(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0098640
(43) 공개일자 2008년11월11일

(51) Int. Cl.
H04Q 7/24 (2006.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2008-7021541
(22) 출원일자 2008년09월02일
심사청구일자 2008년09월02일
번역문제출일자 2008년09월02일
(86) 국제출원번호 PCT/EP2007/051039
국제출원일자 2007년02월02일
(87) 국제공개번호 WO 2007/088203
국제공개일자 2007년08월09일
(30) 우선권주장
0650401 2006년02월03일 프랑스(FR)

(71) 출원인
장쁠뤼
프랑스 제므노 세덱스 브와뜨 뽀스딸 100-13881 빠르끄 닥띠비떼 드 제므노 아브뉘 뒤 삐끄 드 베르따뉴
(72) 발명자
마르티네, 프레드릭
프랑스 에프-13011 마르세유 비디 데 라 제르망 7
보드, 안토니
프랑스 13710 프비오 도멘 드오루무 17
모쎄, 프랭크
프랑스 13130 베레 이에땅 비스 블러바드 헨리 바르뷔스 71
(74) 대리인
양영준, 백만기

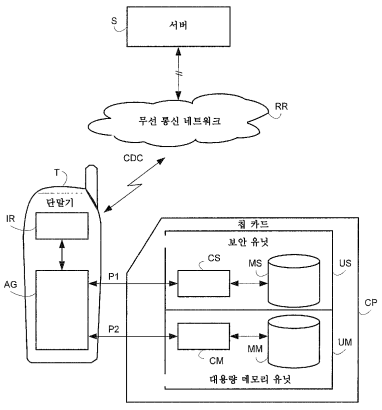
전체 청구항 수 : 총 7 항

(54) 휴대형 통신 객체 내의 대용량 기억부 및 보안 기억부를 원격 액세스하기 위한 시스템

(57) 요 약

본 발명은 휴대형 통신 객체 내의 대용량 기억부 및 보안 기억부에 원격 액세스하는 시스템에 관한 것이다. 본 발명에 따르면, 멀티미디어 스마트 카드 등의 휴대형 통신 객체(CP)와 연관된 모바일 등의 터미널(T)은 서버(S)로부터, 통신 네트워크(RR)를 통해 휴대형 통신 객체(CP) 내의 멀티미디어 데이터 및 보안 기억부(MS)를 기억할 수 있는 대용량 기억부(MM)로의 액세스를 용이하게 하기 위한 에이전트(AG)를 포함한다. 상기 에이전트는 원격 서버와 터미널 간의 단일 통신 채널(CDC)을 확립하고, 서버와 휴대형 통신 객체의 기억부들 중 하나를 포함하는 2개의 요소 중 하나로부터 상기 에이전트에 송신되는 데이터를 처리하여, 상기 에이전트는 상기 데이터를 상기 2개의 요소들 중 다른 하나에 송신할 수 있다.

대 표 도 - 도1



특허청구의 범위

청구항 1

통신 네트워크(RR)를 통해 서버(S)에 의해, 단말기(T)와 연관된 휴대형 통신 객체(CP) 내의 대용량 메모리(MM) 및 보안 메모리(MS)에 원격 액세스하는 방법으로서,

상기 원격 서버와 상기 휴대형 통신 객체의 메모리들 중 하나 또는 다른 하나 사이의 데이터 전송들을 라우팅하기 위한 상기 단말기 내의 에이전트(AG)를 제공하는 단계;

상기 원격 서버와 상기 단말기 내의 에이전트 사이에 통신 채널(CDC)을 설정하는 단계(E0);

상기 서버 및 상기 휴대형 통신 객체의 메모리들 중 하나를 포함하는 2개의 요소 중 하나에서 상기 단말기 내의 에이전트(AG)로 데이터(D)를 전송하는 단계(E1); 및

상기 에이전트가 상기 전송된 데이터를 상기 2개의 요소 중 다른 하나로 전송하도록, 상기 에이전트(AG)로 전송된 데이터를 처리하는 단계(E2)

를 포함하는 메모리 액세스 방법.

청구항 2

제1항에 있어서,

상기 서버(S)에 의한 상기 대용량 메모리(MM)의 원격 액세스는, 상기 데이터(D)의 전송(E1) 전에, 상기 단말기(T) 내의 에이전트(AG)를 통한, 상기 보안 메모리를 포함하는 보안 유닛(US)과 상기 서버 간의 상호작용들에 의해 안전하게 되는 메모리 액세스 방법.

청구항 3

제2항에 있어서,

상기 원격 서버(S)와 상기 단말기(T) 간의 통신 채널(CDC)의 설정(E0) 후에, 비밀 데이터(RND1, RND2)의 교환에 의한 상기 서버와 상기 휴대형 통신 객체(CP)의 보안 유닛(US) 간의 인증(EA, FA, GA)을 포함하고, 상기 인증이 확인되자마자 상기 에이전트(AG)를 통한 상기 서버에 의한 상기 휴대형 통신 객체의 대용량 메모리(MM)의 액세스를 허가하는(EA8) 메모리 액세스 방법.

청구항 4

제2항 또는 제3항에 있어서,

상기 서버(S)와 상기 단말기(T) 간의 통신 채널(CDC)의 설정(F0) 후에, 응답으로서 암호화/해독 키(KS)를 얻기(F7) 위한 상기 에이전트(AG)에 의한 요청(RQ_KS)의 상기 보안 유닛(US)으로의 전송(F5), 상기 서버(S) 및 상기 에이전트(AG)를 포함하는 2개의 수단 중 하나에 의한 상기 데이터(D)의 암호화(F3), 상기 암호화된 데이터의 상기 2개의 수단(AG, S) 중 다른 하나로의 전송(F4), 및 상기 2개의 수단 중 상기 다른 하나에 의한 상기 암호화된 데이터(D)의 해독(F8)을 포함하는 메모리 액세스 방법.

청구항 5

제2항 또는 제3항에 있어서,

상기 서버(S)와 상기 단말기(T) 간의 통신 채널(CDC)의 설정(G0) 후에, 응답으로서 암호화/해독 키(KS)를 얻기(G7) 위한, 상기 휴대형 통신 객체에 포함된 대용량 메모리의 제어기(CM)에 의한 요청(REQ_KS)의 상기 보안 유닛(US)으로의 전송(G6), 상기 서버(S) 및 상기 대용량 메모리 제어기(CM)를 포함하는 2개의 수단 중 하나에 의한 상기 데이터(D)의 암호화(G3), 상기 암호화된 데이터의 상기 2개의 수단(CM, S) 중 다른 하나로의 전송(G4, G5), 및 상기 2개의 수단 중 상기 다른 하나에 의한 상기 암호화된 데이터(D)의 해독(G9)을 포함하는 메모리 액세스 방법.

청구항 6

서버(S)가 통신 네트워크(RR)를 통해 휴대형 통신 객체(CP) 내의 대용량 메모리(MM) 또는 보안 메모리(MS)에 원

격 액세스할 수 있도록 상기 휴대형 통신 객체(CP)와 연관된 단말기(T)로서,

에이전트(AG)를 포함하되,

상기 에이전트(AG)는,

상기 원격 서버와 상기 휴대형 통신 객체의 메모리들 중 하나 또는 다른 하나 사이의 데이터 전송들을 라우팅하고,

상기 원격 서버와 상기 단말기 사이에 통신 채널(CDC)을 설정하며,

상기 서버 및 상기 휴대형 통신 객체의 메모리들 중 하나를 포함하는 2개의 요소 중 하나에서 상기 에이전트(AG)로 전송된 데이터를 처리하여, 상기 전송된 데이터를 상기 2개의 요소 중 다른 하나로 전송하는 단말기.

청구항 7

서버(S)가 통신 네트워크(RR)를 통해 휴대형 통신 객체(CP) 내의 대용량 메모리(MM) 또는 보안 메모리(MS)에 원격 액세스할 수 있도록 상기 휴대형 통신 객체(CP)와 연관된 단말기(T)에서 구현될 수 있는 프로그램으로서,

상기 단말기에서 실행될 때,

상기 원격 서버와 상기 휴대형 통신 객체의 메모리들 중 하나 또는 다른 하나 사이의 데이터 전송들을 라우팅하기 위한 상기 단말기 내의 에이전트(AG)를 제공하는 단계;

상기 원격 서버와 상기 단말기 내의 에이전트 사이에 통신 채널(CDC)을 설정하는 단계(E0);

상기 서버 및 상기 휴대형 통신 객체의 메모리들 중 하나를 포함하는 2개의 요소 중 하나에서 상기 단말기 내의 에이전트(AG)로 데이터(D)를 전송하는 단계(E1); 및

상기 에이전트가 상기 전송된 데이터를 상기 2개의 요소 중 다른 하나로 전송하도록, 상기 에이전트(AG)로 전송된 데이터를 처리하는 단계(E2)

를 수행하는 명령들을 포함하는 프로그램.

명 세 서

기 술 분 야

<1> 본 발명은 단말기와 연관된, 높은 저장 용량을 갖는 휴대형 통신 객체에 포함된 대용량 메모리 및 보안 메모리에 대한 단일 서버의 원격 액세스에 관한 것이다.

배 경 기 술

<2> 휴대형 통신 객체는, 예를 들어 "플래시 메모리 카드", "보안 디지털 카드" 또는 "멀티미디어 카드" 타입의 카드의 메모리에 대응하는, 메모리 제어기 및 대용량 메모리를 포함하는 대용량 메모리 유닛, 및 보안 제어기 및 관련 보안 메모리를 포함하는 UICC 카드(Universal Integrated Circuit(s) Card)의 SIM(Subscriber Identity Module) 또는 USIM(Universal Subscriber Identity Module)과 같은 보안 유닛을 포함하는 특별한 특징을 갖는다.

