United States Patent and Trademark Office
Before the Patent Trial and Appeal Board

Google LLC
(Petitioner)

v.

Ericsson AB
(Patent Owner)

Inter Partes Review

No. IPR2024-00003 | **U.S. Patent No. 9,313,178**

No. IPR2024-00004 | **U.S. Patent No. 11,122,313**

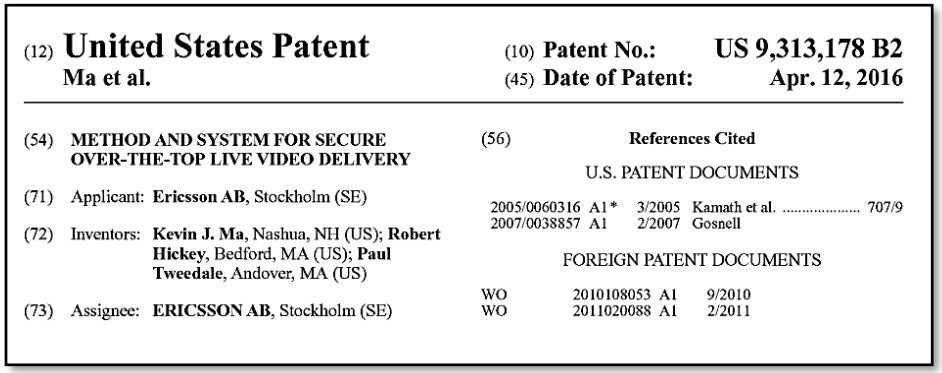
Petitioner's Demonstrative Exhibits

Google Exhibit 1050
Google v. Ericsson
IPR2025-00003

January 27, 2026

Grounds for Unpatentability

US 9,313,178 B2



(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)

(56) **References Cited**

U.S. PATENT DOCUMENTS

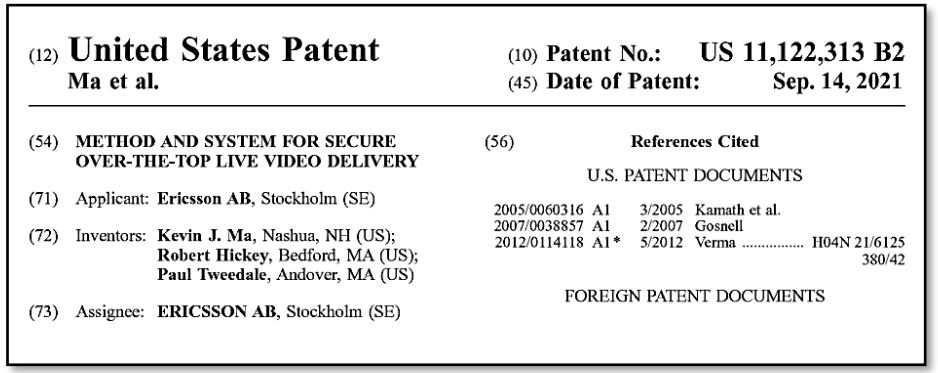
2005/0060316 A1* 3/2005 Kamath et al. 707/9
2007/0038857 A1 2/2007 Gosnell

FOREIGN PATENT DOCUMENTS

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

IPR2025-00003 EX-1001

US 11,122,313 B2



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

(10) **Patent No.: US 11,122,313 B2**
(45) **Date of Patent: Sep. 14, 2021**

(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)

(56) **References Cited**

U.S. PATENT DOCUMENTS

2005/0060316 A1 3/2005 Kamath et al.
2007/0038857 A1 2/2007 Gosnell
2012/0114118 A1* 5/2012 Verma H04N 21/6125 380/42

FOREIGN PATENT DOCUMENTS

IPR2025-00004 EX-1001

Ground and Reference(s)		Claims	Basis
1	Peterka (EX-1005)	1-6, 10, 12, 16-18, 20	§ 103
2	Peterka, Suzuki (EX-1006)	1-6, 10, 12, 16-18, 20	§ 103
3	Peterka, Bocharov (EX-1007)	1-6, 10, 12, 14, 16-18, 20	§ 103
4	Peterka, Suzuki, Bocharov	1-6, 10, 12, 14, 16-18, 20	§ 103
5	Peterka, Bocharov, Peterka308 (EX-1008), Chen (EX-1009)	7-8, 19	§ 103

IPR2025-00003 Pet., 7.

Ground and Reference(s)		Claims	Basis
1	Peterka (EX-1005)	1-4, 6-7, 11-14, 16-17	§ 103
2	Peterka, Suzuki (EX-1006)	1-4, 6-7, 11-14, 16-17	§ 103
3	Peterka, Bocharov (EX-1007)	1-4, 6-7, 9, 11-14, 16-17, 19	§ 103
4	Peterka, Suzuki, Bocharov	1-4, 6-7, 9, 11-14, 16-17, 19	§ 103
5	Peterka, Bocharov, Peterka308 (EX-1008), Chen (EX-1009)	5, 15	§ 103

IPR2025-00004 Pet., 7.

Secure Distribution of Content

IPR2025-00003 Pet., x
IPR2025-00004 Pet., ix

US 9,313,178 B2

1. A method for handling secure distribution of content comprising:

initiating a media playback request and receiving a playback request response;

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;

retrieving content and manifest files from a content delivery server;

detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content;

issuing requests to a 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

applying the second key for content decryption after the key rotation boundary is reached.

US 11,122,313 B2

1. A method for handling secure distribution of live video content comprising:

sending a request for live media playback;

receiving a live media playback request response, the live media playback request response comprising content encryption keys and content encryption key identifiers;

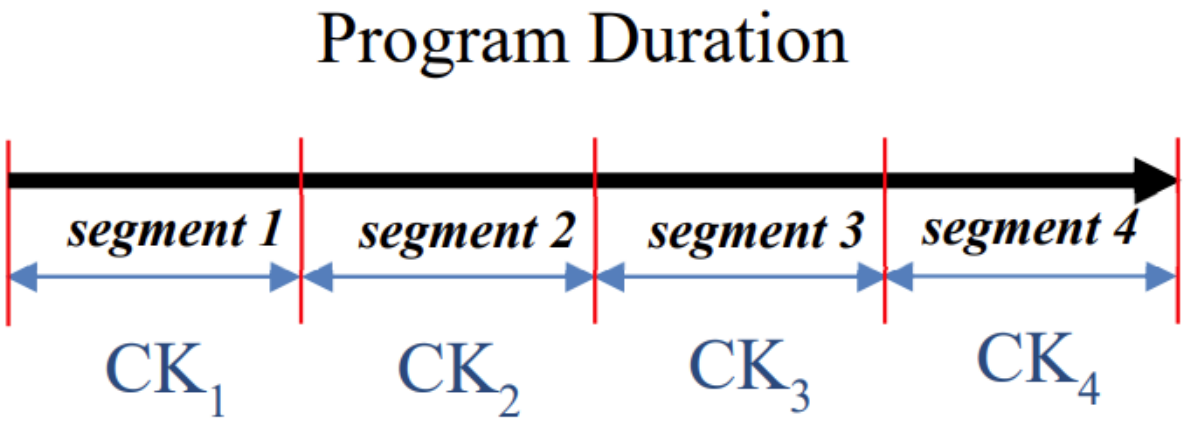
receiving encrypted live media content and manifest files from a content delivery server, wherein the encrypted live media content comprises one or more content encryption key rotation boundaries wherein each content encryption key rotation boundary is associated with a change to a different content encryption key to decrypt the received encrypted live media content;

applying a first content encryption key to the encrypted live media content before a first content encryption key rotation boundary;

prior to reaching the first key rotation boundary, obtaining a second content encryption key, the second content encryption key to be used after the first content encryption key rotation boundary is reached; and

applying the second content encryption key for content decryption after the key rotation boundary is reached.

Key Rotation



IPR2025-00003 Pet., 43

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Independent Method Claims

IPR2025-00003 Pet., x; Pet. Reply, 1
IPR2025-00004 Pet., ix; Pet. Reply, 1

US 9,313,178 B2

1. A method for handling secure distribution of content comprising:

initiating a media playback request and receiving a playback request response;

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;

retrieving content and manifest files from a content delivery server;

detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content;

issuing requests to a 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

applying the second key for content decryption after the key rotation boundary is reached.

Initiating playback

Acquiring content

Acquiring more keys during playback

US 11,122,313 B2

1. A method for handling secure distribution of live video content comprising:

sending a request for live media playback;

receiving a live media playback request response, the live media playback request response comprising content encryption keys and content encryption key identifiers;

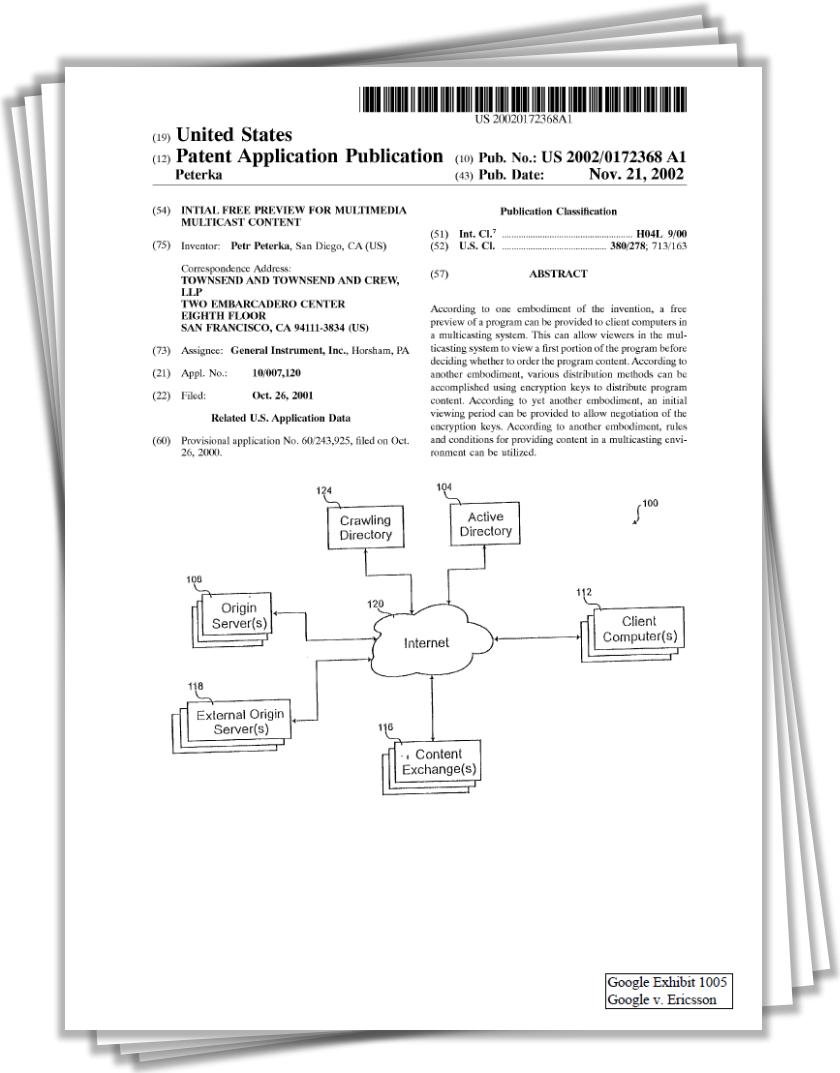
receiving encrypted live media content and manifest files from a content delivery server, wherein the encrypted live media content comprises one or more content encryption key rotation boundaries wherein each content encryption key rotation boundary is associated with a change to a different content encryption key to decrypt the received encrypted live media content;

applying a first content encryption key to the encrypted live media content before a first content encryption key rotation boundary;

prior to reaching the first key rotation boundary, obtaining a second content encryption key, the second content encryption key to be used after the first content encryption key rotation boundary is reached; and

applying the second content encryption key for content decryption after the key rotation boundary is reached.

Peterka (EX-1005)



US 20020172368A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2002/0172368 A1**

Peterka (43) **Pub. Date: Nov. 21, 2002**

(54) **INTIAL FREE PREVIEW FOR MULTIMEDIA MULTICAST CONTENT**

(75) Inventor: **Petr Peterka**, San Diego, CA (US)

Correspondence Address:
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834 (US)

(73) Assignee: **General Instrument, Inc.**, Horsham, PA

(21) Appl. No.: **10/007,120**

(22) Filed: **Oct. 26, 2001**

Related U.S. Application Data

(60) Provisional application No. 60/243,925, filed on Oct. 26, 2000.

Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**

(52) **U.S. Cl.** **380/278**; 713/163

(57) **ABSTRACT**

According to one embodiment of the invention, a free preview of a program can be provided to client computers in a multicasting system. This can allow viewers in the multicasting system to view a first portion of the program before deciding whether to order the program content. According to another embodiment, various distribution methods can be accomplished using encryption keys to distribute program content. According to yet another embodiment, an initial viewing period can be provided to allow negotiation of the encryption keys. According to another embodiment, rules and conditions for providing content in a multicasting environment can be utilized.

Google Exhibit 1005
Google v. Ericsson

Peterka (EX-1005)

[0002] This invention relates generally to the area of multicasting networks. More specifically, the invention relates to providing a preview portion of a program distributed to clients on the network.

EX-1005, [0002]

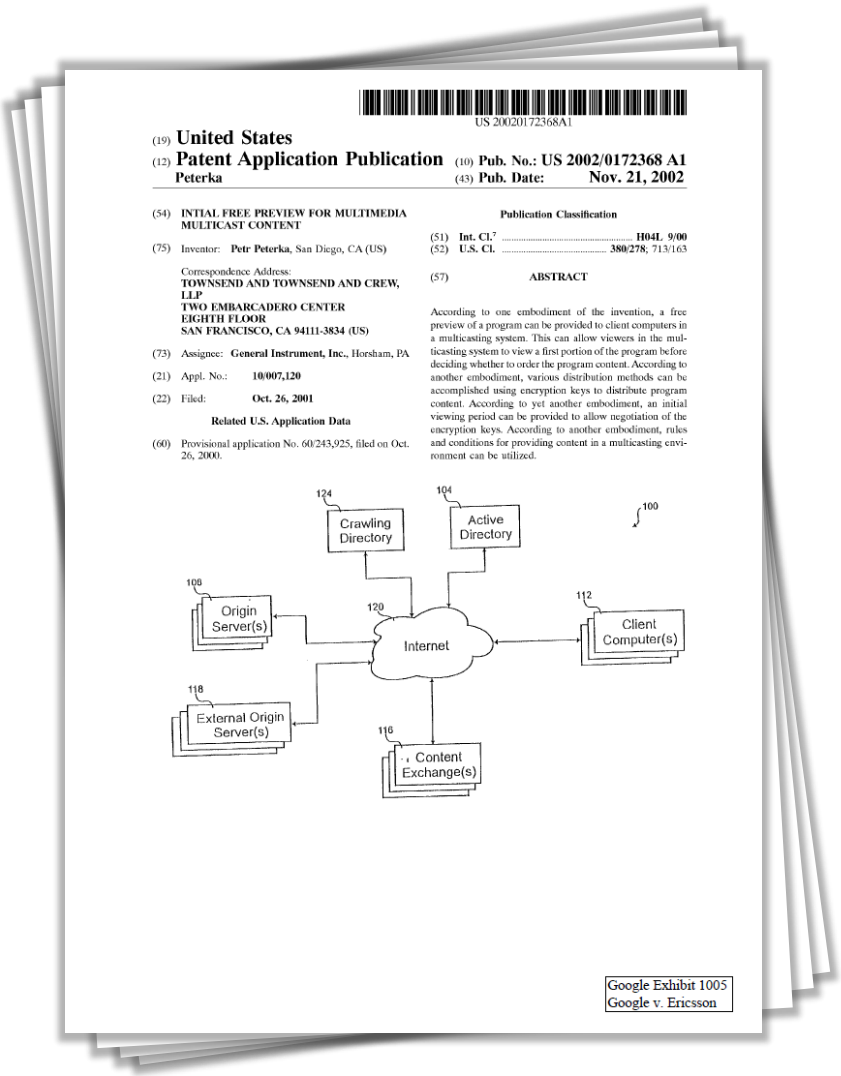
[0058] Multicast—Multicast is similar to the existing TV broadcast. It delivers the same content to one or more consumers at the same time. This is usually scheduled and can be live content.

