



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
61/500,316	06/23/2011		110	1082-018		

CONFIRMATION NO. 7568

47654
BAINWOOD HUANG & ASSOCIATES LLC
2 CONNECTOR ROAD
WESTBOROUGH, MA 01581

FILING RECEIPT



OC000000048585270

Date Mailed: 07/07/2011

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. 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**

Applicant(s)

Kevin J. Ma, Nashua, NH;
Robert Hickey, Bedford, MA;
Paul Tweedale, Andover, MA;

Power of Attorney:

James Thompson--36699

If Required, Foreign Filing License Granted: 07/05/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/500,316**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

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).

TITLE:

Method and System for Secure Over-the-Top Live Video Delivery

ABSTRACT:

A method is provided for managing key rotation and secure key distribution in over-the-top delivery of content. The method provided supports supplying a first content encryption key to a content packaging engine for encryption of a first portion of a video stream. Once the first content encryption key has expired, a second content encryption key is provided to the content packaging engine for encryption of a second portion of a video stream. The method further provides for notification of client devices of imminent key changes, as well as support for secure retrieval of new keys by client devices. A system is also specified for implementing a client and server infrastructure in accordance with the provisions of the method.

CLAIMS:

1. A method for managing the secure distribution of content, the method comprising the following steps: generating a first content encryption key; providing a first encryption key to a packaging server; encrypting content using the first encryption key; providing the first content encryption key to a license server; expiring the first content encryption key, generating a second content encryption key; providing the second content encryption key to the packaging server; encrypting subsequent content with the new content encryption key; providing the second content encryption key to the license server; notifying client devices of the content encryption key expiration; and providing the appropriate content encryption keys to the client.
2. The method of claim 1, wherein the content is audio/video content.
3. The method of claim 1, wherein the encryption algorithms include AES128, HC128, and RC4.
4. The method of claim 1, wherein the content encryption keys are generated using strong entropy sources.
5. The method of claim 1, wherein the content encryption key is provided to the packaging server through a secure interface.
6. The method of claim 5, further comprising: using SSL to secure the interface.
7. The method of claim 5, further comprising: pushing a content encryption key to the packaging server when the license server determines expiration of the previous key is necessary.
8. The method of claim 5, further comprising: pushing a content encryption key and predetermined expiration time to the packaging server.

9. The method of claim 8, further comprising: pushing the content encryption key and predetermined expiration time only in response to a request for a new content encryption key from the packaging server.
10. The method of claim 9, further comprising: the packaging server requesting a new key in anticipation of the expiration of its current key.
11. The method of claim 1, wherein the client is notified at session initiation of the fixed period for content key expiration.
12. The method of claim 1, wherein the client is notified in real-time content key expiration.
13. The method of claim 12, further comprising: the packaging server inserting a key change notification into a content encryption metadata header as part of the unencrypted portion of the encrypted file.
14. The method of claim 13, further comprising: the header being a PlayReady header.
15. The method of claim 12, further comprising: the packaging server inserting a key change notification into a content manifest file.
16. The method of claim 15, further comprising: the manifest file being an m3u8 file.
17. The method of claim 15, further comprising: the manifest file being an IIS Smooth Streaming manifest file.
18. The method of claim 12, further comprising: the packaging server inserting a key change notification into the file name of the segment files being generated.
19. The method of claim 1, wherein the content encryption key is provided to the license server through a secure interface.
20. The method of claim 19, further comprising: using SSL to secure the interface.
21. The method of claim 1, wherein, content encryption keys for a given media are versioned
22. The method of claim 21, further comprising: using monotonically increasing integer values.
23. The method of claim 22, further comprising: maintaining a direct correlation between the version and the content segment number or duration
24. The method of claim 1, wherein the license server distributes content encryption keys and content encryption key expiration information to clients using a secure channel.
25. The method of claim 24, further comprising: using SSL to secure the interface.
26. The method of claim 21, further comprising: providing the client with the two most recently generated content encryption keys.
27. The method of claim 26, further comprising: returning content encryption keys and expiration information only when the client requests it.
28. The method of claim 27, further comprising: verifying client identity and content rights before returning content encryption key or expiration information.
29. The method of claim 21, further comprising: allowing clients to request any previous content encryption key and expiration information.

30. The method of claim 21, further comprising: allowing clients to only request a fixed number of most recently generated content encryption keys and expiration information.
31. The method of claim 3, further comprising: resetting the initialization vector when the content encryption key is rotated.
32. [insert apparatus claims here].

BACKGROUND:

This invention relates in general to over-the-top (OTT) media delivery and more specifically to encryption key rotation for live streaming media.

As content delivery models move away from streaming distribution over private networks to Web-based delivery of files over the public Internet, referred to as over-the-top (OTT) delivery, traditional content protection paradigms must be modified to support new delivery protocols, e.g., HTTP Live Streaming. For live streaming content with long or indefinite durations, use of a single encryption key for the entire duration increases the probability that the key may be compromised. Traditional key rotation schemes used in private multiple system operator (MSO) and mobile network operator (MNO) distribution networks, where physical security protects the key distribution path, do not extend to use over the public Internet, where communications channels are more susceptible to attack. Furthermore, the encryption used with nascent segment-based HTTP distribution protocols (e.g., HTTP Live Streaming, Silverlight Smooth Streaming, MPEG/3GP Dynamic Adaptive Streaming over HTTP (DASH), etc.) also differs from traditional streaming techniques. Encryption of non-segmented content is typically performed using a single encryption key using a single continuous pass over the content, from start to finish. For segment-based formats, each segment may use the same content encryption key. Though the content encryption key may be salted with a unique initialization vector (IV) for each segment, the IV is not random and does not provide the same security as key rotation. New methods are required for the management of key rotation and key distribution to ensure security for OTT content delivery.

