(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06K 19/073 (2006.01)
G06K 19/07 (2006.01)
G06K 19/077 (2006.01)

(45) 공고일자 2006년11월27일
(11) 등록번호 10-0648540
(24) 등록일자 2006년11월15일

(21) 출원번호 10-2005-0091209
(22) 출원일자 2005년09월29일
심사청구일자 2005년09월29일

(65) 공개번호
(43) 공개일자

(73) 특허권자 주식회사 유비닉스
서울 서초구 서초동 1603-65 센서스빌딩 2층

(72) 발명자 박준석
경기도 용인시 동천동 동천마을현대홈타운아파트 206-1006

구경본
서울 노원구 상계10동 주공7단지 705동 508호

이세광
서울시 관악구 봉천동 1579-24

(74) 대리인 신동준

(56) 선행기술조사문헌
JP10327142 A
JP2004252578 A
JP2004288080 A
JP2004334542 A
JP2004348526 A
* 심사관에 의하여 인용된 문헌

심사관 : 이승주

전체 청구항 수 : 총 27 항

(54) 스마트 카드, 카드 관리 시스템 및 그 키 관리 방법

(57) 요약

본 발명에 따른 스마트 카드는 소정의 서비스를 제공하고자 하는 서비스 제공자의 관리키(key)를 서비스 제공자의 카드 관리 시스템을 통해 저장 받아 상기 소정의 서비스를 수행한다. 스마트 카드는 인증 기관으로부터 제공받은 상기 스마트 카드에 대한 인증서를 저장하는 인증서 저장부, 인증 기관으로부터 인증서와 함께 제공받은 스마트 카드에 대한 개인키를 저장하는 스마트 카드 개인키 저장부, 및 암호화되어 수신되는 서비스 제공자의 관리키를 스마트 카드 개인키로 복호화하는 복호화부를 포함한다.

대표도

도 4

특허청구의 범위

청구항 1.

소정의 서비스를 제공하고자 하는 서비스 제공자의 관리키(key)를 상기 서비스 제공자의 카드 관리 시스템을 통해 저장받아 상기 소정의 서비스를 수행할 수 있는 스마트 카드에 있어서,

인증 기관으로부터 제공받은 상기 스마트 카드에 대한 인증서를 저장하는 인증서 저장부;

상기 인증 기관으로부터 상기 인증서와 함께 제공받은 상기 스마트 카드에 대한 개인키를 저장하는 스마트 카드 개인키 저장부; 및

암호화되어 수신되는 상기 서비스 제공자의 관리키를 상기 스마트 카드 개인키로 복호화하는 복호화부;

를 포함하는 스마트 카드 시큐리티 도메인을 포함하는 스마트 카드.

청구항 2.

제1항에 있어서,

상기 암호화된 서비스 제공자 관리키는 상기 카드 관리 시스템에서 상기 스마트 카드 인증서로부터 획득되는 상기 스마트 카드 공개키로 암호화된 것인 스마트 카드.

청구항 3.

제1항 또는 제2항에 있어서,

상기 소정의 서비스의 수행을 위한 서비스 제공자 어플리케이션; 및

상기 복호화된 서비스 제공자 관리키를 저장하며, 상기 서비스 제공자 어플리케이션을 관리하는 서비스 제공자 시큐리티 도메인;

을 더 포함하는 스마트 카드.

청구항 4.

제3항에 있어서,

상기 서비스 제공자 시큐리티 도메인이 상기 카드 관리 시스템으로부터 상기 암호화된 서비스 제공자 관리키를 수신 받고, 수신된 서비스 제공자 관리키를 상기 스마트 카드 시큐리티 도메인에 전달하는 스마트 카드.

청구항 5.

소정의 서비스를 제공하고자 하는 서비스 제공자의 관리키를 상기 서비스 제공자의 카드 관리 시스템을 통해 저장 받아 상기 소정의 서비스를 수행할 수 있는 스마트 카드에 있어서,

인증 기관으로부터 제공받은 상기 스마트 카드에 대한 인증서 및 인증 기관 공개키를 저장하는 인증서 저장부;

상기 인증 기관으로부터 상기 인증서와 함께 제공받은 상기 스마트 카드에 대한 개인키를 저장하는 스마트 카드 개인키 저장부;

상기 카드 관리 시스템으로부터 수신된 서비스 제공자 인증서를 검증하고, 상기 서비스 제공자 인증서로부터 서비스 제공자 공개키를 획득하는 인증서 검증부;

상기 카드 관리 시스템으로 전달하기 위한 스마트 카드 임시키를 생성하는 스마트 카드 임시키 생성부;

상기 카드 관리 시스템으로부터 수신된 서비스 제공자 임시키와 스마트 카드 임시키를 이용하여 서비스 제공자 공유키를 생성하는 서비스 제공자 공유키 생성부;

상기 스마트 카드 임시키를 상기 서비스 제공자 공개키로 암호화하는 암호화부; 및

암호화되어 수신되는 상기 서비스 제공자의 임시키를 상기 스마트 카드 개인키로 복호화하고, 암호화되어 수신되는 상기 서비스 제공자의 관리키를 상기 서비스 제공자 공유키로 복호화하는 복호화부;

를 포함하는 스마트 카드 시큐리티 도메인을 포함하는 스마트 카드.

청구항 6.

제5항에 있어서,

상기 암호화된 서비스 제공자 임시키는 상기 카드 관리 시스템에서 상기 스마트 카드 인증서로부터 획득되는 상기 스마트 카드 공개키로 암호화된 것인 스마트 카드.

청구항 7.

제5항에 있어서,

상기 암호화된 서비스 제공자 관리키는 상기 카드 관리 시스템에서 상기 서비스 제공자 공유키로 암호화된 것인 스마트 카드.

청구항 8.

제5항에 있어서,

상기 인증서 검증부는 상기 서비스 제공자 인증서를 생성한 인증 기관의 공개키를 이용하여 상기 서비스 제공자 인증서를 검증하는 스마트 카드.

청구항 9.

제5항 내지 제8항 중 어느 한 항에 있어서,

상기 소정의 서비스의 수행을 위한 서비스 제공자 어플리케이션; 및

상기 복호화된 서비스 제공자 관리키를 저장하며, 상기 서비스 제공자 어플리케이션을 관리하는 서비스 제공자 시큐리티 도메인;

을 더 포함하는 스마트 카드.

청구항 10.

제9항에 있어서,

상기 서비스 제공자 시큐리티 도메인이 상기 카드 관리 시스템으로부터 상기 암호화된 서비스 제공자 임시키를 수신 받고, 수신된 서비스 제공자 임시키를 상기 스마트 카드 시큐리티 도메인에 전달하는 스마트 카드.

청구항 11.

제1항, 제2항, 제5항 내지 제8항 중 어느 한 항에 있어서,

상기 스마트 카드가 소정의 단말기 형태로 이루어진 스마트 카드.

청구항 12.

제11항에 있어서,

상기 단말기가 휴대폰, PDA, 데스크톱 컴퓨터, 노트북 컴퓨터, MP3 플레이어, PMP 등으로 구성된 군에서 선택되는 스마트 카드.

청구항 13.

소정의 서비스를 제공하고자 하는 서비스 제공자의 관리키를 생성하고 생성된 서비스 제공자 관리키를 스마트 카드에 전달하는 카드 관리 시스템에 있어서,

상기 스마트 카드와 데이터 통신을 수행하는 스마트 카드 통신부;

상기 스마트 카드로부터 수신된 스마트 카드 인증서를 검증하고, 상기 스마트 카드 인증서로부터 스마트 카드 공개키를 획득하는 인증서 검증부;

상기 서비스 제공자 관리키를 생성하는 서비스 제공자 관리키 생성부; 및

상기 서비스 제공자 관리키를 상기 스마트 카드 공개키로 암호화하는 암호화부;

를 포함하는 카드 관리 시스템.

청구항 14.

제13항에 있어서,

상기 인증서 검증부는 상기 스마트 카드 인증서를 생성한 인증 기관의 공개키를 이용하여 상기 스마트 카드 인증서를 검증하는 카드 관리 시스템.

청구항 15.

소정의 서비스를 제공하고자 하는 서비스 제공자의 관리키를 생성하고 생성된 서비스 제공자 관리키를 스마트 카드에 전달하는 카드 관리 시스템에 있어서,

상기 스마트 카드와 데이터 통신을 수행하는 스마트 카드 통신부;

인증 기관으로부터 제공받은 상기 서비스 제공자 인증서 및 서비스 제공자 개인키를 저장하는 인증서 및 개인키 저장부;

상기 스마트 카드로부터 수신된 스마트 카드 인증서를 검증하고, 상기 스마트 카드 인증서로부터 스마트 카드 공개키를 획득하는 인증서 검증부;

상기 스마트 카드에 전달하기 위한 서비스 제공자 임시키를 생성하는 서비스 제공자 임시키 생성부;

암호화되어 수신되는 상기 스마트 카드 임시키를 상기 서비스 제공자 개인키로 복호화하는 복호화부;

복호화된 상기 스마트 카드 임시키와 상기 서비스 제공자 임시키를 이용하여 서비스 제공자 공유키를 생성하는 서비스 제공자 공유키 생성부;

상기 서비스 제공자 관리키를 생성하는 서비스 제공자 관리키 생성부; 및

상기 서비스 제공자 임시키를 상기 스마트 카드 공개키로 암호화하고, 상기 서비스 제공자 관리키를 상기 서비스 제공자 공유키로 암호화하는 암호화부;

를 포함하는 카드 관리 시스템.

청구항 16.

제15항에 있어서,

상기 인증서 검증부는 상기 스마트 카드 인증서를 생성한 인증 기관의 공개키를 이용하여 상기 스마트 카드 인증서를 검증하는 카드 관리 시스템.

청구항 17.

제15항에 있어서,

상기 암호화된 스마트 카드 임시키는 상기 스마트 카드에서 상기 서비스 제공자 인증서로부터 획득되는 서비스 제공자 공개키로 암호화된 것인 카드 관리 시스템.

청구항 18.

소정의 서비스를 제공하고자 하는 서비스 제공자의 관리키를 생성하여 스마트 카드에 저장하는 스마트 카드의 키 관리 방법에 있어서,

카드 관리 시스템에서 상기 스마트 카드에 저장된 스마트 카드 인증서를 검증하고, 상기 스마트 카드 인증서로부터 스마트 카드 공개키를 획득하는 단계;

상기 카드 관리 시스템에서 상기 소정의 서비스에 대응하는 서비스 제공자 관리키를 생성하는 단계;

상기 카드 관리 시스템은 상기 생성된 서비스 제공자 관리키를 상기 스마트 카드 공개키로 암호화하고, 상기 스마트 카드에 전달하는 단계; 및

상기 스마트 카드는 암호화되어 수신된 상기 서비스 제공자 관리키를 인증 기관으로부터 제공받은 스마트 카드 개인키로 복호화하는 단계;

를 포함하는 스마트 카드 키 관리 방법.

