

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. 06517.P002C
(maximum 12 characters)First Named Inventor Luc Vantalou, et al.Title: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVERFiled by EFS-WEB on: September 12, 2012ADDRESS TO: Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450**APPLICATION ELEMENTS**

See MPEP chapter 600 concerning utility patent application contents.

1. ☐ Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)
2. ☐ Applicant Claims Small Entity Status. (37 CFR 1.27)
3. ☒ Specification (Total Pages 48)
(preferred arrangement set forth below)
 - Descriptive Title of the Invention
 - Cross Reference to Related Applications
 - Statement Regarding Fed sponsored R & D
 - Reference sequence listing, a table,
or a computer program listing appendix
 - Background of the Invention
 - Brief Summary of the Invention
 - Brief Description of the Drawings (if filed)
 - Detailed Description
 - Claim(s)
 - Abstract of the Disclosure
4. ☒ Drawings(s) (35 USC 113) (Total Sheets 19)
5. ☒ Oath or Declaration (Total Pages 3)
 - a. ☐ Newly Executed (Original or Copy)
 - b. ☒ Copy from a Prior Application (37 CFR 1.63(d))
(for Continuation/Divisional with Box 18 completed)
 - i. ☐ DELETIONS OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
 - c. ☐ Unsigned.
6. ☐ Application Data Sheet. (37 CFR 1.76)
7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix)
8. ☐ Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
 - a. ☐ Computer Readable Form (CRF)
 - b. ☐ Specification Sequence Listing on:
 - i. ☐ CD-ROM or CD-R (2 copies); or
 - ii. ☐ paper
 - c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. _____ Assignment Papers (cover sheet & documents(s))
10. _____ a. Separate 37 CFR 3.73(b) Statement (where there is an assignee)
 _____ b. Power of Attorney
11. _____ English Translation Document (if applicable)
12. _____ a. Information Disclosure Statement (IDS)/PTO-1449
 _____ b. Copies of IDS Citations
13. _____ Preliminary Amendment
14. _____ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
15. _____ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. _____ Nonpublication Request under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
- 17A. _____ Claim for Foreign Priority
- 17B. _____ Other: _____

17C. ☒ Pursuant to 37 C.F.R. 1.136(a)(3), applicant(s) hereby request and authorize the U.S. Patent and Trademark Office to (1) treat any concurrent or future reply that requires a petition for extension of time as incorporating a petition for extension of time for the appropriate length of time and (2) charge all required fees, including extension of time fees and fees under 37 C.F.R. 1.16 and 1.17, to Deposit Account No. 02-2666.

18. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title (e.g., by way of preliminary amendment), or in an Application Data Sheet Under 37 C.F.R. 1.76:

☒ Continuation _____ Divisional _____ Continuation-in-part (CIP)
 Of Prior Application No.: 11/007,116 Examiner Avery, Jeremiah L. Group Art Unit 2431
 (which is a _____ continuation/ _____ divisional/ _____ CIP of prior application no. _____,
 which is a _____ continuation/ _____ divisional/ _____ CIP of prior application no. _____) (List entire chain of priority)

Applicant(s): Also include a Preliminary Amendment to amend the specification to claim priority.

For CONTINUATION AND DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. Correspondence Address
☒ Customer Number or Bar Code Label 08791
 or
 _____ Correspondence Address Below
 (Insert Customer No. or Attach Bar Code Label here)

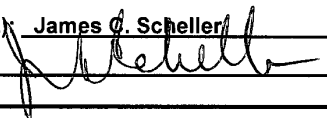
NAME James C. Scheller

ADDRESS BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
1279 Oakmead Parkway

CITY Sunnyvale STATE California ZIP CODE 94085

Country U.S.A. TELEPHONE (408) 720-8300 FAX (408) 720-8383

Name (PRINT/TYPE) James C. Scheller Registration No.: 31,195

Signature:  Date: September 12, 2012

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION (37 CFR 1.63)		Attorney Docket Number	6517P002
		First Named Inventor	Luc Vantalou
☒ Declaration Submitted with Initial Filing OR ☐ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16(e)) required)		COMPLETE IF KNOWN	
		Application Number	
		Filing Date	
		Art Unit	
		Examiner Name	

As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below, next to my name.

I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

<p align="center">Methods And Apparatuses For Secondary Conditional Access Server</p>
--

(Title of the Invention)

the specification of which

☒ is attached hereto.

OR

☐ was filed on (if applicable):

or _____ as United States Application Number _____
as PCT International Application Number _____

and was amended on _____ (if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment specifically referred to above.

I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application. I do not know and do not believe that the claimed invention was in public use or on sale in the United States of America more than one year prior to this application, nor do I know or believe that the invention has been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

Docket No. 6517P002

-1-

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, or inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT International application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s):

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?
			☐	☐ Yes ☐ No
			☐	☐ Yes ☐ No
			☐	☐ Yes ☐ No
			☐	☐ Yes ☐ No
			☐	☐ Yes ☐ No

Appointment of Practitioners:

I hereby appoint the practitioners associated with Customer Number: **08791** as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the U.S. Patent and Trademark Office connected herewith.

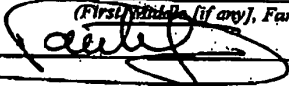
If this patent application is assigned, then the undersigned hereby authorizes the patent attorneys and patent agents named herein to accept and follow instructions from the assignee(s) as to any action to be taken in the United States Patent and Trademark Office regarding this application without direct communication between the patent attorneys and patent agents and the undersigned. In the event of a change in the persons from whom instructions may be taken, at least one patent attorney or patent agent named herein will be so notified by the undersigned.

Correspondence:

Direct all correspondence to Customer Number **08791**.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR: ☐ A petition has been filed for this undersigned inventor

Full Name: Luc Vantalon
 (First, Middle (if any), Family Name (or Surname), and Suffix (if any))
 Inventor's Signature:  Date: 12-06-04
 Residence: Sunnyvale, California USA Citizenship: France
 (City, State, Country) (Country)
 Mailing Address: 868 Helena Drive
Sunnyvale, California 94087 USA

Docket No. 6517P002

NAME OF SECOND INVENTOR: ☐ A petition has been filed for this undersigned inventor

Full Name: Paolo Siccardo
(First, Middle [if any], Family Name (or Surname), and Suffix [if any])
Inventor's Signature  Date Dec 6, 2004
Residence Los Altos, California USA Citizenship USA
(City, State, Country) (Country)
Mailing Address 22261 Ainsworth Drive
Los Altos, California 94024 USA

NAME OF THIRD INVENTOR: ☐ A petition has been filed for this undersigned inventor

Full Name: _____
(First, Middle [if any], Family Name (or Surname), and Suffix [if any])
Inventor's Signature _____ Date _____
Residence _____ Citizenship _____
(City, State, Country) (Country)
Mailing Address _____

NAME OF FOURTH INVENTOR: ☐ A petition has been filed for this undersigned inventor

Full Name: _____
(First, Middle [if any], Family Name (or Surname), and Suffix [if any])
Inventor's Signature _____ Date _____
Residence _____ Citizenship _____
(City, State, Country) (Country)
Mailing Address _____

NAME OF FIFTH INVENTOR: ☐ A petition has been filed for this undersigned inventor

Full Name: _____
(First, Middle [if any], Family Name (or Surname), and Suffix [if any])
Inventor's Signature _____ Date _____
Residence _____ Citizenship _____
(City, State, Country) (Country)
Mailing Address _____

06517.P002C

UNITED STATES PATENT APPLICATION

FOR

METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

INVENTORS:

LUC VANTALON
PAOLO SICCARDO

PREPARED BY:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085

(408) 720-8300

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being deposited with the United States Patent and Trademark Office via electronic filing through the United States Patent and Trademark Electronic Filing System on:

September 12, 2012

Date of Deposit

Connie Thayer

Name of Person Filing Correspondence

Connie Thayer

Signature

9-12-12

Date

METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

[0001] This application is a continuation of co-pending U.S. Application No. 11/007,116 filed on December 7, 2004.

FIELD OF THE TECHNOLOGY

[0002] The invention relates to conditional access (CA) for systems such as a digital cable television system, a satellite television system, etc.

BACKGROUND

[0003] Conditional access (CA) is a technique for limiting the access of content (e.g., audiovisual works such as movies) to authorized users. For example, CA systems have been developed for cable TV and non-cable TV including digital television (DTV). In a CA system for digital television, the media content is scrambled (encrypted) using a standard algorithm before broadcasting. The key used for scrambling/descrambling the media content in a CA system is called a control word (CW). The control word is securely provided to the subscribers through entitlement control messages and entitlement management messages. A security device uses the control word to descramble (decrypt) the received media content.

[0004] Typically, the control word changes frequently (e.g., about every 0.1 second). To prevent unauthorized access, the control words are protected (scrambled/encrypted) using a service key (SK) when being broadcast. Only the security devices in possession of the service key can recover the control word for descrambling the media content protected by the CA system.

[0005] An entitlement control message (ECM) is typically used to broadcast the control word in an encrypted form, which can be decrypted using the service key. The entitlement control message is checked against the access criteria in order to provide authorization. The control word is released if authorization is granted. Using the service key, the system can securely broadcast

common information, such as the control word, to subscribers simultaneously without having to individually broadcast a message for each of the subscribers.

[0006] To individually manage each security device, each security device has a unique identity so that the CA system can broadcast a message specifically for one security device. An entitlement management message (EMM) typically contains the actual authorization data (e.g., entitlement) to authorize the security device for certain access criteria. Entitlement management messages are individually addressed to particular security devices. An entitlement management message may be only for one particular security device with a unique identity. The system broadcasts an entitlement management message for each of the entire population of the security devices to individually control the security devices. Typically, each security device has a unique, secret user key (UK) so that an entitlement management message for one security device can only be decrypted using the unique user key of the security device.

[0007] Typically, the service key also changes periodically (e.g., once a month for subscription TV or once a movie for Pay-per-View). An entitlement management message can be used to send the service key to a particular security device for a subscriber. The CA system broadcasts an entitlement management message for each subscribing security device to deliver the service key. After the service key is individually delivered to the subscribing security devices using the entitlement management messages, the CA system can broadcast the encrypted control words that can be decrypted using the service key.

[0008] Through the use of entitlement management messages and entitlement control messages, a CA system can offer capabilities such as pay-per-view (PPV), interactive features such as video-on-demand (VOD) and games, the ability to restrict access to certain material, and the ability to direct messages to specific receiving devices (e.g., set-top boxes with a smart card).

[0009] In digital television, the media content (e.g., video and audio signals) is converted into a digital form using the MPEG-2 format. The digital form of the media content of one program is multiplexed together with those of other programs for transmission so that multiple programs appear to be transmitted simultaneously. The CA system scrambles the digital form of

programs and transmits the entitlement control messages and the entitlement management messages with the digital form of programs for broadcast either within the multiplex (e.g., Satellite) or through an out-of-band channel (e.g., Cable).

[0010] Typically, a set-top box (STB) at the receiving end descrambles the data stream and decodes the MPEG-2 data for viewing. A tuner portion of the STB receives the incoming signal, demodulates it and reconstitutes the transport stream, which contains many packets of information. The set-top box can de-multiplex the entitlement management messages and entitlement control messages and the media content. The data (e.g., service key and control word) contained in the entitlement management message and entitlement control message are used to descramble the encrypted programming material. The set-top box then renders the MPEG-2 data for viewing.

[0011] A digital rights management (DRM) system manages rights digitally. Digital rights management uses encryption software to protect electronic information and prevent widespread distribution. In a typical digital rights management scheme, a DRM server software program wraps the digital content through encryption according to applicable policies. A DRM client software program unwraps the content and makes it accessible in accordance with its rights. The rights are typically distributed to clients separately from the wrapped electronic information. DRM clients may include desktop PCs, handheld devices, set-top boxes, mobile phones and other portable devices. In addition to encrypting/scrambling the digital content to limit the distribution, a digital rights management system may also provide the description, identification, trading, protection, monitoring and tracking of various forms of rights.

[0012] Content encryption is typically performed using symmetric key cryptography, while key encryption is typically using public/private key cryptography. In symmetric key cryptography, the same key is used to both encrypt and decrypt the content. In public/private key cryptography, different but related keys are used to encrypt and decrypt the content.

SUMMARY OF THE DESCRIPTION

[0013] Methods and apparatuses for bridging two security systems so that a primary security system can control premium content distribution to external devices secured by a secondary security system. Some embodiments of the present invention are summarized in this section.

[0014] In one embodiment of the present invention, the primary security system is a broadcast CA system, used to secure the distribution of premium content only to legitimate subscribers; and the secondary security system includes a digital rights management system used to secure the distribution of premium content only to the legitimate devices of the subscriber.

[0015] In one embodiment of the present invention, the primary security system is a broadcast CA system, used to secure the distribution of premium content only to legitimate local broadcasters; and the secondary security system includes another broadcast CA system, used to secure the re-distribution of premium content only to the legitimate local subscribers.

[0016] In one embodiment of the present invention, the primary security system is a digital rights management system, used to secure the distribution of premium content only to legitimate devices of the subscriber; and the secondary security system is another digital rights management system, used to secure the further distribution of premium content only to other devices of the subscribers not supporting the primary digital rights management system.

[0017] In at least some embodiments of the present invention, a primary CA server provides entitlement data and/or decryption keys to multiple primary CA clients, along with some encrypted premium content. A secondary CA server acts as a legitimate primary CA client; the secondary CA server tries to recover the protected content and to provide with the protected content a new set of entitlement data and/or decryption keys consistent with the original entitlements to one or more secondary CA clients.

[0018] In one embodiment of the present invention, the secondary CA server may completely remove the primary security system encryption before processing it for distribution to the secondary CA clients; or may keep some or the totality of the primary security system

encryption, still hand over it to the secondary CA client but add provision to the content so that it can be further authorized at playback time.

[0019] In one embodiment of the present invention, the primary CA server may enable the secondary CA server to first distribute protected but non-authorized content to secondary CA clients and then authorize it later.

[0020] In one aspect of the present invention, a method to control a presentation of content, includes: receiving a representation of content from a first CA server which provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access; and presenting the content, at a user's request, through a second CA server which is coupled to the first CA server. The presenting of the content is authorized through a client server relationship between the second and the first CA servers respectively. The second CA server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content. In one example, the content is presented by a network client of the second CA server using the second set of cryptographic keys; and the first CA server provides the second CA server the first set of cryptographic keys for authorized use. In one example of an embodiment, the second CA server authorizes the network client to use the content through the digital rights management system in accordance with authorization to use received from the first CA server. In one example, the second CA server translates authorization to access the content from authorization received from the first CA server to authorization for the network client. In one example of an embodiment, the secondary CA server acts as a primary CA server to another CA server. In one example of an embodiment, the first CA server provides authorization to the second CA server according to an identity of the second CA server; the second CA server provides authorization to the client according to an identity of the client; and the first CA server is not aware of an identity of the client.

[0021] One aspect of the present invention includes a method for the secondary CA server to distribute protected but non-authorized content to secondary CA clients; and to enable the same clients to play back the content when later authorized by the primary CA server.

[0022] One aspect of the present invention includes a method for a secondary CA server to process entitlement management messages from a primary CA server and to transmit to secondary CA clients through a network connection access controlled data that is in an access controlled format and that is at least partially derived from the entitlement management messages. In one example of an embodiment, the secondary CA server has a user key representing a subscriber of the primary security system; and processing the entitlement management messages includes: decrypting an entitlement management message to obtain a service key of the primary security system.

[0023] In one example of an embodiment, the method further includes: receiving, at the secondary CA server, an entitlement control message of the primary security system; and processing the entitlement control message to obtain a control word of the primary security system; where the access controlled data includes the control word. In one example, the access controlled data comprises a decrypted version of the entitlement control message.

[0024] In one example of an embodiment, the method further includes: receiving, at the secondary CA server, an entitlement control message of the primary security system; and processing the entitlement control message on the secondary CA server to generate a substitutive entitlement control message as a replacement of the entitlement control message; where the access controlled data includes the substitutive entitlement control message. In one example, the substitutive entitlement control message has a control word encrypted using a key of the secondary CA server. In one example, the substitutive entitlement control message is to be decrypted using a user key of the primary security system. In one example, the entitlement control message and the substitutive entitlement control message have a same control word. In another example, the entitlement control message has a first control word; the substitutive entitlement control message has a second control word; and the first and second control words are different. In one example, the access controlled data further includes the first and second control words.

[0025] In one example of an embodiment, the method further includes: receiving, at the secondary CA server, a first entitlement control message containing a first control word and content scrambled by the first control word; generating a second entitlement control message containing a second control word that is different from the first control word; and descrambling the content using the first control word and rescrambling the content by the second control word; where the access controlled data comprises the content rescrambled by the second control word and second entitlement control message. In one example, the method further includes: storing, at the secondary CA server, the content rescrambled by the second control word; and retrieving the content rescrambled by the second control word in response to a request from the secondary CA clients.

[0026] In another aspect of the present invention, a method to process media content provided by a primary security system, includes: receiving, at a secondary CA client from a secondary CA server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from entitlement management messages of the primary security system. In one example of an embodiment, the secondary CA client does not have a user key representing a subscriber of the primary security system. In one example of an embodiment, the access controlled format protects access to data using a digital rights management system.

[0027] In one example, the method further includes: automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data; descrambling and recording the portion of the media content in response to a determination to descramble; and recording the portion of the media content without descrambling in response to a determination not to descramble.

[0028] In one example of an embodiment, the method further includes: sending, from the client of the secondary conditional server to the secondary CA server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form; where the access controlled data comprises the control word. In one

example, the method further includes: descrambling media content using the control word; and storing the media content in a storage under protection of a secondary security system. In another example, the method further includes: descrambling media content using the control word; and rendering the media content for presentation. In one example, the entitlement control message is retrieved from a storage device; the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary CA client to the secondary conditional server and when the access controlled data is received at the secondary CA client. In one example, the access controlled data includes a decrypted version of the entitlement control message.

[0029] In one example of an embodiment, the access controlled data includes a result of descrambling media content scrambled by the primary security system.

[0030] In one example of an embodiment, the method further includes: receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; and sending the first entitlement control message from the secondary CA client to the secondary CA server through a network connection. The access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; and the second entitlement control message is stored with the portion of the media content. In one example, both the first and the second entitlement control messages contain a same control word; the second entitlement control message is encrypted for decryption using a key of the secondary CA server. In another example, the first entitlement control message contains a first control word; the second entitlement control message contains a second control word; the first and second control words are different; the access controlled data further comprises the first and second control words; and the method further includes: descrambling the content using the first control word and rescrumbling the content using the second control word.

[0031] The present invention includes methods and apparatuses which perform these methods, including data processing systems which perform these methods, and computer readable media which when executed on data processing systems cause the systems to perform these methods.

[0032] Other features of the present invention will be apparent from the accompanying drawings and from the detailed description which follows.

BRIEF DESCRIPTION OF THE DRAWINGS

[0033] The present invention is illustrated by way of example and not limitation in the figures of the accompanying drawings in which like references indicate similar elements.

[0034] **Figure 1** shows a block diagram example of a data processing system which may be used with the present invention.

[0035] **Figures 2A and 2B** shows a primary security system bridged to a secondary security system according to one embodiment of the present invention.

[0036] **Figure 3** illustrates a complex networked system with multiple primary security systems reaching multiple secondary security systems clients across a home network environment according to one embodiment of the present invention.

[0037] **Figure 4** illustrates a conditional access arrangement which may be used with the present invention.

[0038] **Figure 5** illustrates a system having a secondary CA server for providing control words to secondary CA clients according to one embodiment of the present invention.

[0039] **Figure 6** illustrates a system having a secondary CA server for providing media content to secondary CA clients according to one embodiment of the present invention.

[0040] **Figure 7** illustrates a system having a secondary CA server for decoding entitlement control messages for secondary CA clients according to one embodiment of the present invention.

[0041] **Figure 8** illustrates a system having a secondary CA server for providing substitutive entitlement control messages to secondary CA clients according to one embodiment of the present invention.

[0042] **Figure 9** illustrates a system having a secondary CA server for re-scrambling media content for secondary CA clients according to one embodiment of the present invention.

[0043] **Figure 10A** illustrates an authorization process for recorded media content according to one embodiment of the present invention.

[0044] **Figure 10B** illustrates a prior art scenario to access recorded content.

[0045] **Figure 10C** illustrates a scenario to access recorded content according to one embodiment of the present invention.

[0046] **Figure 11** illustrates a system in which a secondary CA server is configured to decode the control words for the captured media content retrieved from a storage device according to one embodiment of the present invention.

[0047] **Figure 12** illustrates a system in which a secondary CA server is configured to decode the control words for capturing media content into a storage device according to one embodiment of the present invention.

[0048] **Figure 13** illustrates a system in which a secondary CA server is configured to automatically decode the control words before capturing media content into a storage device, or after retrieving captured media content from the storage device, according to one embodiment of the present invention.

[0049] **Figure 14** illustrates a system in which a secondary CA server is configured to generate substitutive entitlement control messages and decode the control words for the captured media content retrieved from a storage device according to one embodiment of the present invention.

[0050] **Figure 15** shows a method of using a secondary CA server according to one embodiment of the present invention.

[0051] **Figure 16** shows a detailed method of a secondary CA server according to one embodiment of the present invention.

DETAILED DESCRIPTION

[0052] The following description and drawings are illustrative of the invention and are not to be construed as limiting the invention. Numerous specific details are described to provide a thorough understanding of the present invention. However, in certain instances, well known or conventional details are not described in order to avoid obscuring the description of the present invention. References to one or an embodiment in the present disclosure are not necessarily references to the same embodiment; and, such references mean at least one.

[0053] **Figure 2A** shows a primary security system bridged to a secondary security system according to one embodiment of the present invention. In **Figure 2A**, the primary CA server (253) controls the access to the content in the primary security domain (251). The primary security domain (251) is typically a broadcast CA system. The primary CA server (253) transmits entitlement management messages and entitlement control messages so that only authorized clients, such as a subscriber's set top box (e.g., 257) can access (decrypt) the CA protected content.

[0054] In one embodiment of the present invention, a secondary CA server (255) bridges the primary security domain (251) and the secondary security domain (261). The secondary security domain typically includes a set of secondary CA clients (e.g., 271, 273, ..., 279). The bridge (259) typically passes CA protected content from the primary security domain (251) to the secondary security domain (261) so that the secondary CA clients (e.g., 271, 273, ..., 279) in the secondary security domain (261) may access the content secured in the secondary security domain under the control of the secondary CA server (255) in accordance with security messages provided by the primary security domain (251) to the secondary CA server (255). The secondary CA clients (e.g., 271, 273, ..., 279) rely on the secondary CA server (255) to obtain the content. The secondary CA server (255) is partially in the primary security domain (251), since the secondary CA server is capable of processing the control information for conditional access provided by the primary CA server (253). The secondary CA server (255) acts as a client of the

primary security domain (251) and as a control information provider of the secondary security domain (261). According to the access terms and conditions given by the primary CA server (253), the secondary CA server (255) conditionally allows the secondary CA clients (e.g., 271, 273, ..., 279) to access the content.

