(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0057734
(43) 공개일자 2012년06월07일

(51) 국제특허분류(Int. Cl.)
G06F 13/14 (2006.01) *G06F 21/20* (2006.01)
(21) 출원번호 10-2010-0116406
(22) 출원일자 2010년11월22일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
최종일
서울특별시 성동구 금호로 15, 118동 1501호 (금호동4가, 서울숲푸르지오아파트)
이상권
경기도 수원시 팔달구 권광로 243, 205동 203호 (인계동, 래미안노블클래스)
(뒷면에 계속)
(74) 대리인
이동욱, 허성원, 서동헌

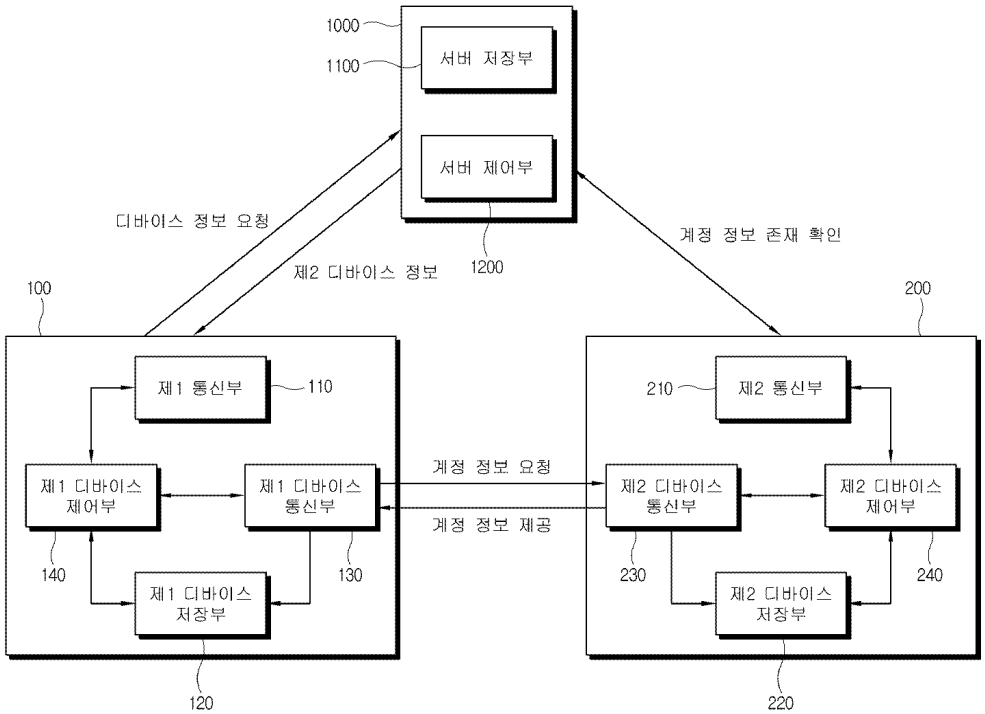
전체 청구항 수 : 총 21 항

(54) 발명의 명칭 **서버, 서버에 접속하는 디바이스 및 그 제어방법**

(57) 요 약

본 발명은 서버, 상기 서버에 접속하는 디바이스 및 그 제어방법에 관한 것이다. 본 발명에 따른 Single Sign On을 위한 서버는 디바이스의 사용자 정보를 저장하고 있는 저장부와; 제1디바이스로부터 컨텐츠 프로바이더에 대한 계정 정보가 요청되면, 상기 제1디바이스의 사용자와 동일한 사용자에 의하여 접속되고, 상기 계정 정보를 포함하고 있는 제2디바이스를 파악하는 제어부를 포함하는 것을 특징으로 하는 제어부를 포함한다. 이에 의해 컨텐츠 프로바이더에 대한 계정 정보를 공유할 수 있는 서버, 상기 서버에 접속하는 디바이스 및 그 제어방법이 제공된다.

대 표 도



(72) 발명자

강춘운

서울특별시 은평구 진관4로 107, 816동 501호 (진관동, 은평뉴타운 상림마을)

한세준

대전광역시 서구 도산로308번길 16 (가장동)

조윤정

경기도 수원시 권선구 곡반정로 95-1, 304호 (곡반정동)

특허청구의 범위

청구항 1

Single Sign On을 위한 서버에 있어서,

디바이스의 사용자 정보를 저장하고 있는 저장부와;

제1디바이스로부터 컨텐츠 프로바이더에 대한 계정 정보가 요청되면, 상기 제1디바이스의 사용자와 동일한 사용자에 의하여 접속되고, 상기 계정 정보를 포함하고 있는 제2디바이스를 파악하는 제어부를 포함하는 것을 특징으로 하는 제어부를 포함하는 것을 특징으로 하는 서버.

청구항 2

제1항에 있어서,

상기 제어부는 검색된 상기 제2디바이스에 대한 정보를 상기 제1디바이스에 제공하는 것을 특징으로 하는 서버.

청구항 3

제1항에 있어서,

상기 제어부는 상기 제2 디바이스로 상기 계정 정보를 요청하고, 수신된 상기 계정 정보를 상기 제1 디바이스로 제공하는 것을 특징으로 하는 서버.

청구항 4

제3항에 있어서,

상기 제2 디바이스로부터 수신된 상기 계정 정보는 PIN 코드와 함께 암호화 되어 있는 것을 특징으로 하는 서버.

청구항 5

제1항에 있어서,

상기 제어부는 상기 제1디바이스의 사용자와 동일한 사용자에 의하여 접속되고, 상기 계정 정보를 포함하고 있는 제2디바이스가 검색되지 않는 경우, 상기 제2 디바이스를 검색할 수 없다는 정보를 상기 제1 디바이스로 제공하는 것을 특징으로 하는 서버.

청구항 6

Single Sign On을 위한 서버에 접속하는 디바이스에 있어서,

상기 서버와 통신하는 서버 통신부와;

상기 서버에 접속하여 현재 사용자에 대한 컨텐츠 프로바이더의 계정 정보를 상기 서버에 요청하도록 상기 서버 통신부를 제어하는 제어부를 포함하는 것을 특징으로 하는 디바이스.

청구항 7

제6항에 있어서,

네트워크를 통해 외부 디바이스와 통신하는 디바이스 통신부를 더 포함하고,

상기 제어부는 현재 사용자와 동일한 사용자에 의하여 접속되고, 상기 계정 정보를 포함하고 있는 제2디바이스에 대한 디바이스 정보를 상기 서버로부터 수신하도록 상기 서버 통신부를 제어하고, 상기 디바이스 정보에 대응하는 상기 제2 디바이스로 상기 계정 정보를 요청하고, 상기 제2 디바이스로부터 상기 계정 정보를 수신하도록 상기 디바이스 통신부를 제어하는 것을 특징으로 하는 디바이스.

청구항 8

제7항에 있어서,

상기 디바이스 통신부는 상기 제2 디바이스와 DLNA에 기초한 네트워킹 통신을 수행하는 것을 특징으로 하는 디바이스.

청구항 9

제6항에 있어서,

상기 제어부는 상기 서버로부터 PIN 코드와 함께 암호화 되어 있는 상기 계정 정보를 수신하고, 사용자로부터 상기 PIN 코드를 수신하면 상기 계정 정보를 복호화 하는 것을 특징으로 하는 디바이스.

청구항 10

Single Sign On을 위한 서버에 있어서,

디바이스의 사용자 정보를 저장하고 있는 저장부와;

제1 디바이스로부터 프라이빗 키에 대한 요청을 수신하면, 상기 프라이빗 키 및 이에 대응하는 퍼블릭 키를 생성하고, 생성된 상기 프라이빗 키를 상기 제1 디바이스에 전송하고, 상기 제1 디바이스와 다른 제2 디바이스로부터 상기 퍼블릭 키에 대한 요청을 수신하면, 상기 사용자 정보에 기초하여 상기 제1디바이스의 사용자와 상기 제2 디바이스의 사용자가 동일한지 판단하고, 판단 결과, 상기 제1디바이스의 사용자와 상기 제2 디바이스의 사용자가 동일하면 상기 퍼블릭 키를 상기 제2 디바이스에 제공하는 제어부를 포함하는 것을 특징으로 하는 서버.

청구항 11

Single Sign On을 위한 서버에 접속하는 디바이스에 있어서,

사용자에 대한 컨텐츠 프로바이더의 계정 정보를 저장하고 있는 저장부와;

상기 서버에 프라이빗 키를 요청하고, 상기 서버로부터 수신한 상기 프라이빗 키를 이용하여 상기 계정 정보를 암호화하는 제어부를 포함하는 것을 특징으로 하는 디바이스.

청구항 12

Single Sign On을 위한 서버에 접속하는 디바이스에 있어서,

저장부와;

암호화된 컨텐츠 프로바이더의 계정 정보가 입력되면, 상기 서버에 퍼블릭 키를 요청하고, 상기 서버로부터 수신한 상기 퍼블릭 키를 이용하여 상기 계정 정보를 복호화하고, 복호화된 상기 계정 정보를 상기 저장부에 저장하는 제어부를 포함하는 것을 특징으로 하는 디바이스.

청구항 13

Single Sign On을 위한 서버의 제어방법에 있어서,

접속된 제1디바이스로부터 컨텐츠 프로바이더에 대한 계정 정보의 요청 신호를 수신하는 단계와,

상기 제1디바이스의 사용자와 동일한 사용자에 의하여 접속되고, 상기 계정 정보를 포함하고 있는 제2디바이스를 파악하는 단계를 포함하는 것을 특징을 하는 서버의 제어방법.

