(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년01월07일
(11) 등록번호 10-0877064
(24) 등록일자 2008년12월26일

(51) Int. Cl.
G06F 15/00 (2006.01)
(21) 출원번호 10-2006-0069357
(22) 출원일자 2006년07월24일
심사청구일자 2006년07월24일
(65) 공개번호 10-2008-0009584
(43) 공개일자 2008년01월29일
(56) 선행기술조사문헌
KR1020060074936 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 매탄동 416
(72) 발명자
장명수
서울 구로구 개봉3동 278-29호 20/1
김형식
서울 서대문구 창천동 68-19 정년 유스빌 401호
김상현
서울 성북구 동선동3가 23번지 403호
(74) 대리인
정상빈, 특허법인가산

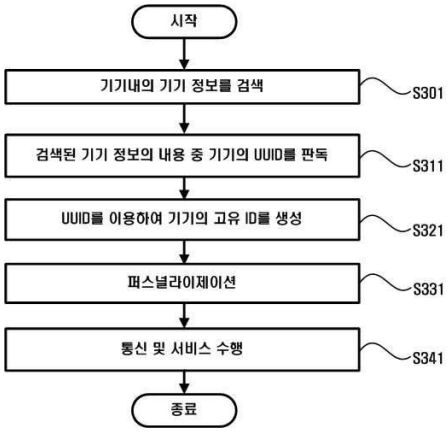
전체 청구항 수 : 총 6 항 심사관 : 천대녕

(54) 고유 ＩＤ 생성 장치 및 방법

(57) 요 약

고유 ID 생성 장치 및 방법을 제공한다. 고유 ID 생성 장치는 소정 네트워크에 참여한 소정 기기내의 UUID를 이용하여 상기 기기의 고유 ID를 생성하는 장치에 있어서, 상기 기기내의 기기 정보를 검색하는 검색부와 검색된 기기 정보의 내용 중 기기의 UUID를 판독하는 판독부 및 판독된 UUID를 이용하여 기기의 고유 ID를 생성하는 생성부를 포함한다.

대 표 도 - 도3



특허청구의 범위

청구항 1

디스커버리 서비스가 가능한 네트워크에 참여한 소정 기기내의 UUID(Universally Unique Identifier)를 이용하여 상기 기기의 고유 ID를 생성하는 장치에 있어서,

상기 기기내의 기기 정보를 검색하는 검색부;

상기 검색된 기기 정보의 내용으로부터 상기 기기의 UUID를 판독하는 판독부; 및

상기 판독된 UUID를 이용하여 상기 기기의 고유 ID를 생성하는 생성부를 포함하며,

상기 기기는 DRM 상호 운용성을 위한 NEMO(Networked Environment for Media Orchestration) 서비스 지원이 가능한 기기인, 고유 ID 생성장치.

청구항 2

삭제

청구항 3

제 1항에 있어서,

상기 네트워크는 UPnP, 블루투스(Bluetooth), JINI, 및 UDDI 중 어느 하나이고 상기 고유 ID는 상기 UUID와 동일 값으로 생성된, 고유 ID 생성장치.

청구항 4

제 3항에 있어서,

상기 네트워크가 UPnP인 경우, 상기 기기가 상기 UPnP 네트워크에 추가되면 상기 UPnP 네트워크의 컨트롤 포인트는 상기 기기로부터 상기 고유 ID와 상기 기기가 지원 가능한 서비스 목록을 제공받아 상기 기기 및 상기 기기의 제공 서비스를 인식하는, 고유 ID 생성장치.

청구항 5

삭제

청구항 6

디스커버리 서비스가 가능한 네트워크에 참여한 소정 기기내의 UUID를 이용하여 상기 기기의 고유 ID를 생성하는 방법에 있어서,

상기 기기내의 기기 정보를 검색하는 단계;

상기 검색된 기기 정보의 내용으로부터 상기 기기의 UUID(Universally Unique Identifier)를 판독하는 단계; 및

상기 판독된 UUID를 이용하여 상기 기기의 고유 ID를 생성하는 단계를 포함하며,

상기 기기는 DRM 상호 운용성을 위한 NEMO(Networked Environment for Media Orchestration) 서비스 지원이 가능한 기기인, 고유 ID 생성방법.

청구항 7

삭제

청구항 8

제 6항에 있어서,

상기 네트워크는 UPnP, 블루투스(Bluetooth), JINI, 및 UDDI 중 어느 하나이고 상기 고유 ID는 상기 UUID와 동

일 값으로 생성된, 고유 ID 생성방법.

청구항 9

제 8항에 있어서,

상기 네트워크가 UPnP인 경우, 상기 기기가 상기 UPnP 네트워크에 추가되면 상기 UPnP 네트워크의 컨트롤 포인트가 상기 기기로부터 상기 고유 ID와 상기 기기가 지원 가능한 서비스 목록을 제공받아 상기 기기 및 상기 기기의 제공 서비스를 인식하는 단계를 더 포함하는, 고유 ID 생성방법.

청구항 10

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<12> 본 발명은 고유 ID 생성 장치 및 방법에 관한 것으로서, 더욱 상세하게는 고유 ID를 이용하여 특정 서비스를 지원하는 기기를 기존의 네트워크 인프라의 통신 환경에 접목시켜 기기간 통신 및 컨텐츠 서비스를 제공하는 고유 ID 생성 장치 및 방법에 관한 것이다.

