기 추가 데이터 및 상기 적어도 하나의 암호화 데이터 요소를 포함함 - 가 트랜잭션 처리 시스템에 보내지게끔 하도록 구성된다.

[0036] 본 발명의 제 14 측면에 있어서, 트랜잭션 메시지를 처리하기 위한 컴퓨터 프로그램이 제공되고, 상기 컴퓨터 프로그램은: 트랜잭션 처리 시스템의 제 1 부로부터, 트랜잭션 메시지 - 상기 트랜잭션 메시지는 제 1 트랜잭션 디바이스 식별자 및 적어도 2개의 암호화 데이터 요소를 포함함 - 를 수신하고; 암호 키로서 제 1 암호화 데이터 요소를 사용하여 제 2 암호화 데이터 요소를 복호화하여 제 2 트랜잭션 디바이스 식별자를 결정하며; 상기 제 2 트랜잭션 디바이스 식별자를 기초로 상기 트랜잭션 메시지를 처리하도록 구성된다.

[0037] 본 발명의 제 15 측면에 있어서, 트랜잭션 메시지를 처리하는 컴퓨터 프로그램이 제공되고, 상기 컴퓨터 프로그램은: 트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지 - 상기 트랜잭션 메시지는 제 1 트랜잭션 디바이스 식별자, 암호화 데이터 요소 및 추가 데이터를 포함함 - 를 수신하고; 적어도 상기 추가 데이터를 사용하여 암호 키를 생성하고; 상기 암호 키를 사용하여 상기 암호화 데이터 요소를 복호화하여 제 2 트랜잭션 디바이스 식별자를 결정하며; 상기 제 2 트랜잭션 디바이스 식별자를 기초로 상기 트랜잭션 메시지를 처리하도록 구성된다.

[0038] 본 발명의 제 16 측면에 있어서, 트랜잭션 디바이스 식별자를 갖는 트랜잭션 디바이스로부터 트랜잭션 메시지를 전송하는 방법이 제공되고, 상기 방법은: 트랜잭션 디바이스에서, 트랜잭션 디바이스 식별자를 암호화하는 단계; 상기 트랜잭션 디바이스에서, 트랜잭션 시스템에 대한 트랜잭션 메시지를 생성하는 단계 - 상기 트랜잭션

메시지는, 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함함 - ; 및 트랜잭션 처리 시스템에 상기 트랜잭션 메시지를 보내는 단계를 포함하고, 상기 트랜잭션 메시지를 생성하는 단계는, 상기 트랜잭션 디바이스를 식별하지 않는 데이터를 상기 트랜잭션 메시지의 상기 제 1 데이터 필드에 제공하는 단계 및 상기 트랜잭션 메시지의 상기 제 2 데이터 필드에 암호화된 상기 트랜잭션 디바이스 식별자를 제공하는 단계를 포함한다.

[0039] 본 발명의 제 17 측면에 있어서, 트랜잭션 메시지를 처리하는 방법이 제공되고, 상기 방법은: 트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지를 수신하는 단계 - 상기 트랜잭션 메시지는, 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함함 - ; 보조 데이터 필드 내의 데이터를 복호화해서 복호화된 데이터를 생성하는 단계; 상기 제 1 데이터 필드의 데이터 대신 상기 트랜잭션 디바이스 식별자를 형성하도록 상기 복호화된 데이터를 사용하여 상기 트랜잭션 메시지를 처리하는 단계를 포함한다.

[0040] 본 발명의 제 18 측면에 있어서, 트랜잭션 디바이스로부터 트랜잭션 메시지를 전송하는데 사용하기 위한 장치가 제공되며, 상기 장치는: 트랜잭션 디바이스 식별자를 암호화하고; 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함하는 트랜잭션 메시지를 생성하며; 상기 트랜잭션 처리 시스템에 상기 트랜잭션 메시지를 보내도록 구성되고, 상기 장치는, 상기 트랜잭션 디바이스를 식별하지 않는 데이터가 상기 제 1 데이터 필드에 제공되며, 암호화된 상기 트랜잭션 디바이스 식별자가 상기 제 2 데이터 필드에 제공되도록, 상기 트랜잭션 메시지를 생성하도록 배열된다.

[0041] 본 발명의 제 19 측면에 있어서, 트랜잭션 메시지를 처리하는 장치가 제공되고, 상기 장치는: 트랜잭션 처리 시스템의 제 1 부로부터 트랜잭션 메시지 - 상기 트랜잭션 메시지는 적어도, 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성되는 제 2 데이터 필드를 포함함 - 를 수신하고; 복호화된 데이터를 생성하도록 보조 데이터 필드 내의 데이터를 복호화하며; 상기 제 1 데이터 필드의 상기 데이터 대신 상기 트랜잭션 디바이스 식별자를 형성하도록 상기 복호화된 데이터를 사용하여 상기 트랜잭션 메시지를 처리하도록 구성된다.

[0042] 추가 특징 및 장점은 오직 예시로서 주어진 선호되는 실시예의 이하의 기재로부터 명백할 것이며, 이것은 동반하는 도면을 참조하여 기재된다.

도면의 간단한 설명

[0043] 시스템, 장치 및 방법은 동반하는 참조하여 오직 예시로, 실시예로서 기재될 것이다.

도 1는 본 발명의 실시예가 수행될 수 있는 트랜잭션 시스템의 개략도를 도시한다.

도 2는 일 실시예에 따른 통신 흐름을 도시한다.

도 3은 일 실시예에 따른 방법을 도시한다.

도 4는 일 실시예에 따른 추가 방법을 도시한다.

도 5는 본 발명의 실시예에서 사용될 수 있는 디바이스의 개략도를 도시한다.

실시예들의 특정 부분, 구성요소 및/또는 단계는 하나 이상의 도면에 나오지만, 명료성을 위하여, 동일한 참조번호가 모든 도면의 동일한 부분, 구성요소 또는 단계를 지칭하도록 사용될 것이다.

발명을 실시하기 위한 구체적인 내용

[0044] 도 1은 트랜잭션 시스템(10)을 도시한다. 트랜잭션 디바이스(12)가 제공된다. 적절한 트랜잭션 디바이스의 예시는 스마트카드, 액세스 카드, 포브(fob), 지불 카드와 같은 금융 수단, 휴대 전화 및 태블릿 및 스마트 워치와 같은 기타 휴대 가능한 전자 기기를 포함한다. 트랜잭션 디바이스(12)는 트랜잭션 단말(14)에 대한 데이터 연결을 갖는다. 적절한 트랜잭션 단말의 예시는 지불 단말, 수송 시스템(transit system)에 대한 액세스 포인트 및 문을 포함한다.

[0045] 트랜잭션 디바이스(12)와 트랜잭션 단말(14) 사이의 데이터 연결은 무접점(contactless)일 수 있다. 사용될 수 있는 무접점 연결 기술의 예시는 근거리 무선 통신(NFC) 및 광학 시스템을 포함하고, 광학 시스템은 예컨대 단말의 스크린 상에 제시되는 데이터를 식별하고 판독하도록 휴대 전화의 카메라를 사용하는 시스템에 의해 제공된다. 데이터 연결은 대안적으로 통신을 가능하게 하도록 전기적으로 전도성인 패드 및 핀의 적절한 배열을 사

용하는 접촉 연결이 될 수 있다.