<3> 이러한 새로운 기술은 휴대형 통신 객체 내의 메모리의 크기를 크게 증가시킨다. 이것은 128 킬로옥텟에서 128 메가옥텟으로 증가시키며, 수 기가옥텟에 이를 수 있다. 증가된 크기의 대용량 메모리는 사진들 및 이메일 어드레스들을 갖는 멀티미디어 전화 번호부, 원격 다운로드된 음악, 사진들, 전문가들, 음악에 대한 프리젠테이션들과 같이 통신 객체의 사용자에게 고유한 모든 멀티미디어 데이터를 그 안에 저장하는 것을 가능하게 한다.

<4> 2개의 제어기를 2개의 메모리와 개별적으로 연관시키는 아키텍처는 원격 서버에 의한 휴대형 통신 객체의 2개의 메모리 중 하나에 대한 독점적인 액세스를 수반한다. 이러한 액세스들은 서버와 휴대형 통신 객체 사이의 2개의 통신 채널에 의해 각각 구현된다. 안전하지 않은 제1 통신 채널은 단말기에 의해 관리되며, 2개의 전송 프로토콜을 포함한다. OTA("Over The Air") 타입의 제1 프로토콜은 서버와 단말기 사이의 데이터 전송과 관련된다. MMC("Multi-Media Card") 타입의 제2 프로토콜은 단말기와 통신 객체의 대용량 메모리 유닛 간의 고속 액세스 데이터 전송과 관련된다. 제2 통신 채널은 단말기를 통한 원격 서버와 휴대형 통신 객체의 보안 유닛 간의 안전하고, 신뢰성 있고, 인지되는 단일 데이터 전송 채널을 포함하지만, 제1 프로토콜보다 덜 빠른 액세스를

제공한다. 또한, 제2 프로토콜에 대해, 단말기는 투명 라우터로 간주된다.

<5> 이러한 기술의 하나의 주요 단점은 원격 서버가 휴대형 통신 객체의 대용량 메모리 및 보안 메모리에 동시에 액세스할 수 없다는 점이다. 이를 행하기 위해서는, 서버는 전술한 바와 같은 2개의 통신 채널을 설정해야 한다.

<6> <발명의 요약>

<7> 본 발명의 목적은 서버와 같은 원격 엔티티가 단말기와 연관된 휴대형 통신 객체의 대용량 메모리 및 보안 메모리 양자에 액세스하는 것을 보다 쉽게 함으로써 전술한 문제를 해결하는 것이다.

<8> 이러한 목적을 달성하기 위하여, 통신 네트워크를 통해 서버에 의해, 단말기와 연관된 휴대형 통신 객체 내의 대용량 메모리 및 보안 메모리에 원격 액세스하는 방법은,

<9> 상기 원격 서버와 상기 휴대형 통신 객체의 메모리들 중 하나 또는 다른 하나 사이의 데이터 전송들을 라우팅하기 위한 상기 단말기 내의 에이전트를 제공하는 단계;

<10> 상기 원격 서버와 상기 단말기 내의 에이전트 사이에 통신 채널을 설정하는 단계;

<11> 상기 서버 및 상기 휴대형 통신 객체의 메모리들 중 하나를 포함하는 2개의 요소 중 하나에서 상기 단말기 내의 에이전트로 데이터를 전송하는 단계; 및

<12> 상기 에이전트가 상기 전송된 데이터를 상기 2개의 요소 중 다른 하나로 전송하도록, 상기 에이전트로 전송된 데이터를 처리하는 단계

<13> 를 포함하는 것을 특징으로 한다.

<14> 예를 들어, 휴대형 통신 객체는 보안 메모리를 포함하는 보안 유닛을 포함하는 멀티미디어 칩 카드이다. 이어서, 서버에 의한 대용량 메모리의 원격 액세스는 멀티미디어 데이터와 같은 데이터의 전송 전에 단말기 내의 에이전트를 통한 보안 유닛과 서버 간의 상호작용들에 의해 안전하게 된다.

<15> 바람직하게는, 상기 원격 서버와 상기 단말기 간의 통신 채널의 설정 후에, 비밀 데이터의 교환에 의한 상기 서버와 상기 휴대형 통신 객체의 보안 유닛 간의 인증이 존재하고, 상기 인증이 확인되자마자 상기 에이전트를 통한 상기 서버에 의한 상기 휴대형 통신 객체의 대용량 메모리의 액세스를 허가한다.

<16> 제1 실시예에 따르면, 본 발명의 방법은, 상기 서버와 상기 단말기 간의 통신 채널의 설정 후에, 응답으로서 암호화/해독 키를 얻기 위한 상기 에이전트에 의한 요청의 상기 보안 유닛으로의 전송, 상기 서버 및 상기 에이전트를 포함하는 2개의 수단 중 하나에 의한 상기 데이터의 암호화, 상기 암호화된 데이터의 상기 2개의 수단 중 다른 하나로의 전송, 및 상기 2개의 수단 중 상기 다른 하나에 의한 상기 암호화된 데이터의 해독을 더 포함한다.

<17> 제2 실시예에 따르면, 본 발명의 방법은, 상기 서버와 상기 단말기 간의 통신 채널의 설정 후에, 응답으로서 암호화/해독 키를 얻기 위한, 상기 휴대형 통신 객체에 포함된 대용량 메모리의 제어기에 의한 요청의 상기 보안 유닛으로의 전송, 상기 서버 및 상기 대용량 메모리 제어기를 포함하는 2개의 수단 중 하나에 의한 상기 데이터의 암호화, 상기 암호화된 데이터의 상기 2개의 수단 중 다른 하나로의 전송, 및 상기 2개의 수단 중 상기 다른 하나에 의한 상기 암호화된 데이터의 해독을 더 포함한다.

<18> 본 발명은 또한, 서버가 통신 네트워크를 통해 휴대형 통신 객체 내의 대용량 메모리 또는 보안 메모리에 원격 액세스할 수 있도록 상기 휴대형 통신 객체와 연관된 단말기(T)에 관한 것이다. 상기 단말기는 에이전트(AG)를 포함하되, 상기 에이전트(AG)는 상기 원격 서버와 상기 휴대형 통신 객체의 메모리들 중 하나 또는 다른 하나 사이의 데이터 전송들을 라우팅하고, 상기 원격 서버와 상기 단말기 사이에 통신 채널(CDC)을 설정하며, 상기 서버 및 상기 휴대형 통신 객체의 메모리들 중 하나를 포함하는 2개의 요소 중 하나에서 상기 에이전트(AG)로 전송된 데이터를 처리하여, 상기 전송된 데이터를 상기 2개의 요소 중 다른 하나로 전송하는 것을 특징으로 한다.

<19> 마지막으로, 본 발명은 본 발명에 따른 단말기에서 구현될 수 있는 프로그램에 관한 것이다.

<20> 본 발명의 다른 특징들 및 이점들은, 비제한적인 예로서, 대응하는 첨부 도면들을 참조하여 주어지는 본 발명의 여러 바람직한 실시예에 대한 아래의 설명을 읽을 때 보다 명확해질 것이다.

발명의 상세한 설명

<26> 후술하는 본 발명의 바람직한 일 실시예는 데이터가 휴대형 통신 객체의 멀티미디어 콘텐츠 서버 또는 관리 서버와, 휴대형 통신 객체와 연관된 단말기 사이에 전송될 수 있는 무선 통신 네트워크들의 분야에 관한 것이다.

<27> 그러나, 본 발명은 회계 또는 은행 데이터, 의료 데이터 등에 관련된 다른 분야들에 적용될 수 있다.

<28> 도 1 및 2를 참조하면, 본 발명에 따른 통신 시스템은 적어도 하나의 무선 통신 네트워크(RR)를 통해, 예를 들어 칩 카드(CP)와 같이 높은 저장 용량을 갖는 휴대형 통신 객체와 연관된 이동 단말기(T)와 통신하는 원격 서버(S)를 포함하는데, 본 설명의 나머지에서 휴대형 통신 객체는 칩 카드(CP)로서 참조된다. 무선 통신 네트워크(RR)는 UMTS 타입, GPRS 네트워크에 기초하는 GSM 타입, 또는 WIFI, WIMAX, WIBRO 타입이다.

<29> 3개의 엔티티(S, T, CP)는 기능 블록들의 형태로 도시되어 있으며, 이들 대부분은 본 발명과 관련된 기능들을 수행하며, 소프트웨어 및/또는 하드웨어 모듈들에 대응할 수 있다.

<30> 서버(S)는 무선 통신 네트워크(RR)의 운영자에 의해 관리되는 멀티미디어 콘텐츠 서버 및/또는 칩 카드 관리 서버이며, OTA 플랫폼을 구성한다.

<31> 도 2를 참조하면, 서버(S)는 관리자(GE), 메모리(ME) 및 통신 인터페이스(IC)를 포함한다. 서버(S)는 데이터베이스(BD)에 접속되거나, 이를 포함한다.

