



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0071982
(43) 공개일자 2012년07월03일

(51) 국제특허분류(Int. Cl.)

G06Q 20/20 (2012.01) G06Q 20/04 (2012.01)

G06Q 20/40 (2012.01) H04B 5/02 (2006.01)

(21) 출원번호 10-2010-0133733

(22) 출원일자 2010년12월23일

심사청구일자 없음

(71) 출원인

주식회사 케이티

경기도 성남시 분당구 불정로 90 (정자동 206 번지)

(72) 발명자

박재민

서울특별시 관악구 남부순환로247길 14, 401호 (봉천동)

김경태

서울특별시 광진구 광나루로56길 32, 현대2차 APT 206동 501호 (구의동)

(74) 대리인

특허법인명문

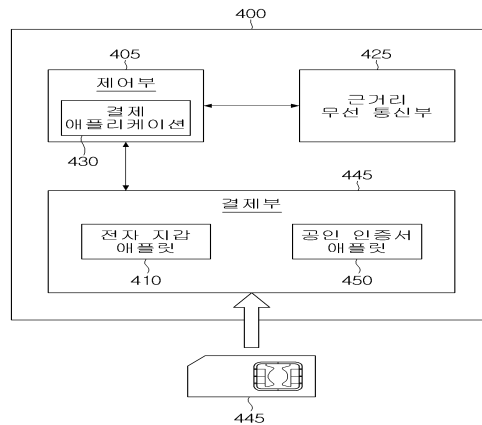
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 안전 결제를 위한 근거리 무선 통신 단말, 및 근거리 무선 통신 단말을 이용한 안전 결제 방법

(57) 요약

안전 결제를 위한 근거리 무선 통신 단말은, 근거리 무선 통신부 및 결제부를 포함한다. 근거리 무선 통신부는 외부의 결제 단말과 통신한다. 결제부는 결제 단말이 외부의 결제 서버에 결제를 요청하도록 거래 정보에 대한 처리 결과 및 거래 정보에 대한 전자 서명값을 근거리 무선 통신부를 통해 결제 단말로 전달한다. 결제부에 포함된 공인 인증서 애플릿은 거래 정보에 대한 전자 서명값을 생성하고 결제부에 포함된 전자 지갑 애플릿은 거래 정보에 대한 처리 결과 및 전자 서명값을 결제 단말에 전달한다.

대표도 - 도3



특허청구의 범위

청구항 1

외부의 결제 단말과 통신하는 근거리 무선 통신부; 및

상기 결제 단말이 외부의 결제 서버에 결제를 요청하도록 거래 정보에 대한 처리 결과 및 상기 거래 정보에 대한 전자 서명값을 상기 근거리 무선 통신부를 통해 상기 결제 단말로 전달하는 결제부를 포함하며,

상기 결제부에 포함된 공인 인증서 애플릿은 상기 거래 정보에 대한 전자 서명값을 생성하고 상기 결제부에 포함된 전자 지갑 애플릿은 상기 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 상기 결제 단말에 전달하는 안전 결제를 위한 근거리 무선 통신 단말.

청구항 2

제1항에 있어서, 상기 근거리 무선 통신 단말은,

상기 근거리 무선 통신부의 동작과, 상기 결제부의 동작을 제어하는 제어부를 더 포함하며,

상기 전자 지갑 애플릿은 상기 제어부에 포함된 결제 애플리케이션을 호출하고 상기 결제 단말로부터 전송되는 거래 정보를 상기 결제 애플리케이션에 전달하며,

상기 결제 애플리케이션은 상기 근거리 무선 통신 단말의 이용자에 의해 공인 인증서 패스워드가 입력되도록 유저 인터페이스(user interface)를 제공하고,

상기 결제 애플리케이션은 상기 공인 인증서 패스워드를 통해 상기 공인 인증서 애플릿으로부터 상기 전자 서명값을 획득하고 상기 거래 정보를 처리하여 상기 거래 정보에 대한 처리 결과를 생성하여 상기 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 상기 전자 지갑 애플릿에 전달하는 안전 결제를 위한 근거리 무선 통신 단말.

청구항 3

제2항에 있어서,

상기 결제 단말은 상기 전자 지갑 애플릿으로부터 전달되는 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 암호화하여 상기 결제 서버로 전송하는 안전 결제를 위한 근거리 무선 통신 단말.

청구항 4

외부의 결제 단말과 통신하는 근거리 무선 통신부;

상기 결제 단말이 외부의 결제 서버에 결제를 요청하도록 거래 정보에 대한 처리 결과 및 상기 거래 정보에 대한 전자 서명값을 상기 근거리 무선 통신부를 통해 상기 결제 단말로 전달하는 결제부; 및

상기 근거리 무선 통신부의 동작과, 상기 결제부의 동작을 제어하는 제어부를 포함하며,

상기 결제부에 포함된 전자지갑 애플릿과 상기 결제부에 포함된 공인 인증서 애플릿과 상기 제어부에 포함된 결제 애플리케이션은 서로 연동하여 상기 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 생성하여 상기 결제 단말로 전달하는 안전 결제를 위한 근거리 무선 통신 단말.

청구항 5

외부의 결제 단말과 통신하는 근거리 무선 통신부;

상기 결제 단말이 외부의 결제 서버에 결제를 요청하도록 거래 정보에 대한 처리 결과 및 상기 거래 정보에 대한 전자 서명값을 상기 근거리 무선 통신부를 통해 상기 결제 단말로 전달하는 결제부; 및

상기 근거리 무선 통신부의 동작과, 상기 결제부의 동작을 제어하는 제어부를 포함하며,

상기 결제부에 포함된 전자 지갑 애플릿은 상기 제어부에 포함된 결제 애플리케이션을 호출하고 상기 결제 단말로부터 전송되는 거래 정보를 상기 결제 애플리케이션에 전달하고, 상기 결제 애플리케이션은 상기 결제부

에 포함된 공인 인증서 애플릿이 거래 정보에 대한 전자 서명값을 생성하도록 요청하고,

상기 결제 애플리케이션은 상기 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 상기 전자 지갑 애플릿에 전달하고,

상기 전자 지갑 애플릿은 상기 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 상기 결제 단말에 전달하는 안전 결제를 위한 근거리 무선 통신 단말.