[0046] 트랜잭션 단말(14)은 제 1 트랜잭션 처리 서버(16)에 연결되고, 이것은 결국 제 2 트랜잭션 처리 서버(18)에 연결된다. 단말(14) 및 서버들(16 및 18)은 함께, 트랜잭션 처리 시스템(20)을 구성하는 것으로 고려될 수 있다. 도시되지 않았으나, 하나 이상의 추가 트랜잭션 처리 서버는 트랜잭션 단말(14)과 제 1 트랜잭션 처리 서버(16) 사이에 제공될 수 있다. 마찬가지로, 하나 이상의 추가 트랜잭션 처리 서버는 제 1 트랜잭션 처리 서버(16)와 제 2 트랜잭션 처리 서버(18) 사이에 제공될 수 있다. 집합적으로, 트랜잭션 단말(14) 및 트랜잭션 단말(14)과 제 1 트랜잭션 처리 서버(16) 사이의 임의의 추가 트랜잭션 처리 서버들은 트랜잭션 처리 시스템(20)의 제 1 부로서 고려될 수 있다. 동일하게, 제 2 트랜잭션 처리 서버(18) 및 제 1 트랜잭션 처리 서버(16)와 제 2 트랜잭션 처리 서버(18) 사이의 임의의 추가 트랜잭션 처리 서버들은 트랜잭션 처리 시스템(20)의 제 2 부로서 고려될 수 있다.

[0047] 디바이스(12), 단말(14) 및 서버들(16 및 18)의 각각의 단일 예시만이 도시되되, 트랜잭션 시스템(10)은 복수의 디바이스(12)(복수의 사용자에게 제공된 디바이스), 복수의 단말(14)(예컨대, 복수의 지불 단말 또는 액세스 단말) 및 심지어 복수의 서버(16 및 18)를 갖고 실질적으로 더욱 복잡해질 수 있는 것이 이해될 것이다.

[0048] 트랜잭션 동안 도 1에 도시된 트랜잭션 시스템(10)의 작동은 이제 도 2를 참조하여 기재될 것이다. 일반적으로, 이러한 트랜잭션에서, 트랜잭션 디바이스(12)는 트랜잭션 단말(14)에 주어지며, 트랜잭션 처리 시스템(20)은 트랜잭션을 승인하거나 거절(deny)하도록 동작한다. 트랜잭션이 승인되거나 거절되는 것의 여부에 따라, 트랜잭션 단말 또는 그에 연결된 디바이스는 특정 행동(문을 여는 것과 같은 행동)을 수행할 수 있고, 대안적으로 또는 추가적으로, 메시지가 트랜잭션 디바이스로 다시 보내질 수 있다. 더 구체적인 기재는 이하와 같다.

[0049] 제 1 단계(22)에서, 트랜잭션이 착수되며 트랜잭션 디바이스(12)는 트랜잭션 단말(14)에 연결된다. 트랜잭션의 착수는 예컨대 구매할 재화 및 용역를 선택하고 또는 티켓팅(ticketing) 트랜잭션에 대한 목적지를 선택하는 사용자를 포함할 수 있다. 이는, 사용자 입력을 요할 수 있고 또는 대안적으로 트랜잭션 단말의 아이덴티티(identity)을 기초로 사전결정될 수 있고, 예컨대, 수송 시스템(transit system) 상의 트랜잭션 단말의 아이덴티티는 임의의 특정 사용자 입력 없이 요구되는 용역를 규정한다.

[0050] 트랜잭션 디바이스(12)와 트랜잭션 단말(14) 사이의 연결은 단말에 주어지는 트랜잭션 디바이스(12) 및 무접점, 예컨대 근거리 무선 통신(NFC), 연결이 수립되는 것에 의해 수립된다. 대안적으로, 트랜잭션 디바이스(12)는 전기적 연결이 수립되는 것을 가능하게 하도록 물리적으로 트랜잭션 단말(14) 내로 인서트되거나 연결될 수 있다. 이러한 방법은 선행기술에서 알려져 있으며 여기서 상세히 기재될 필요가 없다.

[0051] 단계(22)에서, 트랜잭션을 착수시키고 연결을 수립하여, 단계(24)에서 트랜잭션과 관련된 트랜잭션 데이터가 트랜잭션 단말(14)로부터 트랜잭션 장치(12)로 보내질 수 있다. 이러한 트랜잭션 데이터는, 예컨대 트랜잭션에서 지불될 가격 또는 수송 시스템(transit system)상의 티켓팅 트랜잭션에 대하여 진입 또는 출입(egress) 포인트의 아이덴티티를 포함할 수 있다. 일반적으로, 상기 기재된 트랜잭션의 특성은 트랜잭션 데이터를 규정할 것이다.

[0052] 단계(26)에서, 트랜잭션 디바이스는 트랜잭션 메시지를 준비하며 단계(28)에서 트랜잭션 메시지는 트랜잭션 디바이스로부터 트랜잭션 단말(14)로 보내진다. 이러한 메시지의 내용의 더욱 상세한 기재 및 단계(24) 내지 단계(28)에서 생성된 방법들은 도 3을 참조하여 이하에서 제공될 것이다.

[0053] 단계(30)에서, 트랜잭션 단말은 이어서 제 1 트랜잭션 처리 서버(16) 상에 메시지를 포워드한다. 상기 기재로부터 이해되는 바와 같이, 이것은 하나 이상의 추가 트랜잭션 처리 서버를 통해 메시지를 보내는 단계를 포함할 수 있다.

[0054] 단계(32)에서, 제 1 트랜잭션 처리 서버(16)는 트랜잭션 메시지를 처리한다. 특정 실시예에서, 제 1 트랜잭션 처리 서버(16)는 트랜잭션을 승인하거나 거절할 수 있다. 이러한 경우에, 시그널링 흐름(signalling flow)은 이하에서 기재된 단계(40)로 바로 통과할 수 있다.

[0055] 대안에서, 제 2 트랜잭션 처리 서버(18)는 트랜잭션을 승인하거나 거절할 수 있는 엔티티(entity)가 될 수 있다. 이러한 경우에, 제 1 트랜잭션 처리 서버(16)는 메시지를 변경할 수 있다. 변경된 메시지는 단계(34)에서 제 2 트랜잭션 처리 서버(18)로 보내질 수 있다.

[0056] 제 2 트랜잭션 처리 서버(18)는 이어서 트랜잭션을 승인하거나 거절하며 단계(38)에서, 제 1 트랜잭션 처리 서버(16)에 응답 메시지를 전달한다. 이러한 응답 메시지는 단계(40)에서 변경된 응답 메시지가 트랜잭션 단말

(14)로 보내지기 전에 제 1 트랜잭션 처리 서버(16)에 의해 다시 처리될 수 있다. 단계들(30 내지 40)에서 제 1 트랜잭션 처리 서버(16)에 의한 메시지의 처리의 더 상세한 기재는 도 4를 참조하여 제공될 것이다.

