



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년04월03일
 (11) 등록번호 10-1722159
 (24) 등록일자 2017년03월27일

(51) 국제특허분류(Int. Cl.)
 G06K 17/00 (2006.01) G06F 21/34 (2013.01)
 G06F 21/85 (2013.01) G06K 19/07 (2006.01)
 (21) 출원번호 10-2010-0091345
 (22) 출원일자 2010년09월17일
 심사청구일자 2015년06월24일
 (65) 공개번호 10-2012-0029521
 (43) 공개일자 2012년03월27일
 (56) 선행기술조사문헌
 KR1020040074212 A*
 KR1020070007424 A*
 KR1020080098640 A*
 *는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 에스엠이네트웍스
 서울특별시 서초구 서초대로54길 29-6, 5층 501호(서초동)
 (72) 발명자
김동영
 경기도 성남시 분당구 중앙공원로 20, 404동 208호 (서현동, 현대아파트)
 (74) 대리인
신용길

전체 청구항 수 : 총 3 항

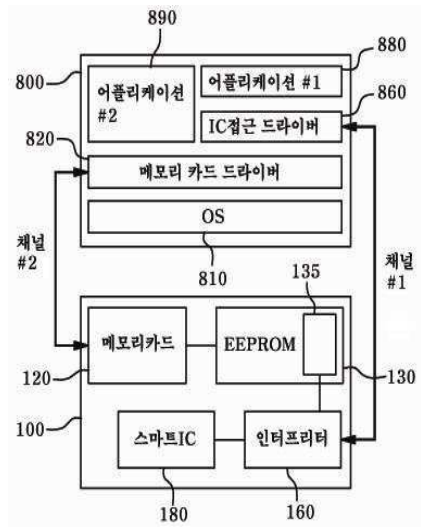
심사관 : 임정복

(54) 발명의 명칭 **보안 메모리 카드**

(57) 요약

본 발명의 데이터 저장 장치는, 소정의 메모리 카드 프로토콜에 따른 데이터 입출력을 수행하는 메모리 카드 인터페이스; 상기 메모리 카드 인터페이스로 인가되는 신호에 따라, 소정의 RF 통신 프로토콜에 따른 근거리 무선 통신을 수행하는 NFC 인터페이스; 및 상기 메모리 카드 인터페이스를 통해 입력되는 데이터를 저장하는 저장부로 이루어질 수 있다.

대표도 - 도1



명세서

청구범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

스마트 칩 및 비휘발성 메모리를 구비하는 보안 메모리 카드가 접속한 호스트에서의 상기 비휘발성 메모리에 대한 드라이버를 이용하는 상기 스마트 칩에 대한 제어 방법에 있어서,

상기 호스트에 설치된 어플리케이션 프로그램으로부터 상기 스마트 칩에 대한 제어명령을 수령하는 단계;

상기 제어명령을 포함하는 제어파일을 작성하는 단계;

상기 제어파일을 상기 비휘발성 메모리에 대한 드라이버를 이용하여 소정의 인터프리터 영역에 저장하는 단계;

상기 비휘발성 메모리에 대한 드라이버를 이용하여 상기 인터프리터 영역에 저장된 응답파일을 확인하는 단계;
 상기 응답파일을 리딩하는 단계;
 상기 응답파일을 해석하여 상기 제어명령에 대한 상기 스마트 칩의 응답을 획득하는 단계; 및
 상기 응답을 상기 어플리케이션 프로그램으로 전송하는 단계
 를 포함하는 스마트 칩 제어 방법.

청구항 14

제 13 항에 있어서,
 상기 보안 메모리 카드는,
 소정의 메모리 카드 프로토콜에 따른 데이터 입출력을 수행하는 메모리 카드 인터페이스,
 상기 메모리 카드 인터페이스를 통해 입력되는 데이터를 저장하는 저장부,
 소정의 스마트 칩 통신 프로토콜에 따른 작업을 수행하는 스마트 칩, 및
 상기 저장부의 지정된 영역에 기록된 정보를 상기 스마트 칩 통신 프로토콜에 따른 제어신호로 해석하여 상기 스마트 칩으로 전달하는 인터프리터
 를 포함하는 스마트 칩 제어 방법.

청구항 15

제 13 항에 있어서,
 상기 호스트의 운영체제 계층 상에 메모리 카드 드라이버가 설치되어 있으며,
 상기 메모리 카드 드라이버 계층 상에 칩 접근 드라이버가 설치되어 있으며,
 상기 칩 접근 드라이버 상에 상기 어플리케이션 프로그램이 설치되어 있으며,
 상기 스마트 칩 제어 방법은, 상기 칩 접근 드라이버에 의해 수행되는 것을 특징으로 하는 스마트 칩 제어 방법.

발명의 설명

기술 분야

[0001] 본 발명은, 메모리 카드 형태의 데이터 저장 장치로서, 특정 전자 기기(즉, 호스트)의 슬롯에 끼워진 상태에서, 소정의 보안 기능을 수행하는 스마트 칩을 구비한 메모리 카드에 관한 것이다.

배경 기술

[0002] 본 발명은 데이터의 보안 및 저장을 위한 보안 메모리 카드에 관한 것으로, 특히, 메모리 카드에 스마트 칩과 같은 보안 칩이 결합되어 데이터를 안전하게 저장할 수 있으며, 소정의 보안 기능을 지원할 수 있는 메모리 카드 인터페이스를 갖는 보안 메모리 카드에 관한 것이다.

[0003] 보안 데이터를 저장하기 위한 스마트 칩은 자체적인 운영체제(OS)로써 칩 OS(Chip Operating System)를 탑재하고 중앙처리장치(CPU)와 암호화 모듈 및 메모리를 갖추고 있다. 스마트 칩은 암호화 기술을 채용하고 있어, 여러가지 트랜잭션(transaction)을 안전하게 처리할 수 있고, 암호화된 데이터를 저장하기 때문에 전자 지갑, 전자 통장, 개인 인증 등의 분야에서 널리 사용되고 있다.

- [0004] 그리고 휴대용 저장 장치로써 SD(Secure Digital) 카드, 멀티미디어 카드(Multimedia Card, MMC) 또는 콤팩트 플래시(Compact Flash, CF) 카드 등과 같은 카드 형태의 메모리가 존재한다. 특히 SD 카드 중에서 휴대성을 높이기 위해 보다 작은 크기로 만들고 추후 용도를 확장하기 위해 SD 카드의 입출력 단자의 수를 늘린 mini SD 카드가 있다. 이러한 메모리 카드들은 플래시 메모리를 그 내부에 구비한 휴대용 저장장치의 일종으로 휴대전화, 전자책, PDA(Personal Digital Assistant), 스마트폰(smart phone), 디지털 카메라, MP3 플레이어, 캠코더, 개인용 컴퓨터 등의 데이터 저장 장치로써 많이 사용된다.
- [0005] 그러나 종래의 메모리 카드는 상술한 바와 같이 플래시 메모리를 그 내부에 갖추고 있을 뿐 스마트 칩과 같은 보안 칩을 가지고 있지 않아 데이터를 안전하게 저장하는 데는 한계가 있다.
- [0006] 상기 메모리 카드의 한계를 극복하기 위해, 메모리 카드 내에 스마트 칩과 같은 보안 칩을 구비한 보안 메모리 카드가 제안되었다. 그러나, 단순히, 보안 칩을 구비한 메모리 카드는 서로 다른 2개의 데이터 전송 프로토콜들을 겸하거나 프로토콜 변환 처리를 위해, 기존 데이터 전송 프로토콜에 약간의 변화를 주었다. 이는 관점에 따라서는 새로운 규격의 메모리 카드를 제안하는 것이 되어, 그 결과 제안된 메모리 카드의 호환성이 저하되는 문제점을 가지고 있다.
- [0007] 상기 호환성의 문제는 보안 메모리 카드 측의 장애일 뿐만 아니라, 보안 메모리 카드를 이용한 서비스를 제공하는 프로그램에도 큰 제한을 불러온다. 이는 응용 서비스 프로그램 제작자가 보안 메모리 카드를 적용하는 것을 꺼리게 만들어, 보안 메모리 카드의 보급에 장애가 된다.