청구항 6

근거리 무선 통신 단말을 이용한 안전 결제 방법에 있어서,

(a) 외부의 결제 단말로부터 거래 정보를 수신한 상기 근거리 무선 통신 단말의 결제부에 포함된 전자 지갑 애플릿이 상기 근거리 무선 통신 단말의 제어부에 포함된 결제 애플리케이션을 호출하고 상기 전자 지갑 애플릿이 상기 거래 정보를 상기 결제 애플리케이션에 전달하는 단계;

(b) 상기 결제 애플리케이션이 상기 결제부에 포함된 공인 인증서 애플릿을 호출하여 상기 공인 인증서 애플릿이 상기 거래 정보에 대한 전자 서명값을 생성하는 단계; 및

(c) 상기 결제 애플리케이션이 상기 거래 정보를 처리하여 상기 거래 정보에 대한 처리 결과를 생성하고 상기 생성된 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 상기 전자 지갑 애플릿에 전달하는 단계를 포함하며,

상기 거래 정보에 대한 처리 결과 및 상기 전자 서명값은 상기 결제 단말로 전달되는 근거리 무선 통신 단말을 이용한 안전 결제 방법.

청구항 7

제6항에 있어서, 상기 (b) 단계는,

상기 결제 애플리케이션이 상기 근거리 무선 통신 단말의 이용자에 의해 공인 인증서 패스워드가 입력되도록 유저 인터페이스(user interface)를 제공하여 상기 공인 인증서 애플릿이 호출되도록 하는 단계를 더 포함하는 근거리 무선 통신 단말을 이용한 근거리 무선 통신 단말을 이용한 안전 결제 방법.

청구항 8

제6항에 있어서,

상기 결제 단말은 상기 전자 지갑 애플릿으로부터 전달된 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 암호화하여 외부의 결제 서버로 전송하는 근거리 무선 통신 단말을 이용한 안전 결제 방법.

명세서

기술 분야

[0001] 본 발명은, 이동통신 단말기(mobile communication terminal)에 관한 것으로서, 보다 상세하게는, 안전 결제를 위한 근거리 무선 통신 단말, 및 근거리 무선 통신 단말을 이용한 안전 결제 방법이다.

배경 기술

[0002] 일반적으로, 상점이나 식당 등에서 비용을 지불할 경우에 있어서, 현금에 의한 결제뿐만 아니라 신용카드 등에 의한 결제가 널리 행해지고 있다. 상기 신용카드에 의한 결제 방법으로는 각 가맹점에 카드사와 유선망으로 연결된 결제 단말기를 구비하고, 상기 결제 단말기의 리더기를 통해 상기 신용카드를 읽힘으로써 결제가 이루어지게 된다.

[0003] 최근에는 상기 신용카드를 통한 결제 방법뿐만 아니라 비접촉식 RF(radio frequency) 액세스 장치에 의한 휴대폰 결제 방법들이 제안되어 실용화되고 있다. 또한, 상기 신용카드에도 RF 모듈을 내장하여 비접촉식 결제가 이루어질 수 있도록 구현되는 방법이 제안되고 있다.

[0004] 한편, 휴대폰을 이용하여 결제할 때 결제 금액이 특정 금액(예를 들어, 30만원) 이상일 경우 또는 신용카드 사업자가 원할 경우, 오프라인(offline) 상의 매장에서 전자 서명(electronic signature)이 필요한 경우가 있

을 수 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명이 해결하고자 하는 기술적 과제는, 전자 서명을 오프라인(offline)상에서 간편하게 수행할 수 있는 안전 결제를 위한 근거리 무선 통신 단말, 및 근거리 무선 통신 단말을 이용한 안전 결제 방법을 제공하는 것이다.

과제의 해결 수단

[0006] 상기 기술적 과제를 달성하기 위하여, 본 발명의 실시예에 따른 안전 결제를 위한 근거리 무선 통신 단말은, 외부의 결제 단말과 통신하는 근거리 무선 통신부; 및 상기 결제 단말이 외부의 결제 서버에 결제를 요청하도록 거래 정보에 대한 처리 결과 및 상기 거래 정보에 대한 전자 서명값을 상기 근거리 무선 통신부를 통해 상기 결제 단말로 전달하는 결제부를 포함할 수 있다.

[0007] 상기 결제부에 포함된 공인 인증서 애플릿은 상기 거래 정보에 대한 전자 서명값을 생성하고 상기 결제부에 포함된 전자 지갑 애플릿은 상기 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 상기 결제 단말에 전달할 수 있다.

[0008] 상기 근거리 무선 통신 단말은, 상기 근거리 무선 통신부의 동작과, 상기 결제부의 동작을 제어하는 제어부를 더 포함할 수 있다. 상기 전자 지갑 애플릿은 상기 제어부에 포함된 결제 애플리케이션을 호출하고 상기 결제 단말로부터 전송되는 거래 정보를 상기 결제 애플리케이션에 전달할 수 있다. 상기 결제 애플리케이션은 상기 근거리 무선 통신 단말의 이용자에 의해 공인 인증서 패스워드가 입력되도록 유저 인터페이스(user interface)를 제공할 수 있다. 상기 결제 애플리케이션은 상기 공인 인증서 패스워드를 통해 상기 공인 인증서 애플릿으로부터 상기 전자 서명값을 획득하고 상기 거래 정보를 처리하여 상기 거래 정보에 대한 처리 결과를 생성하여 상기 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 상기 전자 지갑 애플릿에 전달할 수 있다.