[0057] 단계(40)에서 응답 메시지의 수신 직후, 트랜잭션 단말(14)은 임의의 수의 작동(action)을 수행할 수 있다. 예컨대, 트랜잭션 단말(14)은 트랜잭션 디바이스(42)에 응답 메시지를 보낼 수 있다. 이러한 응답 메시지는 트랜잭션이 승인되는 것을 표시하는 데이터를 포함할 수 있고, 필요 시에, 추후 사용을 위하여 트랜잭션 디바이스(12)에 의해 저장될 수 있는 티켓 또는 기타 데이터 구조를 포함할 수 있다. 대안적으로 또는 추가적으로, 트랜잭션 디바이스는 단계(44)에 의해 도시되는 적절한 작동을 취할 수 있다. 예컨대, 이러한 작동은 문 또는 개찰구를 열 수 있거나 트랜잭션이 승인되는 것(그리고 그러므로 사용자가 구매한 재화 또는 용역를 제공받을 수 있는 것)의 표시를 제공일 수 있다.

[0058] 상기 처리 흐름은 트랜잭션 시스템들의 선행 기술에서 알려져 있으므로 개략적으로만 기재된다.

[0059] 상기 기재된 바와 같이, 단계들(24 내지 28)에서 트랜잭션 디바이스의 작동의 더욱 상세한 기재는 도 3을 참조하여 제공될 것이다. 여기서, 트랜잭션 디바이스는 트랜잭션 식별자가 제공되는 것으로 가정될 것이다. 이것은 트랜잭션 처리 시스템이 트랜잭션 디바이스(12)를 식별하고 다른 유사한 트랜잭션 디바이스들로부터 이것을 구분하는 것을 가능하게 하는 값 또는 코드이다. 적절한 트랜잭션 디바이스 식별자의 예시는 금융 수단의 주 계좌 번호(PAN)이다. 트랜잭션 디바이스 식별자에 더하여, 인증 데이터가 트랜잭션 디바이스(12)에 의해 저장될 수 있다. 이러한 인증 데이터는 트랜잭션 디바이스(12)로부터 보내진 메시지가 트랜잭션 처리 시스템에 의해 인증되는 것을 가능하게 하여, 트랜잭션 처리 시스템이 임의의 주어진 트랜잭션을 승인하거나 거절하는 것을 가능하게 하도록 사용될 수 있다. 승인 데이터는 트랜잭션 디바이스(12)에 먼저 제공되는 보조 크리덴셜(credential) 및 암호 키를 포함할 수 있다.

[0060] 단계(24)에서, 상기 기재된 바와 같이, 트랜잭션 디바이스(12)는 트랜잭션 처리 시스템으로부터 트랜잭션 데이터를 수신할 수 있다. 이러한 트랜잭션 데이터는 트랜잭션 단말(14)의 아이덴티티와 관련된 데이터, 예컨대, 단말을 제공하거나 사용하는 상인(merchant) 또는 수송 서비스의 아이덴티티, 단말 그 자체의 아이덴티티, 단말에 대한 위치, 단말과의 통신과 관련된 채널 또는 도메인(이것은 무선 또는 전기적 접촉이 사용되는지를 표시할 수 있음) 및 상인이 지불을 수신하는 것을 가능하게 하는 지불 상세를 포함할 수 있다. 또한, 트랜잭션 데이터는 트랜잭션 자체에 특정되는 데이터, 예컨대, 트랜잭션을 위한 시간을 표시하는 데이터, 지불의 양, 선지불 티켓의 감소에 대한 양 및/또는 트랜잭션과 관련된 임의의 재화 또는 용역의 식별을 포함한다. 트랜잭션 데이터는 트랜잭션 디바이스 식별자가 아닌 적어도 일부 데이터를 포함한다.

[0061] 단계(26A)에서, 트랜잭션 디바이스(12)는 수신된 트랜잭션 데이터를 사용하여 암호 키를 생성한다. 통상적으로, 암호 키는 하나 이상의 암호화 함수에 대한 입력으로서 트랜잭션 데이터를 사용하여 생성될 것이다. 트랜잭션 데이터는 함수에 대한 유일한 입력이 아닐 수 있으며, 이하의 추가 입력이 사용될 수 있다:

[0062] - 예컨대 트랜잭션 디바이스(12) 상에 저장된 해싱 키 또는 씨드 값과 같이 트랜잭션 디바이스 식별자와 고유하게 관련된 값;

[0063] - 트랜잭션 디바이스 식별자(상기 지칭된 트랜잭션 데이터가 트랜잭션 디바이스 식별자가 아닌 데이터를 표시하는 것이 명백해짐);

[0064] - 트랜잭션 디바이스(12)에 의해 먼저 수행되거나 완성된 트랜잭션의 수를 표시하는 값; 및

[0065] - 트랜잭션을 위해 사용되는 채널 또는 도메인을 표시하는 데이터.

[0066] 암호 키가 생성될 수 있는 방법의 일 예시가 기재될 것이다. 이러한 예시는 타원 곡선 암호법(Elliptic Curve Cryptography (ECC)) 및 키 합의(key agreement)를 위한 ECC El Gamal로 불리는 방법을 사용할 것이다. 순환 그룹(cyclic group)(G)은 생성기 값(g)을 기초로 규정된 것이 가정될 것이다. 트랜잭션 처리 서버, 예컨대 서버(16)에 대한 공개 키(P_S)는 그 서버에 대한 개인 키(d_S) 및 그룹(G)을 기초로 생성된다. 예컨대:

[0067] $$P_S = d_S \bullet G = g^{d_S}$$

[0068] 이러한 공개 키는 트랜잭션 디바이스에 이용가능해진다. 또한, 추가 키(K), 해싱 키가 규정되고, 트랜잭션 디바이스(12)와 제 1 트랜잭션 처리 서버(16) 모두에 알려진다. 해싱 키(K)는 트랜잭션 디바이스와 고유하게 관련된 값이 될 수 있다.