EX-1005, [0058]

[0053] Pay-By-Time (PBT)—A purchase mechanism in which the client pays for the time duration of the content that was actually watched. The discrete time increments may have different durations for different programs or services.

EX-1005, [0053]

Content in Peterka is Segmented and Encrypted



US 20020172368A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2002/0172368 A1**

Peterka (43) **Pub. Date: Nov. 21, 2002**

(54) **INTIAL FREE PREVIEW FOR MULTIMEDIA MULTICAST CONTENT**

(75) Inventor: **Petr Peterka**, San Diego, CA (US)

Correspondence Address:
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834 (US)

(73) Assignee: **General Instrument, Inc.**, Horsham, PA

(21) Appl. No.: **10/007,120**

(22) Filed: **Oct. 26, 2001**

Related U.S. Application Data

(60) Provisional application No. 60/243,925, filed on Oct. 26, 2000.

Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**

(52) **U.S. Cl.** **380/278**; 713/163

(57) **ABSTRACT**

According to one embodiment of the invention, a free preview of a program can be provided to client computers in a multicasting system. This can allow viewers in the multicasting system to view a first portion of the program before deciding whether to order the program content. According to another embodiment, various distribution methods can be accomplished using encryption keys to distribute program content. According to yet another embodiment, an initial viewing period can be provided to allow negotiation of the encryption keys. According to another embodiment, rules and conditions for providing content in a multicasting environment can be utilized.

Google Exhibit 1005
Google v. Ericsson

Peterka (EX-1005)

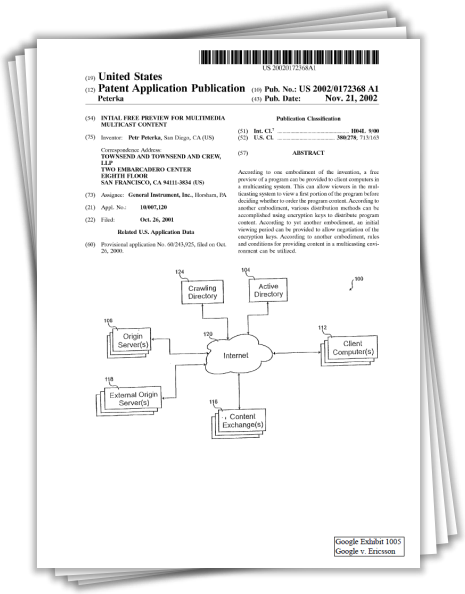
[0101] Content Key (CK): This key is used to encrypt the content itself. It should change at least as often as the PSK. It can be distributed in several ways, e.g.: (1) encrypted under the PSK for those viewers who select the pay-by-time option, (2) encrypted under the PK or UK for users who select the PPV option; or (3) encrypted under a SK for those who are subscribers to the service.

EX-1005, [0101]

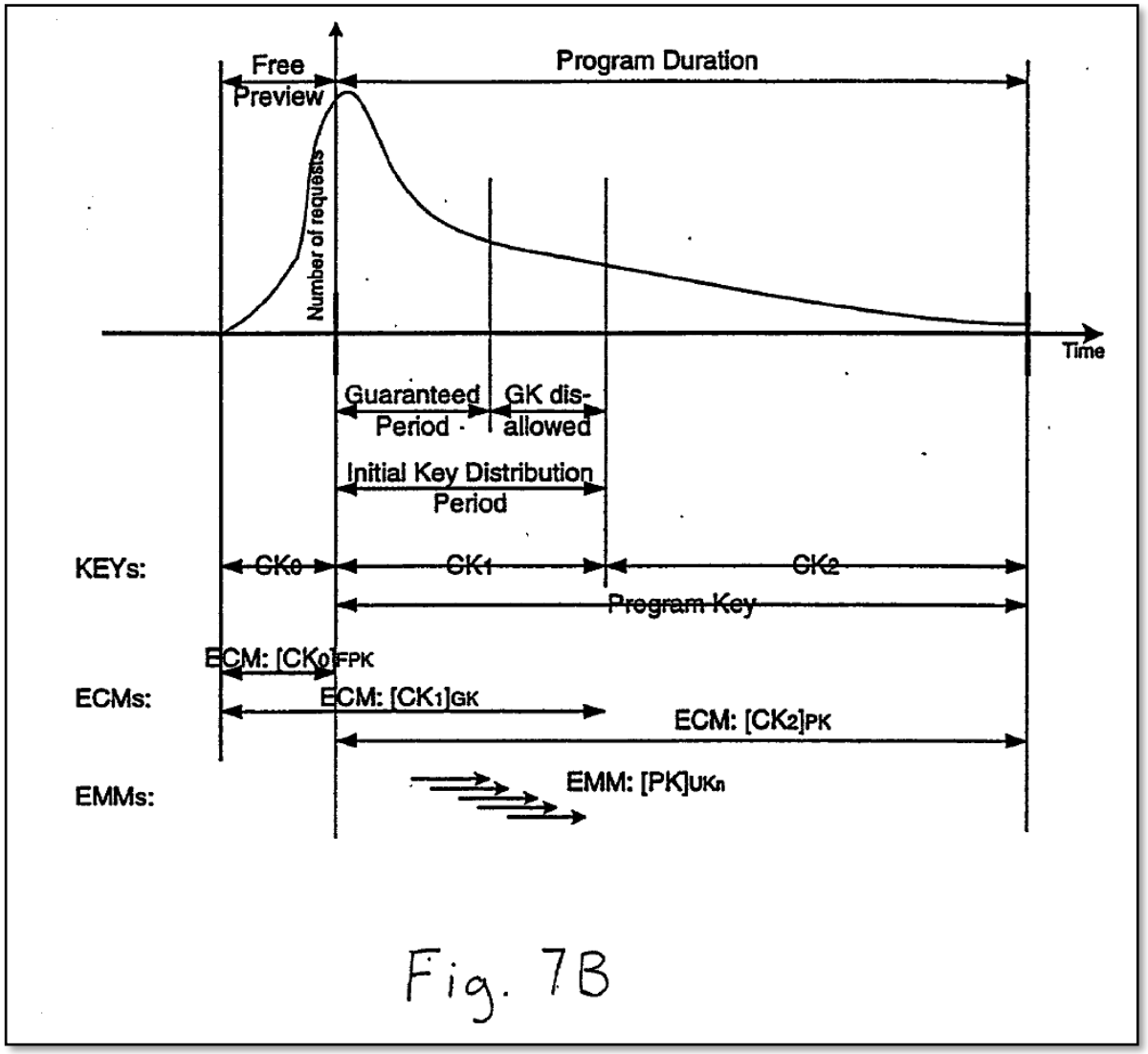
[0099] Program Segment Key (PSK): This key is used to divide a single program event or an entire service into purchasable segments. The PSKs are delivered either using unicast or multicast distribution. Clients using the pay-by-time purchase option will get the PSK using the key request message exchange. Clients using the PPV purchase option

EX-1005, [0099]

Content in Peterka is Segmented and Encrypted

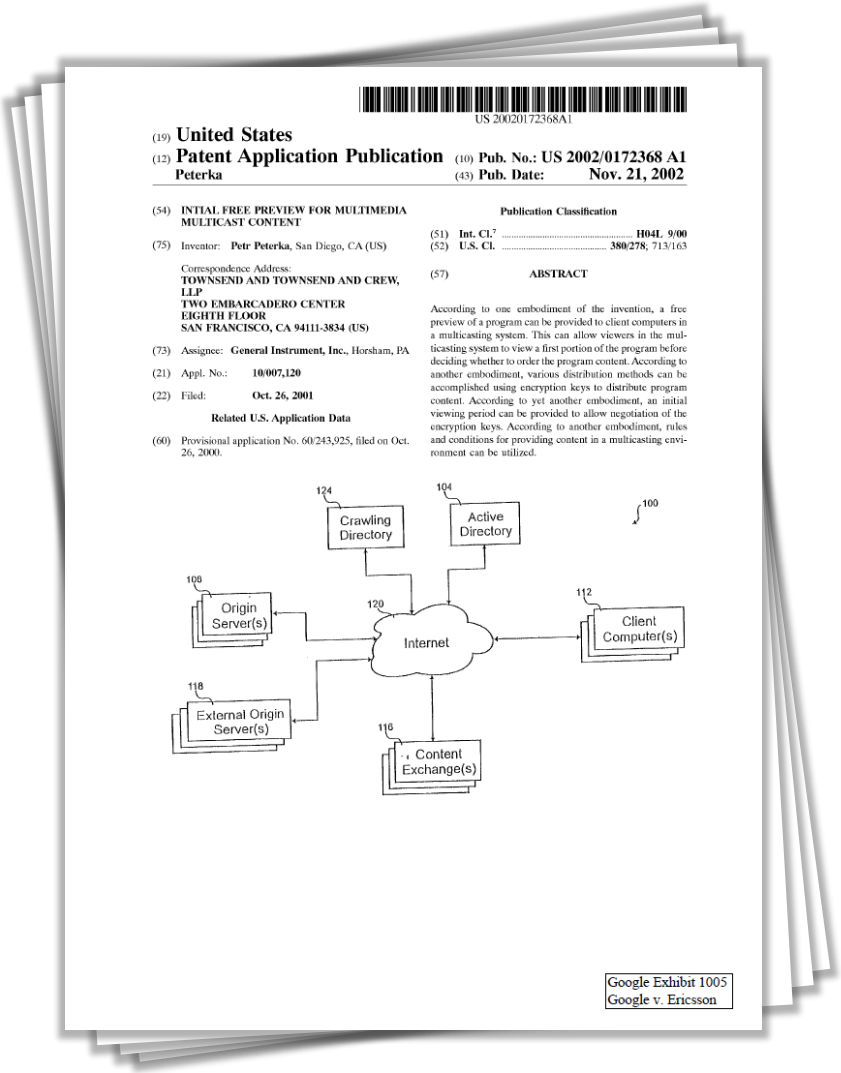


Peterka (EX-1005)



EX-1005, FIG. 7B

Content Delivery in Peterka



US 20020172368A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2002/0172368 A1**

Peterka (43) **Pub. Date: Nov. 21, 2002**

(54) **INTIAL FREE PREVIEW FOR MULTIMEDIA MULTICAST CONTENT**

(75) Inventor: **Petr Peterka**, San Diego, CA (US)

Correspondence Address:
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834 (US)

(73) Assignee: **General Instrument, Inc.**, Horsham, PA

(21) Appl. No.: **10/007,120**

(22) Filed: **Oct. 26, 2001**

Related U.S. Application Data

(60) Provisional application No. 60/243,925, filed on Oct. 26, 2000.

Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**

(52) **U.S. Cl.** **380/278**; 713/163

(57) **ABSTRACT**

According to one embodiment of the invention, a free preview of a program can be provided to client computers in a multicasting system. This can allow viewers in the multicasting system to view a first portion of the program before deciding whether to order the program content. According to another embodiment, various distribution methods can be accomplished using encryption keys to distribute program content. According to yet another embodiment, an initial viewing period can be provided to allow negotiation of the encryption keys. According to another embodiment, rules and conditions for providing content in a multicasting environment can be utilized.

Google Exhibit 1005
Google v. Ericsson

Peterka (EX-1005)

[0082] When the client negotiates encryption keys with the caching server, it will start receiving the multicast content. The client will monitor the expiration time for each pay period and request a new set of keys from the caching server. If the viewer stops watching or moves to another service the client will not request new keys or it will actively notify the caching server that it wants to leave the current multicast session. The caching server will record the time when each client joins and leaves the multicast for billing purposes.

EX-1005, [0082]

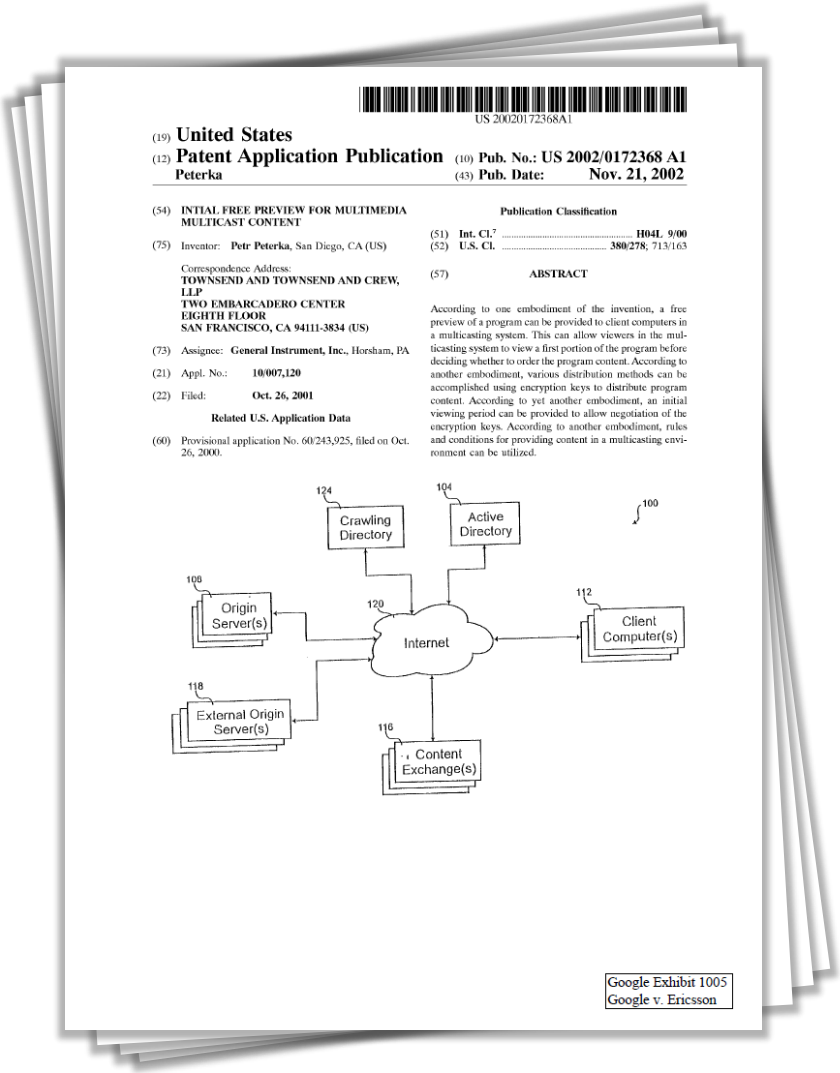
[0043] The network of **FIG. 1** can be implemented in a variety of ways. For example, according to one embodiment, we can assume the use of User Datagram Protocol (UDP) which can carry "Real-Time Transport Protocol"/"Real-Time Control Protocol" (RTP/RTCP) "Internet Group Man-

EX-1005, [0043]

new content key should be used. **FIG. 14** illustrates a flow chart **1400** for implementing a signaling method. **FIG. 14** refers to use of an RTP packet for distributing program content; however, it could equally apply to other protocols utilized in distributing content. Thus, it merely exemplifies

EX-1005, [0117]

Key Change Signals in Peterka's Content Packets



US 20020172368A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2002/0172368 A1**

Peterka (43) **Pub. Date: Nov. 21, 2002**

(54) **INTIAL FREE PREVIEW FOR MULTIMEDIA MULTICAST CONTENT**

(75) Inventor: **Petr Peterka**, San Diego, CA (US)

Correspondence Address:
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834 (US)

(73) Assignee: **General Instrument, Inc.**, Horsham, PA

(21) Appl. No.: **10/007,120**

(22) Filed: **Oct. 26, 2001**

Related U.S. Application Data

(60) Provisional application No. 60/243,925, filed on Oct. 26, 2000.

Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**

(52) **U.S. Cl.** **380/278**; 713/163

(57) **ABSTRACT**

According to one embodiment of the invention, a free preview of a program can be provided to client computers in a multicasting system. This can allow viewers in the multicasting system to view a first portion of the program before deciding whether to order the program content. According to another embodiment, various distribution methods can be accomplished using encryption keys to distribute program content. According to yet another embodiment, an initial viewing period can be provided to allow negotiation of the encryption keys. According to another embodiment, rules and conditions for providing content in a multicasting environment can be utilized.

Google Exhibit 1005
Google v. Ericsson

Peterka (EX-1005)

[0116] As part of the key distribution system, the content key is utilized for decrypting the program content throughout the course of the distribution of the program content. Thus, when a new content key is implemented, the implementation will be signaled to the clients so that the clients can begin utilizing the new content key with which they have been provided. Oftentimes the clients are provided with an encrypted version of the content key which is decrypted for example, with a program segment key. Similarly, that program segment key might be encrypted with a service key or even a unique key.

EX-1005, [0116]

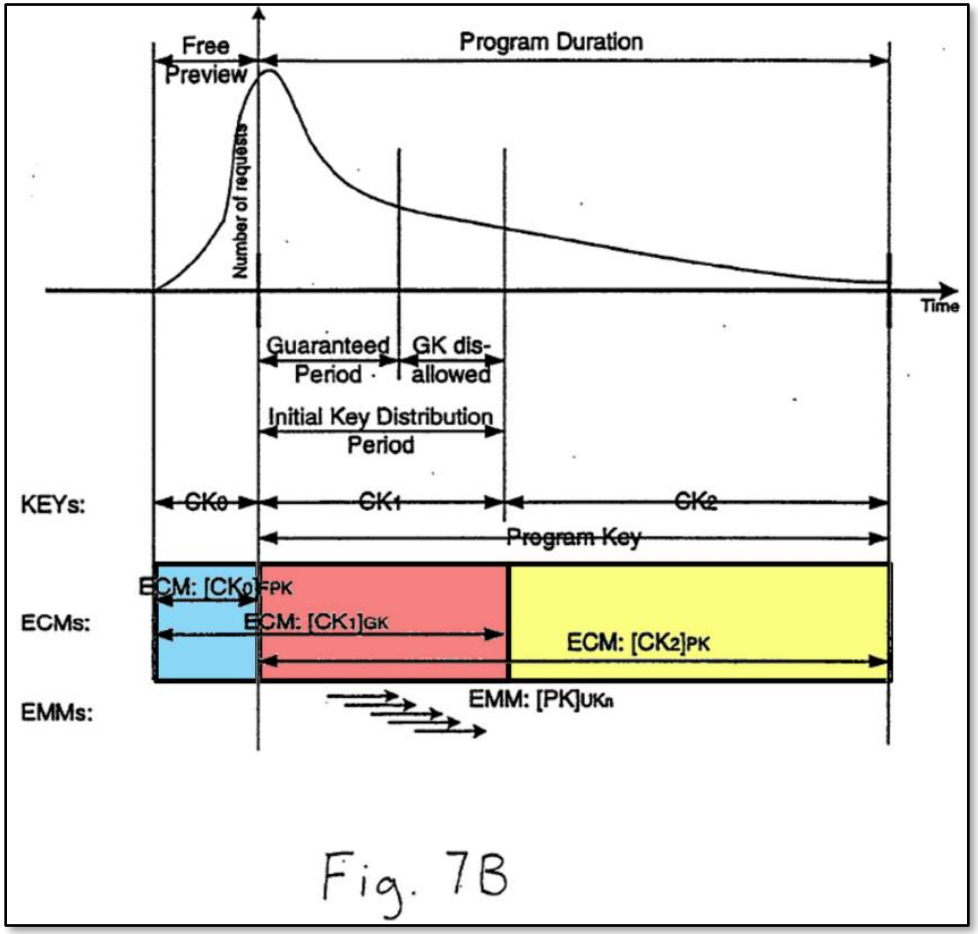
[0117] A signaling method can be used to indicate the implementation of a new key. For example, a predetermined bit can be used to indicate if an old or current content key should be used as opposed to a new content key which has recently been distributed to the client. Thus, a client can check the predetermined bit in a packet and determine the proper content key to use. As one example, if a single bit is used, a "1" could be used to indicate the current content key already in use, while a "0" could be used to indicate that the new content key should be used. **FIG. 14** illustrates a flow chart **1400** for implementing a signaling method. **FIG. 14** refers to use of an RTP packet for distributing program content; however, it could equally apply to other protocols utilized in distributing content. Thus, it merely exemplifies

EX-1005, [0117]

Key Delivery in Peterka

[0121] In multicasting program content such as audio and visual material, entitlement management messages and entitlement control messages can be sent from a server to client computer. One embodiment of the invention provides a format for such messages. Under this format, a sequence number or a time stamp to protect against replay attacks is provided. Furthermore, in another field of the EMM and ECM messages, a keyed message authentication code (MAC), or a public key digital signature for authentication is provided. Note that neither the keyed-hashing for message authentication (HMAC) nor the signature can be verified until a client performs the key request exchange. Yet another field would include the type of key included in the message, such as a content key, a group key, a program segment key, a service key, etc. Furthermore, a field would be provided for the type of key used to encrypt the key in the message. Thus, a unique key could be indicated for a message transmitting a service key, for example. Another field can be provided for the time remaining in the lifetime of the key. Furthermore, a key parity bit matching the parity bit in the RTP packet can be provided. Also, a user identification, which is often needed when multiple EMMs are delivered in a single multicast message, can be provided. Each field of the data structure applies to each of these fields. Thus, they can be arranged in any order such that the data structure includes one or more of these fields.

EX-1005, [0121]

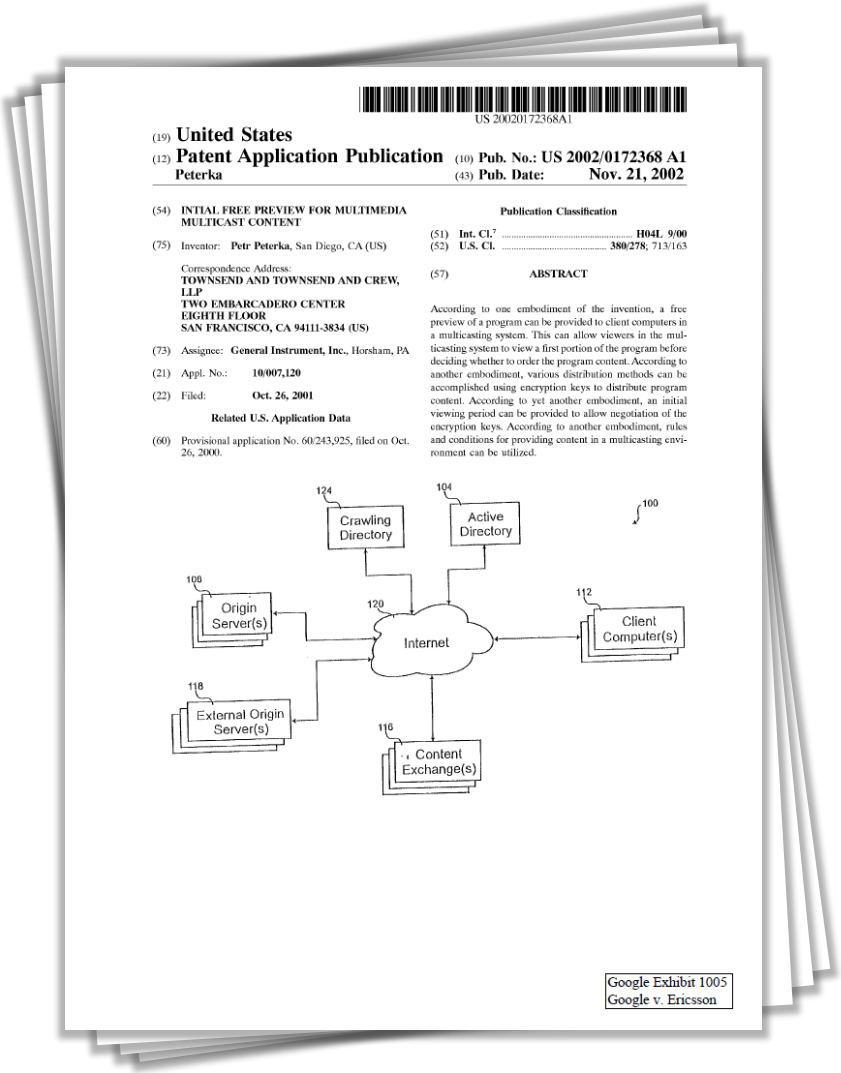


EX-1005, FIG. 7B (annotated)

[0021] **FIGS. 7A and 7B** are graphs showing exemplary distribution of cryptographic keys during portions of a program.

EX-1005, [0021]

Key Delivery in Peterka



US 20020172368A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2002/0172368 A1**

Peterka (43) **Pub. Date: Nov. 21, 2002**

(54) **INTIAL FREE PREVIEW FOR MULTIMEDIA MULTICAST CONTENT**

(75) Inventor: **Petr Peterka**, San Diego, CA (US)

Correspondence Address:
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834 (US)

(73) Assignee: **General Instrument, Inc.**, Horsham, PA

(21) Appl. No.: **10/007,120**

(22) Filed: **Oct. 26, 2001**

Related U.S. Application Data

(60) Provisional application No. 60/243,925, filed on Oct. 26, 2000.

Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**

(52) **U.S. Cl.** **380/278**; 713/163

(57) **ABSTRACT**

According to one embodiment of the invention, a free preview of a program can be provided to client computers in a multicasting system. This can allow viewers in the multicasting system to view a first portion of the program before deciding whether to order the program content. According to another embodiment, various distribution methods can be accomplished using encryption keys to distribute program content. According to yet another embodiment, an initial viewing period can be provided to allow negotiation of the encryption keys. According to another embodiment, rules and conditions for providing content in a multicasting environment can be utilized.

Google Exhibit 1005
Google v. Ericsson

Peterka (EX-1005)

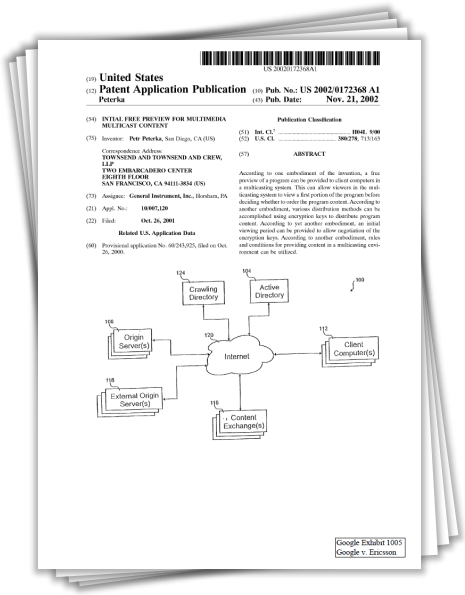
[0104] Table 1 shows various embodiments of the invention for distributing the various keys to clients. As shown in Table 1, only keys distributed to individual clients (shown as keys encrypted under the UK) using the UK are delivered in a unicast fashion. These unit-addressed messages fulfill the Entitlement Management Message (EMM) function. Alternatively, for improved efficiency multiple EMMs encrypted with different UKs may be combined into a single multicast message. Other keys can be encrypted only once for a group of authorized clients and multicast because they can be decrypted only by those clients who possess the higher level keys. These group-addressed multicast messages play the role of Entitlement Control Message (ECM) messages.

TABLE 1

	PPV	Subscription	Pay-by-time
UK			
SR		(SK)UK	
PK	(PK)UK	(PK)SK	
PSK	(PSK)GK or (PSK)PK or (PSK)FPK	Optional: (PSK)SK or (PSK)PK	(PSK)UK
CK	(CK)PK or (CK)FPK or (CK)GK or (CK)UK	(CK)PSK or (CK)SK or (CK)PK	(CK)PSK (CK)FPK (CK)GK
GK	(GK)UK or provisioned		(GK)UK or provisioned
FPK	(FPK)UK or provisioned		(FPK)UK or provisioned

EX-1005, [0104], Table 1

Large Server Load on Segment Boundaries



US 20020172368A1

(19) United States
(12) Patent Application Publication
Peterka

(10) Pub. No.: US 2002/0172368 A1
(43) Pub. Date: Nov. 21, 2002

(54) INITIAL FREE PREVIEW FOR MULTIMEDIA MULTICAST CONTENT

(75) Inventor: Petr Peterka, San Diego, CA (US)

Correspondence Address:
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834 (US)

(73) Assignee: General Instrument, Inc., Horsham, PA

(21) Appl. No.: 10/007,120

(22) Filed: Oct. 26, 2001

Related U.S. Application Data

(60) Provisional application No. 60/243,025, filed on Oct. 26, 2000.

Publication Classification

(51) Int. Cl.
(52) U.S. Cl.

(57) ABSTRACT

Crawling Directory
Active Directory
Origin Server(s)
Internet
Client Computer(s)
External Origin Server(s)
Content Exchange(s)

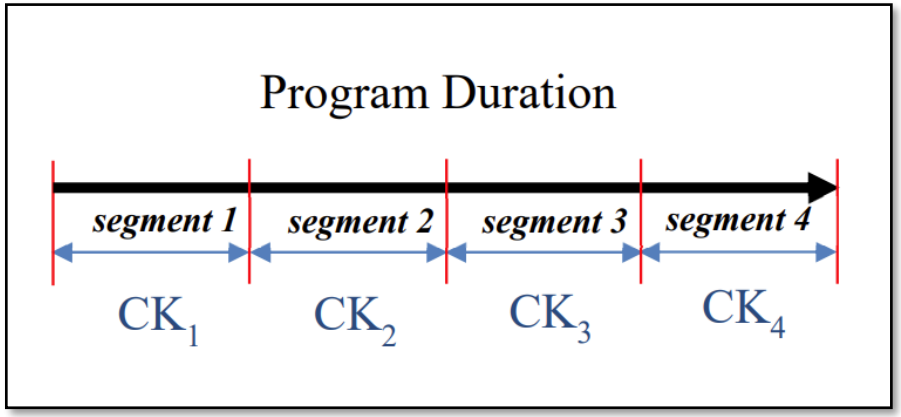
Google Exhibit 1005
Google v. Ericsson

Peterka (EX-1005)

Pay-By-Time

[0080] For a quasi-PBT approach, a caching server may divide the content into pay segments and assign segment keys to them. All consumer computers would negotiate a key for each segment in order to keep track of how may segments they watched. This generates a large load on the caching server on the segment boundaries. This can be mitigated with a key management approach where each rabbit is given keys to the current as well as the next segment. This will give the caching server enough time to distribute the next segment keys during the current segment.

EX-1005, [0080]



IPR2025-00003 Pet., 43

"Current" and "Next" Key Management Approach

Wechselberger:

[0106], FIG. 8. To mitigate excessive server loads at media segment boundaries in such an embodiment—that is, an embodiment (as Peterka teaches) where clients actively request and negotiate keys for segments—the POSITA would have understood Peterka to teach distributing ***multiple*** keys (*e.g.*, multiple ECMs) to a client (*e.g.*, for the current ***and*** next media segment) in response to such a request.

IPR2025-00003 EX-1003, ¶52; IPR2025-00004 EX-1003, ¶51

CK_2 is used (yellow). *Id.* Providing a client with a content key for the next segment in response to a client's request to begin playback during the current segment as taught in Peterka was desirable (and indeed obvious), since this would predictably reduce the volume of requests that the server needed to respond to ahead of the upcoming segment boundary and help reduce disruptions in content distribution due to latency caused by any network congestion that arises from many clients using the network to transmit requests. Additionally, the POSITA would have understood it to be beneficial for the client to have both the current and the next content keys for scenarios in which servers become temporarily unable to distribute the content key for the next segment, which would disrupt the client's ability to continue decrypting after the next segment boundary.