청구항 14

제13항에 있어서,

상기 제2디바이스에 대한 정보를 상기 제1디바이스에 제공하는 단계를 더 포함하는 것을 특징으로 하는 서버의 제어방법.

청구항 15

제13항에 있어서,

상기 제2 디바이스로 상기 계정 정보를 요청하는 단계와;

수신된 상기 계정 정보를 상기 제1 디바이스로 제공하는 단계를 더 포함하는 것을 특징으로 하는 서버의 제어방법.

청구항 16

Single Sign On을 위한 서버에 접속하는 디바이스의 제어방법에 있어서,

상기 서버에 접속하는 단계와;

현재 사용자에 대한 컨텐츠 프로바이더의 계정 정보를 상기 서버에 요청하는 단계를 포함하는 것을 특징으로 하는 디바이스의 제어방법.

청구항 17

제16항에 있어서,

현재 사용자와 동일한 사용자에 의하여 접속되고, 상기 계정 정보를 포함하고 있는 제2디바이스에 대한 디바이스 정보를 상기 서버로부터 수신하는 단계와;

상기 디바이스 정보에 대응하는 상기 제2 디바이스로 상기 계정 정보를 요청하는 단계와;

상기 제2 디바이스로부터 상기 계정 정보를 수신하여 저장하는 단계를 더 포함하는 것을 특징으로 하는 디바이스의 제어방법.

청구항 18

제16항에 있어서,

상기 서버로부터 PIN 코드와 함께 암호화 되어 있는 상기 계정 정보를 수신하는 단계와;

사용자로부터 상기 PIN 코드를 수신하는 단계와;

수신된 상기 PIN 코드에 기초하여 상기 계정 정보를 복호화 하는 단계를 더 포함하는 것을 특징으로 하는 디바이스의 제어방법.

청구항 19

Single Sign On을 위한 서버의 제어방법에 있어서,

디바이스의 사용자 정보를 저장하고 있는 저장부와;

제1 디바이스로부터 프라이빗 키에 대한 요청을 수신하는 단계와;

상기 프라이빗 키 및 이에 대응하는 퍼블릭 키를 생성하는 단계와;

생성된 상기 프라이빗 키를 상기 제1 디바이스에 전송하는 단계와;

상기 제1 디바이스와 다른 제2 디바이스로부터 상기 퍼블릭 키에 대한 요청을 수신하는 단계와;

상기 사용자 정보에 기초하여 상기 제1디바이스의 사용자와 상기 제2 디바이스의 사용자가 동일한지 판단하는 단계와;

판단 결과, 상기 제1디바이스의 사용자와 상기 제2 디바이스의 사용자가 동일하면 상기 퍼블릭 키를 상기 제2 디바이스에 제공하는 단계를 포함하는 것을 특징으로 하는 서버의 제어방법.

청구항 20

Single Sign On을 위한 서버에 접속하는 디바이스의 제어방법에 있어서,

사용자에 대한 컨텐츠 프로바이더의 계정 정보를 저장하는 단계와;

상기 서버에 프라이빗 키를 요청하는 단계와;

상기 서버로부터 수신한 상기 프라이빗 키를 이용하여 상기 계정 정보를 암호화하는 단계를 포함하는 것을 특

징으로 하는 디바이스의 제어방법.

청구항 21

Single Sign On을 위한 서버에 접속하는 디바이스의 제어방법에 있어서,

암호화된 컨텐츠 프로바이더의 계정 정보를 수신하는 단계와;

상기 서버에 퍼블릭 키를 요청하는 단계와;

상기 서버로부터 수신한 상기 퍼블릭 키를 이용하여 상기 계정 정보를 복호화하는 단계와;

복호화된 상기 계정 정보를 저장하는 단계를 포함하는 것을 특징으로 하는 디바이스의 제어방법.

명 세 서

기 술 분 야

[0001] 본 발명은 서버, 상기 서버에 접속하는 디바이스 및 그 제어방법에 관한 것으로서, 보다 상세하게는 Single Sign On을 위한 서버, 상기 서버에 접속하는 디바이스 및 그 제어방법에 관한 것이다.

배 경 기 술

[0002] Single Sign On(SSO)은 여러 개의 사이트에서 한 번의 로그인으로 여러 가지 다른 사이트들을 자동적으로 접속, 사용하는 방법을 말한다. 일반적으로 서로 다른 시스템, 서로 다른 사이트에서는 각각의 사용자 정보를 관리하게 된다. 여러 개의 사이트를 운영하는 대기업이나 인터넷 관련 기업이 각각의 회원을 통합 관리할 필요성이 생김에 따라 개발된 방식이다.

[0003] 개인의 경우, 사이트에 접속하기 위하여 아이디와 패스워드는 물론 이름?전화번호 등 개인 정보를 각 사이트마다 일일이 기록해야 하던 것을 한 번의 작업으로 끝나므로 불편함이 해소되며, 기업에서는 회원에 대한 통합관리가 가능해 마케팅을 극대화시킬 수 있다는 장점이 있다.

[0004] 최근 인터넷 텔레비전의 확산으로 인하여 텔레비전에서 웹에 접속하여 다양한 서비스를 이용하고 있다. 이 경우, 사용자의 편리성을 증대시키기 위하여 Single Sign On이 구현하는 것과 서로 상이한 디바이스에서는 특정 사이트의 계정 정보를 공유할 수 있도록 하는 것 등이 요구되고 있다.

발명의 내용

[0005] 본 발명의 일 실시예는 컨텐츠 프로바이더에 대한 계정 정보를 공유할 수 있는 서버, 상기 서버에 접속하는 디바이스 및 그 제어방법을 제공한다.

[0006] 본 발명의 다른 실시예는 저장매체를 이용하여 컨텐츠 프로바이더에 대한 계정 정보를 공유할 수 있는 서버, 상기 서버에 접속하는 디바이스 및 그 제어방법을 제공한다.

[0007] 또한, 본 발명의 다른 실시예는 디바이스 정보를 보다 용이하게 서버에 등록시킬 수 있는 서버, 상기 서버에 접속하는 디바이스 및 그 제어방법을 제공한다.

[0008] 본 발명의 일 실시예에 따른 Single Sign On을 위한 서버는 디바이스의 사용자 정보를 저장하고 있는 저장부와; 제1디바이스로부터 컨텐츠 프로바이더에 대한 계정 정보가 요청되면, 상기 제1디바이스의 사용자와 동일한 사용자에 의하여 접속되고, 상기 계정 정보를 포함하고 있는 제2디바이스를 파악하는 제어부를 포함한다.

[0009] 상기 제어부는 검색된 상기 제2디바이스에 대한 정보를 상기 제1디바이스에 제공한다.

[0010] 또는, 상기 제어부는 상기 제2 디바이스로 상기 계정 정보를 요청하고, 수신된 상기 계정 정보를 상기 제1 디바이스로 직접 제공할 수도 있다.

[0011] 이 때, 계정 정보의 보안을 위한 위하여 상기 제2 디바이스로부터 수신된 상기 계정 정보는 PIN 코드와 함께 암호화 되는 것이 바람직하다.

[0012] 상기 제어부는 상기 제1디바이스의 사용자와 동일한 사용자에 의하여 접속되고, 상기 계정 정보를 포함하고 있는 제2디바이스가 검색되지 않는 경우, 상기 제2 디바이스를 검색할 수 없다는 정보를 상기 제1 디바이스로

제공할 수도 있다.

[0013] 한편, 본 발명의 일 실시예에 따른 Single Sign On을 위한 서버에 접속하는 디바이스는 상기 서버와 통신하는 서버 통신부와; 상기 서버에 접속하여 현재 사용자에 대한 컨텐츠 프로바이더의 계정 정보를 상기 서버에 요청하도록 상기 서버 통신부를 제어하는 제어부를 포함할 수 있다.

[0014] 디바이스는 네트워크를 통해 외부 디바이스와 통신하는 디바이스 통신부를 더 포함하고, 상기 제어부는 현재 사용자와 동일한 사용자에 의하여 접속되고, 상기 계정 정보를 포함하고 있는 제2디바이스에 대한 디바이스 정보를 상기 서버로부터 수신하도록 상기 서버 통신부를 제어하고, 상기 디바이스 정보에 대응하는 상기 제2 디바이스로 상기 계정 정보를 요청하고, 상기 제2 디바이스로부터 상기 계정 정보를 수신하도록 상기 디바이스 통신부를 제어할 수 있다.

[0015] 상기 디바이스 통신부는 상기 제2 디바이스와 DLNA에 기초한 네트워킹 통신을 수행할 수 있다.

[0016] 상기 제어부는 상기 서버로부터 PIN 코드와 함께 암호화 되어 있는 상기 계정 정보를 수신하고, 사용자로부터 상기 PIN 코드를 수신하면 상기 계정 정보를 복호화할 수 있다.