[0009] 상기 결제 단말은 상기 전자 지갑 애플릿으로부터 전달되는 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 암호화하여 상기 결제 서버로 전송할 수 있다.

[0010] 상기 기술적 과제를 달성하기 위하여, 본 발명의 다른 실시예에 따른 안전 결제를 위한 근거리 무선 통신 단말은, 외부의 결제 단말과 통신하는 근거리 무선 통신부; 상기 결제 단말이 외부의 결제 서버에 결제를 요청하도록 거래 정보에 대한 처리 결과 및 상기 거래 정보에 대한 전자 서명값을 상기 근거리 무선 통신부를 통해 상기 결제 단말로 전달하는 결제부; 및 상기 근거리 무선 통신부의 동작과, 상기 결제부의 동작을 제어하는 제어부를 포함할 수 있다.

[0011] 상기 결제부에 포함된 전자지갑 애플릿과 상기 결제부에 포함된 공인 인증서 애플릿과 상기 제어부에 포함된 결제 애플리케이션은 서로 연동하여 상기 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 생성하여 상기 결제 단말로 전달할 수 있다.

[0012] 상기 기술적 과제를 달성하기 위하여, 본 발명의 다른 실시예에 따른 안전 결제를 위한 근거리 무선 통신 단말은, 외부의 결제 단말과 통신하는 근거리 무선 통신부; 상기 결제 단말이 외부의 결제 서버에 결제를 요청하도록 거래 정보에 대한 처리 결과 및 상기 거래 정보에 대한 전자 서명값을 상기 근거리 무선 통신부를 통해 상기 결제 단말로 전달하는 결제부; 및 상기 근거리 무선 통신부의 동작과, 상기 결제부의 동작을 제어하는 제어부를 포함할 수 있다.

[0013] 상기 결제부에 포함된 전자 지갑 애플릿은 상기 제어부에 포함된 결제 애플리케이션을 호출하고 상기 결제 단말로부터 전송되는 거래 정보를 상기 결제 애플리케이션에 전달하고, 상기 결제 애플리케이션은 상기 결제부에 포함된 공인 인증서 애플릿이 거래 정보에 대한 전자 서명값을 생성하도록 요청할 수 있다. 상기 결제 애플리케이션은 상기 전자 지갑 애플릿에 상기 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 전달할 수 있다. 상기 전자 지갑 애플릿은 상기 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 상기 결제 단말에 전달할 수 있다.

[0014] 상기 기술적 과제를 달성하기 위하여, 본 발명의 다른 실시예에 따른 안전 결제를 위한 근거리 무선 통신 단말을 이용한 안전 결제 방법에 관한 것으로서, 상기 안전 결제 방법은, (a) 외부의 결제 단말로부터 거래 정

보를 수신한 상기 근거리 무선 통신 단말의 결제부에 포함된 전자 지갑 애플릿이 상기 근거리 무선 통신 단말의 제어부에 포함된 결제 애플리케이션을 호출하고 상기 전자 지갑 애플릿이 상기 거래 정보를 상기 결제 애플리케이션에 전달하는 단계; (b) 상기 결제 애플리케이션이 상기 결제부에 포함된 공인 인증서 애플릿을 호출하여 상기 공인 인증서 애플릿이 상기 거래 정보에 대한 전자 서명값을 생성하는 단계; 및 (c) 상기 결제 애플리케이션이 상기 거래 정보를 처리하여 상기 거래 정보에 대한 처리 결과를 생성하고 상기 생성된 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 상기 전자 지갑 애플릿에 전달하는 단계를 포함할 수 있다. 상기 거래 정보에 대한 처리 결과 및 상기 전자 서명값은 상기 결제 단말로 전달될 수 있다.

[0015] 상기 (b) 단계는, 상기 결제 애플리케이션이 상기 근거리 무선 통신 단말의 이용자에 의해 공인 인증서 패스워드가 입력되도록 유저 인터페이스(user interface)를 제공하여 상기 공인 인증서 애플릿이 호출되도록 하는 단계를 더 포함할 수 있다.

[0016] 상기 결제 단말은 상기 전자 지갑 애플릿으로부터 전달된 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 암호화하여 외부의 결제 서버로 전송할 수 있다.

발명의 효과

[0017] 본 발명에 따른 안전 결제를 위한 근거리 무선 통신 단말, 및 근거리 무선 통신 단말을 이용한 안전 결제 방법은, 근거리 무선 통신 단말에 내장된 전자 지갑 애플릿(applet)과 결제 애플리케이션과 공인 인증서 애플릿을 서로 연동시켜 거래 정보에 대한 전자 서명 값을 생성시킬 수 있으므로, 본 발명의 근거리 무선 통신 단말의 사용자인 상품의 구입자가 전자 서명(또는 디지털 서명)을 간편하게 수행하여 상품에 대해 오프라인(offline)으로 결제할 수 있도록 할 수 있다. 예를 들어, 매장의 결제 동글(dongle)과 같은 결제 단말에 결제할 때 본 발명을 이용하면 전자 서명이 필요한 결제 서비스가 용이하게 수행될 수 있다.

[0018] 또한, 본 발명에 따른 안전 결제를 위한 근거리 무선 통신 단말, 및 근거리 무선 통신 단말을 이용한 안전 결제 방법은 공인 인증서가 저장된 공인 인증서 애플릿을 이용하므로, 정보 유출 등의 위험을 줄이고 개인정보 도용이나 변조를 차단하여 물품을 구입할 때 안전한 결제가 가능하게 할 수 있고, 무선 동글과 같은 결제 단말에 의한 개인 정보의 유출을 최소화할 수 있다.

