(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. 7
H04Q 7/24

(11) 공개번호 특2003-0043738
(43) 공개일자 2003년06월02일

(21) 출원번호 10-2002-0074085
(22) 출원일자 2002년11월26일

(30) 우선권주장 JP-P-2001-00359940 2001년11월26일 일본(JP)
JP-P-2002-00321844 2002년11월05일 일본(JP)

(71) 출원인 마츠시타 덴끼 산교 가부시키가이샤
일본 오오사카후 가도마시 오오아자 가도마 1006

(72) 발명자 미네무라아츠시
일본도쿄174-0074이타바시쿠도신쵸1-36-B-103

(74) 대리인 특허법인 신성

심사청구 : 없음

(54) 어플리케이션 인증 시스템

요약

단말(100)에 다운로딩된 어플리케이션이 부정한 동작을 수행할 가능성이 있기 때문에, 다운로딩된 어플리케이션의 동작은, 엄격히 제한이 되고 있고, 어플리케이션은 단말의 로컬 리소스를 사용할 수 없다는 문제가 있다.

상기 문제를 해결하기 위해, 상기 인증 모듈(101)의 내템퍼 영역에 유지되는 어플리케이션의 인증을 위한 정보를 이용하여, 단말(100)의 다운로딩부(102)에 다운로딩된 어플리케이션의 인증을 수행하여 출처의 확인이나 정정이 수행되었는지의 여부의 확인을 수행한다. 인증이 된 어플리케이션에만 단말(100)이나 인증 모듈(101)의 로컬 리소스의 이용을 허가함으로써, 부정한 어플리케이션이 로컬 리소스를 이용하는 것을 방지할 수 있다. 또한 단말에 내템퍼 영역을 구비시킬 필요가 없어지기 때문에, 단말의 제조 비용을 낮출 수 있다.

대표도

도 1

색인어

컴퓨터 시스템, 이동 통신, 단말, 인증, 어플리케이션, 로컬 리소스

명세서

도면의 간단한 설명

도1은 실시예1에 따른 어플리케이션 인증 시스템의 기능 블록도.

도2는 실시예1에 따른 어플리케이션 인증 시스템의 실시예를 도시한 도면.

도3은 실시예1에 따른 어플리케이션 인증 시스템의 실시예를 도시한 도면.

도4는 실시예2에 따른 어플리케이션 인증 시스템의 기능 블록도.

도5는 실시예2에 따른 어플리케이션 인증 시스템의 기능 블록도.

도6은 어플리케이션 본체와 서명과의 관계를 설명하는 도면.

도7은 실시예2에 따른 단말의 동작을 설명하는 순서도.

도8은 실시예2에 따른 인증 모듈의 동작을 설명하는 순서도.

도9는 실시예3에 따른 인증 모듈의 기능 블록도.

도10은 실시예3에 따른 인증 모듈의 동작을 설명하는 순서도.

도11은 실시예4에 따른 어플리케이션 인증 시스템의 기능 블록도.

도12는 실시예4에 따른 인증 모듈을 단말이 인증하는 처리를 설명하는 순서도.

도13은 실시예5에 따른 어플리케이션 인증 시스템의 기능 블록도.

도14는 어플리케이션 이용 리소스 정보를 모식적으로 도시한 도면.

도15는 어플리케이션 이용 리소스 정보가 어플리케이션과 함께 다운로딩되는 상태를 모식적으로 도시한 도면.

도16은 실시예6에 따른 어플리케이션 인증 시스템의 기능 블록도.

도17은 실시예7에 따른 어플리케이션 인증 시스템의 기능 블록도.

도18은 실시예8에 따른 어플리케이션 인증 시스템의 기능 블록도.

도19는 실시예8에 따른 단말의 동작을 설명하는 순서도.

도20은 실시예8에 따른 인증 모듈의 동작을 설명하는 순서도.

도21은 실시예9에 따른 어플리케이션 인증 시스템의 기능 블록도.

도22는 실시예9에 따른 인증 모듈의 동작을 설명하는 순서도.

도23은 실시예9에 따른 인증 모듈의 동작을 설명하는 순서도.

도24는 실시예9에 따른 어플리케이션 인증 시스템의 기능 블록도.

도25는 실시예9를 IC 카드에서 구현한 예를 도시한 도면.

도26은 실시예9를 IC 카드에서 구현한 예를 도시한 도면.

도27은 실시예10에 따른 어플리케이션 인증 시스템의 기능 블록도.

도28은 실시예11에 따른 어플리케이션 인증 시스템의 기능 블록도.

도29는 실시예12에 따른 어플리케이션 인증 시스템의 기능 블록도.

도30은 실시예12에 따른 어플리케이션 인증 시스템의 동작을 설명하는 시퀀스 도면.

도31은 실시예13에 따른 어플리케이션 인증 시스템의 기능 블록도.

도32는 실시예13에 따른 어플리케이션 인증 시스템의 동작을 설명하는 시퀀 스 도면.

도33은 실시예14에 따른 어플리케이션 인증 시스템의 기능 블록도.

도34는 JAVA(등록 상표) 어플리케이션의 어플리케이션 본체와 어플리케이션 정의 파일을 모식적으로 도시한 도면.

도35는 선택 영역에 저장된 서명을 이용하여 어플리케이션의 인증을 수행하는 처리를 설명하는 순서도.

도36은 실시예2의 어플리케이션 인증 시스템의 TRM 억세스 라이브러리부가 어플리케이션 관리자와 장치 드라이버를 포함하고 있는 도면.

도37은 실시예16의 단말의 기능 블록도.

도38은 실시예17의 단말의 기능 블록도.

도39는 실시예17의 단말에서의 처리의 흐름을 설명하는 순서도.

도40은 실시예18에 따른 어플리케이션 인증 시스템의 기능 블록도.

도41은 실시예19에 따른 어플리케이션 인증 시스템의 기능 블록도.

도42는 실시예19에 따른 어플리케이션 인증 시스템의 처리의 흐름을 설명하는 순서도.

도43은 3개의 기기에 의해 구성되는 어플리케이션 인증 시스템의 기능 블록도.

도44는 제1 기기의 동작의 흐름을 설명하는 순서도.

도45는 제2 기기의 동작의 흐름을 설명하는 순서도.

도46은 어플리케이션 인증 시스템이 3개의 기기로 구성되는 경우에 있어서의 제3 기기의 동작의 흐름을 설명하는 순서도.

도47은 4개의 기기로 구성되는 어플리케이션 인증시스템의 기능 블록도.

도48은 어플리케이션 인증 시스템이 4개의 기기로 구성되는 경우에 있어서의 제3 기기의 동작의 흐름을 설명하는 순서도.

도49는 어플리케이션 인증 시스템이 4개의 기기로 구성되는 경우에 있어서의 제4 기기의 동작의 흐름을 설명하는 순서도.

도50은 5개의 기기로 구성되는 어플리케이션 인증 시스템의 기능 블록도.

도51은 N+1개의 기기로 구성되는 어플리케이션 인증 시스템의 기능 블록도.

도52는 제i 기기의 동작의 흐름을 설명하는 순서도.

도53은 제(N+1) 기기의 동작의 흐름을 설명하는 순서도.

도54는 상자 구조를 이용하여 기기가 접속되어 있는 것을 도시한 모식도.

도55는 실시예21에 따른 제i 기기의 동작의 흐름을 설명하는 순서도.

도면의 부호에 관한 간단한 설명

100: 단말 101: 인증 모듈

102: 다운로딩부 103: TRM 억세스부

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 휴대전화 등의 단말과 IC 카드 등의 인증 모듈을 구비하는 시스템에 있어서, 단말과 단말 사이에서 동작하는 어플리케이션을 인증 모듈에 의해 인증하는 기술에 관한 것이다.

종래, IC 카드를 단말에 장착하여 서버와 상거래 조작을 수행하는 시스템에 있어서는, 단말에 내(耐)템퍼성(Tamper Resistant)을 가진 영역을 확보할 수 없기 때문에, 서버내에서 동작하는 어플리케이션 프로그램(이하, 간단히 「어플리케이션」이라고 함)이 직접 IC 카드를 인증하게 되어 있었다. 따라서, 단말은 서버와 IC 카드간의 통신을 중계하는 것뿐이었다.

한편, 최근에는 휴대전화 등에 서버로부터 어플리케이션을 다운로딩하여 휴대단말에서 동작하는 것이 가능해졌다.

발명이 이루고자 하는 기술적 과제

그러나, 휴대전화 등에 다운로딩된 어플리케이션이 부정한 동작을 수행할 가능성이 있기 때문에, 다운로딩된 어플리케이션의 동작이 엄격히 제한되고 있다.

예를 들면, 휴대전화에 다운로딩된 어플리케이션은 휴대전화에 장착된 IC 카드에 데이터를 기록할 수 없거나, 각종 인터페이스의 사용이 제한(금지)되는 등, 로컬 리소스의 사용 제한이 크다.

또한, 휴대전화에 다운로딩된 어플리케이션은, 휴대전화나 IC 카드 등이 유지하고 있는 전화번호부나 어드레스장 등에 기록된 메일 어드레스나 메일의 수신 상자에 저장된 메일의 내용 등의 개인에 관한 정보 등의 읽고 쓰기를 할 수 없도록 제한을 받고 있다. 이것은, 해당 어플리케이션이 정규의 것이며, 휴대전화나 IC 카드 등의 내부에 유지되어 있는 정보에 억세스하는 권리가 있는지의 여부, 또한, 부정한 동작을 하는지의 여부 등을 검증할 수 없기 때문이다.

이것은, 장래 요구되고 있는 휴대기기의 용도 범용화(다양화)나 E-커머스(EC)에의 응용에는 매우 큰 저해 요인이 된다.

이러한 제한을 없애기 위해서는, 다운로딩된 어플리케이션을 인증하여 어플리케이션의 내력을 확인해야 한다. 예를 들면, 어플리케이션에 제3자가 붙인 서명을 어플리케이션과 함께 다운로딩하고, 그 서명과 서명이 맞다고 검증하는데 필요한 정보를 IC 카드에 제시하여 인증을 수행하는 것을 생각할 수 있다. 그러나, 휴대전화가 어플리케이션과 서명을 다운로딩한 후에, 그 휴대전화에 의해 서명이 맞다고 판단하는데 필요한 정보(예를 들면, 해쉬함수에 의해 생성되는 다이제스트)가 생성되기 때문에, 다운로딩된 어플리케이션에 붙은 서명과는 별도의 더미인 서명과 그 서명에 의해 검증할 수 있는 조작이 실시된 다이제스트가 휴대전화에 의해 IC 카드에 제시될 가능성이 있다. 이 때문에, IC 카드에 제시된 서명과 다이제스트가, 실제로 다운로딩된 어플리케이션이 것이면 IC 카드가 신뢰할 수 없어, 다운로딩된 어플리케이션을 IC 카드가 인증을 수행할 수 없다는 문제가 있다.

또한, 휴대전화 등의 단말에 다운로딩된 어플리케이션(이하, 간단히 「단말 어플리케이션」이라고 함)이 IC 카드에 억세스할 수 있도록 하여, 그 IC 카드에 보호되도록 저장되어 있는 정보를 읽고 쓰기할 수 있기 위해서는, 마찬가지로, IC 카드로 억세스를 수행하는 단말 어플리케이션의 인증을 위한 처리를, 그 IC 카드가 수행하고 억세스를 허가해도 좋은지의 여부를 판단하는 것이 필요하다.

IC 카드등의 보안 장치가 그것에 억세스를 수행하는 단말 어플리케이션을 인증하기 위한 처리로서는, 종래에는, 보안 장치가 유지되어 있는 것과 같은 비밀인 정보를 단말 어플리케이션이 가지고 있는지의 여부를 판단한다고 하는 처리가 수행되고 있었다. 그러나, 단말에는, 내템퍼성을 가진 영역 등의 비밀인 정보를 보안하게 유지하기 위한 영역도 기능도 없다. 이 때문에, 이러한 비밀인 정보가 누설될 가능성이 있고, 종래의 방법으로는 누설된 정보를 단말 어플리케이션이 사용하고 있을 가능성을 배제할 수 없고, 보안 장치가 단말 어플리케이션을 엄밀하게 인증할 수 없다는 문제가 있다.

발명의 구성 및 작용

상기와 같은 문제를 해결하기 위해, 본 발명에서는 IC 카드 등의 인증 모듈내의 내템퍼 영역에 휴대전화 등의 단말의 ROM에 기록된 프로그램(이하에서, 「라이브러리」라고 기재하는 경우가 있음)을 인증하기 위한 정보를 구비시켜, 인증 모듈은 단말의 ROM이나 TRM 등의 쉽게 다시 기록할 수 없는 영역(이하, 간단히 ROM이라고 함)에 기록된 라이브러리의 인증을 수행하도록 했다.

이와 같이 인증된 라이브러리가 다운로딩된 어플리케이션의 서명과 함께 서 명이 맞다고 판단하는데 필요한 정보를 스스로 생성하여 IC 카드에 제시하면, IC 카드에서는, 인증한 라이브러리에 의해 제시된 서명과 정보가 실제로 다운로딩된 어플리케이션의 것이면 신뢰할 수 있게 되고, 단말에 다운로딩된 어플리케이션을 IC 카드가 인증할 수 있게 된다. 결과로서, 인증된 어플리케이션이 IC 카드에 데이터를 기록하는 것 등이 가능해지고, 종래의 단말을 사용한 상거래의 조작보다도 복잡한 조작을 실현할 수 있게 된다.

또한, 이와 같이, 단말에 다운로딩된 어플리케이션이 IC 카드에 의해 인증되게 됨으로써, 다운로딩된 어플리케이션에 단말의 외부 인터페이스의 이용을 허가하는 것도 가능해진다.

또한, 본 발명의 실시에는, 다운로딩되는 어플리케이션의 서명을 다운로딩하는 것이 필요하다. 그 때문에, 어플리케이션의 서명을 어플리케이션과는 별도로 다운로딩할 뿐만 아니라, 기존의 데이터 수단에도 대응할 수 있도록, 어플리케이션의 정의 파일에 저장하는 것을 가능하게 한다. 이 때문에, 서명을 어플리케이션의 다운로딩과는 별도로 다운로딩하는 것이 필요 없게 된다.

실시예

본 발명은, 단말과 인증 모듈을 포함하는 어플리케이션 인증 시스템에 관한 것이지만, 「단말」이란, 휴대전화로 대표되는 휴대 가능한 전자기기일 수 있다. 또한, PC나 거리에 설치된 공중 단말과 같이 휴대가 사실상 불가능한 것일 수도 있고, 다음에 설명하는 인증 모듈이 장착 가능한 전자기기이며 내부에서 어플리케이션을 동작하는 것이 가능한 것이다. 이하에 설명하는 바와 같은 단말은, 그 내부에 각종 부를 가지지만, 단말에 ROM, RAM, CPU를 구비함으로써, 이러한 부는 소프트웨어에 의해 실현 가능해진다.

「인증 모듈」이란, 내부에 기억 영역을 가진 것이며, (SD)메모리 카드, IC카드, 스마트 카드가 있고, 장착된 단말에서 데이터를 입력하면 그것에 대한 응답을 하는 동작을 수행한다. 또한, 인증 모듈은, 내템퍼 영역이라고 하여, 거기에 저장된 정보가 부정한 판독 및 부정한 재기록을 방지하는 영역이 있다. 이하에 설명하는 인증 모듈내의 부 중 몇 개는, 이러한 IC 카드내에서 동작하는 카드 어플리케이션에 의해서 실현할 수도 있다.

통상, 단말에 인증 모듈이 장착되어, 단말과 인증 모듈의 사이에서 전기 회로가 형성되고, 정보의 교환이 수행된다. 단, 단말의 본체와 인증 모듈이 장착되는 부분이 분리되고, 통신에 의해서 정보의 교환이 수행되는 형태도 있다.

또한, 단말에서 동작하는 어플리케이션은, 산술 연산, 로컬 인터페이스의 이용, 서버로의 억세스, 내템퍼 영역으로의 억세스, 외부 메모리로의 억세스중 어느 하나 이상의 동작을 수행한다. 「로컬 인터페이스」란, 단말이 가지는 외부 인터페이스이며, 예를 들면, IrDA(적외선 통신을 위한 인터페이스), Bluetooth, 그 외의 무선통신, 및 유선 통신을 위한 인터페이스 등을 들 수 있다.

또, 상기에서는, 단말과 인증 모듈을 용이하게 분리 가능하다고 기재했지만, 인증 모듈이 단말의 회로에 대해 압착이 되거나 땜납 등이 됨으로써 단말의 내부에 구비되어 용이하게 분리할 수 없도록 되어 있을 수 있다.

또한, 상기에서, 「단말」이라고 기재했지만, 본 발명은, 휴대 가능한 기기 에 한정되지 않고, 단말을 사용하는 대신에 PC나 워크스테이션 등을 이용하여 실시 하는 것이 가능하다.

또한, 본 발명은, 다수의 기기가 직렬로 접속된 상태로, 한쪽 단의 기기에서 다른쪽 단의 기기가 저장하는 어플리케이션을 인증하기 위한 처리에 응용하는 것도 가능하다.

(실시예 1)

도1은, 본 발명의 실시예1에 관한 어플리케이션 인증 시스템의 기능 블록도 이다. 본 실시예에 있어서의 어플리케이션 인증 시스템은, 단말(100)과 인증 모듈(101)로 구성된다.

단말(100)은 어플리케이션을 다운로딩하는 다운로딩부(102)를 가진다. 「어플리케이션을 다운로딩한다」는 말은 다운로딩부(102)의 외부에서 어플리케이션의 실행을 위한 데이터를 판독하는 것을 말한다. 여기에 「어플리케이션의 실행을 위한 데이터」란, 어플리케이션이 단말(100)에 의해 직접 실행 가능한 2진 데이터이면, 그 2진 데이터이며, 어플리케이션이 단말(100)에 의해서 해석 실행되는 언어로 기술된 것이면, 그 기술이다. 다운로딩부는, 어플리케이션

을 실행하기 위한 데이터를 판독하고, 그 데이터를 유지하는 것을 수행한다.

인증 모듈(101)은, TRM부(103)를 포함하고 있다. TRM부(103)는, 어플리케이션의 인증의 처리를 위한 정보를 내템퍼 영역에 유지한다. 또, 「TRM」은, 「Tamper Resistant Module」의 약자이다. 「어플리케이션」이란, 단말(100)의 다운로딩부(102)에 다운로딩된 어플리케이션이며, 「어플리케이션의 인증」이란, 어 플리케이션이, 신뢰할 수 있는 사람에 의해서 발행되었는지의 여부, 부정한 동작을 하지 않는다는 보증을 받고 있는 것인지의 여부, 또는, 신뢰할 수 있는 사람에게서 발행된 후의 정정(改竄), 또는, 부정한 동작을 하지 않는 것이 보증된 후의 정정이 되어 있는지의 여부 등 어플리케이션이 부정한 동작을 하지 않는 것인 것을 확인하는 것이다. 「어플리케이션의 인증의 처리」란, 이러한 확인을 하기 위한 처리이다.

상기 인증의 처리 방법으로서는, 통상, SHA-1(Secure Hash Standard-1)이나 MD5(Message Digest 5) 등의, 해쉬함수(「해쉬함수」의 대신에「요약함수」라고 불리는 경우도 있음)를 이용하여, 어플리케이션의 실행을 위한 데이터를 입력 데이터로 하여 처리하여 획득할 수 있는 결과 데이터를 구하고, 그것을 암호화한 것(소위 「서명」)이 사용된다. 여기에서 「해쉬함수」란, 입력 데이터를 처리하여 획득할 수 있는 결과 데이터가 일치하는 두개의 다른 입력 데이터를 찾아내는 것이 계산양적으로 곤란한 결과를 되돌려 주는 함수이다. 따라서「어플리케이션의 인증의 처리를 위한 정보」란, 이 서명 그 자체, 또는, 서명을 복호하여 해쉬값을 얻는데 필요한 복호키이다. 「내템퍼 영역」이란, 인증 모듈의 기억 영역이며, 그 기억 영역의 데이터를 부정하게 판독하는 하는 것이나, 그 기억 영역의 데이터를 부정하게 재기록하는 것인 곤란한 기억 영역이다. 그와 같은 기억 영역은, 예를 들면, 그 기억 영역에 억세스하기 위해서는, 올바른 절차를 수행하지 않으면 억세스할 수 없는 하드웨어를 경유하도록 하거나, 기억 영역에 기억되어 있는 데이터가 암호화되어 있도록 하여 실현된다.

어플리케이션의 인증은, 단말(100)이 다운로딩부(102)로 다운로딩된 어플리케이션의 해쉬값을 구하고, 그 해쉬값과 함께 서명을 인증 모듈에 제시하고, 인증 모듈(101)은, TRM부(103)에 유지된 정보에 의해, 그 해쉬값으로부터 그 서명을 생성할 수 있는지의 여부, 또는, 그 해쉬값이 서명을 복호하여 얻을 수 있는 해쉬값과 일치하는지의 여부를 조사한다. 또한, 단말(100)이 다운로딩부로 다운로딩된 어플리케이션 그 자체와 서명을 인증 모듈에 제시하고, 어플리케이션 그 자체와 서명과의 관계를 조사하여 인증을 수행하도록 해도 좋다.

이러한 구성의 어플리케이션 인증 시스템에 의해, 다운로딩부(102)로 다운로딩된 어플리케이션을, 인증 모듈(101)의 TRM부(103)에 유지된 정보에 의해, 인증할 수 있기 때문에, 부정한 어플리케이션이 다운로딩되어 단말(100)내에서 실행, 또는, 인증 모듈(101)내에 저장되어 버리는 것을 방지할 수 있다.

도2는, 본 실시예의 어플리케이션 인증 시스템의 일례를 나타낸다. 본 예에 있어서, 어플리케이션(201)이 저장된 상태로 인증 모듈(101)을 서비스 제공 회사(200)가 배포를 수행한다. 인증 모듈(101)을 입수한 사람이 단말(100)에 인증 모듈(101)을 장착하면, 인증 모듈(101)로부터 단말(100)의 다운로딩부(102)로 어플리케이션(201)이 다운로딩된다(화살 표시(203)). 다운로딩된 어플리케이션(202)이, 인증 모듈(101)의 TRM부에 저장된 정보에 의해 인증이 되면, 어플리케이션(202)이 단말(100)내에서 동작을 하여, 서비스 제공 회사(200)로부터 서비스의 제공을 받는다(화살 표시(204)).

도3은 본 실시예의 어플리케이션 인증 시스템의 다른 예를 나타낸다. 본 예 에 있어서, 서비스 제공 회사(200)는, 단말(100)의 다운로딩부(102)로 어플리케이션(302)을 다운로딩한다(화살 표시(303)). 어플리케이션(302)에 대해, 인증 모듈(101)의 TRM부에 유지된 정보에 의해 인증이 수행되고, 부정한 어플리케이션이 아니라는 것이 확인되면, 인증 모듈(101)로 어플리케이션(301)으로서 저장된다(화살 표시(304)). 그 후, 어플리케이션(301)은 필요에 따라서 단말(100)의 다운로딩부(102)로 다운로딩되어 단말(100) 내에서 실행된다.

도2와 도3에 있어서는, 단말(100) 내에서 실행되는 어플리케이션은 인증 모듈로부터 다운로딩되지만, 단말이 접속한 서버에서 다운로딩되고, 인증 모듈의 TRM부에 유지된 정보에 의해 인증이 수행되고, 부정한 어플리케이션이 아닌 것이 확인되면, 그 어플리케이션이 단말내에서 실행되도록 되어 있는 예도 들 수 있다.

또한, 「단말」이라는 단어를 사용했지만, 이것은, 휴대전화로 대표되는 휴대 가능한 단말 등에 한정되는 것을 의미하지 않는다. 예를 들면, 가정용 전화 제품일 수도 있고, 소위, 정보 가전이나 네트워크 가전이라고 불리는 것일 수도 있다. 그와 같은 제품을 예시 열거하면, 에어컨, 가습기, 제습기, 공기청정기, 전자레인지, 오븐, 냉장고, 식기 세척기, 전기포트, 다리미, 전기 청소기, 세탁기, 건조기, 전기 담요, 조명기기, 텔레비전 수상기, 라디오 수신기, 테이프 레코더 등의 오디오기기, 카메라, IC 레코더, 전화기, 팩시밀리 송수신기, 복사기, 프린터, 스캐너, PC 등을 들 수 있다.

(실시예2)

도4는 본 발명의 실시예2에 따른 어플리케이션 인증 시스템의 기능 블록도를 나타내고, 어플리케이션 인증 시스템은 단말(100)과 인증 모듈(101)로 이루어진다. 단말(100)은 다운로딩부(102)와 TRM 억세스 라이브러리부(401)를 구

비한다. 인증 모듈(101)은 TRM부(103)와 TRM 억세스 라이브러리부 인증부(402)를 구비한다.

다운로딩부(102)는 어플리케이션을 다운로딩한다.

TRM 억세스 라이브러리부(401)는 인증 모듈(101)에 자신이 인증되는 것을 조건으로 하여 어플리케이션의 인증을 위한 처리를 한다. 즉, TRM 억세스 라이브러리부(401)는 먼저, 인증 모듈(101)에 자신을 인증시켜, 올바르게 인증된 경우에, 어플리케이션의 인증을 위한 처리를 수행한다.

TRM 억세스 라이브러리부(401)가 인증 모듈(101)에 자신을 인증시키는 방법으로서는, 단말(100)에 고유의 정보를 인증 모듈(101)에 출력하고, 인증 모듈(101)은, 출력된 정보가 내템퍼 영역에 저장된 정보와 적합한지의 여부로 인증을 수행하는 방법이 있다. 「단말(100)에 고유의 정보」로서는, ① 단말이 휴대전화인 경우에는, 그 전화 번호를 들 수 있다. 또한, 단말(100)에 고유의 정보의 다른 것으로서는, ② 단말(100)의 종류를 특정하는 식별자나, 단말(100)에 붙여진 제조번호 등의 개개의 단말마다 다른 것이 부여된 식별자일 수 있다. 또한, ③ 단말(100)에 인스톨되어 있는 어플리케이션의 조합에 관한 정보를 이용하여 TRM 억세스 라이브러리부(401)를 인증하는 방법이 있다. 「단말(100)에 인스톨되어 있는 어플리케이션」이란, 단말(100) 내에 구비된 어플리케이션을 의미하고, 단말의 외부로부터 다운로딩된 어플리케이션이나, 단말의 ROM에 저장된 어플리케이션이다. 이 경우, TRM 억세스 라이브러리부(401)는 인증 모듈(101)로 단말(100) 내에 어떤 어플리케이션 이 인스톨되어 있는지의 정보(예를 들면, 인스톨되어 있는 어플리케이션의 식별자 등)를 출력하고, 인증 모듈(101)은 출력된 정보가 내템퍼 영역에 저장된 정보와 적합한지의 여부로 인증을 수행한다. 또는, 부정한 단말의 정보가 내템퍼 영역에 저장되어 있고, 부정한 단말의 정보에 적합하지 않는지의 여부로 인증을 수행한다.

상기에 기술한 ③으로서 예를 들면, 서비스 A와 서비스 B의 양쪽의 서비스의 제공을 받기 위한 회원이 되어 있는 사람에게, 새로운 서비스 C의 제공이 된다고 하자. 이 경우, 서비스 A의 제공을 받기 위한 어플리케이션 A와, 서비스 B의 제공을 받기 위한 어플리케이션 B가 단말(100)에 인스톨되어 있는 것을 조건으로 하여 TRM 억세스 라이브러리부(401)가 인증 모듈(101)에 의해 인증되는 것으로 하면, 단말에 인스톨되어 있는 서비스 A와 서비스 B의 회원에 대해, 서비스 C의 제공을 받기 위한 어플리케이션 C를 제공하는 것이 가능해진다.

또한, TRM 억세스 라이브러리부(401)를 식별하기 위한 정보를 이용하여 TRM 억세스 라이브러리부(401)를 인증하는 방법도 있다. 「TRM 억세스 라이브러리부(401)를 식별하기 위한 정보」란, 예를 들면, TRM 억세스 라이브러리부(401)를 구성하는 소프트웨어를 식별하기 위한 정보이며, 그 소프트웨어의 이름이나 버전번호나 일련번호 등이다. TRM 억세스 라이브러리부(401)는, TRM 억세스 라이브러리부(401)를 식별하기 위한 정보를 인증 모듈로 출력하고, 인증 모듈(101)은 출력된 정보가 내템퍼 영역에 저장된 정보와 적합한지의 여부로 인증을 수행한다.

「어플리케이션의 인증을 위한 처리」란, 다운로딩부(102)에 다운로딩된 어 플리케이션의 인증을 위한 처리이다. TRM 억세스 라이브러리부(401)가 어플리케이션의 인증에 관한 처리의 일부를 수행할 수 있다. 또한, TRM 억세스 라이브러리부(401)는 인증 모듈에 의해서 인증되어 있기 때문에, 어플리케이션의 인증에 관한 처리 모두를 수행할 수도 있다.

또한, TRM 억세스 라이브러리부(401)가 수행하는 처리는, 어플리케이션의 인증을 위한 처리에 한정될 필요는 없다. 예를 들면, 도36에 도시한 바와 같이, TRM 억세스 라이브러리부(401)는 그 내부에 어플리케이션 관리자와 장치 드라이버를 포함하고, 그들의 처리를 수행하도록 할 수 있다.

「어플리케이션 관리자」란, 다운로딩부(102)에 다운로딩된 어플리케이션의 기동, 종료, 중지 등 어플리케이션의 동작의 제어를 수행하는 기능을 제공한다. 또한, 어플리케이션 관리자의 다른 명칭으로서는, 예를 들면, 「어플리케이션 제어 프로그램」을 들 수 있다.

「장치 드라이버」란, 인증 모듈과의 입출력을 관리하는 프로그램이다. 예를 들면, 인증 모듈마다 다른 입출력을 위한 조작의 수단을 흡수하고, 동일한 인터페이스의 조작에 의해서 어플리케이션이 입출력을 수행할 수 있도록 하기 위한 프로그램이다. 또한, 장치 드라이버의 다른 명칭으로서는, 「인증 모듈 억세스 프로그램」을 들 수 있다.

TRM부(103)는 TRM 억세스 라이브러리부 인증 정보를 내템퍼 영역에 유지한다. 「TRM 억세스 라이브러리부 인증 정보」란, TRM 억세스 라이브러리부(401)를 인증하기 위한 정보이다. 이미 설명한 바와 같이, 이 정보는, 휴대전화 번호 등의 단말(100)에 고유의 정보인 경우나, 단말(100)에 인스톨되어 있는 어플리케이션의 조합에 관한 정보인 경우나, TRM 억세스 라이브러리부(401)를 식별하기 위한 정보인 경우 등이 있다. TRM 억세스 라이브러리부 인증 정보는 내템퍼 영역에 유지되기 때문에, 휴대전화 번호, 단말(100)에 인스톨되어 있는 어플리케이션을 식별하기 위한 정보, TRM 억세스 라이브러리부(401)를 식별하기 위한 정보가 암호화되어 유지되고 있는 경우도 있다.

TRM 억세스 라이브러리부 인증부(402)는, TRM 억세스 라이브러리부 인증 정보에 기초하여 단말의 TRM 억세스 라

이브러리부(401)를 인증한다. 즉, TRM 억세스 라이브러리부(401)에서 인증 모듈로 출력되는 인증을 위한 정보와, TRM부(103)에 보존되는 TRM 억세스 라이브러리부 인증 정보에 의해, TRM 억세스 라이브러리부(401)를 인증하는 것을 수행한다.

도5는 어플리케이션을 본 실시예의 어플리케이션 인증 시스템에 있어서, 어플리케이션의 인증의 방법을 설명하기 위한 도면이다. 도4와 도5에 도시된 어플리케이션 인증 시스템의 차이는, 도5의 단말(100)의 다운로딩부(102)가 정정이 없음을 인증하기 위해서 사용하는 정보인 서명이 부가된 어플리케이션을 다운로딩하는 점과, 단말(100)이 서명 인증 정보 출력부(501)를 더 구비하는 점과, 인증 모듈(101)이 서명 인증 정보 입력부(502)와 서명 인증부(503)를 더 구비하는 점이다.

「정정이 없음을 인증하기 위해서 사용하는 정보인 서명」이란, 어플리케이션이 정정되어 있지 않음을 확인하기 위한 정보이다. 도6은, 어플리케이션과 서명 의 관계를 나타낸다. 어플리케이션 본체(601)를 데이터로 간주하고 그것에 대해, SHA-1나 MD5 등의 해쉬함수를 적용하여 획득하는 값을 암호화한 것이 서명(602)이다. 서명(602)을 이용하여 어플리케이션 본체가 정정되어 있지 않음을 확인하기 위해서는 먼저, 서명을 복호하여 해쉬값를 얻는다. 다음으로, 어플리케이션 본체에 대해 해쉬함수를 적용하고, 획득하는 값이 서명을 복호하여 획득하는 해쉬값와 같은지의 여부를 확인한다. 또는, 어플리케이션 본체에 해쉬함수를 적용하여 해쉬값를 획득하여, 그것에 대해 암호화를 수행하고, 획득된 것이 서명과 같은지의 여부를 확인한다. 전자의 방법은, 예를 들면, 서명이 공개 키 암호화 방식을 사용하는 경우에 보통 이용되는 방법이며, 서명은 해쉬값를 서명을 수행하는 사람의 비밀키에 의해서 암호화되고, 어플리케이션 본체가 정정되어 있지 않음을 확인할 때에, 서명을 수행한 사람의 비밀키에 대응하는 공개키에 의해서 복호된다. 후자의 방법은, 예를 들면, 어플리케이션 본체가 정정되어 있지 않음을 확인하는 사람이 서명을 수행한 사람의 비밀키를 알고 있는 경우나, 공통 키 암호화 방식이 사용되는 경우에 사용된다.

본 실시예에 있어서, TRM 억세스 라이브러리부(401)는, 자신을 인증 모듈에 인증시킨 후에, 다운로딩부(102)로 다운로딩된 어플리케이션의 인증을 위한 처리의 일부인 처리, 즉, 다운로딩부(102)로 다운로딩된 어플리케이션으로부터 서명 인증용 다이제스트를 생성하는 것을 수행한다. 「서명 인증용 다이제스트」란, 상기에서 든 SHA-1나 MD5 등의 해쉬함수에 의한 해쉬값이다.

서명 인증 정보 출력부(501)는, TRM 억세스 라이브러리부(401)에서 생성된 서명 인증용 다이제스트(504)와 서명(505)을 포함하는 서명 인증 정보(506)를 인증 모듈로 출력한다. 여기에 「서명(505)」이란, 다운로딩부(102)로 다운로딩된 어플리케이션에 부가된 서명이다.

서명 인증 정보 입력부(502)는, 서명 인증 정보 출력부(501)에서 출력된 서명 인증 정보(506)를 입력한다.

서명 인증부(503)는 서명 인증 정보 입력부(502)로부터 입력되는 서명 인증용 다이제스트와 서명에 기초하여 서명의 검증을 수행한다. 검증의 방법으로서는, 예를 들면, 서명이 공개키 암호화 방식의 비밀키로 암호화되어 있는 경우에는, 그 비밀키에 대응하는 공개키로 복호하고, 그 복호의 결과와 서명 인증용 다이제스트를 비교하여 같은지의 여부로 인증을 수행한다. 또는, 내템퍼 영역에 공통키를 유지해 두고, 그 공통키로 서명을 복호하여 서명 인증용 다이제스트와 비교하는 방법, 또는, 그 비밀키를 내템퍼 영역에 유지하여, 그 비밀키로 서명 인증용 다이제스트를 암호화하여 서명과 비교하는 방법이 있다.

도7은 단말(100)의 동작을 설명하는 순서도이다. 이 순서도의 처리를 수행하는 것을 전제로 하여, TRM 억세스 라이브러리부(401)는 인증 모듈에 의해 인증되어 있다고 한다. 단계(S701)에서, 다운로딩부(102)에 어플리케이션을 다운로딩한다. 단계(S702)에서, 다운로딩한 어플리케이션으로부터 서명 인증용 다이제스트를 TRM 억세스 라이브러리부(401)에서 생성한다. 단계(S703)에서, 단계(S702)에서 요청된 서명 인증용 다이제스트와 다운로딩된 어플리케이션에 부가된 서명을 포함하는 서명 인증 정보(506)를 서명 인증 정보 출력부(501)에서 인증 모듈(101)로 출력한다.

도8은 인증 모듈(101)의 서명 인증 정보 입력부(502)와 서명 인증부(503)의 동작을 설명하는 순서도이다. 이 순서도의 처리를 수행하는 것을 전제로 하여, TRM 억세스 라이브러리부(401)는 인증 모듈에 의해 인증되어 있다고 한다. 이를 위해, 예를 들면, TRM 억세스 라이브러리부 인증부(402)는 인증의 결과를 인증 모듈(101) 내에 설정해 두는 것으로 하고, 도8의 순서도의 처리를 수행할 때에는, 그 설정된 인증의 결과를 참조하여, TRM 억세스 라이브러리부(401)가 인증되어 있는 경우에 한해서, 도8의 순서도의 처리를 수행하도록 하는 방법이 있다. 단계(S801)에서, 서명 인증 정보(506)를 서명 인증 정보 입력부(502)에 의해 입력한다. 단계(S802)에서, 서명 인증용 다이제스트(504)와 서명(505)에 기초하여 서명의 검증을 수행한다. 서명의 검증의 방법에 대해서는, 상기에서 설명한 바와 같다.

본 실시예에서는, TRM 억세스 라이브러리부(401)는, 인증 모듈(101)에 의해서 인증이 된 것을 조건으로 하여, 다운로딩부(102)에 다운로딩된 어플리케이션의 서명 인증용 다이제스트를 생성하고, 생성된 서명용 인증용 다이제스트가 인증 모듈(101)에 입력되기 때문에, 서명 인증용 다이제스트는 신뢰할 수 있는 것이며, 다운로딩부(102)로 다운로딩된 어플리케이션의 인증을 인증 모듈(101)이 수행할 수 있다.

(실시예3)

도9는 본 발명의 실시예3에 따른 인증 모듈(101)의 기능 블록도를 나타낸다. 본 실시예는 실시예2에서의 서명 인증 정보에 의한 인증 방법을 더욱 구체적으로 한 것이며, 실시예2의 인증 모듈(101)이 서명 유래 다이제스트 생성 정보 취득부(901)와 서명 유래 다이제스트 생성부(902)를 더 포함하고 있다.

