(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2025년06월26일
(11) 등록번호 10-2825432
(24) 등록일자 2025년06월23일

(51) 국제특허분류(Int. Cl.)
G06Q 20/40 (2012.01) *G06Q 20/10* (2012.01)
G06Q 20/12 (2012.01) *G06Q 20/20* (2012.01)
G06Q 20/32 (2012.01) *G06Q 20/34* (2012.01)
G06Q 20/38 (2012.01) *H04L 9/06* (2006.01)
(52) CPC특허분류
G06Q 20/40975 (2020.05)
G06Q 20/108 (2013.01)
(21) 출원번호 10-2021-7004499
(22) 출원일자(국제) 2019년10월02일
심사청구일자 2022년07월21일
(85) 번역문제출일자 2021년02월16일
(65) 공개번호 10-2021-0069033
(43) 공개일자 2021년06월10일
(86) 국제출원번호 PCT/US2019/054186
(87) 국제공개번호 WO 2020/072575
국제공개일자 2020년04월09일
(30) 우선권주장
62/740,352 2018년10월02일 미국(US)
(뒷면에 계속)
(56) 선행기술조사문헌
EP03343488 A1*
JP2009514262 A*
JP2018137587 A*
US08196131 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
캐피탈 원 서비시즈, 엘엘씨
미국 버지니아주 22102, 맥린, 캐피탈 원 드라이브 1680
(72) 발명자
오스본, 케빈
미국 매사추세츠주 02461, 뉴턴 하이랜즈, 힐사이드 로드 49
애쉬필드, 제임스
미국 버지니아주 23113, 미들로디언, 올드 포트 드라이브 14106
(뒷면에 계속)
(74) 대리인
김동완

전체 청구항 수 : 총 20 항 심사관 : 강명수

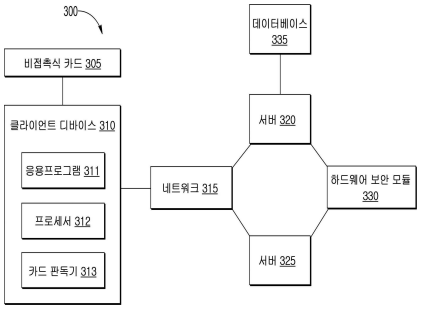
(54) 발명의 명칭 **비접촉식 카드의 암호화 인증을 위한 시스템 및 방법**

(57) 요 약

FIDO 인증을 지원하는 비접촉식 카드와 클라이언트 디바이스 간의 데이터 전송을 위한 시스템 및 방법의 예시적인 실시형태를 제공하는 것이다. 하나의 실시형태에서 진행중인 거래와 관련하여 서버에 의해 발행된 챌린지를 수신하면 비접촉식 카드는 챌린지에 응답하기 위해 FIDO 개인 키를 사용하도록 클라이언트 디바이스를 승인할 수

(뒷면에 계속)

대 표 도



있다. 챌린지에 대한 응답이 성공하면 FIDO 인증이 진행되고 거래가 완료된다.

(52) CPC특허분류
G06Q 20/12 (2013.01)
G06Q 20/204 (2013.01)
G06Q 20/3226 (2013.01)
G06Q 20/341 (2013.01)
G06Q 20/343 (2013.01)
G06Q 20/352 (2013.01)
G06Q 20/3825 (2013.01)
G06Q 20/3829 (2013.01)
H04L 9/0631 (2013.01)

(72) 발명자
치구루파티, 스리니바사
미국 일리노이주 60047, 롱 그로브, 틸 코트 5804
룰, 제프리
미국 메릴랜드주 20815, 체비 체이스, 레어드 플레이스 3906

(30) 우선권주장
16/205,119 2018년11월29일 미국(US)
16/590,429 2019년10월02일 미국(US)

명 세 서

청구범위

청구항 1

클라이언트 응용프로그램, 마스터 키 및 다양화 키를 저장하는 비일시적 메모리에 있어서,

상기 클라이언트 응용프로그램은 프로세서, 메모리 및 통신 인터페이스를 포함하는 클라이언트 디바이스 상에서 실행하기 위한 명령어를 포함하고, 및

상기 클라이언트 응용프로그램은

서버로부터 챌린지를 수신하고,

비접촉식 카드로 인증 요청 시그널을 전송하고,

인증 데이터는 다양화 키로 암호화 되어 있고, 비접촉식 카드로부터 수신된 인증 데이터를 서버로 전송하고,

신속한 온라인 인증(FIDO) 개인 키의 사용을 허용하는 검증인 비접촉식 카드로부터 조회된 인증 데이터에 대한 검증을 서버로부터 수신하고,

FIDO 개인 키를 사용하여 챌린지에 서명하고, 및

서명된 챌린지를 서버로 전송;

하도록 형상화 됨을 특징으로 하는 비일시적 메모리.

청구항 2

제 1항에 있어서, 상기 클라이언트 응용프로그램은 FIDO 공개 키를 서버로 전송하도록 형상화 됨을 특징으로 하는 비일시적 메모리.

청구항 3

제 1항에 있어서, 상기 클라이언트 응용프로그램은 FIDO 개인 키를 클라이언트 디바이스의 메모리 내에 저장함을 특징으로 하는 비일시적 메모리.

청구항 4

제 1항에 있어서, 상기 클라이언트 응용프로그램은 서버로부터 챌린지를 수신하기 전에 챌린지에 대한 요청을 서버로 전송하도록 형상화 됨을 특징으로 하는 비일시적 메모리.

청구항 5

제 1항에 있어서, 상기 인증 데이터는 통신 인터페이스에 의해 생성된 근거리 통신 필드를 통해 비접촉식 카드로부터 수신됨을 특징으로 하는 비일시적 메모리.

청구항 6

제 1항에 있어서, 상기 클라이언트 응용프로그램은 FIDO 개인 키를 사용하여 챌린지에 서명하기 전에 검증 입력을 수신하도록 형상화 됨을 특징으로 하는 비일시적 메모리.

청구항 7

제 1항에 있어서,

비일시적 메모리는 식별 정보와 마스터 키를 더욱 저장하고, 및

응용프로그램은 마스터 키와 함께 식별 정보를 사용하여 다양화 키를 생성하도록 형상화 됨

을 특징으로 하는 비일시적 메모리.

청구항 8

제 7항에 있어서, 상기 식별 정보는 웹사이트에 대한 사이트 식별자를 포함함을 특징으로 하는 비일시적 메모리.

청구항 9

제 1항에 있어서, 상기 서버는 웹사이트와 연관됨을 특징으로 하는 비일시적 메모리.

청구항 10

제 1항에 있어서,

비일시적 메모리는 카운터 및 마스터 키를 저장하고, 및

응용프로그램은 마스터 키와 카운터를 사용하여 다양화 키를 생성하도록 형상화 됨

을 특징으로 하는 비일시적 메모리.

청구항 11

제 1항에 있어서, 상기 클라이언트 응용프로그램은 서버로부터 카운터를 수신하도록 형상화 됨을 특징으로 하는 비일시적 메모리.

청구항 12

제 1항에 있어서, FIDO 개인 키는 비접촉식 카드에 저장되고 다양화 키를 사용하여 암호화된 후, 비접촉식 카드의 NFC 판독을 통해 클라이언트 응용프로그램으로 전송됨을 특징으로 하는 비일시적 메모리.

청구항 13

제 1항에 있어서, 상기 챌린지는 난수 또는 난수 문자열 중 하나를 포함함을 특징으로 하는 비일시적 메모리.

청구항 14

프로세서, 신속한 온라인 인증(FIDO) 개인 키와 FIDO 공개키를 저장하는 메모리 및 통신 인터페이스를 포함하는 클라이언트 디바이스 상에서 실행하기 위한 명령어를 포함하는 클라이언트 응용프로그램에 의해 서버로부터 챌린지를 수신하는 단계;

비접촉식 카드로 인증 요청을 클라이언트 응용프로그램에 의해 전송하는 단계;

비접촉식 카드로부터 수신된 인증 데이터를 클라이언트 응용프로그램에 의해서버로 전송하고,

FIDO 개인 키의 사용을 허용하는 검증인 비접촉식 카드로부터 조회된 인증 데이터에 대한 검증을 클라이언트 응용프로그램에 의해 서버로부터 수신하는 단계;

FIDO 개인 키를 사용하여 클라이언트 응용프로그램에 의해 챌린지에 서명하는 단계; 및

서명된 챌린지를 서버로 클라이언트 응용프로그램에 의해 전송하는 단계.

를 포함하는 방법.

청구항 15

제 14항에 있어서, 상기 FIDO 공개 키를 서버로 클라이언트 응용프로그램에 의해 전송하는 단계를 포함함을 특징으로 하는 방법.

청구항 16

제 14항에 있어서, 상기 클라이언트 응용프로그램은 FIDO 개인 키를 클라이언트 디바이스의 메모리 내에 저장함을 특징으로 하는 방법.

청구항 17

제 14항에 있어서, FIDO 개인 키를 사용하여 챌린지에 서명하기 전에 검증 입력을 클라이언트 응용프로그램에 의해 수신하는 단계를 포함함을 특징으로 하는 방법.

청구항 18

카운터, 다양화 키, 신속한 온라인 인증(FIDO) 공개 키 및 FIDO 개인 키를 포함하는 메모리;

통신 인터페이스; 및

메모리 및 통신 인터페이스와 통신하는 프로세서;를 포함하는 비접촉식 카드에 있어서,

상기 프로세서는:

통신 인터페이스가 클라이언트 디바이스와 연관된 통신 필드의 범위 내에 있을 때 카운터를 업데이트하고;

클라이언트 디바이스로부터 거래 검증 요청을 통신 인터페이스를 통해 수신하고;

FIDO 개인 키를 저장하는 암호문을 다양화 키와 카운터를 사용하여 생성하고; 및

트랜잭션 검증 응답은 FIDO 개인 키를 챌린지와 결합하여 암호화된 형태로 클라이언트 디바이스에 제공하고, 암호를 포함하는 트랜잭션 검증 응답을 클라이언트 디바이스에 전송

하도록 형상화 됨을 특징으로 하는 비접촉식 카드.

청구항 19

제 18항에 있어서, 상기 프로세서는 클라이언트 디바이스 상에서 실행되는 응용프로그램에 통신 인터페이스를 통해 암호문을 전송하도록 형상화 됨을 특징으로 하는 비접촉식 카드.

청구항 20

제 18항에 있어서, 트랜잭션 검증 응답 내의 암호는 클라이언트 디바이스에 의해 검증 서버로 전송되는 FIDO 공개 키를 더 포함함을 특징으로 하는 비접촉식 카드.

발명의 설명

기 술 분 야

[0001] 본 출원은 2018년 10월 2일에 출원된 미국 잠정 특허출원 제62/740,352호, 2018년 10월 2일에 출원된 미국 특허출원 제16/590,429호 우선권을 주장하는 2018년 11월 29일자로 부분 계속 출원된 미국 특허출원 16/205,119호의 우선권을 주장하며 이들 모두는 전체적으로 본 출원에 참고 문헌으로 통합되어 있다.

[0002] 본 명세서는 암호화에 관한 것으로, 더욱 상세하게는 비접촉식 카드의 암호화 인증을 위한 시스템 및 방법에 관한 것이다.

배 경 기 술

[0003] 데이터 보안 및 거래 무결성(integrity)은 기업과 소비자에게 매우 중요하다. 전자 거래가 점점 더 많은 상업 활동의 기반이 됨에 따라 이러한 요구는 계속해서 증가하고 있다.

[0004] 이메일은 거래를 검증하는 도구로 사용될 수 있지만 이메일은 공격을 받기 쉽고 해킹이나 기타 무단 액세스에

취약하다. 단문 메시지 서비스(SMS) 메시지도 사용할 수 있으나 이는 손상될 수 있다. 또한 트리플 DES 알고리즘과 같은 데이터 암호화 알고리즘도 유사한 취약점을 지니고 있다.

[0005] 예를 들어 금융 카드(예: 신용카드 및 기타 지불 카드)를 포함하는 다양한 카드를 활성화하려면 카드 소지자가 전화 번호로 전화를 걸거나 웹 사이트를 방문하고 카드 정보를 입력하거나 제공하는 데 시간이 많이 소요된다. 또한 칩 기반 금융 카드의 사용이 증가함에 따라 직접 구매를 위한 종래 기술(예: 마그네틱 띠 카드)보다 더 안전한 기능을 제공하지만 계정 접근은 카드 소유주의 신원을 확인하기 위해 여전히 로그인 자격증명(예: 사용자 이름 및 암호)에 의존할 수 밖에 없다. 그러나 로그인 자격증명이 도용되면 다른 사람이 해당 사용자의 계정에 접근할 수 있다.

[0006] 보안에 대한 우려에도 불구하고, 계정 액세스 및 중요 정보를 보호하기위한 로그인 자격 증명 암호의 광범위한 사용이 계속되고 있다. 이 문제에 대한 잠재적인 해결책인 FIDO 인증 표준을 만들기 위해 FIDO2 프로젝트의 형태로 FIDO Alliance에서 제안하고 있다. FIDO2 프로젝트는 W3C의 웹 인증 사양과 FIDO 클라이언트 인증 프로토콜을 통합하여 통상의 디바이스를 사용하여 온라인 서비스를 인증하고 계정 액세스를 제어할 수 있도록 하는 것이다. FIDO2 프로젝트는 개인 키를 사용하여 인증 장치에서 응답하는 암호화 챌린지로 시작되는 디바이스 인증을 제공하는 것이다. 그러나 디바이스 인증 프로세스를 시작할 때 권한이 부여된 사용자가 존재함을 입증하는 데 어려움이 있는 등 보안 문제가 남아 있다.

[0007] 이러한 결함과 기타 결함이 존재한다. 따라서 비접촉식 카드에 대한 데이터 보안, 인증 및 검증을 제공하기 위해 이러한 결함을 극복하는 적절한 솔루션을 사용자에게 제공할 필요가 있다. 또한, 카드를 활성화하는 개선된 방법과 계정 액세스를 위한 개선된 인증이 모두 요구된다.

발명의 내용

과제의 해결 수단

[0008] 개시된 기술의 측면은 비접촉식 카드의 암호화 인증을 위한 시스템 및 방법을 포함한다. 다양한 실시형태는 비접촉식 카드의 암호화 인증을 구현하고 관리하기 위한 시스템 및 방법을 설명한다.

[0009] 본 발명의 실시형태는 프로세서; FIDO 공개 키, FIDO 개인 키 및 계정 정보를 포함하는 메모리; 및 비접촉식 카드와 서버 간에 데이터 커뮤니케이션하는 통신 필드를 지니는 통신 인터페이스를 포함하는 클라이언트 디바이스를 제공하는 것으로, 이때 프로세서는 거래를 시작하라는 명령어를 수신하면, 프로세서는 거래와 관련된 계정 정보 및 거래 정보를 포함하는 거래 요청을 제1 서버로 전송하고; 제2 서버로부터 챌린지를 수신하고; 비접촉식 카드로부터 거래 확인을 요청하며; 통신 인터페이스를 통해 비접촉식 카드가 통신 필드에 입력되면 챌린지와 관련하여 FIDO 개인 키의 사용을 허용하게 함으로서 비접촉식 카드로부터 거래 확인을 수신하고; 개인 키를 사용하여 챌린지에 서명하고; 및 서명된 챌린지를 제2 서버로 전송하도록 형상화 된 것이다.

[0010] 본 발명의 실시형태는 클라이언트 디바이스에서 실행하기 위한 명령어를 포함하는 클라이언트 응용프로그램에 의해 제1 서버와의 거래를 시작하는 단계; 클라이언트 응용프로그램에 의해 거래 정보를 제1 서버로 전송하는 단계; 클라이언트 응용프로그램에 의해 제2 서버에 의해 전송된 챌린지를 수신하는 단계; 클라이언트 응용프로그램에 의해 거래 확인을 요청하는 단계; 거래 확인은 챌린지에 서명할 수 있도록 클라이언트 응용프로그램에 클라이언트 디바이스의 메모리 내에 저장된 FIDO 개인 키의 사용을 승인하면서 클라이언트 응용프로그램에 의해 거래 확인을 수신하는 단계; 클라이언트 응용프로그램에 의해 FIDO 개인 키를 사용하여 챌린지를 서명하는 단계; 클라이언트 응용프로그램에 의해 서명된 챌린지를 서버로 전송하는 단계; 및 클라이언트 응용프로그램에 의해 거래가 승인되었다는 표시를 서버로부터 수신하는 단계;를 포함하는 승인 방법을 제공하는 것이다.

[0011] 본 발명의 실시형태는 애플릿, 카운터 값, 마스터 키, 다양화 키, FIDO 공개 키 및 FIDO 개인 키를 지닌 메모리를 포함하는 기판; 통신 인터페이스; 메모리 및 통신 인터페이스와 통신하는 프로세서로 이루어지고, 이때 프로세서는 통신 인터페이스가 클라이언트 디바이스의 통신 필드 범위 내에 있을 때 카운터 값을 업데이트하고, 다양화 키와 카운터 값을 사용하여 암호를 생성하고, 암호는 FIDO 공개 키를 저장하고, 통신 인터페이스를 통해 암호를 전송할 수 있도록 형상화된 비접촉식 카드를 제공하는 것이다.

[0012] 개시된 본 발명의 추가 특징 및 이에 의해 제공되는 이점은 첨부된 도면에 예시된 특정 예시적 실시예를 참조하여 다음과 같이 상세히 설명한다.

도면의 간단한 설명

[0013] 도 1a는 예시적인 실시형태에 따른 데이터 전송 시스템의 다이어그램이다.

도 1b는 예시적인 실시형태에 따라 인증된 접근을 제공하기 위한 순서를 나타내는 다이어그램이다.

도 2는 예시적인 실시형태에 따른 데이터 전송 시스템의 다이어그램이다.

도 3은 예시적인 실시형태에 따른 비접촉식 카드를 사용하는 시스템의 다이어그램이다

도 4는 예시적인 실시형태에 따른 키 다양화 방법을 나타내는 흐름도이다.

도 5a는 예시적인 실시형태에 따른 비접촉식 카드의 예시이다.

도 5b는 예시적인 실시형태에 따른 비접촉식 카드 접촉 패드의 예시이다.

도 6은 예시적인 실시형태에 따라 디바이스와 통신하기 위한 메시지를 도시하는 예시이다.

도 7은 예시적인 실시형태에 따른 메시지 및 메시지 포맷을 도시하는 예시이다.

도 8은 예시적인 실시형태에 따른 키 작동을 나타내는 흐름도이다.

도 9는 예시적인 실시형태에 따른 키 시스템의 다이어그램이다.

도 10은 예시적인 실시형태에 따른 암호를 생성하는 방법의 흐름도이다.

도 11은 예시적인 실시형태에 따른 키 다양화 프로세스를 나타내는 흐름도이다.

도 12는 예시적인 실시형태에 따른 카드 활성화를 위한 방법을 나타내는 흐름도이다.

도 13은 하나의 실시형태에 따른 데이터 전송 시스템을 사용하는 FIDO 시스템을 나타낸 것이다.

도 14는 예시적인 실시형태에 따른 온라인 결제를 처리하기 위한 흐름도를 도시한 것이다.

도 15는 예시적인 실시형태에 따른 온라인 결제를 처리하기 위한 클라이언트 디바이스를 위한 사용자 인터페이스를 도시한 것이다.

도 16은 예시적인 실시형태에 따른 온라인 결제를 처리하기 위한 클라이언트 디바이스를 위한 사용자 인터페이스를 도시한 것이다.

발명을 실시하기 위한 구체적인 내용

[0014] 실시형태에 대한 다음의 설명은 본 발명의 상이한 측면의 특징 및 교시를 구체적으로 설명하기 위해 숫자를 참조하는 비-제한적인 대표적 실시예를 제공한다. 설명된 실시형태는 실시형태의 설명과 별도로 또는 다른 실시형태와 조합하여 구현할 수 있는 것으로 인식되어야 한다. 실시형태의 설명을 검토하는 당업자는 본 발명의 다른 설명된 측면을 배우고 이해할 수 있어야 한다.

[0015] 실시형태의 설명은 다른 실시형태가 가능한 정도로 본 발명의 이해를 용이하게 해야 하며 구체적으로 다루지는 않지만 실시형태의 설명을 읽은 당업자의 지식 내에서 본 발명의 적용이 상응하는 것으로 이해될 것이다.

[0016] 본 명세서의 일부 실시형태의 목적은 하나 이상의 비접촉식 카드에 하나 이상의 키를 구축하는 것이다. 이러한 실시형태에서 비접촉식 카드는 인증 및 여러 다른 기능을 수행할 수 있으며 그렇지 않으면 사용자가 비접촉식 카드 외에 별도의 물리적 토큰을 휴대해야할 수 있다. 비접촉식 인터페이스를 적용함으로써 비접촉식 카드는 사용자의 디바이스(예: 이동 전화)와 카드 자체 사이에서 상호 작용하고 통신하는 방법을 제공할 수 있다.

[0017] 예를 들어 많은 신용카드 거래의 기초가 되는 EMV 프로토콜에는 Android® 운영 체제에는 충분하지만 iOS®에는 문제가 있는 인증 프로세스가 포함되어 있다. 이는 근거리 무선 통신(NFC) 사용과 관련하여 더 제한적이며 읽기 전용 방식으로 만 사용할 수 있기 때문이다. 본 명세서에 설명된 비접촉식 카드의 예시적인 실시형태는 NFC 기술을 이용한다.

[0018] 도 1a는 예시적인 실시형태에 따른 데이터 전송 시스템을 도시한다. 하기에 추가로 논의되는 바와 같이 시스템(100)은 비접촉식 카드(105), 클라이언트 디바이스(110), 네트워크(115) 및 서버(120)를 포함할 수 있다. 도 1a는 컴포넌트의 단일 인스턴스를 도시하지만 시스템(100)은 임의의 수의 컴포넌트를 포함할 수 있다.

[0019] 시스템(100)은 하나 이상의 비접촉식 카드(105)를 포함할 수 있으며 이는 도 5a 내지 도 5b를 참조하여 다음에 더욱 상세히 설명한다. 일부 실시형태에서 비접촉식 카드(105)는 실시예에서 NFC를 사용하여 클라이언트 디바이

스(110)와 무선 통신할 수 있다.

[0020] 시스템(100)은 네트워크-가능 컴퓨터일 수 있는 클라이언트 디바이스(110)를 포함할 수 있다. 본 명세서에서 언급된 바와 같이 네트워크-가능 컴퓨터는 예를 들어 서버, 네트워크 기기, 개인용 컴퓨터, 워크스테이션, 전화기, 핸드헬드 PC, 개인 정보 단말기, 씬 클라이언트, 팻 클라이언트, 인터넷 브라우저 또는 기타 디바이스를 포함하는 통신 디바이스 또는 컴퓨터 디바이스를 포함하나 이에 한정되지는 않는다.

[0021] 또한 클라이언트 디바이스(110)는 모바일 디바이스일 수 있다. 예를 들어 모바일 디바이스는 Apple®의 아이폰, 아이팟, 아이패드 또는 Apple의 iOS® 운영 체제를 실행하는 다른 모든 모바일 디바이스, Microsoft의 Windows® 모바일 운영 체제를 실행하는 모든 디바이스, Google의 Android® 운영 체제를 실행하는 모든 디바이스, 및/또는 다른 스마트폰, 태블릿 또는 유사한 웨어러블 모바일 디바이스일 수 있다.

[0022] 클라이언트 디바이스(110) 디바이스는 프로세서 및 메모리를 포함할 수 있으며, 처리 회로는 본 명세서 내에 설명된 기능을 수행하는 데 필요한 프로세서, 메모리, 오류 및 패리티/CRC 검사기, 데이터 인코더, 충돌 방지 알고리즘, 컨트롤러, 명령 디코더, 보안 기본 요소 및 변조 방지 하드웨어를 포함하는 추가적인 컴포넌트를 포함할 수 있음을 이해해야 한다.

[0023] 클라이언트 디바이스(110)는 디스플레이 및 입력 디바이스를 더욱 포함할 수 있다. 디스플레이는 컴퓨터 모니터, 평면 패널 디스플레이 및 액정 디스플레이, 발광 다이오드 디스플레이, 플라즈마 패널 및 음극선 관 디스플레이를 포함하는 모바일 디바이스 화면과 같은 시각 정보를 제공하기 위한 임의의 유형의 디바이스일 수 있다.

[0024] 입력 디바이스에는 터치 스크린, 키보드, 마우스, 커서 제어 디바이스, 터치 스크린, 마이크, 디지털 카메라, 비디오 레코더 또는 캠코더와 같이 사용자 디바이스에서 사용 가능하고 지원하는 정보를 사용자 디바이스에 입력하기 위한 모든 디바이스가 포함될 수 있다.

