(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년03월12일
(11) 등록번호 10-2088451
(24) 등록일자 2020년03월06일

(51) 국제특허분류(Int. Cl.)
G06Q 20/40 (2012.01) *G06Q 20/16* (2012.01)
G06Q 20/32 (2012.01) *G06Q 20/34* (2012.01)
(21) 출원번호 10-2014-7027322
(22) 출원일자(국제) 2013년02월28일
심사청구일자 2018년02월22일
(85) 번역문제출일자 2014년09월29일
(65) 공개번호 10-2014-0137400
(43) 공개일자 2014년12월02일
(86) 국제출원번호 PCT/CA2013/000185
(87) 국제공개번호 WO 2013/126996
국제공개일자 2013년09월06일
(30) 우선권주장
61/604,613 2012년02월29일 미국(US)
(56) 선행기술조사문헌
KR1020110115107 A*
US20100207742 A1*
KR1020110117744 A
US20110078081 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
모비웨이브 인코포레이티드
캐나다 에이치3씨 2엔5 퀘벡 몬트리올 뤼 퀸 80 스위트 502
(72) 발명자
폰테인 세바스챤
캐나다 에이치2엠 2엘3 퀘벡 몬트리올 애비뉴 안드레 그라세트 8673
돌리치노 루크
캐나다 에이치7브이 2와이1 퀘벡 라발 74이 애비뉴 648
(뒷면에 계속)
(74) 대리인
유미특허법인

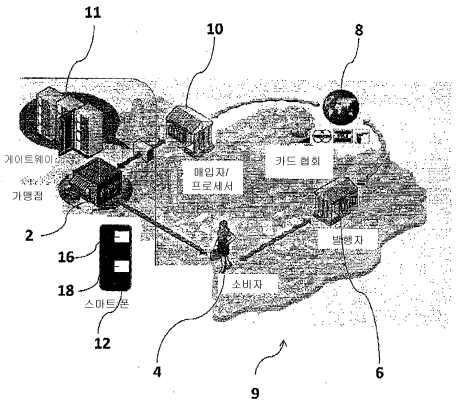
전체 청구항 수 : 총 18 항 심사관 : 박장환

(54) 발명의 명칭 **디바이스로 보안 금융 거래를 행하는 방법, 디바이스 및 보안 요소**

(57) 요 약

보안 금융 거래를 행하기 위한 디바이스 및 보안 요소가 개시된다. 상기 디바이스는 중앙처리장치; 상기 디바이스와 금융 계좌에 관련된 금융 기관 간의 통신을 확립하기 위한 통신 인터페이스; 상기 금융 계좌에 관한 데이터를 획득하기 위한 인터페이스; 상기 인터페이스에 의해 획득되는 상기 금융 계좌에 관한 데이터 중의 적어도 일부분을 처리하기 위한 보안 요소; 및 상기 금융 계좌로부터 데빗팅될 구매 금액을 획득하며 상기 금융 계좌에 관련된 금융 기관으로부터 거래 승인을 획득하는 제어 로직을 포함하며, 상기 거래 승인은 적어도 부분적으로, 상기 중앙처리장치에 의해 처리되는 데이터에 관계없이 상기 보안 요소에 의해서만 처리되는 데이터에 기초한다. 또한, 보안 금융 거래를 행하기 위한 방법, 및 보안 요소에 의해 실행되는 컴퓨터 프로그램 제품이 개시된다.

대 표 도 - 도1



(72) 발명자

두 헤이스 벤자민

캐나다 에이치3엑스 2와이3 퀘벡 햄스테드 뤼 두페린 260

드 난클라스 맥심

캐나다 에이치2제이 2엠7 퀘벡 몬트리올 뤼 리바드 4241

알베르티 자이버

캐나다 에이치2에스 1제이3 몬트리올(퀘벡) 수트 308 애비뉴 뷰몽트 80

명 세 서

청구범위

청구항 1

결제 단말로서 사용되는 디바이스에 설치하기 위한 보안 요소로서,

상기 디바이스는 POS(point of sale) 애플리케이션을 실행하고, 상기 POS 애플리케이션은 결제 제어 애플리케이션을 포함하며, 상기 결제 제어 애플리케이션은 상기 보안 요소를 제어하기 위한 제어 명령을 포함하고, 상기 디바이스는 프로세서, 인터페이스 및 통신 인터페이스를 포함하며, 상기 보안 요소는 비일시적 컴퓨터 판독가능 저장 매체로부터 액세스되는 명령을 포함하되 상기 명령을 실행하는 경우 상기 보안 요소로 하여금:

결제 장치로부터 상기 디바이스의 인터페이스에 의해 획득되는 데이터를 처리하도록 구성되는 EMV(Europay, MasterCard, and Visa) 거래 모듈로서, 상기 인터페이스는 상기 결제 장치로부터 비접촉식으로 데이터를 수신하도록 구성되는 비접촉식 인터페이스인, EMV 거래 모듈; 및

상기 EMV 거래 모듈에 의해 제공되는 데이터를 처리하도록 구성되는 운영 시스템(OS)

을 실행하도록 하며, 상기 EMV 거래 모듈은:

상기 보안 요소에 의해, 상기 디바이스의 프로세서 상에서 실행되는 상기 결제 제어 애플리케이션에 의해 송신되는 보안 금융 거래를 행하기 위한 요청을 수신하고;

상기 보안 요소에 의해, 상기 디바이스의 인터페이스를 통하여, 상기 결제 장치로부터 금융 계좌에 관한 데이터를 획득하되, 상기 획득은 (i) 상기 결제 장치에 PPSE(Select Proximity Payment System Environment) 요청을 전송하는 것, (ii) 상기 결제 장치에 의해 지원되는 결제 애플리케이션을 나타내는, 상기 결제 장치로부터의 응답을 수신하는 것, 및 (iii) 이용가능한 것 중에서 결제 애플리케이션을 선택하는 것을 포함하고;

상기 보안 요소에 의해, 서버와의 통신 채널을 확립하기 위한 요청을 결제 제어 애플리케이션에 전송함으로써, 상기 디바이스의 통신 인터페이스를 통해 상기 서버와의 보안 통신 채널을 확립하고;

상기 보안 요소에 의해, 상기 보안 금융 거래를 수행하기 위한 승인 요청을 상기 보안 통신 채널을 통해 상기 서버에 전송하되, 상기 승인 요청은 상기 금융 계좌에 관한 데이터의 적어도 일 부분을 포함하고;

상기 보안 통신 채널을 통해 상기 서버로부터 상기 승인 요청에 대한 응답을 수신한 다음 상기 보안 통신 채널을 폐쇄하며;

상기 승인 요청에 대한 응답을 처리하여 상기 보안 금융 거래의 상태를 생성하도록 구성되는, 결제 단말로서 사용되는 디바이스에 설치하기 위한 보안 요소.

청구항 2

제 1 항에 있어서,

상기 보안 요소는 상기 디바이스의 회로에 내장되는 칩셋, 가입자 식별 모듈(SIM) 카드, SD(secure digital) 카드, 비휘발성 메모리 카드, 및 상기 디바이스에 플러그되는 하우징 중의 하나에 내장되는, 결제 단말로서 사용되는 디바이스에 설치하기 위한 보안 요소.

청구항 3

제 1 항에 있어서,

상기 EMV 거래 모듈은 EMVCo 표준의 레벨 2, 및 EMVCo 표준의 레벨 3 중의 적어도 하나에 따라 인증되는, 결제 단말로서 사용되는 디바이스에 설치하기 위한 보안 요소.

청구항 4

제 1 항에 있어서,

상기 보안 금융 거래를 행하기 위한 요청은, 상기 금융 계좌로부터 데빗팅될 구매 금액을 포함하는, 결제 단말로서 사용되는 디바이스에 설치하기 위한 보안 요소.

청구항 5

제 1 항에 있어서,

상기 디바이스의 인터페이스는 데이터를 비접촉식으로 수신하도록 구성되는 비접촉식 인터페이스이고, 상기 결제 장치는 결제 카드 및 모바일 디바이스 중의 하나인, 결제 단말로서 사용되는 디바이스에 설치하기 위한 보안 요소.

청구항 6

제 1 항에 있어서,

상기 금융 계좌에 관한 데이터는 키, 인증서, 및 결제 카드 번호 중의 적어도 하나를 포함하는, 결제 단말로서 사용되는 디바이스에 설치하기 위한 보안 요소.

청구항 7

결제 단말로서 사용되는 디바이스의 보안 요소에 의해 실행되기 위한 컴퓨터 실행가능 명령을 포함하는 비일시적 컴퓨터 판독가능 저장 매체로서,

상기 디바이스는 POS 애플리케이션을 실행하고, 상기 POS 애플리케이션은 결제 제어 애플리케이션을 포함하며, 상기 결제 제어 애플리케이션은 상기 보안 요소를 제어하기 위한 제어 명령을 포함하고, 상기 컴퓨터 실행가능 명령은 프로세서에 의해 실행되는 경우 상기 보안 요소로 하여금:

결제 장치로부터 상기 디바이스의 인터페이스에 의해 획득되는 데이터를 처리하도록 구성되는 EMV(Europay, MasterCard, and Visa) 거래 모듈로서, 상기 인터페이스는 상기 결제 장치로부터 비접촉식으로 데이터를 수신하도록 구성되는 비접촉식 인터페이스인, EMV 거래 모듈; 및

상기 EMV 거래 모듈에 의해 제공되는 데이터를 처리하도록 구성되는 운영 시스템(OS)

을 실행하도록 하며, 상기 EMV 거래 모듈은:

상기 보안 요소에 의해, 상기 디바이스의 프로세서 상에서 실행되는 상기 결제 제어 애플리케이션에 의해 송신되는 보안 금융 거래를 행하기 위한 요청을 수신하고;

상기 보안 요소에 의해, 상기 디바이스의 인터페이스를 통하여, 상기 결제 장치로부터 금융 계좌에 관한 데이터를 획득하되, 상기 획득은 (i) 상기 결제 장치에 PPSE 요청을 전송하는 것, (ii) 상기 결제 장치에 의해 지원되는 결제 애플리케이션을 나타내는, 상기 결제 장치로부터의 응답을 수신하는 것, 및 (iii) 이용가능한 것 중에서 결제 애플리케이션을 선택하는 것을 포함하고;

상기 보안 요소에 의해, 서버와의 통신 채널을 확립하기 위한 요청을 결제 제어 애플리케이션에 전송함으로써, 상기 디바이스의 통신 인터페이스를 통해 상기 서버와의 보안 통신 채널을 확립하고;

상기 보안 요소에 의해, 상기 보안 금융 거래를 수행하기 위한 승인 요청을 상기 보안 통신 채널을 통해 상기 서버에 전송하되, 상기 승인 요청은 상기 금융 계좌에 관한 데이터의 적어도 일 부분을 포함하고;

상기 보안 통신 채널을 통해 상기 서버로부터 상기 승인 요청에 대한 응답을 수신한 다음 상기 보안 통신 채널을 폐쇄하며;

상기 승인 요청에 대한 응답을 처리하여 상기 보안 금융 거래의 상태를 생성하도록 구성되는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 8

제 7 항에 있어서,

상기 보안 금융 거래를 행하기 위한 요청은, 상기 금융 계좌로부터 데빗팅될 구매 금액을 포함하는, 비일시적

컴퓨터 판독가능 저장 매체.

청구항 9

제 7 항에 있어서,

상기 디바이스의 인터페이스는 데이터를 비접촉식으로 수신하도록 구성되는 비접촉식 인터페이스이고, 상기 결제 장치는 결제 카드 및 모바일 디바이스 중의 하나인, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 10

제 7 항에 있어서,

상기 금융 계좌에 관한 데이터는 키, 인증서, 및 결제 카드 번호 중의 적어도 하나를 포함하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 11

제 7 항에 있어서,

상기 보안 요소는 상기 디바이스의 회로에 내장되는 칩셋, 가입자 식별 모듈(SIM) 카드, SD(secure digital) 카드, 비휘발성 메모리 카드, 및 상기 디바이스에 플러그되는 하우징 중의 하나에 내장되는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 12

제 7 항에 있어서,

상기 EMV 거래 모듈은 EMVCo 표준의 레벨 2, 및 EMVCo 표준의 레벨 3 중의 적어도 하나에 따라 인증되는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

청구항 16

제1항 내지 제6항 중 어느 한 항에 있어서,

상기 보안 요소는 EMVCo 표준에 따라 인증되는 소프트웨어 컴포넌트에 의해 특징지어지는 프로세싱 엔티티인, 결제 단말로서 사용되는 디바이스에 설치하기 위한 보안 요소.

청구항 17

제1항 내지 제6항 중 어느 한 항에 있어서,

상기 보안 요소는 EMVCo 표준에 따라 인증되는 특정 하드웨어 및 소프트웨어 컴포넌트에 의해 특징지어지는 프로세싱 엔티티인, 결제 단말로서 사용되는 디바이스에 설치하기 위한 보안 요소.

청구항 18

프로세서, 비일시적 컴퓨터 판독가능 저장 매체, 및 보안 요소를 포함하는 디바이스로서,

상기 디바이스는 POS(point of sale) 애플리케이션을 실행하고, 상기 POS 애플리케이션은 결제 제어 애플리케이션을 포함하며, 상기 결제 제어 애플리케이션은 상기 보안 요소를 제어하기 위한 제어 명령을 포함하고, 상기 비일시적 컴퓨터 판독가능 저장 매체는 상기 보안 요소에 의해 실행되기 위한 컴퓨터 실행가능 명령을

포함하고, 상기 컴퓨터 실행가능 명령은 상기 보안 요소에 의해 실행되는 경우 상기 보안 요소로 하여금:

결제 장치로부터 상기 디바이스의 인터페이스에 의해 획득되는 데이터를 처리하도록 구성되는 EMV(Europay, MasterCard, and Visa) 거래 모듈로서, 상기 인터페이스는 상기 결제 장치로부터 비접촉식으로 데이터를 수신하도록 구성되는 비접촉식 인터페이스인, EMV 거래 모듈; 및

상기 EMV 거래 모듈에 의해 제공되는 데이터를 처리하도록 구성되는 운영 시스템(OS)

을 실행하도록 하며, 상기 EMV 거래 모듈은:

상기 보안 요소에 의해, 상기 디바이스의 프로세서 상에서 실행되는 상기 결제 제어 애플리케이션에 의해 송신되는 보안 금융 거래를 행하기 위한 요청을 수신하고;

상기 보안 요소에 의해, 상기 디바이스의 인터페이스를 통하여, 상기 결제 장치로부터 금융 계좌에 관한 데이터를 획득하되, 상기 획득은 (i) 상기 결제 장치에 PPSE(Select Proximity Payment System Environment) 요청을 전송하는 것, (ii) 상기 결제 장치에 의해 지원되는 결제 애플리케이션을 나타내는, 상기 결제 장치로부터의 응답을 수신하는 것, 및 (iii) 이용가능한 것 중에서 결제 애플리케이션을 선택하는 것을 포함하고;

상기 보안 요소에 의해, 서버와의 통신 채널을 확립하기 위한 요청을 결제 제어 애플리케이션에 전송함으로써, 상기 디바이스의 통신 인터페이스를 통해 상기 서버와의 보안 통신 채널을 확립하고;

상기 보안 요소에 의해, 상기 보안 금융 거래를 수행하기 위한 승인 요청을 상기 보안 통신 채널을 통해 상기 서버에 전송하되, 상기 승인 요청은 상기 금융 계좌에 관한 데이터의 적어도 일 부분을 포함하고;

상기 보안 통신 채널을 통해 상기 서버로부터 상기 승인 요청에 대한 응답을 수신한 다음 상기 보안 통신 채널을 폐쇄하며;

상기 승인 요청에 대한 응답을 처리하여 상기 보안 금융 거래의 상태를 생성하도록 구성되는, 디바이스.

청구항 19

제18항에 있어서,

상기 보안 요소는 특정 하드웨어에 의해 특징지어지는 프로세싱 엔티티인, 디바이스.

청구항 20

제18항에 있어서,

상기 보안 요소는 EMVCo 표준에 따라 인증되는 소프트웨어 컴포넌트에 의해 특징지어지는 프로세싱 엔티티인, 디바이스.

청구항 21

제18항에 있어서,

상기 보안 요소는 EMVCo 표준에 따라 인증되는 특정 하드웨어 및 소프트웨어 컴포넌트에 의해 특징지어지는 프로세싱 엔티티인, 디바이스.

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

청구항 36

삭제

청구항 37

삭제

청구항 38

삭제

청구항 39

삭제

청구항 40

삭제

청구항 41

삭제

청구항 42

삭제

청구항 43

삭제

청구항 44

삭제

청구항 45

삭제

청구항 46

삭제

청구항 47

삭제

청구항 48

삭제

청구항 49

삭제

청구항 50

삭제

청구항 51

삭제

청구항 52

삭제

청구항 53

삭제

청구항 54

삭제

청구항 55

삭제

청구항 56

삭제

청구항 57

삭제

청구항 58

삭제

청구항 59

삭제

발명의 설명

기 술 분 야

[0001] 관련 출원(들)에 대한 상호 참조

[0002] 본원은 Sebastien FONTAINE 등에 의해 2012년 2월 29일에 출원된, 발명의 명칭 "SYSTEM AND METHOD FOR CONDUCTING A SECURED TRANSACTION ON A DEVICE"인 미국 가특허출원 US61/604,613호를 참조로서 포함하는 것을 허용하는 관할지역(jurisdictions)에서 그 전체를 참조로서 포함한다.

[0003] 발명의 분야

[0004] 본 발명은 디바이스 상에서 보안 거래, 특히 보안 금융 거래를 행하기 위한 방법, 디바이스 및 보안 요소에 관한 것이다.