[0017] 한편, 본 발명의 다른 실시예에 따른 Single Sign On을 위한 서버는 디바이스의 사용자 정보를 저장하고 있는 저장부와; 제1 디바이스로부터 프라이빗 키에 대한 요청을 수신하면, 상기 프라이빗 키 및 이에 대응하는 퍼블릭 키를 생성하고, 생성된 상기 프라이빗 키를 상기 제1 디바이스에 전송하고, 상기 제1 디바이스와 다른 제2 디바이스로부터 상기 퍼블릭 키에 대한 요청을 수신하면, 상기 사용자 정보에 기초하여 상기 제1디바이스의 사용자와 상기 제2 디바이스의 사용자가 동일한지 판단하고, 판단 결과, 상기 제1디바이스의 사용자와 상기 제2 디바이스의 사용자가 동일하면 상기 퍼블릭 키를 상기 제2 디바이스에 제공하는 제어부를 포함할 수 있다.

[0018] 이에 대응하여, Single Sign On을 위한 서버에 접속하는 제1디바이스는 사용자에 대한 컨텐츠 프로바이더의 계정 정보를 저장하고 있는 저장부와; 상기 서버에 프라이빗 키를 요청하고, 상기 서버로부터 수신한 상기 프라이빗 키를 이용하여 상기 계정 정보를 암호화하는 제어부를 포함할 수 있다.

[0019] 또한, 이에 대응하는 제2 디바이스는 저장부와; 암호화된 컨텐츠 프로바이더의 계정 정보가 입력되면, 상기 서버에 퍼블릭 키를 요청하고, 상기 서버로부터 수신한 상기 퍼블릭 키를 이용하여 상기 계정 정보를 복호화하고, 복호화된 상기 계정 정보를 상기 저장부에 저장하는 제어부를 포함할 수 있다.

[0020] 또한, 본 발명의 다른 실시예에 따른 Single Sign On을 위한 서버의 제어방법은 접속된 제1디바이스로부터 컨텐츠 프로바이더에 대한 계정 정보의 요청 신호를 수신하는 단계와, 상기 제1디바이스의 사용자와 동일한 사용자에 의하여 접속되고, 상기 계정 정보를 포함하고 있는 제2디바이스를 파악하는 단계를 포함할 수 있다.

[0021] 이상 설명한 바와 같이, 본 발명의 일 실시예에 따르면 컨텐츠 프로바이더에 대한 계정 정보를 공유할 수 있는 서버, 상기 서버에 접속하는 디바이스 및 그 제어방법이 제공된다.

[0022] 본 발명의 다른 실시예에 따르면 저장매체를 이용하여 컨텐츠 프로바이더에 대한 계정 정보를 공유할 수 있는 서버, 상기 서버에 접속하는 디바이스 및 그 제어방법이 제공된다.

[0023] 또한, 본 발명의 다른 실시예에 따르면 디바이스 정보를 보다 용이하게 서버에 등록시킬 수 있는 서버, 상기 서버에 접속하는 디바이스 및 그 제어방법이 제공된다.

도면의 간단한 설명

[0024] 도 1은 본 발명의 일 실시예에 따른 서버 및 디바이스의 제어블럭도이고,

도 2는 도 1의 서버 및 디바이스의 제어방법을 설명하기 위한 제어흐름도이고,

도 3은 본 발명의 다른 실시예에 따른 서버 및 디바이스의 제어블럭도이고,

도 4는 도 3의 서버 및 디바이스의 제어방법을 설명하기 위한 제어흐름도이고,

도 5는 본 발명의 또 다른 실시예에 따른 서버 및 디바이스의 제어블럭도이고,

도 6은 도 5의 서버 및 디바이스의 제어방법을 설명하기 위한 제어흐름도이고,

도 7은 본 발명에 따른 서버 및 디바이스의 등록 방법을 설명하기 위한 제어흐름도이고,

도 8은 도 7의 디바이스 식별 컨텐츠를 생성하기 위한 유저 인터페이스이고,

도 9는 도 7의 식별 컨텐츠 검색을 설명하기 위한 유저 인터페이스이다.

발명을 실시하기 위한 구체적인 내용

[0025] 이하, 첨부한 도면을 참고로 하여 본 발명의 실시예들에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예들에 한정되지 않는다. 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 동일 또는 유사한 구성요소에 대해서는 동일한 참조부호를 붙이도록 한다.

[0026] 도 1은 본 발명의 일 실시예에 따른 서버 및 디바이스의 제어블럭도이다.

[0027] 도시된 바와 같이, 서버(1000)는 서버 저장부(1100) 및 서버 제어부(1200)를 포함하고, 제1 디바이스(100)는 제1 통신부(110), 제1 디바이스 저장부(120), 제1 디바이스 통신부(130) 및 제1 디바이스 제어부(140)를 포함하고, 제2 디바이스(200)는 제2 통신부(210), 제2 디바이스 저장부(220), 제2 디바이스 통신부(230) 및 제2 디바이스 제어부(240)를 포함한다.

[0028] 서버(1000)에는 제1 디바이스(100) 및 제2 디바이스(200)의 정보가 등록되어 있으며, 서버(1000)는 제1 디바이스(100) 및 제2 디바이스(200)에서 Single Sign On을 구현하기 위한 다양한 정보를 제1 디바이스(100) 및 제2 디바이스(200)에 제공한다. 이러한 서버(1000)는 제1 디바이스(100) 및 제2 디바이스(200)를 제조한 제조자가 운영하는 서버를 포함할 수 있다.

[0029] 제1 디바이스(100) 및 제2 디바이스(200)는 인터넷 프로토콜을 통하여 다양한 서비스를 제공 받을 수 있는 IP TV로 구현될 수도 있고, 개인용 컴퓨터, 휴대용 전화기, 스마트폰, PMP, 넷북, 노트북, 전자북과 같은 개인 단말기로 구현될 수도 있다. 제1 디바이스(100)와 제2 디바이스(200)는 인터넷 접속을 통하여 다양한 컨텐츠 프로바이더로부터 컨텐츠를 제공 받아 표시하고, 실행할 수 있는 모든 디바이스를 포함한다.

[0030] 사용자가 제1 디바이스(100) 및 제2 디바이스(200)에서 서버(1000)로 접속하여 사용자 계정을 생성 및 등록하면, 사용자 ID와 같은 사용자 정보, 디바이스의 모델 번호, 모델 코드 및 제조 번호 등과 같은 디바이스 고유 정보가 서버(1000)에 제공되고, 서버(1000)는 사용자와 디바이스에 대한 정보에 기초하여 디바이스를 통하여 사용자에게 다양한 서비스를 제공할 수 있다. 서버(1000)는 사용자 별로 개별적인 계정 정보(아이디 및 비밀번호)를 저장할 수 있다. 즉, 디바이스(100, 200)가 공용으로 사용되는 텔레비전으로 구현되면, 각 사용자는 개별적으로 사용자 정보를 생성하여 서버(1000)에 등록할 수 있으며, 서버(1000)는 개별적인 사용자에 대응하는 서비스를 제공한다.

[0031] 사용자가 서버(1000)에 사용자 정보 및 디바이스 정보를 등록시킨 후, 사용자가 서버(1000)에 재 접속하면, 서버(1000)는 기존에 등록된 사용자 정보 및 디바이스 정보에 기초하여 사용자 인증 과정을 수행하고, 유효한 사용자 및 디바이스로 인증되면, 서버(1000)는 사용자에게 인증 토큰(authentication token)을 발급할 수 있다. 이러한 인증 토큰은 한 번 발행되면 하루 또는 이틀과 같이 정해진 특정 시간 동안만 유효하고 특정 시간이 경과하면 그 효력을 잃도록 설정될 수 있다.

[0032] 서버(1000)가 제공할 수 있는 복수의 서비스, 예컨대, 메일링 서비스, SNS(social network service), 블로그 서비스, 미디어 제공 서비스 등이 존재하는 경우, 사용자는 복수의 서비스를 이용하기 위하여 복수의 로그인을 수행하지 않아도 된다. 인증 토큰이 발급된 후, 사용자가 특정 서비스에 접속하면 서버(1000)에 의하여 발급 받은 인증 토큰의 유효성이 체크된다. 인증 토큰의 유효성만 확인되면 사용자는 서비스 이용을 위한 추가 로그인 없이 서버(1000)가 운영하는 서비스를 이용할 수 있다. 서버(1000)는 인증 토큰을 발급함으로써 Single Sign On를 구현하고, 사용자 역시 복수의 로그인 없이 편리하게 서비스를 이용할 수 있다. 서버 저장부(1100)는 등록된 사용자 정보와 디바이스 정보를 저장하고 있으며, 사용자에게 발급한 인증 토큰 또한 저장하고 있다. 서버 제어부(1200)는 서버 저장부(1100)에 저장되어 있는 정보를 이용하여 어떠한 사용자에게 어떠한 인증 토큰이 발급되었는지 알 수 있다.

[0033] 서버 제어부(1200)는 제1 디바이스(100) 및 제2 디바이스(200)와 통신하며, 서버(1000)에 접속하여 등록한 사용자 정보 및 디바이스 정보를 서버 저장부(1100)에 저장하고 사용자가 로그인할 때마다 인증 토큰을 발급한다. 또한, 서버 제어부(1200)는 제1 디바이스(100)로부터 컨텐츠 프로바이더에 대한 계정 정보(아이디와 비밀번호)가 요청되면, 제1 디바이스(100)의 사용자와 동일한 사용자에 의하여 접속되고, 계정 정보를 포함하고

있는 제2 디바이스(200)를 파악한다.

