(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0036613
(43) 공개일자 2010년04월08일

(51) Int. Cl.
H04N 7/167 (2006.01) *H04N 7/16* (2006.01)
(21) 출원번호 10-2008-0095918
(22) 출원일자 2008년09월30일
심사청구일자 없음

(71) 출원인
세종대학교산학협력단
서울 광진구 군자동 98 세종대학교
(72) 발명자
신동규
서울 서초구 서초2동 우성5차아파트 501-502 502-1102
이영렬
서울특별시 송파구 가락동 192 극동APT 1-704
신동일
서울 송파구 신천동 롯데캐슬골드아파트 101동 2107호

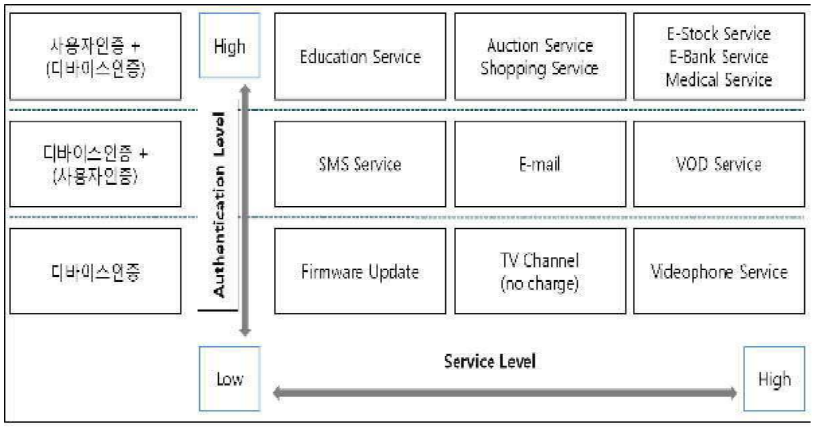
전체 청구항 수 : 총 4 항

(54) ＩＰＴＶ 인증 정책과 서비스 시나리오

(57) 요 약

IPTV는 기존의 DTV와 인터넷환경에서 가능한 거의 모든 서비스를 제공한다. 하지만 IPTV의 입력장치가 현재로서는 리모컨처럼 단순한 기기이기 때문에 사용자가 원하는 다양한 입력을 표현하기에는 다소 무리가 있으므로 디바이스인증이나 사용자인증을 통한 간단명료한 인증장치가 필요하다. IPTV 인증 정책 및 서비스 시나리오는 IPTV 서비스 계층에 맞게 Level 1 디바이스 인증, Level 2 디바이스인증+(사용자인증), Level 3 사용자인증+(디바이스인증)을 적용한 간단명료한 인증정책 이다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	11098
부처명	서울시
연구사업명	서울시 산학연 협력사업(2006년 서울시 신기술 연구개발 지원사업)
연구과제명	차세대 DMB/DTV를 위한 비디오 압축기술 및 저작권관리 시술 연구
주관기관	세종대학교 산학협력단
연구기간	2006.12.01 ~ 2008.11.30

특허청구의 범위

청구항 1

IPTV 서비스레벨과 인증레벨을 조합하여 구성한 서비스 계층도;

상기 서비스 계층도에 적용한 3단계 인증 정책;

상기 인증 정책에 Level 1 디바이스 인증;

상기 인증 정책에 Level 2 디바이스인증+(사용자인증);

상기 인증 정책에 Level 3 사용자인증+(디바이스인증)

청구항 2

제 1 항에 있어서, Firmware update 및 TV chanel(flat rate) IPTV 서비스에 적용한 디바이스인증 인증 정책

청구항 3

제 1 항에 있어서, 문자메시지(SMS)및 E-mail IPTV서비스에 적용한 디바이스+(사용자인증) 인증 정책

청구항 4

제 1 항에 있어서, 의료정보 IPTV서비스에 적용한 사용자인증+(디바이스인증) 인증 정책

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 IPTV 서비스에서의 인증방법이며, 보안기술 중 인증기술 분야에 속한다. 국내 인증 기술로는 ETRI 정보보호연구단에서 개발한 PKI 기술이 PKI 업체 등에 기술이전이 되어, 인터넷 뱅킹, 사이버증권 거래 등의 보안을 위해 활용되고 있다. 그리고 사용자 인증을 위한 생체인증기술의 활용성이 증가하고 있어, 향후 PKI 또는 보안 IC카드 등과 연계하여 새로운 기술로 발전할 것이다.