배 경 기 술

[0005] 본 섹션은 이하에 기술되고/되거나 청구되는 본 발명의 각종 양태와 관련될 수 있는 기술의 다양한 양태에 대하여, 독자에게 소개하기 위한 것이다. 본 논의는 독자에게 배경 정보를 제공함으로써 본 발명의 각종 양태에 대한 보다 나은 이해를 용이하게 하는데 유용할 것으로 생각된다. 따라서, 이러한 진술들은 종래 기술의 인정으로서가 아닌, 이러한 견지에서 독해되어야 함을 이해해야 한다.

[0006] 흔히, 가맹점들은 결제 단말을 사용하여 고객들과의 보안 금융 거래를 행하게 된다. 일반적으로, 이러한 고객들은 금융 기관이나 결제 카드 기관에 의해 발행된 결제 카드를 소지하고 있다. 몇몇 예들에서, 결제 카드들은 결제 단말의 자기 스트립 판독기에 카드를 대거나 또는 결제 단말의 스마트 카드 판독기에 결제 카드를 넣는 것에 의하여 거래가 개시될 수 있게 하는 자기 스트립 및/또는 스마트 카드 칩을 포함하고 있다. 다른 예들에서, 결제 카드는 결제 단말 가까이에 결제 카드를 제공함으로써 거래가 발생할 수 있게 하는 비접촉 거래 가능형일 수도 있다. 금융 거래 동안의 보안을 보장하기 위하여, EMV(Europay, MasterCard, and Visa) 거래 표준과 같은 보안 표준들이 개발되어 결제 단말들과 결제 카드들 모두를 인증하는데 사용되고 있다. 그러나, 보안 표준들을 충족하기 위해 필요한 기술적 복잡성을 포함하는 각종 요인들로 인하여, 일반적으로 보안 금융 거래들을 행하는데 사용되는 결제 단말들은 오로지 금융 거래들의 수행에 전용인 디바이스들이다.

[0007] 그러므로, 임의의 디바이스들, 특히 단순한 금융 거래들의 수행 이외의 다른 기능들도 제공하는 디바이스들로부터 보안 거래를 행하기 위한 방법, 디바이스 및 보안 요소에 대한 기술이 필요하다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0008] 본 발명의 목적은 결제 단말로서 사용되는 디바이스 상에서 보안 금융 거래를 행하는 방법을 제공하는 것이며, 상기 디바이스는 중앙처리장치와 보안 요소를 포함한다. 상기 방법은 금융 계좌로부터 데빗팅될 구매 금액을 획득하는 단계와, 상기 디바이스를 통해 상기 금융 계좌에 관한 데이터를 획득하는 단계와, 상기 금융 계좌와 관련된 금융 기관으로부터 거래 승인을 얻는 단계를 포함한다. 상기 승인은 적어도 부분적으로는, 상기 중앙처

리장치에 의해 처리되는 데이터에 관계없이 상기 보안 요소에 의해서만 처리되는 데이터에 기초한다. 상기 보안 요소에 의해서만 처리되는 데이터는 상기 획득된 금융 계좌에 관한 데이터 중의 적어도 일 부분을 포함한다.

[0009] 본 발명의 다른 목적은 보안 금융 거래를 행하기 위해 결제 단말로서 사용되는 디바이스를 제공하는 것이다. 상기 디바이스는 중앙처리장치와, 상기 디바이스와 금융 계좌에 관련된 금융 기관 간의 통신을 확립하도록 구성되는 통신 인터페이스와, 상기 금융 계좌에 관한 데이터를 획득하기 위한 인터페이스와, 상기 인터페이스에 의해 획득되는 상기 금융 계좌에 관한 데이터 중의 적어도 일 부분을 처리하기 위한 보안 요소와, 상기 금융 계좌로부터 데빗팅될 구매 금액을 획득하며 상기 금융 계좌에 관련된 금융 기관으로부터 거래 승인을 획득하도록 구성되는 제어 로직을 포함한다. 상기 거래 승인은 적어도 부분적으로, 상기 중앙처리장치에 의해 처리되는 데이터에 관계없이 상기 보안 요소에 의해서만 처리되는 데이터에 기초한다. 상기 보안 요소에 의해서만 처리되는 데이터는 상기 획득된 금융 계좌에 관한 데이터 중의 적어도 일 부분을 포함한다.

[0010] 본 발명의 다른 목적은 결제 단말로서 사용되는 디바이스에 설치하기 위한 보안 요소를 제공하는 것이다. 상기 보안 요소는 인증 표준에 따라 상기 디바이스의 인터페이스에 의해 획득되는 데이터를 처리하도록 구성되는 EMV(Europay, MasterCard, and Visa) 거래 모듈; 및 EMVCo 표준의 레벨 1에 따라 상기 EMV 거래 모듈에 의해 제공되는 데이터를 처리하도록 구성되는 운영 시스템(OS)을 실행시키는 명령들을 포함한다.

[0011] 본 발명의 다른 목적은 결제 단말로서 사용되는 디바이스에 의해 실행되는 컴퓨터 프로그램 제품을 제공하는 것이며, 상기 디바이스는 컴퓨터 프로그램 로직을 내장하는 컴퓨터 판독가능 저장매체를 구비한다. 상기 컴퓨터 프로그램 로직은, 상기 디바이스에 의해 실행될 시에, 인증 표준에 따라 상기 디바이스의 인터페이스에 의해 획득되는 데이터를 처리하도록 구성되는 EMV(Europay, MasterCard, and Visa) 거래 모듈; 및 EMVCo 표준의 레벨 1에 따라 상기 EMV 거래 모듈에 의해 제공되는 데이터를 처리하도록 구성되는 운영 시스템(OS)을 실행시킨다.

[0012] 본 발명의 다른 목적은 결제 단말로서 사용되는 디바이스의 보안 요소에서 실행되는 거래 모듈이며, 상기 거래 모듈은, 상기 디바이스에서 실행되는 결제 제어 애플리케이션으로부터 금융 거래를 행하기 위한 요청을 수신하고, 상기 디바이스의 인터페이스를 통해 결제 장치로부터 금융 계좌에 관한 데이터를 획득하고, 상기 디바이스의 통신 인터페이스를 통해 상기 금융 계좌와 관련된 금융 기관의 서버와의 보안 통신 채널을 확립하고, 상기 금융 거래를 수행하기 위한 승인 요청을 상기 보안 통신 채널을 통해 상기 서버에게 전송하되, 상기 승인 요청은 상기 금융 계좌에 관련된 데이터의 적어도 일 부분을 포함하고, 상기 보안 통신 채널을 통해 상기 서버로부터 상기 승인 요청에 대한 응답을 수신하고, 상기 승인 요청에 대한 응답을 처리하여 상기 금융 거래의 상태를 생성하고, 또한 상기 결제 제어 애플리케이션에게 상기 금융 거래의 상태를 전송한다.

도면의 간단한 설명

[0013] 이제, 본 명세서에 첨부된 도면들과 함께 본 발명에 대하여 기술하도록 한다.

도 1은 본 발명의 일 실시예에 따른, 보안 디바이스로부터 보안 금융 거래를 행하는 시스템의 다이어그램 표현이다.

도 2는 본 발명의 일 실시예에 따른, 비접촉 거래 발생의 다이어그램 표현이다.

도 3은 본 발명의 일 실시예에 따른, 보안 금융 거래를 행하는 방법을 도시한 흐름도이다.

도 4는 본 발명의 일 실시예에 따른, 보안 금융 거래가 일어날 수 있는 디바이스의 단순 블록도이다.

도 5는 본 발명의 일 실시예에 따른, 도 4의 디바이스에 내장된 보안 요소의 다이어그램 표현이다.

도 6은 본 발명의 각종 실시예들에 따른, 보안 요소를 내장한 디바이스들의 각종 아키텍처들의 다이어그램 표현이다.

도 7은 본 발명의 일 실시예에서, 결제 제어 애플리케이션을 인에이블하여 보안 요소의 소프트웨어와 통신하는 소프트웨어 스택들의 다이어그램 표현이다.

도 8a, 8b 및 8c는 본 발명의 각종 실시예들에서, 보안 요소의 소프트웨어 아키텍처의 다이어그램 표현들이다.

도 9a, 9b 및 9c는 본 발명의 일 실시예에 따라, 보안 요소 및 디바이스 상에서 보안 금융 거래를 행하는 몇몇 다른 엔티티들 간의 통신 흐름의 흐름도 표현이다.

도 10은 보안 요소와 금융 기관 간의 보안 통신 채널의 다이어그램 표현이다.

도 11은 본 발명의 일 실시예에 따른, 보안 요소에서의 결제 소프트웨어 로딩, 업데이팅 및 구성 프로세스의 다이어그램 표현이다.

도 12는 본 발명의 일 실시예에 따른, 보안 요소에서의 결제 소프트웨어 로딩, 업데이팅 및 구성 프로세스를 도시한 흐름도이다.

도 13은 본 발명의 일 실시예에서, 보안 요소의 소프트웨어와 통신하는 결제 제어 애플리케이션을 도시한 흐름도이다.

도면들에는, 본 발명의 실시예들이 예시의 방법으로 도시되어 있다. 상세한 설명 및 도면은 단지 예시의 목적이며 이해에 대한 보조를 위한 것임이 명백히 이해될 것이다. 이들은 본 발명에 대한 한정들의 규정인 것으로 의도되지 않는다.

발명을 실시하기 위한 구체적인 내용

[0014] 이제, 하나 이상의 고려된 실시예들과 함께 본 발명에 대하여 기술하도록 한다. 기술된 실시예들은 본 발명의 범위를 한정하는 것이 아닌 본 발명의 예시인 것으로 의도된다. 즉, 본 발명의 특정 실시예들에 관심의 초점이 맞추어지겠지만, 이러한 실시예들이 본 발명을 한정하는 것으로 의도되지 않는다. 반대로, 이하에 제공되는 예들은 본 발명의 광범위한 범위를 설명하기 위한 것으로 의도된다.

[0015] 용어(TERMINOLOGY)

[0016] 본 명세서의 전반에 걸쳐, 보안 거래들(예를 들어, 접촉 및 비접촉 거래들이며, 이에 한정되지 않음), 보안 요소들(예를 들어, 칩셋, 보안 칩셋, 보안 컴포넌트를 내장한 하드웨어, 보안 컴포넌트를 내장한 소프트웨어, 또는 보안 컴포넌트를 내장한 펌웨어이며, 이에 한정되지 않음) 및 보안 표준들에 대한 참조가 이루어진다. 보안 표준들의 예로는 EMV(Europay, MasterCard, and Visa), EMVCo, MasterCard®, Visa®, American Express®, JCB®, Discover® 및 PCI SSC(Payment Card Industry Security Standards Council(MasterCard®, Visa®, American Express®, Discover® 및 JCB®에 의해 설립되었으며, 금융 거래들에 대한 보안 표준들의 정의를 구체적으로 다룸))로부터의 인증 표준들을 포함하며, 이에 한정되지 않는다. 보안 거래들, 보안 요소들, 및 보안 표준들에 대한 참조는 예시의 목적으로 이루어지고, 본 발명의 범위의 한정이 아닌 본 발명의 예시인 것으로 의도된다.

[0017] 보안 요소: 특정 보안 표준들에 따른 특정 레벨의 보안을 보장하는 인증의 적용을 받는 특정 하드웨어 및/또는 소프트웨어 컴포넌트들에 의해 특징지어지는 프로세싱 엔티티. 하드웨어 관점에서, 보안 요소는 컴퓨팅 엔티티, 즉 마이크로컨트롤러(예컨대, CPU), 메모리(예컨대, RAM 또는 FLASH 메모리), 통신 인터페이스들 등 중의 적어도 하나에서 발견되는 일반 컴포넌트들을 포함한다. 또한, 특정 하드웨어 컴포넌트들이 보안 요소에 특별한 특정 기능들을 구현하기 위해 포함될 수도 있다. 예를 들어, 암호화 가속기가 포함될 수도 있다. 또한, 도청(eavesdropping)으로부터 보안 요소(16)를 보호하기 위해, RF 및 전자기 차단을 제공하는 모듈이 포함될 수도 있다. 금융 거래들의 맥락에서, 보안 요소의 인증은, 다양한 금융 엔티티들이 의도하는 보안 요소를 사용하여 중요한 금융 데이터를 저장 및 처리하고, 또한 그 중요한 금융 데이터를 사용하여 보안 금융 거래들을 수행하는 것을 보장한다.

[0018] 정보/데이터: 용어들 "정보" 및 "데이터"는 상호 교환적으로 사용되며, 본 발명의 목적을 위한 유사한 의미를 갖는다.

[0019] 보안 표준들은 복수의 보안 레벨들, 예를 들어 레벨 1 , 레벨 2, 또는 레벨 3을 포함할 수 있으며, 이에 한정되지 않는다. 일 예로서, 레벨 1은 레벨 2보다 높으며, 결과적으로, 레벨 3보다 높은 보안 레벨에 대응할 수 있으며, 이에 한정되지 않는다. 예를 들어, EMCo 표준은 보안 레벨들과 승인 및 인증 표준들의 예들, 예를 들어 단말 타입 승인 프로세스, 보안 평가 프로세스, 카드 타입 승인 프로세스, 또는 모바일 타입 승인 프로세스를 제공할 수 있으며, 이에 한정되지 않는다.

[0020] 예를 들어, 단말 타입 승인 프로세스는 EMV(Europay, MasterCard, and Visa) 명세의 준수를 테스트하는 메커니즘일 수 있다. 단말 타입 승인은 호환 애플리케이션들 간의 상호운용성 및 일관된 동작이 달성될 수 있는 신뢰도의 레벨을 제공할 수 있다. 일 예에서, 단말 타입 승인 테스트는 2개의 레벨들, 즉 레벨 1 및 레벨 2로 나누어질 수 있다. 레벨 1 타입 승인 프로세스는 EMV 명세에서 규정된 전기기계 특성, 논리 인터페이스, 및 송신

프로토콜 요구사항들의 준수를 테스트할 수 있다. 레벨 2 타입 승인은 EMV 명세에 규정된 데빗/크레딧 애플리케이션 요구사항들의 준수를 테스트할 수 있다. 또한, 단말 타입 승인 테스트는 단말에서 실행되는 애플리케이션과 금융 기관 간의 보안 통신들을 보장하는 레벨 3 승인을 포함할 수 있다.

[0021] 예를 들어, 보안 평가 프로세스는 EMVCo 멤버스의 발행자들에게 일반 보안 성능 특성과 제품들과 관련된 스마트 카드 및 IC(integrated circuits) 칩-기반 토큰들의 사용의 적합성에 관한 정보를 제공하는 것으로 의도될 수 있다. EMVCo 보안 평가 프로세스는 제품군 및 컴포넌트 레벨에 있어서 이들 제품들에 대한 강건한 보안 기반(security foundation)을 보장하도록 설계될 수 있다. 다르게는, 보안 평가 프로세스는 PCI SSC 멤버스의 발행자들에게 일반 보안 성능 특성과 제품들과 관련된 스마트 카드 및 IC(integrated circuits) 칩-기반 토큰들의 사용의 적합성에 관한 정보를 제공하는 것으로 의도될 수도 있다. PCI SSC의 경우, 소프트웨어 계층들도 이러한 보안 표준들 및 요구사항들에 의해 커버된다.

[0022] 예를 들어, 카드 타입 승인 프로세스는 EMV 및 공통 결제 애플리케이션(CPA) 명세의 준수를 테스트하는 메커니즘을 생성할 수 있다. 카드 타입 승인 프로세스는 호환 애플리케이션들 간의 상호운용성 및 일관된 동작이 달성될 수 있는 신뢰도의 레벨을 제공할 수 있다. 별개의 카드 타입 승인 프로세스들이 공통 핵심 정의(CCD) 명세를 구현하는 카드들 또는 CPA 명세를 구현하는 카드들에 대해 규정될 수 있다.

[0023] 예를 들어, 모바일 타입 승인 프로세스는 EMV 명세의 준수를 테스트하는 메커니즘을 생성하는 비접촉 모바일 결제(CMP) 제품 타입 승인 프로세스를 포함할 수 있다. CMP 제품 타입 승인 프로세스는 호환 모바일 제품들 간의 상호운용성 및 일관된 동작이 달성될 수 있는 신뢰도의 레벨을 제공할 수 있다.

[0024] 비접촉 인터페이스: 비접촉 인터페이스는 물리적 접촉없이도 2개의 엔티티들(예컨대, 본 명세서의 컨텍스트에서는 모바일 폰 및 신용 카드) 간의 데이터 교환을 가능하게 하는, 이 2개의 엔티티들 간의 인터페이스이다. 본 명세서에서는 NFC(near field communication) 인터페이스들이 기술되어 있지만, 2개의 엔티티들 간의 비접촉 데이터 교환을 가능하게 하는 임의의 기술 및 통신 프로토콜들은 본 발명과 관련된다.