[0055] For example, in **Figure 2A**, the bridge 259 may hand over the scrambled (encrypted) content to the secondary CA clients. To descramble (decrypt) the content, the secondary CA clients request information from the secondary CA server (255). For example, in one embodiment, the secondary CA server (255) provides control words for descrambling the content to the authorized secondary CA clients. The control words are provided under the protection of a DRM system in the secondary security domain (261). The secondary security domain can include another CA server (not shown). In **Figure 2A**, the bridge (259) may also be partially or completely combined within the secondary CA server (255) as a single physical component of a distributed system.

[0056] Note that in **Figure 2A**, a bridge and a further secondary CA server can be used to extend from the secondary domain (261) into another domain. For example, the client (279) can be replaced with a bridge and a further secondary CA server in a way similar to the bridge (259) and secondary CA server (255) replacing a set top box. Such an approach can be used recursively to form a chain of security domains bridged through the use of a hierarchy of cascaded secondary CA servers.

[0057] In one embodiment of the present invention, the secondary security domain is for a localized network, such as a network within a home or hotel or other domain. Alternatively, the secondary security domain may include Internet.

[0058] **Figure 2B** illustrates a bridge (283) in relation with a secondary CA server (281). In **Figure 2B**, the secondary CA server processes security messages, such as CA messages from the primary security domain. In one embodiment of the present invention, the secondary CA server translates authorization from the primary security domain into authorization in the secondary security domain. The secondary CA server generates security message for the secondary

security domain in accordance with authorization obtained from security messages in the primary security domain. Thus, entities not known in the primary security domain can be provisioned through the use of the secondary CA server, which has an identity known in the primary security domain and knows the entities in the secondary security domain. In one embodiment, the secondary CA server follows rules (e.g., CA messages) of the primary CA server to manage a secondary subscriber management system (SMS) that is different from the primary subscriber management system managed by the primary CA server. In one embodiment, the client identities and authentication methods used by the secondary CA server in the secondary subscriber management system are independent from those used by the primary CA server in the primary subscriber management system. As a server in the secondary subscriber management system and a client in the primary subscriber management system, the secondary CA server bridges the two subscriber management systems. In one embodiment of the present invention, the CA servers support two different roots of trust for security. The secondary CA server and the primary CA server supports root of trust independent from each other. In one embodiment, the root of trust is used to authenticate clients; the client authentication in the secondary security domain is completely independent from the client authentication in the primary security domain; and the authorization to use in the secondary security domain is in accordance with the authorization to use conveyed in the primary security domain.

[0059] In **Figure 2B**, a number of components are illustrated for the bridge (283), such as a physical interface (285), a transcoder (287) and another physical interface (289). For example, the physical interface (285) may be a tuner which converts the signals representing the CA protected content into a data format; the transcoder (287) may convert the protected content from one protected (e.g., encrypted) format to another protected (e.g., encrypted) format; and the physical interface (289) may be a data network communication interface for transmitting the protected content to a client in the secondary security domain. The secondary CA server may receive information from the physical interface (285). The secondary CA server (281) may directly provide the content to the physical interface (289) in accordance with the authorization

from the CA messages. The secondary CA server (281) may provide messages to control the operations of the transcriber (287) and physical interface (289) in accordance with the authorization derived from the CA messages. In general, a bridge may include more or less components than those illustrated in **Figure 2B**. For example, a bridge may have one or more of: as a tuner, a transcriber, a transcoder, a physical interface, a network communication interface, a cable, a storage device, etc.

[0060] **Figure 3** illustrates a complex networked system with two primary security system sources (211 and 215) with their own primary CA servers (226 and 228), two secondary CA servers (227 and 225) and many secondary CA clients (207, 209, 217, 221, 231 and 233). In one embodiment of the present invention, a secondary CA server is used to provide services to a plurality of devices connected to a network (201), such as a local area network (LAN) or a wireless LAN. The network (201) may be partially a wired Ethernet in a home of a service subscriber with one or more wireless access points for mobile devices such as a personal data assistant (PDA), a palm computer, a notebook computer, or a cellular phone (e.g., connected to the network through a WiFi or Bluetooth connection). For example, in **Figure 3**, the PDA (243) connects to the access point (241) through the wireless connection (245) and further to other components through the network (201). The network may also be a network for an organization or a commercial establishment (e.g., a hotel or a motel chain), such as an intranet or a virtual private network.

[0061] In **Figure 3**, a cable TV secondary CA server (225) is used with the cable TV service. The cable primary CA server (228) couples with the cable headend (215) to provide the CA protected media content through the cable television transmission system to the cable TV bridges (e.g., 217 and 219) which may include cable TV tuners. The cable TV bridges receive the data packages and de-multiplex the entitlement management messages and entitlement control messages and the scrambled media content. Under the control and with the help of the cable TV secondary CA server (225), the media content can be secured on a storage (e.g., 221, 223 or 235) for access by various devices which can play back the media content, such as the personal

computer (233) the media player (231), or the PDA (243). The personal computer (233) typically displays the video content on the display device (239), such as a Cathode Ray Tube (CRT) monitor or a flat Liquid-Crystal Display (LCD) panel. The media player (231) typically presents the media content on a television set (237). A media player may also be integrated with a television set to form a network-ready digital television set.

[0062] In one embodiment, the cable TV secondary CA server provides services to descramble/decrypt the cable TV broadcast. The decrypted/descrambled information is protected in a digital rights management system so that the media content from the broadcast of the cable TV system can be used in an authorized way. When authorized, the content can be recorded and played back at any time on any device convenient to the user in accordance with the rights of the subscriber. For example, with a subscription to only one simultaneous use, a user may choose to use cable TV bridge (217) to receive the broadcast and view the program on the TV (247), or use cable TV bridge (219) to record the program on the storage (223) for playing back at a different time using the PDA (243), the personal computer (233) or the media player (231).

[0063] In **Figure 3**, a satellite TV secondary CA server (227) is used to provide services to both the satellite TV bridge A (207) and the satellite TV bridge B (209). The satellite TV secondary CA server (227) may store the protected media content on its storage (229) or on other storage devices on the network, such as the storage (235) of the personal computer (233) or the storage (221). Typically, a satellite (211) broadcasts (213) the protected media content to a geographical area. Separate satellite dishes (e.g., 203 and 205) are used for different satellite bridges (e.g., 207 and 209) respectively.

[0064] Traditionally, to access two different channels simultaneously, two set-top boxes are used. Satellite set-top boxes are independent from each other. The satellite broadcasts to the two set-top boxes as if the set-top boxes were for two different subscribers. In one embodiment of the present invention, the satellite TV secondary CA server provides services to both the satellite TV bridges. The satellite TV secondary CA server (227), not the satellite TV bridges (207 and 209),

has the data representing the subscriber. Thus, one subscriber needs only one unique identification for the operation of multiple tuners.

[0065] In one embodiment, different secondary CA servers are used to extend the services of different primary CA servers, since different primary CA systems typically use entirely different algorithms and protocols for the entitlement management messages and entitlement control messages. In one embodiment of the present invention, the different secondary CA servers are physically in one data processing device with different software and smart cards for the processing of the messages of different CA systems. Further, a secondary CA server may be integrated with a bridge, a storage device, a renderer (e.g., PDA 243, personal computer 223, media player 231), or a combination of them. For example, the satellite TV secondary CA server may include a storage for recording media content, a bridge for interfacing with a satellite dish and a renderer for decoding the media content into standard video signals (for a television set and/or for a computer monitor).

[0066] Further details about various different arrangements of the components (e.g., secondary CA server, bridge, storage, renderer) and the operations of the components are provided below.

[0067] **Figure 4** illustrates a conditional access arrangement which may be used with the present invention. In one embodiment of the present invention, a secondary CA server contains a security device (307) which has a unique user key (331) to represent the subscriber. The user key (331) can be used to decrypt the entitlement management message (EMM) (301), which has the encrypted service key (311). In one embodiment of the present invention, the secondary CA server performs the EMM decryption (321) for secondary CA clients using the user key (331) to recover the service key (SK) (333). The entitlement control message (ECM) (303) contains the encrypted control word (313). In one embodiment of the present invention, the secondary CA server further performs the ECM decryption (323) using the service key (333) to recover the control word (CW) (335) for the secondary CA clients. The scrambled content (305) can be descrambled using the control word (335) to generate the content (337). In one embodiment, the

secondary CA server provides the control word to an authorized secondary CA client to descramble the content (305). Alternatively, the secondary CA server may further include a descrambler (325) to descramble the content for secondary CA clients.

[0068] The descrambler of a digital television system uses a standard algorithm (e.g., Common Scrambling for DVB, DES for Advanced Television Systems Committee (ATSC) standard (Conditional Access System for Terrestrial Broadcast)). The descrambler (325) can be conveniently located on any of the components (e.g., a bridge, a renderer or a storage).

[0069] In one embodiment of the present invention, a secondary CA server performs ECM decryption (323) and then generates a replacement entitlement control message. The replacement entitlement control is encrypted for decryption using a different service key, which is under the control of the secondary CA server, so that the secondary CA server does not need to maintain the service key (333) for recorded contents. The replacement entitlement control can be recorded with the scrambled content (305) protected by the DRM system for later use.

[0070] In one embodiment of the present invention, the control word is further changed for recording. After the descrambler (325) generates the clear content (337), the clear content is re-scrambled using a different control word for recording. For the recorded content, the CA protection may be translated so that the control word may change in-frequently (e.g., one control word for one entire movie).

[0071] Typically, a secondary CA server performs both EMM decryption (321) and ECM decryption (323) for all the secondary CA clients (e.g., a bridge, a renderer or a storage), since both the ECM and EMM are specific to a particular CA system.

[0072] In one embodiment of the present invention, the results of a secondary CA server are protected using a DRM system; and the DRM system manages the rights according to the data in the EMM (and/or ECM).

[0073] Although **Figure 4** shows a particular encryption/decryption arrangement of a CA system, it is understood that different arrangements can also be used with the present invention. For example, in a CA system, the service key may be delivered physically instead of through

broadcasting. In general, the entitlement management messages are broadcast to individual devices to individually authorize entitlement; and the entitlement control messages are typically broadcast to all devices to provide the common key for descrambling the broadcast stream. It is understood that a service key represents the entitlement recovered from the entitlement management message; and the control word represents the key recovered from the entitlement control message for descrambling the media content.

[0074] **Figure 5** illustrates a system having a secondary CA server for providing control words to secondary CA clients according to one embodiment of the present invention. In **Figure 5**, the secondary CA server (431) uses its user key (UK 433) to recover the control word from the encrypted entitlement management message (EMM 435) and entitlement control message (ECM 437) for the secondary CA clients over the network (439). The recovered control word (441) is protected using a DRM system; and only a secondary CA client with appropriate rights (443) can use the control word (445) to descramble the content (447) to obtain the clear content (449) that is not encrypted/scrambled.

[0075] The rights to the control word can be determined from the data in the EMM at the time of recording and/or at the time of playback. The control word can also be provided to the secondary CA clients in real time as the broadcast is received for immediate viewing.

[0076] Since the control word is provided through the network (439) which may cause unpredictable network communication delay, arrangement is made to synchronize the control word with the decoding of the media content. In one embodiment, the secondary CA client synchronizes the control word obtained from the server with the stream of media content for descrambling operation. In one embodiment of the present invention, a secondary CA client for playing back the media content buffers a time period worth of content in a pipeline for playback in anticipation of unpredictable network delay in obtaining the control word, which changes frequently (e.g., every 0.1 second). When a control word is delay, the descrambled content in the pipeline decreases and the scrambled content in the pipeline increases; when the control word is received, the descrambling operation resumes to increase the descrambled content in the pipeline

and decrease the scrambled content in the pipeline. Thus, the buffering allows the secondary CA client to maintain a constant rate of descrambled content for rendering in real time.

[0077] In one embodiment of the present invention, a secondary CA server further includes a descrambler so that the secondary CA clients do not need a descrambler.

[0078] In one embodiment of the present invention, the secondary CA server (431) uses both the data in the EMM received prior to the content reception and the data in the EMM received prior to the content consumption, if different, to determine the rights of the user for the service key. For example, in one embodiment of the present invention, when the user is entitled to the content at the time of recording, the service key can be recovered for the data in the EMM at the time of recording. When the recorded content is retrieved from the storage for playback, the secondary CA server may further determine the rights according to the data in the EMM for the current time period. In one embodiment, for example, the user is entitled to view the recorded content only if the user is currently a valid subscriber of the service (e.g., subscribing for the viewing of recorded contents). Alternatively, the secondary CA server uses only the data in the EMM at the time of recording to determine the rights to the recorded contents.

[0079] In one embodiment of the present invention, a primary CA server provides entitlement only at playback time. For example, the system can allow the user to record programs that the user is not entitled to use at the time of recording. After the user obtains the required rights (e.g., through purchase for pay-per-view, or upgrading a subscription package), the user can then playback the recorded information at any convenient time.

[0080] Generally, different CA systems (e.g., primary or secondary CA servers) have entirely different implementations of EMM and ECM but similar or same descramblers for content protection (e.g., according to the ATSC Standard). In one embodiment of the present invention, a secondary CA server decodes both the EMM and ECM and other client components process the content in standard formats (e.g., using a standard descrambling algorithm).

[0081] **Figure 6** illustrates a system having a secondary CA server for providing media content to secondary CA clients according to one embodiment of the present invention. In

Figure 6, the secondary CA server (461) has a user key (463) to decrypt the encrypted entitlement management message (EMM 471) and the encrypted entitlement control message (ECM 473) and the scrambled content (475). The secondary CA server descrambles the content and provides the DRM protected content (467) through the network (465) so that only the secondary CA client with the appropriate rights (469) can use the content (477).

[0082] In one embodiment of the present invention, the secondary CA server (461) includes one or more bridges and a storage device. The content can be recorded and stored in the storage device for later viewing or provided for real time use. The secondary CA server may directly record the original CA protected content, or record the descrambled content (with encryption for DRM protection), or record the content with substitutive CA protection (e.g., with replacement entitlement control message, or rescrambling using a different control word). In one embodiment of the present invention, the DRM protected content (467) is provided to the secondary CA clients according to the rights determined from EMM (and/or ECM) messages (e.g., at the time of recording and/or the time of playback).

[0083] **Figure 7** illustrates a system having a secondary CA server for decoding entitlement control messages for secondary CA clients according to one embodiment of the present invention. In **Figure 7**, the secondary CA server (501) with the user key (503) decodes the entitlement management message (EMM 507) and the entitlement control message (ECM_a 509) to provide, over the network (505), the local entitlement control message (ECM_b 511), which is protected under a DRM system. The secondary CA client with the rights (513) to the local entitlement control message (ECM_b 511) can use the control word (515) in ECM_b (511) to descramble the content (517). Typically, the secondary CA client sends the local entitlement control message (ECM_b 511) back at the playback time for the control word (515) and then generates the clear content (519) using the control word (515) received from the secondary CA server (501). In one embodiment, the clear content (519) is rescrambled using a different scheme before stored on a storage. Alternatively, the descrambled content (519) can be recorded and stored in a storage under the protection of a DRM system.

[0084] Alternatively, a storage records the scrambled content (517) with the DRM protected ECM_b (511) so that a device with rights (513) can retrieve the media content (517) and ECM_b (511) for viewing at a different time. The decoded entitlement control message ECM_b (511) may be used to replace the original encrypted entitlement control message ECM_a (509) to generate a stream for storage and access under the DRM system. Since the use of the decoded entitlement control message (ECM_b 511) does not require the service key of the primary security system, the management of the recorded content can be simplified.

[0085] In one embodiment of the present invention, a secondary CA server generates substitutive entitlement control messages which are encrypted for decryption by a different service key that is managed by the secondary CA server (e.g., generated and maintained by the CA server). Typically, the CA system of a primary security system changes the service key periodically (e.g., once a month). Entitlement control messages recorded from different time periods need different service keys for decryption. In one embodiment of the present invention, to simplify the service key management for the recorded content, a secondary CA server re-encrypts the entitlement control message to generate a substitutive entitlement control message for recording. The secondary CA server can later decrypt the substitutive entitlement control message without using the original service key.

[0086] **Figure 8** illustrates a system having a secondary CA server for providing substitutive entitlement control messages to secondary CA clients according to one embodiment of the present invention. In **Figure 8**, the secondary CA server (531) receives the entitlement management message (EMM 541) and the entitlement control message (ECM_a 543) which is to be decrypted using a service key (SK_a) provided by the EMM (541). The secondary CA server (531) decrypts the EMM (541) using the user key (533) to obtain the service key (SK_a) and then further decrypts the ECM_a (543) using the service key (SK_a) and obtains the control word (CW). The secondary CA server manages a service key SK_b (535) and re-encrypts the control word to create a local entitlement control message (ECM_b 545), which can then be decrypted using the service key SK_b (535). The decryption of the local entitlement control message ECM_b (545) does

not need the original service key (SK_a) sent in the EMM (541). The secondary CA server (531) provides the ECM_b (545) as a substitutive entitlement control message to a secondary CA client through the network (537). The original entitlement control message (ECM_a 543) is replaced with the substitutive entitlement control message (ECM_b 545) to record and store the scrambled content (547) on the storage (539). When the scrambled content is retrieved from the storage (539) for use in a renderer, the secondary CA server (531) can decode the ECM_b (545) using the service key (SK_b 535) to retrieve the control word in the ECM_b (545). The secondary CA server can then provide the control word to a secondary CA client in a way illustrated in **Figure 5**. The secondary CA server (531) may further determine whether or not to release the control word based on the entitlement management message received at the time of decrypting the substitutive control message (ECM_b 545). In one embodiment, the information stored on the storage (539) is further protected under a DRM system.

[0087] In a typical conditional access of a primary security system (e.g., digital TV or satellite TV), the control word changes frequently (e.g., once every 0.1 second). To protect the recorded and stored content, which may be further protected under a DRM system, it may not be necessary to change the control word as frequently. For example, an entire recorded movie may be rescrambled using one control word. In one embodiment of the present invention, a secondary CA server is used to descramble and re-scramble the CA protected content for recording.

[0088] **Figure 9** illustrates a system having a secondary CA server for re-scrambling media content for secondary CA clients according to one embodiment of the present invention. In **Figure 9**, the secondary CA server (561) receives the broadcast, including the entitlement management message (EMM 571), the entitlement control message (ECM_a 573) and the scrambled content (575). The secondary CA server (561) uses the user key (563) to access the data in EMM (571) (e.g., recovering the service key), to access the data in ECM_a (573) (e.g., recovering the control word), and to descramble the content (575). The secondary CA server (561) then rescrambles the content (e.g., using a different control word) and provides the rescrambled content (569) with the new entitlement management message (ECM_b 567) to one or

more secondary CA clients through the network (565). In one embodiment, the ECM_b (567) is protected under a DRM system so that only the secondary CA clients with appropriate rights (581) can challenge the secondary CA server by sending the ECM_b (567) at playback time and get in return the control word (CW_b 577) for descrambling the content (569) to recover the clear content (579). In one embodiment of the present invention, the ECM_b (567) is further encrypted for decryption with a substitutive service key in a way similar to that illustrated in **Figure 8**.

[0089] **Figure 10A** illustrates an authorization process for recorded media content according to one embodiment of the present invention. In **Figure 10A**, the primary CA system (e.g., a digital TV system, or a satellite TV system) first sends (731) an entitlement management message (EMM) requesting caching of a program. The user may not already subscribe to the program (e.g., a movie or a sport program). Thus, the device of the user may not be authorized to descramble the program. According to one embodiment of the present invention, the device of the user can record (743) the scrambled program after receiving the EMM that requests caching the program at a subscriber system. The primary CA system then starts (733) broadcasting the program. After a period of time based on the length of the program, the content providing system ends (735) broadcasting the program. During the period, the device of the user records (743) the scrambled program. Since the user is not a subscriber to the program, the device is not authorized to playback the scrambled content at the time of recording. After the recording, the user may be prompted for availability of the program. If the user requests (745) authorization (which may be at any time) to use the recorded program, an authorization EMM (737) is generated. The authorization EMM may be generated locally at the device, in a way similar to impulse pay per view (IPPV), or generated after the user calls the operator to obtain the authorization, in a way similar to over the phone pay per view (OPPV), or generated after the device transmits the request to the CA system through a data connection, in a way similar to Video-on-Demand (VOD). Once the device obtains the authorization to playback the recorded program, the device can descramble the program for playback (747).

[0090] In one embodiment of the present invention, a secondary CA server is used to process and manage the EMM for secondary CA clients. The authorization for playback is requested and granted through the secondary CA server. In one embodiment, the primary CA server is aware of the secondary CA server as a subscriber. For example, the primary CA server is aware of the identity of the secondary CA server and provides authorization according to the subscription status of the secondary CA server. However, the primary CA server may not aware of the identities of the secondary CA clients. In one embodiment of the present invention, the secondary CA server translates the authorization obtained from the primary CA server into authorization for the clients of the secondary server in a way consistent with the policy of the primary CA server.

[0091] For example, the secondary CA server may not consume the content; and the secondary CA server may be used to authorize one of its clients to use the subscription and consume the content (e.g., playback the media content in real time or after the media content is recorded). Thus, the secondary CA server may dynamically attach its subscriber identity to one of its clients so that the combined secondary CA server and the corresponding client, which is dynamically selected, can be viewed as a subscriber that is known to the primary CA server.

[0092] Further, the secondary CA server may translate access policies in other sophisticated ways. For example, the secondary CA server may determine the authorization of simultaneous access by multiple devices to the same or different media contents. For example, a subscriber may have a subscription to use two independent players to see different channels. Instead of providing the subscriber with two set top boxes with two different identities, the vendor can provide the subscriber with a secondary CA server, which has one identity and authorizes two players to play back the media content according to the authorization from the primary CA server based on the subscription.

[0093] **Figure 10B** illustrates a prior art scenario to access recorded content. In **Figure 10B**, a user device (755), such as a set top box, that has an identity recognized as a subscriber interacts with the primary CA server (753) directly in the authorization process. For example, after the

primary CA server sends a request to cache a program to a recorder (751), which is typically a part of a set top box, CA protected media content (765) can be recorded in recorder (751). At the time of recording the user may not be entitled to view the media content. The CA protected media content can then be stored in the recorder (751) in a CA protected format. To use the media content (759), the user device needs authorization from the primary CA server. If the user device has not already obtained the authorization, the user device (755) requests (763) authorization to use in communication with the primary CA server (753), which may then send an authorization message (761) to the user device. The request for authorization may be alternatively sent through a user phone call, or through a data link between the primary CA server (753) and the user device (755).

