(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0094095
(43) 공개일자 2017년08월17일

(51) 국제특허분류(Int. Cl.)
G06K 19/07 (2006.01) *G06Q 20/34* (2012.01)
(52) CPC특허분류
G06K 19/07 (2013.01)
G06Q 20/34 (2013.01)
(21) 출원번호 10-2017-0079206(분할)
(22) 출원일자 2017년06월22일
심사청구일자 2017년06월22일
(62) 원출원 특허 10-2016-0159737
원출원일자 2016년11월28일
심사청구일자 2016년11월28일

(71) 출원인
주식회사 비즈모델라인
서울특별시 마포구 와우산로 77, 6층 (서교동, 대창빌딩)
(72) 발명자
김재형
서울특별시 강남구 압구정로 313, 42동 302호 (압구정동, 한양아파트)
권봉기
경기도 안양시 동안구 시민대로 287 1214호 (관양동,동양그라테아)

전체 청구항 수 : 총 4 항

(54) 발명의 명칭 **비보안 단말을 이용한 비접촉 IC칩의 보안 처리 방법**

(57) 요 약

본 발명은, 카드에 구비된 비접촉 IC칩과 비접촉 인터페이스되는 단말과 통신하고 상기 비접촉 IC칩에 대한 암/복호 정보를 구비한 저장매체를 운영하는 서버를 통해 실행되는 방법에 있어서, 상기 비접촉 IC칩의 암/복호 정보를 구비하지 않은 비보안 상태의 단말이 상기 비접촉 IC칩과 비접촉 인터페이스된 후 상기 비접촉 IC칩에서 상

(뒷면에 계속)

대 표 도 - 도1

기 비접촉 인터페이스를 통해 상기 단말로부터 수신되는 정보를 이용하여 상기 단말의 인증 레벨이 상기 비접촉 IC칩의 암호화된 카드정보에 접근 가능한 권한인지 인증하는 단말 인증 과정을 수행하고, 상기 비접촉 IC칩에서 상기 단말 인증 과정을 수행하여 상기 단말의 인증 레벨이 상기 비접촉 IC칩의 암호화된 카드정보를 수신 가능한 특정 인증 레벨에 도달한 경우 상기 비접촉 IC칩에서 상기 비접촉 인터페이스를 통해 상기 암호화된 카드정보를 상기 단말로 전송하고, 상기 특정 인증 레벨에 도달한 단말에서 상기 비접촉 인터페이스를 통해 상기 비접촉 IC칩의 암호화된 카드정보를 수신하고 상기 암호화된 카드정보에 대한 복호화를 포함하는 정보 처리 없이 상기 비접촉 IC칩의 암/복호 정보를 구비한 저장매체를 운영하는 서버로 상기 상기 비접촉 IC칩의 암호화된 카드정보를 전송하고, 상기 서버는 상기 특정 인증 레벨에 도달한 단말로부터 상기 비접촉 IC칩의 암호화된 카드정보를 수신하고 상기 저장매체의 암/복호 정보를 통해 상기 암호화된 카드정보가 복호화되도록 처리한다.

명 세 서

청구범위

청구항 1

카드에 구비된 비접촉 IC칩과 비접촉 인터페이스되는 단말과 통신하고 상기 비접촉 IC칩에 대한 암/복호 정보를 구비한 저장매체를 운영하는 서버를 통해 실행되는 방법에 있어서,

상기 비접촉 IC칩의 암/복호 정보를 구비하지 않은 비보안 상태의 단말이 상기 비접촉 IC칩과 비접촉 인터페이스된 후 상기 비접촉 IC칩에서 상기 비접촉 인터페이스를 통해 상기 단말로부터 수신되는 정보를 이용하여 상기 단말의 인증 레벨이 상기 비접촉 IC칩의 암호화된 카드정보에 접근 가능한 권한인지 인증하는 단말 인증 과정을 수행하는 제1 단계;

상기 비접촉 IC칩에서 상기 단말 인증 과정을 수행하여 상기 단말의 인증 레벨이 상기 비접촉 IC칩의 암호화된 카드정보를 수신 가능한 특정 인증 레벨에 도달한 경우 상기 비접촉 IC칩에서 상기 비접촉 인터페이스를 통해 상기 암호화된 카드정보를 상기 단말로 전송하는 제2 단계;

상기 특정 인증 레벨에 도달한 단말에서 상기 비접촉 인터페이스를 통해 상기 비접촉 IC칩의 암호화된 카드정보를 수신하고 상기 암호화된 카드정보에 대한 복호화를 포함하는 정보 처리 없이 상기 비접촉 IC칩의 암/복호 정보를 구비한 저장매체를 운영하는 서버로 상기 상기 비접촉 IC칩의 암호화된 카드정보를 전송하는 제3 단계;

상기 서버는 상기 특정 인증 레벨에 도달한 단말로부터 상기 비접촉 IC칩의 암호화된 카드정보를 수신하고 상기 저장매체의 암/복호 정보를 통해 상기 암호화된 카드정보가 복호화되도록 처리하는 제4 단계;를 포함하는 비보안 단말을 이용한 비접촉 IC칩의 보안 처리 방법.

청구항 2

제 1항에 있어서,

상기 단말 인증 과정은, 사용자 입력 조작 없이 상기 비접촉 IC칩에 대한 상기 단말의 접근 권한을 인증받는 과정이고,

상기 암호화된 카드정보는, 지정된 암호화 방식에 따라 암호화되어 상기 비접촉 IC칩에 저장된 정보이고, 상기 암/복호 정보를 구비하지 않은 단말에 대한 단말 인증 과정을 거쳐 상기 단말로 수신된 경우 상기 저장매체를 운영하는 서버를 통해서만 복호화되도록 제한되는 것을 특징으로 하는 비보안 단말을 이용한 비접촉 IC칩의 보안 처리 방법.

청구항 3

제 1항에 있어서,

상기 단말의 인증 레벨을 인증하는 과정을 수행하면서 상기 단말의 인증 레벨이 상기 특정 인증 레벨에 도달하기 전인 경우 상기 비접촉 IC칩에서 암호화되지 않은 비암호화된 카드정보를 상기 비접촉 인터페이스를 통해 상기 단말로 전송하는 단계; 및

상기 단말에서 상기 비접촉 인터페이스를 통해 상기 비암호화된 카드정보를 수신하여 상기 서버로 전송하는 단계;를 더 포함하여 이루어지는 것을 특징으로 하는 비보안 단말을 이용한 비접촉 IC칩의 보안 처리 방법.