서명 유래 다이제스트 생성 정보 취득부(901)는, 서명 인증 정보 입력부(502)에서 입력되는 서명을 이용하여 서명 유래 다이제스트를 생성하기 위한 서명 유래 다이제스트 생성 정보를 취득한다. 서명이 어플리케이션 본체의 해쉬값을 암호화한 것이면, 「서명 유래 다이제스트 생성 정보」는, 암호화한 것을 복호 하는 복호키이다. 암호화로서 공개키 암호화 방식이 사용된 경우에는, 어플리케이션 본체의 해쉬값를 암호화하기 위해 사용된 비밀키에 대응하는 공개키가 서명 유래다이제스트 생성 정보가 된다. 이 공개키는 인증 모듈에 유지되어 있을 수 있다. 또한, 단말(100) 등을 경유하여 적당한 서버로부터 취득하도록 되어 있을 수 있다.

서명 유래 다이제스트 생성부(902)는, 서명 인증 정보 입력부에서 입력된 서명(903)과 서명 유래 다이제스트 생성 정보 취득부에 유지된 서명 유래 다이제스트 생성 정보를 이용하여 서명 유래 다이제스트(905)를 생성한다. 즉, 서명 유래 다이제스트 생성 정보가 공개키이면, 서명(903)을 그 공개키로 복호하여 어플리케이션 본체의 해쉬값인 서명 유래 다이제스트(905)를 생성한다.

서명 인증부(503)는, 서명 유래 다이제스트 생성부(902)에서 생성된 서명 유래 다이제스트(905)와 서명 인증 정보 입력부(502)로부터 입력된 서명 인증용 다이제스트(904)에 기초하여 인증을 수행한다. 즉, 서명 유래 다이제스트(905)와 서명 인증용 다이제스트(904)를 비교하여, 동일한 것이면, 다운로딩부(102)로 다운로딩된 어플리케이션을 인증하고, 다른 것이면, 인증하지 않는다.

도10은 본 실시예에 있어서의 서명 인증 정보 입력부(502)와, 서명 유래 다 이제스트 생성 정보 취득부(901)와, 서명 유래 다이제스트 생성부(902)와, 서명 인증부(503)의 동작을 설명하는 순서도이다. 이 순서도의 처리를 수행하는 것을 전제로 하여, TRM 억세스 라이브러리부(401)는 인증 모듈(101)에 의해 인증되어 있는 것으로 한다. 이를 위해서는 예를 들면, TRM 억세스 라이브러리부 인증부(402)는 인증의 결과를 인증 모듈(101) 내에 설정해 두는 것으로 하고, 도10의 순서도의 처리를 수행할 때에는, 그 설정된 인증의 결과를 참조하여, TRM 억세스 라이브러리부(401)가 인증되어 있는 경우에 한해, 도10의 순서도의 처리를 수행하도록 하는 방법이 있다. 단계(S1001)에 있어서, 서명 인증 정보(506)를 서명 인증 정보 입력부(502)에 의해 입력하고, 서명(903)과 서명 인증용 다이제스트(904)를 획득한다. 단계(S1002)에서, 서명 유래 다이제스트 생성 정보를 서명 유래 다이제스트 생성 정보 취득부(901)에 의해 취득한다. 단계(S1003)에서, 서명(903)과 서명 유래 다이제스트 생성 정보로부터 서명 유래 다이제스트 생성부(902)에서, 서명 유래 다이제스트(905)를 생성한다. 단계(S1004)에 있어서, 서명 유래 다이제스트(905)와 서명 인증용 다이제스트(904)에 기초하여, 서명 인증부(503)에서 인증을 수행한다.

(실시예4)

도11은 본 발명의 실시예4에 관한 어플리케이션 인증 시스템의 기능 블록도를 나타낸다. 본 실시예에서는, 실시예2 또는 실시예3에서의 어플리케이션 인증 시스템의 단말이 인증 모듈 인증부(1101)를 더 포함하고 있다.

인증 모듈 인증부(1101)는 인증 모듈(101)을 인증한다. 이 인증의 방법으로 서는, 도12에 도시한 순서도에 나타낸 방법이 있다. 이 방법을 이용함에 있어서는, 인증 모듈에 대해 공개키 암호화 방식의 비밀키와 그것에 대응하는 공개키가 생성되고, 인증 모듈은, 그 비밀키를 저장하고 있는 것을 전제로 한다. 단계(S1201)에서, 인증 모듈 인증부(1101)는 난수(亂數)를 발생시킨다. 단계(S1202)에서, 인증 모듈(101)이 가지는 공개키에 의해 단계(S1201)에서 발생시킨 난수를 암호화한다. 단계(S1203)에서, 인증 모듈(101)에 단계(S1202)에서 암호화한 난수를 입력하고, 복호하도록 요구한다. 단계(S1204)에서, 인증 모듈(101)로부터의 복호의 결과를 받아, 단계(S1205)에서 단계(S1201)에서 발생시킨 난수와 단계(S1204)에서 받은 복호의 결과가 같은지를 판단한다. 다른 방법으로서는, 인증 모듈 인증부(1101)는, 발생시킨 난수를 인증 모듈(101)에 입력하고, 그 난수를 인증 모듈(101)의 비밀키로 암호화하도록 요구하는 방법이 있다. 인증 모듈 인증부(1101)는, 그 암호화의 결과를 획득하여, 인증 모듈(101)의 공개키로 복호하고, 인증 모듈(101)에 입력한 난수와 같은지의 여부를 판단한다.

이와 같이, 단말(100)이 인증 모듈(101)을 인증하기 위한 인증 모듈 인증부(1101)를 가짐으로써, 단말(100)이 인증 모듈(101)을 인증할 수 있고, 단말(100)내에서 동작하는 어플리케이션이 기밀성이 높은 정보(프라이버시 정보, E-커머스(EC)의 로그, 은행 거래에 있어서의 구좌 잔액 등)을 인증 모듈(101)에 기록할 때에, 인증 모듈(101)이 정당한 것인지의 여부를 확인할 수 있다.

(실시예5)

도13은 본 발명의 실시예5에 관한 어플리케이션 인증 시스템의 기능 블록도 를 나타낸다. 본 실시예는, 실시예4에서의 어플리케이션 인증 시스템의 TRM 억세스 라이브러리부(401)가 어플리케이션 이용 리소스 정보 유지 수단(1301)을 더 포함하고 있는 형태이다.

어플리케이션 이용 리소스 정보 유지 수단(1301)은 어플리케이션 이용 리소스 정보를 유지한다. 「어플리케이션 이용 리소스 정보」란, 인증된 어플리케이션에 대해 이용을 인정하는 리소스에 관한 정보이다. 「인증된 어플리케이션」이란, 다운로딩부(102)에 다운로딩된 어플리케이션이며, TRM 억세스 라이브러리부(401)에 의한 인증을 위한 처리가 수행되고, 올바르게 인증된 어플리케이션이다. 「리소스」란, 어플리케이션이 이용하는 어플리케이션의 외부의 자원이다. 리소스에는, 단말(100) 및 그것에 장착된 인증 모듈(101)의 자원인 로컬 리소스와, 그 이외의 리소스, 예를 들면, 단말(100)의 통신할 곳인 서버의 자원인 리소스가 있다. 로컬 리소스에는, 메모리의 사용, 파일의 사용, IrDA의 사용, Bluetooth의 사용, 통신의 사용, TRM의 사용, 어플리케이션의 사용, 비접촉/접촉 IC 카드 I/F의 사용 등의 종류가 있다. 또한, 로컬 리소스중, 메모리의 사용 등의 경우에는, 사용할 수 있는 메모리의 양이나 메모리의 번지 등의 범위에 관한 것도 있다. 또한, 사용할 수 있는 시간이라는 범위도 들 수 있다.

도14는 어플리케이션 이용 리소스 정보를 예시하고 있다. 도14에 있어서, 어플리케이션 이용 리소스 정보(1400)는, 메모리의 사용(1401), 파일의 사용(1402), IrDA의 사용(1403), Bluetooth의 사용(1404),통신의 사용(1405), TRM의 사용(1406), 어플리케이션의 사용(1407), 비접촉/접촉 IC 카드 I/F의 사용(1408), 동작(1409), 사용 일시(1410) 등의 항목으로 이루어져 있다.

메모리의 사용(1401)의 항목으로서는, 예를 들면, 메모리로서 사용 가능한 양, 사용 가능한 범위의 어드레스, 기록할 수 있는 회수, 판독할 수 있는 회수, 메모리가 사용 가능한 일시, 사용 불가능한 일시 등을 들 수 있다. 플래시 메모리에 있어서는, 기록은 부담이 가해지는 조작이기 때문에, 메모리의 기록 회수를 제한하는 것에는 특히 의미가 있다.

파일의 사용(1402)의 항목으로서는, 단말(100)이 가지는 파일이나 인증 모듈(101) 등의 단말(100)에 접속된 외부의 메모리가 가지는 파일에 대한 억세스의 제한을 기술(記述)하는 것을 들 수 있고, 예를 들면, 억세스 가능한 디렉토리명, 억세스 가능한 파일명, 억세스 가능한 파일의 종류(예를 들면, 파일의 확장자에 의해서 지정된다), 사용 가능한 일시, 사용 불가능한 일시 등이 있다.

IrDA의 사용(1403)은 단말(100)이 가지는 적외선 통신의 기능의 사용을 인정할 것인지의 여부를 나타내는 항목이며, 그 기능이 사용 가능/불가능한 시간, 사용 가능한 토탈 시간, 사용 회수 등을 들 수 있다.

Bluetooth의 사용(1404)은 단말(100)이 가지는 Bluetooth에 의한 통신의 기능의 사용을 인정할 것인지의 여부를 나타내는 항목이며, 그 기능이 사용 가능한 시간, 사용 가능한 토탈 시간, 사용 회수의 이외에, 사용 가능한 전파의 강도, 로밍 회수, 사용 가능/불가능한 일시 등을 들 수 있다. 사용 가능한 전파의 강도를 지정함으로써, 통신 가능한 거리를 지정할 수 있다.

통신의 사용(1405)은 서버 등과의 통신의 기능의 사용을 인정할 것인지의 여 부를 나타내는 항목이며, 그 기능이 사용 가능/불가능한 시간, 사용 가능한 토탈 시간, 사용 회수, 사용 가능한 전파의 강도, 로밍 회수의 이외에, 억세스 가능한 서버 등을 들 수 있다. 억세스 가능한 서버는 IP 어드레스에 의한 어드레스의 지정, 도메인명에 의한 지정, 또는, 메일 서버나 FTP 서버 등의 서버의 기능 또는 서버와의 통신의 프로토콜에 의한 지정에 의해, 어플리케이션이 서버 등을 이용할 수 있는지의 여부가 지정된다.

TRM의 사용(1406)은 인증 모듈(101) 등의 내템퍼 영역으로의 억세스를 인정할 것인지의 여부를 나타내는 항목이며, 그 내템퍼 영역으로 억세스를 할 수 있는 일시, 억세스를 할 수 없는 일시, 억세스 회수나, 내템퍼 영역을 가지는 IC 카드내에서 동작하는 카드 어플리케이션이며, 억세스 가능한 카드 어플리케이션, 이용 가능한 IC 카드 커맨드의 종류 등을 들 수 있다.

어플리케이션의 사용(1407)은 어플리케이션이 연휴 가능한 다른 어플리케이션을 지정하는 항목이다. 예를 들면, 어드레스장이나 메일, 스케쥴러, 게임 등이다. 또한, 다른 어플리케이션과 제휴 가능한 일시도 포함될 수 있다. 단말(100)이 휴대전화인 경우에는, 전화 통신시에 어플리케이션이 통화와 병행하여 동작하는 것을 인정할 것인지의 여부, 통화의 개시시에 정지 또는 종료해야 할 것인지의 여부를 지정하도록 할 수 있다.

접촉/비접촉 IC 카드 I/F의 사용(1408)은, 단말(100)과 교신이 가능한 접촉/비접촉 IC 카드나 IC 카드 리더 라이터와 교신하기 위한 인터페이스의 사용을 인정할 것인지의 여부에 관한 항목이다. 그 인터페이스가 사용 가능한 시간, 사용 가능 한 토탈 시간, 사용 가능/불가능한 회수, 사용 가능 I/F(Type A, Type B, Type C 등), 이용 가능한 IC 카드 커맨드의 종류 등을 들 수 있다.

사용 일시(1410)는 어플리케이션이 동작 가능한 일시를 지정한다. 또는, 어플리케이션의 동작을 정지해야 할 일시를

지정한다.

다운로딩부(102)에 다운로딩된 어플리케이션이, 리소스를 사용하는 때는, TRM 억세스 라이브러리부(401)에 대해 리소스에 사용의 요구를 내고, TRM 억세스 라이브러리부(401)는 어플리케이션 이용 리소스 정보 유지 수단(1301)에 유지되어 있는 어플리케이션 이용 리소스 정보를 참조하고, 요구된 리소스가 사용 가능한지의 여부를 판단하고, 만약 사용 가능하면, 그 요구된 리소스를 어플리케이션에 사용시킨다.

어플리케이션 이용 리소스 정보는, 다운로딩부(102)에 다운로딩되는 어플리케이션과 함께 다운로딩되어, 어플리케이션 이용 리소스 정보 유지 수단(1301)에 유지되도록 되어 있을 수 있다. 도15는 어플리케이션과 함께 어플리케이션 이용 리소스 정보가 다운로딩되는 데이터를 모식적으로 표현한 도면이다. 먼저, 어플리케이션 본체인 어플리케이션 데이터(1501)가 있고, 어플리케이션 데이터(1501)를 인증하기 위한 서명인 어플리케이션 데이터 서명 데이터(1502)가 이어지고, 그 뒤에, 어플리케이션 이용 리소스 정보(1503)가 있고, 어플리케이션 이용 리소스 정보를 인증하기 위한 어플리케이션 이용 리소스 정보 서명 데이터(1504)가 있다. 어플리케이션 이용 리소스 정보(1503)에는, 부호(1505)가 부여된 부분과 같이, 「IrDA 1」에 의해, IrDA가 사용 가능하고, 「Bluetooth 0」에 의해, Bluetooth는 사용 불가능하다는 것 등이 표현된다.

또한, 어플리케이션 이용 리소스 정보는 인증 모듈(101)에 저장되고, 필요에 따라서 판독되고, 어플리케이션 이용 리소스 정보 유지 수단(1301)에 의해 유지되도록 되어 있을 수 있다.

이와 같이, 어플리케이션 이용 리소스 정보 유지 수단(1301)을 TRM 억세스 라이브러리부(401)가 가지는 구성에 의해, 다운로딩된 어플리케이션이 사용 가능한 자원을 제한하는 것이 가능해진다. 이것에 의해, 어플리케이션 이용 리소스 정보를 어플리케이션의 제작자나 서비스 제공자 등에 대해 발행하여 대가를 얻는 비지니스를 수행할 수 있다. 이 로컬 리소스의 허가의 제어에는, 어플리케이션 이용 리소스 정보를 사용할 수 있고, 특정한 어플리케이션에 대해 로컬 리소스의 이용을 세세하게 허가/불허로 할 수 있다. 로컬 리소스의 허가를 수행하는 경우에는, 어플리케이션 이용 리소스 정보의 발행자에게 사용료를 지불하도록 하면, 어플리케이션 이용 리소스 정보의 발행에 의한 상거래가 가능해진다. 또한, 단말(100)의 이용자는 대가를 지불함으로써, 단말(100)에 다운로딩된 어플리케이션의 리소스의 사용에 대한 제한이 더욱 적은 어플리케이션 이용 리소스 정보를 입수하는 것이 가능해지고, 단말(100)의 이용자를 상대로 하는 상거래도 실현할 수 있다.

또한, 실시예2 내지 실시예5에 있어서, 다운로딩부(102)가 사용 허락서를 다운로딩할 수 있다. 「사용 허락서」란, 다운로딩 어플리케이션의 서명이 부가된 어플리케이션 이용 리소스 정보이다. 「다운로딩 어플리케이션」이란, 다운로딩부(102)에 다운로딩된 어플리케이션이다. 「서명이 부가된 어플리케이션 이용 리소스 정보」란, 어플리케이션 이용 리소스 정보에 그 어플리케이션 이용 리소스 정보의 서명을 부가한 것이다. 어플리케이션 이용 리소스 정보는, 다운로딩된 어플리케이션이 단말(100)이나 인증 모듈(101)의 리소스를 사용하기 위한 허가증이기 때문에, 어플리케이션 이용 리소스 정보의 진실성을 보증하는 것이 중요하고, 그 때문에 서명을 어플리케이션 이용 리소스 정보에 부가하도록 한다.

또, 다운로딩된 어플리케이션의 서명의 검증과, 어플리케이션 이용 리소스 정보의 서명의 검증은 동시에 수행될 수 있고, 다른 때에 수행될 수도 있다. 예를 들면, 최초에 어플리케이션의 서명의 검증이 수행되고, 어플리케이션이 동작하여, 리소스에 억세스를 했을 때에, 어플리케이션 이용 리소스 정보의 서명의 검증이 수행되어, 진짜인 것인지를 확인하여 리소스의 억세스가 허용될 것인지의 여부를 판단하도록 할 수 있다. 또한, 다운로딩된 어플리케이션의 서명과 어플리케이션 이용 리소스 정보의 서명의 작성자는 동일하거나 다를 수 있다. 서명의 작성자가 다를 수 있는 이유는, 어플리케이션의 작성자와 어플리케이션 이용 리소스 정보의 발행자는 다르고, 전자가 후자에 대해 리소스의 이용의 허가를 신청하여, 후자로부터 어플리케이션 이용 리소스 정보의 발행을 받는 일이 있기 때문이다. 또, 리소스의 이용의 허가의 신청시에 대가의 수수가 수행될 수 있다.

또한, 사용 허락서의 어플리케이션 이용 리소스 정보에, 어플리케이션이 리소스를 억세스할 수 있는 시간적 한도를 나타내는 기한일 정보가 포함되어 있는 경우에는, 그 기한일 정보에 기초하여 인정될 수 있는 시간적 정보가 이미 기한이 지난 경우에는, 다운로딩부(102)는 사용 허락서를 다운로딩하여, 사용 허락서를 갱신 하도록 할 수 있다.

또한, 다운로딩된 어플리케이션의 실행시, 또는/및 어플리케이션의 인증시에 사용 허락서를 다운로딩하도록 할 수 있다. 사용 허락서의 다운로딩은 단말(100)이 통신할 수 있는 서버에서 수행할 수 있다. 또한, 인증 모듈(101)에서 수행할 수도 있다.

또한, 다운로딩부(102)는 서버에서 다운로딩한 사용 허락서를 계속 유지하는 것도 고려할 수 있지만, 이 경우, 사용 허락서가 서버내에서 갱신되어 있는 경우가 있고, 다운로딩부(102)에 유지되고 있는 사용 허락서가 실효되어 있을 가능성이 있다. 그래서, 다운로딩부(102)는 다운로딩된 어플리케이션의 실행시, 또는/및 어플리케이션의 인증시에, 다운로딩된 사용 허락서의 유효성을 서버에 문의하도록 할 수 있다.

또한, 다운로딩부(102)는, 다운로딩부(102) 또는 단말(100)의 다른 부가 사용 허락서의 내용을 서버에 대해 온라인으로 문의하여, 어플리케이션의 리소스의 이용이 허가되어 있는지의 여부를 문의하도록 할 수 있다.

(실시예6)

도16은 본 발명의 실시예6에 관한 어플리케이션 인증 시스템의 기능 블록도를 나타낸다. 본 실시예는 실시예4 또는 실시예5의 어플리케이션 인증 시스템의 단말(100)의 TRM 억세스 라이브러리부(401)가 어플리케이션 이용 리소스 정보 출력 수단(1601)을 구비한다.

어플리케이션 이용 리소스 정보 출력 수단(1601)은 인증 모듈 인증부(1101) 에 의한 인증이 된 인증 모듈에 대해 어플리케이션 이용 리소스 정보를 출력한다.

본 실시예에 있어서, 인증 모듈(101)의 TRM부(103)는 어플리케이션 이용 리소스 정보 출력 수단(1601)에서 출력된 어플리케이션 이용 리소스 정보를 내템퍼 영역에 재기록 가능하게 유지하는 일을 수행한다.

이와 같이 내템퍼 영역에 유지된 어플리케이션 이용 리소스 정보는, 필요에 따라서 단말(100)로 판독되고, 다운로딩부(102)에 다운로딩된 어플리케이션이 자원을 사용하고자 할 때에, 그 자원을 사용할 수 있는지의 여부를 판단하기 위해서 참조된다.

이와 같이, 단말(100)의 TRM 억세스 라이브러리부(401)가 어플리케이션 이용 리소스 정보 출력 수단(1601)을 포함하고, 어플리케이션 이용 리소스 정보 출력 수단(1601)에 의해 출력된 어플리케이션 이용 리소스 정보를 TRM부(103)가 유지함으로써, 인증 모듈(101)에 유지된 상태로 어플리케이션 이용 리소스 정보가 제공된 후에도, 필요에 따라서 어플리케이션 이용 리소스 정보를 재기록 할 수 있다. 예를 들면, 어플리케이션 이용 리소스 정보의 유효 기한을 재기록하는 것 등이 가능해진다. 또한, 예를 들면, 서비스의 제공자나 서비스의 이용자가 대가를 지불함으로써, 내템퍼 영역이 유지하고 있는 어플리케이션 이용 리소스 정보를, 어플리케이션의 사용 가능한 자원을 제한하는 일이 적은 것으로 갱신할 수 있다. 재기록은, 미리 서명 인증 정보 입력부(502)에 의해서 인증된 TRM 억세스 라이브러리부(401)에 의해 수행되기 때문에, 부정한 재기록을 방지할 수 있다.

(실시예7)

도17은 본 발명의 실시예7에 관한 어플리케이션 인증 시스템의 기능 블록도를 나타낸다. 본 실시예는, 실시예5 또는 실시예6에서의 어플리케이션 인증 시스템의 단말(100)이 어플리케이션 이용 리소스 정보 다운로딩부(1701)를 포함하고 있다.

어플리케이션 이용 리소스 정보 다운로딩부(1701)는 서명(1703)이 부가된 어플리케이션 이용 리소스 정보(1702)를 다운로딩한다. 상기 다운로딩은 도15에 도시한 바와 같이 다운로딩부(102)로 다운로딩되는 어플리케이션과 함께 다운로딩될 수 있다. 또한, 다운로딩부(102)로 다운로딩된 어플리케이션과는 별도로 다운로딩될 수도 있다. 예를 들면, 먼저 어플리케이션을 다운로딩해 두고, 그 어플리케이션이 자원에 억세스하려고 할 때에, 어플리케이션 이용 리소스 정보가 다운로딩될 수 있다.

본 실시예에서, TRM 억세스 라이브러리부(401)가 어플리케이션 이용 리소스 정보 다운로딩부(1701)로 다운로딩된 어플리케이션 이용 리소스 정보(1702)에 부가된 서명(1703)을 인증할 수 있다. TRM 억세스 라이브러리부(401)는, 인증 모듈(101)에 의해서 인증되기 때문에, 정확하게 인증된 TRM 억세스 라이브러리부(401)에 의해, 어플리케이션 이용 리소스 정보(1702)의 서명(1703)을 인증한 결과는 인증 모듈(101)에 있어서 신뢰할 수 있는 것이 되어 있다. 따라서, 이와 같이 인증된 어플리케이션 이용 리소스 정보(1702)에 따라서, 다운로딩된 어플리케이션이 인증 모듈(101)로 억세스를 허가해도 부정한 조작은 발생하지 않는 것이 보증된다.

(실시예8)

도18은 본 발명의 실시예8에 관한 어플리케이션 인증 시스템의 기능 블록도를 나타낸다. 본 실시예는, 실시예5 또는 실시예6에 있어서의 어플리케이션 인증 시스템의 단말(100)이 어플리케이션 이용 리소스 정보 다운로딩부(1701)와, 어플리케이션 이용 리소스 정보 서명 인증 정보 출력부(1801)를 포함하고, 인증 모듈(101)이 어플리케이션 이용 리소스 정보 서명 인증 정보 입력부(1802)와, 어플리케이션 이용 리소스 정보 서명 인증부(1803)를 포함하고 있다. 본 실시예는, 실시예7에 있어서, TRM 억세스 라이브러리부(401)가 어플리케이션 이용 리소스 정보(1702)에 부가된 서명(1703)을 인증하는 대신에, 인증 모듈에 의해서 서명(1703)을 인증하는 형태이다.

어플리케이션 이용 리소스 정보 다운로딩부(1701)는 서명(1703)이 부가된 어플리케이션 이용 리소스 정보(1702)를 다운로딩한다.

본 실시예에 있어서, TRM 억세스 라이브러리부(401)는 어플리케이션 이용 리소스 정보 다운로딩부(1701)로 다운로딩된 어플리케이션 이용 리소스 정보(1702)로부터 서명 인증용 다이제스트를 생성하고, 어플리케이션 이용 리소스 정보 서명 인증 정보 출력부(1801)는 생성된 서명 인증용 다이제스트와 서명(1703)을 포함하는 서명 인증 정보(1806)를 인증 모듈로 출력한다.

어플리케이션 이용 리소스 정보 서명 인증 정보 입력부(1802)는 어플리케이션 이용 리소스 정보 서명 인증 정보 출력부(1801)에서 출력된 서명 인증 정보(1806)를 입력한다. 서명 인증 정보(1806)는 TRM 억세스 라이브러리부(401)에서 생성된 서명 인증용 다이제스트(1804)와, 어플리케이션 이용 리소스 정보(1702)에 부가된 서명(1703)인 서명(1805)을 포함한다.

어플리케이션 이용 리소스 정보 서명 인증부(1803)는, 어플리케이션 이용 리소스 정보 서명 인증 정보 입력부(1802)로부터 입력되는 서명 인증용 다이제스트(1804)와 서명(1805)에 기초하여 서명의 검증을 수행한다.

도19는 본 실시예에 있어서의 단말(100)의 동작을 설명하는 순서도이다. 단계(S1901)에서, 어플리케이션 이용 리소스 정보(1702)로부터 TRM 억세스 라이브러리부(401)로 서명 인증용 다이제스트(1804)를 생성한다. 단계(S1902)에서, 서명 인증용 다이제스트(1804)와 서명(1805)을 포함하는 서명 인증 정보(1806)를 어플리케이션 이용 리소스 정보 서명 인증 정보 출력부(1801)에 의해 인증 모듈(101)로 출력한다. 단계(S1903)에서, 인증 모듈(101)로부터 인증 결과를 받는 것을 수행한다.

도20은 본 실시예에 있어서의 인증 모듈(101)의 동작을 설명하는 순서도이다. 단계(S2001)에서, 서명 인증 정보(1806)를 어플리케이션 이용 리소스 정보 서명 인증 정보 입력부(1802)에 의해 입력한다. 단계(S2002)에서, 서명 인증용 다이제스트(1804)와 서명(1805)에 기초하여 서명(1805)의 검증을 어플리케이션 이용 리소스 정보 서명 인증부(1803)에서 수행한다. 단계(S2003)에서, 검증의 결과를 단말(100)로 되돌려준다.

이러한 실시예에 있어서, 인증 모듈(101)에 의해서 인증된 TRM 억세스 라이브러리부(401)에 의해 생성된 서명용 인증용 다이제스트에 기초하여 어플리케이션 이용 리소스 정보(1702)의 서명이 인증되기 때문에, 그 인증의 결과는 신뢰할 수 있는 것이 된다. 또한, 어플리케이션 이용 리소스 정보 서명 인증부(1803)에서의 인증을 암호화에 기초하지 않고, 인증 모듈(101)의 TRM부에 저장된 서명에 적합한지의 여부로 인증하는 것도 가능해지기 때문에, 인증을 간단하게 수행할 수 있다.

(실시예9)

본 발명의 실시예9는, 인증 모듈내에서 동작하는 인증 모듈내 어플리케이션이, TRM 억세스 라이브러리부가 인증 모듈에 의해서 인증되어 있음을 조건으로, 단말내에서 동작하는 어플리케이션으로부터의 억세스를 받아들이는 것을 특징으로 한다.

도21은 본 실시예에 관한 어플리케이션 인증 시스템의 기능 블록도를 나타낸다. 본 실시예는, 실시예2 내지 실시예3에 있어서의 어플리케이션 인증 시스템의 단말(100)이 단말 어플리케이션 유지부(2101)를 포함하고, 인증 모듈(101)은, 인증 모듈내 어플리케이션 유지부(2103)를 구비하는 TRM부(103)를 갖는다.

단말 어플리케이션 유지부(2101)는 인증 모듈(101)의 TRM부에 억세스를 하는 단말 어플리케이션(2102)을 유지한다. 「단말 어플리케이션(2102)」이란, 단말(100)의 내부에서 실행되는 어플리케이션이다. 어플리케이션은 다운로딩부(102)에 의해서 다운로딩된 어플리케이션일 수 있고, 또한, 단말의 ROM에 유지되어 있는 어플리케이션일 수도 있다. 「유지한다」란, 단말 어플리케이션(2102)을 실행 가능하게 하는 것이다. 따라서, 단말 어플리케이션 유지부(2101)는 단말 어플리케이션(2102)을 실행시키기 위해서, 단말 어플리케이션(2102)의 전부 또는 일부를 로드하는 단말(100)의 재기록 가능한 메모 리 영역에 의해 실현된다.

인증 모듈내 어플리케이션 유지부(2103)는 인증 모듈내 어플리케이션(2104)을 유지한다. 「인증 모듈내 어플리케이션(2104)」이란 인증 모듈(101)내에서 동작하는 어플리케이션이다. 인증 모듈(101)이 IC 카드이면, 인증 모듈내 어플리케이션(2104)은 카드 어플리케이션이 된다. 「유지한다」란, 인증 모듈내 어플리케이션(2104)을 실행 가능하게 하는 것이다. 따라서, 인증 모듈내 어플리케이션 유지부(2103)는 인증 모듈내 어플리케이션(2104)을 실행시키기 위해서, 인증 모듈내 어플리케이션(2104)의 전부 또는 일부를 로드하는 인증 모듈의 재기록 가능한 메모리 영역에 의해 실현된다.

본 실시예에 있어서, 인증 모듈내 어플리케이션(2104)은, TRM 억세스 라이브러리부 인증부(402)에 의한 TRM 억세스 라이브러리부(401)의 인증을 조건으로 하여 단말 어플리케이션(2102)으로부터의 억세스를 받아들여 동작한다. 이 때문에, 인증 모듈내에 TRM 억세스 라이브러리부(401)가 인증되었는지의 여부를 나타내는 값을 저장해 두고, 도22에 도시한 바와 같이, 단계(S2201)에서, 그 값 자신 또는, 그와 같은 값이 존재하는지 여부를 조사하여 TRM 억세스

라이브러리부(401)의 인증이 성공했는지의 여부를 판정한다. 만약에 인증이 성공했으면, 단계(S2202)로 이행하고, 단말 어플리케이션(2102)으로부터의 억세스를 받아들인다. 단계(S2201)의 판정은, 인증 모듈내 어플리케이션(2104)에서 수행하는 경우와, 인증 모듈내 어플리케이션(2104) 이외에서 수행하는 경우가 있다. 인증 모듈내 어플리케이션(2104)에서 수행하는 경우는, 인증 모듈내 어플리케이션(2104)이 기동 한 후, 단말 어플리케이션(2102)이 억세스하기까지의 사이에, TRM 억세스 라이브러리부(401)가 인증됐는지의 여부를 나타내는 값을 보고 판단하게 된다. 인증 모듈내 어플리케이션(2104) 이외에 있어서 단계(S2201)의 판정을 수행하는 경우는, 인증 모듈내 어플리케이션(2104)이 기동될 때에, TRM 억세스 라이브러리부(401)가 인증되었는지의 여부를 나타내는 값이 확인된다.

인증 모듈(101)이 IC 카드인 경우에는, 인증 모듈내 어플리케이션(2104)을 기동하는 것은, 카드 관리자이기 때문에, 카드 관리자가 인증 모듈내 어플리케이션(2104)을 기동할 것인지의 여부를, TRM 억세스 라이브러리부(401)가 인증되었는지의 여부를 나타내는 값을 보고 판단하게 된다. 또한, 인증 모듈(101)의 단말과의 인터페이스 부분(도21에서 도시하지 않음)이, 단말 어플리케이션(2102)으로부터 인증 모듈내 어플리케이션(2104)으로의 억세스를 허가할 것인지의 여부를 결정할 때에, TRM 억세스 라이브러리부(401)가 인증되었는지의 여부를 나타내는 값을 보고 판단하도록 할 수 있다.

또한, 인증 모듈내 어플리케이션(2104)이, 단말 어플리케이션(2102)으로부터의 억세스를 접수할 때마다, TRM 억세스 라이브러리부(401)가 인증되었는지의 여부를 나타내는 값을 보고, 그 억세스를 받아들여 동작할 것인지의 여부를 결정하도록 할 수 있다. 도23은 이러한 경우의 인증 모듈내 어플리케이션의 동작을 설명하는 순서도이다. 단계(S2301)에 있어서, 단말 어플리케이션(2102)으로부터의 억세스를 인증 모듈내 어플리케이션(2104)에서 접수한다. 단계(S2302)에서, TRM 억세스 라이브러리부(401)가 인증되었는지의 여부를 나타내는 값을 인증 모듈내 어플리케이션(2104)이 체크하여, TRM 억세스 라이브러리부(401)의 인증이 성공했는지의 여부를 판단하고, 만약에 그 인증이 성공했으면, 단계(S2303)에서, 단말 어플리케이션(2102)으로부터의 억세스를 받아들여 동작한다.

도24는 TRM 억세스 라이브러리부(401)가 인증되었는지의 여부를 나타내는 값을 TRM부(103)에 저장하도록 한 형태를 나타낸다. TRM부(103)는 인증 결과 식별자 생성 수단(2401)을 포함하고 있다. 인증 결과 식별자 생성 수단(2401)은, TRM 억세스 라이브러리부 인증부(402)에 의한 TRM 억세스 라이브러리부(401)의 인증 성공을 조건으로 하여 인증 결과 식별자(2402)를 생성한다. 인증 모듈내 어플리케이션(2104)은 인증 결과 식별자(2402)의 존재를 조건으로 하여, 단말 어플리케이션(2102)으로부터의 억세스를 받아들인다.

또한, 인증 결과 식별자(2402)는, TRM 억세스 라이브러리부 인증부(402)에 의한 TRM 억세스 라이브러리부(401)의 인증 성공을 나타낼 뿐만 아니라, 인증의 실패를 나타내는 내용을 가질 수도 있다. 이 경우에는, 인증 결과 식별자 생성 수단(2401)은 TRM 억세스 라이브러리부 인증부(402)에 의한 TRM 억세스 라이브러리부(401)의 인증 성공/실패에 따른 내용을 가지는 인증 결과 식별자(2402)를 생성한다. 또한, 인증 모듈내 어플리케이션(2104)은, 인증 결과 식별자(2402)의 내용을 보고, 인증이 성공했는지의 여부를 판단한다.

도25는 인증 모듈(101)이 IC 카드인 경우에 있어서의, 인증 결과 식별자의 실현 방법을 나타낸다. 도25에 있어서, TRM 억세스 라이브러리부(401)를 인증하는 것이 카드 어플리케이션 A(2501)이며, TRM 억세스 라이브러리부(401)가 인증되면, 재기록 가능한 메모리 영역, 예를 들면, RAM 영역(2503)에 인증 결과 식별자를 설정한다. 도25에 있어서, 깃발 표시가 인증 결과 식별자를 모식적으로 표현하고 있다. RAM 영역(2503)은, 카드 어플리케이션 A(2501)는 판독 기록을 할 수 있지만, IC 카드내의 어플리케이션 사이에서, 각각 나쁜 영향을 서로 미치게 하지 않도록, 각 어플리케이션을 독립적으로 기동시키기 위한 방화벽 기능에 의해, 다른 카드 어플리케이션 B(2502)는 RAM 영역(2503)에 직접 억세스할 수 없다. 그래서, 카드 어플리케이션 A(2501)가 상대방을 지정하여 인터페이스를 공개할 수 있는 공개 인터페이스(Sharable Interface) 기능을 이용하여 공개 인터페이스(2504)를 제공하고, 이 공개 인터페이스(2504)를 통해서, 단말 어플리케이션(2402)으로부터 억세스가 된 카드 어플리케이션(2502)은 RAM 영역(2503)에 인증 결과 식별자가 존재하는지의 여부를 확인한다.

또한, 도26은 인증 모듈(101)이 IC 카드인 경우에 있어서의, 인증 결과 식별자의 다른 실현 방법을 나타낸다. 부호(2601), (2602)가 부여된 직사각형은 데디케이트 파일(DF)을 나타내고 있다. 각 DF는 각 카드 어플리케이션에 대응하고 있다. 이 때문에, DF가 셀렉트되면 대응하는 카드 어플리케이션이 기동한다. 이후에는, 부호(2601)의 DF는 카드 어플리케이션 A에 대응하고, 마찬가지로 부호(2602)의 DF는 어플리케이션 B에 대응하고 있다고 하자. 부호(2603), (2604), (2605), (2606), (2607)가 부여된 직사각형은 엘레멘터리 파일(EF:Elementary File)을 나타내고 있다. DF에 대응하는 카드 어플리케이션이 기동하면, 그것에 대응하는 DF 바로 아래의 EF를 조작할 수 있게 되어 있다. 예를 들면, 부호(2601)의 DF가 셀렉트되고, 카 드 어플리케이션 A가 기동하면, 카드 어플리케이션 A는 부호(2603), (2604)의 EF를 억세스할 수 있게 된다.

이후에서는, 카드 어플리케이션 A가 TRM 억세스 라이브러리부(401)를 인증하고, 정확하게 인증된 경우에, 부호(2604)의 EF에 인증 결과 식별자를 설정한다고 가정한다. 부호(2604)가 부여된 EF의 상태를 부호(2601)가 부여된 DF의 보안 상태에 포함시킴으로써, DF와 EF가 형성하는 나무 구조에 있어서의 부호(2601)가 부여된 DF의 자손(子孫)에 상당하는 DF의 셀렉트를 제어할 수 있다. 즉, 부호(2602)의 DF의 셀렉트는, 부호(2601)가 부여된 DF의 자손중

어느 하나, 여기서는, 부호(2604)가 부여된 EF 내의 식별자의 존재를 조건으로 하는 설정을 한다. 즉, 카드 어플리케이션 A에 의한 TRM 억세스 라이브러리부(401)의 인증의 결과에 의해, 카드 어플리케이션 B에 대응하는 DF의 셀렉트를 제어할 수 있게 되기 때문에, 카드 어플리케이션 B를 TRM 억세스 라이브러리부(401)가 인증된 경우에만 기동시킬 수 있게 된다.

이러한 실시예에 의해, TRM 억세스 라이브러리부(401)가 인증 모듈(101)에 의해서 인증되지 않는 한, 인증 모듈내 어플리케이션(2104)은 단말 어플리케이션(2102)으로부터 억세스되는 일이 없기 때문에, 인증 모듈(101)의 보안이 유지된다.