SUMMARY:

Methods and apparatus are disclosed for managing the distribution of a plurality of content encryption keys for use in the protection of live streaming content. A workflow management system, referred to herein as a workflow manager, is responsible for managing the acquisition of source content from a content management system, preparation of the content, including, but not limited to, transcoding of the content into different encodings (e.g., different bitrates, frame rates, resolutions, sample rates, codecs, etc.), storing the transcoded content in different formats (e.g., 3GP, segmented 3GP, MP4, fragmented MP4, MPEG-TS, segmented MPEG-TS, RTP, etc.), and encrypting the different formats, so that the content is suitable for delivery to a plurality of client devices over a plurality of network infrastructures. The prepared content is then uploaded to a

CDN for delivery to clients. The invention includes provisions for managing when content encryption keys expire, distributing content encryption keys to packaging engines, and distributing content encryption keys to clients.

In the preparation and distribution of content, specifically video content, modern protocols (e.g., HTTP Live Streaming, Silverlight Smooth Streaming, MPEG/3GP Dynamic Adaptive Streaming over HTTP (DASH), etc.) employ segment-based rate adaptation to deal with fluctuations in bandwidth, whereby segment boundaries provide natural demarcation points for switching bitrates. Another example of a protocol and file format suitable for segment-based rate adaptation is described in PCT Application No. PCT/US2010/027893 filed March 19, 2010, and entitled, Method for Scalable Live Streaming Delivery for Mobile Audiences. Yet another example of a protocol and file format suitable for segment-based rate adaptation is described in PCT Application No. PCT/US2010/028309 filed March 23, 2010, and entitled, Method and System for Efficient Streaming Video Dynamic Rate Adaptation. There are many protocols and methods for generating segmented content, as should be known to those skilled in the art. Any of these segmentation methods are suitable for use in accordance with provisions of the invention. For segment-based formats (e.g., segmented 3GP, fragmented MP4, segmented MPEG-TS, etc.), each segment is independently playable, and therefore needs to be independently encrypted and decryptable. Segments are typically of a fixed duration and, in the case of video content, begin with a key-frame and contain no inter-segment references. Segmentation is performed on each of the different encoding generated by the transcoder, by parsing the resultant encoding and determining segment boundaries. In one embodiment segment boundaries are based on a fixed number of bytes of data. In another embodiment segment boundaries are based on a fixed number of video key frames.

Segments are encrypted on segment boundaries using the current content encryption key and current initialization vector (IV). In one embodiment, the IV may be a simple incrementing integer value. In another embodiment, the IV may be a pseudo-random stream of bits produced by a pseudo-random number generator or stream cipher. Though the IV provides some additional cryptographic strength, it is not random. The generation of new strongly random values for use as content encryption keys and the rotation of content encryption keys provides protection from content encryption keys being compromised in long lived streams. In one embodiment, IVs are reinitialized whenever a content encryption key is rotated. In another embodiment, IVs are not reinitialized when content encryption keys are rotated.

In one embodiment the workflow manager generates content encryption keys with a fixed duration lifespan on a fixed periodic basis. In one embodiment, the content encryption keys may be generated using weak sources of entropy (e.g., processor or wall clock time, /dev/urandom, etc). In another embodiment, the content encryption keys may be generated using strong sources of entropy (e.g., hardware sources which rely on electrical static or radioactive decay, /dev/random/, etc.). There are many ways to generate random numbers, as should be known to

those skilled in the art. Any method for generating random numbers may be used in accordance with provisions of this method. The workflow manager distributes the content encryption keys and content encryption key lifespan to both a license server and content packaging engine, referred to herein as a packager. The fixed duration lifespan is directly correlated to a fixed period of the live content. The changing of content encryption keys based on the fixed period of the live content is referred to herein as rotation. A history of individual content encryption keys and the order in which they were generated is maintained. Each content encryption key in the history is assigned a unique identifier which is referred to herein as the content encryption key identifier. In one embodiment, the content encryption key identifiers are selected based on the wall clock time offset from the beginning of the live stream. In another embodiment, the content encryption key identifiers are selected based on a segment number of the prepared content. In one embodiment the segment boundaries are based on a fixed number of bytes of data. In another embodiment the segment boundaries are based on a fixed number of video key frames. The content packaging engine is responsible for encrypting the associated content using the content encryption key. In one embodiment, the packager recognizes the imminent end to the fixed duration lifespan and requests a new content encryption key from the workflow manager. The license server is responsible for distributing content encryption keys to clients. In one embodiment, the license server also distributes fixed duration lifespan information to clients. In one embodiment, when initiating playback of the stream, the client requests the current content encryption key, the next future content encryption key, and the fixed duration lifespan of the keys. The client uses the content encryption keys to decrypt the associated content.