[0025] 이러한 디바이스는 정보를 입력하고 본 명세서 내에 설명된 소프트웨어 및 기타 디바이스와 상호 작용하는 데 사용될 수 있다.

[0026] 일부 실시예에서 시스템(100)의 클라이언트 디바이스(110)는 예를 들어 시스템(100)의 하나 이상의 컴포넌트와의 네트워크 통신을 가능하게 하고 데이터를 전송 및/또는 수신하는 소프트웨어 응용프로그램과 같은 하나 이상의 응용프로그램을 실행할 수 있다.

[0027] 클라이언트 디바이스(110)는 하나 이상의 네트워크(115)를 통해 하나 이상의 서버(120)와 통신할 수 있고, 각각의 프론트-엔드에서 백-엔드 쌍으로서 서버(120)와 작동할 수 있다. 클라이언트 디바이스(110)는 예를 들어 클라이언트 디바이스(110)에서 실행되는 모바일 디바이스 응용프로그램으로부터 하나 이상의 요청을 서버(120)로 전송할 수 있다. 하나 이상의 요청은 서버(120)로부터 데이터를 조회하는 것과 연관될 수 있다.

[0028] 서버(120)는 클라이언트 디바이스(110)로부터 하나 이상의 요청을 수신할 수 있다. 클라이언트 디바이스(110)로부터의 하나 이상의 요청에 기반하여 서버(120)는 하나 이상의 데이터베이스로부터 요청된 데이터를 조회하도록 형상화될 수 있다(도시되지 않음). 하나 이상의 데이터베이스로부터 요청된 데이터의 수신에 기반하여 서버(120)는 수신된 데이터를 클라이언트 디바이스(110)로 전송하도록 형상화될 수 있으며 수신된 데이터는 하나 이상의 요청에 응답한다.

[0029] 시스템(100)은 하나 이상의 네트워크(115)를 포함할 수 있다. 일부 실시예에서 네트워크(115)는 무선 네트워크, 유선 네트워크 또는 무선 네트워크와 유선 네트워크의 임의의 조합 중 하나 이상일 수 있으며 클라이언트 디바이스(110)를 서버에 연결하도록 형상화될 수 있다. 예를 들어 네트워크(115)는 광섬유 네트워크, 수동 광 네트워크, 케이블 네트워크, 인터넷 네트워크, 위성 네트워크, 무선 근거리 네트워크(LAN), 이동 통신을 위한 글로벌 시스템, 개인 통신 서비스, 개인 영역 네트워크, 무선 응용프로그램 프로토콜, 멀티미디어 메시지 서비스, 향상된 메시지 서비스, 단문 메시지 서비스, 시간 분할 다중화 기반 시스템, 코드 분할 다중 액세스 기반 시스템, D-AMPS, Wi-Fi, 고정 무선 데이터, IEEE 802.11b, 802.15.1, 802.11n 및 802.11g, 블루투스, NFC, 무선 주파수 식별(RFID), Wi-Fi 등 중 하나 이상을 포함할 수 있다.

[0030] 또한 네트워크(115)는 전화선, 광섬유, IEEE Ethernet 902.3, 광역 네트워크, 무선 개인 영역 네트워크, LAN, 또는 인터넷과 같은 글로벌 네트워크를 제한없이 포함할 수 있다. 또한 네트워크(115)는 인터넷 네트워크, 무선 통신 네트워크, 셀룰러 네트워크 등 또는 이들의 임의의 조합을 지원할 수 있다. 네트워크(115)는 하나의 네트워크, 독립형 네트워크로서 또는 서로 협력하여 작동하는 상기에서 언급된 임의의 수의 예시적인 유형의 네트워

크를 더욱 포함할 수 있다.

[0031] 네트워크(115)는 통신 가능하게 결합되는 하나 이상의 네트워크 엘레멘트의 하나 이상의 프로토콜을 이용할 수 있다. 네트워크(115)는 네트워크 디바이스의 하나 이상의 프로토콜로 또는 다른 프로토콜로부터 네트워크 디바이스의 하나 이상의 프로토콜로 변환될 수 있다. 네트워크(115)는 단일 네트워크로 도시되어 있으나 하나 이상의 실시예에 따르면 네트워크(115)는 예를 들어 인터넷, 서비스 공급자의 네트워크, 케이블 텔레비전 네트워크, 신용카드 연결 네트워크 및 홈 네트워크와 같은 회사 네트워크와 같은 다수의 상호 연결된 네트워크를 포함할 수 있음을 이해해야 한다.

[0032] 시스템(100)은 하나 이상의 서버(120)를 포함할 수 있다. 일부 실시예에서 서버(120)는 메모리에 결합되는 하나 이상의 프로세서를 포함할 수 있다. 서버(120)는 중앙 시스템, 서버 또는 플랫폼으로 구성되어 다수의 워크플로우 액션을 실행하기 위해 서로 상이한 시간에 다양한 데이터를 제어하고 호출할 수 있다. 서버(120)는 하나 이상의 데이터베이스에 연결하도록 형상화될 수 있다. 서버(120)는 적어도 하나의 클라이언트 디바이스(110)에 연결될 수 있다.

[0033] 도 1b는 본 명세서의 하나 이상의 실시형태에 따라 인증된 접근을 제공하기 위한 예시적인 순서를 나타내는 타이밍 다이어그램이다. 시스템(100)은 응용프로그램(122) 및 프로세서(124)를 포함할 수 있는 비접촉식 카드(105) 및 클라이언트 디바이스(110)를 포함할 수 있다. 도 1b는 도 1a 내에 예시된 유사한 컴포넌트를 참조할 수 있다.

[0034] 단계 102에서 응용프로그램(122)은 비접촉식 카드(105)와 통신한다(예를 들어 비접촉식 카드(105)에 근접한 후). 응용프로그램(122)과 비접촉식 카드(105) 사이의 통신은 비접촉식 카드(105)가 응용프로그램(122)과 비접촉식 카드(105) 사이의 NFC 데이터 전송을 가능하게 하기 위해 클라이언트 디바이스(110)의 카드 판독기(나타내지 않음)에 충분히 근접하는 것을 포함할 수 있다.

[0035] 단계 104에서 클라이언트 디바이스(110)와 비접촉식 카드(105) 사이에 통신이 설정된 후, 비접촉식 카드(105)는 메시지 인증 코드(MAC) 암호를 생성한다. 일부 실시예에서 이것은 비접촉식 카드(105)가 응용프로그램(122)에 의해 판독될 때 발생할 수 있다. 특히 NFC 데이터 교환 형식에 따라 생성될 수 있는 근거리 데이터 교환(NDEF) 태그의 NFC 판독과 같은 판독 시 발생할 수 있다. 예를 들어 응용프로그램(122)과 같은 판독기는 NDEF 생성 애플릿의 애플릿 ID와 함께 애플릿 선택 메시지와 같은 메시지를 전송할 수 있다.

[0036] 선택이 확인되면 일련의 파일 선택 메시지와 판독 파일 메시지가 전송될 수 있다. 예를 들어 시퀀스에는 "Select Capabilities file", "Read Capabilities file" 및 "Select NDEF file"이 포함될 수 있다. 이 시점에서 비접촉식 카드(105)에 의해 유지되는 카운터 값이 업데이트되거나 증가될 수 있으며, 그 뒤에 "Read NDEF file"이 이어질 수 있다. 이 시점에서 헤더와 공유 비밀을 포함할 수 있는 메시지가 생성될 수 있다. 세션 키가 그 후에 생성될 수 있다.

[0037] MAC 암호는 헤더와 공유 비밀을 포함할 수 있는 메시지로부터 생성될 수 있다. MAC 암호는 하나 이상의 임의 데이터 블록과 연결될 수 있으며 MAC 암호 및 난수(RND)는 세션 키로 암호화될 수 있다. 그 후 암호문과 헤더가 연결되며 ASCII 16 진수로 암호화 되고 NDEF 메시지 형식으로 반환될 수 있다("Read NDEF file" 메시지에 대한 응답으로).

[0038] 일부 실시예에서 MAC 암호는 NDEF 태그로서 전송될 수 있으며 다른 실시예에서 MAC 암호는 통합 자원 식별자와 함께 (예를 들어 포맷된 문자열로서) 포함될 수 있다.

[0039] 일부 실시예에서 응용프로그램(122)은 비접촉식 카드(105)로 요청을 전송하도록 형상화될 수 있으며 요청은 MAC 암호를 생성하기 위한 명령어를 포함한다.

[0040] 단계 106에서 비접촉식 카드(105)는 MAC 암호를 응용프로그램(122)에 전송한다. 일부 실시예에서 MAC 암호의 전송은 NFC를 통해 발생하지만 본 발명은 이에 제한되지 않는다. 다른 실시예에서 이러한 통신은 블루투스, Wi-Fi 또는 기타 무선 데이터 통신 수단을 통해 발생할 수 있다.

[0041] 단계 108에서 응용프로그램(122)은 MAC 암호를 프로세서(124)에 전달한다.

[0042] 단계 112에서 프로세서(124)는 응용프로그램(122)으로부터의 명령에 따라 MAC 암호를 검증한다. 예를 들어 MAC 암호는 다음과 같이 검증될 수 있다.

[0043] 일부 실시예에서 MAC 암호를 검증하는 것은 클라이언트 디바이스(110)와 데이터 통신하는 서버(120)와 같은 클

라이언트 디바이스(110) 이외의 디바이스에 의해 수행될 수 있다(도 1a에 나타난 바와 같음). 예를 들어 프로세서(124)는 MAC 암호를 검증할 수 있는 서버(120) 로의 전송을 위해 MAC 암호를 출력할 수 있다.

[0044] 일부 실시예에서 MAC 암호는 검증을 위한 디지털 서명으로 기능할 수 있다. 공개 키 비대칭 알고리즘, 예를 들면 디지털 서명 알고리즘 및 RSA 알고리즘 또는 영 지식(zero knowledge) 프로토콜과 같은 다른 디지털 서명 알고리즘이 이러한 검증을 수행하는 데 사용될 수 있다.

[0045] 도 2는 예시적인 실시형태에 따른 데이터 전송 시스템을 도시한다. 시스템(200)은 예를 들어 하나 이상의 서버(220)와 함께 네트워크(215)를 통해 통신 내에서 전송 또는 송신 디바이스(205), 수신 또는 수취 디바이스(210)를 포함할 수 있다. 전송 또는 송신 디바이스(205)는 도 1a를 참조하여 상기에서 논의된 클라이언트 디바이스(110)와 동일 또는 유사할 수 있다. 수신 또는 수취 디바이스(210)는 도 1a를 참조하여 상기에서 논의된 클라이언트 디바이스(110)와 동일 또는 유사할 수 있다.

[0046] 네트워크(215)는 도 1a를 참조하여 상기에서 논의된 네트워크(115)와 유사할 수 있다. 서버(220)는 도 1a를 참조하여 상기에서 논의된 서버(120)와 유사할 수 있다. 도 2는 시스템(200) 컴포넌트의 단일 인스턴스를 나타내었으나 시스템(200)은 도시된 컴포넌트를 임의의 수로 포함할 수 있다.

[0047] 암호화 알고리즘, 해시-기반 메시지 인증 코드(HMAC) 알고리즘 및 암호-기반 메시지 인증 코드(CMAC) 알고리즘과 같은 대칭 암호화 알고리즘을 사용하는 경우, 대칭 알고리즘과 키를 사용하여 보호되는 데이터를 원래 처리하는 당사자와 동일한 암호화 알고리즘 및 동일한 키를 사용하여 데이터를 수신하고 처리하는 당사자 사이에서 키가 비밀로 유지되는 것이 중요하다.

[0048] 동일한 키를 너무 많이 사용하지 않는 것도 중요하다. 키가 너무 자주 사용되거나 재사용되면 해당 키가 손상될 수 있다. 키가 사용될 때마다 동일한 키를 사용하는 암호화 알고리즘에 의해 처리된 추가 데이터 샘플을 공격자에게 제공한다. 공격자가 동일한 키로 처리된 데이터를 많이 지닐수록 공격자가 키의 값을 발견할 가능성이 증가한다. 자주 사용되는 키는 다양한 공격 내에 포함될 수 있다.

[0049] 또한 대칭 암호화 알고리즘이 실행될 때마다 대칭 암호화 작업 중에 사용된 키에 대한 정보(예: 사이드-채널 데이터)를 공개할 수 있다. 사이드-채널 데이터에는 키를 사용하는 동안 암호화 알고리즘이 실행될 때 발생하는 미세한 전력 변동이 포함될 수 있다. 공격자가 키를 복구할 수 있게 하는 키에 대한 충분한 정보를 공개하기 위해 사이드-채널 데이터를 충분히 측정할 수 있다. 데이터 교환에 동일한 키를 사용하면 동일한 키로 처리된 데이터가 반복적으로 표시된다.

[0050] 그러나 특정 키가 사용되는 횟수를 제한함으로써 공격자가 수집할 수 있는 사이드-채널 데이터의 양이 제한되어 본 유형의 공격과 다른 유형의 공격에 대한 노출을 감소시킨다. 본 명세서에 추가로 설명된 바와 같이 암호화 정보 교환에 관련된 당사자(예: 발신자 및 수신자)는 카운터 값과 결합하여 초기 공유 마스터 대칭 키로부터 독립적으로 키를 생성할 수 있으며, 따라서 사용 중인 공유 대칭 키를 주기적으로 교체하여 당사자를 동기화 상태로 유지하기 위해 모든 형태의 키 교환을 준비해야 한다. 발신자와 수신자가 사용하는 공유 비밀 대칭 키를 주기적으로 교체함으로써 상기에서 설명한 공격이 불가능해진다.

[0051] 다시 도 2를 참조하면 시스템(200)은 키 다양화를 구현하도록 형상화될 수 있다. 예를 들어 발신자와 수신자는 각각의 디바이스(205 및 210)를 통해 데이터(예를 들어 원래의 민감한 데이터) 교환을 원할 수 있다. 상기에서 설명한 바와 같이 송신 디바이스(205) 및 수신 디바이스(210)의 단일 인스턴스가 포함될 수 있으나 각 당사자가 동일한 공유 비밀 대칭 키를 공유하는 한, 하나 이상의 송신 디바이스(205) 및 하나 이상의 수신 디바이스(210)가 관련될 수 있다.

[0052] 일부 실시예에서 송신 디바이스(205) 및 수신 디바이스(210)는 동일한 마스터 대칭 키로 프로비저닝 될 수 있다. 또한 동일한 비밀 대칭 키를 보유하는 임의의 당사자 또는 디바이스가 송신 디바이스(205)의 기능을 수행할 수 있고 유사하게 동일한 비밀 대칭 키를 보유하는 임의의 당사자가 수신 디바이스(210)의 기능을 수행할 수 있다는 것으로 이해된다. 대칭 키는 보안 데이터 교환에 관여하는 송신 디바이스(205) 및 수신 디바이스(210) 이외의 모든 당사자로부터 비밀로 유지되는 공유 비밀 대칭 키를 포함할 수 있다.

[0053] 또한 송신 디바이스(205)와 수신 디바이스(210) 모두 동일한 마스터 대칭 키가 제공되는 것으로 이해될 수 있으며, 또한 송신 디바이스(205)와 수신 디바이스(210) 사이에서 교환되는 데이터의 일부는 카운터 값이라고 언급되는 적어도 일부의 데이터를 포함한다. 카운터 값은 송신 디바이스(205)와 수신 디바이스(210) 사이에서 데이터가 교환될 때마다 변경되는 넘버를 포함할 수 있다.

[0054] 시스템(200)은 하나 이상의 네트워크(215)를 포함할 수 있다. 일부 실시에서 네트워크(215)는 무선 네트워크, 유선 네트워크 또는 무선 네트워크와 유선 네트워크의 임의의 조합 중 하나 이상일 수 있으며, 하나 이상의 송신 디바이스(205) 및 하나 이상의 수신 디바이스(210)를 서버(220)로 연결하도록 형상화될 수 있다.

[0055] 예를 들어 네트워크(215)는 광섬유 네트워크, 수동 광 네트워크, 케이블 네트워크, 인터넷 네트워크, 위성 네트워크, 무선 LAN, 글로벌 이동 통신 시스템, 개인 통신 서비스, 개인 영역 네트워크, 무선 응용프로그램 프로토콜, 멀티미디어 메시지 서비스, 향상된 메시지 서비스, 단문 메시지 서비스, 시분할 다중화 기반 시스템, 코드 분할 다중 액세스 기반 시스템, D-AMPS, Wi-Fi, 고정 무선 데이터, IEEE 802.11b, 802.15.1, 802.11n 및 802.11g, 블루투스, NFC, RFID, Wi-Fi 등의 네트워크 중 하나 이상을 포함할 수 있다.

[0056] 또한 네트워크(215)는 제한없이 전화선, 광섬유, IEEE Ethernet 902.3, 광역 네트워크, 무선 개인 영역 네트워크, LAN 또는 인터넷과 같은 글로벌 네트워크를 포함할 수 있다. 또한 네트워크(215)는 인터넷 네트워크, 무선 통신 네트워크, 셀룰러 네트워크 등 또는 이들의 임의의 조합을 지원할 수 있다. 네트워크(215)는 하나의 네트워크, 또는 독립형 네트워크로서 또는 서로 협력하여 작동하는 상기에서 언급된 임의의 수의 예시적인 유형의 네트워크를 더욱 포함할 수 있다. 네트워크(215)는 통신 가능하게 결합되는 하나 이상의 네트워크 엘레멘트의 하나 이상의 프로토콜을 이용할 수 있다.

[0057] 네트워크(215)는 네트워크 디바이스의 하나 이상의 프로토콜로 또는 다른 프로토콜로부터 네트워크 디바이스의 하나 이상의 프로토콜로 변환할 수 있다. 네트워크(215)는 단일 네트워크로 도시되었으나 하나 이상의 실시예에 따르면 네트워크(215)는 예를 들어 인터넷, 서비스 공급자의 네트워크, 케이블 텔레비전 네트워크, 신용카드 연결 네트워크 및 홈 네트워크와 같은 기업 네트워크와 같은 다수의 상호 연결된 네트워크를 포함할 수 있음을 이해해야 한다.

[0058] 일부 실시예에서 하나 이상의 송신 디바이스(205) 및 하나 이상의 수신 디바이스(210)는 네트워크(215)를 통과하지 않고 서로 간에 데이터를 통신하고 송신 및 수신하도록 형상화될 수 있다. 예를 들어 하나 이상의 송신 디바이스(205)와 하나 이상의 수신 디바이스(210)는 NFC, 블루투스, RFID, Wi-Fi 등 중 적어도 하나를 통해 발생할 수 있다.

[0059] 블록 225에서 송신 디바이스(205)가 대칭 암호화 작동으로 민감한 데이터를 처리할 준비할 때 발신자는 카운터를 업데이트할 수 있다. 또한 발신 디바이스(205)는 대칭 암호화 알고리즘, HMAC 알고리즘 및 CMAC 알고리즘 중 적어도 하나를 포함하는 적절한 대칭 암호화 알고리즘을 선택할 수 있다.

[0060] 일부 실시예에서 다양화 값을 처리하기 위해 사용되는 대칭 알고리즘은 원하는 길이 다양화 대칭 키를 생성하는데 필요에 따라 사용되는 임의의 대칭 암호화 알고리즘을 포함할 수 있다. 대칭 알고리즘의 비-제한적인 예는 3DES 또는 AES128과 같은 대칭 암호화 알고리즘; HMAC-SHA-256과 같은 대칭 HMAC 알고리즘; 및 AES-CMAC와 같은 대칭 CMAC 알고리즘;을 포함한다.

[0061] 선택된 대칭 알고리즘의 출력이 충분히 긴 키를 생성하지 않는 경우, 다른 입력 데이터와 동일한 마스터 키를 사용하여 대칭 알고리즘의 여러 반복을 처리하는 것과 같은 기술은 충분한 길이의 키를 생성하기 위한 필요시 결합될 수 있는 여러 출력을 생성할 수 있다.

[0062] 블록 230에서 발신 디바이스(205)는 선택된 암호화 알고리즘을 취할 수 있으며 마스터 대칭 키를 사용하여 카운터 값을 처리할 수 있다. 예를 들어 발신자는 대칭 암호화 알고리즘을 선택하고 발신 디바이스(205)와 수신 디바이스(210) 사이의 모든 대화를 업데이트하는 카운터를 사용할 수 있다. 그러면 송신 디바이스(205)는 다양화 대칭 키를 생성하는 마스터 대칭 키를 사용하여 선택된 대칭 암호화 알고리즘으로 카운터 값을 암호화할 수 있다.

[0063] 일부 실시예에서 카운터 값은 암호화되지 않을 수 있다. 이러한 실시예에서 카운터 값은 암호화없이 블록 230에서 송신 디바이스(205)와 수신 디바이스(210) 사이에서 전송될 수 있다.

[0064] 블록 235에서 수신 디바이스(210)로 결과를 전송하기 전에 다양화 대칭 키가 민감한 데이터를 처리하는 데 사용될 수 있다. 예를 들어 송신 디바이스(205)는 보호된 암호화 데이터를 포함하는 출력과 다양화 대칭 키를 사용하는 대칭 암호화 알고리즘을 사용하여 민감한 데이터를 암호화할 수 있다. 그 후 송신 디바이스(205)는 카운터 값과 함께 보호된 암호화 데이터를 처리를 위해 수신 디바이스(210)에 송신할 수 있다.

[0065] 블록 240에서 수신 디바이스(210)는 카운터 값을 먼저 취한 다음, 암호화에 대한 입력으로 카운터 값을 사용하고 암호화를 위한 키로서 마스터 대칭 키를 사용하여 동일한 대칭 암호화를 수행한다. 암호화의 출력은 발신자

가 생성한 동일한 다양화 대칭 키 값일 수 있다.

[0066] 블록 245에서 수신 디바이스(210)는 보호된 암호화 데이터를 취하고 다양화 대칭 키와 함께 대칭 복호화 알고리즘을 사용하여 보호된 암호화 데이터를 복호화할 수 있다.

[0067] 블록 250에서 보호된 암호화 데이터를 복호화한 결과, 원래의 민감한 데이터가 공개될 수 있다.

[0068] 다음에 민감한 데이터가 각각의 송신 디바이스(205) 및 수신 디바이스(210)를 통해 발신자로부터 수신자에게 발신될 필요가 있을 때, 서로 다른 다양화 대칭 키를 생성하는 서로 다른 카운터 값이 선택될 수 있다. 마스터 대칭 키 및 동일한 대칭 암호화 알고리즘을 사용하여 카운터 값을 처리함으로써, 송신 디바이스(205)와 수신 디바이스(210) 모두 동일한 다양화 대칭 키를 독립적으로 생성할 수 있다. 마스터 대칭 키가 아닌 이러한 다양화 대칭 키는 민감한 데이터를 보호하는 데 사용된다.

[0069] 상기한 바와 같이 송신 디바이스(205) 및 수신 디바이스(210)는 공유된 마스터 대칭 키를 초기에 각각 소유한다. 공유 마스터 대칭 키는 원래의 중요한 데이터를 암호화하는 데 사용되지 않는다. 다양화 대칭 키는 송신 디바이스(205)와 수신 디바이스(210) 모두에 의해 독립적으로 생성되기 때문에 두 당사자 간에는 절대로 전송되지 않는다.

[0070] 따라서 공격자는 다양화 대칭 키를 가로챌 수 없으며 공격자는 마스터 대칭 키로 처리된 데이터를 볼 수 없다. 중요한 데이터가 아닌 마스터 대칭 키로 카운터 값 만이 처리된다.

[0071] 결과적으로 마스터 대칭 키에 대한 감소된 사이드-채널 데이터가 표시된다. 또한 송신 디바이스(205) 및 수신 디바이스(210)의 작동은 새로운 다양화 값, 따라서 새로운 다양화 대칭 키를 얼마나 자주 생성하는지에 대한 대칭 요건에 의해 관리될 수 있다. 하나의 실시형태에서 송신 디바이스(205)와 수신 디바이스(210) 사이의 모든 교환에 대해 새로운 다양화 값 및 따라서 새로운 다양화 대칭 키가 생성될 수 있다. 일부 실시예에서 키 다양화 값은 카운터 값을 포함할 수 있다.

[0072] 주요 다양화 값의 또 다른 비-제한적인 실시예는 새로운 다양화 키가 필요할 때마다 생성되는 랜덤 논스, 송신 디바이스(205)로부터 수신 디바이스(210)로 전송되는 랜덤 논스; 송신 디바이스(205) 및 수신 디바이스(210)로부터 전송된 카운터 값의 전체 값; 송신 디바이스(205) 및 수신 디바이스(210)로부터 전송된 카운터 값의 일부; 송신 디바이스(205) 및 수신 디바이스(210)에 의해 독립적으로 유지되지만 두 디바이스 간에는 전송되지 않는 카운터; 송신 디바이스(205)와 수신 디바이스(210) 사이에서 교환되는 일회성 암호; 및 민감한 데이터의 암호화 해시;

[0073] 를 포함한다.