[0069] 제 1 단계에서, 트랜잭션 디바이스(12)는 해시 값을 계산한다. 이것은 키 헤싱 메시지 인증 코드(keyed-hash

message authentication code (HMAC))를 사용하여 수행될 수 있다. 해시 함수에 대한 입력은 해싱 키(K) 및 이러한 경우에 트랜잭션 디바이스와 디바이스 식별자(I_D)의 연결을 포함한다. 해싱 함수의 출력은 h로 표시되며 이하와 같이 기재될 수 있다:

[0070] $$h = HMAC(K, I_D || \text{트랜잭션 데이터})$$

[0071] h 및 순환 그룹(G)을 사용하여, 트랜잭션 디바이스(12)는 트랜잭션에서 사용하기 위한 장치를 위한 단명(ephemeral) 공개 키(P_D)를 생성할 수 있다. 이러한 공개 키(P_D)는 상기 기재된 암호 키를 나타낸다. 예컨대:

[0072] $$P_D = h \bullet G = g^h$$

[0073] 또한, 제 1 트랜잭션 처리 서버(16)의 공개 키(P_S)와 h를 사용하여, 트랜잭션 디바이스(12)는 공유된 비밀(S)을 생성할 수 있다. 예컨대:

[0074] $$S = h \bullet P_S = {P_S}^h = g^{a_S h}$$

[0075] 단명 암호 키(P_D)가 생성되고 그로부터 공유된 비밀(S)을 연산하여, 단계(26B)에서, 트랜잭션 디바이스(12)는 암호화된 트랜잭션 디바이스 식별자(C)를 생성하여 공유된 비밀(S)을 사용하여 디바이스 식별자(I_D)를 암호화한다. 예컨대:

[0076] $$C = \text{enc}(S, I_D)$$

[0077] 암호 키(P_D) 및 암호화된 트랜잭션 디바이스 식별자(C)는, 각각, 트랜잭션 메시지에서 트랜잭션 단말(14)로 보내질 수 있는 고려된 암호화 데이터 소자가 될 수 있다.

[0078] 암호화된 트랜잭션 디바이스 식별자(C)를 생성하는데 더하여, 단계(26C)에서, 트랜잭션 디바이스(12)는 임시 트랜잭션 디바이스 식별자를 생성할 수 있다. 임시 트랜잭션 디바이스 식별자는 전체적으로 랜덤으로 또는 의사 랜덤으로 생성될 수 있다. 대안적으로, 이는 암호화된 트랜잭션 디바이스 식별자(C)를 기초로 하거나 추가 데이터를 사용하여 생성될 수 있고, 이들의 적어도 일부는 트랜잭션 디바이스 식별자외의 데이터, 예컨대 상기 기재된 트랜잭션 데이터 또는 상기 디바이스에 대하여 생성된 공개 키(P_D)이다.

[0079] 임시 트랜잭션 디바이스 식별자는 입력으로서 상기 기재된 값들 중 하나를 갖고 추가 함수를 사용하여 생성될 수 있다. 예컨대, 이것은 통상적으로 디바이스 식별자가 특정 포맷(format), 예컨대 특정 길이를 갖는 경우이다. 이러한 경우에, 입력 값은 임시 트랜잭션 디바이스 식별자를 제공하도록 변경될 수 있다. 임시 트랜잭션 디바이스 식별자는 전체적으로 생성될 수 없으며, 실제 트랜잭션 디바이스 식별자의 일부와 같은 미리 결정된 데이터를 부분적으로 기초로 할 수 있다.

[0080] 예시로서, 트랜잭션 디바이스 식별자는 16자 PAN일 경우, 처음 6자리는 은행 식별 번호(Bank Identification Number (BIN)) 또는 발행인 식별 번호(Issuer identification number (IIN))를 표시하며 마지막 숫자는 검사 번호(check digit)를 표시한다. 기존 트랜잭션 디바이스 식별자로부터의 BIN/IIN가 유지될 수 있으며 적절한 검사 번호 및 임시 트랜잭션 디바이스 식별자의 9자리로 늘어난다.

[0081] 단계(26D)에서, 트랜잭션 디바이스(12)는 상기 생성된 값을 사용하여 트랜잭션 처리 시스템에 보내질 트랜잭션 메시지를 생성한다. 이것은, 종종, 트랜잭션 메시지가 특정 기준을 따라야 하는 경우가 될 것이다. 예컨대, 트랜잭션 메시지는 지불 처리에 대한 EMV 기준에 따라 포맷될 수 있으며, 이것은, 트랜잭션 디바이스 식별자로서 PAN을 전달하도록 구성된 데이터 요소를 포함하는 트랜잭션 메시지에 대한 필수 데이터 요소를 명시한다. 따라서, 이러한 기준은, 메시지가 적어도 트랜잭션 디바이스 식별자를 홀드하도록 구성된 제 1 데이터 필드 및 보조 데이터를 홀드하도록 구성된 제 2 데이터 필드를 포함해야 하는 것을 명시할 수 있다. 따라서, 트랜잭션 디바이스(12)를 실제로 식별하지 않는 임시 트랜잭션 디바이스 식별자는 제 1 데이터 필드에 제공될 수 있으며 암호화된 트랜잭션 디바이스 식별자를 제 2 데이터 필드에 제공할 수 있다. 추가로, 트랜잭션 메시지는 제 3 데이터 필드를 포함할 수 있으며, 트랜잭션 디바이스 식별자의 암호화와 관련된 암호 키(P_D)는 제 3 데이터 필드에 제공될 수 있다. 암호 키(P_D)는 트랜잭션 디바이스 식별자의 암호화에서 그 자체가 사용되지 않는 것이 이해될 것이다. 대신, 암호화에서 사용되는 공유된 비밀과 관련된 공개 키에 의해, P_D는 트랜잭션 디바이스 식별자의 암호화와 관련된 암호 키를 식별하는 데이터를 포함한다. 마지막으로, 트랜잭션 데이터의 일부 또는 전부는 메시지의

다른 필드에 제공될 수 있다.

[0082] 적절한 트랜잭션 메시지가 생성되고, 단계(28)에서, 트랜잭션 디바이스(12)는 트랜잭션 메시지를 트랜잭션 처리 시스템, 즉, 트랜잭션 단말(14)에 보낸다.

[0083] 단계들(30 내지 40)의 제 1 트랜잭션 처리 서버(16)의 동작의 더욱 상세한 기재는 도 4를 참조하여 이제 제공될 것이다.

[0084] 단계(30)에서, 제 1 트랜잭션 처리 서버(16)는 트랜잭션 메시지를 수신한다. 상기 기재와 유사하게, 트랜잭션 디바이스(12)에 의해 생성된 메시지는 임시 트랜잭션 디바이스 식별자, 트랜잭션 디바이스 식별자(C) 및 단명 암호 키(P_D)를 포함한다. 암호화된 트랜잭션 디바이스 식별자(C) 및 단명 암호 키(P_D)는 암호화 데이터 요소로서 고려될 수 있다. 또한, 메시지는 트랜잭션 데이터의 적어도 일부를 포함할 수 있다.

[0085] 단계(32A)에서, 제 1 트랜잭션 처리 서버(16)는 암호 키(P_D)를 사용하여 공유된 비밀(S)을 생성할 수 있다. 예컨대:

[0086] $$S = d_S \bullet P_D = P_D{}^{d_S} = g^{h^{d_S}}$$

[0087] 공유된 비밀(S)은 기존 트랜잭션 디바이스 식별자(I_D)를 생성하도록 암호화된 트랜잭션 디바이스 식별자(C)를 복호화하도록 사용될 수 있다.