청구항 4

제 1항에 있어서,

상기 서버는 상기 복호화된 카드정보를 이용하여 상기 단말을 통해 요청된 결제를 위한 절차를 수행하는 단계를

더 포함하여 이루어지는 것을 특징으로 하는 비보안 단말을 이용한 비접촉 IC칩의 보안 처리 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은, 카드에 구비된 비접촉 IC칩과 비접촉 인터페이스되는 단말과 통신하고 상기 비접촉 IC칩에 대한 암/복호 정보를 구비한 저장매체를 운영하는 서버를 통해 실행되는 방법에 있어서, 상기 비접촉 IC칩의 암/복호 정보를 구비하지 않은 비보안 상태의 단말이 상기 비접촉 IC칩과 비접촉 인터페이스된 후 상기 비접촉 IC칩에서 상기 비접촉 인터페이스를 통해 상기 단말로부터 수신되는 정보를 이용하여 상기 단말의 인증 레벨이 상기 비접촉 IC칩의 암호화된 카드정보에 접근 가능한 권한인지 인증하는 단말 인증 과정을 수행하고, 상기 비접촉 IC칩에서 상기 단말 인증 과정을 수행하여 상기 단말의 인증 레벨이 상기 비접촉 IC칩의 암호화된 카드정보를 수신 가능한 특정 인증 레벨에 도달한 경우 상기 비접촉 IC칩에서 상기 비접촉 인터페이스를 통해 상기 암호화된 카드정보를 상기 단말로 전송하고, 상기 특정 인증 레벨에 도달한 단말에서 상기 비접촉 인터페이스를 통해 상기 비접촉 IC칩의 암호화된 카드정보를 수신하고 상기 암호화된 카드정보에 대한 복호화를 포함하는 정보 처리 없이 상기 비접촉 IC칩의 암/복호 정보를 구비한 저장매체를 운영하는 서버로 상기 상기 비접촉 IC칩의 암호화된 카드정보를 전송하고, 상기 서버는 상기 특정 인증 레벨에 도달한 단말로부터 상기 비접촉 IC칩의 암호화된 카드정보를 수신하고 상기 저장매체의 암/복호 정보를 통해 상기 암호화된 카드정보가 복호화되도록 처리하는 비보안 단말을 이용한 비접촉 IC칩의 보안 처리 방법에 관한 것이다.

배 경 기 술

[0003] 정보통신 기술의 발전으로 IC칩을 구비한 IC카드를 이용한 카드거래, 또는 IC칩을 탑재(또는 이탈착)하는 장치가 점차 활성화되고 있으며, 상기 IC칩이 가지고 있는 우수한 보안/인증 기능으로 인해 상기 IC카드를 이용한 카드거래, 또는 IC칩을 탑재(또는 이탈착)하는 장치는 종래의 다른 카드거래 또는 장치보다 그 신뢰성이 우수한 것으로 평가되고 있다.

[0005] 그러나, 종래의 IC칩은 보안저장모듈, 또는 인증모듈의 기능만을 수행할 뿐, 대부분의 정보 처리는 상기 IC칩과 인터페이스하는 장치에서 수행됨으로 인해, 상기 IC칩과 인터페이스하는 장치가 해킹되거나, 부정 사용되는 경우에는 상기 IC칩을 이용한 카드거래, 또는 IC칩을 탑재(또는 이탈착)하는 장치의 신뢰성이 훼손되는 문제점을 지니고 있다.

발명의 내용

해결하려는 과제

[0007] 본 발명의 목적은, 카드에 구비된 비접촉 IC칩과 비접촉 인터페이스되는 단말과 통신하고 상기 비접촉 IC칩에 대한 암/복호 정보를 구비한 저장매체를 운영하는 서버를 통해 실행되는 방법에 있어서, 상기 비접촉 IC칩의 암/복호 정보를 구비하지 않은 비보안 상태의 단말이 상기 비접촉 IC칩과 비접촉 인터페이스된 후 상기 비접촉 IC칩에서 상기 비접촉 인터페이스를 통해 상기 단말로부터 수신되는 정보를 이용하여 상기 단말의 인증 레벨이 상기 비접촉 IC칩의 암호화된 카드정보에 접근 가능한 권한인지 인증하는 단말 인증 과정을 수행하는 제1 단계와 상기 비접촉 IC칩에서 상기 단말 인증 과정을 수행하여 상기 단말의 인증 레벨이 상기 비접촉 IC칩의 암호화된 카드정보를 수신 가능한 특정 인증 레벨에 도달한 경우 상기 비접촉 IC칩에서 상기 비접촉 인터페이스를 통해 상기 암호화된 카드정보를 상기 단말로 전송하는 제2 단계와 상기 특정 인증 레벨에 도달한 단말에서 상기 비접촉 인터페이스를 통해 상기 비접촉 IC칩의 암호화된 카드정보를 수신하고 상기 암호화된 카드정보에 대한 복호화를 포함하는 정보 처리 없이 상기 비접촉 IC칩의 암/복호 정보를 구비한 저장매체를 운영하는 서버로 상기 상기 비접촉 IC칩의 암호화된 카드정보를 전송하는 제3 단계와 상기 서버는 상기 특정 인증 레벨에 도달한 단말로부터 상기 비접촉 IC칩의 암호화된 카드정보를 수신하고 상기 저장매체의 암/복호 정보를 통해 상기 암호화된 카드정보가 복호화되도록 처리하는 제4 단계를 포함하는 비보안 단말을 이용한 비접촉 IC칩의 보안 처리 방법을

제공함에 있다.

과제의 해결 수단

[0009] 본 발명에 따른 비보안 단말을 이용한 비접촉 IC칩의 보안 처리 방법은, 카드에 구비된 비접촉 IC칩과 비접촉 인터페이스되는 단말과 통신하고 상기 비접촉 IC칩에 대한 암/복호 정보를 구비한 저장매체를 운영하는 서버를 통해 실행되는 방법에 있어서, 상기 비접촉 IC칩의 암/복호 정보를 구비하지 않은 비보안 상태의 단말이 상기 비접촉 IC칩과 비접촉 인터페이스된 후 상기 비접촉 IC칩에서 상기 비접촉 인터페이스를 통해 상기 단말로부터 수신되는 정보를 이용하여 상기 단말의 인증 레벨이 상기 비접촉 IC칩의 암호화된 카드정보에 접근 가능한 권한인지 인증하는 단말 인증 과정을 수행하는 제1 단계와 상기 비접촉 IC칩에서 상기 단말 인증 과정을 수행하여 상기 단말의 인증 레벨이 상기 비접촉 IC칩의 암호화된 카드정보를 수신 가능한 특정 인증 레벨에 도달한 경우 상기 비접촉 IC칩에서 상기 비접촉 인터페이스를 통해 상기 암호화된 카드정보를 상기 단말로 전송하는 제2 단계와 상기 특정 인증 레벨에 도달한 단말에서 상기 비접촉 인터페이스를 통해 상기 비접촉 IC칩의 암호화된 카드정보를 수신하고 상기 암호화된 카드정보에 대한 복호화를 포함하는 정보 처리 없이 상기 비접촉 IC칩의 암/복호 정보를 구비한 저장매체를 운영하는 서버로 상기 상기 비접촉 IC칩의 암호화된 카드정보를 전송하는 제3 단계와 상기 서버는 상기 특정 인증 레벨에 도달한 단말로부터 상기 비접촉 IC칩의 암호화된 카드정보를 수신하고 상기 저장매체의 암/복호 정보를 통해 상기 암호화된 카드정보가 복호화되도록 처리하는 제4 단계를 포함하는 것을 특징으로 한다.