<32> 관리자(GE)는 서버(S)와 칩 카드(CP) 또는 단말기(T) 간의 데이터 전송 동안, 서버와 칩 카드(CP) 간의 인증, 서버와 칩 카드 또는 단말기 사이에 교환되는 데이터를 암호화하고 해독하는 동작들에 필요한 세션 키의 결정과 같은 다양한 동작을 관리한다. 관리자(GE)는 또한 무선 통신 네트워크(RR)의 운영자가 단말기(T)와 연관된 칩 카드(CP)의 제어를 유지하고 칩 카드의 내용을 수정하는 것을 가능하게 한다. 운영자가 주도하는 이러한 동작들은 예를 들어, 운영자에 의해 관리되는 장비에서 카드(CP)와 같은 칩 카드들로의 파일, 구체적으로 멀티미디어 파일의 다운로딩, 및 파일 또는 소정의 애플리케이션에서 적어도 카드(CP)로의 파일의 다운로딩 또는 삭제 또는 수정과 관련된다.

<33> 메모리(ME)는 암호화 알고리즘(A1), 해독 알고리즘(A2), 인증 키(KA) 및 세션 키 결정 알고리즘(A3)을 포함한다. 알고리즘(A3)은 세션 키(KS)를 결정하며, 이어서 이 키는 메모리(ME)에 저장된다.

<34> 통신 인터페이스(IC)는 적어도 무선 통신 네트워크(RR)를 통해 데이터를 송수신한다.

<35> 데이터베이스(BD)는 특히, 멀티미디어 데이터일 수 있는 데이터(D), 및 칩 카드(CP)의 다양한 파라미터 및 특성을 포함한다.

<36> 칩 카드(CP)는 높은 저장 용량을 갖는 최신의 접촉 기반 또는 무접촉 칩 카드이다. 도 1에 도시된 바와 같이, 칩 카드는 2개의 특성 논리 유닛을 포함한다. 보안 유닛(US)으로 참조되는 제1 유닛은 보안 제어기(CS)라고 하는 제1 제어기, 및 보안 메모리(MS)라고 하는 제1 메모리를 포함한다. 대용량 메모리 유닛(UM)으로 참조되는 제2 유닛은 대용량 메모리 제어기(CM)라고 하는 제2 제어기, 및 상당한 저장 공간을 필요로 하는 멀티미디어 데이터와 같은 데이터를 저장하는 대용량 메모리(MM)라고 하는 제2 메모리를 포함한다. 바람직하게, 보안 제어기 및 대용량 메모리 제어기는 공통 물리 컴포넌트 내의 논리 모듈들이다. 다른 예에 따르면, 제어기들은 서로 접속된 개별 물리 컴포넌트들 내에 집적된다. 메모리들(MM, MS)에 대한 액세스들은 개별적이며, 제어기들(CS, CM)에 의해 각각 제어된다. 예를 들어, 보안 유닛(US) 또는 보다 구체적으로 보안 제어기(CS)는 유닛(UM)의 대용량 메모리(MM)에 데이터를 기입할 수 없다. 마찬가지로, 대용량 메모리 제어기(CM)는 유닛(US)의 보안 메모리(MS)에 데이터를 기입할 수 없다.

<37> 대용량 메모리 유닛(UM)은 대용량 메모리(MM)에 멀티미디어 데이터를 기입하거나 판독하거나 삭제하도록 대용량 메모리 제어기(CM)에게 지시하는 단말기(T)에 의해 전적으로 제어되는데, 이는 보안 제어기(CS)가 대용량 메모리(MM)에 기입하는 것을 방지한다. 대용량 메모리 유닛(UM)은 USB(Universal Serial Bus) 키 또는 플래시 메모리 카드 또는 보안 디지털 카드 또는 MMC 타입의 멀티미디어 카드와 유사할 수 있는 기능들 및 구조를 갖는다.

<38> 본 발명의 바람직한 실시예에 따르면, 보안 유닛(US)의 보안 제어기(CS)는 관련 단말기(T)가 GSM 또는 GPRS 타입의 이동 단말기일 경우의 SIM 애플리케이션, 또는 UMTS(Universal Mobile Telecommunications System) 또는 UTRAN(UMTS Terrestrial Radio Access Network) 타입의 제3 세대(3GPP) 또는 CDMA 2000 타입의 제3 세대(3GPP2)의 CDMA(Code Division Multiple Access)에서 동작하는 이동 단말기와 연관된 USIM, RUIM(Romovable User Identity Module) 또는 ISIM(IP Subscriber Identity Module) 애플리케이션이다. 보안 유닛(US)은 단말기(T)를 통해 투명한 방식으로 데이터를 전송하기 위해 원격 서버(S)와의 OTA 타입의 통신 채널을 공지 방식으

로 설정할 수 있다.

<39> 보안 유닛(US)은 대용량 메모리 유닛(UM)의 "보안 록(lock)"을 구성하며, 공유 인증 키(KA)에 의한 서버(S)와 보안 유닛((US) 간의 인증의 함수로서 대용량 메모리 유닛(UM)에 대한 액세스를 허가하거나 금지한다. 보안 유닛은 서버(S)와 단말기(T) 또는 칩 카드(CP) 사이에서 암호화된 형태로, 따라서 보안 방식으로 전송되는 데이터(D)를 암호화하고 해독하는 데 필요한 세션 키(KS)를 결정한다.

<40> 도 2를 참조하면, 칩 카드(CP)의 마이크로 제어기는 하나의 프로세서(PC) 또는 복수의 프로세서, 및 3개의 메모리(MC1 내지 MC3)를 포함한다. 카드는 단말기(T)로부터 커맨드들 또는 요청들을 수신하며, 응답들을 입출력 포트(PES)를 통해 단말기(T)로 전송한다.

<41> 메모리(MC1)는 ROM 또는 플래시 타입이며, 카드의 운영 체제, 암호화 알고리즘(A1), 해독 알고리즘(A2) 및 세션 키(KS)를 결정하기 위한 알고리즘(A3)을 포함한다. 메모리(MC1)는 또한, 보안 유닛(US)의 보안 제어기(CS) 및 대용량 메모리 유닛(UM)의 대용량 메모리 제어기(CM)를 포함한다.

<42> 메모리(MC2)는, 특히 인증 키(KA), 일단 결정된 세션 키(KS), PIN 코드 및 다른 보안 데이터와 같은, 카드를 소유하는 사용자의 프로파일의 식별 번호들 및 다른 파라미터들을 저장하기 위한, 예를 들어 EEPROM 또는 플래시 타입의 비휘발성 메모리이다. 메모리(MC2)는 보안 유닛에 의해서만 액세스될 수 있다.

<43> 하나의 변형으로서, 보안 메모리(MS)는 메모리(MC2)의 내용을 포함한다.

<44> 메모리(MC3)는 보다 구체적으로 데이터를 처리하기 위해 기능하는 RAM 또는 SRAM 메모리이다.

<45> 대용량 메모리(MM)는 서버(S)와 교환되는 멀티미디어 데이터를 저장한다.

<46> 도 6의 후속 설명에 관련된 변형에 따르면, 대용량 메모리 제어기(CM)는 암호화 알고리즘(A1) 및 해독 알고리즘(A2)을 포함한다.

<47> 카드 내의 프로세서(P), 메모리(ROM), 보안 제어기(CS), 메모리들(MC2, MC3), 보안 메모리(MS) 및 포트(PES)는 양방향 보안 버스(BS)에 의해 서로 접속된다. 마찬가지로, 카드 내의 프로세서(P), 메모리(ROM), 대용량 메모리 제어기(CM), 메모리(MC3), 대용량 메모리(MM) 및 포트(PES)는 양방향 버스(BM)에 의해 서로 접속된다. 도 2에 도시된 카드의 실시예에 따르면, 2개의 제어기(CS, CM)는 하나의 동일한 물리 컴포넌트 내에 집적된다.

<48> 단말기(T)는 프로세서(PT), 메모리들(MT), 무선 인터페이스(IR) 및 칩 카드(CP)의 포트(PES)와 통신하기 위한 카드 판독기(LT)를 포함한다. 단말기의 다양한 요소는 양방향 버스(BT)에 의해 서로 접속된다.

<49> 메모리들(MT)은 3개의 메모리(MT1, MT2, MT3)를 포함한다. 메모리(MT1)는 ROM 또는 플래시 타입이며, 단말기(T)의 운영 체제를 포함한다. 메모리(MT2)는 예를 들어 EEPROM 또는 플래시 타입의 비휘발성 메모리이며, 특히 도 5의 후속 설명에 관련된 변형에 따르면 암호화 알고리즘(A1) 및 해독 알고리즘(A2)을 포함할 수 있다. 메모리(MT3)는 보다 구체적으로, 데이터를 처리하도록 기능하는 RAM 또는 SRAM 메모리이다.

<50> 단말기(T)는 본 발명과 더 관련하여, 메모리들(MT1, MT2)에 분산된 소프트웨어 에이전트일 수 있는 에이전트(AG)를 포함한다. 에이전트(AG)는 서버(S)와 칩 카드(CP)의 유닛들(US, UM) 사이의 중간 컴퓨터 도구이다. 에이전트(AG)의 역할은 전송되는 데이터, 특히 멀티미디어 데이터를 서버와 카드의 보안 유닛(US)의 제어기(CS) 사이에서, 또는 서버와 카드의 대용량 메모리 유닛(UM)의 제어기(CM) 사이에서 라우팅하는 것이다. 소프트웨어 에이전트(AG)는 카드의 2개의 유닛(US, UM) 중 하나에 액세스하기 위해 이롭게도 에이전트(AG)하고만 대화하는 원격 서버(S)와의 OTA 타입의 단일 통신 채널(CDC)을 설정한다. 따라서, 서버는 단말기와의 단일 통신 프로토콜만을 관리한다.

<51> 에이전트(AG)는 또한, 서버와 칩 카드와 연관된 단말기 간의 인증에 관한 문제들을 담당한다.