[0034] 상술한 바와 같이, 제1 디바이스(100) 및 제2 디바이스(200)는 인터넷을 통하여 다양한 컨텐츠 프로바이더에 접속할 수 있는 전자 디바이스로 구현된다. 설명의 편의를 위하여 이하, 제1 디바이스(100)는 컨텐츠 프로바이더의 계정 정보를 저장하고 있지 않고, 제2 디바이스(200)는 제1 디바이스(100)에서 요청한 컨텐츠 프로바이더의 계정 정보를 저장하고 있는 것으로 가정한다. 동일한 사용자라 하여도 제2 디바이스(200)가 아닌 제1 디바이스(100)에는 컨텐츠 프로바이더에 대한 계정 정보가 없기 때문에 사용자는 제1 디바이스(100)에서 컨텐츠 프로바이더로 접속하기 위하여는 계정 정도를 또 등록해야 하는 불편함이 있다. 예를 들어, 서재에 있는 텔레비전에 facabook 또는 tweeter와 같은 SNS 사이트의 계정 정보가 저장되어 있어도, 거실에 있는 텔레비전에서는 이러한 계정 정보를 이용할 수 없다.

[0035] 또한, 제1 디바이스(100)와 제2 디바이스(200)가 Single Sign On을 구현할 수 있는 경우, 사용자가 제2 디바이스(200)에서 서버(1000)에 로그인 하면, 다른 컨텐츠 프로바이더에 자동으로 로그인 될 수 있다. 하지만, 제1 디바이스(100)에서는 컨텐츠 프로바이더에 대한 계정 정보가 존재하기 않기 때문에 컨텐츠 프로바이더에 로그인 하는 것이 불가능하다.

[0036] 이러한 점을 개선하기 위하여, 서버 제어부(1200)는 현재 로그인 되어 있는 디바이스 중 동일한 사용자에 의하여 로그인되어 있고, 사용자로부터 요청된 계정 정보를 저장하고 있는 디바이스를 파악하여 이를 사용자에게 알려준다.

[0037] 제1 통신부(110) 및 제2 통신부(210)는 제1 디바이스 제어부(140)와 제2 디바이스 제어부(240)의 제어에 따라 서버(1000)에 접속하여, 사용자 정보 및 디바이스 정보를 서버(1000)에 제공하고, 서버(1000)로부터 다양한 데이터를 수신한다.

[0038] 제1 디바이스 저장부(120)와 제2 디바이스 저장부(220)는 각각 사용자 정보, 디바이스 정보 및 서버(1000)로부터 수신한 인증 토큰을 저장하고 있다. 이러한 인증 토큰은 상술한 바와 같이, 사용자 인증이 필요한 때 서버(1000)로 전송되어 인증 과정을 거치게 된다. 또한, 제2 디바이스(200)는 사용자에 대한 계정 정보를 저장하고 있다. 사용자 정보 및 계정 정보는 특정 개인에 대한 정보로써 하나의 디바이스를 복수의 사용자가 사용할 경우, 사용자 별로 저장된다. 예를 들어, 아빠가 서버(1000)에 접속하면 아빠에 해당하는 사용자 정보가 저장되고, 아빠가 컨텐츠 프로바이더에 접속하면 아빠의 계정 정보가 개별적으로 저장된다. 각 사용자는 각 디바이스(100, 200)에서 자신의 정보를 서버(1000)에 등록하고, 컨텐츠 프로바이더에 접속하여 계정 정보를 생성해야 한다.

[0039] 제1 디바이스 통신부(130)는 네트워크를 통해 제2 디바이스 통신부(230)와 통신한다. 제1 디바이스 통신부(130)와 제2 디바이스 통신부(230)는 블루투스, 와이파이, 지그비(zigbee), IR 통신, RF 통신, 그 밖의 유선 통신과 같은 다양한 통신방법에 대응하는 통신모듈을 포함할 수도 있다.

[0040] 한편, 가정의 컴퓨터, 가전제품, 휴대용 단말기 등의 전자기기에 저장되어 있는 음악, 사진, 비디오 같은 디지털 컨텐츠를 공유할 수 있는 홈네트워킹을 지원하는 미들웨어에는 UPnP(Universal Plug and Play), HaVi(Home Audio Video Interoperability), Jini, VESA, DLNA(digital living network alliance)...등이 있다. 본 실시예에 따른 제1 디바이스(100)와 제2 디바이스(200)는 이미 구축되어 있는 공개 표준, 예컨대 HTTP, UPnP, 와이 파이 등의 업계 표준에 기초하여 구축된 DLNA 에 따라 통신할 수 있다. DLNA는 TV, VCR, 디지털 카메라, 오디오시스템 등의 기기들로부터 제공되는 모든 컨텐츠를 공유하는 것에 초점이 맞추어져 있으며 모바일 장치나 PC(Personal Computer) 등과 같은 개인 영역의 장치로부터 많은 디지털 미디어 컨텐츠(예컨대, 사진, 음악 및 비디오 등)를 획득하고, 전송하며, 관리할 수 있도록 지원한다. 제1 디바이스(100)와 제2 디바이스(200)는 DLNA 기반에 기초한 네트워킹을 통하여 컨텐츠 프로바이더에 대한 계정 정보을 송수신할 수 있다.

[0041] 제1 디바이스 제어부(140)는 현재 사용자에 대한 컨텐츠 프로바이더의 계정 정보를 서버(1000)에 요청하도록 제1 디바이스 통신부(130)를 제어하고, 서버(1000)로부터 현재 사용자와 동일한 사용자에 의하여 접속되고, 계정 정보를 포함하고 있는 제2 디바이스(200)에 대한 디바이스 정보를 서버(1000)로부터 수신한다.

[0042] 제2 디바이스 제어부(240)는 서버(1000)에 접속하여, 컨텐츠 프로바이더에 대한 계정 정보의 존재 확인 요청에 응답하고, 제1 디바이스(100)의 요청에 따라 저장하고 있던 컨텐츠 프로바이더에 대한 계정 정보를 제2 디바이스 통신부(230)를 통하여 제1 디바이스(100)로 전송한다.

[0043] 도 2는 도 1의 서버 및 디바이스의 제어방법을 설명하기 위한 제어흐름도이다. 이를 참조하여 제1 디바이스

(100)와 제2 디바이스(200)가 계정 정보의 공유하는 방법을 설명하면 다음과 같다.

[0044] 우선, 제1 디바이스(100) 및 제2 디바이스(200)는 각각 서버(1000)에 로그인 되어 있다.

[0045] 본 실시예에 따른 제1 디바이스(100)는 컨텐츠 프로바이더에 대한 계정 정보를 획득하기 위하여 서버(1000)에 계정 정보를 가지고 있는 디바이스, 즉, 제2 디바이스(200)에 대한 정보를 요청한다(S10).

[0046] 서버(1000)는 제1 디바이스(100)로부터 수신된 요청 신호에 대응하여, 제1 디바이스(100)의 현재 사용자와 동일한 사용자에 의하여 접속된 디바이스를 체크한다(S20). 서버 저장부(1100)에는 어떠한 사용자에게 어떠한 인증 토큰가 발급되었는지 저장되어 있기 때문에 서버 제어부(1200)는 서버 저장부(1100)를 이용하여 로그인 한 사용자의 동일성을 파악할 수 있다.

[0047] 동일 사용자가 접속한 디바이스를 파악한 서버(1000)는 디바이스에 컨텐츠 프로바이더에 대한 계정 정보가 존재하는지 여부를 확인한다(S30).

[0048] 계정 정보를 저장하고 있는 디바이스, 즉 제2 디바이스(200)는 서버(1000)의 이러한 요청에 대응하여 컨텐츠 프로바이더에 대한 계정 정보를 전송할 준비가 되었음을 알리는 신호를 서버(1000)로 전송한다(S40).

[0049] 서버(1000)는 제2 디바이스(200)로부터 수신된 신호에 기초하여, 계정 정보를 포함하고 있는 제2 디바이스(200)에 대한 정보를 제1 디바이스(100)로 제공한다(S50). 디바이스에 대한 정보는 제1 디바이스(100)와 통신할 수 있는 제2 디바이스(200)의 통신 정보일 수도 있고, 동일한 사용자에 의하여 로그인 된 복수의 디바이스 중에서 계정 정보를 포함하는 디바이스를 식별할 수 있는 GUI 정보일 수도 있다.

[0050] 제1 디바이스(100)는 제1 디바이스 통신부(130)를 통하여 계정 정보를 포함하고 있는 제2 디바이스(200)로 계정 정보를 요청한다(S60).

[0051] 제2 디바이스(200)는 계정 정보를 암호화(encryption)하여(S70), 암호화된 계정 정보를 제2 디바이스 통신부(230)를 통하여 제1 디바이스(100)로 전송한다(S80).

[0052] 제1 디바이스(100)는 계정 정보를 복호화하여 이를 제1 디바이스 저장부(120)에 저장한다(S90). 컨텐츠 프로바이더에 대한 계정 정보를 저장한 제1 디바이스(100)는 한번의 로그인을 통하여 컨텐츠 프로바이더에 접속하는 Single Sign On을 구현할 수 있다.

[0053] 도 3은 본 발명의 다른 실시예에 따른 서버 및 디바이스의 제어블럭도이다.

[0054] 본 실시예에 따른, 제1 디바이스(100)와 제2 디바이스(200)는 도 1과는 달리 제1 디바이스 통신부(130) 및 제2 디바이스 통신부(230)를 포함하지 않으며, 다른 구성 요소는 도 1의 실시예와 실질적으로 동일하다.