[0011] 본 발명에 따른 비보안 단말을 이용한 비접촉 IC칩의 보안 처리 방법에 있어서, 상기 단말 인증 과정은, 사용자 입력 조작 없이 상기 비접촉 IC칩에 대한 상기 단말의 접근 권한을 인증받는 과정이고, 상기 암호화된 카드정보는, 지정된 암호화 방식에 따라 암호화되어 상기 비접촉 IC칩에 저장된 정보이고, 상기 암/복호 정보를 구비하지 않은 단말에 대한 단말 인증 과정을 거쳐 상기 단말로 수신된 경우 상기 저장매체를 운영하는 서버를 통해서만 복호화되도록 제한되는 것을 특징으로 한다.

[0013] 본 발명에 따른 비보안 단말을 이용한 비접촉 IC칩의 보안 처리 방법에 있어서, 상기 단말의 인증 레벨을 인증하는 과정을 수행하면서 상기 단말의 인증 레벨이 상기 특정 인증 레벨에 도달하기 전인 경우 상기 비접촉 IC칩에서 암호화되지 않은 비암호화된 카드정보를 상기 비접촉 인터페이스를 통해 상기 단말로 전송하는 단계 및 상기 단말에서 상기 비접촉 인터페이스를 통해 상기 비암호화된 카드정보를 수신하여 상기 서버로 전송하는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0015] 본 발명에 따른 비보안 단말을 이용한 비접촉 IC칩의 보안 처리 방법에 있어서, 상기 서버는 상기 복호화된 카드정보를 이용하여 상기 단말을 통해 요청된 결제를 위한 절차를 수행하는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0018] 본 발명에 따른 비접촉 IC칩을 이용한 결제 방법은, 외부의 비접촉 IC칩과 비접촉 인터페이스된 지정된 단말과 상기 비접촉 IC칩의 암호 방식에 대응하는 복호화 정보를 구비한 저장매체를 운영하는 서버를 통해 실행되는 IC칩을 이용한 결제 방법에 있어서, 상기 비접촉 IC칩의 복호화 정보를 구비하지 않은 단말이 상기 비접촉 IC칩과 비접촉 인터페이스되고 상기 단말의 인증 레벨이 상기 비접촉 IC칩으로부터 암호화 카드정보를 리딩 가능한 특정 인증 레벨에 도달한 경우, 상기 특정 인증 레벨의 단말에서 상기 비접촉 IC칩으로부터 암호화 카드정보를 리딩하는 제1 단계와 상기 비접촉 IC칩과 비접촉 인터페이스된 특정 인증 레벨의 단말에서 상기 비접촉 IC칩의 암호화 카드정보를 복호화하지 않고 상기 비접촉 IC칩의 복호화 정보를 구비한 저장매체를 운영하는 서버로 상기 비접촉 IC칩의 암호화 카드정보를 전송하는 제2 단계와 상기 서버는 상기 특정 인증 레벨의 단말로부터 상기 비접촉 IC칩의 암호화 카드정보를 수신하는 제3 단계와 상기 특정 인증 레벨의 단말로부터 수신된 암호화 카드정보가 미리 지정된 비접촉 IC칩의 암호화 카드정보인 경우, 상기 서버는 상기 저장매체의 복호화 정보를 통해 상

기 암호화 카드정보를 복호화 처리하는 제4 단계 및 상기 서버는 상기 복호화된 카드정보를 이용하여 상기 단말을 통해 요청된 결제를 위한 절차를 수행하는 제5 단계를 포함하며, 상기 특정 인증 레벨은, 상기 단말과 비접촉 인터페이스된 비접촉 IC칩을 통해 수행된 인증의 결과를 근거로 부여되고, 상기 비접촉 IC칩은, 상기 복호화 정보를 구비하지 않고 비접촉 인터페이스된 단말의 인증 레벨이 상기 특정 인증 레벨이 아닌 경우 상기 단말로 상기 암호화 카드정보를 제공하지 않으며, 상기 암호화 카드정보는, 상기 복호화 정보를 구비하지 않은 단말로 리딩된 경우 상기 저장매체를 운영하는 어느 한 서버를 통해서만 복호화되도록 제한되는 것을 특징으로 한다.

[0020] 본 발명에 따른 비접촉 IC칩을 이용한 결제 방법에 있어서, 상기 단말에서 상기 비접촉 IC칩과 비접촉 인터페이스되는 경우 상기 비접촉 IC칩을 통해 상기 단말이 상기 비접촉 IC칩에 접근하기 위한 접근 권한을 인증받는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0022] 본 발명에 따른 비접촉 IC칩을 이용한 결제 방법에 있어서, 상기 제2 단계는, 상기 단말에서 상기 비접촉 IC칩의 암호화 카드정보를 포함하는 결제요청을 전송하는 단계를 더 포함하고, 상기 제3 단계는, 상기 서버는 상기 비접촉 IC칩의 암호화 카드정보를 포함하는 결제요청을 수신하는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0024] 본 발명에 따른 아이씨칩을 이용한 결제 방법은, 외부의 비접촉 IC칩과 비접촉 인터페이스된 지정된 단말과 통신하며 상기 비접촉 IC칩의 암호 방식에 대응하는 복호화 정보를 구비한 저장매체를 운영하는 서버를 통해 실행되는 아이씨칩을 이용한 결제 방법에 있어서, 상기 서버는 상기 비접촉 IC칩과 비접촉 인터페이스된 단말로부터 상기 비접촉 IC칩의 암호화 카드정보를 수신하는 제1 단계와 상기 서버는 상기 저장매체의 복호화 정보를 통해 상기 단말로부터 수신된 암호화 카드정보가 복호화되도록 처리하는 제2 단계 및 상기 서버는 상기 복호화된 카드정보를 이용하여 상기 단말을 통해 요청된 결제를 위한 절차를 수행하는 제3 단계를 포함하며, 상기 암호화 카드정보는, 상기 비접촉 IC칩으로부터 상기 비접촉 인터페이스된 지정된 단말로 수신되고, 상기 단말을 통해 복호화되지 않으며, 상기 저장매체를 운영하는 서버를 통해서만 복호화되는 것을 특징으로 한다.

[0025] 본 발명에 따른 아이씨칩을 이용한 결제 방법에 있어서, 상기 제1 단계는, 상기 단말 외부의 비접촉 IC칩을 통해 상기 비접촉 IC칩에 접근하는 권한을 인증받는 절차를 수행한 단말로부터 상기 비접촉 IC칩의 암호화 카드정보를 포함하는 결제요청을 수신하는 것을 특징으로 한다.

