

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
16 July 2009 (16.07.2009)

PCT

(10) International Publication Number
WO 2009/088490 A1

(51) International Patent Classification:
H04N 7/16 (2006.01)

(21) International Application Number:

PCT/US2008/014150

(22) International Filing Date:

31 December 2008 (31.12.2008)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/010,763 11 January 2008 (11.01.2008) US
12/169,508 8 July 2008 (08.07.2008) US

(71) Applicant (for all designated States except US): **APPLE INC.** [US/US]; 1 Infinite Loop, Cupertino, CA 95014 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **FARRUGIA, Augustin, J.** [FR/US]; 10411 Tula Lane, Cupertino, CA 95014 (US). **ROBBIN, Jeffrey** [US/US]; 270 Frances Drive, Los Altos, CA 94022 (US). **MITSUJI, Hiro** [JP/US]; 436 14th Street, San Francisco, CA 94103 (US). **DESPOTOVIC, Mihailo** [US/US]; 3610 Flora Vista Avenue, #338, Santa Clara, CA 95051 (US). **MELDRUM, Colin** [GB/US]; 1340 McGee Avenue, Berkeley, CA 94703 (US).

(74) Agents: **KLIVANS, Norman, R.** et al.; Morrison & Foerster LLP, 755 Page Mill Road, Palo Alto, CA 94304-1018 (US).

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

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report
— with amended claims

(54) Title: METHOD AND APPARATUS FOR ON DEMAND VIDEO AND OTHER CONTENT RENTAL

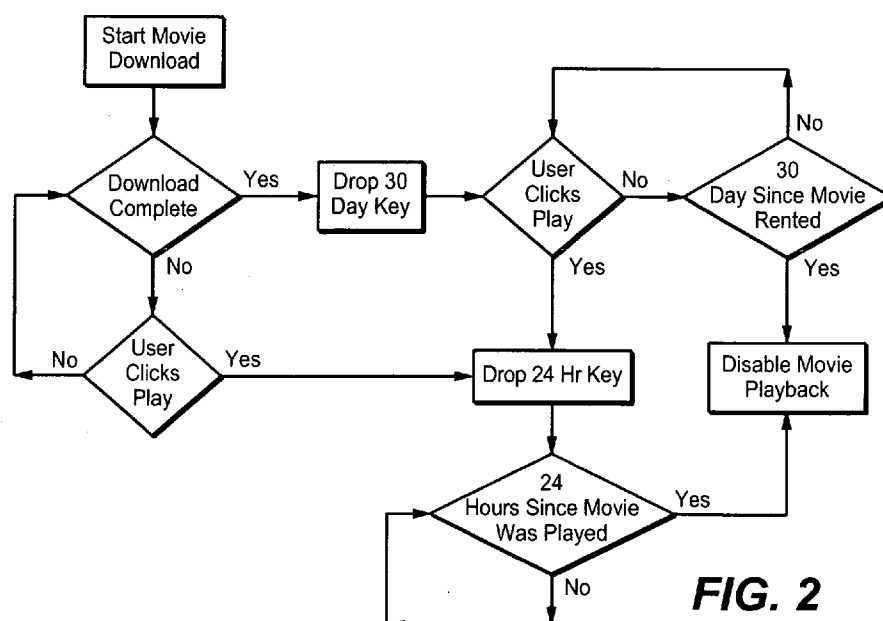


FIG. 2

(57) Abstract: A video on demand system in the context of the Internet, for video rentals. A user accesses an on-line store to rent a video program or movie. The rental is for a limited time (such as 30 days) and within that thirty days, the video program or movie can only be viewed for a 24 hour time window. The time limits are enforced by the on-line store which maintains a database of each rental transaction and allows supply of the needed keys for decrypting the (encrypted) video or movie only if within the time limits.

WO 2009/088490 A1

METHOD AND APPARATUS FOR ON DEMAND VIDEO AND OTHER CONTENT RENTAL

CROSS REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to U.S. provisional application 61/010,763, filed January 11, 2008 incorporated herein by reference in its entirety.

FIELD OF THE INVENTION

[0002] This invention generally relates to video on demand and more specifically to controlling use of video on demand content.

BACKGROUND

[0003] Video on demand is a well-known technology. It generally allows users to select and watch digital video content over a network, such as cable TV, as part of an interactive television system. VOD systems either stream content allowing viewing in real time or download it in which the program is brought in its entirety to a set top box in the cable television context before viewing starts. Most current video on demand systems are in the context of cable and telephone company or satellite television distribution systems. In most of these systems the user buys or selects a movie or television program and it begins to play in the television set almost immediately. Typically a payment must be made for each viewing.