<13> DRM(Digital Rights Management)은 인터넷을 통해 디지털 음악 및 동영상, e-Book 등 유료 컨텐츠의 불법복제 방지를 목적으로 사용되었으나, 최근 모바일과 기업문서 보안, 그리고 디지털 방송과 디지털 홈 엔터테인먼트 등 다양한 분야에서 사용되고 있다.

<14> DRM이 도입되어야 하는 이유는 디지털 데이터가 갖는 여러가지 특성으로부터 도출할 수 있다. 디지털 데이터는 아날로그 데이터와는 달리 손실이 없이 복제가 가능하다는 특성과, 재사용 및 가공이 용이한 특성과, 쉽게 제3자에게 배포할 수 있다는 특성을 가지고 있으며, 매우 적은 비용으로 이러한 복제와 배포를 손쉽게 할 수 있다는 특성을 가지고 있다. 그에 반해 디지털 컨텐츠는 그 제작에 많은 비용과 노력 및 시간을 필요로 한다. 따라서 디지털 컨텐츠의 무단 복제 및 배포가 용인될 경우에, 이는 디지털 컨텐츠 제작자의 이익을 침해하게 되고 디지털 컨텐츠 제작자의 창작 의욕은 꺾이게 될 것이고 이는 디지털 컨텐츠 산업의 활성화에 큰 저해요소가 된다.

<15> 디지털 컨텐츠를 보호하고자 하는 노력은 과거에도 있었으나, 과거에는 주로 디지털 컨텐츠 무단접근 방지에 중점을 두고 있었다. 다시 말하면, 디지털 컨텐츠에 대한 접근(access)은 대가를 지불한 일부 사람에게만 허용되었다. 따라서 대가를 지불한 사람은 암호화되지 않은 디지털 컨텐츠에 접근할 수 있으며, 그렇지 않은 사람은 디지털 컨텐츠에 접근할 수 없었다. 그렇지만 대가를 지불한 사람이 접근한 디지털 컨텐츠를 고의적으로 제3자에게 배포할 경우에 제3자는 대가를 지불하지 않고도 디지털 컨텐츠를 사용할 수 있게 된다. 이러한 문제점을 해결하고자 DRM이라는 개념이 도입되었다.

<16> DRM은 어떤 암호화된 디지털 컨텐츠에 대한 접근은 누구에게나 무제한으로 허용하고 있으나, 암호화된 디지털 컨텐츠를 복호화하여 재생시키려면 권리객체(Rights Object)라는 라이센스를 필요하도록 하고 있다. 여기서 권리객체란 디지털 컨텐츠를 복호화하는 복호키, 디지털 컨텐츠를 사용하는 형태를 정의하는 사용허가 정보, 디지털 컨텐츠의 사용을 제한하는 사용제한 정보를 가지거나 디지털 컨텐츠를 사용시 할당된 권리의 종류를 포함하는 정보를 가지는 멀티미디어 디지털 컨텐츠 저작권을 의미한다. 따라서, DRM을 적용하면 디지털 컨텐츠를 기존과는 달리 효과적으로 보호할 수 있게 된다.

<17> 하지만, 최근 디지털 컨텐츠의 불법복제방지 및 저작권 보호를 위해 DRM 벤더(vendor)들이 독자적인 기술 규격을 사용하여 다양한 DRM 제품들을 출시하고 있으며, 이에 따라 DRM 기술간 상호 운용성(interoperability)이 보장되지 않고 있다. 즉, 각각의 DRM 벤더들이 DRM 구현에 있어서 다른 파일 포맷(formats), 코덱(codecs), 독자적인 컨텐츠 보호 방법(proprietary content-protection) 또는 이들의 조합(combinations)을 지원하고 있어서, 사용자가 온라인 스토어(online store)에서 구입한 디지털 컨텐츠를 자신의 플레이어(player)나 멀티플 플레이

어(multiple players)에서 플레이하는 데 있어서 제한이 따르고 있다.

<18> 이러한 DRM의 상호 운용성 보장을 위해 CORAL, MPEG-21, OMA(Open Mobile Alliance), DMP(Digital Media Project) 등 많은 국제 표준 단체에서 DRM 표준 기술을 개발하고 있다. 예를 들어 OMA는 Phase 1(candidate)단계의 OMA DRM v1.0을 발표하였으며, 이어서 OMA DRM v2.0 표준을 발표한 바 있으며, MPEG-21은 범용적으로 사용될 수 있는 DRM 프레임워크(framework)의 표준 기술을 개발하였다.

<19> 또한, CORAL은 사용자가 보호된 DRM 컨텐츠(DRM-protected content)를 언제 어디서나 사용할 수 있도록 DRM 기술간의 상호 운용성을 위해 NEMO 기술을 주장한 바 있다. NEMO(Networked Environment for Media Orchestration) 기술은 서비스 지향 아키텍쳐(service-oriented architecture)로써, DRM 시스템간 상호 운용성이 가능하도록 하여 사용자가 컨텐츠에 대한 권리(Rights)를 정당하게(legitimately) 갖고 있는 한 자신의 기기가 무엇인지에 상관없이 컨텐츠를 사용할 수 있도록 한다. 즉, NEMO 기술은 광범위한 DRM과 관련된 기기, 포맷, 네트워크 및 서비스 타입간의 상호 운용성을 목표로 하고 있다.