<52> 다른 예들에 따르면, 단말기(T)는 칩 카드와 통신할 수 있는 임의의 단말기로 대체되며, 메시지들을 전송하기 위한 휴대형 장치, 또는 칩 카드 판독기를 구비한 개인용 컴퓨터(PC), 또는 차변 또는 대변 칩 카드를 수납하는 은행 단말기와 같은 고정 단말기일 수 있다. 이어서, 네트워크(RR)는 예를 들어 인트라넷, 무선 로컬 네트워크 또는 인터넷에 결합될 수 있다.

<53> 에이전트(AG)는 칩 카드와 연관된 이동 단말기에 접속되는 개인용 컴퓨터 내에 통합될 수도 있다.

<54> 데이터는 HTTP(HyperText Transfer Protocol) 타입의 프로토콜(P1) 또는 임의의 다른 타입의 TCP/IP(Transmission Control Protocol/Internet Protocol) 기반 프로토콜에 따라, 또는 변형으로서

APDU(Application Protocol Data Unit) 커맨드들에 기초하는 사용 ISO-7816에 의해 정의되는 프로토콜에 따라 에이전트(AG)와 보안 유닛(US) 사이에 전송된다. 데이터는 MMC 타입의 프로토콜(P2)에 따라 에이전트(AG)와 대용량 메모리 유닛(UM) 사이에 전송된다.

<55> 에이전트(AG)와 서버(S) 간의 통신을 위한 프로토콜은 요청들 및 응답들에 기초한다. 예를 들어, 에이전트(AG)는 서버의 데이터베이스(BD)에 저장된 데이터를 검색하기 위해 서버에 요청을 전송한다. 요청은 보안 유닛 또는 단말기의 사용자로부터의 보다 이른 요청과 관련되며, 요청된 데이터가 데이터베이스에 저장되어 있는 URI(Unified Resource Identifier) 저장 어드레스, 및 데이터의 속성들을 나타내는 정보를 포함한다. 요청에 응답하여, 서버는 데이터의 속성들을 나타내는 정보 및 데이터가 카드 내에서 저장되어야 하는 2개의 유닛(US, UM) 중 하나에 관한 식별자(IU)를 동반하는 데이터를 전송한다. 에이전트(AG)는 수신된 정보를 분석하고, 이들이 향하는 유닛에 따라 데이터를 특유하게 처리한다. 데이터가 보안 유닛으로 향하는 경우, 에이전트는 데이터를 프로토콜 P1을 통해 보안 제어기로 전송하며, 이어서 보안 제어기는 데이터를 처리한다. 데이터가 대용량 메모리 유닛으로 향하는 경우, 에이전트는 프로토콜 P2를 통해 유닛(UM)의 대용량 메모리(MM) 내의 데이터의 기입, 판독 또는 삭제를 지시한다.

<56> 에이전트와 서버 사이에서 2개의 통신 모드가 고려된다.

<57> 제1 통신 모드에 따르면, 데이터에 관한 URI 어드레스를 포함하는 요청이 에이전트(AG)에 의해 미리 전송되고, 요청에 응답하여, 요청된 데이터가 서버(S)에 의해 에이전트(AG)로 전송되며, 에이전트는 데이터를 카드의 2개의 유닛(US, UM) 중 하나로 라우팅한다.

<58> 제2 모드에서는, 데이터가 서버로부터 에이전트(AG)로 다운로드되며, 에이전트는 다운로드된 데이터를 카드의 2개의 유닛(US, UM) 중 하나로 라우팅한다. 에이전트(AG)는 데이터가 다운로드되어야 하는지를 나타내는 요청을 서버로 전송함으로써 다운로드를 개시한다. 이에 응답하여, 서버(S)는 다운로드될 데이터가 저장되는 URI 어드레스들을 전송한다. 전송된 각각의 URI 어드레스에 대해, 에이전트(AG)는 URI 어드레스를 포함하는 요청을 서버로 전송한다. 이에 응답하여, 서버는 데이터베이스로부터 판독되고, 전송된 URI 어드레스에 의해 지정되는 요청된 데이터를 전송한다.

<59> 도 3 및 4와 관련된 본 발명에 따른 방법의 일 실시예는 보다 구체적으로는 서버(S)에 의해 제1 통신 모드에 따라 칩 카드의 유닛들(UM, US) 중 하나로 제공되는 데이터(D)의 갱신에 관련된다.

<60> 도 3을 참조하면, 본 발명에 따른 방법의 일 실시예는 원격 서버(S)에서 유닛들(UM, US) 중 하나로의 데이터 전송들을 관리하기 위한 단계들(E0 내지 E11)을 포함한다.

<61> 최초 단계 E0에서, 단말기(T)의 에이전트(AG)는 예를 들어, 칩 카드의 메모리들(MM, MS) 중 하나에서 데이터(D)의 갱신을 트리거하기 위해 서버(S)에 의해 전송되는 푸시 모드(push mode)의 쇼트 메시지(short message)에 응답하여, 무선 통신 네트워크(RR)를 통한 서버(S)와의 통신 채널(CDC)의 설정을 지시한다. 에이전트(AG)와 서버(S) 간의 모든 전송은 단말기의 무선 인터페이스(IR) 및 서버(S)의 통신 인터페이스(IC)를 통해 각각 실행된다.

<62> 단계 E1에서, 에이전트(AG)는 서버의 데이터베이스(BD)에 저장되는 검색될 데이터를 식별하는 URI 어드레스를 포함하는 요청(RQ)을 서버로 전송한다.

<63> 단계 E2에서, 서버(S)의 관리자(GE)는 데이터(D) 및 데이터가 향하는 카드의 유닛(US 또는 UM)을 나타내는 식별자(IU)를 포함하는 응답을 에이전트(AG)로 전송한다. 단계 E3에서, 에이전트(AG)는 식별자(IU)와 유닛들(US 또는 UM)의 식별자들을 비교한다.

<64> 식별자(IU)가 대용량 메모리 유닛(UM)의 식별자에 대응하는 경우, 에이전트(AG)는 단계 E4에서 데이터(D)를 처리하여, 데이터(D)를 대용량 메모리(MM)에 기입하라는 커맨드와 함께 데이터(D)를 유닛(UM)의 대용량 메모리 제어기(CM)로 적절히 전송한다. 단계 E5에서, 제어기(CM)는 데이터(D)를 대용량 메모리(MM)에 기입한 후, 통지(NTF)를 단말기의 에이전트(AG)로 전송하여, 수행된 기입 동작의 올바르거나 올바르지 않은 상태를 보고한다.

<65> 대용량 메모리(MM)에 대한 기입이 올바르지 않은 경우, 에이전트(AG)는, 서버(S)가 카드 관리자 서버일 때, 데이터베이스(BD) 및 대용량 메모리에 저장된 데이터 간의 검사를 수행하기 위해 데이터를 복원한다.

<66> 단계 E3에서 식별자(IU)가 보안 유닛(US)의 식별자에 대응하는 경우, 에이전트는 단계 E7에서 프로토콜 P1을 통해 데이터(D)를 보안 유닛(US)으로 전송한다. 보안 제어기(CS)는 단계 E8에서 예를 들어 데이터(D)를 보안 메모리(MS)에 기입함으로써 데이터(D)를 처리한다. 이어서, 보안 제어기는 단계 E9에서 통지(NTF)를 단말기의 에

이전트(AG)로 전송하여, 수행된 전송의 올바르거나 올바르지 않은 상태를 보고한다.

<67> 단계 E10에서, 에이전트(AG)는 수신의 확인(AR)을 서버(S)로 전송하며, 서버는 단계 E11에서 확인(AQ)으로 그에 응답한다.

<68> 도 4에 도시된 본 발명의 방법의 일 변형 실시예에 따르면, 방법은 전술한 단계들(E0와 E1) 사이에 삽입되는 인증 단계(EA)를 포함한다. 인증 단계는 서버(S)와 칩 카드의 보안 유닛(US) 간의 인증에 관련되며, 단계들(EA1 내지 EA12)을 포함한다. 먼저, 대용량 메모리 유닛(UM)에 대한 액세스가 보안 유닛(US)에 의해 록킹되며, 보안 유닛(US)은 인증의 결과에 따라 이러한 액세스의 개시를 허가하거나 금지한다. 이러한 보안 유닛에 의한 대용량 메모리 유닛의 액세스의 록킹 또는 언록킹이 가능한 이유는 2개의 유닛의 2개의 제어기(CS, CM)가 도 2에 도시된 바와 같은 하나의 동일 물리 컴포넌트의 일부를 구성하거나, 서로 접속된 2개의 개별 물리 컴포넌트의 일부를 구성하기 때문이다.

<69> 단계 EA1에서, 단말기(T)의 에이전트(AG)는 난수(RND)를 얻기 위한 요청(RQ_RND)을 칩 카드의 보안 유닛(US)으로 전송한다. 보안 유닛(US)은 단계 EA2에서 난수(RND1)를 생성하고, 단계 EA3에서 이를 에이전트(AG)로 전송한다. 에이전트는 단계 EA4에서 난수(RND1)를 서버(S)의 관리자(GE)로 전송한다. 관리자(GE)는 인증 키(KA)에 종속하는 암호화 알고리즘(A1)을 난수에 적용하여 난수(RND1)를 암호화하여, 암호화된 제1 난수(RND1C)를 생성한다.