[0004] Typically in the video on demand context, the commerce-related part of the transaction is similar to renting a video since viewing is strictly limited in terms of time and/or number of viewings. In some video on demand systems for instance one may watch the video as many times as one wants, but only beginning for a period of 24 hours beginning when the rental is made. Such video on demand systems are very limited in terms of user control and access and they typically require viewing to begin immediately upon purchase. This is due to the inherent limitations of the delivery system and the user's device which is typically a cable television set top box or equivalent.

SUMMARY

[0005] In accordance with this disclosure, a video on demand system is provided, not in the context of cable television, but instead in the computer network (Internet) context. It is known of course to purchase (or obtain without payment) video and audio material from a website via the Internet, which is then downloaded partially or in its entirety to the user's device typically a personal computer, or consumer electronics device such as an iPod or Apple TV device or other such device. If these are purchases the viewer then owns the content and can view it as many times as he wants indefinitely. However in the context of the system disclosed here, instead a video on demand approach is used in which the user rents use of the audio or video material for a limited time for a fixed payment and then can view the rented content at the time and place of his choosing using his consumer electronics device, such as an Apple TV or iPod device. Some such devices may require connection to the Internet via a host computer.

[0006] Hence in one embodiment, the present system supports movie rental from, for instance, the Apple iTunes Store which is a central website, providing content. Users are able to rent movies or other video material and view it on their Apple TV or iPod device. In some embodiments, the material may be transferred from one client (user) device to another. Typically upon purchase of the audio or video asset (program or movie and also referred to as content), a 30-day or other defined time period begins. The material may be viewed and/or listened to any time during that 30-day time. In addition, any time during that 30-day time when the viewer actually plays the material, a 24-hour window begins during which unlimited viewing is permitted. However once that 24-hour window has ended no more viewing is permitted. Of course these time limits are merely illustrative. In one embodiment, the present system supports both high definition television and standard definition television. In one embodiment, each individual program has its own assigned rental period both in terms of the overall time of rental such as the 30-day time span and also the 24-hour window.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] FIG. 1 shows the environment in which the present system operates.

[0008] FIG. 2 shows a flowchart showing the process of renting a movie in this example.

[0009] FIGS. 3A-3E shows various timelines for renting and viewing a movie under different circumstances.

DETAILED DESCRIPTION

[0010] FIG. 1 shows the environment in which the present system operates. Most elements here are conventional and hence not explained in further detail. At the head end, there is a digital video on demand delivery service such as the iTunes Store 12 in one embodiment, more broadly a set of content and commerce servers operated by a commercial entity for storing (or accessing) a number of programs and/or movies and/or audio items such as music. This element 12 of the system is conventional since for instance such stores or more broadly content storage facilities already exist. The iTunes Stores 12 is conventionally coupled to the Internet 14. Also connected to the Internet 14 at the user end is a client device 18 indicated here as an Apple TV device, but which might be an Apple iPod device (with its host computer) or similar consumer electronic devices or computers available from other manufacturers and which are currently available. Each such device 18 has as shown here a global universal identifier GUID 20 which identifies that particular device.

[0011] Also provided here at the head end is a conventional DRM (digital rights management) server 24. Such servers already exist in the content of present video and audio downloads and viewing services. Digital rights management refers to the policy enforcement for protecting the content from unauthorized use. Typically this involves some form of encryption. The content is transferred from the iTunes Store 12 or other source to the client device 18 in encrypted form and must be decrypted at the client device 18. Some such encryption schemes are sophisticated. For instance typically the encryption applied to each particular content transfer is different. Also the decryption keys supplied may be useful only for a small portion of each piece of content. In this case what is referred to as a key bag or a file is provided as part of the DRM file holding a number of keys for decrypting the content. The encryption may be symmetric or asymmetric (public key-private key) as known in the field. Typically the security information is provided in the form of a set of DRM data transferred along with or associated with the downloaded encrypted content and is necessary for decrypting and viewing same. The DRM data includes conventionally data defining a

security policy associated with that content item, restricting a number of available plays and device transfers. The commerce aspect of ordering the content by the client device 18 is shown by the “rental order” from the client device and is received via the Internet 14 at the iTunes Store 12 which charges the user of the client device 18 the appropriate rental to a credit card or other account. In response, the iTunes Store 12 provides the “encrypted content” or asset along with at the same time or a later time the relevant DRM data which is transferred to the client device 18. Generally, the encrypted content is downloaded from the iTunes Store 12 to the client device 18 first, without the DRM data (including the key bag) needed to play the content. The DRM data is transmitted later, usually in response to the play request by the user, including the key bag as explained further below.

[0012] Also shown here is what is referred to as a content rental database and logic 26. This element here is not present in conventional audio/video content purchase systems. Its operation is explained further below, but essentially it controls delivery of the relevant DRM data as so as to enforce the rental time limits. It may be resident on its own server or part of the iTunes Store server(s) 12.