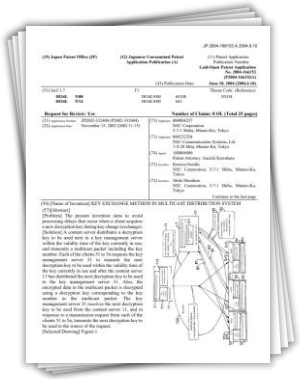
IPR2025-00003 EX-1003, ¶79; IPR2025-00004 EX-1003, ¶78

conventional to transmit multiple keys (*e.g.*, current and next) in a single message in response to a client request for keys. For documentary evidence corroborating this knowledge of a POSITA, see Suzuki, [0076]-[0077], FIGs. 5-6.

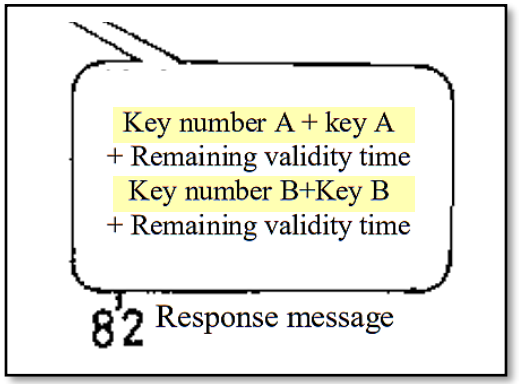
IPR2025-00003 EX-1003, ¶81; IPR2025-00004 EX-1003, ¶80

“Current” and “Next” Key Management Approach

IPR2025-00003 Pet., 22; Pet. Reply, 18-19
IPR2025-00004 Pet., 21-22; Pet. Reply, 19



Suzuki (EX-1006)



EX-1006, FIG. 5 (excerpted)

[0072]
FIG. 5 is a diagram specifically showing the information in each key information management table and the contents of each packet/request/message. In FIG. 5, the key currently in use is indicated as key A, the next key to be used is indicated as key B, and their key numbers are indicated as "key number A" and "key number B." In this example, the encryption key and the decryption key are assumed to be the same key (for example, key A is both the encryption key and the decryption key). Further, the first setting value is indicated by X, and the second setting value is indicated by Y.

EX-1006, [0072]

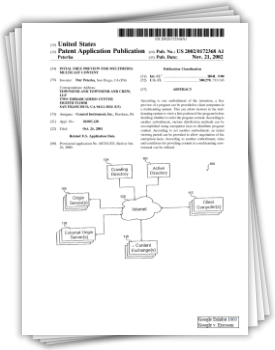
[0076]
When the remaining validity time of key A reaches Y (second setting value), the client 51 transmits a key information request 81 to the key management server 31, requesting key information on the next key to be used.
[0077]
In response to this key information request 81, the key management server 31 transmits a response message 82 having key information relating to the key currently in use (key A) and the next key to be used (key B). As a result, the client 51 has key information relating to the keys A and B, as shown in FIG. 5.

EX-1006, [0076]-[0077]

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

"Current" and "Next" Key Management Approach

IPR2025-00003 Pet., 20
IPR2025-00004 Pet., 19-20



Peterka (EX-1005)

keys to them. All consumer computers would negotiate a key for each segment in order to keep track of how may segments they watched. This generates a large load on the caching server on the segment boundaries. This can be mitigated with a key management approach where each rabbit is given keys to the current as well as the next segment. This will give the caching server enough time to distribute the next segment keys during the current segment.

EX-1005, [0080]

Petitions:

As discussed *supra* § VIII.A, Peterka teaches distributing multiple keys (e.g., current and next) to a client when it negotiates access to media content. Peterka, [0080], [0130], FIG. 7B. Specifically, Peterka describes "a key management approach where each [client] is given keys to the current as well as the next segment." *Id.*, [0080]. Peterka teaches that such an approach can "mitigate[]" "large load[s]" on a server that occur at "the segment boundaries" of a media stream—e.g., in a pull model where users pay for time increments corresponding to media segments and a server is likely to receive key requests from many clients at each media segment boundary. *Id.*; *see also id.*, [0053]; Wechselberger, ¶77.

IPR2025-00003 Pet., 20; *see* IPR2025-00004 Pet., 19-20

"Current" and "Next" Key Management Approach

Petitions:

> Peterka FIG. 7B (annotated below)—"showing exemplary distribution of cryptographic keys during portions of a program" (Peterka, [0021])—confirms that this key management approach was applicable/desirable in any distribution scheme in which key requests from many clients are expected at segment boundaries.

IPR2025-00003 Pet., 20 (citing EX-1003, ¶¶78-79);
IPR2025-00004 Pet., 20 (citing EX-1003, ¶¶77-78)

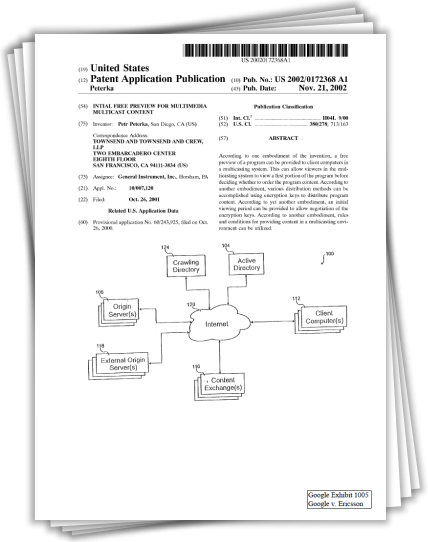
Wechselberger:

> CK_2 is used (yellow). *Id.* Providing a client with a content key for the next segment in response to a client's request to begin playback during the current segment as taught in Peterka was desirable (and indeed obvious), since this would predictably reduce the volume of requests that the server needed to respond to ahead of the upcoming segment boundary and help reduce disruptions in content distribution due to latency caused by any network congestion that arises from many clients using the network to transmit requests. Additionally, the POSITA would have understood it to be beneficial for the client to have both the current and the next content keys for scenarios in which servers become temporarily unable to distribute the content key for the next segment, which would disrupt the client's ability to continue decrypting after the next segment boundary.

IPR2025-00003 EX-1003, ¶79; IPR2025-00004 EX-1003, ¶78

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

"Current" and "Next" Key Management Approach



(19) United States
(12) Patent Application Publication
Peterka
(10) Pub. No.: US 2002/0172368 A1
(43) Pub. Date: Nov. 21, 2002

(54) INITIAL FREE PREVIEW FOR MULTIMEDIA MULTICAST CONTENT

(75) Inventor: Petr Peterka, San Diego, CA (US)

Correspondence Address:
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834 (US)

(73) Assignee: General Instrument, Inc., Horsham, PA

(21) Appl. No.: 10/007,120

(22) Filed: Oct. 26, 2001

Related U.S. Application Data

(60) Provisional application No. 60/243,053, filed on Oct. 26, 2000.

Publication Classification

(51) Int. Cl.[7] H04L 9/00
(52) U.S. Cl. 380/278; 713/163

(57) ABSTRACT

According to one embodiment of the inventions, a free preview of a program can be provided to client computers in a multicasting system. This can allow viewers in the multicasting system to view a first portion of the program before deciding whether to order the program content. According to another embodiment, various distribution methods can be accomplished using encryption keys to distribute program content. According to yet another embodiment, an initial viewing period can be provided to allow negotiation of the encryption keys. According to another embodiment, rules and conditions for providing content in a multicasting environment can be utilized.

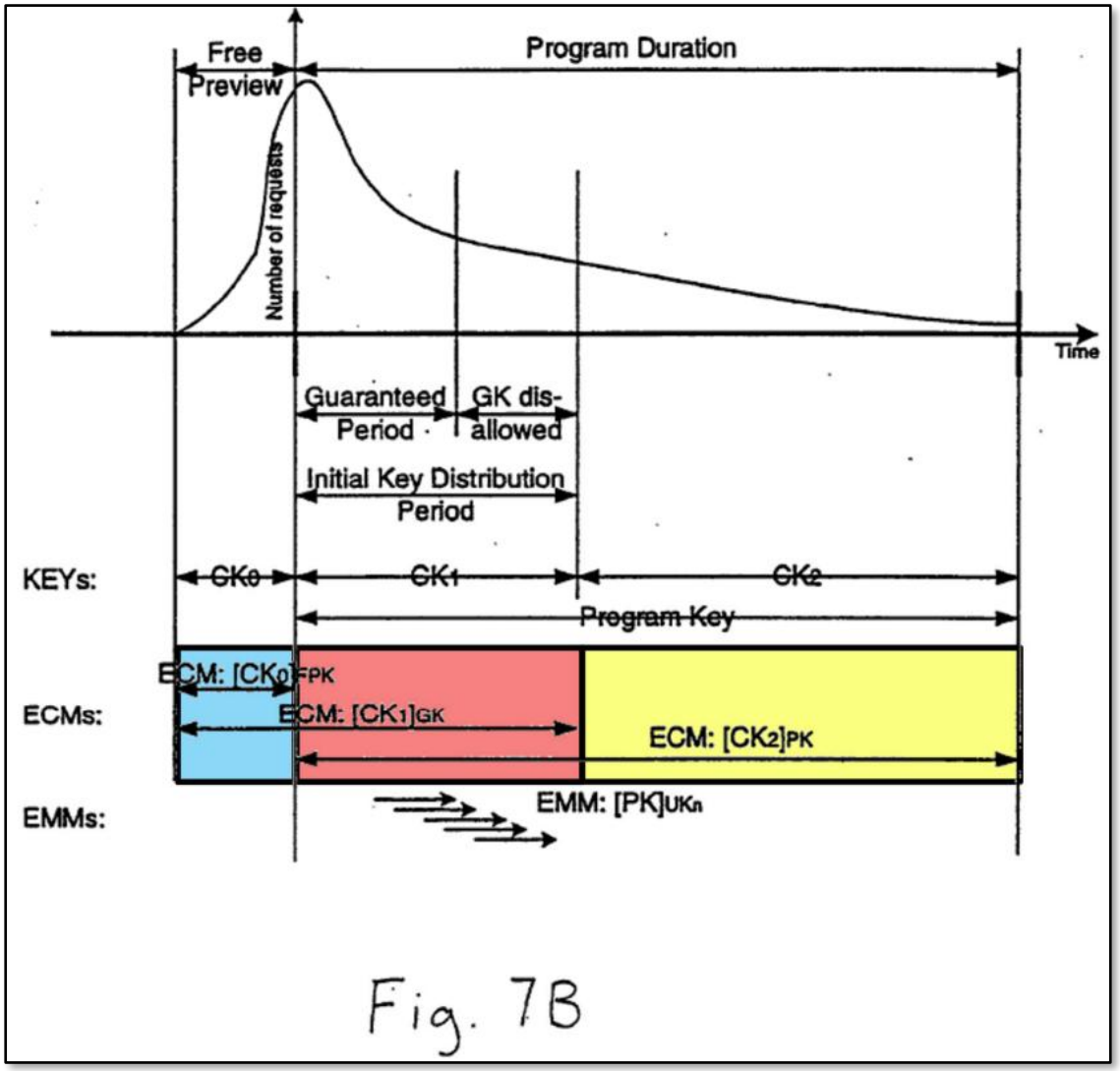
Crawling Directory
Active Directory
Origin Server(s)
Internet
Client Computer(s)
External Origin Server(s)
Content Exchange(s)

Google Exhibit 1005
Google v. Ericsson

Peterka (EX-1005)

mitigated with a key management approach where each rabbit is given keys to the current as well as the next segment. This will give the caching server enough time to distribute the next segment keys during the current segment.

EX-1005, [0080]



EX-1005, FIG. 7B (annotated)

"Current" and "Next" Key Management Approach

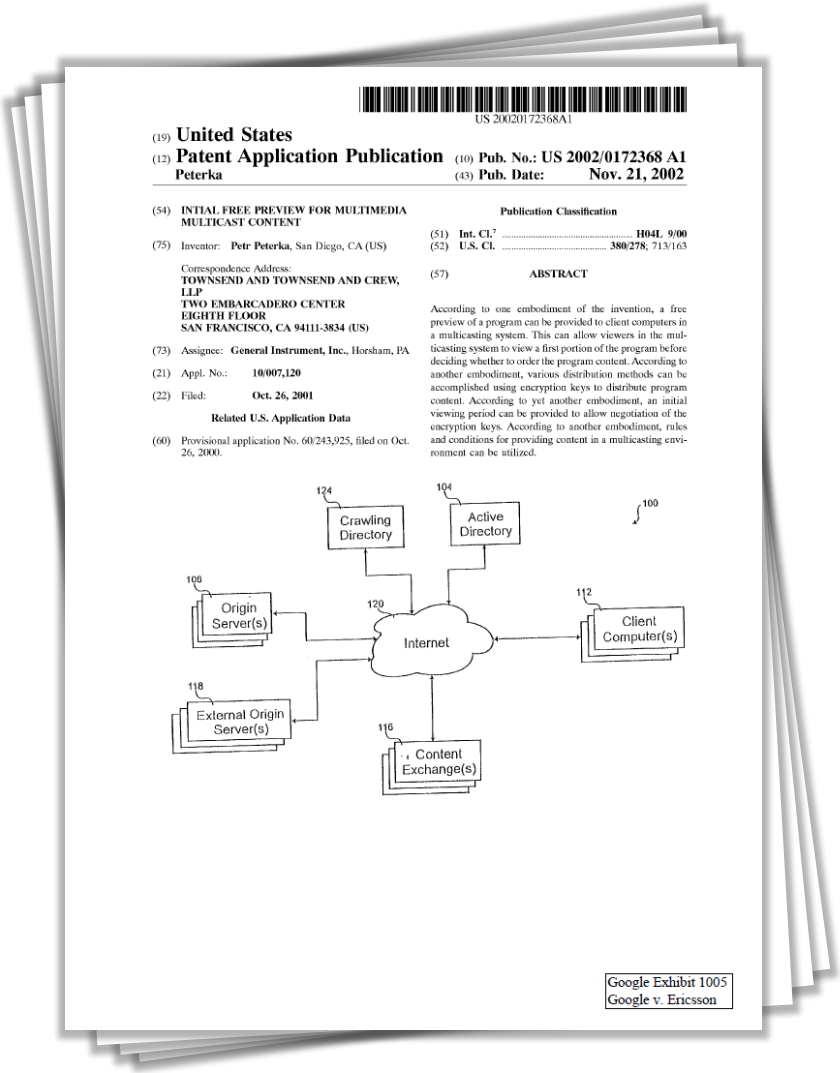
IPR2025-00003 Pet., 22
IPR2025-00004 Pet., 21-22

Petitions:

> To the extent "playback request response" is interpreted to require data transmitted in one message—a narrow interpretation that improperly uses the claim term "response" interchangeably with the word "message"—it would have been obvious to package multiple keys/entitlement messages (ECMs or EMMs) into a "single" "combined" "multicast message," in view of Peterka's express teachings that this was a viable option for "improved efficiency," and a POSITA's knowledge that multiple keys were conventionally transmitted in one message in response to a client request. Wechselberger, ¶81 (citing Peterka, [0104], [0121]; Suzuki, [0076]-[0077], FIGs. 5-6).

IPR2025-00003 Pet., 22; *see* IPR2025-00004 Pet., 21-22

"Pull" Model for Distributing Keys During Playback



US 20020172368A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2002/0172368 A1**

Peterka (43) **Pub. Date: Nov. 21, 2002**

(54) **INTIAL FREE PREVIEW FOR MULTIMEDIA MULTICAST CONTENT**

(75) Inventor: **Petr Peterka**, San Diego, CA (US)

Correspondence Address:
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834 (US)

(73) Assignee: **General Instrument, Inc.**, Horsham, PA

(21) Appl. No.: **10/007,120**

(22) Filed: **Oct. 26, 2001**

Related U.S. Application Data

(60) Provisional application No. 60/243,925, filed on Oct. 26, 2000.

Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**

(52) **U.S. Cl.** **380/278**; 713/163

(57) **ABSTRACT**

According to one embodiment of the invention, a free preview of a program can be provided to client computers in a multicasting system. This can allow viewers in the multicasting system to view a first portion of the program before deciding whether to order the program content. According to another embodiment, various distribution methods can be accomplished using encryption keys to distribute program content. According to yet another embodiment, an initial viewing period can be provided to allow negotiation of the encryption keys. According to another embodiment, rules and conditions for providing content in a multicasting environment can be utilized.