[0055] 제1 디바이스(100)는 컨텐츠 프로바이더에 대한 계정 정보를 제2 디바이스(200)와의 통신이 아닌 서버(1000)를 통하여 제공 받는다. 도 4는 도 3의 서버 및 디바이스의 제어방법을 설명하기 위한 제어흐름도이다.

[0056] 제1 디바이스(100)는 컨텐츠 프로바이더에 대한 계정 정보를 획득하기 위하여 서버(1000)에 계정 정보를 요청한다(S11).

[0057] 서버(1000)는 제1 디바이스(100)로부터 수신된 요청 신호에 대응하여, 제1 디바이스(100)의 현재 사용자와 동일한 사용자에 의하여 접속된 디바이스를 체크하고(S20), 동일 사용자가 접속한 디바이스로 파악한 디바이스에 컨텐츠 프로바이더에 대한 계정 정보가 존재하는지 여부를 확인한다(S30). 제2 디바이스(200)는 서버(1000)의 요청에 대응하여 컨텐츠 프로바이더에 대한 계정 정보를 전송할 준비가 되었음을 알리는 신호를 서버(1000)로 전송한다(S40).

[0058] 제2 디바이스(200)로부터 계정 정보를 전송할 준비가 되었음을 알리는 신호를 수신한 서버(1000)는 제2 디바이스(200)로 계정 정보를 요청한다(S51).

[0059] 제2 디바이스(200)는 PIN 코드와 함께 계정 정보를 암호화 한다(S71).

[0060] 그런 후, 제2 디바이스(200)는 암호화된 계정 정보를 서버(1000)로 전송하고, 서버(1000)로 전송된 계정 정보는 서버(1000)를 바이 패스하여 제1 디바이스(100)로 전송된다(S81). 즉, 본 실시예에 따른 서버(1000)는 제2 디바이스(200)로부터 계정 정보를 수신하여 이를 제1 디바이스(100)로 전달하는 전달 매개체 역할을 한다. 계정 정보는 서버(1000)에 저장되지 않는다. 서버(1000)는 암호화된 계정 정보가 전송되면, 제1 디바이스(100)와 제2 디바이스(200)의 사용자가 동일한지 다시 한 번 더 확인할 수도 있다.

[0061] 제1 디바이스(100)는 사용자로부터 입력된PIN 코드를 이용하여 암호화된 계정 정보를 복호화하고, 이를 저장

한다(S91). 동일한 사용자라면 제2 디바이스(200)에 입력된 PIN 코드를 제1 디바이스(100)에 동일하게 입력할 수 있을 것이다. 이 과정에서 각 디바이스(100, 200)가 로그인 시 발급 받은 인증 토큰의 유효 기간이 경과하면 PIN 코드가 유효하더라도 계정 정보가 전달되지 않을 수 있다.

[0062] 서버 제어부(1200)는 제1 디바이스(100)로부터 제2 디바이스(200)에 대한 정보 또는 계정 정보의 요청을 수신하였을 때, 제1 디바이스(100)의 사용자와 동일한 사용자에 의하여 접속되고, 계정 정보를 포함하고 있는 제2 디바이스(200)가 검색되지 않는 경우, 제2 디바이스(200)를 검색할 수 없다는 정보를 제1 디바이스(100)로 제공할 수 있다. 또한, 이 경우, 서버 제어부(1200)는 제2 디바이스(200)가 로그인 되면 제1 디바이스(100)로부터 계정 정보의 요청이 있었음을 알리는 메시지를 전송할 수도 있다. 도 5는 본 발명의 또 다른 실시예에 따른 서버 및 디바이스의 제어블럭도이다.

[0063] 본 실시예에 따른 제1 디바이스(100)와 제2 디바이스(200)는 제1 디바이스 저장부(120) 및 제2 디바이스 저장부(220) 이외에 외부의 저장부가 접속할 수 있는 인터페이스인 제1 저장매체 접속부(150) 및 제2 저장매체 접속부(250)를 포함한다. 제1 저장매체 접속부(150) 및 제2 저장매체 접속부(250)는 USB 메모리와 같은 이동 저장 매체가 접속할 수 있는 접속 포트로 구현될 수 있고, 저장부를 포함하는 외부 디바이스가 연결될 수 있는 유, 무선 네트워크 접속부를 포함할 수도 있다.

[0064] 본 실시예에 따르면, 제1 저장매체 접속부(150) 및 제2 저장매체 접속부(250)에 접속될 수 있는 저장매체(300)가 계정 정보를 운반하는 매개체가 된다.

[0065] 도 6은 도 5의 서버 및 디바이스의 제어방법을 설명하기 위한 제어흐름도이다.

[0066] 우선, 컨텐츠 프로바이더에 대한 계정 정보를 저장하고 있는 제2 디바이스(200)는 서버(1000)에 프라이빗 키를 요청한다(S100).

[0067] 서버(1000)는 프라이빗 키 및 이에 대응하는 퍼블릭 키를 생성하고(S110), 생성된 프라이빗 키를 제2 디바이스(200)에 전송한다(S120).

[0068] 제2 디바이스(200)는 서버(1000)로부터 수신한 프라이빗 키를 이용하여 계정 정보를 암호화한다(S130).

[0069] 이러한 암호화된 계정 정보는 저장매체(300)에 저장되고, 이동 가능한 저장매체(300)는 제1 디바이스(100)의 제1 저장매체 접속부(150)에 접속될 수 있다.

[0070] 제1 디바이스(100)는 저장매체(300)를 이용하여 암호화된 계정 정보를 수신하고(S140), 암호 해독을 위한 퍼블릭 키를 서버(1000)에 요청한다(S150).

[0071] 서버(1000)는 사용자 정보에 기초하여 제1디바이스(100)의 사용자와 제2 디바이스(200)의 사용자가 동일한지 여부, 즉 프라이빗 키를 제공한 제2 디바이스(200)의 사용자와 동일한 사용자에 의하여 퍼블릭 키가 요청되는지 여부를 판단한다(S160).

[0072] 판단 결과, 제1 디바이스(100)의 사용자와 제2 디바이스(200)의 사용자가 동일하면 서버(1000)는 퍼블릭 키를 제1 디바이스(100)에 제공한다(S170).

[0073] 제1 디바이스(100)는 서버(1000)로부터 수신한 퍼블릭 키를 이용하여 계정 정보를 복호화하고, 복호화된 계정 정보를 제1 디바이스 저장부(120)에 저장한다(S180).

[0074] 제1 디바이스(100)는 로그인 시 발급 받은 인증 토큰의 유효 기간이 경과하기 전에, 퍼블릭 키를 서버(1000)에 요청해야 한다.

[0075] 다른 실시예에 따르면, 서버(1000)는 제2 디바이스(200)로부터 수신한 컨텐츠 프로바이더에 대한 계정 정보를 사용자 별로 저장할 수 있다. 제1 디바이스(100)로부터 계정 정보에 대한 요청 신호를 수신하면, 제1 디바이스(100) 및 제2 디바이스(200)의 인증을 수행하고, 미리 저장되어 있던 계정 정보를 제1 디바이스(100)에 전송할 수 있다. 또는, 제1 디바이스(100)로부터 계정 정보에 대한 요청 신호를 수신하면, 동일한 사용자가 로그인 되어 있고 제1 디바이스(100)가 요청한 계정 정보를 저장하고 있는 제2 디바이스(200)를 검색한 후, 계정 정보를 요청하여 수신할 수 있다. 계정 정보를 서버(1000)에 저장하고 있으면, 이 후 동일한 사용자에 의하여 계정 정보가 요청될 경우 제2 디바이스(200)의 도움 없이 계정 정보를 제1 디바이스(100)에 제공할 수 있다. 이런 경우, 서버(1000)는 제2 디바이스(200)가 턴온되어 있지 않아도 계정 정보를 제1디바이스(100)에 제공하고, 향후 제2 디바이스(200)가 턴온되는 경우 계정 정보가 제1 디바이스(100)에 의하여 이용되었음을 알리는 알림 메시지를 제2 디바이스(200)에 제공할 수 있다.

[0076] 또한, 서버(1000)는 사용자 별로, 즉, 사용자의 계정 정보에 대응하여 다양한 개별 정보를 저장할 수 있다. 예를 들어, 사용자의 컨텐츠 이용 패턴, 컨텐츠 선호도, 프로그램 선호도, 방송 채널의 히스토리, 방송 시청 시간 등을 수집하여 저장할 수 있으며, 이에 대응하여 다양한 서비스를 제공할 수 있다. 예를 들어 서버(1000)는 사용자가 관심을 가질 가능성이 있는 컨텐츠를 추천하거나 다른 방송 채널을 추천하라 수 있다. 이런 사용자 개별 정보는 사용자가 로그인한 디바이스와 무관하게 서버(1000)에 저장되고 서버(1000)에 의하여 관리된다. 따라서, 사용자가 제1디바이스(100)를 통하여 컨텐츠를 재생하거나 방송 프로그램을 시청한 후, 이에 대한 사용자 정보가 서버(1000)에 저장되면 사용자가 제2 디바이스(200)을 통하여 서버(1000)에 접속하더라도 서버(1000)는 사용자 별로 저장된 사용자 정보에 기초하여 사용자에게 서비스를 제공할 수 있다.도 7은 본 발명에 따른 서버 및 디바이스의 등록 방법을 설명하기 위한 제어흐름도이다. 제1 디바이스(100) 또는 제2 디바이스(200)가 서버(1000)와 통신하기 위해서는 디바이스에 대한 정보가 서버(1000)로 제공되어야 한다. 사용자가 텔레비전과 같은 전자 디바이스를 새롭게 구입하면, 제품의 제조사 또는 서비스 관련 업체의 서버에 디바이스를 등록할 수 있다.