[0025] 디바이스 상에서 보안 금융 거래를 행하기 위한 시스템 및 방법

[0026] 도 1은 본 발명의 일 실시예에 따른, 디바이스(12)로부터 보안 금융 거래를 행하기 위한 시스템(9)의 다이어그램 표현을 도시한 것이다. 본 발명의 일 실시예에서, 고객(4)은 고객의 금융 계좌를 관리하는 금융 기관(6)과 계약 관계에 있다. 금융 기관(6)은 고객의 당좌예금 계좌 또는 신용 카드 계좌를 관리하는 은행일 수 있다. 금융 기관(6)은 금융 거래 동안에 강력한 인증(strong authentication)을 제공하는 토큰을 고객(4)에게 제공한다. 이러한 토큰은, 예를 들어, 결제 카드 및/또는 고객(4)의 디바이스(예컨대, 모바일 폰)에 내장될 수 있는 보안화된 고유 식별 컴포넌트일 수 있다. 결제 카드는 결제 카드 회사(8)에 의해 관리되며, 예를 들어, 직불 카드 Interac® 회사로부터의 직불 카드 또는 MasterCard®, Visa®, American Express®, JCB®, 및 Discover®와 같은 신용 카드 회사들 중의 하나로부터의 신용 카드일 수 있다. 결제 카드는 자기 스트립, 스마트 카드 칩을 통해 및/또는 RFID(radio frequency identification) 회로를 가진 태그를 통해 고객의 금융 계좌에 관한 데이터를 포함할 수 있으며, 이에 한정되지 않는다. RFID 회로를 포함하는 태그는 비접촉 거래 능력들, 특히 EMV(Europay, MasterCard, and Visa) 보안 표준들(예컨대, Visa Paywave®, MasterCard PayPass®, American Express ExpressPay®, Interac Flash®, Discover Zip®)을 준수하는 비접촉 거래 능력들을 제공할 수 있다. 다른 실시예들에서, RFID 회로를 포함하는 태그는 결제 카드 이외의 다른 지원으로, 예를 들어 모바일 폰과 같은 디바이스에 내장될 수 있다(예컨대, 고객의 디바이스에 내장된 Google Wallet® 모듈). 고객의 금융 계좌와 관련된 데이터는 거래 동안에 금융 계좌가 식별될 수 있게 하는 임의 종류의 데이터일 수 있다. 예를 들어, 이러한 데이터는 키, 인증서, 및 결제 카드 번호를 포함할 수 있으며, 이에 한정되지 않는다.

[0027] 가맹점(2)은 가맹점의 금융 계좌를 관리하는 금융 기관(10)과 계약 관계에 있다. 금융 기관(10)은 가맹점의 당좌예금 계좌 또는 신용 카드 계좌를 관리하는 은행일 수 있다. 금융 기관(10)은 가맹점(2)으로 하여금 게이트웨이(11)를 통하여, 고객과, 예를 들어 고객(4)과 금융 거래들을 행할 수 있게 한다. 도 1에는 게이트웨이(11)가 도시되어 있지만, 이러한 게이트웨이 없이, 가맹점(2)과 금융 기관(10) 사이의 금융 거래들이 직접 일어날 수도 있다. 본 발명의 일 실시예에서, 가맹점(2)은 디바이스(12)를 통하여 고객(4)과의 보안 금융 거래를 개시 및 완료할 수 있다. 디바이스(12)는 보안 요소(16) 및 인터페이스(18)를 포함한다. 본 발명의 일 실시예에서, 인터페이스(18)는 예를 들어, 자기 스트립 판독기, 스마트 카드 판독기, 또는 NFC(near field communication) 인터페이스일 수 있으며, 이에 한정되지 않는다. 인터페이스(18)는 고객(4)의 결제 카드 및/또는 고객(4)의 디

바이스 간의 접촉 및/또는 비접촉 거래가 디바이스(12)로 일어날 수 있게 한다. 접촉 거래는, 예를 들어 자기 스트립 판독기에 자기 스트립을 대거나 또는 스마트 카드 판독기에 스마트 카드 칩을 접촉시키는 것일 수 있으며, 이에 한정되지 않는다. 또한, 비접촉 거래는 결제 카드 또는 모바일 디바이스가 비접촉 판독기에 물리적으로 접촉할 수 있는 거래를 포함할 수도 있다. 즉, 비접촉 거래는 비접촉이지만 결제 카드 또는 모바일 디바이스가 비접촉 판독기와 물리적으로 접촉하는 동안에 일어날 수 있는 통신을 지칭할 수도 있다. 본 발명의 일 실시예에서, 거래는 보안화되며, EMV 거래 표준과 적용가능 PCI SSC 표준들을 준수하는 금융 거래이다. 적용가능 PCI SSC 표준들은 결제 애플리케이션 데이터 보안 표준(PA-DSS), PIN 거래 보안(PTS) 및/또는 포인트-투-포인트 암호화 (P2PE) 중의 하나 일 수 있다. 다른 실시예들에서, 거래는 그 밖의 보안 거래 표준들을 준수할 수도 있다.

[0028] 이제, 도 1 및 도 2에 대한 참조가 동시에 이루어지며, 여기서 도 2는 도 1의 고객(4)과 가맹점(2) 간에 발생하는 비접촉 거래의 다이어그램 표현이다. 본 발명의 일 실시예에서, 거래는 보안 금융 거래이며, 금융 기관(10) 및 결제 카드 회사(8)와 통신하는 디바이스(12)를 통해서 가맹점(2)에 의해 개시된다. 가맹점(2)은 디바이스(12)에 구매 금액을 입력하는 것에 의해 거래를 개시한다. 이어서, 고객(4)은 예를 들어, 디바이스(12)의 인터페이스(18)(이 예에서는 NFC 인터페이스)에 근접하게 자신의 결제 카드(예를 들어, Visa Paywave® 비접촉 가능형 신용 카드(13))를 제시함으로써, Visa Paywave® 비접촉 가능형 신용 카드(13)와 디바이스(12)의 보안 요소(16) 간의 통신을 확립한다. 보안 요소(16)가 Visa Paywave® 비접촉 가능형 신용 카드(13)로부터의 데이터 판독을 완료하고 나면, 디바이스(12)는 고객(4)에게 PIN(personal identification number), 서명, 패스코드, 생체인식 데이터 또는 고객의 아이덴티티를 확인할 수 있게 하는 임의의 데이터를 입력하도록 안내할 수 있다. 고객(4)에 의하여 필요한 정보가 입력되고 나면, 디바이스(12)에 의하여 고객(4)의 금융 기관(6)에 대한 및/또는 결제 카드 회사(8)에 대한 금융 거래 승인이 요청된다. 이어서, 고객(4)의 금융 기관(6) 및/또는 결제 카드 회사(8)는 금융 거래를 승인 또는 거절(본 케이스일 수 있음)하고, 디바이스(12)와 통신하여 그 승인 상태를 통지하게 된다. 디바이스(12)에 의해 금융 거래 상태를 수신하면, 그 금융 거래가 고객(4)의 금융 기관(6) 및/또는 결제 카드 회사(8)에 의해 승인 또는 거절되었음이 고객(4)에게 통지된다. 본 발명의 다른 실시예들에서, 고객(4)은 MasterCard PayPass® 비접촉 가능형 신용 카드(15), 보안 비접촉 거래 능력들을 제공하는 RFID 회로를 포함하는 모바일 폰(또는 태블릿 컴퓨터)(17)을 사용하여 금융 거래를 개시할 수도 있다. 본 발명의 다른 실시예들에서, 보안 요소(16) 및 인터페이스(18)는 디바이스(12) 이외의 다른 디바이스들에 내장되어 있을 수도 있다. 예를 들어, 보안 요소(16) 및 인터페이스(18)는 태블릿 컴퓨터(14), 캐시 레지스터(20), 프린터(22), 벤딩 머신(24), 결제 단말(26), 및/또는 ATM(automatic telling machine)(28)(고객(4)이 가맹점(2)과의 상호작용하지 않고서, 즉 자신의 결제 카드 회사(8) 또는 자신의 금융 기관(6)과만 상호작용하여 거래를 행하는 경우)과 같은 디바이스들에 내장될 수도 있으며, 이에 한정되지 않는다. 보안 요소(16) 및 인터페이스(18)가 내장될 수 있는 디바이스들에 대한 다른 예들로는, TV, 비디오 게임 시스템, 인터넷에 액세스하기 위한 셋업 박스, 또는 애플사의 Apple TV®를 포함하며, 이에 한정되지 않는다.

[0029] 도 3은 본 발명의 일 실시예에 따른, 거래를 행하는 방법(111)을 도시한 흐름도이다. 방법(111)은 각종 타입의 거래들, 예를 들어 보안 접촉 및/또는 비접촉 금융 거래들을 행하기 위해 이용될 수 있으며, 이에 한정되지 않는다. 방법(111)은 디바이스(12)에서 실행되는 POS(point of sale) 애플리케이션(112)과 같은 소프트웨어 애플리케이션으로 구현될 수도 있다. POS 애플리케이션(112)은 방법(111)에 따라 고객(4)과 가맹점(2) 간에서 거래가 행해질 수 있게 하는 각종 소프트웨어 컴포넌트들을 포함할 수 있다. 특히, 각종 소프트웨어 컴포넌트들 중의 일부가 디바이스(12)의 보안 요소(16) 상에서 실행될 수 있으며, 다른 소프트웨어 컴포넌트들은 디바이스(12)의 CPU에 의해 실행될 수도 있다.

[0030] 예시의 목적에 있어서, 디바이스(12)의 인터페이스(18)는 비접촉 가능형 결제 카드 상의 데이터를 판독가능한 NFC 인터페이스이다. 방법(111)은 가맹점(2)에 의해서, 디바이스(12)에 구매 금액을 입력하는 단계 100에서 시작될 수 있다. 이어서, 단계 102에서, 고객(4)은 디바이스(12)의 NFC 인터페이스(18)에 근접하게 자신의 결제 카드, 예를 들어 Visa Paywave® 비접촉 가능형 신용 카드(13)를 제시함으로써, Visa Paywave® 비접촉 가능형 신용 카드(13)와 디바이스(12)의 보안 요소(16) 간의 통신을 확립한다. 보안 요소(16)가 Visa Paywave® 비접촉 가능형 신용 카드(13)로부터의 데이터 판독을 완료하고 나면, 단계 104에서, 디바이스(12)는 고객(4)에게 PIN, 서명, 패스코드, 생체인식 데이터 또는 고객의 아이덴티티를 확인할 수 있게 하는 임의의 데이터를 입력할 것을 안내할 수 있다. 고객(4)에 의하여 필요한 정보가 입력되고 나면, 단계 106에서, 디바이스(12)에 의하여 고객(4)의 금융 기관(6) 및/또는 결제 카드 회사(8)에게 금융 거래 승인이 요청된다. 이어서, 고객(4)의 금융 기관(6) 및/또는 결제 카드 회사(8)는 그 금융 거래를 승인 또는 거절(본 케이스일 수 있음)하고, 단계 108에서, 디바이스(12)와 통신하여 그 승인 상태를 통지하게 된다. 디바이스(12)에 의하여 금융 거래 상태가

수신되면, 단계 110에서, 고객(4)의 금융 기관(6) 및/또는 결제 카드 회사(8)에 의하여 금융 거래가 승인 또는 거절되었음이 고객(4)에게 통지된다. 금융 거래 상태가 거래 영수증의 형태로 고객(4)에게 제공될 수도 있다. 거래 영수증은 디바이스(12)에 디스플레이되거나 또는 전자적 수단을 통하여(예컨대, 이메일, MMS(multimedia message service), 및/또는 SMS(short message service)를 통하여) 고객에게 전송되는 전자적 영수증일 수 있다. 또한, 거래 영수증은 디바이스(12)와 통신하는 프린터에 의해 생성되는 물리적 영수증(예컨대, 종이 영수증)일 수도 있다.

[0031] 본 발명의 다른 실시예에서, 디바이스(12)는 로열티 카드, 기프트 카드, 선불 카드, 쿠폰 카드, 리워드 카드, 포인트 카드, 어드밴티지 카드, 클럽 카드 등으로부터 데이터를 보안적으로 판독할 수 있으며, 또한 그 카드와 관련된 기관과 보안 거래를 수행할 수 있다(이 기관은 로열티 프로그램의 멤버로서 카드 소지자를 식별함). 디바이스(12)와 카드 간의 통신들은, 예를 들어 디바이스(12)의 NFC 인터페이스(18)를 사용하는, 비접촉 거래일 수 있다. 카드와 관련된 기관과의 보안 거래는 고객의 계좌 상의 충분한 로열티 포인트의 가용성을 검증하는 것으로 이루어질 수 있다.

[0032] 보안 금융 거래를 행하기 위한 디바이스

[0033] 도 4는 본 발명의 일 실시예에 따른 예시적 디바이스(12)의 각종 예시의 컴포넌트들 및 특징들을 도시한 블록도이며, 이것에 대한 참조를 통하여 디바이스(12)에 대한 추가적인 세부사항들이 더욱 양호하게 이해될 수 있다. 디바이스는 보안 요소(16), NFC 인터페이스(19), 스마트 카드 판독기(55), 가입자 식별 모듈(SIM) 카드 슬롯(36), 통신 인터페이스(38), 제어 회로(40), 디바이스(12)의 운영 시스템(OS)이 실행하는 CPU(central processing unit)(42), 입/출력(I/O) 제어기(44), 디스플레이(46), 키패드(48), 프린터(도 4에는 미도시), 자기 스트립 판독기(52), 및 메모리(54)를 포함할 수 있다. CPU(42)로 실행되는 OS의 예들로는 애플사로부터 입수가능한 iOS®의 버전이나 그 아류; 구글사로부터 입수가능한 Android OS®의 버전이나 그 아류; RIM사로부터 입수가능한 PlayBook OS®의 버전이나 그 아류를 포함하며, 이에 한정되지 않는다. 본 발명의 범위로부터 벗어나지 않는 범위 내라면 그 밖의 사유 OS 또는 고객 제조 OS가 동등하게 사용될 수도 있다.

[0034] 본 발명의 일 실시예에서, 디바이스(12)는 CPU(42) 및 제어 회로(40)에 의해 제어됨으로써 디바이스(12)의 OS를 실행하는데 필요한 처리 능력을 제공한다. CPU(42)는 단일 프로세서를 포함하거나 복수의 프로세서들을 포함할 수도 있다. 예를 들어, CPU(42)는 "범용" 마이크로프로세서들, 범용 및 전용 마이크로프로세서들의 조합, 명령 세트 프로세서들, 그래픽 프로세서들, 또는 전용 프로세서들을 포함할 수 있다. 제어 회로(40)는 디바이스(12)의 컴포넌트들 간에 데이터와 명령들을 전송하는 하나 이상의 데이터 버스들을 포함할 수 있다. 또한, 제어 회로(40)는 캐싱(caching)을 위한 온보드 메모리를 포함할 수 있다.

[0035] 본 발명의 몇몇 실시예들에서, CPU(42)에 의해 사용되는 정보는 메모리(54)에 위치될 수 있다. 메모리(54)는 비휘발성 메모리 예를 들면, ROM(read only memory), 플래시 메모리, 하드 드라이브, 또는 임의의 다른 적절한 광학, 자기적, 또는 솔리드-스테이트 컴퓨터 판독가능 매체, 그리고 이들의 조합일 수 있다. 메모리(54)는 CPU(42)의 동작을 위해 필요한 데이터와 그 밖의 디바이스(12)를 위해 필요한 데이터를 저장하는데 사용될 수 있다. 예를 들어, 메모리(54)는 디바이스(12)의 펌웨어를 저장할 수도 있다. 펌웨어는 OS, 그리고 전자 디바이스(12)의 각종 기능들, 그래픽 사용자 인터페이스(GUI) 기능들, 또는 프로세서 기능들을 가능하게 하는 그 밖의 프로그램들을 포함할 수 있다. 메모리(54)는 GUI를 위한 컴포넌트들, 예를 들어 그래픽 요소들, 스크린들, 및 템플릿들을 저장할 수도 있다. 또한, 메모리(54)는 연결 정보(예컨대, 통신을 확립하는데 사용되는 정보)와 같은 데이터 파일들, 또는 디바이스(12)가 결제 제어 애플리케이션을 실행할 수 있게 하는 데이터를 포함할 수도 있다. 결제 제어 애플리케이션은 POS 애플리케이션(112)의 (디바이스(12)의 CPU(42)에 의해 실행되는) 소프트웨어 컴포넌트들 중의 하나이다. 디바이스(12)가 결제 제어 애플리케이션을 실행할 수 있게 하는 메모리(54)에 저장된 데이터는, 보안 금융 거래를 행하는데 사용되는 디스플레이(46) 상에 GUI를 생성하기 위한 데이터 및 보안 금융 거래를 완료하기 위해 필요한 처리 능력들을 포함한다. 또한, 메모리(54)는 NFC 인터페이스(19)의 활성화/비활성화를 제어하기 위한 데이터 및, 활성화된 경우, NFC 인터페이스(19)의 동작 모드(예컨대, 수동 또는 능동)를 제어하기 위한 데이터를 저장할 수 있다. 예를 들어, NFC 인터페이스(19)는 POS 애플리케이션(112)이 실행되지 않는 경우 수동 모드로 동작할 수 있다.

[0036] 통신 인터페이스(38)는 정보를 송수신하기 위한 추가의 연결 채널들을 제공할 수도 있다. 예를 들어, 통신 인터페이스(38)는 디바이스(12)로 하여금 게이트웨이(11) 및 금융 기관(10)의 은행 서버를 통해 신용 카드 정보(8)를 처리하는 엔티티와 통신할 수 있게 하는 연결 기능들을 제공할 수도 있다. 통신 인터페이스(38)는 예를

들어, 하나 이상의 네트워크 인터페이스 카드들(NIC) 또는 네트워크 제어기 그리고 관련 통신 프로토콜들을 나타낼 수 있다. 통신 인터페이스(38)는 WLAN(wireless local area network) 인터페이스, LAN(local area network) 인터페이스, WAN(wide area network) 인터페이스, MMS(multimedia message service), 및 SMS(short message service) 인터페이스를 포함하는 몇몇 타입의 인터페이스들을 포함할 수 있으며, 이에 한정되지 않는다.

[0037] 몇몇 실시예들에서, 디바이스(12)는 디바이스 식별 네트워킹 프로토콜을 사용하여, 네트워크 인터페이스를 통한 외부 디바이스와의 연결을 확립할 수도 있다. 예를 들어, 디바이스(12) 및 외부 디바이스 양쪽 모두는 인터넷 프로토콜(IP)을 사용하여 식별 정보를 브로드캐스팅할 수 있다. 그 후에, 디바이스들은 그 식별 정보를 사용하여 디바이스들 간의 네트워크 연결, 예를 들어 LAN 연결을 확립할 수 있다.