<70> 반대로, 단계 EA5에서, 관리자(GE)는 제2 난수(RND2)를 생성한다. 단계 EA6에서, 암호화된 제1 난수(RND1C) 및 제2 난수(RND2)는 옵션으로서, 보안 유닛을 지시하는 식별자(IU)와 함께, 단말기의 에이전트(AG)로 전송되며, 에이전트는 단계 EA7에서 식별자(IU)를 검증하고, 난수들을 보안 유닛(US)으로 라우팅한다. 단계 EA8에서, 보안 유닛(US)은 암호화 알고리즘(A1)의 역이고 보안 유닛에 저장된 인증 키(KA)에 종속하는 해독 알고리즘(A2)을 수신된 난수에 적용하여 수신된 난수(RND1C)를 해독한다. 보안 유닛은 해독된 난수와 단계 EA2에서 생성된 난수(RND1)를 비교한다. 2개의 난수가 동일한 경우, 보안 유닛에 의한 서버의 인증이 확인되며, 보안 유닛의 보안 제어기는 서버에 의한 소프트웨어 에이전트(AG)를 통한 대용량 메모리 유닛(UM)의 액세스를 허가한다. 2개의 난수가 동일하지 않은 경우, 대용량 메모리 유닛에 대한 액세스는 록킹 상태로 유지되며, 보안 유닛은 단계들 EA2 내지 EA8을 재개하기 위하여 서버로 전송할 새로운 난수를 생성한다.

<71> 보안 유닛에 의한 서버의 간단한 인증을 위해, 인증 단계는 단계 EA8에서 중지되며, 방법은 단말기가 데이터(D)를 수신하는 단계 E1에서 계속된다.

<72> 보안 유닛과 서버 간의 상호 인증을 위해, 보안 유닛(US)이 단계 EA5에서 서버(S)의 관리자(GE)에 의해 생성된 제2 난수(RND2)를 암호화하는 단계 EA9가 단계 EA8에 이어진다. 보안 유닛은 관리자(GE)에서의 암호화 알고리즘과 동일하고 인증 키(KA)에 종속하는 암호화 알고리즘(A1)을 난수(RND2)에 적용한다. 이어서, 단계 EA10에서, 보안 유닛은 암호화된 제2 난수(RND2C)를 에이전트(AG)로 전송하며, 단계 EA11에서 에이전트는 이를 관리자(GE)로 전송한다.

<73> 단계 EA12에서, 관리자(GE)는 보안 유닛에서의 해독 알고리즘과 동일하고 인증 키(KA)에 종속하는 해독 알고리즘(A2)을 난수에 적용하여 난수(RND2C)를 해독한다. 관리자(GE)는 해독된 난수와 단계 EA5에서 생성된 난수(RND2)를 비교한다. 2개의 난수가 동일한 경우, 상호 인증이 확인되며, 방법은 단말기가 데이터(D)를 수신하는 단계 E1에서 계속된다. 동일하지 않은 경우, 관리자는 단계 EA5 내지 EA12를 재개하기 위해 보안 유닛으로 전송될 새로운 난수를 생성한다.

<74> 서버(S)와 대용량 메모리 유닛(UM) 간의 멀티미디어 데이터(D)의 보안 전송에 관한 두 가지 변형이 도 5 및 6에 각각 도시되어 있다.

<75> 도 5를 참조하면, 본 발명의 방법은 단계들 F0 내지 F14를 포함한다. 단계 F0는 도 3을 참조하여 설명된 최초 단계 E0와 유사한 최초 단계이며, F0에 이어지는 단계 FA는 도 4를 참조하여 설명된 인증 단계(EA)와 유사하다.

<76> 서버(S)의 관리자(GE) 및 보안 유닛(US)의 보안 제어기(CS)에 의해 각각 수행되는 단계들 F1 및 F2에서, 교환된 난수들(RND1, RND2) 및 인증 키(KA)를 알고리즘(A3)에 적용함으로써 세션 키(KS)가 결정된다. 키(KS)는 서버의 메모리(ME)에, 그리고 칩 카드(CP)의 메모리(MC2 또는 MS)에 저장된다.

<77> 단계 F3에서, 에이전트(AG)는 서버의 데이터베이스(BD)에 저장되는 검색될 데이터를 식별하는 URI 어드레스를 포함하는 요청(RQ)을 서버로 전송한다.

<78> 단계 F4에서, 관리자(GE)는 URI 어드레스에 따라 데이터베이스에서 멀티미디어 데이터(D)를 검색하고, 단계들

EA5 및 EA9에서 이용된 것과 동일하거나 동일하지 않을 수 있고 단계 F1에서 결정된 세션 키(KS)에 종속하는 암호화 알고리즘(A1)을 적용하여 이들을 암호화함으로써 암호화된 멀티미디어 데이터(DC)를 생성한다. 단계 F5에서, 이 데이터는 에이전트(AG)로 전송되며, 유닛(UM)을 지시하는 식별자(IU)를 또한 포함하는 응답(REP)에 포함된다.

<79> 단계 F6에서, 에이전트(AG)는 암호화된 데이터(DC)를 수신하고, 데이터(DC)를 해독하는 데 필요한 세션 키(KS)를 얻기 위해 요청(RQ_KS)을 보안 유닛(US)으로 전송한다. 단계 F7에서, 보안 유닛은 단계 F2에서 결정된 키(KS)에 대해 메모리(MC2) 또는 보안 메모리(MS)를 검색하여, 단계 F8에서 이를 에이전트(AG)로 전송한다.

<80> 단계 F9에서, 에이전트(AG)는 단계 EA8 및 EA12에서 사용된 것과 동일하거나 동일하지 않을 수 있고 전송된 키(KS)에 종속하는 해독 알고리즘(A2)을 적용하여 데이터(DC)를 해독함으로써, 해독된 멀티미디어 데이터(D)를 생성한다. 데이터(D)를 해독하기 위한 이러한 변형에서, 알고리즘(A2)은 단말기(T)의 메모리(MT2)에 저장된다.

<81> 이어서, 데이터(D)는 도 3을 참조하여 설명된 단계들 E4 내지 E6 및 E10 및 E11과 유사한 방식으로 단계들 F10 내지 F14에서 처리된다.

<82> 도 6을 참조하면, 서버(S)와 대용량 메모리 유닛(UM) 간의 멀티미디어 데이터(D)의 보안 전송을 위한 다른 변형에 따른 방법은 단계들 G0 내지 G14를 포함한다.

<83> 단계들 G0 내지 G5는 전술한 단계들 F0 내지 F5와 유사하다.

<84> 단계 G6에서, 에이전트(AG)는 암호화된 멀티미디어 데이터(DC)를 동반하는 데이터(DC) 기입 커맨드를 대용량 메모리 유닛(UM)으로 전송한다.

<85> 단계 G7에서, 대용량 메모리 제어기(CM)는 세션 키(KS)를 얻기 위해 요청(REQ_KS)을 보안 유닛으로 전송한다. 요청의 전송은 제어기(CM)와 제어기(CS) 사이에서 소프트웨어를 통해 설정되는데, 이는 2개의 제어기가 공통 물리 컴포넌트 내의, 또는 서로 접속되는 2개의 개별 물리 컴포넌트 내의 논리 모듈들이기 때문이다.

<86> 단계 G8에서, 보안 유닛(US)은 단계 G2에서 결정된 키(KS)에 대해 메모리(MC2) 또는 보안 메모리(MS)를 검색하고, 단계 G9에서 이를 대용량 메모리 유닛(UM)으로 전송한다.

<87> 단계 G10에서, 대용량 메모리 제어기(CM)는 단계들 EA8 및 EA12에서 사용된 것과 동일하거나 동일하지 않을 수 있고 전송된 키(KS)에 종속하는 해독 알고리즘(A2)을 적용하여 데이터(DC)를 해독함으로써 해독된 멀티미디어 데이터(D)를 생성한다. 데이터(D)를 해독하기 위한 이러한 변형에서, 알고리즘(A2)은 유닛(UM)의 대용량 메모리 제어기(CM)에 저장된다.

<88> 이어지는 단계들 G11 내지 G13은 도 3을 참조하여 설명된 단계들 E4 내지 E6과 동일하다.

<89> 전술한 실시예와 반대로, 대용량 메모리에 원격 액세스하기 위한 방법의 다른 실시예는 서버(S)의 데이터베이스(BD) 내의 멀티미디어 데이터의 갱신과 관련되는데, 이 데이터는 유닛(UM)의 대용량 메모리로부터 유래된다. 이러한 다른 실시예에서, 암호화되거나 암호화되지 않은 데이터를 서버에 접속된 데이터베이스(BD)에 저장하기 위해 서버로 전송하는 것은 에이전트(AG)이다. 예를 들어, 에이전트(AG)는 사진들을 포함하고 대용량 메모리에 저장되는 전화 번호부를 전송하며, 이는 칩 카드의 사용자가 칩 카드를 갱신하거나 분실한 후에 그의 모든 지인(contact)을 검색하는 것을 가능하게 한다.

<90> 이러한 다른 실시예에서, 멀티미디어 데이터는 데이터의 보안 전송을 위한 두 가지 변형 중 하나에 따라 단말기의 에이전트(AG)에 의해 또는 대용량 메모리 제어기(CM)에 의해 해독 대신 암호화된다. 이러한 두 가지 변형에서, 멀티미디어 데이터를 암호화하는 엔티티(AG, CM)는 데이터를 암호화하는 데 필요한 세션 키(KS)를 얻기 위해 요청(RQ_KS, REQ_KS)을 보안 유닛(US)으로 전송한다.

<91> 본 발명은 전기 통신 분야로 한정되지 않는다. 휴대형 통신 객체는 USB 키의 보안 유닛에 의해 보안 액세스가 관리되는 USB 키의 대용량 메모리에 저장된 비밀 데이터를 교환하기 위한 USB 키일 수 있다.