발명의 내용

해결하려는 과제

- [0008] 본 발명은, 호환성이 우수한 보안 메모리 카드를 제공하고자 한다.
- [0009] 또는, 본 발명은, 그 응용 서비스 프로그램의 제작이 용이한 보안 메모리 카드를 제공하고자 한다.

과제의 해결 수단

- [0010] 본 발명의 일 측면에 따른 보안 메모리 카드는, 소정의 메모리 카드 프로토콜에 따른 데이터 입출력을 수행하는 메모리 카드 인터페이스; 상기 메모리 카드 인터페이스를 통해 입력되는 데이터를 저장하는 저장부; 소정의 스마트 칩 통신 프로토콜에 따른 작업을 수행하는 스마트 칩; 및 상기 저장부의 지정된 영역에 기록된 정보를 상기 스마트 칩 통신 프로토콜에 따른 제어신호로 해석하여 상기 스마트 칩으로 전달하는 인터프리터를 포함한다.
- [0011] 여기서, 상기 인터프리터는, 상기 저장부의 지정된 영역에 기록된 정보의 해석 및 전송을 완료하면, 상기 저장부에 완료됨을 표시할 수 있다.
- [0012] 여기서, 상기 인터프리터는, 상기 스마트 칩이 출력하는 신호를 소정의 데이터 구조로 상기 저장부에 기록할 수 있다.
- [0013] 여기서, 상기 메모리 카드 인터페이스는, 호스트 시스템에 설치된 메모리 카드 드라이버와 데이터 통신 채널을 형성할 수 있다.
- [0014] 여기서, 상기 인터프리터는, 호스트 시스템에 설치된 메모리 카드 드라이버 계층 상에 설치된 칩 접근 드라이버와 데이터 통신 채널을 형성할 수 있다.
- [0015] 여기서, 상기 스마트 칩에는 칩 어플리케이션이 저장되며, 상기 인터프리터는 상기 스마트 칩이 상기 칩 어플리케이션을 실행시킨 결과값을 소정의 데이터 구조로 상기 지정된 영역에 기록할 수 있다.
- [0016] 여기서, 상기 인터프리터는, 상기 저장부의 소정의 인터프리터 영역에 저장된 제어파일을 확인하는 단계; 상기 제어파일을 리딩하는 단계; 상기 제어파일을 해석하여 상기 스마트 칩 통신 프로토콜에 따른 제어신호를 생성하는 단계; 상기 생성된 제어신호를 상기 스마트 칩으로 전송하는 단계; 상기 스마트 칩으로부터 상기 제어신호에 대한 응답을 수령하는 단계; 상기 응답에 대한 정보를 포함하는 응답파일을 작성하는 단계; 및 상기

응답파일을 상기 인터프리터 영역에 저장하는 단계를 수행할 수 있다.

- [0017] 본 발명의 다른 측면에 따른 스마트 칩 비휘발성 메모리를 구비하는 보안 메모리 카드의 스마트 칩 제어 방법은, 상기 비휘발성 메모리의 소정의 인터프리터 영역에 저장된 제어파일을 확인하는 단계; 상기 제어파일을 리딩하는 단계; 상기 제어파일을 해석하여 상기 스마트 칩에 대한 제어신호를 생성하는 단계; 상기 생성된 제어신호를 상기 스마트 칩으로 전송하는 단계; 상기 스마트 칩으로부터 상기 제어신호에 대한 응답을 수령하는 단계; 상기 응답에 대한 정보를 포함하는 응답파일을 작성하는 단계; 및 상기 응답파일을 상기 인터프리터 영역에 저장하는 단계를 포함한다.
- [0018] 여기서, 상기 제어파일을 리딩하는 단계 이후, 상기 리딩된 제어파일을 상기 인터프리터 영역에서 삭제하거나, 해당 제어파일에 대한 리딩이 완료되었음을 표시하는 단계를 더 포함할 수 있다.
- [0019] 여기서, 상기 응답파일을 저장하는 단계 이전에, 상기 인터프리터 영역의 상기 제어파일을 삭제하거나, 해당 제어파일에 대한 처리가 완료되었음을 표시하는 단계를 더 포함할 수 있다.
- [0020] 여기서, 상기 제어파일을 확인한 결과, 상기 인터프리터 영역에 리딩해야 할 제어파일이 존재하지 않으면, 소정의 지연 시간이 경과한 후, 상기 제어파일을 확인하는 단계를 반복할 수 있다.
- [0021] 여기서, 상기 스마트 칩은 칩 어플리케이션을 저장하며, 상기 스마트 칩에 대한 제어신호는 상기 칩 어플리케이션에 대한 작업 수행 요청이며, 상기 응답은 상기 작업 수행 요청에 대하여 상기 스마트 칩이 상기 칩 어플리케이션이 제공하는 기능을 실행시킨 결과일 수 있다.
- [0022] 본 발명의 또 다른 측면에 따른 스마트 칩 및 비휘발성 메모리를 구비하는 보안 메모리 카드가 접속한 호스트에서의 상기 스마트 칩에 대한 제어 방법은, 상기 호스트에 설치된 어플리케이션 프로그램으로부터 상기 스마트 칩에 대한 제어명령을 수령하는 단계; 상기 제어명령을 포함하는 제어파일을 작성하는 단계; 상기 제어파일을 소정의 인터프리터 영역에 저장하는 단계; 상기 인터프리터 영역에 저장된 응답파일을 확인하는 단계; 상기 응답파일을 리딩하는 단계; 상기 응답파일을 해석하여 상기 제어명령에 대한 상기 스마트 칩의 응답을 획득하는 단계; 및 상기 응답을 상기 어플리케이션 프로그램으로 전송하는 단계를 포함한다.
- [0023] 여기서, 상기 보안 메모리 카드는, 소정의 메모리 카드 프로토콜에 따른 데이터 입출력을 수행하는 메모리 카드 인터페이스; 상기 메모리 카드 인터페이스를 통해 입력되는 데이터를 저장하는 저장부; 소정의 스마트 칩 통신 프로토콜에 따른 작업을 수행하는 스마트 칩; 및 상기 저장부의 지정된 영역에 기록된 정보를 상기 스마트 칩 통신 프로토콜에 따른 제어신호로 해석하여 상기 스마트 칩으로 전달하는 인터프리터를 포함한다.
- [0024] 여기서, 상기 호스트의 운영체제 계층 상에 메모리 카드 드라이버가 설치되어 있으며, 상기 메모리 카드 드라이버 계층 상에 칩 접근 드라이버가 설치되어 있으며, 상기 칩 접근 드라이버 상에 상기 어플리케이션 프로그램이 설치되어 있으며, 상기 스마트 칩 제어 방법은, 상기 칩 접근 드라이버에 의해 수행될 수 있다.

발명의 효과

- [0025] 상기 구성에 따른 본 발명의 데이터 저장 장치는, 스마트 칩을 구비한 보안 메모리 카드 또는 그 응용 프로그램의 호환성을 높일 수 있는 이점이 있다.

도면의 간단한 설명

- [0026] 도 1은 본 발명의 일 실시예에 따른 보안 메모리 카드 및 보안 메모리 카드가 접속되는 호스트의 소프트웨어 계층 구조를 도시한 블록도.
- 도 2는 도 1의 인터프리터의 상세 구조의 일 실시예를 도시한 블록도.
- 도 3은 도 1의 보안 메모리 카드의 인터프리터에서 수행될 수 있는 스마트 칩 제어 방법의 일 실시예를 도시한 흐름도.

도 4는 도 1의 호스트의 칩 접근 드라이버에서 수행될 수 있는 스마트 칩 제어 방법의 일 실시예를 도시한 흐름도.

도 5는 본 발명의 사상에 따라 공인인증서를 위한 보안 메모리 카드를 스마트 칩을 구비한 마이크로 SD 카드로 구체화한 실시예의 세부 구성과, 상기 실시예에 따른 마이크로 SD 카드에 대한 호스트로서 스마트 폰의 소프트웨어 계층을 도시한 블록도.

도 6은 도 5의 마이크로 SD 카드에서 수행되는 스마트 칩 제어 방법의 일 실시예를 도시한 흐름도.