[0077] 사용자는 서버에 접속하여 디바이스 정보를 입력하게 되는데, 통상적으로 이러한 디바이스 정보는 모델명, 모델코드, 인증 번호, 제조 번호 등과 같은 긴 문자를 포함하고 있다. 사용자가 이러한 등록 과정이 어렵고 복잡하여 새로운 디바이스를 서버에 등록하지 않을 수 있다.

[0078] 디바이스 활용도를 높이고, 사용자가 서버에서 제공하는 다양한 서비스를 보다 용이하게 제공 받기 위하여 본 실시예에 따른 서버(1000) 및 디바이스(100, 200)는 디바이스 식별 컨텐츠를 생성한다. 디바이스는 제1 디바이스(100)를 예를 들어 설명된다. 도 7 내지 도 9를 참조하여 이를 설명하면 다음과 같다.

[0079] 우선, 도 8과 같이 디바이스 식별 컨텐츠 및 비밀번호를 생성한다(S200). 도 8은 디바이스 식별 컨텐츠를 생성하기 위한 유저 인터페이스로서 제1 디바이스(100)에 표시된다. 사용자는 제1 디바이스를 식별하기 위한 고유한 식별 컨텐츠(Ⅰ)를 생성한다. 식별 컨텐츠(Ⅰ)는 정지 영상, 동영상, 텍스트, 음성 신호 등을 포함할 수 있고, 본 실시예에 따를 경우 식별 컨텐츠(Ⅰ)는 사진과 같은 정지 영상과 제1 디바이스(100)를 명명하는 별명을 포함한다. 또한, 사용자는 식별 컨텐츠(Ⅰ)와 함께 비밀 번호(Ⅱ)도 생성한다. 비밀 번호(Ⅱ)는 보안 정도에 따라 문자, 숫자, 숫자 및 문자 등을 포함할 수 있고 그 길이도 변경될 수 있다.

[0080] 그런 후, 사용자가 디바이스의 식별 컨텐츠(Ⅰ)를 서버(1000)로 전송하기 위한 등록 항목(Ⅲ)을 선택하면, 식별 컨텐츠(Ⅰ), 비밀 번호(Ⅱ) 및 제1 디바이스(100)에 대한 디바이스 정보가 서버(1000)로 전송된다(S210). 디바이스 정보는 제1 디바이스(100)에 저장되어 있는 고유 정보이며, 저장되어 있던 디바이스 정보는 식별 컨텐츠(Ⅰ) 및 비밀 번호(Ⅱ)와 같이 서버(1000)로 전송된다.

[0081] 사용자는 서버(1000)에 로그 인 후, 서버(1000)로 전송된 제1 디바이스(100)에 대한 식별 컨텐츠(Ⅰ)를 검색한다(S220). 도 9는 식별 컨텐츠 검색을 설명하기 위한 유저 인터페이스이다. 사용자가 별명을 입력하면, 서버(1000)는 사용자가 입력한 별명을 포함하거나 별명과 관련된 정지 영상을 보여줄 수 있다. 이 때, 정지 영상 상에는 하이라이트 또는 프레임과 같은 포커스(Ⅳ)가 위치할 수 있으며, 포커스(Ⅳ)는 사용자의 선택에 따라 정지 영상 상을 이동할 수 있다.

[0082] 사용자는 자신이 전송했던 식별 컨텐츠를 선택한 후, 비밀 번호를 이용하여 디바이스 정보를 등록한다(S230). 서버(1000)는 사용자가 선택한 식별 컨텐츠(Ⅰ)와 입력된 비밀 번호(Ⅱ)가 서로 대응되면, 식별 컨텐츠(Ⅰ)와 함께 전송되었던 디바이스 정보를 저장한다. 이로써, 디바이스 정보가 등록되어 서버(1000)는 디바이스 정보에 대응하는 디바이스와 관련하여 발생되는 이벤트 또는 정보를 사용자에게 제공할 수 있다.

[0083] 비록 본 발명의 몇몇 실시예들이 도시되고 설명되었지만, 본 발명이 속하는 기술분야의 통상의 지식을 가진 당업자라면 본 발명의 원칙이나 정신에서 벗어나지 않으면서 본 실시예를 변형할 수 있음을 알 수 있을 것이다. 발명의 범위는 첨부된 청구항과 그 균등물에 의해 정해질 것이다.

부호의 설명

[0084]

100	: 제1 디바이스	110	: 제1 통신부
120	: 제1 디바이스 저장부	130	: 제1 디바이스 통신부
140	: 제1 디바이스 제어부	150	: 제1 저장매체 접속부
200	: 제2 디바이스	210	: 제2 통신부