[0038] NFC 인터페이스(19)는 예를 들어, ISO 14443, ISO 15693, ISO 18092 또는 ISO 21481와 같은 표준들을 준수하는 각종 데이터 레이트들에서의 근거리 통신을 가능하게 할 수도 있다. NFC 인터페이스(19)는 디바이스(12)의 일부인 칩셋에 내장되는 NFC 디바이스를 통해 구현될 수도 있다. 다르게는, NFC 인터페이스(19)는 별개의 컴포넌트이며 통신 인터페이스(38)를 통해 디바이스(12)와 통신하는 NFC 디바이스를 통하여 구현되거나, 또는 디바이스(12)의 추가 포트(도 4에 미도시)를 통하여 구현될 수 있다. NFC 인터페이스(19)는 하나 이상의 프로토콜들, 예를 들어 다른 NFC 가능형 디바이스와 통신하는 근거리 통신 인터페이스 및 프로토콜들(NFCIP-1)을 포함할 수 있다. 프로토콜들은 통신 속도에 적응하고, 근거리 통신을 제어하는 이니시에이터 디바이스로서 연결 디바이스들 중의 하나를 지정하도록 사용될 수 있다. 몇몇 실시예들에서, NFC 인터페이스(19)는 다른 통신 인터페이스를 통한 연결을 위해 사용되는 SSID(service set identifier), 채널, 및 암호화 키와 같은 정보를 수신하는데 사용될 수 있다. 본 발명의 일 실시예에서, NFC 인터페이스(19)는 보안 요소(16) 및 제어 회로(40) 양쪽 모두와 직접 통신한다. 본 발명의 다른 실시예들에서, NFC 인터페이스(19)는 예를 들어, 제어 회로(40), I/O 제어기(44), 또는 이들 모두에 연결될 수 있으며, 이에 한정되지 않는다.

[0039] NFC 인터페이스(19)는 디바이스(12)의 근거리 통신 모드를 제어할 수 있다. 예를 들어, NFC 인터페이스(19)는 NFC 태그들을 판독하기 위한 판독기/기록기 모드들, 다른 NFC 가능형 디바이스와 데이터를 교환하기 위한 피어-투-피어 모드, 및 다른 NFC 가능형 디바이스가 데이터를 판독할 수 있게 하는 카드 에뮬레이션 모드 간에서 디바이스(12)를 전환하도록 구성될 수 있다. 또한, NFC 인터페이스(19)는 디바이스(12)가 자신의 RF 필드를 생성하는 활성 모드와 디바이스(12)가 부하 변조를 사용하여 RF 필드를 생성하는 다른 디바이스로 데이터를 전송하는 수동 모드 간에서 디바이스(12)를 전환하도록 구성될 수도 있다. 수동 모드에서의 동작은 디바이스(12)의 배터리 수명을 연장시킬 수 있다. 몇몇 실시예들에서, NFC 인터페이스(19)의 모드들은 사용자 선호 또는 제조자 선호에 기초하여 제어될 수 있다.

[0040] 일 실시예에서, NFC 통신은 대략 2 내지 4 cm 범위 내에서 일어날 수 있다. NFC 인터페이스(19)와의 근거리 통신은 자기장 유도를 통해 발생할 수 있으며, 이것은 NFC 인터페이스(19)로 하여금 다른 NFC 디바이스들과 통신하거나 RFID 회로를 가진 태그들로부터 데이터를 검색할 수 있게 한다. 도 2를 참조하여 전술한 바와 같이, NFC 인터페이스(19)는 데이터, 특히 신용 카드들(13 및 15) 또는 모바일 디바이스들(스마트폰이나 태블릿 컴퓨터)(17)로부터, 보안 비접촉 금융 거래를 가능하게 하는 데이터를 획득하기 위해 사용될 수 있다.

[0041] 보안 요소(16)는, POS 애플리케이션(112)이 EMV 거래들용으로 확립된 보안 표준들을 충족하기에 충분한 레벨의 보안을 제공하면서 디바이스 상에서 실행될 수 있도록 구성된다. 일 실시예에서, 보안 요소(16)는 NFC 인터페이스(19)와 협력하여 비접촉 결제 기능을 제공하는 제어 회로(40)에 연결된 칩셋으로 구현된다. 다른 실시예에서, 보안 요소(16)는 스마트 카드 판독기(55)와 협력하여 결제 기능을 제공하는 제어 회로(40)에 연결된 칩셋으로 구현된다. 또 다른 실시예에서, 보안 요소(16)는 자기 스트립 판독기(52)와 협력하여 결제 기능을 제공하는 제어 회로(40)에 연결된 칩셋으로 구현된다. 예를 들어, 보안 요소(16)가 구현되는 칩셋은 STMicroelectronics 사로부터 입수가능한 ST32® 또는 ST33® 칩셋 계열의 모델, 또는 그 아류일 수 있으며, 이에 한정되지 않는다. 이하, 도 5를 참조하여 보안 요소(16)에 대하여 더욱 상세히 기술하도록 한다.

[0042] SIM 카드 슬롯(36)은 SIM 카드가 디바이스(12) 내부에 삽입될 수 있게 한다. SIM 카드 슬롯(36) 내에 삽입된 SIM 카드는 디바이스(12)의 사용자를 식별 및 인증하는데 사용되는 IMSI(International Mobile Subscriber Identity)와 관련 키를 포함한다.

[0043] I/O 제어기(44)는 제어 회로(40), CPU(42), 및 입/출력 디바이스들 간에서 데이터를 교환하기 위한 인프라스트럭처를 제공할 수 있다. I/O 제어기(44)는 하나 이상의 집적 회로들을 포함할 수 있으며, 제어 회로(40) 내에 통합되거나 또는 별개의 컴포넌트로서 존재할 수도 있다. I/O 제어기(44)는 디스플레이(46), 키패드(48), 프린

터(도 4에는 미도시), 자기 스트립 판독기(52), 또는 스마트 카드 판독기(55)와 통신하기 위한 인프라스트럭처를 제공할 수도 있다. 도 4에는 자기 스트립 판독기(52) 및 스마트 카드 판독기(55)가 I/O 제어기(44)에 연결되는 것으로 도시되어 있지만, 자기 스트립 판독기(52) 및 스마트 카드 판독기(55)는 예를 들어 제어 회로(40) 및/또는 보안 요소(16)와 직접 연결될 수도 있으며, 이에 한정되지 않는다.

[0044] 또한, I/O 제어기(44)는 외부 디바이스들과의 통신을 위한 인프라스트럭처를 제공할 수 있으며, 외부 컴퓨터, 바코드 스캐너, 오디오 헤드폰들 등에 대하여 디바이스(12)를 연결시키는데 사용될 수도 있다.

[0045] 본 발명의 일 실시예에서, 디바이스(12)는 그 이동성이 모바일 세일즈 거래를 수행하는데 특히 적합하게 되는 모바일 디바이스이다. 예를 들어, 모바일 디바이스는 모바일 폰(예를 들어, 애플사로부터 입수가능한 iPhone®의 모델이거나 그 아류; RIM사로부터 입수가능한 Blackberry®의 모델이거나 그 아류; 삼성사로부터 입수가능한 Galaxy®의 모델이거나 그 아류), 태블릿 컴퓨터(예를 들어, 애플사로부터 입수가능한 iPad®의 모델이거나 그 아류; 삼성사로부터 입수가능한 Galaxy Tab®의 모델이거나 그 아류; RIM사로부터 입수가능한 PlayBook®의 모델이거나 그 아류), 및 랩탑 컴퓨터일 수 있으며, 이에 한정되지 않는다. 휴대성 및 모션 편의성을 위하여, 디바이스(12)는 디바이스(12)에 전력을 공급하는 통합 전원을 포함할 수 있다. 전원은 사용자-탈착가능하거나 디바이스(12)에 고정될 수 있는 하나 이상의 배터리들, 예를 들어 리튬-이온 배터리를 포함할 수 있다.

[0046] 디바이스(12)의 휴대성으로 인하여, 세일즈 거래는 각종의 환경들에서 행해질 수 있다. 예를 들어, 세일즈 거래는 택시에서, 또는 고객의 집의 문앞에서 물품을 전달하면서 행해질 수 있다. 또한, 본 발명은 전용 결제 단말이 아닌 디바이스를 통해, 예를 들어 보안 요소(16), NFC 인터페이스(19), 스마트 카드 판독기(55), 자기 스트립 판독기(52), 또는 그들의 다양한 조합을 내장하는 모바일 폰을 통하여 금융 거래를 행할 수 있는 능력을 가맹점에게 제공한다.

[0047] 본 발명의 다른 실시예에서, 보안 요소(16), NFC 인터페이스(19), 스마트 카드 판독기(55), 자기 스트립 판독기(52), 또는 이들의 조합은 예를 들어 프린터, 퍼스널 컴퓨터, 캐시 레지스터, 결제 단말, ATM(automatic telling machine), 벤딩 머신, TV, 비디오 게임 시스템, 인터넷에 액세스하기 위한 셋업 박스, 또는 애플사의 Apple TV®에서 POS 애플리케이션(112)을 실행시키는 비-모바일 디바이스들에 내장될 수 있다. 보안 요소(16) 및 인터페이스(18)를 포함할 수 있는 각종 디바이스들로 인하여, 광범위한 보안 거래들이 행해질 수 있다. 예를 들어, 고객은 자신의 TV로부터 영화를 주문할 수 있으며, 보안 요소(16) 및 인터페이스(18)를 내장하는 그 TV 상에서 직접 보안 거래를 수행할 수도 있다.

[0048] 디바이스 상에서 보안 금융 거래를 행하기 위한 POS(point of sale) 애플리케이션

[0049] 도 5는 디바이스(12) 상에서 POS 애플리케이션(112)이 실행되어 EMV 인증된 보안 거래를 수행하는 아키텍처의 개략도를 예시한 것이다. 본 발명의 일 실시예에서, 아키텍처는 POS 애플리케이션(112)의 활성 시에 보안 요소(16) 및 CPU(42)에 의해 실행되는 메모리(54)에 저장된 소프트웨어 컴포넌트를 실행시키는 칩셋에서 실행되는 사전-프로그래밍된 하드웨어 또는 펌웨어 요소들(예를 들어, ASIC(application specific integrated circuit)들)의 조합으로서 구현된다. 보안 요소(16)에서 실행되는 컴포넌트들은 단독의 사전-프로그래밍된 하드웨어 요소들, 다르게는, 단독의 펌웨어 또는 소프트웨어 요소들로 동등하게 실현가능하다는 것을 이해해야 한다. 본 발명의 일 실시예에서, 보안 요소(16)가 실행되는 칩셋은 메모리 및 처리 능력들(예컨대, 제어기 및/또는 마이크로프로세서)을 포함한다.

[0050] POS 애플리케이션(112)의 활성 시에 CPU(42)에 의해 실행되는 메모리(54)에 저장된 소프트웨어 컴포넌트는 결제 제어 애플리케이션(208)을 포함한다. 또한, 결제 제어 애플리케이션(208)은 메모리(54)가 아닌 다른 장소에 저장될 수도 있는 것으로 고려된다. 본 발명의 일 실시예에서, 결제 제어 애플리케이션(208)은 CPU(42) 상에 실행되는 OS에 의해 실행된다. 결제 제어 애플리케이션(208)은 보안 요소(16)를 제어하여 EMV 거래 표준들(예컨대, MasterCard®, Visa®, American Express®, Interac®)을 준수하는 금융 거래, 특히 EMV 비접촉 거래 표준들(Visa Paywave®, MasterCard PayPass®, American Express ExpressPay®, Interac Flash®, Discover Zip®)을 준수하는 비접촉 거래들을 개시 및 완료하는 명령들을 포함한다. 결제 제어 애플리케이션(208)은 가맹점(2), 금융 기관(10), 금융 기관(6), 및 결제 카드 회사(8) 중의 적어도 하나와 고객(4) 간의 통신을 관리한다. 결제 제어 애플리케이션(208)은 I/O 제어기(44)를 통하여, 디스플레이(46) 상에서 진행중인 거래의 디스플레이를 직접 또는 간접적으로 관리한다. 또한, 결제 제어 애플리케이션(208)은 보안 요소(16)를 통하여, 결제 카드들 또는 RFID-가능형 디바이스들로부터 NFC 인터페이스(19)에 의해 판독되는 데이터의 처리를 관리할 수도

있다. 또한, 결제 제어 애플리케이션(208)은 보안 요소(16)를 통하여, 결제 카드들로부터 스마트 카드 판독기(55)에 의해 판독되는 데이터의 처리를 관리할 수도 있다. 또한, 결제 제어 애플리케이션(208)은 보안 요소(16)를 통하여, 결제 카드들로부터 자기 스트립 판독기(52)에 의해 판독되는 데이터의 처리를 관리할 수도 있다. 또한, 결제 제어 애플리케이션(208)은 보안 요소(16)를 통하여, 예를 들어, PIN(personal identification number), 사용자 서명, 패스코드, 사용자 생체인식 데이터 또는 사용자의 보안 식별을 가능하게 하는 임의의 데이터와 같은 데이터의 처리를 관리할 수도 있다. 결제 제어 애플리케이션(208)은 예를 들어 MasterCard®, Visa®, American Express®, JCB®, 및 Discover®이며 이에 한정되지 않는 주요 결제 브랜드들로부터의 표준들에 따라 처리하는 보안 결제 카드 데이터를 위하여 레벨 3 인증되도록 설계된다.

[0051] POS 애플리케이션(112)을 실행하는 보안 요소(12)의 컴포넌트들에 대해서는, 보안 요소에 대한 설명을 하면서 아래의 상세한 설명에서 보다 상세히 기술하도록 한다.

[0052] 이제 도 7을 참조하면, 보안 요소(16) 상에서 POS 애플리케이션(112)을 실행시키는 소프트웨어와 결제 제어 애플리케이션(208)이 통신할 수 있게 하는 소프트웨어 스택들의 예시가 도시되어 있다. 도 7에 도시된 본 발명의 일 실시예에서, 제어 회로(40)의 CPU(42) 상에서 실행되는 결제 제어 애플리케이션(208)은 다음의 소프트웨어 스택들, 즉 SEEK(보안 요소 평가 키트), 운영 시스템(예컨대, Android OS), 및 저 레벨 드라이버들을 통해, 보안 요소(16)와 직접 통신한다. SEEK는 Android 애플리케이션이 보안 요소, SIM 카드, 또는 MicroSD 카드와 통신할 수 있게 하는 Android OS용 소프트웨어 라이브러리이다. 보안 요소(16)와 제어 회로(40) 간의 물리 통신은 ISO7816 링크(도 7에는 미도시)를 통해 구현된다. 도 7에 도시된 본 발명의 다른 실시예에서, 제어 회로(40)의 CPU(42) 상에서 실행되는 결제 제어 애플리케이션(208)은 앞서의 실시예와 동일한 소프트웨어 스택들을 사용하여, 비접촉 프론트 엔드(CLF)(710)를 통해 보안 요소(16)와 통신한다. CLF(710)와 제어 회로(40) 간의 물리 통신은 I2C 링크(도 7에는 미도시)를 통해 구현된다.

[0053] 도 13은 전술한 소프트웨어 스택들을 통해 보안 요소(16) 상에서 실행되는 단말 애플릿과 결제 제어 애플리케이션(208) 간의 통신을 예시한 흐름도이다. 흐름도에 도시된 예에서는, ISO7816 링크가 사용된다. 다르게는, 통신들이 CLF(710)을 통해 행해질 수도 있다.

[0054] 디바이스 상에서 보안 금융 거래를 행하기 위한 보안 요소

[0055] 도 5를 다시 참조하면, 보안 요소(16)는 제 1 모듈(200), 제 2 모듈(202), 및 제 3 모듈 EMV 접촉/비접촉 거래 모듈(204) 및/또는 제 3 모듈 MAG(206)을 포함한다. 본 명세서에는, 모듈 또는 모듈들로 지칭하고 있지만, 모듈은 예를 들어, 컴퓨터 프로그램 로직, 컴퓨터 프로그램 명령들, 소프트웨어, 스택, 펌웨어, 하드웨어 회로 또는 필요한 능력들을 제공하는 이들의 조합을 포함할 수 있으며, 이에 한정되지 않는다는 것을 이해해야 한다. 제 1 모듈(200)은 보안 요소(16)가 실행되는 칩셋의 드라이버들을 포함하며, 보안 요소(16)의 하드웨어 계층에 대한 액세스를 제공한다. 제 1 모듈(200)는 EMVCo 레벨 1 접촉 및 비접촉 표준에 따라 처리하는 보안 결제 카드 데이터를 위하여 레벨 1 인증되도록 설계된다. 결제 카드 데이터로 지칭되었지만, 임의의 다른 지원들(예컨대, 보안 비접촉 결제 처리를 위해 RFID 기능들을 내장하는 모바일 디바이스)의 결제 카드에 위치되는 임의의 데이터가 또한 고려된다는 것을 이해해야 한다. 제 2 모듈(202)은 보안 요소(16)를 실행하는 칩셋의 운영 시스템(OS)을 포함한다. 본 발명의 일 실시예에서, OS는 Oracle사의 Java Card®이다. 본 발명의 다른 실시예에서, OS는 글로벌 플랫폼 표준을 준수한다. 본 발명의 또 다른 실시예에서, OS는 인증되거나 인증되지 않은, 고객 제조 OS이다. 또 다른 실시예에서는, 제 1 모듈(200) 상에서 어떠한 OS도 실행되지 않는다. 본 발명의 일 실시예에서는, 제 2 모듈(202)의 OS는 제 1 모듈(200) 상에서 실행되며, 또한 EMVCo 레벨 1 접촉 및 비접촉 표준에 따라 처리하는 보안 결제 카드 데이터를 위하여 레벨 1 인증된다.