[0074] 일부 실시예에서 키 다양화 값의 하나 이상의 부분은 다수의 다양화 키를 생성하기 위해 당사자에 의해 사용될 수 있다. 예를 들어 카운터를 키 다양화 값으로 사용할 수 있다. 또한 상기한 바와 같은 예시적인 키 다양화 값 중 하나 이상의 조합이 사용될 수 있다.

[0075] 다른 실시예에서 카운터의 일부는 키 다양화 값으로 사용될 수 있다. 다수의 마스터 키 값이 당사자간에 공유되는 경우, 본 명세서에 설명된 시스템 및 프로세스에 의해 다수의 다양화 키 값이 획득될 수 있다.

[0076] 새로운 다양화 값, 따라서 새로운 다양화 대칭 키가 필요한 만큼 자주 생성될 수 있다. 가장 안전한 경우에 송신 디바이스(205)와 수신 디바이스(210) 사이의 민감한 데이터의 각각의 교환에 대해 새로운 다양화 값이 생성될 수 있다. 실제로 이것은 일회용 세션 키와 같은 일회성 사용 키를 생성할 수 있다.

[0077] 도 3은 비접촉식 카드를 사용하는 시스템(300)을 도시한다. 시스템(300)은 비접촉식 카드(305), 하나 이상의 클라이언트 디바이스(310), 네트워크(315), 서버(320, 325), 하나 이상의 하드웨어 보안 모듈(330) 및 데이터베이스(335)를 포함할 수 있다. 도 3은 컴포넌트의 단일 인스턴스를 예시하였으나 시스템(300)은 임의의 수의 컴포넌트를 포함한다.

[0078] 시스템(300)은 하나 이상의 비접촉식 카드(305)를 포함할 수 있으며 이는 도 5a 내지 도 5b와 관련하여 다음과 같이 설명된다. 일부 실시예에서 비접촉식 카드(305)는 클라이언트 디바이스(310)와 무선 통신, 예를 들어 NFC 통신할 수 있다. 예를 들어 비접촉식 카드(305)는 NFC 또는 다른 단거리 프로토콜을 통해 통신하도록 형상화 된 무선 주파수 식별 칩과 같은 하나 이상의 칩을 포함할 수 있다.

[0079] 또 다른 실시형태에서 비접촉식 카드(305)는 블루투스, 위성, Wi-Fi, 유선 통신 및/또는 무선 및 유선 연결의 임의의 조합을 포함하지만 이에 제한되지 않는 다른 수단을 통해 클라이언트 디바이스(310)와 통신할 수 있다.

일부 실시형태에 따르면 비접촉식 카드(305)는 비접촉식 카드(305)가 카드 판독기(313)의 범위 내에 있을 때 NFC를 통해 클라이언트 디바이스(310)의 카드 판독기(313)와 통신하도록 형상화될 수 있다. 다른 실시예에서 비접촉식 카드(305)와의 통신은 예를 들면 범용 직렬 버스 인터페이스 또는 카드 스와이프 인터페이스와 같은 물리적 인터페이스를 통해 수행될 수 있다.

[0080] 시스템(300)은 네트워크 가능 컴퓨터일 수 있는 클라이언트 디바이스(310)를 포함할 수 있다. 본 명세서에서 언급되는 바와 같이 네트워크 가능 컴퓨터는 예를 들어 컴퓨터 디바이스 또는 예를 들어 서버, 네트워크 기기, 개인용 컴퓨터, 워크 스테이션, 모바일 디바이스, 전화, 핸드헬드 PC, 개인용 디지털 비서, 씬 클라이언트, 팻 클라이언트, 인터넷 브라우저 또는 다른 디바이스를 포함하는 통신 디바이스를 포함할 수 있으나 이에 제한되지는 않는다.

[0081] 또한 하나 이상의 클라이언트 디바이스(310)는 모바일 디바이스 일 수 있으며; 예를 들어 모바일 디바이스에는 Apple®의 iPhone, iPod, iPad 또는 Apple의 iOS® 운영 체제를 실행하는 다른 모든 모바일 디바이스, Microsoft의 Windows® Mobile 운영 체제를 실행하는 모든 디바이스, Google의 Android® 운영 체제를 실행하는 모든 디바이스 또는 다른 스마트폰 또는 유사한 웨어러블 모바일 디바이스가 포함될 수 있다. 일부 실시예에서 클라이언트 디바이스(310)는 도 1a 또는 도 1b를 참조하여 설명된 클라이언트 디바이스(110)와 동일하거나 유사할 수 있다.

[0082] 클라이언트 디바이스(310)는 하나 이상의 네트워크(315)를 통해 하나 이상의 서버(320 및 325)와 통신할 수 있다. 클라이언트 디바이스(310)는 예를 들어 클라이언트 디바이스(310)에서 실행되는 응용프로그램(311)으로부터 하나 이상의 요청을 하나 이상의 서버(320 및 325)로 전송할 수 있다. 하나 이상의 요청은 하나 이상의 서버(320, 325)로부터 데이터를 검색하는 것과 연관될 수 있다. 서버(320 및 325)는 클라이언트 디바이스(310)로부터 하나 이상의 요청을 수신할 수 있다.

[0083] 클라이언트 디바이스(310)로부터의 하나 이상의 요청에 기반하여 하나 이상의 서버(320 및 325)가 하나 이상의 데이터베이스(335)로부터 요청된 데이터를 검색하도록 형상화될 수 있다. 하나 이상의 데이터베이스(335)로부터 요청된 데이터의 수신에 기반하여 하나 이상의 하나 이상의 서버(320 및 325)는 수신된 데이터를 클라이언트 디바이스(310)로 전송하도록 형상화될 수 있으며, 수신된 데이터는 하나 이상의 요청에 응답한다.

[0084] 시스템(300)은 하나 이상의 하드웨어 보안 모듈(HSM)(330)을 포함할 수 있다. 예를 들어 하나 이상의 HSM(330)은 본 명세서에 개시된 바와 같은 하나 이상의 암호화 작동을 수행하도록 형상화될 수 있다. 일부 실시예에서 하나 이상의 HSM(330)은 하나 이상의 암호화 작동을 수행하도록 형상화되는 특수 목적 보안 디바이스로서 형상화될 수 있다.

[0085] HSM(330)은 키가 HSM(330) 외부에서 결코 드러나지 않고 대신 HSM(330) 내에서 유지되도록 형상화될 수 있다. 예를 들어 하나 이상의 HSM(330)은 키 유도, 복호화 및 MAC 작동 중 적어도 하나를 수행하도록 형상화될 수 있다. 하나 이상의 HSM(330)은 서버(320 및 325) 내에 포함되거나 서버와 데이터 통신할 수 있다.

[0086] 시스템(300)은 하나 이상의 네트워크(315)를 포함할 수 있다. 일부 실시예에서 네트워크(315)는 무선 네트워크, 유선 네트워크 또는 무선 네트워크와 유선 네트워크의 임의의 조합 중 하나 이상일 수 있으며 클라이언트 디바이스(315)를 서버(320 및 325)에 연결하도록 형상화될 수 있다.

[0087] 예를 들어 네트워크(315)는 광섬유 네트워크, 수동 광 네트워크, 케이블 네트워크, 셀룰러 네트워크, 인터넷 네트워크, 위성 네트워크, 무선 LAN, 글로벌 이동 통신 시스템, 개인 통신 서비스, 개인 영역 네트워크, 무선 응용 프로토콜, 멀티미디어 메시지 서비스, 향상된 메시지 서비스, 단문 메시지 서비스, 시분할 다중화 기반 시스템, 코드 분할 다중 액세스 기반 시스템, D-AMPS, Wi-Fi, 고정 무선 데이터, IEEE 802.11b, 802.15.1, 802.11n 및 802.11g, 블루투스, NFC, RFID, Wi-Fi 및/또는 이들 모든 네트워크 조합 중 하나 이상을 포함할 수 있다. 비제한적인 실시예로서 비접촉식 카드(305) 및 클라이언트 디바이스(310)로부터의 통신은 NFC 통신, 클라이언트 디바이스(310)와 캐리어 사이의 셀룰러 네트워크, 캐리어와 백-엔드 사이의 인터넷을 포함할 수 있다.

[0088] 또한 네트워크(315)는 전화선, 광섬유, IEEE Ethernet 902.3, 광역 네트워크, 무선 개인 영역 네트워크, 근거리 네트워크, 또는 인터넷과 같은 글로벌 네트워크를 특별한 제한없이 포함할 수 있다. 또한 네트워크(315)는 인터넷 네트워크, 무선 통신 네트워크, 셀룰러 네트워크 등 또는 이들의 임의의 조합을 지원할 수 있다.

[0089] 네트워크(315)는 하나의 네트워크, 독립형 네트워크로서 또는 서로 협력하여 작동하는 상기에서 언급된 임의의 수의 예시적인 유형의 네트워크를 더욱 포함할 수 있다. 네트워크(315)는 통신 가능하게 결합되는 하나 이상의 네트워크 엘레멘트의 하나 이상의 프로토콜을 이용할 수 있다. 네트워크(315)는 네트워크 디바이스의 하나 이상

의 프로토콜로 또는 다른 프로토콜로부터 네트워크 디바이스의 하나 이상의 프로토콜로 변환할 수 있다.

[0090] 네트워크(315)가 단일 네트워크로 도시되어 있으나 하나 이상의 실시예에 따르면 네트워크(315)는 예를 들어 인터넷, 서비스 공급자의 네트워크, 케이블 텔레비전 네트워크, 신용카드 연결 네트워크 및 홈 네트워크와 같은 회사 네트워크와 같은 다수의 상호 연결된 네트워크를 포함할 수 있음을 이해해야 한다.

[0091] 본 명세서에 따른 다양한 실시예에서 시스템(300)의 클라이언트 디바이스(310)는 하나 이상의 응용프로그램(311)을 실행할 수 있으며 하나 이상의 프로세서(312) 및 하나 이상의 카드 판독기(313)를 포함할 수 있다. 예를 들어 소프트웨어 응용프로그램과 같은 하나 이상의 응용프로그램(311)은 예를 들어 시스템(300)의 하나 이상의 컴포넌트와의 네트워크 통신을 가능하게 하고 데이터를 전송 및/또는 수신하도록 형상화될 수 있다. 클라이언트 디바이스(310) 컴포넌트의 단일 인스턴스 만이 도 3에 도시되어 있으나 임의의 수의 디바이스(310)가 사용될 수 있는 것으로 이해된다.

[0092] 카드 판독기(313)는 비접촉식 카드(305)로부터 판독 및/또는 통신하도록 형상화될 수 있다. 하나 이상의 응용프로그램(311)과 관련하여, 카드 판독기(313)는 비접촉식 카드(305)와 통신할 수 있다.

[0093] 임의의 클라이언트 디바이스(310)의 응용프로그램(311)은 단거리 무선 통신(예를 들어 NFC)을 사용하여 비접촉식 카드(305)와 통신할 수 있다. 응용프로그램(311)은 비접촉식 카드(305)와 통신하도록 형상화된 클라이언트 디바이스(310)의 카드 판독기(313)로 인터페이스 하도록 형상화될 수 있다. 주목해야하는 바와 같이 당업자는 20cm 미만의 거리가 NFC 범위와 일치한다는 것을 이해할 것이다.

[0094] 일부 실시형태에서 응용프로그램(311)은 비접촉식 카드(305)와 연관된 판독기(예를 들어 카드 판독기(313))를 통해 통신한다.

[0095] 일부 실시형태에서 카드 활성화는 사용자 인증없이 발생할 수 있다. 예를 들어 비접촉식 카드(305)는 NFC를 통해 클라이언트 디바이스(310)의 카드 판독기(313)를 통해 응용프로그램(311)과 통신할 수 있다. 통신(예를 들어 클라이언트 디바이스(310)의 카드 판독기(313)에 근접한 카드의 탭)은 응용프로그램(311)이 카드와 관련된 데이터를 읽고 활성화를 수행할 수 있게 한다.

[0096] 일부 경우에 탭은 응용프로그램(311)을 활성화하거나 시작한 다음 후속 사용을 위한 카드 활성화를 위해 계정 서버(325)와 하나 이상의 작동 또는 통신을 개시할 수 있다. 일부 경우에 응용프로그램(311)이 클라이언트 디바이스(310)에 설치되지 않은 경우, 카드 판독기(313)에 대한 카드의 탭은 응용프로그램(311)의 다운로드(예를 들어 응용프로그램 다운로드 페이지로의 탐색)를 개시할 수 있다.

[0097] 설치 후에 카드의 탭은 응용프로그램(311)을 활성화하거나 시작한 다음, 카드의 활성화를 개시(예를 들어 응용프로그램 또는 기타 백-엔드 통신을 통해)할 수 있다. 활성화 후, 카드는 상거래를 포함한 다양한 거래에 사용될 수 있다.

[0098] 일부 실시형태에 따르면 비접촉식 카드(305)는 가상 결제 카드를 포함할 수 있다. 이러한 실시형태에서 응용프로그램(311)은 클라이언트 디바이스(310) 상에 구현된 디지털 지갑에 액세스함으로써 비접촉식 카드(305)와 관련된 정보를 검색할 수 있으며, 여기서 디지털 지갑은 가상 지불 카드를 포함한다. 일부 실시예에서 가상 지불 카드 데이터는 하나 이상의 정적 또는 동적으로 생성된 가상 카드 번호를 포함할 수 있다.

[0099] 서버(320)는 데이터베이스(335)와 통신하는 웹 서버를 포함할 수 있다. 서버(325)는 계정 서버를 포함할 수 있다. 일부 실시예에서 서버(320)는 데이터베이스(335) 내의 하나 이상의 자격 증명과 비교하여 비접촉식 카드(305) 및/또는 클라이언트 디바이스(310)로부터의 하나 이상의 자격 증명을 검증하도록 형상화될 수 있다. 서버(325)는 비접촉식 카드(305) 및/또는 클라이언트 디바이스(310)로부터의 지불 및 거래와 같은 하나 이상의 요청을 승인하도록 형상화될 수 있다.

[0100] 도 4는 본 명세서의 실시예에 따른 키 다양화 방법(400)을 예시한다. 방법(400)은 도 2에서 참조된 송신 디바이스(205) 및 수신 디바이스(210)와 유사한 송신 디바이스 및 수신 디바이스를 포함할 수 있다.

[0101] 예를 들어 발신자와 수신자는 송신 디바이스와 수신 디바이스를 통해 데이터(예를 들어 원래의 민감한 데이터)를 교환하고자 할 수 있다. 상기한 바와 같이 이들 두 당사자가 포함될 수 있지만, 각 당사자가 동일한 공유 비밀 대칭 키를 공유하는 한 하나 이상의 송신 디바이스 및 하나 이상의 수신 디바이스가 관련될 수 있음을 이해해야 한다. 일부 실시예에서 송신 디바이스 및 수신 디바이스는 동일한 마스터 대칭 키로 프로비저닝 될 수 있다.

[0102] 또한 동일한 비밀 대칭 키를 보유하는 임의의 당사자 또는 디바이스가 송신 디바이스의 기능을 수행할 수 있고 유사하게 동일한 비밀 대칭 키를 보유하는 임의의 당사자가 수신 디바이스의 기능을 수행할 수 있음이 이해된다.

[0103] 일부 실시예에서 대칭 키는 보안 데이터를 교환하는 데 관여하는 송신 디바이스 및 수신 디바이스 이외의 모든 당사자로부터 비밀로 유지되는 공유 비밀 대칭 키를 포함할 수 있다.

[0104] 또한 송신 디바이스와 수신 디바이스 모두에 동일한 마스터 대칭 키가 제공될 수 있으며, 또한 송신 디바이스와 수신 디바이스 사이에서 교환되는 데이터의 일부는 카운터 값으로 지칭될 수 있는 데이터의 적어도 일부를 포함한다. 카운터 값은 송신 디바이스와 수신 디바이스 사이에서 데이터가 교환될 때마다 변경되는 숫자를 포함할 수 있다.

[0105] 블록 410에서 송신 디바이스 및 수신 디바이스는 동일한 마스터 대칭 키와 같은 동일한 마스터 키로 프로비저닝될 수 있다. 송신 디바이스가 대칭 암호화 작동으로 민감한 데이터의 처리 준비를 할 때, 발신자는 카운터를 업데이트할 수 있다. 또한 송신 디바이스는 대칭 암호화 알고리즘, HMAC 알고리즘 및 CMAC 알고리즘 중 적어도 하나를 포함할 수 있는 적절한 대칭 암호화 알고리즘을 선택할 수 있다.

[0106] 일부 실시예에서 다양화 값을 처리하기 위해 사용되는 대칭 알고리즘은 원하는 길이의 다양화 대칭 키를 생성하기 위해 필요에 따라 사용되는 임의의 대칭 암호화 알고리즘을 포함할 수 있다.

[0107] 대칭 알고리즘의 비-제한적인 실시예는 3DES 또는 AES128과 같은 대칭 암호화 알고리즘; HMAC-SHA-256과 같은 대칭 HMAC 알고리즘; 및 AES-CMAC와 같은 대칭 CMAC 알고리즘을 포함할 수 있다. 선택된 대칭 알고리즘의 출력이 충분히 긴 키를 생성하지 못하는 경우, 상이한 입력 데이터와 동일한 마스터 키를 사용하여 대칭 알고리즘의 다수 반복을 처리하는 것과 같은 기술이 충분한 길이의 키를 생성하기 위해 필요하고, 이에 따라 결합할 수 있는 다수의 출력을 생성하는 것으로 이해된다.

[0108] 송신 디바이스는 선택된 암호화 알고리즘을 취하고 마스터 대칭 키를 사용하여 카운터 값을 처리할 수 있다. 예를 들어 발신자는 대칭 암호화 알고리즘을 선택하고 송신 디바이스와 수신 디바이스 간의 모든 대화를 업데이트하는 카운터를 사용할 수 있다.

[0109] 블록 420에서 송신 디바이스는 마스터 대칭 키를 사용하여 선택된 대칭 암호화 알고리즘으로 카운터 값을 암호화하여 다양화 대칭 키를 생성할 수 있다. 다양화 대칭 키는 결과를 수신 디바이스로 전송하기 전에 민감한 데이터를 처리하는 데 사용될 수 있다. 예를 들어 송신 디바이스는 다양화 대칭 키를 사용하는 대칭 암호화 알고리즘을 사용하여 민감한 데이터를 암호화할 수 있으며, 출력은 보호된 암호화 데이터를 포함한다.

[0110] 송신 디바이스는 처리를 위해 카운터 값과 함께 보호된 암호화 데이터를 수신 디바이스로 전송할 수 있다. 일부 실시예에서 암호화 이외의 암호화 작동이 수행될 수 있으며 보호된 데이터의 전송 이전에 다양화 대칭 키들을 사용하는 다수의 암호화 작동이 수행될 수 있다.

[0111] 일부 실시예에서 카운터 값은 암호화되지 않을 수 있다. 이러한 실시예에서 카운터 값은 암호화없이 블록 420에서 송신 디바이스와 수신 디바이스 사이에 전송될 수 있다.

[0112] 블록 430에서 민감한 데이터는 하나 이상의 암호화 알고리즘 및 다양화 키를 사용하여 보호될 수 있다. 카운터를 사용하는 키 다양화에 의해 생성될 수 있는 다양화 세션 키는 민감한 데이터를 보호하기 위해 하나 이상의 암호화 알고리즘과 함께 사용될 수 있다. 예를 들어 데이터는 제1 다양화 세션 키를 사용하여 MAC에 의해 처리될 수 있고, 이에 따른 출력은 보호된 데이터를 생성하는 제2 다양화 세션 키를 사용하여 암호화될 수 있다.

[0113] 블록 440에서 수신 디바이스는 암호화에 대한 입력으로서 카운터 값을 사용하고 암호화를 위한 키로서 마스터 대칭 키를 사용하여 동일한 대칭 암호화를 수행할 수 있다. 암호화의 출력은 발신자에 의해 생성된 동일한 다양화 대칭 키 값일 수 있다.

[0114] 예를 들어 수신 디바이스는 카운터를 사용하는 제1 및 제2 다양화 세션 키의 자체 복사본을 독립적으로 생성할 수 있다. 이후, 수신 디바이스는 제2 다양화 세션 키를 사용하여 보호 데이터를 복호화 함으로써 송신 디바이스가 생성한 MAC의 출력을 나타낼 수 있다. 수신 디바이스는 제1 다양화 세션 키를 사용하여 MAC 작동을 통해 결과 데이터를 처리할 수 있다.

[0115] 블록 450에서 수신 디바이스는 보호된 데이터를 검증하기 위해 하나 이상의 암호화 알고리즘과 함께 다양화 키를 사용할 수 있다.

[0116] 블록 460에서 원래의 데이터가 검증될 수 있다. MAC 작동의 출력(첫 번째 다양화 세션 키를 사용하여 수신 디바이스를 통해)이 복호화에 의해 나타난 MAC 출력과 일치하면 데이터는 유효한 것으로 간주될 수 있다.

[0117] 다음에 민감한 데이터를 송신 디바이스에서 수신 디바이스로 보내야할 때 상이한 카운터 값을 선택하여 상이한 다양화 대칭 키를 생성할 수 있다. 마스터 대칭 키와 동일한 대칭 암호화 알고리즘으로 카운터 값을 처리함으로써 송신 디바이스와 수신 디바이스 모두 독립적으로 동일한 다양화 대칭 키를 생성할 수 있다. 마스터 대칭 키가 아닌 이 다양화 대칭 키는 민감한 데이터를 보호하는 데 사용된다.

[0118] 위에서 설명한 바와 같이 송신 디바이스와 수신 디바이스는 각각 초기에 공유 마스터 대칭 키를 소유한다. 공유 마스터 대칭 키는 원래의 중요한 데이터를 암호화하는 데 사용되지 않는다. 다양화 대칭 키는 송신 디바이스와 수신 디바이스 모두에서 독립적으로 생성되기 때문에 두 당사자간에 전송되지 않는다.

[0119] 따라서 공격자는 다양화 대칭 키를 가로챌 수 없으며 공격자는 마스터 대칭 키로 처리된 데이터를 볼 수 없다. 민감한 데이터가 아닌 작은 카운터 값만 마스터 대칭 키로 처리된다. 결과적으로 마스터 대칭 키에 대한 감소된 사이드-채널 데이터가 표시된다.

[0120] 또한 발신자와 수신자는 예를 들어 사전 배열 또는 다른 수단에 의해 새로운 분산 값을 생성하는 빈도, 따라서 새로운 분산 대칭 키를 생성하는 데 동의할 수 있다. 하나의 실시형태에서 새로운 다양화 값 및 따라서 새로운 다양화된 대칭 키가 송신 디바이스와 수신 디바이스 사이의 모든 교환에 대해 생성될 수 있다.

[0121] 일부 실시예에서 키 다양화 값은 카운터 값을 포함할 수 있다.

[0122] 주요 다양화 값의 다른 비-제한적인 실시예는 새로운 다양화된 키가 필요할 때마다 생성되는 랜덤 논스, 송신 디바이스에서 수신 디바이스로 전송되는 랜덤 논스; 송신 디바이스 및 수신 디바이스로부터 전송된 카운터 값의 전체 값; 송신 디바이스 및 수신 디바이스로부터 전송된 카운터 값의 일부; 송신 디바이스와 수신 디바이스에 의해 독립적으로 유지되지만 둘 사이에 전송되지 않는 카운터; 송신 디바이스와 수신 디바이스 사이에서 교환되는 일회성 암호; 민감한 데이터의 암호화 해시;를 포함한다.

[0123] 일부 실시예에서 키 다양화 값의 하나 이상의 부분은 다수의 다양화 키를 생성하기 위해 당사자에 의해 사용될 수 있다. 예를 들어 카운터를 키 다양화 값으로 사용할 수 있다.

[0124] 또 다른 실시예에서 카운터의 일부는 키 다양화 값으로 사용될 수 있다. 다수의 마스터 키 값이 당사자간에 공유되는 경우, 본 명세서에 설명된 시스템 및 프로세스에 의해 다수의 다양화 키 값이 수득될 수 있다.

[0125] 새로운 다양화 값, 따라서 새로운 다양화된 대칭 키가 필요한 만큼 자주 생성될 수 있다. 가장 안전한 경우, 송신 디바이스와 수신 디바이스 사이에 민감한 데이터를 교환할 때마다 새로운 다양화 값이 생성될 수 있다. 실제로 이것은 단일 세션 키와 같은 일회용 키를 생성할 수 있다.

[0126] 마스터 대칭 키의 사용 횟수를 제한하는 것과 같은 다른 실시예에서 송신 디바이스의 발신자와 수신 디바이스의 수신자가 새로운 다양화 값에 동의할 수 있으며 따라서 새로운 다양화 대칭 키가 주기적으로만 발생한다.