<20> 한편 소정의 유선 또는 무선 기기가 DRM 컨텐츠를 이용하고자 시도하면, 먼저 상기 기기는 퍼스널라이즈(personalized)되어야 하며, 퍼스널라이즈된 기기는 자신의 고유 ID와 인증서를 포함한 퍼스널러티(personality) 정보를 얻게 된다. 이러한 과정을 퍼스널라이제이션(personalization)이라 하며, 상기 과정을 거친 기기들은 합법적인 기기로 인정되어 상호간 통신 및 DRM 컨텐츠를 기기의 종류에 상관없이 이용할 수 있게 된다.

<21> 도 1은 종래 NEMO 퍼스널라이제이션 과정을 도시한다.

<22> 도 1에서는 DRM 상호 운용성을 위한 서비스 프레임워크를 기반으로 동작하는 NEMO-enabled 기기(3)와 외부 인증기관(5)간의 퍼스널라이제이션 과정을 예로 들어 설명하기로 한다.

<23> NEMO 서비스를 지원이 가능한 NEMO-enabled 기기(3)(제1 기기)가 외부의 인증기관(Certificate Authority)으로 퍼스널라이제이션을 요청한다(S2). 이때, NEMO-enabled 기기(3)와 인증기관은 비밀을 서로 공유(shared secret)하며, 상기 공유된 비밀 정보는 NEMO-enabled 기기(3)가 퍼스널라이제이션 요청시 인증기관이 NEMO-enabled 기기(3)가 정당한 자격을 갖추었는 지 판단하는 데에 사용될 수 있다. 그리고, 상기 NEMO-enabled 기기(3)가 전송한 퍼스널라이제이션 요청 메시지는 NEMO-enabled 기기(3)의 아이덴터티(identity)(ID)와 관련된 정보를 포함할 수 있으며, 상기 정보는 페이로드 데이터(payload data)에 포함될 수 있다. 또한 상기 페이로드 데이터에는 퍼스널라이제이션의 타입(예를 들어 Personalization type=NEMO)을 비롯한 인증 기관(5)과 무결성과 기밀성이 보장되는 통신을 하기 위한 비밀 키들에 관한 정보들을 포함할 수 있다.

<24> 인증기관은 상기 NEMO-enabled 기기(3)의 요청이 적법한 것인지 검증하고, 페이로드 데이터를 처리한다(S4). 이때, 인증기관은 NEMO-enabled 기기(3)와 공유하고 있는 비밀 값으로 NEMO-enabled 기기(3)의 요청이 적법한지 검증할 수 있다.

<25> 다음 단계에서 인증 기관(5)은 상기 NEMO-enabled 기기(3)에 부여될 NEMO ID 정보를 포함하는 퍼스널러티(personality) 정보를 생성하고, 응답 메시지로 NEMO-enabled 기기(3)에게 전송한다(S6, S8). 보다 더 구체적으로 상기 퍼스널러티 정보에는, NEMO ID외에도 공개키를 포함하고 있는 인증서, 개인 키들, 핑거프린트(fingerprint)에 관련된 정보들을 포함할 수 있다. 그리고 상기 인증서는 NEMO ID(즉 NEMO-enabled 디바이스의 ID) 및 공개키를 이용하여 생성될 수 있으며, 상기 정보들은 페이로드 데이터에 포함되어 NEMO-enabled 기기(3)로 전송된다.

<26> 다음 단계에서 NEMO-enabled 기기(3)는 수신한 응답 메시지 내의 인증서를 검증하고, 퍼스널러티 정보를 획득한다(S10, S12).

<27> 이후, 상기 NEMO-enabled 기기는 다른 NEMO-enabled 기기와 통신이 가능하며, 또한 DRM 컨텐츠를 기기의 모델에 상관없이 이용할 수 있다.

<28> 그러나 NEMO 네트워크에 있어서, NEMO-enabled 기기간 통신을 수행하기 위해서 실질적으로 어떤 네트워크 인프라를 사용할 것인지에 대한 기술이 부재한 상황이다.

발명이 이루고자 하는 기술적 과제

<29> 본 발명은 고유 ID 생성 장치 및 방법을 제공하여 특정 서비스를 지원하는 기기를 기존의 네트워크 인프라의 통신 환경에 접목시켜 기기간 통신 및 컨텐츠 서비스를 제공할 수 있도록 하는 데 그 목적이 있다.

<30> 본 발명의 목적들은 이상에서 언급한 목적들로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해되어질 수 있을 것이다.

발명의 구성 및 작용

<31> 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 고유 ID 생성 장치는 소정 네트워크에 참여한 소정 기기내의 UUID를 이용하여 상기 기기의 고유 ID를 생성하는 장치에 있어서, 상기 기기내의 기기 정보를 검색하는 검색부와 검색된 기기 정보의 내용 중 기기의 UUID(Universally Unique Identifier)를 판독하는 판독부 및 판독된 UUID를 이용하여 기기의 고유 ID를 생성하는 생성부를 포함한다.

<32> 본 발명의 실시예에 따른 고유 ID 생성방법은 소정 네트워크에 참여한 소정 기기내의 UUID를 이용하여 기기의 고유 ID를 생성하는 방법에 있어서, 기기내의 기기 정보를 검색하는 단계와 검색된 기기 정보의 내용 중 기기의 UUID를 판독하는 단계 및 판독된 UUID를 이용하여 기기의 고유 ID를 생성하는 단계를 포함한다.