청구항 19.

소정의 서비스를 제공하고자 하는 서비스 제공자의 관리키를 생성하여 스마트 카드에 저장하는 스마트 카드의 키 관리 방법에 있어서,

카드 관리 시스템에서 상기 스마트 카드에 저장된 스마트 카드 인증서를 검증하고, 상기 스마트 카드 인증서로부터 스마트 카드 공개키를 획득하는 단계;

상기 카드 관리 시스템에서 상기 소정의 서비스에 대응하는 서비스 제공자 임시키를 생성하는 단계;

상기 카드 관리 시스템에서 상기 서비스 제공자 임시키를 상기 스마트 카드 공개키로 암호화하는 단계;

상기 카드 관리 시스템은 상기 서비스 제공자 인증서 및 암호화된 서비스 제공자 임시키를 상기 스마트 카드에 전달하는 단계;

상기 스마트 카드에서 상기 서비스 제공자 인증서를 검증하고, 상기 서비스 제공자 인증서로부터 서비스 제공자 공개키를 획득하는 단계;

상기 스마트 카드는 스마트 카드 임시키를 생성하는 단계;

상기 스마트 카드는 수신된 암호화된 서비스 제공자 임시키를 인증 기관으로부터 제공받은 스마트 카드 개인키로 복호화하는 단계;

상기 스마트 카드는 상기 스마트 카드 임시키 및 상기 복호화된 서비스 제공자 임시키를 이용하여 서비스 제공자 공유키를 생성하는 단계;

상기 스마트 카드는 상기 스마트 카드 임시키를 상기 서비스 제공자 공개키로 암호화하고, 상기 카드 관리 시스템에 전달하는 단계;

상기 카드 관리 시스템은 수신된 암호화된 스마트 카드 임시키를 상기 인증 기관으로부터 제공받은 서비스 제공자 개인키로 복호화하는 단계;

상기 카드 관리 시스템은 복호화된 스마트 카드 임시키 및 상기 서비스 제공자 임시키를 이용하여 상기 서비스 제공자 공유키를 생성하는 단계;

상기 카드 관리 시스템은 서비스 제공자 관리키를 생성하고, 상기 서비스 제공자 관리키를 상기 서비스 제공자 공유키로 암호화하고, 암호화된 상기 서비스 제공자 관리키를 상기 스마트 카드로 전달하는 단계; 및

상기 스마트 카드는 수신된 암호화된 서비스 제공자 관리키를 상기 서비스 제공자 공유키로 복호화하는 단계;

를 포함하는 스마트 카드 키 관리 방법.

청구항 20.

제18항 또는 제19항에 있어서,

상기 스마트 카드는 상기 스마트 카드를 발급하는 스마트 카드 발급 시스템을 통해 상기 인증 기관과 인증 과정을 수행하는 단계;

상기 스마트 카드는 상기 스마트 카드 발급 시스템을 통해 상기 암호화된 스마트 카드 개인키를 수신하는 단계;

상기 스마트 카드는 상기 암호화된 스마트 카드 개인키를 상기 인증 기관으로부터 전달 받은 인증 기관 관리키를 이용하여 복호화하는 단계; 및

상기 스마트 카드는 상기 인증 기관으로부터 수신된 스마트 카드 인증서 및 상기 복호화된 스마트 카드 개인키를 저장하는 단계;

를 더 포함하는 스마트 카드 키 관리 방법.

청구항 21.

제20항에 있어서,

상기 스마트 카드는 상기 스마트 카드 발급 시스템을 통해 상기 인증 기관으로부터 수신된 인증 기관 공개키를 더 저장하는 스마트 카드 키 관리 방법.

청구항 22.

스마트 카드의 스마트 카드 시큐리티 도메인과 인증 기관과 통신하여 상기 스마트 카드에 스마트 카드 인증서 및/또는 스마트 카드 개인키를 저장하는 스마트 카드 발급 시스템에 있어서,

상기 스마트 카드 시큐리티 도메인이 상기 인증 기관으로부터 전달 받은 인증 기관 관리키를 이용하여 상기 인증 기관과 상호 인증하도록 하는 인증부; 및

상기 인증 기관으로부터 전달되는 상기 스마트 카드 인증서 및 암호화된 스마트 카드 개인키를 상기 스마트 카드에 전달하고, 상기 스마트 카드 시큐리티 도메인이 상기 인증 기관 관리키를 이용하여 상기 암호화된 스마트 카드 개인키를 복호화하도록 하는 스마트 카드 제어부;

를 포함하는 스마트 카드 발급 시스템.

청구항 23.

제22항에 있어서,

상기 암호화된 스마트 카드 개인키는 상기 인증 기관에서 상기 인증 기관 관리키로 암호화된 것인 스마트 카드 발급 시스템.

청구항 24.

컴퓨터가 판독 가능한 기록 매체로서,

인증 기관으로부터 제공받은 스마트 카드에 대한 인증서를 저장하는 기능;

상기 인증 기관으로부터 상기 인증서와 함께 제공받은 상기 스마트 카드에 대한 개인키를 저장하는 기능; 및

암호화되어 수신되는 상기 서비스 제공자의 관리키를 상기 스마트 카드 개인키로 복호화하는 기능;

을 실행하는 프로그램이 기록된 기록 매체.

청구항 25.

컴퓨터가 판독 가능한 기록 매체로서,

스마트 카드로부터 수신된 스마트 카드 인증서를 검증하고, 상기 스마트 카드 인증서로부터 스마트 카드 공개키를 획득하는 기능;

상기 스마트 카드에 제공될 서비스 제공자 관리키를 생성하는 기능; 및

상기 서비스 제공자 관리키를 상기 스마트 카드 공개키로 암호화하는 기능;

을 실행하는 프로그램이 기록된 기록 매체.

청구항 26.

컴퓨터가 판독 가능한 기록 매체로서,

카드 관리 시스템으로부터 수신된 서비스 제공자 인증서를 검증하고, 상기 서비스 제공자 인증서로부터 서비스 제공자 공개키를 획득하는 기능;

상기 카드 관리 시스템으로 전달하기 위한 스마트 카드 임시키를 생성하는 기능;

상기 카드 관리 시스템으로부터 수신된 서비스 제공자 임시키와 스마트 카드 임시키를 이용하여 서비스 제공자 공유키를 생성하는 기능; 및

상기 스마트 카드 임시키를 상기 서비스 제공자 공개키로 암호화하는 기능;

암호화되어 수신되는 상기 서비스 제공자의 임시키를 상기 스마트 카드 개인키로 복호화하고, 암호화되어 수신되는 상기 서비스 제공자의 관리키를 상기 서비스 제공자 공유키로 복호화하는 기능;

을 실행하는 프로그램이 기록된 기록 매체.

청구항 27.

컴퓨터가 판독 가능한 기록 매체로서,

스마트 카드로부터 수신된 스마트 카드 인증서를 검증하고, 상기 스마트 카드 인증서로부터 스마트 카드 공개키를 획득하는 기능;

상기 스마트 카드에 전달하기 위한 서비스 제공자 임시키를 생성하는 기능;

암호화되어 수신되는 상기 스마트 카드 임시키를 상기 서비스 제공자 개인키로 복호화하는 기능;

복호화된 상기 스마트 카드 임시키와 상기 서비스 제공자 임시키를 이용하여 서비스 제공자 공유키를 생성하는 기능;

상기 서비스 제공자 관리키를 생성하는 기능; 및

상기 서비스 제공자 임시키를 상기 스마트 카드 공개키로 암호화하고, 상기 서비스 제공자 관리키를 상기 서비스 제공자 공유키로 암호화하는 기능;

을 실행하는 프로그램이 기록된 기록 매체.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 스마트 카드, 카드 관리 시스템 및 그 키 관리 방법에 관한 것이다. 더 구체적으로는 본 발명은 공개키 기반 구조의 개방형 플랫폼 스마트 카드, 카드 관리 시스템 및 그 키 관리 방법에 관한 것이다.

스마트 카드는 집적회로(IC) 기억 소자를 포함함으로써 소정의 응용 어플리케이션 등 대용량의 정보를 저장할 수 있는 카드를 의미한다. 이러한 스마트 카드는 집적회로(IC) 기억 소자를 포함하고 있으므로, 흔히 IC 카드(integrated circuit card)라고도 한다. 이러한 스마트 카드는 종래의 마그네틱 카드와 비교할 때, 매우 큰 기억 용량과 고도의 기능 및 안전성을 가지고 있어 널리 사용되고 있다.

도 1은 종래의 스마트 카드의 구성을 보여주는 블럭도이다.

도 1에서 볼 수 있는 바와 같이, 종래의 스마트 카드는 해당 스마트 카드의 발급자가 설치한 스마트 카드 발급자 어플리케이션(1), 해당 스마트 카드에 소정의 서비스를 제공하는 서비스 제공자가 설치한 서비스 제공자 어플리케이션(3), 서비스 제공자 어플리케이션을 관리하기 위한 서비스 제공자 시큐리티 도메인(5), 스마트 카드 발급자 어플리케이션을 관리하기 위한 스마트 카드 발급자 시큐리티 도메인(7), 및 해당 스마트 카드의 전체 동작을 제어하는 스마트 카드 제어 모듈(9)을 포함한다.

스마트 카드는 스마트 카드 발급자 또는 서비스 제공자 등 외부와 연계하여 소정의 서비스를 안전하게 실행하기 위해 일정한 암호화 및 복호화 시스템을 이용한다. 이러한 암호화 및 복호화에 소정의 키(key)를 사용한다. 따라서, 스마트 카드의 안전한 이용을 위해 소정의 키 관리 방법이 필요하다.

이하 이러한 키 관리 방법으로서 도 2를 참조하여 서비스 제공자(30)가 스마트 카드(10)의 서비스 제공자 시큐리티 도메인(5)에 서비스 제공자 관리키를 전달하는 방법을 설명한다.

도 2는 도 1의 스마트 카드의 키 관리 방법을 보여주는 블럭도이다.

도 2에서 볼 수 있는 바와 같이, 종래의 스마트 카드의 키 관리 방법은 먼저 서비스 제공자(30)가 서비스 제공자 관리키를 스마트 카드 발급자(20)에 전달한다(S1). 다음 스마트 카드 발급자(20)는 스마트 카드 발급자 관리키를 이용하여 스마트 카드(10)의 서비스 제공자 시큐리티 도메인(5)과 서로 상호 인증한다(S2). 그 후 스마트 카드 발급자(20)는 스마트 카드 발급자 관리키로 서비스 제공자 관리키를 암호화하고(S3), 암호화된 서비스 제공자 관리키를 서비스 제공자 시큐리티 도

메인(5)을 통해 스마트 카드 발급자 시큐리티 도메인(7)에 전달한다(S4). 그러면, 스마트 카드 발급자 시큐리티 도메인(7)은 스마트 카드 발급자 관리키로 암호화된 서비스 제공자 관리키를 복호화할 수 있게 된다(S5). 다음, 스마트 카드 발급자 시큐리티 도메인(7)은 복호화된 서비스 제공자 관리키를 서비스 제공자 시큐리티 도메인(5)에 전달하게 된다(S6).