[0002] 국외 인증 기술로는 미국의 FPKI, 캐나다의 GOC PKI, 호주의 PKAF, 유럽의 ICE-TEL등 국가차원의 PKI 체계를 구축하고 있다. 또한 미국의 생체여권과 같이 사용자 인증을 위한 생체 인식기술이 활성화되고 있다.

배 경 기 술

[0003] 본 발명은 IPTV 서비스에서 효율적인 인증정책을 위해 디바이스인증과 사용자인증을 조합하여 IPTV 서비스 계층에 맞게 Level 1 디바이스 인증, Level 2 디바이스인증+(사용자인증), Level 3 사용자인증+(디바이스인증)을 적용하여 간단명료한 인증정책 및 서비스 시나리오를 제공한다.

[0004] IPTV, IPTV STB, Home Server/Gateway 등의 홈 네트워크의 중심적인 역할을 하는 댁내 디바이스에 사용자 인증서를 저장하는 방식은, 인증서의 보관 및 디바이스의 펌웨어와 사용자 인증서의 업데이트에는 용이하나, 이동성이 부족하여 사용자로 하여금 불편을 초래할 수 있다.

[0005] 이동식 저장장치(USB메모리, 휴대폰, PDA등)를 이용해 사용자 인증서를 저장하는 방식으로, 댁내 디바이스에 사용자 인증서를 저장하는 방식보다 사용자의 이동성을 월등히 보장한다. 하지만 저장장치의 분실 우려와 타인에 의한 악의적인 사용을 초래할 수도 있다. 현재는 이동식 저장장치에 생체인식 기술을 도입하여 분실했을 경우에도 타인에 의한 사용을 차단하는 방법이 있지만, 추가비용의 문제로 보편화 되어 있지 않다.

[0006] 사용자 인증서의 "댁내 디바이스 저장"과 "이동식 저장장치 저장" 방식의 장단점을 고루 수용하여 사용자 중심의 편리한 인증서비스를 제공하기 위해 고안된 방식이다. 전자 상거래시에 필요한 사용자 인증서를 공인된 기관(웹서버)에 통합적으로 모아 관리함으로서 사용자로 하여금 이동성을 확보해 주고, 저장장치의 분실에 따른 부수적인 위험부담을 줄여주며, 통합적인 인증서 관리가 용이하다. 하지만 키 로밍 서버의 보안이 보장되어야 하고, 인증서의 안정성에 대한 사용자의 거부감이 문제시 된다.

[0007] 디바이스 인증에서 키 생성 방식은 디바이스 제품 출시 시에 각 기기마다 고유의 인증넘버를 가지고 있으며, 사용자의 요청에 따라서 해당 서비스 제공자에게 등록되어 인증 요구 시 추출되어 사용함으로서 저장 개념이 불필요하다. BIOS Level에서 생성되어 외부 침입으로부터 높은 안정성을 보인다. 비밀번호와 사용자 인증서 등을 사용하는 인증 솔루션의 경우, 사용자의 액세스를 관리 하는데 중요한 툴이지만 단지 사용자의 신원확인을 해 줄 뿐이다. 사용자가 적합한 사람이라고 판단되면 사용하는 디바이스에 상관없이 해당 네트워크에 접속할 수 있다. 알려지지 않거나 관리되지 않은 디바이스가 네트워크에 접속할 경우, 바이러스에 대한 통로를 제공하는 셈이 되며 다른 악성 코드나 바이러스가 침투할 가능성도 높아진다. 이러한 위험 요소를 최소화하고 관리하기 위해 네트워크와 보안 정책을 준수하는 신뢰성 있는 디바이스만이 네트워크와 리소스에 접근하도록 해야 한다. 사용자와 디바이스를 모두 입증하는 방법만이 진정한 보안을 제공할 수 있으며, 이를 기업으로 네트워크 보안을 강화 할 수 있다.