또한, 인증 모듈내 어플리케이션 유지부(2103)는 TRM부(103)의 외부에 있을 수 있다. 이 경우, 인증 모듈내 어플리케이션(2104)은 TRM 억세스 라이브러리부 인증부(402)에 의해 TRM 억세스 라이브러리부(401)가 인증되어 있는지의 여부를 조사 하여 단말 어플리케이션(2102)의 억세스를 받아들여 동작하게 된다.

(실시예10)

도27은 본 발명의 실시예10에 관한 어플리케이션 인증 시스템의 기능 블록도를 나타낸다. 본 발명의 실시예10에서는, 인증 모듈내 어플리케이션은 단말에서 동작하는 어플리케이션의 인증을 조건으로 하여, 그 어플리케이션으로부터의 억세스를 받아들여 동작한다. 도27은 본 실시예에 있어서의 어플리케이션 인증 시스템의 기능 블록도를 나타낸다. 본 실시예에 있어서의 어플리케이션 인증 시스템에서는, 실시예9에서의 어플리케이션 인증 시스템의 TRM부(103)가 어플리케이션 인증 결과 식별자 생성 수단(2701)을 포함하고 있는 형태로 되어 있다.

어플리케이션 인증 결과 식별자 생성 수단(2701)은 TRM 억세스 라이브러리부(401)에 의한 어플리케이션의 인증 성공을 조건으로 하여 어플리케이션 인증 결과 식별자(2702)를 생성한다. 여기에서, 「어플리케이션」이란, 다운로딩부(102)로 다운로딩된 어플리케이션이다. 「TRM 억세스 라이브러리부(401)에 의한 어플리케이션의 인증」이란, 어플리케이션에 부가된 서명과 TRM 억세스 라이브러리부(401)가 생성한 서명 인증용 다이제스트에 기초하여 수행되는 인증을 의미한다.

본 실시예에 있어서, 인증 모듈내 어플리케이션(2104)은, 인증 성공을 나타내는 어플리케이션 인증 결과 식별자의 존재를 조건으로 하여, 단말 어플리케이션에 대해 인증 모듈내 어플리케이션(2104)에 대한 억세스를 가능하게 하고, 인증 모듈내 어플리케이션(2104)은 단말 어플리케이션으로부터의 억세스를 받아들인다.

예를 들면, 최초에 단말 어플리케이션(2102)이 동작을 하고 있고, 그것에 대해, 인증 모듈내 어플리케이션이 아직 동작을 하지 않고 있는 경우, 인증 모듈내 어플리케이션을 기동할 때에는, 어플리케이션 인증 결과 식별자(2702)가 존재하는 경우에 한해, 인증 모듈내 어플리케이션이 기동된다. 또는, 단말 어플리케이션(2102)과 인증 모듈내 어플리케이션(2104)의 양쪽이 기동되고 있는 경우에는, 단말 어플리케이션(2102)에서 인증 모듈내 어플리케이션(2104)으로 억세스가 발생한 경우에는, 어플리케이션 인증 결과 식별자(2702)의 존재하는 경우에 한해, 그 억세스를 받아들인다.

단말(100) 내에서 인증 모듈내 어플리케이션으로 억세스하는 단말 어플리케이션이 하나만 동작하는 것이면, 어플리케이션 인증 결과 식별자(2702)는 한 종류만 있으면 충분하다. 그러나, 그와 같은 단말 어플리케이션이 다수개, 단말(100) 내에서 동작하는 것이면, 어떤 단말 어플리케이션이 인증되었는가를 나타내기 위해, 단말 어플리케이션별로 어플리케이션 인증 결과 식별자가 어플리케이션 인증 결과 식별자 생성 수단(2701)에 의해 생성되게 된다. 또는, 2개 이상의 단말 어플리케이션이 동시에 인증 모듈내 어플리케이션으로 억세스하는 일이 없다고 보증되는 경우에는, 어플리케이션 인증 식별자는 한 종류만 생성되는 것으로 하고, 인증된 단말 어플리케이션이 인증 모듈내 어플리케이션으로 억세스하는 순간만 그 어플리케이션 인증 식별자가 생성되고, 인증된 단말 어플리케이션에 의한 인증 모듈내 어플리케이션의 억세스가 종료되면, 그 어플리케이션 인증 식별자를 삭제하도록 할 수 있다.

이러한 실시예에 의해, 인증을 받은 단말 어플리케이션만이 인증 모듈내 어플리케이션에 억세스할 수 있고, 인증 모듈(101)의 보안이 확보된다.

(실시예11)

도28은 본 발명의 실시예11에 관한 어플리케이션 인증 시스템의 기능 블록도를 나타낸다. 본 실시예에 있어서의 어플리케이션 인증 시스템은 단말과 인증 모듈과 어플리케이션을 단말에 다운로딩하는 서버로 이루어진다.

도28에 있어서, 단말(2801)은 다운로딩부(2804)를 구비한다. 다운로딩부(2804)는 어플리케이션을 다운로딩하는 부이다. 예를 들면, 서버(2803)로부터 어플리케이션을 다운로딩한다.

인증 모듈(2802)은 TRM부(2805)를 구비한다. TRM부(2805)는 어플리케이션의 인증의 처리를 위한 정보를 내템퍼

영역에 유지한다. 여기서, 「어플리케이션」이란, 단말(2801)의 다운로딩부(2804)에 다운로딩된 어플리케이션을 의미한다. 「어플리케이션의 인증」이란, 어플리케이션이 신뢰할 수 있는 사람에 의해서 발행됐는지의 여부, 부정한 동작을 하지 않는 것의 보증을 받고 있는 것인지의 여부, 또는, 신뢰할 수 있는 사람으로부터 발행되고 난 후 정정 또는 부정한 동작을 하지 않는 것이 보증된 후 정정이 되어 있는지의 여부 등 어플리케이션이 부정한 동작을 하지 않는 것을 확인하는 것이다. 이 처리의 방법으로서는, 통상, SHA-1이나 MD5 등의 입력 데이터를 처리하여 획득하는 결과 데이터가 일치하는 두개의 다른 입력데이터를 발견하기 어려운 해쉬함수를 이용하여, 어플리케이션의 실행을 위한 데이터를 입력 데이터로서 처리하여 획득할 수 있는 결과 데이터를 구하고, 그것을 암호 화한 것(소위 「서명」)이 사용된다. 따라서 「어플리케이션의 인증의 처리를 위한 정보」한, 이 서명 그 자체, 또는, 서명을 복호하여 해쉬값를 얻는데 필요한 복호키이다. 「내템퍼 영역」이란, 인증 모듈의 기억 영역이며, 그 기억 영역의 데이터를 부정하게 판독하는 것이나, 그 기억 영역의 데이터를 부정하게 재기록하는 것이 곤란한 기억 영역이다. 예를 들면, 그 기억 영역에 억세스하기 위해서는, 올바른 절차를 수행하지 않으면 억세스할 수 없는 하드웨어를 경유하도록 하거나, 기억 영역에 기억되어 있는 데이터가 암호화되어 있도록 한다.

서버(2803)는 단말 인증부(2806)를 구비한다. 단말 인증부(2806)는 단말(2801)을 통한 인증 모듈(2802)의 인증이 성공하는 것을 조건으로 단말(2801)의 인증이 성공했다고 판단한다. 즉, 서버(2803)는, 인증 모듈(2802)을 인증하는 것을 수행한다. 그 때, 서버(2803)와 인증 모듈(2802)은 통신을 수행할 필요가 있지만, 그 통신은 단말(2801)을 중계하여 수행된다. 서버(2803)가 인증 모듈(2802)의 인증을 수행하는 방법으로서는, 서버(2803)는 난수를 발생하고, 그 난수를 인증 모듈의 공개키에 의해서 암호화를 수행하고, 단말(2801)을 통하여 인증 모듈(2802)로, 암호화된 난수를 복호하도록 요구한다. 인증 모듈(2802)은, 내템퍼 영역에 저장되어 있는 인증 모듈(2802)의 비밀키를 사용한 복호에 의해 서버(2803)가 발생한 난수를 취득하고, 그것을 단말(2801)의 중계에 의해 서버(2803)로 되돌려 준다. 서버(2803)는 발생한 난수와 인증 모듈(2802)로부터 전송되어온 난수가 같은지의 여부를 판단하여 인증을 수행한다. 또는, 서버(2803)는 난수를 그대로 인증 모듈(2802)로 전송하고, 인증 모듈(2802)은 비밀키에 의해서 암호화를 수행하여, 그 결과를 서버(2803)로 되돌려주고, 서버(2803)는 인증 모듈(2802)의 공개키에 의해 복호를 수행하고, 인증 모듈(2802)로 전송한 난수와 같은지의 여부로 인증 모듈을 인증하는 방법도 있다.

인증 모듈(2802)은 단말(2801)에 장착되는 것이기 때문에, 서버(2803)가 인증 모듈(2802)을 인증함으로써, 인증 모듈(2802)이 장착된 단말(2801)도 인증되게 된다. 또한, 단말(2801)이 가지는 고유의 정보, 예를 들면, 단말(2801)의 제조 번호나, 기기의 종별을 나타내는 식별자, 단말(2801)의 ROM에 저장된 식별자, 버전 번호가 인증 모듈의 내템퍼 영역에 존재하는 것을 조건으로 하여 인증 모듈(2802)이 단말(2801)을 인증하는 것으로 하면, 인증이 더욱 확실한 것이 된다.

이것에 의해, 서버(2803)는 단말(2801)에 내템퍼 영역이 없더라도 단말(2801)을 인증하는 것이 가능해지고, 서버(2803)는, 단말(2801)을 정확하게 인증할 수 있고, 서버(2803)와 단말(2801)의 사이에서 과금 처리, 결제 처리 등을 수행할 수 있다. 또한, 서버(2803)에서 단말(2801)로 기밀성이 높은 데이터를 포함하는 어플리케이션을 다운로딩하는 것이 가능해지고, 복잡한 상거래 조작이 본 실시예에서의 어플리케이션 인증 시스템에 있어서 실행하는 것이 가능해진다.

(실시예12)

도29는 본 발명의 실시예12에 관한 어플리케이션 인증 시스템의 기능 블록도를 나타낸다. 본 실시예에서, 어플리케이션 인증 시스템은 실시예11과 같이 단말(2801), 인증 모듈(2802), 어플리케이션을 단말(2801)로 다운로딩하는 서버(2803)로 이루어진다.

단말(2801)은 다운로딩부(2804)와 TRM 억세스 라이브러리부(2901)를 포함하고 있다. 다운로딩부(2804)는 어플리케이션을 다운로딩한다. 이 경우, 어플리케이션은 서버(2803)에서 다운로딩된다. 또는, 서버(2803) 이외로부터 다운로딩될 수 있다. TRM 억세스 라이브러리부(2901)는 인증 모듈(2802)에 자신이 인증되는 것을 조건으로 하여 어플리케이션의 인증을 위한 처리를 한다. 즉, TRM 억세스 라이브러리부(2901)는 인증 모듈(2802)에 자신을 인증시켜, 정확하게 인증이 수행되면 다운로딩부(2804)로 다운로딩된 어플리케이션의 인증을 위한 처리를 수행한다. TRM 억세스 라이브러리부(2901)가 인증 모듈(2802)에 자신을 인증시키는 방법으로서는, 단말(2801)의 고유의 정보, 예를 들면, 제조 번호나, 종류를 나타내는 식별자, 또는, TRM 억세스 라이브러리부(2901)를 실현하는 소프트웨어의 일련 번호, 버전 번호 등을 인증 모듈(2802)로 출력하고, 인증 모듈(2802)의 내템퍼 영역으로 출력된 단말(2801)의 고유의 정보나 일련 번호, 버전 번호 등이 존재하는지의 여부로 수행하는 방법이 있다.

인증 모듈(2802)은 TRM부(2805)와 TRM 억세스 라이브러리부 인증부(2902)를 구비한다. TRM부(2805)는 TRM 억세스 라이브러리부(2901)를 인증하기 위한 정보인 TRM 억세스 라이브러리부 인증 정보를 내템퍼 영역에 유지한다. 「TRM 억세스 라이브러리부 인증 정보」로서는 상술한 바와 같이, 단말(2801)의 고유의 정보, 예를 들면, 제조 번호나 종류를 나타내는 식별자, 또는 TRM 억세스 라이브러리부(2901)를 실현하는 소프트웨어의 일련 번호, 버전 번호 등을 들 수 있다. TRM 억세스 라이브러리부 인증부(2902)는 TRM 억세스 라이브러리부 인증 정보에 기초하여 단말(2801)의 TRM 억세스 라이브러리부(2901)를 인증한다. 이 인증의 방법으로서는, 상술한 바와 같이, TRM 억세

스 라이브러리부(2901)에서 출력된 단말(2801)의 고유의 정보나 TRM 억세스 라이브러리부의 일련 번호, 버전 번호 등의 식별 정보를 TRM 억세스 라이브러리부 인증부(2902)가 받고, TRM부(2805)에 그 식별 정보가 존재하는지의 여부로 수행하는 방법이 있다. 이 인증의 결과는, TRM 억세스 라이브러리부 인증부(2902)에서 TRM 억세스 라이브러리부(2901)로 출력된다. 또한, 이 인증의 결과는, 인증 모듈(2802)내에 유지되고, 그 후의 단말과의 정보의 교환시에 참조되고, TRM 억세스 라이브러리부(2901)가 정확하게 인증되어 있으면, 인증 모듈(2802)은 정확한 정보의 교환을 수행하고, 그렇지 않으면, 정확하지 않은 정보의 교환을 수행하도록 한다.

서버(2803)는 서버 TRM 억세스 라이브러리부 인증부(2903)를 구비한다. 서버 TRM 억세스 라이브러리부 인증부(2903)는 단말(2801)의 억세스 라이브러리부(2901)를 통한 인증 모듈(2802)의 TRM부(2805)의 인증이 성공하는 것을 조건으로 하여 TRM 억세스 라이브러리부(2901)의 인증이 성공했다고 판단한다. 서버 TRM 억세스 라이브러리부 인증부(2903)가 단말(2801)의 억세스 라이브러리부(2901)를 통한 인증 모듈(2802)의 TRM부(2805)의 인증을 수행하는 방법으로서는 다음의 것이 있다. 즉, 서버(2803)는 난수를 발생하고, 그 난수를 인증 모듈(2802)의 공개키에 의해서 암호화를 수행하고, 단말(2801)을 통하여 인증 모듈(2802)로 암호화된 난수를 복호하도록 요구한다. 인증 모듈(2802)은 내템퍼 영역에 저장되어 있는 자신의 비밀키를 이용하여 난수를 복호하고, 그것을 단말(2801)을 통해 서버(2803)로 되돌려준 다. 서버(2803)는 발생한 난수와 인증 모듈(2802)로부터 전송되어온 난수가 같은지의 여부를 판단하여 인증을 수행한다. 또는, 서버(2803)는 난수를 그대로 인증 모듈(2802)로 전송하고, 인증 모듈(2802)은 자신의 비밀키에 의해서 암호화를 수행하고, 그 결과를 서버(2803)로 되돌려주고, 서버(2803)는 인증 모듈(2802)의 공개키에 의해서 복호를 수행하고, 인증 모듈(2802)로 전송한 난수와 같은지의 여부로 인증 모듈을 인증하는 방법도 있다.

도30은 서버 TRM 억세스 라이브러리부 인증부(2903)와, TRM 억세스 라이브러리부(2901)와, 인증 모듈(2802)의 상호 작용을 설명하는 시퀀스 도면이다. 단계(S3001)에서, TRM 억세스 라이브러리부(2901)에서 자신을 인증하는 요구가 인증 모듈(2802)로 출력되고, 단계(S3002)에서, 인증 모듈에서의 인증 결과가 출력된다. 단계(S3003)에서, 서버 TRM 억세스 라이브러리부 인증부(2903)에서 TRM 억세스 라이브러리부(2901)로 인증 요구가 출력되고, 이것에 대응하여, 단계(S3004)에서, 인증 요구가 TRM 억세스 라이브러리부(2901)에서 인증 모듈(2802)로 출력되고, 단계(S3005)에서, 인증 모듈은 자신이 서버 TRM 억세스 라이브러리부 인증부(2903)로 인증되도록 결과를 되돌려준다. 이 때, TRM 억세스 라이브러리부(2901)가 정확하게 인증되어 있는지의 여부에 의해서, 올바른 결과를 되돌려주거나, 정확하지 않은 결과를 되돌려준다. 단계(S3006)에서, TRM 억세스 라이브러리부(2901)는, 서버 TRM 억세스 라이브러리부 인증부(2903)로 인증 모듈(2802)에서 출력된 결과를 되돌려준다. 서버 TRM 억세스 라이브러리부 인증부(2903)는 이 결과를 조사하여, 인증 모듈(2802)이 인증할 수 있으면, TRM 억세스 라이브러리부(2901)도 인증된 것으로 판단하게 된다.

상술한 바와 같이, TRM 억세스 라이브러리부(2901)의 TRM 억세스 라이브러리부 인증부(2902)에 의한 인증의 결과는 인증 모듈(2802)내에 유지되고, 그 인증의 결과에 따라, 인증 모듈(2802)은 정확한 정보의 교환을 수행하거나, 수행하지 않기 때문에, 서버(2803)가 TRM 억세스 라이브러리부(2901)를 통하여 인증 모듈의 TRM 부의 인증을 수행하고, 정확하게 인증이 되면, TRM 억세스 라이브러리부(2901)의 인증이 성공했다고 판단해도 된다.

이것에 의해, 서버(2803)는 단말(2801)에 내템퍼 영역이 없더라도 단말(2801)을 인증하는 것이 가능해지고, 서버(2803)는 단말(2801)을 정확하게 인증할 수 있고, 서버(2803)와 단말(2801)의 사이에서 과금 처리, 결제 처리 등을 수행할 수 있다. 또한, 서버(2803)에서 단말(2801)로 기밀성이 높은 데이터를 포함하는 어플리케이션을 다운로딩하는 것이 가능해지고, 복잡한 상거래 조작이 본 실시예에서의 어플리케이션 인증 시스템에 있어서 실행하는 것이 가능해진다.

또한, TRM 억세스 라이브러리부(2901)가 TRM 억세스 라이브러리부 인증부(2902)에 의해 인증되면, TRM 억세스 라이브러리부(2901)는 인증 모듈에 의해 신뢰할 수 있는 것으로 판단된다. 이것에 의해, 다운로딩부(2804)에 다운로딩된 어플리케이션의 인증의 처리의 전부 또는 일부를 TRM 억세스 라이브러리부(2901)에 수행하도록 하면, TRM 억세스 라이브러리부(2901)에 의한 어플리케이션의 인증의 처리의 전부 또는 일부의 결과는 인증 모듈(2802)에 있어서 신뢰할 수 있는 것이 된다. 따라서, TRM 억세스 라이브러리부(2901)에 의한 어플리케이션의 인증의 처리 의 전부 또는 일부의 결과를 이용하여, 인증 모듈(2802)은 다운로딩부(2804)로 다운로딩된 어플리케이션의 인증을 수행하는 것이 가능해진다. 이 결과, 정확하게 인증된 어플리케이션에, 인증 모듈내의 데이터의 억세스를 허가할 수 있고, 복잡한 상거래의 조작을 수행할 수 있게 된다.

또, TRM 억세스 라이브러리부(2901)에 의한 어플리케이션의 인증을 위한 처리는 어플리케이션이 인증 모듈(2802)의 TRM부(2805)의 내템퍼 영역으로 억세스한 것을 조건으로 수행할 수 있다. 이것에 의해, 내템퍼 영역에 억세스하지 않는 어플리케이션의 인증을 수행할 필요가 없어진다.

또한, TRM 억세스 라이브러리부(2901)는 어플리케이션의 인증을 위한 처리를 어플리케이션이 다운로딩부(2804)로 다운로딩된 것을 조건으로 수행할 수 있다. 이것에 의해, 다운로딩된 어플리케이션이 모두 인증되고, 부정한 어플리케이션이 단말(2801)에서 실행될 우려가 없어진다.

또한, TRM 억세스 라이브러리부(2901)는 어플리케이션 인증을 위한 처리를 어플리케이션의 실행의 시작을 트리거로 하여 수행할 수 있다. 이것에 의해, 다운로딩되었지만, 실행되지 않는 어플리케이션의 인증을 생략할 수 있다.

(실시예13)

도31은 본 발명의 실시예13에 관한 어플리케이션 인증 시스템의 기능 블록도를 나타낸다. 본 실시예에 관한 어플리케이션 인증 시스템은 단말(2801), 인증 모듈(2802), 어플리케이션을 단말(2801)로 다운로딩하는 서버(2803)로 이루어진다.

단말(2801)은 다운로딩부(2804)와 TRM 억세스 라이브러리부(2901)를 포함하 고, TRM 억세스 라이브러리부(2901)는 서명용 다이제스트 생성 수단(3101)과, 다운로딩 어플리케이션 서명 취득 수단(3102)과, 어플리케이션 인증 데이터 출력 수단(3103)을 포함하고 있다.

다운로딩부(2804)는 어플리케이션(3104)을 다운로딩한다. 어플리케이션(3104)은 서버(2803)에서 다운로딩될 수 있다. 또한, 서버(2803) 이외, 예를 들면, 인증 모듈(2802)로부터 다운로딩될 수 있다. 본 실시예에 있어서는 어플리케이션(3104)은 어플리케이션(3104)의 서명(3105)과 함께 다운로딩되는 것으로 한다. 「서명(3105)과 함께 다운로딩된다」란, 동시에 다운로딩된다는 것뿐만 아니라, 어플리케이션(3104)의 다운로딩과 서명(3105)의 다운로딩은 전후에 수행될 수 있고, 후술하는 어플리케이션(3104)의 인증이 수행될 때 까지는, 어플리케이션(310)과 서명(3105)이 다운로딩되어 있음을 의미한다.

서명용 다이제스트 생성 수단(3101)은 어플리케이션으로부터 서명용 다이제스트를 생성한다. 즉, 다운로딩부(2804)에 다운로딩된 어플리케이션(3104)으로부터 서명용 다이제스트를 생성한다. 「서명용 다이제스트」란, 서명(3105)을 생성할 때에 사용된 해쉬함수와 동일한 해쉬함수를 이용하여 획득하는 값이다.

다운로딩 어플리케이션 서명 취득 수단(3102)은 어플리케이션(3104)의 다운로딩과 함께 다운로딩된 서명(3105)을 취득한다. 상술한 바와 같이 「어플리케이션(3104)의 다운로딩과 함께 다운로딩되었다」란, 동시에 다운로딩되었다는 것뿐만 아니라, 후술하는 어플리케이션(3104)의 인증이 수행될 때 까지는 어플리케이션(3104)과 서명(3105)의 다운로딩이 종료되어 있음을 의미한다.

어플리케이션 인증 데이터 출력 수단은 취득한 서명과 서명용 다이제스트 생성 수단(3101)에 의하여 생성된 서명용 다이제스트를 서버로 송신한다. 「취득한 서명」이란 다운로딩 어플리케이션 서명 취득 수단(3102)에 의해 취득된 서명(3105)이다.

서명용 다이제스트 생성 수단(3101)과 다운로딩 어플리케이션 서명 취득 수단(3102)과 어플리케이션 인증 데이터 출력 수단(3103)은, 다운로딩부(2804)에 다운로딩된 어플리케이션(3104)을 인증하기 위한 처리를 수행한다. 이 처리는, TRM 억세스 라이브러리부(2901)가 인증 모듈(2802)에 의해 인증된 것을 조건으로 하여 수행될 수 있다.

인증 모듈은 TRM부(2805)와 TRM 억세스 라이브러리부 인증부(2902)를 포함하고 있다. TRM부(2805)와 TRM 억세스 라이브러리부 인증부(2902)는 실시예12의 TRM부와 TRM 억세스 라이브러리부와 동일한 것이다.

서버(2803)는 서버 TRM 억세스 라이브러리부 인증부(2903)와 어플리케이션 인증 데이터 입력부(3106)와 서버 어플리케이션 인증부(3107)를 구비한다.

서버 TRM 억세스 라이브러리부 인증부(2903)는 실시예12에서의 것과 동일하며, 단말(2801)의 TRM 억세스 라이브러리부(2901)를 통한 인증 모듈의 TRM부(2805)의 인증이 성공하는 것을 조건으로 하여 TRM 억세스 라이브러리부(2901)의 인증이 성공했다고 판단한다.

어플리케이션 인증 데이터 입력부(3106)는 서버 TRM 억세스 라이브러리부 인증부(2903)에 의해 인증이 성공했다고 판단된 TRM 억세스 라이브러리부(2901)의 어플리케이션 인증 데이터 출력 수단(3103)에서 출력된 서명용 다이제스트와 서명을 입력한다.

서버 어플리케이션 인증부(3107)는 어플리케이션 인증 데이터 입력부(3106)에 입력된 서명용 다이제스트와 서명에 기초하여 어플리케이션의 인증을 수행한다. 인증은 서명을 복호하여 다이제스트를 구하고, 그 다이제스트가 서명용 다이제스트와 같은지의 여부를 판단함으로써 수행된다. 만약, 서명이 공개키 암호화 방식의 서버(2803)의 비밀키로 암호화되어 있는 경우에는, 어플리케이션 인증 데이터 입력부(3106)에 입력된 서명용 다이제스트를 서버(2803)의 비밀키로 암호화하고, 획득한 것이 어플리케이션 인증 데이터 입력부(3106)에 입력된 서명과 같은지의 여부로 판단할 수 있다.

도32는 본 실시예에서의 어플리케이션 인증 시스템을 구성하는 서버(2803), 단말(2801), 인증 모듈(2802)의 시간에 따른 상호 작용을 나타낸다. 단계(S3201)에서 단계(S3206)까지는, 실시예12에서의 도30에 있어서의 단계(S3001)에서 단계(S3006)까지와 동일하다. 단계(S3206) 후, 어플리케이션(3104)이 다운로딩부(2804)로 다운로딩되면, 서명용 다이제스트 생성 수단(3101)에 의해 어플리케이션(3104)의 서명용 다이제스트가 생성되고, 다운로딩 어플리케이션 서명 취득 수단(3102)에 의해 서명(3105)이 취득되고, 어플리케이션 인증 데이터 출력 수단(3103)에 의해 어플리케이션 인증 데이터 입력부(3106)로 서명용 다이제스트와 서명이 입력된다(단계(S3207)). 그 후, 서버 어플리케이션 인증부(3107)에 의해 어플리케이션 인증 데이터 입력부(3106)로 입력된 서명용 다이제스트와 서명에 의해 어플리케이션(3104)의 인증이 수행된다.

본 실시예에 의하면, 서버(2803)의 서버 TRM 억세스 라이브러리부 인증부(2903)가, 단말(2801)의 TRM 억세스 라이브러리부(2901)를 통한 인증 모듈(2802)의 TRM부(2805)의 인증이 성공하는 것을 조건으로 하여 단말(2801)의 TRM 억세스 라이브러리부(2901)의 인증이 성공했다고 판단한다. 이 때문에, 서버(2803)는, TRM 억세스 라이브러리부(2901)의 어플리케이션 인증 데이터 출력 수단(3103)이 어플리케이션 인증 데이터 입력부(3106)로 송신하는 어플리케이션(3104)의 서명용 다이제스트와 서명(3105)이 실제로 어플리케이션(3104)에 유래하는 것이라고 판단할 수 있고, 서버는 어플리케이션(3104)을 인증할 수 있다.

(실시예14)

도33은 본 발명의 실시예14에 관한 어플리케이션 인증 시스템의 기능 블록도를 나타낸다. 본 실시예13에서는, 다운로딩부(2804)로 다운로딩된 어플리케이션의 인증의 처리의 일부가 서버(2803)에서 실행되도록 되어 있었지만, 본 실시예에서는, 서버(2803) 이외에서 어플리케이션의 인증이 수행되고, 서버(2803)는 인증의 결과만을 취득하도록 되어 있다.

단말(2801)은 다운로딩부(2804)와 TRM 억세스 라이브러리부(2901)를 포함하고 있다. 다운로딩부(2804)는 어플리케이션을 다운로딩한다. TRM 억세스 라이브러리부(2901)는 인증 성공 정보 생성 수단(3301)과 인증 성공 정보 출력 수단(3303)을 포함하고 있다.

인증 성공 정보 생성 수단(3301)은 어플리케이션의 인증 성공을 나타내는 인증 성공 정보(3302)를 생성한다. 본 실시예에서, 어플리케이션의 인증은, TRM 억세스 라이브러리부(2901)내에서만 수행되도록 되어 있을 수 있다. 또한, TRM 억세스 라이브러리부(2901)와 인증 모듈(2802)이 협동하여 수행하도록 있어도 좋고, 인증 성공 정보 생성 수단(3301)은 그 인증의 결과를 취득하고, 인증이 성공했는지의 여부를 나타내는 인증 성공 정보(3302)를 생성한다. 이 때, 인증 성공 정보(3302)를 인증 모듈(2802)의 비밀키나 서버(2803)의 공개키에 의해 인증 성공 정보(3302)가 암호화될 수 있다.

인증 성공 정보 출력 수단(3303)은 인증 성공 정보 생성 수단(3301)에서 생성된 인증 성공 정보(3302)를 출력한다. 만약, 인증 성공 정보(3302)가 암호화되어 있지 않은 경우에는, 인증 성공 정보(3302)를 인증 모듈(2802)의 비밀키나 서버(2803)의 공개키에 의해 인증 성공 정보(3302)를 암호화하여 출력하도록 해도 좋다.

인증 모듈(2802)은 TRM부(2805)와 TRM 억세스 라이브러리부 인증부(2902)를 포함하고, 실시예13과 동일한 동작을 한다.

서버(2803)는 서버 TRM 억세스 라이브러리부 인증부와, 인증 성공 정보 입력부(3304)와, 서버 어플리케이션 인증부(3305)를 포함하고 있다.

서버 TRM 억세스 라이브러리부 인증부는 실시예13과 동일한 동작을 한다.

인증 성공 정보 입력부(3304)는 서버 TRM 억세스 라이브러리부 인증부에 의해 인증이 성공했다고 판단된 TRM 억세스 라이브러리부의 인증 성공 정보 출력 수 단에서 출력된 인증 성공 정보를 입력한다. TRM 억세스 라이브러리부(2901)가 서버 TRM 억세스 라이브러리부 인증부에 의해 인증이 성공했다고 판단된 경우에는, TRM 억세스 라이브러리부(2901)와 인증 모듈(2802)에 의해 출력되는 정보는, 서버(2803)에 있어서 신뢰할 수 있는 것이기 때문에, 인증 성공 정보 출력 수단(3303)의 내용은 신뢰할 수 있는 것으로 판단할 수 있다.

서버 어플리케이션 인증부(3305)는, 인증 성공 정보 입력부(3304)에 입력된 인증 성공 정보에 기초하여 어플리케이션의 인증을 수행한다. 예를 들면, 인증 성공 정보 출력 수단(3303)에 의해 출력된 인증 성공 정보가 인증 모듈(2802)의 비밀키나 서버(2803)의 공개키로 암호화되어 있는 경우에는, 복호를 수행하고, 인증 성공 정보의 내용을 조사하여 다운로딩부(2804)에 다운로딩된 어플리케이션을 인증한다.

(실시예15)

본 발명에서는, 어플리케이션(어플리케이션 프로그램)을 인증하기 위해서, 어플리케이션의 다운로딩을 수행하고 또한, 서명을 다운로딩하는 것이 필요하다. 이하에서는, 어플리케이션 중에 어플리케이션의 서명을 저장한 어플리케이션을 설명한다.

어플리케이션 프로그램은, 통상, 어플리케이션 본체와 어플리케이션 정의 파일로 나눌 수 있다. 「어플리케이션 본체」란, 어플리케이션 프로그램을 실행하기 위한 코드나 데이터이며, 「어플리케이션 정의 파일」이란, 어플리케이션 본체의 속성을 기술하는 파일이며, 「어플리케이션 본체의 속성」이란, 예를 들면, 어플리 케이션 본체의 크기, 어플리케이션 프로그램을 실행하기 위한 엔트리 포인트, 어플리케이션 프로그램의 실행시에 어플리케이션 프로그램에 넘겨져야 할 파라미터(Java(등록 상표)에 있어서는, 메인클래스의 기동 파라미터) 등이 있다. 어플리케이션 정의 파일에 있어서, 어플리케이션 본체의 속성을 기술하는 부분을 「속성 정보 저장부」로 부르기로 하면, 속성 정보 저장부에, 어플리케이션의 작성자가 자유롭게 이용할 수 있는 선택 영역이 존재하는 경우가 있다. 그래서, 이 선택 영역에, 어플리케이션 본체의 서명 데이터를 저장할 수 있다. 또, 어플리케이션 본체는, 코드와 데이터 그 자체가 아니라, 코드와 데이터를 압축한 것일 수 있다. 마찬가지로, 어플리케이션 정의 파일도 어플리케이션 본체의 속성의 기술을 압축한 것일 수도 있다.

도34는 Java(등록 상표) 어플리케이션, 특히, i어플리(iアプリ: NTT DoCoMo의 인터넷 접속 서비스)의 어플리케이션의 구조를 예시하고 있다. i어플리에 있어서는, 어플리케이션 본체는 JAR 파일(3401)에 저장되고, 어플리케이션 정의 파일은, ADF 파일(3402)로서 제공되도록 되어 있다. ADF 파일(3402)에 저장된 어플리케이션 본체의 속성은, 어플리케이션의 이름으로서 AppName라는 필수키에 의해 나타내지고, 어플리케이션 본체의 사이즈는 AppSize라는 필수키에 의해 나타내진다. 또한, 어플리케이션의 작성자가 자유롭게 이용할 수 있는 선택 영역으로서, AppParam라는 선택키로 나타내지는 것이 있다. 이 AppParam으로 나타내지는 영역은 최장 255바이트 이용가능하다. 한편, 어플리케이션 본체의 서명은 160비트의 타원 암호를 사용하면 20바이트 필요하고, 1024비트의 RSA 암호를 사용하는 것이면, 128바이트 필요하고, AppParam로 나타내지는 영역에 수용되게 된다. 따라서 어플리케이션 본체의 서명을 AppParam으로 표시되는 영역에 저장하는 것이 가능해진다.

도35는 이와 같이, 선택 영역에 어플리케이션 본체의 서명 데이터를 저장한 어플리케이션을 인증하는 경우의 동작을 설명하는 순서도이다. 단계(S3501)에서, 선택 영역에서 서명 데이터를 취득한다. 단계(S3502)에서, 단계(S3501)에서 취득된 서명 데이터를 이용하여, 서명을 검증하는 것을 수행한다. 이들 단계는 프로그램에 의해서 실행 가능하다.

또한, 도34는 어플리케이션 프로그램의 데이터 구조를 나타내고 있다고 간주할 수도 있다. 즉, 코드 및 데이터의 압축 파일인 JAR 파일을 저장하는 JAR 파일부(3401)와 어플리케이션의 정의 파일인 ADF 파일을 저장하는 ADF 파일부(3402)로 이루어지는 데이터 구조라고 간주할 수도 있다. 이러한 데이터구조에 있어서, ADF 파일부(3402)의 ADF 파일에는, 메인클래스의 기동 파라미터 등을 저장하는 AppParam으로 표시되는 영역이 있고, AppParam으로 표시되는 영역에 JAR 파일부(3401)에 저장되어 있는 JAR 파일의 서명이 저장되어 있다.

AppParam으로 표시되는 영역에 저장되는 JAR 파일의 서명은, 어플리케이션의 동작을 보증하는 사람에 의한 서명일 수 있다. 여기에, 「어플리케이션의 동작을 보증하는 사람」이란, JAR 파일에 저장된 코드와 데이터에 의해 동작하는 어플리케이션을 작성한 사람, 그 어플리케이션을 배포하는 사람, 그 어플리케이션의 작성한 사람, 그 어플리케이션의 동작을 검증하여 부정한 동작을 하지 않는 것을 보증하는 제3자 등이다.

도34에 도시한 어플리케이션 프로그램의 데이터 구조는, 비트열(bit stream)에 의해서 표현 가능하기 때문에, 이러한 비트열을 기록한 (SD)메모리 카드나, 플로피디스크, 콤팩트디스크 등의 기록 매체를 작성할 수 있다.

이러한 어플리케이션 프로그램에 의해, 어플리케이션을 다운로딩하면 어플리케이션 본체뿐만 아니라, 어플리케이션 본체의 서명도 다운로딩되게 되고, 별도로 서명을 다운로딩하는 시간을 생략할 수 있다.

(실시예16)

도37은 본 발명의 실시예16에 관한 단말의 기능 블록도를 예시한다. 본 실시예의 특징은 실시예1의 어플리케이션 인증 시스템에 있어서의 단말의 내부에 인증 모듈을 구비하도록 하여 일체화한 것이다.

본 실시예에 있어서, 단말(3700)은 다운로딩부(3701)와 TRM부(3702)를 구비한다.

다운로딩부(3701)는 어플리케이션을 다운로딩한다. 즉, 실시예1에 있어서의 다운로딩부(102)와 같은 기능을 갖는다.

TRM부(3702)는 어플리케이션의 인증을 위한 정보를 내템퍼 영역에 유지한다. 즉, 실시예1에서의 인증 모듈(101)내의 TRM부(103)와 같은 기능을 갖는다.

따라서, 본 실시예의 단말에서는 어플리케이션의 다운로딩의 절차나 다운로딩된 어플리케이션의 인증의 절차는 실시예1에 있어서의 것과 동일해도 좋다.

이와 같은 단말을 사용함으로써, 예를 들면, 서비스제공회사에서 단말(3700)의 다운로딩부(3701)로 다운로딩된 어플리케이션에 대해 인증의 처리를 수행하고, 그 인증의 처리가 성공한 경우에, 어플리케이션에 대해, TRM부(3702)의 유지된 정보등의 단말에 저장된 정보로의 억세스를 보안하게 허가하는 것이 가능해진다.

또한, 「단말」이란 단어를 사용했지만, 이것은, 휴대전화로 대표되는 휴대가능한 단말 등에 한정되는 것을 의미하지 않는다. 예를 들면, 가정용 전화 제품이더라도 좋고, 소위, 정보가전이나 네트워크 가전이라고 불리는 것이더라도 좋다. 그와 같은 제품을 예시 열거하면, 에어컨, 가습기, 제습기, 공기청정기, 전자레인지, 오븐, 냉장고, 식기 세척기, 전기포트, 다리미, 전기 청소기, 세탁기, 건조기, 전기 담요, 조명기기, 텔레비전 수상기, 라디오 수신기, 테이프 레코더 등의 오디오기기, 카메라, IC 레코더, 전화기, 팩시밀리 송수신기, 복사기, 프린터, 스캐너, PC 등을 들 수 있다(이 것은, 다음에 설명하는 실시예17에 있어서의, 「단말」에 관해서도 마찬가지다).