<33> 기타 실시예들의 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

<34> 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

<35> 이하 본 발명의 실시예들은 종래 네트워크 인프라(infra) 중 UPnP 네트워크를 기반으로 주로 설명할 것이지만, 상기 UPnP 네트워크외에 디스커버리 서비스(discovery service)가 가능한 블루투스(Bluetooth), JINI(Java Intelligent Network Infra-structure), UDDI(Universal Description, Discovery, and Integration) 등의 네트워크를 기반으로 적용가능하다.

<36> 또한, NEMO-enabled 기기를 예로 들어 주로 설명할 것이지만, 상기 NEMO-enabled 기기외에 기존의 네트워크 인프라를 활용하여 통신 및 기타 서비스를 제공하고자 하는 기기들에게도 적용가능함은 물론이다.

<37> 도 2는 본 발명의 일 실시예에 따른 고유 ID 생성장치의 블록도이다.

<38> 고유 ID 생성장치(200)는 검색부(210), 판독부(220), 생성부(230), 인증 요청부(240) 및 송수신부(250)를 포함한다.

<39> 검색부(210)는 소정 네트워크에 참여한 소정 기기내에 포함된 본 발명의 장치(200)내의 구성요소로서 상기 기기내의 기기 정보를 검색한다. 상기 기기 정보는 예를 들어 기기내의 설명서(device description document)로서, 해당 기기 공급 업체의 고유의 제조 정보 즉, UUID(Universally Unique Identifier), 모델명, 일련번호, 제조업체 이름, 제조업체 URL 등을 포함할 수 있다. 또한, 기기 정보는 제어, 이벤트 및 프리젠테이션을 위한 URL 뿐만 아니라 많은 내장된 기기 및 서비스에 관한 목록도 포함할 수 있다.

<40> 판독부(220)는 상기 검색된 기기 정보의 내용 중 상기 기기의 UUID(Universally Unique Identifier)를 판독한다. 일반적으로 기기 정보는 XML로 표현되어 있으며, 판독부(220)는 해당 XML 문서를 파싱(parsing)하여 UUID를 검출할 수 있다.

<41> 생성부(230)는 상기 판독된 UUID를 이용하여 상기 기기의 고유 ID를 생성한다. 이때, 바람직하게는 UUID와 동일한 값으로 고유 ID를 생성할 수 있다.

<42> 인증 요청부(240)는 상기 생성된 고유 ID를 인증 기관으로 전송하여 상기 기기가 상기 고유 ID를 자신의 식별 정보로 사용할 것에 대한 인증을 요청한다. 예를 들어 NEMO-enabled 기기는 상기 생성된 고유 ID를 인증 기관으로 전송하여 상기 NEMO-enabled 기기가 상기 고유 ID를 자신의 NEMO ID로 사용할 것에 대한 인증을 요청하고, 기존의 퍼스널라이제이션 과정을 거쳐 NEMO-enabled 기기간 서로 통신을 수행할 수 있도록 할 수 있다. 보다 구체적인 설명은 이하 도 4를 참조하기 바란다.

<43> 송수신부(250)는 상기 퍼스널라이제이션 과정에서 송수신되는 데이터 및 네트워크상의 기기간의 각종 데이터를 송수신한다.

<44> 도 2에서 도시된 각각의 구성요소는 일종의 '모듈'로 구성될 수 있다. 상기 '모듈'은 소프트웨어 또는 Field Programmable Gate Array(FPGA) 또는 주문형 반도체(Application Specific Integrated Circuit, ASIC)과 같은

하드웨어 구성요소를 의미하며, 모듈은 어떤 역할들을 수행한다. 그렇지만 모듈은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. 모듈은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 실행시키도록 구성될 수도 있다. 따라서, 일 예로서 모듈은 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들, 및 변수들을 포함한다. 구성요소들과 모듈들에서 제공되는 기능은 더 작은 수의 구성요소들 및 모듈들로 결합되거나 추가적인 구성요소들과 모듈들로 더 분리될 수 있다.

<45> 도 3은 상기 도 2를 이용하여 고유 ID를 생성하는 순서도이다.

<46> 상기 도 2에서 상술된 중복된 내용은 되도록 생략하며, 고유 ID를 생성하는 과정을 각 단계별로 설명하기로 한다.

<47> 검색부(210)는 소정 네트워크에 참여한 소정 기기내에 포함된 본 발명의 장치(200)내의 구성요소로서 상기 기기내의 기기 정보를 검색한다(S301).

<48> 판독부(220)는 상기 검색된 기기 정보의 내용 중 상기 기기의 UUID(Universally Unique Identifier)를 판독한다(S311).

<49> 생성부(230)는 상기 판독된 UUID를 이용하여 상기 기기의 고유 ID를 생성한다(S321). 이때, 바람직하게는 UUID와 동일한 값으로 고유 ID를 생성한다.

<50> 인증 요청부(240)는 상기 생성된 고유 ID를 인증 기관으로 전송하여 상기 기기가 상기 고유 ID를 자신의 식별 정보로 사용할 것에 대한 인증을 요청한다(S331). 이를 통해 퍼스널라이제이션 과정을 거치게 되며, 이후 기기간 통신을 수행할 수 있게 된다. 퍼스널라이제이션 과정에 대한 구체적인 각 단계들은 이하 도 4를 참조하기 바란다.