[0127] 하나의 실시에서 이것은 송신 디바이스와 수신 디바이스 사이의 매 10 번의 송신과 같이 미리 결정된 사용 횟수 이후일 수 있다. 다른 실시예에서 이것은 특정 기간 이후, 전송 후 특정 기간 또는 주기적(예를 들어 지정된 시간에 매일; 지정된 날짜의 지정된 시간에 매주) 일 수 있다.

[0128] 다른 실시예에서 이것은 이후의 통신에서 키를 변경하기를 원한다고 송신 디바이스에 수신 디바이스가 신호하는 매번 발생할 수 있다. 이는 정책에 따라 제어될 수 있으며, 예를 들어 수신 디바이스의 수신자가 인식하는 현재 위험 수준에 따라 달라질 수 있다.

[0129] 도 5a는 카드(500)의 앞면 또는 뒷면에 표시된 서비스 공급자(505)에 의해 발행된 신용카드, 직불 카드 또는 기프트 카드와 같은 지불 카드를 포함할 수 있는 하나 이상의 비접촉식 카드(500)를 도시한다. 일부 실시예에서 비접촉식 카드(500)는 결제 카드와 관련이 없으며 신분증을 제한없이 포함할 수 있다.

[0130] 일부 실시예에서 결제 카드는 이중 인터페이스 비접촉식 결제 카드를 포함할 수 있다. 비접촉식 카드(500)는 단일 층 또는 플라스틱, 금속 및 기타 재료로 구성된 하나 이상의 적층된 층을 포함하는 기판(510)을 포함할 수 있다. 예시적인 기판 재료는 폴리염화비닐, 폴리염화비닐아세테이트, 아크릴로니트릴부타디엔스티렌, 폴리카보네이트, 폴리에스테르, 양극성 산화티타늄, 팔라듐, 금, 탄소, 종이 및 생분해성 물질을 포함한다.

[0131] 일부 실시예에서 비접촉식 카드(500)는 ISO/IEC 7810 표준의 ID-1 형식을 준수하는 물리적 특성을 지닐 수 있으

며 그렇지 않으면 비접촉식 카드는 ISO/IEC 14443 표준을 준수할 수 있다. 그러나 본 발명에 따른 비접촉식 카드(500)는 서로 다른 특성을 지닐 수 있으며 본 발명은 결제 카드 내에 비접촉식 카드를 구현할 필요가 없는 것으로 이해된다.

[0132] 비접촉식 카드(500)는 또한 카드의 앞면 및/또는 뒷면에 표시된 식별 정보(515) 및 접촉 패드(520)를 포함할 수 있다. 접촉 패드(520)는 사용자 디바이스, 스마트폰, 랩톱, 데스크톱 또는 태블릿 컴퓨터와 같은 다른 통신 디바이스와 접촉을 설정하도록 형상화될 수 있다.

[0133] 또한 비접촉식 카드(500)는 도 5a에 도시되지 않은 처리 회로, 안테나 및 기타 컴포넌트를 포함할 수 있다. 이들 컴포넌트는 접촉 패드(520) 뒤에 또는 기판(510)의 다른 곳에 위치할 수 있다. 비접촉식 카드(500)는 또한 카드의 후면에 위치할 수 있는 자기 스트립 또는 테이프를 포함할 수 있다(도 5a에 도시되지 않음).

[0134] 도 5b에 도시된 바와 같이, 도 5a의 접촉 패드(520)는 마이크로 프로세서(530) 및 메모리(535)를 포함하는 정보를 저장하고 처리하기 위한 처리 회로(525)를 포함할 수 있다. 처리 회로(525)는 본 명세서에 설명된 기능을 수행하는 데 필요한 프로세서, 메모리, 오류 및 패리티/CRC 검사기, 데이터 인코더, 충돌 방지 알고리즘, 컨트롤러, 명령어 디코더, 보안 프리미티브 및 변조 방지 하드웨어를 포함하는 추가 컴포넌트를 포함할 수 있음을 이해해야 한다.

[0135] 메모리(535)는 읽기 전용 메모리, 1회 쓰기 다회 읽기 메모리 또는 읽기/쓰기 메모리, 예를 들어 RAM, ROM 및 EEPROM 일 수 있으며 비접촉식 카드(500)는 이들 메모리 중 하나 이상을 포함할 수 있다. 읽기 전용 메모리는 공장에서 읽기 전용 또는 일회성 프로그래밍이 가능하다. 일회성 프로그래밍 기능은 한 번 쓰고 여러 번 읽을 수 있는 기회를 제공한다. 1회 쓰기/다회 읽기 메모리는 메모리 칩이 공장에서 출고된 후 특정 시점에 프로그래밍 될 수 있다. 메모리가 프로그래밍 되면 다시 쓸 수는 없으나 여러 번 읽을 수 있다. 읽기/쓰기 메모리는 출고 후 여러 번 프로그래밍 및 재 프로그래밍 될 수 있다. 또한 여러 번 읽을 수 있다.

[0136] 메모리(535)는 하나 이상의 애플릿(540), 하나 이상의 카운터(545) 및 고객 식별자(550)를 저장하도록 형상화될 수 있다. 하나 이상의 애플릿(540)은 자바 카드 애플릿과 같이 하나 이상의 비접촉식 카드에서 실행하도록 형상화된 하나 이상의 소프트웨어 응용프로그램을 포함할 수 있다.

[0137] 그러나 애플릿(540)은 자바 카드 애플릿으로 제한되지 않으며 대신 비접촉식 카드 또는 제한된 메모리를 지니는 다른 디바이스에서 작동 가능한 소프트웨어 응용프로그램일 수 있음을 이해해야 한다.

[0138] 하나 이상의 카운터(545)는 정수를 저장하기에 충분한 숫자 카운터를 포함할 수 있다. 고객 식별자(550)는 비접촉식 카드(500)의 사용자에게 할당된 고유한 영숫자 식별자를 포함할 수 있으며 식별자는 비접촉식 카드의 사용자를 다른 비접촉식 카드 사용자와 구별할 수 있다. 일부 실시예에서 고객 식별자(550)는 고객 및 그 고객에게 할당된 계정 모두를 식별할 수 있으며 고객의 계정과 관련된 비접촉식 카드를 추가로 식별할 수 있다.

[0139] 전술한 예시적인 실시형태의 프로세서 및 메모리 소자는 접촉 패드를 참조하여 설명하였으나 본 명세서는 이에 제한되지 않는다. 이들 엘레멘트는 패드(520)의 외부에서 구현되거나 완전히 분리되어 구현될 수 있거나, 또는 접촉 패드(520) 내에 위치한 프로세서(530) 및 메모리(535) 엘레멘트에 추가하여 추가 엘레멘트로서 구현될 수 있음이 이해된다.

[0140] 일부 실시예에서 비접촉식 카드(500)는 하나 이상의 안테나(555)를 포함할 수 있다. 하나 이상의 안테나(555)는 비접촉식 카드(500) 내부 및 접촉 패드(520)의 처리 회로(525) 주위에 배치될 수 있다. 예를 들어 하나 이상의 안테나(555)는 처리 회로(525)와 통합될 수 있으며 하나 이상의 안테나(555)는 외부 부스터 코일과 함께 사용될 수 있다. 다른 실시예로서 하나 이상의 안테나(555)는 접촉 패드(520) 및 처리 회로(525)의 외부에 있을 수 있다.

[0141] 하나의 실시형태에서 비접촉식 카드(500)의 코일은 공심 변압기의 2차 역할을 할 수 있다. 단말기는 전력 또는 진폭 변조를 차단함으로써 비접촉식 카드(500)와 통신할 수 있다. 비접촉식 카드(500)는 하나 이상의 커패시터를 통해 기능적으로 유지될 수 있는 비접촉식 카드의 전원 연결의 갭을 이용하여 단말로부터 전송된 데이터를 추론할 수 있다.

[0142] 비접촉식 카드(500)는 비접촉식 카드 코일 상의 부하를 전환하거나 부하 변조를 통해 다시 통신할 수 있다. 간섭을 통해 단자 코일에서 부하 변조를 감지할 수 있다.

[0143] 상기한 바와 같이 비접촉식 카드(500)는 스마트 카드 또는 JavaCard와 같은 제한된 메모리를 지니는 다른 디바이스에서 작동 가능한 소프트웨어 플랫폼 상에 구축될 수 있으며, 하나 이상의 응용프로그램 또는 애플릿이 안

전하게 실행될 수 있다. 다양한 모바일 응용프로그램-기반 사용 시 다중 인증(MFA)을 위한 일회용 암호(OTP)를 제공하기 위해 비접촉식 카드에 애플릿을 추가할 수 있다.

[0144] 애플릿은 모바일 NFC 리더와 같은 판독기로부터의 근거리 데이터 교환 요청과 같은 하나 이상의 요청에 응답하고 NDEF 텍스트 태그로 인코딩된 암호화 보안 OTP를 포함하는 NDEF 메시지를 생성하도록 형상화될 수 있다.

[0145] 도 6은 예시적인 실시형태에 따른 NDEF 단기 레코드 레이아웃(SR = 1)(600)을 도시한다. 하나 이상의 애플릿이 OTP를 NDEF 유형 4 잘 알려진 유형 텍스트 태그로 인코딩하도록 형상화될 수 있다. 일부 실시예에서 NDEF 메시지는 하나 이상의 레코드를 포함할 수 있다. 애플릿은 OTP 레코드에 추가하여 하나 이상의 정적 태그 레코드를 추가하도록 형상화될 수 있다.

[0146] 예시적인 태그는 제한없이 Tag type: well known type, text, encoding English(en); Applet ID: D2760000850101; Capabilities: read-only access; Encoding: the authentication message may be encoded as ASCII hex;를 포함하며 type-length-value(TLV) 데이터는 NDEF 메시지를 생성하는 데 사용될 수 있는 개인화 파라미터로 제공될 수 있다. 하나의 실시형태에서 인증 템플릿은 실제 동적 인증 데이터를 제공하기 위한 잘 알려진 인덱스와 함께 첫 번째 레코드를 포함할 수 있다.

[0147] 도 7은 예시적인 실시형태에 따른 메시지(710) 및 메시지 포맷(720)을 도시한다. 하나의 실시예에서 추가 태그가 부가되는 경우 첫 번째 바이트는 메시지가 시작되지만 끝이 아님을 나타내도록 변경될 수 있으며 후속 레코드가 부가될 수 있다. ID 길이가 0이므로 ID 길이 필드와 ID가 레코드에서 생략된다. 예시적인 메시지는 다음을 포함할 수 있다: UDK AUT key; Derived AUT session key(using 0x00000050); Version 1.0; pATC = 0x00000050; RND = 4838FB7DC171B89E; MAC = <eight computed bytes>.

[0148] 일부 실시예에서 데이터는 보안 채널 프로토콜 2 하에서 STORE DATA(E2)를 구현함으로써 개인화 시간에 비접촉식 카드에 저장될 수 있다. 하나 이상의 값은 EMBOSS 파일에서 개인화 부서에 의해 읽혀질 수 있다. 애플릿 ID) 및 하나 이상의 저장 데이터 명령이 인증 및 보안 채널 설정 후 비접촉식 카드로 전송될 수 있다.

[0149] pUID는 16 자리 BCD 인코딩 숫자를 포함할 수 있다. 일부 실시예에서 pUID는 14 자리 숫자를 포함할 수 있다.

[0150]

아이템	길이(바이트)	암호화?	참조
pUID	8	아니오	
AutKey	16	예	MAC 세션 키 파생을 위한 3DES 키
AutKCV	3	아니오	Key 체크 값
DEKKey	16	예	암호화 세션 키 파생을 위한 3DES 키
DEKKCV	3	아니오	Key 체크 값
Card Shared Random	4 바이트	아니오	4 바이트 트루 무작위 수 (사전-생성됨)
NTLV	X 바이트	아니오	NDEF 메시지를 위한 TLV 데이터

[0151] 일부 실시예에서 하나 이상의 애플릿은 잠금 해제되고 인증된 경우에만 개인화를 허용하기 위한 개인화 상태를 유지하도록 형상화될 수 있다. 다른 상태는 사전-개인화 표준 상태를 포함할 수 있다. 종료된 상태로 들어가면 하나 이상의 애플릿이 개인화 데이터를 제거하도록 형상화될 수 있다. 종료된 상태에서 하나 이상의 애플릿은 모든 응용 프로토콜 데이터 단위(APDU) 요청에 대한 응답을 중지하도록 형상화될 수 있다.

[0152] 하나 이상의 애플릿은 인증 메시지에 사용될 수 있는 애플릿 버전(2 바이트)을 유지하도록 형상화될 수 있다. 일부 실시예에서 이것은 최상위 바이트 주요 버전, 최하위 바이트 부 버전으로 해석될 수 있다. 각 버전에 대한 규칙은 인증 메시지를 해석하도록 형상화된다.

[0153] 예를 들어 주요 버전과 관련하여 여기에는 각 주요 버전이 특정 인증 메시지 레이아웃과 특정 알고리즘으로 구성되는 것을 포함할 수 있다. 부 버전의 경우 여기에는 인증 메시지 또는 암호화 알고리즘에 대한 변경 사항이 포함되지 않을 수 있으며 버그 수정, 보안 강화 외에도 정적 태그 콘텐츠에 대한 변경 사항이 포함될 수 있다.

[0154] 일부 실시예에서 하나 이상의 애플릿은 RFID 태그를 에뮬레이트 하도록 형상화될 수 있다. RFID 태그는 하나 이상의 다형성 태그를 포함할 수 있다. 일부 실시예에서 태그가 판독될 때마다 비접촉식 카드의 진위를 나타내는 상이한 암호화 데이터가 제시된다. 하나 이상의 응용프로그램에 기반하여 태그의 NFC 판독이 처리될 수 있으며

토큰이 백엔드 서버와 같은 서버로 전송될 수 있고 토큰이 서버에서 검증될 수 있다.

[0155] 일부 실시예에서 비접촉식 카드 및 서버는 카드가 적절하게 식별될 수 있도록 특정 데이터를 포함할 수 있다. 비접촉식 카드는 하나 이상의 고유 식별자를 포함할 수 있다. 읽기 작동이 발생할 때마다 카운터는 업데이트하도록 형상화될 수 있다. 일부 실시예에서 카드가 판독될 때마다 유효성 검사를 위해 서버로 전송되고 카운터가 동일한 지 여부를(검증의 일부로) 결정한다.

[0156] 하나 이상의 카운터는 리플레이 공격을 방지하도록 형상화될 수 있다. 예를 들어 암호를 획득하고 리플레이 한 경우 카운터를 읽거나 사용했거나 다른 방법으로 전달하면 해당 암호가 즉시 거부된다. 카운터를 사용하지 않은 경우 다시 리플레이할 수 있다.

[0157] 일부 실시예에서 카드에 업데이트되는 카운터는 트랜잭션을 위해 업데이트되는 카운터와 상이하다. 일부 실시예에서 비접촉식 카드는 트랜잭션 애플릿일 수 있는 제1 애플릿 및 제2 애플릿을 포함할 수 있다. 각 애플릿은 카운터를 포함할 수 있다.

[0158] 일부 실시예에서 카운터는 비접촉식 카드와 하나 이상의 서버 사이에서 동기화되지 않을 수 있다. 예를 들어 비접촉식 카드가 활성화되어 카운터가 업데이트되고 비접촉식 카드에 의해 새로운 통신이 생성될 수 있으나 하나 이상의 서버에서 처리를 위해 통신이 전송되지 않을 수 있다.

[0159] 이로 인해 비접촉식 카드의 카운터와 하나 이상의 서버에서 유지되는 카운터가 동기화되지 않을 수 있다. 예를 들어 카드가 디바이스에 인접하여 저장되고(예: 디바이스와 함께 주머니에 휴대됨) 비접촉식 카드가 비스듬히 판독되는 경우를 포함하여 의도하지 않게 발생할 수 있다. 비접촉식 카드는 NFC 필드에 전원이 공급되지만 읽을 수 없다.

[0160] 비접촉식 카드가 기기에 인접해 있으면 기기의 NFC 필드가 켜져 비접촉식 카드에 전원이 공급되어 카운터가 업데이트 되지만 기기의 응용프로그램이 통신을 수신하지 않는다.

[0161] 카운터를 동기화 상태로 유지하기 위해 백그라운드 응용프로그램과 같은 응용프로그램을 실행하여 모바일 디바이스가 깨어나면 감지하고 하나 이상의 서버와 동기화하기 위해 형상화 되어 카운터를 앞으로 이동시키기 위해 감지로 인해 발생한 판독을 나타낸다.비접촉식 카드의 카운터와 하나 이상의 서버가 동기화되지 않을 수 있으므로 하나 이상의 서버에 의해 판독되고 여전히 유효한 것으로 간주되기 전에 하나 이상의 서버는 비접촉식 카드의 카운터가 임계 값 또는 미리 결정된 횟수를 업데이트 하도록 형상화될 수 있다.

[0162] 예를 들어 비접촉식 카드의 활성화를 나타내는 각각의 출현에 대해 하나씩 증가(또는 감소)하도록 카운터가 형상화된 경우, 하나 이상의 서버는 비접촉식 카드에서 판독한 모든 카운터 값을 유효한 것으로 허용하거나 임계 값 범위(예: 1부터 10 까지) 안에 있는 모든 카운터 값을 허용할 수 있다.

[0163] 또한 하나 이상의 서버는 사용자 탭과 같은 비접촉식 카드와 관련된 제스처를 요청하도록 형상화될 수 있으며 10을 넘지만 다른 임계 범위 값(예: 1000) 미만인 카운터 값을 읽는 경우에 가능하다. 사용자 탭에서 카운터 값이 원하는 범위 또는 허용 범위 내에 있으면 인증이 성공한다.

[0164] 도 8은 예시적인 실시형태에 따른 키 작동(800)을 예시하는 흐름도이다. 도 8에 도시된 바와 같이 블록 810에서 2 개의 은행 식별자 번호(BIN) 레벨 마스터 키가 카드 당 2 개의 고유한 파생 키(UDK)를 생성하기 위해 계좌 식별자 및 카드 시퀀스 번호와 함께 사용될 수 있다.

[0165] 일부 실시예에서 은행 식별자 번호는 계좌번호 또는 하나 이상의 서버에 의해 제공되는 예측 불가 번호와 같은 하나 이상의 번호의 조합 또는 하나의 번호를 포함할 수 있으며 세션 키 생성 및/또는 다양화를 위해 사용될 수 있다. UDK(AUTKEY 및 ENCKEY)는 개인화 프로세스 중에 카드에 저장될 수 있다.

[0166] 블록 820에서 카운터는 카드 당 하나의 고유한 키 세트가 생성되는 마스터 키 파생과는 반대로 각 사용에 따라 변경되고 매번 다른 세션 키를 제공하기 때문에 다양화 데이터로 사용될 수 있다. 일부 실시예에서는 두 작업 모두에 4 바이트 방법을 사용하는 것이 선호된다.

[0167] 따라서 블록 820에서 UDK로부터의 각 트랜잭션에 대해 2 개의 세션 키, 즉 AUTKEY로부터의 하나의 세션 키 및 ENCKEY로부터의 하나의 세션 키가 생성될 수 있다. 카드에서 MAC 키(즉, AUTKEY에서 생성된 세션 키)의 경우 OTP 카운터의 하위 2 바이트가 다양화에 사용될 수 있다. ENC 키(즉, ENCKEY에서 생성된 세션 키)의 경우 OTP 카운터의 전체 길이가 ENC 키로 사용될 수 있다.

[0168] 블록 830에서 MAC 키는 MAC 암호를 준비하는 데 사용될 수 있으며 ENC 키는 암호를 암호화하는 데 사용될 수 있

다. 예를 들어 MAC 세션 키는 암호를 준비하는 데 사용될 수 있으며 하나 이상의 서버로 전송되기 전에 결과를 ENC 키로 암호화 시킬 수 있다.

[0169] 블록 840에서 2 바이트 다양화가 지불 HSM의 MAC 인증 기능에서 직접 지원되기 때문에 MAC의 검증 및 처리가 단순화된다. 암호의 해독은 MAC 검증 전에 수행된다.

[0170] 세션 키는 하나 이상의 서버에서 독립적으로 파생되어 제1 세션 키(ENC 세션 키)와 제2 세션 키(MAC 세션 키)가 된다. 제2 파생 키(즉, ENC 세션 키)는 데이터를 복호화 하는 데 사용될 수 있으며 제1 파생 키(즉, MAC 세션 키)는 복호화된 데이터를 검증하는 데 사용될 수 있다.

[0171] 비접촉식 카드의 경우 카드에 인코딩 된 응용프로그램 주 계좌 번호(PAN) 및 PAN 시퀀스 번호와 관련되는 상이한 고유 식별자가 파생된다. 키 다양화는 마스터 키와 함께 입력으로서 식별자를 수신하도록 형상화되어 각각의 비접촉식 카드에 대해 하나 이상의 키가 생성되게 한다.

[0172] 일부 실시예에서 이러한 다양화 키는 제1 키 및 제2 키를 포함할 수 있다. 제1 키는 인증 마스터 키(카드 암호 생성/인증 키 - Card-Key-Auth)를 포함할 수 있으며, MAC 암호 생성 및 검증시 사용되는 MAC 세션 키를 생성하기 위해 더욱 다양화될 수 있다. 제2 키는 암호화 마스터 키(카드 데이터 암호화 키 - Card-Key-DEK)를 포함할 수 있으며, 암호화된 데이터를 암호화 및 복호화할 때 사용되는 ENC 세션 키를 생성하기 위해 더욱 다양화될 수 있다.

[0173] 일부 실시예에서 제1 및 제2 키는 카드의 고유 ID 번호(pUID) 및 결제 애플릿의 PAN 시퀀스 번호(PSN)와 결합하여 발급자 마스터 키를 다양화함으로써 생성될 수 있다. pUID는 16 자리 숫자 값을 포함할 수 있다. 상기에서 설명한 바와 같이 pUID는 16 자리 BCD 인코딩 번호를 포함할 수 있다. 일부 실시예에서 pUID는 14 자리 숫자 값을 포함할 수 있다.

[0174] 일부 실시예에서 EMV 세션 키 유도 방법은 2^16 사용으로 랩핑 될 수 있기 때문에 전체 32 비트 카운터와 같은 카운터가 다양화 방법의 초기화 어레이에 추가될 수 있다.

[0175] 신용카드와 같은 다른 실시예에서 하나 이상의 서버에 의해 제공되는 계좌 번호 또는 예측할 수 없는 번호와 같은 번호가 세션 키 생성 및/또는 다양화를 위해 사용될 수 있다.

[0176] 도 9는 본 명세서의 하나 이상의 실시형태를 구현하도록 구성된 시스템(900)의 다이어그램을 도시한다. 하기에 설명된 대로 비접촉식 카드 생성 프로세스 중에 두 개의 암호화 키가 각 카드에 고유하게 할당될 수 있다. 암호화 키는 데이터의 암호화 및 복호화 모두에 사용될 수 있는 대칭 키를 포함할 수 있다. 3DES(Triple DES) 알고리즘은 EMV에서 사용할 수 있으며 비접촉식 카드의 하드웨어로 구현된다. 키 다양화 프로세스를 사용하면 키를 필요로 하는 각각의 엔티티에 대해 고유하게 식별 가능한 정보를 기반으로 마스터 키에서 하나 이상의 키가 파생될 수 있다.

[0177] 마스터 키 관리와 관련하여 하나 이상의 애플릿이 발행되는 포트폴리오의 각 부분에 대해 두 개의 발급자 마스터 키(905, 910)가 필요할 수 있다. 예를 들어 제1 마스터 키(905)는 발급자 암호화 생성/인증 키(Iss-Key-Auth)를 포함할 수 있으며 제2 마스터 키(910)는 발급자 데이터 암호화 키(Iss-Key-DEK)를 포함할 수 있다.

[0178] 본 명세서에서 더욱 설명되는 바와 같이 2 개의 발급자 마스터 키(905, 910)는 각 카드에 대해 고유한 카드 마스터 키(925, 930)로 다양화된다. 일부 실시예에서 백 오피스 데이터로서 네트워크 프로파일 레코드 ID(pNPR)(915) 및 파생 키 인덱스(pDKI)(920)는 인증을 위한 암호화 프로세스에서 사용할 발급자 마스터 키(905, 910)를 식별하는 데 사용될 수 있다. 인증을 수행하는 시스템은 인증시 비접촉식 카드에 대한 pNPR(915) 및 pDKI(920)의 값을 검색하도록 형상화될 수 있다.

[0179] 일부 실시예에서 솔루션의 보안을 높이기 위해 세션 키(예: 세션 당 고유 키)가 파생될 수 있으나 상기에 설명한 바와 같이 마스터 키를 사용하는 대신 고유 카드 파생 키와 카운터가 다양화 데이터로 사용될 수 있다. 예를 들어 카드가 작동 중에 사용될 때마다 메시지 인증 코드(MAC)를 생성하고 암호화를 수행하기 위해 상이한 키가 사용될 수 있다.