이와 같이 종래의 스마트 카드 키 관리 방법은 서비스 제공자(30)는 자신의 서비스 제공자 관리키를 스마트 카드(10)의 서비스 제공자 시큐리티 도메인(5)에 저장하기 위해서는 먼저 스마트 카드 발급자(20)에 전달하여야 한다. 따라서 서비스 제공자(30)는 스마트 카드 발급자(20)에 대하여 자신의 서비스 제공자 관리키의 보안을 유지하기 어려운 문제가 있다. 결국 서비스 제공자(30)는 자신의 서비스 제공자 관리키를 안전하게 관리하기 어렵게 된다.

발명이 이루고자 하는 기술적 과제

상기와 같은 기술적 과제를 해결하기 위해, 본 발명은 스마트 카드 발급자를 통하지 않고, 서비스 제공자가 자신의 서비스 제공자 관리키를 스마트 카드의 서비스 제공자 시큐리티 도메인에 직접 저장할 수 있는 스마트 카드의 키 관리 방법을 제공하고자 한다.

또한 본 발명은 전술한 스마트 카드의 키 관리 방법이 적용될 수 있는 새로운 스마트 카드를 제공하고자 한다.

또한 본 발명은 전술한 스마트 카드의 키 관리 방법이 적용될 수 있는 카드 관리 시스템을 제공하고자 한다.

발명의 구성

상기와 같은 기술적 과제의 해결을 위한, 본 발명의 한 특징에 따른 스마트 카드는 소정의 서비스를 제공하고자 하는 서비스 제공자의 관리키를 서비스 제공자의 카드 관리 시스템을 통해 저장 받아 상기 소정의 서비스를 수행한다. 스마트 카드는 인증 기관으로부터 제공받은 스마트 카드에 대한 인증서를 저장하는 인증서 저장부, 인증 기관으로부터 인증서와 함께 제공받은 스마트 카드에 대한 개인키를 저장하는 스마트 카드 개인키 저장부, 및 암호화되어 수신되는 서비스 제공자의 관리키를 스마트 카드 개인키로 복호화하는 복호화부를 포함한다.

본 발명의 또 다른 특징에 따른 스마트 카드는 소정의 서비스를 제공하고자 하는 서비스 제공자의 관리키를 서비스 제공자의 카드 관리 시스템을 통해 저장 받아 소정의 서비스를 수행한다. 스마트 카드는 인증 기관으로부터 제공받은 스마트 카드에 대한 인증서를 저장하는 인증서 저장부, 인증 기관으로부터 인증서와 함께 제공받은 스마트 카드에 대한 개인키를 저장하는 스마트 카드 개인키 저장부, 카드 관리 시스템으로부터 수신된 서비스 제공자 인증서를 검증하고, 서비스 제공자 인증서로부터 서비스 제공자 공개키를 획득하는 인증서 검증부, 카드 관리 시스템으로 전달하기 위한 스마트 카드 임시키를 생성하는 스마트 카드 임시키 생성부, 카드 관리 시스템으로부터 수신된 서비스 제공자 임시키와 스마트 카드 임시키를 이용하여 서비스 제공자 공유키를 생성하는 서비스 제공자 공유키 생성부, 스마트 카드 임시키를 상기 서비스 제공자 공개키로 암호화하는 암호화부, 및 암호화되어 수신되는 서비스 제공자의 임시키를 스마트 카드 개인키로 복호화하고, 암호화되어 수신되는 서비스 제공자의 관리키를 서비스 제공자 공유키로 복호화하는 복호화부를 포함한다. 스마트 카드는 카드 관리 시스템으로부터 암호화된 서비스 제공자 임시키 및 서비스 제공자 인증서를 수신하고, 암호화된 스마트 카드 임시키를 카드 관리 시스템에 전달하고, 카드 관리 시스템으로부터 암호화된 서비스 제공자 관리키를 수신한다.

본 발명의 또 다른 특징에 따른 카드 관리 시스템은 소정의 서비스를 제공하고자 하는 서비스 제공자의 관리키를 생성하고 생성된 서비스 제공자 관리키를 스마트 카드에 전달한다. 카드 관리 시스템은 스마트 카드와 데이터 통신을 수행하는 스마트 카드 통신부, 스마트 카드로부터 수신된 스마트 카드 인증서를 검증하고, 스마트 카드 인증서로부터 스마트 카드 공개키를 획득하는 인증서 검증부, 서비스 제공자 관리키를 생성하는 서비스 제공자 관리키 생성부, 및 서비스 제공자 관리키를 스마트 카드 공개키로 암호화하는 암호화부를 포함한다.

본 발명의 또 다른 특징에 따른 카드 관리 시스템은 소정의 서비스를 제공하고자 하는 서비스 제공자의 관리키를 생성하고 생성된 서비스 제공자 관리키를 스마트 카드에 전달한다. 카드 관리 시스템은 스마트 카드와 데이터 통신을 수행하는 스마트 카드 통신부, 인증 기관으로부터 제공받은 서비스 제공자 인증서 및 서비스 제공자 개인키를 저장하는 인증서 및 개인키 저장부, 스마트 카드로부터 수신된 스마트 카드 인증서를 검증하고, 스마트 카드 인증서로부터 스마트 카드 공개키를 획득하는 인증서 검증부, 스마트 카드에 전달하기 위한 서비스 제공자 임시키를 생성하는 서비스 제공자 임시키 생성부, 암호화되어 수신되는 스마트 카드 임시키를 서비스 제공자 개인키로 복호화하는 복호화부, 복호화된 스마트 카드 임시키와 서비스 제공자 임시키를 이용하여 서비스 제공자 공유키를 생성하는 서비스 제공자 공유키 생성부, 서비스 제공자 관리키를 생성하는 서비스 제공자 관리키 생성부, 및 서비스 제공자 임시키를 스마트 카드 공개키로 암호화하고, 서비스 제공

자 관리키를 상기 서비스 제공자 공유키로 암호화하는 암호화부를 포함한다. 카드 관리 시스템은 암호화된 서비스 제공자 임시키 및 서비스 제공자 인증서를 스마트 카드에 전달하고, 스마트 카드로부터 암호화된 스마트 카드 임시키를 수신하고, 암호화된 서비스 제공자 관리키를 스마트 카드에 전달한다.

본 발명의 또 다른 특징에 따른 스마트 카드 키 관리 방법은 카드 관리 시스템에서 스마트 카드에 저장된 스마트 카드 인증서를 검증하고, 스마트 카드 인증서로부터 스마트 카드 공개키를 획득하는 단계, 카드 관리 시스템에서 소정의 서비스에 대응하는 서비스 제공자 관리키를 생성하는 단계, 카드 관리 시스템은 생성된 서비스 제공자 관리키를 스마트 카드 공개키로 암호화하고, 스마트 카드에 전달하는 단계, 및 스마트 카드는 암호화되어 수신된 서비스 제공자 관리키를 인증 기관으로부터 제공받은 스마트 카드 개인키로 복호화하는 단계를 포함한다.

본 발명의 또 다른 특징에 따른 스마트 카드 키 관리 방법은 카드 관리 시스템에서 스마트 카드에 저장된 스마트 카드 인증서를 검증하고, 스마트 카드 인증서로부터 스마트 카드 공개키를 획득하는 단계, 카드 관리 시스템에서 소정의 서비스에 대응하는 서비스 제공자 임시키를 생성하는 단계, 카드 관리 시스템에서 서비스 제공자 임시키를 스마트 카드 공개키로 암호화하는 단계, 카드 관리 시스템은 서비스 제공자 인증서 및 암호화된 서비스 제공자 임시키를 스마트 카드에 전달하는 단계, 스마트 카드에서 상기 서비스 제공자 인증서를 검증하고, 서비스 제공자 인증서로부터 서비스 제공자 공개키를 획득하는 단계, 스마트 카드는 스마트 카드 임시키를 생성하는 단계, 스마트 카드는 수신된 암호화된 서비스 제공자 임시키를 인증 기관으로부터 제공받은 스마트 카드 개인키로 복호화하는 단계, 스마트 카드는 스마트 카드 임시키 및 복호화된 서비스 제공자 임시키를 이용하여 서비스 제공자 공유키를 생성하는 단계, 스마트 카드는 스마트 카드 임시키를 서비스 제공자 공개키로 암호화하고, 카드 관리 시스템에 전달하는 단계, 카드 관리 시스템은 수신된 암호화된 스마트 카드 임시키를 인증 기관으로부터 제공받은 서비스 제공자 개인키로 복호화하는 단계, 카드 관리 시스템은 복호화된 스마트 카드 임시키 및 서비스 제공자 임시키를 이용하여 서비스 제공자 공유키를 생성하는 단계, 카드 관리 시스템은 서비스 제공자 관리키를 생성하고, 서비스 제공자 관리키를 서비스 제공자 공유키로 암호화하고, 암호화된 서비스 제공자 관리키를 스마트 카드로 전달하는 단계, 및 스마트 카드는 수신된 암호화된 서비스 제공자 관리키를 서비스 제공자 공유키로 복호화하는 단계를 포함한다.

본 발명의 또 다른 특징에 따른 스마트 카드 발급 시스템은 스마트 카드의 스마트 카드 시큐리티 도메인 및 인증 기관과 통신하여 스마트 카드에 인증 기관의 인증서 및/또는 스마트 카드 개인키를 저장한다. 스마트 카드 발급 시스템은 스마트 카드 시큐리티 도메인이 인증 기관으로부터 전달 받은 인증 기관 관리키를 이용하여 인증 기관과 상호 인증하도록 하는 인증부, 및 인증 기관으로부터 전달되는 인증서 및 암호화된 스마트 카드 개인키를 스마트 카드에 전달하고, 스마트 카드 시큐리티 도메인이 인증 기관 관리키를 이용하여 암호화된 스마트 카드 개인키를 복호화하도록 하는 스마트 카드 제어부를 포함한다.

아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다.

먼저 도 3을 참조하여 본 발명의 실시예에 따른 스마트 카드를 설명한다.

도 3은 본 발명의 실시예에 따른 스마트 카드의 구성을 보여주는 블럭도이다.

