(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년05월18일
(11) 등록번호 10-1844993
(24) 등록일자 2018년03월28일

(51) 국제특허분류(Int. Cl.)
G06Q 20/40 (2012.01)
(21) 출원번호 10-2011-0140288
(22) 출원일자 2011년12월22일
심사청구일자 2016년12월05일
(65) 공개번호 10-2013-0082895
(43) 공개일자 2013년07월22일
(56) 선행기술조사문헌
KR1019990086998 A*
KR1020010000329 A*
KR1020080032810 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 케이티
경기도 성남시 분당구 불정로 90(정자동)
(72) 발명자
이민구
경기도 성남시 분당구 판교로 430, 건영아파트 106동 801호 (이매동, 아름마을)
김동완
서울특별시 중구 다산로 32, 10동 604호 (신당동, 남산타운)
(74) 대리인
유미특허법인

전체 청구항 수 : 총 10 항 심사관 : 유원석

(54) 발명의 명칭 **전자카드 결제 방법 및 시스템**

(57) 요 약

전자카드 결제 방법 및 시스템이 개시된다. 결제 시스템은, 상기 결제 서버로부터 서버 인증 정보를 획득하고, 상기 획득된 서버 인증 정보를 이용하여 서버 인증을 수행하고, 상기 결제 서버의 인증 응답에 따라 결제 정보를 포함하는 결제 요청을 상기 결제 서버로 전송하는 전자 카드; 상기 전자 카드와 상기 결제 서버간의 인증 및 결제를 위한 메시지를 중개하는 가맹점 단말; 및 상기 서버 인증에 상응하여 상기 전자 카드로부터 클라이언트 인증 정보를 획득하여 클라이언트 인증을 수행하여 상기 인증 응답을 상기 전자 카드로 전송하고, 상기 결제 요청에 따른 결제 승인을 상기 가맹점 단말을 통해 상기 전자 카드로 전송하는 결제 서버를 포함한다.

대 표 도 - 도1

명 세 서

청구범위

청구항 1

결제 시스템에 있어서,

전자 카드,

상기 전자 카드에서 요청된 결제를 수행하는 결제 서버, 그리고

상기 전자 카드로 결제 정보를 포함하는 결제 정보 확인 요청을 하고, 상기 전자카드와 상기 결제 서버간의 인증 및 결제를 위한 메시지를 중계하여, 상기 결제 서버로부터 상기 결제 정보에 대한 결제 승인 정보를 수신하는 가맹점 단말을 포함하고,

상기 전자 카드는

상기 결제 정보에 대해 결제하기 위한 카드 식별정보를 상기 가맹점 단말로 전송하고, 상기 가맹점 단말로부터 상기 카드 식별정보에 해당하는 서버 인증 정보를 수신하며, 상기 서버 인증 정보를 해독하여 서버 인증을 수행한 후, 상기 결제 서버에서 해독할 수 있는 클라이언트 인증 정보를 상기 가맹점 단말로 전송하고, 상기 가맹점 단말로부터 상기 클라이언트 인증 정보에 대한 인증 성공 메시지를 수신하면, 상기 가맹점 단말로 결제 정보를 포함하는 결제 요청을 하고,

상기 결제 서버는

상기 가맹점 단말로부터 상기 카드 식별정보를 수신하면, 상기 카드 식별정보에 해당하는 서버 인증 정보를 상기 전자 카드에서 해독할 수 있도록 암호화하여 상기 가맹점 단말로 전송하고, 상기 가맹점 단말로부터 상기 클라이언트 인증 정보를 수신하면, 상기 클라이언트 인증 정보를 해독하여 클라이언트 인증을 수행한 후, 상기 가맹점 단말로 상기 인증 성공 메시지를 전송하고, 상기 가맹점 단말로부터 상기 결제 요청을 수신하면, 상기 결제 요청에 따른 상기 결제 승인 정보를 상기 가맹점 단말로 전송하는 결제 시스템.

청구항 2

제1 항에 있어서,

상기 서버 인증 정보는 상기 결제 서버 인증을 위한 서버 인증서 또는 공유 비밀키이고,

상기 클라이언트 인증 정보는 상기 전자 카드 인증을 위해 사전에 상기 결제 서버 또는 공인기관 서버를 통해 발급받은 클라이언트 인증서인 또는 공유 비밀키를 이용하여 생성된 인증정보인 것을 특징으로 하는 결제 시스템.

청구항 3

제1 항에 있어서,

상기 전자 카드 및 상기 결제 서버는 상호 인증을 위해 상기 가맹점 단말에 규약되지 않은 인증 프로토콜을 이용하여 상기 서버 인증 정보 및 상기 클라이언트 인증 정보를 캡슐화하여 상기 가맹점 단말을 통해 전송하여 상호 인증하는 것을 특징으로 하는 결제 시스템.

청구항 4

삭제

청구항 5

제1 항에 있어서,

상기 카드 식별정보는 상기 전자 카드의 카드 번호와 다른 정보인 것을 특징으로 하는 결제 시스템.

청구항 6

전자 카드와 결제 서버간의 인증 및 결제를 위한 메시지를 중계하는 가맹점 단말과 통신하여, 상기 전자 카드가 상기 가맹점 단말에서 요청된 전자 결제를 수행하는 방법에 있어서,

카드 식별정보를 상기 가맹점 단말로 전송하는 단계,

상기 가맹점 단말로부터 상기 카드 식별정보에 해당하는 서버 인증 정보를 수신하는 단계,

상기 서버 인증 정보를 해독하여 서버 인증을 수행한 후, 상기 결제 서버에서 해독할 수 있는 클라이언트 인증 정보를 생성하여 상기 가맹점 단말로 전송하는 단계,

상기 가맹점 단말로부터 상기 클라이언트 인증 정보에 대한 인증 성공 메시지를 수신하는 단계, 그리고

상기 가맹점 단말로 결제 정보를 포함하는 결제 요청을 하는 단계를 포함하고,

상기 서버 인증 정보는 상기 전자 카드에서 해독할 수 있도록 상기 결제 서버에서 생성되고,

상기 인증 성공 메시지는 상기 결제 서버에서 상기 클라이언트 인증 정보를 해독하여 클라이언트 인증하여 생성되는, 전자 결제 방법.

청구항 7

제6 항에 있어서,

상기 전자 카드가 상기 카드 식별정보를 상기 결제 서버로 전송시, 피기백(piggyback)으로 결제 정보를 페이로드하여 함께 전송하는 것을 특징으로 하는 전자 결제 방법.

청구항 8

제6 항에 있어서,

상기 가맹점 단말로부터 상기 결제 요청에 대한 결제 승인 정보를 수신하는 단계를 더 포함하고,

상기 결제 승인 정보는 상기 결제 서버에서 상기 결제 요청에 따른 결제를 수행하여 생성되는, 전자 결제 방법.

청구항 9

제6 항에 있어서,

상기 서버 인증 및 상기 클라이언트 인증을 위해, 상기 전자 카드 및 상기 결제 서버는 각각 상기 가맹점 단말에 규약되지 않은 인증 방식으로 인증을 위해 송수신되는 정보를 캡슐화하여 상호 인증을 수행하는 것을 특징으로 하는 전자 결제 방법.