[0094] In **Figure 10C**, the identity of the client of primary CA server (753) is directly attached to the user device which may be authorized according to the identity to remove CA protection from the received media content and play back (consume) the media content.

[0095] **Figure 10C** illustrates a scenario to access recorded content according to one embodiment of the present invention. In **Figure 10C**, the authorization process is through the secondary CA server (772), which is a client of the primary CA server (773). The secondary CA server (772) has an identity recognized as a subscriber of the primary CA server (773). The secondary CA server (772) may forward, translate, and/or manage its authorization received from the primary CA server (773) into authorization for its clients, such as the media player (775). Thus, even though the media player (775) may not have an identity recognizable as a client of the primary CA server (773), through the secondary CA server (772) the media player (775) is effectively recognized as a legitimate subscriber. Thus, one embodiment of the present invention allows the dynamic integration of two devices (e.g., the secondary CA server and a media player) into one logical entity, which may provide the functionality of a traditional set top box.

[0096] Further, one embodiment of the present invention allows the separation of the identity of the client of primary CA server (753) in one device (e.g., a secondary CA server) and a user

device which may be authorized according to the identity to remove CA protection from the received media content and/or play back the media content. Such an arrangement allows enormous flexibility in a content delivery system according to one embodiment of the present invention. For example, the media player (775) may use a different content protection system, such as a DRM system; the primary CA server don't have to support all media players of its users/subscribers; and the secondary CA sever can be used to extend the service and functionality of the primary CA system. Further, for example, the user can copy the protected content and move it to other storage medium and still be able to watch the content through the control of the secondary CA server. For example, the protected content can be distributed on a local network (e.g., within a home, a hotel, a campus, a building, etc.) through various available communication tools, media and protocols while the rights to use the protected content can be managed though the control of the secondary CA server in accordance with the authorization the secondary CA server obtained from the primary CA server.

[0097] In one embodiment, the secondary CA server (772) provides the authorization to its clients in a way consistent with the authorization it obtained from the primary CA server (773). Thus, the secondary CA server (772) conveys legitimate rights to its clients in accordance with the authorization from the primary CA server (773) without providing illegitimate access.

[0098] For example, in **Figure 10C**, the primary CA server may request (777) the recorder (771) to cache a program. The recorder (771) then records the CA protected media content (785) for later retrieval. The recorder (771) can be a device separated from the secondary CA server (772) and the media player (775), or a component integrated within the secondary CA server (772) or the media player (775). To play back the media content (779), the media player (775) requests (789) authorization to use from the secondary CA server (772), since the media player (775) is not a direct client of the primary CA server (773). If the secondary CA server (772) has not yet obtained the authorization, the secondary CA server (772) sends an authorization request (787) to the primary CA server (773), which can then provide an authorization message (781) to the secondary CA server (772) based on the identity of the secondary CA server (772) as a client

of the primary CA server (773). The secondary CA server then sends an authorization message (783) to the media player (775) based on the identity of the media player (775) as a client of the secondary CA server (772), in accordance with the authorization message (781) received from the primary CA server (773).

[0099] In one embodiment of the present invention, a secondary CA server has data to represent a subscriber. The secondary CA server is used to processing the entitlement management message and/or the entitlement control message of the primary CA server. A bridge interfaces with the primary security system to reconstitute the data stream, including the entitlement management message, the entitlement control message and the scrambled content. A storage is used to store the content for playing back at a different time. A renderer is used to process the content for presentation. Since the content is typically control word scrambled/descrambled using a standard algorithm, a standard scrambler/descrambler can be continually located on the conditional access, the bridge, or the renderer, depending on the network configuration and/or other considerations.

[00100] Although some of the figures (e.g., **Figures 11 – 14**) and descriptions show a secondary CA server, a bridge, a storage, a renderer separately, it is understood that a secondary CA server, a bridge, a storage, a renderer can be physically combined in various different ways. The communication between these components is not necessarily all through network connections. For example, a secondary CA server may be physically separate from a bridge and a renderer and communicating to the bridge and renderer through a network; and the bridge and the renderer may be physically separated from each other or combined in one device. Alternatively, the secondary CA server may be combined with a bridge, communicating with a renderer over a network, or be combined with a renderer, communicating with a bridge over a network. The storage may be connected through a network to a secondary CA server, a bridge and a renderer, which may be combined in various ways as illustrated above. Alternatively, the storage may be in at least one of the secondary CA server, the bridge and the renderer and connected to the rest of the components through a network. Further, a storage may partially in

one component and partially in another. As illustrated in **Figure 3**, a networked system may have multiple bridges, multiple renderers and multiple storages. Typically, one secondary CA server is a client of one primary CA server. However, one secondary CA server may also be a client of multiple CA systems.

[00101] In one embodiment of the present invention, a secondary CA server is used on a network to provide services to secondary CA clients. For example, a secondary CA server may decode entitlement management messages to determine rights for a DRM system, decode entitlement control messages to recover control words for secondary CA clients, generate substitutive entitlement control messages, descramble CA protected contents for secondary CA clients, rescrumble CA protected contents for secondary CA clients, etc.

[00102] **Figure 11** illustrates a system in which a secondary CA server is configured to decode the control words for the captured media content retrieved from a storage device according to one embodiment of the present invention. In **Figure 11**, the bridge (603) interfaces with the primary security system to receive the broadcast feed (601), including the user key (UK) protected entitlement management message (EMM 615), the service key (SK) protected entitlement control message (ECM 613) and the control word (CW) scrambled content (611).

[00103] The bridge (603) may include one or more components, such as a tuner, a transcriber, a transcoder, a physical interface, a network communication interface, a cable, a storage device, etc.

[00104] The bridge (603) sends the entitlement management message (627) to the secondary CA server (609), which has the user key (621) that represents the identity of the subscriber. The secondary CA server (609) determines the entitlement of the subscriber to the content from the entitlement management message (627). For example, the secondary CA server (609) uses the user key (621) to retrieve the service key from the entitlement management message (627). The storage (605) stores the content and the entitlement control message (617) under the protection of a DRM system.

[00105] Although **Figure 11** shows a link between the bridge (603) and the storage (605), it is understood that the recording of the content is not necessary through a direct path from the bridge to the storage. For example, the content and the entitlement control message may be sent to the secondary CA server, which then records the content into the storage (605) in accordance to the data in EMM (627). The storage (605) can be physically integrated within the secondary CA server (609). Alternatively, or in addition, the bridge (603) may be physically integrated within the secondary CA server (609).

[00106] In one embodiment of the present invention, only the content that the subscriber is entitled to according to the EMM at the time of recording is recorded into the storage (605). For example, the storage (605) may be a separate network device or integrated within the bridge (603); and the secondary CA server (609) authorizes the bridge (603) to record the content in accordance with the entitlement of the EMM (627).

[00107] In one embodiment of the present invention, the bridge records the content on the storage. In one embodiment, the bridge records only the content that the subscriber is entitled to use at the time of recording. Based on the data in EMM (627), the secondary CA server determines whether or not the subscriber is entitled to use the scrambled content and sends a message to the bridge about the determination. The secondary CA server maintains data derived from the EMM (627), such as the service key, so that the recorded content can be later decrypted/descrambled after the recorded content is retrieved from the storage (605) for use.

[00108] Alternatively, the bridge may record the scrambled content and the entitlement control message regardless the entitlement. The secondary CA server maintains data derived from the EMM (627), such as the service key, so that the recorded content can be later correlated with the corresponding data derived from the EMM (627) for decryption/descrambling operations.

[00109] After the renderer (607) retrieves the recorded content and the associated entitlement control message (617) from the storage (605), the renderer (605) sends the entitlement control message (625) to the secondary CA server (609) protected by the DRM system. The secondary

CA server (609) decodes the entitlement control message (625) and releases the control word (619) only when the access criteria are satisfied. The released control word (619) is protected under a DRM system so that only the renderer (607) with the appropriate rights (623) can use the released control word (619) to descramble the content retrieved from the storage (605).

[00110] In one embodiment of the present invention, the released control word (619) is access controlled according to the entitlement management message received for the time period when the content is recorded and/or according to the entitlement management message received for the time period when the content is retrieved for use. For example, a movie may be played back at any time after being recording if the subscriber is entitled to view it at the time of recording. Alternatively, a recorded movie may be viewed only if the user is a current subscriber. Thus, even if the user is authorized to play the movie at the time of recording, the secondary CA server still needs to verify that the user is currently a subscriber at the time of playback according to the entitlement management message for the current time period. In one embodiment of the present invention, a movie can be recorded even if the subscriber is not entitled to view it at the time of recording, since the entitlement may be obtained after the recording.

[00111] In one embodiment of the present invention, a CA system can send entitlement management messages for delayed authorization. For example, an entitlement management message may include a service key for the system to record the content without the authorization for playback. The secondary CA server (609) can manage the service key so that when the user is subsequently authorized to view the content, the CA system of the primary security system does not have to recall which service key was used for the recorded content. When the user obtains the authorization to view after the recording (e.g., through a pay-per-view scheme, or upgrading the subscription package), the secondary CA server (609) can decrypt the entitlement control message using the service key maintained by the secondary CA server.

[00112] In one embodiment of the present invention, the secondary CA server (609) communicates with the bridge (603) and the renderer (607) through a network connection. Alternatively, the secondary CA server (609) may communicate with either the bridge (603) or

the renderer (607) through a network connection (e.g., when the secondary CA server is integrated with either the renderer or the bridge).

[00113] **Figure 12** illustrates a system in which a secondary CA server is configured to decode the control words for capturing media content into a storage device according to one embodiment of the present invention. In **Figure 12**, the bridge (603) receives the broadcast feed (601), which includes the EMM (615), ECM (613) and CA protected content (611). The bridge (603) provides the EMM (627) and ECM (625) to the secondary CA server (609), which has the user key (621). The secondary CA server (609) recovers the control word (641) for descrambling the content. The secondary CA server provides the DRM protected control word to the authorized bridge (603) through a network connection. The authorized bridge descrambles the content and stores the content in the storage (605). The recorded content (643) in the storage (605) is protected using a DRM system. Only the renderer (607) with the appropriate rights (623) can use the recorded content (643). In one embodiment of the present invention, the rights to the recorded content (643) are derived from the entitlement management message and the entitlement control message of the CA system of the primary security system. In one embodiment, the rights are derived from the messages at the time of recording. In one embodiment of the present invention, the rights may be further changed according to subsequent entitlement management messages.

[00114] In one embodiment, the bridge (603) is combined with renderer (607), which can play back the media content in real time. Since the control word is provided through the network, unpredictable network delay may cause glitches in synchronizing the control word with the media stream. In one embodiment of the present invention, the bridge buffers a time period of media stream so that the network delay does not interrupt the continuous playback of the media stream.

[00115] In one embodiment of the present invention, a system can automatically switch between removing the CA protection at the time of recording and removing the CA protection at the time of playing back. For example, the system may automatically remove the CA protection

at the time of recording for the content that the user is entitled to use at the time of recording and remove the CA protection at the time of playing back for the content that the user is not entitled to use at the time of recording. Alternatively, the switching may be based on a user preference, or based on the capability of the components used on the system (e.g., whether or not a bridge has a standard descrambler, or whether or not renderer has a standard descrambler), or partially based on the data in an entitlement management message.

[00116] **Figure 13** illustrates a system in which a secondary CA server is configured to automatically decode the control words before capturing media content into a storage device, or after retrieving captured media content from the storage device, according to one embodiment of the present invention. In **Figure 13**, the bridge (603) receives the broadcast (601), which includes the EMM (615), ECM (613) and CA protected content (611). The bridge (603) provides the EMM (627) and ECM (625) to the secondary CA server (609), which has the user key (621). For the content that the user is entitled to use at the time of recording, the secondary CA server (609) extracts the control word (641) from the ECM (625) and EMM (627) for the bridge (603). The bridge (603) can then descramble the content. After the CA protection is removed, the content (643) in the storage (605) is placed in a DRM system to prevent unauthorized use. If the CA protection for the content is to be removed at the time of playback, the scrambled content and the ECM (617) are stored in the storage (605), protected by the DRM system. Alternatively, the secondary CA server (609) may manage the service keys for the decryption of the entitlement control message at a later time. After retrieving the CA protected content, if the CA protection is not already removed, the renderer (607) sends the ECM (625) to the secondary CA server (609) protected by the DRM system, which releases the control word (619) only to a renderer (607) with the appropriate rights (623).

[00117] In one embodiment of the present invention, a system according to the present invention performs a CA translation so that the condition access protection for a recorded content is more suitable for the protection of content stored on a storage.

[00118] **Figure 14** illustrates a system in which a secondary CA server is configured to generate substitutive entitlement control messages and decode the control words for the captured media content retrieved from a storage device according to one embodiment of the present invention. In **Figure 14**, the bridge (603) receives the broadcast (601), which includes the EMM (615), ECM_a (613) and CA protected content (611). The bridge (603) provides the EMM (627) and ECM_a (625) to the secondary CA server (609), which has the user key (621). The secondary CA server (609) decrypts the ECM_a (625) and generates the local ECM_b (651). The local ECM_b (651) is provided as a substitutive entitlement control message to replace the original entitlement control message for recording. Typically only the secondary CA server (609) can decrypt the local ECM_b (651). For example, the secondary CA server (609) may generate a unique service key to create local entitlement control message; alternatively, the secondary CA server (609) may encrypt the entitlement control message so that the local entitlement control message can only be decrypted using the user key (621). The local entitlement control message replaces the original entitlement control message; and the local entitlement control message and the scrambled contents are recorded in the storage (605). The recorded data (653) in the storage (605) may be optionally protected using a DRM system. To use the recorded content, the renderer (607) sends the local entitlement control message (655) back to the secondary CA server (609) protected by the DRM system to get in return the control word (619). To prevent unauthorized access, the secondary CA server provides the control word (619) under the protection of a DRM system so that only the renderer (607) with the appropriate rights (623) can use the control word (619).

[00119] In one embodiment of the present invention, a substitutive entitlement control message contains a control word that is different from the original control word in the original entitlement control message. In addition to sending the substitutive entitlement control message to the bridge (603), the secondary conditional server (609) also sends the original and the substitutive control words to the bridge (603), under the protection of a DRM system. The bridge (603) then descrambles the content using the original control word, re-scrambles the content

using the substitutive control word, and replaces the original entitlement control message with the substitutive entitlement control message for recording. In one embodiment of the present invention, the CA protection is translated so that the CA protection for the recorded content is suitable for the management of playing back. For example, an entire recorded movie may be re-scrambled using one same control word so that only one control word is need to play the entire recorded movie. In one embodiment of the present invention, the bridge and the secondary CA server are combined in one; thus, the secondary CA server can performed the task of the descrambling/re-scrambling. Alternatively, the bridge may send the content to the secondary condition access server through a network connection for the descrambling/re-scrambling task, which may increase the network traffic substantially.

[00120] **Figure 15** shows a method of using a secondary CA server according to one embodiment of the present invention. Operation 701 receives, at a secondary CA server, entitlement management messages of a primary security system (e.g., digital cable television, or satellite television, or a digital radio broadcast system). The entitlement management messages may be directly received from the primary security system, or indirectly received from a bridge through a network connection.. Operation 703 processes the entitlement management messages on the secondary CA server. The secondary CA server has data (e.g., a user key) representing the subscriber, which is used to access data in the entitlement management messages. Operation 705 transmits access controlled data that is in an access controlled format and that is at least partially derived from the entitlement management messages from the secondary CA server to a secondary CA client through a network connection. Operation 707 receives the access controlled data at the secondary CA client from the secondary CA server through the network connection. The access controlled data can be entitlement (such as a service key) extracted from the entitlement management messages, control word, a decrypted entitlement control message (e.g., for an entitlement control message received directly from the primary security system, indirectly from a bridge across a network connection, or retrieved from a storage), a substitutive

entitlement control message, control word descrambled content, control word rescrumbled content, etc.

[00121] **Figure 16** shows a detailed method of a secondary CA server according to one embodiment of the present invention. In one embodiment of the present invention, a secondary CA server can provide services to various different clients according to the requests received from the secondary CA clients. Operation 801 determines if an entitlement management message (EMM) is received. If an EMM is received (e.g., from a network bridge, or directly from the broadcast), operation 803 processes the EMM; and operation 805 determines the rights of secondary CA clients according to the data in the EMM. For example, the secondary CA server can extract the entitlement (such as the service key). Operation 807 determines if a request for data is received from a secondary CA client. If a request for data is received, operation 809 determines if the client is entitled to use the data.

[00122] In one embodiment of the present invention, a network bridge may record the content even if the subscriber is not entitled to use the content at the time of recording, since the subscriber may obtain the authorization to use the recorded content after the content is recorded. The network bridge may request a substitutive ECM even if the bridge is not entitled to use. The substitutive ECM is encrypted so that the network bridge cannot obtain the control word from the substitutive ECM. The network bridge can replace the original ECM with the substitutive ECM for recording so that when the subscriber later obtains the authorization to play back the content, the secondary CA server can decrypt the substitutive ECM.

[00123] In one embodiment, if operation 809 determines the client is not entitled to use the data and operation 811 determines the request is not for a substitutive ECM, access to the data is denied in operation 813. If the request is for a substitutive ECM, operation 815 determines if the decryption key for the ECM is available. In one embodiment of the present invention, a CA system may or may allow the recording of certain content. Thus, the secondary conditional server may or may not have the decryption key for the ECM. If the decryption is not available, operation 813 denies the access; otherwise, operation 817 generates a substitutive ECM through

decrypting the original ECM and re-encrypting the ECM so that the substitutive ECM can be later decrypted using a key available to the secondary CA server. Operation 819 then sends the substitutive ECM to the secondary CA client.

[00124] If operation 809 determines the client is entitled to use the data, operation 825 determines if an ECM is received for processing. An ECM may be received from a secondary CA client (e.g., from a bridge that obtains the ECM from the broadcast, or from a renderer that obtains the ECM from a storage for recorded media content) or directly from the broadcast. If an ECM is received for processing, operation 827 determines the decryption key of the ECM. The decryption key may be derived from a recently received EMM, or from the data maintained by the secondary CA server for recorded content. The decryption key can be used to access the control word in the ECM. If operation 827 determines that the request is for the control word, operation 831 sends the control word to the secondary CA client. The control word can be sent in a similar way for sending the service key to prevent unauthorized use. Other data, such as descrambled content, can also be sent in a similar way.

[00125] If operation 829 determines the request is not for the control word and operation 833 determines the request is for a substitutive ECM, operation 835 determines if rescrambling is required. If rescrambling is required, operation 837 obtains a new control word; and operation 839 sends both the original and the new control words to the secondary CA client. Operation 841 generates a substitutive ECM. The substitutive ECM has the new control word if rescrambling is required; otherwise, the substitutive ECM contains the original control word. Operation 843 then sends the substitutive ECM to the secondary CA client.

[00126] If operation 845 determines the request is for content, operation 849 determines whether the scrambled content is received. If the content is not received, operation 851 retrieves the content from a storage. In one embodiment of the present invention, the secondary CA server has a storage to record the scrambled content. Then, the secondary CA server processes the scrambled content.

[00127] If operation 853 determines descrambling is required, operation 855 control word descrambles the content using the control word in the ECM associated with the content. If operation 857 determines that rescrambling is required, operation 859 control word rescrambles the content using a new control word. If operation 861 determines that the request is for recording the content, operation 865 stores the content; otherwise, operation 863 sends the content to the secondary CA client.

[00128] If operation 845 determines the request is for the content, operation 847 further processes request. For example, the client may request the entitlement information, available contents recorded on a storage, rights to play back or record, or others.

[00129] It is understood that **Figure 16** illustrates an example flow chart of the operations in a secondary CA server according to one embodiment of the present invention. Some implementations of secondary CA servers may include more or less operations. And the operation sequences are illustrative. From this description, one person skilled in the art understands that many variations and combinations can be implemented.

[00130] In one embodiment of the present invention, various components, such as a bridge, a renderer, a secondary CA server, a storage, or various different combinations of these components, can be implemented using a digital data processing system, such as a computer.

[00131] **Figure 1** shows one example of a typical computer system which may be used with the present invention. Note that while **Figure 1** illustrates various components of a computer system, it is not intended to represent any particular architecture or manner of interconnecting the components as such details are not germane to the present invention. It will also be appreciated that network computers and other data processing systems which have fewer or more components may also be used with the present invention. The computer system of **Figure 1** may, for example, be a Sun workstation, or a personal computer (PC) running a Windows operating system, or an Apple Macintosh computer, or a set top box, or other media controller.

[00132] As shown in **Figure 1**, the computer system 101, which is a form of a data processing system, includes a bus 102 and system core logic 112 which interconnect a microprocessor 103,

a ROM 107, and volatile RAM 105 and a non-volatile memory 106. The microprocessor 103, which may be, for example, a G3 or G4 or G5 microprocessor from Motorola, Inc. or IBM is coupled to cache memory 104 as shown in the example of **Figure 1**. The bus 102 and system core logic 112 interconnect these various components together and also interconnects these components 103, 107, 105, and 106 to a display controller and display device 108 and to peripheral devices such as input/output (I/O) devices which may be mice, keyboards, modems, network interfaces, printers, scanners, video cameras and other devices which are well known in the art. Typically, the input/output devices 110 are coupled to the system through input/output controllers 109. The volatile RAM 105 is typically implemented as dynamic RAM (DRAM) which requires power continually in order to refresh or maintain the data in the memory. The non-volatile memory 106 is typically a magnetic hard drive, a magnetic optical drive, or an optical drive (e.g., a DVD RAM), or other type of memory system which maintains data even after power is removed from the system. Typically, the non-volatile memory will also be a random access memory although this is not required. While **Figure 1** shows that the non-volatile memory is a local device coupled directly to the rest of the components in the data processing system, it will be appreciated that the present invention may utilize a non-volatile memory which is remote from the system, such as a network storage device that is coupled to the data processing system through a network interface such as a modem or Ethernet interface. The bus 102 may include one or more buses connected to one another through various bridges, controllers and/or adapters as is well known in the art. In one embodiment the I/O controller 109 includes a USB (Universal Serial Bus) adapter for controlling USB peripherals, and/or an IEEE-1394 bus adapter for controlling IEEE-1394 peripherals.

[00133] It will be apparent from this description that aspects of the present invention may be embodied, at least in part, in software. That is, the techniques may be carried out in a computer system or other data processing system in response to its processor, such as a microprocessor, executing sequences of instructions contained in a memory, such as ROM 107, volatile RAM 105, non-volatile memory 106, cache 104 or a remote storage device. In various embodiments,

hardwired circuitry may be used in combination with software instructions to implement the present invention. Thus, the techniques are not limited to any specific combination of hardware circuitry and software nor to any particular source for the instructions executed by the data processing system. In addition, throughout this description, various functions and operations are described as being performed by or caused by software code to simplify description. However, those skilled in the art will recognize what is meant by such expressions is that the functions result from execution of the code by a processor, such as the microprocessor 103.