도 7은 도 5의 스마트 폰의 칩 접근 드라이버에서 수행될 수 있는 스마트 칩 제어 방법의 일 실시예를 도시한 흐름도.

발명을 실시하기 위한 구체적인 내용

- [0027] 이하, 도면을 참조하여 본 발명의 실시예들을 설명하겠다.
- [0028] 도 1은 본 발명의 일 실시예에 따른 보안 메모리 카드 및 보안 메모리 카드가 접속되는 호스트의 소프트웨어 계층 구조를 도시하고 있다.
- [0029] 도시한 보안 메모리 카드(100)는, 소정의 메모리 카드 프로토콜에 따른 데이터 입출력을 수행하는 메모리 카드 인터페이스(120); 상기 메모리 카드 인터페이스를 통해 입력되는 데이터를 저장하는 저장부(130); 소정의 스마트 칩 통신 프로토콜에 따른 작업을 수행하는 스마트 칩(180); 및 상기 저장부(130)의 지정된 영역에 기록된 정보를 상기 스마트 칩 통신 프로토콜에 따른 제어신호로 해석하여 상기 스마트 칩(180)으로 전달하는 인터프리터(160)를 포함한다.
- [0030] 상기 메모리 카드 인터페이스(120)는, 종래의 메모리 카드 인터페이스 회로를 포함하도록 구현될 수 있다. 예컨대, 종래의 SD 카드에 사용되는 인터페이스 회로를 포함할 수 있다.
- [0031] 상기 보안 메모리 카드가 데이터를 장기간 저장하는 보조 메모리 장치로 사용될 수 있도록, 상기 저장부(130)는 전기공급이 끊겨도 데이터를 보존할 수 있는 비휘발성 메모리로 구현되는 것이 바람직하다. 예컨대, 상기 저장부(130)는 NAND 메모리나 EEPROM으로 구현될 수 있다.
- [0032] 상기 스마트 칩(180)은, 자체적인 운영체제(OS)로써 칩 OS(Chip Operating System)를 탑재하고 중앙처리장치(CPU)와 암호화 모듈 및 메모리를 갖추고 암호화 기술을 채용할 수 있다. 또한, 상기 스마트 칩(180)은 칩 어플리케이션이라는 응용 프로그램 소프트웨어를 선택적으로 설치하고 실행시킬 수 있다.
- [0033] 상기 스마트 칩 통신 프로토콜에 따른 제어신호를 위해 상기 인터프리터(160)가 상기 저장부(130)의 지정된 영역을 독출하는데, 상기 지정된 영역을 인터프리터 영역(135)이라 칭하겠다.
- [0034] 상기 인터프리터(160)가 상기 인터프리터 영역(135)에서 상기 스마트 칩을 제어하기 위해 독출하는 정보는 파일 형태를 가지도록 구현할 수 있는데, 상기 파일을 제어파일이라 칭하겠다.
- [0035] 또한, 상기 인터프리터(160)는 상기 스마트 칩에서 출력하는 신호에 대한 정보를 상기 인터프리터 영역(135)에 기록할 수 있다. 예컨대, 상기 인터프리터(160)는 상기 제어파일을 해석하여 제어 신호를 상기 스마트 칩(160)에 전송하면 상기 스마트 칩(160)은 제어 신호에 따른 작업을 수행하고 그 응답 신호를 상기 인터프리터(160)로 출력한다. 이에 대하여, 상기 인터프리터(160)는 상기 응답 신호를 해석한 정보를 상기 인터프리터 영역(135)에 파일 형태로 기록할 수 있다. 이하, 상기 인터프리터(160)가 상기 스마트 칩(180)의 출력 신호를 해석하여 상기 인터프리터 영역(135)에 기록하는 파일을 응답파일이라 칭하겠다.
- [0036] 예컨대, 상기 인터프리터(160)는 상기 스마트 칩의 출력 신호를 디지털화한 데이터를 상기 응답파일의 바디에 기록하고, 응답파일임을 나타내는 헤더를 첨부하여 응답파일을 작성할 수 있다.
- [0037] 도시한 호스트(800)의 소프트웨어 계층은, 상기 호스트 장치를 구동시키기 위한 운영체제 계층(810); 상기 운영체제 계층(810) 상에 설치되며 상기 호스트에 접속된 메모리 카드에 접근하기 위한 메모리 카드 드라이버 계층(820); 상기 메모리 카드 드라이버 계층(820) 상에 설치되며 본 발명의 사상에 따른 보안 메모리 카드(100)가 구비한 스마트 칩(180)에 접근하기 위한 칩 접근 드라이버(860); 상기 칩 접근 드라이버(860) 계층 상에 설

치되며 상기 스마트 칩(180)을 이용한 작업을 수행하는 제1 어플리케이션 프로그램(880)을 포함한다.

- [0038] 상기 보안 메모리 카드(100)의 상기 메모리 카드 인터페이스(120)는, 상기 메모리 카드 드라이버(820)와 제2 데이터 통신 채널을 형성하며, 상기 인터프리터(160)는 상기 칩 접근 드라이버(860)와 제1 데이터 통신 채널을 형성한다. 상기 제2 데이터 통신 채널의 구조는 일반적인 메모리 카드와 호스트에 설치된 메모리 카드 드라이버로 형성되는 데이터 통신 채널과 동일할 수 있다.
- [0039] 여기서, 본 발명의 사상에 따른 상기 제1 데이터 통신 채널을 형성하는 인터프리터(160)와 상기 칩 접근 드라이버(860) 사이에 직접 데이터 신호가 실시간적으로 전송되지 않고, 상기 인터프리터 영역(135)을 이용하여 파일을 주고 받는 방식으로 데이터 통신이 이루어진다.
- [0040] 즉, 상기 인터프리터(160)가 상기 칩 접근 드라이버(860)로 데이터를 전송할 때에는, 전송할 데이터를 상기 인터프리터 영역(135)에 응답파일로 저장하고, 상기 칩 접근 드라이버(860)가 상기 인터프리터(160)로 데이터를 전송할 때에는, 전송할 데이터를 상기 인터프리터 영역(135)에 제어파일로 저장한다.
- [0041] 이는 상기 인터프리터(160)와 상기 칩 접근 드라이버(860) 사이의 경로에 위치하는 저장부(130)가 신호를 연속적으로 중계하는 회로가 아니며, 오히려, 연속적인 신호 전송의 차단물로 작용하기 때문이다. 그래서, 상기 제어파일 또는 응답파일을 저장한 후에도, 이를 상대방에게 직접 통보해 줄 수 없다.
- [0042] 이를 극복하기 위해, 상기 인터프리터(160)는 상기 인터프리터 영역(135)에 응답파일을 저장한 후, 주기적으로 이에 대한 답신으로서 제어파일이 저장되어 있는지 상기 인터프리터 영역(135)을 모니터링할 수 있다.
- [0043] 상기 인터프리터(160)는 상기 인터프리터 영역을 주기적으로 모니터링하다가 제어파일을 확인하면 이를 독출하고, 독출한 제어파일을 해석하여 상기 스마트 칩(180)에 대한 제어신호를 생성한다.
- [0044] 반대로, 상기 칩 접근 드라이버(860)는 상기 인터프리터 영역(135)에 응답파일을 저장한 후, 주기적으로 이에 대한 답신으로서 응답파일이 저장되어 있는지 상기 인터프리터 영역(135)을 모니터링할 수 있다.
- [0045] 상기 칩 접근 드라이버(860)는 상기 인터프리터 영역(135)을 주기적으로 모니터링하다가 응답파일을 확인하면 이를 독출하고, 독출한 응답파일을 해석하여 상기 스마트 칩의 응답 신호를 획득하여 상기 제1 어플리케이션(880)에 전달할 수 있다.
- [0046] 상술한 인터프리터(160)와 칩 접근 드라이버(860)의 파일을 매개한 간접적인 데이터 통신 방식은, 동일한 제어파일 또는 응답파일을 중복적으로 독출하여 처리할 위험이 존재한다. 따라서, 상기 위험을 방지하기 위한 수단이 필요하다.
- [0047] 상기 위험의 방지 수단은, 독출 또는 처리가 완료된 제어파일 또는 응답파일을 삭제하는 방식과, 제어파일 또는 응답파일의 독출 또는 처리가 완료되면 이를 표시(예: 플래그를 토글)하는 방식으로 구분할 수 있다.
- [0048] 예컨대, 제1 위험 방지 수단으로서, 상기 인터프리터(160)는 제어파일을 리딩한 후, 상기 제어파일을 상기 인터프리터 영역(135)에서 삭제할 수 있다. 마찬가지로, 상기 칩 접근 드라이버(860)는 응답파일을 리딩한 후, 상기 응답파일을 상기 인터프리터 영역(135)에서 삭제할 수 있다.
- [0049] 예컨대, 제2 위험 방지 수단으로서, 상기 인터프리터(160)는 상기 스마트 칩(180)의 출력 신호를 포함하는 응답파일을 생성한 후, 그 직전에 리딩하였던 제어파일을 상기 인터프리터 영역(135)에서 삭제할 수 있다. 마찬가지로, 상기 칩 접근 드라이버(860)는 상기 스마트 칩(180)으로 전송할 신호를 포함하는 제어파일을 생성한 후, 그 직전에 리딩하였던 응답파일을 상기 인터프리터 영역(135)에서 삭제할 수 있다.
- [0050] 예컨대, 제3 위험 방지 수단으로서, 상기 인터프리터(160)는 상기 스마트 칩(180)의 출력 신호를 포함하는 응답파일을 생성하여 상기 인터프리터 영역(135)에 저장한 후, 그 직전에 리딩하였던 제어파일을 상기 인터프리터 영역(135)에서 삭제할 수 있다. 마찬가지로, 상기 칩 접근 드라이버(860)는 상기 스마트 칩(180)으로 전송할 신호를 포함하는 제어파일을 생성하여 상기 인터프리터 영역(135)에 저장한 후, 그 직전에 리딩하였던 응답파일을 상기 인터프리터 영역(135)에서 삭제할 수 있다.
- [0051] 제어파일 또는 응답파일의 독출 또는 처리가 완료되면 이를 표시(예: 플래그를 토글)하는 방식의 경우에도, 제어/응답파일을 리딩한 후 표시하거나, 제어/응답파일에 대한 답신으로서 응답/제어파일을 생성한 후 표시하거나, 제어/응답파일에 대한 답신으로서 응답/제어파일을 상기 인터프리터 영역(135)에 저장한 후 표시할

