(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0035518
(43) 공개일자 2009년04월09일

(51) Int. Cl.
G06F 9/06 (2006.01) *G06F 12/14* (2006.01)
G06K 19/073 (2006.01)
(21) 출원번호 10-2009-7000702
(22) 출원일자 2009년01월13일
심사청구일자 없음
번역문제출일자 2009년01월13일
(86) 국제출원번호 PCT/US2007/015706
국제출원일자 2007년07월10일
(87) 국제공개번호 WO 2008/008321
국제공개일자 2008년01월17일
(30) 우선권주장
11/486,578 2006년07월14일 미국(US)

(71) 출원인
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
미소레, 시바람 에이치.
미국 98052-6399 워싱턴주 레드몬드 원 마이크로소프트 웨이 마이크로소프트 코포레이션 국제특허부
(74) 대리인
양영준, 백만기

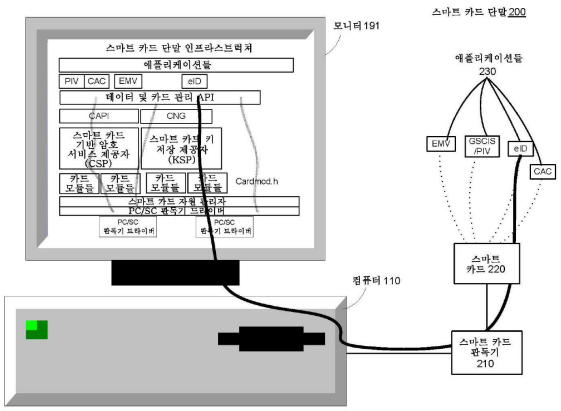
전체 청구항 수 : 총 20 항

(54) 스마트 카드 단말 인프라스트럭쳐, 스마트 카드 단말 애플리케이션과 스마트 카드 애플리케이션 간의 상호 운용 방법 및 스마트 카드의 보안 모델 적용 방법

(57) 요 약

스마트 카드 단말의 데이터 및 관리 프레임워크는 스마트 카드 단말과 스마트 카드 간, 특히 단말과 카드의 애플리케이션들 간의 상호 운용을 제공하도록 기능한다. API(application program interface)는 데이터 및 관리 프레임워크에 기록되며, 데이터 및 관리 프레임워크는 스마트 카드 단말에 의해 스마트 카드에 포함된 스마트 카드 애플리케이션에 액세스하고 이를 처리하는 스마트 카드 단말 인프라스트럭쳐의 일부이다. API는, 대응하는 단말 애플리케이션이 2개의 애플리케이션들 간의 통신을 위한 정보를 통합할 수 있도록 스마트 카드 애플리케이션과 관련된 정보를 단말에 제공한다. 추가적으로, 스마트 카드와 관련된 보안 모델 및 정책들이 스마트 카드 단말에 의해 적용될 수 있다.

대 표 도



특허청구의 범위

청구항 1

스마트 카드 단말(200)에 대한 스마트 카드 단말 인프라스트럭쳐(300)로서,

데이터 및 관리 프레임워크(310)를 포함하고, 상기 프레임워크(310)는,

스마트 카드(220) 상의 스마트 카드 애플리케이션(230)과 관련된 정보를 획득하기 위한 인터페이스 컴포넌트(410);

상기 스마트 카드(220)의 에러를 검출하기 위한 에러 상태 관리 컴포넌트(420);

상기 스마트 카드(220)와 관련된 사용 정책을 적용(enforcing)하기 위한 사용 관리 컴포넌트(430); 및

상기 스마트 카드(220)와 상기 스마트 카드 단말(200) 간에 통신하기 위한 통신 컴포넌트(440)

를 포함하는 스마트 카드 단말 인프라스트럭쳐.

청구항 2

제1항에 있어서,

상기 데이터 및 관리 프레임워크(310)는 API(application program interface)인 스마트 카드 단말 인프라스트럭쳐.

청구항 3

제1항에 있어서,

상기 스마트 카드(220) 상의 상기 스마트 카드 애플리케이션(230)과 관련된 상기 정보는, (ⅰ) 상기 스마트 카드 애플리케이션(230)의 인터페이스; (ii) 상기 스마트 카드 애플리케이션(230)에 의해 사용되는 프로토콜; 및 (iii) 상기 스마트 카드(220)의 보안 모델 중 적어도 하나인 스마트 카드 단말 인프라스트럭쳐.

청구항 4

제1항에 있어서,

상기 스마트 카드(220) 상의 상기 스마트 카드 애플리케이션(230)과 관련된 정보를 상기 데이터 및 관리 프레임워크(310)에 제공하기 위한 카드 모듈(340)을 더 포함하는 스마트 카드 단말 인프라스트럭쳐.

청구항 5

제4항에 있어서,

상기 스마트 카드 애플리케이션(230)에 대응하고 상기 스마트 카드(220) 상의 상기 스마트 카드 애플리케이션(230)과 관련된 상기 정보로부터 생성되는 단말 애플리케이션(305)을 더 포함하는 스마트 카드 단말 인프라스트럭쳐.

청구항 6

제1항에 있어서,

상기 에러 상태 관리 컴포넌트(420)는 상기 에러의 검출 시에 에러 메시지를 상기 통신 컴포넌트(440)에 중계하도록 추가적으로 동작하는 스마트 카드 단말 인프라스트럭쳐.

청구항 7

제6항에 있어서,

상기 통신 컴포넌트(440)는, (ⅰ) 디스플레이 장치(191) 상에 상기 에러 메시지를 디스플레이하는 것; (ii) 상기 에러 메시지에 대응하는 로그 엔트리를 생성하는 것; 및 (iii) 애플리케이션으로 상기 에러 메시지를 송신하

는 것 중 적어도 하나에 의해 상기 스마트 카드 단말(200)의 상기 에러 메시지를 중계하는 스마트 카드 단말 인프라스트럭쳐.

청구항 8

제1항에 있어서,

상기 사용 관리 컴포넌트(430)는 상기 스마트 카드(220)와 관련된 사용 정책의 위반의 검출 시에 사용 정보를 상기 통신 컴포넌트(440)에 중계하도록 추가적으로 동작하는 스마트 카드 단말 인프라스트럭쳐.

청구항 9

제8항에 있어서,

상기 통신 컴포넌트(440)는, (ⅰ) 디스플레이 장치(191) 상에 상기 위반의 표시(indication)를 디스플레이하는 것; (ii) 상기 위반에 대응하는 로그 엔트리를 생성하는 것; 및 (iii) 애플리케이션으로 상기 위반의 표시를 송신하는 것 중 적어도 하나에 의해 상기 스마트 카드(220)와 관련된 사용 정책의 위반의 표시를 중계하는 스마트 카드 단말 인프라스트럭쳐.

청구항 10

제1항에 있어서,

상기 데이터 및 관리 프레임워크(310)는,

에러가 검출되지 않거나 사용 정책이 적용된다면 상기 스마트 카드 애플리케이션(230)과 대응하는 단말 애플리케이션(305) 간의 채널을 생성하기 위한 접속 컴포넌트(450)를 더 포함하는 스마트 카드 단말 인프라스트럭쳐.

청구항 11

제1항에 있어서,

상기 데이터 및 관리 프레임워크(310)는,

상기 스마트 카드 애플리케이션(230)의 처리와 관련된 단말 정책들 또는 제약들을 통합시키기 위한 단말 정책 컴포넌트(460)를 더 포함하는 스마트 카드 단말 인프라스트럭쳐.

청구항 12

스마트 카드 단말 애플리케이션(305)과 스마트 카드(220) 상의 스마트 카드 애플리케이션(230) 간의 상호 운용(interoperability) 방법으로서,

스마트 카드 단말의 프레임워크에 기록된 API를 획득하는 단계(505);

상기 API로부터 상기 스마트 카드 애플리케이션과 관련된 정보를 획득하는 단계(510); 및

상기 스마트 카드 애플리케이션과 관련된 상기 정보를 상기 스마트 카드 단말 애플리케이션으로 통합시키는 단계(515)

를 포함하는 상호 운용 방법.

청구항 13

제12항에 있어서,

상기 API로부터 상기 스마트 카드 애플리케이션과 관련된 정보를 획득하는 단계(510)는,

(ⅰ) 상기 스마트 카드 애플리케이션의 인터페이스; (ii) 상기 스마트 카드 애플리케이션에 의해 사용되는 프로토콜; 및 (iii) 상기 스마트 카드의 보안 모델 중 적어도 하나를 획득하는 단계를 포함하는 상호 운용 방법.