[0088] 또한, 제 1 트랜잭션 처리 서버(16)는 트랜잭션 메시지에 제공되는 임의의 트랜잭션 데이터를 확인(validate)할 수 있다. 이것은, 트랜잭션 디바이스(12)에 대한 해싱 키(K)를 찾도록 기존 트랜잭션 디바이스 식별자(I_D)를 사용하여 그리고 이어서 상기 기재된 바와 같이 해시 값(h') 및 단명 공개 키(P'_D)를 재생성하여 수행될 수 있다. 예컨대:

$$h' = HMAC(K, I_D || \text{트랜잭션 데이터})$$

[0089] $$P'_D = h' \bullet G = g^{h'}$$

[0090] 새로 생성된 공개 키(P'_D)와 트랜잭션 메시지에 보내진 공개 키(P_D)의 비교는 메시지에서 수신된 트랜잭션 데이터가 공개 키(P_D)를 생성하도록 사용된 트랜잭션 데이터에 상응하는 지를 증명할 것이다.

[0091] 제 1 트랜잭션 처리 서버(16)는 기존 트랜잭션 디바이스 식별자를 기초로 하여 트랜잭션 메시지를 처리할 수 있다(즉, 제 2 데이터 필드에 제공된 암호화된 데이터로부터 기인한 복호화된 데이터의 적어도 일부). 다시 말해서, 트랜잭션 메시지는, 임시 트랜잭션 디바이스 식별자를 기존 트랜잭션 디바이스 식별자(I_D)로 교체되는 것과 같이 처리될 수 있다. 상기 언급된 바와 같이, 제 1 트랜잭션 처리 서버(16) 자체는 이러한 지점에서 트랜잭션을 승인하거나 거절할 수 있다. 이러한 경우, 단계(32E)에서, 제 1 트랜잭션 처리 서버(16)는, 트랜잭션을 승인하거나 거절할 지를 기존 트랜잭션 디바이스 식별자(I_D)를 사용하여 결정하며, 적절한 응답 메시지를 생성한다. 단계(40)에서, 제 1 트랜잭션 처리 서버(16)는 응답 메시지를 트랜잭션 단말(14)로 다시 보낸다.

[0092] 그러나 대안에서, 제 1 트랜잭션 처리 서버(16)는 단계(32C)에서, 트랜잭션 메시지를 변경하여 임시 트랜잭션 디바이스 식별자를 기존 트랜잭션 디바이스 식별자(I_D)로 교체할 수 있다. 제 1 트랜잭션 처리 서버(16)는 추가로, 단계(32D)에서, 임시 트랜잭션 디바이스 식별자와 기존 트랜잭션 디바이스 식별자(I_D)사이의 관련성을 저장할 수 있다.

[0093] 이어서, 단계(34)에서, 제 1 트랜잭션 처리 서버(16)는 임시 트랜잭션 디바이스 식별자가 기존 트랜잭션 디바이스 식별자로 교체된, 변경된 트랜잭션 메시지를 제 2 트랜잭션 처리 서버(18)에 전달할 수 있다. 제 2 트랜잭션 처리 서버(18)는 암호화되지 않은 트랜잭션 디바이스 식별자가 기존에 제공된 노멀(normal) 메시지로서 변경된 트랜잭션 메시지를 처리할 수 있다.

[0094] 단계(36)에서, 제 1 트랜잭션 처리 서버(16)는 제 2 트랜잭션 처리 서버(18)로부터 응답 메시지를 수신할 수 있다. 이러한 응답 메시지는 트랜잭션 디바이스 식별자를 홀드하도록 구성되는 데이터 필드를 포함할 수 있고, 따

라서, 기존 트랜잭션 디바이스 식별자(I_D)를 포함한다.

[0095] 단계(38)에서, 제 1 트랜잭션 처리 서버(16)는 단계(32D)에서 저장된 관련성을 사용하여 기존 제 2 트랜잭션 디바이스 식별자(I_D)를 제 1 트랜잭션 디바이스 식별자로 교체하도록 응답 메시지를 변경할 수 있다. 변경된 응답 메시지는 단계(40)에서, 트랜잭션 단말(14)로 보내질 수 있다.

[0096] 상기 기재된 방법은 이하의 장점을 제공한다. 먼저, 통상적인 트랜잭션 시스템에 트랜잭션 디바이스 식별자를 포함하도록 설계된 필드는 사이즈에 있어서 제한적이며 엄격한 포맷 규칙을 지킬 필요가 있다. 이것은, 임시 트랜잭션 디바이스 식별자에 대한 자유도를 제한한다. 메시지의 임시 트랜잭션 디바이스 식별자를 제공하고 암호화된 트랜잭션 디바이스 식별자를 제공하여, 트랜잭션 디바이스 식별자를 암호화하기 위한 자유도가 증가되므로 보안이 상응하게 증가된다. 동일하게, 랜덤 또는 의사 랜덤인 요건을 충족할 필요만 있고 이에 따라 트랜잭션 메시지는 트랜잭션 시스템에 의해 적절하게 다뤄지는 것을 가능하게 하여 임시 트랜잭션 디바이스 식별자를 생성하는 것이 수월하다.

[0097] 또한, 트랜잭션 메시지를 단명 암호 키에 제공하여, 트랜잭션 메시지에 제공된 정보가 사용자를 추적하기 위해 사용될 수 없는 것을 보장할 수 있다. 이는, 단명 암호 키가 그 자체가 비결정적이거나 랜덤이므로 사용자를 추적하도록 사용될 수 없기 때문이다.

[0098] 시스템이, 트랜잭션 디바이스 식별자가 수신 서버의 공개 키만을 사용하여 암호화되는 곳에서 사용될 수 있는 것이 주목되어야 한다. 이러한 시스템의 단점은, 상대적으로 고정(static) 키(서버의 키)는 복수의 메시지가 동일한 키를 사용하여 모두 보내져서 결국 시스템의 보안을 감소시키는 것을 의미하기 때문에 공격에 취약하다는 점이다.

[0099] 추가 장점은, 트랜잭션 디바이스 식별자의 유효한 암호화를 가능하게 하도록 요구되는 암호 키의 사이즈에 관한 것이다. 예컨대, 적절한 암호화를 제공하도록 요구되는 ECC 암호 키의 통상적인 길이는 32바이트 이상이다. 메시지에서 이러한 키를 제공하는 것은 대량의 메시지 데이터, 종종 트랜잭션 디바이스 식별자 그 자체 보다 훨씬 많은 양을 차지한다. 예컨대, PAN은 8바이트 미만의 데이터에 의해 고유하게 식별될 수 있고, 이것의 키의 데이터 사이즈의 1/4는 PAN을 암호화하도록 사용될 수 있다. 그러나, 이러한 실시예에서, 암호 키는 또한 트랜잭션 데이터가 증명될 수 있게 하는 데이터의 역할을 한다. 이러한 이중 사용은 임의의 메시지의 데이터 사이즈 효율을 개선하며 상기 기재된 실시예에 따라 암호화된 메시지가 임의의 메시지의 사이즈에 대한 제한을 갖는 기존의 시스템을 사용하여 전송될 수 있다.