(실시예17)

도38은 본 발명의 실시예17에 관한 단말의 기능 블록도를 예시한다. 본 실시예의 특징은, 실시예2 등의 어플리케이션 인증 시스템에서의 단말의 내부에 인증 모듈을 구비하도록 하여 단말과 인증 모듈을 일체화한 것이다.

본 실시예에 있어서, 단말(3800)은 인증 모듈(3801)을 구비한 단말이며, 다운로딩부(3802), TRM 억세스 라이브러리부(3803)를 포함하고 있다. 인증 모듈(3801)은 TRM부(3804)와 TRM 억세스 라이브러리부 인증부(3805)를 포함하고 있다.

인증 모듈(3801)은 내템퍼 영역에 정보를 유지하고 그 정보를 이용하여 인증 을 위한 처리를 수행한다. 상세한 것에 관해서는 후술된다.

다운로딩부(3802)는 어플리케이션을 다운로딩한다. 즉, 실시예2 등에 있어서의 다운로딩부(102)와 같은 기능을 가진다.

TRM 억세스 라이브러리부(3803)는 인증 모듈(3801)에 자신이 인증되는 것을 조건으로 하여 어플리케이션의 인증을 위한 처리를 한다. 즉, 실시예2 등에 있어서의 TRM 억세스 라이브러리부(401)와 같은 기능을 가진다. 또한, 「인증 모듈(3801)에 자신이 인증된다」란, 후술하는 바와 같이, TRM 억세스 라이브러리부 인증부(3805)에 의해 인증이 되는 것을 의미한다.

TRM부(3804)는, TRM 억세스 라이브러리부 인증 정보를 상기 내템퍼 영역에 유지한다. 「TRM 억세스 라이브러리 인증 정보」란, TRM 억세스 라이브러리부를 인증하기 위한 정보이며, 실시예2의 정의와 같다. 따라서, TRM부(3804)는 실시예2 등의 TRM부(103)와 같은 기능을 가진다. 또, 내템퍼 영역은 TRM부(3804)의 내부에 있을 수 있고, 인증 모듈(3801)의 내부이며 TRM부(3804)의 외부에 있을 수도 있다.

TRM 억세스 라이브러리부(3805)는 TRM 억세스 라이브러리부 인증 정보에 기초하여 TRM 억세스 라이브러리부(3803)를 인증한다. 따라서, TRM 억세스 라이브러리부(3805)는 실시예2 등의 TRM 억세스 라이브러리부(402)와 같은 기능을 가진다.

도39는 본 실시예에 있어서의 단말(3800)의 처리의 흐름을 설명하는 순서도를 예시한다. 이 순서도에 예시된 처리에 있어서는, 다운로딩부(3802)에 어플리케이션이 다운로딩되어 있는 것이 가정되어 있다.

단계(S3901)에서, TRM 억세스 라이브러리부 인증부(3805)에 의해 TRM 억세스 라이브러리부(3803)의 인증의 처리를 수행한다.

단계(S3902)에서, TRM 억세스 라이브러리부(3803)가 인증되었는지의 여부가 판단되고, 혹시 인증되었다면, 단계(S3903)로 처리가 진행된다. 도39에서는, 만약 인증되지 않으면, 처리가 종료되도록 되어 있지만, 그 대신에, 다운로딩부(3802)에 다운로딩된 어플리케이션의 파기가 수행되도록 되어 있을 수 있다.

단계(S3903)에서, 다운로딩부(3802)에 다운로딩된 어플리케이션의 인증의 처리를 TRM 억세스 라이브러리부(3803)에 의해 수행한다.

단계(S3904)에서, 다운로딩된 어플리케이션이 인증었다면, 단계(S3905)로 처리가 진행된다. 만약에 인증되지 않았으면, 처리가 종료된다. 처리를 종료하는 대신에, 다운로딩부(3802)로 다운로딩된 어플리케이션의 파기가 수행되도

록 되어 있을 수 있다.

단계(S3905)에서, 다운로딩된 어플리케이션에 의한 인증 모듈로의 억세스가 허가된다. 이 허가를 수행하는 것은 인증 모듈(3801)이다. 또는, 어플리케이션이 인증 모듈(3801)로 억세스하는 경우에, 반드시, TRM 억세스 라이브러리부(3803)의 기능을 이용하는 것이면, TRM 억세스 라이브러리부(3803)에 의해 인증 모듈로의 억세스가 허가되도록 되어 있을 수 있다.

또한, 실시예2에서 언급한 바와 같이, TRM 억세스 라이브러리부(3802)는 어플리케이션 관리자, 장치 드라이버 등을 포함하고 있을 수 있다.

본 실시예에 의하면, 단말의 내부에 인증 모듈을 구비함으로써, 단말의 내부에 고도로 보호되어야 할 정보를 유지하는 것이 가능해지고, 단말로 다운로딩된 어 플리케이션의 인증을 수행하는 것이 가능해진다.

(실시예18)

본 발명의 실시예18은, 제1 기기와 인증 모듈로 이루어지는 어플리케이션 인증 시스템에 관한 것이다. 본 실시예에서는, 인증 모듈이 유지하는 정보를 이용하여, 제1 기기에 저장된 어플리케이션이 인증된다.

도40은 본 실시예의 어플리케이션 인증 시스템의 기능 블록도를 예시하고 있다. 어플리케이션 인증 시스템은, 제1 기기(4001)와 인증 모듈(4002)로 이루어진다. 제1 기기는 단말에 한정되는 것은 아니고, 예를 들면, PC, 워크스테이션, 대형 계산기, 또는 서버 장치일 수 있다. 또한, 제1 기기(4001)와 인증 모듈(4002)은 전기적으로 직접 접속되어 있을 필요는 없고, 또한, 물리적으로 접촉하고 있을 필요도 없다. 예를 들면, 무선에 의해서 접속되어 있을 수 있다. 또한, 인터넷으로 대표되는 네트워크에 의해 접속되어 있을 수 있다. 특히, 그 네트워크는 광케이블 등의 전기의 전도를 사용하지 않는 매체를 이용하여 구축되어 있을 수 있다.

제1 기기(4001)는 어플리케이션 저장부(4003)를 포함하고 있다. 어플리케이션 저장부(4003)는 어플리케이션을 저장한다. 어플리케이션이란, 제1 기기(4001)에서 동작하는 프로그램에 한정되지 않는다. 제1 기기(4001) 이외의 기기에서 동작하는 어플리케이션일 수 있다. 또한, 「저장한다」란, 어플리케이션을 유지하는 것이다. 유지하는 시간의 길이는 문제삼지 않는다. 또한, 유지의 목적도 문제삼지 않는다. 예를 들면, 어플리케이션을 제1 기기(4001)에서 동작시키기 위한 저장이 목적일 수 있다. 또한, 어플리케이션을 제1 기기(4001)로 다운로딩하여 동작시키는 것 이 목적일 수 있다. 또는, 어플리케이션이 통신으로 전송될 때에, 제1 기기(4001)가 중계하기 위한 일시적인 유지가 목적일 수 있다. 또는, 어플리케이션을 제1 기기(4001) 이외의 기기에 다운로딩하기 위한 유지가 목적일 수 있다.

인증 모듈(4002)은 TRM부(4004)를 갖는다. TRM부(4004)는 어플리케이션의 인증의 처리를 위한 정보를 내템퍼 영역에 유지한다. 어플리케이션의 인증의 처리를 위한 정보로서는, 예를 들면, 암호를 위한 비밀키나 어플리케이션의 서명의 진실성을 확인하기 위한 증명서 등을 들 수 있다. 여기서 말하는 어플리케이션이란 제1 기기(4001)의 어플리케이션 저장부(4003)에 저장되는 어플리케이션이다. 따라서, 본 실시예에서의 인증 모듈의 TRM부(4004)는 실시예1의 TRM부와 같은 기능을 갖는 것일 수 있다. 그 경우, 어플리케이션의 인증의 처리의 방법 등은 실시예와 같은 것이 된다.

본 실시예의 어플리케이션 인증 시스템에 의해, 제1 기기(4001)의 어플리케이션 저장부(4003)에 저장되어 있는 어플리케이션을 인증하는 것이 가능해지기 때문에, 예를 들면, 그 어플리케이션이 부정한 동작을 하는 것을 방지할 수 있다.

또한, 제1 기기(4001)는 가정용 전화 제품일 수 있다. 또한, 소위, 정보가전이나 네트워크 가전이라고 불리는 것일 수 있다. 그와 같은 제품을 예시 열거하면, 에어컨, 가습기, 제습기, 공기청정기, 전자레인지, 오븐, 냉장고, 식기 세척기, 전기포트, 다리미, 전기 청소기, 세탁기, 건조기, 전기 담요, 조명기기, 텔레비전 수상기, 라디오 수신기, 테이프 레코더 등의 오디오 기기, 카메라, IC 레코더, 전화기, 팩시밀리 송수신기, 복사기, 프린터, 스캐너, PC 등을 들 수 있다.

(실시예19)

본 발명의 실시예19도 실시예18과 같이, 제1 기기와 인증 모듈로 이루어지는 어플리케이션 인증 시스템에 관한 것이다. 본 실시예에서는, 제1 기기에 저장되는 어플리케이션의 인증이 수행될 때에는, 제1 기기내에서 그 인증을 수행하는 부분이 인증 모듈에 의해 인증된다.

도41은 본 실시예에서의 어플리케이션 인증 시스템의 기능 블록도를 예시하고 있다. 어플리케이션 인증 시스템은 제1 기기(4101)와 인증 모듈(4102)로 이루어진다. 또, 실시예18에서와 같이, 제1 기기(4101)와 인증 모듈(4102)은 전기적으로 직접 접속되어 있을 필요도 없고, 또한, 물리적으로 접촉하고 있을 필요도 없다.

제1 기기(4101)는 어플리케이션 저장부(4103)와 TRM 억세스 라이브러리부(4104)를 포함하고 있다.

어플리케이션 저장부(4103)는 어플리케이션을 저장한다. 예를 들면, 실시예18에서의 어플리케이션 저장부(4003)와 같은 기능을 갖고 있다.

TRM 억세스 라이브러리부(4104)는 인증 모듈(4102)에 자신이 인증되는 것을 조건으로 하여 어플리케이션의 인증을 위한 처리를 한다. 여기서 「자신」이란, TRM 억세스 라이브러리부(4104)를 의미한다. 또는, 「자신」이란, TRM 억세스 라이브러리부(4104)를 포함하는 부분일 수 있다. 예를 들면, 제1 기기(4101) 자체가 「자신」이라고 할 수 있다.

또한, 「어플리케이션」이란 어플리케이션 저장부(4003)에 저장된 어플리케이션을 의미한다.

따라서, TRM 억세스 라이브러리부(4104)는 자신을 인증 모듈에 의해서 인증되는 처리가 수행되고, 그 처리의 결과, 정확하게 인증된 경우에, 어플리케이션 저장부(4103)에 저장된 어플리케이션의 인증의 처리를 수행한다.

또한, TRM 억세스 라이브러리부(4104)는, 실시예2에서 설명한 바와 같이, 어플리케이션 관리자와 장치 드라이버를 포함하고, 그들의 처리를 수행하도록 되어 있을 수 있다.

인증 모듈(4102)은 TRM부(4105)와 TRM 억세스 라이브러리부 인증부(4106)를 갖고 있다.

TRM부(4105)는 TRM 억세스 라이브러리부 인증 정보를 내템퍼 영역에 유지한다. 「TRM 억세스 라이브러리부 인증 정보」란, TRM 억세스 라이브러리부를 인증하기 위한 정보이다. 예를 들면, 제1 기기를 특정하기 위한 정보를 들 수 있다. 이러한 정보로서는, 제1 기기의 제조자 번호와 제조 번호, 제1 기기에 전화 번호가 배당되어 있는 경우에는, 그 전화 번호를 예로서 들 수 있다. 또한, 제1 기기가 접속되어 있는 다른 기기의 정보나 제1 기기에 장비되어 있는 부품을 특정하는 정보, 또는, 제1 기기에 인스톨되어 있는 프로그램의 버전 번호 등 제1 기기가 놓여 있는 있는 상황을 나타내는 것일 수 있다. 또한, 제1 기기가 어떤 비밀의 정보, 예를 들면, 암호키 등을 유지할 수 있는 경우에는, 그 암호키가 진정한 것을 검출하기 위한 정보를 TRM 억세스 라이브러리부 인증 정보로 할 수 있다.

또한, 내템퍼 영역에 관해서는 실시예2의 설명을 참조하면 된다.

TRM 억세스 라이브러리부 인증부(4106)는 TRM 억세스 라이브러리부 인증 정 보에 기초하여 제1 기기(4101)의 TRM 억세스 라이브러리부(4104)를 인증한다. 즉, TRM 억세스 라이브러리부(4104)에서 전송되어 오는 정보를 취득하고, TRM 억세스 라이브러리부(4104)로부터 획득하는 정보가 TRM 억세스 라이브러리부 인증 정보에 적합한 것인지를 판단하고, 인증의 처리를 수행한다.

또한, TRM 억세스 라이브러리부 인증부(4106)가 인증하는 대상은 TRM 억세스 라이브러리부(4104)에만 한정되는 것이 아니라, TRM 억세스 라이브러리부(4104)를 포함하는 부분일 수 있고, 예를 들면, 제1 기기(4101)의 전체를 인증하도록 되어 있을 수 있다. 이 경우에는, TRM 억세스 라이브러리부 인증 정보는 제1 기기4101)의 제조 번호 등이나 제1 기기(4101)가 놓인 상황 등을 이용하도록 되어 있을 수 있다.

도42는 본 실시예에서의 어플리케이션 인증 시스템의 동작을 설명하는 순서도를 예시한다.

단계(S4201)에서, TRM 억세스 라이브러리부(4104)의 인증의 처리를 TRM 억세스 라이브러리부 인증부(4106)에 의해 수행한다. 이 때, 내템퍼 영역에 유지된 TRM 억세스 라이브러리부 인증 정보가 사용된다.

단계(S4202)에서, 단계(S4201)의 처리에 의해 TRM 억세스 라이브러리부(4104)가 인증되었는지의 여부를 판단한다. 만약 인증되었다고 판단된 경우에는, 단계(S4203)에서, 어플리케이션 저장부(4103)에 저장된 어플리케이션의 인증의 처리를 TRM 억세스 라이브러리부(4104)에 의해 수행한다.

본 실시예에서는, 인증 모듈(4102)의 TRM 억세스 라이브러리부 인증부(4106) 에 의해 인증된 TRM 억세스 라이브러리부(4104)가 어플리케이션의 인증을 수행한다. 이 때문에, 어플리케이션의 인증의 결과가 인증 모듈(4102)에 있어서 신뢰할 수 있는 것이 된다. 이 결과, 어플리케이션 저장부(4103)에 저장된 어플리케이션의 실행에 의해, 인증 모듈로의 억세스가 발생한 경우에, 인증 모듈은 그 억세스를 허가할 수 있다. 또한, 예를 들면, 어플리케이션 저장부(4103)가 다른 기기로 어플리케이션을 다운로딩할 목적으로 구비된 것이어도, 어플리케이션 저장부(4103)에서 다운로딩된 어플리케이션으로부터의 인증 모듈로의 억세스를 허가할 수 있다. 또한, 어플리케이션에, 인증 모듈(4102)에 의해 인증된 것을 나타내는 정보를 부가하는 것도 가능하다. 이것에 의해, 종래의 처리보다도 복잡한 처리를 실현하는 것이 가능해진다.

(실시예20)

실시예19 등에서 나타낸 어플리케이션 인증 시스템은 제1 기기와 인증 모듈의 2개의 주요 기기로 구성되어 있었다. 그러나, 본 실시예에서 나타낸 바와 같이, 주요 기기의 수는 2개로 한정되는 것은 아니다.

도43은 주요한 기기의 수를 3개로 한 경우의 어플리케이션 인증 시스템의 기능 블록도를 예시하고 있다. 이 어플리케이션 인증 시스템은, 제1 기기(4301)(단 이하에서 언급하는 제1 기기는 상기 실시예18 및 실시예19에서의 제1 기기와 상이함)와, 제2 기기(4302)와, 제3 기기(4303)로 이루어진다. 즉, 어플리케이션 인증 시스템은 3개의 주요한 부분을 가진다. 또, 이들의 3개의 주요한 부분은 직렬로 접속되어 있지만, 실시예18과 실시예19에서 설명한 바와 같이, 전기적으로 직접 접속 되어 있거나, 물리적으로 접촉되어 있을 필요는 없다. 또한, 제1 기기(4301),제2 기기(4302),제3 기기(4303)를 소유 또는 점유하고 있는 사람이 한사람일 수도 있고, 이들 3개의 기기가 각각 다른 사람에 의해 소유 또는 점유되어 있을 수도 있다.

실시예19 등의 어플리케이션 인증 시스템과의 대응은 다음과 같다. 즉, 제1 기기(4301)가 인증 모듈에 상당하고, 제3 기기(4303)가 단말이나 실시예19에서의 제1 기기(4101)에 상당한다.

제1 기기(4301)는 TRM부(4304)와 제1 인증 처리부(4305)를 포함하고 있다.

TRM부(4304)는 제2 기기를 인증하기 위한 인증 정보를 내템퍼 영역에 유지한다. 따라서, 실시예19 등의 TRM부와 같은 기능을 가진다. 단, 내템퍼 영역에 유지되는 정보가 제2 기기를 인증하기 위한 인증 정보가 되어 있는 점이 다르다. 또, 내템퍼 영역에는, 제2 기기를 인증하기 위한 정보뿐만 아니라, 제3 기기를 인증하기 위한 정보도 유지되어 있을 수 있다. 이 인증 정보로서는, 실시예19에서의 TRM 억세스 라이브러리부 인증 정보와 마찬가지로, 기기의 제조번호나, 기기가 놓인 상황을 나타내는 정보, 또는 기기가 암호키나 증명서를 유지할 수 있는 경우에는, 그 암호키나 증명서의 진실성을 검출하기 위한 정보를 들 수 있다.

제1 인증 처리부(4305)는 상기 인증 정보에 기초하여 제2 기기(4302)를 인증한다. 「상기 인증 정보」란 내템퍼 영역에 유지된 인증 정보이다.

제2의 기기(4302)는 제2 인증 처리부(4306)를 갖는다. 제2 인증 처리부(4306)는 제1 인증 처리부에 자신이 인증되는 것을 조건으로 하여 제3 기기(4303)를 인증한다. 여기에서 「자신」이란, 제2 인증 처리부(4306)를 포함하는 제2 기기(3402)를 의미한다.

제2 기기(4302)가 제1 인증 처리부(4305)에 의해 인증된 경우, 제2 기기(4302)는 제1 기기(4301)에 있어서 신뢰할 수 있는 기기라고 간주할 수 있다. 그 때문에, 제1 기기(4301)는 내템퍼 영역에 유지되는 정보로 제2 기기(4302)가 억세스하는 것을 허용할 수 있다. 그래서, 제2 인증 처리부(4306)가 제3 기기(4303)를 인증하는 경우에는, 내템퍼 영역에 유지된 정보를 사용하는 것이 가능하다. 그래서, 제2 인증 처리부(4306)가 제3 기기(4303)를 인증할 때는, 내템퍼 영역에 유지된 정보를 사용하도록 할 수 있다.

이와 같이, 제2 인증 처리부(4306)는 제1 기기(4301)로 억세스하기 위한 장치 드라이버의 기능을 포함하고 있을 수 있다.

또한, 제2 인증 처리부(4306)는 제3 기기(4303)를 인증하기 위해 필요한 정보를 제1 기기나 제3 기기와는 다른 별도의 기기로부터 취득하도록 할 수 있다. 이 취득시에, 제2 인증 처리부(4306)는 제2 기기(4302)가 제1 인증 처리부(4305)에 의해 인증되어 있는 것을 나타내는 정보를 제시하도록 할 수 있다.

제3 기기(4303)는 어플리케이션 저장부(4307)와 제3 인증 처리부(4308)를 포함하고 있다. 어플리케이션 저장부(4307)는 어플리케이션을 저장한다. 따라서, 실시예19 등에 있어서의 어플리케이션 저장부와 같은 기능을 가진다. 이 때문에, 어플리케이션을 저장하는 시간의 길이나 저장하는 목적은 특히 한정되지 않는다.

제3 인증 처리부(4308)는 제2 기기(4302)에 자신이 인증되는 것을 조건으로 하여, 상기 어플리케이션의 인증을 위한 처리를 한다. 「상기 어플리케이션」이란, 어플리케이션 저장부(4307)에 저장되어 있는 어플리케이션을 의미한다. 또한, 「자신」이란 제3 기기(4303)를 의미한다.

제3 기기(4303)가 제2 인증 처리부(4306)에 의해 인증된 경우, 제3 기기(4303)는 제1 기기(4301)에 있어서 신뢰할 수 있는 기기라고 간주할 수 있다. 그 때문에, 제1 기기(4301)는 내템퍼 영역에 유지되는 정보로 제3 기기(4303)가 억세스하는 것을 허용할 수 있다. 그래서, 제3 인증 처리부(4306)가 어플리케이션을 인증하는 경우에는, 내템퍼 영역에 유지된 정보를 사용하는 것이 가능하다.

또한, 제3 인증 처리부(4308)는 어플리케이션을 인증하기 위해서 필요한 정보를 제1 기기나 제2 기기와는 다른 별도의 기기로부터 취득하도록 할 수 있다. 이 취득시에, 제3 인증 처리부(4308)는 제3 기기(4302)가 제2 인증 처리부(4306)에 의해 인증되어 있음을 나타내는 정보를 제시하도록 해도 좋다. 또한, 그 때, 제2 기기(4302)가 제1 인증 처리부(4305)에 의해 인증되어 있음을 나타내는 정보를 제시할 수 있다.

도44는 제1 기기(4301)의 동작을 설명하는 순서도를 예시한다. 단계(S4401)에서, 제1 인증 처리부(4305)는 TRM부(4304)가 내템퍼 영역에 유지하는 인증 정보를 취득한다. 단계(S4402)에서, 제2 기기의 인증의 처리를 수행하고, 단계(S4403)에서, 인증되었는지의 여부를 판단한다. 만약에 인증되었다면, 단계(S4404)에서, 제2 기기로 인증된 것을 전달한다.

도45는 제2 기기(4302)의 동작을 설명하는 순서도를 예시한다. 단계(S4501) 에서, 제1 인증 처리부(4305)에 의해 인증되었는지의 여부를 판단한다. 이 판단은, 도44에 도시한 단계(S4404)에서, 인증된 것이 제1 기기(4301)로부터 전달되었는지의 여부에 의해 판단된다. 만약에 인증되었다면, 단계(S4502)에서, 제3 기기의 인증의 처리를 제2 인증 처리부(4306)에 의해 수행한다. 단계(S4503)에서, 인증되었는지의 여부를 판단한다. 만약에 인증되었다면, 단계(S4504)에서, 제3 기기로 인증된 것을 전달한다.

도46은 제3 기기(4303)의 동작을 설명하는 순서도를 예시한다. 단계(S4601)에 있어서, 제2 인증 처리부(4306)에 의해 인증되었는지의 여부를 판단한다. 이 판단은, 도45에 도시한 단계(S4504)에서, 인증된 것이 제2 기기(4302)로부터 전달되었는지의 여부에 의해 판단된다. 만약에 인증된 것이면, 단계(S4602)에서, 어플리케이션의 인증의 처리를 수행한다. 도46에서는, 여기서 처리가 종료되지만, 어플리케이션의 인증의 처리의 결과를, 예를 들면, 제1 기기(4301)로 전달할 수 있다. 또한, 제2 기기(4302)로 전달할 수 있다. 또한, 만약에 어플리케이션이 다른 기기로 억세스하는 경우에는, 제3 인증 처리부(4308)에 의해 인증되었음을 나타내는 정보를 제시하도록 할 수 있다. 또는, 어플리케이션에 제3 인증 처리부(4308)에 의해 인증되었음을 나타내는 정보를 부가할 수 있다.

이상은, 3개의 주요한 기기에 의해 어플리케이션 인증 시스템이 구성되는 경우였지만, 도47에 예시된 바와 같이, 어플리케이션 인증 시스템은 4개의 주요한 기기에 의해 구성되어 있을 수 있다.

도47에서, 어플리케이션 인증 시스템은 제1 기기(4701)와 제2 기기(4702)와 제3 (기기4703)와 제4 기기(4704)에 의해 구성된다. 제1 기기(4701)는 TRM부(4705)와 제1 인증 처리부(4706)를 포함하고 있고, 이들은, 도43에 예시된 TRM부(4304)와 제1 인증 처리부(4305)에 대응한다. 제2 기기(4702)는 제2 인증 처리부(4707)를 포함하고 있다. 이것은 도43에 예시된 제2 인증 처리부(4306)에 대응한다.

제3 기기는 제3 인증 처리부(4708)를 포함하고 있다. 제3 인증 처리부(4708)는 제2 인증 처리부(4707)에 자신이 인증되는 것을 조건으로 하여 제4 기기(4704)를 인증한다. 제2 인증 처리부(4707)에 의해 제3 기기(4703)가 인증되면, 제3 기기(4703)는 제1의 기기(4701)에 있어서 신뢰할 수 있는 기기가 되기 때문에, 제1 기기(4701)는, 제3 기기(4703)가 TRM부(4705)가 내템퍼 영역에 유지하는 정보에 억세스하는 것을 허가할 수 있다. 그래서, 제3 인증 처리부(4708)는, TRM부(4705)가 내템퍼 영역에 유지하는 정보를 취득하고, 제4 기기(4704)를 인증하도록 할 수 있다. 또한, 다른 기기에 유지되어 있는 정보를 취득하고 인증하도록 할 수 있다.

또, 제3 인증 처리부(4708)가 TRM부(4705)가 내템퍼 영역에 유지하는 정보를 취득하는 경우에는, 제3 기기(4703)와 제1 기기(4701)가 직접 통신을 수행할 수 있 도록 하기 위해, 제3 기기(4703)와 제1 기기(4701)에 통신부가 구비되어 있을 수 있다. 또는, 제2 인증 처리부(4707)가 제1 기기(4701)로 억세스하기 위한 장치 드라이버의 기능을 포함하고 있는 경우에는 다음과 같이 할 수 있다. 즉, 제3 인증 처리부(4708)는 제2 인증 처리부(4707)가 구비하는 장치 드라이버의 기능을 이용하여, 제2 기기(4702)를 통하면서, TRM부(4705)가 내템퍼 영역에 유지하는 정보를 취득한다. 따라서, 제3 인증 처리부(4708)는 제2 인증 처리부(4707)로 억세스하기 위한 장치 드라이버의 기능을 포함하고 있어도 좋다.

제4 기기(4704)는 어플리케이션 저장부(4709)와 제4 인증 처리부(4710)를 구비한다. 어플리케이션 저장부(4709)는 도43의 어플리케이션 저장부(4307)에 대응한다. 제4 인증 처리부(4710)는 제3 인증 처리부(4708)에 자신이 인증되는 것을 조건으로 하여, 어플리케이션을 인증한다. 여기서, 「자신」이란, 제4 기기를 의미하고 있다. 따라서, 제3 인증 처리부(4708)에 의해 제4 기기가 인증되어 있으면, 제1 인증 처리부(4706)에 의해 인증되었다고 간주되기 때문에, 제4 인증 처리부는, TRM부(4705)가 내템퍼 영역에 유지하는 정보를 이용하여, 어플리케이션 저장부(4709)에 저장되어 있는 어플리케이션의 인증을 할 수 있다. 또한, 제4 인증 처리부(4710)는 제3 인증 처리부(4708)에 의해 인증되었음을 나타내는 정보를 다른 기기에 제시하여, 어플리케이션의 인증을 위한 정보를 취득하여, 어플리케이션의 인증을 수행하도록 할 수 있다.

이와 같이, 4개의 주요한 기기에 의해 어플리케이션 인증 시스템이 구성되는 경우의 동작은 다음과 같다. 제1 기기(4701)의 동작은, 도44에 예시된 것과 같다. 마찬가지로 제2 기기(4702)의 동작은 도45에 예시되어 있다. 제3 기기(47

03)의 동작은, 도48에 예시되어 있는 것이 된다. 즉, 제3 기기(4703)가 제2 인증 처리부(4707)에 의해 인증되었는지의 여부를 단계(S4801)에서 판단한다. 만약에 인증된 것이면, 단계(S4802)에서 제4 기기(4704)의 인증의 처리를 수행한다. 단계(S4803)에서 인증이 되었는지의 여부를 판단하고, 만약에 인증되었다면, 단계(S4804)에서, 제4 기기(4704)로 인증되었음을 전달한다.

제4 기기의 동작은 도49에 예시되어 있다. 제3 인증 처리부(4708)에 의해 인증되었는지의 여부를 단계(S4901)에서 판단하고, 만약 인증되었다면, 단계(S4902)에서, 어플리케이션의 인증의 처리를 수행한다. 이 어플리케이션의 인증의 처리의 결과를, 예를 들면, 제1 기기(4701)로 전달할 수 있다. 또한, 제2 기기(4702)로 전달할 수 있다. 또한, 만약에 어플리케이션이 다른 기기로 억세스하는 경우에는, 제3 인증 처리부(4708)에 의해 인증되었음을 나타내는 정보를 제시하도록 할 수 있다. 또는, 어플리케이션에 제3 인증 처리부(4708)에 의해 인증되었음을 나타내는 정보를 부가할 수 있다.

또한, 주요한 기기의 수는 4개로 한정되지 않고, 도50에 예시된 바와 같이, 제1 기기(5001)와 제2 기기(5002)와 제3 기기(5003)와 제4 기기(5004) 및 제5 기기(5005)의 5개의 기기에 의해 어플리케이션 인증 시스템이 구성되어 있을 수 있다.

도51은 주요한 수를 일반화한 경우의 어플리케이션 인증 시스템의 기능 블록도를 예시한 것이다. 도51에서, 어플리케이션 인증 시스템은 제1 기기(5101)에서 제(N+1)의 기기(5105)까지를 직렬로 접속하여 이루어진 (N+1)개의 기기에 의해 구성된다. 「접속」이라고 기술했지만, 이것은 전기적으로 직접 접속되어 있는 것, 또는, 물리적으로 접촉하고 있는 것만을 의미하고 있는 것은 아니다. 예를 들면, 인터넷으로 대표되는 것과 같은 네트워크에 의해서 접속되어 있을 수 있다. 특히, 광케이블을 이용한 네트워크에 의해서 접속되어 있을 수 있다. 또한, 무선에 의해서 접속되어 있을 수 있다. 또한, 각각의 기기가 서로 접속되어 있을 수 있다.

제1 기기(5101)는 TRM부(5101)와 제1 인증 처리부(5102)를 포함하고 있다. TRM부(5101)는 제2 기기(5102)를 인증하기 위한 정보인 인증 정보를 내템퍼 영역에 유지한다. 제1 인증 처리부(5102)는 인증 정보에 기초하여 제2 기기(5102)를 인증한다.

이하에서는, 제2 기기(5102)에서 제N 기기까지중 어느 하나의 기기를 제i 기기로 표기하기로 한다. 제i 기기는, 제i 인증 처리부를 구비한다. 제i 인증 처리부는 제(i-1) 인증 처리부에 자신이 인증되는 것을 조건으로 하여 제(i+1)의 기기를 인증한다. 여기서 「자신」이란, 제i의 기기를 의미한다. 따라서, 제i 인증 처리부는, 제i 기기가 제(i-1) 인증 처리부에 인증되어 있으면, 제(i+1)의 기기를 인증한다. 제i 기기가 제(i-1) 인증 처리부에 인증되어 있으면, 제1 기기(5101)에 있어서, 제i 기기는 신뢰할 수 있다고 간주할 수 있기 때문에, 제1 기기(5101)는 제i 기기가 TRM부(5101)에 의해 내템퍼 영역에 유지되어 있는 정보로 억세스를 허용할 수 있다. 그래서, 제i 기기는 내템퍼 영역에 유지된 정보를 이용하여, 제(i+1)의 기기를 인증하도록 할 수 있다.

예를 들면, 제i 인증 처리부가 TRM부(5107)에 의해 내템퍼 영역에 유지되어 있는 정보에 억세스하는 경우에는, 제i 기기와 제1 기기가 직접 통신을 수행하도록 할 수 있다.

또한, 제i 인증 처리부는 제(i-1) 인증 처리부로 억세스하기 위한 장치 드라이버 등의 기능을 포함하고 있을 수 있다. 이 구비된 기능에 의해, 정보의 요구가 제i 인증 처리부에서 제1 인증 처리부(5107)로 차례로 출력되고, 요구된 정보가 제1 인증 처리부(5107)에서 제i 인증 처리부로 차례로 회신된다.

제(N+1)의 기기(5105)는 어플리케이션 저장부(5111)와 제(N+1) 인증 처리부(5112)를 포함하고 있다. 어플리케이션 저장부(5111)는 어플리케이션을 저장한다. 어플리케이션을 저장하고 있는 시간은 특별히 한정하지 않고, 예를 들면, 제(N+1)의 기기(5105)로 어플리케이션을 실행하기 위해서 어플리케이션이 저장되도록되어 있을 수 있고, 어플리케이션의 전달을 중계하기 위해서만 일시적으로 저장되도록 되어 있을 수도 있다. 또한, 저장의 목적도 특별히 한정되지 않고, 제(N+1) 기기(5105)로 어플리케이션을 실행하는 경우뿐만 아니라, 다른 기기에서의 어플리케이션의 실행을 위한 다운로딩의 목적으로 저장할 수 있다. 또한, 제(N+1) 기기(5105)로 어플리케이션을 다운로딩하여 실행할 목적으로 저장할 수 있다. 또, 어플리케이션이라는 명칭을 사용했지만, 프로그램일 필요는 없고 데이터일 수도 있다.

제(N+1) 인증 처리부(5112)는 제N 인증 처리부에 자신이 인증되는 것을 조건으로 하여, 어플리케이션을 인증한다. 「자신」이란 제(N+1) 기기(5105)를 의미하고, 「어플리케이션」이란 어플리케이션 저장부(5111)에 저장된 어플리케이션을 의미한다.

제1 기기(5101)의 동작을 설명하는 순서도는 도44에 예시되어 있다.

도52는 제2 기기에서 제N 기기까지 중 어느 하나의 기기의 동작을 설명하는 순서도이다. 단계(S5201)에서, 제(i-1)

인증 처리부에 의해 인증되었는지의 여부를 판단하고, 만약 인증되면, 제(i+1) 기기의 인증의 처리를 단계(S5202)에서 수행한 다. 제(i+1) 기기가 인증되었는지의 여부를 단계(S5203)에서 판단하고, 만약 인증되었다면, 제(i+1) 기기로 인증되었음을 전달한다. 이것에 의해, 제2 기기로부터 차례로 인증이 제N 기기까지가 인증되게 된다.

도53은 제(N+1) 기기(5105)의 동작의 순서도를 예시하고 있다. 제N 인증 처리부(5105)에 의해 인증되었는지의 여부를 단계(S5301)에서 판단하고, 만약 인증되었다고 판단되면, 단계(S5302)에서 어플리케이션의 인증의 처리를 수행한다. 어플리케이션의 인증이 되면, 그 결과를 제1 기기(5101) 등으로 전달하고, 어플리케이션에 의한 제1 기기(5101)로의 억세스하는 것을 허가하도록 한다. 또는, 인증이 되었다는 것을 나타내는 정보를 어플리케이션에 부가하도록 할 수 있다.

도43, 도47, 도50, 도51에서는 기기가 직렬로 접속되어 있지만, 상자 구조를 이용하여 기기가 접속되어 있을 수 있다. 도54는 상자 구조를 이용하여 기기가 접속되어 있는 것을 모식적으로 예시하고 있다. 보안 장치(5401)가 제1 기기에 상당하고, TRM부와 제1 인증 처리부를 구비한다. 보안 장치(5402)는 제2 기기에 상당하는 어댑터(5402)의 일부로서 장착되도록 접속된다. 어댑터(5402)는 제3 기기에 상당하는 통신 모듈(5403)의 일부로서 장착되도록 접속되어 있다. 또한 통신 모듈(5403)은 제4 기기에 상당하는 PDA(Personal Digital Assistance)(5404)의 일부로서 장착되도록 접속된다. PDA(5404)는, 서버(5405)와 통신 회선 등을 통해 제5 기기에 상당하는 서버에 접속된다. 이와 같이 접속이 수행됨으로써, 예를 들면, 서버(5405)에 저장된 어플리케이션을 보안 장치(5401)의 내템퍼 영역에 유지된 정보를 이용하여 인증할 수 있다.

또한, 제(N+1) 기기(5105)는, 예를 들면, 가정용 전화 제품일 수 있다. 또한, 소위, 정보 가전이나 네트워크 가전으로 불리는 것일 수 있다. 그와 같은 가정 전화 제품을 예시 열거하면, 에어컨, 가습기, 제습기, 공기청정기, 전자레인지, 오븐, 냉장고, 식기 세척기, 전기포트, 다리미, 전기 청소기, 세탁기, 건조기, 전기 담요, 조명기기, 텔레비전 수상기, 라디오 수신기, 테이프 레코더 등의 오디오 기기, 카메라, IC 레코더, 전화기, 팩시밀리 송수신기, 복사기, 프린터, 스캐너, PC 등을 들 수 있다.

(실시예21)

실시예20에서는, 제2 기기에서 제N 기기까지중 어느 하나를 제i 기기로 표기할 때, 제i 기기는, 제(i+1) 기기의 인증을 수행하기 위해서 필요한 정보를 유지하도록 되어 있을 수 있다. 예를 들면, 제i 기기가 내템퍼 영역을 포함하고, 거기에 인증을 수행하는데 필요한 정보를 유지하고 있을 수 있다.

이와 같이 제i 기기가 인증을 수행하기 위해서 필요한 정보인 인증 정보를 유지하고 있는 경우가 있을 수 있을 때, 제i 기기가 제i 인증 정보 취득부를 포함하고 있을 수 있다. 여기에, 제i 인증 정보 취득부란, 제i 기기가 인증 정보를 저장하고 있는 영역인 인증 정보 저장 영역을 포함하고 있는 경우에는, 그 인증 정보 저장 영역에서 인증 정보를 취득하는 부이다. 또한, 제i 인증 정보 취득부는, 제1 기기의 TRM부에 인증 정보가 저장되어 있는 경우에는, 제2 기기에서 제(i-1) 기기까지의 기기를 통해, TRM부로부터 인증 정보를 취득한다. 「제2 기기에서 제(i-1) 기기까지의 기기를 통해」란 다음의 것을 의미한다. 즉, 제i 인증 정보 취득부가 제(i-1) 인증 정보 취득부로 인증 정보의 요구를 출력하고, 마지막에는 제2 인증 정보 취득부가 제1 기기로 인증 정보의 요구를 출력한다. 제2 인증 정보 취득부가 제1 기기로부터 인증 정보를 취득하면, 제3 인증 정보 취득부로 인증 정보를 출력하고, 마지막으로는, 제(i-1) 인증 정보 취득부가 제i 인증 정보 취득부로 인증 정보를 출력한다.