<51> 이후, NEMO-enabled 기기의 경우, 퍼스널라이제이션 과정을 거쳐 획득한 자신의 고유 ID와 인증서를 포함한 퍼스널러티(personality) 정보를 이용하여 다른 NEMO-enabled 기기와 통신을 수행할 수 있게 된다(S341). 즉, NEMO-enabled 기기(제1 기기와 제2기기)간 서로 통신을 수행하는 과정에서, 제1 기기가 제2 기기에게 메시지를 암호화해서 보낸다고 할 때, 먼저 제1 기기는 제2 기기에게 공개키를 요청하고, 제2 기기로부터 수신한 공개키를 이용하여 제2 기기에게 메시지를 암호화해서 전송한다. 상기 제2 기기는 제1 기기로부터 수신한 메시지를 자신의 개인키를 이용하여 복호화하여 확인하게 된다. 이와 같이 DRM-enabled 디바이스간 메시지의 기밀성(confidentiality), 무결성(integrity), 신뢰성(authentication)을 보장한 통신을 수행할 수 있게 되고, MEMO ID 정보를 가진 디바이스는 DRM 컨텐츠에 접근하여 이용할 수 있게 된다. 그리고, 상기 고유 ID를 이용하여 후술될 UPnP를 비롯한 디스커버리 기능이 있는 네트워크 인프라를 기반으로 NEMO-enabled 기기간 통신 및 다양한 서비스를 제공할 수 있다.

<52> 도 4는 본 발명의 일 실시예에 따른 퍼스널라이제이션 과정(S331)을 도시한다.

<53> 상기 도 1에서 상술된 중복된 내용은 되도록 생략하며, 상기 도 2의 고유 ID 생성 장치를 이용하여 생성된 고유 ID를 가진 기기가 인증 기관과 퍼스널라이제이션 과정을 거치는 단계를 간략히 설명하기로 한다. 또한 이하의 각 단계들은 NEMO 퍼스널라이제이션 과정을 예로 들어 설명하기로 하며, NEMO 퍼스널라이제이션 과정에 관한 보다 상세한 내용은 'NEMO Personalization Service' 스펙을 참조하기 바란다.

<54> 먼저, 인증 요청부(240)는 생성부(230)가 생성한 고유 ID를 인증 기관으로 전송하여 상기 고유 ID를 해당 기기(NEMO-enabled 기기)의 식별 정보로 사용할 것에 대한 인증을 요청한다(S401). 이때, NEMO-enabled 기기와 인증기관은 비밀 정보을 서로 공유(shared secret)하며, 상기 공유된 비밀 정보는 NEMO-enabled 기기가 퍼스널라이제이션 요청시 인증기관이 NEMO-enabled 기기가 정당한 자격을 갖추었는 지 판단하는 데에 사용될 수 있다.

<55> 인증기관은 NEMO-enabled 기기와 공유하고 있는 비밀 값으로 NEMO-enabled가 적법한지 검증하고, 상기 수신한 고유 ID 정보를 포함하는 퍼스널러티(personality) 정보를 생성하고, 응답 메시지로 NEMO-enabled 기기에게 전송한다(S411, S421). 보다 더 구체적으로 상기 퍼스널러티 정보에는, 고유 ID외에도 공개키를 포함하고 있는 인증서, 개인 키들, 핑거프린트(fingerprint)에 관련된 정보들을 포함할 수 있다. 그리고 상기 인증서는 고유 ID 및 공개키를 이용하여 생성될 수 있다.

<56> NEMO-enabled 기기는 수신한 응답 메시지 내의 인증서를 검증하고, 또한 응답 메시지내의 퍼스널러티 정보를 획

득한다(S431).

<57> 이하 도 5 및 도 6에서 상기 생성된 고유 ID를 이용한 다양한 활용예를 설명하기로 한다.

<58> 도 5는 본 발명의 일 실시예에 따른 컨트롤 포인트와 피제어 기기간에 수행되는 UPnP 동작을 도시한다.

<59> UPnP 네트워크 상에 NEMO 서비스를 지원하는 NEMO-enabled 기기가 참여하면, 상기 도 3의 단계(S301 내지 S321)를 거쳐 고유 ID를 생성하고, 상기 도 4에서 상술된 바와 같이 생성된 고유 ID를 이용하여 인증 기관으로부터 퍼스널러티(personality) 정보를 얻게 된다. 퍼스널러티 정보에는 고유 ID, 공개키를 포함한 인증서, 개인키 들에 대한 정보들을 포함할 수 있다. 이하, UPnP에서 구현된 통신 방법을 이용한 NEMO-enabled 기기간 통신 수행 및 컨텐츠 이용에 대해서 보다 구체적으로 후술하기로 한다.

<60> 도시된 바와 같이, 컨트롤 포인트(510)과 피제어 기기(520)간에 수행되는 UPnP 동작을 나타낸다. 피제어 기기(520)는 예를 들어 NEMO-enabled 기기이고, 퍼스널러티(personality) 정보를 갖고 있다고 가정한다.

<61> UPnP 네트워크의 기반은 TCP/IP 프로토콜이며 이 프로토콜의 핵심은 주소 지정 기능이다. 각 피제어 기기(520)는 DHCP (동적 호스트 구성 프로토콜) 클라이언트를 가지고 있어야 하며, 피제어 기기(520)가 맨 처음 네트워크에 연결되면 DHCP 서버를 검색한다.