[0013] FIG. 2 shows in a flowchart the overall digital rights management for a rental in accordance with this disclosure using the FIG. 1 system. Not shown here is the initial order by the user or the content encryption which is conventional, since FIG. 2 shows the sequence of events at a high level. The initial action 32 here is that the movie (content) download is initiated to the user device 18 (after of course the ordering procedure has been completed and the content encrypted.). In the next step 34 it is determined if at the present time the download has been completed. This is a query made for instance every 5 seconds. If before the download is completed (“No”) the user has clicked “play” on his user device 18, that is he wants to start playing, the download is continued during playing. Thus this functions as a conventional video on demand system where the user watches the video as it is being downloaded. However there is no requirement to do so. That is one may alternatively download the content and watch it later. In this case if after the download is completed, the user has not yet clicked play, at 36 a 30-day key or token (counter) is provided at the content rental database of FIG. 1. That is, this token expires in for instance 30 days. This time period is only an example here. This is the duration of the rental time in this particular example.

[0014] The next step 40 is that at some time after the download begins and after beginning of the 30-day period, the user does decide to play the content. This condition is checked periodically such as every 1 second. If at any particular time the user has not selected play, it is determined in the next step 42 if the 30 day token has expired. If “No”, control returns to the “user clicks play” step 40. If “Yes” at 42, the movie playback is disabled at the next step 46 because the 30-day rental time has expired. If the user however clicks play at 38 then the 24-hour window key or token is initiated at 48 at the content rental database. This begins the 24-hour viewing window. This is checked whether the user clicks play during the download or after the download. Then it is checked periodically at 50 such as every 5 seconds if the 24-hours since the play was initiated has expired. If “No”, play is resumed. If “Yes”, the movie playback is disabled at the next step 46.

[0015] Thus in this particular example, the user has 30 days to view the movie after the download begins. In one embodiment this time is a variable designated the rental duration. The user also has 24 hours in this example to view the movie after initiating the first play. (The 24 hours here is only exemplary.) This variable is designated playback duration. Both of these variables may be unique to each asset as determined by the system operator and entered into the content rental database 26 for each content item. Generally after the 30-day or 24-hour periods have expired, the item becomes unplayable due to expiration of its token. However if the time limit is hit while the movie is still playing, the play will not be interrupted. Generally the play will be allowed to finish, that is one can finish watching the movie as long as the movie is not stopped or paused by the user for the remainder of the movie. There is also provided generally both in the user device 18 and in terms of the tokens a pause function. That is one may pause viewing and this also stops the tolling of the 24-hour time limit. The pause time limit is for example 12 hours or for instance a number of times of the actual movie duration.

[0016] Various time lines or scenarios for various circumstances of operation of the FIG. 2 method are shown in FIGS. 3A-3E which are largely self-explanatory. In this case the horizontal line represents the passage of time. Exemplary dates and times of day are shown for purposes of illustration. With reference to FIG. 3A, the first action at point 1 is that the user makes rental and the 30-day rental time begins. At point 2 (shaded), the customer actually starts to view (play) the movie and the 24-hour viewing window begins. There is unlimited playback allowed during this

24-hour window, that is one may watch the movie or other item as much as one wants and as many times as one wants within the 24 hour window. The 24 hours expires at point 3, in this case 24 hours after the initialization of play. The 30 days expires as shown at point 4. Of course in the typical situation the 30 day limit will not be relevant unless the 24 hours begins in the last day of the 30-day window.

[0017] FIG. 3B shows a similar situation as FIG. 3A except that in this case the customer starts viewing the movie at 2 during the download (which may take for instance 30 minutes). Obviously in this case the 30-day rental window at 4 is irrelevant. Note that typically downloading movies takes a considerable amount of time due to the large amount of digital information involved. In this case, the movie viewing window expires at 3 24 hours after the beginning of the viewing time.

[0018] FIG. 3C shows the more complex situation where there is a pause involved as an example of an implementation of the present method. Typically pauses are initiated by the viewer when he wants to stop viewing and do something else and return to viewing later. As shown at point 1, the download is initiated and the 30-day window begins. At point 2, the user begins to view the movie and his 24-hour window begins. Again he has unlimited playback during this 24-hour window. At point 3, part way through the movie, the customer pauses the movie. In this case, he pauses it for two days until point 4 where he pushes the play button on his consumer electronics playback device and resumes viewing. In this case, even though his 24-hour window has expired, the pausing enables him to view the rest of the movie as long as he does not pause or stop the movie again. The viewing period will then expire immediately after completion of the movie. Again in this case point five which is the 30-day rental window is irrelevant.