도55는 본 실시예에 있어서의 제i 기기의 동작을 설명하는 순서도를 예시한 것이다. 단계(S5501)에서 제(i-1) 인증 처리부에 의해 인증되었는지의 여부를 판단한다. 인증되었다고 판단되면, 단계(S5502)로 처리가 진행되고, 인증 정보 저장 영역에 제(i+1) 기기의 인증 정보가 저장되어 있는지의 여부를 판단한다. 예를 들면, 인증 정보 저장 영역에 저장되어 있는 정보를 판독하고, 인증 정보가 획득되었는지의 여부를 판단한다. 만약 저장되어 있지 않으면, 단계(S5503)로 처리가 진행되고, 제2 기기에서 제(i-1) 기기까지를 통해 TRM부로부터 인증 정보를 취득한다. 단계(S5504)에서, 제(i+1) 기기의 인증의 처리를 수행하고, 인증되었는지의 여부를 단계(S5505)에서 판단한다. 만약 인증되었다면, 단계(S5506)에서, 제(i+1) 기기로 인증된 것을 전달한다.

이러한 처리를 수행함으로써, 어플리케이션 인증 시스템을 구성하는 기기의 수가 증가되더라도, 기기가 인증 정보를 가지고 있으면, 그 인증 정보를 사용하여 인증이 되기 때문에, 예를 들면, 모든 기기의 인증의 시간을 단시간에 끝내는 것이 가능해진다.

발명의 효과

이상과 같이 본 발명에 따르면, 인증 모듈과 단말을 조합하여, 단말내에서 동작하는 어플리케이션을 인증 모듈이 가지는 정보로 인증함으로써, 바람직하지 못한 어플리케이션이 단말내에서 실행되는 것을 방지할 수 있다.

또한, 단말내의 TRM 억세스 라이브러리가 인증 모듈에 의해서 인증됨으로써, TRM 억세스 라이브러리가 어플리케이션의 인증을 위한 처리를 수행하는 것이 가능해진다. 이 결과, 높은 보안이 요구되는 어플리케이션의 실행이 가능해지고, 단말을 사용한 상거래의 조작이 가능해진다. 또한, 내템퍼 영역은 인증 모듈에 있으면 좋고, 단말에 내템퍼 영역을 설치할 필요가 없어지기 때문에, 단말의 제조 비용을 낮출 수 있다.

또한, 단말내에서 동작하는 어플리케이션이 인증됨으로써, 어플리케이션의 출처가 보증되고, 단말이나 인증 모듈의 로컬 리소스의 억세스를 어플리케이션에 허가할 수 있다.

또한, 서버가 인증 모듈의 TRM부를 인증함으로써, 단말을 인증하는 것, 및 단말내에서 동작하는 어플리케이션의 인증을 수행할 수 있기 때문에, 기밀성이 높은 정보를 단말내에서 동작하는 어플리케이션과 교환할 수 있고, 복잡한 상거래의 조작을 서버, 단말, 인증 모듈사이에서 실현할 수 있다.

또한, 선택 영역에 어플리케이션본체의 서명을 저장함으로써, 어플리케이션의 다운로딩과 동시에 어플리케이션 본체의 서명을 다운로딩하는 것이 가능해지고, 별도로 어플리케이션 본체의 서명을 다운로딩하는 시간을 생략할 수 있다.

또한, 3개 이상의 기기가 직렬로 접속된 상태로, 한편의 끝의 기기에서 차례로 인증을 수행하고, 다른 끝의 기기에 저장된 어플리케이션의 인증이 가능해진다.

(57) 청구의 범위

청구항 1.
단말 및 인증 모듈을 포함하는 어플리케이션 인증 시스템에 있어서,

상기 단말은 어플리케이션을 다운로딩하는 다운로딩부를 포함하고,

상기 인증 모듈은 상기 어플리케이션의 인증 처리를 위한 정보를 내템퍼(tamper resistant) 영역에 유지하는 TRM부를 포함하는

어플리케이션 인증 시스템.

청구항 2.
단말 및 인증 모듈을 포함하는 어플리케이션 인증 시스템에 있어서,

상기 단말은, 어플리케이션을 다운로딩하는 다운로딩부; 및 상기 인증 모듈에 자신이 인증되는 것을 조건으로 하여 어플리케이션의 인증을 위한 처리를 하는 TRM 억세스 라이브러리부를 포함하고,

상기 인증 모듈은, 상기 TRM 억세스 라이브러리부를 인증하기 위한 정보인 TRM 억세스 라이브러리부 인증 정보를 내템퍼 영역에 유지하는 TRM부; 및 상기 TRM 억세스 라이브러리부 인증 정보에 기초하여 상기 단말의 TRM 억세스 라이브러리부를 인증하는 TRM 억세스 라이브러리부 인증부를 포함하는

어플리케이션 인증 시스템.

청구항 3.
제2항에 있어서,

상기 단말의 다운로딩부는 정정이 없음을 인증하기 위해 사용하는 정보인 서명이 부가된 어플리케이션을 다운로딩하고,

상기 TRM 억세스 라이브러리부는 상기 다운로딩부에 다운로딩된 어플리케이션으로부터 서명 인증용 다이제스트를 생성하고, 상기 생성한 서명 인증용 다이제스트와 서명을 포함하는 서명 인증 정보를 상기 인증 모듈로 출력하는 서명 인증 정보 출력부를 더 포함하고,

상기 인증 모듈은, 상기 서명 인증 정보 출력부에서 출력된 서명 인증 정보를 입력하는 서명 인증 정보 입력부; 및 상기 서명 인증 정보 입력부에서 입력되는 서명 인증용 다이제스트와 서명에 기초하여 서명의 검증을 수행하는 서명 인증부를 더 포함하는

어플리케이션 인증 시스템.

청구항 4.
제3항에 있어서,

상기 인증 모듈은, 상기 서명 인증 정보 입력부에서 입력되는 서명을 이용하여 서명 유래 다이제스트를 생성하기 위한 서명 유래 다이제스트 생성 정보를 취득하는 서명 유래 다이제스트 생성 정보 취득부; 및 상기 서명 인증 정보 입력부에서 입력된 서명과 서명 유래 다이제스트 생성 정보 취득부에 유지된 서명 유래 다이제 스트 생성 정보를 이용하여 서명 유래 다이제스트를 생성하는 서명 유래 다이제스트 생성부를 더 포함하고,

상기 서명 인증부는 상기 서명 유래 다이제스트 생성부에서 생성된 서명 유래 다이제스트와 서명 인증 정보 입력부에서 입력된 서명 인증용 다이제스트에 기초하여 인증을 수행하는

어플리케이션 인증 시스템.

청구항 5.
제2항 내지 제4항 중 어느 한 항에 있어서,

상기 단말은 상기 인증 모듈을 인증하기 위한 인증 모듈 인증부를 포함하는

어플리케이션 인증 시스템.

청구항 6.
제5항에 있어서,

상기 TRM 억세스 라이브러리부는 인증된 어플리케이션에 대해 이용을 인정하는 리소스에 관한 정보인 어플리케이션 이용 리소스 정보를 유지하는 어플리케이션 이용 리소스 정보 유지 수단을 포함하는

어플리케이션 인증 시스템.

청구항 7.
제5항 또는 제6항에 있어서,

상기 단말의 TRM 억세스 라이브러리부는 상기 인증 모듈 인증부에 의해 인증된 상기 인증 모듈의 TRM부에 대해 어플리케이션 이용 리소스 정보를 출력하는 어플리케이션 이용 리소스 정보 출력 수단을 더 포함하고,

상기 인증 모듈의 TRM부는 상기 단말의 TRM 억세스 라이브러리부의 어플리케이션 이용 리소스 정보 출력 수단으로부터 출력된 어플리케이션 이용 리소스 정보를 내템퍼 영역에 재기록 가능하게 유지하는

어플리케이션 인증 시스템.

청구항 8.
제6항 또는 제7항에 있어서,

상기 TRM 억세스 라이브러리부는 상기 어플리케이션 이용 리소스 정보에 기초하여, 상기 어플리케이션에 대해 리소스의 이용을 인정하는

어플리케이션 인증 시스템.

청구항 9.
제6항 내지 제8항 중 어느 한 항에 있어서,

상기 단말은 서명이 부가된 어플리케이션 이용 리소스 정보를 다운로딩하는 어플리케이션 이용 리소스 정보 다운로딩부를 포함하고,

상기 TRM 억세스 라이브러리부는 상기 어플리케이션 이용 리소스 정보 다운로딩부에 다운로딩된 어플리케이션 이용 리소스 정보에 부가된 서명을 검증하는

어플리케이션 인증 시스템.

청구항 10.
제6항 내지 제8항 중 어느 한 항에 있어서,

상기 단말은 서명이 부가된 어플리케이션 이용 리소스 정보를 다운로딩하는 어플리케이션 이용 리소스 정보 다운로딩부를 포함하고,

상기 TRM 억세스 라이브러리부는 상기 어플리케이션 이용 리소스 정보 다운로딩부에 다운로딩된 어플리케이션 이용 리소스 정보로부터 서명 인증용 다이제스트를 생성하고, 생성된 서명 인증용 다이제스트와 서명을 포함하는 서명 인증 정보를 상기 인증 모듈로 출력하는 어플리케이션 이용 리소스 정보 서명 인증 정보 출력부를 포함하고.

상기 인증 모듈은, 상기 어플리케이션 이용 리소스 정보 서명 인증 정보 출력부에서 출력된 서명 인증 정보를 입력하는 어플리케이션 이용 리소스 정보 서명 인증 정보 입력부; 및 상기 어플리케이션 이용 리소스 정보 서명 인증 정보 입력부로부터 입력되는 서명 인증용 다이제스트와 서명에 기초하여 서명의 검증을 수행하는 어플리케이션 이용 리소스 정보 서명 인증부를 더 포함하는

어플리케이션 인증 시스템.

청구항 11.
제2항에 있어서,

상기 TRM 억세스 라이브러리부 인증 정보는 상기 단말의 고유 정보인

어플리케이션 인증 시스템.

청구항 12.
제2항에 있어서,

상기 TRM 억세스 라이브러리부 인증 정보는 상기 단말에 인스톨되어 있는 어플리케이션의 조합에 관한 정보인

어플리케이션 인증 시스템.

청구항 13.
제2항에 있어서,

상기 TRM 억세스 라이브러리부 인증 정보는 상기 TRM 억세스 라이브러리부를 식별하기 위한 정보인 라이브러리 식별 정보인

어플리케이션 인증 시스템.

청구항 14.
제2항 내지 제4항 중 어느 한 항에 있어서,

상기 단말은 상기 인증 모듈의 TRM부에 억세스를 하는 단말 어플리케이션을 유지하는 단말 어플리케이션 유지부를 포함하고,

상기 인증 모듈의 TRM부는 상기 내템퍼 영역의 상기 인증 모듈내에서 동작하는 인증 모듈내 어플리케이션을 유지하는 인증 모듈내 어플리케이션 유지부를 포함하고,

상기 인증 모듈내 어플리케이션은 상기 TRM 억세스 라이브러리부 인증부에 의한 TRM 억세스 라이브러리부의 인증 성공을 조건으로 하여 상기 단말 어플리케이션으로부터의 억세스를 받아들여 동작하는

어플리케이션 인증 시스템.

청구항 15.
제14항에 있어서,

상기 인증 모듈의 TRM부는 상기 TRM 억세스 라이브러리부 인증부에 의한 TRM 억세스 라이브러리부의 인증 성공

을 조건으로 하여 인증 결과 식별자를 생성하는 인증 결과 식별자 생성 수단을 포함하고,

상기 인증 모듈내 어플리케이션은 인증을 나타내는 인증 결과 식별자의 존재를 조건으로 하여 상기 단말 어플리케이션에 대해 인증 모듈내 어플리케이션에 대한 억세스를 가능하게 하고, 상기 인증 모듈내 어플리케이션은 상기 단말 어플리케이션으로부터의 억세스를 받아들이는

어플리케이션 인증 시스템.

청구항 16.
제14항에 있어서,

상기 인증 모듈의 TRM부는 상기 TRM 억세스 라이브러리부에 의한 어플리케이션의 인증 성공을 조건으로 하여 어플리케이션 인증 결과 식별자를 생성하는 어플리케이션 인증 결과 식별자 생성 수단을 포함하고,

상기 인증 모듈내 어플리케이션은 상기 인증 성공을 나타내는 어플리케이션 인증 결과 식별자의 존재를 조건으로 하여 상기 단말 어플리케이션에 대해 인증 모듈내 어플리케이션에 대한 억세스를 가능하게 하고, 상기 인증 모듈내 어플리케이션은 단말 어플리케이션으로부터의 억세스를 받아들이는

어플리케이션 인증 시스템.

청구항 17.
단말, 인증 모듈, 및 어플리케이션을 상기 단말로 다운로딩하는 서버를 포함하는 어플리케이션 인증 시스템에 있어서,

상기 단말은 상기 어플리케이션을 다운로딩하는 다운로딩부를 포함하고,

상기 인증 모듈은 상기 어플리케이션의 인증 처리를 위한 정보를 내템퍼 영역에 유지하는 TRM부를 포함하고,

상기 서버는 상기 단말을 통한 인증 모듈의 인증 성공을 조건으로 상기 단말의 인증이 성공했다고 판단하는 단말 인증부를 포함하는

어플리케이션 인증 시스템.

청구항 18.
단말, 인증 모듈, 및 어플리케이션을 상기 단말로 다운로딩하는 서버를 포함하는 어플리케이션 인증 시스템에 있어서,

상기 단말은, 상기 어플리케이션을 다운로딩하는 다운로딩부; 및 상기 인증 모듈에 자신이 인증되는 것을 조건으로 하여 상기 어플리케이션의 인증을 위한 처리를 하는 TRM 억세스 라이브러리부를 포함하고,

상기 인증 모듈은, 상기 TRM 억세스 라이브러리부를 인증하기 위한 정보인 TRM 억세스 라이브러리부 인증 정보를 내템퍼 영역에 유지하는 TRM부; 및 상기 TRM 억세스 라이브러리부 인증 정보에 기초하여 상기 단말의 TRM 억세스 라이브러리부를 인증하는 TRM 억세스 라이브러리부 인증부를 포함하고,

상기 서버는, 상기 단말의 TRM 억세스 라이브러리부를 통한 상기 인증 모듈의 TRM부의 인증 성공을 조건으로 하여 상기 TRM 억세스 라이브러리부의 인증이 성공했다고 판단하는 서버 TRM 억세스 라이브러리부 인증부를 포함하는

어플리케이션 인증 시스템.

청구항 19.
단말, 인증 모듈. 및 어플리케이션을 단말로 다운로딩하는 서버로 이루어지는 어플리케이션 인증 시스템에 있어서,

상기 단말은, 상기 어플리케이션을 다운로딩하는 다운로딩부; 상기 어플리케이션으로부터 서명용 다이제스트를 생성하는 서명용 다이제스트 생성 수단; 상기 어플리케이션의 다운로딩과 함께 다운로딩된 서명을 취득하는 다운로딩 어플리케이션 서명 취득 수단; 및 상기 취득한 서명과 서명용 다이제스트 생성 수단에 의해서 생성된 서명용 다이제스트를 상기 서버로 송신하는 어플리케이션 인증 데이터 출력 수단을 포함하는 TRM 억세스 라이브러리부를 포함하고,

상기 인증 모듈은, 상기 TRM 억세스 라이브러리부를 인증하기 위한 정보인 TRM 억세스 라이브러리부 인증 정보를 내템퍼 영역에 유지하는 TRM부; 및 상기 TRM 억세스 라이브러리부 인증 정보에 기초하여 상기 단말의 TRM 억세스

라이브러리부를 인증하는 TRM 억세스 라이브러리부 인증부를 포함하고,

상기 서버는, 상기 단말의 TRM 억세스 라이브러리부를 통한 상기 인증 모듈의 TRM부의 인증 성공을 조건으로 하여 상기 TRM 억세스 라이브러리부의 인증이 성공했다고 판단하는 서버 TRM 억세스 라이브러리부 인증부; 상기 서버 TRM 억세스 라이브러리부 인증부에 의해 인증이 성공했다고 판단된 TRM 억세스 라이브러리부의 어플리케이션 인증 데이터 출력 수단으로부터 출력된 서명용 다이제스트와 서명을 입력하는 어플리케이션 인증 데이터 입력부; 및 상기 어플리케이션 인증 데이터 입력부에 입력된 서명용 다이제스트와 서명에 기초하여 상기 어플리케이션의 인증을 수행하는 서버 어플리케이션 인증부를 포함하는

어플리케이션 인증 시스템.

청구항 20.

단말, 인증 모듈, 및 어플리케이션을 단말로 다운로딩하는 서버를 포함하는 어플리케이션 인증 시스템에 있어서,

상기 단말은, 상기 어플리케이션을 다운로딩하는 다운로딩부; 상기 어플리케이션의 인증 성공을 나타내는 인증 성공 정보를 생성하는 인증 성공 정보 생성 수단; 및 상기 인증 성공 정보 생성 수단에서 생성된 인증 성공 정보를 출력하는 인증 성공 정보 출력 수단을 포함하는 TRM 억세스 라이브러리부를 포함하고,

상기 인증 모듈은, 상기 TRM 억세스 라이브러리부를 인증하기 위한 정보인 TRM 억세스 라이브러리부 인증 정보를 내템퍼 영역에 유지하는 TRM부; 및 상기 TRM 억세스 라이브러리부 인증 정보에 기초하여 상기 단말의 TRM 억세스 라이브러리부를 인증하는 TRM 억세스 라이브러리부 인증부를 포함하고,

상기 서버는, 상기 단말의 TRM 억세스 라이브러리부를 통한 상기 인증 모듈의 TRM부의 인증 성공을 조건으로 하여 상기 TRM 억세스 라이브러리부의 인증이 성공했다고 판단하는 서버 TRM 억세스 라이브러리부 인증부; 상기 서버 TRM 억세스 라이브러리부 인증부에 의해 인증이 성공했다고 판단된 상기 TRM 억세스 라이브러리부의 인증 성공 정보 출력 수단에서 출력된 인증 성공 정보를 입력하는 인증 성공 정보 입력부; 및 상기 인증 성공 정보 입력부에 입력된 인증 성공 정보에 기초하여 어플리케이션의 인증을 수행하는 서버 어플리케이션 인증부를 포함하는

어플리케이션 인증 시스템.

청구항 21.

어플리케이션 본체 및 어플리케이션 정의 파일을 포함하는 어플리케이션 프 로그램을 저장하는 기록 매체에 있어서,

상기 어플리케이션 정의 파일은 상기 어플리케이션 본체의 속성을 나타내는 정보인 속성 정보 저장부에 어플리케이션의 작성자가 자유롭게 이용할 수 있는 선택 영역을 포함하고, 상기 선택 영역에 어플리케이션 본체의 서명 데이터를 저장하고,

상기 어플리케이션 프로그램은 상기 선택 영역에서 서명 데이터를 취득하는 단계; 및 상기 취득한 서명 데이터를 이용하여 서명을 검증하는 단계를 컴퓨터에서 실행하도록 하는

기록 매체.

청구항 22.

제21항에 있어서,

상기 어플리케이션 프로그램은 i어플리(iアプリ)이고, 상기 선택 영역은 AppParam인

기록 매체.

청구항 23.

어플리케이션 프로그램의 데이터 구조에 있어서,

코드 및 데이터의 압축 파일인 JAR 파일을 저장하는 JAR 파일부; 및

어플리케이션의 정의 파일인 ADF 파일을 저장하는 ADF 파일부;

를 포함하고,

상기 ADF 파일에는 메인 클래스의 기동 파라미터를 저장하는 AppParam이 있고, 상기 AppParam중에 JAR 파일의 서명이 저장되어 있는

어플리케이션 프로그램의 데이터 구조.

청구항 24.
제23항에 있어서,

상기 JAR 파일의 서명은 상기 어플리케이션 프로그램의 동작을 보증하는 사람에 의한 서명인

데이터 구조.

청구항 25.
제23항 또는 제24항에 기재된 데이터 구조에 의해 어플리케이션 프로그램을 컴퓨터로 판독 가능하게 기록한 기록 매체.

청구항 26.
제2항 내지 제4항 중 어느 한 항에 있어서,

상기 다운로딩부는 다운로딩 어플리케이션의 어플리케이션 이용 리소스 정보를 기술한 서명 첨부의 사용 허락서를 다운로딩하는

어플리케이션 인증 시스템.

청구항 27.
제26항에 있어서,

상기 어플리케이션 이용 리소스 정보는 로컬 리소스의 종류인

어플리케이션 인증 시스템.

청구항 28.
제26항에 있어서,

상기 어플리케이션 이용 리소스 정보는 상기 로컬 리소스의 사용을 인정하는 범위인

어플리케이션 인증 시스템.

청구항 29.
제18항에 있어서,

상기 TRM 억세스 라이브러리부는 상기 어플리케이션의 인증을 위한 처리를 상기 어플리케이션이 인증 모듈의 TRM부의 내템퍼 영역으로 억세스한 것을 조건으로 수행하는

어플리케이션 인증 시스템.

청구항 30.
제18항에 있어서,

상기 TRM 억세스 라이브러리부는 상기 어플리케이션의 인증을 위한 처리를 상기 어플리케이션이 다운로딩부로 다운로딩된 것을 조건으로 수행하는

어플리케이션 인증 시스템.

청구항 31.
제18항에 있어서,

상기 TRM 억세스 라이브러리부는 상기 어플리케이션 인증을 위한 처리를 상기 어플리케이션의 실행의 시작을 트리거로 하여 수행하는

어플리케이션 인증 시스템.

청구항 32.
제26항에 있어서,

상기 사용 허락서의 어플리케이션 이용 리소스 정보에는 상기 어플리케이션이 리소스를 억세스할 수 있는 시간적 한도를 나타내는 기한일 정보가 포함되어 있고,

상기 기한일 정보에 기초하여 인정되는 시간적 한도가 이미 기한이 다 된 경우, 상기 다운로딩부는 사용 허락서를 다운로딩하는

어플리케이션 인증 시스템.

청구항 33.
제2항 내지 제4항 중 어느 한 항에 있어서,

상기 다운로딩부는 다운로딩된 어플리케이션의 실행시 또는/및 어플리케이션의 인증시에 서버로부터 사용 허락서를 다운로딩하는

어플리케이션 인증 시스템.

청구항 34.
제26항에 있어서,

상기 다운로딩부는 다운로딩된 어플리케이션의 실행시 또는/및 어플리케이션의 인증시에 다운로딩된 사용 허락서의 유효성을 서버에 문의하는

어플리케이션 인증 시스템.

청구항 35.
제1항 내지 제21항, 제26항 내지 제34항 중 어느 한 항에 기재된 단말.

청구항 36.
제1항 내지 제21항 중 어느 한 항에 기재된 인증 모듈.

청구항 37.
어플리케이션을 다운로딩하는 다운로딩부; 및

상기 어플리케이션의 인증 처리를 위한 정보를 내템퍼 영역에 유지하는 TRM부

를 포함하는 단말.

청구항 38.
내템퍼 영역에 정보를 유지하고 그 정보를 이용하여 인증을 위한 처리를 수행하는 인증 모듈을 포함하는 단말에 있어서,

어플리케이션을 다운로딩하는 다운로딩부; 및

상기 인증 모듈에 자신이 인증되는 것을 조건으로 하여 상기 어플리케이션의 인증을 위한 처리를 하는 TRM 억세스 라이브러리부

를 포함하고,

상기 인증 모듈은, 상기 TRM 억세스 라이브러리부를 인증하기 위한 정보인 TRM 억세스 라이브러리부 인증 정보를 상기 내템퍼 영역에 유지하는 TRM부; 및 상기 TRM 억세스 라이브러리부 인증 정보에 기초하여 상기 TRM 억세스 라이브러리부를 인증하는 TRM 억세스 라이브러리부 인증부를 포함하는

단말.

청구항 39.
제1 기기 및 인증 모듈을 포함하는 어플리케이션 인증 시스템에 있어서,

상기 제1 기기는 어플리케이션을 저장하는 어플리케이션 저장부를 포함하고,

상기 인증 모듈은 상기 어플리케이션의 인증 처리를 위한 정보를 내템퍼 영역에 유지하는 TRM부를 포함하는

어플리케이션 인증 시스템.

청구항 40.
제1 기기 및 인증 모듈을 포함하는 어플리케이션 인증 시스템에 있어서,

상기 제1 기기는, 어플리케이션을 저장하는 어플리케이션 저장부; 및 상기 인증 모듈에 자신이 인증되는 것을 조건으로 하여 상기 어플리케이션의 인증을 위한 처리를 하는 TRM 억세스 라이브러리부를 포함하고,

상기 인증 모듈은, 상기 TRM 억세스 라이브러리부를 인증하기 위한 정보인 TRM 억세스 라이브러리부 인증 정보를 내템퍼 영역에 유지하는 TRM부; 및 상기 TRM 억세스 라이브러리부 인증 정보에 기초하여 상기 제1 기기의 TRM 억세스 라이브러리부를 인증하는 TRM 억세스 라이브러리부 인증부를 포함하는

어플리케이션 인증 시스템.

청구항 41.
제1 기기부터 제(N+1) 기기까지 직렬로 접속하여 이루어지는 (N+1)개의 기기에 의해 구성되는 어플리케이션 인증 시스템에 있어서,

상기 제1 기기는, 제2 기기를 인증하기 위한 정보인 인증 정보를 내템퍼 영역에 유지하는 TRM부; 및 상기 인증 정보에 기초하여 상기 제2 기기를 인증하는 제1 인증 처리부를 포함하고,

상기 제2 기기부터 제N 기기까지 중 어느 하나의 기기를 제i 기기라 할 때,

상기 제i 기기는 제i 인증 처리부를 포함하고,

상기 제i 인증 처리부는 제(i-1) 인증 처리부에 자신이 인증되는 것을 조건으로 하여 제(i+1) 기기를 인증하고,

상기 제(N+1) 기기는, 상기 어플리케이션을 저장하는 어플리케이션 저장부; 및 제N 인증 처리부에 자신이 인증되는 것을 조건으로 하여 상기 어플리케이션의 인증을 위한 처리를 하는 제(N+1) 인증 처리부를 포함하는

어플리케이션 인증 시스템.

청구항 42.
제41항에 있어서,

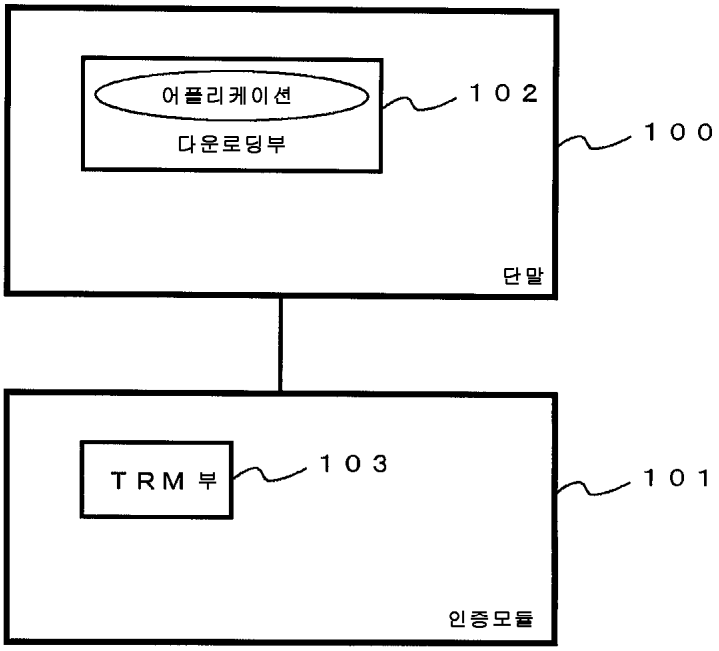
상기 제i 기기는 제(i+1) 기기를 인증하기 위한 인증 정보를 취득하는 제i 인증 정보 취득부를 포함하고,

상기 제i 인증 정보 취득부는 상기 제i 기기가 인증 정보를 저장하고 있는 영역인 인증 정보 저장 영역을 포함하고 있는 경우, 그 인증 정보 저장 영역으로부터 상기 인증 정보를 취득하고, 상기 제1 기기의 상기 TRM부에 상기 인증 정보가 저장되어 있는 경우, 상기 제2 기기부터 제(i-1) 기기까지의 기기를 통하여, 상기 TRM부로부터 상기 인증 정보를 취득하는

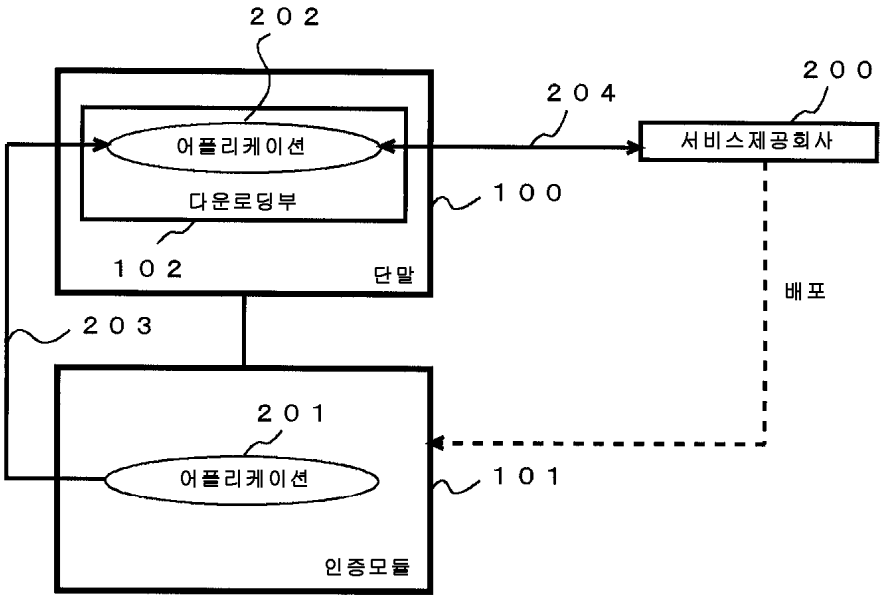
어플리케이션 인증 시스템.

도면

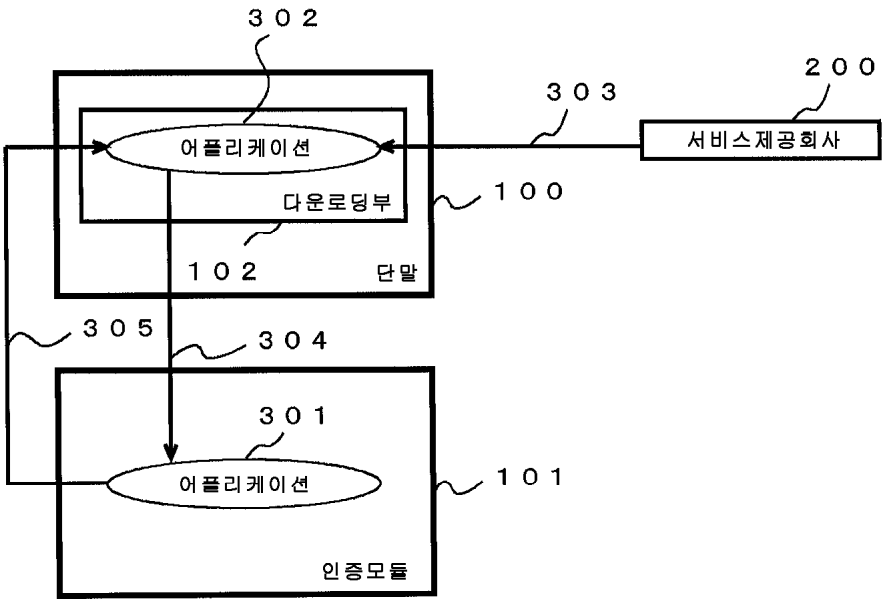
도면1


어플리케이션
다운로딩부
102
100
단말
TRM 부
103
101
인증모듈

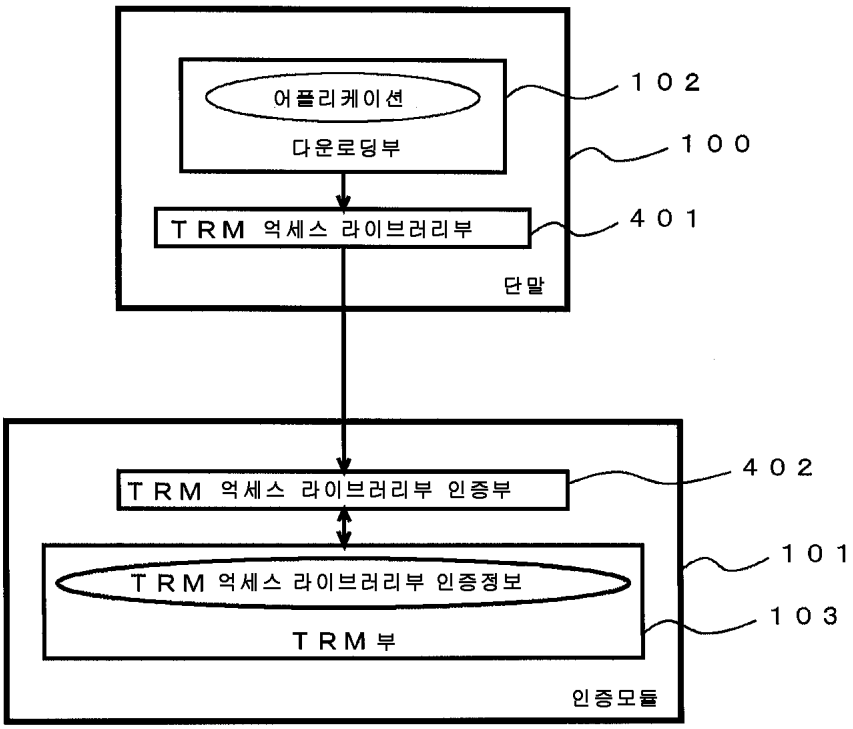
도면2


202
200
204
어플리케이션
서비스제공회사
다운로딩부
100
102
단말
배포
203
201
어플리케이션
101
인증모듈

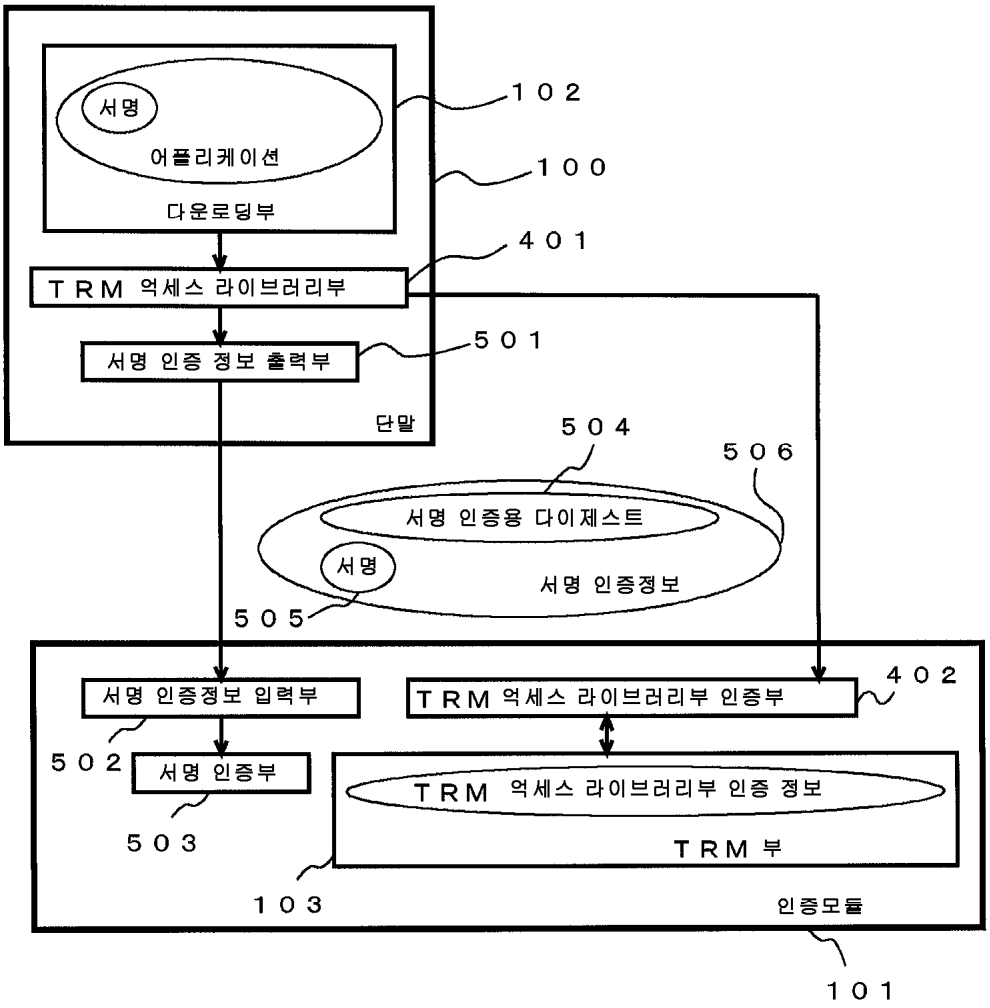
도면3


302
303
200
어플리케이션
서비스제공회사
다운로딩부
100
102
단말
305
304
301
어플리케이션
101
인증모듈

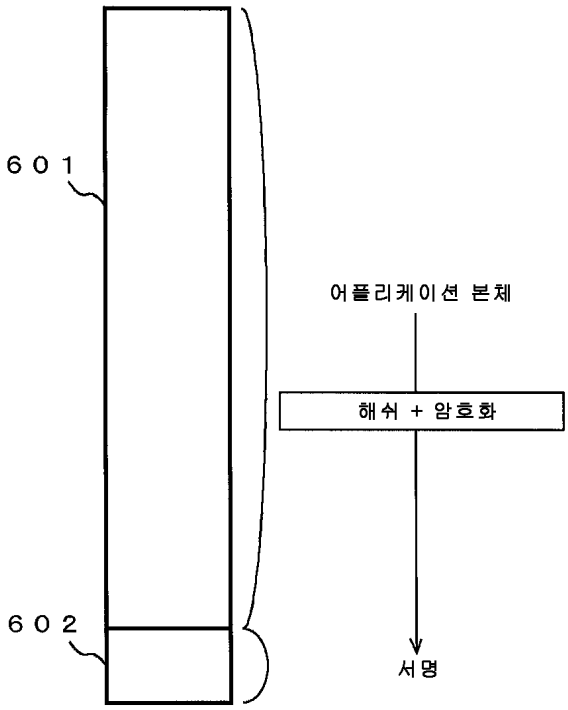
도면4


어플리케이션
다운로딩부
102
100
TRM 억세스 라이브러리부
401
단말
TRM 억세스 라이브러리부 인증부
402
TRM 억세스 라이브러리부 인증정보
101
TRM부
103
인증모듈