[0008] 디바이스 인증에서 인증키 분배 방식은 PKI방식과 유사하게 공인 인증기관에서 관리하는 방식으로 디바이스 제작사가 공인인증기관에 인증서 발급을 요청하면 인증기관에서는 제작사의 공개키를 이용하여 키쌍 및 디바이스 인증서를 암호화 한 뒤 디바이스 제작사에게 전달한다. 디바이스 사용자는 그것을 개인키로 복호화 하여 디바이스에 키와 인증서를 탑재한다.

발명의 내용

해결 하고자하는 과제

[0009] 본 발명이 이루고자 하는 기술적 과제는 IPTV에서 제공되는 다양한 서비스가 리모컨처럼 단순한 기기로는 사용자가 원하는 다양한 입력을 표현하기에는 다소 무리가 있으므로 디바이스인증과 사용자인증을 조합하여 간단명료한 인증장치를 구현하는 것이다.

[0010] 본 발명의 목적들은 이상에서 언급한 목적들로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제 해결수단

[0011] 상기 목적을 달성하기 위하여, 본 발명의 일 실시예에 따른 IPTV 인증 정책 및 서비스 시나리오는 IPTV 서비스 계층에 맞게 Level 1 디바이스 인증, Level 2 디바이스인증 + (사용자인증), Level 3 사용자인증 + (디바이스인증)을 적용하여 간단명료한 인증정책 및 서비스 시나리오를 구현한다.

효 과

[0012] 상기한 바와 같은 본 발명의 IPTV 인증 정책 및 서비스 시나리오에 따르면 다음과 같은 효과가 있다.

[0013] 첫째, IPTV 등 신규 홈네트워크 환경에서의 인증 시스템 구축을 위한 구체적인 아키텍처를 제시한다는 장점이 있다.

[0014] 둘째, IPTV 등 신규 홈네트워크 환경에서의 사용자 인증 및 접근제어에 대한 표준적인 적용지침을 제시한다는 장점이 있다.

[0015] 셋째, 저렴한 IPTV 인증 환경을 정착 시킬 수 있다는 장점도 있다.

발명의 실시를 위한 구체적인 내용

[0016] 상기 목적을 달성하기 위하여, 본 발명의 일 실시예에 따른 IPTV 인증 정책 및 서비스 시나리오는 IPTV 서비스 계층에 맞게 Level 1 디바이스 인증, Level 2 디바이스인증 + (사용자인증), Level 3 사용자인증 + (디바이스인증)을 적용하여 간단명료한 인증정책 및 서비스 시나리오를 구현한다.

[0017] 기타 실시예들의 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

[0018] 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.

[0019] 이하, 본 발명의 실시예들에 의하여 IPTV 인증 정책 및 서비스 시나리오를 설명하기 위한 도면들을 참고하여 본 발명에 대해 설명하도록 한다.

[0020] 먼저, IPTV 서비스 계층 에 대하여 설명을 한다.

[0021] 도 1은 다양한 서비스의 중요도에 따라 사용자인증과 디바이스인증을 이용한 서비스 계층 도면이다. IPTV는 기존의 DTV와 인터넷환경에서 가능한 거의 모든 서비스를 제공한다. 하지만 IPTV의 입력장치가 현재로서는 리모컨처럼 단순한 기기이기 때문에 사용자가 원하는 다양한 입력을 표현하기에는 다소 무리가 있으므로 디바이스인증이나 사용자인증을 통한 간단명료한 인증장치가 필요하다. IPTV 인증 정책 및 서비스 시나리오는 IPTV 서비스 계층에 맞게 Level 1 디바이스 인증, Level 2 디바이스인증+(사용자인증), Level 3 사용자인증+(디바이스인증)을 적용하여 간단명료한 인증정책 및 서비스 시나리오를 구현한다.