220 : 제2 디바이스 저장부 230 : 제2 디바이스 통신부

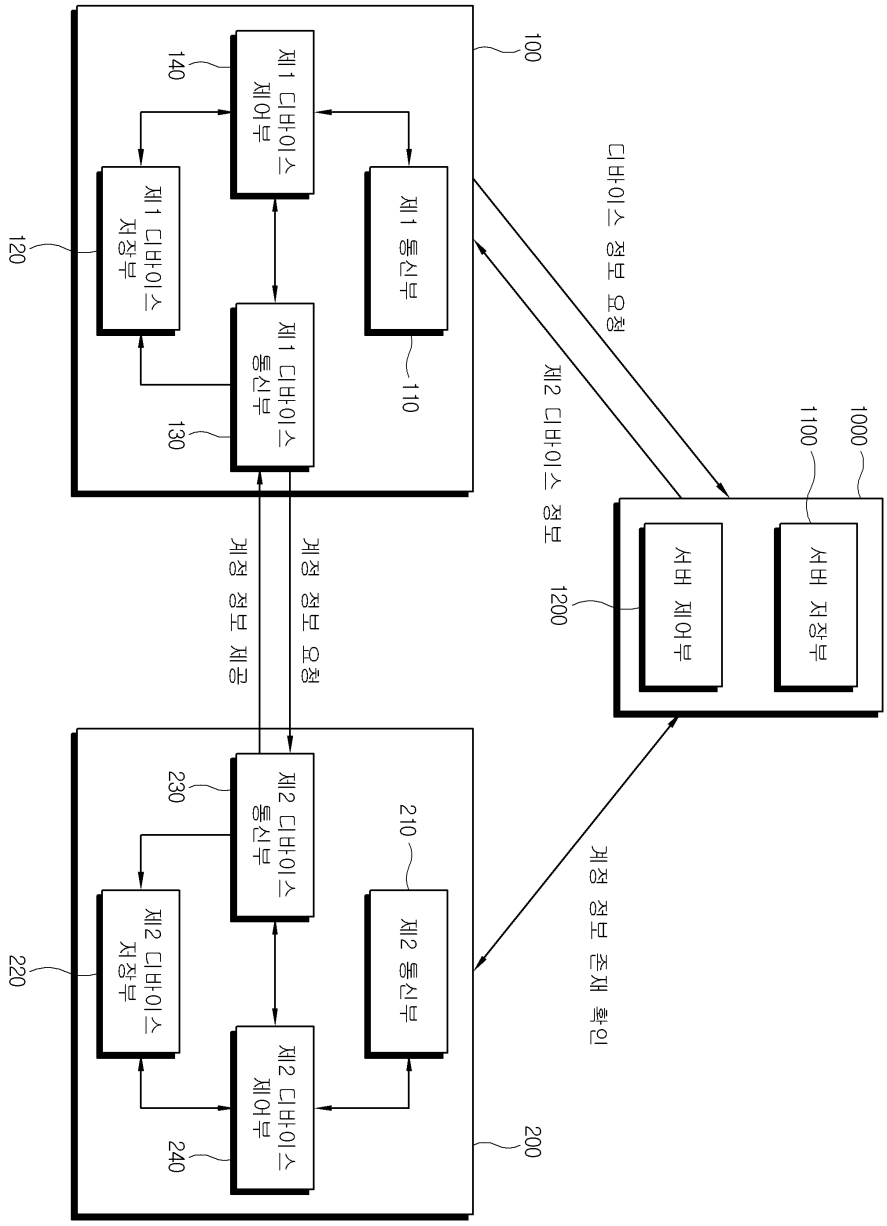
240 : 제2 디바이스 제어부 250 : 제2 저장매체 접속부

300 : 저장매체 1000 : 서버

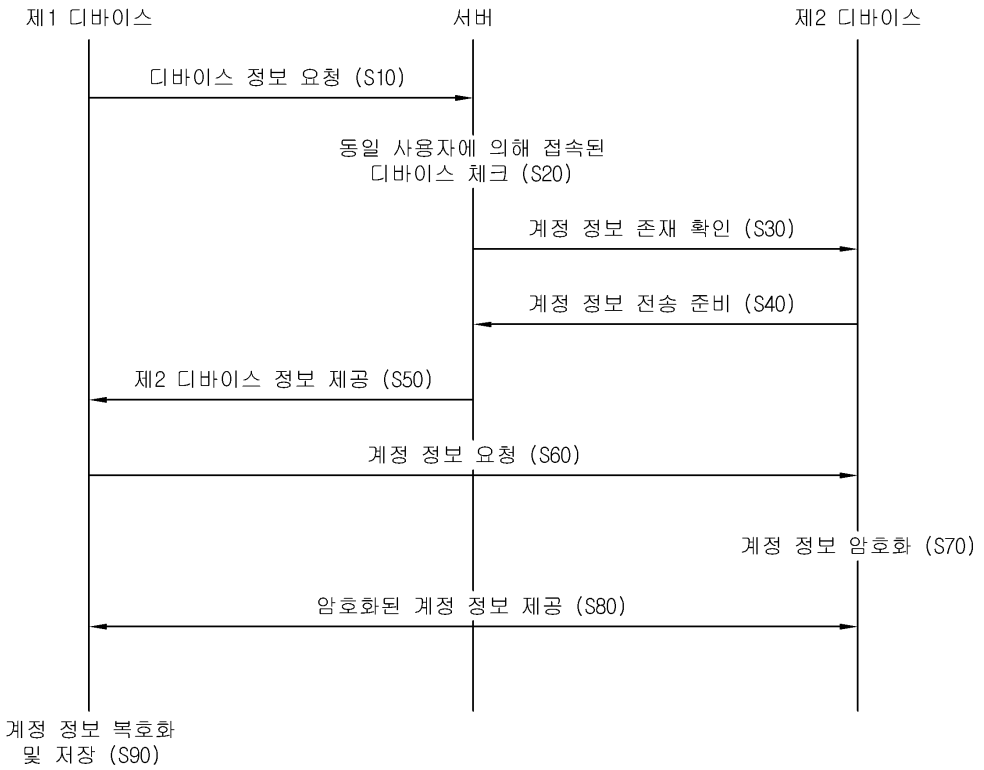
1100 : 서버 저장부 1200 : 서버 제어부

도면

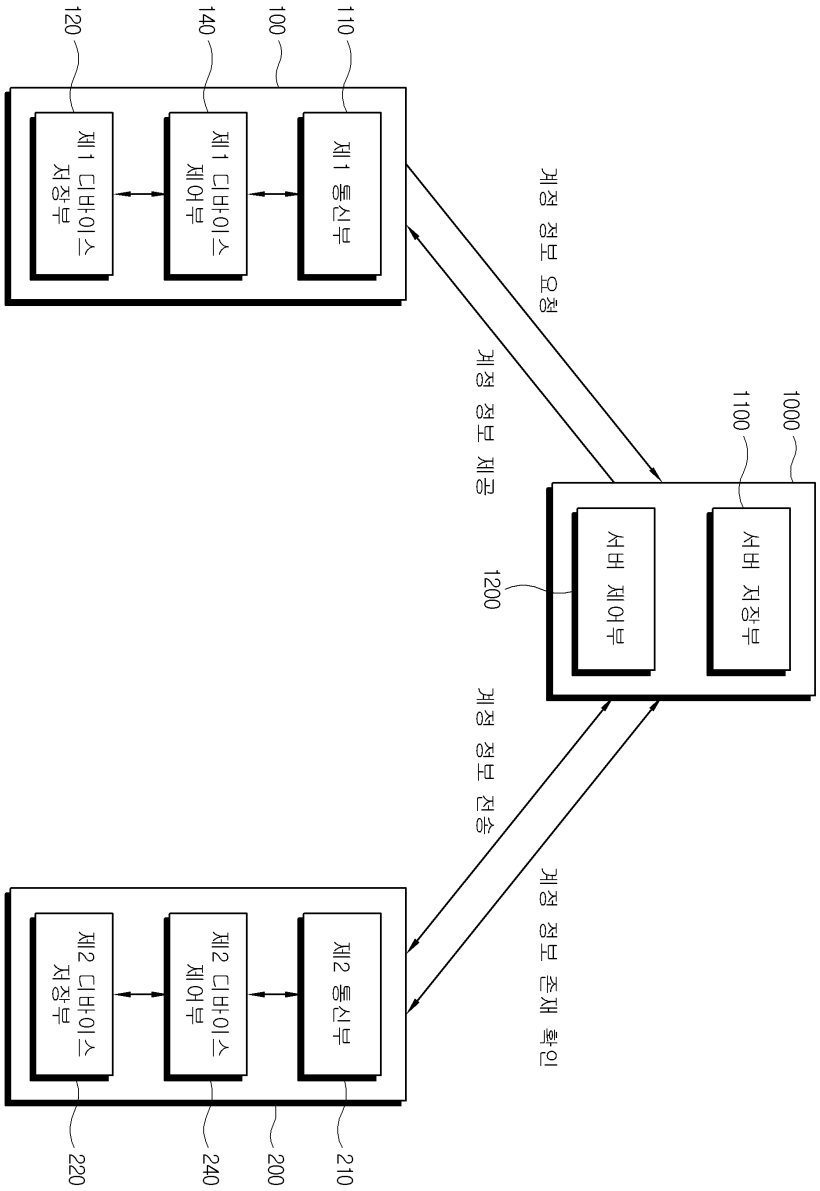
도면1



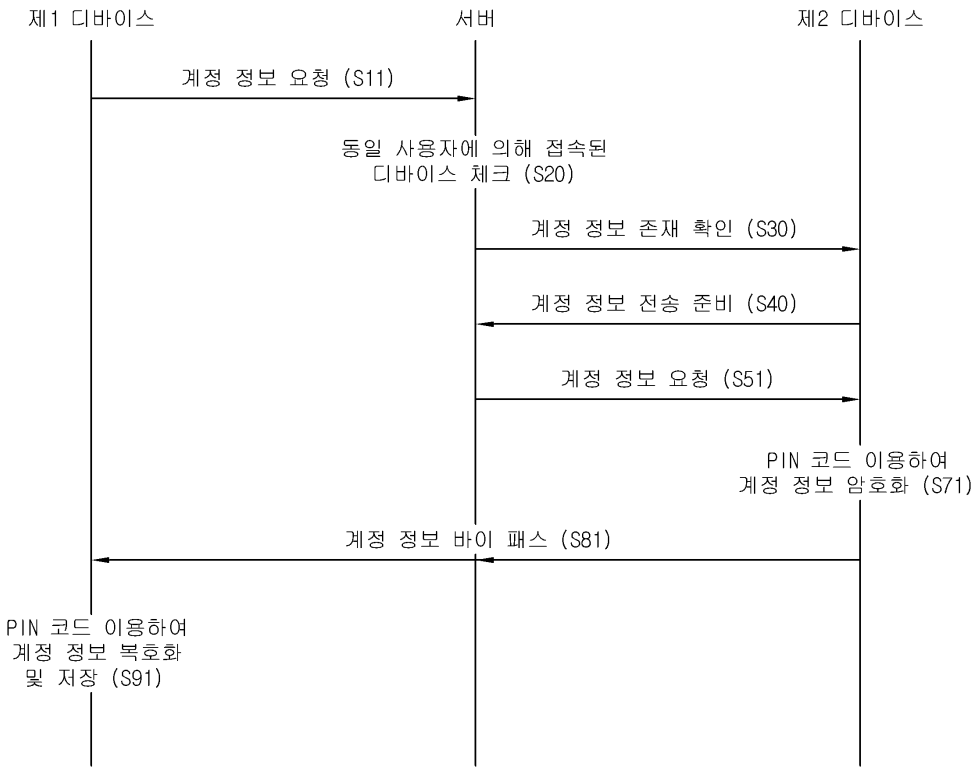
도면2


제1 디바이스
서버
제2 디바이스
디바이스 정보 요청 (S10)
동일 사용자에 의해 접속된
디바이스 체크 (S20)
계정 정보 존재 확인 (S30)
계정 정보 전송 준비 (S40)
제2 디바이스 정보 제공 (S50)
계정 정보 요청 (S60)
계정 정보 암호화 (S70)
암호화된 계정 정보 제공 (S80)
계정 정보 복호화
및 저장 (S90)

