

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구  
국제사무국



PCT



(10) 국제공개번호

WO 2010/062028 A3

(43) 국제공개일  
2010년 6월 3일 (03.06.2010)

- (51) 국제특허분류:  
H04N 7/16 (2006.01)
- (21) 국제출원번호: PCT/KR2009/005230
- (22) 국제출원일: 2009년 9월 15일 (15.09.2009)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:  
10-2008-0117399 2008년 11월 25일 (25.11.2008) KR
- (71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **충남대학교 산학협력단 (THE INDUSTRY & ACADEMIC COOPERATION IN CHUNGNAM NATIONAL UNIVERSITY (IAC))** [KR/KR]; 대전 유성구 궁동 220 충남대학교, 305-764 Daejeon (KR).
- (72) 발명자: **김**
- (75) 발명자/출원인 (US 에 한하여): **류재철 (RYOU, Jaechul)** [KR/KR]; 대전광역시 유성구 어은동 한빛아파트 1032-801, 305-755 Daejeon (KR). **이중후 (LEE,**

**Jonghoo)** [KR/KR]; 대전광역시 유성구 관평동 대덕테크노밸리아파트 504-301, 305-509 Daejeon (KR). **김민영 (KIM, Minyoung)** [KR/KR]; 충청남도 천안시 서북구 입장면 하장리 초원아파트 105-605, 330-827 Chungcheongnam-do (KR).

(74) 대리인: **김원준 (KIM, Wonjoon)**; 대전광역시 서구 만년동 386 골드벤처타워 205호, 302-823 Daejeon (KR).

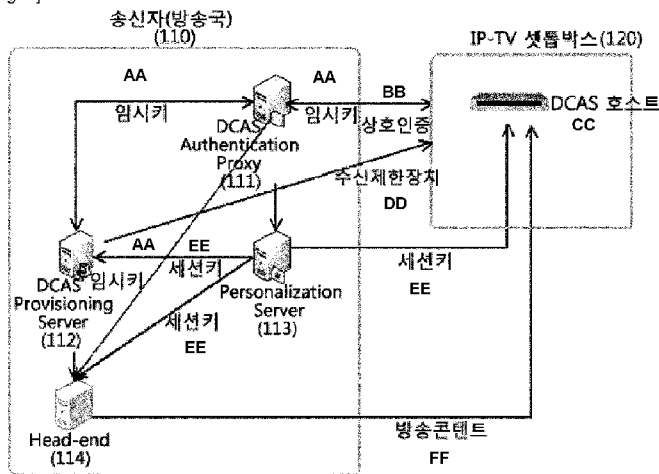
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[다음 쪽 계속]

(54) Title: METHOD FOR DOWNLOADING CONDITIONAL ACCESS SYSTEM FOR DIGITAL BROADCASTING

(54) 발명의 명칭: 디지털 방송용 제한수신장치를 다운로드하는 방법

[Fig. 1]



AA ... Temporary key  
BB ... Mutual authentication  
CC ... DCAS host  
DD ... Conditional access system  
EE ... Session key  
FF ... Broadcast content

110 ... Transmitter (Broadcasting station)  
120 ... IP-TV set-top box  
114 ... Head-end  
112 ... Provisioning Server  
113 ... Personalization Server  
111 ... Authentication Proxy

(57) Abstract: The present invention provides a method for downloading a conditional access system in a broadcasting system in which a transmitter has a DCAS authentication proxy (AP), a personalization server, a DCAS provisioning server, and a head end, and in a digital broadcasting system in which a receiver has a set-top box including a DCAS host. The method for downloading a conditional access system for a digital broadcasting comprises (A) a mutual authentication between the DCAS AP and the DCAS host and key distribution process, (B) a mutual authentication between the DCAS personalization server and the DCAS host and key distribution process, and (C) a mutual authentication between the DCAS provisioning server and the DCAS host and key distribution process. The mutual authentication between the DCAS AP and the DCAS host and key distribution process includes: 1) a step of generating a common key from the license number input in the set-top box, 2) a step of performing a mutual authentication between the DCAS AP and the DCAS host by using the common key, and 3) a step of permitting the DCAS AP to generate a temporary key (TK) and distribute the generated key to the DCAS host and the personalization server, when the mutual authentication is finished. The mutual authentication between the DCAS personalization server and the DCAS host and key distribution process includes: 1) a step of performing a mutual authentication between the personalization server and the DCAS host by using the temporary key, and 2) a step of permitting the personalization server to generate a session key (SK) and distribute the generated key to the DCAS host and the DCAS provisioning server, when the mutual authentication is finished. The mutual authentication between the DCAS provisioning server and the DCAS host and key distribution process includes: 1) a step of permitting the DCAS provisioning server to encode a conditional access system software by using the session key (SK) and transmitting the encoded software to the DCAS host, and 2) a step of permitting the DCAS host to decode the conditional access system software by using the session key (SK) and installing the software.