[0019] FIGS. 3D and 3E illustrate the situation where the viewing only begins in the last 24 hours of the 30-day window. In FIG. 3D at point 1, the customer initiates the download and the 30-day rental window begins. The customer however only starts to view the movie at point 2, 29 days into the 30-day rental window. The 24-hour viewing window starts immediately. At point 3, the customer stops the movie. Normally the viewing period would have ended at point 4, which is the expiration of the 30-day window. At this point at 5, the customer attempts to resume watching the movie, but since the 30-day window expired he cannot watch it anymore. In another embodiment

rather than the 30-day token dominating the 24-hour token, the 24-hour token may be allowed to dominate in which case viewing may be continued as long as it is completed within 24 hours of point 4. This would result in viewing terminating at point 5 in any situation.

[0020] FIG. 3E shows a variation on FIG. 3D where at point 1 the customer initiates the download and the 30-day rental period starts. At point 2, the customer starts to view the movie in the 29th day of the 30-day rental period. The 24-hour viewing window starts immediately. At point 3, the customer pauses the movie and leaves his playback device on pause. Normally at point 4 the 30-day rental period would initially have ended. At point 5, the 24-hour window would have ended. However at point 6, the customer resumes play by pushing the play button on his device. In this case, the 24-hour window has expired but the user may view the remainder of the movie as long as the movie is not paused or stopped again. The movie-watching period expires immediately after play is completed.

[0021] Note in certain embodiments, the content item may be transferred by the user from one consumer electronics device to another as explained further below. However the 30-day time period and 24-hour window still obtain.

[0022] The following is directed to the DRM aspects and what is referred to here as “check-in” and “check-out” procedures in accordance with this disclosure. This is explained in the context of the FIG. 1 system. It is understood that this is carried out in the context of a set of computer programs typically part of the content rental database and logic with co-operating aspects in the DRM server and iTunes Store. These programs are readily coded in light of this disclosure. Typically they would be coded in for instance the C++ language, but this is merely illustrative. Of course the actual code being executed would typically be in compiled form. Moreover the actual encryption/decryption and other DRM aspects are largely conventionally except as explained herein. Hence no further discussion is given of the encryption/decryption or other verification and security aspects. Instead the focus here is on the present rental aspect of the content as opposed to the conventional purchase/download approach.

[0023] First, there is provided here what is referred to as a “rental bag” that is part of the DRM for rentals. This entity is a set of data for each rental transaction, and includes the following: a rental

identification (rentalid) which is a unique identifier assigned by the content rental database to each rental transaction; an account identifier which is an identifier for each user's iTunes account assigned by the iTunes Store; an identifier for the particular content item (program or movie) being rented; and other DRM specific data, including the conventional key bag. This rental bag is illustrated in FIG. 1 and its use explained further below.

[0024] Also provided are three rental related processes referred to here as deauthorization, check in and check out. Deauthorization occurs when a user who has rented a content item purchases a new computer or playback device and wishes to transfer the rented item to the new computer or device. Check in is associated with deauthorization. Briefly, a transfer involves checking in the rental item (to the content rental database) and then subsequently checking the same item out to the new (or another) device. Hence check in occurs when a user deauthorizes his old computer or device in favor of a new one, or when he transfers an asset (content item) from one device to another, such as from his computer to his iPod. A check in is followed by a check out, to the new or other device.

[0025] In more detail, check in involves the following actions, referring to FIG. 1. First, the iTunes client software (which is inherently resident in the iTunes client device 18) passes the rental bag, via the iTunes Store 12, to the content rental database and logic 26. The content rental database and logic 26 (hereinafter "rental database") checks whether the rental bag is eligible for check in. If not, an error indication is returned to the iTunes client. If eligible, the rental database sends the rental bag to the DRM server 24. The DRM server 24 processes the rental bag and extracts from it and returns to the content database 26 the rentalid, the date of the first playback of the content item, and the user account identifier. The rental database checks in the item then indicating the rental is terminated. In other words, it renders that content item (as still resident on the iTunes playback device 18 but in encrypted form) no longer playable. The rental database then sends the updated rental bag back to the iTunes client device 18.

[0026] The check out process occurs more frequently. Not only is it used as the second part of a transfer to complete the transfer, it is also invoked for each new rental (content item download.) Also, the check out process is invoked in the case when the client device 18 attempts to play a

content item but does not have the requisite rental bag for decryption. For instance, this happens when the user attempts to play the item during the initial download. The check out process first requires the iTunes client device 26 to pass a rental bag (one received earlier by the client in a prior rental transaction) to the database 26. Also sent is the client device GUID 20. The database 26 sends this data on to the DRM server 24. The DRM server 24 processes the rental bag and returns to the database 26 the rentalid, the first playback time and date of the content item, and the user account identifier. The database 26 checks in response whether the rental bag is eligible for check out. If ineligible, an error message is returned to the iTunes client device 18. If eligible, the database 26 sends to the DRM server 24 the original rental bag and the new data associated with the current content item being checked out. This data includes the rental id, key(s), rental expiration date (30 days) and rental duration date (24 hour period). The DRM server 24 in response formulates an updated rental bag with the data associated with the current content item being checked out, and send this updated rental bag to the database 26. The database 26 then associates the GUID (global universal identifier) and the rentalid of the updated rental bag in its database, thereby rendering that content item playable upon that device 18. The database 26 then sends the updated rental bag to the client device 18.