[00134] A machine readable medium can be used to store software and data which when executed by a data processing system causes the system to perform various methods of the present invention. This executable software and data may be stored in various places including for example ROM 107, volatile RAM 105, non-volatile memory 106 and/or cache 104 as shown in **Figure 1**. Portions of this software and/or data may be stored in any one of these storage devices.

[00135] Thus, a machine readable medium includes any mechanism that provides (i.e., stores and/or transmits) information in a form accessible by a machine (e.g., a computer, network device, personal digital assistant, manufacturing tool, any device with a set of one or more processors, etc.). For example, a machine readable medium includes recordable/non-recordable media (e.g., read only memory (ROM), random access memory (RAM), magnetic disk storage media, optical storage media, flash memory devices, etc.), as well as electrical, optical, acoustical or other forms of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.), etc.

[00136] In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will be evident that various modifications may be made thereto without departing from the broader spirit and scope of the invention as set forth in the following claims. The specification and drawings are, accordingly, to be regarded in an illustrative sense rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to control a presentation of content, wherein a first conditional access server has authenticated a client of the first conditional access server through a first authentication process that used a first root of trust, the method comprising:
 - receiving, at a second conditional access server, content from the client of the first conditional access server in a first security domain;
 - processing the content on the second conditional access server;
 - authorizing a client of the second conditional access server to present content in accordance with authorization the second conditional access server received from the first conditional access server;
 - transmitting, from the second conditional access server to the client of the second conditional access server through a network connection in a second security domain, the content that is in an access controlled format that is specified by the second conditional access server; and
 - wherein the second conditional access server authenticates client devices of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust.
2. The medium of claim 1, wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain and wherein the content is video content.

3. The medium of claim 2, wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the client device of the second conditional access server comprises a digital rights management client.

4. The medium of claim 1, wherein the client of the first conditional access server receives security messages from the first conditional access server and the security messages comprise an entitlement management message and an entitlement control message; and wherein the second conditional access server generates a substitutive entitlement control message as a replacement of the entitlement control message.

5. A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause a client system in a second security domain to present content provided by a first conditional access server wherein the first conditional access server has authenticated a client device of the first conditional access server through a first authentication process using a first root of trust for a first security domain and wherein a second conditional access server is configured to substitute the first security domain with the second security domain for client devices under a second root of trust, the method comprising:

receiving, at a second conditional access client of the second conditional access server, an authentication through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses the second root of trust for the second security domain which is independent of and different than the first root of trust; and

receiving, at the second conditional access client, content that is in an access controlled format specified by the second conditional access server in the second security domain, the second conditional access client being in the second security domain.

6. The medium in claim 5, wherein the second conditional access client does not have a user key representing a subscriber of the first security system.

7. The medium in claim 5, wherein the content comprises a decrypted version of an entitlement control message.
8. The medium in claim 5, wherein the content comprises a result of descrambling data scrambled by a conditional access system of the first security system.
9. A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method by a first conditional access server in a first security domain to provide conditional access in an environment which includes a second conditional access server that has authenticated a client of the second conditional access server through a second authentication process that used a second root of trust for a second security domain and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for client devices under the second root of trust, the method comprising:
- receiving, from the client of the second conditional access server in the second security domain via the second conditional access server, a client request for the transmission of content protected by the first conditional access server;
 - broadcasting the requested content from the first conditional access server in the first security domain;
 - receiving, from the client of the second conditional access server, a client request to use the content after said broadcasting; and
 - responding to the client request from the client of the second conditional access server via the second conditional access server,
- wherein the first conditional access server authenticates a client device of the first conditional access server through a first authentication process using a first root of trust which is independent of and different than the second authentication process and the second root of trust.
10. The medium of claim 9, wherein the method further comprises:
- transmitting a second entitlement management message to authorize the client to playback the data response to the client request.

11. The medium of claim 10, wherein the client of the second conditional access server caches the broadcasted content but is not authorized to use the content before the second entitlement management message.
12. A method to control a presentation of content, wherein a first conditional access server has authenticated a client of the first conditional access server through a first authentication process that used a first root of trust, the method comprising:
- receiving, at a second conditional access server, content from the client of the first conditional access server in a first security domain;
 - processing the content on the second conditional access server;
 - authorizing a client of the second conditional access server to present content in accordance with authorization the second conditional access server received from the first conditional access server;
 - transmitting, from the second conditional access server to the client of the second conditional access server through a network connection in a second security domain, the content that is in an access controlled format that is specified by the second conditional access server; and
- wherein the second conditional access server authenticates client devices of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust.
13. The method of claim 12, wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain and wherein the content is video content.

14. The method of claim 13, wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the client device of the second conditional access server comprises a digital rights management client.

15. The method of claim 12, wherein the client of the first conditional access server receives security messages from the first conditional access server and the security messages comprise an entitlement management message and an entitlement control message; and wherein the second conditional access server generates a substitutive entitlement control message as a replacement of the entitlement control message.

16. A method at a client system in a second security domain to present content provided by a first conditional access server wherein the first conditional access server has authenticated a client device of the first conditional access server through a first authentication process using a first root of trust for a first security domain and wherein a second conditional access server is configured to substitute the first security domain with the second security domain for client devices under a second root of trust, the method comprising:

receiving, at a second conditional access client of the second conditional access server, an authentication through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses the second root of trust for the second security domain which is independent of and different than the first root of trust; and
receiving, at the second conditional access client, content that is in an access controlled format specified by the second conditional access server in the second security domain, the second conditional access client being in the second security domain.

17. The method in claim 16, wherein the second conditional access client does not have a user key representing a subscriber of the first security system.

18. The method in claim 16, wherein the content comprises a decrypted version of an entitlement control message.

19. The method in claim 16, wherein the content comprises a result of descrambling data scrambled by a conditional access system of the first security system.

20. A method by a first conditional access server in a first security domain to provide conditional access in an environment which includes a second conditional access server that has authenticated a client of the second conditional access server through a second authentication process that used a second root of trust for a second security domain and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for client devices under the second root of trust, the method comprising:

receiving, from the client of the second conditional access server in the second security domain via the second conditional access server, a client request for the transmission of content protected by the first conditional access server;

broadcasting the requested content from the first conditional access server in the first security domain;

receiving, from the client of the second conditional access server, a client request to use the content after said broadcasting; and

responding to the client request from the client of the second conditional access server via the second conditional access server,

wherein the first conditional access server authenticates a client device of the first conditional access server through a first authentication process using a first root of trust which is independent of and different than the second authentication process and the second root of trust.

21. The method of claim 20, wherein the method further comprises:

transmitting a second entitlement management message to authorize the client to playback the data response to the client request.

22. The method of claim 21, wherein the client of the second conditional access server caches the broadcasted content but is not authorized to use the content before the second entitlement management message.

ABSTRACT OF THE DISCLOSURE

Conditional access to media content of primary security systems on a secondary networked environment. In one embodiment, a conditional access server is used to provide services to secondary CA clients (e.g., a bridge, a renderer, a storage, or their different combinations) through network connections. Containing data representing the subscriber, a conditional access server recovers entitlement data and/or decryption keys of a primary security system for the conditional access protected content, such as service keys and control words, and/or enforces conditional access to the content by secondary CA clients according to the authorization of the primary security system for the secondary CA clients. In one embodiment, a conditional access system provides delayed authorization for use so that the content can be recorded for later use when authorized and broadcasts rights for use on multiple secondary CA clients.