청구항 10

제6 항에 있어서,

상기 서버 인증 정보 및 상기 클라이언트 인증 정보는 각각 공인 인증서 또는 공유 비밀키를 이용하여 생성된 인증정보인 것을 특징으로 하는 전자 결제 방법.

청구항 11

전자 카드와 결제 서버간의 인증 및 결제를 위한 메시지를 중계하는 가맹점 단말과 통신하여, 상기 결제 서버가 상기 가맹점 단말에서 요청된 전자 결제를 수행하는 방법에 있어서,

상기 가맹점 단말로부터 카드 식별정보를 수신하는 단계,

상기 카드 식별정보에 해당하는 서버 인증 정보를 상기 전자 카드에서 해독할 수 있도록 생성하여 상기 가맹점 단말로 전송하는 단계,

상기 가맹점 단말로부터 클라이언트 인증 정보를 수신하는 단계,

상기 클라이언트 인증 정보를 해독하여 클라이언트 인증을 수행한 후, 상기 가맹점 단말로 인증 성공 메시지를 전송하는 단계,

상기 가맹점 단말로부터 결제 정보를 포함하는 결제 요청을 수신하는 단계, 그리고

상기 결제 요청에 따른 결제 승인 정보를 상기 가맹점 단말로 전송하는 단계를 포함하고,

상기 카드 식별정보는 상기 전자 카드에서 상기 가맹점 단말로 전송되고,

상기 클라이언트 인증 정보는 상기 전자 카드에서 상기 서버 인증 정보를 해독하여 서버 인증을 수행한 후, 생성되고,

상기 결제 요청은 상기 인증 성공 메시지를 수신한 상기 전자 카드에서 전송되는, 전자 결제 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 결제 시스템에 관한 것으로, 보다 상세하게 전자카드와 결제 서버간의 상호 인증을 통한 결제 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 플라스틱 신용카드는 마그네틱 선을 카드 리더기를 통하여 읽고 복제하는 것이 매우 간단하다. 이로 인해, 이를 이용한 다양한 신용카드 해킹 사례가 지속적으로 보고되고 있다. 이를 극복하기 위하여 비접촉식 스마트카드를 이용한 신용카드의 도입이 시도되었으나, 역시 MITM 공격등에 취약점이 알려져 있다. 이러한 문제의 근본 원인은 수동형 신용카드인 마그네틱 혹은 RFID 기반 신용카드의 결제 방식에 신용카드 정보(카드 번호, 유효기간 등)를 카드리더기가 읽어 중앙의 신용 승인 시스템에 요청을 하는 방식이기 때문이다.

[0003] 그러므로 원칙적으로 신용카드 정보는 결제를 수행하는 순간 신용카드 리더기에서 알 수 있게 되며, 또한 비 접촉식인 스마트 카드 형태에서는 무선통신에 의한 도청에 취약한 문제가 있다. 스마트카드에서의 도청 및 해킹 문제는 우리나라의 대중교통 카드로 널리 쓰이고 있는 Mifare RFID 카드의 해킹 사례가 뉴스에도 보도되는 것에서 그 심각함을 알 수 있다. 그러므로 신용카드 리더기에서 신용카드 정보를 파악할 수 있게 하는 것은 MITM이나 기타 공격에 취약할 수 밖에 없으므로, 능동형 신용카드를 도입하여 신용카드 리더기가 신용카드의 정보를 모르는 상황에서 신용카드와 중앙 신용 승인 시스템간 직접 결재를 처리하는 방식이 필요하다.

선행기술문헌

특허문헌

[0004] (특허문헌 0001) 대한민국공개특허공보 제10-2005-0060543(2005년06월22일)

발명의 내용

해결하려는 과제

[0005] 본 발명은 전자 카드와 결제 서버간의 상호 인증을 이용하여 전자 결제를 수행할 수 있는 방법 및 절차를 제공하기 위한 것이다.

[0006] 또한, 본 발명은 가맹점 단말과 같이 결제를 단순히 전달하는 중계 장치에서, 결제를 위해 필요한 카드 정보 또는 인증 정보가 미노출되도록 할 수 있는 전자 결제 방법 및 시스템을 제공하기 위한 것이다.

[0007] 이로 인해, 본 발명은 카드 리더, 가맹점 단말 등과 같은 중계 장치에서의 악의적인 해킹 및 도청을 방지할 수 있는 이점이 있다.

[0008] 또한, 본 발명은 향후 보안 위협이 발생하여 새로운 인증 규약을 도입하는 경우에 기 구축 되어 있는 카드 리더, 가맹점 단말 등과 같은 중계 장치의 수정 없이 적용이 가능한 전자 결제 방법 및 시스템을 제공하기 위한 것이다.

과제의 해결 수단

[0009] 본 발명의 일 측면에 따르면, 전자 카드와 결제 서버간의 상호 인증을 이용하여 전자 결제를 수행할 수 있는 결제 시스템이 제공된다.

[0010] 본 발명의 일 실시예에 따르면, 전자 카드, 가맹점 단말 및 결제 서버를 포함하는 결제 시스템에 있어서, 상기 결제 서버로부터 서버 인증 정보를 획득하고, 상기 획득된 서버 인증 정보를 이용하여 서버 인증을 수행하고, 상기 결제 서버의 인증 응답에 따라 결제 정보를 포함하는 결제 요청을 상기 결제 서버로 전송하는 전자 카드; 상기 전자 카드와 상기 결제 서버간의 인증 및 결제를 위한 메시지를 중개하는 가맹점 단말; 및 상기 서버 인증에 상응하여 상기 전자 카드로부터 클라이언트 인증 정보를 획득하여 클라이언트 인증을 수행하여 상기 인증 응답을 상기 전자 카드로 전송하고, 상기 결제 요청에 따른 결제 승인을 상기 가맹점 단말을 통해 상기 전자 카드로 전송하는 결제 서버를 포함하는 결제 시스템이 제공될 수 있다.

[0011] 상기 서버 인증 정보는 상기 결제 서버 인증을 위한 서버 인증서 또는 공유 비밀키등이고, 상기 클라이언트 인증 정보는 상기 전자 카드 인증을 위해 사전에 상기 결제 서버 또는 공인기관 서버를 통해 발급받은 클라이언트 인증서 또는 공유 비밀키 등을 이용하여 생성된 인증정보이다.

[0012] 상기 전자 카드 및 상기 결제 서버는 상호 인증을 위해 상기 가맹점 단말에 규약되지 않은 인증 프로토콜을 이용하여 상기 서버 인증 정보 및 상기 클라이언트 인증 정보를 캡슐화하여 상기 가맹점 단말을 통해 전송하여 상호 인증할 수 있다.

[0013] 상기 전자 카드는 상기 상호 인증 이전에, 상기 가맹점 단말의 요청에 따라 카드 식별정보를 상기 가맹점 단말을 통해 상기 결제 서버로 전송할 수 있다.

[0014] 상기 카드 식별정보는 상기 전자 카드의 카드 번호가 아니다.