<92> 휴대형 통신 객체는 카드를 소지하는 환자에 대한 디지털 X 레이들 또는 분석 보고서들을 포함하는 대용량 메모리 유닛을 포함하는 건강 카드일 수 있으며, 이러한 멀티미디어 데이터는 보안 유닛에 의해 관리되는 건강 카드의 인증 후에 카드에 액세스하는 건강 전문가들 사이에 교환된다.

<93> 저작권 보호의 분야에서, 휴대형 통신 객체는 보안 유닛에 의해 액세스 권리가 관리되는 필름, 비디오 클립 또는 문학 작품에 관한 멀티미디어 데이터를 그의 대용량 메모리에 포함할 수 있다.

<94> 본 발명은 예를 들어 이전에 수행되어 대용량 메모리에 기록된 거래들의 주기적이고 안전한 전송을 위해 은행 업무 분야에도 적용될 수 있다.

<95> 본 발명의 제1 이용에 따르면, 멀티미디어 애플리케이션은 여러 컴포넌트로 분할된다. 각각의 애플리케이션 컴포넌트는 그의 특성의 함수로서 저장된다. 어떠한 특정 보안도 필요로 하지 않는 컴포넌트들은 단말기에 저장된다. 높은 레벨의 보안 및 제한된 메모리 공간을 필요로 하는 애플리케이션 컴포넌트들은 보안 유닛에 저장된다. 큰 메모리 공간 및 보안 유닛에 의해 관리되는 보안 레벨을 필요로 하는 애플리케이션 컴포넌트들은 대용량 메모리에 저장된다.

<96> 제1 이용에 관한 제1 예에 따르면, 멀티미디어 전화 번호부 애플리케이션은 2개의 애플리케이션 컴포넌트, 즉 보안 유닛에 저장되는 지인들의 이름들 및 전화 번호들, 및 대용량 메모리 유닛에 저장되는 지인들의 사진들로 분할될 수 있다.

<97> 따라서, 휴대형 통신 객체가 보안 방식으로 대용량 메모리에 액세스하는 것을 가능하게 하는 에이전트를 포함하지 않는 단말기에 접속되는 경우, 사용자는 보안 유닛에 포함된 지인들의 이름들 및 전화 번호들에 통상의 방식으로 액세스할 수 있을 것이다.

<98> 제1 이용의 제2 예에 따르면, 다른 타입의 멀티미디어 애플리케이션은 다음과 같은 컴포넌트들, 즉 멀티미디어 애플리케이션의 표시를 관리하는 관리 엔진, 애플리케이션의 코어이고, 제어된 액세스 및 높은 레벨의 보안을 필요로 하는 애플리케이션 로직, 및 빠른 액세스를 필요로 하는 멀티미디어 데이터를 포함할 수 있다. 따라서, 관리 엔진은 단말기에 저장되고, 애플리케이션 로직은 보안 유닛에 저장되며, 멀티미디어 데이터는 대용량 메모리 유닛의 대용량 메모리에 저장된다.

<99> 이러한 애플리케이션의 일례는 비디오 게임이다. 게임의 사람/기계 인터페이스는 단말기에 의해 관리된다. 예를 들어 스코어를 계산하고, 얻어진 스코어에 따라 하나의 배경에서 다른 배경으로 변경하는 것 등을 위해 기능하는 게임 로직은 보안 유닛에 저장된다. 배경, 캐릭터 등을 표시하는 데 필요한 멀티미디어 데이터는 대용량 메모리에 저장된다.

<100> 본 발명의 제2 이용에 따르면, 무선 통신 네트워크 운영자는 휴대형 통신 객체가 사용자에게 전달되기 바로 전에 사용자의 프로파일의 함수로서 휴대형 통신 객체의 멀티미디어 개인화를 종료한다. 이러한 이용은 운영자의 휴대형 통신 객체들의 재고들에 대한 보다 정확한 관리를 가능하게 한다. 예를 들어, 휴대형 통신 객체가 전달될 때, 운영자의 서버(S)는 가입자의 프로파일에 대응하는 멀티미디어 콘텐츠를 대용량 메모리에 저장하기 위해 이를 전송한다. 다른 예에 따르면, 대용량 메모리는 공장에서의 휴대형 통신 객체의 제조시에 다양한 사용자 프로파일의 멀티미디어 콘텐츠를 포함한다. 휴대형 통신 객체의 전달에 앞서, 사용자 프로파일에 따라 하나의 콘텐츠가 선택되고, 다른 콘텐츠들은 삭제된다.

<101> 본 발명의 다른 실시예에 따르면, 서버(S)는 직렬 접속 또는 USB 접속 타입의 유선 접속을 통해, 또는 블루투스, WIFI, 적외선(IrDA: Infrared Data Association) 또는 지그비 타입의 무선 접속을 통해 단말기(T)에 접속되는 개인용 컴퓨터(PC)일 수 있다.

<102> 본 발명의 또 다른 실시예에 따르면, 개인용 컴퓨터(PC)는 서버와 단말기 간의 게이트웨이로서 기능한다. 서버(S)는 인터넷 타입의 통신 네트워크를 통해 컴퓨터와 통신하고, 컴퓨터는 블루투스, WIFI, 적외선(IrDA: Infrared Data Association) 또는 지그비 타입의 무선 접속을 통해 단말기와 통신한다.

<103> 여기에 설명되는 본 발명은 서버(S)가 무선 통신 네트워크(RR)를 통해 휴대형 통신 객체(CP) 내의 멀티미디어 데이터를 저장할 수 있는 대용량 메모리(MM) 및 보안 메모리에 단일 통신 채널을 통해 원격 액세스할 수 있도록 하는 휴대형 통신 객체(CP)와 연관된 방법 및 단말기(T)에 관한 것이다. 바람직한 일 실시예에 따르면, 본 발명의 방법의 단계들은 특히 단말기에 포함된 컴퓨터 프로그램의 명령들에 의해 결정된다. 프로그램은, 프로그램이 단말기에 로딩되어 실행되고, 이어서 단말기의 동작이 프로그램의 실행에 의해 제어될 때,

<104> 원격 서버와 휴대형 통신 객체의 메모리들 중 하나 또는 다른 하나 사이의 데이터 전송들을 라우팅하기 위한 단말기 내의 에이전트를 제공하는 단계;

<105> 원격 서버와 단말기 내의 에이전트 사이에 통신 채널을 설정하는 단계;

<106> 서버 및 휴대형 통신 객체의 메모리들 중 하나를 포함하는 2개의 요소 중 하나에서 단말기 내의 에이전트로 데이터를 전송하는 단계; 및

<107> 에이전트가 전송된 데이터를 2개의 요소 중 다른 하나로 전송하도록, 에이전트로 전송된 데이터를 처리하는 단계

<108> 를 포함하는 본 발명에 따른 방법의 단계들을 수행하는 프로그램 명령들을 포함한다.

<109> 결과적으로, 본 발명은 컴퓨터 프로그램, 특히 본 발명을 구현하는 데 적합한 데이터 매체 상의 또는 데이터 매체 내의 컴퓨터 프로그램에도 적용된다. 이러한 프로그램은 임의의 프로그래밍 언어를 이용할 수 있으며, 소스 코드 형태, 객체 코드 형태, 또는 부분적으로 컴파일된 형태, 또는 본 발명에 따른 방법을 구현하는 데 바람직한 임의의 다른 형태 등의 소스 코드와 객체 코드의 중간 코드 형태일 수 있다.

도면의 간단한 설명

<21> 도 1은 휴대형 통신 객체, 단말기 및 서버를 접속하는 본 발명의 바람직한 일 실시예에 따른 통신 시스템의 개략 블록도.

<22> 도 2는 도 1에 관한 보다 상세한 개략 블록도.

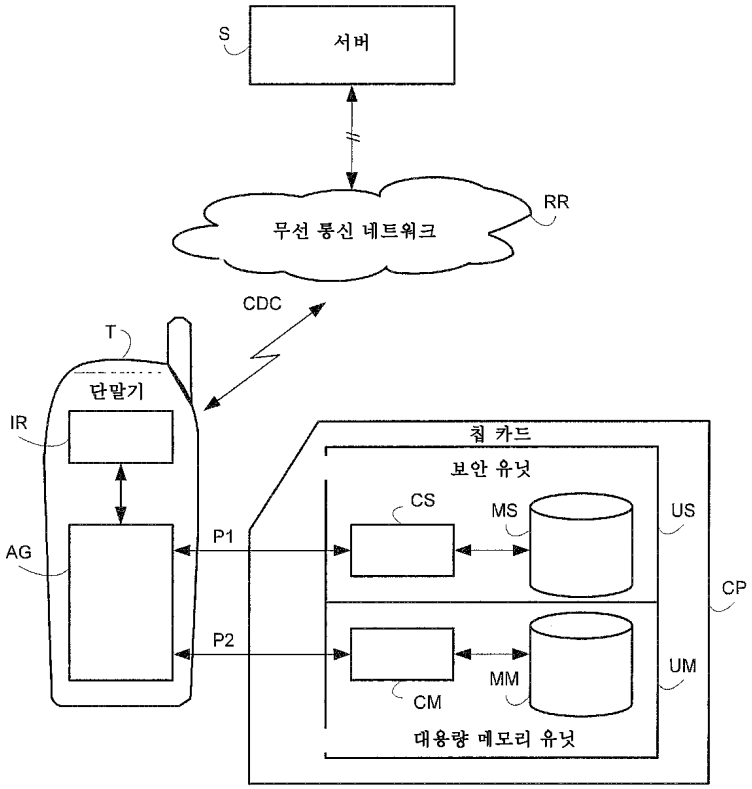
<23> 도 3은 본 발명에 따른 휴대형 통신 객체의 대용량 메모리 유닛 및 보안 유닛에 원격 액세스하는 방법의 알고리즘을 나타내는 도면.