[0026] 본 발명에 따른 아이씨칩을 이용한 결제 방법에 있어서, 상기 제3 단계는, 상기 암호화 카드정보에 대응하는 결제조건에 따라 결제를 위한 절차를 수행하는 것을 특징으로 하며, 상기 결제조건은, 상기 암호화 카드정보를 이용한 결제에 대한 결제한도 조건, 결제승인 조건, 결제금액 정산 조건 중 적어도 하나를 포함하여 이루어지는 것을 특징으로 한다.

[0027] 본 발명에 따른 아이씨칩을 이용한 결제 방법에 있어서, 상기 암호화 카드정보는, 상기 비접촉 IC칩을 발급한 발급사에서 설정한 암호 방식에 따라 암호화되어 상기 비접촉 IC칩의 메모리에 기록된 것을 특징으로 한다.

[0028] 본 발명에 따른 IC카드는, IC카드 단말과 데이터를 교환하는 입출력 인터페이스와, 카드 발급사에 의해서만 복호화 가능한 암호화 방식으로 암호화된 카드정보(1)와 비암호화된 카드정보(2)를 연계하여 저장하는 메모리부 및 IC카드 단말의 인증 방식(또는 인증 레벨)에 따라 상기 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 상기 IC카드 단말로 제공하는 애플리케이션을 구동하는 프로세서를 구비하여 이루어지는 것을 특징으로 한다.

[0030] 본 발명에 따른 IC카드를 이용한 결제 시스템은, IC카드 단말로부터 카드 발급사에 의해서만 복호화 가능한 암호화 방식으로 암호화되어 IC카드에 저장된 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 포함하는 결제승인요청 전문을 수신하는 전문 수신수단과, 상기 결제승인요청 전문에 포함된 카드정보를 확인하고, 상기 암호화된 카드정보(1)가 확인되면, 상기 암호화된 카드정보(1)를 기 설정된 복호화 방식에 따라 복호화하는 정보 처리수단 및 상기 결제승인요청 전문에 암호화된 카드정보(1)가 포함된 경우, 상기 암호화된 카드정보(1)에 대응하는 결제조건(1)에 따라 상기 결제승인요청 전문에 대응하는 결제를 처리하고, 상기 결제승인요청 전문에 비암호화된 카드정보(2)가 포함된 경우, 상기 비암호화된 카드정보(2)에 대응하는 결제조건(2)에

따라 상기 결제승인요청 전문에 대응하는 결제를 처리하는 결제 처리수단을 구비하여 이루어지는 것을 특징으로 한다.

[0032] 본 발명에 따르면, 상기 비암호화된 카드정보(2)는, 상기 IC카드 단말에서 암호화되는 것을 특징으로 한다.

[0034] 본 발명에 따르면, 상기 결제조건(1)와 결제조건(2)은, 결제한도 조건, 결제승인 조건, 결제금액 정산 조건이 하나 이상 상이한 것을 특징으로 한다.

[0036] 본 발명에 따른 IC카드를 이용한 결제 방법은, IC카드 단말로부터 카드 발급사에 의해서만 복호화 가능한 암호화 방식으로 암호화되어 IC카드에 저장된 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 포함하는 결제승인요청 전문을 수신하는 단계와, 상기 결제승인요청 전문에 포함된 카드정보를 확인하고, 상기 암호화된 카드정보(1)가 확인되면, 상기 암호화된 카드정보(1)를 기 설정된 복호화 방식에 따라 복호화하는 단계 및 상기 결제승인요청 전문에 암호화된 카드정보(1)가 포함된 경우, 상기 암호화된 카드정보(1)에 대응하는 결제조건(1)에 따라 상기 결제승인요청 전문에 대응하는 결제를 처리하고, 상기 결제승인요청 전문에 비암호화된 카드정보(2)가 포함된 경우, 상기 비암호화된 카드정보(1)에 대응하는 결제조건(2)에 따라 상기 결제승인요청 전문에 대응하는 결제를 처리하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

[0038] 본 발명은 전술한 IC카드를 이용한 결제 방법을 실행하는 프로그램을 기록한 것을 특징으로 하는 컴퓨터로 판독 가능한 기록매체를 포함한다.

발명의 효과

[0040] 본 발명에 따르면, IC카드에 카드 발급사에 의해서만 복호화 가능한 암호화 방식으로 암호화되어 IC카드에 저장된 암호화된 카드정보(1)를 구비한 후, 상기 암호화된 카드정보(1)를 상기 IC카드 단말로 제공하여 카드결제를 처리하도록 함으로써, 상기 장치가 해킹되거나 부정 사용되는 경우에도 안전하게 카드결제를 처리하도록 하는 이점이 있다.

[0042] 본 발명에 따르면, IC카드에 카드 발급사에 의해서만 복호화 가능한 암호화 방식으로 암호화되어 IC카드에 저장된 암호화된 카드정보(1)와 비암호화된 카드정보(2)를 연계하여 구비한 후, IC카드 단말의 인증 방식 또는 인증 레벨에 따라 상기 암호화된 카드정보(1)를 상기 IC카드 단말로 제공하여 카드결제를 처리하도록 하거나, 또는 비암호화된 카드정보(2)를 상기 IC카드 단말로 제공하여 카드결제를 처리하도록 하되, 상기 암호화된 카드정보(1)와 비암호화된 카드정보(2)에 상이한 결제조건을 적용함으로써, IC카드 단말의 인증 방식 또는 인증 레벨에 따라 서로 다른 조건의 카드결제를 제공하는 이점이 있다.

도면의 간단한 설명

[0044] 도 1은 발명의 실시 방법에 따라 IC카드의 기능 구성을 도시한 도면이다.

도 2는 본 발명의 실시 방법에 따른 IC카드를 이용한 결제 시스템 구성을 도시한 도면이다.

도 3은 본 발명의 일 실시 방법에 따른 IC카드를 이용한 결제 과정을 도시한 도면이다.

도 4는 본 발명의 다른 일 실시 방법에 따른 IC카드를 이용한 결제 과정을 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0045] 이하 첨부된 도면과 설명을 참조하여 본 발명의 바람직한 실시예에 대한 동작 원리를 상세히 설명한다. 다만, 하기에 도시되는 도면과 후술되는 설명은 본 발명의 특징을 효과적으로 설명하기 위한 여러 가지 방법 중에서

바람직한 실시 방법에 대한 것이며, 본 발명이 하기의 도면과 설명만으로 한정되는 것은 아니다. 또한, 하기에서 본 발명을 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서, 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 발명에서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0047] 결과적으로, 본 발명의 기술적 사상은 청구범위에 의해 결정되며, 이하 실시예는 진보적인 본 발명의 기술적 사상을 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 효율적으로 설명하기 위한 일 수단일 뿐이다.

[0049] 도면1은 본 발명의 실시 방법에 따라 IC카드(100)의 기능 구성을 도시한 도면이다.