[0015] 본 발명의 다른 측면에 따르면, 전자 카드와 결제 서버간의 상호 인증을 이용하여 전자 결제를 수행할 수 있는 방법이 제공된다.

[0016] 본 발명의 일 실시예에 따르면, 전자 카드, 가맹점 단말 및 결제 서버를 포함하는 결제 시스템에서 전자 결제를 수행하는 방법에 있어서, 상기 전자 카드가 상기 가맹점 단말의 요청에 따라 카드 식별정보를 상기 가맹점 단말을 통해 상기 결제 서버로 전송하는 단계; 상기 결제 서버가 상기 카드 식별정보 수신에 따라 서버 인증 정보를 상기 가맹점 단말을 통해 상기 전자 카드로 전송하고, 상기 전자 카드로부터 클라이언트 인증 정보를 획득하여 클라이언트 인증을 수행하는 단계; 및 상기 결제 서버가 상기 클라이언트 인증이 성공한 경우, 결제 절차를 수행하여 결제 승인 또는 결제 실패 메시지를 상기 가맹점 단말을 통해 상기 전자 카드로 전송하는 단계를 포함하는 전자 결제 방법이 제공될 수 있다.

[0017] 상기 전자 카드가 상기 카드 식별정보를 상기 결제 서버로 전송시, 피기백(piggyback)으로 결제 정보를 페이로드하여 함께 전송할 수 있다.

[0018] 상기 결제 서버의 클라이언트 인증 수행 이후, 상기 전자 카드가 결제 정보를 포함하는 결제 요청을 상기 가맹

점 단말을 통해 상기 결제 서버로 전송하는 단계를 더 포함하되, 상기 결제 서버의 전자 결제 수행시, 상기 결제 요청에 포함된 결제 정보에 따라 결제 승인 여부를 수행할 수 있다.

[0019] 상기 서버 인증 및 상기 클라이언트 인증을 위해, 상기 전자 카드 및 상기 결제 서버는 각각 상기 가맹점 단말에 규약되지 않은 인증 방식으로 인증을 위해 송수신되는 정보를 캡슐화하여 상호 인증을 수행할 수 있다.

[0020] 상기 서버 인증 정보 및 상기 클라이언트 인증 정보는 각각 공인 인증서 또는 비밀 공유키 등을 이용하여 생성된 인증정보이다.

발명의 효과

[0021] 본 발명의 일 실시예에 따른 전자 결제 방법 및 시스템을 제공함으로써, 전자 카드와 결제 서버간의 상호 인증을 이용하여 전자 결제를 수행할 수 있다.

[0022] 또한, 본 발명은 가맹점 단말과 같이 결제를 단순히 전달하는 중계 장치에서, 결제를 위해 필요한 카드 정보 또는 인증 정보가 미노출되도록 할 수 있다.

[0023] 이로 인해, 본 발명은 카드 리더, 가맹점 단말 등과 같은 중계 장치에서의 악의적인 해킹 및 도청을 방지할 수 있는 이점이 있다.

[0024] 또한, 본 발명은 보안 위협이 발생하여 새로운 인증 규약을 도입하는 경우에 기 구축 되어 있는 카드 리더, 가맹점 단말 등과 같은 중계 장치의 수정 없이 적용이 가능한 이점이 있다.

도면의 간단한 설명

[0025] 도 1은 전자 카드와 결제 서버간의 상호 인증을 통해 결제하는 결제 시스템의 구성을 개략적으로 도시한 블록도.

도 2는 가맹점 단말의 내부 구성을 설명하기 위해 도시한 도면.

도 3은 결제 서버와의 상호 인증을 통해 결제를 수행하는 전자 카드의 내부 구성을 개략적으로 도시한 블록도.

도 4는 사용자 단말에 결합된 형태의 전자 카드를 설명하기 위해 도시한 도면.

도 5는 본 발명의 일 실시예에 따른 전자 결제 절차를 나타낸 흐름도.

도 6은 본 발명의 일 실시예에 따른 전자 결제 절차를 나타낸 흐름도.

도 7은 본 발명의 다른 실시예에 따른 전자 결제 절차를 나타낸 흐름도.

도 8은 본 발명의 또 다른 실시예에 따른 전자 결제 절차를 나타낸 흐름도.

발명을 실시하기 위한 구체적인 내용

[0026] 본 발명은 다양한 변환을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변환, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0027] 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0028] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부

품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0029] 이하, 본 발명의 실시예를 첨부한 도면들을 참조하여 상세히 설명하기로 한다.

[0030] [도 1 및 도 2 설명]

[0031] 도 1은 전자 카드와 결제 서버간의 상호 인증을 통해 결제하는 결제 시스템의 구성을 개략적으로 도시한 블록도이고, 도 2는 가맹점 단말의 내부 구성을 설명하기 위해 도시한 도면이다.

[0032] 도 1을 참조하면, 결제 시스템은 전자 카드(110), 가맹점 단말(120) 및 결제 서버(130)를 포함하여 구성된다. 도 1에는 명시되어 있지 않으나, 본 발명의 일 실시예에 따른 결제 시스템은 가맹점 단말과 결제 서버 중간에 위치하여 프락시(proxy) 형태로 인증 및 결제 절차를 중개하는 카드 결제 대행 시스템과 연동될 수도 있다.

[0033] 전자 카드(110)는 근거리 통신 모듈을 구비하고, 결제 서버(130)와 상호 인증을 통해 결제 절차를 수행하기 위한 장치이다. 전자 카드(110)는 결제를 위해 사용되기 이전에 결제 서버(130)에 접속하여 당해 전자 카드(110)의 인증을 위해 필요한 카드 식별정보를 사전 등록한 후 해당 전자 카드(110)의 내부 저장 공간에 저장하고, 해당 카드 식별정보를 이용하여 결제 서버(130)에 인증을 요청할 수 있다. 여기서, 카드 식별정보는 해당 전자 카드(110)에 고유하게 부여되는 카드 번호(예를 들어, 신용카드 번호) 이외에, 사용자가 해당 결제 서버(130)를 통해 전자 카드(110)에 상응하여 별도로 등록 요청하여 발급받은 카드 아이디(ID)이다.

[0034] 또한, 전자 카드(110)는 인증 기관(미도시)를 통해 발급받은 클라이언트 인증서, 공유 비밀키 등을 저장하며, 이를 이용하여 결제 서버(130)와 연동되어 사용자에 대한 인증을 수행할 수 있다.

[0035] 전자 카드(110)의 동작에 대해서는 이하에서 관련 도면을 참조하여 보다 상세히 설명하기로 한다.

[0036] 가맹점 단말(120)은 근거리 무선 통신 모듈 및 원거리 유/무선 통신 모듈을 각각 구비하며, 해당 전자 카드(110)와 결제 서버(130)간에 결제를 위한 절차를 중개하기 위한 수단이다.

[0037] 예를 들어, 가맹점 단말(120)은 전자 카드(110)와는 근거리 무선 통신을 통해 데이터를 송수신하고, 결제 서버(130)와는 원거리 무선 통신(예를 들어, 이동통신)을 통해 데이터를 송수신할 수 있다.