도면의 간단한 설명

[0019] 본 발명의 상세한 설명에서 사용되는 도면을 보다 충분히 이해하기 위하여, 각 도면의 간단한 설명이 제공된다.

도 1은 본 발명의 실시예에 따른 근거리 무선 통신 단말을 이용한 안전 결제 방법(100)을 설명하는 도면이다.

도 2는 도 1에 도시된 근거리 무선 통신 단말(400)의 안전 결제를 위한 예시적 동작(108)을 설명하는 도면이다.

도 3은 본 발명의 실시예에 따른 안전 결제를 위한 근거리 무선 통신 단말(400)을 설명하는 블록 다이어그램(block diagram)이다.

도 4는 본 발명의 다른 실시예에 따른 근거리 무선 통신 단말을 이용한 안전 결제 방법(500)을 설명하는 흐름도(flow chart)이다.

발명을 실시하기 위한 구체적인 내용

[0020] 본 발명 및 본 발명의 실시예에 의하여 달성되는 목적을 충분히 이해하기 위해서는, 본 발명의 실시예를 예시하는 첨부 도면 및 첨부 도면에 기재된 내용이 참조되어야 한다.

[0021] 이하, 첨부한 도면을 참조하여 본 발명의 실시예를 설명하는 것에 의해, 본 발명을 상세히 설명한다. 각 도면에 제시된 동일한 참조 부호는 동일한 구성 요소를 나타낸다.

[0022] 도 1은 본 발명의 실시예에 따른 근거리 무선 통신 단말을 이용한 안전 결제 방법(100)을 설명하는 도면이다. 도 2는 도 1에 도시된 근거리 무선 통신 단말(400)의 안전 결제를 위한 예시적 동작(108)을 설명하는 도면이다.

[0023] 도 1 및 도 2를 참조하여 근거리 무선 통신 단말을 이용한 안전 결제 방법(100)이 다음과 같이 설명된다.

[0024] 도 1을 참조하면, 근거리 무선 통신 단말을 이용한 안전 결제 방법(100)은 금융 기관 또는 신용카드 사업자의

결제 인프라(infra)에 포함된 결제 서버(200)와 매장의 결제 동글(dongle)(휴대폰 결제 인식기)과 같은 결제 단말(300)과 근거리 무선 통신 단말(400)이 서로 연동하여 동작한다. 상기 결제 동글은, 백화점, 대형 마트, 편의점, 또는 가맹점에 설치될 수 있다.

- [0025] 입력 단계(102)에 따르면, 매장 직원에 의해 결제 단말(300)에 결제 금액이 특정 금액(예를 들어, 30만원) 이상이 입력될 때 전자 서명의 입력이 요구될 수 있거나 또는 상품(물품)에 대한 결제가 수행될 때 상품의 구입자가 가입한 신용카드 사업자에 의해 결제 단말(300)에 전자 서명의 입력이 요구될 수 있다.
- [0026] 통신 단계(104)에 따르면, 결제 단말(300)과 근거리 무선 통신 단말(400)이 서로 근거리 무선 통신을 수행한다. 보다 상세히 설명하면, 결제 단말(300)의 통신부는 근거리 무선 통신 단말(400)의 근거리 무선 통신부(NFC(near field communication) 통신 칩(chip))와 통신을 수행하여 근거리 무선 통신 단말(400)의 결제부인 NFC USIM(universal subscriber identity module) 카드에 포함된 전자 지갑 애플릿을 선택하여 결제를 요청한다. 상기 결제 요청에 대한 응답으로, 근거리 무선 단말(400)의 전자 지갑 애플릿이 구동되고, 상기 전자 지갑 애플릿은 거래 정보를 요청한다.
- [0027] 전달 단계(106)에 따르면, 결제 단말(300)은 상기 전자 지갑 애플릿의 거래 정보에 대한 요청에 따라 자신의 통신부를 이용하여 상품에 대한 거래 정보(hashed value)를 근거리 통신 단말(400)의 전자 지갑 애플릿에 전달한다.
- [0028] 도 2를 참조하면, 근거리 무선 통신 단말(400)은, 전자 지갑 애플릿(410), 결제 애플리케이션(application)(430), 및 공인 인증서 애플릿(450)을 포함한다. 전자 지갑 애플릿(410), 결제 애플리케이션(application)(430), 및 공인 인증서 애플릿(450)은 서로 연동하여 동작한다. 전자지갑 애플릿(410) 및 공인 인증서 애플릿(450)은 근거리 무선 통신 단말(400)에 삽입(설치)되는 NFC 유심(USIM) 카드에 내장되는 소프트웨어일 수 있고, 자바 카드 플랫폼(java card platform)으로 구성(구현)될 수 있다. 결제 애플리케이션(430)은 근거리 무선 통신 단말(400)의 제어부에 포함된 전자 결제를 위한 소프트웨어이다. 자바 카드는, 개인 금융, 신용 카드, 교통 카드, 및 의료 카드 등 많은 분야에서 다양한 형태로 이용될 수 있다.
- [0029] 호출 단계(108a)에 따르면, 전자 지갑 애플릿(410)은 휴먼 컴퓨터 인터랙션(Human Computer Interaction, HCI) 표준의 연결(connectivity)을 이용하여 결제 애플리케이션(또는 단말 애플리케이션)(430)을 호출하고 전자 서명 대상의 거래 정보를 결제 애플리케이션(430)에 전달한다. 상기 호출에 사용되는 인터페이스는, 예를 들어, 자바 카드 어플리케이션(API: Application Program Interface, 응용프로그램 인터페이스)일 수 있다.
- [0030] 입력 단계(108b)에 따르면, 근거리 무선 통신 단말(400)의 사용자는 결제 애플리케이션(430)에 의해 제공되는 단말의 유저 인터페이스(UI)(user interface)를 통해 공인 인증서의 패스워드를 입력한다.
- [0031] 요청 단계(108c)에 따르면, 입력 단계(108b)에서 입력된 공인 인증서 패스워드에 따라 결제 애플리케이션(430)은 공인 인증서 애플릿(450)을 호출하여 공인 인증서 애플릿(450)에 거래 정보에 대해 전자 서명을 요청한다.
- [0032] 획득 단계(108d)에 따르면, 결제 애플리케이션(430)은 공인 인증서 애플릿(450)으로부터 요청 단계(108c)에서 요청한 전자 서명값을 획득한다.
- [0033] 응답 단계(108e)에 따르면, 결제 애플리케이션(430)은 상기 거래 정보를 처리하여 거래 정보에 대한 결과를 생성하여 거래 정보에 대한 결과 및 상기 전자 서명값을 전자 지갑 애플릿(410)로 응답(전달)한다.
- [0034] 유심(USIM) 카드에 내장된 전자 지갑 애플릿(410) 및 공인 인증서 애플릿(450)과, 결제 애플리케이션(430) 상호간의 데이터 통신은 APDU(Application Protocol Data Unit) 통신일 수 있다.
- [0035] 전자 지갑 애플릿(410), 결제 애플리케이션(application)(430), 및 공인 인증서 애플릿(450) 상호간의 호출에 사용되는 인터페이스는, 예를 들어, API일 수 있다.
- [0036] 다시 도 1을 참조하면, 응답 단계(110)에서 근거리 무선 통신 단말(400)의 전자 지갑 애플릿(410)이 근거리 무선 통신 단말(400)의 근거리 무선 통신부를 통해 거래 정보에 대한 처리 결과 및 전자 서명값을 결제 단말(300)에 응답(전달)한다.
- [0037] 암호화 단계(112)에 따르면, 결제 단말(300)은 응답 단계(110)에서 전달된 거래 정보의 처리 결과 및 전자 서명값을 이용하여 전자 서명값이 포함된 거래 정보 원본을 생성하고 거래 정보 원본을 암호화할 수 있다. 여기서, 결제 단말(300)은, 예를 들어, PKCS(public-key cryptography system) #7과 같은 암호화 프로그램을 이용