청구항 14

제12항에 있어서,

상기 스마트 카드 단말에서 상기 스마트 카드의 보안 모델을 적용하는 단계(520)를 더 포함하는 상호 운용 방법.

청구항 15

제14항에 있어서,

상기 스마트 카드의 보안 모델을 적용하는 단계(520)는,

상기 스마트 카드의 사용을 감시하는 단계(525); 및

감시된 사용이 상기 보안 모델을 위반했다고 판정할 시에(530), 위반 메시지를 표시하는 단계(535)

를 포함하는 상호 운용 방법.

청구항 16

제12항에 있어서,

상기 스마트 카드와 상기 스마트 카드 단말 간의 보안 통신 채널을 생성하는 단계(540)를 더 포함하는 상호 운용 방법.

청구항 17

제12항에 있어서,

단말 정책 또는 제약을 추가적으로 규정하도록 상기 스마트 카드 단말 애플리케이션을 구성하는 단계(545)를 더 포함하는 상호 운용 방법.

청구항 18

스마트 카드의 보안 모델을 스마트 카드 단말에 적용하는 방법으로서,

상기 스마트 카드 단말의 데이터 및 관리 프레임워크로부터 상기 스마트 카드의 보안 모델을 획득하는 단계(610); 및

상기 스마트 카드에 대응하는 스마트 카드 단말 애플리케이션으로 상기 보안 모델을 통합시키는 단계(615)

를 포함하는, 스마트 카드의 보안 모델 적용 방법.

청구항 19

제18항에 있어서,

상기 스마트 카드 단말의 데이터 및 관리 프레임워크로부터 상기 스마트 카드의 보안 모델을 획득하는 단계는,

상기 데이터 및 관리 프레임워크에 적용된 API를 판독하는 단계를 포함하는, 스마트 카드의 보안 모델 적용 방법.

청구항 20

제18항에 있어서,

상기 보안 모델에 의해 규정된 에러 상태를 검출하는 단계(620); 및

상기 에러 상태의 검출 시에 상기 에러 상태에 대응하는 에러 메시지를 전송하는 단계(625)를 더 포함하는, 스마트 카드의 보안 모델 적용 방법.

명 세 서

배 경 기 술

<1> 스마트 카드란 컴퓨터와 유사하게 데이터를 저장, 처리, 수신 및 전달하기 위한 메모리 및 프로세서를 포함하는 전자 카드이다. 스마트 카드의 작은 사이즈 외에도, 스마트 카드들은 내탬퍼성(tamper-resistant)을 가지며,

보안 모델을 사용하여 민감하고 개인적인 데이터가 안전하게 운반되고 저장될 수 있게 하므로, 더욱 바람직하다. 따라서, 스마트 카드들은 식별 목적, 금융 거래 및 보안 액세스 애플리케이션에 대해 종종 이용된다. 또한, 데이터의 안전한 관리 및 저장을 필요로 하거나 그에 의해 향상될 수 있는 기타 애플리케이션들도 스마트 카드들을 사용할 수 있다.

<2> 스마트 카드 단말은 스마트 카드에 포함된 데이터를 수용하고 판독함으로써 스마트 카드에 저장된 애플리케이션들에 액세스하는 디바이스이다. 예를 들어, 금융 스마트 카드 단말에서의 화폐 스마트 카드의 사용은 스마트 카드의 사용자의 계좌로 금전이 전송될 수 있게 하고, 시설에 위치된 스마트 카드 단말에 삽입된 식별 스마트 카드는 식별 스마트 카드의 사용자에 대해 시설로의 액세스를 제공할 수 있다.

<3> 현재, 하나 이상의 애플리케이션을 포함하는 스마트 카드에 대해, 단말에서 스마트 카드 애플리케이션를 발견하는 데 어려움이 있다. 그 단말은 스마트 카드 애플리케이션들에 의해 제공되는 인터페이스 및 스마트 카드 애플리케이션들에 의해 이용되는 프로토콜을 인지하지 못할 수 있다. 발견의 문제점은 단말기 측에서의 애플리케이션의 생성(production)에 어려움을 일으킨다. 또한, 스마트 카드의 보안 모델은 단말에서 적용(enforcing)되지 않는다. 따라서, 단말에서 스마트 카드의 보안 모델을 적용하면서, 추가적으로 단말로 하여금 스마트 카드의 애플리케이션을 실행하는 데 필요한 관련 정보를 획득할 수 있게 하는 특징은 매우 바람직하다. 스마트 카드 및 스마트 카드 단말에 대한 추가적인 바람직한 개선사항은 에러 및 사용 관리 제어를 포함한다.

발명의 상세한 설명

<4> [개요]

<5> 스마트 카드와 스마트 카드의 애플리케이션에 액세스하는 스마트 카드 단말 간의 상호 운용(interoperability)이 데이터 및 관리 프레임워크(data and management framework)에 의해 제공된다. API(application program interface)는 스마트 카드 단말 인프라스트럭처의 일부인 데이터 및 관리 프레임워크에 기록될 수 있다. 스마트 카드 단말 인프라스트럭처는 스마트 카드에 포함된 스마트 카드 애플리케이션에 액세스하고 이를 처리하고 실행한다. API는 대응하는 단말 애플리케이션이 개발(developing)될 수 있도록 스마트 카드 애플리케이션과 관련된 필요한 정보를 단말에 제공한다. 그러면, 대응하는 단말 애플리케이션은 단말과 스마트 카드 애플리케이션들 간의 상호 운용, 발견 및 보안을 위해 정보를 통합할 수 있다. 스마트 카드와 관련된 보안 모델 및 정책들은 스마트 카드 단말에 의해 적용될 수 있다.

<6> 본 개요는 상세한 설명에서 추가적으로 설명될 개념들의 선택을 단순화된 양식으로 소개하고자 제공된다. 예시적인 실시예들이 도면에서 도시되지만, 이러한 실시예들은 도면에 도시된 특정 방법 및 수단에 제한되지 않는다.

<7> 상술한 개요 및 이하의 상세한 설명은 첨부된 도면과 연계하여 읽을 때 더욱 잘 이해된다. 예시적인 실시예들이 도면에 도시되었지만, 이러한 실시예들은 도면에 도시된 구체적인 방법들 및 수단들에 제한되지 않는다는 것을 이해할 것이다.

실 시 예

<14> 도 1과 관련하여, 본 발명을 구현하는 예시적인 시스템은 컴퓨터(110) 형태의 범용 컴퓨팅 장치를 포함한다. 컴퓨터(110)의 컴포넌트들은 처리 장치(120), 시스템 메모리(130), 및 시스템 메모리를 비롯한 각종 시스템 컴포넌트들을 처리 장치(120)에 연결시키는 시스템 버스(121)를 포함하지만 이에 제한되는 것은 아니다. 시스템 버스(121)는 메모리 버스 또는 메모리 컨트롤러, 주변 장치 버스 및 각종 버스 아키텍처 중 임의의 것을 이용하는 로컬 버스를 비롯한 몇몇 유형의 버스 구조 중 어느 것이라도 될 수 있다. 예로서, 이러한 아키텍처는 ISA(industry standard architecture) 버스, MCA(micro channel architecture) 버스, EISA(Enhanced ISA) 버스, VESA(video electronics standard association) 로컬 버스, 그리고 (메자닌 버스(mezzanine bus)로도 알려진) PCI(peripheral component interconnect) 버스 등을 포함하지만 이에 제한되는 것은 아니다.

<15> 컴퓨터(110)는 통상적으로 각종 컴퓨터 판독가능 매체를 포함한다. 컴퓨터(110)에 의해 액세스 가능한 매체는 그 어떤 것이든지 컴퓨터 판독가능 매체가 될 수 있고, 이러한 컴퓨터 판독가능 매체는 휘발성 및 비휘발성 매체, 이동식 및 비이동식 매체를 포함한다. 예로서, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 포함하지만 이에 제한되는 것은 아니다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보를 저장하는 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성, 이동식 및 비이동식 매체를 포함한다. 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술,

CD-ROM, DVD(digital versatile disk) 또는 기타 광 디스크 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 또는 컴퓨터(110)에 의해 액세스되고 원하는 정보를 저장하는 데 이용될 수 있는 임의의 기타 매체를 포함하지만 이에 제한되는 것은 아니다. 통신 매체는 통상적으로 반송파(carrier wave) 또는 기타 전송 메커니즘(transport mechanism)과 같은 피변조 데이터 신호(modulated data signal)에 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터 등을 구현하고 모든 정보 전달 매체를 포함한다. "피변조 데이터 신호"라는 용어는, 신호 내에 정보를 인코딩하도록 그 신호의 특성들 중 하나 이상을 설정 또는 변경시킨 신호를 의미한다. 예로서, 통신 매체는 유선 네트워크 또는 직접 배선 접속(direct-wired connection)과 같은 유선 매체, 그리고 음향, RF, 적외선, 기타 무선 매체와 같은 무선 매체를 포함한다. 상술된 매체들의 모든 조합이 또한 컴퓨터 판독가능 매체의 영역 안에 포함되는 것으로 한다.