[0100] **대안적인 실시예 및 변형**

[0101] ECC 암호법의 특정 구현이 상기 기재되었으나, 암호 키의 생성 및 사용을 위해 변경이 수행될 수 있고 또는 전체적으로 상이한 시스템이 사용될 수 있음이 이해될 것이다. 예컨대, 공유된 비밀(S)은 디바이스 식별자를 바로 암호화하는데 사용될 수 있되, 대안적으로, S를 사용하여 생성된 추가 키가 사용될 수 있다. 대안적으로, 구현은 NTRU와 같은 격자(lattice) 기반 암호화 방법을 사용할 수 있다. 이러한 구현에 있어서, 암호화 메커니즘의 출력이 유효하게 랜덤이므로 서버에 별개의 단명 키를 통신할 필요가 없다.

[0102] 상기 기재된 특정 구현에서, 임시 트랜잭션 디바이스 식별자는 랜덤이므로 트랜잭션 메시지의 정보는 트랜잭션 디바이스(12)를 추적하는데 사용될 수 없고 따라서 트랜잭션 디바이스(12)의 사용자를 잠재적으로 추적하지 않는다. 대안적으로, 랜덤인 임시 트랜잭션 디바이스 식별자 대신, 본 발명을 활용하는 다수의 또는 모든 트랜잭션 디바이스에 동일한 트랜잭션 디바이스(12)에 의해 저장된 고정 숫자는 트랜잭션 디바이스 식별자를 위한 트랜잭션 메시지의 필드에 인서트될 수 있다. 이런 식으로, 트랜잭션 메시지내의 트랜잭션 디바이스 식별자 필드 내에서 진입으로부터 트랜잭션 디바이스의 아이덴티티를 결정하는 것이 불가능하다. 또한, 이러한 정적 트랜잭션 디바이스 식별자는 실제 트랜잭션 디바이스 식별자의 암호화된 버전이 트랜잭션 메시지의 별개의 필드에 제공된다는 트랜잭션 메시지의 수신을 표시하도록 사용될 수 있다.

[0103] 실시예는 기존의 시스템과 호환 가능하도록 의도된다. 따라서, 트랜잭션 디바이스(12)에 의해 보내진 메시지는 기존 프로토콜에 따를 수 있다. 특히, 트랜잭션 디바이스(12) 및 제 1 트랜잭션 처리 서버(16)만이 전체 시스템이 이전과 같이 작동하게 할 수 있도록 변경될 필요가 있도록 의도된다. 결과적으로, 제 1 트랜잭션 처리 서버(16)는 제 2 트랜잭션 처리 서버(18)의 변경을 요하지 않고 트랜잭션 디바이스(12)에 의해 제공된 임의의 메시지를 제 2 트랜잭션 처리 서버(18)에 의해 사용가능한 포맷으로 전환되도록 작동할 수 있다.

[0104] 특정 실시예에서, 임시 트랜잭션 디바이스 식별자가 암호화된 트랜잭션 디바이스 식별자에 상응할 수 있으며 따

라서 기존 디바이스 식별자를 회수하도록 사용될 수 있다. 이것은 임의의 추가 필드에 대한 요구를 회피한다.

[0105] 암호 키가 트랜잭션 메시지를 갖고 전송되는 것으로 기재되되, 일부 실시예들은 제 1 트랜잭션 처리 서버(16)에 의해 복제될 수 있는 방식으로 트랜잭션 데이터로부터 암호 키를 생성하도록 배열될 수 있다. 따라서, 제 1 트랜잭션 처리 서버(16)에서, 암호 키는 트랜잭션 메시지에 제공된 적어도 트랜잭션 데이터를 사용하여 생성될 수 있다. 이러한 암호 키는 기존 트랜잭션 디바이스 식별자를 포함하는 암호화 데이터 소자를 복호화하도록 사용될 수 있다.

[0106] 실시예에서, 기존 트랜잭션 디바이스 식별자는 제 2 트랜잭션 처리 서버(18)에 의해 사용 가능한 트랜잭션 디바이스 식별자에 대한 포인터가 될 수 있다. 이러한 제 1 트랜잭션 처리 서버(16)는 적절한 트랜잭션 디바이스 식별자를 포인터가 식별하도록 사용될 수 있는 룩업 테이블을 소지할 수 있다. 그러므로, 제 2 트랜잭션 처리 서버(18)가 요구되지 않되, 트랜잭션 디바이스(12)와 제 1 트랜잭션 처리 서버(16) 사이에서 통과된 식별자는 제 2 트랜잭션 처리 서버(18)에 의해 이용 가능한 적절한 식별자에 대한 요건에 따라 선택될 필요가 없다.

[0107] 상기 기재된 특정 구현에서, 트랜잭션 단말(14)은 트랜잭션 메시지를 트랜잭션 디바이스(12)로부터 제 1 트랜잭션 처리 서버(16)로 보내며 제 1 트랜잭션 처리 서버(16)는 트랜잭션 디바이스(12)에 대한 트랜잭션 디바이스 식별자를 회복한다. 특정 구현에서, 트랜잭션 단말(14)은 트랜잭션 단말이 제 1 트랜잭션 처리 서버로부터 응답을 대기할 경우 성취될 수 있는 더 빠른 트랜잭션을 승인하도록 요구될 수 있다. 이러한 구현의 예시는, 티켓 게이트 내의 트랜잭션 단말이 트랜잭션을 승인하고 티켓 정보를 단시간 내에 트랜잭션 디바이스(12)로 전달할 필요가 있는 티켓 게이트 배열이다. 이러한 구현에서, 트랜잭션 단말(14)은 트랜잭션 단말(14)에 대한 공개 키 인증서를 포함하는 메시지를 트랜잭션 디바이스(12)에 전달할 수 있으며, 트랜잭션 디바이스(12)는 트랜잭션 단말(14)에 대한 인증서로부터 생성된 또는 추출된 공개 키를 사용하여, 바람직하게, 상기 기재된 암호화 스킴을 사용하여 트랜잭션 디바이스 식별자를 암호화하며 암호화된 트랜잭션 디바이스 식별자를 트랜잭션 단말(14)에 전달할 수 있다. 트랜잭션 단말(14)은 트랜잭션 디바이스 식별자를 회복하며 예컨대 회복된 트랜잭션 디바이스 식별자와, 트랜잭션 단말(14)에 의해 저장된 트랜잭션 디바이스 식별자의 블랙리스트를 비교하여, 트랜잭션이 트랜잭션 승인 전에 일어나서는 안되는 트랜잭션 디바이스(12)를 표시할 수 있다.

[0108] 실시예에서, 트랜잭션 디바이스 그 자체는 스마트카드 또는 포브와 같은 자장(self-contained) 디바이스가 될 수 있다. 다른 실시예에서, 트랜잭션 디바이스(12)는 휴대 전화 또는 컴퓨터와 같은 상용 컴퓨팅 디바이스가 될 수 있으며, 이것은, 트랜잭션 메시지를 생성하는 장치를 포함하거나 그에 연결된다. 이러한 장치는 변형 억제(tamper resistant) 하드웨어; 즉 보안 요소일 수 있다. 이러한 경우에, 단말에 메시지를 전달하는 것과 같은 주어진 동작을 수행하는 트랜잭션 디바이스에 대한 참조는 다른 디바이스(예컨대, 휴대 전화)에 이러한 메시지를 전달하도록 하는 트랜잭션 디바이스를 나타내는 것으로 이해될 것이다.