하여 거래 정보 원본을 암호화할 수 있다.

- [0038] 요청 단계(114)에 따르면, 결제 단말(300)은 암호화 단계(114)에서 생성된 거래 정보 원본의 암호화 값(유심(USIM) 정보)을 금융기관(은행 등) 또는 신용카드 사업자(신용 카드 업체)의 결제 서버(200)에 전송하여 결제를 요청한다.
- [0039] 승인 단계(116)에 따르면, 결제 서버(또는 웹 서버)(200)는 전송 단계(114)에서의 암호화 값에 대해 확인하고 승인하여 요청 단계(114)에서의 결제 요청에 대한 결제 결과를 결제 단말(300)로 전송한다.
- [0040] 결제 단말(300)은, 예를 들어, 결제 서버(200)와 무선접속장치(AP, access point) 또는 기지국을 통해 무선 인터넷 망 또는 유선 인터넷 망을 통해 통신할 수 있다.
- [0041] 도 3은 본 발명의 실시예에 따른 안전 결제를 위한 근거리 무선 통신 단말(400)을 설명하는 블록 다이어그램(block diagram)이다.
- [0042] 도 3을 참조하면, 근거리 무선 통신 단말(400)은, 제어부(405), 근거리 무선 통신부(425), 및 결제부(445)를 포함한다. 근거리 무선 통신 단말(400)은 스마트 폰(smart phone)과 같은 휴대폰 또는 PDA(personal digital assistant)일 수 있다.
- [0043] 근거리 무선 통신부(425)는 근거리 무선 통신 단말(400)의 외부에 배치된 결제 단말(도 1의 300)과 통신한다. 근거리 무선 통신부(425)는 NFC 칩으로 구현가능하고, NFC 칩은, 예를 들어, 13.56 (MHz) 대역에서 RFID(radio Frequency identification) 리더 기능과 함께 태그 기능을 동시에 수행할 수 있는 칩으로 근거리 데이터 통신을 가능하게 한다.
- [0044] 근거리 무선 통신부(425)는, 근거리 무선 통신을 위한 무선 안테나(RF(radio frequency) 안테나) 및 NFC 칩(near field communication 모듈)을 포함할 수 있다. 근거리(단거리) 무선 통신(NFC, near field communication)은 모바일(mobile) RFID(radio frequency identification)의 한 방식으로 장치 상호간의 통신이 가능한 기술이다. NFC 기술이 탑재된 휴대폰을 결제 장치에 접촉하면 인증(authentication)과 결제가 가능하다.
- [0045] NFC(Near Field Communication)는 근거리 무선통신 기술로 모바일 RFID의 일종으로, 기존 유심(USIM)카드를 이용한 T머니 서비스 등과 비슷하지만 읽기와 쓰기가 가능해 쌍방향 데이터 전송이 가능한 기술이다.
- [0046] 결제부(445)는 보안 모듈(가입자 인증 모듈)인 USIM (universal subscriber identity module)을 탑재한다. USIM은 가입자 정보를 탑재한 SIM(subscriber identity module) 카드와 UICC(universal IC card)가 결합된 형태로써 사용자 인증과 글로벌 로밍, 전자 상거래 등 다양한 기능을 1장의 카드에 구현한 것이다. 3세대 이동통신(WCDMA)의 단말기에 탑재된다.
- [0047] 결제부(445)는 외부의 결제 단말(도 1의 300)이 외부의 결제 서버(도 1의 200)에 결제를 요청하도록 거래 정보에 대한 처리 결과 및 거래 정보에 대한 전자 서명값을 근거리 무선 통신부(425)를 통해 상기 결제 단말로 전달한다. 상기 결제 단말은 전자 지갑 애플릿(410)으로부터 전달된 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 암호화하여 결제 서버(도 1의 200)로 전송한다.
- [0048] 결제부(445)는 전자 지갑(electronic wallet 또는 digital wallet) 애플릿(410) 및 공인 인증서 애플릿(450)을 포함한다. 전자 지갑 애플릿(410) 또는 공인 인증서 애플릿(450)은 결제부(445) 내부의 메모리(미도시)에 저장될 수 있다. 도 4에 근거리 무선 통신 단말(400)에 설치(삽입)되는 실제 형태의 NFC 유심(USIM) 카드(445)가 도시되어 있다. 유심(USIM) 카드(445)는 결제부(445)에 대응할 수 있다.
- [0049] 유심(USIM) 카드(또는 스마트 카드(smart card))는, ISO(International Standardization Organization) 7816에 규정된 인터페이스 방식에 따라 데이터를 송수신하는 마이크로프로세서와 메모리 및 다양한 응용프로그램을 내장하여 전자지갑, 신용카드, 의료카드, SIM(subscriber identity module) 카드 등 보다 높은 보안성이 요구되는 분야에 있어서 휴대성, 편리성, 보안성 등의 기능을 제공하는 카드일 수 있다.
- [0050] 전자 지갑 애플릿(410)은 제어부(405)에 포함된 결제 애플리케이션(430)을 호출하고 상기 결제 단말로부터 전송되는 거래 정보를 결제 애플리케이션(430)에 전달한다. 전자 지갑 애플릿(410)은 결제 애플리케이션(430)에서 처리된 거래 정보에 대한 처리 결과 및 거래 정보에 대한 전자 서명값을 근거리 무선 통신부(425)를 통해 상기 결제 단말에 전달한다. 본 발명의 다른 실시예에 있어서, 근거리 무선 통신부(425)와 결제부(445)는 도 3에 도시된 바와 달리 제어부(405)를 통해 데이터 신호를 교환하지 않고 제어부(405)의 제어에 따라 직접 데