<16> 시스템 메모리(130)는 판독 전용 메모리(ROM)(131) 및 랜덤 액세스 메모리(RAM)(132)와 같은 휘발성 및/또는 비휘발성 메모리 형태의 컴퓨터 저장 매체를 포함한다. 시동 중과 같은 때에, 컴퓨터(110) 내의 구성요소들 사이의 정보 전송을 돕는 기본 루틴을 포함하는 기본 입/출력 시스템(BIOS)(133)은 통상적으로 ROM(131)에 저장되어 있다. RAM(132)은 통상적으로 처리 장치(120)가 즉시 액세스 할 수 있고 및/또는 현재 동작시키고 있는 데이터 및/또는 프로그램 모듈을 포함한다. 예로서, 도 1은 운영 체제(134), 애플리케이션 프로그램(135), 기타 프로그램 모듈(136) 및 프로그램 데이터(137)를 도시하고 있지만 이에 제한되는 것은 아니다.

<17> 컴퓨터(110)는 또한 기타 이동식/비이동식, 휘발성/비휘발성 컴퓨터 저장매체를 포함한다. 단지 예로서, 도 1은 비이동식·비휘발성 자기 매체에 기록을 하거나 그로부터 판독을 하는 하드 디스크 드라이브(141), 이동식·비휘발성 자기 디스크(152)에 기록을 하거나 그로부터 판독을 하는 자기 디스크 드라이브(151), CD-ROM 또는 기타 광 매체 등의 이동식·비휘발성 광 디스크(156)에 기록을 하거나 그로부터 판독을 하는 광 디스크 드라이브(155)를 포함한다. 예시적인 운영 환경에서 사용될 수 있는 기타 이동식/비이동식, 휘발성/비휘발성 컴퓨터 저장 매체로는 자기 테이프 카세트, 플래시 메모리 카드, DVD, 디지털 비디오 테이프, 고상(solid state) RAM, 고상 ROM 등이 있지만 이에 제한되는 것은 아니다. 하드 디스크 드라이브(141)는 통상적으로 인터페이스(140)와 같은 비이동식 메모리 인터페이스를 통해 시스템 버스(121)에 접속되고, 자기 디스크 드라이브(151) 및 광 디스크 드라이브(155)는 통상적으로 인터페이스(150)와 같은 이동식 메모리 인터페이스에 의해 시스템 버스(121)에 접속된다.

<18> 위에서 설명되고 도 1에 도시된 드라이브들 및 이들과 관련된 컴퓨터 저장 매체는, 컴퓨터(110)를 위해, 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 및 기타 데이터를 저장한다. 도 1에서, 예를 들어, 하드 디스크 드라이브(141)는 운영 체제(144), 애플리케이션 프로그램(145), 기타 프로그램 모듈(146), 및 프로그램 데이터(147)를 저장하는 것으로 도시되어 있다. 여기서 주의할 점은 이들 컴포넌트가 운영 체제(134), 애플리케이션 프로그램(135), 기타 프로그램 모듈(136), 및 프로그램 데이터(137)와 동일하거나 그와 다를 수 있다는 것이다. 이에 관해, 운영 체제(144), 애플리케이션 프로그램(145), 기타 프로그램 모듈(146) 및 프로그램 데이터(147)에 다른 번호가 부여되어 있다는 것은 적어도 이들이 다른 사본(copy)이라는 것을 나타내기 위한 것이다. 사용자는 키보드(162), 마우스, 트랙볼(trackball) 또는 터치 패드와 같은 포인팅 장치(161) 등의 입력 장치를 통해 명령 및 정보를 컴퓨터(110)에 입력할 수 있다. 다른 입력 장치(도시 생략)로는 마이크, 조이스틱, 게임 패드, 위성 안테나, 스캐너 등을 포함할 수 있다. 이들 및 기타 입력 장치는 종종 시스템 버스에 결합된 사용자 입력 인터페이스(160)를 통해 처리 장치(120)에 접속되지만, 병렬 포트, 게임 포트 또는 USB(universal serial bus) 등의 다른 인터페이스 및 버스 구조에 의해 접속될 수도 있다. 모니터(191) 또는 다른 유형의 디스플레이 장치도 비디오 인터페이스(190) 등의 인터페이스를 통해 시스템 버스(121)에 접속될 수 있다. 모니터 외에, 컴퓨터는 스피커(197) 및 프린터(196) 등의 기타 주변 출력 장치를 포함할 수 있고, 이들은 출력 주변장치 인터페이스(195)를 통해 접속될 수 있다.

<19> 컴퓨터(110)는 원격 컴퓨터(180)와 같은 하나 이상의 원격 컴퓨터로의 논리적 접속을 사용하여 네트워크화된 환경에서 동작할 수 있다. 원격 컴퓨터(180)는 또 하나의 퍼스널 컴퓨터, 서버, 라우터, 네트워크 PC, 피어 장치 또는 기타 통상의 네트워크 노드일 수 있고, 통상적으로 컴퓨터(110)와 관련하여 상술된 구성요소들의 대부분 또는 그 전부를 포함하지만, 단지 메모리 저장 장치(181)만이 도 1에 도시되어 있다. 도시된 논리적 접속으로는 LAN(171) 및 WAN(173)이 있지만, 기타 네트워크를 포함할 수도 있다. 이러한 네트워킹 환경은 사무실, 전사적 컴퓨터 네트워크(enterprise-wide computer network), 인트라넷, 및 인터넷에서 일반적인 것이다.

<20> LAN 네트워킹 환경에서 사용될 때, 컴퓨터(110)는 네트워크 인터페이스 또는 어댑터(170)를 통해 LAN(171)에 접속된다. WAN 네트워킹 환경에서 사용될 때, 컴퓨터(110)는 통상적으로 인터넷과 같은 WAN(173)을 통해 통신을 설정하기 위한 모뎀(172) 또는 기타 수단을 포함한다. 내장형 또는 외장형일 수 있는 모뎀(172)은 사용자 입력

인터페이스(160) 또는 기타 적절한 메커니즘을 통해 시스템 버스(121)에 접속된다. 네트워크화된 환경에서, 컴퓨터(110) 또는 그의 일부와 관련하여 기술된 프로그램 모듈은 원격 메모리 저장 장치에 저장될 수 있다. 예로서, 도 1은 원격 애플리케이션 프로그램(185)이 메모리 장치(181)에 있는 것으로 도시하고 있지만 이에 제한되는 것은 아니다. 도시된 네트워크 접속은 예시적인 것이며 이 컴퓨터들 사이에 통신 링크를 설정하는 기타 수단이 사용될 수 있다는 것을 이해할 것이다.

<21> 본 명세서에서 설명된 방법들의 전부 또는 일부는 하드웨어, 소프트웨어 또는 그 둘의 결합으로 구현될 수 있다. 소프트웨어로 구현된 경우에, 방법들 또는 그 특정한 양태들 또는 부분들은 컴퓨팅 시스템에 의해 실행되는 경우에, 컴퓨팅 시스템으로 하여금 그 방법들을 수행하게 하는 프로그램 코드의 형식으로 구현될 수 있다. 이러한 프로그램 코드는 앞서 규정된 용어와 같은 임의의 컴퓨터 판독가능 매체에 저장될 수 있다.

<22> 스마트 카드 단말은 메모리 및 프로세서를 포함하는 소형 전자 카드인 스마트 카드에 저장된 애플리케이션에 액세스하고 이를 처리하는 장치이다. 스마트 카드는 컴퓨터와 유사할 수 있으며, 데이터를 저장하고, 처리하고 수신하고 전송하도록 기능한다. 스마트 카드는 스마트 카드 단말에 의한 처리를 위해 액세스될 수 있는 하나 이상의 애플리케이션을 포함할 수 있다.

<23> 예시적인 스마트 카드 단말(200)이 도 2에 도시되어 있다. 스마트 카드 단말(200)은 컴퓨터(110)와 같은 컴퓨터, 모니터(191) 또는 기타 유형의 디스플레이 장치 및 스마트 카드 판독기(210)를 포함할 수 있다. 스마트 카드 판독기(210)는 도 2에 도시된 스마트 카드(220)와 같은 스마트 카드와 컴퓨터(110) 사이의 인터페이스로서 동작하여, 컴퓨터(110)로 하여금 스마트 카드(220)의 애플리케이션들(230)에 액세스하고 이들을 처리할 수 있게 한다.

