US009313178B2

(12) **United States Patent**
Ma et al.

(10) **Patent No.: US 9,313,178 B2**
(45) **Date of Patent: Apr. 12, 2016**

(54) **METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY**

(71) Applicant: **Ericsson AB**, Stockholm (SE)

(72) Inventors: **Kevin J. Ma**, Nashua, NH (US); **Robert Hickey**, Bedford, MA (US); **Paul Tweedale**, Andover, MA (US)

(73) Assignee: **ERICSSON AB**, Stockholm (SE)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/266,368**

(22) Filed: **Apr. 30, 2014**

(65) **Prior Publication Data**

US 2014/0237243 A1 Aug. 21, 2014

Related U.S. Application Data

(63) Continuation of application No. 13/530,997, filed on Jun. 22, 2012, now Pat. No. 8,751,807.

(60) Provisional application No. 61/500,316, filed on Jun. 23, 2011.

(51) **Int. Cl.**

H04L 9/32	(2006.01)
H04L 29/06	(2006.01)
H04L 9/08	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 63/0428*** (2013.01); ***H04L 9/0891*** (2013.01); *H04L 2209/60* (2013.01)

(58) **Field of Classification Search**

None

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2005/0060316	A1 *	3/2005	Kamath et al.	707/9
2007/0038857	A1	2/2007	Gosnell	

FOREIGN PATENT DOCUMENTS

WO	2010108053	A1	9/2010
WO	2011020088	A1	2/2011

OTHER PUBLICATIONS

Pantos et al., HTTP Live Streaming, downloaded from http://tools.ietf.org/html/draft-pantos-http-live-streaming-06, published Mar. 31, 2011.

Microsoft Corporation, Using Silverlight DRM, Powered by PlayReady, with Windows Media DRM Content, downloaded from http://download.microsoft.com/download/7/6/D/76D540F7-A008-427C-8AFC-BE9E000D8435/Using_Silverlight_with_Windows_Media_DRM-Whitepaper_FINAL.doc, published Nov. 2008.

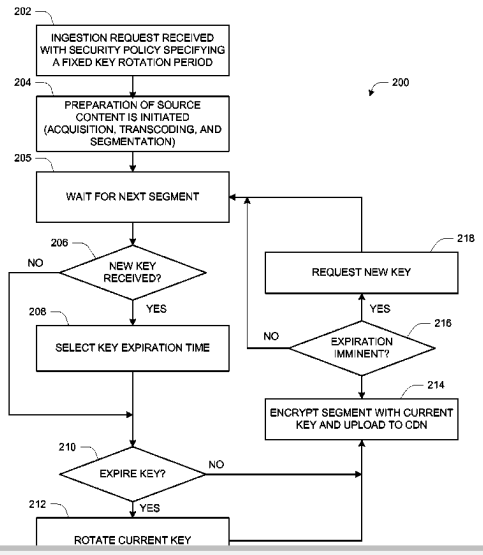
* cited by examiner

Primary Examiner — Brandon Hoffman

(57) **ABSTRACT**

A method is provided for managing key rotation (use of series of keys) and secure key distribution in over-the-top content delivery. 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.