[0180] 세션 키 생성과 관련하여, 암호를 생성하고 하나 이상의 애플릿에서 데이터를 암호화하는 데 사용되는 키는 카드 고유 키(Card-Key-Auth 925 및 Card-Key-Dek 930)에 기반한 세션 키를 포함할 수 있다. 세션 키(Aut-Session-Key 935 및 DEK-Session-Key 940)는 하나 이상의 애플릿에 의해 생성될 수 있고 하나 이상의 알고리즘과 함께 응용프로그램 트랜잭션 카운터(pATC)(945)를 사용하여 파생될 수 있다.

[0181] 데이터를 하나 이상의 알고리즘에 맞추기 위해 4-바이트 pATC 945의 하위 2 바이트만 사용된다. 일부 실시예에서 4 바이트 세션 키 파생 방법은 다음을 포함할 수 있다. F1 := PATC(lower 2 bytes) || 'F0' || '00' || PATC(four bytes) F1 := PATC(lower 2 bytes) || '0F' || '00' || PATC(four bytes) SK :={(ALG(MK) [F1]) || ALG(MK) [F2] }, 여기서 ALG는 3DES ECB를 포함할 수 있으며 MK는 카드 고유 파생 마스터 키를 포함할 수 있다.

[0182] 본 명세서에 설명된 바와 같이 하나 이상의 MAC 세션 키는 pATC 945 카운터의 하위 2 바이트를 사용하여 유도될 수 있다. 비접촉식 카드의 각 탭에서 pATC 945는 업데이트 되도록 형상화 되고 카드 마스터 키 Card-Key-AUTH 925 및 Card-Key-DEK 930은 세션 키 Aut-Session-Key 935 및 DEK-Session-KEY 940로 더욱 다양화 된다. pATC(945)는 개인화 또는 애플릿 초기화 시간에 0으로 초기화될 수 있다. 일부 실시예에서 pATC 카운터(945)는 개인화 시 또는 그 전에 초기화될 수 있으며 각각의 NDEF 판독에서 1씩 증가하도록 형상화될 수 있다.

[0183] 또한 각 카드에 대한 업데이트는 고유할 수 있으며 개인화에 의해 할당되거나 pUID 또는 기타 식별 정보에 의해 알고리즘적으로 할당될 수 있다. 예를 들어 홀수 번호 카드는 2씩 증가 또는 감소할 수 있으며 짝수 번호 카드는 5씩 증가 또는 감소할 수 있다.

[0184] 일부 실시예에서 업데이트는 순차적 판독에서 변할 수 있으므로 하나의 카드는 1, 3, 5, 2, 2, … 반복에 의해 순차적으로 증가할 수 있다. 특정 시퀀스 또는 알고리즘 시퀀스는 개인화 시간 또는 고유 식별자에서 파생된 하나 이상의 프로세스에서 정의될 수 있다. 이로 인해 리플레이 공격자는 적은 수의 카드 인스턴스에서 일반화가 더 어려워진다.

[0185] 인증 메시지는 16 진수 ASCII 형식의 텍스트 NDEF 레코드 내용으로 전달될 수 있다. 일부 실시예에서 인증 데이터 및 인증 데이터의 MAC이 뒤따르는 8 바이트 난수 만이 포함될 수 있다. 일부 실시예에서 난수는 암호문 A보다 선행할 수 있으며 한 블록 길이일 수 있다. 다른 실시예에서는 난수 길이에 제한이 없다.

[0186] 추가 실시예에서 총 데이터(즉, 난수 + 암호문)는 블록 크기의 배수일 수 있다. 이러한 실시예에서 MAC 알고리즘에 의해 생성된 블록과 일치하도록 추가 8 바이트 블록이 추가될 수 있다. 다른 실시예로서 채택된 알고리즘이 16 바이트 블록을 사용하는 경우, 해당 블록 크기의 배수도 사용될 수 있거나 출력이 자동 또는 수동으로 해당 블록 크기의 배수로 채워질 수 있다.

[0187] MAC은 기능 키(AUT-Session-Key)(935)에 의해 수행될 수 있다. 암호문에 지정된 데이터는 EMV ARQC 검증 방법과 연관시키기 위해 javacard.signature 메소드(ALG_DES_MAC8_ISO9797_1_M2_ALG3)로 처리될 수 있다. 이러한 연산에 사용되는 키는 상기에서 설명한 바와 같이 세션 키 AUT-Session-Key(935)를 포함할 수 있다.

[0188] 위에서 설명한 바와 같이 카운터의 하위 2 바이트는 하나 이상의 MAC 세션 키에 대해 다양화에 사용될 수 있다. 아래에 설명된 바와 같이 AUT-Session-Key(935)는 MAC 데이터(950)에 사용될 수 있으며 결과 데이터 또는 암호문 A(955) 및 난수 RND는 DEK-Session-Key(940)을 사용하여 암호화되어 메시지 내에 전송된 암호문 B 또는 출력(960)을 생성한다.

[0189] 일부 실시예에서 하나 이상의 HSM 명령이 복호화를 위해 처리될 수 있으므로 최종 16(이진, 32 16진수) 바이트는 MAC 인증 데이터가 뒤따르는 0 IV의 난수를 지니는 CBC 모드를 사용하는 3DES 대칭 암호화를 포함할 수 있다. 이 암호화에 사용되는 키는 Card-Key-DEK(930)에서 파생된 세션 키 DEK-Session-Key(940)를 포함할 수 있다. 이러한 경우에 세션 키 유도를 위한 ATC 값은 카운터 pATC(945)의 최하위 바이트이다.

[0190] 다음 형식은 이진 버전 예시적인 실시형태를 나타낸다. 또한 일부 실시예에서 첫 번째 바이트는 ASCII 'A'로 설정될 수 있다.

메시지 포맷				
1	2	4	8	8
0x43(Message Type ‘A’)	버전	pATC	RND	암호문 A(MAC)

암호문 A(MAC)	8 바이트			
MAC of				
2	8	4	4	18 바이트 입력 데이터
버전	pUID	pATC	공유 비밀	

메시지 포맷			
1	2	4	16
0x43(Message Type ‘A’)	버전	pATC	암호문 B

암호문 A(MAC)	8 바이트			
MAC of				
2	8	4	4	18 바이트 입력 데이터
버전	pUID	pATC	공유 비밀	

암호문 B	16		
Sym Encryption of			
8	8		
RND	암호문 A		

[0191]

[0192] 또 다른 예시적인 형식이 하기에 나타나 있다. 이 실시예에서 태그는 16 진수 형식으로 인코딩될 수 있다.

메시지 포맷				
2	8	4	8	8
버전	pUID	pATC	RND	암호문 A(MAC)
8 바이트				
8	8	4	4	18 바이트 입력 데이터
pUID	pUID	pATC	공유 비밀	

메시지 포맷			
2	8	4	16
버전	pUID	pATC	암호문 B
8 바이트			
8		4	4	18 바이트 입력 데이터
pUID	pUID	pATC	공유 비밀	
암호문 B	16		
Sym Encryption of			
8	8		
RND	암호문 A		

[0193]

[0194] 수신된 메시지의 UID 필드는 마스터 키 Iss-Key-AUTH 905 및 Iss-Key-DEK 910으로부터 특정 카드에 대한 카드 마스터 키(Card-Key-Auth 925 및 Card-Key-DEK 930)를 파생시키기 위해 추출될 수 있다. 카드 마스터 키(Card-Key-Auth 925 및 Card-Key-DEK 930)를 사용하여 수신된 메시지의 카운터(pATC) 필드가 특정 카드에 대한 세션 키(Aut-Session-Key 935 및 DEK-Session-Key 940)를 파생시키기 위해 사용될 수 있다.

[0195] 암호문 B(960)는 DEK-Session-KEY를 사용하여 복호화될 수 있으며, 이는 암호문 A(955) 및 RND를 생성하고 RND는 폐기될 수 있다. UID 필드는 비접촉식 카드의 공유 비밀을 조회하는 데 사용될 수 있다. 이는 메시지의 Ver, UID 및 pATC 필드와 함께 MAC'과 같은 MAC 출력을 생성하기 위해 재-생성된 Aut-Session-Key를 사용하여 암호화 MAC을 통해 처리될 수 있다. MAC'가 암호문 A 955와 동일하면 메시지 복호화 및 MAC 검사가 모두 통과되었음을 나타낸다. 그 후 유효한지 확인하기 위해 pATC가 판독될 수 있다.

[0196] 인증 세션 동안 하나 이상의 응용프로그램에 의해 하나 이상의 암호가 생성될 수 있다. 예를 들어 하나 이상의 암호는 Aut-Session-Key 935와 같은 하나 이상의 세션 키를 통해 방법 2 패딩을 사용하는 ISO 9797-1 알고리즘 3을 사용하여 3DES MAC으로 생성될 수 있다. 입력 데이터(950)는 다음 형식을 취할 수 있다. Version(2), pUID(8), pATC(4), Shared Secret(4).

[0197] 일부 실시예에서 괄호 안의 숫자는 길이(바이트)를 포함할 수 있다. 일부 실시예에서 공유 비밀은 하나 이상의 보안 프로세스를 통해 난수가 예측 불가능하다는 것을 보장하도록 형상화되는 하나 이상의 난수 생성기에 의해 생성될 수 있다.

[0198] 일부 실시예에서 공유 비밀은 인증 서비스에 의해 알려진 개인화 시간에 카드 내에 주입된 임의의 4-바이트 이진 숫자를 포함할 수 있다. 인증 세션 중에 하나 이상의 애플릿에서 모바일 응용프로그램으로 공유 비밀이 제공되지 않을 수 있다. 방법 2 패딩은 입력 데이터 끝에 필수 0x'80'바이트를 추가하는 것과 8 바이트 경계까지 결

과 데이터 끝에 추가될 수 있는 0x'00'바이트를 추가하는 것이 포함될 수 있다. 생성된 암호는 8 바이트 길이를 포함할 수 있다.

[0199] 일부 실시예에서 MAC 암호를 사용하여 공유되지 않은 난수를 첫 번째 블록으로서 암호화하는 한 가지 이점은 대칭 암호화 알고리즘의 CBC(Block chaining) 모드를 사용하는 동안 초기화 벡터로서 역할 한다는 것이다. 이를 통해 고정 또는 동적 IV를 미리 설정할 필요없이 블록 간에 "스크램블" 할 수 있다.

[0200] 응용프로그램 트랜잭션 카운터(pATC)를 MAC 암호 내에 포함된 데이터의 일부로 포함함으로써, 인증 서비스는 클리어 데이터에서 전달된 값이 변조되었는지 여부를 결정하도록 형상화될 수 있다. 또한 하나 이상의 암호에 버전을 포함함으로써 공격자가 암호화 솔루션의 강도를 낮추기 위해 응용 프로그램 버전을 의도적으로 잘못 표시하는 것이 어렵게 된다.

[0201] 일부 실시예에서 pATC는 0에서 시작하고 하나 이상의 응용프로그램이 인증 데이터를 생성할 때마다 1만큼 업데이트될 수 있다. 인증 서비스는 인증 세션 동안 사용되는 pATC를 추적하도록 형상화될 수 있다. 일부 실시예에서 인증 데이터가 인증 서비스에 의해 수신된 이전 값 이하의 pATC를 사용하는 경우, 이는 오래된 메시지를 재생하려는 시도로 해석될 수 있으며 인증된 것이 거부될 수 있다.

[0202] 일부 실시예에서 pATC가 수신된 이전 값보다 큰 경우에 이는 허용 가능한 범위 또는 임계 값 내에 있는지 여부를 결정하기 위해 평가될 수 있으며 범위 또는 임계 값을 초과하거나 그 외부에 있는 경우에는 검증이 실패하거나 신뢰할 수 없는 것으로 간주될 수 있다. MAC 작동(936)에서 데이터(950)는 Aut-Session-Key(935)를 사용하여 MAC을 통해 처리되어 암호화된 MAC 출력(암호문 A)(955)를 생성한다.

[0203] 카드의 키를 노출하는 무차별 대입 공격에 대한 추가 보호를 제공하기 위해 MAC 암호(955)를 암호화 하는 것이 바람직하다. 일부 실시예에서 암호문에 포함될 데이터 또는 암호문 A(955)는 난수(8), 암호(8)를 포함할 수 있다. 일부 실시예에서 괄호 안의 숫자는 길이(바이트)를 포함한다.

[0204] 일부 실시예에서 난수는 하나 이상의 보안 프로세스를 통해 난수가 예측 불가능 함을 보장하도록 형상화될 수 있는 하나 이상의 난수 생성기에 의해 생성될 수 있다. 이러한 데이터를 암호화하는 데 사용되는 키는 세션 키를 포함할 수 있다. 예를 들어 세션 키는 DEK-Session-Key(940)를 포함할 수 있다.

[0205] 암호화 작동(941)에서 데이터 또는 암호문 A(955) 및 RND는 DEK-Session-Key(940)을 사용하여 처리되어 암호화된 데이터인 암호문 B(960)을 생성한다. 데이터(955)는 공격자가 모든 암호문을 넘어 공격을 실행해야 한다는 것을 보장하기 위한 암호 블록 체인화 모드에서 3DES를 사용하여 암호화될 수 있다. 비-제한적인 실시예로서 고급 암호 표준(AES)와 같은 다른 알고리즘이 사용될 수 있다.

[0206] 일부 실시예에서 0x'0000000000000000'의 초기화 벡터가 사용될 수 있다. 이러한 데이터를 암호화하는 데 사용된 키를 무차별 대입(brute force)하려는 공격자는 올바른 키가 사용된 시기를 확인할 수 없다. 올바르게 복호화된 데이터는 난수 출현으로 인해 잘못 복호화된 데이터와 구별할 수 없기 때문이다.

[0207] 인증 서비스가 하나 이상의 애플릿에서 제공하는 하나 이상의 암호를 검증하려면 다음의 데이터가 하나 이상의 애플릿에서 모바일 디바이스로 인증 세션 중에 투명하게 전달되어야 한다: 사용된 암호화 접근 방식 및 암호의 검증을 위한 메시지 형식을 결정하기 위한 버전 번호, 이는 향후 접근 방식 변경이 가능하게 한다; 암호화 자산을 검색하고 카드 키를 파생하는 pUID; 및 암호에 사용되는 세션 키를 파생하는 pATC.

[0208] 도 10은 암호를 생성하기 위한 방법(1000)을 예시한다. 예를 들어 블록 1010에서 네트워크 프로파일 레코드 ID(pNPR) 및 파생 키 인덱스(pDKI)가 인증을 위한 암호화 프로세스에서 사용할 발급자 마스터 키를 식별하는 데 사용될 수 있다. 일부 실시예에서 방법은 인증 시점에 비접촉식 카드에 대한 pNPR 및 pDKI의 값을 검색하기 위한 인증을 수행하는 것을 포함할 수 있다.

[0209] 블록 1020에서 발급자 마스터 키는 카드의 고유 ID 번호(pUID) 및 하나 이상의 애플릿, 예를 들어 지불 애플릿의 PAN 시퀀스 번호(PSN)와 결합하여 다양화될 수 있다.

[0210] 블록 1030에서 카드 키 인증 및 카드 키-DEK(고유 카드 키)는 MAC 암호의 생성에 사용될 수 있는 세션 키를 생성하기 위해 발급자 마스터 키를 다양화함으로써 생성될 수 있다.

[0211] 블록 1040에서 암호를 생성하고 하나 이상의 애플릿 내의 데이터를 암호화하는 데 사용되는 키는 카드 고유 키(Card-Key-Auth 및 Card-Key-DEK) 기반으로 한 블록 1030의 세션 키를 포함할 수 있다. 일부 실시예에서 이러한 세션 키는 하나 이상의 애플릿에 의해 생성되고 pATC를 사용하여 파생되며 세션 키 Aut-Session-Key 및 DEK-

Session-Key가 유도된다.

[0212] 도 11은 하나의 실시예에 따른 키 다양화를 나타내는 예시적인 프로세스(1100)를 도시한다. 초기에는 발신자와 수신자에게 두 개의 서로 다른 마스터 키가 제공될 수 있다. 예를 들어 제1 마스터 키는 데이터 암호화 마스터 키를 포함할 수 있고, 제2 마스터 키는 데이터 무결성 마스터 키를 포함할 수 있다. 발신자는 블록(1110)에서 업데이트 되는 카운터 값 및 수신자와의 보안 공유를 위한 보호될 데이터와 같은 다른 데이터를 지닌다.

[0213] 블록 1120에서 카운터 값은 데이터 암호화 마스터 키를 사용하여 발신자에 의해 암호화되어 데이터 암호화 파생 세션 키를 생성할 수 있으며, 카운터 값은 데이터 무결성 마스터 키를 사용하여 발신자에 의해 또한 암호화되어 데이터 무결성 파생 세션 키를 생성할 수 있다.

[0214] 일부 실시예에서 카운터 값의 전체 또는 카운터 값의 일부가 모든 암호화 동안에 사용될 수 있다. 일부 실시예에서 카운터 값은 암호화되지 않을 수 있다. 이러한 실시예에서 카운터는 투명하게 즉 암호화 없이 발신자와 수신자 사이에서 전송될 수 있다.

[0215] 블록 1130에서 보호될 데이터는 데이터 무결성 세션 키 및 암호화 MAC 알고리즘을 사용하여 발신자에 의해 암호화 MAC 작동으로 처리된다. 일반 텍스트 및 공유 비밀을 포함하는 보호된 데이터는 세션 키 중 하나(AUT-Session-Key)를 사용하여 MAC을 생성하는 데 사용될 수 있다.

[0216] 블록 1140에서 보호될 데이터는 대칭 암호화 알고리즘과 함께 데이터 암호화 파생된 세션 키를 사용하여 발신자에 의해 암호화될 수 있다. 일부 실시예에서 MAC은 예를 들어 각각 8 바이트 길이의 동일한 양의 랜덤 데이터와 결합되고 그 후 두 번째 세션 키(DEK-Session-Key)를 사용하여 암호화된다.

[0217] 블록 1150에서 암호화된 MAC은 암호화의 검증을 위해 추가 비밀 정보(예: 공유 비밀, 마스터 키 등)를 식별하기에 충분한 정보와 함께 발신자로부터 수신자에게 전송된다.

[0218] 블록 1160에서 수신자는 수신된 카운터 값을 사용하여 전술한 바와 같이 2 개의 마스터 키로부터 2 개의 파생된 세션 키를 독립적으로 파생시킨다.

[0219] 블록 1170에서 데이터 암호화 파생된 세션 키는 보호된 데이터를 복호화하기 위해 대칭 복호화 작동과 결합하여 사용된다. 교환된 데이터에 대한 추가 처리가 발생한다. 일부 실시예에서 MAC이 추출된 후, MAC을 재생산하고 일치시키는 것이 바람직하다. 예를 들어 암호를 검증할 때 적절하게 생성된 세션 키를 사용하여 복호화할 수 있다.

[0220] 보호된 데이터는 검증을 위해 재구성될 수 있다. 적절하게 생성된 세션 키를 사용하여 MAC 작동을 수행함으로써 복호화된 MAC과 일치하는지 확인할 수 있다. MAC 작동은 비가역적 프로세스이므로 검증하는 유일한 방법은 원본 데이터에서 다시 생성하는 것이다.

[0221] 블록 1180에서 데이터 무결성 파생 세션 키는 보호된 데이터가 수정되지 않았 음을 검증하기 위해 암호화 MAC 작동과 결합하여 사용된다.

[0222] 본 명세서에 설명된 방법의 일부 실시예는 다음 조건의 충족 하에 성공적인 인증이 결정되었는지 유리하게 확인할 수 있다. 우선, MAC 검증 기능은 파생된 세션 키가 적절함을 나타낸다. 복호화가 성공적이고 적절한 MAC 값을 산출한 경우에만 MAC가 정확할 수 있다.

[0223] 성공적인 복호화는 올바르게 파생된 암호화 키가 암호화된 MAC 복호화에 사용되었음을 나타낼 수 있다. 파생된 세션 키는 발신자(예: 송신 디바이스)와 수신자(예: 수신 디바이스)에게만 알려진 마스터 키를 사용하여 생성되기 때문에 MAC을 원래 생성하고 MAC을 암호화한 비접촉식 카드는 실제로 신뢰할 수 있다. 또한 제1 및 제2 세션 키를 파생하는 데 사용된 카운터 값은 진정한 것으로 나타날 수 있으며 인증 작업을 수행하는 데 사용될 수 있다.

[0224] 그 후 2 개의 파생된 세션 키는 폐기되고 데이터 교환의 다음 반복은 카운터 값을 업데이트할 것이며(블록 1110으로 되돌아가서) 세션 키의 신규 세트가 생성될 수 있다(블록 1120에서). 일부 실시예에서 조합된 랜덤 데이터는 폐기될 수 있다.

[0225] 본 명세서에 설명된 시스템 및 방법의 예시적인 실시형태는 보안 요인 인증을 제공하도록 형상화될 수 있다. 보안 요인 인증은 다수의 프로세스를 포함할 수 있다. 보안 요인 인증의 일부로서 제1 프로세스는 로그인하는 것과 디바이스 상에서 실행되는 하나 이상의 응용프로그램을 통해 사용자를 검증하는 것을 포함할 수 있다.

[0226] 제2 프로세스로서 사용자는 하나 이상의 응용프로그램을 통한 제1 프로세스의 성공적인 로그인 및 검증에 응답하여, 하나 이상의 비접촉식 카드와 관련된 하나 이상의 행동에 관여한다. 사실상 보안 요인 인증은 사용자의 신원을 안전하게 증명하고 비접촉식 카드와 관련된 하나 이상의 탭 제스처를 포함하지만 이에 제한되지 않는 하나 이상의 유형의 행동에 참여하는 것을 모두 포함할 수 있다.

[0227] 일부 실시예에서 하나 이상의 탭 제스처는 사용자에 의한 디바이스로의 비접촉식 카드의 탭을 포함할 수 있다. 일부 실시예에서 디바이스는 모바일 디바이스, 키오스크, 단말기, 태블릿 또는 수신된 탭 제스처를 처리하도록 형상화 된 임의의 다른 디바이스를 포함할 수 있다.

[0228] 일부 실시예에서 비접촉식 카드는 커피와 같은 구매에 응답하는 거래 항목을 수신함에 따라 검증과 신원 확인을 위해 하나 이상의 컴퓨터 키오스크 또는 단말기와 같은 디바이스에 탭 될 수 있다. 비접촉식 카드를 사용하면 로열티 프로그램에서 신원을 증명하는 안전한 방법을 설정할 수 있다. 예를 들어 보상, 쿠폰, 제안 등을 획득하기 위해 신원을 안전하게 증명하거나 혜택을 받는 것은 단순히 바 카드를 스캔하는 것과는 다른 방식으로 설정된다.

[0229] 예를 들어 하나 이상의 탭 제스처를 처리하도록 형상화된 비접촉식 카드와 디바이스 간에 암호화된 트랜잭션이 발생할 수 있다. 상기 설명한 바와 같이 하나 이상의 응용프로그램은 사용자의 신원을 확인한 후 예를 들어 하나 이상의 탭 제스처를 통해 사용자가 이에 따라 행동하거나 응답하도록 형상화될 수 있다. 일부 실시예에서 예를 들어 보너스 포인트, 로열티 포인트, 보상 포인트, 건강 관리 정보 등과 같은 데이터가 비접촉식 카드에 다시 기록될 수 있다.

[0230] 일부 실시예에서 비접촉식 카드는 모바일 디바이스와 같은 디바이스에 탭 될 수 있다. 상기 설명한 바와 같이 사용자의 신원은 하나 이상의 응용프로그램에 의해 검증될 수 있으며 그 후 신원 검증에 기초하여 사용자에게 원하는 혜택을 부여할 수 있다.

[0231] 일부 실시예에서 비접촉식 카드는 모바일 디바이스와 같은 디바이스를 탭 함으로써 활성화될 수 있다. 예를 들어 비접촉식 카드는 NFC 통신을 통해 디바이스의 카드 리더기를 통해 디바이스의 응용프로그램과 통신할 수 있다. 디바이스의 카드 판독기에 근접한 카드의 탭을 통한 통신은 디바이스의 응용프로그램이 비접촉식 카드와 관련된 데이터를 읽고 카드를 활성화하도록 허용한다.

[0232] 일부 실시예에서 활성화는 다른 기능 예를 들어 구매, 계정 또는 제한된 정보로의 접근 또는 다른 기능 수행에 사용될 수 있도록 카드를 승인할 수 있다. 일부 실시예에서 탭은 디바이스의 응용프로그램을 활성화하거나 시작한 다음 비접촉식 카드를 활성화하기 위해 하나 이상의 서버와 하나 이상의 작동 또는 통신을 시작할 수 있다.