<24> 스마트 카드 판독기(210)는 근접형(proximity) 또는 무접촉형 스마트 카드 판독기(210)일 수 있으며, 스마트 카드(220)는 판독기(210)와 카드(220) 간의 어떠한 직접적인 접촉 없이도 스마트 카드 판독기(210)에 의해 판독된다. 예를 들어, 근접형 스마트 카드 판독기(210)는, 스마트 카드(220)가 근접형 스마트 카드 판독기(210)의 부근에 유지되거나 위치될 때 스마트 카드(220)에 액세스할 수 있다. 일 실시예에서, 표준 ISO 14443은 표준 ISO 14443을 준수하는 기타 카드들(220) 및 판독기들(210)과의 호환성을 위해 근접형 스마트 카드(220) 및 근접형 스마트 카드 판독기(210)를 규정하는 데 사용될 수 있다. 표준에 따르면, 근접형 스마트 카드 판독기(210)는 스마트 카드(220)를 판독하기 위하여 매립된 마이크로컨트롤러 및 자기 루프 안테나를 포함하는 무선 주파수 식별(RFID: radio frequency identification) 판독기이다. 자기 루프 안테나는 13.56 MHz의 무선 주파수에서 동작한다. 근접형 스마트 카드 판독기(210)는, 카드(220)가 판독기(210)의 4 인치 내에 있다면 근접형 스마트 카드(220)를 판독할 수 있다. 또한, 표준 ISO 14443은 (ⅰ) 물리적 특성; (ⅱ) 무선 주파수 전력 및 신호 인터페이스; (ⅲ) 초기치 설정 및 충돌방지(anti-collision); 및 (ⅳ) 전송 프로토콜의 4개 파트를 포함한다.

<25> 대안적으로, 스마트 카드 판독기(210)는 삽입가능형(insert-able) 스마트 카드 판독기(210)일 수 있다. 스마트 카드 판독기(210)가 삽입가능형이면, 스마트 카드(220)의 애플리케이션들(230)에의 액세스는, 스마트 카드(220) 또는 스마트 카드(220)의 일부가 삽입가능형 스마트 카드 판독기(210)에 삽입될 때 허가된다. ISO 7816은 삽입가능형 스마트 카드(220)와 같은 접촉형 스마트 카드들을 설명하는 확립된 표준이다. 삽입가능형 스마트 카드(220)는 표준 ISO 7816의 요건에 따라 설계될 수 있는데, 표준 ISO 7816은 카드(220)와 판독기(210) 간에 전송되는 메시지들, 커맨드들 및 응답들의 내용과 관련된 기준; 카드(220) 내의 파일들 및 데이터에 대한 액세스 방법들; 및 보안 메시징을 위한 방법들을 포함한다. 스마트 카드 판독기(210)의 기타 유형이 사용될 수 있으며, 근접형 스마트 카드 판독기(210) 또는 삽입가능형 카드 판독기(210)에 제한은 없다.

<26> 스마트 카드(220)는 하나 또는 그 이상의 애플리케이션(230)을 포함할 수 있다. 예를 들어, 도 2에 도시된 바와 같이, 스마트 카드(220)는 EMV(Europay MasterCard Visa), GSCIS/PIV, eID 및 CAC의 4개의 애플리케이션들(230)을 포함한다. 기타 애플리케이션들(230) 및 다른 개수의 애플리케이션들(230)이 가능하다. 또한, 스마트 카드(220)는 관련되지 않은 애플리케이션들(230)을 포함할 수 있으며/있거나 그 대신에 애플리케이션(230)의 몇몇 변형물을 포함할 수도 있다. 애플리케이션들(230)의 임의의 조합이 스마트 카드(220)에 포함될 수 있다.

<27> 일 실시예에 따른 스마트 카드 인프라스트럭처(300)가 도 3에 도시되어 있다. 스마트 카드 단말 인프라스트럭처(300)는 스마트 카드(220)의 애플리케이션들(230)에 액세스하고, 이들을 처리하고 구현하도록 동작한다. 또한, 인프라스트럭처(300)는 에러 상태(error condition) 및 사용 모델(usage model)의 관리를 허용한다.

<28> 스마트 카드 단말 인프라스트럭처(300)는 단말 애플리케이션들(305); 데이터 및 관리 프레임워크(310); 암호 보안 컴포넌트(320); 추가적인 암호 보안 컴포넌트(325); 스마트 카드 기반 암호 서버 제공자(330); 스마트 카드

키 저장 제공자(335); (도시된 카드 모듈(340a 내지 340d)과 같은) 하나 이상의 카드 모듈(340); 스마트 카드 자원 관리자(345); PC/SC -윈즈카드.h(winscard.h)(350); 및 (판독기 드라이버(355a 및 355b)와 같은) 하나 이상의 판독기 드라이버를 포함하여, 기능들을 수행하기 위한 몇개의 수단들, 장치들, 소프트웨어 및/또는 하드웨어를 포함할 수 있다.

<29> 암호 보안 컴포넌트(320)는 개발자들로 하여금 단말 애플리케이션(305)과 같은 애플리케이션들에 암호 보안을 추가할 수 있게 한다. 암호 보안 컴포넌트들(320)은 예를 들어 인터넷과 같은 비보안 매체 상의 보안 환경에서 문서들 및 기타 데이터의 생성 및 교환을 허용한다. 추가적인 암호 보안 컴포넌트(325)는 암호 보안 컴포넌트(320)와 유사하지만 향상된 기능성을 제공할 수도 있다. 예시적이고 제한적이지 않은 실시예에서, 암호 보안 컴포넌트(320)는 CryptoAPI일 수 있다. 추가적인 예시적이고 제한적이지 않은 실시예에서, 암호 보안 컴포넌트(325)는 CNG 또는 차세대 CryptoAPI일 수도 있다.

<30> 스마트 카드 기반 암호 서버 제공자(330)는 스마트 카드 모듈들(340)을 통해 스마트 카드(220)와 같은 개별 스마트 카드들과 통신하도록 동작할 수 있다. 스마트 카드 기반 암호 서버 제공자(330)는 암호 표준들 및 알고리즘들의 구현체를 포함할 수 있어 암호 보안을 보장한다. 스마트 카드 기반 암호 서버 제공자(330)는 DLL(dynamic link library)을 포함할 수 있으며, DLL은 기능들을 구현할 수 있으며, 운영 시스템과 스마트 카드 기반 암호 서버 제공자(330) 간의 통신의 보조자(facilitator)로서의 역할을 할 수 있다.

<31> 스마트 카드 모듈들(340)은 스마트 카드 자원 관리자(345)를 통한 스마트 카드와의 통신에 의해 특정 스마트 카드들의 특성들을 스마트 카드 단말 인터페이스 인프라스트럭처(300)를 위한 균일한 인터페이스로 변환하도록 기능할 수 있다. 스마트 카드 모듈(340)은 DLL로서 구현될 수 있다. 스마트 카드 키 저장 제공자(335)는 스마트 카드 단말 데이터 인프라스트럭처(300)에 의해 요구되는 키 저장 동작들을 수행하도록 기능한다.

<32> 스마트 카드 자원 관리자(345)는 스마트 카드 판독기들(210)로의, 그리고 스마트 카드들(220)로의 액세스를 관리하는 직무를 담당할 수 있다. 몇몇 수행되는 기능들은 자원들의 식별 및 추적; 복수의 애플리케이션들에 대한 판독기들 및 자원들의 할당; 및 소정의 스마트 카드(220)에서 이용가능한 서비스들에 액세스하기 위한 트랜잭션 프리미티브들(transaction primitives)의 지원을 포함할 수 있다. 스마트 카드 자원 관리자(345)는 자원 관리자 API를 통해 직접 액세스될 수 있거나 스마트 카드 서비스 제공자를 통해 간접적으로 액세스될 수도 있다. 자원 관리자 API는 스마트 카드 자원 관리자(345)의 서비스들로의 직접적인 액세스를 제공하는 함수들의 집합이다.

<33> 스마트 카드 단말 인프라스트럭처(300)의 데이터 및 관리 프레임워크(310)는 단말 애플리케이션들(305)의 개발 및 생성에서 지원하도록 기능한다. 단말 애플리케이션들(305)은 스마트 카드 애플리케이션들(230)에 대응한다. 또한, 데이터 및 관리 프레임워크(310)는 스마트 카드 단말(200)과 스마트 카드(220) 간의 통신을 위해 사용 모델 뿐만 아니라 에러 상태도 관리한다. 추가적으로, 데이터 및 관리 프레임워크(310)는 API일 수 있으며, 일 실시예에서는 단말 애플리케이션들(305)로의 에러 메시지들의 전파를 담당할 수도 있다. 일 실시예에 따른 데이터 및 관리 프레임워크(310)가 도 4에 도시되어 있다.