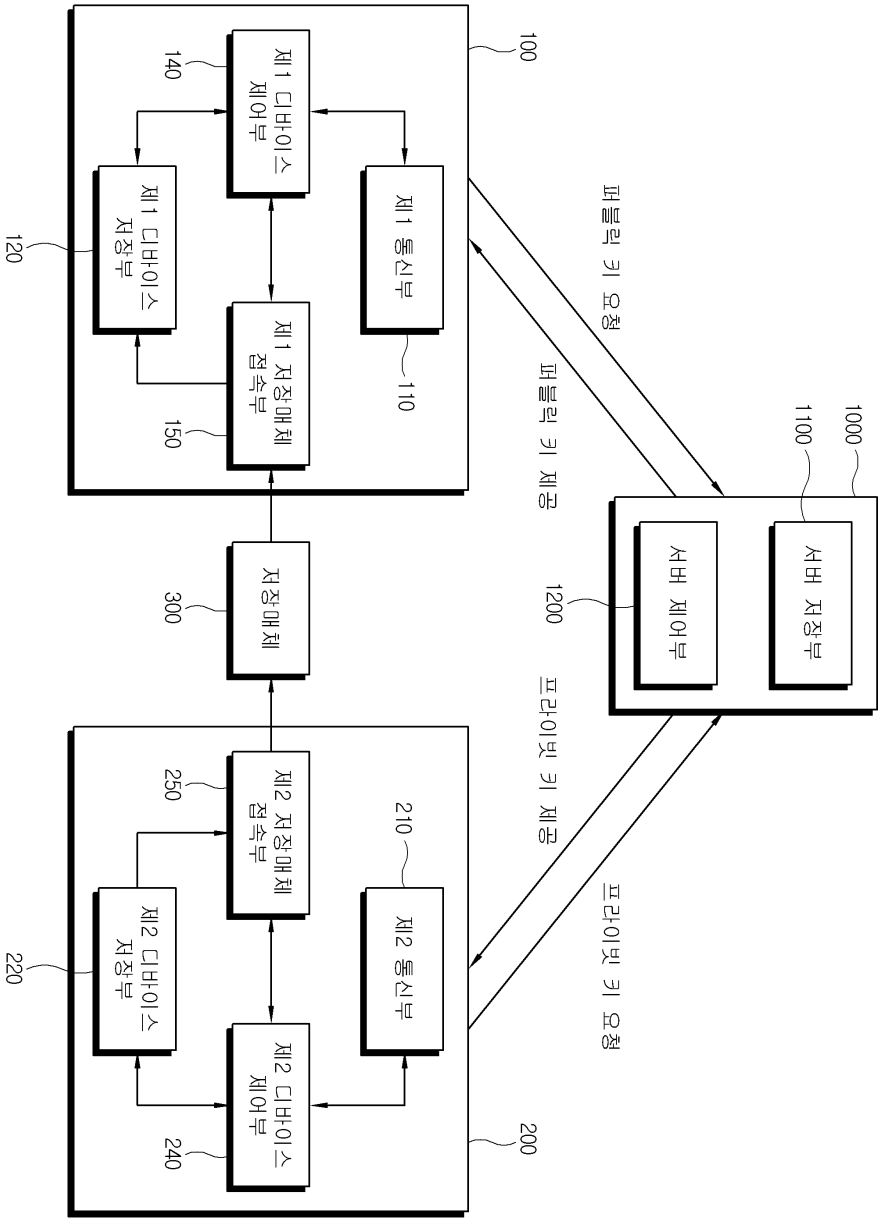
도면3


120
140
100
110
제1 디바이스 저장부
제1 디바이스 제어부
제1 통신부
계정 정보 요청
계정 정보 제공
1100
1000
서버 제어부
서버 저장부
1200
계정 정보 전송
계정 정보 존재 확인
제2 디바이스 저장부
제2 디바이스 제어부
제2 통신부
220
240
200
210

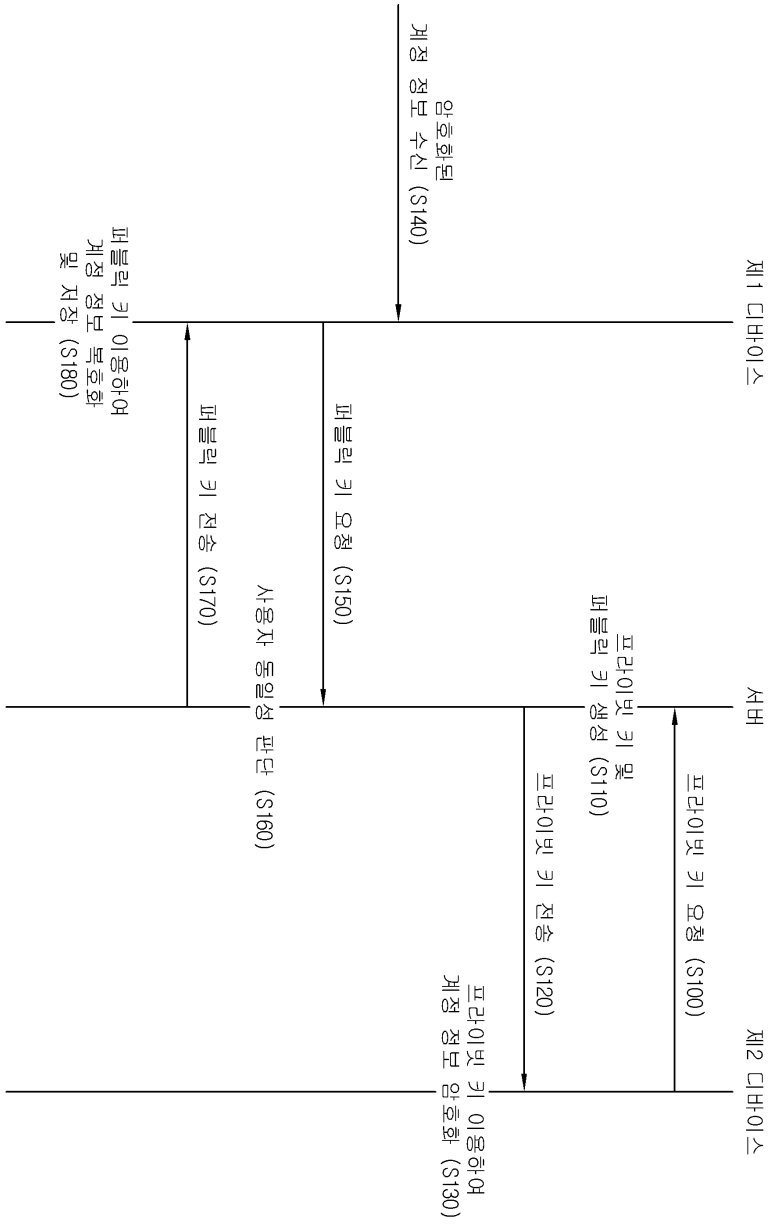
도면4


제1 디바이스
서버
제2 디바이스
계정 정보 요청 (S11)
동일 사용자에 의해 접속된
디바이스 체크 (S20)
계정 정보 존재 확인 (S30)
계정 정보 전송 준비 (S40)
계정 정보 요청 (S51)
PIN 코드 이용하여
계정 정보 암호화 (S71)
계정 정보 바이 패스 (S81)
PIN 코드 이용하여
계정 정보 복호화
및 저장 (S91)

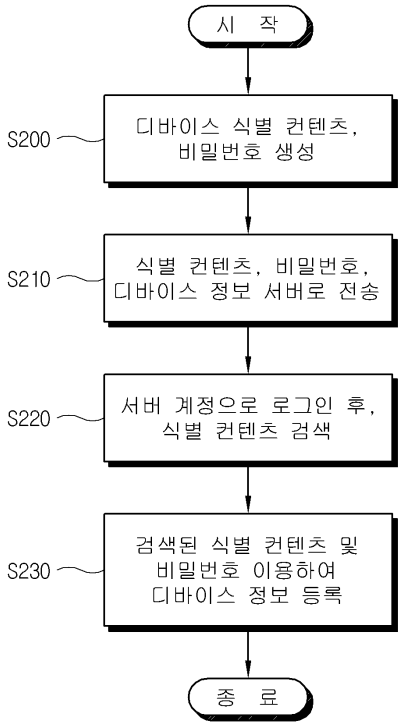
도면5


100
제1 디바이스 제어부
140
제1 디바이스 저장부
120
제1 저장매체 접속부
150
제1 통신부
110
퍼블릭 키 요청
퍼블릭 키 제공
1000
1100
서버 저장부
서버 제어부
1200
저장매체
300
프라이빗 키 제공
프라이빗 키 요청
제2 저장매체 접속부
250
제2 디바이스 저장부
220
제2 디바이스 제어부
240
제2 통신부
210
200

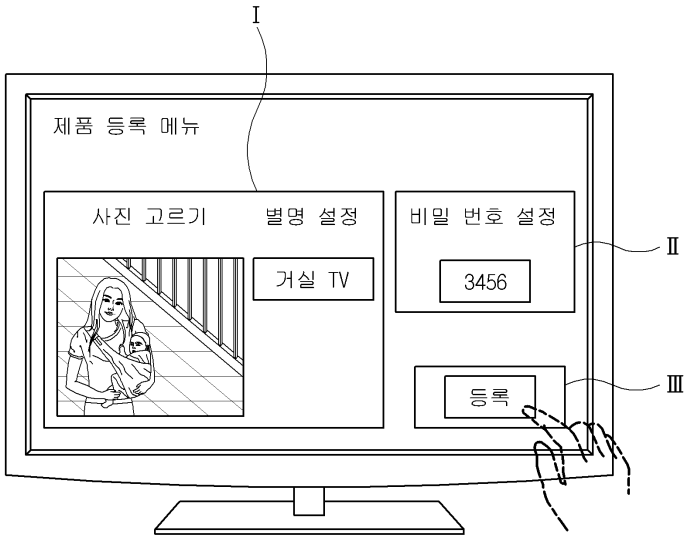
도면6


제1 디바이스
서버
제2 디바이스
프라이빗 키 요청 (S100)
프라이빗 키 및 퍼블릭 키 생성 (S110)
프라이빗 키 전송 (S120)
프라이빗 키 이용하여 계정 정보 암호화 (S130)
암호화된 계정 정보 수신 (S140)
퍼블릭 키 요청 (S150)
사용자 동일성 판단 (S160)
퍼블릭 키 전송 (S170)
퍼블릭 키 이용하여 계정 정보 복호화 및 저장 (S180)

도면7


시 작
S200
디바이스 식별 컨텐츠, 비밀번호 생성
S210
식별 컨텐츠, 비밀번호, 디바이스 정보 서버로 전송
S220
서버 계정으로 로그인 후, 식별 컨텐츠 검색
S230
검색된 식별 컨텐츠 및 비밀번호 이용하여 디바이스 정보 등록
종 료

도면8


I
제품 등록 메뉴
사진 고르기
별명 설정
거실 TV
비밀 번호 설정
3456
Ⅱ
등록
Ⅲ

도면9