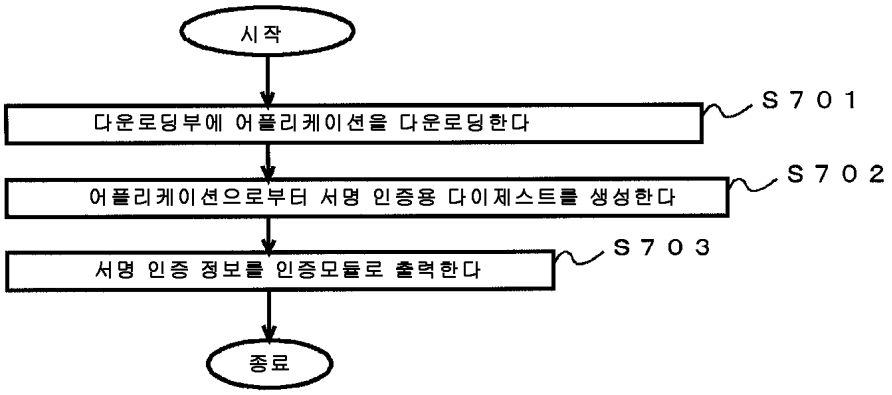
도면5


서명
어플리케이션
다운로딩부
102
100
401
TRM 억세스 라이브러리부
501
서명 인증 정보 출력부
단말
504
506
서명 인증용 다이제스트
서명
서명 인증정보
505
서명 인증정보 입력부
TRM 억세스 라이브러리부 인증부
402
502
서명 인증부
503
TRM 억세스 라이브러리부 인증 정보
TRM 부
103
인증모듈
101

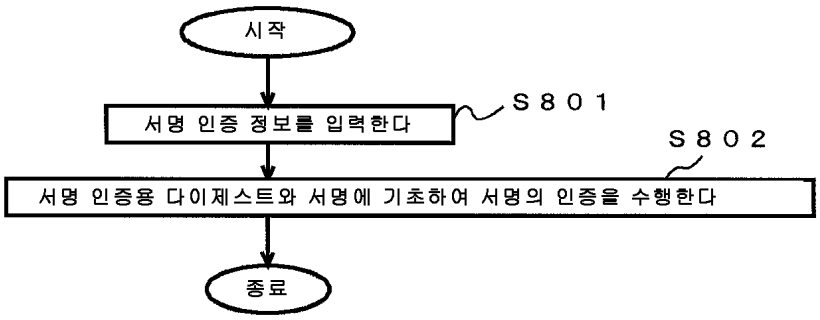
도면6


601
어플리케이션 본체
해쉬 + 암호화
602
서명

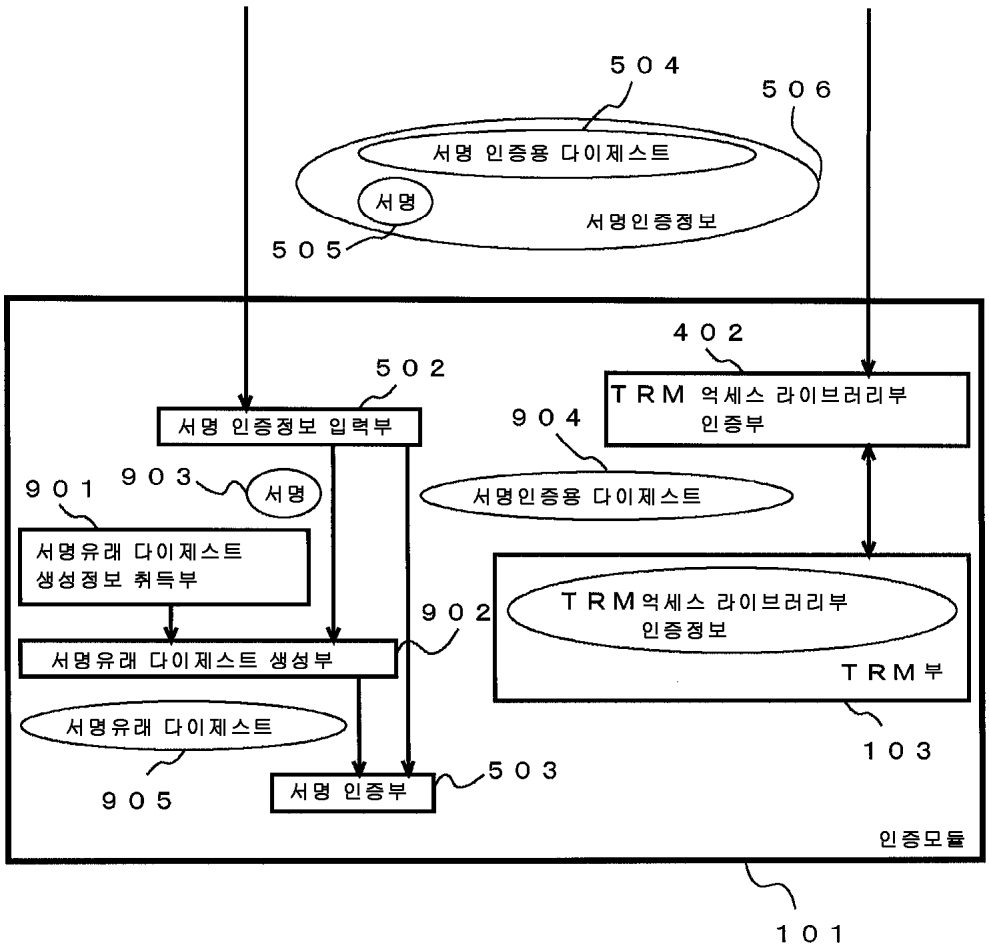
도면7


시작
다운로딩부에 어플리케이션을 다운로딩한다
S701
어플리케이션으로부터 서명 인증용 다이제스트를 생성한다
S702
서명 인증 정보를 인증모듈로 출력한다
S703
종료

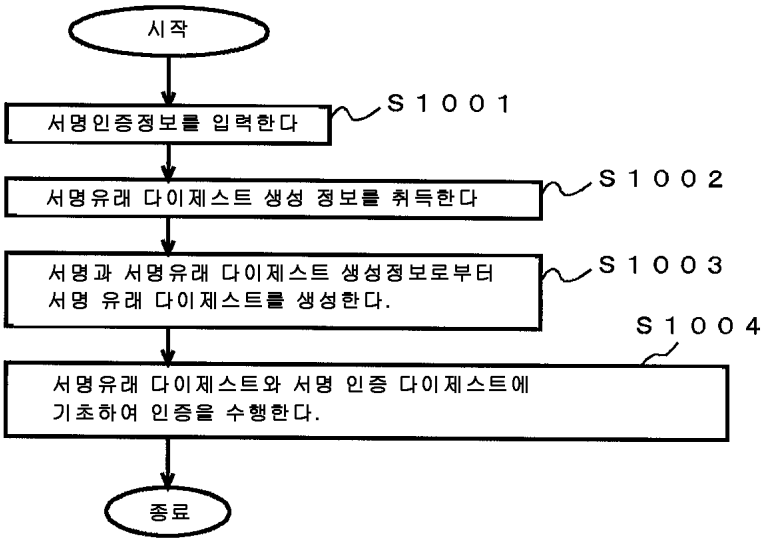
도면8


시작
서명 인증 정보를 입력한다
S801
서명 인증용 다이제스트와 서명에 기초하여 서명의 인증을 수행한다
S802
종료

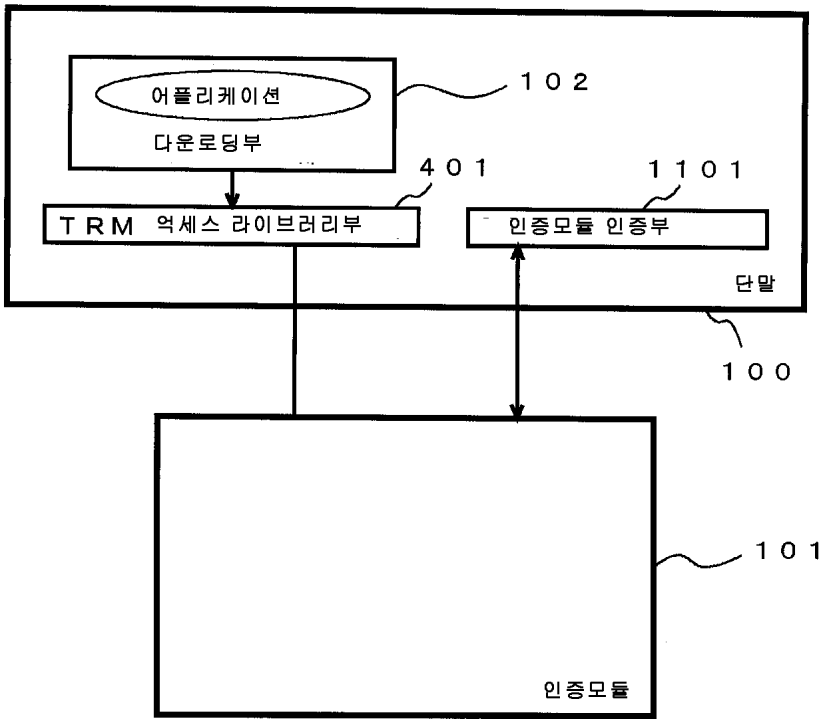
도면9


504
506
서명 인증용 다이제스트
서명
서명인증정보
505
402
502
TRM 억세스 라이브러리부
인증부
서명 인증정보 입력부
904
901
903
서명
서명인증용 다이제스트
서명유래 다이제스트
생성정보 취득부
902
TRM억세스 라이브러리부
인증정보
TRM부
서명유래 다이제스트 생성부
103
서명유래 다이제스트
905
서명 인증부
503
인증모듈
101

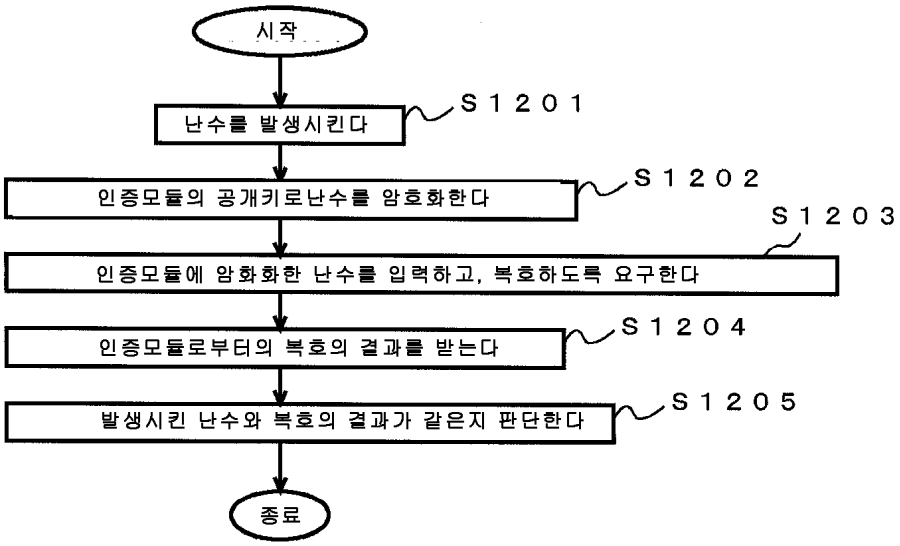
도면10


시작
서명인증정보를 입력한다
S1001
서명유래 다이제스트 생성 정보를 취득한다
S1002
서명과 서명유래 다이제스트 생성정보로부터
서명 유래 다이제스트를 생성한다.
S1003
S1004
서명유래 다이제스트와 서명 인증 다이제스트에
기초하여 인증을 수행한다.
종료

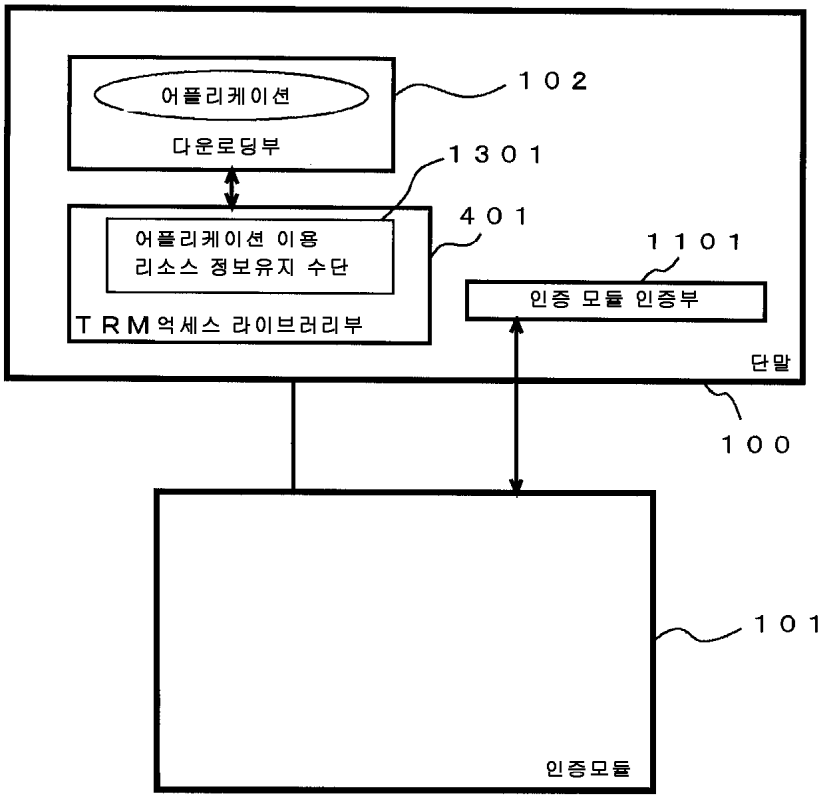
도면11


어플리케이션
다운로딩부
102
401
1101
TRM 억세스 라이브러리부
인증모듈 인증부
단말
100
101
인증모듈

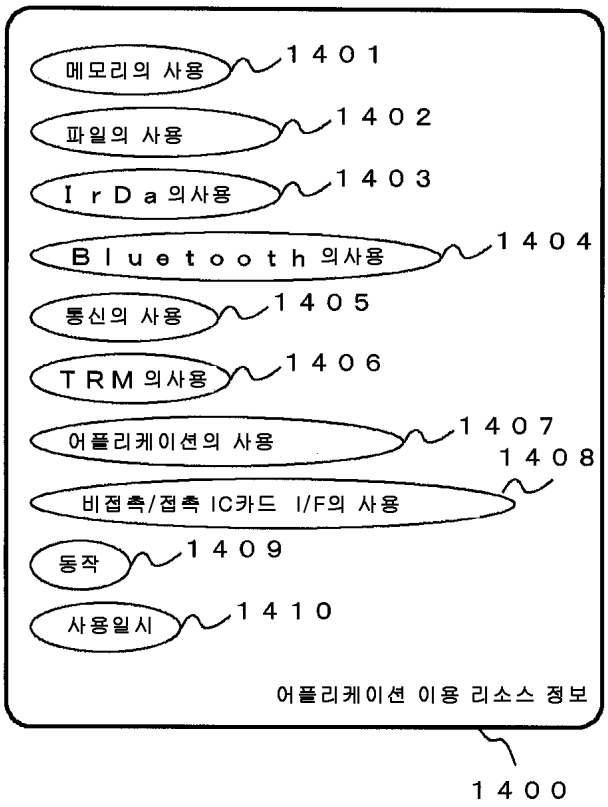
도면12


시작
난수를 발생시킨다
S1201
인증모듈의 공개키로난수를 암호화한다
S1202
인증모듈에 암화화한 난수를 입력하고, 복호하도록 요구한다
S1203
인증모듈로부터의 복호의 결과를 받는다
S1204
발생시킨 난수와 복호의 결과가 같은지 판단한다
S1205
종료

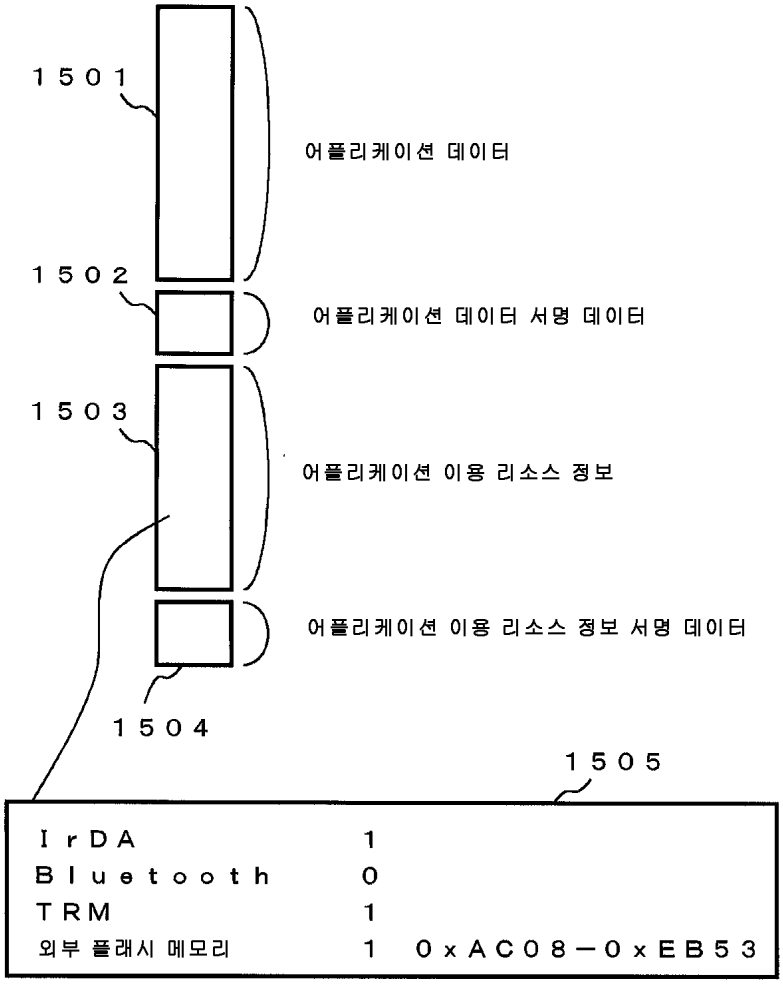
도면13


어플리케이션
다운로딩부
102
1301
어플리케이션 이용
리소스 정보유지 수단
401
TRM억세스 라이브러리부
1101
인증 모듈 인증부
단말
100
101
인증모듈

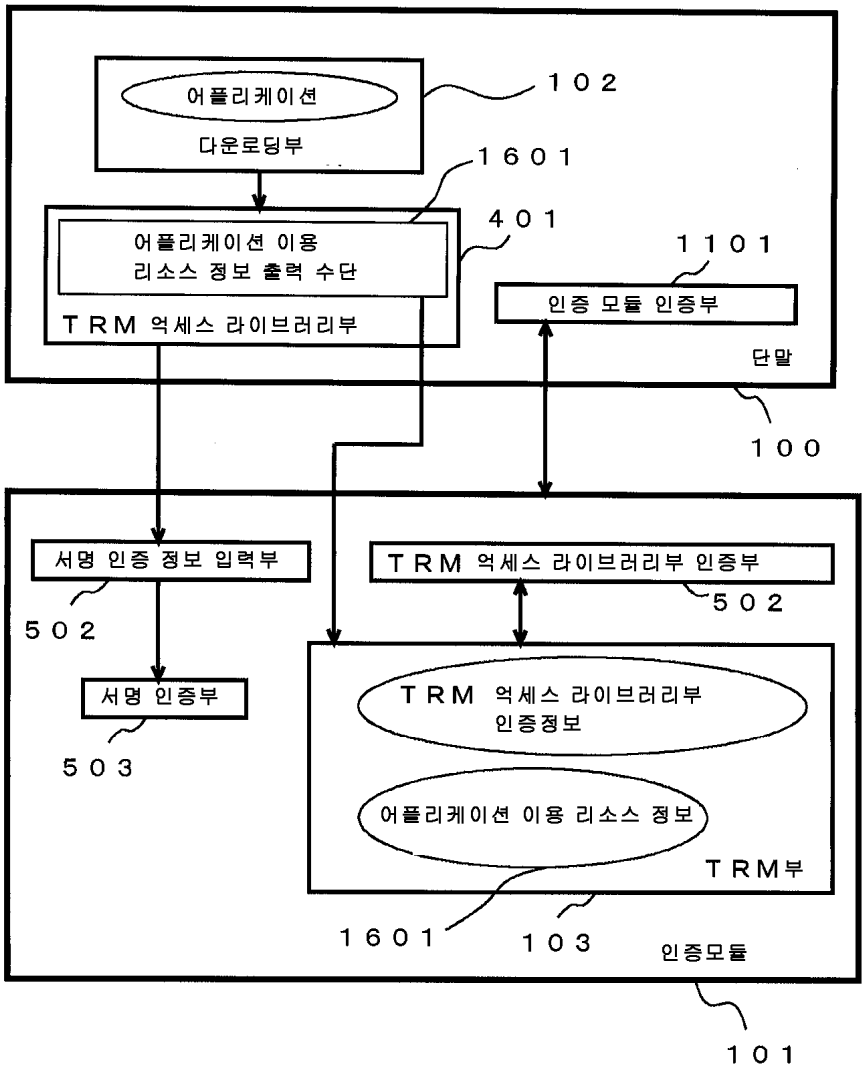
도면14


메모리의 사용
1401
파일의 사용
1402
IrDa 의사용
1403
Bluetooth 의사용
1404
통신의 사용
1405
TRM 의사용
1406
어플리케이션의 사용
1407
1408
비접촉/접촉 IC카드 I/F의 사용
동작
1409
사용일시
1410
어플리케이션 이용 리소스 정보
1400

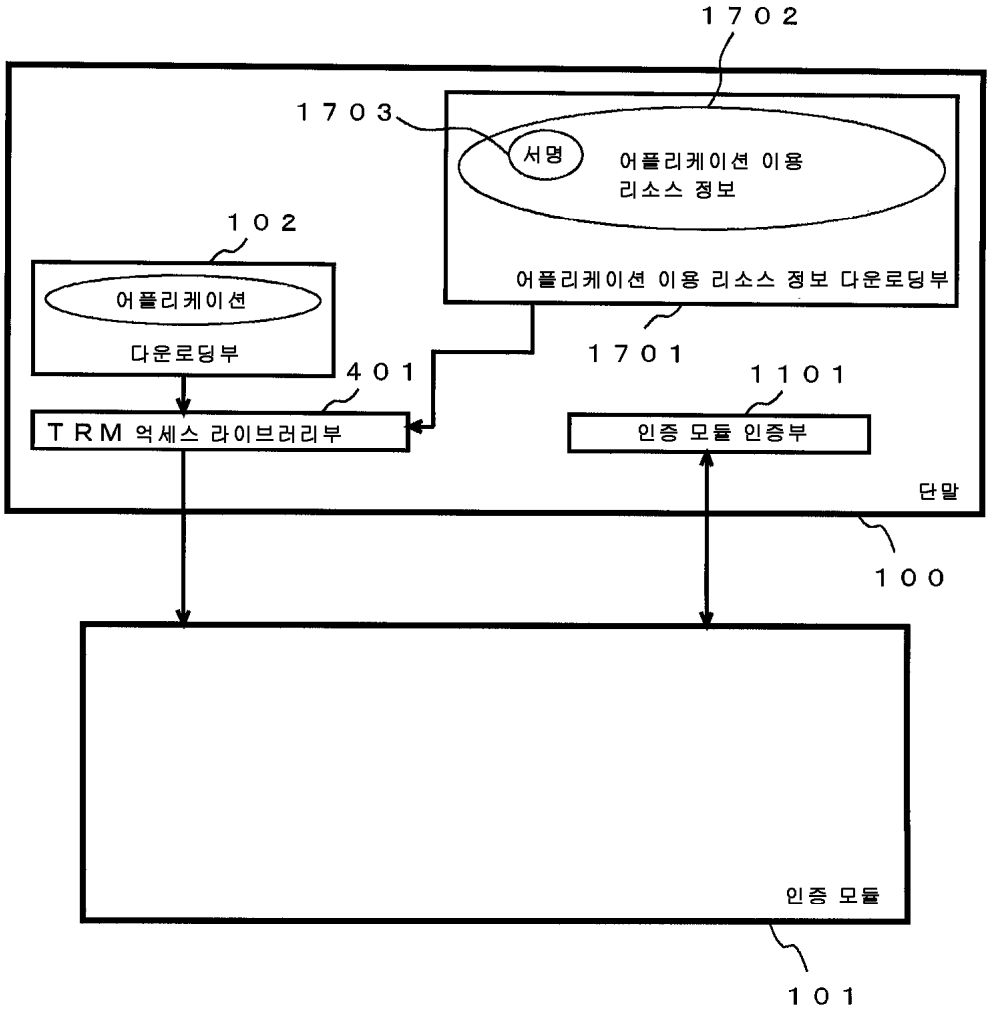
도면15


1501
어플리케이션 데이터
1502
어플리케이션 데이터 서명 데이터
1503
어플리케이션 이용 리소스 정보
어플리케이션 이용 리소스 정보 서명 데이터
1504
1505
IrDA 1
Bluetooth 0
TRM 1
외부 플래시 메모리 1 0xAC08－0xEB53

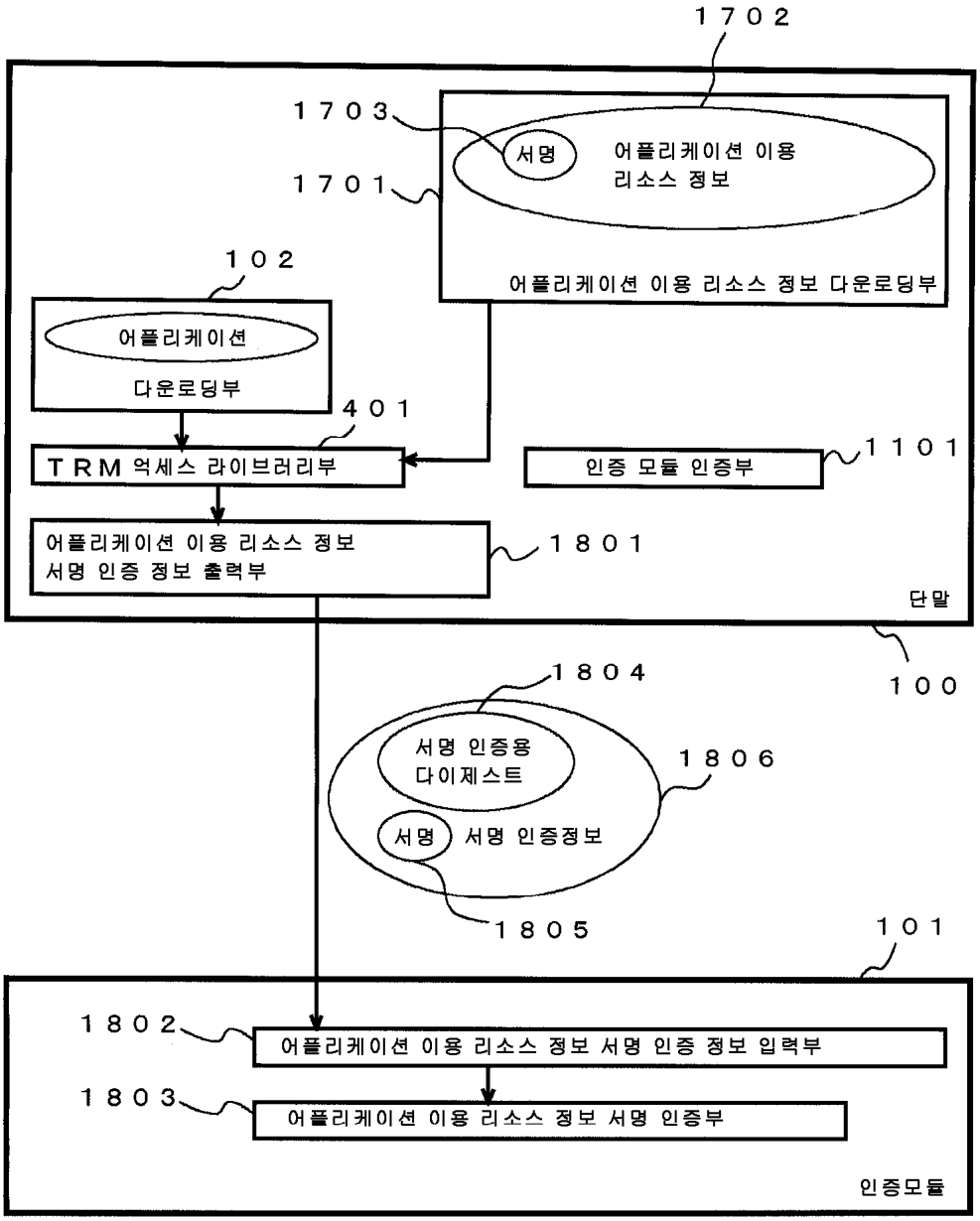
도면16


어플리케이션
다운로딩부
102
1601
401
어플리케이션 이용
리소스 정보 출력 수단
TRM 억세스 라이브러리부
1101
인증 모듈 인증부
단말
100
서명 인증 정보 입력부
502
TRM 억세스 라이브러리부 인증부
502
서명 인증부
503
TRM 억세스 라이브러리부
인증정보
어플리케이션 이용 리소스 정보
TRM부
1601
103
인증모듈
101

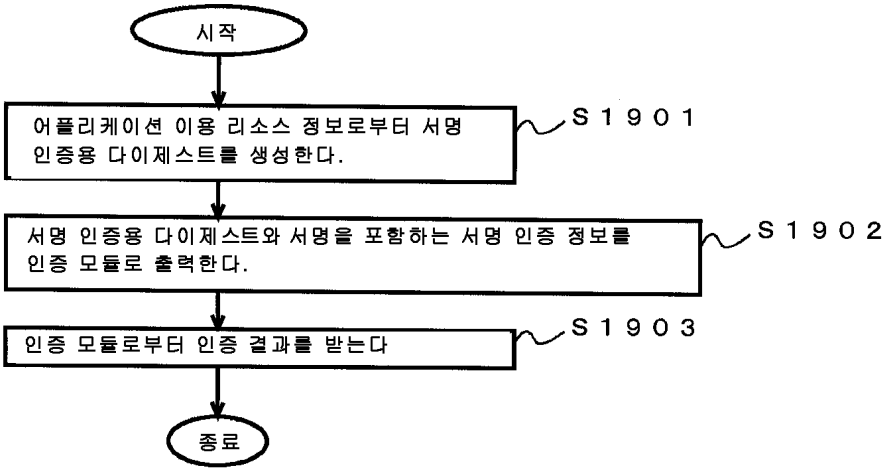
도면17


1702
1703
서명
어플리케이션 이용
리소스 정보
어플리케이션 이용 리소스 정보 다운로딩부
102
어플리케이션
다운로딩부
1701
401
1101
TRM 억세스 라이브러리부
인증 모듈 인증부
단말
100
인증 모듈
101

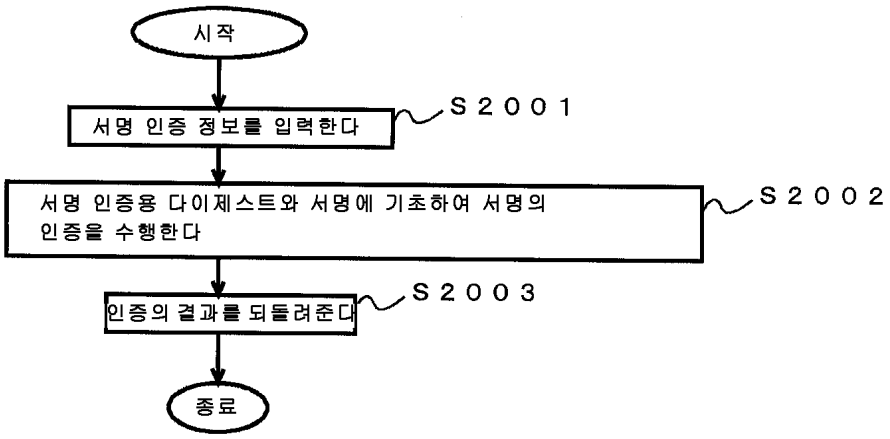
도면18


1702
1703
서명
어플리케이션 이용
리소스 정보
1701
어플리케이션 이용 리소스 정보 다운로딩부
102
어플리케이션
다운로딩부
401
TRM 억세스 라이브러리부
인증 모듈 인증부
1101
어플리케이션 이용 리소스 정보
서명 인증 정보 출력부
1801
단말
100
1804
서명 인증용
다이제스트
1806
서명
서명 인증정보
1805
101
1802
어플리케이션 이용 리소스 정보 서명 인증 정보 입력부
1803
어플리케이션 이용 리소스 정보 서명 인증부
인증모듈

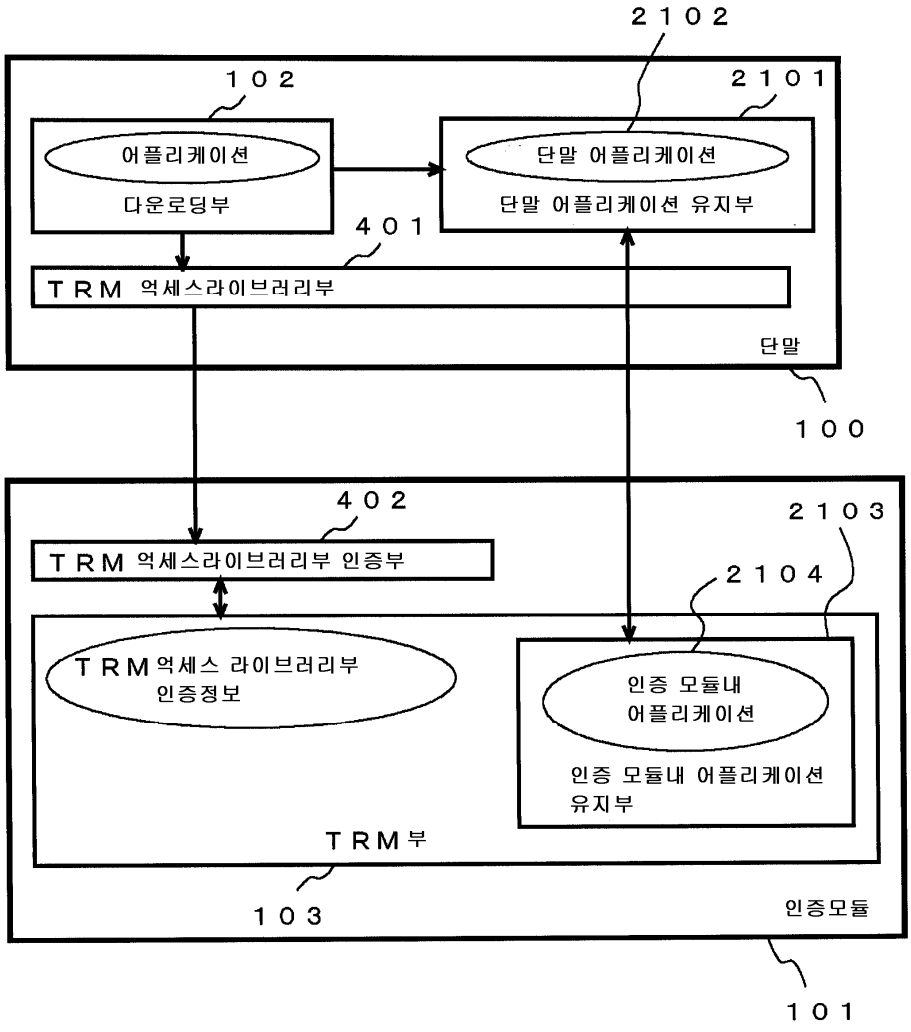
도면19


시작
어플리케이션 이용 리소스 정보로부터 서명
인증용 다이제스트를 생성한다.
S1901
서명 인증용 다이제스트와 서명을 포함하는 서명 인증 정보를
인증 모듈로 출력한다.
S1902
인증 모듈로부터 인증 결과를 받는다
S1903
종료

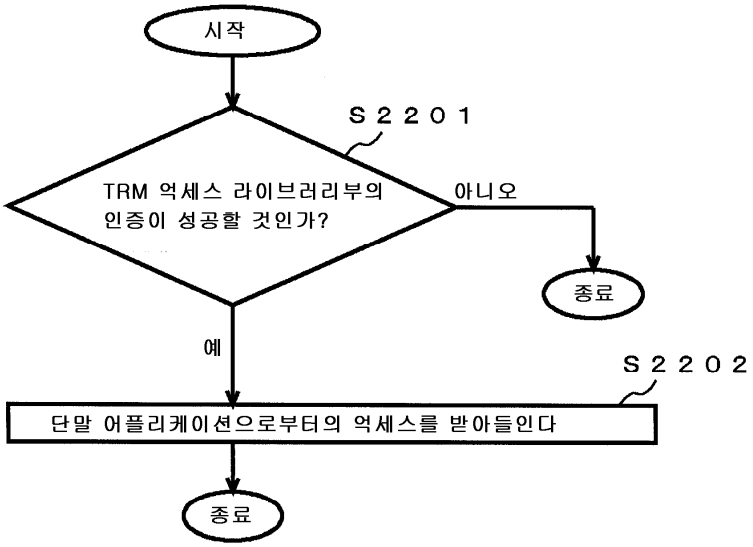
도면20


시작
서명 인증 정보를 입력한다
S2001
서명 인증용 다이제스트와 서명에 기초하여 서명의 인증을 수행한다
S2002
인증의 결과를 되돌려준다
S2003
종료