수 있다.

- [0052] 여기서, 제어파일은 그 내용으로서 스마트 칩에 대한 제어 명령인 경우 뿐만 아니라, 상기 제1 어플리케이션 프로그램(880)이 상기 스마트 칩(180)으로 전송하려는 정보를 포함할 수 있으며, 상기 응답파일은 그 내용으로서 스마트 칩의 응답인 경우 뿐만 아니라, 상기 스마트 칩(180)이 제1 어플리케이션 프로그램(880)으로 전송하려는 정보를 포함할 수 있다.
- [0053] 구현에 따라, 상기 인터프리터 영역(135)은 상기 제어파일이 저장되는 영역과 상기 응답파일이 저장되는 영역을 구분할 수도 있고, 같은 영역에 서로 덮어쓸 수 있다.
- [0054] 상기 응답파일의 헤더에는 목적지가 될 수 있는 칩 접근 드라이버(860) 및/또는 제1 어플리케이션 프로그램(880)의 식별값을 기록할 수 있다.
- [0055] 상기 메모리 카드 드라이버(820) 계층 상에 상기 칩 접근 드라이버(860)와 함께 메모리 카드를 이용한 작업을 수행하는 제2 어플리케이션 프로그램(890)이 설치될 수 있다.
- [0056] 상기 제2 어플리케이션 프로그램(890)은, 일반적인 메모리 카드(예: SD 카드)를 이용하는 호스트 어플리케이션 프로그램일 수 있다.
- [0057] 상기 메모리 카드 인터페이스(120)는, 종래기술에 따른 호스트의 메모리 카드를 이용하는 제2 어플리케이션 프로그램(200)이, 상기 인터프리터 영역(135)에 접근하지 못하도록 차단하는 역할을 수행할 수 있다. 상기 차단하는 역할은 하기 칩 접근 드라이버의 설명으로 보류하겠다.
- [0058] 호스트(800)의 소프트웨어 계층 구조를 살펴보면, 운영체제(810) 계층은 본 발명의 보안 메모리 카드와 무관하게 호스트의 하드웨어 자원에 적합하도록, 호스트의 하드웨어 제조사가 제작하여 제공하거나 또는 범용 운영체제가 될 수 있다. 예컨대, 호스트(800)가 PC인 경우 상기 운영체제(810) 계층은 마이크로소프트의 윈도우즈 또는 리눅스 등의 될 수 있으며, 호스트가 스마트 폰인 경우 상기 운영체제(810) 계층은 안드로이드 또는 바다 등이 될 수 있다.
- [0059] 메모리 카드 드라이버(820) 계층은, 스마트 칩(180)과 무관하게 특정 메모리 카드 규격을 결정하는 단체의 규격을 따르도록 제작된다. 예컨대, SD 메모리 카드의 규격을 따르도록 제작될 수 있다.
- [0060] 본 발명의 사상에 따라 스마트 칩(180)에 파일을 매개하는 방식으로 접근하는 칩 접근 드라이버(860)는, 소프트웨어 계층 구조상에서는 메모리 카드 드라이버(820)와 데이터 입/출력을 수행하며, 운영체제(810)와는 직접 데이터 입/출력을 수행하지 않는다. 한편, 상기 메모리 카드 드라이버(820)는, 하부 운영체제가 무엇이건 간에 상부 프로그램에 대한 데이터 입/출력이 동일하도록, 호환성이 매우 높은 특징을 가지고 있다. 이는 규격 제공 단계에서 해당 메모리 카드가 널리 보급될 수 있도록 정책적으로 호환성을 높이기 때문이다. 따라서, 상기 칩 접근 드라이버(860)의 제작자는, 운영체제(810)를 상관하지 않고, 단지 메모리 카드 드라이버(820)의 데이터 입/출력 인터페이스만 유의하여 상기 칩 접근 드라이버(860)를 제작할 수 있으며, 제작된 칩 접근 드라이버(860)는 큰 개조없이 다른 운영체제를 가지는 호스트에도 적용될 수 있다. 이러한 특징은 본 발명의 이점들 중 하나를 달성한다.
- [0061] 한편, PC와 같은 일반적인 호스트 장치에는 스마트 칩(즉, 스마트 카드)를 사용하는 어플리케이션 프로그램이 설치될 수 있다. 예컨대, 군사 등 보안성이 높은 사이트의 PC에는 사용자가 리더기에 삽입한 스마트 칩을 상호 인증하여 사용자 인증을 수행하는 어플리케이션 프로그램이 설치될 수 있다. 다시 말해, 이미 기 보급된 많은 스마트 칩 사용 어플리케이션들이 존재한다. 그런데, 기 존재하는 스마트 칩 사용 어플리케이션들을 메모리 카드에 내장되는 스마트 칩을 이용하도록 만들기 위해, 기 존재하는 스마트 칩 사용 어플리케이션들에 큰 개조를 가해야 한다면, 중복적인 개발 자원의 낭비가 아닐 수 없다.
- [0062] 그런데, 본 발명이 제안하는 칩 접근 드라이버(860)는, 소프트웨어 계층 구조상 하부로는 메모리 카드 드라이버(820)와 데이터 입/출력을 수행하며, 상부로는 제1 어플리케이션 프로그램(880)과 일반적인 규격에 따른 스마트 칩을 위한 데이터 전송 프로토콜로 데이터 입/출력을 수행한다. 그 결과, 기 존재하는 스마트 칩 사용 어플리케이션들은 큰 개조 없이 본 발명의 사상에 따른 보안 메모리 카드를 위해 사용될 수 있다. 즉, 상기 제1 어플리케이션(880) 프로그램은 기 존재하는 스마트 칩 사용 어플리케이션일 수 있다. 이러한 특징은 본 발명의 이점들

중 하나를 달성한다.