<62> 만약 DHCP 서버가 있으면 해당 피제어 기기(520)는 할당된 IP 주소를 사용하게 되고, 사용 가능한 DHCP 서버가 없는 경우에는 피제어 기기(520)는 주소를 확보하기 위하여 '자동 IP' (Auto IP)를 사용하게 된다(S511).

<63> 다음으로, UPnP의 디스커버리(Discovery) 단계를 거치게 되는데, 일단 피제어 기기(520)가 네트워크에 연결되고 적절한 주소가 지정되면 검색 작업이 진행될 수 있다(S521). 검색 작업은 SSDP(Simple Service Discovery Protocol)을 이용하여 처리한다. 피제어 기기(520)가 네트워크에 추가되면 SSDP는 피제어 기기(520)가 제공하는 서비스를 네트워크 상에 있는 컨트롤 포인트(510)에 알리는 역할을 한다.

<64> UPnP 네트워킹의 다음 단계는 디스크립션(Description) 단계이다(S531). 컨트롤 포인트(510)가 피제어 기기(520)를 검색하기는 했지만, 컨트롤 포인트(510)는 여전히 피제어 기기(520)에 대하여 알고 있는 정보가 아주 적다. 이 컨트롤 포인트(510)가 피제어 기기(520) 및 피제어 기기(520)의 기능에 대한 정보를 자세하게 파악하여 상호작용을 하려면, 컨트롤 포인트(510)는 검색 메시지와 해당되는 피제어 기기(520)가 제공하는 URL로부터 피제어 기기(520)의 기기 정보를 확인해야 한다. 본 실시예에서 피제어 기기(520)는 본 발명의 장치(200)를 통해 생성된 고유 ID를 포함한 기타 디바이스 정보들을 컨트롤 포인트(510)에게 알려줄 수 있다. 상기 디바이스 정보들에는 피제어 기기(520)가 제공하는 NEMO 서비스에 관한 목록을 포함할 수 있다. 즉, 고유 ID와 NEMO 서비스에 관한 목록이 묶여져 있고, 고유 ID가 UUID와 동일한 값으로 생성된 경우, 컨트롤 포인트(510)는 상기 단계(S521, S531)에서 하나의 값으로 기기 인식 및 해당 기기가 제공하는 서비스를 파악할 수 있게 된다.

<65> 컨트롤 포인트(510)는 피제어 기기(520)가 제공한 정보들을 통해 NEMO 서비스를 지원하는 NEMO-enabled 기기라는 것을 인식할 수 있다(S541). 이와 같이 기존 UPnP에서 구현된 통신 방법을 NEMO-enabled 기기에 그대로 적용할 수 있게 된다. 또한 UPnP 뿐만 아니라 블루투스(Bluetooth), JINI, UDDI 등의 네트워크에서도 상기한 원리들을 적용하여 기존의 통신 방법을 활용하여 특정 서비스를 제공하는 기기간 통신할 수 있도록 할 수 있으며, 이때 기기의 고유 ID 정보를 적극 활용하게 된다.

<66> 이후, 본격적인 UPnP 동작 단계가 수행된다(S551). UPnP 동작 단계는, 제어(Control), 이벤트 작업(Eventing) 및 프리젠테이션(Presentation) 등의 동작을 통하여 이루어진다. 상기 제어(Control) 동작을 보면, 컨트롤 포인트(510)는 피제어 기기(520)의 디스크립션을 확보한 후에 피제어 기기(520) 제어를 위한 필수적 작업을 수행한다. 피제어 기기(520)를 제어하기 위하여 컨트롤 포인트(510)는 피제어 기기(520)의 서비스에 동작 명령을 보낸다. 그러기 위해서 컨트롤 포인트(510)는 적절한 제어 메시지를 해당 서비스에 대한 제어 URL(피제어 기기(520)의 기기 정보에 있음)로 보낸다. 제어 메시지도 SOAP(Simple Object Access Protocol)를 사용하여 XML로 표현된다. 해당 서비스는 이 제어 메시지에 대한 응답으로서 특정 동작 값이나 장애 코드를 제공한다. 또한, 상기 이벤트 작업(Eventing)의 동작을 보면, 각 피제어 기기(520)들은 상기한 명령을 받아, 자신의 상태의 변화가 발생하면 이를 컨트롤 포인트(510)에 이벤트 메시지를 통하여 알린다. 이러한 메시지는 한 개 이상의 상태 변수 이름 및 이들 변수들의 현재 값을 포함하고 있으며, XML 형식으로 표현되고 GENA(Generic Event Notification Architecture)를 통하여 포맷된다. 이벤트 내용은 주기적으로 갱신되어 지속적으로 컨트롤 포인트(510)에 통보되며, GENA를 사용하여 가입을 취소할 수도 있다. 그리고, 상기 프리젠테이션(Presentation) 동작을 보면, 피제어 기기(520)가 프리젠테이션용 URL을 가지고 있다면, 컨트롤 포인트(510)는 이 URL을 통하여 페이지를 검색할 수 있고 이 페이지를 브라우저에 로드할 수 있으며, 사용자들은 상기 페이지를 이용하여 피제어 기기(520)를 제

어하거나 피제어 기기(520) 상태를 조회할 수 있다. 이 기능들을 수행할 수 있는 수준은 프리젠테이션 페이지 및 피제어 기기(520)의 특정 기능에 달려있다.