[0038] 예를 들어, 전자 카드(110)와 같이, 당해 전자 카드(110)가 데이터를 입력하기 위한 별도의 입력 수단 및 데이터를 시각 정보의 형태로 표출하기 위한 디스플레이 수단을 미구비하고 있는 경우, 해당 전자 카드(110)는 해당 가맹점 단말(120)과 연결되어 개인 식별 번호(PIN: personal identification number)를 입력하고, 이를 해당 가맹점 단말(120)을 통해 확인할 수 있다.

[0039] 가맹점 단말(120)은 전자 카드(110)와 결제 서버(130) 중간에서 당해 전자 카드(110) 및 결제 서버(130)간에 결제를 위한 인증 및 결제 정보를 중개할 수 있다. 이때, 인증 및 결제 정보는 각각 전자 카드(110) 및 결제 서버(130)간에 약속된 인증 방식으로 암호화되어 있어, 해당 가맹점 단말(120)은 해당 인증 및 결제 정보를 해독하지 못한다.

[0040] 도 2에 도시된 바와 같이, 가맹점 단말(120)은 전자 카드(110)와 근거리 무선 통신을 통해 연결되며, 결제 서버(130)와는 원거리 통신을 통해 통신을 수행할 수 있다. 이로 인해, 가맹점 단말(120)은 전자 카드(110)와 결제 서버(130)간의 상호 인증 또는 결제 서버(130)의 전자 카드(110) 인증을 위해 필요한 정보 송수신시, 이를 중개하는 기능을 수행할 수 있다. 이에 대해서는 하기에서 관련 도면을 참조하여 보다 상세히 설명하기로 한다.

[0041] 또한, 가맹점 단말(120)은 통신 모듈(210), 디스플레이부(215) 및 입력부(220)를 포함한다. 통신 모듈(210)은 복수의 통신 유닛을 포함하며, 통신 유닛 중 어느 하나는 전자 카드(110)와의 근거리 무선 통신을 위한 유닛이고, 다른 하나는 결제 서버(130)와의 원거리 통신을 위한 유닛일 수 있다.

[0042] 디스플레이부(215)는 결제 정보, 결제 승인에 대한 내역 등을 시각 정보의 형태로 표출하기 위한 수단이다. 예를 들어, 디스플레이부(215)는 액정화면(LCD)일 수 있다.

[0043] 입력부(220)는 사용자로부터 결제에 관련된 정보를 입력받기 위한 수단이다. 예를 들어, 입력부(220)는 터치 패널이거나 키버튼일 수도 있다.

[0044] 결제 서버(130)는 전자 카드(110)에 상응하는 결제를 승인하기 위한 장치이다.

[0045] 예를 들어, 결제 서버(130)는 전자 카드(110)의 카드 식별정보에 대응하는 신용카드 정보를 저장하고 있다. 또

한, 결제 서버(130)는 가맹점 단말(120)을 통해 전자 카드(110)로부터 클라이언트 인증서 및 공유 비밀키 등을 이용한 암호학적 연산을 통해 생성된 인증정보를 획득하고, 이를 이용하여 사용자에 대해 인증을 수행한 후 결제 승인 여부를 결정할 수 있다. 이하, 결제 서버(130)의 동작에 대해서는 하기에서 관련 도면을 참조하여 보다 상세히 설명하기로 한다.

[0046] [도 3 설명]

[0047] 도 3은 결제 서버와의 상호 인증을 통해 결제를 수행하는 전자 카드의 내부 구성을 개략적으로 도시한 블록도이다.

[0048] 본 명세서에서 전자 카드(110)는 통신부(310), 인증부(315), 저장부(320) 및 카드 제어부(325)를 포함하여 구성된다.

[0049] 통신부(310)는 통신망을 통해 다른 장치들(예를 들어, 가맹점 단말 등)과 데이터를 송수신하기 위한 수단이다.

[0050] 인증부(315)는 결제 서버(130)에 대한 인증을 수행하거나, 공유 비밀키를 이용하여 인증 결과값을 도출하기 위한 수단이다. 이는 하기의 설명에 의해 보다 명확히 이해될 것이다.

[0051] 저장부(320)는 카드 인증 정보, 공유 비밀키, 카드 식별정보 등을 저장한다. 물론, 저장부(320)는 당해 전자 카드(110)를 운용하기 위해 필요한 다양한 알고리즘이 저장된다.

[0052] 카드 제어부(325)는 본 발명의 일 실시예에 따른 전자 카드(110)의 내부 구성 요소들(예를 들어, 통신부(310), 인증부(315) 및 저장부(320) 등)을 제어하기 위한 수단이다.

[0053] [도 4 설명]

[0054] 도 4는 사용자 단말에 결합된 형태의 전자 카드를 설명하기 위해 도시한 도면이다.

[0055] 도 4에 도시된 바와 같이, 전자 카드(110)는 사용자 단말을 통해 물리적으로 결합될수 있다. 이에 따라, 전자 카드(110)는 사용자 단말의 입력 수단, 화면 출력 수단 등을 통해 개인 식별정보(PIN 번호) 등을 사용자로부터 입력받거나 결제 승인에 따른 내역을 실시간으로 조회할 수 있다. 본 명세서에서는 이해와 설명의 편의를 도모하기 위해 물리적인 형태의 전자 카드(110)를 중심으로 결제 처리하는 방식에 대해 설명하고 있으나, 구현 방법에 따라 전자 카드는 근거리 통신을 지원하는 사용자 단말의 소프트웨어 모듈 형태로 구현될 수도 있다.

[0056] [도 5 설명]

[0057] 도 5는 본 발명의 일 실시예에 따른 전체적인 전자 결제 절차를 나타낸 흐름도이다.

[0058] 단계 510에서 가맹점 단말(120)은 결제 정보를 포함하는 결제 정보 확인 요청을 전자 카드(110)로 전송할 수 있다. 여기서, 결제 정보는 결제 금액, 결제 통화 정보, 할부개월 및 가맹점 정보 중 적어도 하나일 수 있다. 물론, 결제 정보는 이외에도 실제 결제에 필요한 다양한 정보를 포함할 수 있음은 당연하다.

[0059] 단계 515에서 전자 카드(110)는 결제 정보 확인 응답을 가맹점 단말(120)로 전송할 수 있다. 전자 카드의 결제 정보 확인 응답 수신에 따라, 가맹점 단말(120)은 결제 절차를 수행하기 위해, 전자 카드(110)에 대한 카드 식별정보 요청을 해당 전자 카드(110)로 전송할 수 있다(단계 520). 구현 방법에 따라, 가맹점 단말(120)은 전자 카드의 결제 처리 시작 요청에 따라 전자 카드의 카드 식별정보 요청을 전자 카드로 전송할 수도 있다.

[0060] 전술한 바와 같이, 카드 식별정보는 전자 카드(110)에 대한 카드 정보 이외에, 사용자가 결제 서버(130)를 통해 별도로 등록한 카드 아이디 정보로, 해당 카드 아이디 정보만으로는 카드 번호와 같은 카드 정보를 확인할 수 없는 이점이 있다.