Google Exhibit 1005
Google v. Ericsson

Peterka (EX-1005)

[0105] The different embodiments of the invention provide models for distributing the keys outlined above. For example a "Pull" model, a "Push" model, and a combination "Push-Pull" model could be utilized. Under the pull model, each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire so as to avoid service interruptions. Alternatively, the push model migrates the responsibility to the server which keeps track of active clients and distributes new keys to them before the current keys expire. Pure push models may also

EX-1005, [0105]

[0106] The pull key distribution model allows each client to actively request keys from the server. In **FIG. 8, a** flow chart **800** is illustrated for implementing a pull key distribution system. In block **810** a server receives a request for a cryptographic key from a client. The server logs the request for the key in block **814**. For example, such a log entry could be made in a log such as a database maintained by the server. In block **818**, the key and its expiration time are distributed to the client in response to the request by the client. Thus the server need not monitor the status of the client's keys; rather, the responsibility of determining when a new key is required can be passed to the client. In block

EX-1005, [0106]

"Pull" Model for Distributing Keys During Playback

IPR2025-00003 Petition

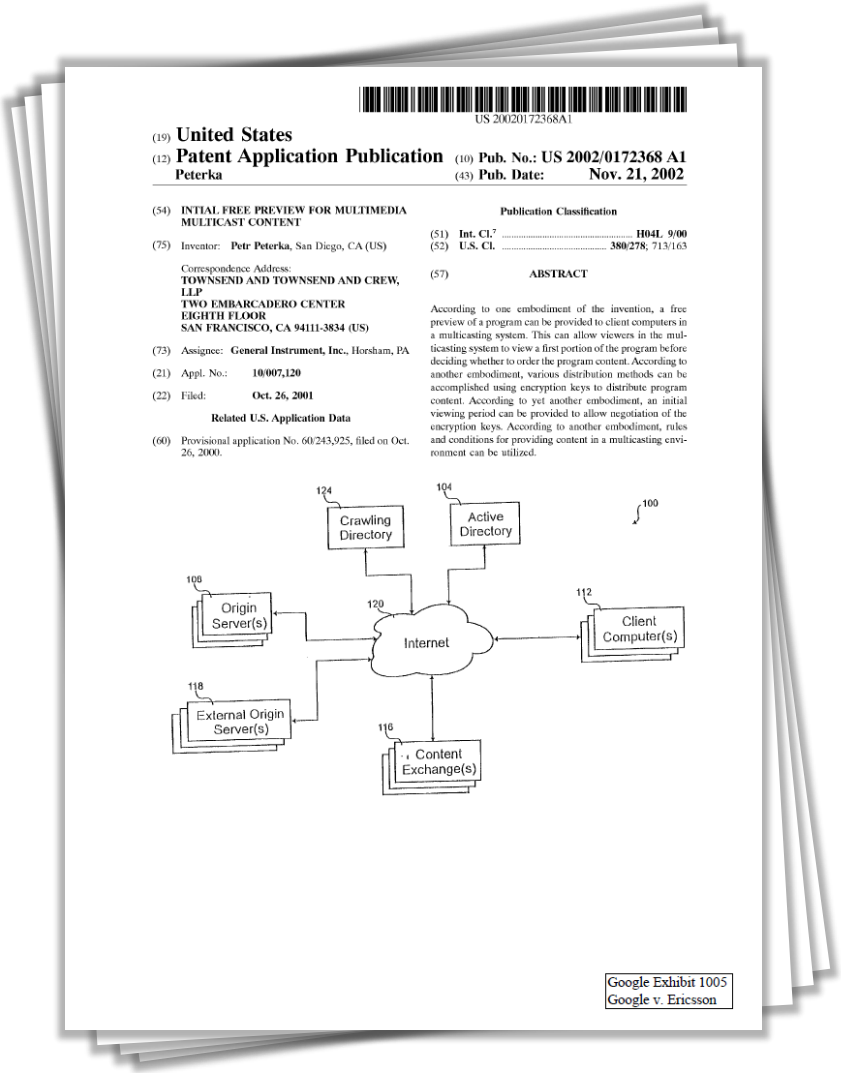
PO's previous attorney-argument suggesting signaling is exclusive to Peterka's push model (EX-1027, 20-21) is incorrect. Peterka's teachings regarding "signaling" ***when to use*** keys (Peterka, [0116]-[0121]) are ***complementary*** to Peterka's pull model for acquiring keys (*id.,* [0105]-[0106]). When to use keys and when to acquire keys are orthogonal concepts; signaling when to use a key in the client's possession ***does not require*** Peterka's server to ***push*** updated keys. Wechselberger, ¶¶115-116 (citing, for corroboration, Suzuki, [0013], [0016], [0043]-[0048], [0059]-[0060], [0076]-[0077], FIGs. 2, 5, describing system with pull key distribution ***and*** key change signaling in content stream). At minimum, using Peterka's key change signaling with Peterka's pull model would have been obvious. Wechselberger, ¶117; Peterka, [0121] (ECM/EMM includes ***both*** key lifetime ***and*** parity bit); *see also, e.g.,* Suzuki, [0016].

IPR2025-00003 Pet., 33-34

See also IPR2025-00003 Pet., 10-11; IPR2025-00004 Pet., 10-11

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

“Pull” Model for Distributing Keys During Playback



US 20020172368A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2002/0172368 A1**

Peterka (43) **Pub. Date: Nov. 21, 2002**

(54) **INTIAL FREE PREVIEW FOR MULTIMEDIA MULTICAST CONTENT**

(75) Inventor: **Petr Peterka**, San Diego, CA (US)

Correspondence Address:
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834 (US)

(73) Assignee: **General Instrument, Inc.**, Horsham, PA

(21) Appl. No.: **10/007,120**

(22) Filed: **Oct. 26, 2001**

Related U.S. Application Data

(60) Provisional application No. 60/243,925, filed on Oct. 26, 2000.

Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**

(52) **U.S. Cl.** **380/278**; 713/163

(57) **ABSTRACT**

According to one embodiment of the invention, a free preview of a program can be provided to client computers in a multicasting system. This can allow viewers in the multicasting system to view a first portion of the program before deciding whether to order the program content. According to another embodiment, various distribution methods can be accomplished using encryption keys to distribute program content. According to yet another embodiment, an initial viewing period can be provided to allow negotiation of the encryption keys. According to another embodiment, rules and conditions for providing content in a multicasting environment can be utilized.

Google Exhibit 1005
Google v. Ericsson

Peterka (EX-1005)

[0121] In multicasting program content such as audio and visual material, entitlement management messages and entitlement control messages can be sent from a server to client computer. One embodiment of the invention provides a format for such messages. Under this format, a sequence number or a time stamp to protect against replay attacks is provided. Furthermore, in another field of the EMM and ECM messages, a keyed message authentication code (MAC), or a public key digital signature for authentication is provided. Note that neither the keyed-hashing for message authentication (HMAC) nor the signature can be verified until a client performs the key request exchange. Yet another field would include the type of key included in the message, such as a content key, a group key, a program segment key, a service key, etc. Furthermore, a field would be provided for the type of key used to encrypt the key in the message. Thus, a unique key could be indicated for a message transmitting a service key, for example. Another field can be provided for the time remaining in the lifetime of the key. Furthermore, a key parity bit matching the parity bit in the RTP packet can be provided. Also, a user identification, which is often needed when multiple EMMs are delivered in a single multicast message, can be provided. Each field of the data structure applies to each of these fields. Thus, they can be arranged in any order such that the data structure includes one or more of these fields.

EX-1005, [0121]

Petitioner's Peterka Implementation (Ground 1)

IPR2025-00003 Pet., 12, 18
IPR2025-00004 Pet., 11-12, 17-18

Petitions:

> Peterka discloses a multimedia distribution system that uses a pay-by-time purchase mechanism and a "pull" key distribution method where clients monitor key expiration times to request new keys before they expire. Wechselberger, ¶71; Peterka, [0053], [0078]-[0082], [0105]-[0106], [0110]; *supra* § VIII.A. Every

IPR2025-00003 Pet., 18; *see* IPR2025-00004 Pet., 17

> interruptions." *Id.*, [0105]-[0106], FIG. 8. To mitigate excessive server loads at media segment boundaries when clients actively request and negotiate keys for segments, Peterka teaches distributing ***multiple*** keys (e.g., multiple ECMs) to a client—e.g., for the current ***and*** next media segment—in response to such a request. *Id.*, [0080]; *see also id.*, [0130], FIG. 7B; Wechselberger, ¶¶51-52.

IPR2025-00003 Pet., 12; IPR2025-00004 Pet., 11-12

Patent Owner's Disputes

IPR2025-00003 POR, Table of Contents
IPR2025-00004 POR, Table of Contents

1. The Petition does not meet "the content information including content encryption keys. . ." as recited in all claims

2. The Petition does not meet "content encryption *key identifiers*" as recited in all claims

PO raises these disputes for both proceedings

3. The Petition's expiration time theory does not meet "detecting content encryption key rotation boundaries"

4. The Petition's notification theory does not meet the "issuing requests" requirement of all challenged claims

PO only raises these disputes for IPR2025-00003 ('178 Patent)

IPR2025-00003 POR, Table of Contents; *see also* IPR2025-00004 POR, Table of Contents

Patent Owner's Multiple CEK Argument

IPR2025-00003 Pet., x; Pet. Reply, 1
IPR2025-00004 Pet., ix; Pet. Reply, 1

US 9,313,178 B2

1. A method for handling secure distribution of content comprising:

initiating a media playback request and receiving a playback request response;

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;

retrieving content and manifest files from a content delivery server;

detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content;

issuing requests to a 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

applying the second key for content decryption after the key rotation boundary is reached.

Initiating playback

Acquiring content

Acquiring more keys during playback

US 11,122,313 B2

1. A method for handling secure distribution of live video content comprising:

sending a request for live media playback;

receiving a live media playback request response, the live media playback request response comprising content encryption keys and content encryption key identifiers;

receiving encrypted live media content and manifest files from a content delivery server, wherein the encrypted live media content comprises one or more content encryption key rotation boundaries wherein each content encryption key rotation boundary is associated with a change to a different content encryption key to decrypt the received encrypted live media content;

applying a first content encryption key to the encrypted live media content before a first content encryption key rotation boundary;

prior to reaching the first key rotation boundary, obtaining a second content encryption key, the second content encryption key to be used after the first content encryption key rotation boundary is reached; and

applying the second content encryption key for content decryption after the key rotation boundary is reached.

Arguments Re: PPV and Subscription Models

IPR2025-00003 POR, Table of Contents
IPR2025-00004 POR, Table of Contents

PORs:

A. The Petition's theory

B. Peterka's teachings contradict and refute the Petition's theory

1. Peterka's Pay-Per-View model cannot meet the challenged claims
2. Peterka's Subscription model cannot meet the challenged claims
3. The Petition's theory also fails under Peterka's Pay-By-Time model

IPR2025-00003 POR, Table of Contents; IPR2025-00004 POR, Table of Contents

Arguments Re: FPK, GK, and Provisioning

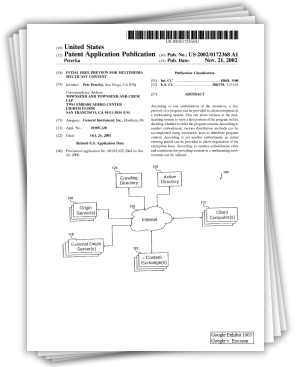
IPR2025-00003 Pet. Reply, 6-7
IPR2025-00004 Pet. Reply, 6-7

Pet. Replies:

PO also argues that Peterka's teachings regarding certain "***free preview key***" implementations of Peterka's "free preview period" (POR, 15-17) and "***group key***" implementations of Peterka's "initial viewing period" only involve keys provided to a client "ahead of time," allegedly before any media playback request, during "***provisioning***" (POR, 17-23, 26-27). These arguments focus on key types and concepts that Petitioner ***did not rely on***. As PO (and PO's expert) acknowledged, the Petition ***did not rely on*** the "free preview key" or "group key." POR, 8; Villasenor-Dec. (EX-2010), ¶¶33-34, 40, 58, 65; Villasenor-Dep. (EX-1040), 51:5-59:18, 65:6-13. The Petition instead relied on Peterka's teachings regarding Peterka's "***content keys.***" Pet., 23-25. Thus, PO's arguments about ***other*** key types are irrelevant to the Petition's grounds.

The Petition also did not rely on any implementations of Peterka where "content keys" are "provisioned," including because Peterka ***never even discloses*** such an option. Peterka, [0104] (Table 1); *see infra* § II.A.3.a. PO's arguments regarding provisioning are likewise irrelevant.

IPR2025-00003 Pet. Reply, 6-7; *see* IPR2025-00004 Pet. Reply, 6-7



Peterka (EX-1005)

TABLE 1

	PPV	Subscription	Pay-by-time
UK			
SR		(SK)UK	
PK	(PK)UK	(PK)SK	
PSK	(PSK)GK or (PSK)PK or (PSK)FPK	Optional: (PSK)SK or (PSK)PK	(PSK)UK
CK	(CK)PK or (CK)FPK or (CK)GK or (CK)UK	(CK)PSK or (CK)SK or (CK)PK	(CK)PSK (CK)FPK (CK)GK
GK	(GK)UK or provisioned		(GK)UK or provisioned
FPK	(FPK)UK or provisioned		(FPK)UK or provisioned

EX-1005, [0104], Table 1

Patent Owner Misreads FIG. 7B

IPR2025-00003 Pet. Reply, 11-12
IPR2025-00004 Pet. Reply, 11-12

Pet. Replies:

PO repeatedly argues that Peterka's client in Fig. 7B receives content keys CK0 and CK1 ***without any request***. *E.g.*, POR, 1 ("…Peterka expressly teaches that the first two content keys (CK0 and CK1) in Figure 7B are provided ***without any request at all***… Content Key 2 (CK2) is the one and ***only*** key that clients obtain through request…") (emphasis original), 26 ("In Fig. 7B, neither the first ECM

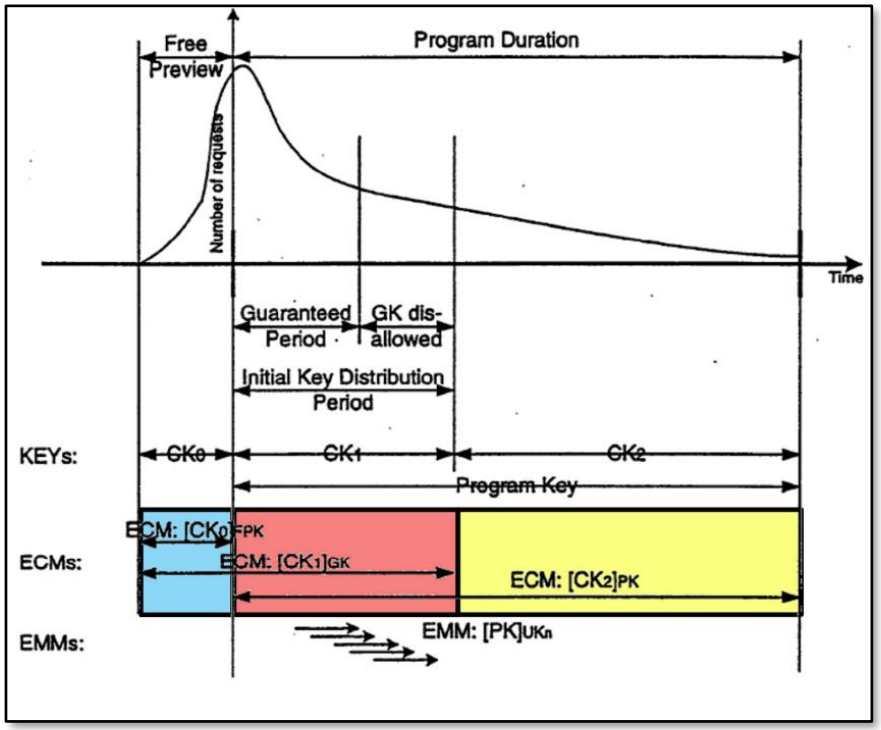
None of the purportedly "extensive teachings" (POR, 26) that PO relies upon to allege that Fig. 7B's CK0 and CK1 are exclusively "provision[ed]" "ahead of time" actually relate to CK0 or CK1. Instead, Peterka's teachings regarding providing keys "ahead of time" (e.g., during "provisioning") exclusively relate to Peterka's "***free preview keys***" (Peterka, [0083], [0085], [0103], [0104]) and "***group keys***" (Peterka, [0102], [0104], [0127]-[0129])—which Petitioner did not rely upon (*see supra* § II.A.1).