<67> 도 6은 본 발명의 일 실시예에 따른 NEMO-enabled 기기가 UPnP 네트워크 상에서 컨텐츠를 이용하는 일 예를 도시한다.

<68> 본 발명에서 생성된 고유 ID는 인증 목록을 작성하는 데 이용될 수 있다. 즉, NEMO-enabled 기기(610)가 인증서와 자신의 고유 ID, 및 공개키를 컨텐츠(DRM 컨텐츠 포함)를 제공하는 서버(620)로 전달하면, 서버(620)는 인증서를 검증함으로써 NEMO-enabled 기기(610)의 정당성을 검증하고, 인증된 NEMO-enabled 기기(610)의 고유 ID와 공개키를 기록한 인증목록을 작성한다(S601, S611).

<69> 또한 서버(620)가 인증목록을 작성한 후, 상기 인증목록에 있는 NEMO-enabled 기기(610)들에 대한 정보와 서버(620) 자신이 생성한 난수(random number)를 이용하여 고유한 도메인 아이디와 도메인 키를 생성한다(S621). 이때, 상기 도메인 키는 사용자의 선택에 의해 형성된 도메인에 속하는 NEMO-enabled 기기(610)들만이 공유하는 비밀키로서, 상기 도메인을 구성하는 구성원들이 변경될 때마다 같이 변경될 수 있고, 상기 도메인 아이디는 다른 도메인과 구별하기 위한 식별자로서 사용될 수 있다.

<70> 서버(620)는 도메인 내에 있는 인증된 NEMO-enabled 기기(610)들에게 각각의 NEMO-enabled 기기(610)들의 공개키를 이용하여 상기 도메인 아이디와 상기 도메인 키를 암호화하여 전달하고, 상기 NEMO-enabled 기기(610)들은 자신의 비밀키를 이용하여 상기 도메인 키를 복구함으로써, 컨텐츠를 이용하기 위한 도메인이 형성된다(S631, S641). 컨텐츠 공유를 위한 도메인이 형성되면 서버(620)는 컨텐츠를 컨텐츠 키에 의해 암호화하고 상기 컨텐츠 키는 상기 도메인 키에 의해 암호화된다.

<71> 암호화된 컨텐츠는 컨텐츠를 이용하고자 하는 NEMO-enabled 기기(610)들이 도메인 키를 이용하여 복호화함으로써 컨텐츠를 이용할 수 있게 된다(S651)

<72> 이상 첨부된 도면을 참조하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다.

발명의 효과

<73> 상기한 바와 같은 본 발명의 고유 ID 생성 장치에 따르면 특정 서비스를 지원하는 기기를 기존의 네트워크 인프라의 통신 환경에 접목시켜 매끄러운 통합이 가능하고, 기기간 통신 및 컨텐츠 서비스를 제공할 수 있다는 장점이 있다.

도면의 간단한 설명

<1> 도 1은 종래 NEMO 퍼스널라이제이션 과정을 도시한다.

<2> 도 2는 본 발명의 일 실시예에 따른 고유 ID 생성장치의 블록도이다.

<3> 도 3은 상기 도 2를 이용하여 고유 ID를 생성하는 순서도이다.

<4> 도 4는 본 발명의 일 실시예에 따른 퍼스널라이제이션 과정(S331)을 도시한다.

<5> 도 5는 본 발명의 일 실시예에 따른 컨트롤 포인트와 피제어 기기간에 수행되는 UPnP 동작을 도시한다.

<6> 도 6은 본 발명의 일 실시예에 따른 NEMO-enabled 기기가 UPnP 네트워크 상에서 컨텐츠를 이용하는 일 예를 도시한다.