<34> 예시적인 데이터 및 관리 프레임워크(310)는 인터페이스 컴포넌트(410), 에러 상태 관리 컴포넌트(420), 사용 관리 컴포넌트(430), 통신 컴포넌트(440), 접속 컴포넌트(450) 및 단말 정책 컴포넌트(460)를 포함하여, 기능들을 수행하기 위한 몇몇 수단들, 장치들, 소프트웨어 및/또는 하드웨어를 포함한다.

<35> 인터페이스 컴포넌트(410)는 스마트 카드 애플리케이션(230)과 관련된 정보를 획득함으로써 스마트 카드 단말(200)로부터 스마트 카드 애플리케이션(230)으로의 링크로서 기능한다. 애플리케이션(230)과 관련된 정보는 스마트 카드(220)의 애플리케이션(230)을 적절하게 식별하고 액세스하는 데 있어 단말(200)을 지원할 수 있는, 애플리케이션(230)의 인터페이스 및/또는 프로토콜을 포함할 수 있다. 또한, 이러한 정보는 단말(200)로 하여금 정책의 존재와 요건들을 인식하게 함으로써 스마트 카드(220)의 정책을 적용하는 데도 이용될 수 있다.

<36> 스마트 카드 애플리케이션(230)에 대응하는 대응 API는 예컨대 스마트 카드 애플리케이션(230)의 판매자 또는 개발자에 의해 생성될 수 있으며, 대응 API는 판매자 또는 개발자에 의해 데이터 및 관리 프레임워크(310)에 기록될 수 있다. 인터페이스 컴포넌트(410)는 이러한 대응 API를 사용하여 스마트 카드 애플리케이션(230)에 대응하는 단말 애플리케이션(305)을 생성할 수 있다.

<37> 에러 상태 관리 컴포넌트는 스마트 카드(220)의 사용과 관련된 에러를 검출하고, 이러한 에러의 검출시에 대응하는 에러 메시지를 중계하도록 기능한다. 에러 메시지는 통신 컴포넌트(440)로 중계될 수 있다. 스마트 카드(220)의 스마트 카드 애플리케이션(230)에 액세스하려는 스마트 카드 단말(200)에 의한 시도로부터 각종 에러들

이 발생한다. 예를 들어, 카드(220)가 스마트 카드 단말 판독기(210)에 부적절하게 삽입될 수 있다. 이러한 에러가 에러 상태 관리 컴포넌트(420)에 의해 검출되면, 이에 따라 그 에러는 통신 컴포넌트(440)에 중계된다. 스마트 카드 단말(200)이 스마트 카드(220) 상에 있지 않은 애플리케이션(230)을 판독하려고 시도하는 경우에 또 다른 에러가 발생할 수 있다. 다시, 에러 상태 관리 컴포넌트(420)는 이러한 에러를 검출할 수 있고, 그렇다면 이 에러의 검출 시에 적절한 에러 메시지를 통신 컴포넌트(440)에 중계하도록 동작할 수 있다.

<38> 사용 관리 컴포넌트(430)는 스마트 카드(220)와 관련된 사용 정책을 적용할 수 있다. 일 실시예에서, 사용 정책은 스마트 카드(220)에 대한 보안 모델이다. 사용 정책은 스마트 카드 애플리케이션과 관련된 정보에 포함될 수 있고, 따라서 데이터 및 관리 프레임워크(310)에 기록된 대응 API에서 통합될 수도 있다. 사용 정책은 예컨대 그룹 정책 설정, 로컬 머신 정책 설정 또는 애플리케이션 정책 설정에 따를 수 있다. 사용 정책은 사용 정책을 획득할 수 있고 스마트 카드(220) 및 그 애플리케이션들(230)의 사용을 감시할 수 있는 사용 관리 컴포넌트(430)에 의해 적용될 수 있다. 규정된 사용 정책이 위반된다면, 사용 관리 컴포넌트(430)는 시도된 액션이 처리되는 것을 허용하지 않음으로써 정책을 적용할 수 있다. 또한, 사용 관리 컴포넌트(430)는 스마트 카드(220)와 관련된 사용 정책의 위반의 검출 시에 위반 메시지일 수 있는 사용 정보를 통신 컴포넌트(440)에 중계하도록 동작할 수 있다.

<39> 스마트 카드(220)와 스마트 카드 단말(200) 간의 통신을 위한 통신 컴포넌트(440)는 예시적인 데이터 및 관리 프레임워크(310)의 추가적인 형태(feature)일 수 있다. 상술한 바와 같이, 에러 상태 관리 컴포넌트(420)와 사용 관리 컴포넌트(430) 모두는 정보를 통신 컴포넌트(440)로 중계할 수 있다. 수신된 정보는 에러 검출, 사용 정책 위반, 또는 또 다른 유형의 통신을 포함할 수 있다. 에러 상태 관리 컴포넌트(420)가 스마트 카드(220)의 사용과 관련된 에러를 검출하여 이 에러의 표시(indication)를 통신 컴포넌트(440)에 송신한다면, 통신 컴포넌트(440)는 스마트 카드 단말(200)의 모니터(191) 상에 에러 메시지를 디스플레이할 수 있다. 에러 메시지는 단말(200) 및 스마트 카드(220)의 사용자에 대한 명령어들을 포함할 수 있다. 또한, 통신 컴포넌트(440)는 사용 관리 컴포넌트(430)에 의해 보고된, 스마트 카드와 관련된 사용 정책의 위반의 표시를 디스플레이할 수 있다. 또한, 이러한 표시는 모니터(191) 상에 디스플레이될 수 있다.

<40> 통신 컴포넌트(440)는 에러 상태 또는 사용 위반의 표시를 수신할 시에 에러 또는 위반의 로그 엔트리(log entry)를 생성할 수 있다. 통신 컴포넌트(440)는 예를 들어, 에러 상태 또는 사용 위반의 애플리케이션에 표시를 제공하기 위해 애플리케이션으로 메시지를 송신할 수 있다. 애플리케이션으로 송신된 메시지는 예를 들어 메시지가 송신되었다는 경보(alert)로서의 역할을 하는 음향 또는 소리를 생성할 수 있다.

<41> 일 실시예에서, 데이터 및 관리 프레임워크(310)는 접속 컴포넌트(450)도 포함할 수 있는데, 접속 컴포넌트는, 어떠한 에러도 검출되지 않고/않거나 사용 정책이 적용된다면 스마트 카드 애플리케이션(230)과 대응하는 단말 애플리케이션(305) 간의 채널을 생성하도록 동작할 수 있다. 생성된 채널은 단말(200)과 카드(220) 간의 보안 채널일 수 있다.

<42> 단말 정책 컴포넌트(460)는 스마트 카드 애플리케이션(230) 상의 추가적인 정책들 및/또는 제약들을 통합하기 위해 데이터 및 관리 프레임워크(310)에 포함될 수 있다. 예를 들어, 단말 애플리케이션(305)의 개발자는 특정 애플리케이션(230)에 대한 단말(200)의 사용에 시간 제한을 설정하기를 원할 수 있다. 추가적인 정책들 및/또는 제약들이 통합될 수도 있다.

<43> 도 5는 스마트 카드 단말 애플리케이션(305)과 스마트 카드(220) 상의 스마트 카드 애플리케이션(230) 간의 예시적인 상호 운용 방법을 도시한다. 상호 운용 방법은, 단말 애플리케이션(305)이 스마트 카드 단말 판독기(210)에 삽입된 스마트 카드(220) 상에 있는 스마트 카드 애플리케이션(230)과 매끄럽게(seamlessly) 동작하도록 스마트 카드 단말 애플리케이션 개발자에 의해 구현될 수 있다.