[0051] 보다 상세하게 본 도면1은 IC카드(100) 단말과 데이터를 교환하는 입출력 인터페이스(105)와, 카드 발급사에 의해서만 복호화 가능한 암호화 방식으로 암호화된 카드정보(1)와 비암호화된 카드정보(2)를 연계하여 저장하는 메모리부(115)와, IC카드(100) 단말의 인증 방식(또는 인증 레벨)에 따라 상기 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 상기 IC카드(100) 단말로 제공하는 애플리케이션을 구동하는 프로세서(110)를 구비한 IC카드(100) 기능 구성을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면1을 참조 및/또는 변형하여 상기 IC카드(100)의 기능 구성에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면1에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0053] ISO/IEC 7816 내지 ISO/IEC 14443 규격을 참조하면, IC카드(100)의 IC칩은 전원 공급(VCC), 리셋 신호(RST), 클럭 신호(CLK), 접지(GND), 프로그래밍 전원 공급(VPP), 및/또는 입출력(I/O) 등과 같은 접촉점을 통해 IC카드(100) 단말과 통신(예컨대, 명령 또는 데이터 교환 등)하는 입출력 인터페이스(105)와, CPU(Central Process Unit), MPU(Micro Process Unit), 및/또는 코프로세서(110)(Coprocessor) 등을 포함하는 적어도 하나 이상의 연산 소자로 이루어진 프로세서(110)부와, ROM(Read Only Memory), RAM(Random Access Memory), EEPROM(Electrically Erasable and Programmable Read Only Memory), FM(Flash Memory) 등을 포함하는 적어도 하나 이상의 메모리 소자로 이루어진 메모리부(115)로 이루어지며, 상기 메모리부(115)는 상기 IC카드(100) 내부 자원을 관리하고 운영하는 칩 운영 체제(Chip Operating System; COS)를 기록하며, 상기 입출력 인터페이스(105)의 전원 공급(VCC) 접촉점을 통해 IC카드(100) 단말로부터 소정의 전원이 공급되면, 상기 메모리부(115)에 저장된 COS는 실행 메모리로 로딩되어 상기 IC칩의 전반적인 동작을 제어하고, 상기 클럭 신호(CLK) 접촉점의 클럭주파수(예컨대, 3.57MHz 또는 4.9MHz)를 기반으로 APDU(Application Protocol Data Unit)를 통해 상기 IC칩과 IC카드(100) 단말 간 데이터 교환을 제어한다.

[0055] 상기 메모리부(115)는, 카드 발급사에서 발급한 카드정보를 상기 카드 발급사에 구비된 카드 발급사에 의해서만 복호화 가능한 암호화 방식으로 암호화된 카드정보(1)와 비암호화된 카드정보(2)를 연계하여 저장하고, 상기 입출력 인터페이스(105)를 통해 인터페이스하는 IC카드(100) 단말의 인증 방식, 또는 인증 레벨에 따라 상기 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 상기 IC카드(100) 단말로 제공하는 애플리케이션에 대응하는 프로그램 코드를 저장하는 것을 특징으로 하며, 상기 프로그램 코드는 상기 IC카드(100)에서 상기 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 상기 IC카드(100) 단말로 제공하기 전에 로딩되어 상기 프로세서(110)에 의해 연산되는 것이 바람직하다.

[0057] 여기서, 상기 암호화된 카드정보(1)와 비암호화된 카드정보(2)는 모두 동일한 카드정보를 포함하고 있으며, 다만 상기 암호화된 카드정보(2)는 상기 카드 발급사에서 상기 메모리부(115)에 상기 카드정보를 기록하는 과정에서 기 설정된 암호화 방식에 따라 미리 암호화하여 기록된 것이다.

[0059] 본 발명의 실시 방법에 따르면, 상기 메모리부(115)는 ISO/IEC 10202에 기반하는 보안구조를 포함하여 이루어지는데, 이에 따르면 상기 메모리부(115)는 CSN(Chip Serial Number)와 같은 비밀정보가 저장되는 보호영역과, COS 제어 영역, 사용자 애플리케이션 영역, 읽기/쓰기 접근 영역, 애플리케이션 프로그램 영역, 및 FAT(File Allocation Table) 관리 영역 등으로 이루어지며, 상기 암호화된 카드정보(1)와 비암호화된 카드정보(2)는 상기 보호영역과 COS 제어 영역을 제외한 카드정보 저장영역에 저장되는 것이 바람직하다.

[0061] 또한, ISO/IEC 7816 내지 ISO/IEC 14443 규격에 따르면, 상기 메모리부(115)는 루트 파일(Root File)에 해당하는 하나의 마스터 파일(Master File; MF)과, 상기 마스터 파일 하위에 하나 이상의 IC카드(100) 애플릿에 대한 기능 정보를 포함하는 ATR(Answer To Reset)과, 각각의 IC카드(100) 애플릿에 대응하는 전용 파일(Dedicate File; DF)과, 각 전용 파일 하위에 배치되며 IC카드(100) 서비스를 위한 실질적인 정보를 저장하는 요소 파일(Element File; EF)로 이루어진 파일 구조를 포함하여 이루어지는 것이 바람직한다.

[0063] 본 발명의 실시 방법에 따르면, 상기 암호화된 카드정보(1)와 비암호화된 카드정보(2)는, 상기 마스터 파일의 하위에 배치되는 전용파일 하위에 배치되는 요소파일 중 하나 이상의 요소파일에 저장되는 것이 바람직하며, 상기 요소파일 중 하나는 파일 제어정보(File Control Information; FCI)를 저장하는 것이 바람직하다.

[0065] 여기서, 상기 파일 제어정보를 저장하는 요소파일은 IC카드(100) 단말이 상기 IC카드(100)로 전송하는 SELECT FILE 명령에 대한 응답에 해당하는 데이터 바이트를 저장하는 요소파일로서, ISO/IEC 7816-4의 TABLE 2에 정의된 BER-TLV(Basic Encoding Rules-Tag, Length, Value) 데이터 객체 FCP(File Control Parameter)를 전달하는 FCP 탬플릿 및/또는 ISO/IEC 7816-4의 TABLE 2에 정의된 BER-TLV 데이터 객체 FMD(File Management Data)를 전달하는 FMD 탬플릿 내지 FCP와 FMD를 전달하는 FCI 탬플릿 등이 있으며, 상기 탬플릿은 SELECT FILE 명령의 선택사항에 따라 검색된다.

[0067] 본 발명의 실시 방법에 따르면, 상기 IC카드(100)에 구비된 다수의 애플릿 중에서 특정 애플릿을 선택하는 방법은, 파일 식별자에 의한 선택방법, 경로에 의한 선택방법, 및 EF 식별자에 의한 선택방법 중 하나 이상을 포함하여 이루어진다.