[0056] 제 3 모듈 EMV 접촉/비접촉 거래 모듈(204)은 제 2 모듈(202) 상에서 실행되며, 예를 들어, MasterCard®, Visa®, American Express®, JCB®, 및 Discover®이며 이에 한정되지 않는 주요 결제 브랜드들로부터 표준들에 따라 레벨 2 인증(선택적으로는 레벨 3 인증)되도록 설계된다. 제 3 모듈 EMV 접촉/비접촉 거래 모듈(204)은 결제 카드들로부터 및/또는 RFID-가능형 디바이스들로부터 NFC 인터페이스(19)에 의해 판독되는 데이터 또는 결제 카드들로부터 스마트 카드 판독기(55)에 의해 판독되는 데이터를 처리하는 명령들을 포함한다. 본 발명의 일 실시예에서, NFC 인터페이스(19), 스마트 카드 판독기(55), 또는 자기 스트립 판독기(52)에 의해 판독되는 데이터는 제어 회로(40)를 통과하지 않고서 보안 요소(16)로 직접 송신될 수 있다. 본 발명의 다른 실시예에서, NFC 인터페이스(19) 또는 스마트 카드 판독기(55)에 의해 판독되는 데이터는 보안 요소(16)로 송신되기 이전에 제어 회로(40)를 통과한다. 제 3 모듈 EMV 접촉/비접촉 거래 모듈(204)은 EMV 거래 표준들에 따라

판독되는 데이터의 보안 처리를 가능하게 한다. 제 3 모듈 EMV 접촉/비접촉 거래 모듈(204)에 의해 처리되는 데이터는 NFC 인터페이스(19) 또는 스마트 카드 판독기(55)로부터 판독되는 데이터를 포함하며, 예를 들어 PIN(personal identification number), 사용자 서명, 패스코드, 사용자 생체인식 데이터 또는 고객의 보안 식별을 가능하게 하는 임의의 데이터와 같은 정보를 포함할 수도 있다. 이러한 정보는 키패드(48), 디스플레이(46)(예컨대, 터치스크린 디스플레이를 통해), 또는 고객으로 하여금 디바이스(12)와 상호작용할 수 있게 하는 임의의 다른 인터페이스로부터 정보를 입력하는 고객에 의해서, I/O 제어기(44)를 통해 제공될 수 있다. 접촉 거래 및 비접촉 거래 능력들 모두를 내장하는 제 3 모듈 EMV 접촉/비접촉 거래 모듈(204)이 도시되어 있지만, 본 발명의 범위로부터 벗어나지 않는다면 접촉 거래 및 비접촉 거래 능력들은 2개의 상이한 EMV 모듈들에 내장될 수도 있다. 또한, 제 3 모듈 EMV 접촉/비접촉 거래 모듈(204)은 예를 들어 자기 스트립 판독기(52)로부터 판독되는 데이터의 처리와 같은 추가 능력들을 내장할 수도 있으며, 이에 한정되지 않는다.

[0057] 다르게는, 보안 요소(16)는 추가적으로, 또는 대체적으로, 제 3 모듈 EMV 접촉/비접촉(203), 제 3 모듈 마그네틱(MAG)(206)을 포함할 수 있다. 제 3 모듈 MAG(206)는 제 2 모듈(202)에 의해 제공되는 OS 상에서 실행되며, 예를 들어 MasterCard®, Visa®, American Express®, JCB®, 및 Discover®이며 이에 한정되지 않는 주요 결제 브랜드들로부터 표준들에 따라 레벨 2 인증(또한 선택적으로는 레벨 3 인증)되도록 설계된다. 제 3 모듈 MAG(206)는 결제 카드들로부터 자기 스트립 판독기(52)에 의해 판독되는 데이터를 처리하는 명령들을 포함한다. 제 3 모듈 MAG(206)는 EMV 거래 표준들에 따라 판독되는 데이터의 보안 처리를 가능하게 한다. 제 3 모듈 MAG(206)에 의해 처리되는 데이터는 자기 스트립 판독기(52)로부터 판독되는 데이터를 포함하며, 또한 예를 들어 PIN(personal identification number), 사용자 서명, 패스코드, 사용자 생체인식 데이터 또는 사용자의 보안 식별을 가능하게 하는 임의의 데이터와 같은 정보를 포함할 수도 있다. 이러한 정보는 키패드(48), 디스플레이(46)(예컨대, 터치스크린 디스플레이를 통해), 또는 고객으로 하여금 디바이스(12)와 상호작용할 수 있게 하는 임의의 다른 인터페이스로부터 정보를 입력하는 사용자에 의해서, I/O 제어기를 통해 제공될 수 있다.

[0058] 보안 요소(16)를 실행시키는 칩셋 상에 내장되는 제 3 모듈 EMV 접촉/비접촉 거래 모듈(204) 및 제 3 모듈 MAG(206), 이 아키텍처는 EMV 거래 표준들에 따라 디바이스(12) 상에서 보안 거래들이 행해질 수 있게 하는 동안에 데이터의 고속 처리를 가능하게 한다. 또한, 본 발명의 일 실시예에서, 이 아키텍처는 CPU(42)에 의해 처리되는 데이터와 관계없이 디바이스(12)가 보안 요소(16)에 의해 처리되는 데이터만을 가질 수 있게 한다. 즉, 보안 요소(16)는 CPU(42) 또는 제어 회로(40)에 의해 액세스될 수 없는 데이터를 처리할 수 있다. 본 발명의 일 실시예에서, 이 아키텍처는 CPU(42) 또는 제어 회로(40)에 의해 처리되는 데이터와 관계없이 보안 요소(16)에 의해서만 처리되는 데이터에 적어도 부분적으로 기초하여, 디바이스(12)가 금융 기관으로부터 거래 승인을 획득할 수 있게 한다.

[0059] 본 발명의 또 다른 실시예에서는, 보안 요소(16)만이 결제 카드들 또는 RFID-가능형 디바이스들로부터 NFC 인터페이스(19)에 의해 판독되는 데이터, 스마트 카드 판독기(55)에 의해 판독되는 데이터, 및 결제 카드들로부터 자기 스트립 판독기(52)에 의해 판독되는 데이터에 액세스한다. 즉, 결제 제어 애플리케이션(208)은 오직 보안 요소(16)에 의해서만 처리되어 그것의 메모리 내에 저장된 상태로 남아 있는 민감 데이터(예컨대, 키, 인증서, 및 결제 카드 번호) 중의 적어도 일부에 액세스할 필요없이 보안 요소(16)와 상호작용함으로써 거래를 관리한다. 예를 들어, MasterCard®, Visa®, American Express®, JCB®, 및 Discover®이며 이에 한정되지 않는 주요 결제 브랜드들로부터의 표준들 및 EMVCo 표준들에 따라 처리하는 보안 결제 카드 데이터를 위하여 레벨 2 인증(또한 선택적으로는 레벨 3 인증)되도록 설계되는 보안 요소(16), 이것은 CPU(42) 또는 제어 회로(40)(예를 들어, 결제 제어 애플리케이션(208)) 상에서 실행되는 임의의 애플리케이션들이 보안 요소(16)에 의해 처리되어 그것의 메모리에 저장된 데이터에 액세스하는 것을 방지함으로써 더 높은 레벨의 보안을 제공한다. 또한, 보안 요소(16)는 별개의 칩셋에 설계되어 사전 설치되며, 이에 따라 보안 요소(16)는 디바이스(12)와 관계없이 EMV 거래 인증될 수 있다. 즉, 본 발명의 일 실시예에서, 제어 회로(40) 상에 보안 요소(16)의 통합으로 인하여 디바이스(12)의 다른 컴포넌트들이 EMV 거래 인증 프로세스를 거칠 필요 없이도 디바이스(12)가 EMV 거래 인증될 수 있게 된다. 다른 실시예에서, 제어 회로(40) 상에 보안 요소(16)의 통합은 EMV 거래 인증을 위하여 적어도 부분적으로, 디바이스(12)가 EMV 인증 프로세스를 거칠 것을 여전히 필요로 한다. 또한, 보안 요소(16)는 예를 들어 MasterCard®, Visa®, American Express®, JCB®, 및 Discover®이며 이에 한정되지 않는 주요 결제 브랜드들로부터의 표준들에 따라 처리하는 보안 결제 카드 데이터를 위하여 레벨 3 인증되도록 설계될 수도 있다. 레벨 3 인증되는 것은 보안 요소(16) 상에서 실행되는 소프트웨어와 금융 기관 간의 보안 데이터 교환들을 보장한다.

[0060] 도 6은 보안 요소(16)를 내장한 다른 실시예의 디바이스들(12a, 12b, 및 12c)과 함께 디바이스(12)의 개략적 표

현을 도시한 것이다. 디바이스들(12a, 12b, 및 12c)의 표현은 보안 요소(16)의 다양한 위치들을 예시한 것이며, 이에 한정되지 않는다. 디바이스(12a)는 보안 요소(16), NFC 인터페이스(19), CPU(42)를 포함하지만, SIM 슬롯 카드를 포함하지 않으므로 SIM 카드를 포함하지 않으며, 디바이스 사용자의 고유 식별은 디바이스(12a)에 내장된 다른 회로 또는 펌웨어/소프트웨어에 의해 제공된다. 디바이스(12b)는 NFC 인터페이스(19), CPU(42), SIM 카드 슬롯(36), 및 SD(secure digital) 카드(60)를 포함한다. SD 카드(60)가 도시되어 있지만, 본 발명의 범위로부터 벗어나지 않는다면 임의의 비휘발성 메모리 카드들이 사용될 수 있음을 이해해야 한다. SD 카드(60)는 제어기(62) 및 메모리(64)를 포함한다. 도 6에 도시된 바와 같이, 보안 요소(16)는 디바이스(12b)에 삽입 또는 제거될 수 있는 SD 카드(60)에 내장된다. 12b에 도시된 본 발명의 실시예의 아키텍처는 본래의 회로에 어떠한 보안 요소들도 포함하지 않는 디바이스에 보안 요소(16)가 설치될 수 있게 하며, 이것에 의해 디바이스(12b)가 본래 EMV 비접촉 거래들을 위해 인증됨 없이도 디바이스(12b)가 EMV 비접촉 거래 가능하게 된다. 디바이스(12c)는 NFC 인터페이스(19), CPU(42), 및 SIM 카드 슬롯(36)을 포함한다. 도시된 바와 같이, 보안 요소(16)는 디바이스(12c)에 삽입 또는 제거될 수 있는 SIM 카드 슬롯(36)에 위치되는 SIM 카드에 내장된다. 본 발명의 일 실시예에서, SIM 카드 슬롯(36)에 위치되는 SIM 카드는 범용 가입자 식별 모듈(USIM) 표준을 준수한다. 12c에 도시된 본 발명의 실시예의 아키텍처는 본래의 회로에 어떠한 보안 요소들도 포함하지 않는 디바이스에 보안 요소(16)가 설치될 수 있게 하며, 이것에 의해 디바이스(12c)가 본래 EMV 비접촉 거래들을 위해 인증됨 없이도 디바이스(12c)가 EMV 비접촉 거래 가능하게 된다. 도 6에 나타나 있지 않은 다른 실시예에서, 보안 요소(16)는 디바이스(12)에 플러그되도록 하우징에 위치될 수 있다.

[0061] 이제, 도 5와, 보안 기능들을 제공하는 보안 요소(16)의 소프트웨어 아키텍처를 예시한 도 8a 및 8b에 대한 참조가 동시에 이루어진다. 도 8a 및 8b에 나타낸 보안 요소(16)는 저-레벨 OS, Java Card JVM(Java Virtual Machine), 및 글로벌 플랫폼 컴포넌트을 포함하며, 이것은 LI 인증 드라이버들(200) 및 OS(202)에 대응한다. 보안 요소(16)는 ISD(Issuer Security Domain), 및 선택적 보충의 보안 도메인(SSD)를 더 포함한다. 컴포넌트들 상에는, java 애플릿들이 보안 환경에서 실행된다. 특히, 결제 애플릿(810)은 레벨 2 인증(또한 선택적으로는 레벨 3 인증) 모듈들, 즉 EMV 접촉/비접촉 거래 모듈(204) 및/또는 MAG 모듈(206)을 실행시킬 수 있다. 각각의 보안 도메인(SD)은 서로 분리되어 있다. 어떤 보안 도메인의 소유자는 다른 보안 도메인에 상주하는 데이터/프로그램들에 액세스할 수 없다. 각각의 보안 도메인은 암호화 키들 및 인증 절차에 의해 보안화된다. 특정 보안 도메인(특정 보안 도메인에 상주하는 애플릿들의 추가/수정/삭제)에 액세스하기 위해, 특정 보안 도메인을 보호하는 암호화 키들이 사용된다. 발행자 보안 도메인(ISD)은 보안 요소(16) 발행자(결제 카드의 은행, 폰 안의 SIM 카드의 셀룰러 오퍼레이터, 또는 폰 내의 내장 보안 요소에 대한 폰 제조업체)의 제어하에 있다. 발행자는 예를 들어 파트너에 의해 사용될 보충의 보안 도메인(SSD)을 생성할 수 있다. 그 후에, 발행자는 보충의 보안 도메인에 액세스할 권한이 부여된 파트너에게 이 보충의 보안 도메인을 제어하는 암호화 키들을 전송하며, 이 SSD에 설치된 것을 제어할 수 있다. 또한, ISD는 SSD들 상에 발행자가 생성한 제한들을 가할 수 있다(예를 들어, SSD의 플래시에 있어서의 최대 풋프린트). 또한, 보안 도메인들의 계층구조가 생성될 수 있으며, 여기서 ISD는 0, 하나, 또는 그 이상의 SSD들을 포함한다.

[0062] 이제, 도 8a 및 8b에 나타낸 결제 애플릿(810)의 소프트웨어 아키텍처를 예시한 도 8c에 대한 참조가 이루어진다. 결제 애플릿(810)은 일반적으로 보안 요소(16)의 하위 레벨 소프트웨어 컴포넌트들(예컨대, OS)과 인터페이싱하는 추상화 계층을 포함한다. 결제 애플릿(810)은 디바이스(12)의 상이한 접촉 및 비접촉 인터페이스들과 인터페이싱하는 인터페이스 모듈들, 즉 스마트 카드 판독기(55)와 인터페이싱하기 위한 EMV 접촉 L1 및 EMV 접촉 L2 코어, NFC 인터페이스(19)와 인터페이싱하기 위한 EMV 비접촉 L1 코어 및 EMV 비접촉 L2 코어, 자기 스트립 판독기(52)와 인터페이싱하기 위한 마그네틱 스트라이프 코어를 포함한다. 결제 애플릿(810)은 디바이스(12)의 통신 인터페이스(38)를 통해 외부 엔티티들(예컨대, 금융 기관)과 통신하기 위한 통신 서비스들을 포함한다. 결제 애플릿(810)은 외부 엔티티들(예컨대, 금융 기관)과의 통신을 보안화하기 위한 보안 서비스들, 즉 인증 서비스들, 암호화 서비스들, 및 암호 저장 서비스들을 더 포함한다. 또한, 결제 애플릿(810)은 매입자 모듈(acquirer module)을 포함한다. 그리고, 결제 애플릿(810)은 상이한 타입의 결제 수단(예컨대, 접촉 또는 비접촉 신용 카드, 비접촉 결제 가능형 모바일 폰 등)에 의해 제공되는 다양한 타입의 결제 애플리케이션들을 지원하기 위한, 몇몇 결제 모듈들(예컨대, MasterCard PayPass MagStripe, Visa PayWave MSD, MasterCard Paypass M/Chip, Visa PayWave qVSDC)을 포함한다.

[0063] 디바이스 상의 보안 요소에 의한 보안 금융 거래의 실행

[0064] 이제, 도 1 , 2, 4, 5, 및 앞서 기술된 본 발명의 실시예들에 따라 디바이스 상에서 보안 금융 거래를 행하는

몇몇 다른 엔티티들과 보안 요소 간의 통신 흐름의 흐름도 표현인 도 9a-c에 대한 참조가 동시에 이루어진다. 구체적으로, 금융 기관(10) 또는 결제 카드 회사(8)의 금융 서버(910)가 나타나 있다. 디바이스(12)의 CPU(42) 상에서 실행되는 결제 제어 애플리케이션(208)이 나타나 있다. NFC 인터페이스(19)가 나타나 있다. 디바이스(12)의 보안 요소(16)가 나타나 있다(결제 애플릿(810)은 보안 요소(16) 상에서 실행됨). 또한, PICC(Proximity Integrated Circuit Card)(920)가 나타나 있다. PICC(920)는 비접촉 가능형 결제 장치(예컨대, 모바일 폰(17) 또는 신용 카드(13))에 통합되며, 금융 계좌와 관련된 데이터를 포함한다. 금융 계좌는 금융 기관(10) 또는 결제 카드 회사(8)와 관련된다.

[0065] 도 9a-c에 도시된 실시예에서는, 결제 제어 애플리케이션(208)과 보안 요소(16) 간의 통신들이 NFC 인터페이스(19)를 통해(예컨대, 비접촉 프론트 엔드 CLF를 통해) 이루어진다. 다른 실시예들이 또한 적용될 수 있다. 예를 들어, 통신들이 제어 회로(40)를 통해 이루어질 수도 있다.

[0066] 또한, 도 9a-c에 도시된 실시예에서, 금융 계좌와 관련된 데이터를 판독하기 위한 디바이스(12)의 인터페이스(18)는 디바이스(12)의 NFC 인터페이스(19)이다. 다르게는, 인터페이스는 디바이스(12)의 자기 스트립 판독기(52) 또는 스마트 카드 판독기(55)일 수 있다.

[0067] 사용자는 결제 제어 애플리케이션(208)을 통해 금융 거래를 개시하며, 금융 거래에 대응하는 금액이 특정된다. 결제 제어 애플리케이션(208)은 NFC 인터페이스(19)를 통해 보안 요소(16)에게 결제 애플릿 시작 메시지를 전송한다. 보안 요소(16)가 활성화되며, 결제 애플릿(810)이 보안 요소(16) 상에서 시작된다. 보안 요소(16)는 결제 애플릿(810)의 시작에 확인 응답할 수 있다(도 9a-c에 미도시). 그 후에, 결제 제어 애플리케이션(208)은 NFC 인터페이스(19)를 통하여 보안 요소(16)에게 거래 시작 메시지(금액과 함께)를 전송한다.