[0022] 상기 IPTV 서비스 계층도를 통해 IPTV 인증 정책 및 서비스 시나리오를 설명 한다. 먼저, IPTV 서비스계층에서 Level 1인 디바이스 인증 해당하는 부분에 대하여 설명을 한다. IPTV의 다양한 서비스 중에서 큰 금액이 부가되지 않거나, 프라이버시 침해의 우려가 없는 낮은 레벨의 서비스들을 디바이스인증만을 사용해 제공하는 인증 정책이다.

[0023] 도 2는 IPTV의 STB 내에 필수적인 펌웨어를 업데이트 하는 내용으로서, 사용자 인증서가 필요 없이 디바이스 인증서만으로 인증을 하고 업데이트를 진행하는 과정의 도면이다.

[0024] 설치가 필수적인 펌웨어를 업데이트 하는 내용으로서 사용자는 "확인"만 해주면 되는 상황이다. 디바이스인증에 대한 요청은 사용자의 개입 없이 제작사와 사용자의 STB간에 이루어진다. STB제작사가 IP망을 이용하여 사용자측의 STB의 펌웨어와 디바이스 인증을 요청한다(1). 사용자측의 STB는 자신의 디바이스 내에서 키를 생성하여 펌웨어버전과 함께 STB제작사에게 보낸다(2). 펌웨어의 업데이트 필요성을 확인한 제작사는 사용자에게 업데이트 할 것임을 "확인"시킨다(3). 사용자는 업데이트 내용을 "확인" 했음을 STB제작사 측에 전달한다(4). STB제작사는 사용자측의 STB펌웨어 업데이트가 인가되었음을 인지하고, 데이터 DB를 통하여 사용자측의 STB의 펌웨어를 업데이트 한다(5).

[0025] 도 3은 IPTV의 기본채널은 정액(flat rate)의 개념으로 서비스 될 것으로 예상되므로, 사용자 권리를 얻기 위한 "정액제도 신청"을 제외하고, 해당 서비스 기간의 기본채널 시청은 디바이스인증 만으로 서비스를 진행하는 과정의 도면이다.

[0026] 사용자가 IPTV를 켜고, 방송국에 접근하려한다(1). 방송국 측에서는 접근하려는 사용자가 정당한 가입자인지 확인하기 위하여 사용자의 디바이스에 인증정보를 요청한다(2). 사용자의 IPTV STB는 자신의 인증키를 생성하여 방송국의 디바이스 인증 서버에 전송한다(3). 정당한 사용자임이 확인된 후 스트리밍 서버를 통하여 방송 서비스를 제공한다(4). (3) 번의 동작은 방송국의 정책이나 서비스의 내용에 따라서 (1)과 통합되어 진행될 수 있다.

[0027] 상기 IPTV 서비스계층 Level 1에 보다 강한인증 단계인 IPTV 서비스계층 Level 2인 디바이스인증+(사용자인증)에 대하여 설명을 한다. 서비스의 이용료가 낮고, 보편적인 서비스라도 프라이버시 문제나 누적되는 이용료 때문에 서비스사용자의 인증이 필요한 경우가 있다. 이런 경우 사용자인증을 옵션으로 사용하여 서비스에 관한 인증 절차를 강화할 필요가 있다.

[0028] 도 4는 문자메시지(SMS)를 IPTV를 통하여 보내는 서비스 시나리오에서, 일정금액(저가상품)내의 서비스는 디바이스 인증만으로도 가능하며 한도가 넘을 경우 사용자인증을 통하여 추가적인 인증을 받는 과정의 도면이다.