<24> 도 4는 본 발명에 따른, 높은 기억 용량을 갖는 휴대형 통신 객체의 대용량 메모리에 대한 액세스를 허가하는 알고리즘을 나타내는 도면.

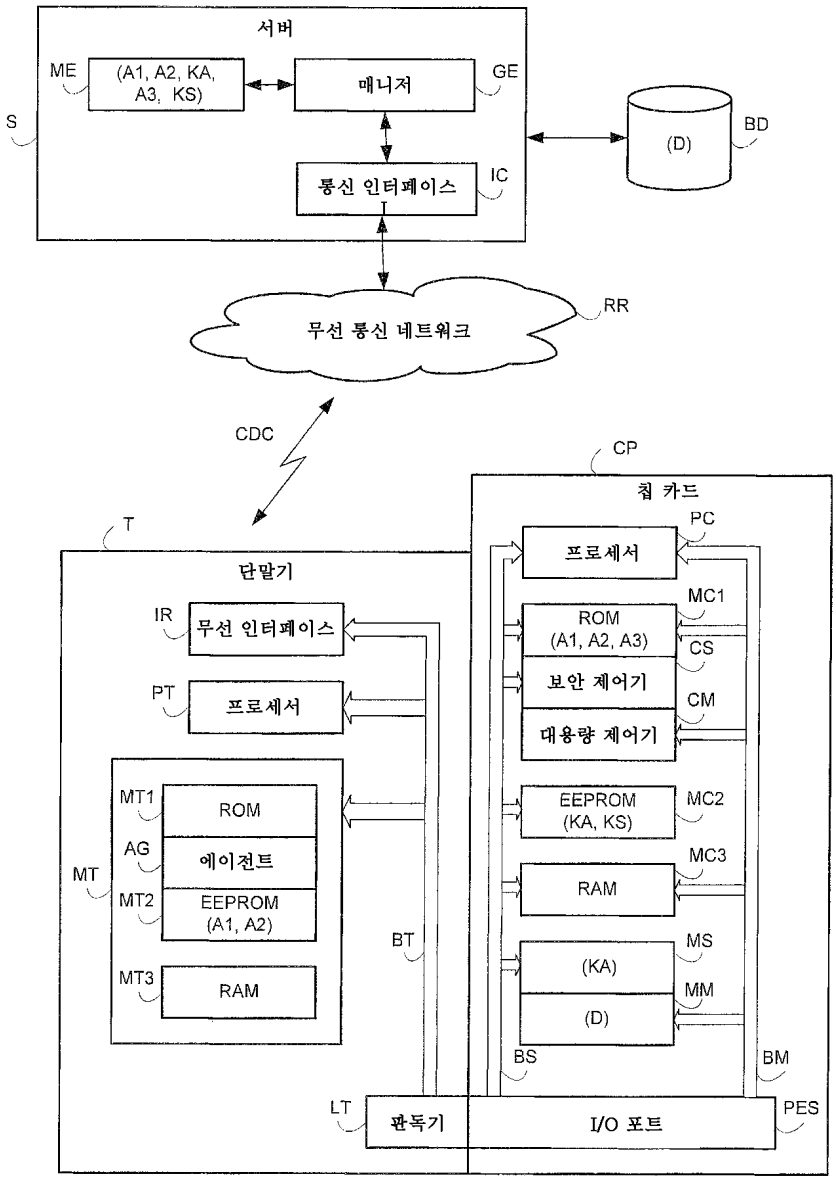
<25> 도 5 및 도 6은 2개의 변형 실시예 각각에 따른, 서버와 휴대형 통신 객체의 대용량 메모리 유닛 간의 보안 데이터 전송을 위한 알고리즘들을 나타내는 도면.

도면

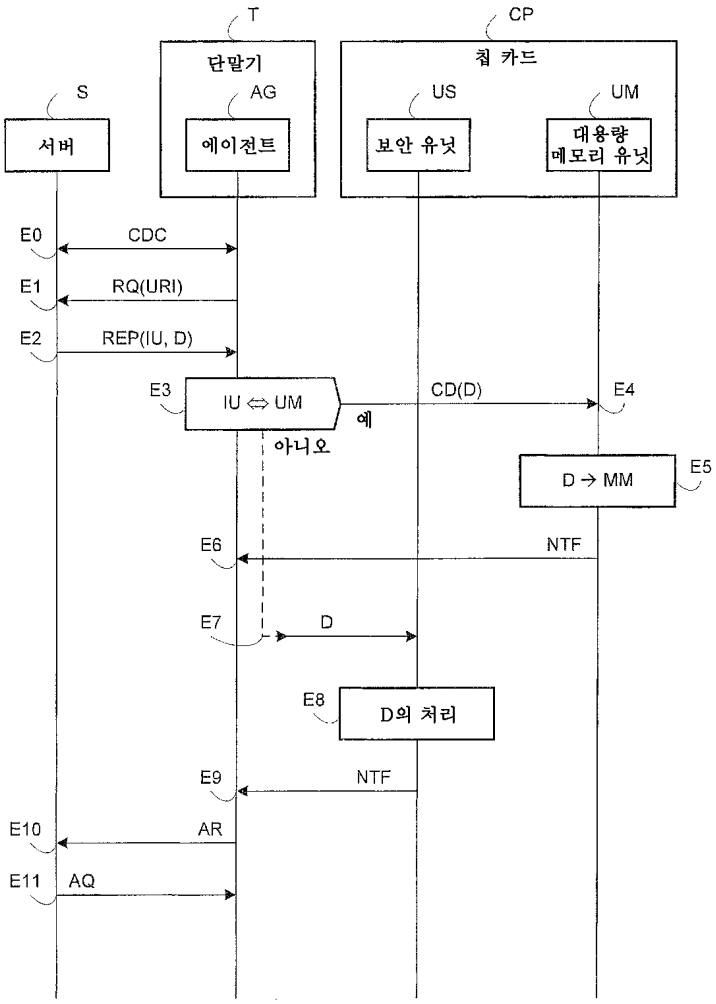
도면1



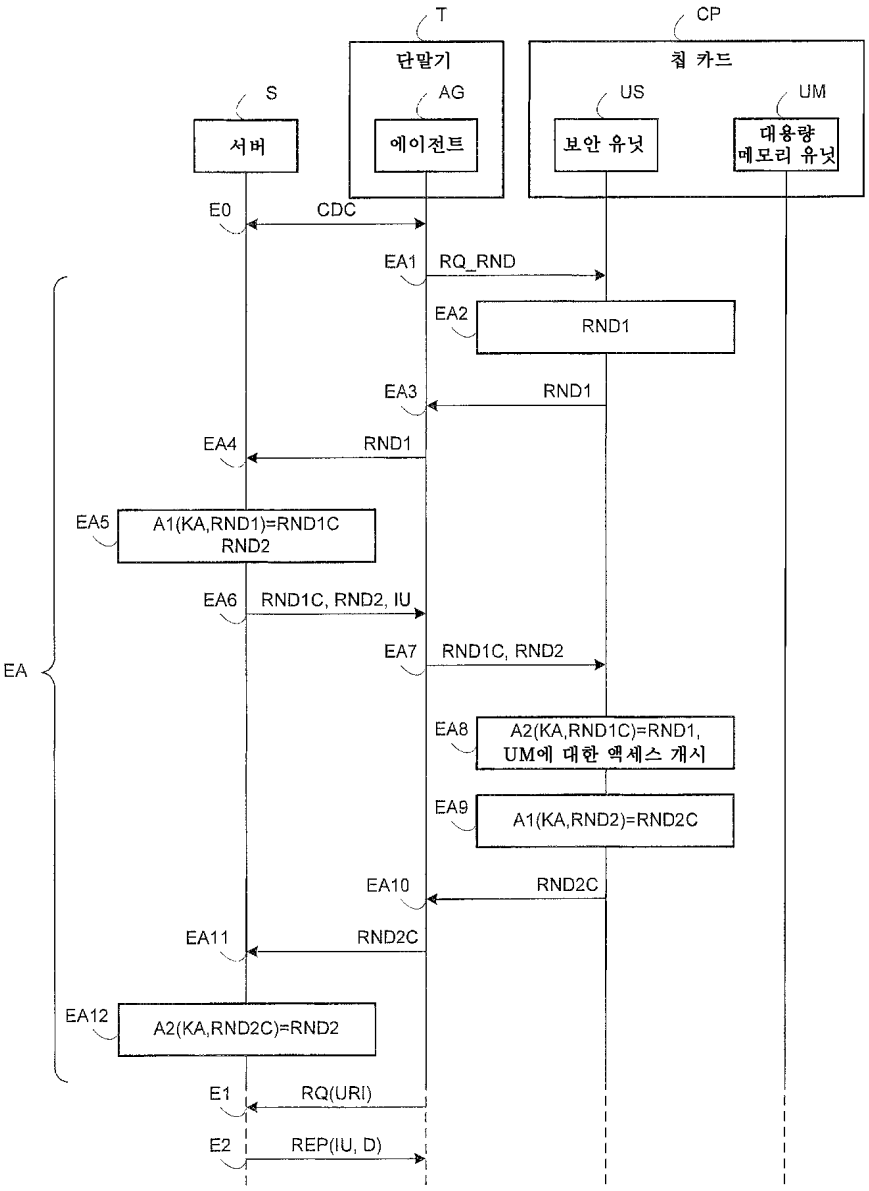
도면2


서버
ME
(A1, A2, KA, A3, KS)
매니저
GE
S
(D)
BD
통신 인터페이스
IC
무선 통신 네트워크
RR
CDC
CP
칩 카드
T
단말기
PC
프로세서
MC1
IR
무선 인터페이스
ROM (A1, A2, A3)
CS
보안 제어기
PT
프로세서
CM
대용량 제어기
MT1
ROM
EEPROM (KA, KS)
MC2
AG
에이전트
MC3
MT
RAM
MT2
EEPROM (A1, A2)
BT
MS
(KA)
MT3
RAM
MM
(D)
BS
BM
LT
판독기
I/O 포트
PES