[0027] Provided in one embodiment is a security check procedure to attempt to defeat hackers, who try to use the system in unauthorized fashion, such as tampering with the content. This procedure is invoked for both check in and check out and does require initially detection by the system of tampering; this detection is part of the DRM process.

[0028] For check in, when the client first accesses the rental database, an element ("flag" in software terminology) is provided in the DRM data indicating the possible detected tampering. The content database then sends the rental bag to the DRM server with this indication. The DRM server then determines if there has been in fact tampering, and if so sends an indication (another flag) back to the content database. The content database maintains a flag counter for this type of flag for each item, and increments the counter upon receipt of each such flag. If the counter value exceeds a predetermined threshold, then that rentalid is excluded so that content item for that device is rendered unplayable. A warning or notice may be provided to the user at this point.

[0029] A similar security process is provided for the check out procedure. The check out here is modified so that when the content database checks whether the rental bag is eligible for check out, if it determines that the content item is already checked out to that GUID, then the transaction is excluded. Further, if the flag counter value for the rental is greater than the threshold, the transaction is excluded as above. If the value of the flag counter is below the threshold, the content is allowed to be played but the counter value is incremented. Again, a warning or notice may be provided to the user.

[0030] In accordance with another aspect, two embodiments are provided for respectively higher/lower levels of security. In the lower security embodiment, when the user elects to play the rented content, the relevant key bag for the entire rented item is downloaded to his client device and stored there. He can then play the content, even if thereafter his client device is no longer in communication with the iTunes Store (e.g., the client device is no longer connected to the Internet). In the higher security embodiment, the keys are downloaded only as needed for each portion of the rented item, so the client device must remain in communication with the iTunes Store.

[0031] This disclosure is illustrative but not limiting. Further modifications will be apparent to those skilled in the art in light of this disclosure and are intended to fall within the scope of the appended claims.

CLAIMS

We claim:

1. A computer enabled method of allowing playing of content on a client device, the content being encrypted, the method comprising the acts of:

receiving over a communications network an order for the content from the client device;

transmitting to the client device over the communications network the encrypted content;

receiving a request from the client to play the transmitted content via the communications network; and

transmitting key information for decrypting the content responsive to the play request, the key information being effective for the decryption only for a predetermined period of time after the receipt of the play request.

2. The method of Claim 1, wherein method is carried out by a server, and the key information is effective for the decryption even if the client device is no longer connected to the server via the communications network.

3. The method of Claim 1, wherein the method is carried out by a server, and the key information is effective for the decryption only if the client device is connected to the server via the communications network.

4. The method of Claim 1, further comprising:

wherein during play and decryption of the content the play is interrupted,

receiving a further request over the communications network for the decryption information in order to resume play.

5. The method of Claim 1, wherein the content is a television program or a movie.

6. The method of Claim 1, further comprising:

transmitting a security policy with the key information, the security policy defining a number of times the key information decrypts the content, and a number of client devices on which the key information may decrypt the content.

7. The method of Claim 6, wherein the security policy and key information are part of a digital rights management file.

8. The method of Claim 1, wherein the key information defines a plurality of decryption keys.

9. The method of Claim 8, wherein the decryption keys are for decrypting a symmetric or asymmetric cipher.

10. The method of Claim 1, wherein the client device is a media player equipped with a port connectable to the communications network, or is a host connectable to a media player and to the communications network.

11. The method of Claim 1, wherein the content is partitioned into portions, each requiring a different key for the decryption, and the key information defines the different keys.

12. The method of Claim 1, further comprising the act of preventing the transmitting of the key information, a predetermined time after the encrypted content is transmitted.

13. A computer enabled method for allowing playing of content on a client device, the content being encrypted, the method comprising the acts of:

transmitting an order over a communications network from the client to a source of the content;

receiving the encrypted content over the communications network from the source;

beginning to play the encrypted content on the client device;

wherein the client device transmits a play request for key information to the source;

receiving the key information at the client device as transmitted from the source, the received key information being effective for decryption of the content only for a predetermined period of time after its transmission.

14. A computer readable medium storing computer code for carrying out the method of Claim 1.

15. A computer server system, comprising:

a receiving portion for receiving an order over a communications network in order for content to be played on a client device;

a transmission portion coupled to the receiving portion for transmitting over the communications network the content, in encrypted form;

a second receiving portion for receiving a request from the client to play the transmitted content over the communications network;

a memory storing key information associated with the content; and

a second transmission portion coupled to the memory and to the second receiving portion, for transmitting the key information responsive to the play request, the transmitted key information being effective only for a predetermined period of time after the receipt of the play request.