In one embodiment, the workflow manager may initiate content encryption key rotation at any time, outside of the fixed duration lifespan of the existing key. The workflow manager is responsible for notifying the packager of the key rotation request. The packager is responsible for selecting when the new key shall be applied and notifying the workflow manager. In one embodiment, the point at which the key is applied is based on the wall clock time offset from the beginning of the live stream. In another embodiment, the point at which the key is applied is based on a segment number of the prepared content. In one embodiment the segment boundaries are based on a fixed number of bytes of data. In another embodiment the segment boundaries are based on a fixed number of video key frames. The workflow manager is then responsible for notifying the license server of the new content encryption key, the content encryption key identifier of the new content encryption key, and the lifespan of the new content encryption key. In one embodiment, content encryption key identifiers are selected based on the fixed period of the live content. In one embodiment, the content encryption key identifiers are selected based on the wall clock time offset from the beginning of the live stream. In another embodiment, the content encryption key identifiers are selected based on a segment number of the prepared content. In one embodiment the segment boundaries are based on a fixed number of bytes of data. In another embodiment the segment boundaries are based on a fixed number of video key frames. The packager is responsible for providing in-band notification to the client for the key

change. In one embodiment, the notification is embedded in a manifest file that describes the encrypted content. In another embodiment, the notification is embedded in the segment file name of the encrypted content. In another embodiment, the notification is embedded in a header prepended to the encrypted content. In one embodiment, the header may be a Microsoft PlayReady header. In another embodiment, the header may be an MPEG/3GP DASH header. In another embodiment, the header may be a proprietary segment format header.

These provisions together with the various ancillary provisions and features which will become apparent to those artisans possessing skill in the art as the following description proceeds are attained by devices, assemblies, systems and methods of embodiments of the present invention, various embodiments thereof being shown with reference to the accompanying drawings, by way of example only, wherein:

FIGURES:

- FIG. 1 is a block diagram of a system which is capable of conducting content encryption key rotations procedures, in accordance with various embodiments of the invention;
- FIG. 2 is a flow chart showing a method for performing content encryption key rotation, in accordance with an embodiment of the present invention; and
- FIG. 3 is a flow chart showing another method for detecting content encryption key rotation, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION:

In the description herein for embodiments of the present invention, numerous specific details are provided, such as examples of components and/or methods, to provide a thorough understanding of embodiments of the present invention. One skilled in the relevant art will recognize, however, that an embodiment of the invention can be practiced without one or more of the specific details, or with other apparatus, systems, assemblies, methods, components, materials, parts, and/or the like. In other instances, well-known structures, materials, or operations are not specifically shown or described in detail to avoid obscuring aspects of embodiments of the present invention.

In FIG. 1 is a block diagram 100 for one embodiment of the present invention. The workflow manager (WFM) 102 is responsible for initiating ingestion and preparation of live content. In one embodiment, preparation includes transcoding audio and video into a plurality of encodings using different codecs, bitrates, frame rates, sample rates, and resolutions. The transcoded content is then written into a plurality of output files. In one embodiment, a plurality of output files contain the same transcoded content encapsulated in different container formats (e.g., 3GP, MP4, MPEG-TS, WMV, MOV, etc.). In one embodiment, the prepared output files are segmented into fixed duration segment files (e.g., MPEG-TS segments, fragmented MP4 segments, 3GP DASH segments, etc.). In one embodiment, the output files, both segmented and un-segmented, are encrypted using standard encryption protocols (e.g., AES-128, HC-128, RC4,

etc.) . In one embodiment, IVs for the encryption protocol are reinitialized by the packager 104 whenever a content encryption key is rotated. In another embodiment, IVs for the encryption protocol are not reinitialized when content encryption keys are rotated. In one embodiment, all preparation steps are performed by a single content packaging server 104, referred to herein as a packager. In another embodiment, individual preparation steps (e.g., transcoding, segmentation, encryption, etc.) may be performed across different physical content packaging servers 104. The packager 104 which performs encryption acquires content encryption keys from the workflow manger 102. In one embodiment the WFM 102 and packager 104 reside in the same physical server. In another embodiment, the WFM 102 and packager 104 reside in different physical servers in the same data center. In another embodiment, the WFM 102 and packager 104 reside in different physical servers in remote data centers.

It will be appreciated that the term "server" used herein refers to a general-purpose or special-purpose computer, generally including memory, input/output circuitry, and instruction processing logic along with interconnections such as one or more high-speed data buses connecting those components together. Many aspects of the disclosed techniques can be embodied as software executing on one or more server computers. Similarly, a "client" herein is a computerized device (also including the above components) capable of receiving content from a network connection and decoding and rendering the content on a display or similar output device. So-called smartphones are specifically included within the definition of client as used herein.

The WFM 102 receives an ingestion request from the content management system (CMS) 112. The CMS specifies a security profile. In one embodiment, the security profile includes content encryption information, including cipher specification and content encryption key expiration policies. The WFM 102 generates an initial content encryption key and assigns it a content encryption key identifier. In one embodiment, the content encryption key identifier is initially set to zero and all future content encryption key identifiers are based on a relative offset to the initial content encryption key identifier. In one embodiment, the content encryption key identifiers are based off the wall clock time offset from the time the initial content encryption key identifier was generated. In another embodiment, the content encryption key identifiers are based off of segment numbers, as produced by the packager 104 during segmentation. In one embodiment the segment boundaries are based on a fixed number of bytes of data. In another embodiment the segment boundaries are based on a fixed number of video key frames.