[0233] 응용프로그램이 디바이스에 설치되어 있지 않은 경우 카드 판독기 근처에 있는 비접촉식 카드를 탭 하여 응용프로그램의 다운로드 페이지 탐색과 같은 응용프로그램 다운로드가 시작될 수 있다. 설치 후 비접촉식 카드를 탭 하여 응용프로그램을 활성화하거나 시작한 다음 예를 들어 응용프로그램 또는 기타 백-엔드 통신을 통해 비접촉식 카드 활성화를 시작할 수 있다. 활성화 후 비접촉식 카드는 상업 거래를 포함하나 이에 한정되지 않는 다양한 활동에 사용될 수 있다.

[0234] 일부 실시형태에서 전용 응용프로그램은 비접촉식 카드의 활성화를 수행하기 위해 클라이언트 디바이스에서 실행되도록 형상화될 수 있다. 다른 실시형태에서 웹 포털, 웹-기반 앱, 애플릿 등이 활성화를 수행할 수 있다. 활성화는 클라이언트 디바이스에서 수행될 수 있거나, 클라이언트 디바이스는 비접촉식 카드와 외부 디바이스(예: 계정 서버) 사이를 이동하는 역할만 할 수 있다.

[0235]

[0236] 일부 실시형태에 따르면 활성화 제공에서 응용프로그램은 활성화를 수행하는 디바이스의 유형(예를 들어 개인용 컴퓨터, 스마트폰, 태블릿 또는 POS(point-of-sale) 디바이스)을 계정 서버에 표시할 수 있다. 또한 응용프로그램은 관련된 디바이스의 유형에 따라 계정 서버에 상이한 및/또는 추가적인 데이터를 전송을 위해 출력할 수 있다.

[0237] 예를 들어 이러한 데이터는 판매자 유형, 판매자 ID와 같은 판매자와 관련된 정보 및 POS 데이터 및 POS ID와 같은 디바이스 유형 자체와 관련된 정보를 포함할 수 있다.

[0238] 일부 실시형태에서 예시적인 인증 통신 프로토콜은 트랜잭션 카드와 POS 디바이스 사이에서 일반적으로 수행되는 EMV 표준의 오프라인 동적 데이터 인증 프로토콜을 일부 수정하여 모방할 수 있다.

[0239] 예를 들어 예시적인 인증 프로토콜은 카드 발급사/결제 프로세서 자체로 결제 거래를 완료하는 데 사용되지 않기 때문에 일부 데이터 값이 필요하지 않으며 카드 발급사와의 실시간 온라인 연결/지불 프로세서 없이 인증을 수행할 수 있다.

[0240] 당 업계에 알려진 바와 같이, POS(Point of Sale) 시스템은 거래 금액을 포함하여 거래를 카드 발급자에게 제출한다. 발급자가 거래를 승인 또는 거부하는지 여부는 카드 발급자가 거래 금액을 인식하는지 여부에 따라 달라질 수 있다. 한편 본 명세서의 특정 실시형태에서 모바일 디바이스로부터 발생하는 트랜잭션은 POS 시스템과 관련된 트랜잭션 값이 부족하다.

[0241] 따라서 일부 실시형태에서 더미 트랜잭션 값(즉 카드 발급자가 인식할 수 있고 활성화가 발생하는 데 충분한 값)이 예시적인 인증 통신 프로토콜의 일부로서 통과될 수 있다. POS 기반 거래는 거래 시도 횟수(예: 거래 카운터)에 따라 거래를 거부할 수도 있다.

[0242] 버퍼 값을 넘어서 여러 번 시도하면 완곡한 거절; 거래를 수락하기 전에 추가 검증을 요구하는 완곡한 거절이 발생할 수 있다. 일부 실시형태에서 거래 카운터에 대한 버퍼 값은 정당한 거래의 거절을 피하기 위해 수정될 수 있다.

[0243] 일부 실시예에서 비접촉식 카드는 수신 디바이스에 따라 선택적으로 정보를 전달할 수 있다. 탭 하면 비접촉식 카드는 탭이 향하는 디바이스를 인식할 수 있으며 이러한 인식을 기반으로 비접촉식 카드는 해당 디바이스에 적절한 데이터를 제공할 수 있다. 이것은 비접촉식 카드가 결제 또는 카드 인증과 같은 즉각적인 행동 또는 거래를 완료하는 데 필요한 정보만을 전송하는 것을 유리하게 허용한다.

[0244] 데이터 전송을 제한하고 불필요한 데이터의 전송을 방지함으로써 효율성과 데이터 보안을 모두 향상시킬 수 있다. 정보의 인식 및 선택적 통신은 카드 활성화, 잔액 이체, 계정 액세스 시도, 상업 거래 및 단계별 사기 감소를 포함한 다양한 시나리오에 적용될 수 있다.

[0245] 비접촉식 카드 탭이 Apple의 iOS® 운영체제를 실행하는 기기(예: 아이폰, 아이팟 또는 아이패드)로 향하는 경우 비접촉식 카드는 iOS® 운영체제를 인식하고 이 기기와 통신하는 데 적합한 데이터를 전송할 수 있다. 예를 들어 비접촉식 카드는 예를 들어 NFC를 통해 NDEF 태그를 사용하여 카드를 인증하는 데 필요한 암호화된 식별 정보를 제공할 수 있다.

[0246] 마찬가지로 비접촉식 카드 탭이 Android® 운영 체제를 실행하는 디바이스(예: Android® 스마트폰 또는 태블릿)로 향하는 경우 비접촉식 카드는 Android® 운영 체제를 인식하고 적절한 데이터(예: 본 명세서에 설명된 방법에 따른 인증에 필요한 암호화된 식별 정보)를 전송하여 이 디바이스와 통신할 수 있다.

[0247] 또 다른 실시예로서 비접촉식 카드 탭은 키오스크, 체크아웃 등록기, 지불 스테이션 또는 기타 단말기를 포함하나 이에 제한되지 않는 POS 디바이스로 향할 수 있다. 탭이 실행되면 비접촉식 카드가 POS 디바이스를 인식하고 작동 또는 거래에 필요한 정보 만 전송할 수 있다.

[0248] 예를 들어 상거래를 완료하는 데 사용되는 POS 디바이스가 인식되면 비접촉식 카드는 EMV 표준에 따라 거래를 완료하는 데 필요한 결제 정보를 전달할 수 있다.

[0249] 일부 실시예에서 거래에 참여하는 POS 디바이스는 비접촉식 카드에 의해 제공되는 추가 정보, 예를 들어 디바이스 특정 정보, 위치 특정 정보 및 거래 특정 정보를 요구하거나 지정할 수 있다. 예를 들어 POS 디바이스가 비접촉식 카드로부터 데이터 통신을 수신하면 POS 디바이스는 비접촉식 카드를 인식하고 작업 또는 거래를 완료하는 데 필요한 추가 정보를 요청할 수 있다.

[0250] 일부 실시예에서 POS 디바이스는 특정 비접촉식 카드에 익숙하거나 특정 비접촉식 카드 거래를 수행하는 데 익숙한 승인된 판매자 또는 기타 엔티티와 제휴할 수 있다. 그러나 설명된 방법의 수행을 위해서는 그러한 제휴가 필요하지 않음을 이해해야 한다.

[0251] 쇼핑 상점, 식료품점, 편의점 등과 같은 일부 실시예에서 비접촉식 카드는 응용프로그램을 오픈하지 않고도 모바일 디바이스에 탭 하여 하나 이상의 구매에 대한 보상 포인트, 로열티 포인트, 쿠폰, 제안 등 하나 이상을 활용하려는 요구 또는 의도를 표시할 수 있다.

[0252] 일부 실시예에서 하나 이상의 응용프로그램은 비접촉식 카드의 하나 이상의 탭 제스처를 통해 도입되었음을 결정하도록 형상화될 수 있다. 즉 도입은 오후 3시 51 분에 발생하고 사용자의 신원을 검증하기 위한 트랜잭션은 3시 56분에 발생한다.

[0253] 일부 실시예에서 하나 이상의 응용프로그램은 하나 이상의 탭 제스처에 응답하는 하나 이상의 동작을 제어하도록 형상화될 수 있다. 예를 들어 하나 이상의 동작은 보상 수집, 포인트 수집, 가장 중요한 구매 결정, 최소 비용 구매 결정 및/또는 실시간으로 다른 동작으로 재구성하는 것을 포함할 수 있다.

[0254] 일부 실시예에서 생체 인식/제스처 인증으로서 탭 동작에 대해 데이터가 수집될 수 있다. 예를 들어 암호화로써 안전하고 도청에 취약하지 않은 고유 식별자가 하나 이상의 백-엔드 서비스로 전송될 수 있다. 고유 식별자는 개인에 대한 2차 정보를 조회하도록 형상화될 수 있다. 2차 정보는 사용자에 대한 개인 식별 정보를 포함할 수 있다. 일부 실시예에서 2차 정보는 비접촉식 카드 내에 저장될 수 있다.

[0255] 일부 실시예에서 디바이스는 청구서를 분할하거나 다수의 개인 간에 지불을 확인하는 응용프로그램을 포함할 수 있다. 예를 들어 각 개인은 비접촉식 카드를 소유하고 동일한 발급 금융 기관의 고객일 수 있으나 반드시 필요한 것은 아니다. 각 개인은 구매를 분할하기 위해 자신의 디바이스에서 응용프로그램을 통해 푸시 알림을 받을 수 있다.

[0256] 결제를 표시하기 위해 한 번의 카드 탭만 허용하는 대신 다른 비접촉식 카드를 사용할 수도 있다. 일부 실시예에서 카드를 탭 하는 개인으로부터 하나 이상의 지불 요청을 시작하기 위한 정보를 제공하기 위해 다른 금융 기관을 보유한 개인은 비접촉식 카드를 소유할 수 있다.

[0257] 다음의 예시적인 사용 사례는 본 명세서의 특정 실시형태의 실시예를 설명한다. 이는 제한하려는 목적이 아니며 설명의 목적으로만 사용된다. 어떤 경우에는 첫 번째 친구(지급인)가 두 번째 친구(수취인)에게 돈을 빚지고 있다. 지급인은 ATM으로 이동하거나 P2P 응용프로그램을 통한 교환을 요구하는 대신 비접촉식 카드를 사용하여 수취인의 스마트폰(또는 기타 디바이스)을 통해 결제하기를 원한다.

[0258] 수취인이 스마트폰의 해당 응용프로그램에 로그온하고 결제 요청 옵션을 선택한다. 이에 대한 응답으로 응용프로그램은 수취인의 비접촉식 카드를 통해 인증을 요청한다. 예를 들어 응용프로그램은 수취인이 자신의 비접촉식 카드를 탭 하도록 요청하는 디스플레이를 출력한다. 수취인이 응용프로그램이 활성화된 상태에서 스마트폰 화면에 비접촉식 카드를 탭 하면 비접촉식 카드를 읽고 검증한다.

[0259] 다음으로 응용프로그램은 지급인이 비접촉식 카드를 탭 하여 결제를 보내라는 메시지를 표시한다. 지급인이 자신의 비접촉식 카드를 탭 하면 응용프로그램은 카드 정보를 읽고 관련 프로세서를 통해 지급인의 카드 발급사에게 지불 요청을 전송한다. 카드 발급사는 거래를 처리하고 거래의 상태 표시기를 스마트폰으로 전송한다. 그 후 응용프로그램은 트랜잭션의 상태 표시기를 나타내기 위해 출력한다.

[0260] 또 다른 실시예의 경우 신용카드 고객은 우편으로 새 신용카드(또는 직불카드, 기타 결제카드 또는 활성화가 필요한 다른 카드)를 받을 수 있다. 카드 발급사와 관련된 제공된 전화 번호로 전화를 걸거나 웹 사이트를 방문하여 카드를 활성화하는 대신에 고객은 자신의 디바이스(예: 스마트폰과 같은 모바일 디바이스)의 응용프로그램을 통해 카드를 활성화할 수 있다.

[0261] 고객은 디바이스의 디스플레이에 표시되는 응용프로그램 메뉴에서 카드 활성화 기능을 선택할 수 있다. 응용프로그램은 고객에게 자신의 신용카드를 화면에 대해 탭 하라는 메시지를 표시할 수 있다. 디바이스 화면에 신용카드를 탭 하면 응용프로그램이 고객의 카드를 활성화하는 카드 발급 서버와 같은 서버와 통신하도록 형상화될 수 있다. 그러면 응용프로그램이 카드의 성공적인 활성화를 나타내는 메시지를 나타낼 수 있다. 그 후 카드 활성화가 완료된다.

[0262] 도 12는 예시적인 실시형태에 따른 카드 활성화를 위한 방법(1200)을 도시한다. 예를 들어 카드 활성화는 카드, 디바이스 및 하나 이상의 서버를 포함하는 시스템에 의해 완료될 수 있다. 비접촉식 카드, 디바이스 및 하나 이상의 서버는 비접촉식 카드(105), 클라이언트 디바이스(110)및 서버(120)와 같이 도 1a, 도 1b, 도 5a 및 도 5b를 참조하여 앞에서 설명한 동일하거나 유사한 컴포넌트를 참조할 수 있다.

[0263] 블록 1210에서 카드는 데이터를 동적으로 생성하도록 형상화될 수 있다. 일부 실시예에서 이러한 데이터는 카드에서 디바이스로 전송될 수 있는 계좌 번호, 카드 식별자, 카드 검증 값 또는 전화 번호와 같은 정보를 포함할 수 있다. 일부 실시예에서 데이터의 하나 이상의 부분은 여기에 개시된 시스템 및 방법을 통해 암호화될 수 있다.

[0264] 블록 1220에서 동적으로 생성된 데이터의 하나 이상의 부분이 NFC 또는 다른 무선 통신을 통해 디바이스의 응용프로그램에 전달될 수 있다.

[0265] 예를 들어 디바이스에 근접한 카드의 탭은 디바이스의 응용프로그램이 비접촉식 카드와 관련된 데이터의 하나

이상의 부분을 판독하게 할 수 있다. 일부 실시예에서 디바이스가 카드의 활성화를 지원하는 응용프로그램을 포함하지 않는 경우, 카드의 탭은 카드를 활성화하기 위해 연관된 응용프로그램을 다운로드 하도록 디바이스를 지시하거나 고객을 소프트웨어 응용프로그램 스토어로 프롬프트 할 수 있다.

[0266] 일부 실시예에서 사용자는 디바이스의 표면에 비스듬히 또는 평평하게 배치되거나 디바이스 표면에 가깝게 배치되는 것과 같이 디바이스의 표면을 향해 카드를 충분하게 제스처, 배치 또는 배향하도록 프롬프트 될 수 있다. 카드의 충분한 제스처, 배치 및/또는 배향에 응답하여 디바이스는 카드로부터 수신된 데이터의 하나 이상의 암호화된 부분을 하나 이상의 서버로 전송하도록 진행할 수 있다.

[0267] 블록 1230에서 데이터의 하나 이상의 부분은 카드 발급자 서버와 같은 하나 이상의 서버로 전달될 수 있다. 예를 들어 데이터의 하나 이상의 암호화된 부분이 카드 활성화를 위해 디바이스에서 카드 발급자 서버로 전송될 수 있다.

[0268] 블록 1240에서 하나 이상의 서버는 본 명세서에 개시된 시스템 및 방법을 통해 데이터의 하나 이상의 암호화된 부분을 복호화할 수 있다. 예를 들어 하나 이상의 서버는 디바이스로부터 암호화된 데이터를 수신할 수 있으며 수신된 데이터를 비교하여 하나 이상의 서버에 액세스 가능한 데이터를 기록하기 위해 이를 복호화할 수 있다.

[0269] 하나 이상의 서버에 의한 데이터의 하나 이상의 복호화된 부분을 비교한 결과가 성공적으로 일치하면 카드가 활성화될 수 있다. 하나 이상의 서버에 의한 데이터의 하나 이상의 복호화된 부분을 비교한 결과가 일치하지 않으면 하나 이상의 프로세스가 발생할 수 있다.

[0270] 예를 들어 일치하지 않는다는 결정에 응답하여 사용자는 카드를 다시 탭 하거나 스와이프 하거나 손을 흔들도록 프롬프트 될 수 있다. 이 경우에 사용자가 카드를 활성화할 수 있는 시도 횟수를 포함하는 미리 결정된 임계 값이 존재할 수 있다.

[0271] 대안적으로 사용자는 카드 검증 시도가 실패했음을 나타내는 디바이스 상의 메시지, 카드 활성화를 지원하기 위한 연관된 서비스 또는 다른 알림의 전화, 이메일 또는 문자, 카드 검증 시도가 실패했음을 나타내는 디바이스 상의 전화, 카드 활성화를 지원하기 위한 연관된 서비스 또는 다른 알림의 전화, 이메일 또는 문자, 카드 검증 시도가 실패했음을 나타내는 디바이스 상의 이메일, 카드 활성화를 지원하기 위한 연관된 서비스의 전화, 이메일 또는 문자와 같은 알림을 수신할 수 있다.

[0272] 블록 1250에서 하나 이상의 서버는 카드의 성공적인 활성화에 기초하여 리턴 메시지를 전송할 수 있다. 예를 들어 디바이스는 하나 이상의 서버에 의한 카드의 성공적인 활성화를 나타내는 하나 이상의 서버로부터 출력을 수신하도록 형상화될 수 있다.

[0273] 디바이스는 카드의 성공적인 활성화를 나타내는 메시지를 표시하도록 형상화될 수 있다. 카드가 활성화되면 부정 사용을 방지하기 위해 데이터를 동적으로 생성하는 것을 중단하도록 카드를 형상화시킬 수 있다. 이러한 방식으로 그 후에 카드는 활성화되지 않으며 하나 이상의 서버에 카드가 이미 활성화되었음을 통지한다.

[0274] 또 다른 실시예에서 고객은 자신의 휴대폰에서 자신의 금융 계정에 액세스 하려고 한다. 고객은 모바일 디바이스에서 응용프로그램(예: 은행 응용프로그램)을 실행하고 사용자 이름과 비밀번호를 입력한다. 이 단계에서 고객은 1 단계 계정 정보(예: 최근 구매)를 보고, 1 단계 계정 옵션(예: 신용카드 지불)을 수행할 수 있다.

[0275] 그러나 사용자가 2 단계 계정 정보(예: 지출 한도)에 액세스 하거나 2 단계 계정 옵션(예: 외부 시스템으로 이전)을 수행하려는 경우에는 2 단계 인증이 있어야 한다. 이에 따라 응용프로그램은 계정 검증을 위해 사용자가 거래 카드(예: 신용카드)를 제공하도록 요청한다.

[0276] 사용자는 자신의 신용카드를 모바일 디바이스에 탭 하고 응용프로그램은 신용카드가 사용자의 계정에 해당하는지 검증한다. 그 후 사용자는 2 단계 계정 데이터를 보거나 2 단계 계정 기능을 수행할 수 있다.

[0277] 일부 실시예에서 본 명세서에 설명된 시스템 및 방법은 예를 들어 FIDO2 인증을 개시하는 사용자의 신원을 확인함으로써 FIDO2 프레임워크를 보충하기 위해 적용될 수 있다. FIDO2 프레임워크의 취약점은 FIDO2 인증 프로세스를 수행하려는 사용자의 신원입니다. FIDO2 프레임 워크를 통해 자격 증명을 등록하고 인증하려는 사용자가 자신이 주장하고 인증을 받을 권한이 있는 사용자임을 확인함으로써 FIDO2 프레임 워크의 보안이 향상되고 권한이 없는 사용자가 제외될 수 있다. 다른 실시예에서 여기에 설명된 시스템 및 방법은 WebAuthn, CTAP FIDO, 또는 다른 인증 구현을 보완하기 위해 적용될 수 있다. 본 발명은 임의의 인증 구현에 적용될 수 있으며 본 발명은 FIDO2 프레임 워크에 제한되지 않음을 이해하여야 한다.

[0278] 본 명세서에 설명된 바와 같이, 본 발명의 실시예는 비접촉식 카드와 클라이언트 디바이스 간에 데이터 전송을 위한 시스템 및 방법을 제공한다. 하나의 실시예에서 비접촉식 카드 및 클라이언트 디바이스 각각은 마스터 키를 포함할 수 있다. 비접촉식 카드는 마스터 키를 이용하여 다양화 키를 생성할 수 있으며, 카운터 값을 클라이언트 디바이스로 전송하기 전에 카운터 값을 보호할 수 있다. 클라이언트 디바이스는 마스터 키와 카운터 값을 기반으로 다양화 키를 생성할 수 있다. FIDO 개인 키는 해당 FIDO 공개 키를 포함하는 클라이언트 디바이스와 서버 간의 FIDO 거래를 용이하게 할 수 있다. 추가 실시예로서, 클라이언트 디바이스는 고유한 공개 및 개인 키 쌍을 무작위로 생성할 수 있으며 클라이언트 디바이스는 마스터 키 및 사용 가능한 식별 정보(예: 서비스 공급자와 관련된 웹 사이트에 대한 사이트 식별자)를 사용하여 하나 이상의 다양화 키를 생성할 수 있다.

[0279] 예시적인 실시형태에서, 본 명세서에 개시된 데이터 전송 시스템은 FIDO 시스템에서 구현될 수 있다. FIDO 시스템은 클라이언트 디바이스 및 서비스 제공자와 관련된 서버를 포함할 수 있다. 클라이언트 디바이스는 FIDO 개인 키를 저장할 수 있고 서버는 FIDO 개인 키와 관련된 FIDO 공개 키를 저장할 수 있다. 예를 들어, 사용자가 서비스 제공자에 계정을 등록하면 클라이언트 디바이스는 FIDO 공개 키 개인 키 쌍을 생성 수 있다. 클라이언트 디바이스는 FIDO 개인 키를 저장하고 FIDO 공개 키를 서비스 제공자의 서버로 전송할 수 있다. 그 후 사용자는 FIDO 개인 키를 사용하여 챌린지에 서명하는 등의 방법으로 계정에 로그인할 수 있다. 서버는 서명 할 클라이언트 디바이스에 챌린지를 제공할 수 있다. 예를 들어, 서버는 사용자에게 긴 랜덤(random) 숫자 또는 긴 랜덤 문자열을 제공할 수 있다. 클라이언트 디바이스는 랜덤 숫자 또는 랜덤 문자를 수신하고 FIDO 개인 키를 사용하여 서명할 수 있다. 또한 클라이언트 디바이스는 서명된 난수를 서버로 전송할 수 있다.

[0280] 서버는 FIDO 공개 키를 사용하여 서명된 챌린지를 확인하고 서명된 챌린지가 원래 챌린지와 일치하는 경우에만 사용자가 계정에 액세스하도록 허용할 수 있다. 예를 들어 서버는 챌린지의 암호화 해시를 수행한 다음 FIDO 공개 키를 사용하여 해시를 확인할 수 있다. 서버가 서버에 저장된 FIDO 공개 키를 사용하여 긴 난수를 확인하여 클라이언트 디바이스에 전송된 것과 동일한 난수 또는 문자를 확인하면 서버는 사용자에게 액세스 권한을 부여할 수 있다. 그렇지 않으면 클라이언트 디바이스(또는 사용자)에 대한 액세스가 거부될 수 있다.

[0281] 하나의 예시적인 실시형태에서, FIDO 개인 키는 실시예에서 FIDO 인증자로서 기능할 수 있는 클라이언트 디바이스에 잠겨 있다. FIDO 개인 키는 클라이언트 디바이스의 보안 요소에 저장될 수 있으며, FIDO 개인 키는 사용자가 클라이언트 디바이스에서 FIDO 개인 키를 잠금 해제한 후에만 사용할 수 있다. 클라이언트 디바이스는 사용자 작업에 의해 FIDO 개인 키를 잠금 해제할 수 있다. 예를 들어, 사용자 동작은 손가락 스와이프, PIN 입력, 마이크에 대고 말하기, 제2 요인 디바이스 삽입 또는 버튼 누르기 일 수 있다.

[0282] 제2 요인 디바이스는 비접촉식 카드 일 수 있다. 일부 실시형태에서 서버는 개인 키를 완성하는 데 필요한 정보를 제공할 수 있으므로 권한이 없는 방식으로 액세스되거나 생성된 경우에도 개인 키를 사용할 수 없다. 이 정보에는 예를 들어 개인 키 자체의 일부, 개인 키를 생성하는 데 사용되는 마스터 키의 일부 또는 서버에서 사용할 수 있는 기타 데이터가 포함될 수 있다. 일부 실시형태에서 개인 키는 서버에 의해 제공되는 정보에 기초하여 반복적으로 생성될 수 있다. 다른 실시형태에서 제2 요인 디바이스부터의 입력을 필요로 하거나 제2 요인 디바이스의 사용시에만 잠금 해제되는 정보가 제공될 수 있다(예를 들어, 제2 요인 디바이스를 포함하는 사용자 동작에 의해).