[0061] 단계 525에서 가맹점 단말(120)은 전자 카드(110)로부터 카드 식별정보를 획득한 후 이를 결제 서버(130)로 전송한다. 전자 카드(110)는 가맹점 단말(120)을 통해 카드 식별정보 요청이 수신되면, 카드 식별정보를 가맹점 단말(120)을 통해 결제 서버(130)로 전송하기 이전에, 사용자로부터 PIN 번호를 입력받기 위한 절차를 더 수행할 수도 있다.

[0062] 이와 같이 PIN 번호 입력 절차를 추가하여 전자 카드(110)의 악의적인 이용을 방지할 수 있는 이점이 있다.

[0063] 단계 530에서 결제 서버(130)는 당해 결제 서버(130)의 인증을 위해 필요한 서버 인증 정보를 제1 인증 프로토콜로 1차 캡슐화하고, 1차 캡슐화된 서버 인증 정보를 제2 인증 프로토콜로 2차 캡슐화하여 가맹점 단말(120)을 통해 전자 카드(110)로 전송한다.

[0064] 본 명세서에서, 결제 서버(130)와 전자 카드(110)는 제1 인증 프로토콜로 캡슐화하여 인증을 위해 필요한 정보들을 송수신하고, 전자 카드(110)와 가맹점 단말(120)은 제2 인증 프로토콜로 캡슐화하여 필요한 정보들을 송수신한다.

[0065] 이에 따라, 결제 서버(130)가 가맹점 단말(120)을 통해 서버 인증 정보를 전송하더라도 가맹점 단말(120)은 해당 2차 캡슐화된 서버 인증 정보를 해독하지 못하여 내용을 확인하지 못한다.

[0066] 단계 535에서 전자 카드(110)는 2차 캡슐화된 서버 인증 정보를 해독하여 서버 인증 정보를 획득하고, 해당 서버 인증 정보를 이용하여 결제 서버(130)에 대한 서버 인증을 수행한다.

[0067] 이어, 단계 540에서 전자 카드(110)는 서버 인증 성공 여부를 판단한다.

[0068] 만일 서버 인증이 성공한 경우, 단계 545에서 전자 카드(110)는 클라이언트 인증 정보를 2차 캡슐화하여 가맹점 단말(120)을 통해 결제 서버(130)로 전송한다.

[0069] 그러나, 만일 서버 인증이 실패한 경우, 단계 547에서 전자 카드(110)는 결제 서버(130)에 대해 인증이 실패했으므로, 결제를 위한 이후의 프로세스를 중단한다. 이때, 전자 카드(110)는 결제 실패에 상응하는 안내 메시지를 당해 전자 카드(110)가 연결 또는 결합된 사용자 단말을 통해 출력할 수 있다. 물론, 전자 카드(110)는 인증 실패에 따른 결제 실패에 대한 안내 메시지를 가맹점 단말(120)로 전송할 수도 있다.

[0070] 단계 550에서 결제 서버(130)는 2차 캡슐화된 클라이언트 인증 정보를 이용하여 클라이언트, 즉 전자 카드(110)에 대한 인증을 수행한다.

[0071] 단계 555에서 결제 서버(130)는 클라이언트 인증이 성공했는지 여부를 확인한다.

[0072] 만일 클라이언트 인증이 실패한 경우, 단계 560에서 결제 서버(130)는 클라이언트 인증 실패에 상응하여 사전에 지정된 실패코드 및 실패 사유 정보를 포함하는 클라이언트 인증 실패 메시지를 가맹점 단말(120)을 통해 전자 카드(110)로 전송한다.

[0073] 그러나 만일 클라이언트 인증이 성공한 경우, 단계 565에서 결제 서버(130)는 클라이언트 인증 성공 메시지를 가맹점 단말(120)을 통해 전자 카드(110)로 전송한다.

[0074] 이에 따라, 단계 570에서 전자 카드(110)는 결제 정보를 포함하는 결제 요청을 가맹점 단말(120)을 통해 결제 서버(130)로 전송한다.

[0075] 단계 575에서 결제 서버(130)는 해당 결제 요청에 포함된 결제 정보에 상응하여 결제를 승인한 후 결제 승인 확인을 가맹점 단말(120)을 통해 전자 카드(110)로 전송한다.

[0076] [도 6 설명]

[0077] 도 6은 본 발명의 일 실시예에 따른 전자 결제 절차를 나타낸 흐름도이다.

[0078] 도 6은 도 5에 따른 전자 결제 절차를 EAP-TLS 인증 방식을 이용하여 전자 카드(110)와 결제 서버(130)가 상호 인증하는 방식을 나타낸 것이다.

[0079] 단계 610에서 전자 카드(110)가 전자 결제 절차를 시작하기 위해 EAP start 메시지를 가맹점 단말(120)로 전송한다. EAP start 메시지는 옵션으로 전자 카드(110)가 가맹점 단말(120)로 전송할 수도 있으며, 구현 방법에 따라 생략될 수도 있다.

[0080] 단계 615에서 가맹점 단말(120)은 결제 정보를 포함하는 결제 요청을 위한 EAP request 메시지를 전자 카드(110)로 전송한다.

[0081] 이어, 단계 620에서 전자 카드(110)는 결제 정보를 포함하는 EAP response 메시지를 가맹점 단말(120)로 전송한다. 이로 인해 가맹점 단말(120)은 전자 카드(110)가 정상적으로 결제 요청을 위한 EAP request 메시지를 수신한 것을 확인할 수 있다.

[0082] 이에 따라, 단계 625에서 가맹점 단말(120)은 전자 카드(110)에 대한 카드 식별정보 요청을 위한 EAP-request(identity)를 전자 카드(110)로 전송하고, 전자 카드(110)는 이에 대한 응답으로 카드 식별정보를 포함하는 EAP-response(identity)를 가맹점 단말(120)을 통해 결제 서버(130)로 전송한다.

[0083] 이어, 단계 630에서 전자 카드(110)와 결제 서버(130)는 각각의 인증 정보를 각각 상호 전송하여, 상호 인증을 수행한다.

[0084] 이때, 가맹점 단말(120)은 전자 카드(110)와 결제 서버(130)간의 상호 인증에 필요한 메시지를 중개하는 전달자의 역할을 수행하며, 전자 카드(110)와 결제 서버(130)간에 상호 인증 절차에 따라 송수신되는 메시지의 내용을 해독하지 못하도록 별도의 인증 프로토콜(예를 들어, EAP TLS)로 캡슐화하여 송수신할 수 있다. 또한, 전자 카드와 결제 서버간의 상호 인증에 필요한 중요 정보는 암호학적으로 계산된 결과만 상호 송수신함으로써 가맹점 단말이 캡슐화된 메시지를 해석하더라도, 해당 정보의 원 정보(plaintext)를 복호하지 못하도록 할 수도 있다.

[0085] 이로 인해, 가맹점 단말(120)은 정상적으로 상호 인증을 위해 전자 카드(110) 및 결제 서버(130)간에 송수신되는 메시지를 해독할 수 없게된다.