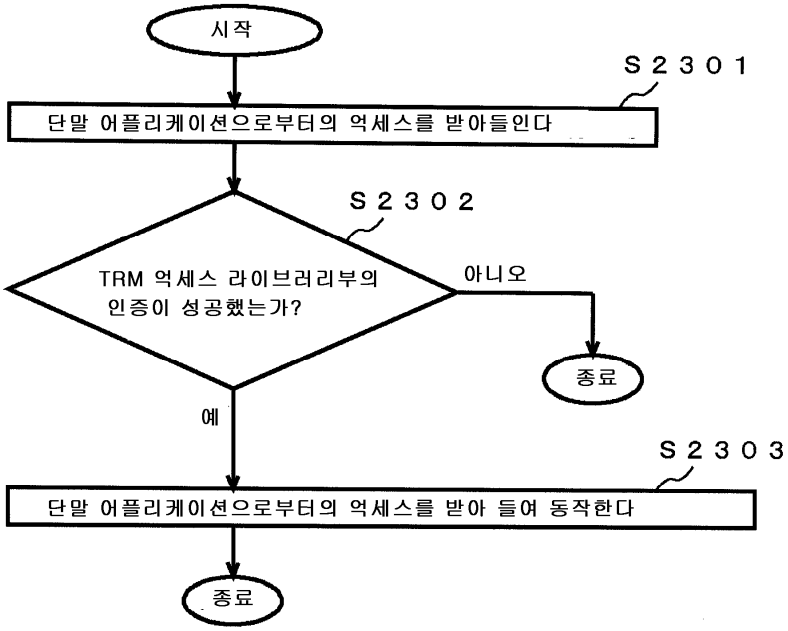
도면21


2102
102
2101
어플리케이션
다운로딩부
단말 어플리케이션
단말 어플리케이션 유지부
401
TRM 억세스라이브러리부
단말
100
402
2103
TRM 억세스라이브러리부 인증부
2104
TRM억세스 라이브러리부 인증정보
인증 모듈내 어플리케이션
인증 모듈내 어플리케이션 유지부
TRM부
103
인증모듈
101

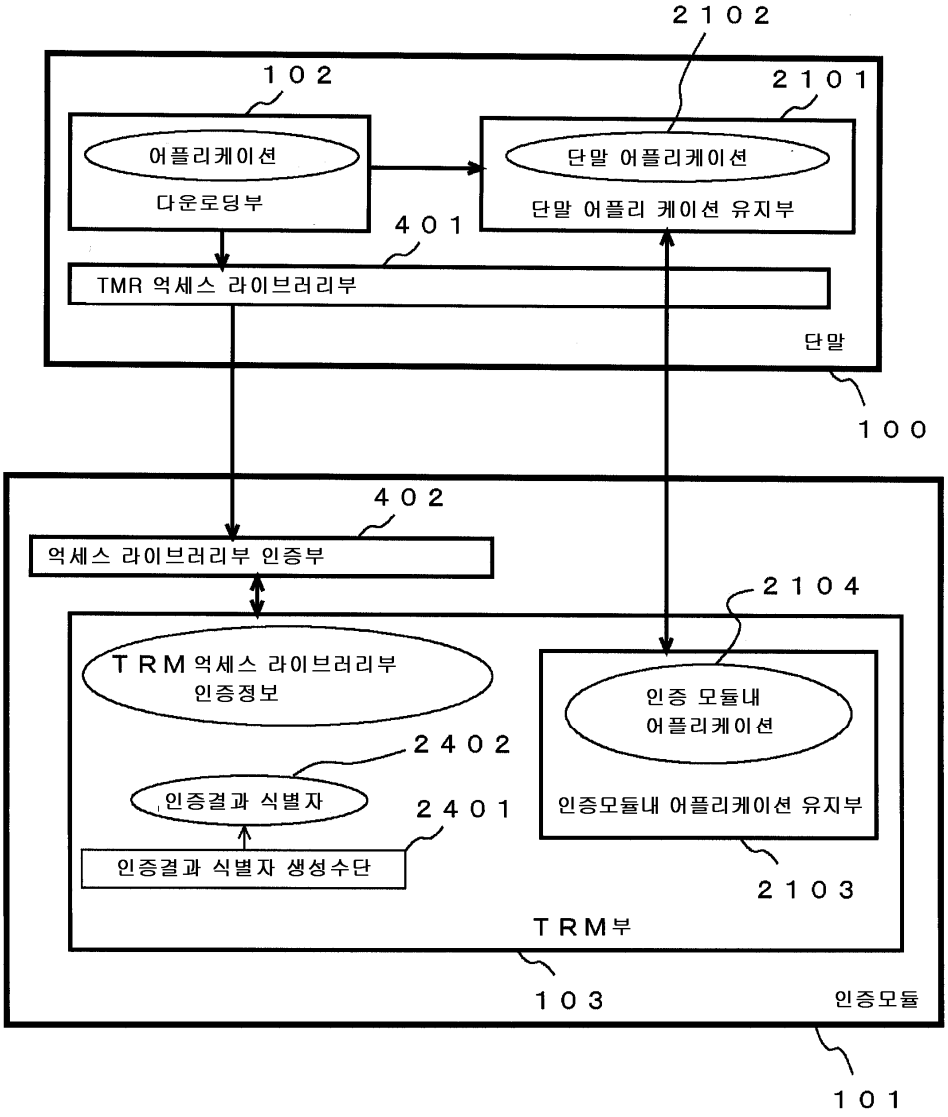
도면22


시작
S 2 2 0 1
TRM 억세스 라이브러리부의
인증이 성공할 것인가?
아니오
종료
예
S 2 2 0 2
단말 어플리케이션으로부터의 억세스를 받아들인다
종료

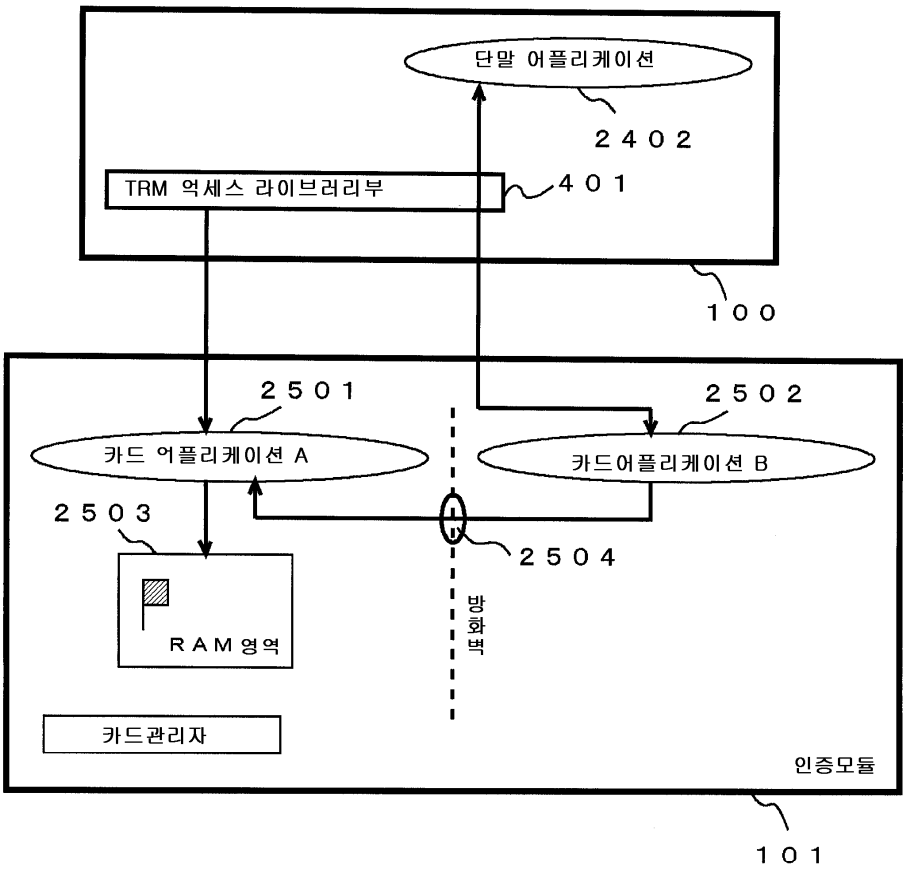
도면23


시작
S 2 3 0 1
단말 어플리케이션으로부터의 억세스를 받아들인다
S 2 3 0 2
TRM 억세스 라이브러리부의
인증이 성공했는가?
아니오
종료
예
S 2 3 0 3
단말 어플리케이션으로부터의 억세스를 받아 들여 동작한다
종료

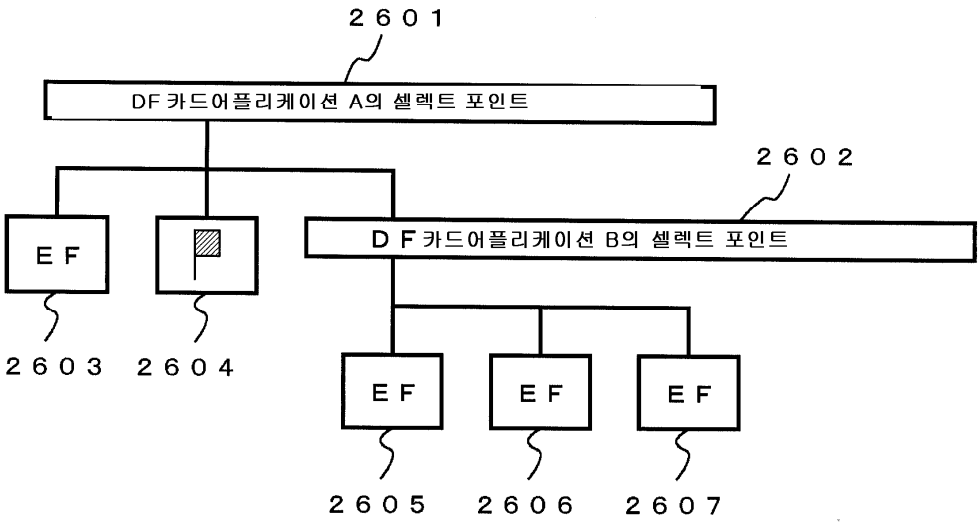
도면24


2102
102
2101
어플리케이션
다운로딩부
단말 어플리케이션
단말 어플리 케이션 유지부
401
TMR 억세스 라이브러리부
단말
100
402
억세스 라이브러리부 인증부
2104
TRM 억세스 라이브러리부
인증정보
인증 모듈내
어플리케이션
2402
인증결과 식별자
2401
인증결과 식별자 생성수단
인증모듈내 어플리케이션 유지부
2103
TRM부
103
인증모듈
101

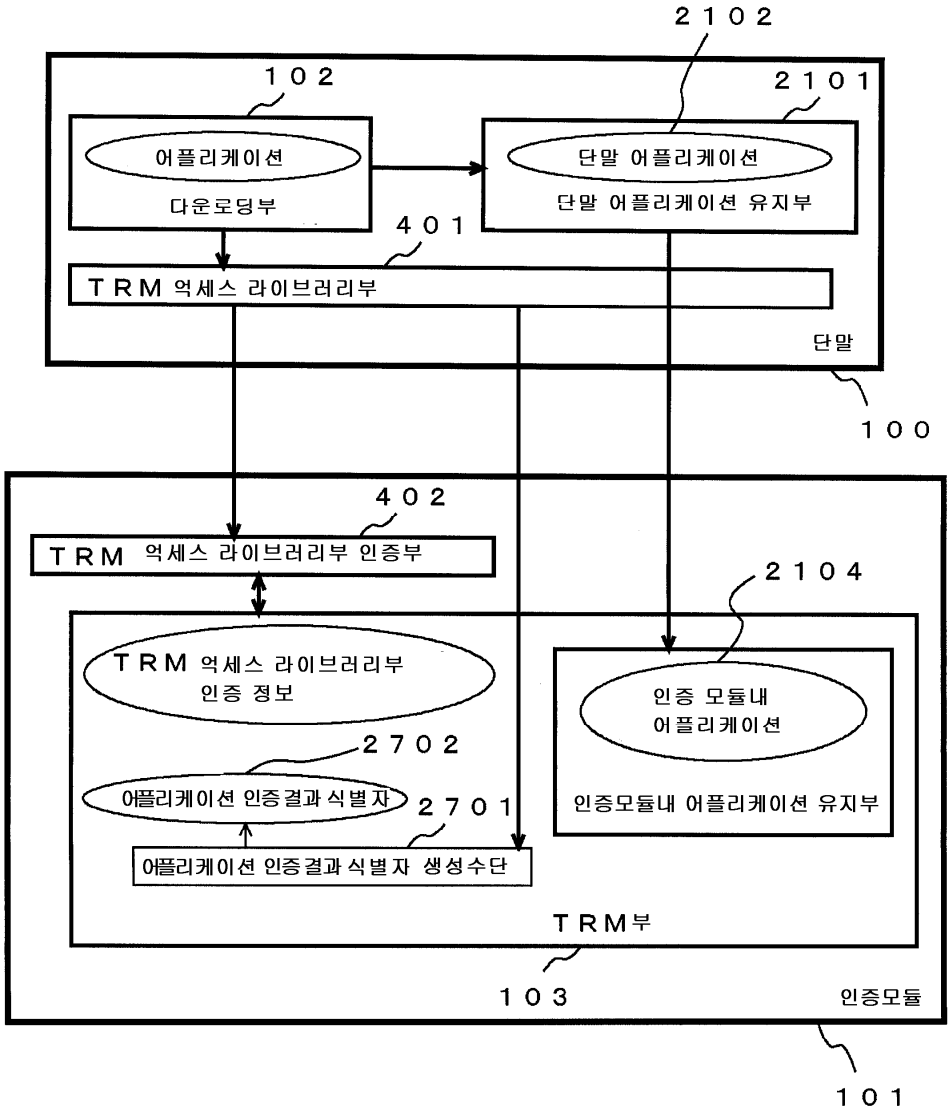
도면25


단말 어플리케이션
2402
TRM 억세스 라이브러리부
401
100
2501
2502
카드 어플리케이션 A
카드어플리케이션 B
2503
2504
RAM 영역
방화벽
카드관리자
인증모듈
101

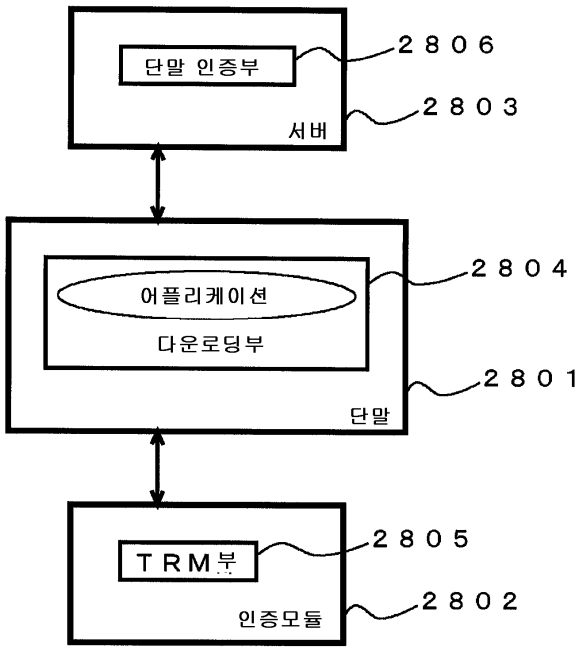
도면26


2601
DF 카드어플리케이션 A의 셀렉트 포인트
2602
EF
DF 카드어플리케이션 B의 셀렉트 포인트
2603
2604
EF
EF
EF
2605
2606
2607

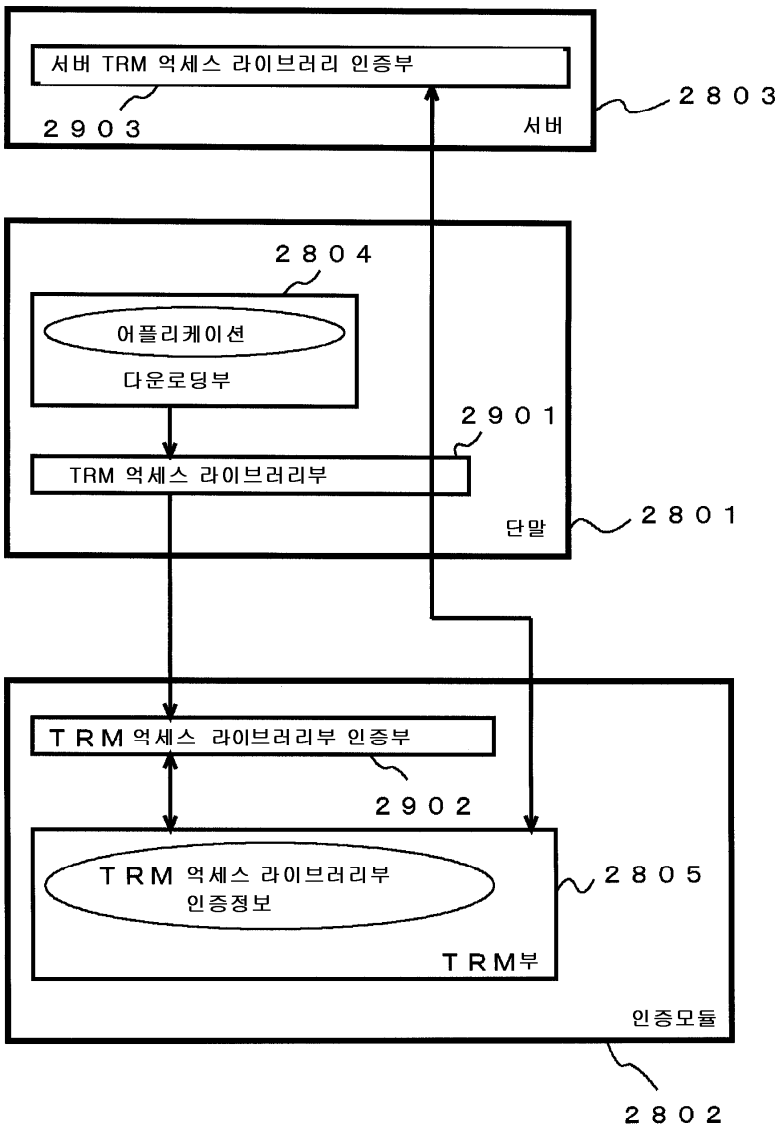
도면27


2102
102
2101
어플리케이션
다운로딩부
단말 어플리케이션
단말 어플리케이션 유지부
401
TRM 억세스 라이브러리부
단말
100
402
TRM 억세스 라이브러리부 인증부
2104
TRM 억세스 라이브러리부
인증 정보
인증 모듈내
어플리케이션
2702
어플리케이션 인증결과 식별자
2701
인증모듈내 어플리케이션 유지부
어플리케이션 인증결과 식별자 생성수단
TRM부
103
인증모듈
101

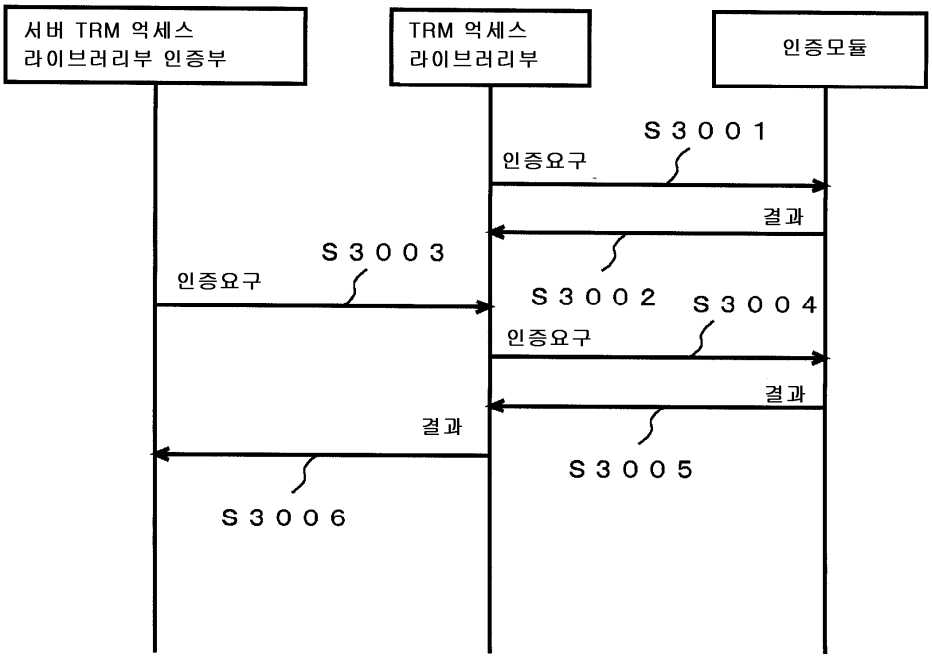
도면28


단말 인증부
2806
서버
2803
2804
어플리케이션
다운로딩부
2801
단말
2805
TRM부
인증모듈
2802

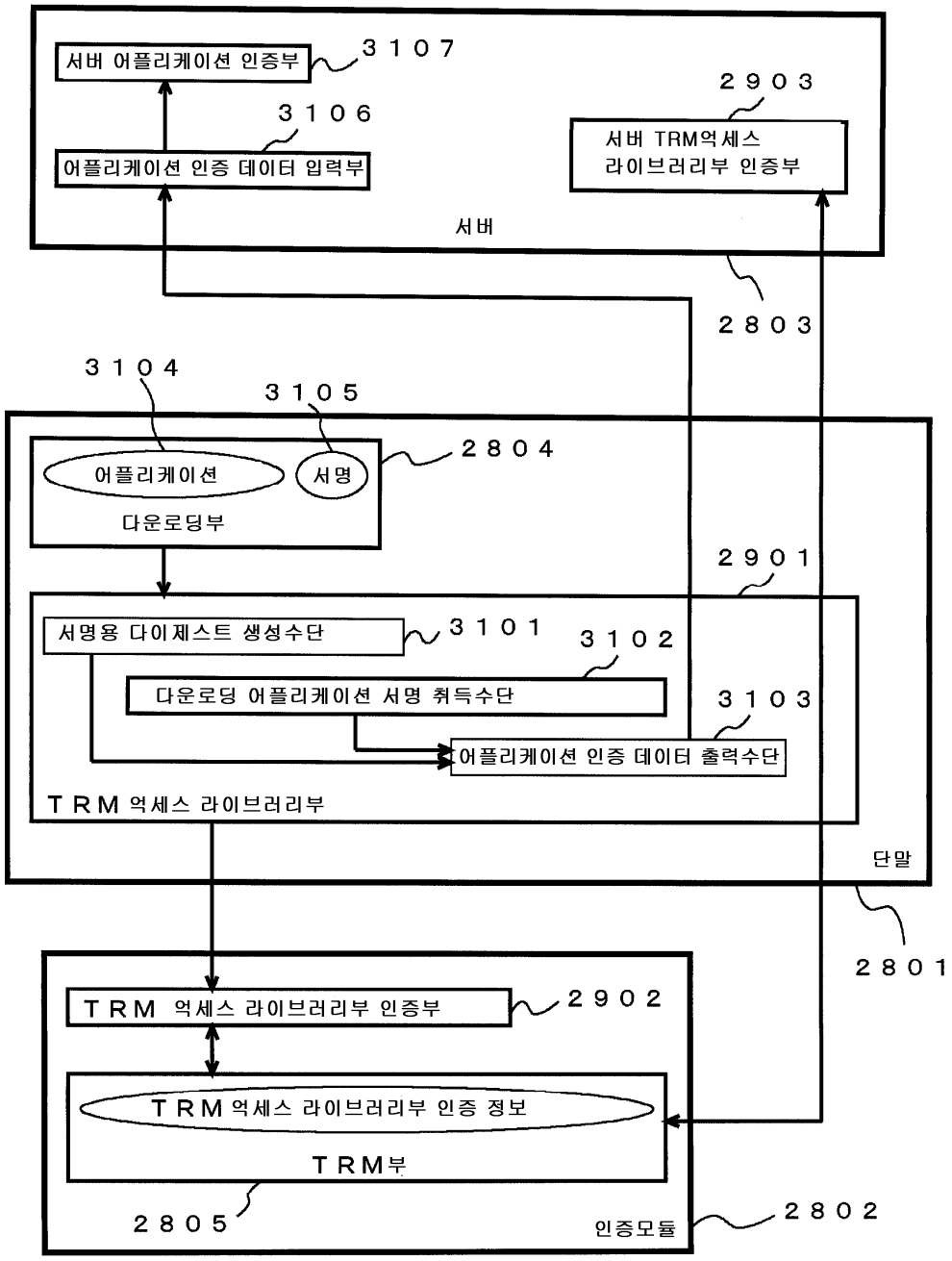
도면29


서버 TRM 억세스 라이브러리 인증부
２９０３
서버
２８０３
２８０４
어플리케이션
다운로딩부
２９０１
TRM 억세스 라이브러리부
단말
２８０１
ＴＲＭ 억세스 라이브러리부 인증부
２９０２
ＴＲＭ 억세스 라이브러리부
인증정보
ＴＲＭ부
２８０５
인증모듈
２８０２

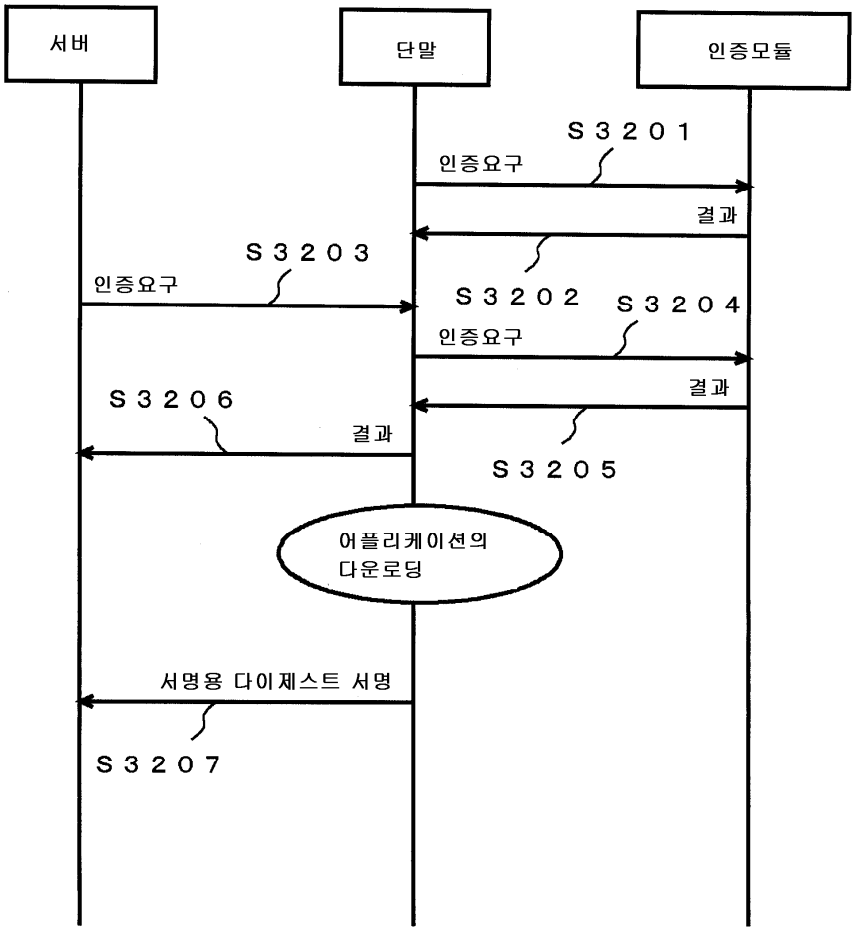
도면30


서버 TRM 억세스
라이브러리부 인증부
TRM 억세스
라이브러리부
인증모듈
Ｓ３００１
인증요구
결과
Ｓ３００３
인증요구
Ｓ３００２
Ｓ３００４
인증요구
결과
결과
Ｓ３００５
Ｓ３００６

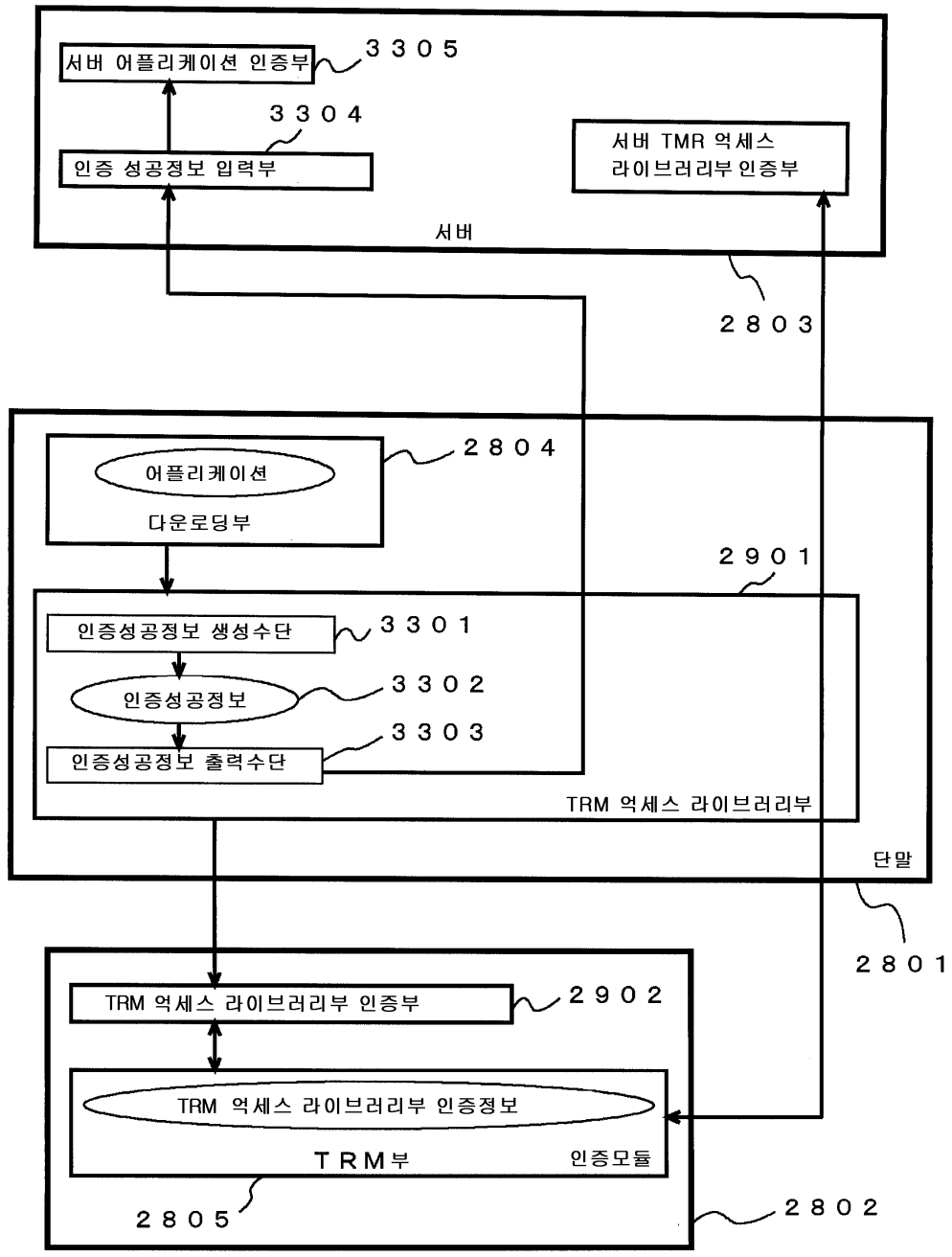
도면31


서버 어플리케이션 인증부
3107
3106
어플리케이션 인증 데이터 입력부
2903
서버 TRM억세스
라이브러리부 인증부
서버
2803
3104
3105
2804
어플리케이션
서명
다운로딩부
2901
서명용 다이제스트 생성수단
3101
3102
다운로딩 어플리케이션 서명 취득수단
3103
어플리케이션 인증 데이터 출력수단
TRM 억세스 라이브러리부
단말
2801
TRM 억세스 라이브러리부 인증부
2902
TRM억세스 라이브러리부 인증 정보
TRM부
2805
인증모듈
2802

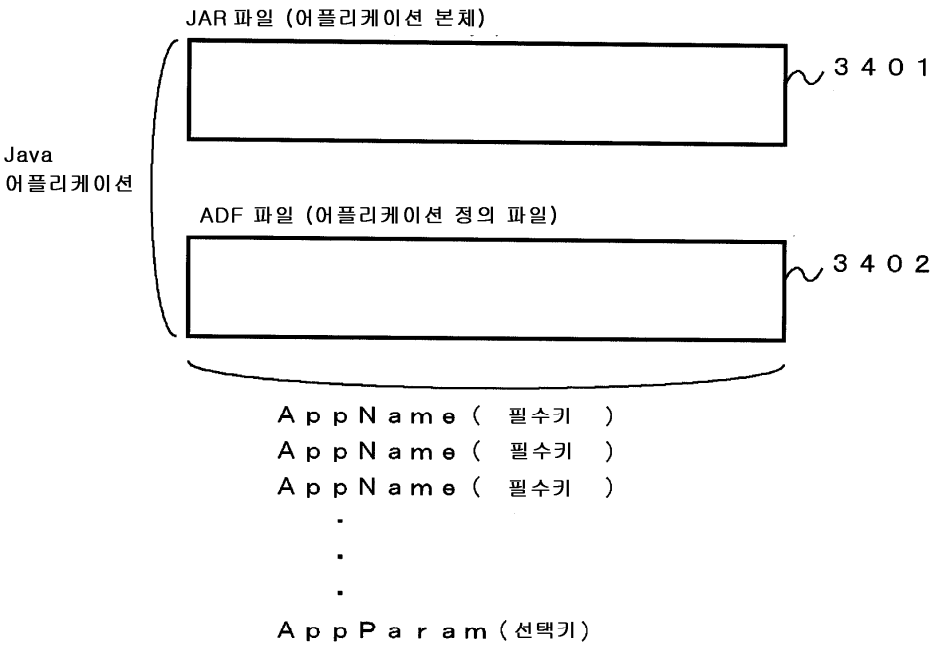
도면32


서버
단말
인증모듈
S 3 2 0 1
인증요구
결과
S 3 2 0 3
인증요구
S 3 2 0 2
S 3 2 0 4
인증요구
결과
S 3 2 0 6
결과
S 3 2 0 5
어플리케이션의
다운로딩
서명용 다이제스트 서명
S 3 2 0 7

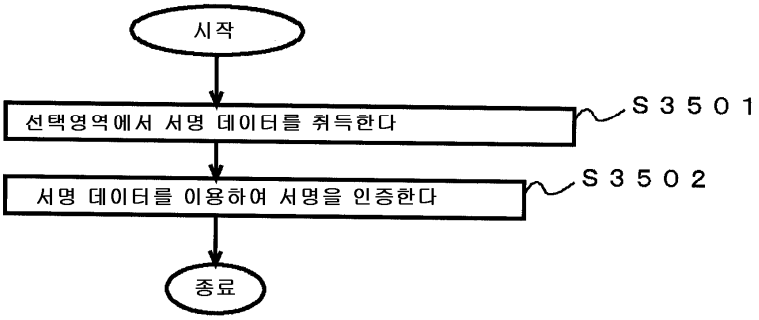
도면33


서버 어플리케이션 인증부
3305
3304
인증 성공정보 입력부
서버 TMR 억세스
라이브러리부 인증부
서버
2803
2804
어플리케이션
다운로딩부
2901
인증성공정보 생성수단
3301
인증성공정보
3302
3303
인증성공정보 출력수단
TRM 억세스 라이브러리부
단말
2801
TRM 억세스 라이브러리부 인증부
2902
TRM 억세스 라이브러리부 인증정보
TRM부
인증모듈
2805
2802

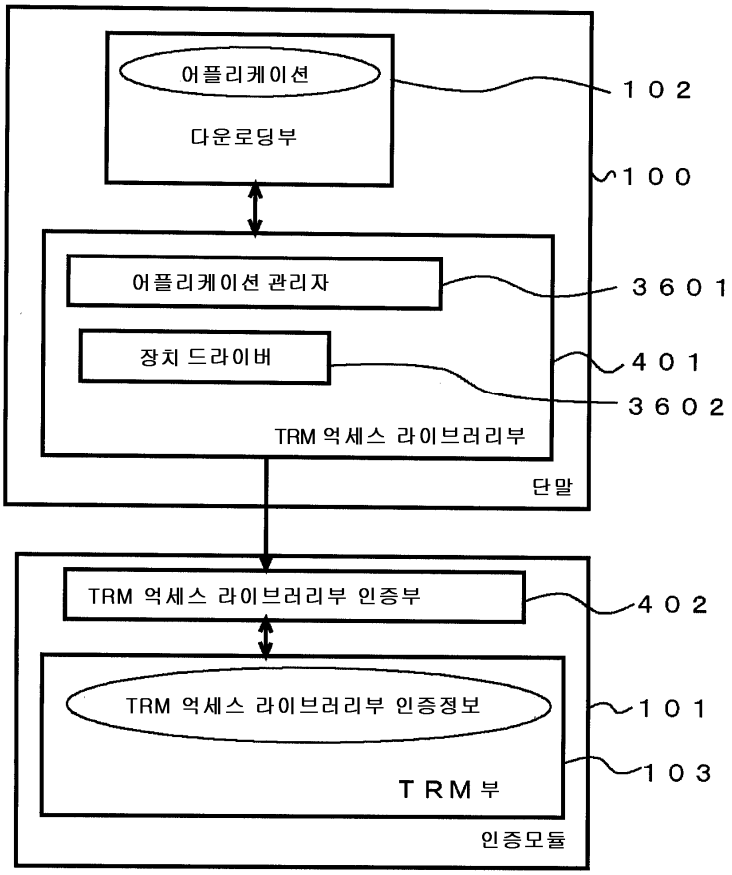
도면34


JAR 파일 (어플리케이션 본체)
3401
Java
어플리케이션
ADF 파일 (어플리케이션 정의 파일)
3402
AppName(필수키)
AppName(필수키)
AppName(필수키)
AppParam(선택키)