[0068] 보안 요소(16)는 NFC 인터페이스(19)의 판독기 모드를 인에이블하도록 하는 요청을 NFC 인터페이스(19)에게 전송한다. NFC 인터페이스(19)의 무선 주파수(RF) 및 비접촉 기능들이 활성화된다. PICC(920)는 그 제시를 알리며, NFC 인터페이스(19)는 PICC(920)의 제시를 검출한다. NFC 인터페이스(19)는 PICC(920)의 제시를 보안 요소(16)에게 통지한다.

[0069] 보안 요소(16)는 검출된 PICC(920)와 결제 거래를 시작한다. 제 1 단계는 (NFC 인터페이스(19)를 통해) PICC(920)에게 PPSE(Select Proximity Payment System Environment) 요청을 전송하는 것으로 이루어진다. PICC(920)는 (NFC 인터페이스(19)를 통해) PICC(920)에 의해 지원되는 결제 애플리케이션들을 표시하는 응답으로 이 요청에 응답한다. 보안 요소(16)는 이들 사용가능한 결제 애플리케이션들 중의 하나를 선택하고, (NFC 인터페이스(19)를 통해) PICC(920)에게 애플리케이션 식별자 선택(AID 선택) 요청을 전송한다. PICC(920)는 (NFC 인터페이스(19)를 통해) 결제 애플리케이션의 선택 상태(ok/nok) 및 그 선택된 결제 애플리케이션과 관련된 설정 옵션들을 표시하는 응답으로 이 요청에 대해 응답한다.

[0070] 제 2 단계는 PICC(920)로부터 선택된 결제 애플리케이션을 위한 결제 크리덴셜들(예컨대, 키(들), 인증서(들), 결제 카드 번호)을 판독하는 것으로 이루어진다. 결제 크리덴셜들을 판독하기 위하여, NFC 인터페이스(19)를 통해, 보안 요소(16)와 PICC(920) 간의 프로토콜 교환이 발생한다. 이 프로토콜 교환은 EMV를 준수함으로써, 결제 크리덴셜들의 보안 판독을 보장한다. 이 제 2 단계 이후에, 보안 요소(16)는 PICC(920)와 통신할 필요가 없다. 따라서, 보안 요소(16)는 NFC 인터페이스(19)의 RF 및 비접촉 기능들을 비활성화시키도록 하는 요청을 NFC 인터페이스(19)에게 전송한다.

[0071] 선택적 단계는 결제 크리덴셜들을 검증하기 위한 (NFC 인터페이스(19)를 통해) 보안 요소(16)와 결제 제어 애플리케이션(208) 간의 교환으로 이루어진다. 예를 들어, 결제 제어 애플리케이션(208)은 PICC(920)에 연관된 PIN 번호를 검색할 수 있다(디바이스(12)의 디스플레이(46) 및 키패드(48)와 PICC(920) 소지자의 상호작용을 통해). PIN 번호는 보안 요소(16)에게 전송되며 결제 크리덴셜들을 검증하는데 사용된다.

[0072] 제 3 단계는 금융 서버(910)와의 통신을 개시하는 것으로 이루어진다. 보안 요소(16)는 (NFC 인터페이스(19)를 통해) 금융 서버(910)와의 통신 채널을 확립하도록 하는 요청을 결제 제어 애플리케이션(208)에게 전송한다. 결제 제어 애플리케이션(208)은 디바이스(12)의 네트워킹 자원들을 사용하여, 디바이스의 통신 인터페이스(38)를 통해, 보안 요소(16)와 금융 서버(910) 간의 통신 채널을 확립한다. 그 후에, 보안 요소(16) 및 금융 서버(910)는 그 통신 채널을 통해(예를 들어, 인증서들, 암호화 키들 등의 교환을 통해) 보안 통신을 확립한다.

[0073] 제 4 단계는 금융 기관으로부터 승인을 요청하는 것으로 이루어진다. 보안 요소(16)는 거래를 승인하도록 하는 요청을 보안 통신 채널을 통해 금융 서버(910)에게 전송한다. 이 승인 요청은 거래를 승인하는데 사용되는 몇몇 파라미터들, 예를 들어 금액, 결제 크리덴셜들, 가맹점 ID(가맹점 ID는 디바이스(12)에 의해 실행되는

POS(point of sale) 애플리케이션을 사용하여 가맹점을 식별하도록 보안 요소(16)에 저장될 수 있음)를 포함한다. 금융 서버(910)는 승인 요청을 처리하고, 금융 거래가 승인될 것인지의 여부를 결정하고, 보안 통신 채널을 통하여 승인 요청에 대한 응답을 전송한다. 이 시점에서, 보안 통신 채널은 폐쇄되며, 그 이유는 보안 요소(16)와 금융 서버(910) 간에는 더 이상의 통신이 필요하지 않기 때문이다.

[0074] 제 5 단계에서, 보안 요소(16)는 금융 기관의 응답을 처리하여 금융 거래의 상태 즉, 승인 또는 거절을 판정한다. 또한, 보안 요소(16)는 거래의 상태와 함께 금융 서버(910)에 의해 송신될 수 있는 파라미터들을 처리한다. 예를 들어, 보안 요소(16)는 결제 픽토그램(pictogram)을 생성할 수 있다. 그 후에, 보안 요소(16)는 (NFC 인터페이스(19)를 통해) 존재하는 경우 파라미터들과 함께(예를 들어, 결제 픽토그램), 거래 상태의 통지를 결제 제어 애플리케이션(208)에게 송신한다.

[0075] 제 6 단계에서, 결제 제어 애플리케이션(208)은 사용자에게 거래 상태를 통지한다. 또한 결제 제어 애플리케이션(208)은 (NFC 인터페이스(19)를 통해) 보안 요소(16)에게 결제 애플릿 중단 메시지를 전송한다. 결제 애플릿(810)은 보안 요소(16) 상에서 중단되며, 보안 요소(16)는 비활성화된다.

[0076] 이제, 보안 요소와 금융 기관 간의 보안 통신 채널의 다이어그램 표현인 도 10에 대한 참조가 이루어진다. 모바일 디바이스(12)의 보안 요소(16)와 금융 기관 서버(910) 간에는 보안 통신 채널(950)이 확립되며, 이것은 도 9a-c와 관련하여 앞서 기술된 보안 통신 채널을 예시하는 것이다. 보안 통신 채널(950)은 예를 들어 모바일 디바이스(12)의 CPU(도 10에 미도시)의 운영 시스템 및 결제 제어 애플리케이션(208)을 포함하는, 모바일 디바이스(12)의 각종 엔티티들에 의해 확립된다. 보안 통신 채널(950)은 모바일 디바이스(12)에 의해 지원되는 통신 인터페이스들 중의 하나를 통해 확립된다. 예시의 목적으로, 도 10에는 3개의 통신 인터페이스가 나타나 있으며(와이파이, 블루투스, 및 셀룰러 데이터), 셀룰러 데이터 인터페이스가 통신 채널(950)의 확립을 위해 사용된다. 보안 통신 채널(950)은 일반적으로 모바일 디바이스(12)와 금융 기관 서버(910) 간의, 비 보안 네트워크(915)(본 예시에서는 셀룰러 데이터 네트워크)를 통해 확립된다. 보안 통신 채널(950)은 초기에 비-보안화되거나, 부분적으로 보안화된 통신 채널이다. 보안화(도 9a-c에 도시된 바와 같은)는, 보안 통신 채널(950)을 통한 보안 금융 거래를 수행하는데 필요한 적절한 레벨의 보안을 구현하기 위하여, (예를 들어, 암호화 키들, 인증서들 등의 교환 및 사용을 통해) 보안 요소(16)과 금융 기관 서버(910)에 의해 제 2 단계에서 수행된다.

[0077] 보안 요소 상의 결제 소프트웨어의 보안 다운로드, 설정 및 업데이트

[0078] 이제, 본 발명의 일 실시예에 따른 보안 요소에서의 결제 소프트웨어 로딩, 업데이팅 및 설정 프로세스의 다이어그램 표현인 도 11에 대한 참조가 이루어진다. 모바일 디바이스(12)의 보안 요소(16)는 보안 요소(16)에 의해 실행되는 결제 소프트웨어(예컨대, 도 8c에 나타낸 결제 애플릿(810))를 로드, 업데이트, 및 설정하기 위하여, 몇몇 엔티티들과 통신할 수 있다. 이러한 엔티티들은 TSM(Trusted Service Manager), 금융 기관, 및 제 3 자 서버를 포함한다.

[0079] TSM(Trusted Service Manager)은 보안 요소(예컨대, SIM 카드, 내장 보안 요소, MicroSD 카드)에서 클라이언트의 보안 도메인(ISD 또는 SSD)를 관리하는 제 3 자이다. TSM은 보안 도메인들에 액세스하기 위한 암호화 키들을 보안적으로 저장 및 사용하고, 소프트웨어 및 데이터를 저장하며, 또한 보안 요소들에 원격 액세스하는 적절한 인프라스트럭처를 구비한다. TSM은 디바이스(12)에 대한 물리적 액세스 없이도 보안 요소(16) 상의 데이터 및 소프트웨어에 대한 신뢰되는 원격 배포를 가능하게 한다. TSM 대신에, 금융 기관 서버 또는 제 3 자 서버가 사용되어 보안 요소(16)에 로딩될 데이터 및 소프트웨어의 보안 저장 및 보안 배포를 관리할 수도 있다. 특히, 제 3 자 서버는 기능들의 용어에서 TSM와 본질적으로 유사지만, 완전한 TSM과 연관된 보안 제한들 및 법적 책임들 모두를 갖지 않을 수 있다. 제 1 단계에서, 디바이스(12) 상에서 실행되는 결제 제어 애플리케이션(208), 및 TSM/금융 기관 서버/제 3 자 서버 간의 통신 채널이 개방된다. 제 2 단계에서, TSM/금융 기관 서버/제 3 자 서버는 디바이스(12)의 보안 요소(16)와의 보안 통신 채널을 개방하고, 보안 요소(16)의 적절한 보안 도메인과 인터페이싱하며, 보안 요소(16) 상의 데이터 및 소프트웨어를 보안적으로 로딩한다.

[0080] 로드/업데이트/설정 프로세스들은 모바일 디바이스(12)의 통신 인터페이스들(예컨대, 와이파이, 블루투스, 또는 셀룰러 데이터) 중의 하나를 사용하여, 일반적으로 비-보안화된 네트워크(915)(예컨대, 셀룰러 데이터 네트워크)를 통해 수행된다. 따라서, 로드/업데이트/설정 프로세스들은 보안화될 필요가 있으며, 이것은 도 12와 관련하여 더 기술될 것이다. 일반적으로, 로드/업데이트/설정 프로세스들은 특정 (보안) 프로토콜, 예를 들어 글로벌 플랫폼 프로토콜에 따라 수행된다.

[0081] 다른 실시예에서는(도 11에는 미도시), 통신 네트워크(915)를 사용하는 대신에, 보안 요소(12)에 업로드될 데이터 및 소프트웨어를 포함하는 MicroSD 카드가 사용될 수도 있다.

[0082] 이제, 본 발명의 일 실시예에 따른 보안 요소에서의 결제 소프트웨어 로딩, 업데이팅 및 설정 프로세스를 도시한 흐름도인 도 12에 대한 참조가 이루어진다. 흐름도는 POS(point of sale) 애플리케이션을 실행하기 위하여, 보안 요소를 내장하는 모바일 디바이스의 모든 필수 소프트웨어 및 데이터의 포괄적인 설치를 예시한 것이다.

[0083] 제 1 단계에서, 모바일 디바이스의 사용자는 자신의 매입자(Acquirer)(예컨대, 도 12에 나타낸 TSM, 금융 기관 서버, 또는 제 3 자 서버)에 대한 결제 애플리케이션을 모바일 디바이스로(예를 들어 마켓, 애플리케이션 스토어 등으로부터) 다운로드한다. 사용자는 결제 애플리케이션을 시작시키며, 이것은 모바일 디바이스의 CPU에 의해 실행된다. 결제 애플리케이션은 매입자와 접촉하기 위하여, 그것의 크리덴셜들을 입력할 것을 사용자에게 요청한다. 사용자는 그것의 크리덴셜들을 입력한다. 결제 애플리케이션은 보안 연결을 통해 매입자와 접촉한다. 매입자는 사용자의 크리덴셜들을 검증한다. 크리덴셜들이 유효하지 않은 경우, 사용자에게는 그것의 크리덴셜들을 재입력할 것이 결제 애플리케이션에 의해 요청된다.

[0084] 제 2 단계에서(크리덴셜들이 검증된 경우), 결제 애플리케이션은 매입자와 보안 요소 간의 통신 채널을 개방한다. 이 통신 채널을 개방하는 절차는 도 10에 관하여 기술한 것과 마찬가지이다. 매입자 및 보안 요소의 보안 도메인은 통신 채널을 통해 보안 통신을 더욱 확립하며, 그들 간에 인증 및 보안 메시징을 제공한다.

[0085] 제 3 단계에서, 매입자는 보안 요소에 특정 결제 애플릿을 로딩하며, 이 특정 결제 애플릿은 (POS(point of sale) 가능형) 모바일 디바이스의 사용자에 대한 적절한 설정에 따라 선택된다. 그 후에, 매입자는 결제 애플릿을 활성화시킨다.

[0086] 제 4 단계에서, 매입자와 결제 애플릿 간에는 상호 인증이 수행되며, 이들 간에는 (매입자와 보안 요소 간에 이미 확립된 보안 통신 채널을 통해) 보안 통신이 확립된다. 그 후에, 매입자는 결제 애플릿에 암호화 인증서들 및 개인 키들을 로딩한다. 또한, 매입자는 결제 애플릿에 (POS(point of sale) 가능형) 모바일 디바이스의 사용자에게 특정한 설정 데이터를 로딩한다. 설정 데이터는 매입자의 호스트네임, 연결 크리덴셜들, 고객 EMV 태그들, 활성화된 결제 모듈들(예컨대, PayPass, PayWave), 국가 코드 및 통화 등을 포함할 수 있다. 이제, 결제 애플릿이 사용될 준비가 되었다.

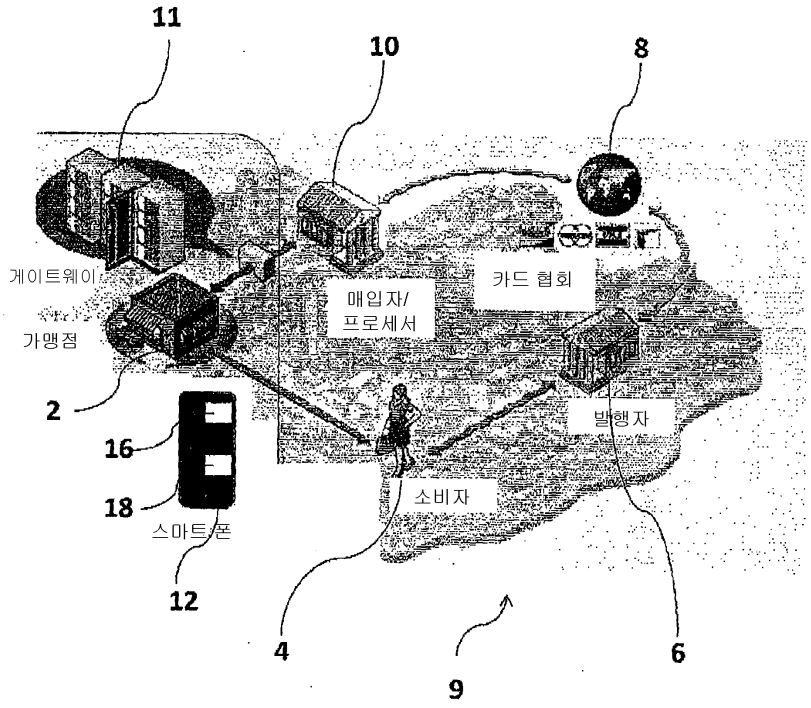
[0087] 결제 애플릿의 업데이트는 전술한 제 2, 제 3, 및 제 4 단계들에 따라 수행될 수 있다.

[0088] 본 발명의 전술한 실시예들이 특정 순서로 수행되는 특정 단계들을 참조하여 기술 및 도시되었지만, 이들 단계들이 본 발명의 교시들로부터 일탈하지 않는 범위 내에서 조합, 하위-분할, 또는 재-순서화 될 수 있다는 것이 이해될 것이다. 따라서, 단계들의 순서 및 그룹화는 본 발명의 한정이 아니다.