[0086] 인증 정보 상호 전달 및 상호 인증이 완료되면, 즉 전자 카드(110)에서 결제 서버에 대해 인증을 수행하여 인증이 성공한 상태에서, 결제 서버(130)로부터 전자 카드(110)에 대한 인증 성공이 수신되면, 단계 635에서 전자 카드(110)는 결제 정보를 피기백으로 EAP-TLS 종료 메시지인 ACK 메시지에 포함하여 가맹점 단말(120)을 통해 결제 서버(130)로 전송한다.

[0087] 이에 따라, 단계 640에서 결제 정보를 이용하여 결제 승인 처리를 수행하고, 그에 따른 승인번호 및 결제 정보를 EAP-success 메시지에 포함하여 가맹점 단말(120)을 통해 전자 카드(110)로 전송한다.

[0088] 가맹점 단말(120)은 전자 카드(110) 및 결제 서버(130)간의 상호 인증 절차에서 미규약된 인증 프로토콜로 한번 더 캡슐화된 메시지는 해독하지 못하였지만, 결제 승에 따른 EAP-success 메시지는 정상적으로 해독하여 승인 정보를 당해 가맹점 단말(120)에 연결된 디스플레이부를 통해 출력할 수 있다.

[0089] [도 7 설명]

[0090] 도 7은 본 발명의 다른 실시예에 따른 전자 결제 절차를 나타낸 흐름도이다.

[0091] 도 7은 도 6의 EAP 메시지를 수정하여 활용한 EAP-TLS 인증 방식을 나타낸 것이다.

[0092] 도 7에서는 도 6에서와 동일한 과정에 대한 설명은 생략하기로 하며, 상이한 부분에 대해서만 설명하기로 한다.

[0093] 단계 710과 같이, 전자 카드(110)에서 전자 결제 시작을 위한 EAP start 메시지를 가맹점 단말(120)로 전송한 이후, 가맹점 단말(120)은 카드 식별정보 요청을 위한 EAP request(identity) 메시지를 보내면서, 페이로드(payload)에 결제 정보를 피기백(piggyback)하여 전자 카드(110)로 전송할 수 있다(단계 715).

[0094] 이어, 단계 720에서 전자 카드(110)는 피기백한 응답 메시지(EAP response(identity))를 가맹점 단말(120)로 전송하고, 가맹점 단말(120)은 결제 서버(130)로 전달한다. 이로 인해, 결제 서버(130)는 카드 식별정보에 따른 인증 절차를 수행하기 이전에, 피기백되어 전달받은 결제 정보를 일시적으로 저장한 후 실제 승인이 가능하도록 준비한다(단계 725).

[0095] 이후의 과정은 도 6과 동일하므로, 상호 인증을 비롯한 이후 과정에 대해서는 설명은 생략하기로 한다.

[0096] 다만, 결제 서버(130)는 상호 인증이 완료된 후, 결제 승인 성공 메시지(EAP-Success)를 가맹점 단말(120)로 전송할 때, 결제 정보를 피기백해 전송하여 가맹점 단말(120)에서 정상 승인 여부를 확인할 수 있도록 할 수 있다.

[0097] 물론, 결제 서버(130)는 결제 실패 메시지(EAP-Failure)를 가맹점 단말(120)로 전송시에도, 실패 코드 및 사유 정보를 포함하여 전송함으로써, 가맹점 단말을 통해 실패 사유가 확인 가능하도록 할 수 있다.

[0098] [도 8 설명]

[0099] 도 8은 본 발명의 또 다른 실시예에 따른 전자 결제 절차를 나타낸 흐름도이다.

[0100] 도 6 및 도 7은 EAP-TLS 기반으로 전자 카드(110) 및 결제 서버(130)가 상호 인증하는 과정을 설명하였으나, EAP-TLS 기반의 인증은 전자 카드(110) 및 결제 서버(130)가 공인 인증서를 탑재, 관리해야만 한다. 이로 인해, 전자 카드(110) 및 결제 서버(130)의 상호 인증시, 공인 인증서를 이용하지 않고 EAP-TTLS, EAP-AKA, EAP-SIM 인증 방식을 활용할 수도 있다.

[0101] 도 8에는 EAP-AKA 인증 방식을 이용하여 전자 카드(110) 및 결제 서버(130)를 상호 인증하는 방식에 대해 설명하기로 한다.

[0102] EAP-AKA 인증 방식은 공유 비밀키를 이용한 인증 방식으로, 전자 카드(110) 및 결제 서버(130) 상호 인증을 위해 공유 비밀키(K, OPc)를 이용한다. 이와 같은 공유 비밀키는 사용자 단말을 통해 조회, 입력 및 삭제가 불가능하도록 사용자 단말의 디스플레이부를 통해 표출되지 않는다.

[0103] 단계 810 내지 단계 825는 도 7의 710 내지 725와 동일하므로 중복되는 설명은 생략하기로 한다.

[0104] 단계 830에서 결제 서버(130)는 전자 카드(110)에 대한 인증을 위해 인증 정보를 포함하는 EAP-request 메시지를 가맹점 단말(120)을 통해 전자 카드(110)로 전송한다.

[0105] 이에 따라, 단계 835에서 전자 카드(110)는 인증 정보와 공유 비밀키를 이용하여 인증 정보에 따른 인증 결과값을 도출하여 가맹점 단말(120)을 통해 결제 서버(130)로 전송한다. 이에 따라, 결제 서버(130)는 전자 카드(110)를 통해 수신된 인증 결과값을 기저장된 인증 결과값과 비교하여 인증 성공 여부를 확인할 수 있다. 이후의 과정은 도 7에서 서명한 바와 동일하므로 중복되는 설명은 생략하기로 한다.

[0106] 본 명세서에서는 이해와 설명의 편의를 도모하기 위해 전자카드에 대한 인증을 위해 EAP 인증을 중심으로 설명하였으나, RADIUS, DIAMETER 등과 같은 별도의 프로토콜을 이용하여 가맹점 단말과 결제 서버간 통신을 수행할 수도 있다. 이와 같이, EAP와 RADIUS/Diameter 등의 규약을 사용하면 향후 신규 EAP 인증 규약의 추가에 가맹점 단말을 수정할 필요가 없으므로 추가적 보안을 쉽게 확보할 수 있는 이점이 있다.

[0107] 한편, 본 발명의 실시예에 따른 전자 결제 절차를 수행하기 위한 방법은 다양한 전자적으로 정보를 처리하는 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 저장 매체에 기록될 수 있다. 저장 매체는 프로그램 명령, 데이터 파일, 데이터 구조등을 단독으로 또는 조합하여 포함할 수 있다.