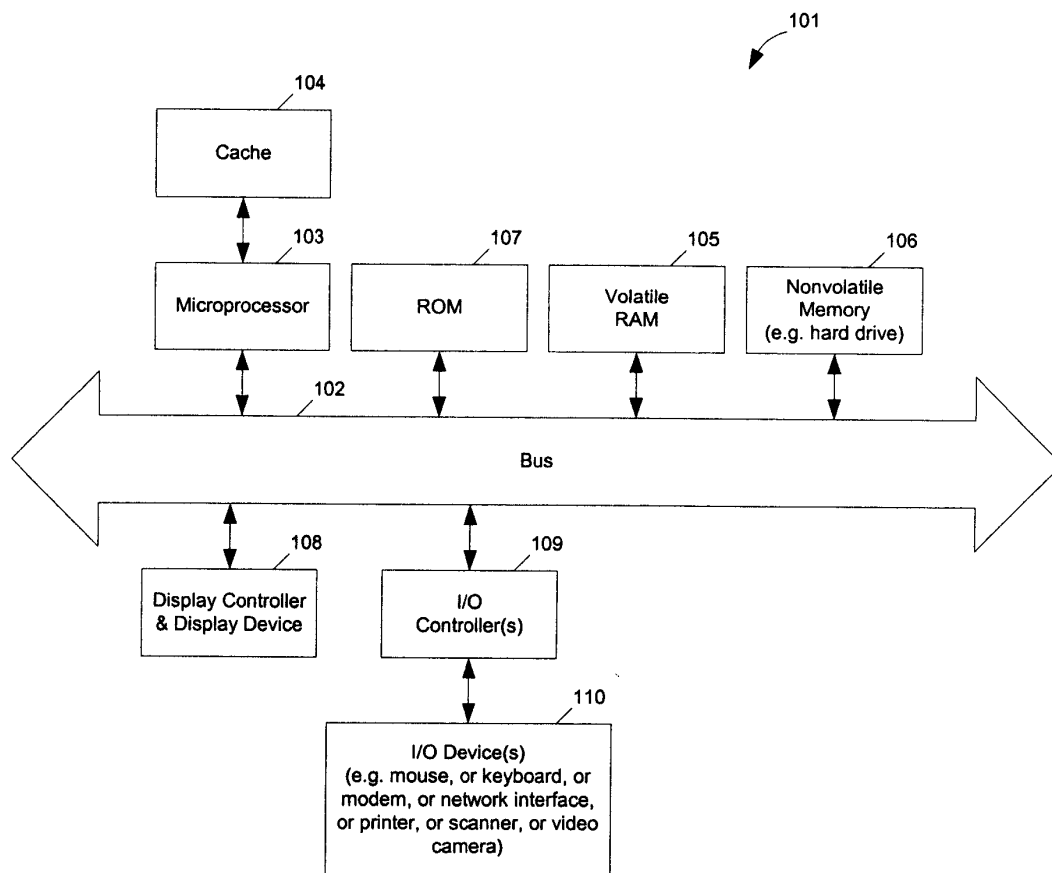


Fig. 1

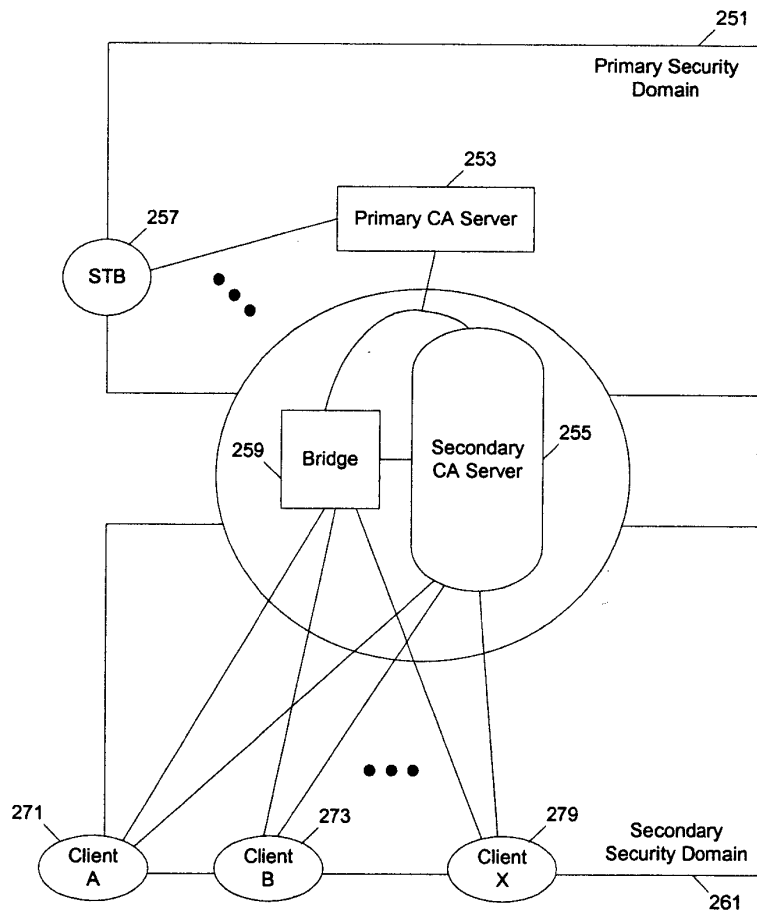


Fig. 2A

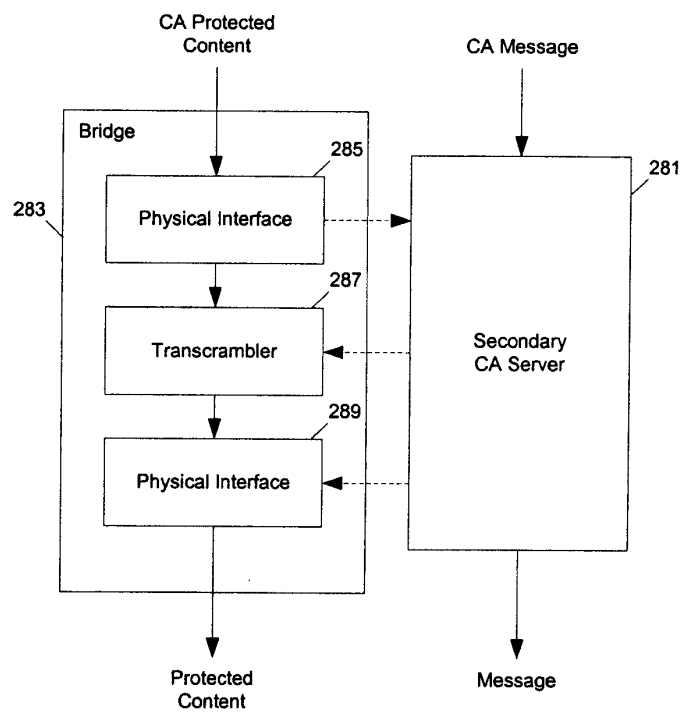


Fig. 2B

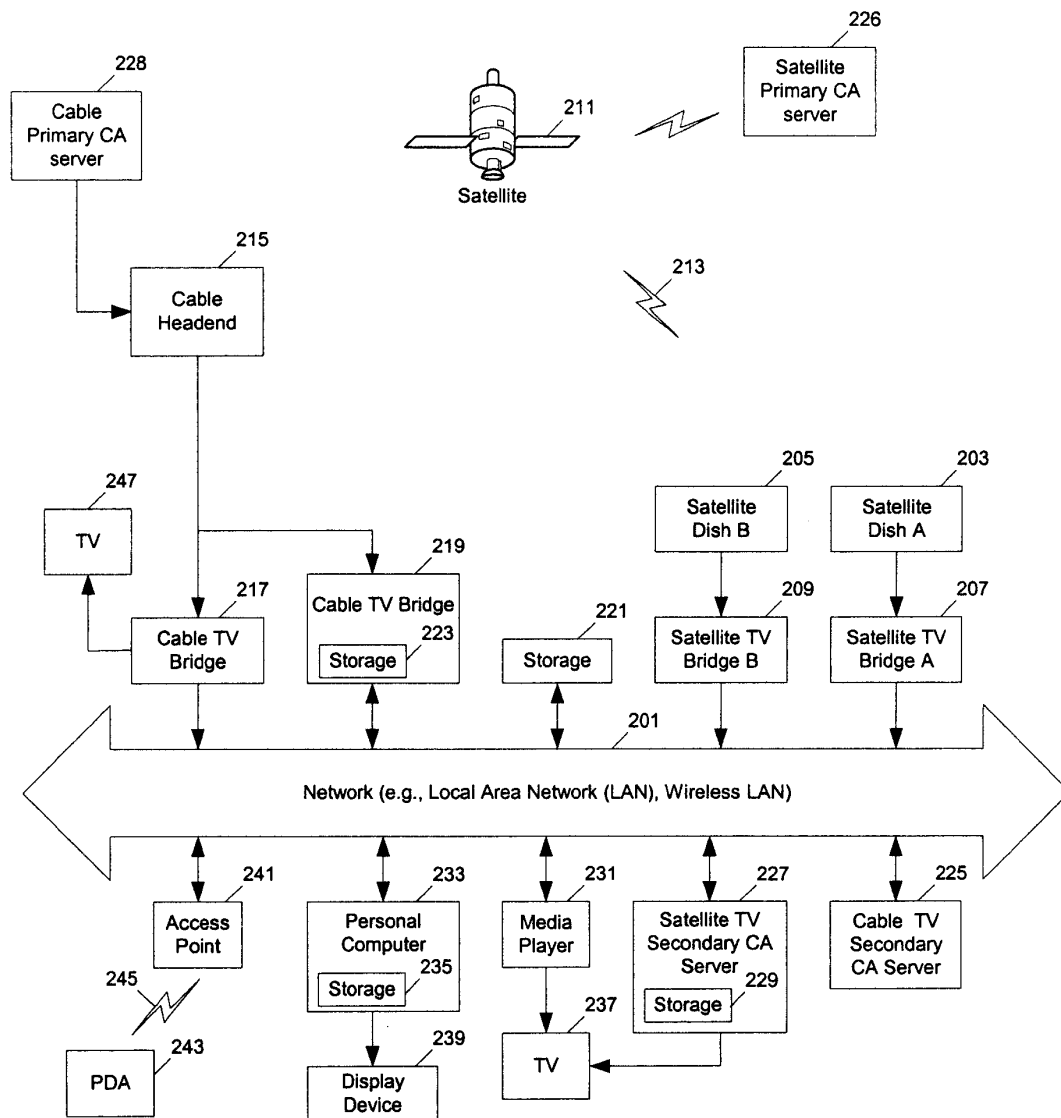


Fig. 3

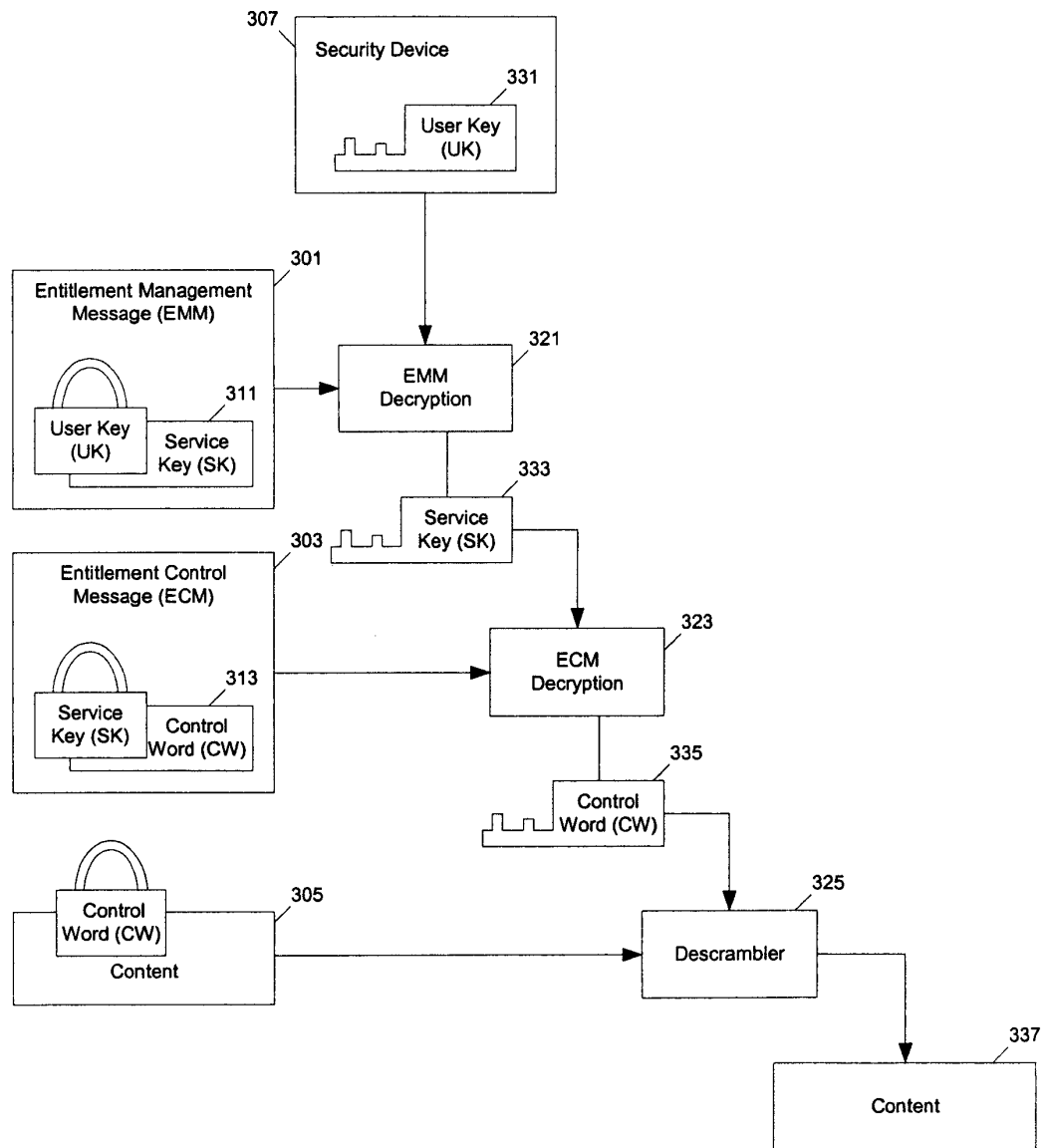


Fig. 4

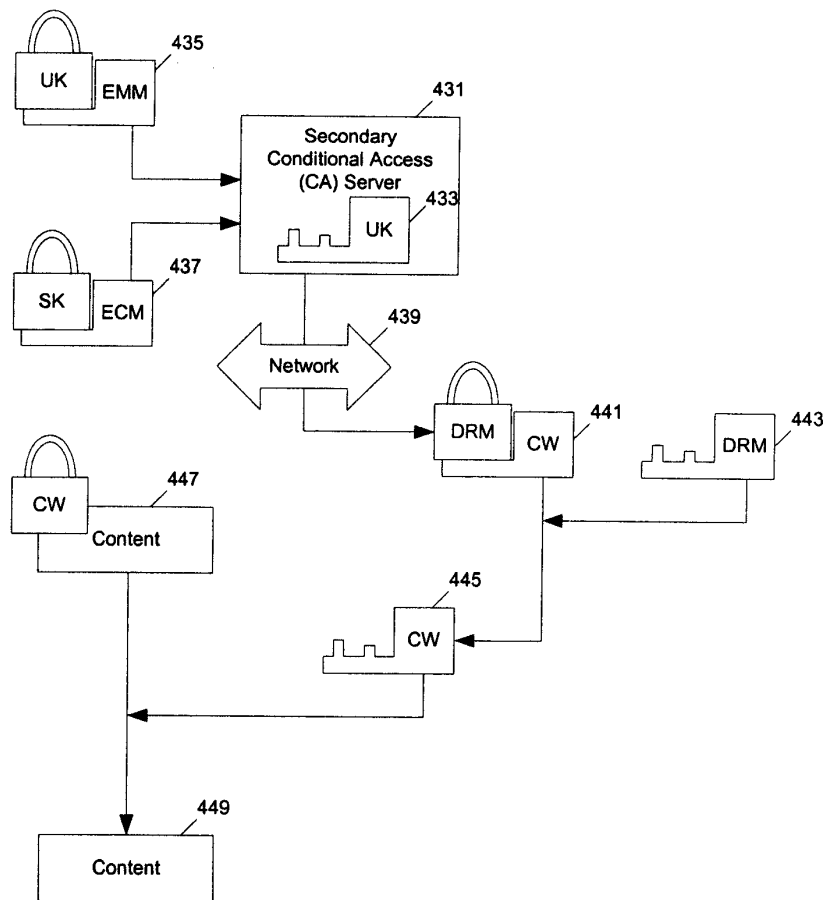


Fig. 5

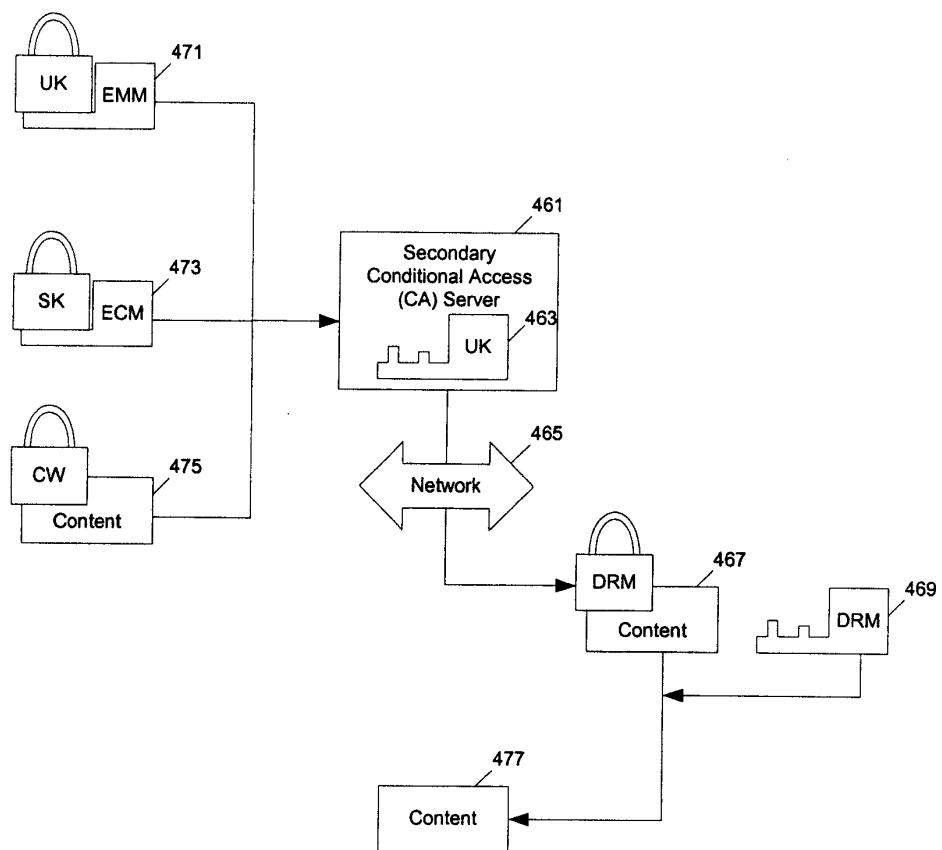


Fig. 6

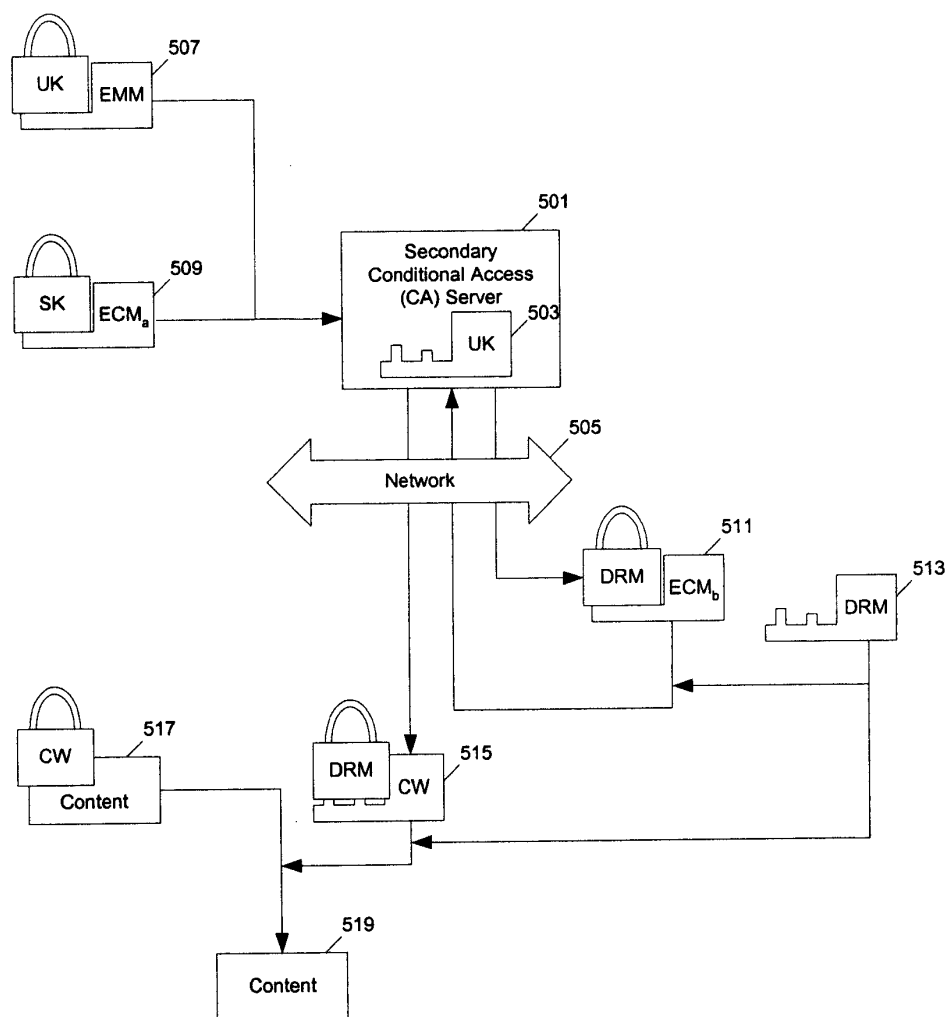


Fig. 7

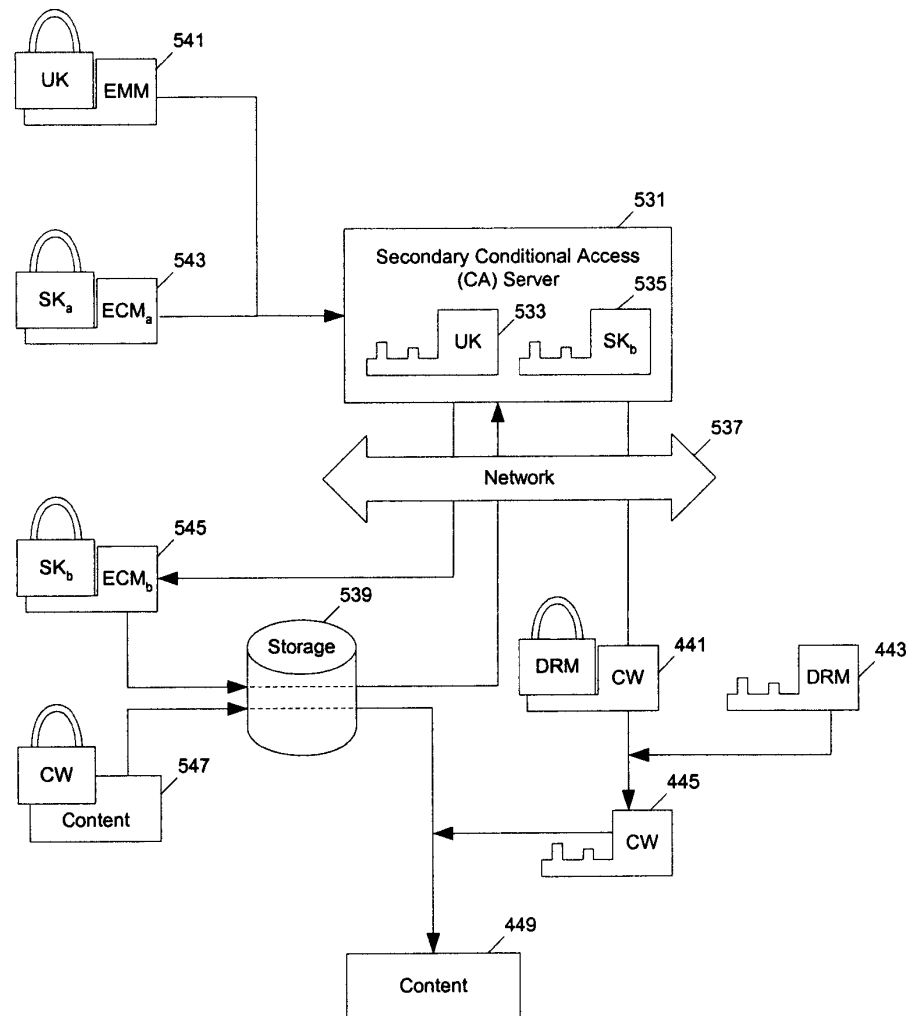


Fig. 8

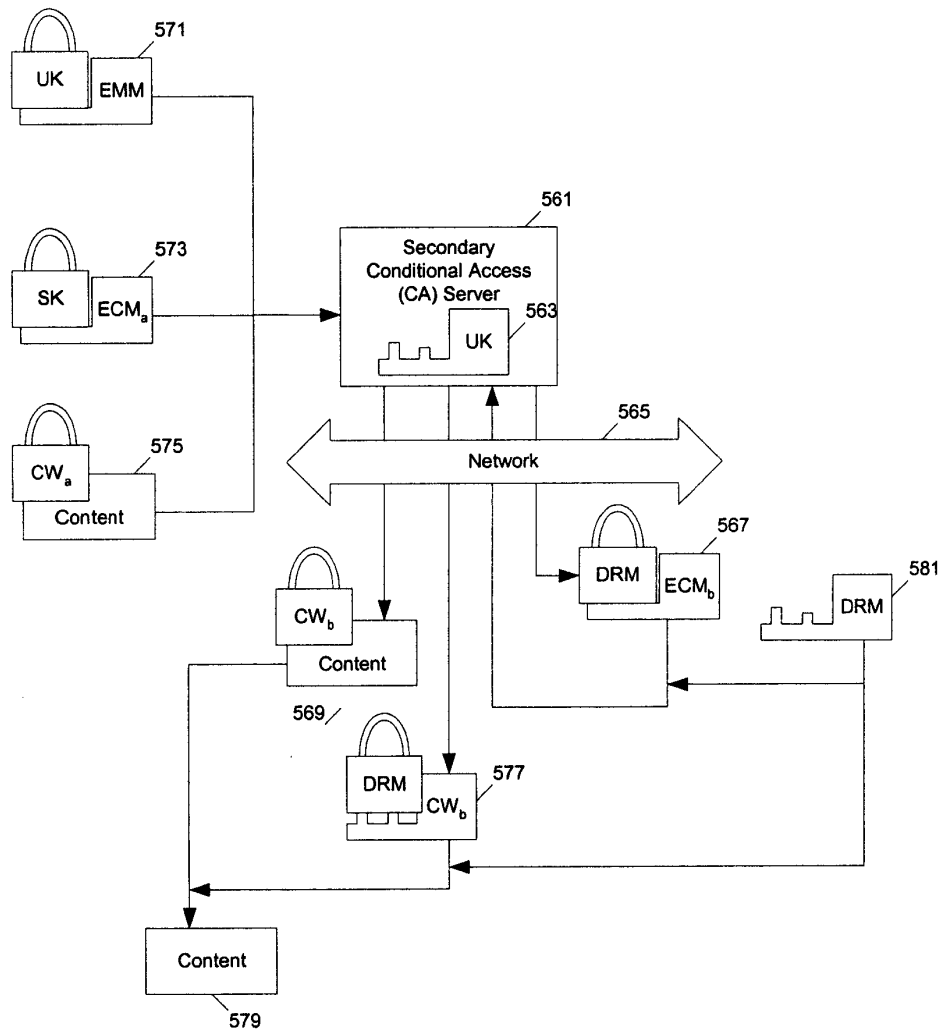


Fig. 9

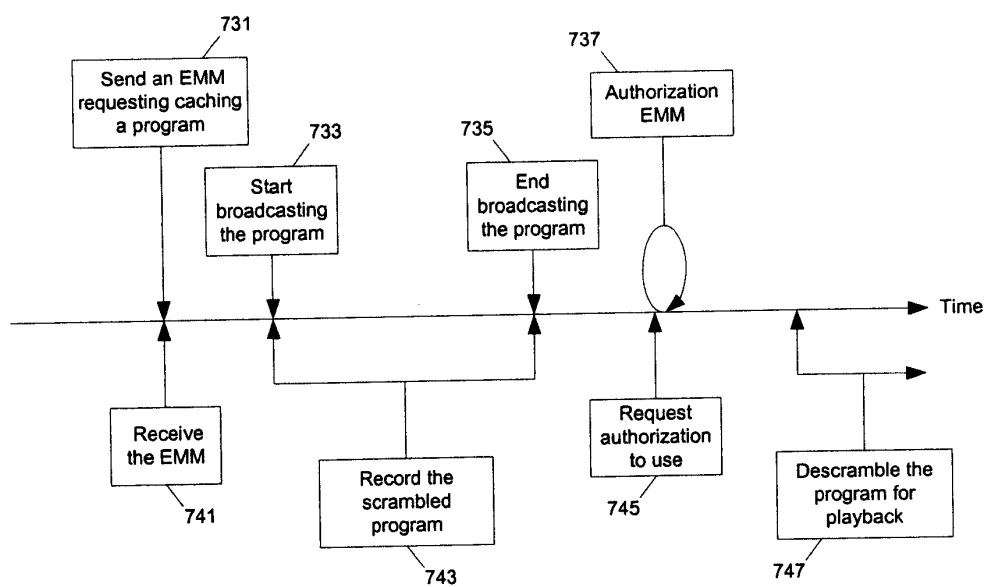
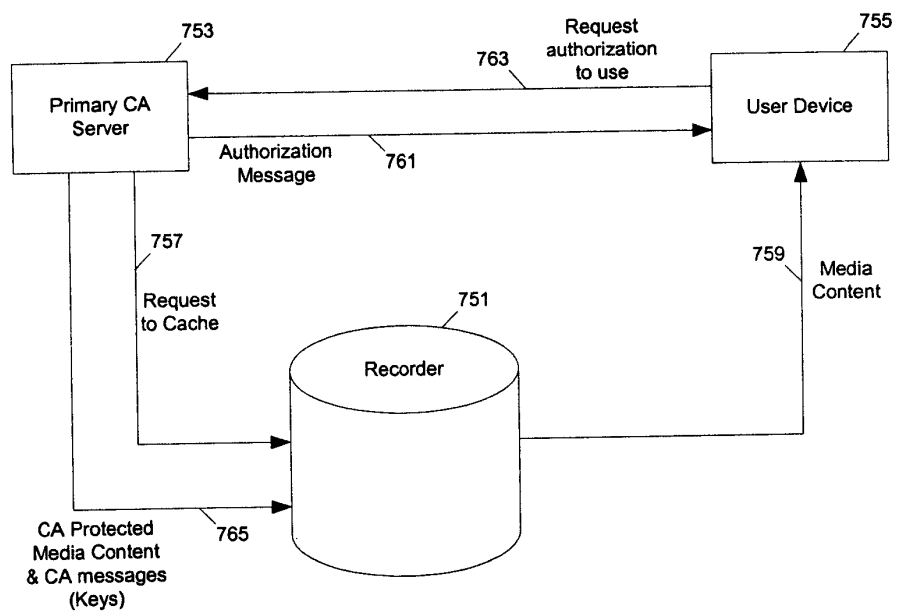


Fig. 10A



(Prior Art)