[0029] 사용자가 IPTV를 이용하여(1) SMS를 보내려 한다. 방송국의 디바이스인증서버는 사용자의 디바이스인증을 요청하고(2) 사용자의 STB는 해당 내용을 디바이스인증서버로 보내어 인증 받는다. 방송국은 SMS를 보내기 위해 해당 내용을 통신사로 보냈으나(3), SMS서비스의 한도 금액이 초과되었음을 파악하고, 방송국을 통해 사용자에게 알린다(1). 사용자는 사용자인증서를 제공하고(4), 추가적인 SMS 서비스를 결제한다. 통신사는 SMS서비스를 제공한 뒤에, 결제 내역과 서비스가 완료 되었음을 알리는 정보를 사용자에게 전달한다 (3), (1).

[0030] 도 5는 E-mail 서비스는 현재와 같이 ID와 Password 입력 등의 간략한 사용자 확인 작업만을 사용하여 접근제어가 가능 하지만, 사내의 기밀문서나 개인적인 사항이 있을 때는 보안의 수준을 더욱 높여 인증하는 과정의 도면이다.

[0031] 사용자가 IPTV를 이용하여 E-mail을 확인하려 한다(1). 포털사이트의 디바이스인증서버는 사용자측에 디바이스인증 자료를 요청하고(2), 사용자의 STB는 인증키를 디바이스인증서버에게 제공한다(3). 디바이스인증 후에,

E-mail Server에서 사용자에게 해당 메일 내용을 제공한다(4). 사용자가 E-mail을 확인 하던 중, 지난달에 받은 종합검진의 결과가 포함되어 있었고, 개인적인 사항이 들어있는 E-mail이기 때문에 디바이스인증 만으로는 확인할 수 없다. 사용자는 메일 확인을 위하여 사용자인증정보를 포털사이트 측에 보내게 되고(1), E-mail Server는 사용자인증을 거친 후 E-mail내용을 사용자에게 재전송 한다(4).

[0032] 마지막으로 IPTV 서비스계층 Level 3에 해당하는 사용자인증+(디바이스인증)에 대하여 설명을 한다.

[0033] 도 6은 의료정보는 매우 개인적인 사안이므로, 타인에게 쉽게 공개 되어서는 안 되기 때문에 디바이스 인증만으로는 부족하여, 필수적으로 사용자인증을 사용한 인증 과정의 도면이다.

[0034] 사용자는 지난달에 받은 건강검진의 결과를 확인하기 위하여 IPTV 서비스인 Medical Service에 접근하려 한다(1). 방송사는 해당 서비스의 인터페이스를 제공하여 사용자가 병원에 접근하도록 돕는다(2). 병원 측에서는 사용자가 원하는 정보에 접근하기 위해서는 사용자인증정보가 필요함을 알리고, 해당 정보를 전달 받아 인증한다(3). 올바른 사용자임이 확인되면, 방송사를 통해서 사용자가 원하는 의료정보를 제공한다(2)(4).

산업이용 가능성

[0035] 상기한 바와 같은 본 발명의 IPTV 인증 정책 및 서비스 시나리오에 따르면 다음과 같은 산업상 이용가능성이 하나 혹은 그 이상 있다.

[0036] 첫째, 저렴한 IPTV 인증환경을 정착 시키는데 이용될 수 있다.

[0037] 둘째, 다수의 사용자에 대한 인증의 간소화를 도모해 IPTV 및 홈 네트워크시장의 활성화 기여에 이용될 수 있다.

[0038] 셋째, 안전하고 효율적인 신규 홈네트워크 서비스 인증 메커니즘 개발에 이용될 수 있다.

도면의 간단한 설명

[0039] 도 1은 다양한 서비스의 중요도에 따라 사용자인증과 디바이스인증을 이용한 서비스 계층 도면이다.

[0040] 도 2는 IPTV의 STB 내에 필수적인 펌웨어를 업데이트 하는 내용으로서, 사용자 인증서가 필요 없이 디바이스 인증서만으로 인증을 하고 업데이트를 진행하는 과정의 도면이다.

[0041] 도 3은 IPTV의 기본채널은 정액(flat rate)의 개념으로 서비스 될 것으로 예상되므로, 사용자 권리를 얻기 위한 "정액제도 신청"을 제외하고, 해당 서비스 기간의 기본채널 시청은 디바이스인증 만으로 서비스를 진행하는 과정의 도면이다.