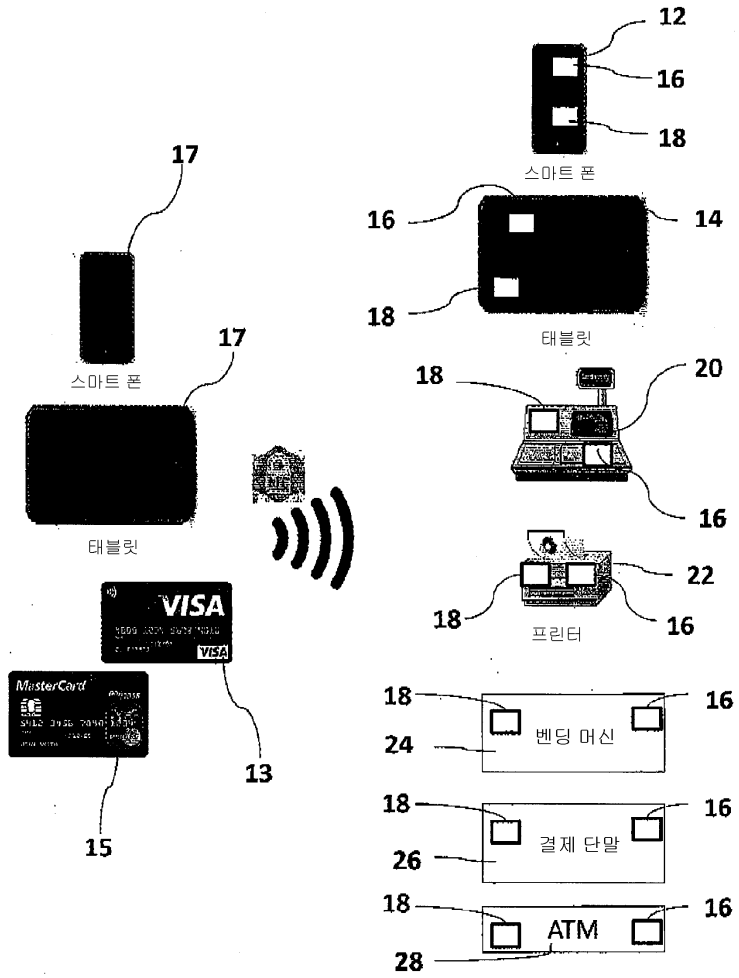
[0089] 본 발명의 전술한 실시예들에 대한 수정 및 개선은 당업자에게 명백해질 수 있다. 전술한 설명은 한정이 아닌 예시인 것으로 의도된다. 따라서, 본 발명의 범위는 첨부된 청구항들의 범위에 의해서만 한정되는 것으로 의도된다.

도면

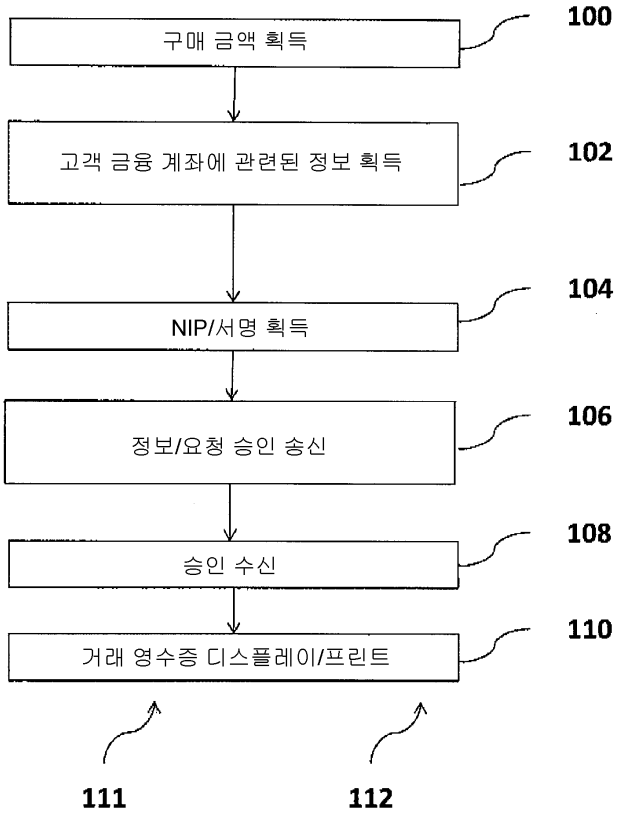
도면1



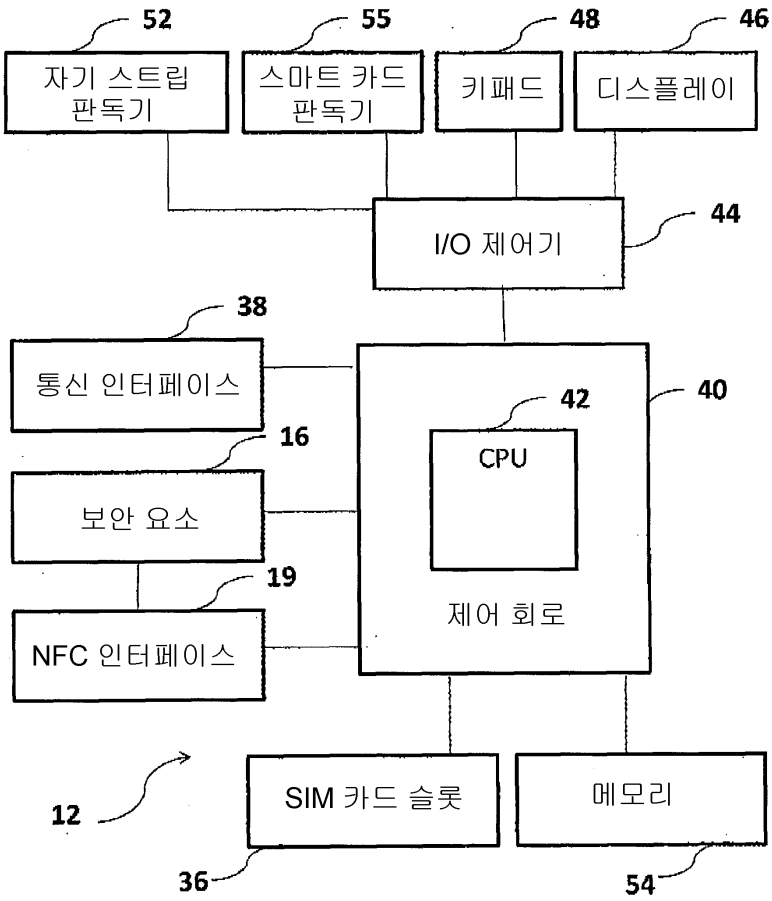
도면2


12
16
18
스마트 폰
16
14
18
태블릿
17
17
스마트 폰
태블릿
18
20
16
22
18
16
프린터
VISA
MasterCard
13
15
18
16
24
벤딩 머신
18
16
26
결제 단말
18
16
28
ATM

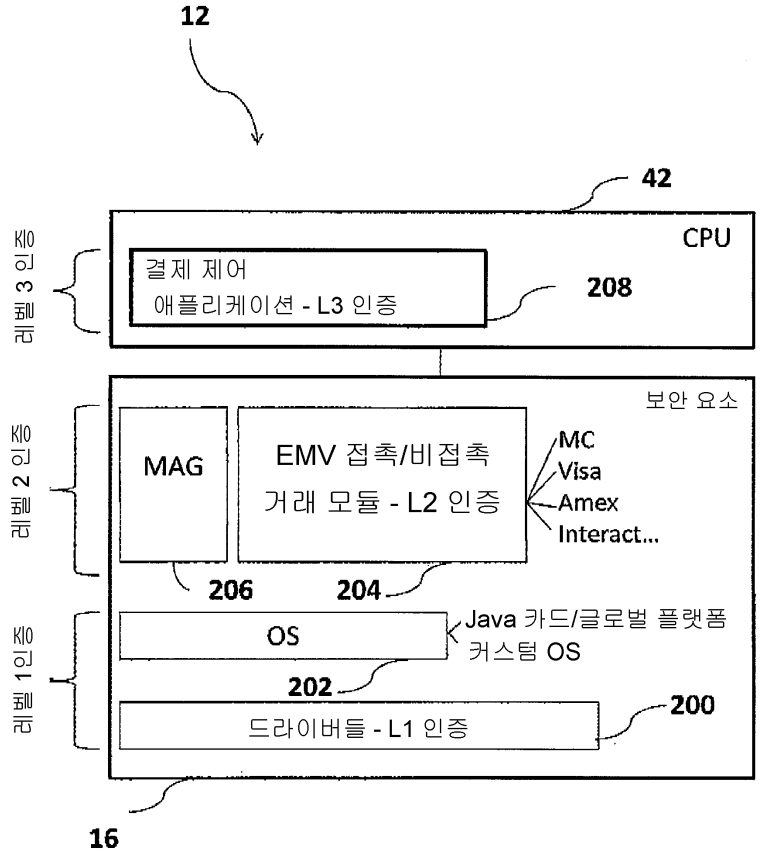
도면3


구매 금액 획득
100
고객 금융 계좌에 관련된 정보 획득
102
NIP/서명 획득
104
정보/요청 승인 송신
106
승인 수신
108
거래 영수증 디스플레이/프린트
110
111
112

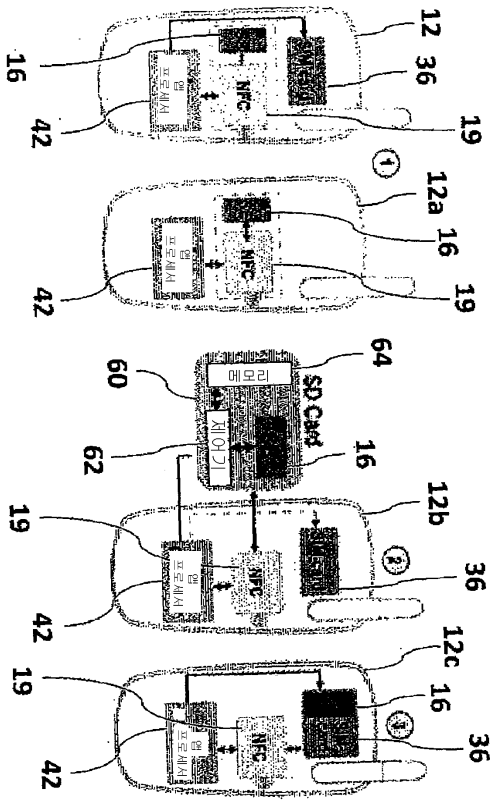
도면4


52
55
48
46
자기 스트립 판독기
스마트 카드 판독기
키패드
디스플레이
I/O 제어기
44
38
통신 인터페이스
42
40
CPU
16
보안 요소
19
NFC 인터페이스
제어 회로
12
SIM 카드 슬롯
메모리
36
54

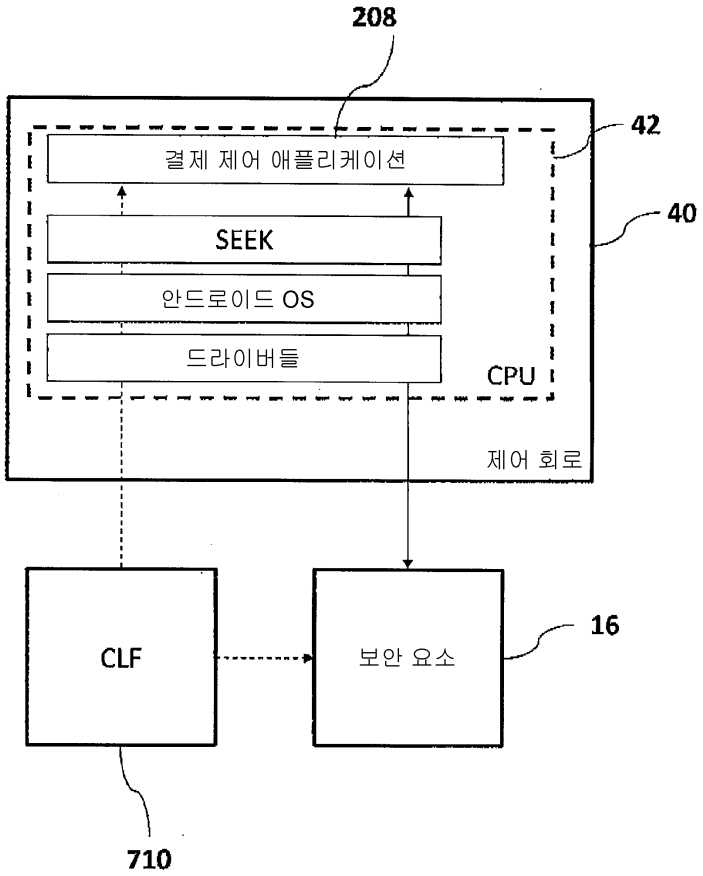
도면5


12
42
CPU
결제 제어
애플리케이션 - L3 인증
208
레벨 3 인증
보안 요소
MAG
EMV 접촉/비접촉
거래 모듈 - L2 인증
MC
Visa
Amex
Interact...
206
204
레벨 2 인증
OS
Java 카드/글로벌 플랫폼
커스텀 OS
202
드라이버들 - L1 인증
200
레벨 1 인증
16