[0108] 저장 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 소프트웨어 분야 당업자에게 공지되어 사용 가능한 것일 수도 있다. 저장 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media) 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 또한 상술한 매체는 프로그램 명령, 데이터 구조 등을 지정하는 신호를 전송하는 반송파를 포함하는 광 또는 금속선, 도파관 등의 전송 매체일 수도 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 전자적으로 정보를 처리하는 장치, 예를 들어, 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0109] 상술한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0110] 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야에서 통상의 지식을 가진 자라면 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0111] 110: 전자 카드

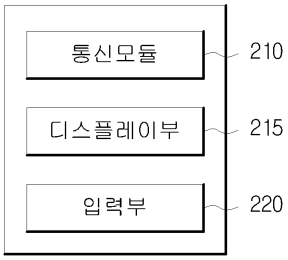
120: 가맹점 단말

130: 결제 서버

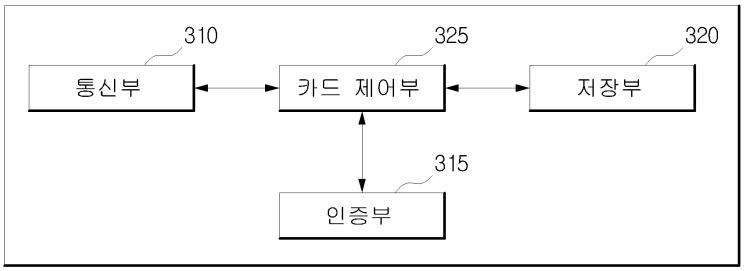
도면

도면1

도면2

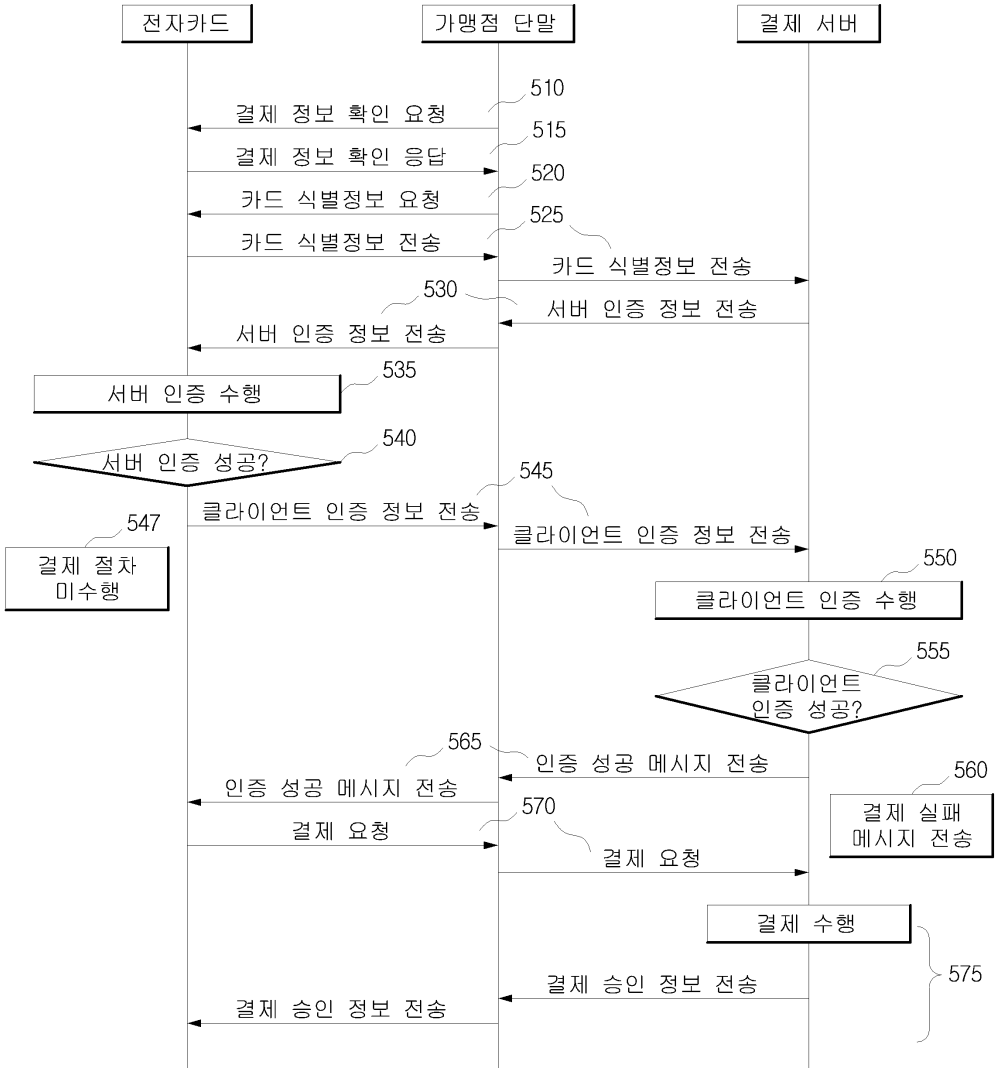


도면3

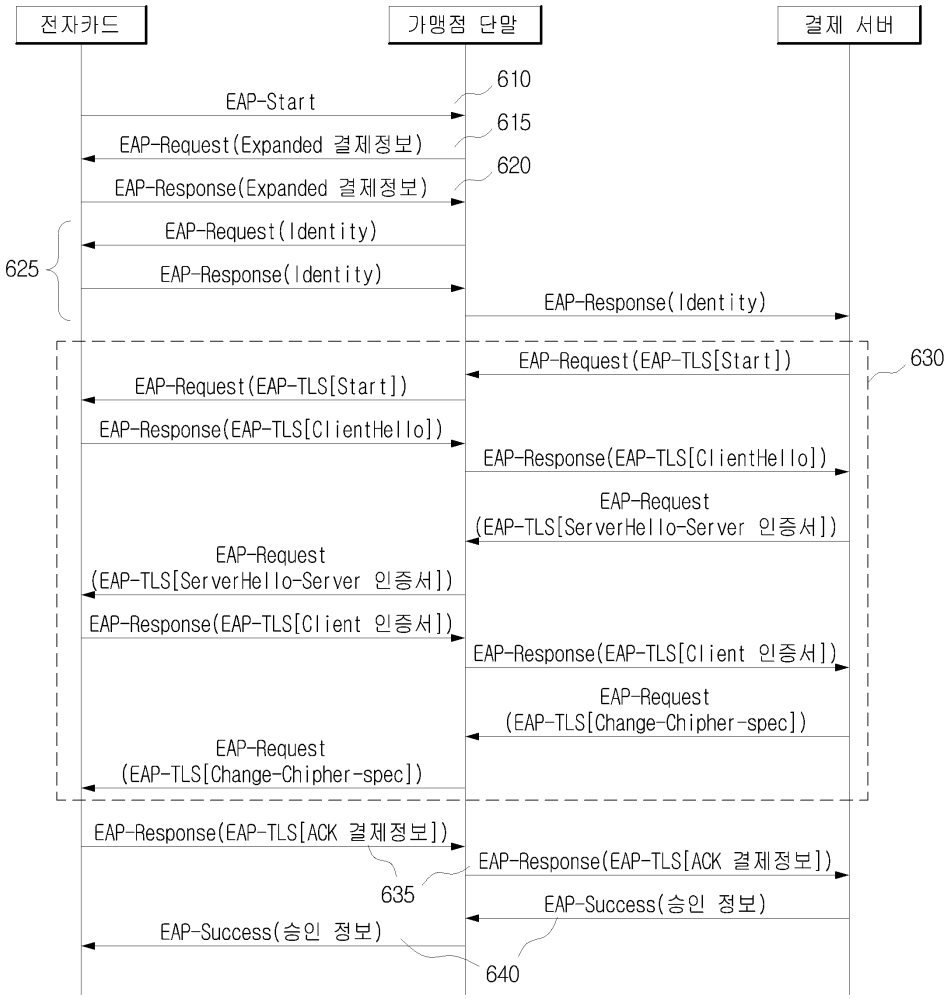


도면4

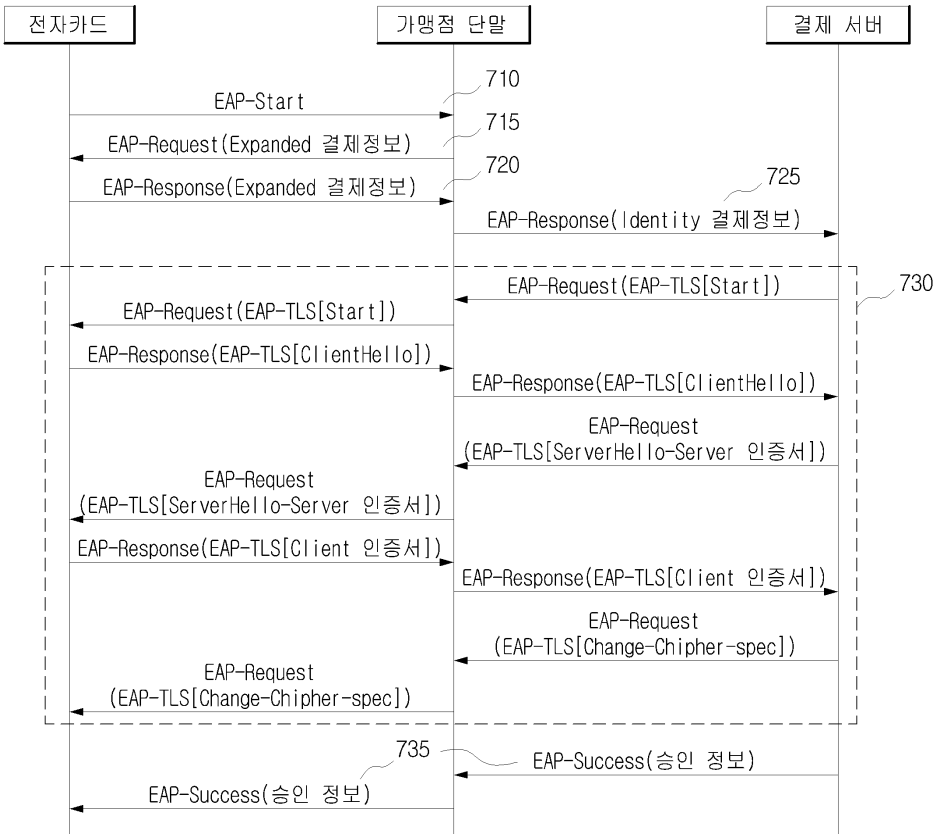
도면5


전자카드
가맹점 단말
결제 서버
510
결제 정보 확인 요청
515
결제 정보 확인 응답
520
카드 식별정보 요청
525
카드 식별정보 전송
카드 식별정보 전송
530
서버 인증 정보 전송