Fig. 10B

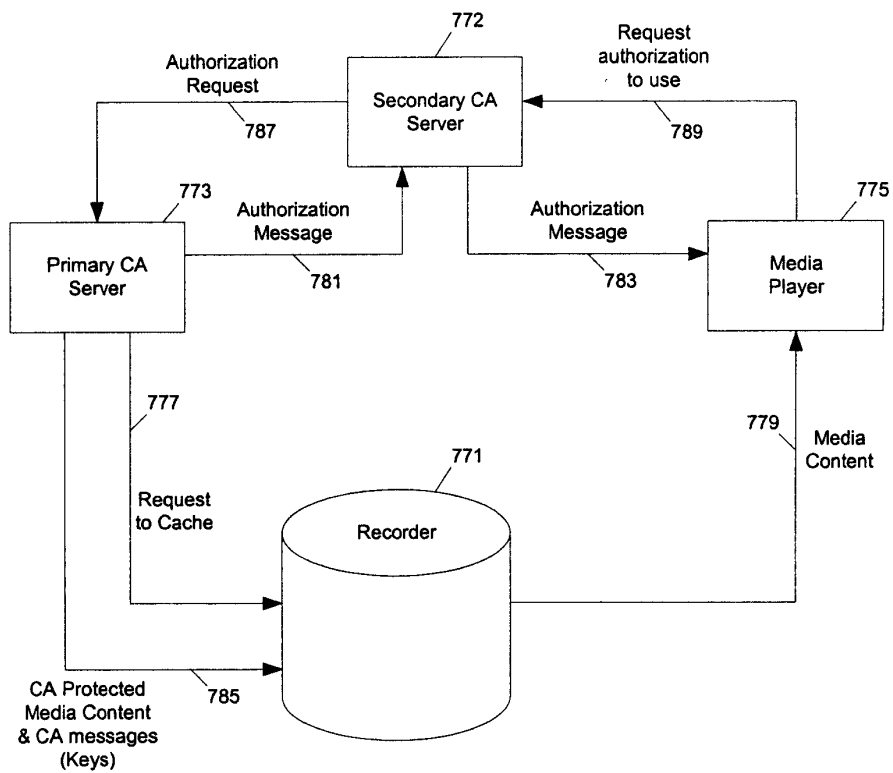


Fig. 10C

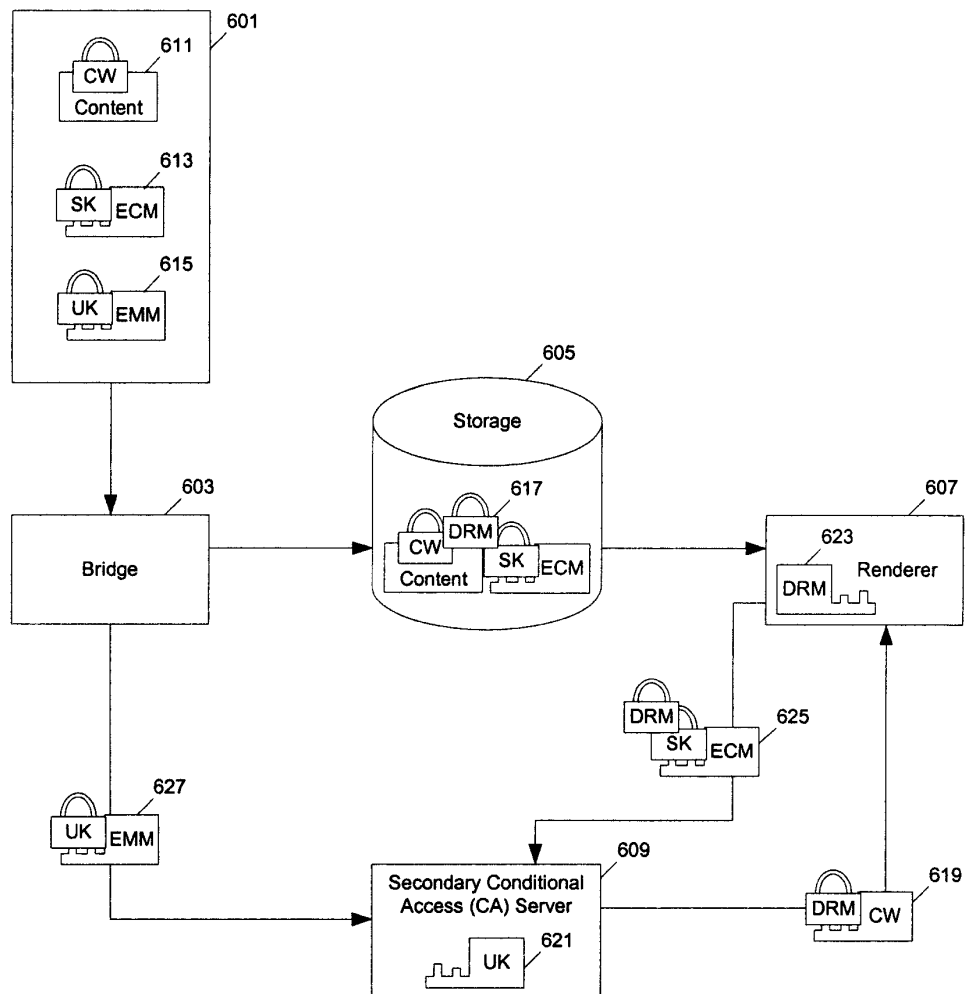


Fig. 11

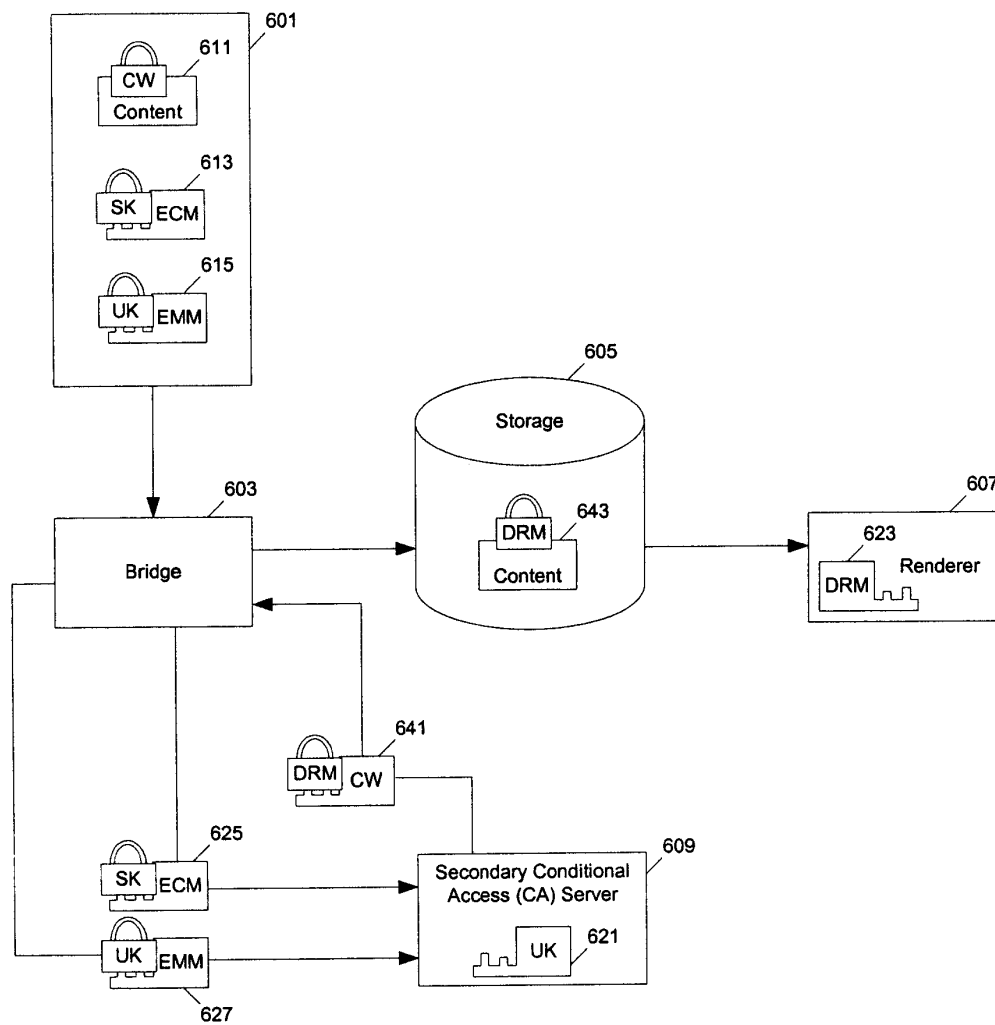


Fig. 12

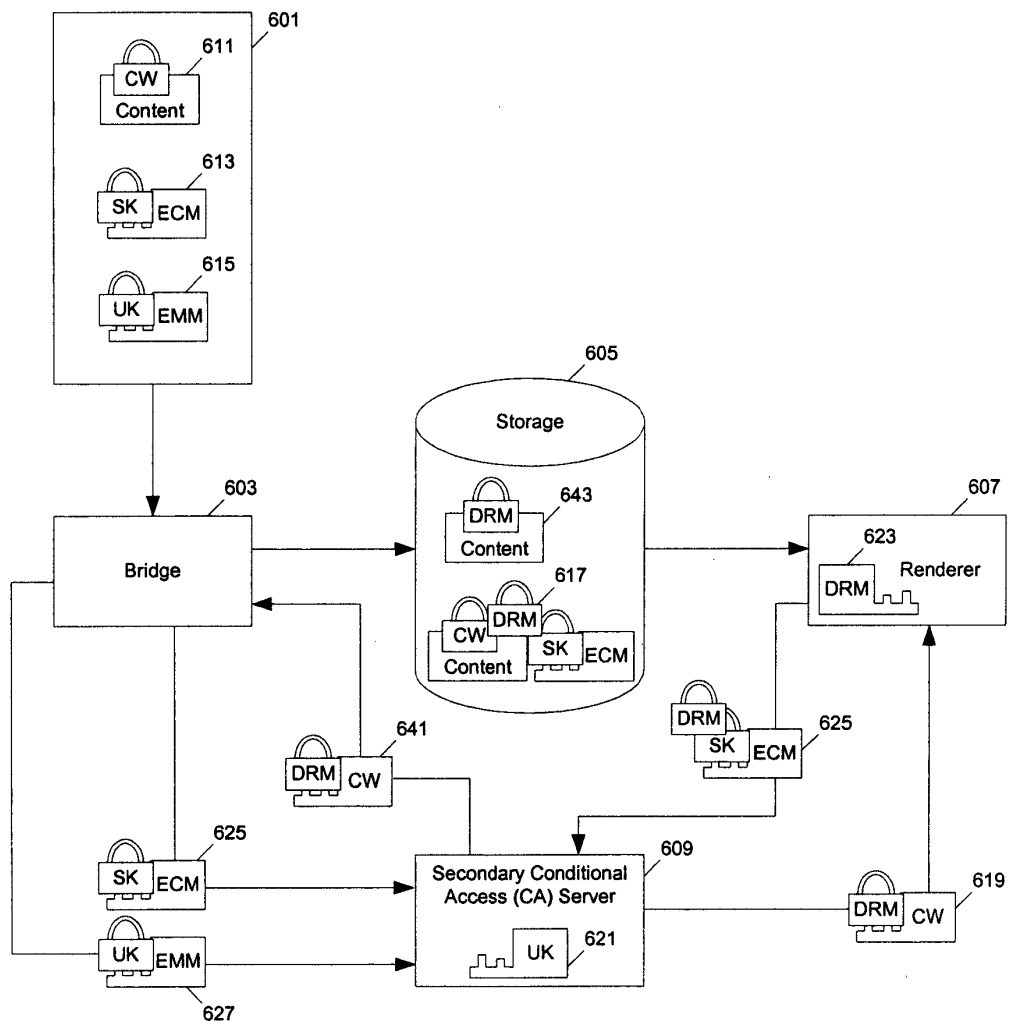


Fig. 13

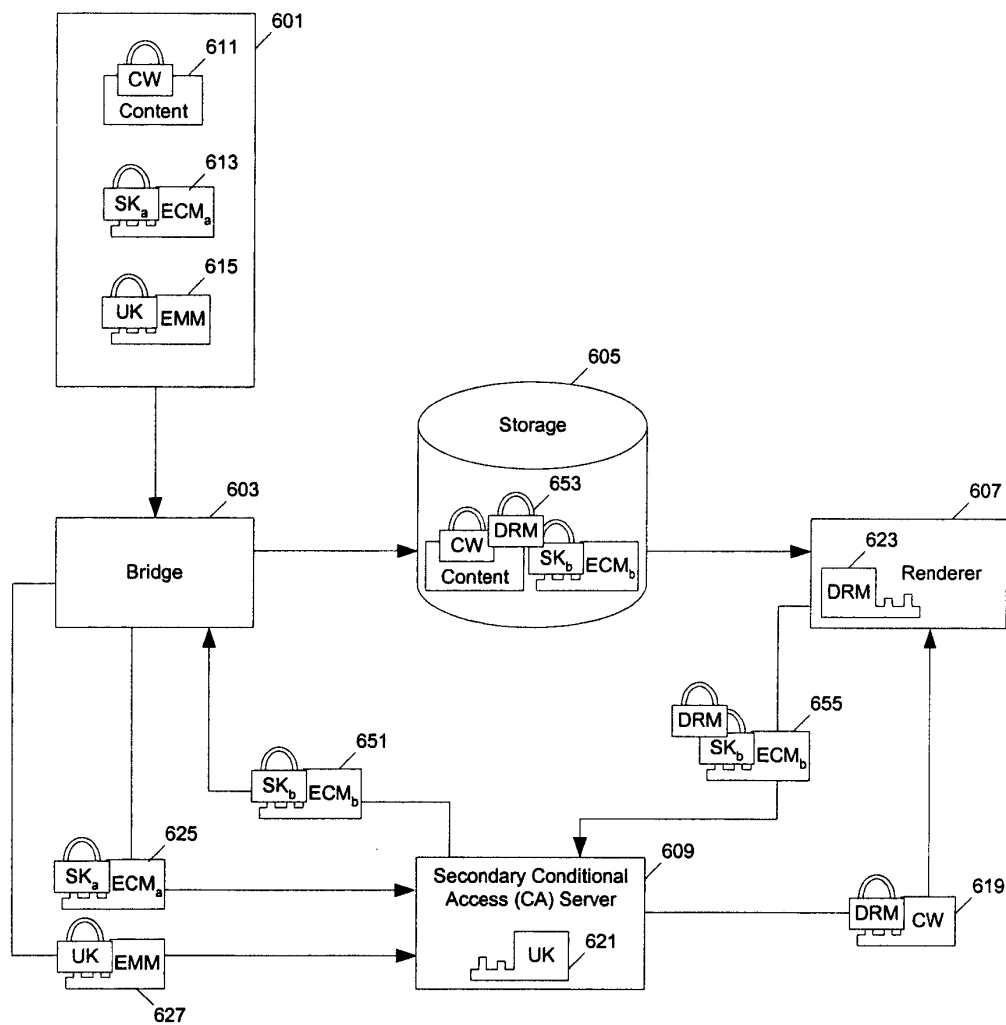


Fig. 14

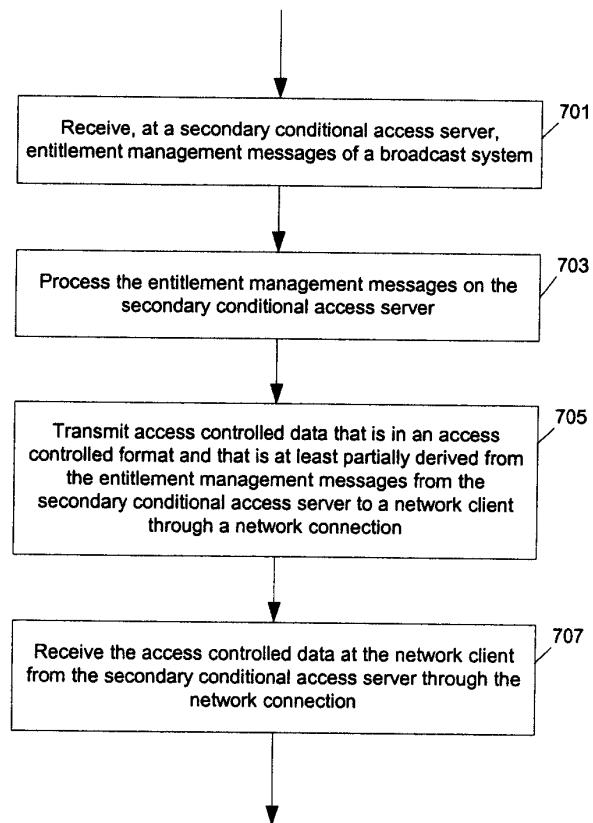


Fig. 15

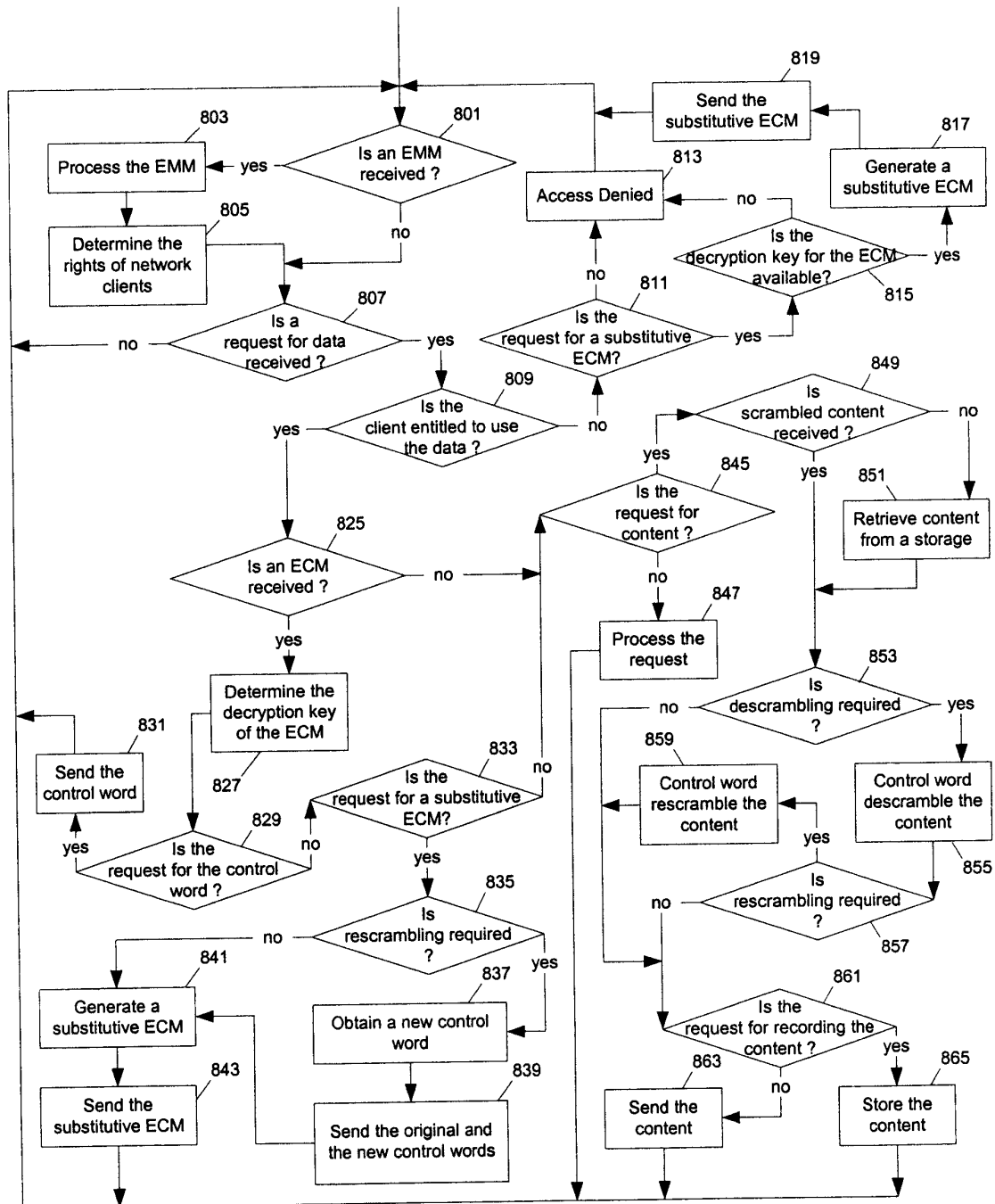


Fig. 16

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER		
First Named Inventor/Applicant Name:		Luc Vantalon		
Filer:		James Scheller Jr./Connie Thayer		
Attorney Docket Number:		06517.P002C		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility application filing	1011	1	380	380
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Pages:				
Claims:				
Claims in excess of 20	1202	2	60	120
Independent claims in excess of 3	1201	3	250	750
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				2120

Electronic Acknowledgement Receipt	
EFS ID:	13728966
Application Number:	13612663
International Application Number:	
Confirmation Number:	6713
Title of Invention:	METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	8791
Filer:	James Scheller Jr./Connie Thayer
Filer Authorized By:	James Scheller Jr.
Attorney Docket Number:	06517.P002C
Receipt Date:	12-SEP-2012
Filing Date:	
Time Stamp:	20:28:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$2120
RAM confirmation Number	9723
Deposit Account	022666
Authorized User	
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)</p>	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	06517P002C_new_appln_transmittal.pdf	99374	no	2
			2764bf43ce3403ea5716e6abc22bc5023d76db52		
Warnings:					
Information:					
2	Oath or Declaration filed	06517P002C_declaration.pdf	280449	no	3
			714632c627d28b950b0b8ee45c48b3c341487b23		
Warnings:					
Information:					
3		06517P002C_application.pdf	2441645	yes	48
			305739a09385e345ae6377c0daca78f1756ddf2d		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	41	
	Claims		42	47	
	Abstract		48	48	
Warnings:					
Information:					
4	Drawings-only black and white line drawings	06517P002C_formal_drawings.pdf	551255	no	19
			13c0695a5f76e2dcca5f6da88b4bad19a27ce747		
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	37706	no	2
			42afddc696c507571406c3a6e3f954f502da3ef3		
Warnings:					
Information:					
Total Files Size (in bytes):			3410429		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt	
EFS ID:	13728966
Application Number:	13612663
International Application Number:	
Confirmation Number:	6713
Title of Invention:	METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	8791
Filer:	James Scheller Jr./Connie Thayer
Filer Authorized By:	James Scheller Jr.
Attorney Docket Number:	06517.P002C
Receipt Date:	12-SEP-2012
Filing Date:	
Time Stamp:	20:28:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$2120
RAM confirmation Number	9723
Deposit Account	022666
Authorized User	
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)</p>	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	06517P002C_new_appln_transmittal.pdf	99374	no	2
			2764bf43ce3403ea5716e6abc22bc5023d76db52		
Warnings:					
Information:					
2	Oath or Declaration filed	06517P002C_declaration.pdf	280449	no	3
			714632c627d28b950b0b8ee45c48b3c341487b23		
Warnings:					
Information:					
3		06517P002C_application.pdf	2441645	yes	48
			305739a09385e345ae6377c0daca78f1756ddf2d		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	41	
	Claims		42	47	
	Abstract		48	48	
Warnings:					
Information:					
4	Drawings-only black and white line drawings	06517P002C_formal_drawings.pdf	551255	no	19
			13c0695a5f76e2dcca5f6da88b4bad19a27ce747		
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	37706	no	2
			42afddc696c507571406c3a6e3f954f502da3ef3		
Warnings:					
Information:					
Total Files Size (in bytes):			3410429		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 13/612,663				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	380			
SEARCH FEE (37 CFR 1.16(k), (j), or (m))	N/A	N/A	N/A			N/A	620			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250			
TOTAL CLAIMS (37 CFR 1.16(i))	22	minus 20 = *	2			x 60 =	120			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	6	minus 3 = *	3			x 250 =	750			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL		TOTAL	2120			
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=		x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=		x	=
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=		x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=		x	=
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	
<div style="font-size: x-small;"> * If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1. </div>										



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
13/612,663	09/12/2012	2431	2120	06517.P002C	22	6

CONFIRMATION NO. 6713

8791

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 Oakmead Parkway
Sunnyvale, CA 94085-4040

FILING RECEIPT



OC000000056731267

Date Mailed: 09/27/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Luc Vantalón, Sunnyvale, CA;
Paolo Siccardo, Los Altos, CA;

Applicant(s)

Luc Vantalón, Sunnyvale, CA;
Paolo Siccardo, Los Altos, CA;

Power of Attorney: The patent practitioners associated with Customer Number 08791

Domestic Priority data as claimed by applicant

This application is a CON of 11/007,116 12/07/2004 PAT 8291236

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.)

If Required, Foreign Filing License Granted: 09/24/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/612,663**

Projected Publication Date: 01/03/2013

Non-Publication Request: No

Early Publication Request: No

Title

METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

Preliminary Class

380

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

Substitute for Form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/612,663
				Filing Date	September 12, 2012
				First Named Inventor:	Luc Vantalon
				Art Unit	2431
				Confirmation No.	6713
				Examiner Name	Not Yet Assigned
				Attorney Docket No.	06517.P002C
Sheet	1	of	2		

U.S. PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Document Number		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code ² (if known)			
		2003/0196092	A1	10-16-2003	Raley, M. et al.	
		2004/0196842	A1	10-07-2004	Dobbins, Kurt A.	
		2005/0021539	B2	01-27-2005	Short et al.	
		6,961,858	B2	11-01-2005	Fransdonk, Robert W.	
		7,036,011	B2	04-25-2006	Grimes et al.	
		7,127,619	B2	10-24-2006	Unger et al.	
		7,152,160	B2	12-19-2006	Lantto et al.	
		7,171,558	B1	01-30-2007	Mourad et al.	
		7,171,588	B2	01-30-2007	Friedman et al.	
		7,174,021	B2	02-06-2007	Krishnaswamy et al.	
		7,177,429	B2	02-13-2007	Moskowitz et al.	
		7,292,692	B2	11-06-2007	Bonan et al.	
		7,296,154	B2	11-13-2007	Evans et al.	
		7,302,058	B2	11-27-2007	Candelore, Brant L.	
		7,316,032	B2	01-01-2008	Tayebi et al.	
		7,325,140	B2	01-29-2008	Carley, Jeffrey Alan	
		7,336,784	B2	02-26-2008	Zuili, Patrick	
		7,493,291	B2	02-17-2009	Simelius, Kim	
		7,546,641	B2	06-09-2006	Robert et al.	
		7,685,206	B1	03-23-2010	Mathew et al.	
		7,757,299	B2	07-13-2010	Robert et al.	

FOREIGN PATENT DOCUMENTS							
Examiner Initials*	Cite No. ¹	Foreign Patent Document		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³	Number ⁴ Kind Code ⁵ (if known)				
		FR	2 843 257 A1	02-06-2004	Viaccess		
		WO	03/010722 A2	02-06-2003	SCM Microsystems GMBH		
		EP	0 858 184 A2	08-12-1998	NDS Limited		
		WO	00/56068 A1	09-21-2000	Thomson Licensing S.A.		
		EP	0 691 787 A1	01-10-1996	Sony Corporation		
Examiner Signature					Date Considered		

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SENT FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Based on Form PTO/SB/08B (08-03) as modified by BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP on 09/10/03.

Substitute for Form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/612,663
				Filing Date	September 12, 2012
				First Named Inventor:	Luc Vantalon
				Art Unit	2431
				Confirmation No.	6713
				Examiner Name	Not Yet Assigned
				Attorney Docket No.	06517.P002C
				Sheet	2

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T ²
		InterTrust's Right/System Platform. InterTrust Technologies Corp.	
		Conditional Access (CA) Tutorial. Digital TV Group. www.dtg.org.uk/reference/tutorial/ca.htm . August 2004, 2 pages.	
		IANNELLA, Renato, "Digital Rights Management (DRM) Architectures" D-Lib Magazine, June 2001, Volume 7, Number 6, ISSN 1082-9873, pages 1-10.	
		MASSEL, Mark, "Conditional Access" Broadcasting Engineering, October 2001.	
		ATSC Standard: Conditional Access System for Terrestrial Broadcast, Revision A. Advanced Television Systems Committee, July 2004, pages 1-31.	
		VAN MOFFAERT, A., et al., "Digital Rights Management: DRM is a key enabler for the future growth of the broadband access market, and the telecom/networking market in general." <i>Alcatel Telecommunications Review</i> , Alcatel, Paris Cedex, FR, April 2003 (2003-2004), XP007005930 ISSN: 1267-7167, pages 1-7.	
		International Search Report and Written Opinion of the International Searching Authority for PCT/US2005/039794, mailed April 3, 2006, 11 pages.	
		PCT Notification Concerning the Transmittal of Preliminary report on Patentability PCT/US2005/039794, mailed June 21, 2007, 7 pages.	
		KAMPERMAN, et al., "Conditional Access System Interoperability Through Software Downloading", IEEE Transactions on Consumer Electronics. Vol. 47, Issue 1, Feb. 2001, pgs. 47-54. Found on the World Wide Web at : http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=920419	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SENT FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Based on Form PTO/SB/08B (08-03) as modified by BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP on 09/10/03.