performing a mutual authentication between the personalization server and the DCAS host by using the temporary key, and 2) a step of permitting the personalization server to generate a session key (SK) and distribute the generated key to the DCAS host and the DCAS provisioning server, when the mutual authentication is finished. The mutual authentication between the DCAS provisioning server and the DCAS host and key distribution process includes: 1) a step of permitting the DCAS provisioning server to encode a conditional access system software by using the session key (SK) and transmitting the encoded software to the DCAS host, and 2) a step of permitting the DCAS host to decode the conditional access system software by using the session key (SK) and installing the software.

(57) 요약서:

[다음 쪽 계속]

WO 2010/062028 A3



(84) **지정국** (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**공개:**

- 국제조사보고서와 함께 (조약 제 21 조(3))
- 청구범위 보정 기한 만료 전의 공개이며, 보정서를 접수하는 경우 그에 관하여 별도 공개함 (규칙 48.2(h))

(88) **국제조사보고서 공개일:**

2010 년 7 월 15 일

본 발명은, 송신자측에 DCAS 인증프록시(AP), 개인화서버, DCAS 제공서버 및 헤드엔드를 포함하는 방송 시스템과, 수신자측에 DCAS 호스트를 포함하는 셋톱박스로 이루어진 디지털방송 시스템에서 제한수신장치를 다운로드하는 방법으로서, (A) ① 셋톱박스에 입력된 라이선스 번호로부터 공유키를 생성하는 단계와, ② 상기 공유키를 이용하여 DCAS AP와 DCAS 호스트가 상호인증하는 단계와, ③ 상호인증되면 DCAS AP가 임시키(TK)를 생성하여 DCAS 호스트와 개인화서버에게 배포하는 단계로 이루어지는 DCAS AP와 DCAS 호스트간의 상호인증 및 키 분배 과정; (B) ① 상기 임시키를 이용해서 개인화서버와 DCAS 호스트가 상호인증하는 단계와, ② 상호인증되면 개인화서버가 세션키(SK)를 생성하여 DCAS 호스트와 DCAS 제공서버에게 배포하는 단계로 이루어지는 DCAS 개인화서버와 DCAS 호스트간의 상호인증 및 키 분배 과정; (C) ① DCAS 제공서버가 상기 세션키(SK)로 제한수신장치 소프트웨어를 암호화하여 DCAS 호스트로 전송하는 단계와, ② DCAS 호스트가 상기 세션키(SK)를 이용하여 제한수신장치 소프트웨어를 복호화하고 이를 설치하는 단계로 이루어지는 DCAS 제공서버와 DCAS 호스트간의 상호인증 및 키 분배 과정;을 포함하는 디지털 방송용 제한수신장치를 다운로드하는 방법에 관한 것이다.

## INTERNATIONAL SEARCH REPORT

International application No.

**PCT/KR2009/005230****A. CLASSIFICATION OF SUBJECT MATTER****H04N 7/16(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

H04N 7/16; H04N 7/173

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models: IPC as above

Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: downloadable, CAS, key, message

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                      | Relevant to claim No. |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| A         | EP 1755340 A1 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 21 February 2007<br>See paragraphs [0026]-[0029] and figures 1-4.              | 1-5                   |
| A         | US 2008-0005326 A1 (HOWARD G. Pinder et al.) 03 January 2008<br>See paragraphs [0028]-[0043] and figures 3-5.                           | 1-5                   |
| A         | US 2008-0098212 A1 (HELMS WILLIAM L. et al.) 24 April 2008<br>See paragraphs [0170]-[0187], [0214], [0309]-[0310] and figures 2, 3g, 4. | 1-5                   |
| A         | US 2008-0177998 A1 (APSANGI SHRIKANT et al.) 24 July 2008<br>See paragraphs [0151]-[0177] and figures 2, 3.                             | 1-5                   |



Further documents are listed in the continuation of Box C.



See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;" document member of the same patent family

Date of the actual completion of the international search

10 MAY 2010 (10.05.2010)

Date of mailing of the international search report

**10 MAY 2010 (10.05.2010)**

Name and mailing address of the ISA/KR



Korean Intellectual Property Office  
Government Complex-Daejeon, 139 Seonsa-ro, Daejeon 302-701,  
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.