IPR2025-00003 Pet. Reply, 11-12; *see* IPR2025-00004 Pet. Reply, 11-12

Patent Owner Misreads FIG. 7B

IPR2025-00003 Pet., 21-22; Pet. Reply, 12-14
IPR2025-00004 Pet., 20; Pet. Reply, 12-14

Peterka (EX-1005):



EX-1005, FIG. 7B (annotated)

[0021] **FIGS. 7A and 7B** are graphs showing exemplary distribution of cryptographic keys during portions of a program.

EX-1005, [0021]

Pet. Replies:

The top half of Fig. 7B shows the "number of requests" for a program that Peterka's system receives during portions of a program, plotted against time. Peterka, [0091] (describing the same plot in Fig. 7A: "FIG. 7A illustrates a plot showing the number of requests for a program versus the program duration."); Villasenor-Dep., 104:8-13 (comparing Fig. 7B with 7A: "I think it's intended to show the same general sort of behavior."). Below the "number of requests" plot, Fig. 7B shows the ECMs that the system "convey[s]" to clients during the same program portions. Peterka, [0122].

Fig. 7B thus shows, at a given time, the number of requests for a program (above the time axis), and the ECMs / content keys that would be sent in response (below the time axis). Pet., 21; Wechselberger, ¶79. For example, during the "free

As can be seen above, Fig. 7B ***does not show*** any distribution of keys that occurs ***before*** clients begin requesting access to a program, because—as PO's own expert acknowledged—the only time in Fig. 7B where there have been no client requests to access a program is before the beginning of Fig. 7B's free preview period (left side of the graph). Villasenor-Dep., 105:18-106:7.

IPR2025-00003 Pet. Reply, 12-14;
see IPR2025-00004 Pet. Reply, 12-14

Patent Owner Misreads FIG. 7B

Villasenor:

Q. And I guess, just like in Figure 7A, the only point on the plot in Figure 7B where there have been no requests for the program is at the beginning of the free preview period, right?

A. Well, at the very beginning they haven't even seen the free preview. It takes people a certain amount of time to see at least a portion of the preview and decide they want to watch it.

So that's why it starts, you know, basically at zero.

Q. Right. And it's not zero anywhere else on this plot, right?

A. This particular plot does not hit zero anywhere but at the very left end.

Villasenor Dep. (EX-1040), 105:18-106:7

Pet. Replies:

The fact that Fig. 7B does not teach content keys (CK0, CK1) provisioned to clients ***before*** any request to access the program (as PO argues) is confirmed by Peterka's description in the paragraphs directly after paragraph [0122]. In paragraphs [0123]-[0124], Peterka describes ***alternatives*** to the embodiment shown in Fig. 7B that do not use CK0 and CK1 and instead uses the FPK and GK. Peterka,

IPR2025-00003 Pet. Reply, 14;
see IPR2025-00004 Pet. Reply, 14-15

Peterka (EX-1005):

[0123] Alternatively, CK**0** does not need to be distributed inside an ECM. The value of FPK already possessed by the plurality of clients may be taken as CK**0**.

[0124] Alternatively, CK**1** does not need to be distributed inside an ECM. The value of GK already possessed by the plurality of clients may be taken as CK**1**.

EX-1005, [0123]-[0124]

Patent Owner's "Unpurchased Keys" Theory

IPR2025-00003 PO Sur-Reply, 4 n.1
IPR2025-00004 PO Sur-Reply, 4 n.1

PO's Sur-Replies:

---

[1] Although Peterka teaches embodiments in which media is provided to prospective pay-by-time clients *before* the clients have made a purchase decision, all such content is provided ***without client request***, and any keys necessary for decrypting all such un-purchased content are likewise provided ***without client request***. POR at 14-22. Accordingly, any such ***unpurchased*** keys cannot meet the challenged claims under the Petition's theory, as was extensively demonstrated in the POR.

IPR2025-00003 PO Sur-Reply, 4 n.1; *see* IPR2025-00004 PO Sur-Reply, 4 n.1

Patent Owner Misreads PBT

IPR2025-00003 Pet. Reply, 16-17
IPR2025-00004 Pet. Reply, 16-17

> PO also argues that "giv[ing] certain clients access to additional future content that they did not purchase" "would defeat the purpose of Peterka's pay-by-time" model. POR, 33-34. This argument is illogical.

IPR2025-00003 Pet. Reply, 16; *see* IPR2025-00004 Pet. Reply, 16

Peterka (EX-1005):

> [**0053**] Pay-By-Time (PBT)—A purchase mechanism in which the client pays for the time duration of the content that was actually watched. The discrete time increments may have different durations for different programs or services.

EX-1005, [0053]

> keys to them. All consumer computers would negotiate a key for each segment in order to keep track of how may segments they watched. This generates a large load on the caching server on the segment boundaries. This can be mitigated with a key management approach where each rabbit is given keys to the current as well as the next segment. This will give the caching server enough time to distribute the next segment keys during the current segment.

EX-1005, [0080]

> [**0082**] When the client negotiates encryption keys with the caching server, it will start receiving the multicast content. The client will monitor the expiration time for each pay period and request a new set of keys from the caching server. If the viewer stops watching or moves to another service the client will not request new keys or it will actively notify the caching server that it wants to leave the current multicast session. The caching server will record the time when each client joins and leaves the multicast for billing purposes.

EX-1005, [0082]

Patent Owner Misreads PBT

IPR2025-00003 Pet. Reply, 16-17
IPR2025-00004 Pet. Reply, 16-17

Cf. POR's other arguments re: Peterka, [0080]:

> content keys to two segments. Ex. 2010 ¶ 60. Rather, that passage explains that the key for the next segment will be provided during the current segment to avoid service interruptions. *Id.*; Ex. 1005 ¶ 80. This is consistent with the rest of Peterka's teachings. For instance, in Figure 7B, the content key for the initial viewing period

IPR2025-00003 POR, 27-28; *see* IPR2025-00004 POR, 27

Peterka (EX-1005):

> keys to them. All consumer computers would negotiate a key for each segment in order to keep track of how may segments they watched. This generates a large load on the caching server on the segment boundaries. This can be mitigated with a key management approach where each rabbit is given keys to the current as well as the next segment. This will give the caching server enough time to distribute the next segment keys during the current segment.

EX-1005, [0080]

Patent Owner Misreads Suzuki

IPR2025-00003 Pet. Reply, 17-20
IPR2025-00004 Pet. Reply, 18-20

> In Ground 1, the Petition cited Suzuki to show that multiple keys were conventionally transmitted in one message in response to a client request, and to support the argument that it was obvious to implement Peterka to return multiple keys in response to a client request. Pet., 22; Suzuki, [0076]-[0077], Figs. 5-6. In

IPR2025-00003 Pet. Reply, 17; *see* IPR2025-00004 Pet. Reply, 18

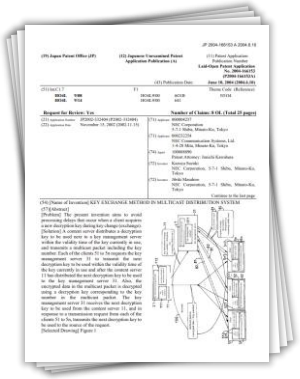
PORs:

> Finally, the Petition's reliance on Suzuki to support its obviousness theory is likewise unavailing. Ex. 2010 ¶ 78. Suzuki's paragraphs 76 and 77 do not teach transmitting multiple "***content encryption keys***," they only disclose providing "key ***information*** relating to the key currently in use (key A) and the next key to be used (key B)." Ex. 1006 ¶¶ 76-77; Ex. 2010 ¶ 78. And Suzuki is not directed to a pay-by-

IPR2025-00003 POR, 36; *see* IPR2025-00004 POR, 35

Patent Owner Misreads Suzuki

IPR2025-00003 Pet. Reply, 17-20
IPR2025-00004 Pet. Reply, 18-20



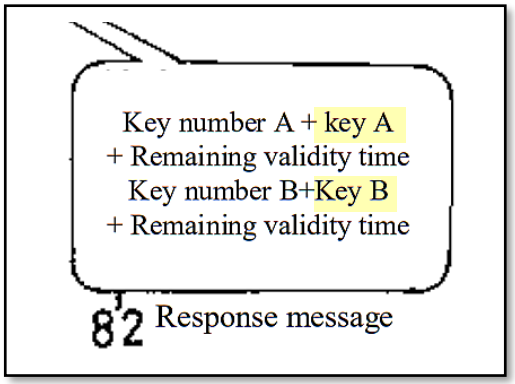
Suzuki (EX-1006)

key information (the key and associated information)

EX-1006, [0012]

key information (a set of a key, a key number, and the remaining validity time)

EX-1006, [0050]



EX-1006, FIG. 5 (excerpted)

[0072]
FIG. 5 is a diagram specifically showing the information in each key information management table and the contents of each packet/request/message. In FIG. 5, the key currently in use is indicated as key A, the next key to be used is indicated as key B, and their key numbers are indicated as "key number A" and "key number B." In this example, the encryption key and the decryption key are assumed to be the same key (for example, key A is both the encryption key and the decryption key). Further, the first setting value is indicated by X, and the second setting value is indicated by Y.

EX-1006, [0072]

[0076]
When the remaining validity time of key A reaches Y (second setting value), the client 51 transmits a key information request 81 to the key management server 31, requesting key information on the next key to be used.
[0077]
In response to this key information request 81, the key management server 31 transmits a response message 82 having key information relating to the key currently in use (key A) and the next key to be used (key B). As a result, the client 51 has key information relating to the keys A and B, as shown in FIG. 5.

EX-1006, [0076]-[0077]

Patent Owner's CEK Identifiers Argument

IPR2025-00003 POR, Table of Contents
IPR2025-00004 POR, Table of Contents

1. The Petition does not meet "the content information including content encryption keys. . ." as recited in all claims

2. The Petition does not meet "content encryption *key identifiers*" as recited in all claims



3. The Petition's expiration time theory does not meet "detecting content encryption key rotation boundaries"

4. The Petition's notification theory does not meet the "issuing requests" requirement of all challenged claims

IPR2025-00003 POR, Table of Contents; *see also* IPR2025-00004 POR, Table of Contents

Petitioner's 1st Argument Re: CEK Identifiers

IPR2025-00003 Pet., 25
IPR2025-00004 Pet., 24

Petitions:

¶90. Peterka discloses that each ECM/EMM includes "a ***sequence number*** or a ***time stamp*** to protect against replay attacks." Peterka, [0121]. Because the sequence number/timestamp is unique to each ECM/EMM (to prevent replay attacks), and each ECM/EMM carries a different content encryption key (*supra* § IX.A.1.b), the sequence number/timestamp each constitutes a unique ***content encryption key identifier***. Wechselberger, ¶91. This is consistent with the '178 specification's teaching of "content encryption key identifiers" that are "selected based on a segment number of the prepared content" and thus apply to an entire media segment. EX-1001, 3:34-35, 4:8-10; *see also id.,* 6:1-3, 6:17-19; Wechselberger, ¶92 (POSITAs would have recognized that one obvious way to "select" an identifier based on a segment number was by using the segment number ***itself*** as the identifier).

IPR2025-00003 Pet., 25; *see* IPR2025-00004 Pet., 24

Peterka (EX-1005):

a format for such messages. Under this format, a sequence number or a time stamp to protect against replay attacks is provided. Furthermore, in another field of the EMM and

EX-1005, [0121]

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Petitioner's 1st Argument Re: CEK Identifiers

IPR2025-00003 Pet., 25
IPR2025-00004 Pet., 24

Petitions:

identifier. Wechselberger, ¶91. This is consistent with the '178 specification's teaching of "content encryption key identifiers" that are "selected based on a segment number of the prepared content" and thus apply to an entire media segment. EX-1001, 3:34-35, 4:8-10; *see also id.*, 6:1-3, 6:17-19; Wechselberger, ¶92 (POSITAs would have recognized that one obvious way to "select" an identifier based on a segment number was by using the segment number ***itself*** as the identifier).

IPR2025-00003 Pet., 25; *see* IPR2025-00004 Pet., 24

Peterka (EX-1005):

a format for such messages. Under this format, a sequence number or a time stamp to protect against replay attacks is provided. Furthermore, in another field of the EMM and

EX-1005, [0121]

Specifications:

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

'178 Patent, 3:32-36; '313 Patent, 3:40-45

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 seg-

'178 Patent, 4:6-10; '313 Patent, 4:12-19

identifier. In one embodiment, the content encryption key identifiers are based off a next sequential integer value, offset from the previous content encryption key identifier. In another 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 seg-

'178 Patent, 5:63-6:4; '313 Patent, 6:6-14

Petitioner's 2nd Argument Re: CEK Identifiers

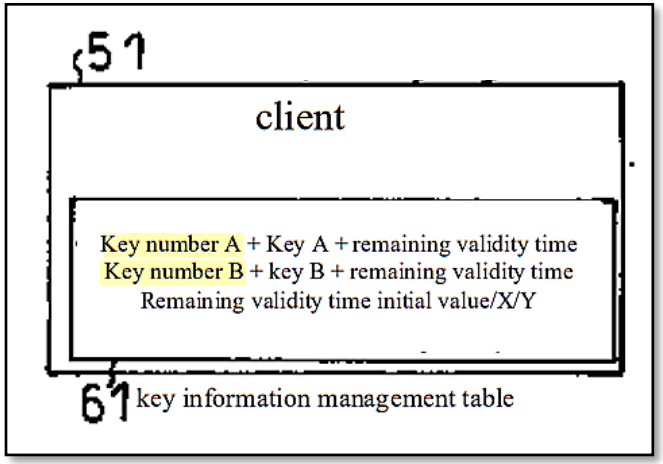
IPR2025-00003 Pet., 26
IPR2025-00004 Pet., 25

Petitions:

Alternatively, POSITAs would have been motivated (in view of, e.g., FIG. 7B, which ***shows*** delivery of content keys with unique designations—CK_0, CK_1, CK_2) to implement Peterka's client to receive and use a key identifier to identify the content key parsed from an ECM/EMM. Wechselberger, ¶94. In systems like Peterka's ([0080, [0122], [0130], FIG. 7B), where multiple keys are utilized, POSITAs would have recognized the need to differentiate between keys, would have been motivated to do so with key identifiers, and would have reasonably expected success. Wechselberger, ¶¶93-96 (citing, for corroboration, Suzuki, [0013] (client "table" with "key number" for each key), [0016] (client receiving "key number" for each key), [0030]-[0031], [0043]-[0048], [0080]-[0084] (client using "key number" to apply correct key), FIG. 5; Pestoni, 12:16-35 ("a key identifier for each key")).

IPR2025-00003 Pet., 26; *see* IPR2025-00004 Pet., 25

Suzuki (EX-1006):



EX-1006, FIG. 5 (excerpted)

Pestoni (EX-1012):

In various embodiments, playback device **100** may be configured to decrypt each segment **440***a-c* with the respective decryption key of key box **420**. In some embodiments, key box **420** may specify a key identifier for each key within the key box. Likewise, each encrypted segment **440***a-c* may include metadata (e.g., header information) that specifies the identifier of the decryption key that is to be utilized to decrypt that segment. For a given segment that is to be decrypted, playback device **100** may be configured to determine that the key identifier specified by that segment's metadata matches a key identifier of a particular decryption key within key box **420**. In response to that determination, playback device 100

EX-1012, 12:16-27

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Petitioner's 3rd Argument Re: CEK Identifiers

IPR2025-00003 Pet., 50-53
IPR2025-00004 Pet., 46-49

Petitions (Ground 2):

> To the extent the "identifiers" recited in Element [1B] or the timing requirements for the "prefetching" recited in claims 4-6 are not considered disclosed or rendered obvious by Peterka alone, Suzuki expressly teaches those limitations.