도 3에서 볼 수 있는 바와 같이, 본 발명의 실시예에 따른 스마트 카드(100)는 스마트 카드 발급자 어플리케이션(110), 서비스 제공자 어플리케이션(120), 서비스 제공자 시큐리티 도메인(130), 스마트 카드 발급자 시큐리티 도메인(140), 스마트 카드 시큐리티 도메인(150) 및 스마트 카드 제어모듈(160)을 포함한다.

스마트 카드 발급자 어플리케이션(110)은 스마트 카드 발급자가 제공하여 설치된 것으로서 스마트 카드 발급자 시큐리티 도메인(140)에 의해 관리된다. 이러한 스마트 카드 발급자 어플리케이션(110)은 필요에 따라 복수 개로 설치될 수 있다.

서비스 제공자 어플리케이션(120)는 해당 스마트 카드를 이용하여 소정의 서비스를 제공하는 서비스 제공자가 해당 서비스의 실현을 위해 설치한 것으로서 서비스 제공자 시큐리티 도메인(130)에 의해 관리된다. 이러한 서비스 제공자 어플리케이션(120)은 필요에 따라 복수 개로 설치될 수 있다.

스마트 카드 제어 모듈(160)은 전술한 스마트 카드 발급자 어플리케이션(110), 서비스 제공자 어플리케이션(120), 서비스 제공자 시큐리티 도메인(130), 스마트 카드 발급자 시큐리티 도메인(140), 스마트 카드 시큐리티 도메인(150)의 동작을 적절히 제어한다.

스마트 카드 시큐리티 도메인(150)은 서비스 제공자의 서비스 제공자 관리키를 안전하게 관리하는 기능을 하며 후술 되는 도 5 및 도 7을 통하여 구체적으로 설명한다.

도 3에서는 도시되어 있지 않으나 스마트 카드는 스마트 카드 발급 시스템, 카드 관리 시스템, 또는 인증 기관과의 통신을 위해 접촉 또는 비 접촉 통신 수단을 포함한다.

이러한 도 3의 스마트 카드(100)는 해당 스마트 카드(100)를 발급한 스마트 카드 발급 시스템(200), 해당 스마트 카드(100)를 이용하여 소정의 서비스를 제공하고자 하는 서비스 제공자의 카드 관리 시스템(300), 및 스마트 카드(100) 및/또는 카드 관리 시스템(300)에 각각 저장되는 스마트 카드 인증서와 스마트 카드 개인키, 및 서비스 제공자 인증서와 서비스 제공자 개인키를 생성하는 인증 기관(400)과 관련된다.

도 4에서 볼 수 있는 바와 같이, 도 3의 스마트 카드(100), 스마트 카드 발급 시스템(200), 카드 관리 시스템(300) 및 인증 기관(400)은 함께 본 발명의 스마트 카드의 키 관리 시스템을 구성한다.

도 4에서는 인증 기관(400)이 스마트 카드 발급 시스템(200)과 구별되는 것으로 도시되었으나, 인증 기관(400)은 스마트 카드 발급 시스템(200) 내에 그 일부로서 포함되도록 구성될 수 있다.

이하, 도 5 및 7을 참조하여 도 3의 스마트 카드 시큐리티 도메인에 대하여 구체적으로 설명한다.

도 5는 도 3의 스마트 카드 시큐리티 도메인(150)의 일례를 보여주는 블럭도이다.

도 5에서 볼 수 있는 바와 같이, 도 5의 시큐리티 도메인(150)은 인증서 저장부(151), 스마트 카드 개인키 저장부(152) 및 복호화부(153)를 포함한다.

인증서 저장부(151)는 인증 기관(400)으로부터 제공받은 스마트 카드 인증서를 저장한다.

스마트 카드 개인키 저장부(152)는 인증 기관(400)으로부터 인증서와 함께 제공받은 스마트 카드 개인키를 저장한다.

도 5에서 도시된 인증서 저장부(151) 및 스마트 카드 개인키 저장부(152)는 설명의 편의상 정의된 것으로서 이에 한정되는 것은 아니다.

복호화부(153)는 암호화된 서비스 제공자 관리키를 수신하는 경우, 스마트 카드 개인키 저장부(152)에 저장된 스마트 카드 개인키를 이용하여 수신된 암호화된 서비스 제공자 관리키를 복호화한다. 이때, 수신된 암호화된 서비스 제공자 관리키는 카드 관리 시스템(300)에서 스마트 카드 공개키를 통해 암호화된 것이다.

따라서 이러한 도 5의 시큐리티 도메인(150)은 이와 함께 동작하는 소정의 카드 관리 시스템(300)을 필요로 한다. 이러한 카드 관리 시스템은 도 6을 참조하여 설명한다.

도 6은 도 4의 카드 관리 시스템(300)의 일례이며, 도 6의 카드 관리 시스템(300)은 도 5의 스마트 카드 시큐리티 도메인(150)을 포함하는 도 3의 스마트 카드(100)에 암호화된 서비스 제공자 관리키를 전달한다.

도 6에서 볼 수 있는 바와 같이, 도 6의 카드 관리 시스템(300)은 스마트 카드 통신부(310), 인증서 검증부(320), 서비스 제공자 관리키 생성부(330), 암호화부(340) 및 중앙 제어부(350)를 포함한다.

스마트 카드 통신부(310)는 도 3의 스마트 카드와 소정의 데이터를 송수신하기 위한 통신 수단을 포함하며, 이러한 통신 방법으로는 접촉식 또는 비접촉식 통신 방법을 모두 포함한다.

인증서 검증부(320)는 도 5의 스마트 카드 시큐리티 도메인(150)의 인증서 저장부(151)로부터 스마트 카드 인증서를 수신하는 경우 인증 기관 공개키를 이용하여 해당 스마트 카드 인증서를 검증하고, 해당 스마트 카드 인증서로부터 스마트 카드 공개키를 획득한다.

서비스 제공자 관리키 생성부(330)는 도 3의 서비스 제공자 시큐리티 도메인(130)에 전달하여 저장하고자 하는 서비스 제공자 관리키를 생성한다.

암호화부(340)는 서비스 제공자 관리키 생성부(330)가 생성한 서비스 제공자 관리키를 인증서 검증부(320)로부터 획득한 스마트 카드 공개키로 암호화한다.

중앙 제어부(350)는 스마트 카드 통신부(310), 인증서 검증부(320), 서비스 제공자 관리키 생성부(330), 및 암호화부(340)의 동작을 적절히 제어하며, 서비스 제공자 관리키가 암호화된 경우 서비스 제공자 시큐리티 도메인(130) 정보를 포함하는 소정의 명령 정보를 서비스 제공자 시큐리티 도메인(130)에 전달하고, 그 후 암호화된 서비스 제공자 관리키를 서비스 제공자 시큐리티 도메인(130)에 전달한다.

이러한 도 5의 스마트 카드 시큐리티 도메인(150) 및 도 6의 카드 관리 시스템(300)은 인증서로서 스마트 카드 인증서만을 사용하는 스마트 카드의 키 관리 시스템에 적용된다.

이하, 도 3의 스마트 카드 시큐리티 도메인의 다른 예를 설명한다.

도 7은 도 3의 스마트 카드 시큐리티 도메인의 다른 예(150')를 보여주는 블럭도이다.

도 7에서 볼 수 있는 바와 같이, 도 7의 스마트 카드 시큐리티 도메인(150')은 인증서 저장부(151'), 스마트 카드 개인키 저장부(152'), 복호화부(153'), 인증서 검증부(154), 스마트 카드 임시키 생성부(155), 서비스 제공자 공유키 생성부(156) 및 암호화부(157)를 포함한다.

인증서 저장부(151')는 인증 기관(400)으로부터 제공받은 스마트 카드 인증서 및 인증 기관 공개키를 저장한다.

스마트 카드 개인키 저장부(152')는 인증 기관(400)으로부터 인증서와 함께 제공받은 스마트 카드 개인키를 저장한다.

도 7에서 도시된 인증서 저장부(151') 및 스마트 카드 개인키 저장부(152')는 설명의 편의상 정의된 것으로서 이에 한정되는 것은 아니다.

인증서 검증부(154)는 카드 관리 시스템(300')으로부터 수신한 서비스 제공자 인증서를 인증 기관 공개키로 검증하고 해당 서비스 제공자 인증서로부터 서비스 제공자 공개키를 획득한다.

스마트 카드 임시키 생성부(155)는 스마트 카드 임시키를 생성한다. 이렇게 생성된 스마트 카드 임시키는 카드 관리 시스템(300')에 전달되어 서비스 제공자 공유키의 생성에 사용된다.

서비스 제공자 공유키 생성부(156)는 카드 관리 시스템(300')으로부터 전달받은 서비스 제공자 임시키와 스마트 카드 임시키 생성부(155)에서 생성된 스마트 카드 임시키를 이용하여 서비스 제공자 공유키를 생성한다.

암호화부(157)는 인증서 검증부(154)에서 획득한 서비스 제공자 공개키를 이용하여 스마트 카드 임시키 생성부(155)에서 생성된 스마트 카드 임시키를 암호화한다.

복호화부(153')는 카드 관리 시스템(300')으로부터 암호화된 서비스 제공자 임시키를 수신하는 경우, 스마트 카드 개인키를 이용하여 수신된 암호화된 서비스 제공자 임시키를 복호화한다. 또한 복호화부(153')는 카드 관리 시스템(300')으로부터 암호화된 서비스 제공자 관리키를 수신하는 경우, 서비스 제공자 공유키를 이용하여 수신된 암호화된 서비스 제공자 관리키를 복호화한다. 이때, 수신된 암호화된 서비스 제공자 임시키는 카드 관리 시스템(300')에서 스마트 카드 공개키를 통해 암호화된 것이며, 수신된 암호화된 서비스 제공자 관리키는 카드 관리 시스템(300')에서 서비스 제공자 공유키로 암호화된 것이다.

따라서 이러한 도 7의 시큐리티 도메인(150')은 이와 함께 동작하는 소정의 카드 관리 시스템(300')을 필요로 한다. 이러한 카드 관리 시스템은 도 8을 참조하여 설명한다.

도 8은 도 4의 카드 관리 시스템의 다른 예를 보여주는 블럭도이다.

도 8에서 볼 수 있는 바와 같이, 도 8의 카드 관리 시스템(300')은 스마트 카드 통신부(310), 인증서 검증부(320'), 서비스 제공자 관리키 생성부(330'), 암호화부(340'), 서비스 제공자 인증서 및 서비스 제공자 개인키 저장부(360), 서비스 제공자 임시키 생성부(370), 복호화부(380), 서비스 제공자 공유키 생성부(390), 및 중앙 제어부(350')를 포함한다.

스마트 카드 통신부(310)는 도 3의 스마트 카드와 소정의 데이터를 송수신하기 위한 통신 수단을 포함하며, 이러한 통신 방법으로는 접촉식 또는 비접촉식 통신 방법을 모두 포함한다.