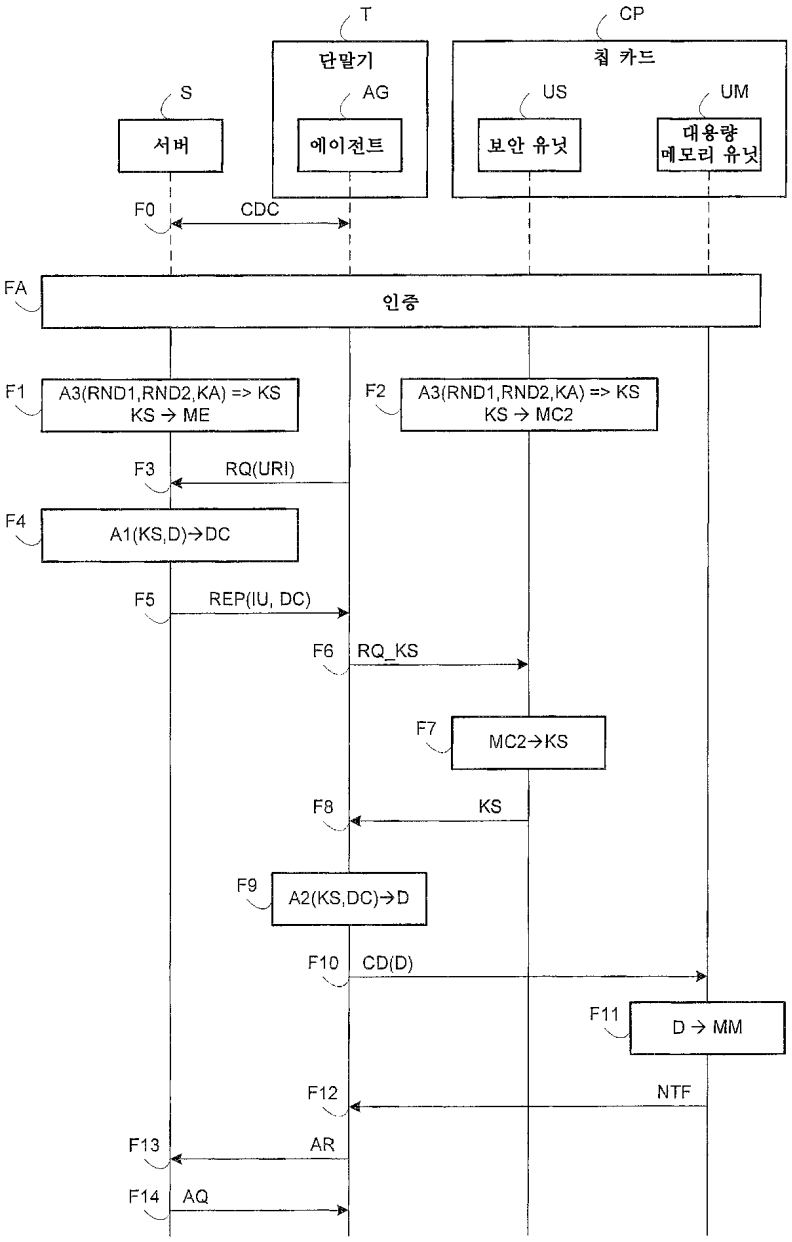
도면3


T
CP
단말기
칩 카드
S
AG
US
UM
서버
에이전트
보안 유닛
대용량 메모리 유닛
E0
CDC
E1
RQ(URI)
E2
REP(IU, D)
E3
IU ⇔ UM
CD(D)
E4
예
아니오
D → MM
E5
E6
NTF
E7
D
E8
D의 처리
E9
NTF
E10
AR
E11
AQ

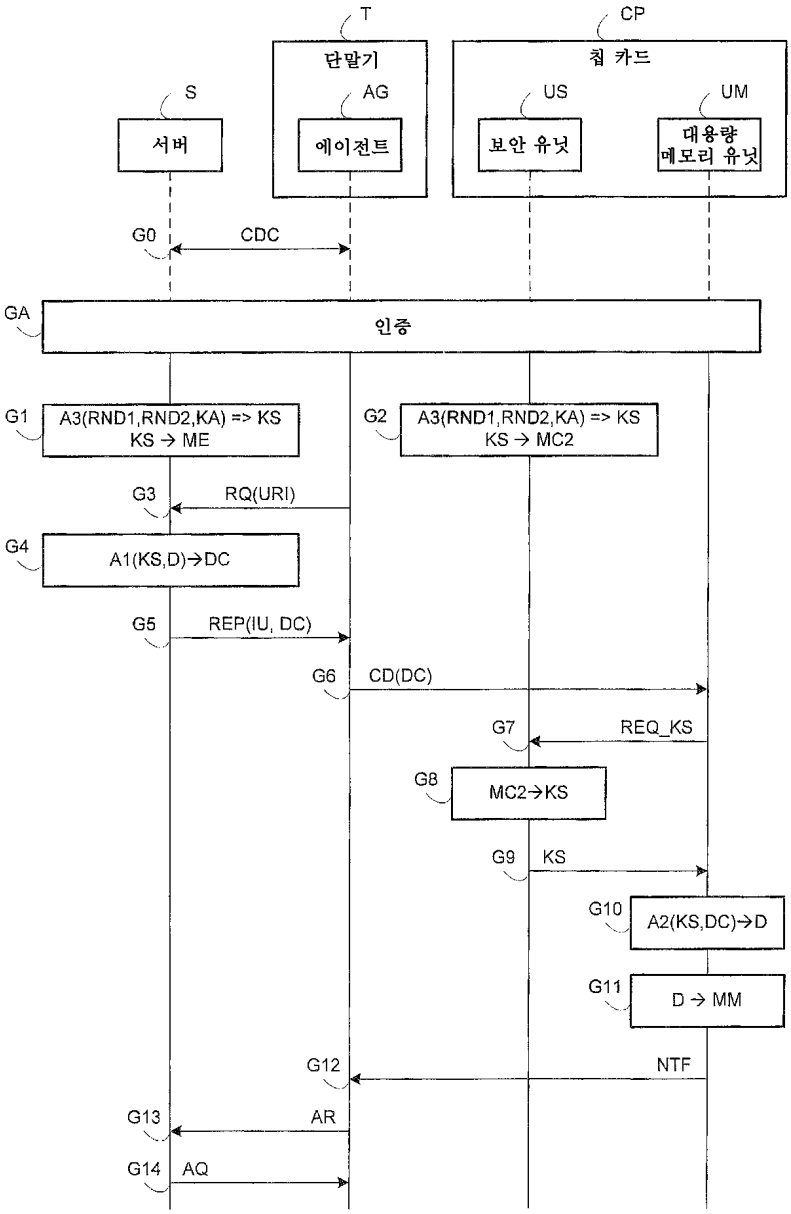
도면4


T
단말기
CP
칩 카드
S
서버
AG
에이전트
US
보안 유닛
UM
대용량 메모리 유닛
E0
CDC
EA1
RQ_RND
EA2
RND1
EA3
RND1
EA4
RND1
EA5
A1(KA,RND1)=RND1C RND2
EA6
RND1C, RND2, IU
EA7
RND1C, RND2
EA
EA8
A2(KA,RND1C)=RND1, UM에 대한 액세스 개시
EA9
A1(KA,RND2)=RND2C
EA10
RND2C
EA11
RND2C
EA12
A2(KA,RND2C)=RND2
E1
RQ(URI)
E2
REP(IU, D)

도면5


T
CP
단말기
칩 카드
S
AG
US
UM
서버
에이전트
보안 유닛
대용량
메모리 유닛
F0
CDC
FA
인증
F1
A3(RND1,RND2,KA) => KS
KS → ME
F2
A3(RND1,RND2,KA) => KS
KS → MC2
F3
RQ(URI)
F4
A1(KS,D)→DC
F5
REP(IU, DC)
F6
RQ_KS
F7
MC2→KS
F8
KS
F9
A2(KS,DC)→D
F10
CD(D)
F11
D → MM
F12
NTF
F13
AR
F14
AQ

도면6


T
단말기
CP
칩 카드
S
서버
AG
에이전트
US
보안 유닛
UM
대용량 메모리 유닛
G0
CDC
GA
인증
G1
A3(RND1,RND2,KA) => KS
KS → ME
G2
A3(RND1,RND2,KA) => KS
KS → MC2
G3
RQ(URI)
G4
A1(KS,D)→DC
G5
REP(IU, DC)
G6
CD(DC)
G7
REQ_KS
G8
MC2→KS
G9
KS
G10
A2(KS,DC)→D
G11
D → MM
G12
NTF
G13
AR
G14
AQ