IPR2025-00003 Pet., 50; *see* IPR2025-00004 Pet., 46

(describing Suzuki):

> "Key number" is used to "identify[] the key," allowing a client to associate keys with their respective "remaining validity time[s]" (e.g., in a table) and to help the client keep track of keys, for example when determining which key to apply when decrypting a segment of content. *Id.*, [0030], [0043]-[0048], [0080], FIG. 2; Wechselberger, ¶164. A POSITA would have recognized the importance of such identifiers to differentiate amongst keys, and that providing unique values (such as key numbers) to keys would ensure that the system does not confuse keys. *Id.*

IPR2025-00003 Pet., 52-53; *see* IPR2025-00004 Pet., 48

Petitioner's 3rd Argument Re: CEK Identifiers

IPR2025-00003 Pet., 54
IPR2025-00004 Pet., 49

Petitions:

As discussed, Peterka-Suzuki applies Suzuki's teachings regarding "key numbers" and "remaining validity times" to Peterka. Peterka-Suzuki's client receives a "key number" and "remaining validity time" corresponding to each received "content encryption key" described *supra* §§ IX.A.1.b, IX.A.1.c.i(1). Wechselberger, ¶168. Peterka-Suzuki uses the "key number" to keep track of keys and the "remaining validity time" to determine when to request a next key. Suzuki, [0043]-[0048], [0072]-[0077], [0080]-[0081], FIGS. 2, 5-6; Wechselberger, ¶169.

Peterka-Suzuki's "key numbers" uniquely identify keys and are ***content encryption key identifiers***, as claimed. Wechselberger, ¶170.

IPR2025-00003 Pet., 54; *see* IPR2025-00004 Pet., 49

POR Relies on Unrecited Requirements

IPR2025-00003 Pet., x; Pet. Reply, 20-22
IPR2025-00004 Pet., ix; Pet. Reply, 20-23

US 9,313,178 B2

1. A method for handling secure distribution of content comprising:
initiating a media playback request and receiving a playback request response;
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;
retrieving content and manifest files from a [illegible] delivery server;

US 11,122,313 B2

1. A method for handling secure distribution of live video content comprising:
sending a request for live media playback;
receiving a live media playback request response, the live media playback request response comprising content encryption keys and content encryption key identifiers;
receiving encrypted live media content and manifest files from a content delivery server, wherein the [illegible] live media content [illegible]

PO's second argument is that Petitioner's Peterka-based grounds do not meet the "content encryption key identifiers" term because it "imposes two" "requirements"—(1) that the identifier is "***unique***" in the context of "***all***" content encryption keys maintained in a "***history***" and (2) that the identifier must be "***assigned*** to the content encryption key ***itself***." POR, 37-43. These purported "requirements" appear ***nowhere in the challenged claims***. And PO agreed the claims included no such requirements before the ITC. EX-1032, 15. PO's attempt to import unrecited requirements should be rejected:

IPR2025-00003 Pet. Reply, 20; *see* IPR2025-00004 Pet. Reply, 20-21

POR Does Not Allege Lexicography or Disavowal

IPR2025-00003 Pet. Reply, 20
IPR2025-00004 Pet. Reply, 21

PORs:

> In view of that language, the specification imposes two requirements for "content encryption key identifiers." Ex. 2010 ¶¶ 82-83. First, each content encryption key identifier must be "***unique***" in the context of ***all*** content encryption keys maintained in the "history." *Id.* Second, each content encryption key identifier must be "***assigned***" to the corresponding content encryption key ***itself***. *Id.* This

IPR2025-00003 POR, 37-38; *see* IPR2025-00004 POR, 36-37

Pet. Replies:

> ***Second***, PO does not establish any basis to depart from the plain and ordinary meaning of "content encryption key identifier." PO does not allege lexicography or disavowal—let alone establish either with the relevant legal analysis. The *one*

IPR2025-00003 Pet. Reply, 20; IPR2025-00004 Pet. Reply, 21

PO's Lexicography Discussion in Sur-Reply

PO's Sur-Replies:

> The POR demonstrated that the specification ***defines*** the term "content key identifiers" to require that each key identifier must be "unique" and that each key identifier must also be "assigned" to the corresponding content encryption key itself. POR 37-38. In particular, Patent Owner quoted the specification's teaching that: "Each content encryption key in the history is ***assigned*** a ***unique*** identifier which is ***referred to herein*** as the content encryption key identifier." Ex. 1001 at 3:28-32 (emphasis added).

IPR2025-00003 PO Sur-Reply, 17; *see* IPR2025-00004 PO Sur-Reply, 17

PO's Lexicography Discussion in Sur-Reply

Specifications:

SUMMARY

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

'178 Patent, 3:21-36; '313 Patent, 3:29-45

DETAILED DESCRIPTION

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 a next sequential integer value, offset from the previous content encryption key identifier. In another 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 seg-

'178 Patent, 5:58-6:3; '313 Patent, 6:29-45

Pet. Replies:

Instead, that sentence describes how ***one*** embodiment of a server-side "***workflow manager***" works—an entity "distinct from the client" that is undisputedly unclaimed. Villasenor-Dep., 132:17-133:4 (discussing the "workflow manager" in

IPR2025-00004 Pet. Reply, 21; *see* IPR2025-00003 Pet. Reply, 21

Patent's Discussion of CEK Identifiers

IPR2025-00003 Pet. Reply, 21
IPR2025-00004 Pet. Reply, 21-22

Pet. Replies:

> ***Third***, PO has no response to Petitioner's showing that using an ECM's "sequence number" or "time stamp" as a CEK identifier closely tracks the '178 specification's teaching of using "content encryption key identifiers" "selected based on a segment number of the prepared content"—Pet., 25 (citing EX-1001, 3:34-35, 4:8-10; *see also id.*, 6:1-3, 6:17-19)—and cites no legal basis to construe the term inconsistently with the specification.

IPR2025-00003 Pet. Reply, 21; *see* IPR2025-00004 Pet. Reply, 21-22

Specifications:

> 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

'178 Patent, 3:32-36; '313 Patent, 3:40-45

> 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 seg-

'178 Patent, 4:6-10; '313 Patent, 4:12-19

> identifier. In one embodiment, the content encryption key identifiers are based off a next sequential integer value, offset from the previous content encryption key identifier. In another 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 seg-

'178 Patent, 5:63-6:4; '313 Patent, 6:6-14

Obviousness Theories Meet Narrow Interpretation

IPR2025-00003 Pet. Reply, 21-22
IPR2025-00004 Pet. Reply, 22-23

Pet. Replies:

> ***Fourth***, even if the claims included PO's "requirements," PO's argument fails. Peterka's "sequence number"/"time stamp" are each undisputedly "unique" enough (Pet., 25) to distinguish amongst the client's stored keys (a "history"). Petitioner also showed there were ***numerous*** reasons to implement Peterka's client to receive and use identifiers that were (1) assigned specifically to keys and (2) sufficiently "unique" to distinguish amongst keys in a "history"—and numerous reasons to combine Peterka with other references disclosing these unrecited features. Pet., 26 (citing Suzuki, Pestoni, and Wechselberger, ¶¶93-96); Pet., 51-55 (Peterka-Suzuki, citing Wechselberger, ¶¶161-172); Pet., 66-68 (Peterka-Suzuki-Bocharov,

Ground 1 (alternative obviousness)

Ground 2

IPR2025-00003 Pet. Reply, 21-22; *see* IPR2025-00004 Pet. Reply, 21

Obviousness Theories Meet Narrow Interpretation

IPR2025-00003 Pet. Reply, 22
IPR2025-00004 Pet. Reply, 22-23

PORs:

> 2010 ¶ 94. Peterka can thus differentiate between keys using message identifiers, and has no need for additional "key identifiers" as recited in the challenged claims. Ex. 2010 ¶ 94.

IPR2025-00003 POR, 41-42; *see* IPR2025-00004 POR, 40-41

Pet. Replies:

> PO's argument fails to credibly rebut Petitioner's obviousness arguments. Regarding the obviousness of using unique CEK IDs assigned specifically to keys (in view of Suzuki and Pestoni, Pet., 26), PO's only response is to acknowledge that there is no meaningful difference between using Peterka's sequence numbers/time stamps as CEK IDs for individual keys and specifically assigning CEK IDs to individual keys. POR, 41-42. Moreover, PO does not dispute that a POSA would have been motivated to use assigned CEK IDs in the "***alternative***" scenario contemplated by the Petition (Pet., 26), where Peterka's sequence numbers/time stamps are not used as CEK IDs.

IPR2025-00003 Pet. Reply, 22; *see* IPR2025-00004 Pet. Reply, 22-23

Multi-Bit Signals (Ground 5)

Petitions:

> Peterka contemplates a client acquiring keys for multiple future media segments and using ***multi-bit*** signals embedded in streaming media packets to select the correct key from among those keys. Peterka, [0117] ("***if*** a single bit is used"), [0118]-[0121]; Wechselberger, ¶209. At minimum, acquiring keys for multiple future segments would have been obvious to reduce the "load" of client requests at segment boundaries. Peterka, [0080], [0105]; Wechselberger, ¶209 (citing, for corroboration, Pestoni, 12:1-46).

IPR2025-00003 Pet., 69; *see* IPR2025-00004 Pet., 63-64

Wechselberger:

> the segment boundaries"). The POSITA would have appreciated, for example, that distributing keys for additional segments beyond just the current and next segments would have beneficially reduced the load of client requests that needed immediate service in order to avoid service interruptions for Peterka's clients. Peterka, [0105]

IPR2025-00003 EX-1003, ¶209; IPR2025-00004 EX-1003, ¶194

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Multiple Future Keys (Ground 5)

Wechselberger:

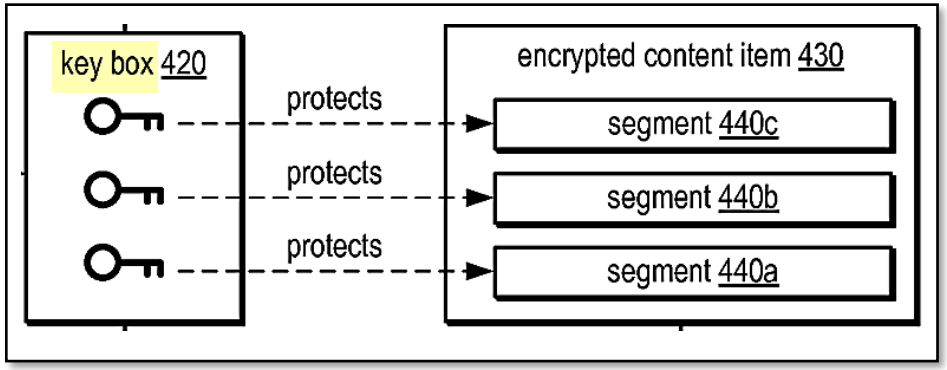
> interruptions."). For corroboration of this background knowledge of a POSITA, see, for example, the Pestoni reference (EX-1012), at 12:1-46 (describing "key box" with

IPR2025-00003 EX-1003, ¶209; IPR2025-00004 EX-1003, ¶194

Pestoni (EX-1012):

> In embodiments that utilize the key box techniques described above, the overall ratio of license requests to content decryption keys may be reduced relative to the embodiment of FIG. **2**. For instance, in the illustrated embodiments of FIG. **2**, one license request yields the use of one content decryption key. However, in the embodiment of FIG. **4**, a single license yields the use of three different content decryption keys. In other words, for a given quantity of content decryption keys utilized for content, the embodiment of FIG. **4** may require license server(s) **120** to process fewer content license requests. Generally, the more decryption keys

EX-1012, 12:36-46



EX-1012, FIG. 4 (excerpted)

Patent Owner's Disputes (IPR2025-00003 Only)

1. The Petition does not meet "the content information including content encryption keys. . ." as recited in all claims

2. The Petition does not meet "content encryption *key identifiers*" as recited in all claims

3. The Petition's expiration time theory does not meet "detecting content encryption key rotation boundaries"

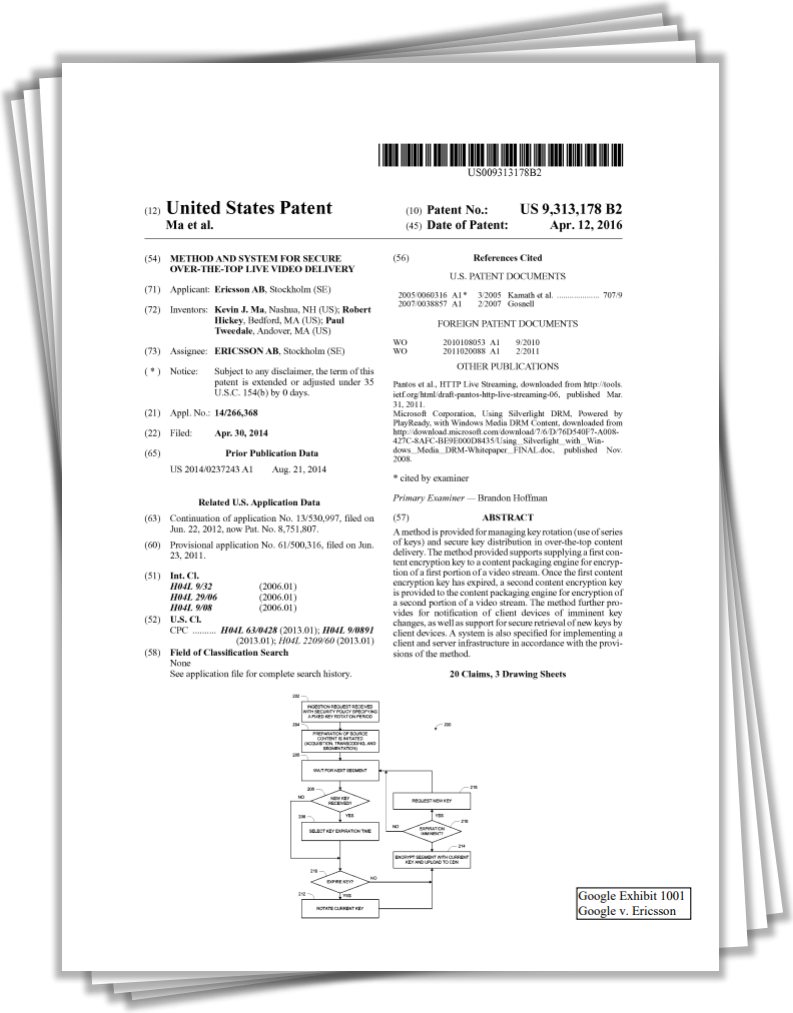


4. The Petition's notification theory does not meet the "issuing requests" requirement of all challenged claims

IPR2025-00003 POR, Table of Contents

Petitioner's Arguments Re: "Detecting"

IPR2025-00003 Pet., 31-34; Pet. Reply, 23-25



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

'178 Patent
(IPR2025-00003 EX-1001)