Electronic Acknowledgement Receipt	
EFS ID:	14243772
Application Number:	13612663
International Application Number:	
Confirmation Number:	6713
Title of Invention:	METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	8791
Filer:	James Scheller Jr./Sarah Mahoney
Filer Authorized By:	James Scheller Jr.
Attorney Docket Number:	06517.P002C
Receipt Date:	15-NOV-2012
Filing Date:	12-SEP-2012
Time Stamp:	20:28:20
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no				
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	06517P002C_IDS_111512.PDF	101744 c1bd485290745e4880eafffa88d39d5c0deb b9a1	no	2
Warnings:					
Information:					

2	Information Disclosure Statement (IDS) Form (SB08)	06517P002C_IDS1449_111512. pdf	57177 8b60a9e7d820e3480e05e26f8b5570367d2f9e59	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
Total Files Size (in bytes):			158921		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	Examiner: Not Yet Assigned
Luc Vantalón et al.	)	
	)	Art Unit: 2431
Application No.: 13/612,663	)	
	)	Confirmation No.: 6713
Filing Date: September 12, 2012	)	
	)	
For: METHODS AND APPARATUSES	)	
FOR SECONDARY CONDITIONAL	)	
ACCESS SERVER	)	
	)	
	)	

E-filed via EFS-Web
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

INFORMATION DISCLOSURE STATEMENT

Sir:

Applicant hereby requests consideration of the enclosed Information Disclosure Statement pursuant to 37 C.F.R. §1.97(b).

Pursuant to 37 C.F.R. §1.98(d), copies of the references are not being provided herewith since they were previously sent to the Patent and Trademark Office during the prosecution of prior Application No. 11/007,116 filed on December 7, 2004. This previous application is relied upon for an earlier filing date under 35 U.S.C. §120. Please consider these cited documents in the currently pending §1.53(b) continuation application filed on September 12, 2012.

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being deposited electronically with the United States Patent and Trademark Office via Electronic Filing System

on: November 15, 2012.

Date of Deposit

By: /Sarah Mahoney/

Name of Person Filing Correspondence

Pursuant to 37 C.F.R. § 1.97, the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability.

Please charge Deposit Account No. 02-2666 for any shortage of fees which may be due in connection with this response.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: Nov. 15, 2012



James C. Scheller
Reg. No. 31,195

1279 Oakmead Parkway
Sunnyvale, CA 94085
(408) 720-8300



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/612,663	09/12/2012	Luc Vantalón	06517.P002C

CONFIRMATION NO. 6713

8791

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 Oakmead Parkway
Sunnyvale, CA 94085-4040

PUBLICATION NOTICE



Title:METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

Publication No.US-2013-0007451-A1

Publication Date:01/03/2013

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/612,663	09/12/2012	Luc Vantalón	06517.P002C	6713

8791 7590 04/22/2013
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 Oakmead Parkway
Sunnyvale, CA 94085-4040

EXAMINER

AVERY, JEREMIAH L

ART UNIT	PAPER NUMBER
----------	--------------

2431

MAIL DATE	DELIVERY MODE
-----------	---------------

04/22/2013

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 13/612,663	Applicant(s) VANTALON ET AL.	
	Examiner JEREMIAH AVERY	Art Unit 2431	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 September 2012.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 5) ☒ Claim(s) 1-22 is/are pending in the application.
5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 1-22 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☒ The drawing(s) filed on 12 September 2012 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

- a) ☐ All b) ☐ Some * c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Interim copies:

- a) ☐ All b) ☐ Some c) ☐ None of the: Interim copies of the priority documents have been received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date ____.
- 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 4) ☐ Other: ____.

DETAILED ACTION

- I. Claims 1-22 have been examined.

Priority

1. Current Application claims priority to United States Patent No. 8,291,236 with a priority date of 12/07/2004.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).
3. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to

be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

4. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

5. Claims 1, 5, 9, 12, 16 and 20 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 10, 32, 48, 62, 66 and 82 of U.S. Patent No. 8,291,236, hereinafter "236". Although the conflicting claims are not identical, they are not patentably distinct from each other because of a genus-species relationship between the current application (genus) and "236" (species).

6. Claim 1 of the current application is directed to a "non-transitory machine readable medium" being utilized "to control a presentation of content" involving "a first authentication process" using "a first root of trust" from "a first conditional access server" and "a second authentication process" using "a second root of trust" from "a second conditional access server". Claim 12 is directed to "a method to control a presentation of content" with the above limitations, as well.

7. Within patent "236", claim 1 is directed to "a method to control a presentation of content" and claim 10 is directed to "a non-transitory machine readable medium" being utilized "to control a presentation of content". Both claims 1 and 10 of "236" possess, inter alia, the claimed inventive concept within the claim limitations of claims 1 and 12 of the current application.

8. Claims 5 and 9 of the current application are directed to "a non-transitory machine readable medium" presenting content across a first and second "security domain" after a first and second "authentication process" between the "first conditional access server" and the "second conditional access server"; further involving "wherein a second conditional access server is configured to substitute the first security domain with the second security domain for client devices under a second root of trust". Claims 16 and 20 are directed to a method which invokes the above limitations, as well.

9. Within patent "236", claim 32 is directed to "a method to process conditional access protection" and claim 48 is directed to "a method to process media content provided by a primary security system", claims 62, 66 and 82 are directed to "a non-transitory machine readable medium" which is utilized "to provide conditional access"; each of these claims possess, inter alia, the claimed inventive concept within the claim limitations of claims 5, 9, 16 and 20 pertaining to the authentication of "the conditional access server" in relation to the clients and also the substituting of the security domains.

Allowable Subject Matter

10. Claims 1-22 are allowable over the existing prior art and this application would be placed in condition for allowance pending the submission and approval of a Terminal Disclaimer.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

12. The following United States Patents are cited to show the state of the art with respect to secure access control and management of data within a network environment, such as:

United States Patent No. 7,325,140 to Carley, which is cited to show secure management access management control for computers.

United States Patent No. 6,961,858 to Fransdonk, which is cited to show a method and system to secure content for distribution via a network.

United States Patent No. 7,152,160 to Lantto et al., which is cited to show a method and arrangement to secure access to a communications network.

United States Patent No. 7,685,206 to Mathew et al., which is cited to show authorization and access control service for distributed network resources.

United States Patent No. 7,174,021 to Krishnaswamy et al., which is cited to show systems and methods for providing secure server key operations.

United States Patent No. 7,171,558 to Mourad et al., which is cited to show transparent digital rights management for extendible content viewers.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

14. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

15. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2431

/NATHAN FLYNN/
Supervisory Patent Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 13/612,663	Applicant(s)/Patent Under Reexamination VANTALON ET AL.	
	Examiner JEREMIAH AVERY	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,171,558	01-2007	Mourad et al.	713/168
*	B	US-7,174,021	02-2007	Krishnaswamy et al.	380/277
*	C	US-7,685,206	03-2010	Mathew et al.	707/785
*	D	US-7,152,160	12-2006	Lantto et al.	713/168
*	E	US-6,961,858	11-2005	Fransdonk, Robert W.	726/29
*	F	US-7,325,140	01-2008	Carley, Jeffrey Alan	713/182
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Receipt date: 11/15/2012

13612663 GAU: 2431

INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/612,663
				Filing Date	September 12, 2012
				First Named Inventor:	Luc Vantalon
				Art Unit	2431
				Confirmation No.	6713
				Examiner Name	Not Yet Assigned
				Attorney Docket No.	06517.P002C
Sheet	1	of	2		

U.S. PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Document Number		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code ² (If known)			
		2003/0196092	A1	10-16-2003	Raley, M. et al.	
		2004/0196842	A1	10-07-2004	Dobbins, Kurt A.	
		2005/0021539	B2	01-27-2005	Short et al.	
		6,961,858	B2	11-01-2005	Fransdonk, Robert W.	
		7,036,011	B2	04-25-2006	Grimes et al.	
		7,127,619	B2	10-24-2006	Unger et al.	
		7,152,160	B2	12-19-2006	Lantto et al.	
		7,171,558	B1	01-30-2007	Mourad et al.	
		7,171,588	B2	01-30-2007	Friedman et al.	
		7,174,021	B2	02-06-2007	Krishnaswamy et al.	
		7,177,429	B2	02-13-2007	Moskowitz et al.	
		7,292,692	B2	11-06-2007	Bonan et al.	
		7,296,154	B2	11-13-2007	Evans et al.	
		7,302,058	B2	11-27-2007	Candelore, Brant L.	
		7,316,032	B2	01-01-2008	Tayebi et al.	
		7,325,140	B2	01-29-2008	Carley, Jeffrey Alan	
		7,336,784	B2	02-26-2008	Zuili, Patrick	
		7,493,291	B2	02-17-2009	Simelius, Kim	
		7,546,641	B2	06-09-2006	Robert et al.	
		7,685,206	B1	03-23-2010	Mathew et al.	
		7,757,299	B2	07-13-2010	Robert et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ Number ⁴ Kind Code ⁵ (if known)				
		FR 2 843 257 A1	02-06-2004	Viaccess		
		WO 03/010722 A2	02-06-2003	SCM Microsystems GMBH		
		EP 0 858 184 A2	08-12-1998	NDS Limited		
		WO 00/56068 A1	09-21-2000	Thomson Licensing S.A.		
		EP 0 691 787 A1	01-10-1996	Sony Corporation		

Examiner Signature	/Jeremiah Avery/	Date Considered	04/18/2013
--------------------	------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SENT FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

Based on Form PTO/SB/08B (08-03) as modified by BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP on 09/10/03.

Receipt date: 11/15/2012

INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>		Complete if Known	
		Application Number	13/612,663
		Filing Date	September 12, 2012
		First Named Inventor:	Luc Vantalon
		Art Unit	2431
		Confirmation No.	6713
		Examiner Name	Not Yet Assigned
		Attorney Docket No.	06517.P002C
Sheet	2	of	2

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T ²
		InterTrust's Right/System Platform. InterTrust Technologies Corp.	
		Conditional Access (CA) Tutorial. Digital TV Group. www.dtg.org.uk/reference/tutorial/ca.htm . August 2004, 2 pages.	
		IANNELLA, Renato, "Digital Rights Management (DRM) Architectures" D-Lib Magazine, June 2001, Volume 7, Number 6, ISSN 1082-9873, pages 1-10.	
		MASSEL, Mark, "Conditional Access" Broadcasting Engineering, October 2001.	
		ATSC Standard: Conditional Access System for Terrestrial Broadcast, Revision A. Advanced Television Systems Committee, July 2004, pages 1-31.	
		VAN MOFFAERT, A., et al., "Digital Rights Management: DRM is a key enabler for the future growth of the broadband access market, and the telecom/networking market in general." <i>Alcatel Telecommunications Review</i> , Alcatel, Paris Cedex, FR, April 2003 (2003-2004), XP007005930 ISSN: 1267-7167, pages 1-7.	
		International Search Report and Written Opinion of the International Searching Authority for PCT/US2005/039794, mailed April 3, 2006, 11 pages.	
		PCT Notification Concerning the Transmittal of Preliminary report on Patentability PCT/US2005/039794, mailed June 21, 2007, 7 pages.	
		KAMPERMAN, et al., "Conditional Access System Interoperability Through Software Downloading", IEEE Transactions on Consumer Electronics. Vol. 47, Issue 1, Feb. 2001, pgs. 47-54. Found on the World Wide Web at : http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=920419	

Examiner Signature	/Jeremiah Avery/	Date Considered	04/18/2013
--------------------	------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SENT FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Based on Form PTO/SB/08B (08-03) as modified by BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP on 09/10/03.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 6713

SERIAL NUMBER 13/612,663	FILING or 371(c) DATE 09/12/2012 RULE	CLASS 713	GROUP ART UNIT 2431	ATTORNEY DOCKET NO. 06517.P002C		
APPLICANTS Luc Vantalón, Sunnyvale, CA; Paolo Siccardò, Los Altos, CA; ** CONTINUING DATA ***** This application is a CON of 11/007,116 12/07/2004 PAT 8291236 ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 09/24/2012						
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☒ No Verified and Acknowledged <u>/JEREMIAH L AVERY/</u> Examiner's Signature		☐ Met after Allowance JLA Initials	STATE OR COUNTRY CA	SHEETS DRAWINGS 19	TOTAL CLAIMS 22	INDEPENDENT CLAIMS 6
ADDRESS BLAKELY SOKOLOFF TAYLOR & ZAFMAN 1279 Oakmead Parkway Sunnyvale, CA 94085-4040 UNITED STATES						
TITLE METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER						
FILING FEE RECEIVED 2120	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			☐ All Fees		
				☐ 1.16 Fees (Filing)		
				☐ 1.17 Fees (Processing Ext. of time)		
				☐ 1.18 Fees (Issue)		
				☐ Other _____		
				☐ Credit		

<i>Search Notes</i> 	Application/Control No. 13612663	Applicant(s)/Patent Under Reexamination VANTALON ET AL.
	Examiner JEREMIAH AVERY	Art Unit 2431

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
none	none	4/18/2013	JLA

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor Search	4/18/2013	JLA
Assignee Search	4/18/2013	JLA
Keyword Search within Class 713, subclasses 153 and 189, Class 726, subclasses 2, 3 and 27 and Class 348, subclasses E5.004 and E7.06	4/18/2013	JLA
Keywords in EAST Search	4/18/2013	JLA

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
none	none	4/18/2013	JLA

--	--

EAST Search History**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	96	(713/189.ccls. or 713/153.ccls. or 726/2.ccls. or 726/3.ccls. or 726/27.ccls. or 348/E5.004.ccls. or 348/E7.06.ccls.) and (((replac\$3 or swap\$4 or substitut\$3 or switch\$) with domain) same server)	US-PGPUB; USPAT; EPO	OR	ON	2013/04/18 16:56
L2	91	L1 and access\$	US-PGPUB; USPAT; EPO	OR	ON	2013/04/18 16:56
L3	3	(DIGITAL-KEystone-INC.as.) and (access\$ and (\$2crypt\$ or \$2cipher\$) and server).clm.	US-PGPUB; USPAT; EPO	OR	ON	2013/04/18 16:56
L4	8	(VANTALON-LUC.in. or SI CCARDO-PAOLO.in.) and (access\$ and (\$2crypt\$ or \$2cipher\$) and server).clm.	US-PGPUB; USPAT; EPO	OR	ON	2013/04/18 16:57
L5	1292	control\$5 and ((\$2crypt\$ or \$2cipher\$) near key) and (\$2crypt\$ or \$2cipher\$) and access\$ and (content or data or information) and (DRM or (Digital near rights near managment)) and (@ad<"20041207" @prad<"20041207")	US-PGPUB; USPAT; EPO	OR	ON	2013/04/18 16:58
L6	1251	L5 and ((first or primary) or (second\$3 or other or next or another) with ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat\$4) with (authentic\$ or verify\$ or verification)))	US-PGPUB; USPAT; EPO	OR	ON	2013/04/18 16:58
L7	161	L6 and (access near server)	US-PGPUB; USPAT; EPO	OR	ON	2013/04/18 16:58
L8	111	L7 and (server same ((\$2crypt\$ or \$2cipher) near key))	US-PGPUB; USPAT; EPO	OR	ON	2013/04/18 16:58
L9	84	L8 and (\$2authoris\$ or \$2authoriz\$)	US-PGPUB; USPAT; EPO	OR	ON	2013/04/18 16:58
L10	65	L9 and ((\$2authoris\$ or \$2authoriz\$) with access\$)	US-PGPUB; USPAT; EPO	OR	ON	2013/04/18 16:58
L11	1	L10 and (((replac\$3 or swap\$4 or substitut\$3 or switch\$) with domain) and server	US-PGPUB; USPAT; EPO	OR	ON	2013/04/18 16:59

4/18/2013 5:00:03 PM

C:\Users\javery\Documents\EAST\Workspaces\11007116.wsp

<i>Index of Claims</i> 	Application/Control No. 13612663	Applicant(s)/Patent Under Reexamination VANTALON ET AL.
	Examiner JEREMIAH AVERY	Art Unit 2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant
 ☐ CPA
 ☐ T.D.
 ☐ R.1.47

CLAIM		DATE									
Final	Original	04/18/2013									
	1	✓									
	2	✓									
	3	✓									
	4	✓									
	5	✓									
	6	✓									
	7	✓									
	8	✓									
	9	✓									
	10	✓									
	11	✓									
	12	✓									
	13	✓									
	14	✓									
	15	✓									
	16	✓									
	17	✓									
	18	✓									
	19	✓									
	20	✓									
	21	✓									
	22	✓									

Attorney's Docket No. 6517P002C

Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor:

Luc Vantalón

Application No.: 13/612,663

Filed: September 12, 2012

For: METHODS AND APPARATUSES
FOR SECONDARY CONDITIONAL
ACCESS SERVER

Examiner: AVERY, Jeremiah L.

Art Unit: 2431

Confirmation No.: 6713

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being
submitted electronically via EFS Web on the date
shown below.

/Tuyen Lam/ September 23, 2013
Tuyen Lam Date

Filed via EFS-Web
Commissioner for Patents
Alexandria, VA 22313-1450

AMENDMENT

Sir:

In response to the Office Action mailed April 22, 2013, applicant submits the
following amendment and remarks for consideration.

IN THE CLAIMS

1. (Original) A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to control a presentation of content, wherein a first conditional access server has authenticated a client of the first conditional access server through a first authentication process that used a first root of trust, the method comprising:
 - receiving, at a second conditional access server, content from the client of the first conditional access server in a first security domain;
 - processing the content on the second conditional access server;
 - authorizing a client of the second conditional access server to present content in accordance with authorization the second conditional access server received from the first conditional access server;
 - transmitting, from the second conditional access server to the client of the second conditional access server through a network connection in a second security domain, the content that is in an access controlled format that is specified by the second conditional access server; and
 - wherein the second conditional access server authenticates client devices of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the second conditional access server is configured to substitute the first

security domain with the second security domain for the client devices
under the second root of trust.

2. (Original) The medium of claim 1, wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain and wherein the content is video content.

3. (Original) The medium of claim 2, wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the client device of the second conditional access server comprises a digital rights management client.

4. (Original) The medium of claim 1, wherein the client of the first conditional access server receives security messages from the first conditional access server and the security messages comprise an entitlement management message and an entitlement control message; and wherein the second conditional access server generates a substitutive entitlement control message as a replacement of the entitlement control message.

5. (Original) A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause a client system in a second security domain to present content provided by a first conditional access server wherein the first conditional access server has authenticated a

client device of the first conditional access server through a first authentication process using a first root of trust for a first security domain and wherein a second conditional access server is configured to substitute the first security domain with the second security domain for client devices under a second root of trust, the method comprising:

receiving, at a second conditional access client of the second conditional access server, an authentication through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses the second root of trust for the second security domain which is independent of and different than the first root of trust; and

receiving, at the second conditional access client, content that is in an access controlled format specified by the second conditional access server in the second security domain, the second conditional access client being in the second security domain.

6. (Original) The medium in claim 5, wherein the second conditional access client does not have a user key representing a subscriber of the first security system.

7. (Original) The medium in claim 5, wherein the content comprises a decrypted version of an entitlement control message.

8. (Original) The medium in claim 5, wherein the content comprises a result of descrambling data scrambled by a conditional access system of the first security system.

9. (Original) A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method by a first conditional access server in a first security domain to provide conditional access in an environment which includes a second conditional access server that has authenticated a client of the second conditional access server through a second authentication process that used a second root of trust for a second security domain and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for client devices under the second root of trust, the method comprising:

receiving, from the client of the second conditional access server in the second security domain via the second conditional access server, a client request for the transmission of content protected by the first conditional access server;

broadcasting the requested content from the first conditional access server in the first security domain;

receiving, from the client of the second conditional access server, a client request to use the content after said broadcasting; and

responding to the client request from the client of the second conditional access server via the second conditional access server,

wherein the first conditional access server authenticates a client device of the first conditional access server through a first authentication process using a

first root of trust which is independent of and different than the second authentication process and the second root of trust.

10. (Original) The medium of claim 9, wherein the method further comprises:
transmitting a second entitlement management message to authorize the client to
playback the data response to the client request.
11. (Original) The medium of claim 10, wherein the client of the second conditional access server caches the broadcasted content but is not authorized to use the content before the second entitlement management message.
12. (Original) A method to control a presentation of content, wherein a first conditional access server has authenticated a client of the first conditional access server through a first authentication process that used a first root of trust, the method comprising:
receiving, at a second conditional access server, content from the client of the first conditional access server in a first security domain;
processing the content on the second conditional access server;
authorizing a client of the second conditional access server to present content in accordance with authorization the second conditional access server received from the first conditional access server;
transmitting, from the second conditional access server to the client of the second conditional access server through a network connection in a second

security domain, the content that is in an access controlled format that is specified by the second conditional access server; and wherein the second conditional access server authenticates client devices of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust.

13. (Original) The method of claim 12, wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain and wherein the content is video content.

14. (Original) The method of claim 13, wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the client device of the second conditional access server comprises a digital rights management client.

15. (Original) The method of claim 12, wherein the client of the first conditional access server receives security messages from the first conditional access server and the security messages comprise an entitlement management message and an entitlement

control message; and wherein the second conditional access server generates a substitutive entitlement control message as a replacement of the entitlement control message.

16. (Original) A method at a client system in a second security domain to present content provided by a first conditional access server wherein the first conditional access server has authenticated a client device of the first conditional access server through a first authentication process using a first root of trust for a first security domain and wherein a second conditional access server is configured to substitute the first security domain with the second security domain for client devices under a second root of trust, the method comprising:

receiving, at a second conditional access client of the second conditional access server, an authentication through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses the second root of trust for the second security domain which is independent of and different than the first root of trust; and

receiving, at the second conditional access client, content that is in an access controlled format specified by the second conditional access server in the second security domain, the second conditional access client being in the second security domain.

17. (Original) The method in claim 16, wherein the second conditional access client does not have a user key representing a subscriber of the first security system.
18. (Original) The method in claim 16, wherein the content comprises a decrypted version of an entitlement control message.
19. (Original) The method in claim 16, wherein the content comprises a result of descrambling data scrambled by a conditional access system of the first security system.
20. (Original) A method by a first conditional access server in a first security domain to provide conditional access in an environment which includes a second conditional access server that has authenticated a client of the second conditional access server through a second authentication process that used a second root of trust for a second security domain and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for client devices under the second root of trust, the method comprising:
- receiving, from the client of the second conditional access server in the second security domain via the second conditional access server, a client request for the transmission of content protected by the first conditional access server;
 - broadcasting the requested content from the first conditional access server in the first security domain;

receiving, from the client of the second conditional access server, a client request to use the content after said broadcasting; and responding to the client request from the client of the second conditional access server via the second conditional access server, wherein the first conditional access server authenticates a client device of the first conditional access server through a first authentication process using a first root of trust which is independent of and different than the second authentication process and the second root of trust.