- [0063] 그런데, 종래기술에 따른 호스트의 메모리 카드를 이용하는 레거시 어플리케이션 프로그램 즉, 제2 어플리케이션 프로그램(200)이, 본 발명의 사상에 따른 인터프리터 영역(135)에 접근하여 데이터를 기록한다면, 본 발명의 사상에 따른 스마트 칩 접근이 불가능해지거나, 상기 제2 어플리케이션 프로그램(200)이 저장한 데이터가 삭제된다. 따라서, 상기 제2 어플리케이션 프로그램(200)이, 상기 인터프리터 영역(135)에 접근하지 못하도록 차단하는 수단이 필요하다.
- [0064] 예컨대, 상기 칩 접근 드라이버(860) 및 상기 메모리 카드 인터페이스(120)는, 상기 인터프리터 영역(135)을 히든 영역으로 취급할 수 있다. 즉, 상기 메모리 카드 드라이버(820)는 접근할 수 있는 데이터 저장부의 어드레스 영역을, 상기 인터프리터 영역(135)을 제외한 영역을 한정하면, 상기 메모리 카드 드라이버(820) 상에서 구동되는 제2 어플리케이션 프로그램(890)은 상기 인터프리터 영역(135)에 접근할 수 없다. 한편, 상기 메모리 카드 인터페이스(120)는 호스트(800)의 상기 데이터 저장부(130) 접근 동작 지시들 중, 그 발송지가 칩 접근 드라이버(860)인 경우에는, 상기 접근 동작 지시에 기재된 데이터 저장부(130)에 대한 어드레스에 소정의 오프셋값을 가하여, 상기 데이터 저장부(130)에 대한 접근 동작을 수행할 수 있다. 여기서, 상기 오프셋값은 상기 인터프리터 영역(135)에 도달하기 위한 것으로, 이에 따라, 상기 칩 접근 드라이버(860)는 상기 인터프리터 영역(135)에 접근하여 리딩/저장할 수 있다.
- [0065] 도 2는 도 1의 인터프리터의 상세 구조의 일 실시예를 도시한 것이다. 도시한 인터프리터(160)는, 상기 저장부(130)의 인터프리터 영역(135)에 파일을 저장하거나 저장된 파일을 독출하는 파일 저장부(162); 상기 파일 저장부(162)가 독출한 정보를 해석하여 상기 스마트 칩(180)에 대한 제어 신호를 생성하는 칩 제어부(164); 및 상기 스마트 칩(180)이 부여된 작업을 수행한 것에 대한 응답을 상기 파일 저장부(262)로 전달하기 위한 응답부(266)를 포함한다.
- [0066] 도 3은 도 1의 보안 메모리 카드(100)의 인터프리터(160)에서 수행될 수 있는 스마트 칩 제어 방법의 일 실시예를 도시한다.
- [0067] 도시한 스마트 칩 제어 방법은, 비휘발성 메모리인 저장부(130) 내 소정의 인터프리터 영역(135)에 저장된 제어파일을 확인하는 단계(S120); 상기 제어파일을 리딩하는 단계(S140); 상기 제어파일을 해석하여 상기 스마트 칩(180)에 대한 제어신호를 생성하는 단계(S160); 상기 생성된 제어신호를 상기 스마트 칩(180)으로 전송하는 단계(S180); 상기 스마트 칩(180)으로부터 상기 제어신호에 대한 응답을 수령하는 단계(S220); 상기 응답에 대한 정보를 포함하는 응답파일을 작성하는 단계(S240); 및 상기 응답파일을 상기 인터프리터 영역(135)에 저장하는 단계(S260)를 포함한다.
- [0068] 상기 S120 단계에서 제어파일을 확인하는 동작은, 제어파일이 상기 인터프리터 영역(135)에 저장되어 있는 것을 확인하는 과정 및 상기 저장된 제어파일이 인터프리터(160)가 처리해야 할, 아직 미처리된 제어파일임을 확인하는 과정을 포함할 수 있다.
- [0069] 상기 S220 단계에서는, 상기 스마트 칩(180)으로부터 직렬 통신 방식으로 출력되는 신호를 버퍼링하는 방식으로 상기 스마트 칩(180)의 응답을 수령할 수 있다.
- [0070] 구현에 따라, 상기 S120 단계에서 상기 제어파일을 확인한 결과, 상기 인터프리터 영역(135)에 리딩해야 할 제어파일이 존재하지 않으면, 소정의 지연 시간이 경과한 후, 상기 제어파일을 확인하는 단계(S120)를 반복 수행할 수 있다.
- [0071] 구현에 따라, 상기 S140 단계 이후, 상기 리딩된 제어파일을 상기 인터프리터 영역(135)에서 삭제하거나, 해당 제어파일에 대한 리딩이 완료되었음을 표시하는 단계를 더 포함할 수 있다.
- [0072] 또는, 상기 S240 단계에서 응답파일의 작성이 성공한 것을 확인하거나, 상기 S260 단계에서 응답파일의 저장을 확인하면, 상기 인터프리터 영역(135)의 상기 제어파일을 삭제하거나, 해당 제어파일에 대한 처리가 완료되었음을 표시하는 단계를 더 포함할 수 있다.

- [0073] 도 4는 도 1의 호스트(800)의 칩 접근 드라이버(860)에서 수행될 수 있는 스마트 칩 제어 방법의 일 실시예를 도시한다.
- [0074] 도시한 칩 제어 방법은, 상기 호스트(800)에 설치된 제1 어플리케이션 프로그램(880)으로부터 상기 스마트 칩(180)에 대한 제어명령을 수령하는 단계(S620); 상기 제어명령을 포함하는 제어파일을 작성하는 단계(S640); 상기 제어파일을 소정의 인터프리터 영역에 저장하는 단계(S660); 상기 인터프리터 영역에 저장된 응답파일을 확인하는 단계(S720); 상기 응답파일을 리딩하는 단계(S740); 상기 응답파일을 해석하여 상기 제어명령에 대한 상기 스마트 칩의 응답을 획득하는 단계(S760); 및 상기 응답을 상기 어플리케이션 프로그램으로 전송하는 단계(S780)를 포함한다.
- [0075] 상기 S620 단계는 상기 제1 어플리케이션 프로그램(880)과 칩 접근 드라이버(860) 사이의 데이터 입/출력 인터페이스에 의해 수행될 수 있다.
- [0076] 상기 S720 단계에서 응답파일을 확인하는 동작은, 응답파일이 상기 인터프리터 영역(135)에 저장되어 있는 것을 확인하는 과정 및 상기 저장된 응답파일이 상기 칩 접근 드라이버(860)가 처리해야 할, 아직 미처리된 응답파일임을 확인하는 과정을 포함할 수 있다.
- [0077] 구현에 따라, 상기 S720 단계에서 상기 응답파일을 확인한 결과, 상기 인터프리터 영역(135)에 리딩해야 할 응답파일이 존재하지 않으면, 소정의 지연 시간이 경과한 후, 상기 응답파일을 확인하는 단계(S720)를 반복 수행할 수 있다.
- [0078] 구현에 따라, 상기 S740 단계 이후, 상기 리딩된 응답파일을 상기 인터프리터 영역(135)에서 삭제하거나, 해당 응답파일에 대한 리딩이 완료되었음을 표시하는 단계를 더 포함할 수 있다.
- [0079] 또는, 상기 S640 단계에서 제어파일의 작성이 성공한 것을 확인하거나, 상기 S660 단계에서 제어파일의 저장을 확인하면, 그 직전에 상기 인터프리터 영역(135)에 기록된 응답파일을 삭제하거나, 해당 응답파일에 대한 처리가 완료되었음을 표시하는 단계를 더 포함할 수 있다.
- [0080] 본 실시예의 보안 메모리 카드는 모바일 폰에 삽입되어, 모바일 폰을 이용한 금융 업무를 수행하는데 적용될 수 있다. 보다 구체적으로, 일종의 모바일 소형 PC인 스마트 폰을 이용해서, 무선 랜 통신을 이용한 무선 네트워크 환경에서 인터넷 뱅킹을 사용하는데 적용될 수 있다.
- [0081] 일반적으로 인터넷 뱅킹의 보안성을 확보하기 위해 소프트웨어 모듈로 된 공인인증서를 사용한다. 그런데, 스마트 폰에 소프트웨어 모듈의 공인인증서를 적용하는데 다음과 같은 문제가 있다. 우선, 스마트 폰은 일반적인 PC보다 하드웨어 성능이 떨어져서, 일반적인 PC에 사용되는 소프트웨어 공인인증서를 구동하기에는 무리가 있다. 그래서, 스마트 폰용 소프트웨어 공인인증서는 보안키 및 연산량이 저하시킨 것을 사용하여야 충분한 속도를 얻을 수 있으나, 그러면, 소프트웨어 공인인증서의 복제 및 불법사용에 대한 안전성이 떨어지게 된다.
- [0082] 상술한 문제점을 극복하기 위해서는 스마트 폰의 인터넷 뱅킹에는 별도의 하드웨어로 된 공인인증서를 사용하는 것이 바람직하며, 공인인증서를 위한 별도의 하드웨어는 독자적인 CPU 및 메모리를 구비한 스마트 칩이 일반적으로 이용된다.
- [0083] 그런데, 현재 보급된 일반적인 규격의 스마트 폰은 스마트 칩을 결합하기 위한 슬롯을 하나 구비하는데, 상기 슬롯은 USIM 이라고 불리는 가입자 식별 확인용 스마트 칩을 위한 용도로 사용되고 있으며, 공인인증서용 스마트 칩이 사용되기에는 그 우선순위가 낮다. 이를 극복하기 위한 최근의 연구는, 하나의 단일 USIM 칩이 가입자 식별 확인 기능 뿐만 아니라 공인인증서 같은 응용 보안 기능을 수행하도록, USIM의 성능 증대 및 용도 확장에 매진하고 있다.
- [0084] 그러나, 무조건 USIM의 성능을 높이면, 당연히 비용의 증대되며, 고성능 USIM을 원하지 않는 사용자에게는 원치않는 비용 부담의 원인이 된다. 또한, 기존 휴대폰에 보안 기능을 추가하려면 USIM 자체를 고성능 USIM으로 교환해야 하므로, 사용자의 비용 부담 및 다양한 형태의 응용, 휴대폰 부가 기능의 빈번한 교체 등을 어렵게 한다. 이는 사용자에게 불편함을 초래함은 물론이다.
- [0085] 한편, 최근의 다기능 휴대 단말기는 멀티미디어 기기의 역할을 수행하게 되어, 대용량 보조 기억 장치가 필요하게 되었다. 그래서, 스마트 폰을 포함한 최근의 멀티미디어 휴대 단말기는, SD 카드, 마이크로 SD 카드, 미니