이더 신호를 교환할 수도 있다.

- [0051] 공인 인증서 애플릿(450)은 결제 애플리케이션(430)의 요청에 따라 상품의 거래 정보에 대한 전자 서명값을 생성한다. 공인 인증서 애플릿(450)에는 공인 인증서가 발급이 완료되어 저장되어 있다.
- [0052] 제어부(405)는 CPU(central processing unit)의 기능을 수행하는 NFC control chip에 대응하며, 근거리 무선 통신부(425)의 동작과, 결제부(445)의 동작을 제어할 수 있다. 제어부(405)에는 결제 애플리케이션(430)이 탑재된다. 결제 애플리케이션(430)은 신용카드 애플리케이션으로도 언급될 수 있다.
- [0053] 결제 애플리케이션(430)은 근거리 무선 통신 단말(400)의 이용자에 의해 공인 인증서 패스워드가 입력되도록 유저 인터페이스(user interface)를 제공할 수 있다.
- [0054] 결제 애플리케이션(430)은 공인 인증서 패스워드를 통해 공인 인증서 애플릿(450)으로부터 전자 서명값을 획득하고 거래 정보를 처리하여 거래 정보에 대한 처리 결과를 생성하여 거래 정보에 대한 처리 결과 및 거래 정보에 대한 전자 서명값을 전자 지갑 애플릿(410)에 전달한다. 결제 애플리케이션(430)은 공인 인증서 애플릿(450)이 거래 정보에 대한 전자 서명값을 생성하도록 요청한다.
- [0055] 전술한 바와 같이, 본 발명의 실시예에 있어서, 전자 지갑 애플릿(410)과 공인 인증서 애플릿(450)과 결제 애플리케이션(430)은 서로 연동하여 거래 정보에 대한 처리 결과 및 상기 거래 정보에 대한 전자 서명값을 생성하여 상기 결제 단말로 전달할 수 있다.
- [0056] 본 발명의 근거리 무선 통신 단말(400)은 전술한 구성 요소 외에 스마트폰과 같은 휴대폰 또는 PDA의 기능을 수행하는 칩(chip)과 같은 구성 요소를 더 포함하여 휴대폰 또는 PDA(personal digital assistant)로도 사용될 수 있다.
- [0057] 도 4는 본 발명의 다른 실시예에 따른 근거리 무선 통신 단말을 이용한 안전 결제 방법(500)을 설명하는 흐름도(flow chart)이다. 근거리 무선 통신 단말을 이용한 안전 결제 방법(500)은 도 1 및 도 2에 도시된 결제 서버, 결제 단말, 및 근거리 무선 통신 단말 또는 도 3에 도시된 근거리 무선 통신 단말에 적용될 수 있다.
- [0058] 도 4를 참조하면, 수신 단계(502)에 있어서, 근거리 무선 통신 단말의 결제부에 포함된 전자 지갑 애플릿은 근거리 무선 통신을 통해 외부의 결제 단말로부터 상품에 대한 거래 정보를 수신한다.
- [0059] 호출 단계(504)에 따르면, 상기 전자 지갑 애플릿은, 상기 근거리 무선 통신 단말의 제어부에 포함된 결제 애플리케이션을 호출하고 상기 거래 정보를 상기 결제 애플리케이션에 전달한다.
- [0060] 호출 단계(506)에 따르면, 상기 결제 애플리케이션이 상기 결제부에 포함된 공인 인증서 애플릿을 호출하고 상기 호출된 공인 인증서 애플릿은 상기 거래 정보에 대한 전자 서명값을 생성한다. 호출 단계(506)는 상기 결제 애플리케이션이 상기 근거리 무선 통신 단말의 이용자에 의해 공인 인증서 패스워드가 입력되도록 유저 인터페이스(user interface)를 제공하여 상기 공인 인증서 애플릿이 호출되도록 하는 단계를 더 포함할 수 있다.
- [0061] 전달 단계(508)에 따르면, 상기 결제 애플리케이션이 상기 거래 정보를 처리하여 상기 거래 정보에 대한 처리 결과를 생성하고 상기 생성된 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 상기 전자 지갑 애플릿에 전달한다. 상기 전자 지갑 애플릿에 전달된 거래 정보에 대한 처리 결과 및 전자 서명값은 상기 결제 단말로 전달될 수 있다.
- [0062] 상기 결제 단말은 상기 전자 지갑 애플릿으로부터 전달된 거래 정보에 대한 처리 결과 및 상기 전자 서명값을 암호화하여 외부의 결제 서버로 전송한다.
- [0063] 한편, 전술한 본 발명의 방법은 컴퓨터 프로그램으로 작성이 가능하다. 그리고 상기 프로그램을 구성하는 코드 및 코드 세그먼트는 당해 분야의 컴퓨터 프로그래머에 의하여 용이하게 추론할 수 있다. 또한, 상기 작성된 프로그램은 컴퓨터가 읽을 수 있는 기록매체(정보저장매체)에 저장되고, 컴퓨터에 의하여 판독되고 실행됨으로써 본 발명의 방법을 구현할 수 있다. 그리고 상기 기록매체는 컴퓨터가 판독할 수 있는 모든 형태의 기록매체를 포함할 수 있다.
- [0064] 이상에서와 같이, 도면과 명세서에서 실시예가 개시되었다. 여기서, 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이며 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술 분야의 통상의 지식을 가진 자는 본 발명으로부터 다양한 변형 및 균등한 실시예가 가능하다는 점을 이해할 수 있을 것이다. 따라서 본 발명의 진정한 기술적 보