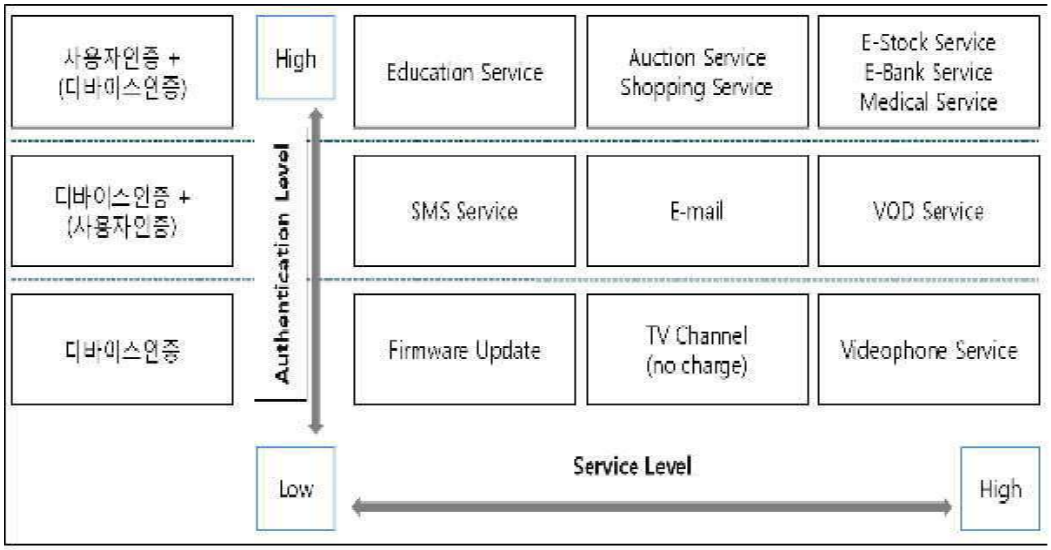
[0042] 도 4는 문자메시지(SMS)를 IPTV를 통하여 보내는 서비스 시나리오에서, 일정금액(저가상품)내의 서비스는 디바이스 인증만으로도 가능하며 한도가 넘을 경우 사용자인증을 통하여 추가적인 인증을 받는 과정의 도면이다.

[0043] 도 5는 E-mail 서비스는 현재와 같이 ID와 Password 입력 등의 간략한 사용자 확인 작업만을 사용하여 접근제어가 가능 하지만, 사내의 기밀문서나 개인적인 사항이 있을 때는 보안의 수준을 더욱 높여 인증하는 과정의 도면이다.

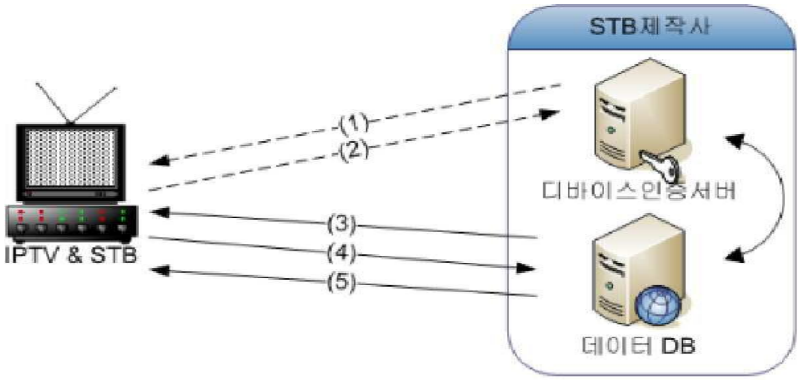
[0044] 도 6은 의료정보는 매우 개인적인 사안이므로, 타인에게 쉽게 공개 되어서는 안 되기 때문에 디바이스 인증만으로는 부족하여, 필수적으로 사용자인증을 사용한 인증 과정의 도면이다.