[0283] 또 다른 예시적인 실시형태에서 서버는 카운터 값을 클라이언트 디바이스로 전송할 수 있다. 예를 들어, 서버는 비접촉식 카드의 거래를 추적할 수 있다. 비접촉식 카드가 거래를 수행할 때마다 서버는 카운터 값을 미리 정해진 숫자만큼 증가시킬 수 있다. 비접촉식 카드는 또한 비접촉식 카드가 서버와 관련하여 거래를 수행할 때마다 카운터 값을 증가시킬 수 있다. FIDO 거래 동안, 예를 들어 클라이언트 디바이스가 챌린지에 서명할 때 서버는 카운터 값을 클라이언트 디바이스로 전송할 수 있다. 이에 따라 비접촉식 카드와 클라이언트 디바이스가 암호화된 FIDO 개인 키를 송수신 할때 동일한 카운터 값을 가질 수 있다.

[0284] 도 13은 예시적인 실시형태에 따른 데이터 전송 시스템을 사용하는 FIDO 시스템(1300)을 나타낸다. 예시적인 실시형태에서, FIDO 시스템(1300)은 서버(1310), 클라이언트 디바이스(1320) 및 비접촉식 카드(1330)를 포함할 수 있다. 서버(1310)는 시스템의 다양한 사용자를 위한 계정 정보를 저장하기 위한 데이터베이스를 포함할 수 있다. 클라이언트 디바이스(1320)는 클라이언트 디바이스(1320)에서의 실행을 위한 명령어를 포함하는 하나 이상의 소프트웨어 응용프로그램과 같은 하나 이상의 응용프로그램을 포함하고 실행할 수 있으며 이는 시스템(1300)의 하나 이상의 컴포넌트와 통신을 가능하게 하고 전송 및 /또는 수신하도록 형상화된다. 여기에 설명된 클라이언트 디바이스 기능을 수행한다. 클라이언트 디바이스(1320)는 다양한 네트워크에 연결되고 NFC 기술을 사용하여 통신을 송수신할 수 있는 스마트폰일 수 있으며 여기에 설명된 기능을 수행하도록 형상화된 하나 이상

의 소프트웨어 응용프로그램을 포함할 수 있다.

[0285] 또 다른 실시형태에서, 클라이언트 디바이스(1320)는 동글(dongle)일 수 있고 다른 실시형태에서 클라이언트 디바이스는 네트워크 가능 컴퓨터 일 수 있다. 비접촉식 카드(1330)는 프로세서, 메모리 및 송신기를 포함할 수 있으며 여기에서 설명하는 비접촉식 카드의 기능을 수행할 수 있다. 서버(1310)는 예를 들어 인터넷과 같은 네트워크를 통해 클라이언트 디바이스(1320)와 통신할 수 있다. 클라이언트 디바이스(1320)는 NFC 기술을 이용하여 비접촉식 카드(1330)로부터 신호를 송수신할 수 있다. 비접촉식 카드(1330)는 비접촉식 카드로 제한되지 않으며, 일부 실시예에서 클라이언트 디바이스(1320)와 동일하거나 유사한 디바이스 일 수 있다는 것이 이해된다.

[0286] 하나의 예시적인 실시형태에서 사용자는 클라이언트 디바이스(1320)의 사용자 인터페이스에서 응용프로그램 또는 웹 사이트를 방문할 수 있다. 응용프로그램은 로그인 버튼(1322) 및 디바이스 설정(1323)을 포함할 수 있는 로그인 페이지(1321)를 디스플레이 할 수 있다. 사용자가 버튼(1322)을 탭 하면, 클라이언트 디바이스(1320)는 FIDO 기술을 사용하여 사용자를 서명할 수 있다. 사용자가 버튼(1323)을 탭 하면 클라이언트 디바이스(1320)는 서비스 제공자에 사용자 계정을 등록하거나 사용자 계정과 관련하여 클라이언트 디바이스(1320)를 등록할 수 있다.

[0287] 예시적인 실시형태에서 사용자는 버튼(1323)을 탭 할 수 있다. 이에 응답하여, 클라이언트 디바이스(1320)는 FIDO 키 쌍, 즉, FIDO 개인 키 및 FIDO 공개 키를 생성할 수 있는 FIDO 인증자 응용프로그램을 활성화할 수 있다. FIDO 키 쌍은 예를 들어 무작위로 생성될 수 있거나, 하나 이상의 다양화 키가 마스터 키를 사용하여 생성될 수 있고 서비스 제공자와 연관된 식별될 수 있다. 다른 실시형태로 마스터 키와 카운터 값을 이용하여 다양화 키를 생성할 수 있다. 클라이언트 디바이스(1320)는 FIDO 개인 키를 저장하고 인터넷과 같은 네트워크를 이용하여 서버(1310)로 FIDO 공개 키를 전송할 수 있다. 서버(1310)가 FIDO 공개 키를 수신하면, 서버(1310)는 FIDO 공개 키를 사용자 계정과 연계하여 데이터베이스에 저장할 수 있다.

[0288] 예시적인 실시형태에서, 사용자는 버튼(1323)을 탭 할 수 있다. 이에 응답하여 클라이언트 디바이스(1320)는 FIDO 키 쌍, 즉, FIDO 개인 키 및 FIDO 공개 키를 생성할 수 있는 FIDO 인증자 응용프로그램을 활성화할 수 있다. FIDO 키 쌍은 예를 들어 무작위로 생성될 수 있거나, 하나 이상의 다양화 키가 마스터 키를 사용하여 생성될 수 있고 서비스 제공자와 연관된 식별될 수 있다. 다른 실시형태로 마스터 키와 카운터 값을 이용하여 다양화 키를 생성할 수 있다. 클라이언트 디바이스(1320)는 FIDO 개인 키를 저장하고 인터넷과 같은 네트워크를 이용하여 서버(1310)로 FIDO 공개 키를 전송할 수 있다. 서버(1310)가 FIDO 공개 키를 수신하면, 서버(1310)는 FIDO 공개 키를 사용자 계정과 연계하여 데이터베이스에 저장할 수 있다.

[0289] 예시적인 실시형태에서 사용자는 버튼(1322)을 탭 할 수 있다. 이에 응답하여, 클라이언트 디바이스(1320)는 서명에 대한 챌린지를 요청하기 위해 신호를 서버(1310)에 전송할 수 있다. 서버(1310)는 챌린지를 클라이언트(1320)로 전송할 수 있다. 챌린지는 예를 들어, 난수의 문자열 일 수 있다. 클라이언트 디바이스(1320)는 또한 비접촉식 카드(1330)로부터 인증을 요청하는 신호를 비접촉식 카드(1330)로 전송할 수 있으며, 인증을 수신하면 클라이언트 디바이스(1320)는 서버(1310)로부터 인증을 중계할 수 있다. 클라이언트 디바이스(1320)에 의해 서버(1310)가 클라이언트 디바이스 (1320)에 저장된 FIDO 개인 키가 잠금 해제될 수 있다.

[0290] 일부 실시형태에서 프록시 인증자는 클라이언트 디바이스(1320) 상에 생성될 수 있다. 예를 들어 프록시 인증자는 인증 프로세스를 개시하고 통신을 설정하기 위해 사용자에게 비접촉식 카드(1330)를 클라이언트 디바이스(1320)에 탭 하도록 프롬프트 할 수 있다. 그러면 서버(1310)는 필요한 인증 프로세스를 수행하고 인증 프로세스의 결과를 클라이언트 디바이스(1320)로 전송할 수 있다. 클라이언트 디바이스(1320)는 서버(1310)와의 상호작용 없이 클라이언트 디바이스 장치(1320)에 의해 생성된 것처럼 결과를 제공할 수 있다. 따라서 프록시 인증자 역할을 한다. 이 프로세스는 서버(1310)에 저장된 하나 이상의 FIDO 개인 키를 잠금 해제하는 데 사용될 수 있다. 챌린지가 수신되면 클라이언트 디바이스(1320)는 챌린지를 서버(1310)로 전달하여 개인 키를 찾고, 챌린지에 필요한 적절한 공개/개인 키 쌍 또는 공개 키를 생성할 수 있다.

[0291] 클라이언트 디바이스(1320)가 FIDO 개인 키를 사용하여 챌린지를 수신하면, 클라이언트 디바이스(1320)는 챌린지에 서명할 수 있으며, 예를 들어 난수 문자열을 암호화할 수 있다. 클라이언트 디바이스(1320)는 서명된 챌린지를 서버(1310)로 전송할 수 있다. 서버(1310)는 FIDO 공개 키를 사용하여 서명된 챌린지를 확인할 수 있다. 확인된 챌린지가 클라이언트 디바이스(1320)로 전송된 챌린지와 동일한 경우, 서버(1310)는 클라이언트 디바이스(1320)(또는 클라이언트 디바이스(1320)의 사용자)를 인증할 수 있다. 확인된 챌린지가 클라이언트 디바이스(1320)로 전송된 챌린지와 동일하지 않은 경우, 서버(1310)는 클라이언트 디바이스(1320)가 서버(1310)(또는 다른 디바이스)에 접근하는 것을 차단할 수 있다.

[0292] 예시적인 실시형태에서 데이터 전송 시스템은 사용자에 대한 온라인 지불을 처리하기 위해 은행에 의해 사용될 수 있다. 은행은 서버를 운영할 수 있고, 사용자는 사용자의 태블릿을 통해 온라인 결제를 요청할 수 있다. 또한 사용자는 은행에서 발급 비접촉식 카드를 소유할 수 있다. 은행이 비접촉식 카드를 발급하면 서버는 사용자를 위해 FIDO 키 쌍을 발급한다. 키 쌍에는 FIDO 개인 키와 FIDO 공개 키가 포함된다. 서버는 FIDO 공개 키를 저장하지만 서버는 FIDO 개인 키를 비접촉식 카드에 저장한다. 태블릿은 하나 이상의 소프트웨어 응용프로그램을 포함할 수 있으며 인터넷을 통해 서버와 통신할 수 있다. 태블릿은 NFC 프로토콜을 사용하여 비접촉식 카드로 신호를 보내고 받을 수도 있다. 온라인 거래의 보안을 강화하기 위해 은행은 고객에게 특정 거래(예: 미리 정해진 결제 금액을 초과하는 결제가 필요한 거래)에 대해 고객의 신원을 확인하도록 요구할 수 있다. 확인은 FIDO 기술을 사용하여 수행될 수 있다. 일부 실시예에서, FIDO 공개 키는 비접촉식 카드와 연관될 수 있다. 이러한 실시예에서, 기본 개인 키 또는 고정 개인 키는 FIDO 인증자를 구현하는 디바이스, 예를 들어 서버 또는 태블릿에 저장될 수 있다.

[0293] 도 14는 온라인 지불을 처리하기 위한 예시적인 흐름도(1400)를 도시한다. 단계 1410에서, 거래는 사용자의 태블릿에서 시작될 수 있다. 예를 들어 사용자는 타사 웹 사이트를 방문하여 다이아몬드 목걸이를 주문할 수 있다. 단계 1420에서, 태블릿은 사용자의 비접촉식 카드 정보(예: 계좌 번호, 계좌 소유자 이름, 계좌 소유자 주소, 보안 코드, 고유 카드 식별자) 및/또는 거래 정보(예 : 금액, 판매자 이름, 판매자 위치, 날짜, 구매한 상품 또는 서비스)를 전송하고 제3자에게 제공하여 거래에 대한 결제를 처리한다. 제3자는 결제 승인을 위해 은행에 연락할 수 있다. 이 예시적인 실시형태에서 다이아몬드 목걸이의 가격은 사용자에 의한 온라인 지불에 대해 정의된 임계 값을 초과하면 은행은 은행이 지불을 처리하기 전에 사용자에게 사용자의 신원을 확인하도록 요구할 수 있다. 이 임계 값은 은행이나 사용자가 정의할 수 있다.

[0294] 단계 1430에서, 태블릿은 은행의 서버로부터 사용자의 신원을 확인하기 위한 챌린지를 수신할 수 있다. 이에 응답하여 단계 1440에서 태블릿에 저장된 응용프로그램(예: 태블릿에 설치된 은행 응용프로그램)이 팝업 창을 띄워 사용자에게 비접촉식 카드를 탭 하도록 요청할 수 있다. 단계 1450에서 사용자는 비접촉식 카드를 태블릿에 탭 할 수 있으며, 이에 따라 태블릿에 FIDO 개인 키 사용 권한이 부여될 수 있다. 단계 1460에서 태블릿은 FIDO 개인 키를 사용하여 챌린지에 서명할 수 있으며, 단계 1470에서 태블릿은 서명된 챌린지를 서버로 전송할 수 있다. 서명된 챌린지를 수신한 서버는 단계 1480에서 사용자의 신원을 확인하고 결제를 승인할 수 있다. 결제가 승인되면 서버는 제3자에게 메시지를 전송할 수 있다. 단계 1490에서, 태블릿은 거래가 처리되었음을 나타내는 메시지를 제3자로부터 수신할 수 있다.

[0295] 도 15는 온라인 지불을 처리하기 위한 클라이언트 디바이스(1320)에 대한 예시적인 사용자 인터페이스를 도시한다. 이 예시적인 실시형태에서, 클라이언트 디바이스(1320)는 체크 아웃 페이지(1510)를 디스플레이 하는 태블릿이다. 이 페이지는 사용자가 선택한 다이아몬드 목걸이와 아이템의 가격을 보여줄 수 있다. 페이지(1510)는 사용자의 신용카드 정보를 입력하기 위한 필드(1520)를 포함할 수 있다. 페이지(1510)는 또한 거래를 처리하기 위한 버튼(1530)을 포함할 수 있다. 사용자가 버튼(1530)을 탭 하면 태블릿은 신용카드 정보를 제3자 공급 업체에 전송할 수 있다. 이 실시예에서 거래 금액이 임계 값을 초과하기 때문에 은행에서 사용자에게 거래 확인을 요구할 수 있다.

[0296] 도 16은 온라인 지불을 확인하기 위한 클라이언트 디바이스(1320)에 대한 예시적인 사용자 인터페이스를 도시한다. 예시적인 실시형태에서 제3자가 지불 처리를 위해 은행에 연락한 후, 은행의 서버는 거래를 확인하기 위해 클라이언트 디바이스 또는 태블릿(1320)에 메시지 또는 통신을 전송할 수 있다. 메시지 또는 통신은 챌린지를 포함하고 태블릿(1320)이 사용자에게 태블릿(1320)에서 사용자의 비접촉식 카드(1330)를 탭 할 것을 요청하는 프롬프트(1610)를 표시하도록 프롬프트 할 수 있다. 이어서 사용자는 태블릿(1320)에서 비접촉식 카드(1330)를 탭 할 수 있고, 비접촉식 카드(1330)는 암호화된 FIDO 개인 키를 태블릿(1320)으로 전송할 수 있다. 태블릿(1320)은 다양화 키를 생성할 수 있으며, 다양화 키를 사용하여 암호화된 FIDO 개인 키를 복호화 할 수 있다. 태블릿(1320)이 FIDO 개인 키를 소유하면, 태블릿(1320)은 챌린지를 은행의 서버로 서명하고 전송할 수 있다.

[0297] 예시적인 하나의 실시형태에서 태블릿(1320)은 은행과 관련된 응용프로그램을 포함할 수 있다. 응용프로그램은 다양한 은행 계좌 정보를 사용자에게 표시할 수 있다. 예를 들어, 응용프로그램은 사용자가 보유하고 있는 각 계정에 대한 계정 잔액을 표시할 수 있다. 응용프로그램은 또한 은행 서버로부터 통신 또는 메시지를 수신하고 사용자에게 태블릿에 프롬프트를 표시할 수 있다. 통신에는 태블릿에 표시될 챌린지 및 메시지가 포함될 수 있다. 응용프로그램이 은행 서버로부터 통신을 수신하면 응용프로그램은 태블릿(1320)의 화면에 프롬프트 또는 창을 표시할 수 있다. 프롬프트 또는 창은 태블릿(1320)에 표시되는 다른 창 또는 페이지에 중첩될 수 있다.

[0298] 본 발명은 FIDO 프레임워크에 대한 엄격한 준수로 제한되지 않으며, 본 발명은 이 프레임워크에 대한 변형을 포함하는 것으로 이해된다. 일부 예시적인 실시형태에서 FIDO 공개 키-개인 키 쌍이 FIDO 인증자에서 생성될 수 있지만 다른 조합도 가능하다. 예를 들어 서버는 FIDO 공개 키-개인 키 쌍을 생성할 수 있으며, 서버는 예를 들어 사용자가 클라이언트 디바이스를 등록하거나 계정을 열기를 원할 때 FIDO 개인 키를 인증자에게 전송할 수 있다. 또 다른 실시예로서 FIDO 공개 키 개인 키 쌍은 비접촉식 카드에 저장될 수 있다. 필요한 경우 FIDO 인증자는 FIDO 공개 또는 FIDO 개인 키를 검색할 수 있다. 예를 들어 클라이언트 디바이스는 FIDO 공개 키를 서버로 전송하여 클라이언트 디바이스를 등록할 수 있으며 클라이언트 디바이스는 서버가 FIDO 개인 키를 검색할 수 있다. 클라이언트 디바이스에 챌린지를 전송한다. 다른 실시예로서 비접촉식 카드로부터 인증 승인을 받으면 FIDO 인증자 자체가 서명 챌린지를 진행하거나 FIDO 등록 완료에 필요한 공개 키를 제공할 수 있다.

[0299] 일부 실시예에서 본 발명은 비접촉식 카드의 탭(tap)에 관한 것이다. 그러나 본 발명은 탭에 한정된 것은 아니고 본 발명은 예를 들면 카드의 흔들림 또는 움직임과 같은 다른 제스처를 포함할 수 있다.

[0300] 명세서 및 청구범위 전체에 걸쳐 다음의 용어는 문맥이 명백하게 달리 지시하지 않는 한 적어도 본 명세서에서 명시적으로 관련된 의미를 취한다. 용어 "또는"은 포괄적인 "또는"을 의미하도록 의도된다. 또한 용어 "a", "an" 및 "the"는 달리 명시되었거나 단수 형태로 지시되는 문맥이 명확하지 않은 한 하나 이상을 의미하는 것으로 의도된다.

[0301] 본 명세서에서 수많은 특정 세부 상세사항이 설명되었다. 그러나 개시된 기술의 실시형태는 이러한 특정 세부사항 없이도 실행될 수 있음을 이해해야 한다. 다른 경우에 잘 알려진 방법, 구조 및 기술은 본 명세서의 이해를 모호하게 하지 않기 위해 자세히 설명하지는 않는다.

[0302] "일부 실시예", "다른 실시예", " 하나의 실시예", "다양한 실시예", "하나의 실시형태", "실시형태", "일부 실시형태", "예시적 실시형태", "다양한 실시형태", "하나의 구현형태", "예시적 구현", "다양한 구현형태", "일부 구현" 등으로 설명된 기술의 구현은 특성, 기능, 구조를 포함할 수 있음을 나타지만 모든 구현형태가 반드시 특성, 기능, 구조를 포함하는 것은 아니다.

[0303] 또한 "하나의 실시예에서", "하나의 실시형태에서" 또는 "하나의 구현형태에서"라는 문구의 반복된 사용은 동일한 실시예 실시형태 또는 구현을 지칭하는 것일 수 있으나 아닐 수도 있다.

[0304] 본 명세서에서 사용된 바와 같이 달리 명시되지 않는 한, 공통 객체를 설명하기 위해 서수 형용사 "첫 번째", "두 번째", "세 번째" 등의 사용은 단지 유사한 물체의 다른 인스턴스가 참조되고 있음을 나타내며 이와 같이 설명된 물체는 시간, 공간, 순위 또는 기타 방식으로 주어진 순서에 있어야 함을 의미한다.

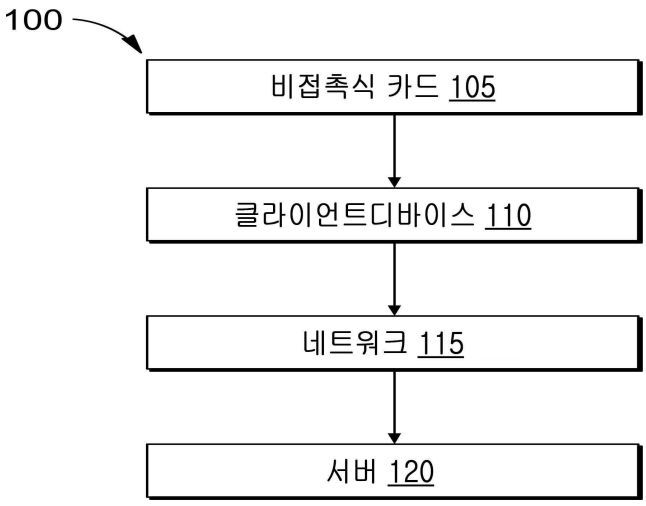
[0305] 개시된 기술의 특정 구현형태가 현재 가장 실용적이고 다양한 구현으로 간주되는 것으로 설명하였으나, 개시된 기술은 개시된 구현 형태에 제한되지 않고 첨부된 청구항의 범위 내에서 다양한 수정 및 균등 배열을 포함하는 것으로 이해된다. 본 명세서에서는 특정 용어가 사용되지만 제한을 목적으로 사용하는 것은 아니며 일반적이고 설명적인 의미로 사용된다.

[0306] 본 기술적 설명은 실시예를 사용하여 최상의 모드를 포함하여 개시된 기술의 특정 구현을 공개하고 또한 당업자로 하여금 본 발명의 디바이스 또는 시스템을 제조 사용하거나 통합된 방법의 실행을 통해 개시된 기술의 특정 구현을 가능케 한다.

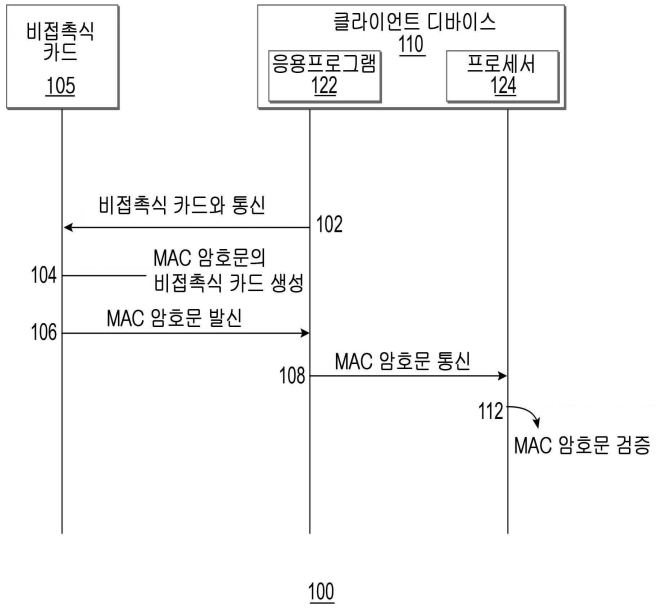
[0307] 개시된 기술의 특정 구현의 가능한 범위는 청구범위로 한정되며, 당업자에게 발생할 수 있는 다른 실시예를 포함할 수 있다. 그러한 다른 실시예는 청구범위의 문언적 의미와 같은 구조적 요소를 지니거나 청구범위의 문언적 의미와 실질적인 차이가 없는 동등한 구조적 요소를 포함하는 경우로 청구범위 내에서 해석된다.