The WFM 102 then initiates content preparation by assigning a packager 104 to begin acquiring the source content and performing transcoding and segmentation as required. The WFM 102 provides the initial content encryption key and lifespan of the key to the packager 104 responsible for encryption of the prepared outputs. The packager 104 encrypts the content using the initial content encryption key until it expires. In one embodiment, the expiration time is based on a relative wall clock time offset to the time preparation was started. In another

embodiment, the content encryption key identifiers are based off of segment numbers, as produced by the packager 104 during segmentation. As described above, segmentation detects segment boundaries and assigns a fixed amount of data to each individual segment. In one embodiment the segment boundaries are based on a fixed number of bytes of data. In another embodiment the segment boundaries are based on a fixed number of video key frames. In one embodiment, before the content encryption key expires, the packager 104 requests a new key from the WFM 102. In one embodiment, the new content encryption key has the same lifespan as the previous content encryption key. The new content encryption key is made available by the WFM 102 to the packager 104 before the previous content encryption key has expired to allow for uninterrupted encryption.

Encrypted content is uploaded by the packager 104 to a content delivery network (CDN) 108, from which it may be retrieved by clients 110. In one embodiment, manifest files are also uploaded by the packager 104 to the CDN 108. The clients 110 must first obtain the content encryption keys from the license server 106, before they may decrypt and render encrypted content. In one embodiment, clients 110 retrieve content encryption keys using HTTPS. In one embodiment, clients 110 are verified by the license server 106 using client certificate verification. In another embodiment, clients 110 are verified using login credentials. The license server 106 is notified of new content encryption keys by the WFM 102 as they are generated. In one embodiment, the license server 106 stores the content encryption key, content encryption key identifier, content encryption key lifespan (or expiration), and the location of the encrypted content. In one embodiment, the information is stored as an encrypted token in a database. In one embodiment the WFM 102 and license server 106 reside in the same physical server. In another embodiment, the WFM 102 and license server 106 reside in different physical servers in the same data center. In another embodiment, the WFM 102 and license server 106 reside in different physical servers in remote data centers. In one embodiment, the license server 106 registers client devices 110 and verifies the right of each client device 110 to view the content. If the client 110 has the right to view the content, the license server 106 provides the content encryption key, content encryption key lifespan (or expiration), and the location of the encrypted content.

In one embodiment, the WFM 102 may issue a new unsolicited content encryption key to the packager 104. In one embodiment, the WFM 102 pushes the new content encryption key to the packager 104 when the current content encryption key is nearing the end of its lifespan. The new content encryption key is pushed ahead of the current content key expiration and the packager 104 waits until the current content encryption key has expired before applying the new content encryption key. In another embodiment, the WFM 102 pushes the new content encryption key to the packager 104 when the current content encryption key is deemed to be no longer secure (e.g., if the content encryption key has been compromised). The packager 104 waits until the next available encryption boundary before applying the new content encryption key, and then notifies

the WFM 102 of the exact boundary at which it expired the previous content encryption key. In one embodiment, the encryption boundary is a segment boundary. In one embodiment the segment boundaries are based on a fixed number of bytes of data. In another embodiment the segment boundaries are based on a fixed number of video key frames.

In one embodiment, the lifespan of the new content encryption key is aligned to the periodic boundaries of the previous content encryption keys. In one embodiment, the expiration of the new content encryption key is set to the expiration time of the previous content encryption key, i.e., if the new content encryption key was applied when the previous content encryption key had 10 minutes left in its lifespan, then the lifespan of the new content encryption key would be set to 10 minutes. In another embodiment, the expiration of the new content encryption key is set to the next periodic expiration time which is greater than half the fixed expiration period duration, i.e., if the lifespan of content encryption keys is 60 minutes and the previous content encryption key had 10 minutes left in its lifespan, then the lifespan of the new content encryption key would be set to 70 minutes ($10 + 60$) because the remaining time of 10 minutes would be less than half the fixed expiration period duration ($60 / 2 = 30$).

In one embodiment, the packager 104 notifies the client 110 of the key change by prepending a header to the encrypted content which contains a flag that describes the expiration of the previous key. In another embodiment, the packager 104 notifies the client 110 of the key change by updating a manifest file that describes the encrypted content with a flag that describes the expiration of the previous key. In another embodiment, the packager 104 notifies the client 110 of the key change in the file name of the encrypted content by appending a flag that describes the expiration of the previous key.

FIG. 2 is a flow chart 200 describing a process for obtaining and rotating content encryption keys in a packager 110. In step 202, the WFM 102 receives an ingestion request from a CMS 110. In one embodiment, the request is an HTTP POST of XML data containing information including, but not limited to, transcode parameters, segmentation parameters, encryption parameters, source content location, and CDN parameters. In one embodiment, the WFM 102 may have predefined profiles for media preparation, content encryption, and CDN upload which are referenced in the ingestion request. In one embodiment the encryption parameters include a fixed period duration for key rotation.

In step 204, the WFM 102 instructs the packager 104 to begin preparation of the content. A packager 104 begins acquiring the source content, transcoding the source content and segmenting the source content. As each segment is produced, it is delivered to the packager 104 responsible for encrypting the prepared content.

In step 220, the packager 104 responsible for encryption, referred to hereafter as the packager 104, waits for new segments to become available. Once a new segment becomes available,

processing proceeds to step 206 where the packager 104 checks to see if a new content encryption key has been received from the WFM 102. The content encryption key may be an initial content encryption key provided by the WFM 102 with the initial content preparation request. The content encryption key may be received in response to a content encryption key request from the packager 104 (originating from step 218). The content encryption key may be received via a proactive push from the WFM 102 in anticipation of a periodic content encryption key expiration event. The content encryption key may be an unsolicited content encryption key pushed by the WFM 102 as necessitated by security policies (e.g., the current content encryption key was compromised or the current content encryption was found to be not sufficiently random).