서비스 제공자 인증서 및 서비스 제공자 개인키 저장부(360)는 인증 기관(400)으로부터 전달받은 서비스 제공자 인증서 및 서비스 제공자 개인키를 저장한다.

인증서 검증부(320')는 도 7의 스마트 카드 시큐리티 도메인(150')의 인증서 저장부(151')로부터 스마트 카드 인증서를 수신하는 경우 인증 기관 공개키를 이용하여 해당 스마트 카드 인증서를 검증하고, 해당 스마트 카드 인증서로부터 스마트 카드 공개키를 획득한다.

서비스 제공자 임시키 생성부(370)는 도 7의 서비스 제공자 시큐리티 도메인(130')에 전달하고자 하는 서비스 제공자 임시키를 생성한다.

복호화부(380)는 서비스 제공자 인증서 및 서비스 제공자 개인키 저장부(360)에 저장된 서비스 제공자 개인키를 이용하여 도 7의 서비스 제공자 시큐리티 도메인(130')로부터 수신된 암호화된 스마트 카드 임시키를 복호화한다.

서비스 제공자 공유키 생성부(390)는 복호화된 스마트 카드 임시키와 생성된 서비스 제공자 임시키를 이용하여 서비스 제공자 공유키를 생성한다.

서비스 제공자 관리키 생성부(330')는 도 7의 서비스 제공자 시큐리티 도메인(130')에 전달하여 저장하고자 하는 서비스 제공자 관리키를 생성한다.

암호화부(340')는 서비스 제공자 임시키를 인증서 검증부(320')가 획득한 스마트 카드 공개키로 암호화하고, 서비스 제공자 관리키를 서비스 제공자 공유키로 암호화한다.

중앙 제어부(350')는 스마트 카드 통신부(310), 인증서 검증부(320'), 서비스 제공자 관리키 생성부(330'), 암호화부(340'), 서비스 제공자 인증서 및 서비스 제공자 개인키 저장부(360), 서비스 제공자 임시키 생성부(370), 복호화부(380), 서비스 제공자 공유키 생성부(390)의 동작을 적절히 제어하며, 서비스 제공자 임시키가 암호화된 경우 서비스 제공자 시큐리티 도메인(130) 정보를 포함하는 소정의 명령 정보를 서비스 제공자 시큐리티 도메인(130)에 전달하고, 그 후 암호화된 서비스 제공자 임시키 및 서비스 제공자 인증서를 서비스 제공자 시큐리티 도메인(130')에 전달하고, 서비스 제공자 관리키가 암호화된 경우 암호화된 서비스 제공자 관리키를 스마트 카드 시큐리티 도메인(150')에 전달한다.

이러한 도 7의 스마트 카드 시큐리티 도메인(150') 및 도 8의 카드 관리 시스템(300')은 인증서로서 스마트 카드 인증서 및 서비스 제공자 인증서 등 두 개의 인증서를 사용하는 스마트 카드의 키 관리 시스템에 적용된다.

본 발명의 실시예에 따른 스마트 카드는 일반적인 카드 형태일 필요는 없다. 따라서, 본 발명의 실시예에 따른 스마트 카드는 다양한 형태로 이루어질 수 있으며, 소정의 단말기 형태로 이루어질 수도 있다. 이러한 단말기는 휴대폰, PDA, 데스크톱 컴퓨터, 노트북 컴퓨터, MP3 플레이어, PMP 등을 포함한다.

이하, 도 9를 참조하여 본 발명의 실시예에 따른 스마트 카드(100)를 발급하는 스마트 카드 발급 시스템(200)을 설명한다.

도 9는 본 발명에 따른 스마트 카드 발급 시스템(200)의 일례를 보여준다.

도 9에서 볼 수 있는 바와 같이, 스마트 카드 발급 시스템(200)은 스마트 카드 통신부(210), 인증부(220) 및 스마트 카드 제어부(230)를 포함한다.

스마트 카드 통신부(210)는 도 3의 스마트 카드와 소정의 데이터를 송수신하기 위한 통신 수단을 포함하며, 이러한 통신 방법으로는 접촉식 또는 비접촉식 통신 방법을 모두 포함한다.

인증부(220)는 스마트 카드(100)의 스마트 카드 시큐리티 도메인(150')이 인증 기관(400)과 상호 인증하도록 한다. 이러한 상호 인증에 스마트 카드(100)에 기저장된 인증 기관의 관리키가 이용된다.

스마트 카드 제어부(230)는 인증 기관(400)으로부터 수신되는 인증 기관 관리키, 스마트 카드 시큐리티 도메인 정보를 포함하는 명령 정보, 스마트 카드 인증서, 암호화된 스마트 카드 개인키를 스마트 카드(100)에 전달하고, 스마트 카드 시큐리티 도메인(150)이 암호화된 스마트 카드 개인키를 기 저장된 인증 기관 관리키를 이용하여 복호화하도록 한다.

도 9에서는 도시 되지 않았으나, 본 발명의 스마트 카드 발급 시스템(200)은 스마트 카드에 설치될 스마트 카드 발급자 어플리케이션(110)을 스마트 카드에 제공하는 어플리케이션 제공부, 및 스마트 카드에 설치될 스마트 카드 발급자 시큐리티 도메인(140), 서비스 제공자 시큐리티 도메인(130), 및 스마트 카드 시큐리티 도메인(150)을 스마트 카드에 제공하는 시큐리티 도메인 제공부를 추가 포함할 수 있다.

이하 도 10 내지 도 12을 참조하여, 본 발명의 실시예에 따라 도 3의 스마트 카드, 도 6 및/또는 도 8의 카드 관리 시스템을 이용하는 스마트 카드의 키 관리 방법에 대하여 구체적으로 설명한다.

본 발명의 실시예에 따른 스마트 카드의 키 관리 방법은 스마트 카드 발급자와 관계없이 스마트 카드와 서비스 제공자의 카드 관리 시스템을 통해 수행된다. 따라서 본 발명의 실시예에 따른 스마트 카드의 키 관리 방법은 스마트 카드와 서비스 제공자의 카드 관리 시스템과의 보안을 위해 정당한 인증기관에서 발행한 인증서가 필요하게 된다. 따라서, 이러한 인증서 및 인증 기관에서 인증서와 함께 발행한 개인키를 스마트 카드에 저장해 두는 방법이 필요하다.

따라서 도 10을 참조하여 도 3의 스마트 카드의 스마트 카드 시큐리티 도메인(150)에 스마트 카드 인증서, 스마트 카드 개인키 및 인증기관 공개키를 저장하는 방법을 먼저 설명한다.

도 10은 본 발명의 실시예에 따라 스마트 카드 시큐리티 도메인(150')에 스마트 카드 인증서, 스마트 카드 개인 키 및 인증 기관 공개키를 저장하는 방법을 보여주는 블럭도이다. 도 10은 스마트 카드 인증서와 서비스 제공자 인증서 둘 다를 사용하는 스마트 카드의 키 관리 방법에 대응한다. 한편, 스마트 카드 인증서만을 사용하는 스마트 카드의 키 관리 방법은 인증 기관 공개키를 스마트 카드에 저장하는 것을 제외하고는 도 10에 도시된 방법과 동일하므로 그에 대한 구체적은 설명은 여기서는 생략한다.

도 10 에서, 스마트 카드 발급 시스템(200)은 스마트 카드(100)와 접촉 또는 비접촉 방법으로 통신하고, 스마트 카드(100)의 스마트 카드 시큐리티 도메인(150)에 인증 기관(400)으로부터 전달받은 스마트 카드 인증서, 스마트 카드 개인키 및 인증 기관 공개키를 저장한다.

먼저, 스마트 카드(100)의 스마트 카드 시큐리티 도메인(150)은 인증 기관(400)으로부터 인증 기관 관리키를 전달 받는다(S110).

인증 기관은 인증 기관 공개키 및 인증 기관 개인키 쌍을 생성하며, 해당 스마트 카드에 대하여 스마트 카드 공개키와 스마트 카드 개인키 쌍, 및 적절한 인증서를 생성한다.

스마트 카드 발급 시스템(200)은 인증 기관(400)으로부터 전달되는 해당 스마트 카드 시큐리티 도메인(150)에 대응하는 스마트 카드 시큐리티 도메인 정보를 포함하는 명령정보를 스마트 카드(100)에 전달한다(S120).

다음, 스마트 카드 발급 시스템(200)은 수신한 명령 정보에 대응하는 스마트 카드 시큐리티 도메인(150)이 기 저장된 인증 기관 관리키를 이용하여 인증 기관(400)과 상호 인증 과정을 처리하도록 제어한다(S130).

해당 상호 인증이 정상적으로 수행되는 경우, 인증 기관(400)은 인증 기관 관리키로 스마트 카드 개인키를 암호화한다(S140).

다음 인증 기관(400)은 해당 스마트 카드에 대응하는 스마트 카드 인증서, 암호화된 스마트 카드 개인키, 및 인증 기관 공개키를 스마트 카드 발급 시스템(200)을 통해 스마트 카드(100)에 전달한다(S150).

한편, 스마트 카드 인증서만을 사용하는 스마트 카드 키 관리 방법에서는 인증 기관 공개키를 스마트 카드 발급 시스템(200)에 전달할 필요는 없다.

다음, 스마트 카드 발급 시스템(200)은 스마트 카드 시큐리티 도메인(150)을 작동시켜, 암호화된 스마트 카드 개인키를 인증 기관 관리키를 이용하여 복호화하게 한다(S160).

이때, 스마트 카드(100)는 스마트 카드 인증서, 스마트 카드 개인키 및 인증 기관 공개키를 저장하고, 스마트 카드 발급 시스템(200)에 수신 확인 정보를 전달한다(S170).

서비스 제공자는 이렇게 스마트 카드 시큐리티 도메인(150)에 저장된 스마트 카드 인증서 및 스마트 카드 개인키를 이용하여 자신이 카드 관리 시스템을 통해 생성한 서비스 제공자 관리키를 서비스 제공자 시큐리티 도메인(130)에 다른 사람도 알 수 없도록 저장할 수 있게 된다.

이하 도 11 및 도 12은 도 10의 방법에 따라 스마트 카드 인증서 및 스마트 카드 개인키가 저장된 스마트 카드 시큐리티 도메인(150)을 포함하는 스마트 카드의 키 관리 방법을 보여준다.

도 11은 인증서로서 스마트 카드에 저장되는 스마트 카드 인증서만을 사용하는 스마트 카드 키 관리 방법에 해당하며, 도 12은 인증서로서 스마트 카드 및 카드 관리 시스템에 각각 저장되는 스마트 카드 인증서 및 서비스 제공자 인증서 둘 다를 사용하는 스마트 카드의 키 관리 방법에 해당한다.