**PCT/KR2009/005230**

| Patent document<br>cited in search report | Publication<br>date | Patent family<br>member                                                  | Publication<br>date                                  |
|-------------------------------------------|---------------------|--------------------------------------------------------------------------|------------------------------------------------------|
| EP 1755340 A1                             | 21.02.2007          | CN 1977537 A<br>EP 1755340 A4<br>US 2007-0172059 A1<br>WO 2006-082812 A1 | 06.06.2007<br>09.05.2007<br>26.07.2007<br>10.08.2006 |
| US 2008-0005326 A1                        | 03.01.2008          | CA 2655620 A1<br>EP 2036349 A2<br>WO 2008-005791 A2<br>WO 2008-005791 A3 | 10.01.2008<br>18.03.2009<br>10.01.2008<br>09.10.2008 |
| US 2008-0098212 A1                        | 24.04.2008          | WO 2008-060388 A2<br>WO 2008-060388 A3                                   | 22.05.2008<br>16.10.2008                             |
| US 2008-0177998 A1                        | 24.07.2008          | NONE                                                                     |                                                      |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                    |                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>A. 발명이 속하는 기술분류(국제특허분류(IPC))</b><br><br><b>H04N 7/16(2006.01)i</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                    |                                                                                                                            |
| <b>B. 조사된 분야</b><br>조사된 최소문헌(국제특허분류를 기재)<br>H04N 7/16; H04N 7/173<br><br>조사된 기술분야에 속하는 최소문헌 이외의 문헌<br>한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC<br>일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                    |                                                                                                                            |
| 국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))<br>eKOMPASS(특허청 내부 검색시스템) & 키워드: downloadable, CAS, key, message                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                    |                                                                                                                            |
| <b>C. 관련 문헌</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                    |                                                                                                                            |
| 카테고리*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 인용문헌명 및 관련 구절(해당하는 경우)의 기재                                                                                         | 관련 청구항                                                                                                                     |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | EP 1755340 A1 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 2007.02.21<br>문단 [0026]-[0029] 및 도면 1-4 참조.               | 1-5                                                                                                                        |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | US 2008-0005326 A1 (HOWARD G. Pinder 외 3명) 2008.01.03<br>문단 [0028]-[0043] 및 도면 3-5 참조.                             | 1-5                                                                                                                        |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | US 2008-0098212 A1 (HELMS WILLIAM L. 외 2명) 2008.04.24<br>문단 [0170]-[0187], [0214], [0309]-[0310] 및 도면 2, 3g, 4 참조. | 1-5                                                                                                                        |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | US 2008-0177998 A1 (APSANGI SHRIKANT 외 5명) 2008.07.24<br>문단 [0151]-[0177] 및 도면 2, 3 참조.                            | 1-5                                                                                                                        |
| <input type="checkbox"/> 추가 문헌이 C(계속)에 기재되어 있습니다. <input checked="" type="checkbox"/> 대응특허에 관한 별지를 참조하십시오.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                    |                                                                                                                            |
| * 인용된 문헌의 특별 카테고리:<br>“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌<br>“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌<br>“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌<br>“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌<br>“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌<br>“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌<br>“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.<br>“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.<br>“&” 동일한 대응특허문헌에 속하는 문헌 |                                                                                                                    |                                                                                                                            |
| 국제조사의 실제 완료일<br>2010년 05월 10일 (10.05.2010)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                    | 국제조사보고서 발송일<br><b>2010년 05월 10일 (10.05.2010)</b>                                                                           |
| ISA/KR의 명칭 및 우편주소<br> 대한민국 특허청<br>(302-701) 대전광역시 서구 선사로 139,<br>정부대전청사<br>팩스 번호 82-42-472-7140                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                    | 심사관<br>조남신<br>전화번호 82-42-481-8589<br> |

국제조사보고서에서  
인용된 특허문헌

공개일

대응특허문헌

공개일

EP 1755340 A1

2007.02.21

CN 1977537 A

2007.06.06

EP 1755340 A4

2007.05.09

US 2007-0172059 A1

2007.07.26

WO 2006-082812 A1

2006.08.10

US 2008-0005326 A1

2008.01.03

CA 2655620 A1

2008.01.10

EP 2036349 A2

2009.03.18

WO 2008-005791 A2

2008.01.10

WO 2008-005791 A3

2008.10.09

US 2008-0098212 A1

2008.04.24

WO 2008-060388 A2

2008.05.22

WO 2008-060388 A3

2008.10.16

US 2008-0177998 A1

2008.07.24

없음