If no new content encryption key was received at step 206, processing proceeds to step 210. If a new content encryption key was received, processing proceeds to step 208 where the expiration times for the current content encryption key and the new content encryption key are determined. If the new content encryption key is an initial content encryption key or a regularly scheduled update in advance of a periodic content encryption key expiration (either requested by the packager 104, or pushed proactively by the WFM 102), the lifespan is set to the fixed period duration. If the new content encryption key is not a regularly scheduled update and must be applied as soon as possible, the expiration of the current content encryption key and the new content encryption key are calculated. In one embodiment, the new content encryption key is applied at the next segment boundary. In one embodiment, the lifespan of the new content encryption key is set to the remainder of the lifespan of the current content encryption key. In another embodiment, the lifespan of the new content encryption key is rounded up to the remainder of the lifespan of the current content encryption key plus one fixed key rotation period duration. Once the content encryption key expirations have been set, processing proceeds to step 210.

In step 210, the packager 104 checks the expiration of current content key to see if a new key should be applied. If the current content encryption key has not yet expired, processing proceeds to step 214. If the current content encryption key needs to be expired, processing proceeds to step 212 where the current content encryption key is expired and replaced with the pending content encryption key. In one embodiment, the IV is reinitialized when the content encryption key is expired. In another embodiment, when content encryption key is expired, the packager 104 continues to use the existing IV stream. Once the new content encryption key is in place, processing proceeds to step 214. In step 214, the segment received in step 220 is encrypted using the current content encryption key and the cipher specified in the ingestion request. Once the segment has been encrypted it is uploaded to the CDN 108 and processing proceeds to step 216.

In step 216, the packager 104 check to see if the current content encryption key is going to expire in the near future. In one embodiment, when the current content encryption key is about to

expire, the packager 104 proactively requests a new content encryption key ahead of time to prevent any interruption of encryption services. If the current content encryption key is not close to expiring, processing proceeds back to step 220 where the packager 104 waits for the next segment to be encrypted. If the current content encryption key is within a fixed threshold of expiring, processing proceeds to step 218 where the packager 104 requests a new content encryption key from the WFM 102. In one embodiment, the threshold is set as a fixed amount of wall clock time before the current content encryption key will expire (e.g., 1 minute prior to the expiration of the current content encryption key). In another embodiment, the threshold is set as a fixed number of segments before the current content encryption key will expire (e.g., 6 segments before the expiration of the current content encryption key, where 10 second fixed duration segments would yield a threshold of approximately 1 minute). In another embodiment, the threshold is set as a fixed percentage of the fixed period content encryption key lifespan (e.g., when the lifespan of the current content encryption key is 90% complete). Once the request for a new content encryption key has been sent in step 218, processing proceeds back to step 220 where the packager 104 waits for the next segment to be encrypted.

FIG. 3 is a flow chart 300 describing a process for detecting the rotation of content encryption keys and retrieving updated content encryption keys. In step 302, the client 110 issues a playback request to the WFM 102. In one embodiment, the initial playback request may require registration of the client 110, user login, or some other authentication mechanism. In step 304, the client 110 retrieves and parses the content information, including content formats, content bitrates, content locations, content encryption keys, and content encryption key expiration. In one embodiment, the WFM 102 and license server 106 are deployed of the same physical machine with the ability to function through a single software interface when dealing with the client 110, and the WFM 102 may return all the necessary information, including content formats, content bitrates, content locations, content encryption keys, and content encryption key expiration, to the client 110. In another embodiment, the WFM 102 and license server 106 are deployed separately, and the client 110 must make a first request to the WFM 102 to retrieve content formats, content bitrates, content locations, and the license server 106 location. The client 110 then makes a second request to the license server 106 to retrieve content encryption keys and content encryption key expiration information. In one embodiment, the retrieval of content encryption keys is performed over a secure channel. In one embodiment, the channel is secured using HTTPS. In another embodiment, the channel could be secured with a proprietary encryption mechanism. There are numerous ways to secure a communications channel, as should be known to those skilled in the art. Any method for securing a communications channel may be applied in step 304. In one embodiment, the channel requires authentication of the client device 110. In one embodiment, authentication is performed using SSL client authentication. In another embodiment, authentication is performed using proprietary certificate validation procedures. In another embodiment, authentication is performed using symmetric key encryption using white-box encryption methods. In another embodiment, user login credentials

are passed over the secure channel. There are numerous ways to authenticate a client device 110, as should be known to those skilled in the art. Any method for authenticating a client device 110 may be applied in step 304. Once the initial playback response message processing has completed, processing proceeds to step 306.