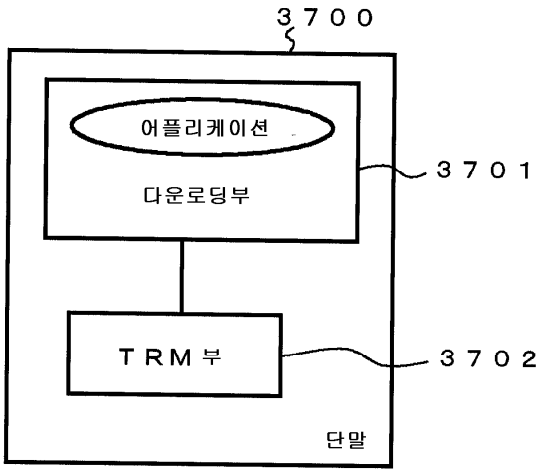
도면35


시작
선택영역에서 서명 데이터를 취득한다
S3501
서명 데이터를 이용하여 서명을 인증한다
S3502
종료

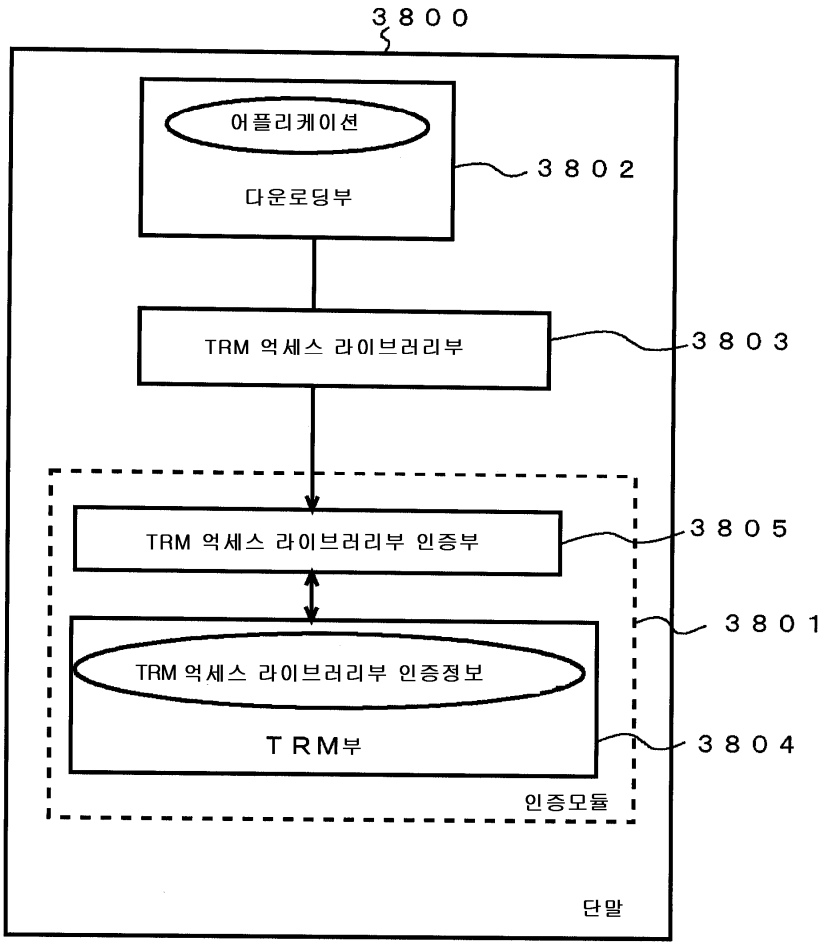
도면36


어플리케이션
다운로딩부
102
100
어플리케이션 관리자
3601
장치 드라이버
401
3602
TRM 억세스 라이브러리부
단말
TRM 억세스 라이브러리부 인증부
402
TRM 억세스 라이브러리부 인증정보
101
TRM부
103
인증모듈

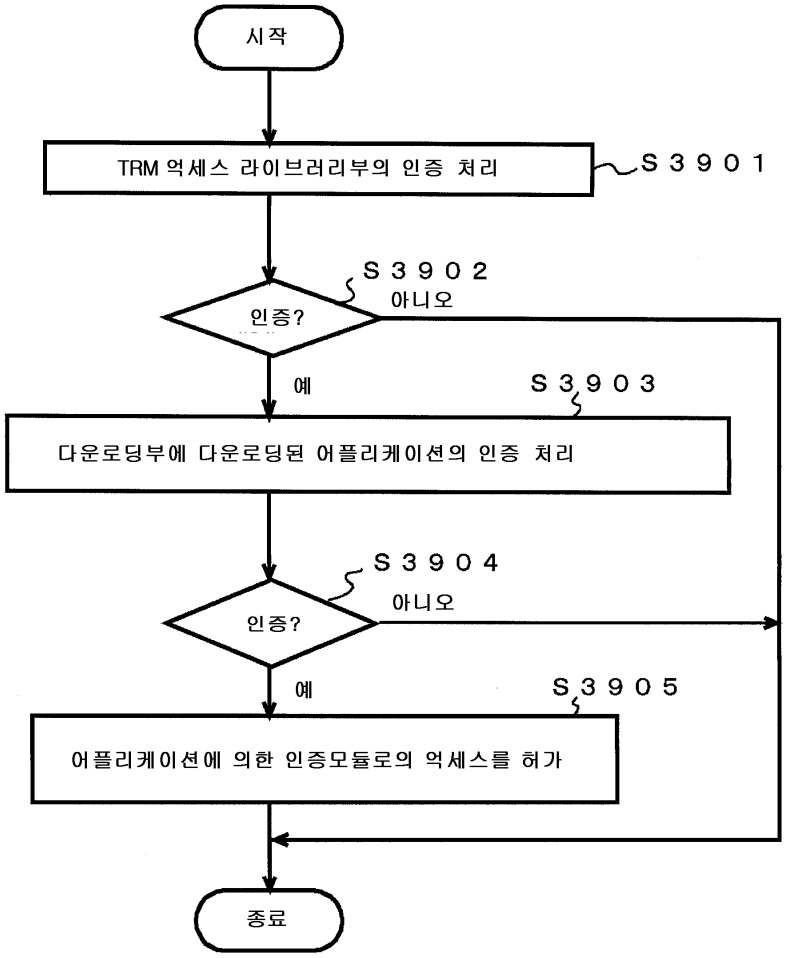
도면37


3700
어플리케이션
다운로딩부
3701
TRM부
3702
단말

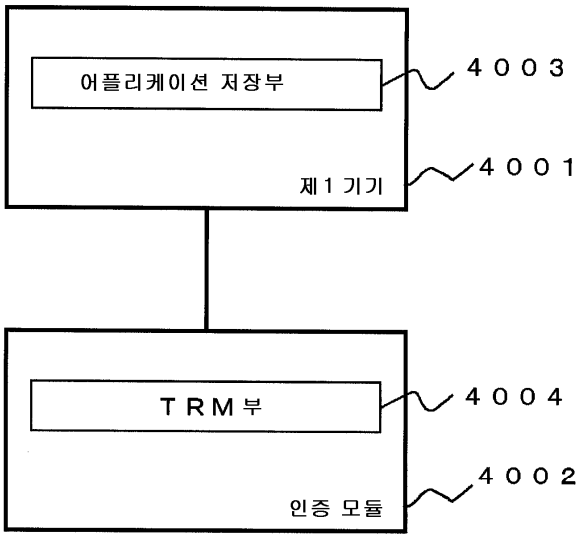
도면38


3800
어플리케이션
다운로딩부
3802
TRM 억세스 라이브러리부
3803
TRM 억세스 라이브러리부 인증부
3805
3801
TRM 억세스 라이브러리부 인증정보
TRM부
3804
인증모듈
단말

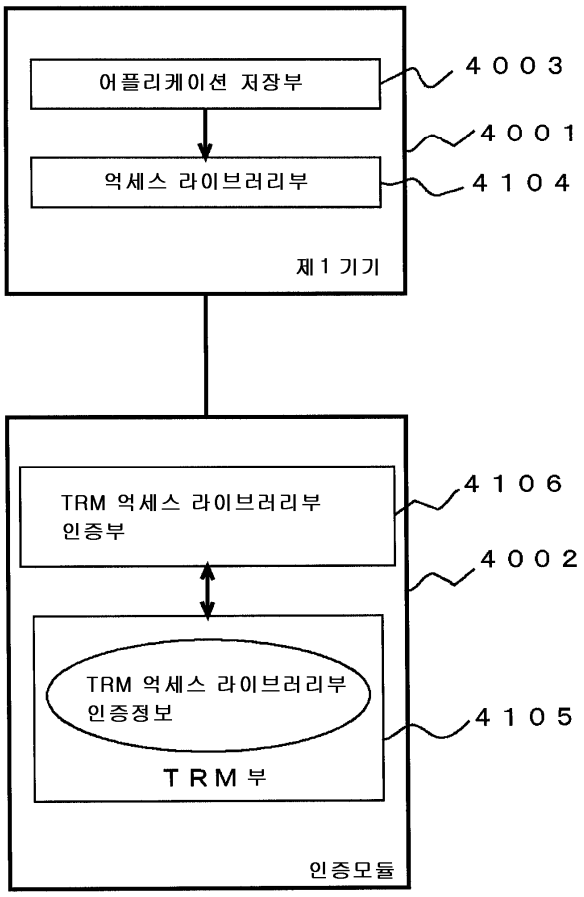
도면39


시작
TRM 억세스 라이브러리부의 인증 처리
S 3 9 0 1
S 3 9 0 2
인증?
아니오
예
S 3 9 0 3
다운로딩부에 다운로딩된 어플리케이션의 인증 처리
S 3 9 0 4
인증?
아니오
예
S 3 9 0 5
어플리케이션에 의한 인증모듈로의 억세스를 허가
종료

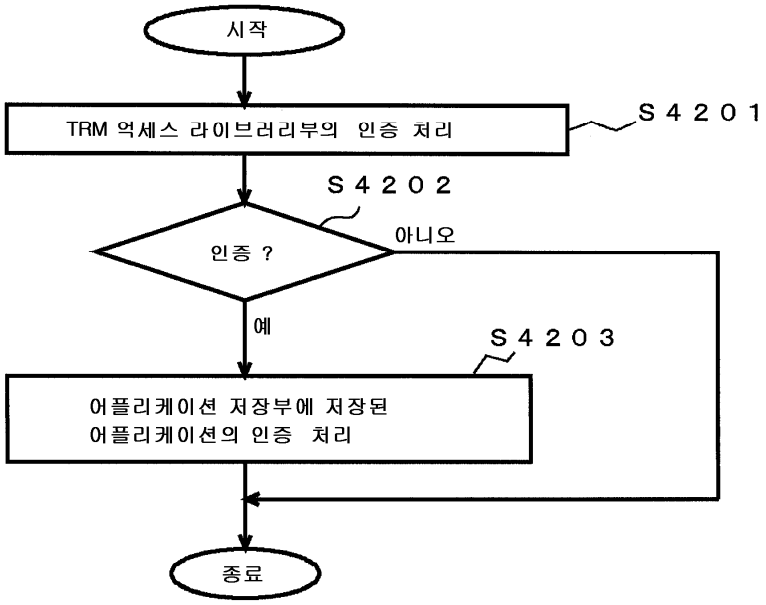
도면40


어플리케이션 저장부
4 0 0 3
제 1 기기
4 0 0 1
TRM부
4 0 0 4
인증 모듈
4 0 0 2

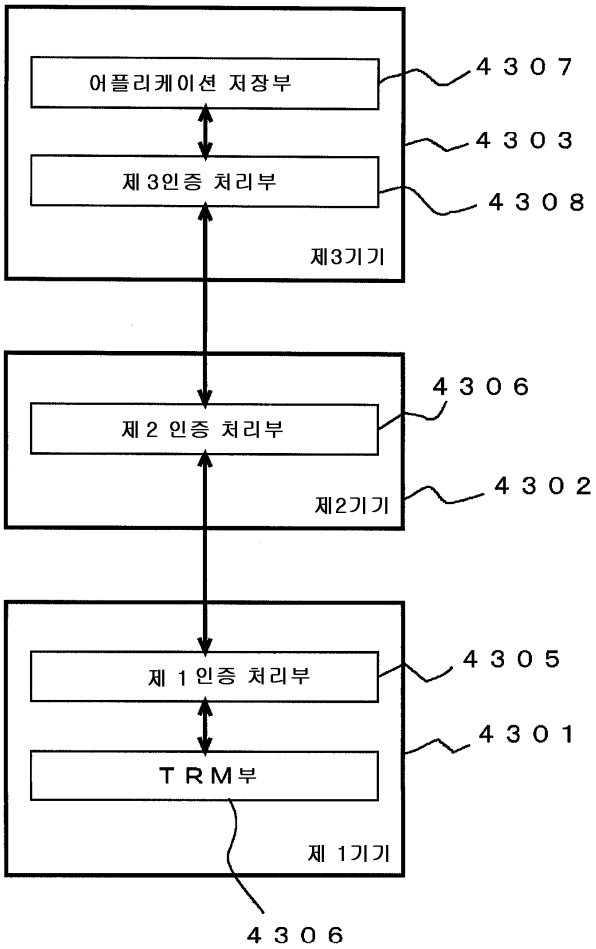
도면41


어플리케이션 저장부
4003
억세스 라이브러리부
4001
4104
제1기기
TRM 억세스 라이브러리부
인증부
4106
4002
TRM 억세스 라이브러리부
인증정보
TRM부
4105
인증모듈

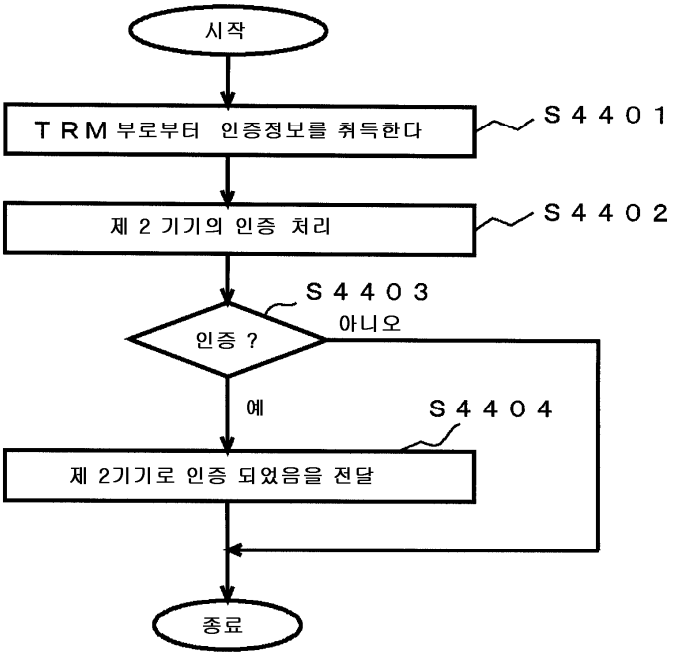
도면42


시작
TRM 억세스 라이브러리부의 인증 처리
S4201
S4202
인증 ?
아니오
예
S4203
어플리케이션 저장부에 저장된
어플리케이션의 인증 처리
종료

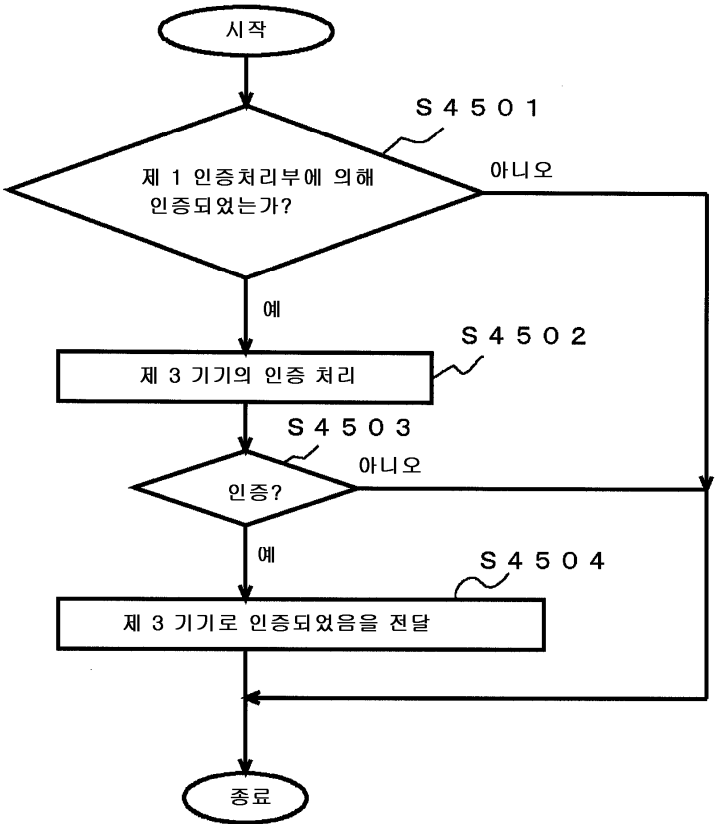
도면43


어플리케이션 저장부
4307
4303
제3인증 처리부
4308
제3기기
4306
제2 인증 처리부
4302
제2기기
4305
제 1 인증 처리부
4301
TRM부
제 1기기
4306

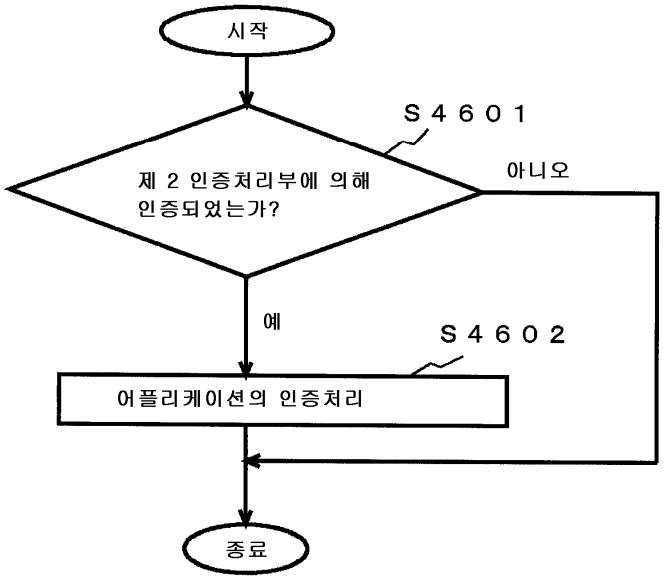
도면44


시작
TRM 부로부터 인증정보를 취득한다
S4401
제 2 기기의 인증 처리
S4402
S4403
인증 ?
아니오
예
S4404
제 2기기로 인증 되었음을 전달
종료

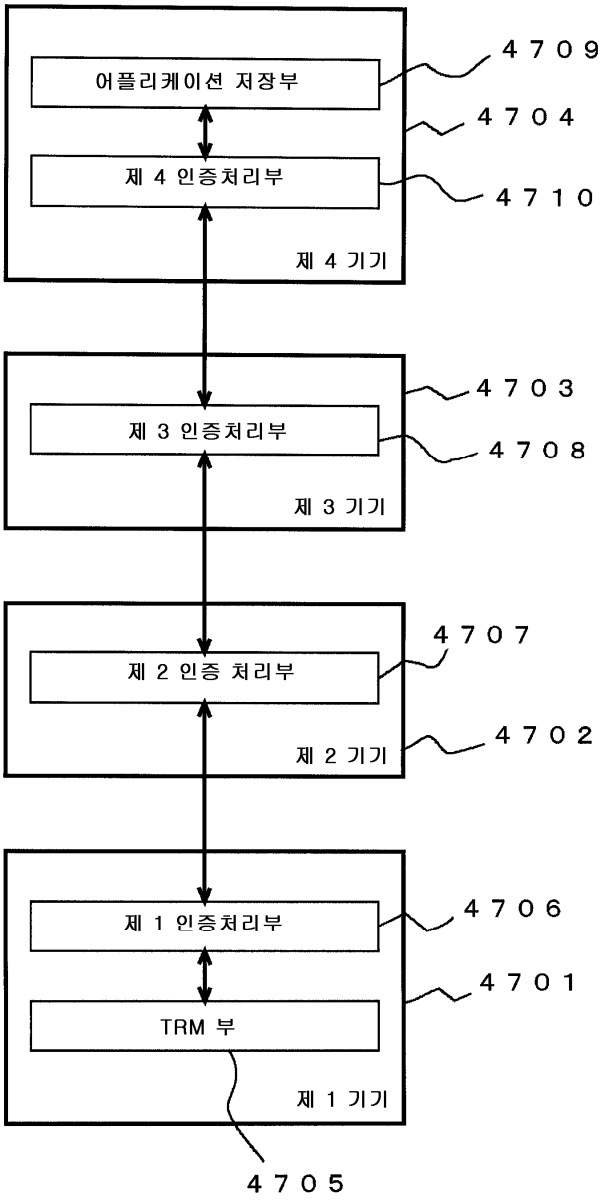
도면45


시작
S 4 5 0 1
제 1 인증처리부에 의해
인증되었는가?
아니오
예
S 4 5 0 2
제 3 기기의 인증 처리
S 4 5 0 3
인증?
아니오
예
S 4 5 0 4
제 3 기기로 인증되었음을 전달
종료

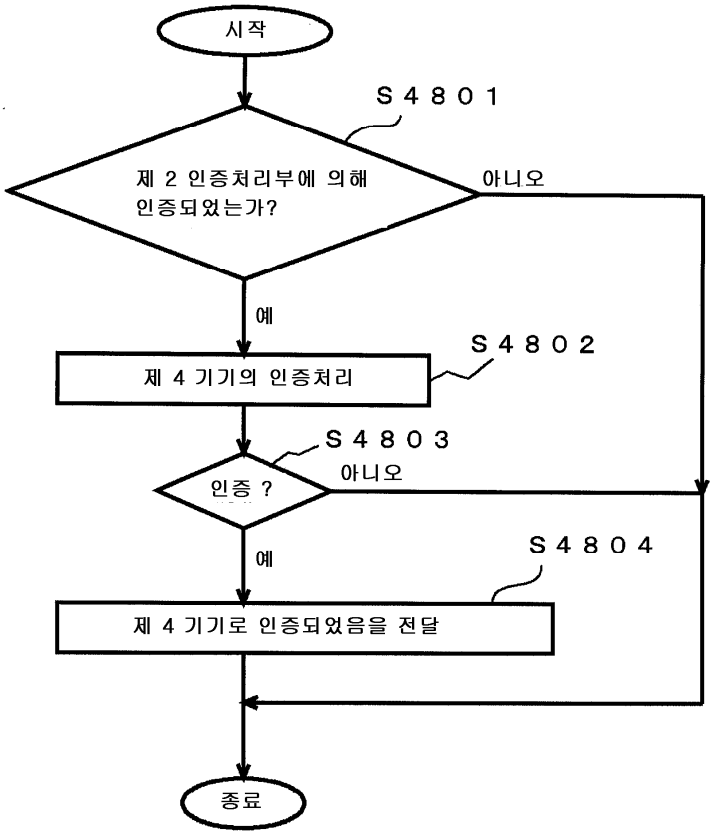
도면46


시작
S 4 6 0 1
제 2 인증처리부에 의해
인증되었는가?
아니오
예
S 4 6 0 2
어플리케이션의 인증처리
종료

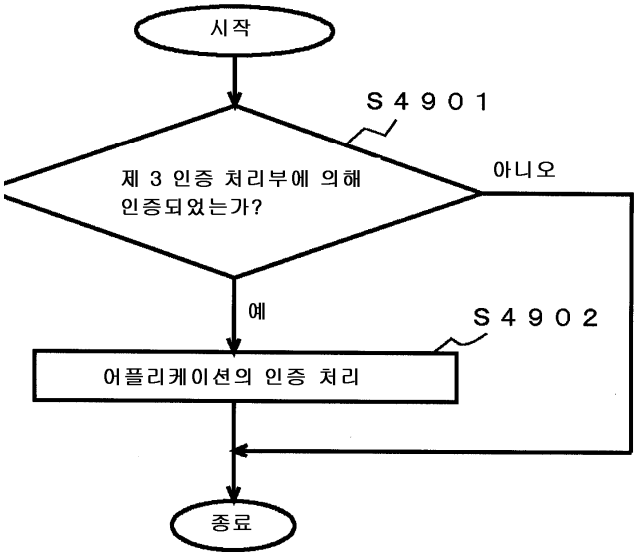
도면47


어플리케이션 저장부
4709
4704
제 4 인증처리부
4710
제 4 기기
4703
제 3 인증처리부
4708
제 3 기기
4707
제 2 인증 처리부
제 2 기기
4702
제 1 인증처리부
4706
4701
TRM 부
제 1 기기
4705

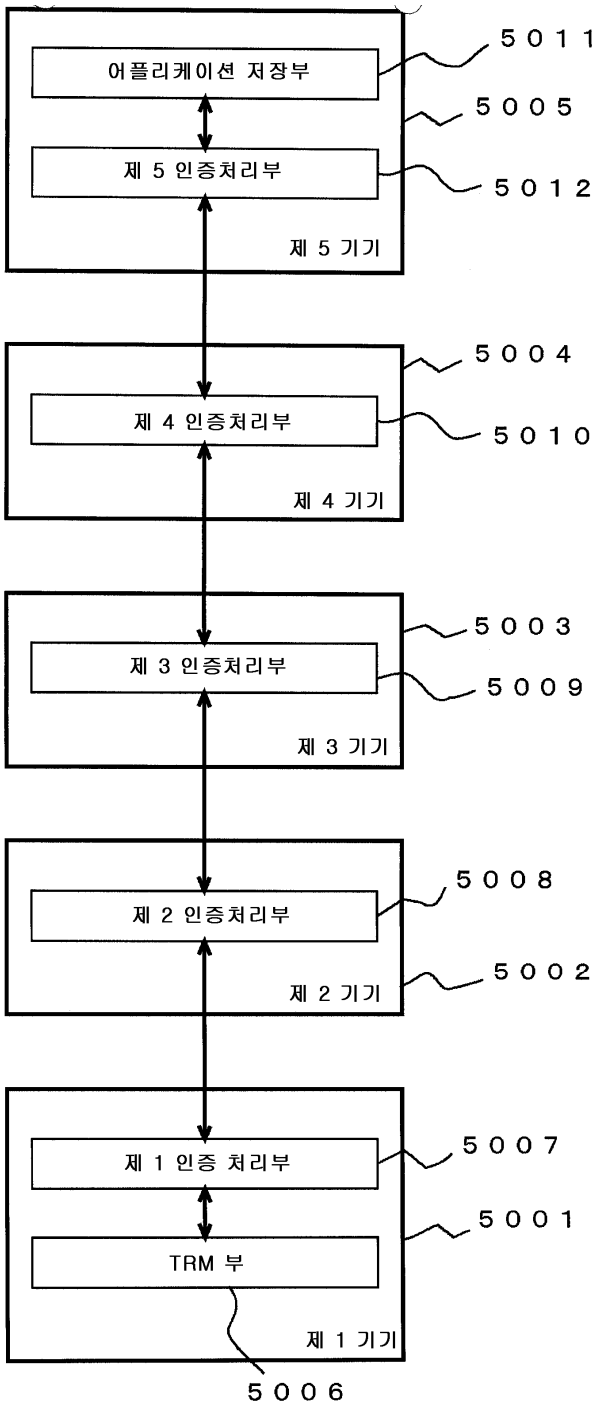
도면48


시작
S 4 8 0 1
제 2 인증처리부에 의해 인증되었는가?
아니오
예
S 4 8 0 2
제 4 기기의 인증처리
S 4 8 0 3
인증 ?
아니오
예
S 4 8 0 4
제 4 기기로 인증되었음을 전달
종료

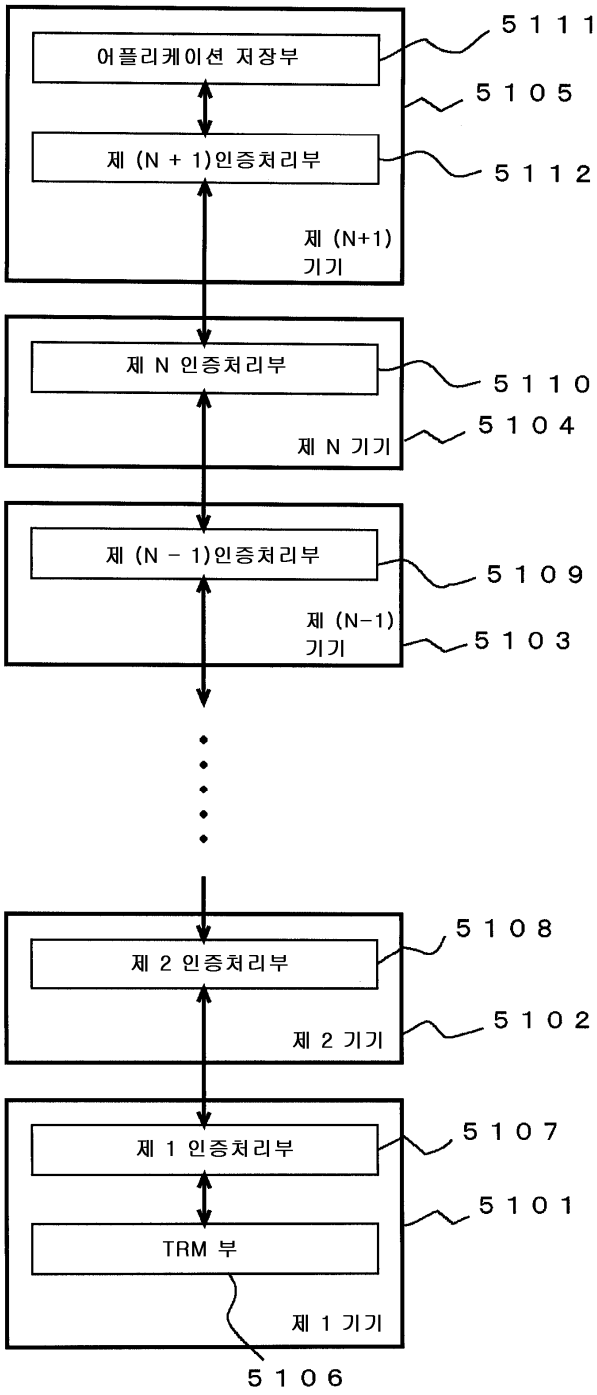
도면49


시작
S 4 9 0 1
제 3 인증 처리부에 의해 인증되었는가?
아니오
예
S 4 9 0 2
어플리케이션의 인증 처리
종료

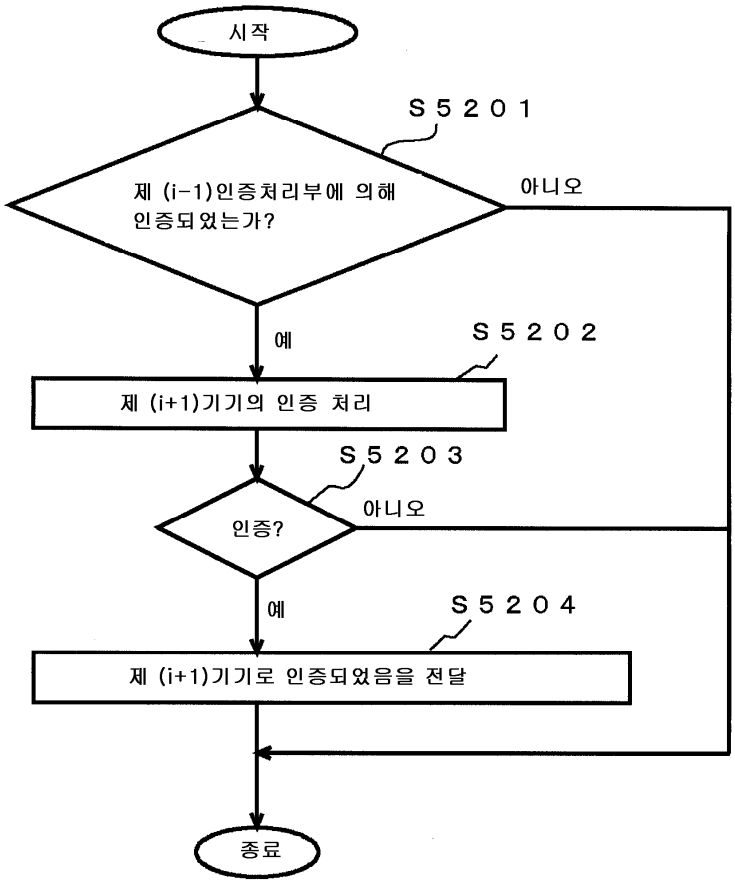
도면50


어플리케이션 저장부
5011
5005
제 5 인증처리부
5012
제 5 기기
5004
제 4 인증처리부
5010
제 4 기기
5003
제 3 인증처리부
5009
제 3 기기
5008
제 2 인증처리부
5002
제 2 기기
제 1 인증 처리부
5007
5001
TRM 부
제 1 기기
5006

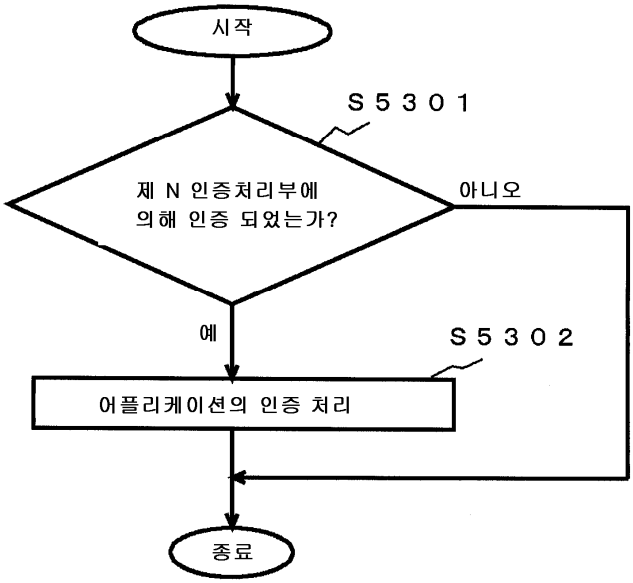
도면51


어플리케이션 저장부
제 (N + 1)인증처리부
제 (N+1) 기기
제 N 인증처리부
제 N 기기
제 (N − 1)인증처리부
제 (N−1) 기기
제 2 인증처리부
제 2 기기
제 1 인증처리부
TRM 부
제 1 기기
5111
5105
5112
5110
5104
5109
5103
5108
5102
5107
5101
5106

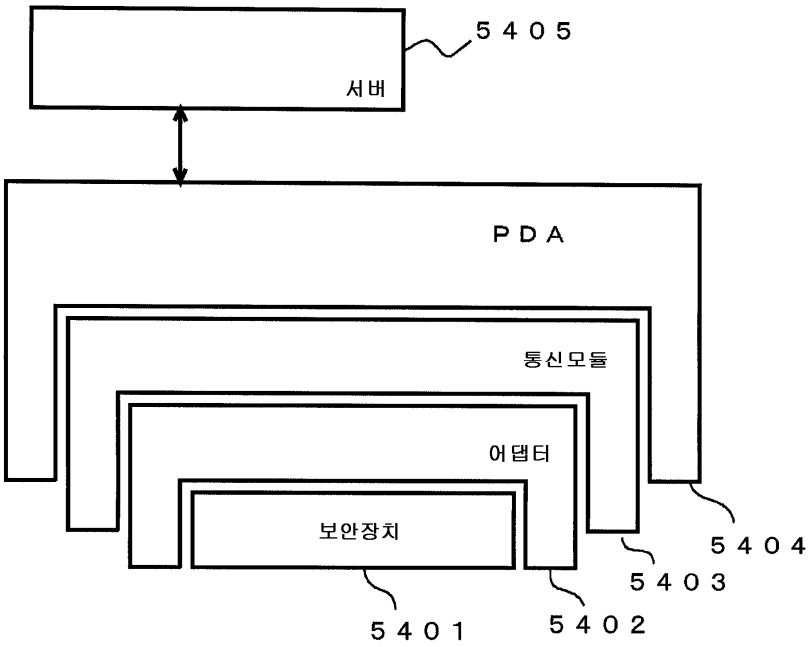
도면52


시작
S5201
제 (i-1)인증처리부에 의해 인증되었는가?
아니오
예
S5202
제 (i+1)기기의 인증 처리
S5203
인증?
아니오
예
S5204
제 (i+1)기기로 인증되었음을 전달
종료

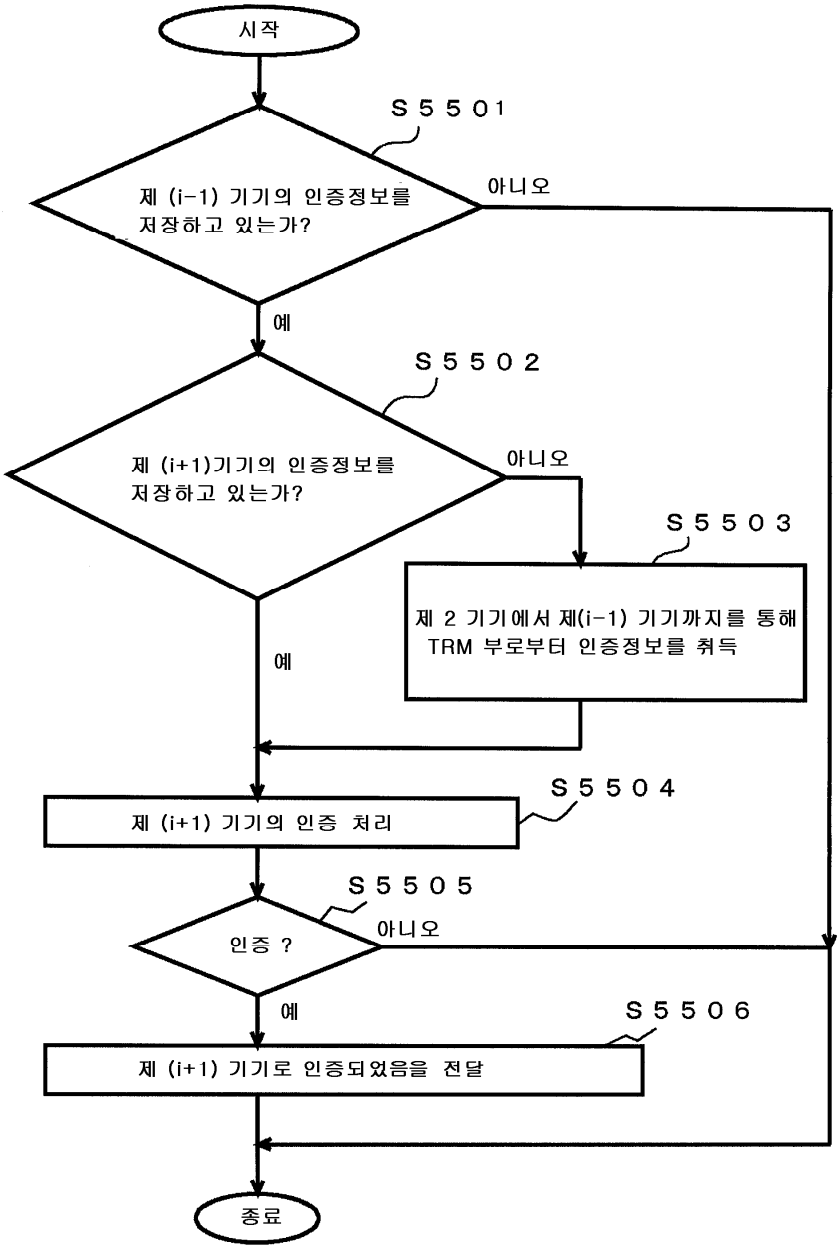
도면53


시작
S5301
제 N 인증처리부에 의해 인증 되었는가?
아니오
예
S5302
어플리케이션의 인증 처리
종료

도면54



도면55


시작
S 5 5 0 1
제 (i-1) 기기의 인증정보를 저장하고 있는가?
아니오
예
S 5 5 0 2
제 (i+1)기기의 인증정보를 저장하고 있는가?
아니오
S 5 5 0 3
제 2 기기에서 제(i-1) 기기까지를 통해 TRM 부로부터 인증정보를 취득
예
S 5 5 0 4
제 (i+1) 기기의 인증 처리
S 5 5 0 5
인증 ?
아니오
예
S 5 5 0 6
제 (i+1) 기기로 인증되었음을 전달
종료