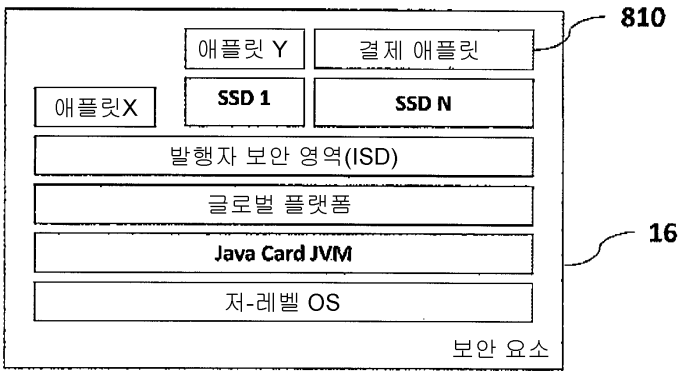
도면6


12
36
16
42
19
12a
60
64
메모리
SD Card
62
12b
12c
NFC

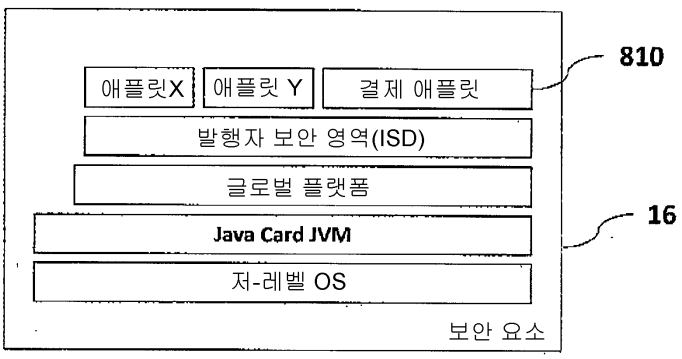
도면7



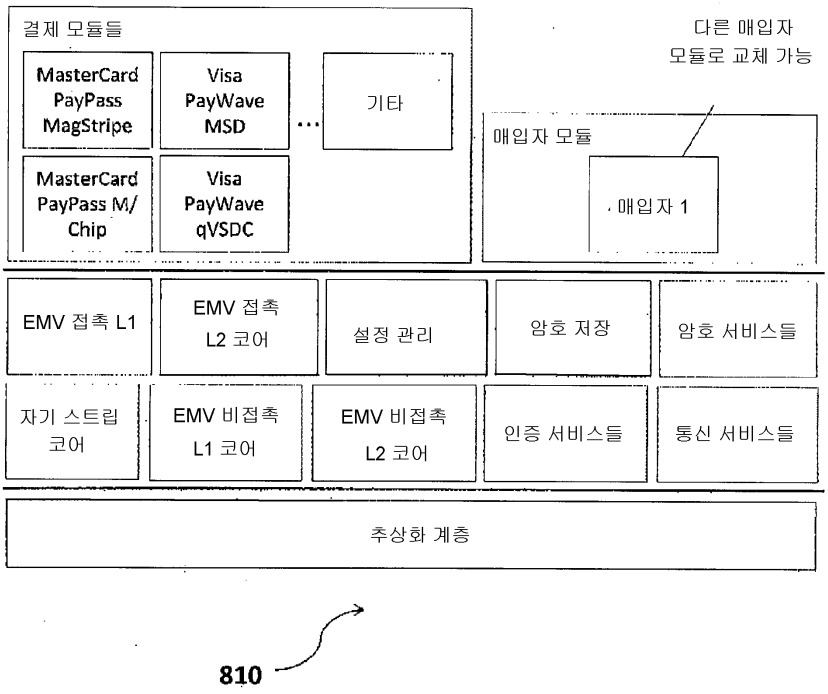
도면8a



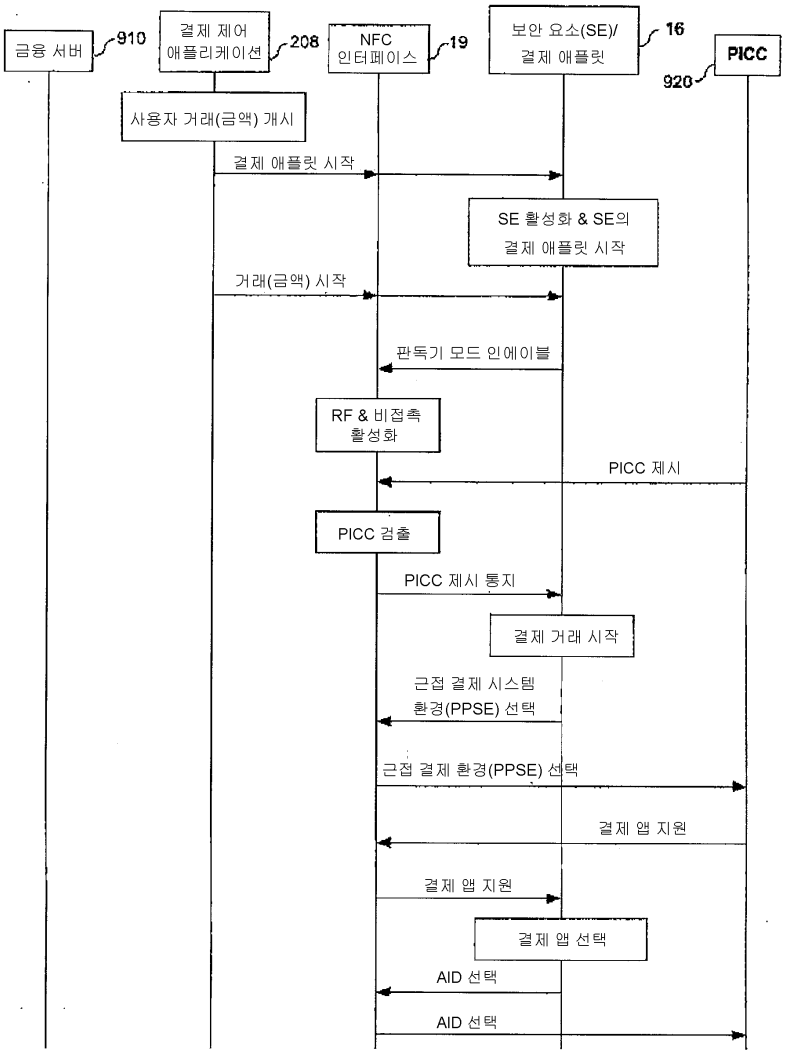
도면8b



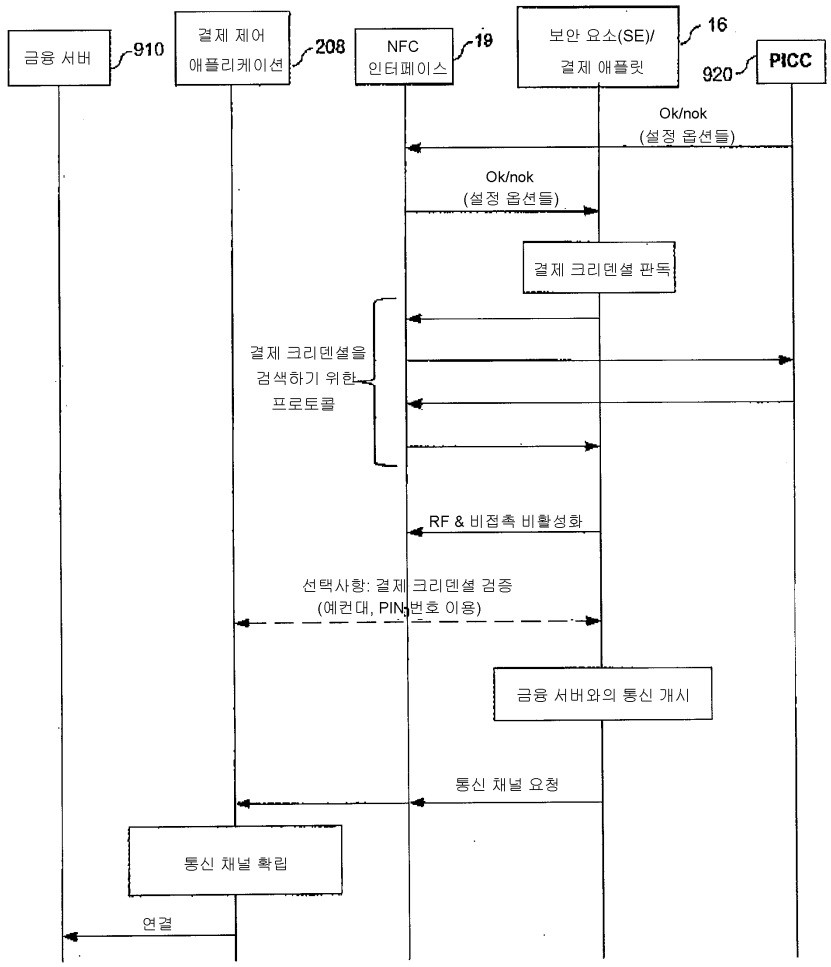
도면8c


결제 모듈들
MasterCard PayPass MagStripe
Visa PayWave MSD
기타
MasterCard PayPass M/Chip
Visa PayWave qVSDC
다른 매입자 모듈로 교체 가능
매입자 모듈
매입자 1
EMV 접촉 L1
EMV 접촉 L2 코어
설정 관리
암호 저장
암호 서비스들
자기 스트립 코어
EMV 비접촉 L1 코어
EMV 비접촉 L2 코어
인증 서비스들
통신 서비스들
추상화 계층
810

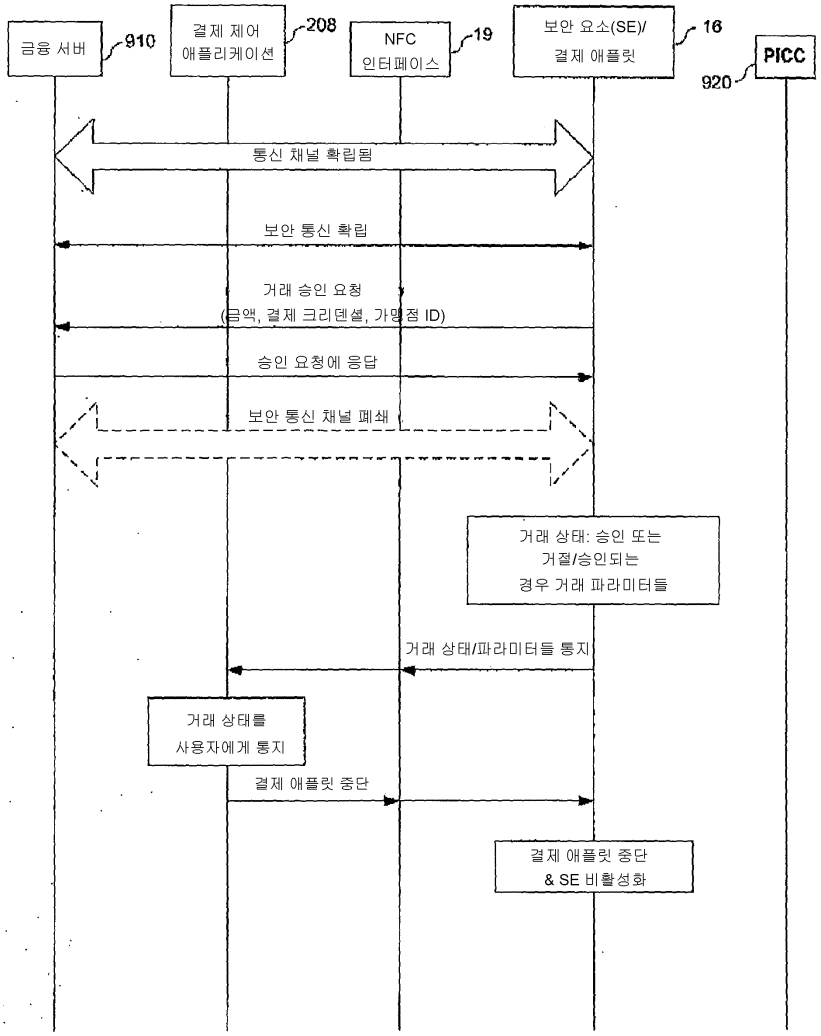
도면9a


금융 서버
910
결제 제어 애플리케이션
208
NFC 인터페이스
19
보안 요소(SE)/ 결제 애플릿
16
PICC
920
사용자 거래(금액) 개시
결제 애플릿 시작
SE 활성화 & SE의 결제 애플릿 시작
거래(금액) 시작
판독기 모드 인에이블
RF & 비접촉 활성화
PICC 제시
PICC 검출
PICC 제시 통지
결제 거래 시작
근접 결제 시스템 환경(PPSE) 선택
근접 결제 환경(PPSE) 선택
결제 앱 지원
결제 앱 지원
결제 앱 선택
AID 선택
AID 선택

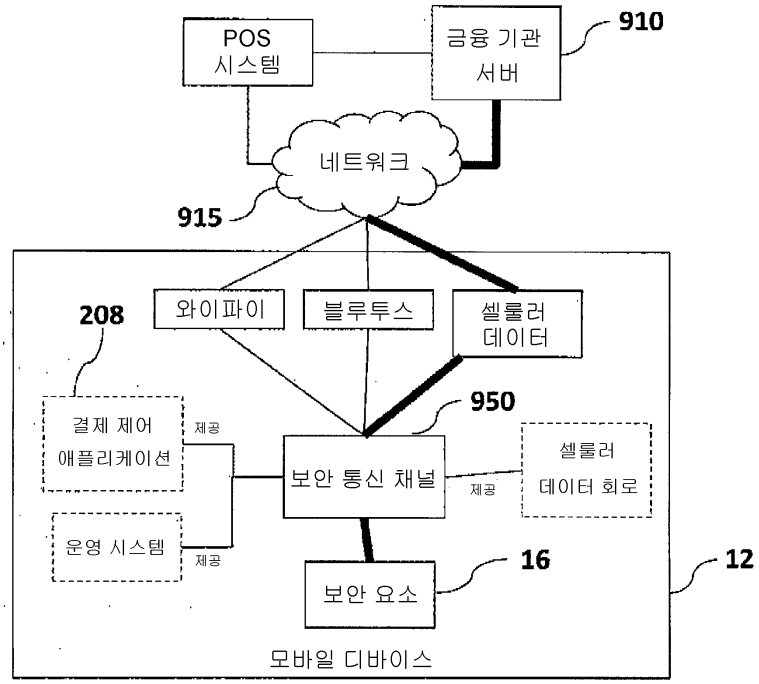
도면9b


금융 서버
910
결제 제어 애플리케이션
208
NFC 인터페이스
19
보안 요소(SE)/ 결제 애플릿
16
920
PICC
Ok/nok (설정 옵션들)
Ok/nok (설정 옵션들)
결제 크리덴셜 판독
결제 크리덴셜을 검색하기 위한 프로토콜
RF & 비접촉 비활성화
선택사항: 결제 크리덴셜 검증 (예컨대, PIN번호 이용)
금융 서버와의 통신 개시
통신 채널 요청
통신 채널 확립
연결

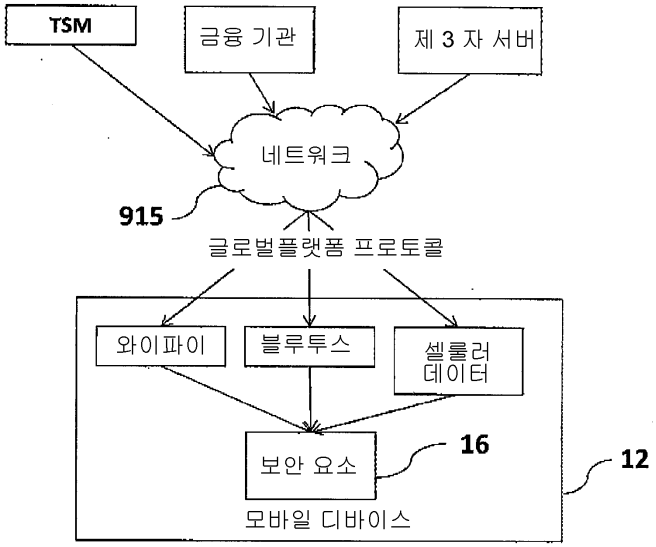
도면9c


금융 서버
910
결제 제어
애플리케이션
208
NFC
인터페이스
19
보안 요소(SE)/
결제 애플릿
16
PICC
920
통신 채널 확립됨
보안 통신 확립
거래 승인 요청
(금액, 결제 크리덴셜, 가맹점 ID)
승인 요청에 응답
보안 통신 채널 폐쇄
거래 상태: 승인 또는
거절/승인되는
경우 거래 파라미터들
거래 상태/파라미터들 통지
거래 상태를
사용자에게 통지
결제 애플릿 중단
결제 애플릿 중단
& SE 비활성화

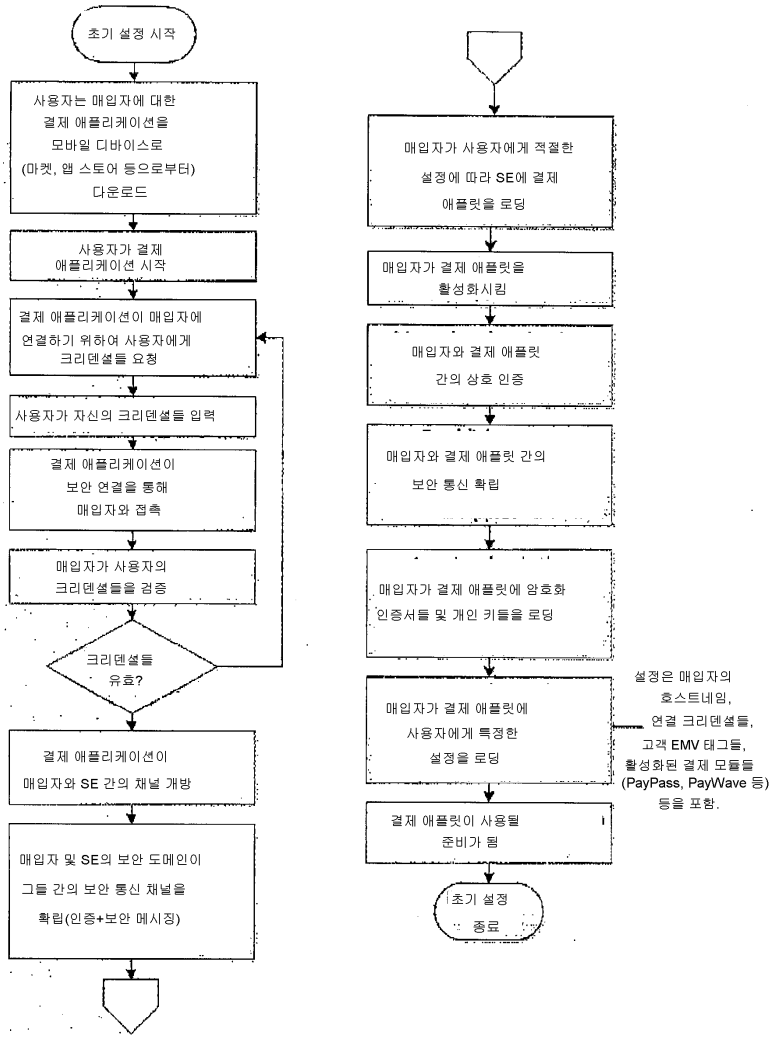
도면10


POS
시스템
금융 기관
서버
910
네트워크
915
208
와이파이
블루투스
셀룰러
데이터
950
결제 제어
애플리케이션
제공
보안 통신 채널
제공
셀룰러
데이터 회로
운영 시스템
제공
16
보안 요소
12
모바일 디바이스

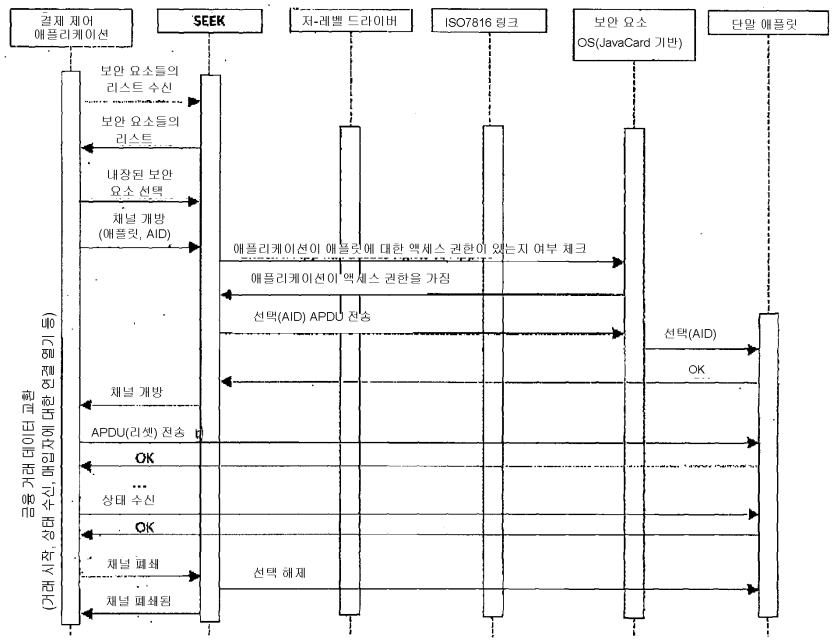
도면11


TSM
금융 기관
제 3 자 서버
네트워크
915
글로벌플랫폼 프로토콜
와이파이
블루투스
셀룰러
데이터
16
보안 요소
12
모바일 디바이스

도면12


초기 설정 시작
사용자는 매입자에 대한 결제 애플리케이션을 모바일 디바이스로 (마켓, 앱 스토어 등으로부터) 다운로드
사용자가 결제 애플리케이션 시작
결제 애플리케이션이 매입자에 연결하기 위하여 사용자에게 크리덴셜들 요청
사용자가 자신의 크리덴셜들 입력
결제 애플리케이션이 보안 연결을 통해 매입자와 접촉
매입자가 사용자의 크리덴셜들을 검증
크리덴셜들 유효?
결제 애플리케이션이 매입자와 SE 간의 채널 개방
매입자 및 SE의 보안 도메인이 그들 간의 보안 통신 채널을 확립(인증+보안 메시징)
매입자가 사용자에게 적절한 설정에 따라 SE에 결제 애플릿을 로딩
매입자가 결제 애플릿을 활성화시킴
매입자와 결제 애플릿 간의 상호 인증
매입자와 결제 애플릿 간의 보안 통신 확립
매입자가 결제 애플릿에 암호화 인증서들 및 개인 키들을 로딩
매입자가 결제 애플릿에 사용자에게 특정한 설정을 로딩
설정은 매입자의 호스트네임, 연결 크리덴셜들, 고객 EMV 태그들, 활성화된 결제 모듈들 (PayPass, PayWave 등) 등을 포함.
결제 애플릿이 사용될 준비가 됨
초기 설정 종료

도면13


결제 제어 애플리케이션
SEEK
저-레벨 드라이버
ISO7816 링크
보안 요소 OS(JavaCard 기반)
단말 애플릿
보안 요소들의 리스트 수신
보안 요소들의 리스트
내장된 보안 요소 선택
채널 개방 (애플릿, AID)
애플리케이션이 애플릿에 대한 액세스 권한이 있는지 여부 체크
애플리케이션이 액세스 권한을 가짐
선택(AID) APDU 전송
선택(AID)
OK
채널 개방
APDU(리셋) 전송
OK
...
상태 수신
OK
채널 폐쇄
선택 해제
채널 폐쇄됨
금융 거래 데이터 교환 (거래 시작, 상태 수신, 매입자에 대한 연결 열기 등)