먼저, 도 11에 도시된 본 발명의 실시예에 따른 스마트 카드의 키 관리 방법을 먼저 설명한다. 도 11 에 도시된 스마트 카드의 키 관리 방법은 도 5의 스마트 카드 시큐리티 도메인(150)을 포함하는 도 3의 스마트 카드와 도 6의 카드 관리 시스템(300)을 사용한다.

스마트 카드 사용자가 특정 서비스 제공자로부터 소정의 서비스를 제공받고자 하는 경우, 해당 스마트 카드 사용자는 해당 스마트 카드에 소정의 서비스에 대응하는 서비스 제공자 관리키를 특정 서비스 제공자로부터 수신 받아 해당 스마트 카드에 저장해야 한다.

서비스 제공자는 스마트 카드 사용자로부터 해당 서비스의 수행을 위한 요청이 수신되는 경우, 카드 관리 시스템(300)을 이용하여 스마트 카드에 저장된 스마트 카드 인증서를 수신한다. 즉 스마트 카드(100)의 스마트 카드 시큐리티 도메인(150)은 저장된 스마트 카드 인증서를 카드 관리 시스템(300)에 전달한다(S210).

카드 관리 시스템(300)은 전달된 스마트 카드 인증서를 인증 기관 공개키로 검증하고(S220), 검증된 스마트 카드 인증서로부터 스마트 카드 공개키를 획득한다(S230).

다음 카드 관리 시스템(300)은 요청된 소정의 서비스에 대응하는 서비스 제공자 관리키를 생성하고(S240), 생성된 서비스 제공자 관리키를 획득한 스마트 카드 공개키를 이용하여 암호화한다(S250).

다음 서비스 제공자는 스마트 카드 내의 자신의 서비스 제공자 시큐리티 도메인을 식별하기 위한 서비스 제공자 시큐리티 도메인 정보를 포함하는 명령 정보를 스마트 카드(100)에 전달한다. 즉 스마트 카드(100)의 서비스 제공자 시큐리티 도메인(130)은 카드 관리 시스템(300)으로부터 명령 정보를 수신한다(S260).

다음 스마트 카드(100)의 서비스 제공자 시큐리티 도메인(130)은 카드 관리 시스템(300)으로부터 암호화된 서비스 제공자 관리키를 수신한다(S270).

서비스 제공자 시큐리티 도메인(130)은 전달된 암호화된 서비스 제공자 관리키를 스마트 카드 시큐리티 도메인(150)에 전달하여 복호화를 요청한다(S280).

스마트 카드 시큐리티 도메인(150)는 암호화된 서비스 제공자 관리키를 기 저장된 스마트 카드 개인키를 이용하여 복호화하고(S290), 복호화된 서비스 제공자 관리키를 복호화를 요청한 서비스 제공자 시큐리티 도메인(130)에 전달한다(S300).

서비스 제공자 시큐리티 도메인(130)은 스마트 카드 시큐리티 도메인(150)으로부터 전달받은 서비스 제공자 관리키를 저장하고, 카드 관리 시스템(300)에 수신 확인 정보를 전달한다(S310).

이상 살펴본 바와 같이, 도 11에 도시된 스마트 카드의 키 관리 방법에서 카드 관리 시스템은 먼저 스마트 카드에 저장된 스마트 카드 인증서를 검증 한 후, 그로부터 스마트 카드 공개키를 획득하고, 스마트 카드 사용자가 요청한 서비스에 해당하는 서비스 제공자 관리키를 획득한 스마트 카드 공개키로 암호화하여 스마트 카드에 전달한다. 다음 스마트 카드의 스마

트 카드 시큐리티 도메인은 암호화된 서비스 제공자 관리키를 저장된 스마트 카드 개인키로 복호화한 뒤, 해당되는 서비스 제공자 시큐리티 도메인에 저장한다. 이렇게 새로운 서비스 제공자 관리키를 저장한 스마트 카드는 서비스 제공자 관리키를 이용하여 안전하게 서비스 제공자와 통신함으로써 서비스 제공자로부터 해당하는 서비스를 제공받을 수 있게 된다.

다음으로, 도 12에 도시된 본 발명의 실시예에 따른 스마트 카드의 키 관리 방법을 설명한다.

도 12에 도시된 스마트 카드의 키 관리 방법은 도 7의 스마트 카드 시큐리티 도메인(150')을 포함하는 도 3의 스마트 카드와 도 8의 카드 관리 시스템(300')을 사용한다.

먼저, 도 12의 키 관리 방법에 사용되는 도 8의 카드 관리 시스템(300')은 인증 기관으로부터 서비스 제공자 인증서 및 서비스 제공자 개인키를 수신하여 저장한다(S410).

다음, 서비스 제공자는 스마트 카드 사용자로부터 해당 서비스의 수행을 위한 요청이 수신되는 경우, 카드 관리 시스템(300')을 이용하여 스마트 카드에 저장된 스마트 카드 인증서를 수신한다. 즉 스마트 카드(100)의 스마트 카드 시큐리티 도메인(150')은 저장된 스마트 카드 인증서를 카드 관리 시스템(300)에 전달한다(S420).

카드 관리 시스템(300')은 전달된 스마트 카드 인증서를 인증 기관 공개키로 검증하고(S430), 검증된 스마트 카드 인증서로부터 스마트 카드 공개키를 획득한다(S440).

다음 카드 관리 시스템(300)은 요청된 소정의 서비스에 대응하는 서비스 제공자 임시키를 생성하고(S450), 생성된 서비스 제공자 임시키를 획득한 스마트 카드 공개키를 이용하여 암호화한다(S460).

다음 서비스 제공자는 스마트 카드 내의 자신의 서비스 제공자 시큐리티 도메인을 식별하기 위한 서비스 제공자 시큐리티 도메인 정보를 포함하는 명령 정보를 스마트 카드(100)에 전달한다. 즉 스마트 카드(100)의 서비스 제공자 시큐리티 도메인(130)은 카드 관리 시스템(300')으로부터 명령 정보를 수신한다(S470).

다음 스마트 카드(100)의 서비스 제공자 시큐리티 도메인(130)은 카드 관리 시스템(300')으로부터 암호화된 서비스 제공자 임시키 및 서비스 제공자 인증서를 수신한다(S480).

서비스 제공자 시큐리티 도메인(130)은 전달된 암호화된 서비스 제공자 임시키 및 서비스 제공자 인증서를 스마트 카드 시큐리티 도메인(150')에 전달하고, 서비스 제공자 임시키의 복호화를 요청한다(S490).

스마트 카드 시큐리티 도메인(150')은 전달된 서비스 제공자 인증서를 인증 기관 공개키로 검증하고(S500), 검증된 서비스 제공자 인증서로부터 서비스 제공자 공개키를 획득한다(S510).

다음 스마트 카드 시큐리티 도메인(150')은 서비스 제공자 공유키의 생성을 위해 스마트 카드 임시키를 생성한다(S520).

한편, 스마트 카드 시큐리티 도메인(150')은 저장된 스마트 카드 개인키를 이용하여 카드 관리 시스템(300')으로부터 수신된 암호화된 서비스 제공자 임시키를 복호화한다(S530).

다음 스마트 카드 시큐리티 도메인(150')은 생성된 스마트 카드 임시키 및 복호화된 서비스 제공자 임시키를 이용하여 서비스 제공자 공유키를 생성한다(S540).

한편, 스마트 카드 시큐리티 도메인(150')은 획득된 서비스 제공자 공개키를 이용하여 생성된 스마트 카드 임시키를 암호화한다(S550).

스마트 카드 시큐리티 도메인(150')은 암호화된 스마트 카드 임시키를 서비스 제공자 시큐리티 도메인(130)을 통해 카드 관리 시스템(300')에 전달한다(S560).

카드 관리 시스템(300')은 서비스 제공자 개인키를 이용하여 수신된 암호화된 스마트 카드 임시키를 복호화한다(S570).

다음, 카드 관리 시스템(300')은 복호화된 스마트 카드 임시키 및 서비스 제공자 임시키를 이용하여 서비스 제공자 공유키를 생성한다(S580).

카드 관리 시스템(300')은 요청된 서비스에 대응하는 서비스 제공자 관리키를 생성한다(S590).

다음, 카드 관리 시스템(300')은 생성된 서비스 제공자 공유키를 이용하여 생성된 서비스 제공자 관리키를 암호화하고(S600), 암호화된 서비스 제공자 관리키를 서비스 제공자 시큐리티 도메인(130)을 통해 스마트 카드 시큐리티 도메인(150')에 전달한다. 즉, 스마트 카드 시큐리티 도메인(150')은 카드 관리 시스템(300')으로부터 암호화된 서비스 제공자 관리키를 수신한다(S610).

다음 스마트 카드 시큐리티 도메인(150')은 저장되어 있는 서비스 제공자 공유키를 이용하여 수신된 암호화된 서비스 제공자 관리키를 복호화하고(S620), 서비스 제공자 시큐리티 도메인에 전달한다(S630).

서비스 제공자 시큐리티 도메인(130)은 스마트 카드 시큐리티 도메인(150')으로부터 전달 받은 서비스 제공자 관리키를 저장하고, 카드 관리 시스템(300')에 수신 확인 정보를 전달한다(S640).

이렇게 새로운 서비스 제공자 관리키를 저장한 스마트 카드는 서비스 제공자 관리키를 이용하여 안전하게 서비스 제공자와 통신함으로써 서비스 제공자로부터 해당하는 서비스를 제공받을 수 있게 된다.

상기에서는 본 발명의 바람직한 실시예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 후술 되는 특허청구범위와 발명의 상세한 설명 및 첨부한 도면의 범위 안에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 본 발명의 보호 범위에 속하는 것은 당연하다.

발명의 효과

상술한 바와 같이, 본 발명의 실시예에 따른 스마트 카드 및 서비스 제공자의 카드 관리 시스템은 스마트 카드 발급자를 통하지 않고, 서비스 제공자가 자신의 서비스 제공자 관리키를 스마트 카드의 서비스 제공자 시큐리티 도메인에 저장할 수 있게 한다.

따라서 서비스 제공자는 스마트 카드 발급자를 통하지 않고 스마트 카드를 위한 서비스 제공자 관리키를 효율적으로 관리할 수 있게 된다. 결국 본 발명의 실시예에 따르면, 서비스 제공자는 스마트 카드 발급자와 상관없이 스마트 카드의 시큐리티 도메인을 자체적으로 관리함으로써 스마트 카드 발급자가 아닌 서비스 제공자에 의해 스마트 카드의 후발급이 이루어지게 된다.

따라서 본 발명의 실시예에 따른 스마트 카드 및 카드 관리 시스템은 서비스 제공자에게 서비스 제공자가 스마트 카드 발급자에게 자신의 관리키를 알리지 않고 자체적으로 관리할 수 있는 환경을 제공할 수 있다.

도면의 간단한 설명

도 1은 종래의 스마트 카드를 나타내는 블럭도이다.