20 Claims, 3 Drawing Sheets



Google Exhibit 1001
Google v. Ericsson

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

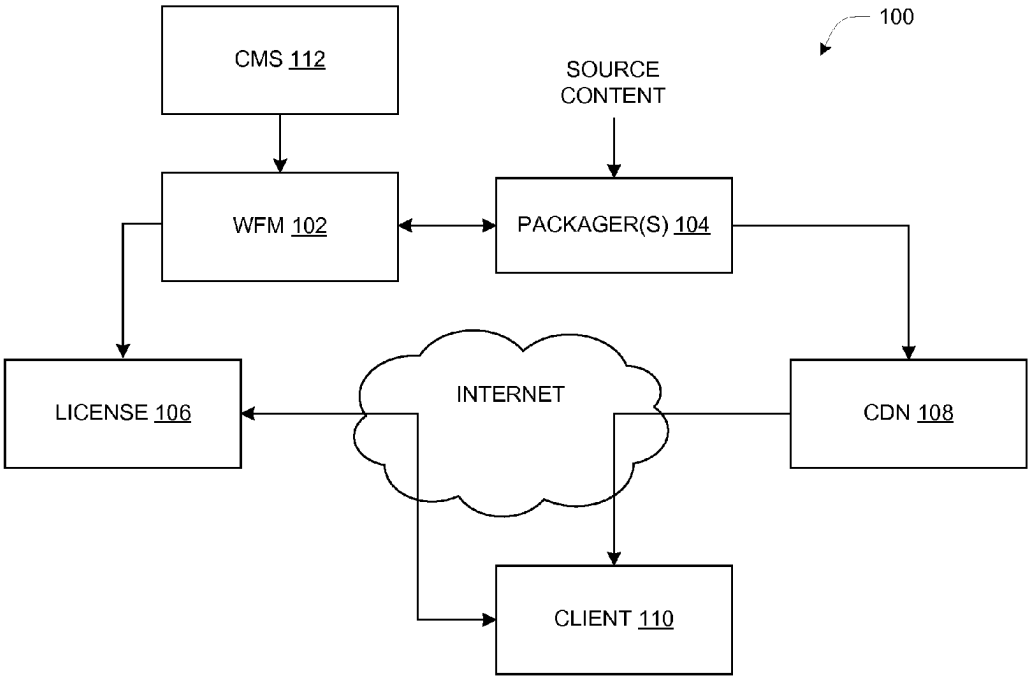


Fig. 1

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

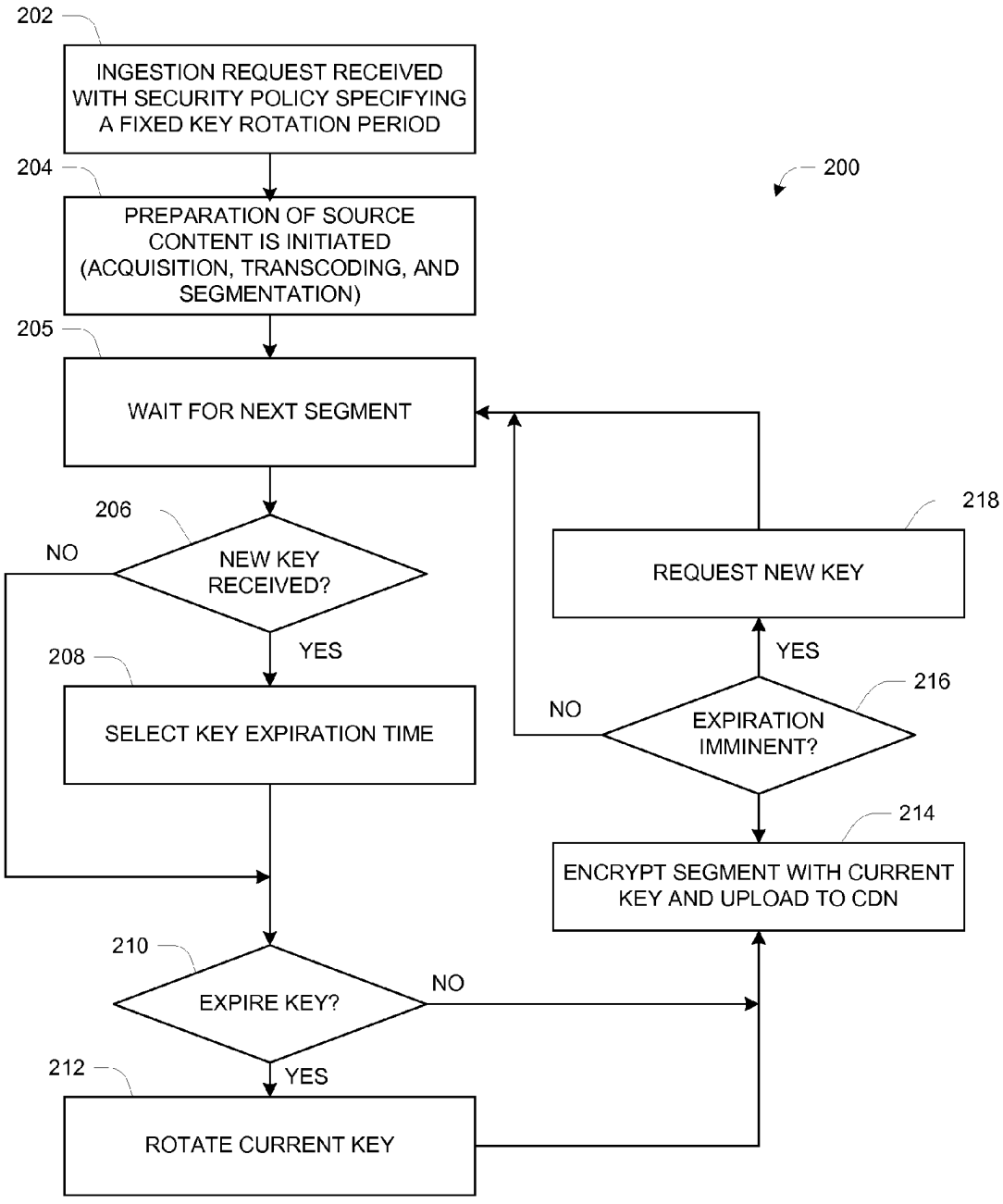


Fig. 2

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

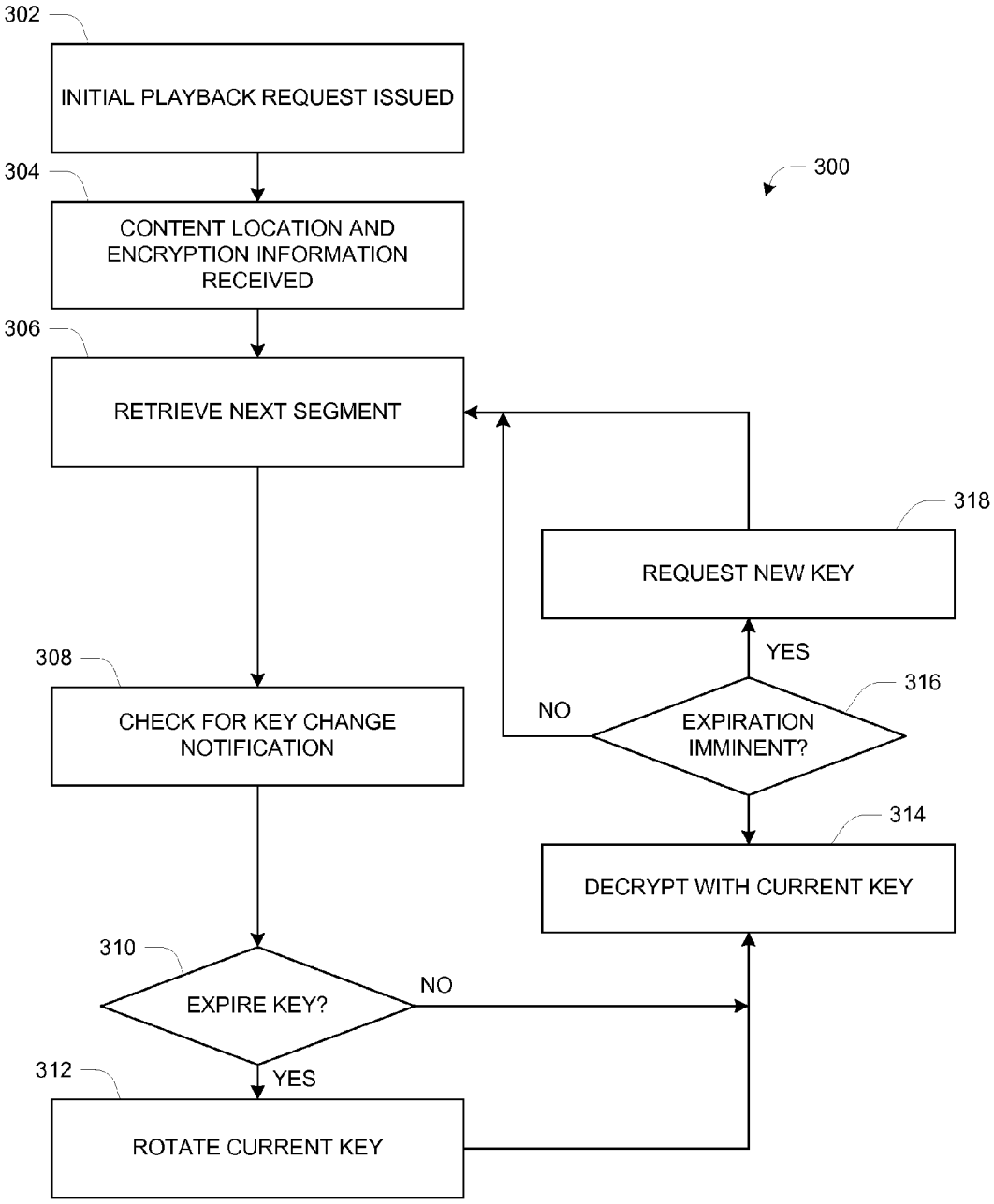


Fig. 3

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

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

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to U.S. application Ser. No. 61/500,316, filed Jun. 23, 2011, and U.S. patent application Ser. No.: 13/530,997, filed on Jun. 22, 2012 now U.S. Pat. No. 8,751,807. The content of the above applications are incorporated by reference in their entirety.

SUMMARY

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 provides only limited security.

Methods and apparatus are disclosed for managing the distribution and use of a plurality of content encryption keys for use in the protection of live streaming content. A disclosed method includes generating a series of content encryption keys and providing them serially to a packaging server for encrypting a content item, wherein each content encryption key is provided upon expiration of a period of use of a serially preceding content encryption key. The packaging server generates packaged content for delivery to client devices via a content delivery network, the packaged content including or accompanied by key expiration information usable by the client devices to identify transitions between sections of the packaged content encrypted by different ones of the content encryption keys. The method further includes providing the content encryption keys to a license server for delivery to the client devices for use in decrypting the content item. The license server is operative to establish that a requesting client device is authorized to access the content item, and further operative to securely deliver the content encryption keys to a requesting client device whose authorization to access the content item has been established. The transitioning between use of different keys is also referred to herein as key "rotation".

tion 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. Provisions are included for managing when content encryption keys expire, distributing content encryption keys to packaging engines, and distributing content encryption keys to clients.

A client device handles the secure distribution of content by a process including initiating a media playback request and receiving a playback request response, and parsing content information from the playback request response, the content information including content encryption keys, content encryption key identifiers, and content encryption key expiration times. The client device retrieves content and manifest files from a content delivery server. During ongoing retrieval of content, the client device detects content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content, issues requests to the license server ahead of a key rotation boundary to retrieve a second content encryption key to be used after a content encryption key rotation boundary is reached, and applies the second key for content decryption after the key rotation boundary is reached.

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 Mar. 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 Mar. 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

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.