<7> <도면의 주요 부분에 관한 부호의 설명>

<8> 210: 검색부

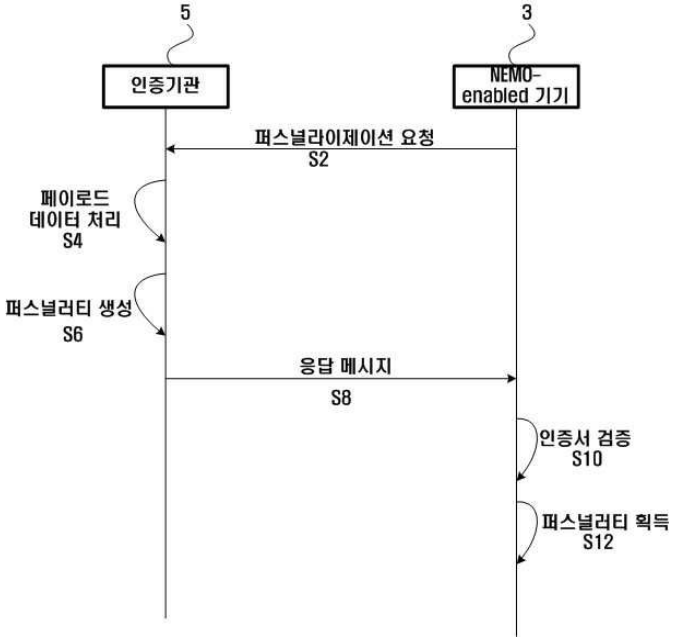
<9> 220: 판독부

<10> 230: 생성부

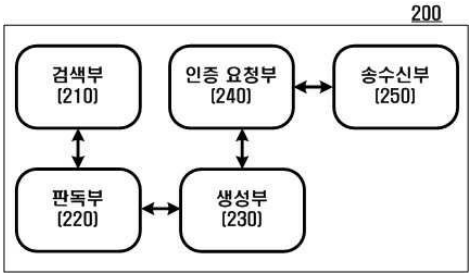
<11> 240: 인증 요청부

도면

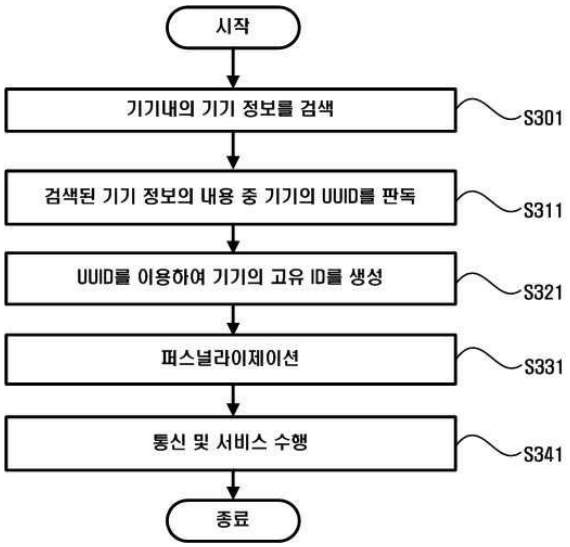
도면1


5
3
인증기관
NEMO-enabled 기기
퍼스널라이제이션 요청
S2
페이로드 데이터 처리
S4
퍼스널러티 생성
S6
응답 메시지
S8
인증서 검증
S10
퍼스널러티 획득
S12

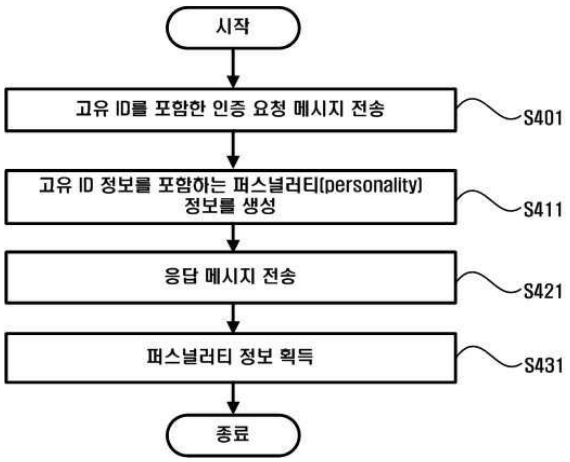
도면2


200
검색부
(210)
인증 요청부
(240)
송수신부
(250)
판독부
(220)
생성부
(230)

도면3


시작
기기내의 기기 정보를 검색
S301
검색된 기기 정보의 내용 중 기기의 UUID를 판독
S311
UUID를 이용하여 기기의 고유 ID를 생성
S321
퍼스널라이제이션
S331
통신 및 서비스 수행
S341
종료

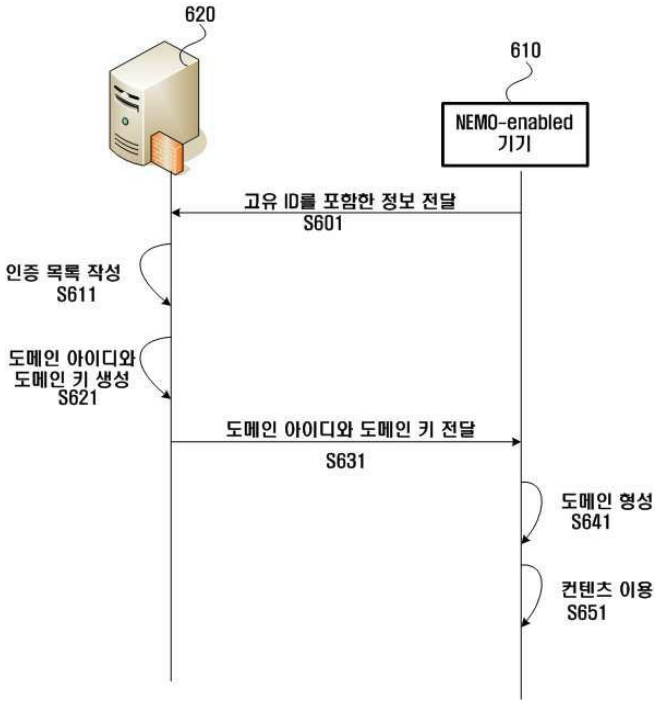
도면4


시작
고유 ID를 포함한 인증 요청 메시지 전송
S401
고유 ID 정보를 포함하는 퍼스널러티(personality) 정보를 생성
S411
응답 메시지 전송
S421
퍼스널러티 정보 획득
S431
종료

도면5


510
DHCP 서버로부터 IP 주소 할당(S511)
디스커버리(S521)
520
디스크립션 파일 요청(HTTP)
S531
디스크립션 파일 전송(HTTP)
피제어 기기의 해당 서비스 인식(S541)
UPnP 동작 단계(S551)
컨트롤 포인트
피제어 기기

도면6


620
610
NEMO-enabled 기기
고유 ID를 포함한 정보 전달
S601
인증 목록 작성
S611
도메인 아이디와 도메인 키 생성
S621
도메인 아이디와 도메인 키 전달
S631
도메인 형성
S641
컨텐츠 이용
S651