21. (Original) The method of claim 20, wherein the method further comprises:
transmitting a second entitlement management message to authorize the client to
playback the data response to the client request.
22. (Original) The method of claim 21, wherein the client of the second conditional access server caches the broadcasted content but is not authorized to use the content before the second entitlement management message.

REMARKS

Reconsideration of this application, as amended, is respectfully requested.

Claims 1-22 stand rejected.

In this response, no claims have been amended. No claims have been canceled.

No claims have been added.

Applicant reserves all rights with respect to applicability of Doctrine of Equivalents.

Applicant notes with appreciation the Examiner's indication of allowance of the claims 1-22 pending the submission and approval of a Terminal Disclaimer.

Claims 1, 5, 9, 12, 16, and 20 were provisionally rejected on the ground of non-statutory obviousness-type double patenting over claims 1, 10, 32, 48, 62, 66, and 82 of U.S. Patent No. 8,291,236.

Applicant submits herewith a terminal disclaimer in compliance with 37 CFR §1.321 without admitting that this rejection is proper.

Therefore, applicant respectfully submits that the Examiner's non-statutory obviousness-type double patenting rejection of claims 1, 5, 9, 12, 16, and 20 has been overcome.

It is respectfully submitted that in view of the amendments and arguments set forth herein, the applicable rejections and objections have been overcome, and claims 1-22 are allowable. If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: September 23, 2013

/Tatiana Rossin/
Tatiana Rossin
Reg. No. 56,833

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300
Fax (408) 720-8383

Customer No. 08791

Electronic Patent Application Fee Transmittal				
Application Number:		13612663		
Filing Date:		12-Sep-2012		
Title of Invention:		METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER		
First Named Inventor/Applicant Name:		Luc Vantalón		
Filer:		Tatiana Rossin/Tuyen Lam		
Attorney Docket Number:		06517.P002C		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 2 months with \$0 paid	1252	1	600	600

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Statutory or Terminal Disclaimer	1814	1	160	160
Total in USD (\$)				760

Electronic Acknowledgement Receipt	
EFS ID:	16932228
Application Number:	13612663
International Application Number:	
Confirmation Number:	6713
Title of Invention:	METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	8791
Filer:	Tatiana Rossin/Tuyen Lam
Filer Authorized By:	Tatiana Rossin
Attorney Docket Number:	06517.P002C
Receipt Date:	23-SEP-2013
Filing Date:	12-SEP-2012
Time Stamp:	21:55:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$760
RAM confirmation Number	8306
Deposit Account	022666
Authorized User	
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)</p>	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	6517P002C_EOT_9-23-13.pdf	19193	no	1
			f77b082c922baa48e618f1a8a121011a84cd1c84		
Warnings:					
Information:					
2	Terminal Disclaimer Filed	6517P002C_TerminalDisclaimer_9-23-13.pdf	143395	no	2
			f48c2ac421488928bf180f2ccb01fc3d4de0c936		
Warnings:					
Information:					
3		6517P002C_R-OA_9-23-13.pdf	48734	yes	12
			c4c679a7757277a4d2b8db9b864536579ab64642		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Claims		2	10	
	Applicant Arguments/Remarks Made in an Amendment		11	12	
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	32027	no	2
			02d98c204eaa0831e07ca2b656efeabf8eb83805		
Warnings:					
Information:					
Total Files Size (in bytes):			243349		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor:

Luc Vantalón

Application No.: 13/612,663

Filed: September 12, 2012

For: METHODS AND APPARATUSES FOR
SECONDARY CONDITIONAL
ACCESS SERVER

Examiner: AVERY, Jeremiah L.

Art Unit: 2431

Confirmation No.: 6713

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being deposited with the United States Patent and Trademark Office via electronic filing through the United States Patent and Trademark Electronic Filing System on:

<u>/Tuyen Lam/</u>	<u>September 23, 2013</u>
Tuyen Lam	Date

EFS Filing
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR EXTENSION OF TIME PURSUANT TO 37 C.F.R. § 1.136 (a)

Sir:

Applicant respectfully petitions pursuant to 37 CFR 1.136(a) for two months extension of time to file this response to the Office Action mailed April 22, 2013. The extended period is set to expire on September 23, 2013. The Director is authorized to charge our Deposit Account No. 02-2666 in the amount of \$600.00 for the fee under 37 C.F.R. § 1.17 (a)(2) for two months extension of time.

Please charge any shortages and credit any overages to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: September 23, 2013

/Tatiana Rossin/
Tatiana Rossin
Reg. No. 56,833

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300

**TERMINAL DISCLAIMER TO OBIATE A DOUBLE PATENTING
REJECTION OVER A "PRIOR" PATENT**Docket Number (Optional)
6517P002C

In re Application of: Luc Vantalon et al.

Application No.: 13/612,663

Filed: September 12, 2012

For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

The owner*, Digital Keystone, of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term **prior patent** No. 8,291,236 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☒ The undersigned is an attorney or agent of record. Reg. No. 31,195

Lester J. Vincent Signature Sept 23, 2013 Date

Lester J. Vincent, Reg. No. 31,460
Typed or printed name

408-720-8300
Telephone Number

- ☒ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 13/612,663		Filing Date 09/12/2012		☐ To be Mailed						
ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO															
APPLICATION AS FILED – PART I															
(Column 1)			(Column 2)												
FOR		NUMBER FILED		NUMBER EXTRA		RATE (\$)		FEE (\$)							
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A		N/A		N/A									
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))		N/A		N/A		N/A									
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A		N/A		N/A									
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 =		*		X \$ =									
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 =		*		X \$ =									
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).													
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))															
* If the difference in column 1 is less than zero, enter "0" in column 2.						TOTAL									
APPLICATION AS AMENDED – PART II															
(Column 1)			(Column 2)			(Column 3)									
AMENDMENT	09/23/2013		CLAIMS REMAINING AFTER AMENDMENT			HIGHEST NUMBER PREVIOUSLY PAID FOR		PRESENT EXTRA		RATE (\$)		ADDITIONAL FEE (\$)			
	Total (37 CFR 1.16(i))		* 22		Minus	** 22		= 0		X \$80 =		0			
	Independent (37 CFR 1.16(h))		* 6		Minus	*** 6		= 0		X \$420 =		0			
	☐ Application Size Fee (37 CFR 1.16(s))														
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))														
	TOTAL ADD'L FEE											0			
(Column 1)			(Column 2)			(Column 3)									
AMENDMENT			CLAIMS REMAINING AFTER AMENDMENT			HIGHEST NUMBER PREVIOUSLY PAID FOR		PRESENT EXTRA		RATE (\$)		ADDITIONAL FEE (\$)			
	Total (37 CFR 1.16(i))		*		Minus	**		=		X \$ =					
	Independent (37 CFR 1.16(h))		*		Minus	***		=		X \$ =					
	☐ Application Size Fee (37 CFR 1.16(s))														
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))														
	TOTAL ADD'L FEE														
<p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.</p>											LIE /KAREN VESTAL/				

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Application Number 	Application/Control No. 13/612,663	Applicant(s)/Patent under Reexamination VANTALON ET AL.	
Document Code - DISQ		Internal Document – DO NOT MAIL	

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 09-23-2013	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:

Dorethea Lawrence



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

8791 7590 10/17/2013
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 Oakmead Parkway
Sunnyvale, CA 94085-4040

EXAMINER

AVERY, JEREMIAH L

ART UNIT

PAPER NUMBER

2431

DATE MAILED: 10/17/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/612,663	09/12/2012	Luc Vantalon	06517.P002C	6713

TITLE OF INVENTION: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1780	\$300	\$0	\$2080	01/17/2014

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or **Fax** **(571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

8791 7590 10/17/2013
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 Oakmead Parkway
Sunnyvale, CA 94085-4040

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/612,663	09/12/2012	Luc Vantalón	06517.P002C	6713

TITLE OF INVENTION: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1780	\$300	\$0	\$2080	01/17/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
AVERY, JEREMIAH L	2431	713-189000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____
- (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
- 3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/612,663	09/12/2012	Luc Vantalón	06517.P002C	6713
8791 7590 10/17/2013 BLAKELY SOKOLOFF TAYLOR & ZAFMAN 1279 Oakmead Parkway Sunnyvale, CA 94085-4040				
EXAMINER AVERY, JEREMIAH L				
ART UNIT		PAPER NUMBER		
2431				

DATE MAILED: 10/17/2013

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

**Notices of Allowance and Fee(s) Due mailed between October 1, 2013 and
December 31, 2013**

(Addendum to PTOL-85)

If the "Notice of Allowance and Fee(s) Due" has a mailing date on or after October 1, 2013 and before January 1, 2014, the following information is applicable to this application.

If the issue fee is being timely paid on or after January 1, 2014, the amount due is the issue fee and publication fee in effect January 1, 2014. On January 1, 2014, the issue fees set forth in 37 CFR 1.18 decrease significantly and the publication fee set forth in 37 CFR 1.18(d)(1) decreases to \$0.

If an issue fee or publication fee has been previously paid in this application, applicant is not entitled to a refund of the difference between the amount paid and the amount in effect on January 1, 2014.

Notice of Allowability	Application No. 13/612,663 Examiner JEREMIAH AVERY	Applicant(s) VANTALON ET AL. Art Unit 2431 AIA (First Inventor to File) Status No
-------------------------------	---	---

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the response filed on 09/23/13.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are 1-22. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
Certified copies:
 a) ☐ All b) ☐ Some *c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
 * Certified copies not received: _____.

Applicant has **THREE MONTHS FROM THE "MAILING DATE"** of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in **ABANDONMENT** of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ **CORRECTED DRAWINGS** (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ **DEPOSIT OF and/or INFORMATION** about the deposit of **BIOLOGICAL MATERIAL** must be submitted. Note the attached Examiner's comment regarding **REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL**.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892) 2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____ 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material 4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____	5. ☐ Examiner's Amendment/Comment 6. ☒ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____
--	---

/Jeremiah Avery/ Examiner, Art Unit 2431	/NATHAN FLYNN/ Supervisory Patent Examiner, Art Unit 2431
---	--

Terminal Disclaimer

1. The terminal disclaimer filed on 09/23/13 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of U.S. Patent No. 8,291,236 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Examiner's Statement of Reasons for Allowance

2. Claims 1-22 are allowed over the prior art.

3. This action is in reply to the applicant's correspondence on 09/23/13.

4. The following is an Examiner's statement of reasons for the indication of allowable claimed subject matter.

5. Nowhere in the prior art is found, alone, or in combination, other than via hindsight, the claim elements, at the time of the invention; serving to patently distinguish the invention from said prior art and thus this application is placed in condition for allowance.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

7. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

8. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2431

/NATHAN FLYNN/

Supervisory Patent Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 13/612,663	Applicant(s)/Patent Under Reexamination VANTALON ET AL.	
	Examiner JEREMIAH AVERY	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,100,048	08-2006	Czajkowski et al.	713/168
*	B	US-7,739,402	06-2010	Roose et al.	709/242
*	C	US-7,325,140	01-2008	Carley, Jeffrey Alan	713/182
*	D	US-7,222,062	05-2007	Goud et al.	703/23
*	E	US-6,961,858	11-2005	Fransdonk, Robert W.	726/29
*	F	US-7,152,160	12-2006	Lantto et al.	713/168
*	G	US-7,685,206	03-2010	Mathew et al.	707/785
*	H	US-7,296,154	11-2007	Evans et al.	713/169
*	I	US-7,174,021	02-2007	Krishnaswamy et al.	380/277
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Varadharajan, Vijay; Calvelli, Claudio. Extending the Schematic Protection Model - I Conditional Tickets and Authentication. 1994 IEEE Computer Society Symposium on Research in Security and Privacy. Pub. Date: 1994. Relevant Pages: 213-229. Found on the World Wide Web at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=296579
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Issue Classification 	Application/Control No. 13612663	Applicant(s)/Patent Under Reexamination VANTALON ET AL.	
	Examiner JEREMIAH AVERY	Art Unit 2431	

CPC						
Symbol					Type	Version
</						

CPC Combination Sets					
Symbol			Type	Set	Ranking

/JEREMIAH AVERY/ Examiner.Art Unit 2431 (Assistant Examiner)	10/01/13 (Date)	Total Claims Allowed: 22	
/NATHAN FLYNN/ Supervisory Patent Examiner.Art Unit 2431 (Primary Examiner)	10/07/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 15

Issue Classification 	Application/Control No. 13612663	Applicant(s)/Patent Under Reexamination VANTALON ET AL.
	Examiner JEREMIAH AVERY	Art Unit 2431

US ORIGINAL CLASSIFICATION						INTERNATIONAL CLASSIFICATION														
CLASS			SUBCLASS			CLAIMED					NON-CLAIMED									
713			189			H	0	4	L	29 / 06 (2006.0)										
CROSS REFERENCE(S)																				
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																			
713	153	168																		
726	2	3	27																	
348	E5.004	E7.06																		

/JEREMIAH AVERY/ Examiner.Art Unit 2431 (Assistant Examiner)	10/01/13 (Date)	Total Claims Allowed: 22	
/NATHAN FLYNN/ Supervisory Patent Examiner.Art Unit 2431 (Primary Examiner)	10/07/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 15

Issue Classification 	Application/Control No. 13612663	Applicant(s)/Patent Under Reexamination VANTALON ET AL.
	Examiner JEREMIAH AVERY	Art Unit 2431

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	17	17												
2	2	18	18												
3	3	19	19												
4	4	20	20												
5	5	21	21												
6	6	22	22												
7	7														
8	8														
9	9														
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
16	16														

/JEREMIAH AVERY/ Examiner.Art Unit 2431 (Assistant Examiner)	10/01/13 (Date)	Total Claims Allowed: 22	
/NATHAN FLYNN/ Supervisory Patent Examiner.Art Unit 2431 (Primary Examiner)	10/07/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 15

Search Notes 	Application/Control No. 13612663	Applicant(s)/Patent Under Reexamination VANTALON ET AL.
	Examiner JEREMIAH AVERY	Art Unit 2431

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
none	none	10/1/2013	JLA

SEARCH NOTES		
Search Notes	Date	Examiner
Updated Inventor Search	10/1/2013	JLA
Updated Assignee Search	10/1/2013	JLA
Updated Keyword Search within Class 713, subclasses 153, 168 and 189, Class 726, subclasses 2, 3 and 27 and Class 348, subclasses E5.004 and E7.06	10/1/2013	JLA
Updated Keywords in EAST Search	10/1/2013	JLA
IEEE Search	10/1/2013	JLA

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
none	((conditional and access and (replac\$3 or swap\$4 or substitu\$3 or switch\$) and domain) and server and (\$2crypt\$ or \$2cipher\$)).clm.	10/1/2013	JLA

--	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	4	(DIGITAL-KEYSTONE-INC.as.) and (access\$ and (\$2crypt\$ or \$2cipher\$) and server).clm.	US-PGPUB; USPAT; EPO	OR	ON	2013/10/01 14:55
L2	9	(VANTALON-LUC.in. or SI CCARDO-PAOLO.in.) and (access\$ and (\$2crypt\$ or \$2cipher\$) and server).clm.	US-PGPUB; USPAT; EPO	OR	ON	2013/10/01 16:28
L3	1303	control\$ and ((\$2crypt\$ or \$2cipher\$) near key) and (\$2crypt\$ or \$2cipher\$) and access\$ and (content or data or information) and (DRM or (Digital near rights near managment)) and (@ad<"20041207" @prad<"20041207")	US-PGPUB; USPAT; EPO	OR	ON	2013/10/01 16:28
L4	1262	L3 and ((first or primary) or (second\$3 or other or next or another) with ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat\$4) with (authentic\$ or verify\$ or verification)))	US-PGPUB; USPAT; EPO	OR	ON	2013/10/01 16:28
L5	162	L4 and (access near server)	US-PGPUB; USPAT; EPO	OR	ON	2013/10/01 16:28
L6	112	L5 and (server same ((\$2crypt\$ or \$2cipher) near key))	US-PGPUB; USPAT; EPO	OR	ON	2013/10/01 16:28
L7	85	L6 and (\$2authoris\$ or \$2authoriz\$)	US-PGPUB; USPAT; EPO	OR	ON	2013/10/01 16:28
L8	66	L7 and ((\$2authoris\$ or \$2authoriz\$) with access\$)	US-PGPUB; USPAT; EPO	OR	ON	2013/10/01 16:28
L9	1	L8 and ((replac\$3 or swap\$4 or substitut\$3 or switch\$) with domain) and server	US-PGPUB; USPAT; EPO	OR	ON	2013/10/01 16:28
L10	112	(713/189.ccls. or 713/153.ccls. or 726/2.ccls. or 726/3.ccls. or 726/27.ccls. or 348/E5.004.ccls. or 348/E7.06.ccls.) and (((replac\$3 or swap\$4 or substitut\$3 or switch\$) with domain) same server)	US-PGPUB; USPAT; EPO	OR	ON	2013/10/01 16:55
L11	112	(713/189.ccls. or 713/153.ccls. or 726/2.ccls. or 726/3.ccls. or 726/27.ccls. or 348/E5.004.ccls. or 348/E7.06.ccls.) and (((replac\$3 or swap\$4 or substitut\$3 or switch\$) with domain) same server)	US-PGPUB; USPAT; EPO	OR	ON	2013/10/01 16:55
L13	139	(713/189.ccls. or 713/153.ccls. or	US-	OR	ON	2013/10/01

EAST Search History

		713/168.ccls. or 726/2.ccls. or 726/3.ccls. or 726/27.ccls. or 348/E5.004.ccls. or 348/E7.06.ccls.) and (((replac\$3 or swap\$4 or substitut\$3 or switch\$) with domain) same server)	PGPUB; USPAT; EPO			17:14
L14	122	I13 and (authentic\$ or verify\$ or verification)	US- PGPUB; USPAT; EPO	OR	ON	2013/10/01 17:14
L15	33	L14 and (server same ((\$2crypt\$ or \$2cipher) near key))	US- PGPUB; USPAT; EPO	OR	ON	2013/10/01 17:14

10/ 1/ 2013 5:18:18 PM

C:\ Users\ javery\ Documents\ EAST\ Workspaces\ 11007116.wsp

<i>Index of Claims</i> 	Application/Control No. 13612663	Applicant(s)/Patent Under Reexamination VANTALON ET AL.
	Examiner JEREMIAH AVERY	Art Unit 2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47

CLAIM		DATE									
Final	Original	10/01/2013									
1	1	=									
2	2	=									
3	3	=									
4	4	=									
5	5	=									
6	6	=									
7	7	=									
8	8	=									
9	9	=									
10	10	=									
11	11	=									
12	12	=									
13	13	=									
14	14	=									
15	15	=									
16	16	=									
17	17	=									
18	18	=									
19	19	=									
20	20	=									
21	21	=									
22	22	=									

EAST Search History**EAST Search History (Interference)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L12	10	((conditional and access and (replac\$3 or swap\$4 or substitu\$3 or switch\$) and domain) and server and (\$2crypt\$ or \$2cipher\$)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/10/01 16:57

10/ 1/ 2013 4:59:20 PM**C:\ Users\ javery\ Documents\ EAST\ Workspaces\ 11007116.wsp**

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

8791 7590 10/17/2013
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
 1279 Oakmead Parkway
 Sunnyvale, CA 94085-4040

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

<u>Connie Thayer</u>	(Depositor's name)
<u>Connie Thayer</u>	(Signature)
<u>January 16, 2014</u>	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/612,663	09/12/2012	Luc Vantalón	06517.P002C	6713

TITLE OF INVENTION: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1780	\$300	\$0	\$2080	01/17/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
AVERY, JEREMIAH L	2431	713-189000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p>☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p>☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.</p>	<p>2. For printing on the patent front page, list</p> <p>(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,</p> <p>(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.</p> <p>1 <u>BLAKELY, SOKOLOFF,</u></p> <p>2 <u>TAYLOR & ZAFMAN LLP</u></p> <p>3 _____</p>
---	--

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

Digital Keystone, Inc.

(B) RESIDENCE: (CITY AND STATE OR COUNTRY)

Mountain View, California

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☒ Issue Fee
- ☒ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 02-2666 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____

Date January 16, 2014

Typed or printed name James C. Scheller

Registration No. 31,195

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Electronic Patent Application Fee Transmittal				
Application Number:		13612663		
Filing Date:		12-Sep-2012		
Title of Invention:		METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER		
First Named Inventor/Applicant Name:		Luc Vantalón		
Filer:		James Scheller Jr./connie thayer		
Attorney Docket Number:		06517.P002C		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	960	960
Publ. Fee- Early, Voluntary, or Normal	1504	1	0	0

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				960

Electronic Acknowledgement Receipt	
EFS ID:	17939006
Application Number:	13612663
International Application Number:	
Confirmation Number:	6713
Title of Invention:	METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	8791
Filer:	James Scheller Jr./connie thayer
Filer Authorized By:	James Scheller Jr.
Attorney Docket Number:	06517.P002C
Receipt Date:	16-JAN-2014
Filing Date:	12-SEP-2012
Time Stamp:	20:29:56
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 960
RAM confirmation Number	6283
Deposit Account	022666
Authorized User	
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)</p>	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	06517P002C_issue_fee_transmittal.pdf	107595	no	2
			fb05f88fb1d64eaa26386d802223bacbee6f229		

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	31844	no	2
			cd301c086bdadaa868881f2fc7740cad1095ccfc		

Warnings:

Information:

Total Files Size (in bytes): 139439

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/612,663	03/04/2014	8667304	06517.P002C	6713

8791 7590 02/12/2014
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 Oakmead Parkway
Sunnyvale, CA 94085-4040

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

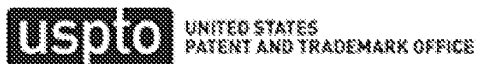
Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Luc Vantalon, Sunnyvale, CA;
Paolo Siccardo, Los Altos, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.



P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

ACKNOWLEDGEMENT OF CHANGE TO SMALL ENTITY STATUS

APPLICATION #	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET #	REQUEST ID
13/612,663	09/12/2012	Luc Vantalon	06517.P002C	104103

The entity status change request below filed through Patent Center on 08/24/2023 has been accepted.

Certifications

APPLICANT ASSERTING SMALL ENTITY STATUS. See 37CFR 1.27.

Signature

I certify, in accordance with 37 CFR 1.4(d)(4), that I am one of the signatories making the entity status change.

Signature	Name	Registration #
/Lester J. Vincent/	Lester Vincent	31460