[0109] 최근, 컴퓨팅 디바이스(휴대 전화)가 보안 요소를 요하지 않고도 사용될 수 있는 시스템이 제안되었다. 이러한 시스템상에서, 트랜잭션 어플리케이션이 디바이스의 어플리케이션 프로세서 내에서 수행되는 "호스트 카드 이뮬레이션(Host Card Emulation)"으로 불린다. 대안적이되 유사한 시스템은, 적절한 디바이스 내의 "신뢰된 수행 환경(Trusted Execution Environment)"의 사용이다. 본 발명의 실시예는 이들 및 유사한 시스템에 적용가능하다.

[0110] 특정 실시예에서, 트랜잭션 디바이스(12)는 트랜잭션 단말(14)로부터 임의의 트랜잭션 데이터를 수신하지 않을 수 있되, 트랜잭션 데이터 그 자체를 생성할 수 있다. 추가 실시예에서, 트랜잭션 데이터는 기타 수단에 의해 수용될 수 있다. 예컨대, 트랜잭션에서 휴대 전화를 사용하고, 이러한 휴대 전화가, 휴대전화와 단말 사이의 무접촉(예컨대, NFC) 연결을 통해 발생할 수 있는 임의의 트랜잭션과 함께 모바일 네트워크를 통해 데이터를 보내고 수신하는 것이 제안되었다. 이러한 경우에, 상기 기재된 통신 중 적어도 일부에서, 트랜잭션 디바이스에 대한 트랜잭션 데이터의 제공 또는 트랜잭션 메시지의 전송의 여부는 트랜잭션 단말(14)이 아닌 기타 통신 시스템을 포함할 수 있는 것이 구상될 수 있다.

[0111] 트랜잭션 디바이스(12)와 트랜잭션 단말(14) 사이의 연결은 상기 기재된 바와 같이 양방향일 수 있되 동등하게 단방향일 수도 있다. 예컨대, 이동 전화는 단방향 연결을 통해(예컨대, 단말에 의해 광학적으로 디스플레이된 코드를 포토그래핑하여) 단말로부터 트랜잭션 데이터를 수신할 수 있으며, 셀룰러 연결 또는 와이파이와 같은 무선 통신 네트워크를 통해 적절한 트랜잭션 메시지를 생성하며 보낼 수 있다. 이러한 경우에, 트랜잭션 단말은 트랜잭션 처리 네트워크를 갖는 임의의 통신 능력을 그 자체가 가질 수 없으며, 예컨대, QR 코드와 같은 광학적 코드를 디스플레이하는 포스터일 수 있다.

[0112] 특정 실시예에서, 이처럼 트랜잭션 단말(14)이 존재할 수 있으며 트랜잭션 디바이스(12)는 네트워크에 의해 그렇게 하여 제 1 트랜잭션 처리 서버(16)에 의해 직접적으로 통신할 수 있다. 이것은, 트랜잭션 디바이스(12)가 연결된 컴퓨터 또는 휴대용 디바이스가 있는 온라인 트랜잭션에 대하여 사용될 수 있다.

[0113] 특정 실시예에서, 메시지가 인증되는 것을 가능하게 하기 위한 크리덴셜과 같은 기타 정보는 디바이스 식별자와 함께 암호화될 수 있다.

[0114] 암호 키는 압축될 수 있다. 예컨대, 완전한 타원 함수 암호 키는 X 구성요소 및 Y 구성요소를 갖는다. Y 구성요소에 대한 사인을 표시하도록 1 비트 또는 2 비트의 데이터와 함께 X 구성요소만을 제공하는 키를 압축하는 것이 가능하다. X 구성요소, 사용된 함수 및 Y 구성요소의 사인의 인지는, 가려낸 암호 키가 재생성되는 것을 가능하게 한다. 상기 기재에서, 키가 결정되거나 제공되는 것으로 기재되는 경우, 그의 압축된 버전은 동등하게 사용될 수 있는 것이 이해될 것이다.

[0115] 트랜잭션 디바이스(12), 트랜잭션 단말(14) 및 트랜잭션 처리 서버(16 및 18)는 선행 기술에 알려진 바와 같이 컴퓨터화된 하드웨어를 포함할 수 있다. 상기 기재된 방법 단계들을 수행할 수 있는 예시적인 컴퓨터화된 시스템(50)은 도 5를 참조하여 이제 기재될 것이다.

[0116] 컴퓨터화된 시스템(50)은 CPU 또는 CPU의 어레이와 같은 처리 시스템(51)을 포함한다. 처리 시스템(51)은 메모리(52)와 같은 컴퓨터로 판독 가능한 저장 매체에 연결된다. 이러한 메모리는 예컨대 고체 상태 드라이브(SSD) 또는 하드 디스크 드라이브(HDD) 메모리인, 예컨대 휘발성 메모리(예컨대, RAM) 또는 비휘발성 또는 비일시적 메모리일 수 있다. 시스템(50)은 또한 시스템의 다른 요소로부터 데이터를 전송하고 및/또는 수신할 수 있는 인터페이스(54)를 포함할 수 있다.

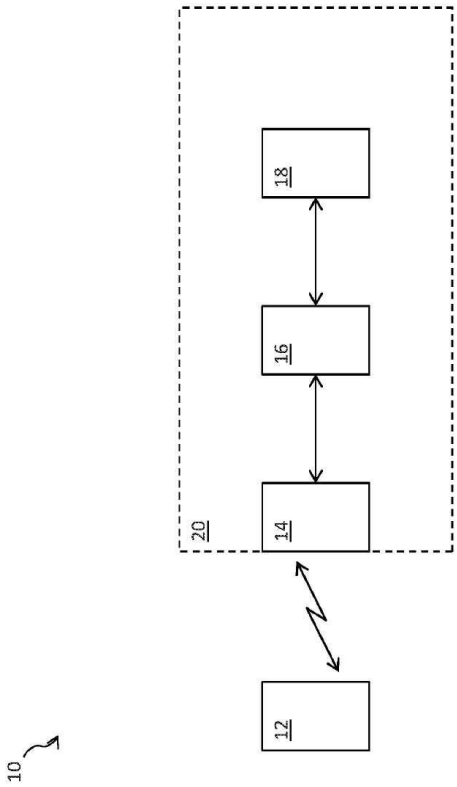
[0117] 메모리(52)는 컴퓨터로 판독 가능한/컴퓨터로 수행 가능한 명령(53)을 저장한다. 컴퓨터 판독 가능한 명령은, 이것이 처리 시스템(51)에 의해 수행될 때 컴퓨터화된 시스템(50)이 상기 기재된 방법을 수행하게끔 되도록 구성될 수 있다. 이를 가능하게 하기 위하여, 처리 시스템(51)은 메모리(52)로부터 컴퓨터 명령(53)을 회수하고 이러한 명령을 수행할 수 있다. 이를 수행하는데 있어서, 처리 시스템(51)은 인터페이스가 필요시에 데이터를 전송하거나 수신하게끔 할 수 있다.