<44> 박스(505)에서, 스마트 카드 단말(200)의 데이터 및 관리 프레임워크(310)에 기록된 API가 획득된다. API는 스마트 카드 애플리케이션(230)에 대응한다. 대응하는 단말 애플리케이션(305)을 생성하기 위하여, 스마트 카드 애플리케이션(230) 관련 정보가 사용된다. 박스(510)에서, 이러한 정보가 API로부터 획득된다. 스마트 카드 애플리케이션(230)과 관련된 정보는 스마트 카드 애플리케이션(230)의 인터페이스, 스마트 카드 애플리케이션(230)에 의해 사용되는 프로토콜 및 스마트 카드(220)의 보안 모델을 포함할 수 있지만 이에 제한되는 것은 아니다. 박스(515)에서, 스마트 카드 애플리케이션(230)과 관련된 획득 정보는 예를 들어 데이터 및 관리 프레임워크(310)의 인터페이스 컴포넌트(410)에 의해 스마트 카드 애플리케이션(230)에 대응하는 단말 애플리케이션(305)으로 통합된다. 단말 애플리케이션(305)이 스마트 카드 애플리케이션(230)과 관련된 정보를 통합함으로써 생성된 후에, 각종 보조적이고 선택적인(optional) 데이터 및 관리 동작들이 데이터 및 관리 프레임워크(310)에

의해 구현될 수 있다.

<45> 박스(520)에서, 스마트 카드 애플리케이션(230)과 관련된 정보의 일부로서 획득될 수 있는, 스마트 카드(220)의 보안 모델이 적용될 수 있다. 박스(525)에서, 적용 동작은 단말(200)에서 스마트 카드(220)의 사용을 감시하는 것을 추가적으로 포함할 수 있다. 감시 동작은 스마트 카드(220)의 보안 모델 또는 사용 정책의 분석과 동시에 일어날 수 있다. 박스(530)에서, 감시된 사용이 보안 모델을 위반하였는지를 확인하기 위해 예를 들어 사용 관리 컴포넌트(430)에 의해 판정이 수행된다. 박스(535)에서, 보안 모델이 위반되었다면, 위반 메시지가 중계될 수 있다. 위반 메시지는 예를 들어 모니터(191)와 같은 디스플레이 장치 상에 메시지를 디스플레이하는 것에 의해, 위반의 로그 엔트리를 생성하는 것에 의해, 또는 애플리케이션으로의 메시지의 전송에 의해 중계될 수 있다. 애플리케이션으로 송신된 메시지는 예를 들어 메시지가 송신되었다는 통지로서의 역할을 하는 음향 또는 소리를 생성할 수 있다. 에러 메시지를 중계하는 임의의 조합이 수행될 수 있다.

<46> 위반 메시지의 중계에 후속하여, 방법은 박스(525)로 되돌아가서 스마트 카드(220)의 사용을 추가적으로 감시할 수 있다. 박스(530)에서 판정된 바와 같이 모델이 위반되지 않았다면, 보안 모델이 그 후의 시간에 위반되었는지를 판정하기 위해 추가적인 판정이 이루어질 수 있다.

<47> 박스(520) 및/또는 박스(530)에 후속하는 박스(540)에서, 보안 모델이 스마트 카드(220)에 의해 위반되지 않았다면, 스마트 카드(220)와 스마트 카드 단말(200) 간의 보안 통신 채널이 생성될 수 있다. 스마트 카드(220) 및 단말(200)이 안전하게 통신하고 스마트 카드(220)의 의도된 기능들을 수행하도록, 카드(220)의 보안 모델이 적용된 후 및/또는 모델이 위반되지 않았다는 판정 후에 채널이 만들어질 수 있다. 예를 들어, 데이터 및 관리 프레임워크(310)가, 예정된 보안 모델이 위반되지 않고 있다고 판정한 후에, 보안 통신 채널이 예를 들어 접속 컴포넌트(450)에 의해 생성될 수 있다.

<48> 박스(545)에서, 스마트 카드 단말 애플리케이션은 단말 정책 및/또는 단말 제약을 추가적으로 규정하도록 구성될 수 있다. 단말 정책 컴포넌트(460)는 스마트 카드(220)의 사용 및/또는 스마트 카드 애플리케이션(230)의 처리에 관한 추가적인 정책들 및/또는 제약들을 확립하고 통합하기 위하여 그 구성을 수행할 수 있다. 스마트 카드(220)의 보안 모델이 위반되지 않았다는 것으로 판정된다면, 그 구성은 박스(520), 박스(530) 및/또는 박스(540)에 후속하여 수행될 수 있다.

<49> 도 6은 스마트 카드(220)의 보안 모델을 스마트 카드 단말(200)에 적용하는 예시적인 방법을 도시한다. 박스(610)에서, 스마트 카드(220)의 보안 모델은 단말 인프라스트럭처(300)의 데이터 및 관리 프레임워크(310)로부터 획득된다. 프레임워크(310)로부터 스마트 카드(220)의 보안 모델을 획득하는 것은 데이터 및 관리 프레임워크(310)에 적용되거나 기록되는 API를 판독하는 것을 포함할 수 있다. 스마트 카드 단말 인프라스트럭처(300)의 데이터 및 관리 프레임워크(310)는 단말 애플리케이션(305)의 개발 및 생성에 있어서 지원하도록 기능할 수 있다. 단말 애플리케이션(305)은 스마트 카드 애플리케이션(230)에 대응한다.

<50> 박스(615)에서, 보안 모델은 스마트 카드 애플리케이션(230)에 대응하도록 개발되는 스마트 카드 단말 애플리케이션(305)에 통합된다. 박스(620)에서, 보안 모델에 의해 규정될 수 있는 에러 상태가 검출되는지를 확인하기 위해 판정이 이루어진다. 이러한 검출은 에러 상태들을 검출하기 위해 주기적으로 또는 연속적으로 수행될 수 있다. 박스(620)에서, 에러 상태가 검출되면, 박스(625)에서 검출된 에러 상태에 대응하는 에러 메시지가 전송된다. 에러 상태 관리 컴포넌트(420)는 에러 상태 검출을 수행할 수 있고, 에러의 검출 시에 에러의 통지를 통신 컴포넌트(440)에 송신할 수 있다. 통신 컴포넌트(440)는 예컨대, 모니터(191)와 같은 디스플레이 장치 상에 대응하는 메시지를 디스플레이하는 것에 의해, 에러의 로그 엔트리를 생성하는 것에 의해, 또는 애플리케이션으로의 메시지의 전송에 의해 에러 메시지를 중계할 수 있다. 애플리케이션에 송신된 메시지는 예를 들어 에러 메시지가 송신되었다는 통지로서의 역할을 하는 음향 또는 소리를 생성한다. 에러 메시지를 중계하는 임의의 조합이 수행될 수 있다.

<51> 이해될 수 있는 바와 같이, 개시된 실시예들은 하나 이상의 컴퓨팅 시스템 또는 장치의 전부 또는 일부로서 구현될 수 있다. 도 1은 그 양태들이 구현되거나 실시될 수 있는 하나의 예시적인 컴퓨팅 시스템(100)의 기능적 컴포넌트들을 도시한다. 본 명세서에서 사용된, "컴퓨팅 시스템", "컴퓨터 시스템" 및 "컴퓨터"라는 용어는 프로그램 코드 및/또는 데이터를 실행하거나 다르게 처리할 수 있는 프로세서를 포함하는 임의의 머신, 시스템 또는 장치를 가리킨다. 컴퓨팅 시스템의 예들은, 어떠한 의도된 제한없이 퍼스널 컴퓨터(PC)들, 미니컴퓨터들, 메인프레임 컴퓨터들, 씬 클라이언트(thin client)들, 네트워크 PC들, 서버들, 워크스테이션들, 랩톱 컴퓨터들, 핸드-헬드 컴퓨터들, 프로그래머블 소비자 가전제품, 멀티미디어 컨솔(conole)들, 게임 컨솔들, 위성 수신기들, 셋탑 박스들, ATM(automated teller machines), 아케이드 게임들, 모바일 전환, PDA(personal digital

assistant)들 및 임의의 기타 프로세서 기반 시스템 또는 머신을 포함한다. "프로그램 코드" 및 "코드"라는 용어는 프로세서에 의해 실행되거나 다르게 처리되는 명령어들의 임의의 세트를 가리킨다. 프로그램 코드 및/또는 데이터는 특정 기능들을 수행하는 루틴들, 프로그램들, 객체들, 모듈들, 데이터 구조체들 등의 형태로 구현될 수 있다.

<52> 상술한 예들은 단지 설명의 목적으로 제공되었으며 제한적인 것으로 해석되어서는 안된다는 것에 유의해야 한다. 본 발명이 각종 실시예들을 참조하여 설명되었지만, 본 명세서에서 사용된 단들은 제한적인 단어들이 아니라 설명 또는 예시의 단어들이다. 또한, 실시예들이 특정 수단들, 재료들 및 예들을 참조하여 본 명세서에서 설명되었지만, 본 실시예들은 본 명세서에서 개시된 특정사항들로 제한되게 하려고 한 것은 아니며, 오히려 실시예들은 첨부된 청구항들의 범위에 속하는 모든 기능적으로 동등한 구조들, 방법들 및 용법들로 확장한다.