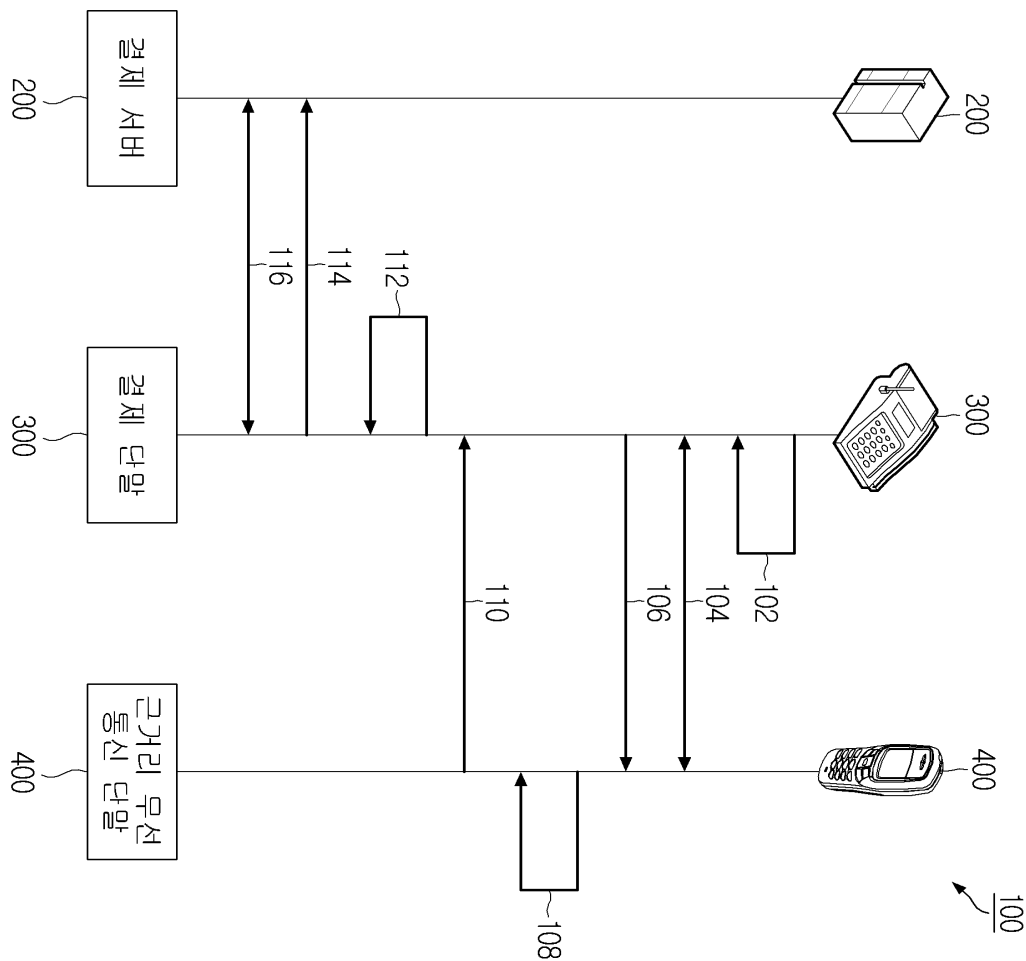
호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