16. The system of Claim 1, further comprising a database of transactions, the database storing the predetermined period of time and a duration of time after the encrypted content is transmitted for further limiting the effectiveness of the key information.

We claim:

1. A computer enabled method of allowing playing of content on a client device, the content being encrypted, the method comprising the acts of:

receiving over a communications network an order for the content from the client device;

transmitting to the client device over the communications network the encrypted content;

receiving a request from the client to play the transmitted content via the communications network; and

transmitting key information for decrypting the content responsive to the play request, the key information being effective for the decryption only for a predetermined period of time after the receipt of the play request.

2. The method of Claim 1, wherein method is carried out by a server, and the key information is effective for the decryption even if the client device is no longer connected to the server via the communications network.

3. The method of Claim 1, wherein the method is carried out by a server, and the key information is effective for the decryption only if the client device is connected to the server via the communications network.

4. The method of Claim 1, further comprising:

wherein during play and decryption of the content the play is interrupted,

receiving a further request over the communications network for the decryption information in order to resume play.

5. The method of Claim 1, wherein the content is a television program or a movie.

6. The method of Claim 1, further comprising:

transmitting a security policy with the key information, the security policy defining a number of times the key information decrypts the content, and a number of client devices on which the key information may decrypt the content.

7. The method of Claim 6, wherein the security policy and key information are part of a digital rights management file.
8. The method of Claim 1, wherein the key information defines a plurality of decryption keys.
9. The method of Claim 8, wherein the decryption keys are for decrypting a symmetric or asymmetric cipher.
10. The method of Claim 1, wherein the client device is a media player equipped with a port connectable to the communications network, or is a host connectable to a media player and to the communications network.
11. The method of Claim 1, wherein the content is partitioned into portions, each requiring a different key for the decryption, and the key information defines the different keys.
12. The method of Claim 1, further comprising the act of preventing the transmitting of the key information, a predetermined time after the encrypted content is transmitted.
13. A computer enabled method for allowing playing of content on a client device, the content being encrypted, the method comprising the acts of:
 - transmitting an order over a communications network from the client to a source of the content;
 - receiving the encrypted content over the communications network from the source;
 - beginning to play the encrypted content on the client device;
 - wherein the client device transmits a play request for key information to the source;
 - receiving the key information at the client device as transmitted from the source, the received key information being effective for decryption of the content only for a predetermined period of time after its transmission.
14. A computer readable medium storing computer code for carrying out the method of Claim 1.
15. A computer server system, comprising:

a receiving portion for receiving an order over a communications network in order for content to be played on a client device;

a transmission portion coupled to the receiving portion for transmitting over the communications network the content, in encrypted form;

a second receiving portion for receiving a request from the client to play the transmitted content over the communications network;