도면

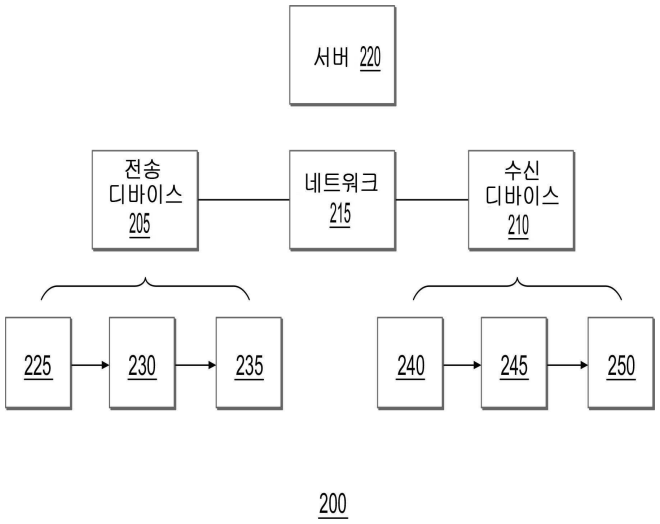
도면1a


100
비접촉식 카드 105
클라이언트디바이스 110
네트워크 115
서버 120

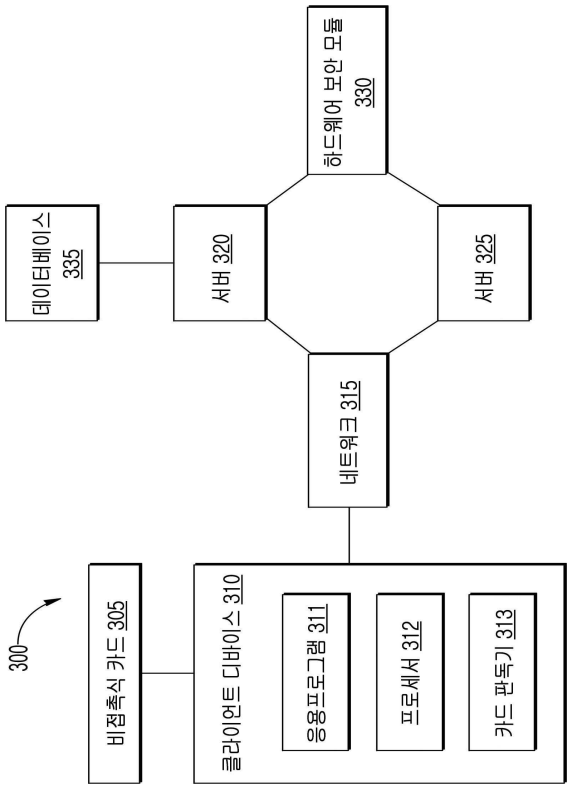
도면1b


비접촉식 카드 105
클라이언트 디바이스 110
응용프로그램 122
프로세서 124
비접촉식 카드와 통신
102
104
MAC 암호문의 비접촉식 카드 생성
106
MAC 암호문 발신
108
MAC 암호문 통신
112
MAC 암호문 검증
100

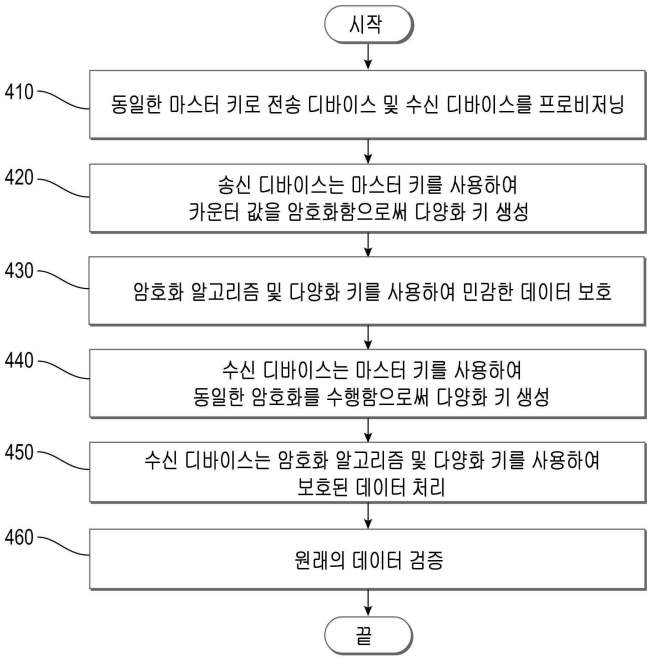
도면2


서버 220
전송 디바이스 205
네트워크 215
수신 디바이스 210
225
230
235
240
245
250
200

도면3

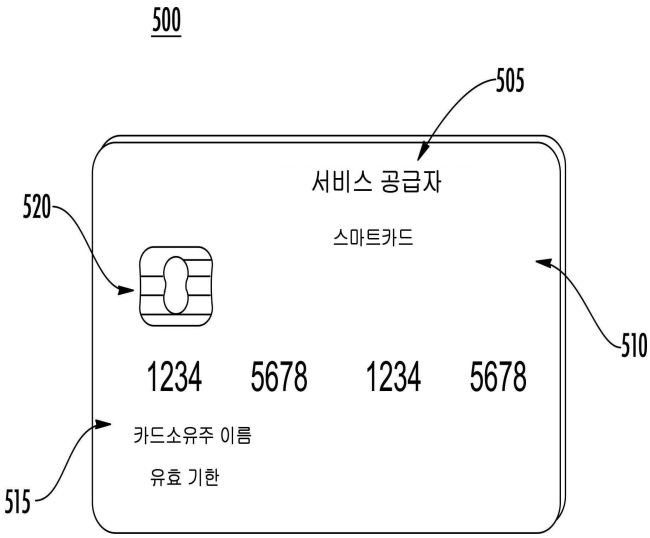

하드웨어 보안 모듈 330
데이터베이스 335
서버 320
서버 325
네트워크 315
300
비접촉식 카드 305
클라이언트 디바이스 310
응용프로그램 311
프로세서 312
카드 판독기 313

도면4

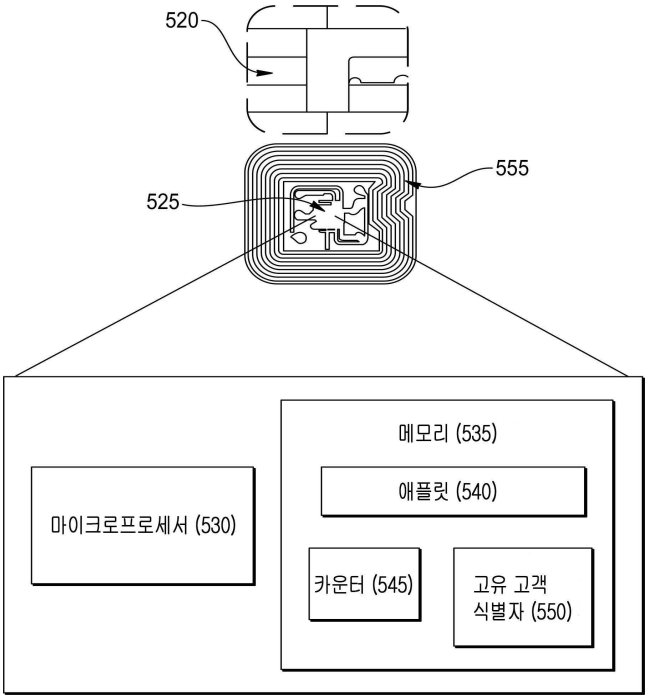

시작
410
동일한 마스터 키로 전송 디바이스 및 수신 디바이스를 프로비저닝
420
송신 디바이스는 마스터 키를 사용하여
카운터 값을 암호화함으로써 다양화 키 생성
430
암호화 알고리즘 및 다양화 키를 사용하여 민감한 데이터 보호
440
수신 디바이스는 마스터 키를 사용하여
동일한 암호화를 수행함으로써 다양화 키 생성
450
수신 디바이스는 암호화 알고리즘 및 다양화 키를 사용하여
보호된 데이터 처리
460
원래의 데이터 검증
끝

400

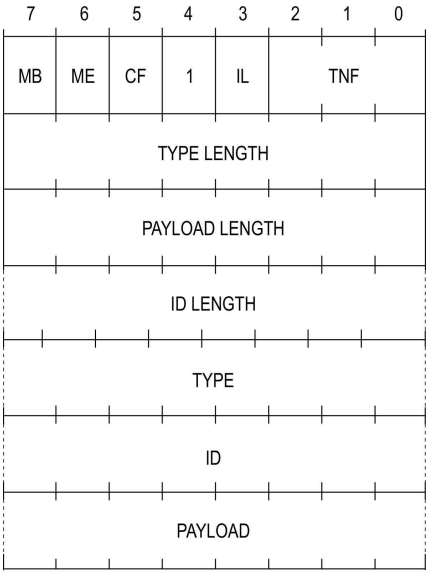
도면5a


500
505
서비스 공급자
520
스마트카드
510
1234 5678 1234 5678
카드소유주 이름
515
유효 기한

도면5b


520
555
525
메모리 (535)
애플릿 (540)
마이크로프로세서 (530)
카운터 (545)
고유 고객
식별자 (550)

도면6


7 6 5 4 3 2 1 0
MB ME CF 1 IL TNF
TYPE LENGTH
PAYLOAD LENGTH
ID LENGTH
TYPE
ID
PAYLOAD

600

도면7

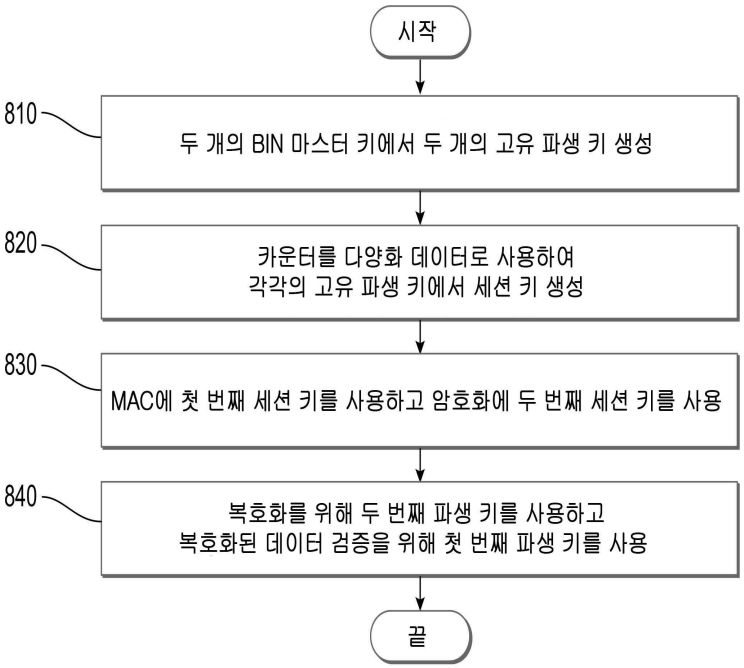
00 D1 (Message Begin, Message End, Short Record, noID length) 01 (well known type) 01 01 Text type
02 <Payload Length including recordID and "EN", or contentlength+3) = 45+3 = 48 (DEC)
03 54 ('T')
04 02 record ID
05 65 6E (language length, 'en')
07 43 01 00 76 a6 62 7b 67 a8 cf bb <eight mac bytes>
D101305402656E 43010076A6627B67A8CFBB <eight mac bytes>

710

VERSION	pUID (8)	pATC	ENCYPHERED CRYPTOGRAM(16)	
0100	0015399555360061	00000050	7D28B8B9D8666E5143153AC9C944E5A6	
DECRYPTED CRYPTOGRAM				
RANDOM (8)	MAC (8)			
4838FB7DC171B89E	CF3F3B8C56DA0BF1			
	MAC(T=[pVERSION (2 BYTES) | | pUID (8 BYTES) | | pATC (4 BYTES) | | pSHSEC (4 BYTES) | | '80' | | '00 00 00 00 00'])			

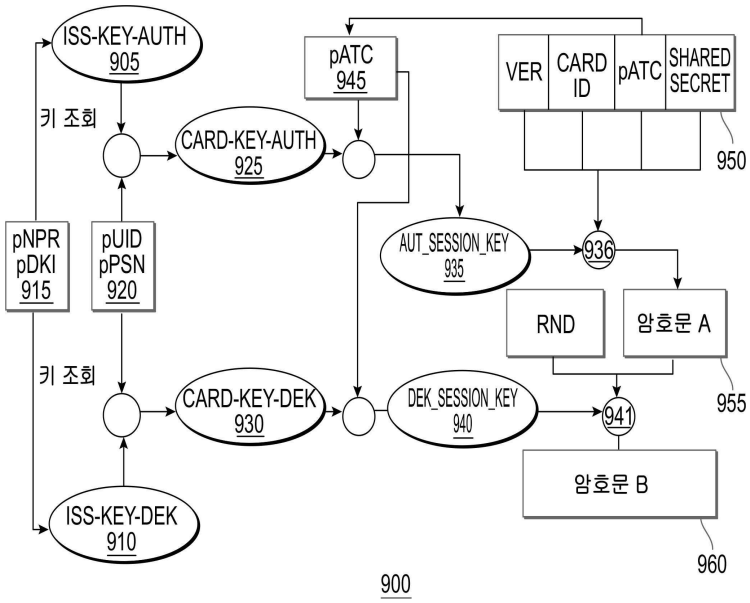
720

도면8

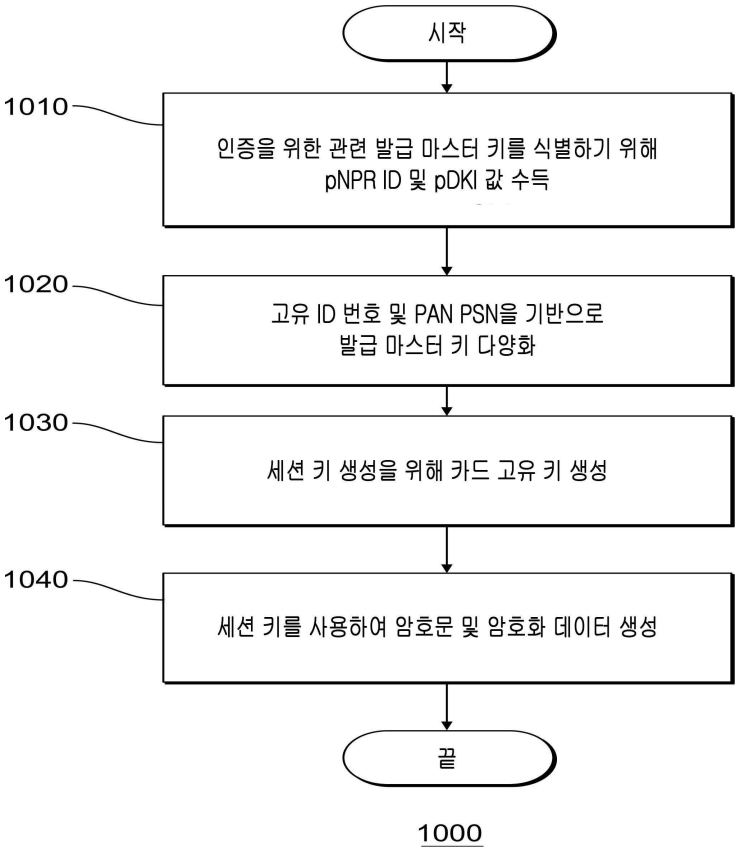


800

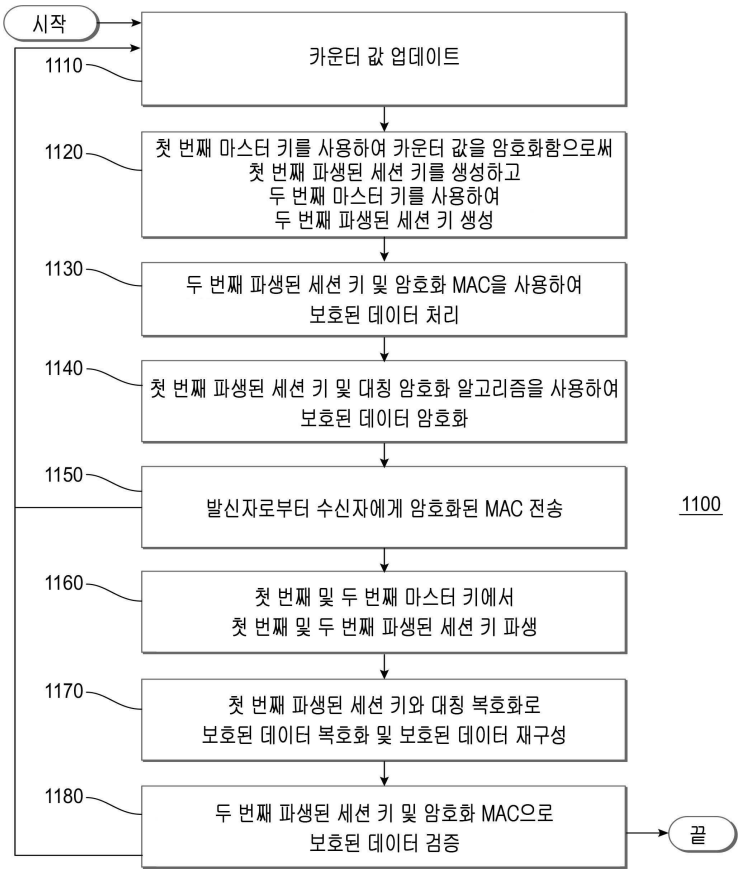
도면9


ISS-KEY-AUTH
905
키 조회
CARD-KEY-AUTH
925
pATC
945
VER
CARD ID
pATC
SHARED SECRET
950
pNPR
pDKI
915
pUID
pPSN
920
AUT_SESSION_KEY
935
936
RND
암호문 A
955
키 조회
CARD-KEY-DEK
930
DEK_SESSION_KEY
940
941
암호문 B
960
ISS-KEY-DEK
910
900

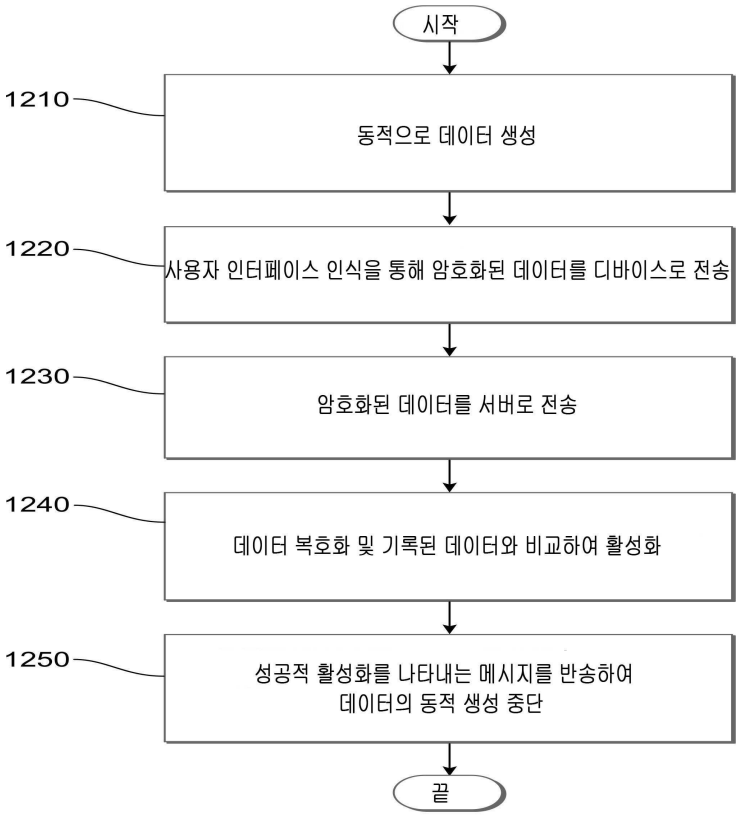
도면10


시작
1010
인증을 위한 관련 발급 마스터 키를 식별하기 위해
pNPR ID 및 pDKI 값 수득
1020
고유 ID 번호 및 PAN PSN을 기반으로
발급 마스터 키 다양화
1030
세션 키 생성을 위해 카드 고유 키 생성
1040
세션 키를 사용하여 암호문 및 암호화 데이터 생성
끝
1000

도면11

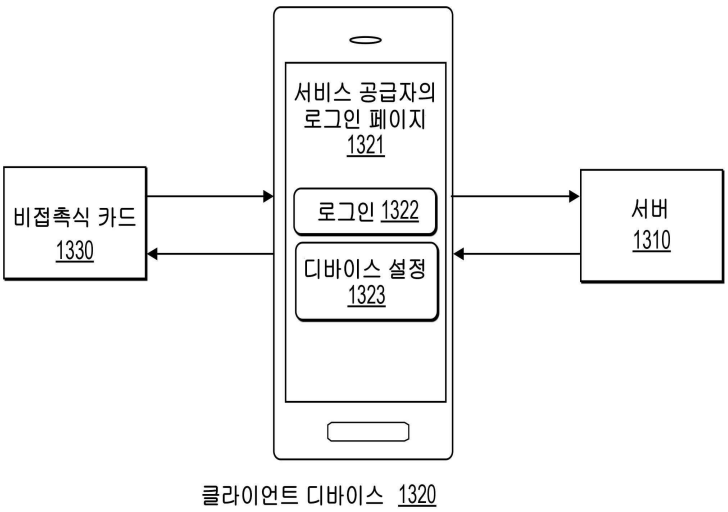

시작
1110
카운터 값 업데이트
1120
첫 번째 마스터 키를 사용하여 카운터 값을 암호화함으로써
첫 번째 파생된 세션 키를 생성하고
두 번째 마스터 키를 사용하여
두 번째 파생된 세션 키 생성
1130
두 번째 파생된 세션 키 및 암호화 MAC을 사용하여
보호된 데이터 처리
1140
첫 번째 파생된 세션 키 및 대칭 암호화 알고리즘을 사용하여
보호된 데이터 암호화
1150
발신자로부터 수신자에게 암호화된 MAC 전송
1100
1160
첫 번째 및 두 번째 마스터 키에서
첫 번째 및 두 번째 파생된 세션 키 파생
1170
첫 번째 파생된 세션 키와 대칭 복호화로
보호된 데이터 복호화 및 보호된 데이터 재구성
1180
두 번째 파생된 세션 키 및 암호화 MAC으로
보호된 데이터 검증
끝

도면12



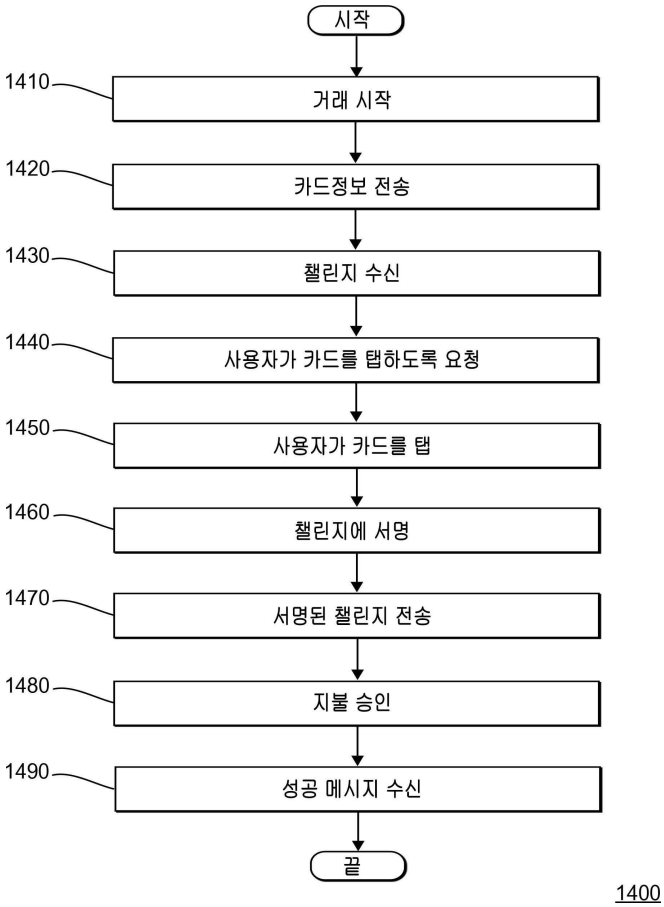
1200

도면13



시스템 1300

도면14

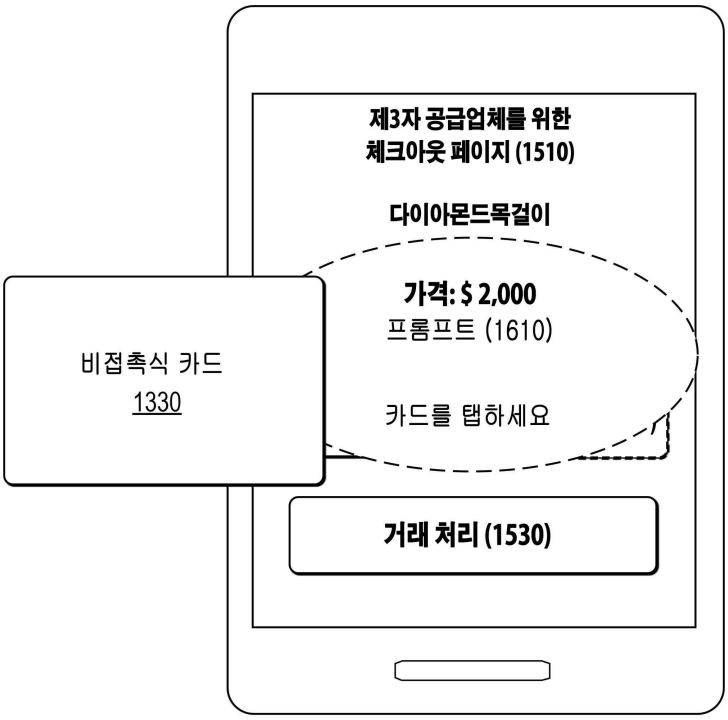


1400

도면15

클라이언트 디바이스 1320

도면16



클라이언트 디바이스 1320