[0069] 상기 프로세서(110)는, 특정 애플릿에 대응하는 프로그램 코드를 실행하는 것을 특징으로 하며, 상기 애플릿 선택방법 중 어느 하나를 통해 상기 암호화된 카드정보(1)와 비암호화된 카드정보(2)를 연계하여 요소파일에 저장한 카드 애플릿이 선택되면, 상기 프로세서(110)는, 하나 이상의 인증 방식(예컨대, PIN 인증)에 따라 상기 IC카드(100) 단말의 카드정보 접근 권한을 인증하거나, 또는 복수의 인증 레벨 중 어느 하나의 인증 레벨을 통해 상기 IC카드(100) 단말의 카드정보 접근 권한을 인증하는 프로그램 코드를 실행하는 것을 특징으로 한다.

[0071] 또한, 상기 프로세서(110)는, 상기 IC카드(100) 단말의 카드정보 접근 권한 인증 방식(예컨대, 글로벌 PIN 인증 방식, 로컬 PIN 인증 방식, IC카드(100)와 IC카드(100) 단말 간 일회용 비밀번호 인증 방식), 또는 인증 레벨(예컨대, 복수의 인증 레벨 별 PIN을 통한 인증)에 따라 상기 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 상기 IC카드(100) 단말로 제공하는 프로그램 코드를 실행하는 것을 특징으로 한다.

[0073] 도면2는 본 발명의 실시 방법에 따른 IC카드(200)를 이용한 결제 시스템 구성을 도시한 도면이다.

[0075] 보다 상세하게 본 도면2는 상기 도면1에 도시된 IC카드(200)에서 상기 IC카드 단말(205)과의 인증 방식 또는 인증 레벨에 따라 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 상기 IC카드 단말(205)로 제공하고, 상기 IC카드 단말(205)에서 상기 IC카드(200)로부터 제공된 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 포함하는 결제승인요청 전문을 생성하여 전송하면, 상기 결제승인요청 전문에 포함된 암호

화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나에 대응하는 결제조건에 따라 결제를 처리하는 결제 시스템 구성을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면2를 참조 및/또는 변형하여 상기 IC카드(200)를 이용한 결제 시스템 구성에 대한 다양한 실시 방법(예컨대, 일부 구성부가 생략되거나, 또는 세분화되거나, 또는 합쳐진 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면2에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0077] 본 발명에 따르면, 상기 IC카드(200)를 이용한 결제 시스템은, 상기 암호화된 카드정보(1)에 대응하는 암/복호화 정보(1)와 결제조건(1)를 연계하여 저장하고, 상기 비암호화된 카드정보(2)에 대응하는 암/복호화 정보(2)와 결제조건(2)를 연계하여 저장하는 저장매체(225)를 구비하여 이루어지는 것을 특징으로 하며, 여기서 상기 비암호화된 카드정보(2)에 대응하는 암/복호화 정보(2)는 상기 비암호화된 카드정보(2)에 대한 IC카드 단말(205)과 정의된 암/복호화 정보를 포함하거나, 또는 널 값을 포함하여 이루어지는 것이 바람직하다.

[0079] 도면2를 참조하면, 상기 IC카드(200)를 이용한 결제 시스템은, IC카드 단말(205)에서 상기 도면1에 도시된 IC카드(200) 기능 구성을 구비한 IC카드(200)로부터 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 리딩하고, 상기 리딩된 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 포함하는 결제승인요청 전문을 생성하여 결제 통신망(예컨대, 부가가치통신망)을 통해 전송하면, 상기 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 포함하는 결제승인요청 전문을 수신하는 전문 수신수단(210)과, 상기 결제승인요청 전문에 포함된 카드정보를 확인하고, 상기 암호화된 카드정보(1)가 확인되면, 상기 암호화된 카드정보(1)를 기 설정된 복호화 방식에 따라 복호화하는 정보 처리수단(215)과, 상기 결제승인요청 전문에 암호화된 카드정보(1)가 포함된 경우, 상기 암호화된 카드정보(1)에 대응하는 결제조건(1)에 따라 상기 결제승인요청 전문에 대응하는 결제를 처리하고, 상기 결제승인요청 전문에 비암호화된 카드정보(2)가 포함된 경우, 상기 비암호화된 카드정보(2)에 대응하는 결제조건(2)에 따라 상기 결제승인요청 전문에 대응하는 결제를 처리하는 결제처리수단(220)을 구비하여 이루어지는 것을 특징으로 한다.

[0081] 상기 도면1에 도시된 IC카드(200)와 인터페이스하는 IC카드 단말(205)에서 상기 IC카드(200)에 구비된 카드정보에 대한 접근 권한 인증 방식, 또는 인증 레벨에 따라 상기 IC카드(200)로부터 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 리딩하고, 상기 리딩된 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 포함하는 결제승인요청 전문을 생성하여 결제 통신망(예컨대, 부가가치통신망)을 통해 전송하면, 상기 전문 수신수단(210)은, 상기 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 포함하는 결제승인요청 전문을 수신하는 것을 특징으로 한다.

[0083] 본 발명의 실시 방법에 따르면, 상기 결제승인요청 전문에 상기 IC카드(200)로부터 리딩된 비암호화된 카드정보(2)가 포함된 경우, 상기 비암호화된 카드정보(2)는, 상기 IC카드 단말(205)에서 암호화되어 상기 결제승인요청 전문에 포함되는 것이 가능하며, 이에 의해 본 발명이 한정되지 아니한다.

[0085] 상기 IC카드 단말(205)로부터 전송된 결제승인요청 전문이 수신되면, 상기 정보 처리수단(215)은, 상기 결제승인요청 전문에 포함된 카드정보를 확인하여 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 것인지 확인하고, 상기 카드정보가 암호화된 카드정보(1)인 경우, 상기 암호화된 카드정보(1)를 기 설정된 복호화 방식에 따라 복호화하는 것을 특징으로 한다.

[0087] 본 발명의 실시 방법에 따라 상기 결제승인요청 전문에 비암호화된 카드정보(2)가 포함되었으나, 상기 비암호화된 카드정보(2)가 상기 IC카드 단말(205)에서 암호화된 경우, 상기 정보 처리수단(215)은, 상기 IC카드 단말(205)과 정의된 암/복호화 방식에 상기 비암호화된 카드정보(2)를 복호화하는 것이 바람직하며, 이에 의해 본 발명이 한정되지 아니한다.

[0089] 만약 상기 결제승인요청 전문에 암호화된 카드정보(1)가 포함된 경우, 상기 결제 처리수단(220)은, 상기 저장매체(225)와 연계하여 상기 암호화된 카드정보(1)에 대응하는 결제조건(1)을 확인하고, 상기 결제조건(1)에 따라 상기 결제승인요청 전문에 대응하는 결제를 처리하는 것을 특징으로 한다.

[0091] 또는, 상기 결제승인요청 전문에 비암호화된 카드정보(2)가 포함된 경우, 상기 결제 처리수단(220)은, 상기 저장매체(225)와 연계하여 상기 비암호화된 카드정보(2)에 대응하는 결제조건(2)을 확인하고, 상기 결제조건(2)에 따라 상기 결제승인요청 전문에 대응하는 결제를 처리하는 것을 특징으로 한다.