SD 카드 등과 같은, 메모리 카드를 끼우기 위한 슬롯을 구비하고 있다.

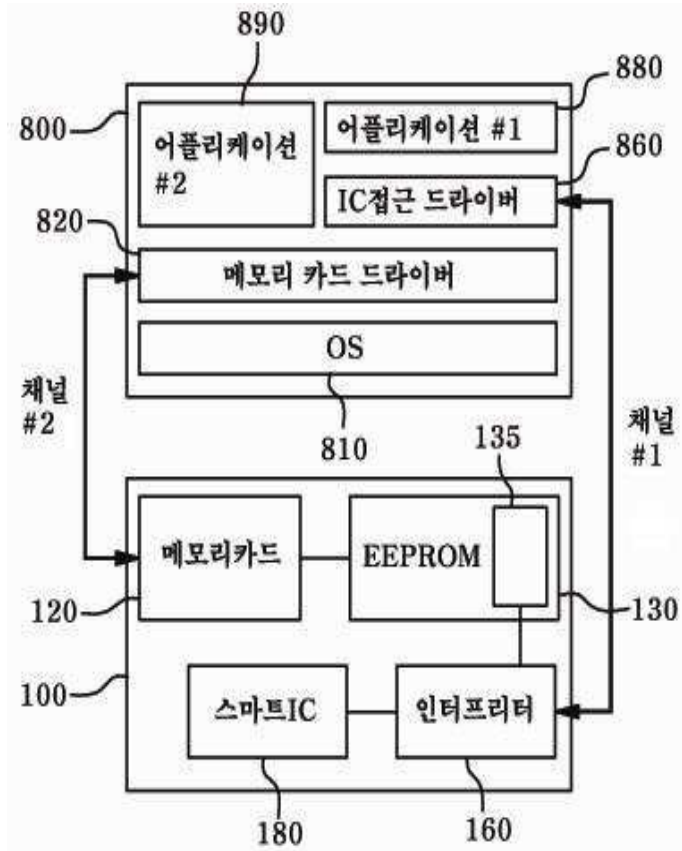
- [0086] 상기 메모리 카드 슬롯을 구비한 스마트 폰에 본 발명의 사상에 따른 보안 메모리 카드를 상기 슬롯에 끼우면, 상기 스마트 폰에 스마트 칩을 이용한 보안 기능으로서 공인인증서 기능을 부여할 수 있다.
- [0087] 도 5는 본 발명의 사상에 따라 공인인증서를 위한 보안 메모리 카드를 스마트 칩을 구비한 마이크로 SD 카드로 구체화한 실시예의 세부 구성과, 상기 실시예에 따른 마이크로 SD 카드에 대한 호스트로서 스마트 폰의 소프트웨어 계층을 도시한다.
- [0088] 도시한 보안 마이크로 SD 카드(100-1)는, 규격에 따른 SD 카드 프로토콜에 따른 데이터 입출력을 수행하는 SD 카드 인터페이스(120-1); 상기 SD 카드 인터페이스를 통해 입력되는 데이터를 저장하는 비휘발성 메모리(130-1); 소정의 스마트 칩 통신 프로토콜에 따른 작업을 수행하는 스마트 칩(180-1); 및 상기 비휘발성 메모리(130-1)의 지정된 영역에 기록된 정보를 상기 스마트 칩 통신 프로토콜에 따른 제어신호로 해석하여 상기 스마트 칩(180)으로 전달하는 인터프리터(160-1)를 포함한다.
- [0089] 상기 SD 카드 인터페이스(120-1)는, SD(Secure Digital) 카드를 위한 표준 규격에 따른 통신 제어 신호인 SD 카드 프로토콜에 대응하여, 데이터를 입/출력하는 구성으로서, 전용 IC와 같은 단일 하드웨어로 구현되거나, 하드웨어 및/또는 소프트웨어 모듈로 구현될 수 있다. 도면에서 상기 SD 카드 인터페이스(120-1)는, 상기 SD 카드 프로토콜에 따라 상기 비휘발성 메모리(130-1)에 데이터를 기록하거나 독출하는 동작을 수행할 수 있다.
- [0090] 상기 도시한 보안 마이크로 SD 카드(100-1)는, 일렬로 정렬된 도전체 스트립 형태를 가지며, 외부의 메모리 카드 슬롯으로서 마이크로 SD 카드 슬롯과 상기 SD 카드 인터페이스(120-1)를 연결 시키는, 메모리 카드 슬롯 접촉부로서 마이크로 SD 카드 슬롯 접촉부(105-1)를 더 구비할 수 있다. 다른 구현에서, 상기 마이크로 SD 카드 슬롯 접촉부(105-1) 대신 일반적인 SD 카드 규격을 따르거나, 미니 SD 카드 규격을 따르는 접촉부를 구비할 수 있다.
- [0091] 상기 비휘발성 메모리(130-1)는, 사용자가 원하는 정보들을 장시간 저장하기 위한 구성으로서, 비교적 대용량을 가지며 비휘발성 저장 메모리인 NAND, EEPROM 등으로 구현될 수 있다. 상기 비휘발성 메모리(130-1)는 대용량 이동식 저장 장치로서의 SD(Secure Digital) 카드의 본연의 기능을 제공하기 위한 것으로, 상기 SD 카드 인터페이스(120-1)에 의해 접근될 수 있는 저장 영역일 수 있다.
- [0092] 상기 스마트 칩(180-1)은, 보안을 위해 규정된 암호화 알고리즘을 수행하는 독립된 단일 칩으로 구현될 수 있다. Mega SIM 등에 사용되는 고성능 스마트 칩으로 구현된 보안 모듈의 경우, 그 내부에 상당한 크기의 비휘발성 메모리를 구비할 수 있다.
- [0093] 상기 스마트 칩(180-1)은, 본 실시예의 보안 마이크로 SD 카드(100-1)의 발급시, 상기 보안 마이크로 SD 카드(100-1)를 식별하기 위한 식별 ID 및/또는 상기 암호화 알고리즘을 위한 암호키가 저장될 수 있다. 또는, 단일 칩으로 구현된 상기 스마트 칩(180-1)은, 상기 단일 칩의 식별 번호를 상기 식별 ID로 사용할 수 있다.
- [0094] 상기 스마트 칩(180-1)은 스마트 칩 통신 프로토콜에 대응하여, 상기 암호화 알고리즘을 수행할 수 있으며, 이를 위해, 상기 인터프리터(160-1)로부터 보안 처리에 대한 명령을 입력받는다. 또한, 상기 스마트 칩(180)은 칩 어플리케이션이라는 응용 프로그램 소프트웨어를 선택적으로 설치하고 실행시킬 수 있는데, 도시한 스마트 칩(180-1)은 칩 어플리케이션으로서, 공인인증서 모듈(185-5)이 설치되어 있다.
- [0095] 도시한 스마트 폰 호스트(800-1)의 소프트웨어 계층은, 상기 스마트 폰을 구동시키기 위한 운영체제 계층(810-1); 상기 운영체제 계층(810-1) 상에 설치되며 상기 스마트 폰의 마이크로 SD 슬롯에 접속된 마이크로 SD 카드에 접근하기 위한 SD 카드 드라이버 계층(820); 상기 SD 카드 드라이버 계층(820) 상에 설치되며 본 발명의 사상에 따른 보안 마이크로 SD 카드(100-1)가 구비한 스마트 칩(180-1)에 접근하기 위한 칩 접근 드라이버(860-