In step 306, the client 110 retrieves the next available segment from the CDN 108. In one embodiment, the first available segment is specified by the WFM 102 in the initial playback response message. In another embodiment, the first available segment is specified in a manifest file retrieved from the CDN 108. In one embodiment, subsequent segments are identified based on sequential segment numbering using a well-known file naming scheme. In another embodiment, subsequent segments are identified by a manifest file in the CDN 108. In another embodiment, subsequent segments are identified based on the relative wall clock time in which they are generated, by performing directory listings or using a watched directory to determine when new segments become available. Once the new segment is retrieved, processing proceeds to step 308 where the client 110 checks to see if an unscheduled key change is signaled, i.e., a key change was requested outside of any fixed duration lifespan. In one embodiment, the packager 104 notifies the client 110 of the key change by prepending a header to the encrypted content which contains a flag that describes the expiration of the previous key. In another embodiment, the packager 104 notifies the client 110 of the key change by updating a manifest file that describes the encrypted content with a flag that describes the expiration of the previous key. In another embodiment, the packager 104 notifies the client 110 of the key change in the file name of the encrypted content by appending a flag that describes the expiration of the previous key. If a content encryption key change request is detected, the client notes the content encryption key change request. The client 110 then proceeds to step 310.

In step 310, the client 110 checks the expiration of current content key to see if a new key should be applied. If the current content encryption key has not yet expired, processing proceeds to step 314. If the current content encryption key needs to be expired, processing proceeds to step 312 where the current content encryption key is expired and replaced with the pending content encryption key. In one embodiment, the IV is reinitialized when the content encryption key is expired. In another embodiment, when content encryption key is expired, the client 110 continues to use the existing IV stream. Once the new content encryption key is in place, processing proceeds to step 314. In step 314, the segment retrieved in step 306 is decrypted using the current content encryption key and the cipher specified in the initial playback response message. Once the segment has been decrypted it is passed to the media player for rendering and processing proceeds to step 316.

In step 316, the client 110 check to see if the current content encryption key is going to expire in the near future or if a content encryption key change request was detected in step 308. In one embodiment, when the current content encryption key is about to expire, the client 110 proactively requests a new content encryption key ahead of time to prevent any interruption of

decryption services. If the current content encryption key is not close to expiring and a content encryption key change request was not detected in step 308, processing proceeds back to step 306 where the client 110 begins retrieving the next segment. If the current content encryption key is within a fixed threshold of expiring or a content encryption key change request was detected in step 308, processing proceeds to step 318 where the client 110 requests a new content encryption key from the license server 106. In one embodiment, the threshold is set as a fixed amount of wall clock time before the current content encryption key will expire. In another embodiment, the threshold is set as a fixed number of segments before the current content encryption key will expire. In another embodiment, the threshold is set as a fixed percentage of the fixed period content encryption key lifespan. Once the request for a new content encryption key has been sent in step 318, processing proceeds back to step 306 where the client 110 begins retrieving the next segment.

Although the above description includes numerous specifics in the interest of a fully enabling teaching, it will be appreciated that the present invention can be realized in a variety of other manners and encompasses all implementations falling within the scope of the claims herein.