서버 인증 정보 전송
535
서버 인증 수행
540
서버 인증 성공?
545
클라이언트 인증 정보 전송
클라이언트 인증 정보 전송
547
결제 절차
미수행
550
클라이언트 인증 수행
555
클라이언트
인증 성공?
565
인증 성공 메시지 전송
인증 성공 메시지 전송
560
결제 실패
메시지 전송
570
결제 요청
결제 요청
결제 수행
575
결제 승인 정보 전송
결제 승인 정보 전송

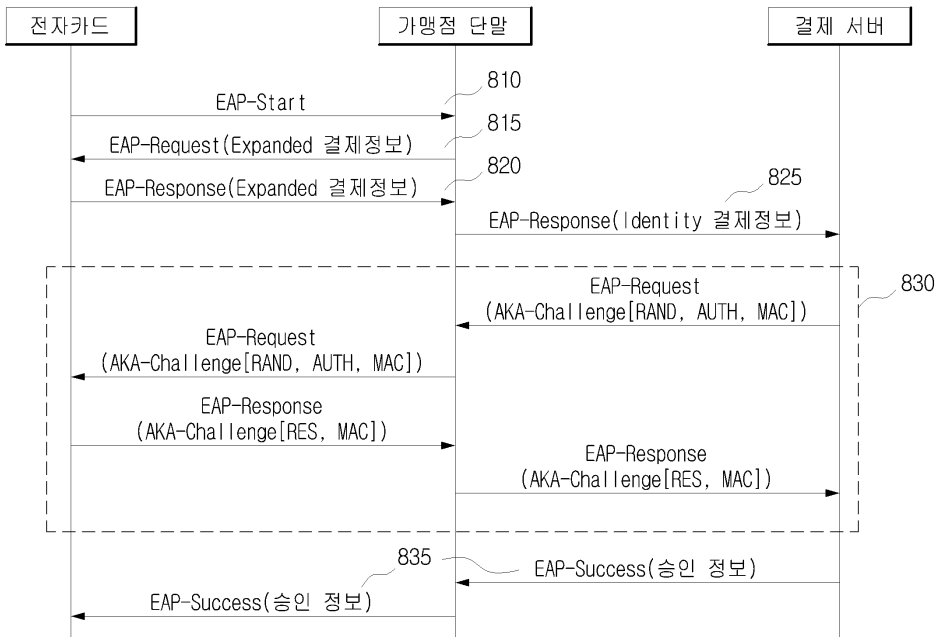
도면6


전자카드
가맹점 단말
결제 서버
610
EAP-Start
615
EAP-Request(Expanded 결제정보)
620
EAP-Response(Expanded 결제정보)
EAP-Request(Identity)
625
EAP-Response(Identity)
EAP-Response(Identity)
630
EAP-Request(EAP-TLS[Start])
EAP-Request(EAP-TLS[Start])
EAP-Response(EAP-TLS[ClientHello])
EAP-Response(EAP-TLS[ClientHello])
EAP-Request
(EAP-TLS[ServerHello-Server 인증서])
EAP-Request
(EAP-TLS[ServerHello-Server 인증서])
EAP-Response(EAP-TLS[Client 인증서])
EAP-Response(EAP-TLS[Client 인증서])
EAP-Request
(EAP-TLS[Change-Chipher-spec])
EAP-Request
(EAP-TLS[Change-Chipher-spec])
EAP-Response(EAP-TLS[ACK 결제정보])
635
EAP-Response(EAP-TLS[ACK 결제정보])
EAP-Success(승인 정보)
EAP-Success(승인 정보)
640

도면7



도면8



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제8항의 4줄

【변경전】

결제 수행하여

【변경후】

결제를 수행하여