도 2는 도 1의 스마트 카드의 키 관리 방법을 보여주는 블럭도이다.

도 3은 본 발명의 실시예에 따른 스마트 카드를 나타내는 블럭도이다.

도 4는 본 발명의 스마트 카드의 키 관리 시스템의 구성을 보여주는 블럭도이다.

도 5는 도 3의 스마트 카드 시큐리티 도메인의 일례를 보여주는 블럭도이다.

도 6은 도 4의 카드 관리 시스템의 일례를 보여주는 블럭도이다.

도 7은 도 3의 스마트 카드 시큐리티 도메인의 다른 예를 보여주는 블럭도이다.

도 8은 도 4의 카드 관리 시스템의 다른 예를 보여주는 블럭도이다.

도 9는 본 발명에 따른 스마트 카드 발급 시스템의 일례를 보여준다.

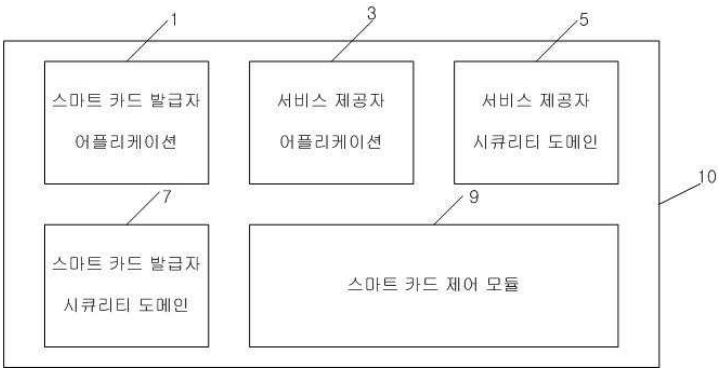
도 10은 본 발명의 실시예에 따라 스마트 카드 시큐리티 도메인에 인증서 및 스마트 카드 개인 키를 저장하는 방법을 보여주는 블럭도이다.

도 11은 본 발명의 실시예에 따른 스마트 카드의 키 관리 방법의 일례를 보여주는 블럭도이다.

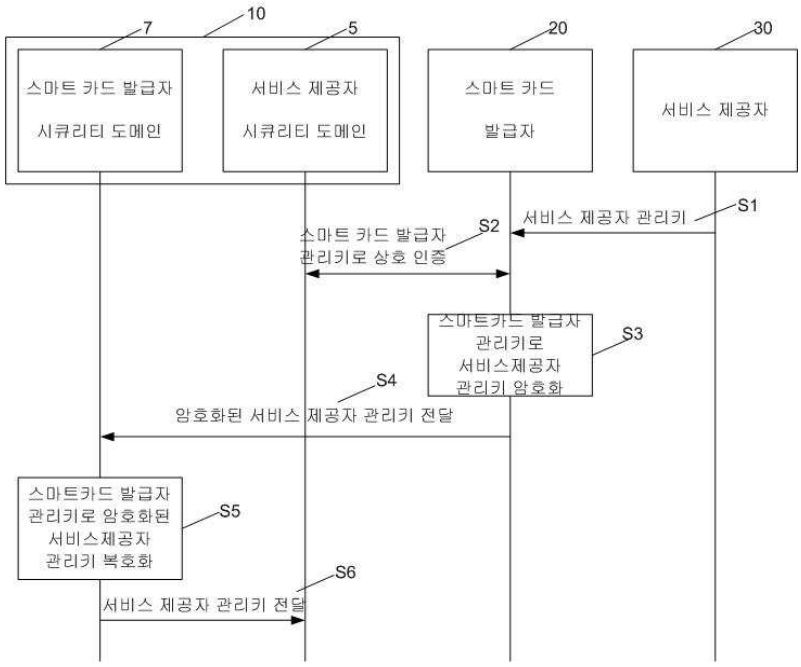
도 12는 본 발명의 실시예에 따른 스마트 카드의 키 관리 방법의 다른 예를 보여주는 블럭도이다.

도면

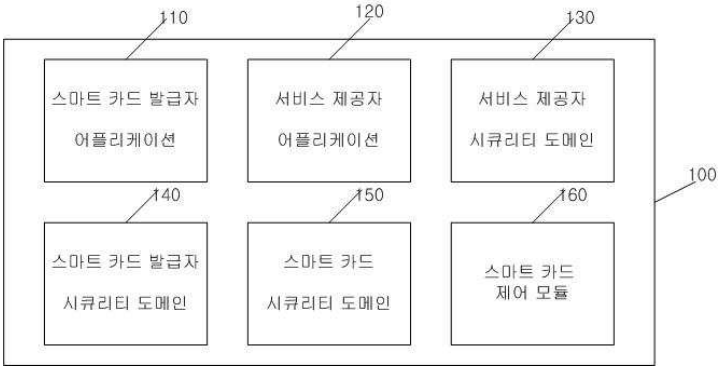
도면1



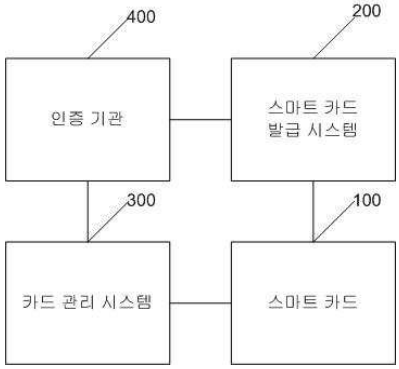
도면2



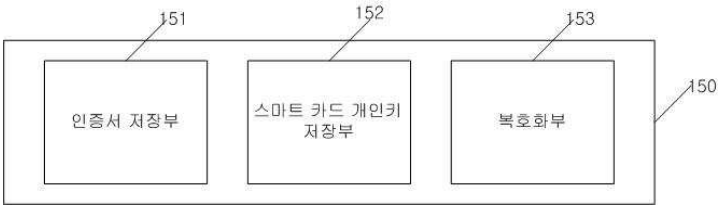
도면3



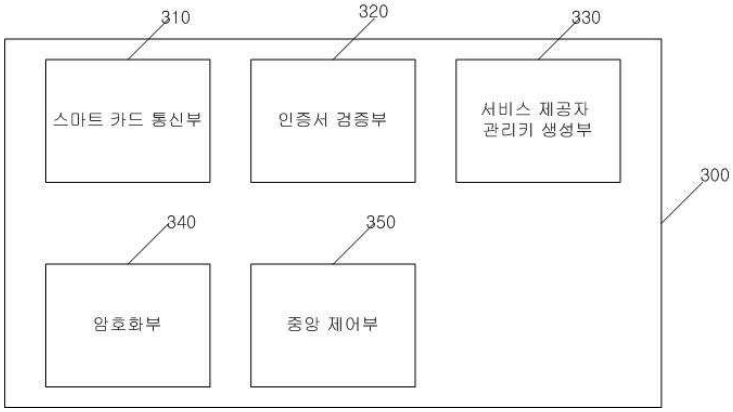
도면4



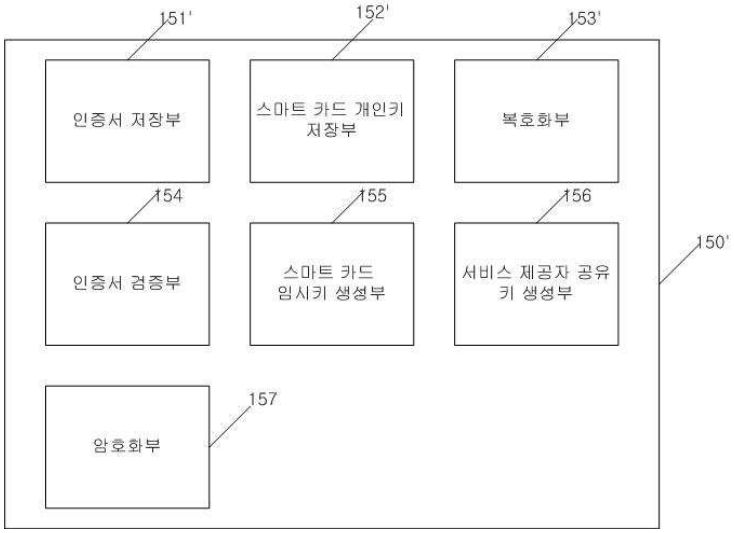
도면5



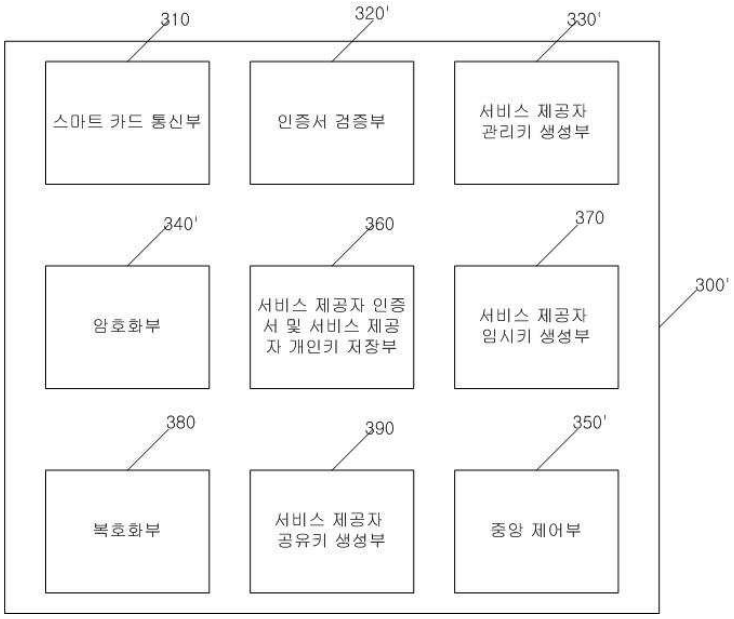
도면6



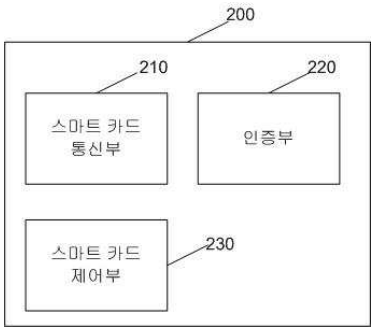
도면7


151'
152'
153'
인증서 저장부
스마트 카드 개인키 저장부
복호화부
154
155
156
인증서 검증부
스마트 카드 임시키 생성부
서비스 제공자 공유키 생성부
150'
157
암호화부