1); 상기 칩 접근 드라이버(860-1) 계층 상에 설치되며 상기 스마트 칩(180-1)에 설치된 공인인증서 모듈(185-1)을 이용한 전자 결제 작업을 수행하는 전자결제 프로그램(880-1)을 포함한다.

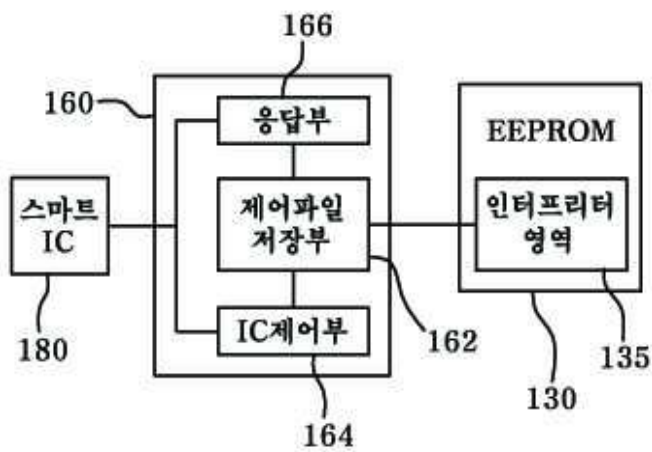
- [0096] 도시한 마이크로 SD 카드와 스마트 폰(800-1)의 소프트웨어 계층의 각 구성요소들은, 도 1의 대응되는 구성요소들을 구체화한 일 레이므로, 도 1의 대응되는 구성 요소에 대한 설명은 도 5의 구성 요소에 그대로 적용될 수 있음은 물론이다.
- [0097] 도 6은 도 5의 마이크로 SD 카드(100-1)에서 수행되는 스마트 칩 제어 방법의 일 실시예를 도시한다.
- [0098] 도시한 스마트 칩 제어 방법은, 비휘발성 메모리(130-1) 내 소정의 인터프리터 영역(135-1)에 저장된 제어파일을 확인하는 단계(S120); 상기 확인 결과 제어 파일이 존재하지 않으면 소정 시간이 경과한 후 상기 S120 단계를 반복하는 단계(S125); 상기 인터프리터 영역(135-1)에 저장된 제어파일을 리딩하는 단계(S140); 상기 제어파일을 해석하여 상기 스마트 칩(180-1)에 대한 제어신호를 생성하는 단계(S160); 상기 생성된 제어신호를 상기 스마트 칩(180-1)으로 전송하는 단계(S180); 상기 스마트 칩(180-1)에서 상기 전송받은 제어신호에 따른 작업을 수행하는 단계(S310); 상기 스마트 칩(180-1)에서 작업 수행에 대한 결과를 상기 인터프리터(160-1)로 전송하는 단계(220); 상기 인터프리터(160-1)에서 전송받은 확인 결과를 포함하는 응답파일을 작성하는 단계(S240); 및 상기 작성된 응답파일을 상기 인터프리터 영역(135-1)에 저장하는 단계(S260)를 포함한다.
- [0099] 한편, 상기 S120 단계 이전에, 도 5의 SD 카드 인터페이스(120-1)가 상기 인터프리터 영역(135-1)에 상기 제어파일을 저장하는 단계를 더 포함할 수 있다.
- [0100] 한편, 상기 S160 단계 이후, 상기 SD 카드 인터페이스(120-1)가 도 5의 호스트 스마트 폰(800-1)의 응답파일 리딩 명령을 접수하면(S65), 상기 인터프리터 영역(135-1)에 저장된 리딩 파일을 리딩하는 단계(S70); 응답파일의 리딩에 실패하면(S80), 상기 스마트 폰(800-1)으로 리딩파일의 리딩에 실패하였음을 통보하고 상기 S70 단계를 반복하는 단계(S85); 리딩파일의 리딩에 성공하면 상기 SD 카드 인터페이스(120-1)가 리딩한 리딩파일을 상기 스마트 폰(800-1)으로 전송하는 단계(S90)를 더 포함할 수 있다.
- [0101] 도 5의 호스트 스마트 폰(800-1)의 전자결제 프로그램(880-1)이 도시한 스마트 칩 제어 방법에 따라, 전자결제를 위한 공인인증서를 이용한 사용자 확인을 수행하는 경우로 구체화하여, 도 6의 흐름을 살펴보겠다.
- [0102] 우선, 상기 S120 단계 이전에, 상기 전자결제 프로그램(880-1)에 의해, 상기 인터프리터 영역(135-1)에, 공인인증서를 이용한 사용자 확인 요청이 기재된 제어파일이 저장될 수 있다.
- [0103] 상기 S160 단계에서는 상기 제어파일에 기재된 공인인증서를 이용한 사용자 확인 요청을 추출하고, 상기 S180 단계에서는 상기 스마트 칩(180-1)에 공인인증서를 이용한 사용자 확인 요청을 전송할 수 있다.
- [0104] 상기 S310 단계에서는 스마트 칩(180-1)이 설치된 공인인증서 모듈을 구동시켜 공인인증서를 이용한 사용자 확인(예 : PASSWORD 확인)을 수행하며, 상기 S220 단계에서는 상기 S310 단계의 수행 결과인 '사용자 확인' 또는 '사용자 미확인'을 상기 인터프리터(160-1)로 전송할 수 있다.
- [0105] 도시한 스마트 칩 제어 방법은, 도 3의 흐름도에 따른 스마트 칩 제어 방법을 구체화한 일 레이므로, 도 3의 대응되는 구성 요소에 대한 설명은 도 6의 구성 요소에 그대로 적용될 수 있음은 물론이다.
- [0106] 도 7은 도 5의 스마트 폰(800-1)의 칩 접근 드라이버(860-1)에서 수행될 수 있는 스마트 칩 제어 방법의 일 실시예를 도시한다.
- [0107] 도시한 칩 제어 방법은, 상기 호스트(800-1)의 칩 접근 드라이버(860-1)가 전자결제 프로그램(880-1)으로부터 상기 스마트 칩(180-1)에 대한 제어명령을 수령하는 단계(S620); 상기 제어명령을 포함하는 제어파일을 작성하는 단계(S640); 상기 제어파일을 소정의 인터프리터 영역에 저장할 것을 SD 카드 드라이버(820-1)에 요청하는 단계(S660); 상기 SD 카드 드라이버(820-1)가 스마트 폰 운영체계를 경유하여 도 5의 마이크로 SD 카드(100-1)로 상기 제어파일을 소정의 인터프리터 영역에 저장할 것을 요청하는 단계(S862); 상기 SD 카드 드라이버(820-1)가 상기 마이크로 SD 카드(100-1)로부터 상기 제어파일의 저장완료를 통보받아(S864), 상기 칩 접근 드