[0093] 여기서, 상기 결제조건(1)와 결제조건(2)은, 결제한도 조건, 결제승인 조건, 결제금액 정산 조건이 하나 이상 상이한 것을 특징으로 한다.

[0095] 도면3은 본 발명의 일 실시 방법에 따른 IC카드(200)를 이용한 결제 과정을 도시한 도면이다.

[0097] 보다 상세하게 본 도면3은 상기 도면1에 도시된 IC카드(200)에서 상기 IC카드 단말(205)의 인증 방식 또는 인증 레벨에 따라 상기 IC카드(200)에 구비된 카드정보 중 카드 발급사에 의해서만 가능한 암호화 방식으로 암호화된 카드정보(1)를 상기 IC카드 단말(205)로 제공하고, 상기 IC카드 단말(205)에서 상기 암호화된 카드정보(1)를 포함하는 결제승인요청 전문을 구성하여 상기 도면2에 도시된 결제 시스템으로 전송한 경우, 상기 결제 시스템에서 상기 암호화된 카드정보(1)에 대응하는 결제조건(1)에 따라 결제를 처리하는 과정을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면3을 참조 및/또는 변형하여 상기 IC카드(200)를 이용한 결제 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면3에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0099] 이하, 본 도면3에서 상기 도면2에 도시된 결제 시스템을 편의상 "서버"라고 한다.

[0102] *도면3을 참조하면, 상기 도면1에 도시된 IC카드(200)는 IC카드 단말(205)로부터 요청된 접근 권한을 인증하고(300), 만약 상기 접근 권한이 인증되면(305), 상기 IC카드 단말(205)의 인증 방식 또는 인증 레벨에 따라 상기 IC카드(200)에 구비된 카드 발급사에 의해서만 복호화 가능한 암호화 방식으로 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 상기 IC카드 단말(205)로 제공하고(310), 이에 대응하여 상기 IC카드 단말(205)은 상기 IC카드(200)로부터 리딩된 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 포함하는 결제승인요청 전문을 생성하여 상기 서버로 전송한다(315).

[0104] 상기 서버는 상기 암호화된 카드정보(1)와 비암호화된 카드정보(2) 중 어느 하나를 포함하는 결제승인요청 전문을 수신 및 판독하여 상기 결제승인요청 전문에 암호화된 카드정보(1)가 포함되어 있는지 확인하며(320), 만약 상기 결제승인요청 전문에 암호화된 카드정보(1)가 포함되어 있다면(325), 상기 서버는 상기 암호화된 카드정보(1)에 대응하여 기 설정된 암/복호화 정보를 확인하고(330), 상기 확인된 암/복호화 정보에 따라 상기 암호화된 카드정보(1)를 복호화 처리한다(335).

[0106] 만약 상기 암호화된 카드정보(1)가 복호화되면(340), 상기 서버는 상기 저장매체(225)로부터 상기 암호화된 카드정보(1)에 대응하는 결제조건(1)을 확인하고(345), 상기 확인된 결제조건(1)에 따라 상기 결제승인요청 전문에 포함된 결제금액을 결제 처리한다(350).

[0108] 도면4는 본 발명의 다른 일 실시 방법에 따른 IC카드(200)를 이용한 결제 과정을 도시한 도면이다.

[0110] 보다 상세하게 본 도면4는 상기 도면3에 도시된 과정을 통해 상기 IC카드 단말(205)에서 상기 비암호화된 카드정보(2)를 포함하는 결제승인요청 전문을 구성하여 상기 도면2에 도시된 결제 시스템으로 전송한 것으로 확인되면, 상기 결제 시스템에서 상기 비암호화된 카드정보(2)에 대응하는 결제조건(2)에 따라 결제를 처리하는 과정을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면4를 참조 및/또는 변형하여 상기 IC카드(200)를 이용한 결제 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면4에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0112] 이하, 본 도면4에서 상기 도면2에 도시된 결제 시스템을 편의상 "서버"라고 한다.

[0114] 도면4를 참조하면, 상기 도면3에 도시된 과정을 통해 상기 IC카드 단말(205)에서 상기 비암호화된 카드정보(2)를 포함하는 결제승인요청 전문을 구성하여 상기 도면2에 도시된 결제 시스템으로 것으로 확인되면, 상기 서버는 상기 비암호화된 카드정보(2)가 상기 IC카드 단말(205)에서 암호화되었는지 확인하며(400), 만약 상기 비암호화된 카드정보(2)가 상기 IC카드 단말(205)에서 암호화된 경우(405), 상기 서버는 상기 저장매체(225)와 연계하여 상기 비암호화된 카드정보(2)에 대한 암/복호화 정보를 확인하고(410), 상기 확인된 암/복호화 정보에 따라 상기 비암호화된 카드정보(2)를 복호화 처리한 후(415), 상기 저장매체(225)로부터 상기 비암호화된 카드정보(2)에 대응하는 결제조건(2)을 확인하고(420), 상기 확인된 결제조건(2)에 따라 상기 결제승인요청 전문에 포함된 결제금액을 결제 처리한다(425).