[0118] 이러한 데이터 그 자체는 메모리(52)에 저장되며, 필요시, 예컨대 인터페이스(54)를 통해 전송되도록 회수될 수 있다.

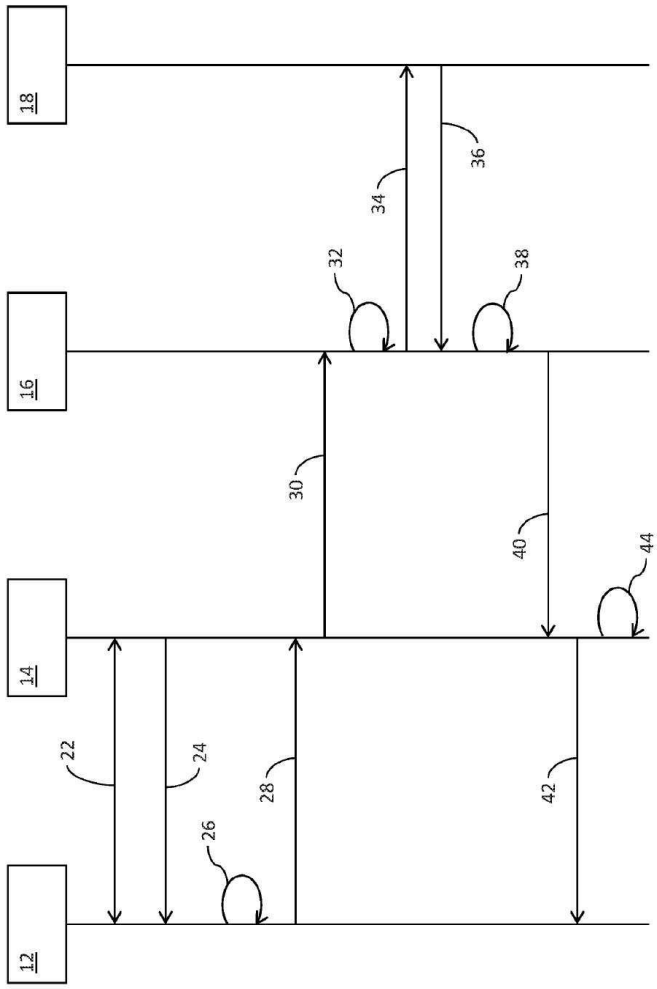
[0119] 임의의 하나의 실시예와 연계하여 기재한 임의의 특성이 단독으로 또는 기재한 다른 특성과 결합하여 사용될 수 있음과, 실시예 중 임의의 다른 것 또는 실시예 중 임의의 다른 것의 임의의 조합의 하나 이상의 특성과 결합하여 사용될 수 있음도 이해해야 할 것이다. 더 나아가, 앞서 기재하지 않은 등가물 및 변경은, 수반하는 청구범위에 한정된 본 발명의 범위에서 벗어나지 않고 이용될 될 수도 있다. 청구범위의 특성은 청구범위에 명시한 것들이 아닌 결합으로 결합될 수 있다.

도면

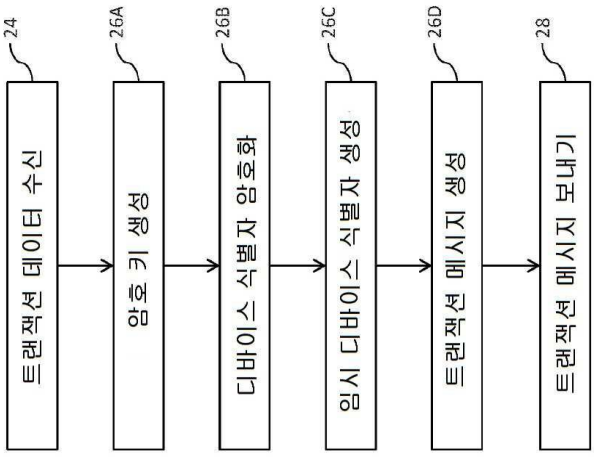
도면1



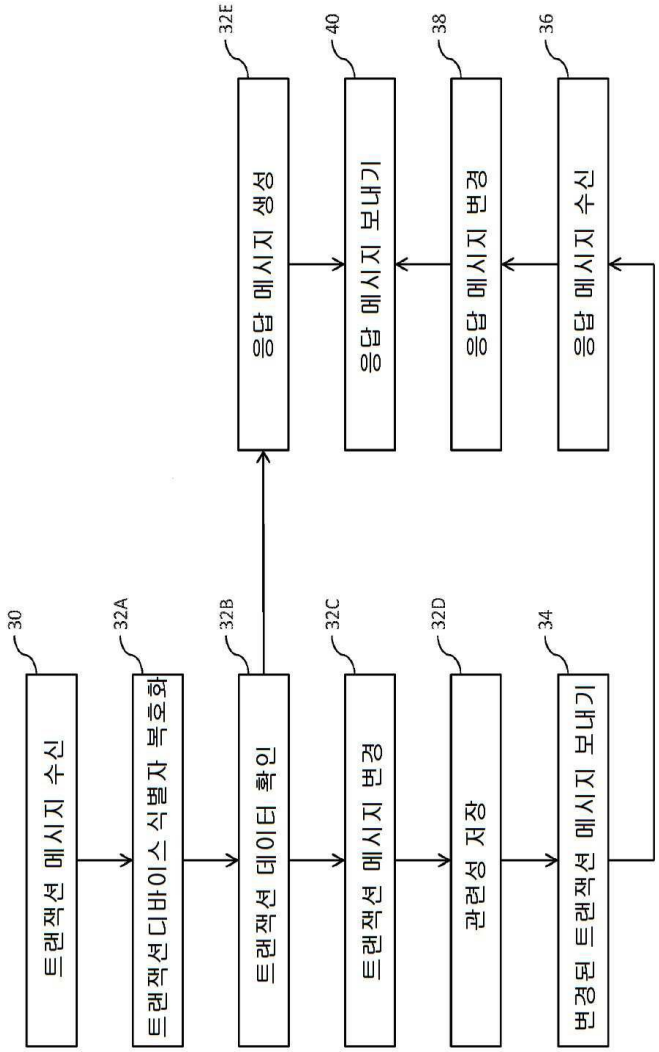
도면2


18
16
14
12
22
24
26
28
30
32
34
36
38
40
42
44

도면3


24
트랜잭션 데이터 수신
26A
암호 키 생성
26B
디바이스 식별자 암호화
26C
임시 디바이스 식별자 생성
26D
트랜잭션 메시지 생성
28
트랜잭션 메시지 보내기

도면4


30
트랜잭션 메시지 수신
32A
트랜잭션디바이스 식별자 복호화
32B
트랜잭션 데이터 확인
32C
트랜잭션 메시지 변경
32D
관련성 저장
34
변경된 트랜잭션 메시지 보내기
32E
응답 메시지 생성
40
응답 메시지 보내기
38
응답 메시지 변경
36
응답 메시지 수신

도면5