FIG. 1

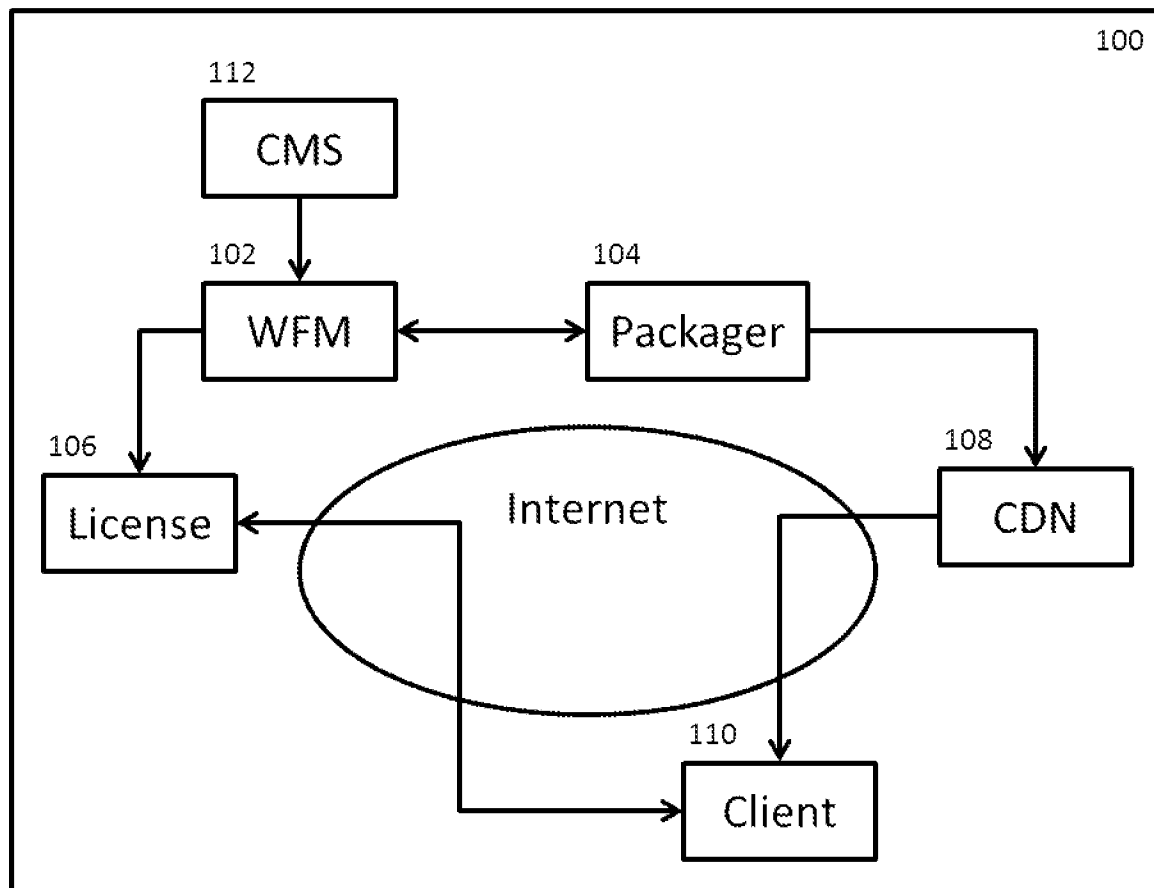


FIG. 2

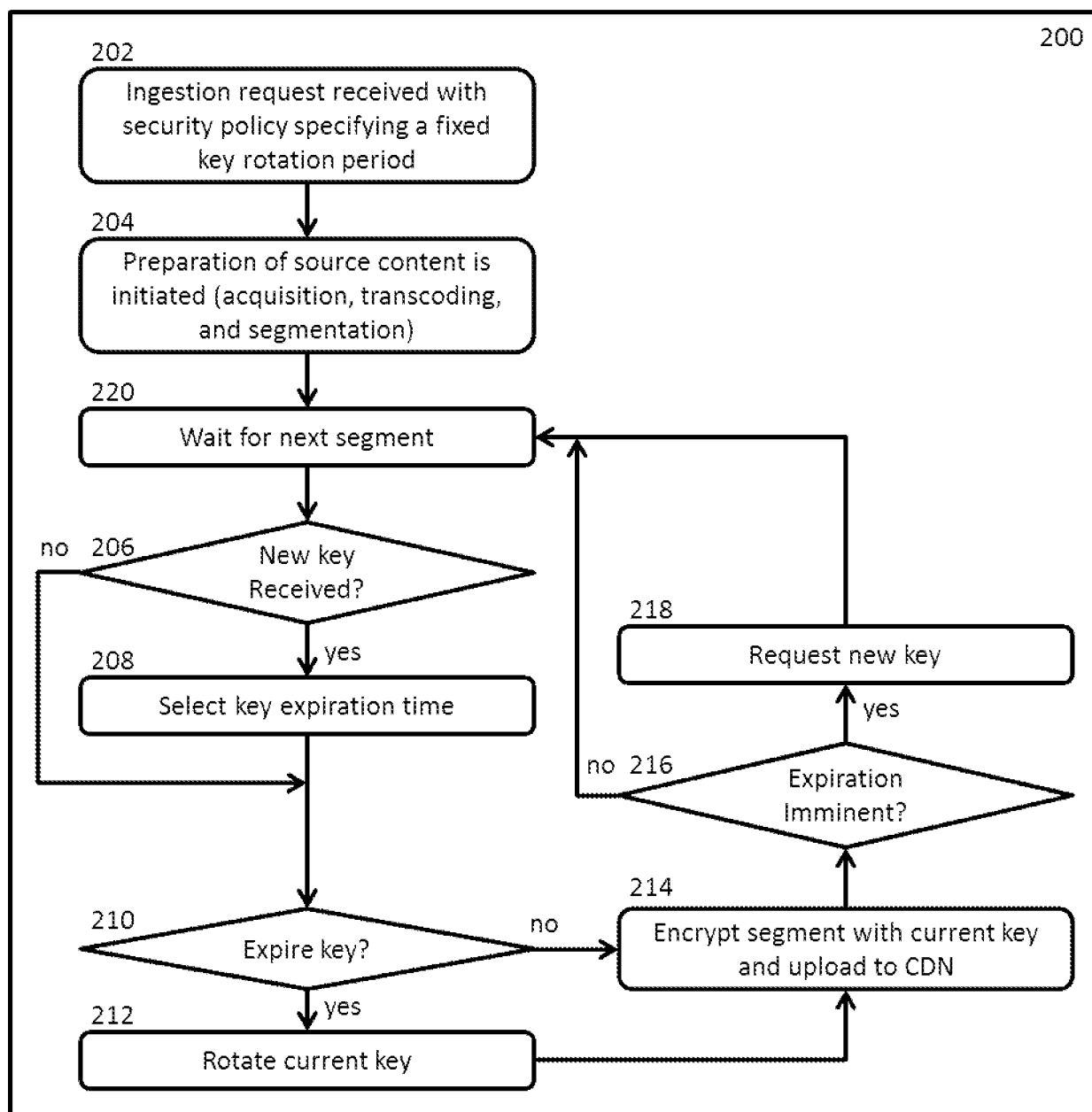
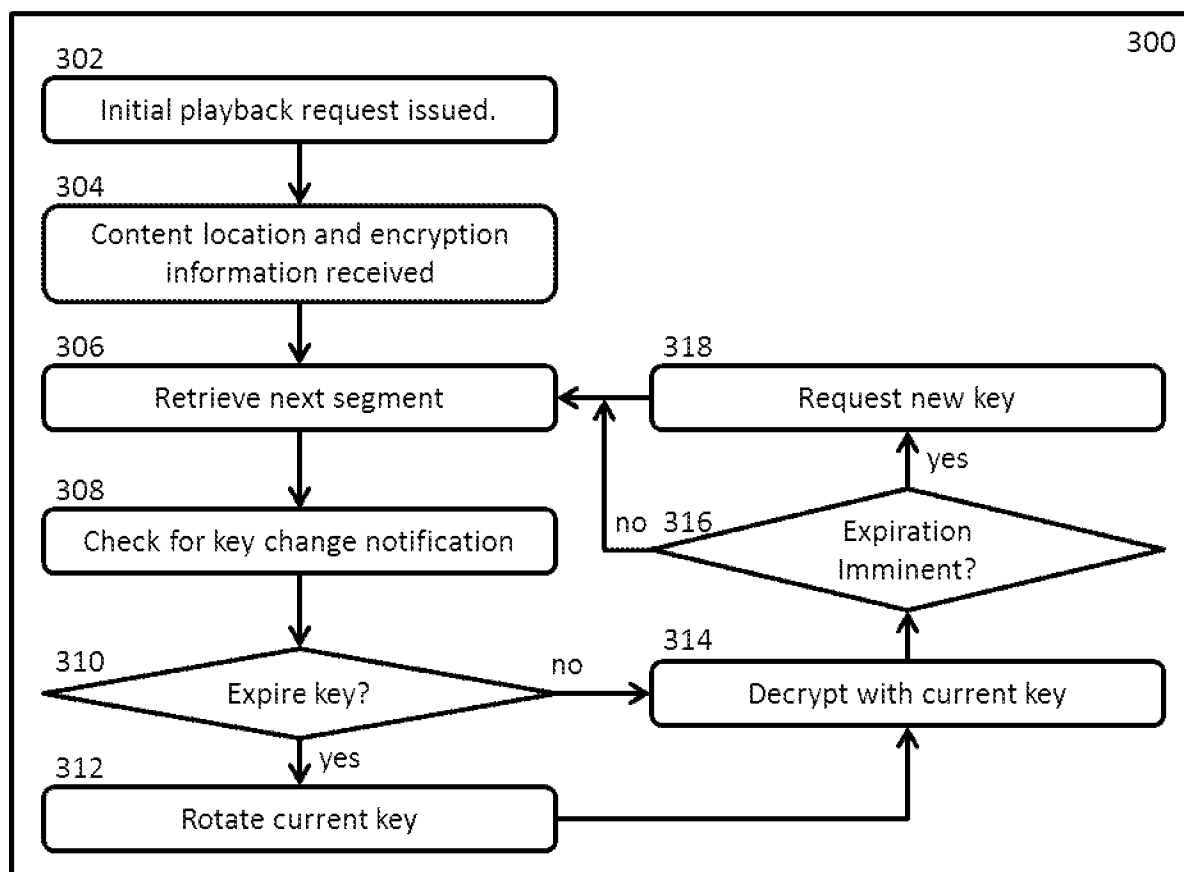