a memory storing key information associated with the content; and

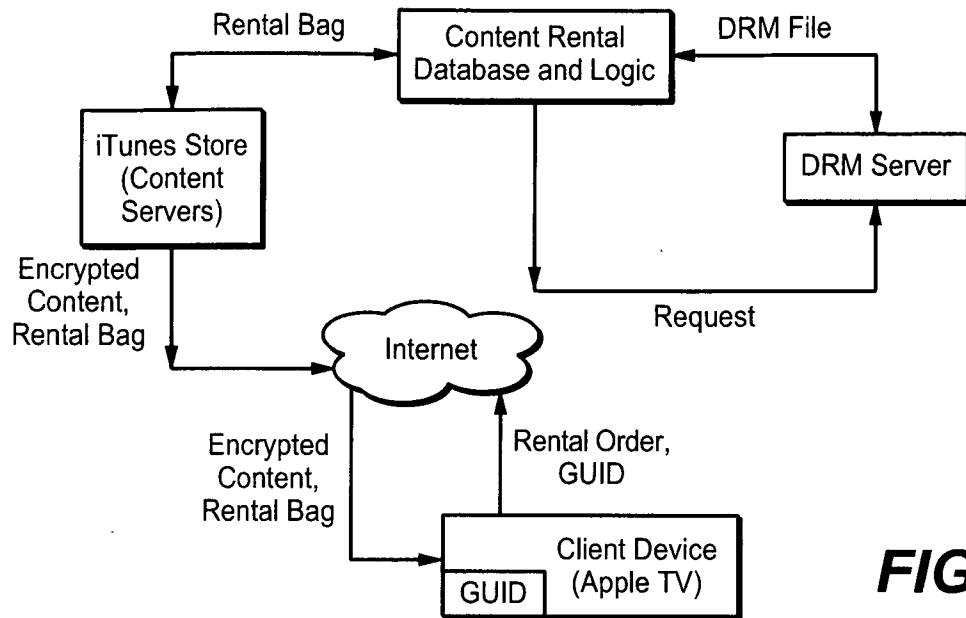
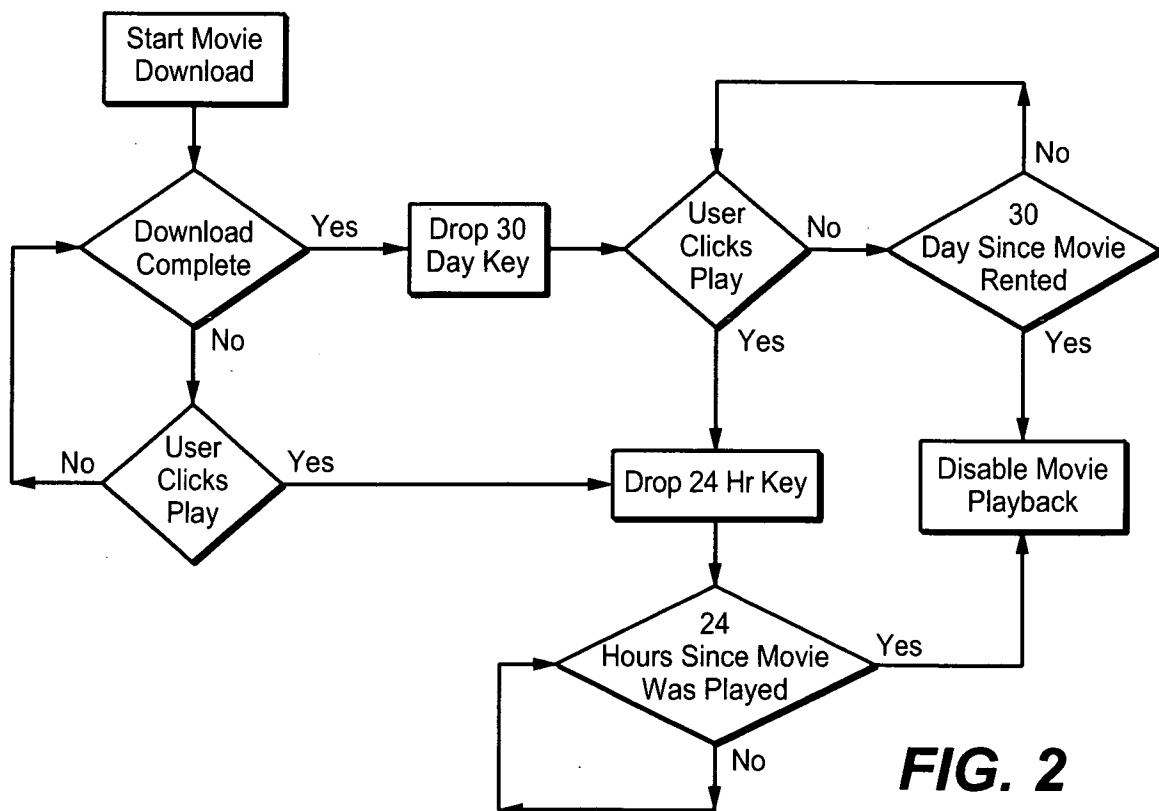
a second transmission portion coupled to the memory and to the second receiving portion, for transmitting the key information responsive to the play request, the transmitted key information being effective only for a predetermined period of time after the receipt of the play request.

16. The system of Claim 1, further comprising a database of transactions, the database storing the predetermined period of time and a duration of time after the encrypted content is transmitted for further limiting the effectiveness of the key information.