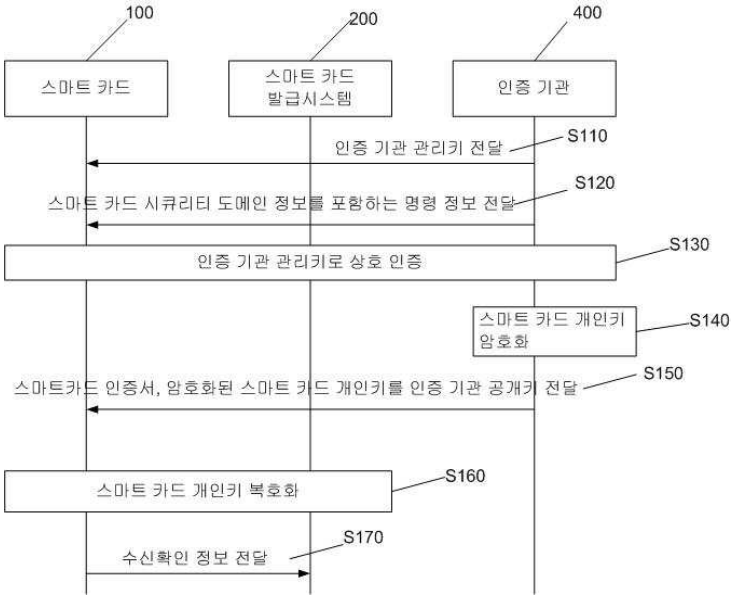
도면8


310
320'
330'
스마트 카드 통신부
인증서 검증부
서비스 제공자 관리키 생성부
340'
360
370
암호화부
서비스 제공자 인증서 및 서비스 제공자 개인키 저장부
서비스 제공자 임시키 생성부
300'
380
390
350'
복호화부
서비스 제공자 공유키 생성부
중앙 제어부

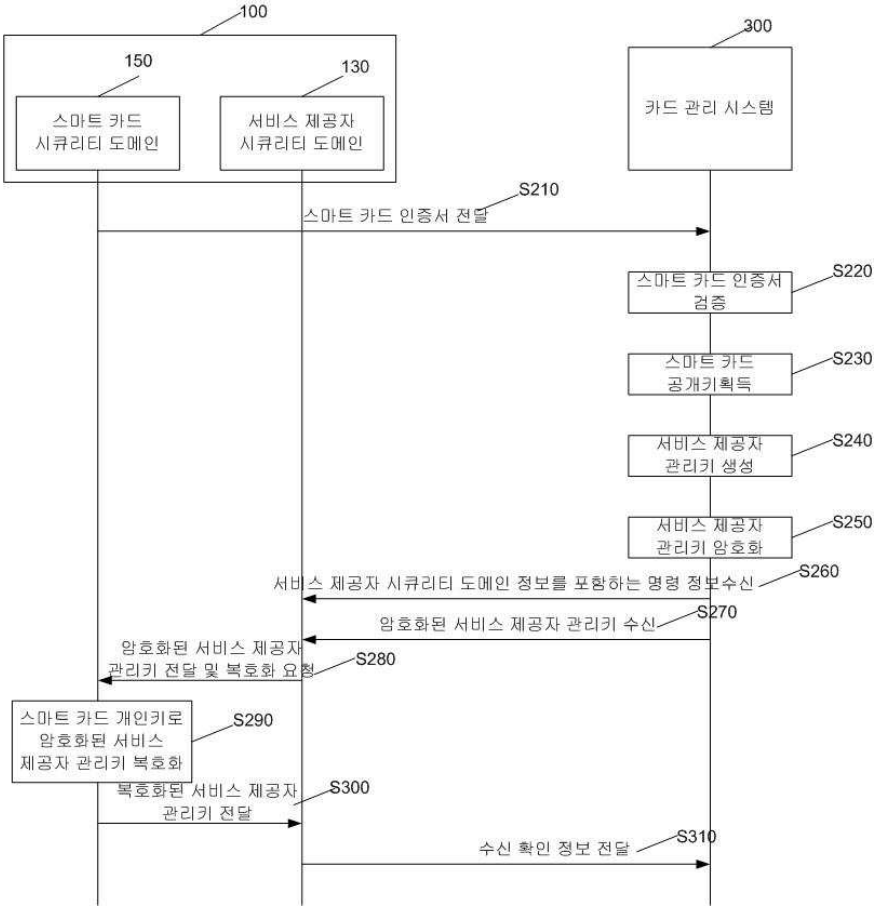
도면9


200
210
220
스마트 카드 통신부
인증부
스마트 카드 제어부
230

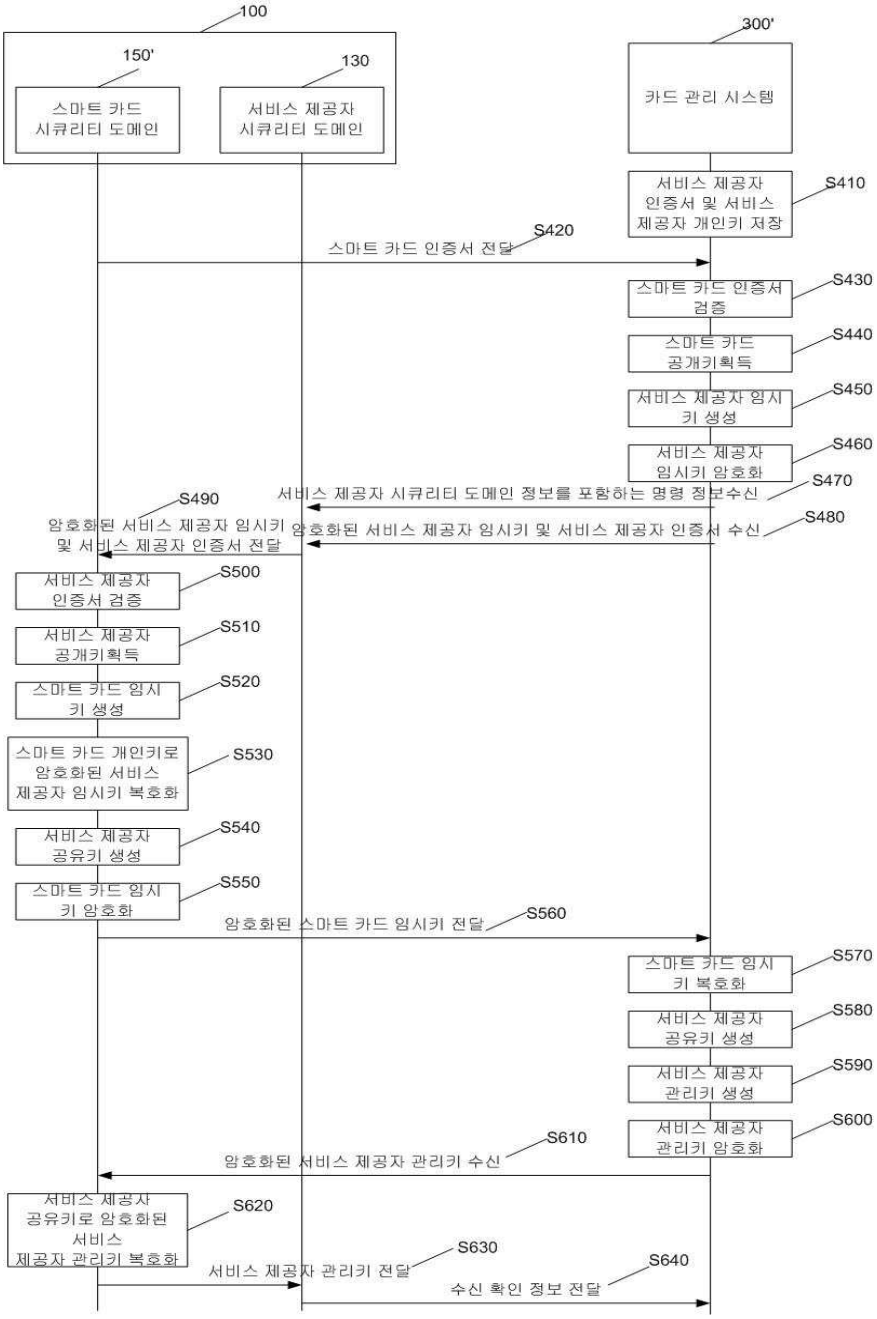
도면10


100
200
400
스마트 카드
스마트 카드 발급시스템
인증 기관
S110
인증 기관 관리키 전달
S120
스마트 카드 시큐리티 도메인 정보를 포함하는 명령 정보 전달
S130
인증 기관 관리키로 상호 인증
스마트 카드 개인키 암호화
S140
S150
스마트카드 인증서, 암호화된 스마트 카드 개인키를 인증 기관 공개키 전달
S160
스마트 카드 개인키 복호화
S170
수신확인 정보 전달

도면11


100
150
130
300
스마트 카드 시큐리티 도메인
서비스 제공자 시큐리티 도메인
카드 관리 시스템
S210
스마트 카드 인증서 전달
스마트 카드 인증서 검증
S220
스마트 카드 공개키획득
S230
서비스 제공자 관리키 생성
S240
서비스 제공자 관리키 암호화
S250
서비스 제공자 시큐리티 도메인 정보를 포함하는 명령 정보수신
S260
암호화된 서비스 제공자 관리키 수신
S270
암호화된 서비스 제공자 관리키 전달 및 복호화 요청
S280
스마트 카드 개인키로 암호화된 서비스 제공자 관리키 복호화
S290
복호화된 서비스 제공자 관리키 전달
S300
수신 확인 정보 전달
S310

도면12


100
150'
스마트 카드
시큐리티 도메인
130
서비스 제공자
시큐리티 도메인
300'
카드 관리 시스템
서비스 제공자
인증서 및 서비스
제공자 개인키 저장
S410
스마트 카드 인증서 전달
S420
스마트 카드 인증서
검증
S430
스마트 카드
공개키획득
S440
서비스 제공자 임시
키 생성
S450
서비스 제공자
임시키 암호화
S460
서비스 제공자 시큐리티 도메인 정보를 포함하는 명령 정보수신
S470
암호화된 서비스 제공자 임시키 및 서비스 제공자 인증서 수신
S480
S490
암호화된 서비스 제공자 임시키
및 서비스 제공자 인증서 전달
서비스 제공자
인증서 검증
S500
서비스 제공자
공개키획득
S510
스마트 카드 임시
키 생성
S520
스마트 카드 개인키로
암호화된 서비스
제공자 임시키 복호화
S530
서비스 제공자
공유키 생성
S540
스마트 카드 임시
키 암호화
S550
암호화된 스마트 카드 임시키 전달
S560
스마트 카드 임시
키 복호화
S570
서비스 제공자
공유키 생성
S580
서비스 제공자
관리키 생성
S590
서비스 제공자
관리키 암호화
S600
암호화된 서비스 제공자 관리키 수신
S610
서비스 제공자
공유키로 암호화된
서비스
제공자 관리키 복호화
S620
서비스 제공자 관리키 전달
S630
수신 확인 정보 전달
S640