부호의 설명

[0116] 100 : IC카드 105 : 입출력 인터페이스

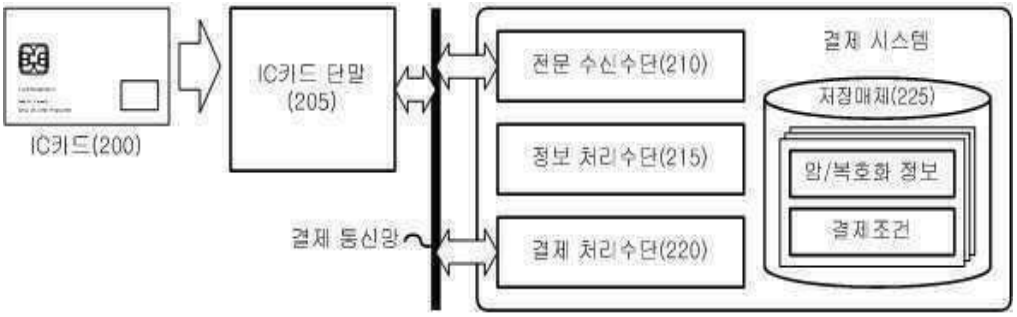
110 : 프로세서 115 : 메모리부

도면

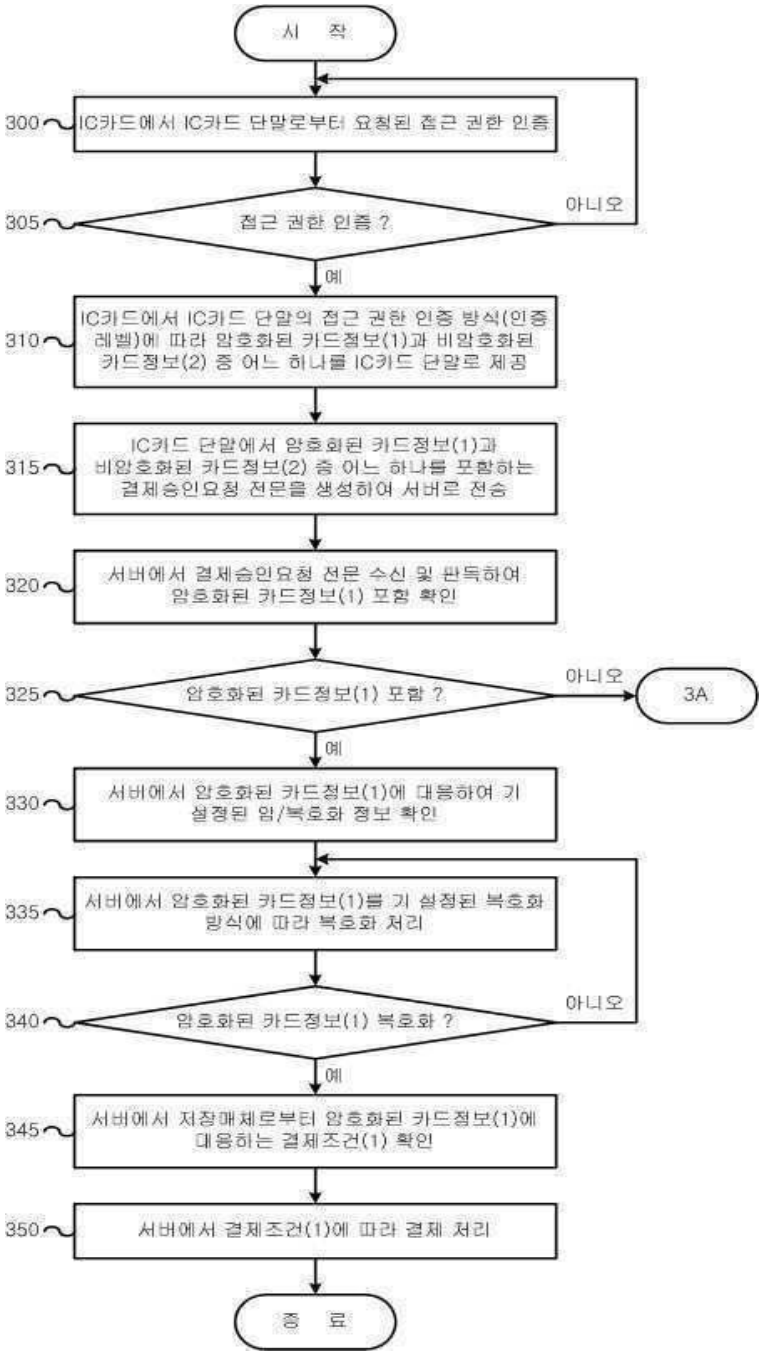
도면1


IC카드(100)
입출력 인터페이스(105)
VCC
RST
CLK
GND
VPP
I/O
IC칩
프로세서(110)
마이크로프로세서
코프로세서
메모리부(115)
ROM
RAM
EEPROM

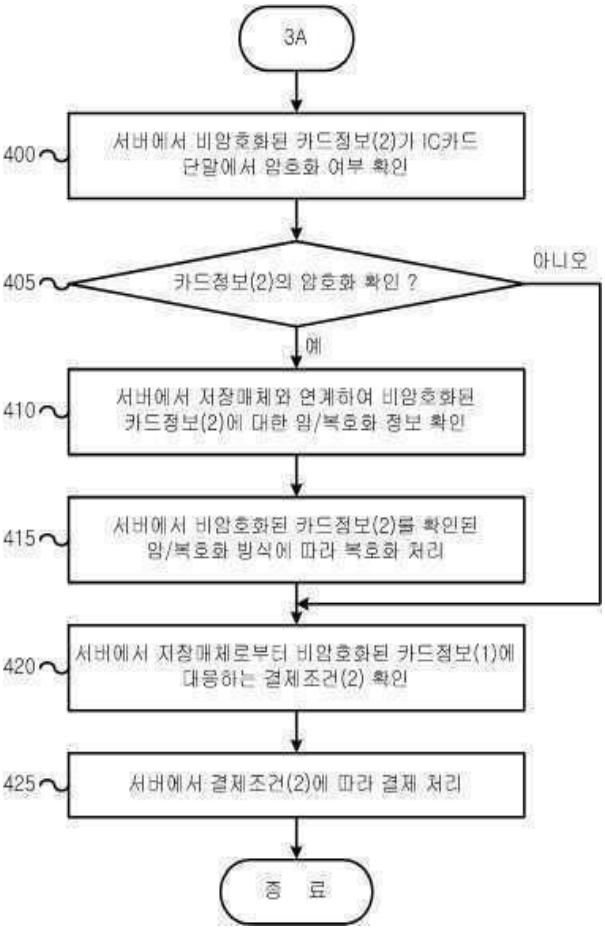
도면2


IC카드(200)
IC카드 단말
(205)
결제 통신망
전문 수신수단(210)
정보 처리수단(215)
결제 처리수단(220)
결제 시스템
저장매체(225)
암/복호화 정보
결제조건

도면3


시 작
300
IC카드에서 IC카드 단말로부터 요청된 접근 권한 인증
305
접근 권한 인증 ?
아니오
예
310
IC카드에서 IC카드 단말의 접근 권한 인증 방식(인증 레벨)에 따라 암호화된 카드정보(1)과 비암호화된 카드정보(2) 중 어느 하나를 IC카드 단말로 제공
315
IC카드 단말에서 암호화된 카드정보(1)과 비암호화된 카드정보(2) 중 어느 하나를 포함하는 결제승인요청 전문을 생성하여 서버로 전송
320
서버에서 결제승인요청 전문 수신 및 판독하여 암호화된 카드정보(1) 포함 확인
325
암호화된 카드정보(1) 포함 ?
아니오
3A
예
330
서버에서 암호화된 카드정보(1)에 대응하여 기 설정된 암/복호화 정보 확인
335
서버에서 암호화된 카드정보(1)를 기 설정된 복호화 방식에 따라 복호화 처리
340
암호화된 카드정보(1) 복호화 ?
아니오
예
345
서버에서 저장매체로부터 암호화된 카드정보(1)에 대응하는 결제조건(1) 확인
350
서버에서 결제조건(1)에 따라 결제 처리
종 료

도면4


3A
400
서버에서 비암호화된 카드정보(2)가 IC카드 단말에서 암호화 여부 확인
405
카드정보(2)의 암호화 확인 ?
아니오
예
410
서버에서 저장매체와 연계하여 비암호화된 카드정보(2)에 대한 암/복호화 정보 확인
415
서버에서 비암호화된 카드정보(2)를 확인된 암/복호화 방식에 따라 복호화 처리
420
서버에서 저장매체로부터 비암호화된 카드정보(1)에 대응하는 결제조건(2) 확인
425
서버에서 결제조건(2)에 따라 결제 처리
종 료