도면의 간단한 설명

<8> 도 1은 예시적인 컴퓨팅 장치를 나타내는 블록도이다.

<9> 도 2는 예시적인 스마트 카드 단말을 나타내는 블록도이다.

<10> 도 3은 예시적인 스마트 카드 단말 인프라스트럭쳐를 나타내는 블록도이다.

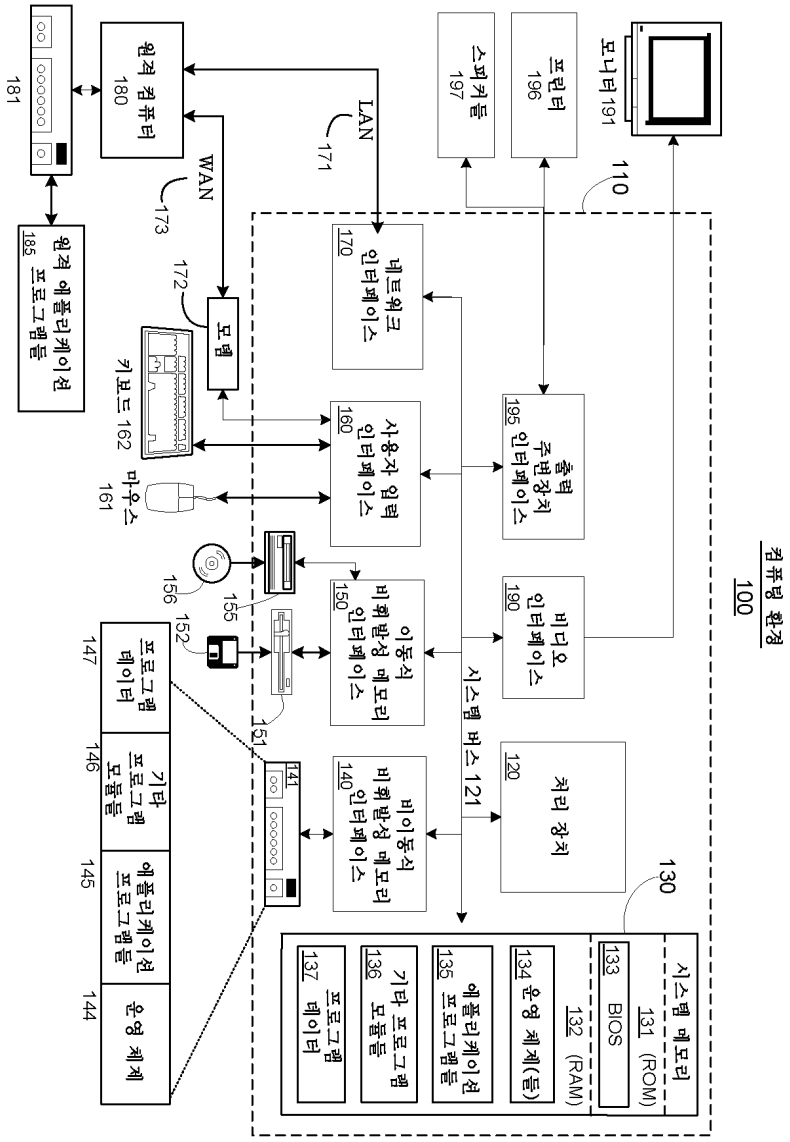
<11> 도 4는 데이터 및 관리 프레임워크를 나타내는 블록도이다.

<12> 도 5는 스마트 카드 단말 애플리케이션과 스마트 카드 상의 스마트 카드 애플리케이션 사이의 상호 운용 방법의 일 실시예를 도시하는 흐름도이다.

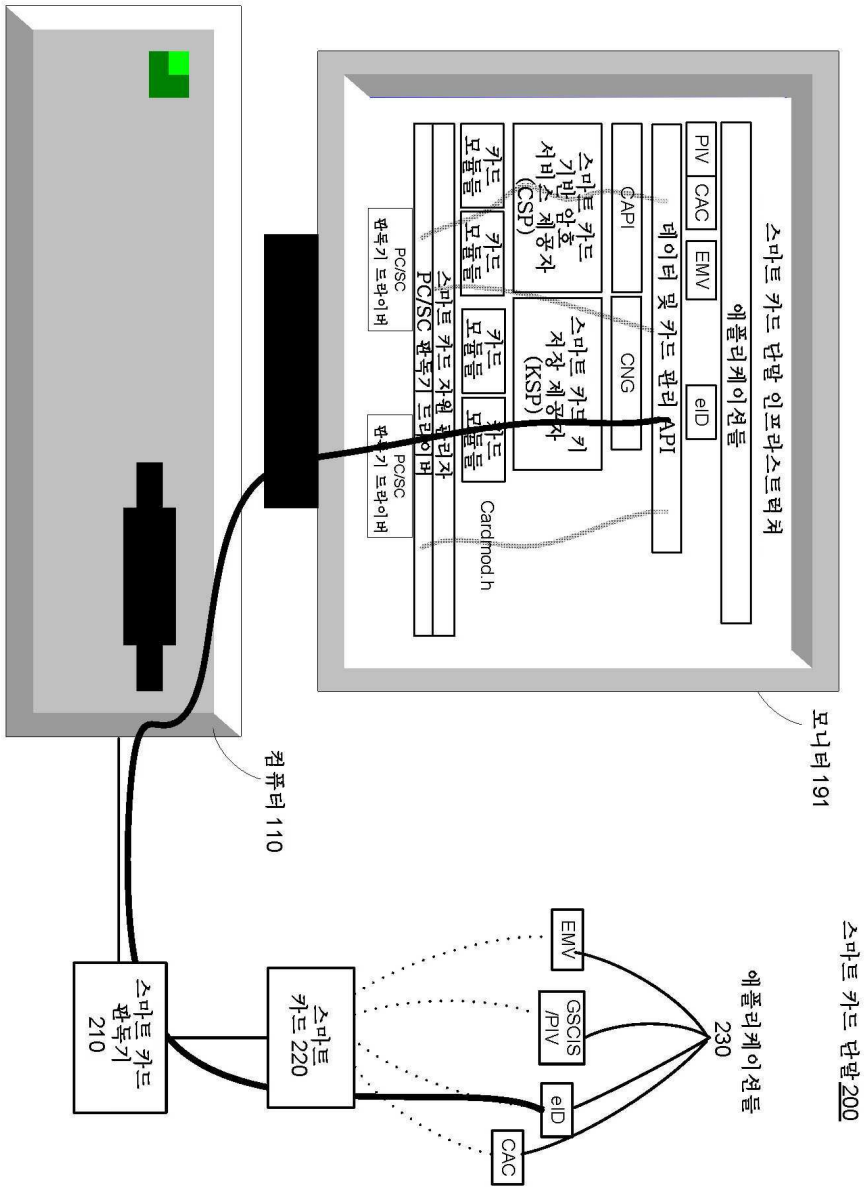
<13> 도 6은 스마트 카드의 보안 모델을 스마트 카드 단말에 적용하는 방법의 일 실시예를 도시하는 흐름도이다.