도면

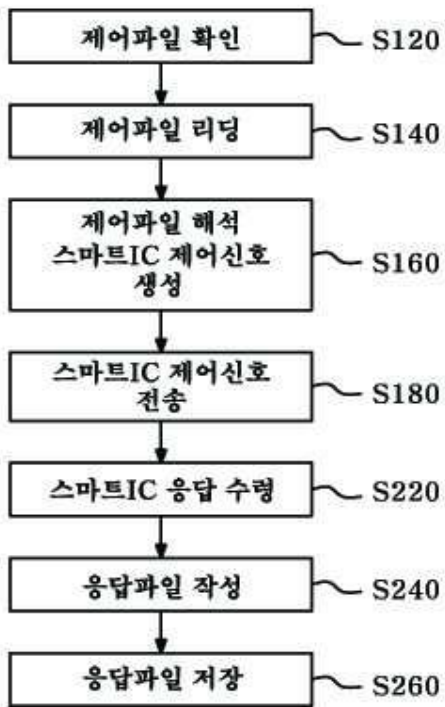
도면1



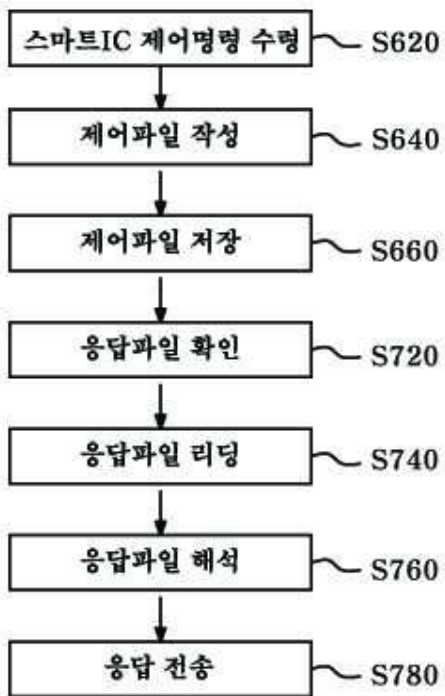
도면2



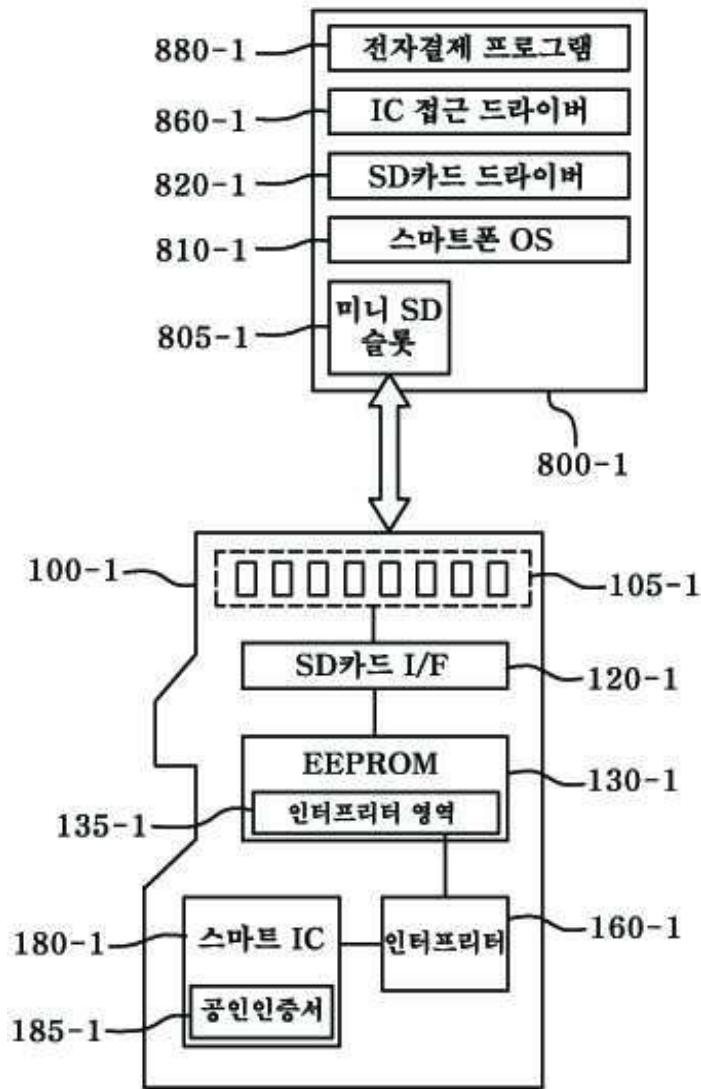
도면3



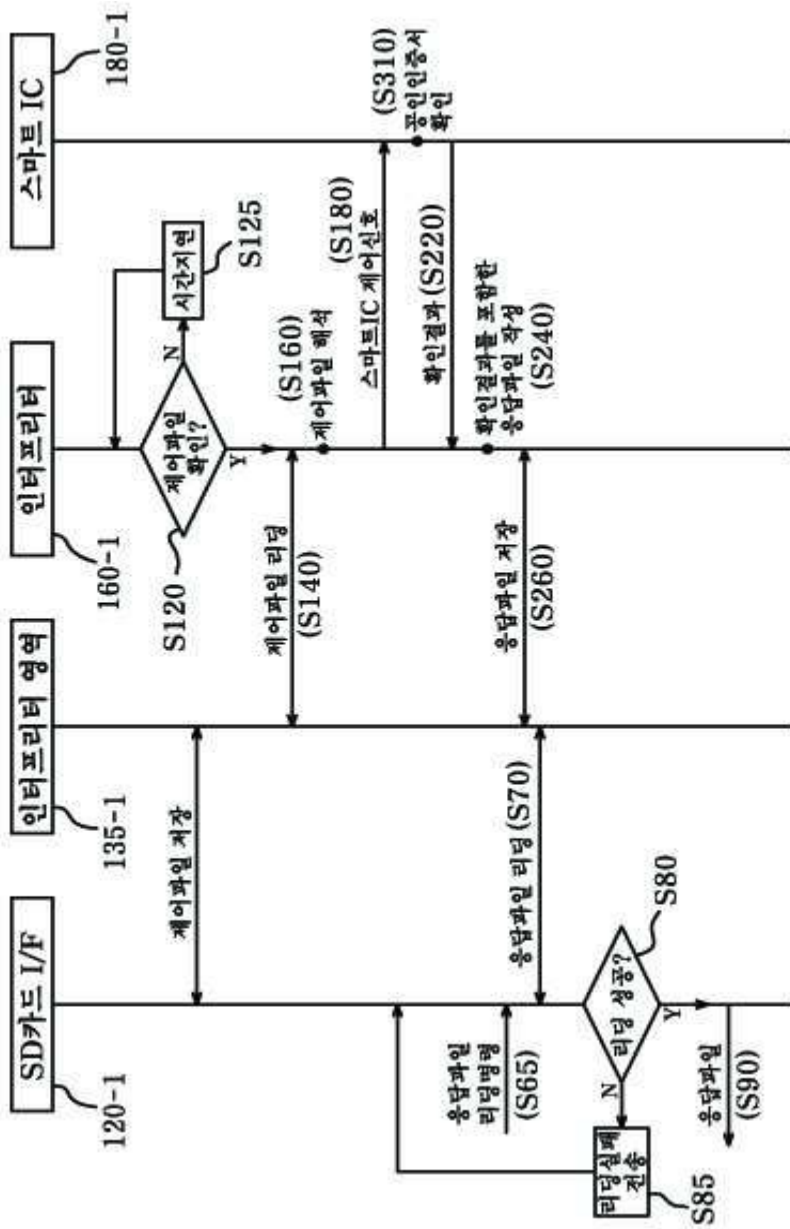
도면4



도면5



도면6



도면7