도면

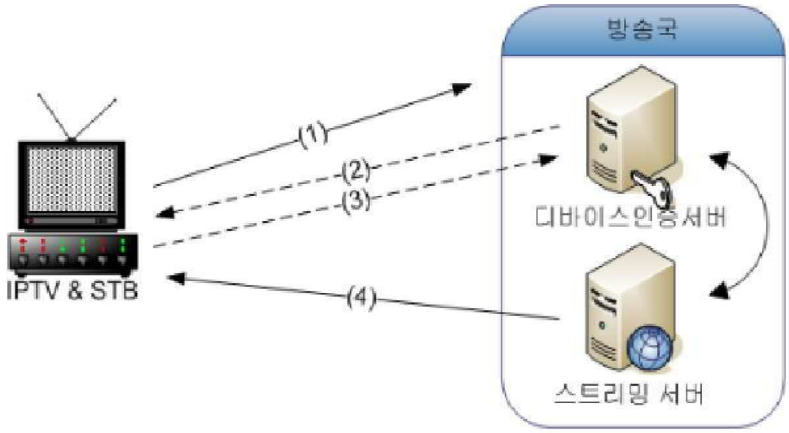
도면1



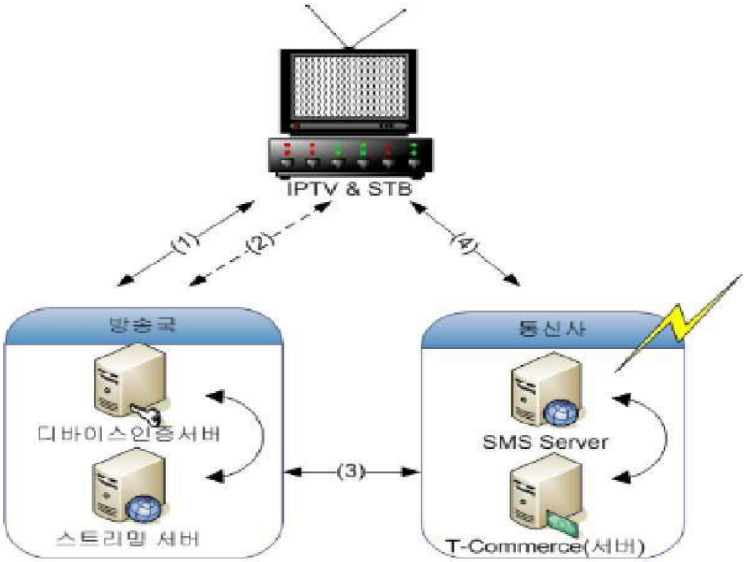
도면2



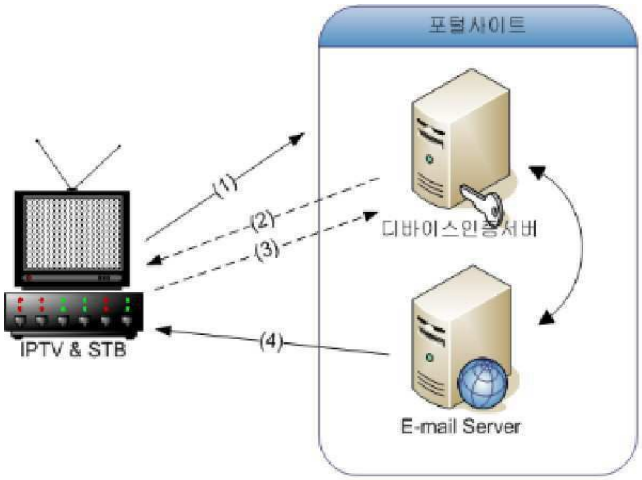
도면3



도면4


IPTV & STB
(1)
(2)
(4)
방송국
디바이스인증서버
스트리밍 서버
(3)
통신사
SMS Server
T-Commerce(서버)

도면5


포털사이트
디바이스인증서버
(1)
(2)
(3)
IPTV & STB
(4)
E-mail Server

도면6