FIG. 3



Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

Inventor(s)

Inventor 1

Remove

Given Name

Middle Name

Family Name

City

State

Country i

Kevin

J.

Ma

Nashua

NH

US

Inventor 2

Remove

Given Name

Middle Name

Family Name

City

State

Country i

Robert

Hickey

Bedford

MA

US

Inventor 3

Remove

Given Name

Middle Name

Family Name

City

State

Country i

Paul

Tweedale

Andover

MA

US

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button.

Add

Title of Invention

METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

Attorney Docket Number (if applicable)

1082-018

Correspondence Address

Direct all correspondence to (select one):

☒ The address corresponding to Customer Number

☐ Firm or Individual Name

Customer Number

47654

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Entity Status

Applicant claims small entity status under 37 CFR 1.27

☒ Yes, applicant qualifies for small entity status under 37 CFR 1.27

☐ No

Warning

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/James F. Thompson/			Date (YYYY-MM-DD)	2011-06-23
First Name	James	Last Name	Thompson	Registration Number (If appropriate)	36699

This collection of information is required by 37 CFR 1.51. 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 8 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, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

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.

Electronic Patent Application Fee Transmittal

Application Number:

Filing Date:

Title of Invention:

METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

First Named Inventor/Applicant Name:

Kevin J. Ma

Filer:

James F. Thompson/Tracy Bessette

Attorney Docket Number:

1082-018

Filed as Small Entity

Provisional Filing Fees

Description

Fee Code

Quantity

Amount

**Sub-Total in
USD(\$)**

Basic Filing:

Provisional Application filing fee

2005

1

110

110

Pages:

Claims:

Miscellaneous-Filing:

Petition:

Patent-Appeals-and-Interference:

Post-Allowance-and-Post-Issuance:

Extension-of-Time:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				110

Electronic Acknowledgement Receipt

EFS ID:	10371045
Application Number:	61500316
International Application Number:	
Confirmation Number:	7568
Title of Invention:	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY
First Named Inventor/Applicant Name:	Kevin J. Ma
Customer Number:	47654
Filer:	James F. Thompson/Tracy Bessette
Filer Authorized By:	James F. Thompson
Attorney Docket Number:	1082-018
Receipt Date:	23-JUN-2011
Filing Date:	
Time Stamp:	15:15:23
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 110
RAM confirmation Number	1623
Deposit Account	503661
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

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	Specification	1082-018-patent-application.pdf	281815	no	16
			8b978a418b54bb8d53a1b09658fee92f583dc843		

Warnings:

Information:

2	Provisional Cover Sheet (SB16)	1082-018-ProvisionalSB16_CoverSheet.pdf	1062991	no	3
			c58668fdb944366c72ba5b6823615b1cb8544fe		

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	29491	no	2
			8cdda66ef286864619129e6ff959b31b29629718		

Warnings:

Information:

Total Files Size (in bytes):			1374297
------------------------------	--	--	---------

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.