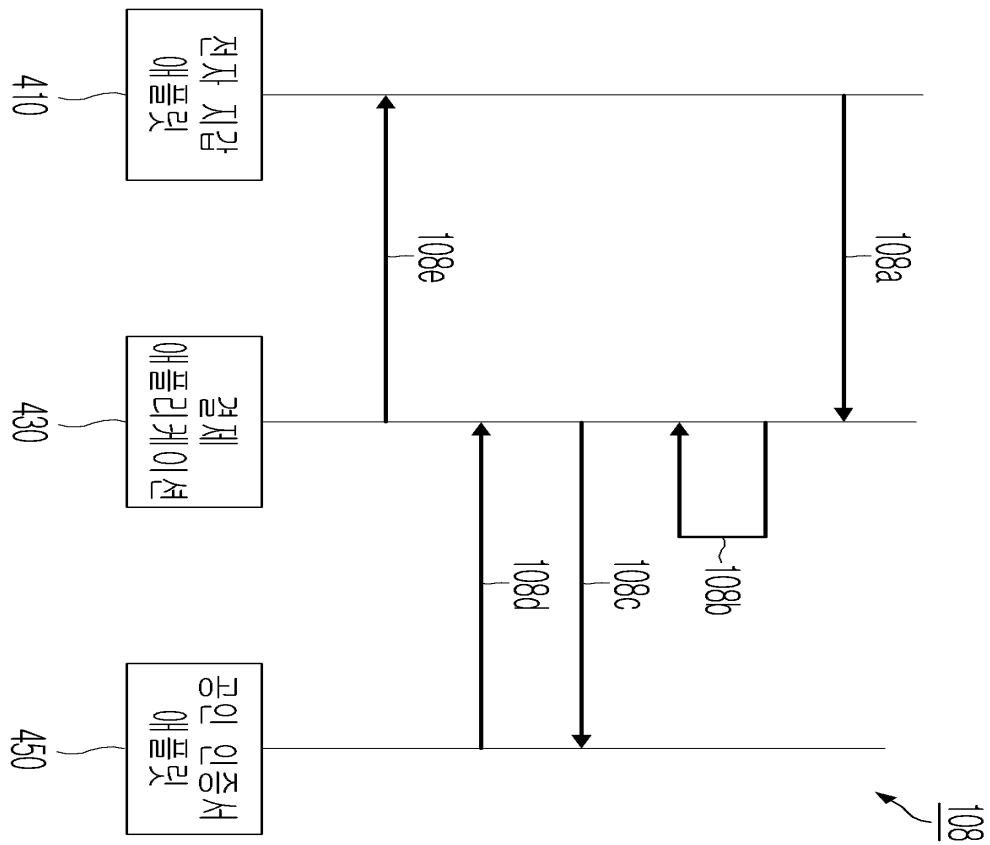
- 200: 결제 서버
- 300: 결제 단말
- 400: 근거리 무선 통신 단말
- 405: 제어부
- 425: 근거리 무선 통신부
- 445: 결제부
- 410: 전자 지갑 애플릿
- 430: 결제 애플리케이션
- 450: 공인 인증서 애플릿

도면

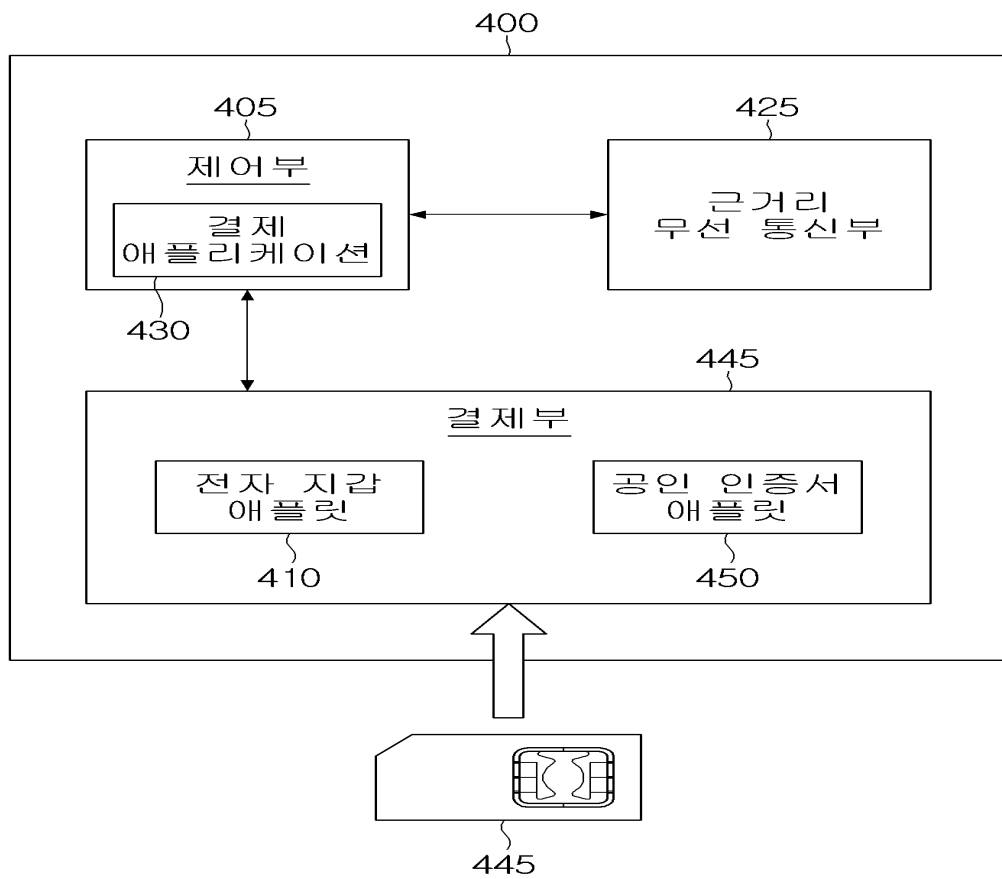
도면1



도면2



도면3



도면4