도면

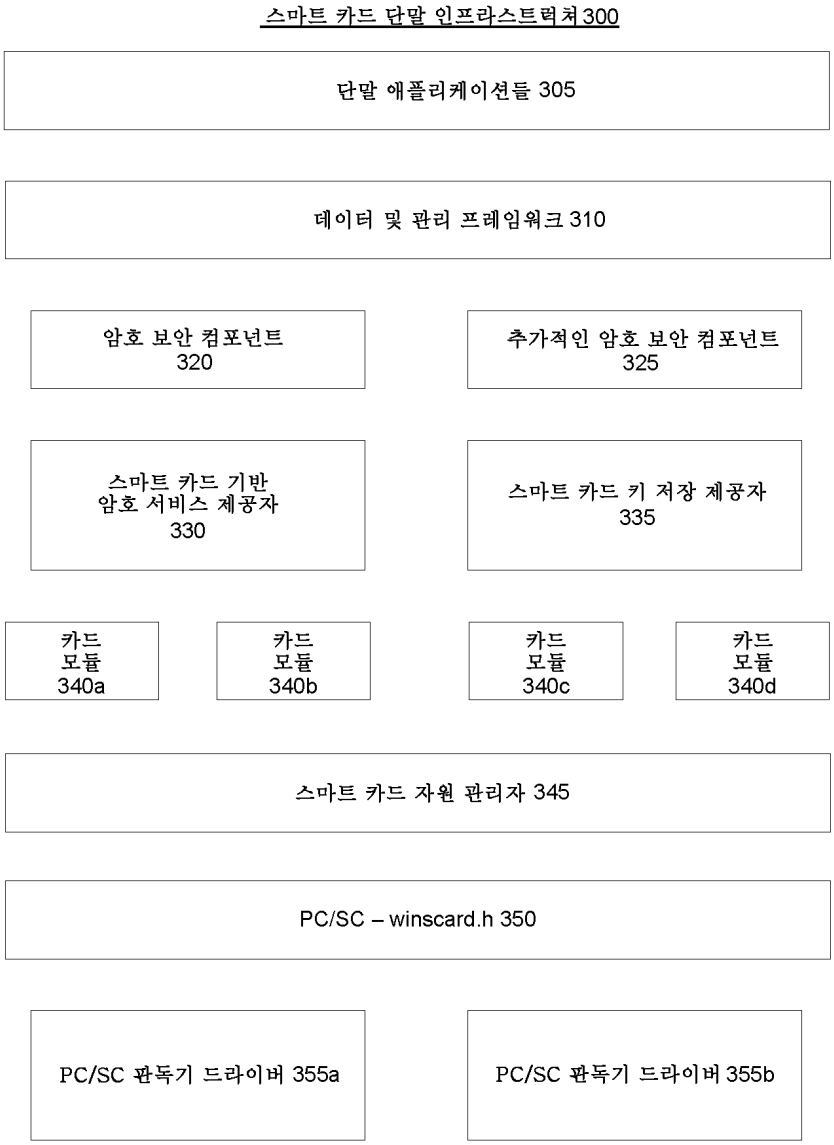
도면1


컴퓨팅 환경
100
모니터 191
프린터 196
스피커들 197
110
네트워크 인터페이스 170
출력 주변장치 인터페이스 195
사용자 입력 인터페이스 160
비디오 인터페이스 190
이동식 비휘발성 메모리 인터페이스 150
비이동식 비휘발성 메모리 인터페이스 140
시스템 버스 121
처리 장치 120
130
시스템 메모리
131 (ROM)
133 BIOS
132 (RAM)
134 운영 체제(들)
135 애플리케이션 프로그램들
136 기타 프로그램 모듈들
137 프로그램 데이터
LAN 171
WAN 173
모뎀 172
원격 컴퓨터 180
181
원격 애플리케이션 프로그램들 185
키보드 162
마우스 161
156
155
152
151
141
147 프로그램 데이터
146 기타 프로그램 모듈들
145 애플리케이션 프로그램들
144 운영 체제

도면2


스마트 카드 단말 200
모니터 191
컴퓨터 110
스마트 카드 단말 인프라스트럭처
애플리케이션들
PIV
CAC
EMV
eID
데이터 및 카드 관리 API
CAPI
CNG
스마트 카드 기반 암호 서비스 제공자 (CSP)
스마트 카드 키 저장 제공자 (KSP)
카드 모듈들
카드 모듈들
카드 모듈들
카드 모듈들
CardMod.h
스마트 카드 자원 관리자
PC/SC 판독기 드라이버
PC/SC 판독기 드라이버
스마트 카드 판독기 210
스마트 카드 220
애플리케이션들 230
EMV
GSCIS /PIV
eID
CAC

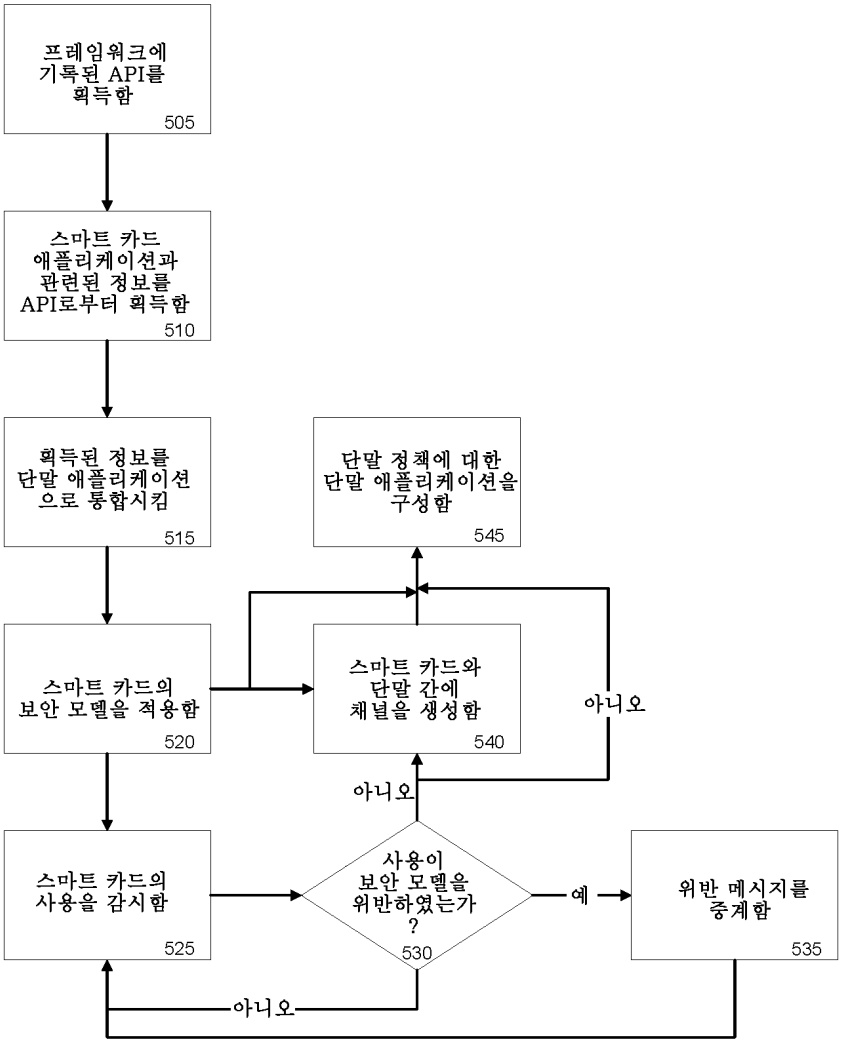
도면3


스마트 카드 단말 인프라스트럭처 300
단말 애플리케이션들 305
데이터 및 관리 프레임워크 310
암호 보안 컴포넌트 320
추가적인 암호 보안 컴포넌트 325
스마트 카드 기반 암호 서비스 제공자 330
스마트 카드 키 저장 제공자 335
카드 모듈 340a
카드 모듈 340b
카드 모듈 340c
카드 모듈 340d
스마트 카드 자원 관리자 345
PC/SC – winscard.h 350
PC/SC 판독기 드라이버 355a
PC/SC 판독기 드라이버 355b

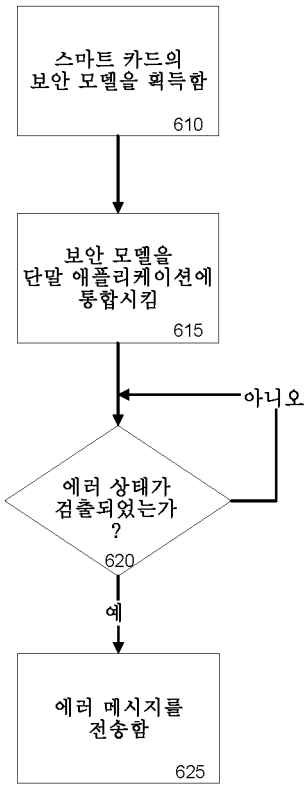
도면4


데이터 및 관리 프레임워크 310
인터페이스 컴포넌트 410
에러 상태 관리 컴포넌트
420
사용 관리 컴포넌트
430
통신 컴포넌트
440
접속 컴포넌트
450
단말 정책 컴포넌트
460

도면5


프레임워크에 기록된 API를 획득함
505
스마트 카드 애플리케이션과 관련된 정보를 API로부터 획득함
510
획득된 정보를 단말 애플리케이션으로 통합시킴
515
단말 정책에 대한 단말 애플리케이션을 구성함
545
스마트 카드의 보안 모델을 적용함
520
스마트 카드와 단말 간에 채널을 생성함
540
아니오
아니오
스마트 카드의 사용을 감시함
525
사용이 보안 모델을 위반하였는가 ?
530
예
위반 메시지를 중계함
535
아니오

도면6


스마트 카드의
보안 모델을 획득함
610
보안 모델을
단말 애플리케이션에
통합시킴
615
아니오
에러 상태가
검출되었는가
?
620
예
에러 메시지를
전송함
625