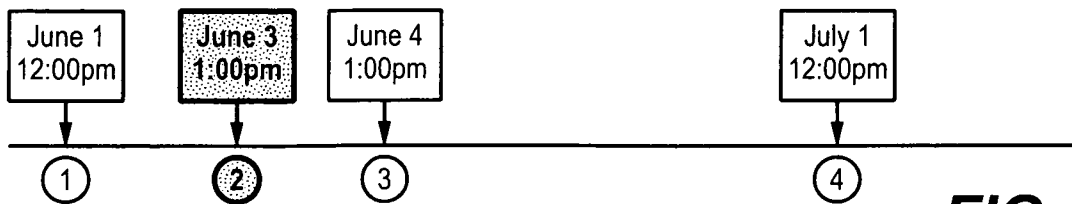
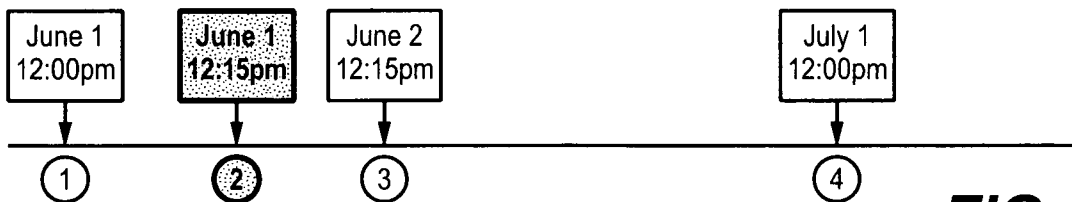
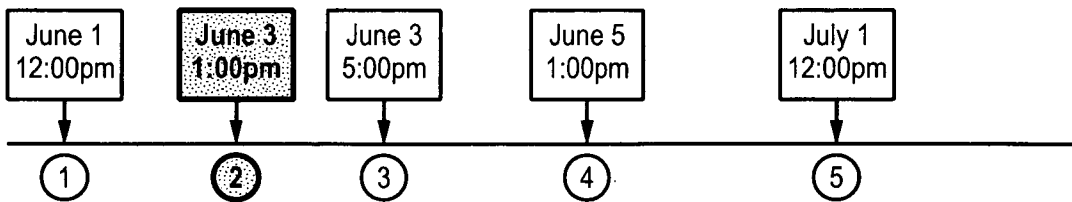
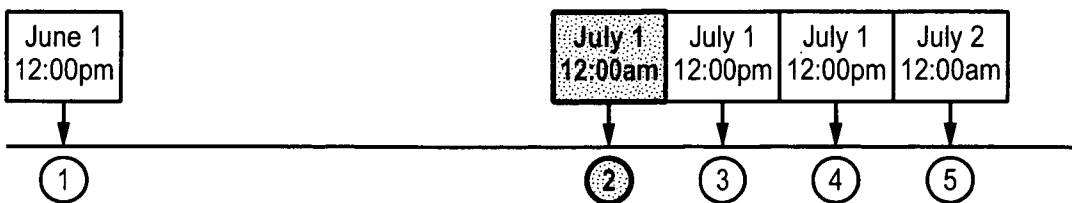
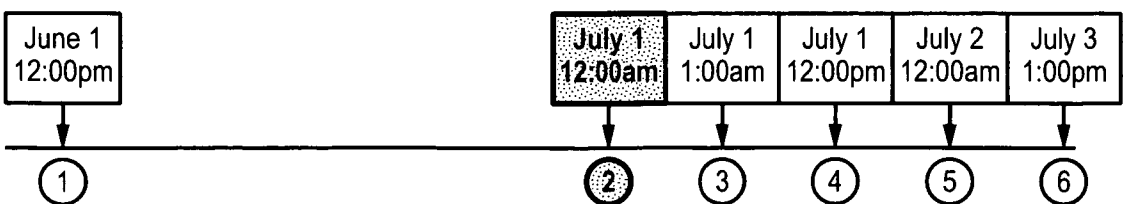
17. The method of Claim 13, wherein even if the predetermined period of time is exceeded, play of the encrypted content is permitted until completed so long as the play was begun prior to expiration of the predetermined period of time.

18. The method of Claim 13, wherein the client device includes a pause function, and wherein if the pause function is invoked during the predetermined period of time, playing of the encrypted content is allowed to continue until completed after the predetermined period of time is exceeded.

1 / 2

**FIG. 1****FIG. 2**

2 / 2

**FIG. 3A****FIG. 3B****FIG. 3C****FIG. 3D****FIG. 3E**

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2008/014150

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04N7/16

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04N

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

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

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/114896 A1 (HUG JOSHUA D [US] ET AL) 26 May 2005 (2005-05-26) paragraphs [0020] - [0048]; figures 1-10	1-16
X	US 2005/276570 A1 (REED OGDEN C JR [US] ET AL) 15 December 2005 (2005-12-15) paragraphs [0064] - [0521]; figures 1-11	1-16
X	US 2002/184515 A1 (OHO MASAHIRO [JP] ET AL) 5 December 2002 (2002-12-05) the whole document	1-16
X	US 2007/098162 A1 (SHIN SUNG-CHOL [KR]) 3 May 2007 (2007-05-03) the whole document	1-16

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *G* document member of the same patent family

Date of the actual completion of the international search

23 February 2009

Date of mailing of the international search report

09/03/2009

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Marzal-Abarca, X

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2008/014150

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005114896	A1	26-05-2005	GB 2423393 A 23-08-2006
			US 2006085352 A1 20-04-2006
			US 2006259429 A1 16-11-2006
			US 2006259436 A1 16-11-2006
			US 2006265329 A1 23-11-2006
			WO 2005052901 A2 09-06-2005
US 2005276570	A1	15-12-2005	NONE
US 2002184515	A1	05-12-2002	CN 1608263 A 20-04-2005
			EP 1479016 A2 24-11-2004
			WO 02097693 A2 05-12-2002
US 2007098162	A1	03-05-2007	CN 1956534 A 02-05-2007
			KR 20070045556 A 02-05-2007