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

'178 Patent, 9:47–49

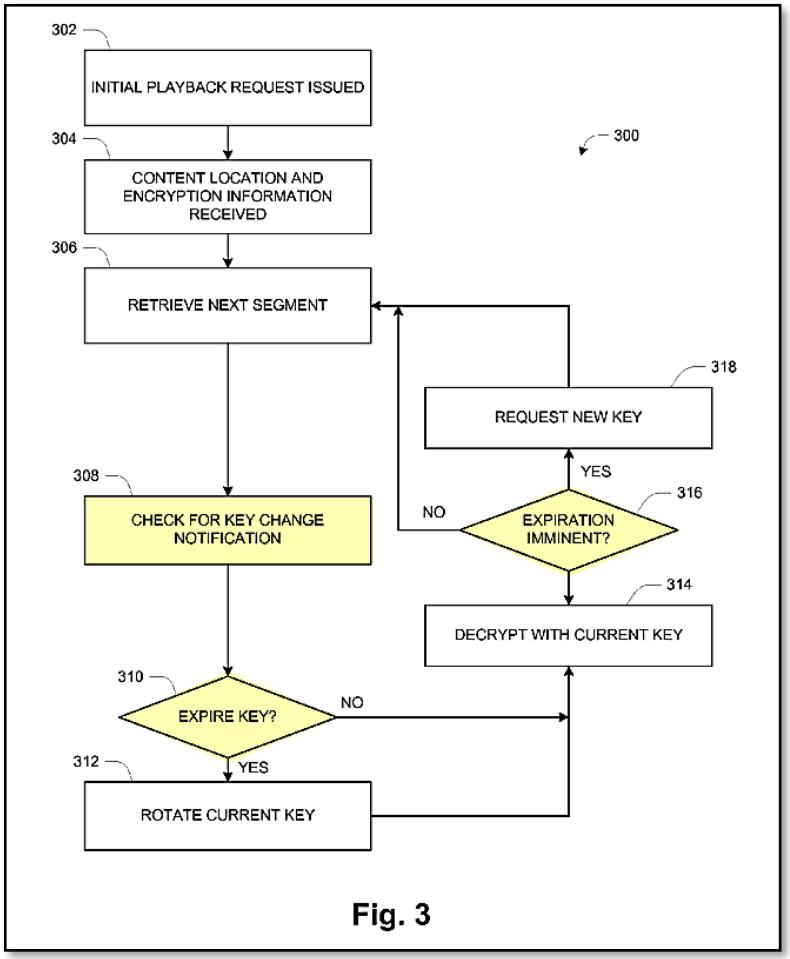


Fig. 3

'178 Patent, Fig. 3

Petitioner's Arguments Re: "Detecting"

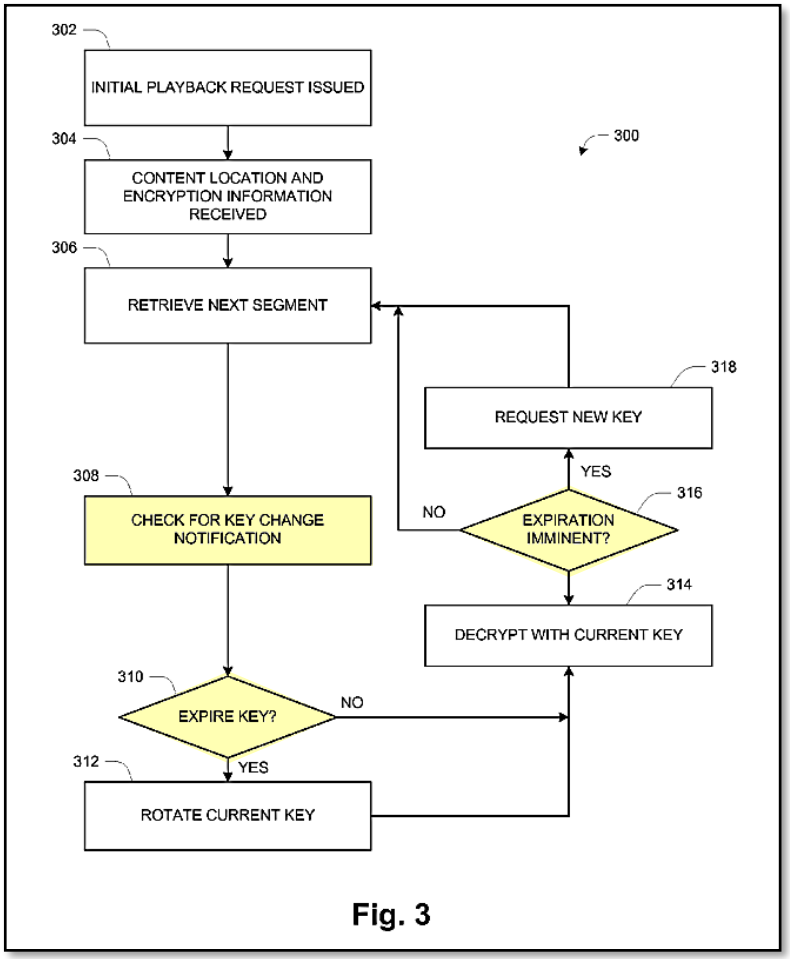
IPR2025-00003 Pet., 31-34; Pet. Reply, 23-25

Petitioner showed that limitation [1D]'s "detecting" requirement was met by Peterka's client in two different ways: (1) by monitoring key expiration times so that the client can ***acquire*** new content keys before current content keys expire (Pet., 31-32, citing Peterka, [0105]-[0106]); and (2) by monitoring the content stream for signals that inform a client when to begin ***utilizing*** a given content key for decryption (Pet., 33, citing Peterka, [0116]-[0121]). Petitioner explained why Peterka's "signaling" teachings regarding key utilization were fully compatible with Peterka's pull model for acquiring keys, including by citing to Peterka's disclosure of sending clients information for ***both*** detection operations in one key distribution message—key lifetime (for monitoring key expirations) ***and*** a key parity bit (for comparing against key change signals in the stream). Pet., 34; Peterka, [0121].

IPR2025-00003 Pet. Reply, 23

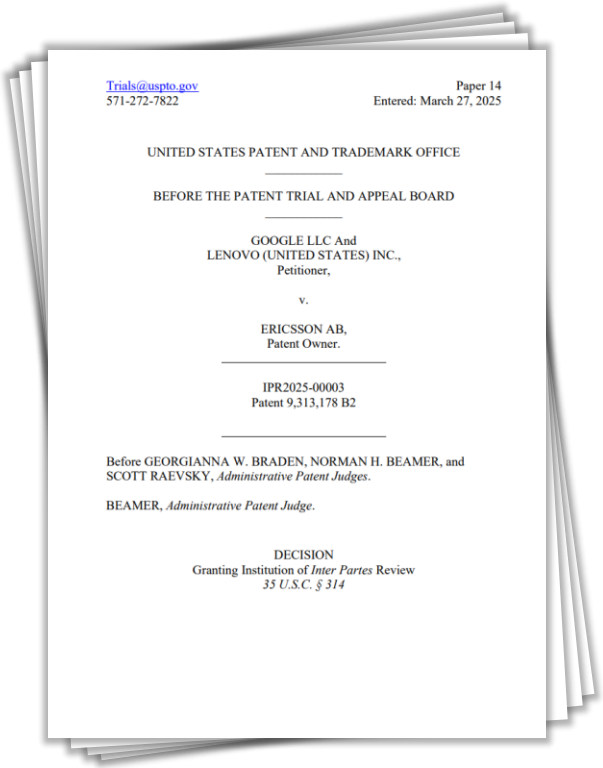
FIG. **3** is a flow chart **300** describing a process for detecting the rotation of content encryption keys and retrieving updated content encryption keys. In step **302**, the client **110** issues a

'178 Patent, 9:47–49



'178 Patent, Fig. 3

Board was Correct at Institution Re: "Detect"



Trials@uspto.gov
571-272-7822

Paper 14
Entered: March 27, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC And
LENOVO (UNITED STATES) INC.,
Petitioner,

v.

ERICSSON AB,
Patent Owner.

IPR2025-00003
Patent 9,313,178 B2

Before GEORGIANNA W. BRADEN, NORMAN H. BEAMER, and SCOTT RAEVSKY, *Administrative Patent Judges*.

BEAMER, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

IPR2025-00003
Institution Decision
(Paper 14)

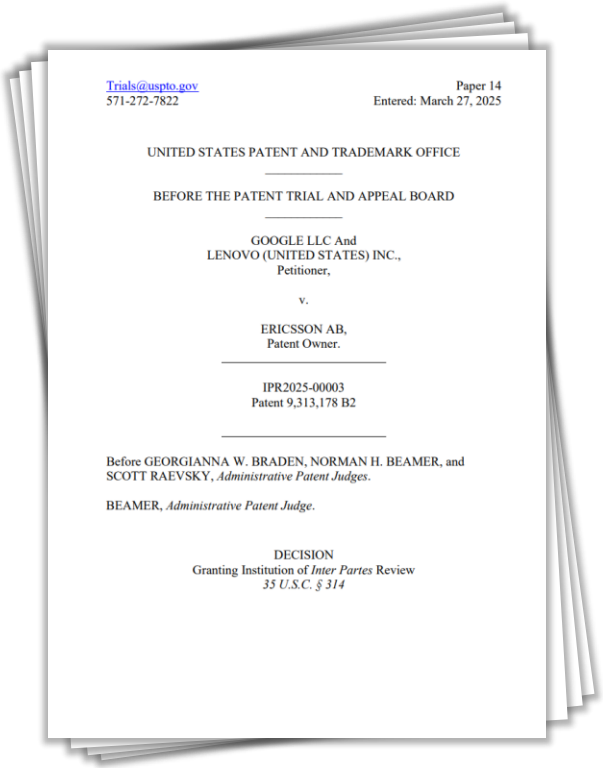
In sum, we conclude at this stage that the "detecting" limitation refers to all boundaries between key rotations, whether caused by normal expiration of a key or by forced rotation due to security issues. The "detecting" part of the limitation refers to detecting any key rotation boundary. Thus, we determine that Petitioner's reliance on the disclosure in Peterka of a "pull model," in which "each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire so as to avoid service interruptions," is reasonably likely to meet the detecting requirement of claims 1 and 16.[10]

Based on this, and on our further review of Petitioner's reliance on Peterka's disclosures in challenging the remaining requirements of claims 1 and 16, we determine for purposes of this Decision that the information presented in the record demonstrates a reasonable likelihood that Petitioner will prevail in establishing that independent claims 1 and 16 are unpatentable under 35 U.S.C. § 103 over Peterka.

IPR2025-00003 Inst. Dec., 23-24

Board was Correct at Institution Re: "Detect"

IPR2025-00003 Inst. Dec., 26-27



Trials@uspto.gov
571-272-7822

Paper 14
Entered: March 27, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC And
LENOVO (UNITED STATES) INC.,
Petitioner,

v.

ERICSSON AB,
Patent Owner.

IPR2025-00003
Patent 9,313,178 B2

Before GEORGIANNA W. BRADEN, NORMAN H. BEAMER, and SCOTT RAEVSKY, *Administrative Patent Judges*.

BEAMER, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

IPR2025-00003
Institution Decision
(Paper 14)

Claim 12 adds to claim 1 the requirement that "actual content encryption key rotation boundaries are detected based on real-time in-band notifications." Ex. 1001, 12:65–67. Claim 20 is commensurate. *Id.* at 14:26–28. For these claims, Petitioner relies on the disclosure in Peterka of a client checking content packets for a signal to start applying a new key. Pet. 48, 50 (citing Ex. 1005, Fig. 14, ¶¶ 116–121; Ex. 1003 ¶¶ 154–155, 159).

This argument by Petitioner depends on Petitioner's alternative argument regarding the detecting requirement of claim 1, relying on the disclosure in Peterka of methods for signaling to the client information for the client to detect content encryption key rotation boundaries, such as including predetermined bit in the header of a packet sent from the server. Pet. 33–34. As discussed above, the parties dispute whether this signalling capability only pertains to the "Push" embodiment of Peterka, and is therefore incompatible with the requirement of the claims that sending keys to the client must be preceded by a request for keys from the client. Prelim. Resp. 22–25; Reply 5; Sur-Reply 5.

At this stage, after reviewing the current record, we determine that Petitioner demonstrates a reasonable likelihood that it will prevail in establishing that claims 12 and 20 are unpatentable under 35 U.S.C. § 103 over Peterka.

IPR2025-00003 Inst. Dec., 26-27

PO Again Argues Monitoring Expiration Times is Not Detecting

IPR2025-00003 Pet. Reply:

PO brings little new to the table. POR, 43-48. PO ***again*** tortures Figure 3 and its accompanying disclosures, which expressly describe a process for "***detecting***" CEK rotation boundaries (EX-1001, 9:47-49) that ***includes*** checking for whether the current key will expire. EX-1001, 11:3-8, 11:38-41, Fig. 3. PO ***again*** identifies nothing in the intrinsic record that justifies narrowing "detecting" from its ordinary meaning to exclude one of the detecting types in Fig. 3.

PO also mischaracterizes the Petition to try distinguishing Peterka, arguing that merely "identifying a key's expiration time alone" cannot be "detecting" a key rotation boundary. POR, 49. But Petitioner never equated "identifying a key's expiration time alone" with "detecting." Instead, Petitioner showed how "***keep[ing] track of***"/"***monitor[ing]***" key expiration times meets the "detecting" described in the '178 Patent. Pet., 31-33.

PO finally tries to argue that "detecting" requires a three-step process that includes "***checking*** for both an express notification and an expiration time, ***analyzing*** the resulting information, and ***determining*** the appropriate rotation boundary in view of the results." POR, 49. Much like the POPR's "partly hidden"/"not clear" argument, PO's new "analyzing"/"determining" argument bears no relation to the claims, finds no support in the intrinsic record, and departs wildly from PO's previous allegations that detecting a key rotation boundary required nothing more than "encountering" a header in a media stream. POPR Reply, 1-3;

IPR2025-00003 Pet. Reply, 23-25

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

IPR2025-00003 PO Sur-Reply:

attempt at misdirection is unavailing. The Patent Owner Response demonstrated in extensive detail, with support from Patent Owner's expert, that the specification defines the "process for detecting the rotation of content encryption keys" through Figure 3 and its associated teachings. POR at 43-49. Patent Owner showed that this

in light of both items of information. *Id.* Patent Owner specifically demonstrated that in the flow diagram of Figure 3, which defines the "detecting" limitation of the claims, the client must ***always*** "check for key change notification" as stated in step 308. POR at 46; Fig. 3; Ex. 2010 ¶ 107. That step is not optional. *Id.*; Ex. 1001 at

IPR2025-00003 PO Sur-Reply, 21-22

SCHEDULING ORDER

with the parties and the Board. Patent Owner is cautioned that any arguments not raised in the response may be deemed waived.

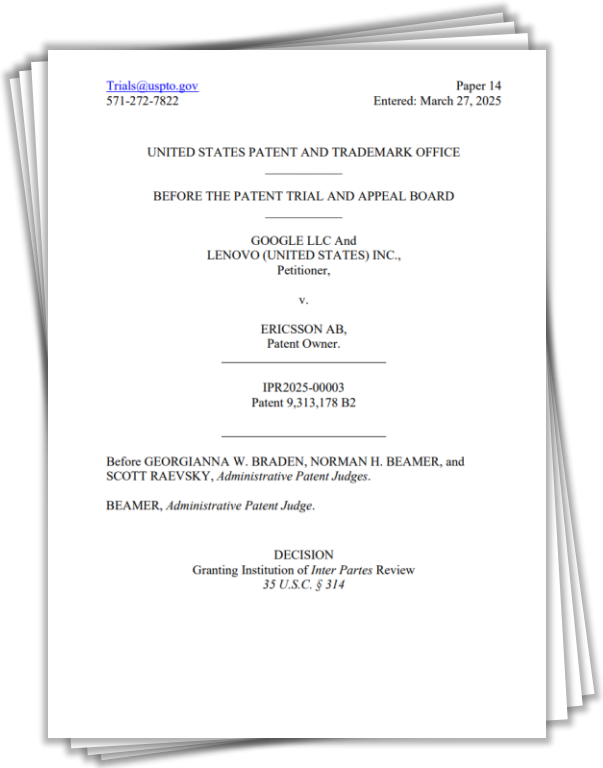
IPR2025-00003 Paper 15 at 9; *see* IPR2025-00004 Paper 14 at 9

IPR2025-00003 PO Sur-Reply:

in light of both items of information. *Id.* Patent Owner specifically demonstrated that in the flow diagram of Figure 3, which defines the "detecting" limitation of the claims, the client must ***always*** "check for key change notification" as stated in step 308. POR at 46; Fig. 3; Ex. 2010 ¶ 107. That step is not optional. *Id.*; Ex. 1001 at 10:39-42. The specification further teaches that at step 310, the client must check ***both*** the expiration time of the current key and any key change notification in order to detect the correct key rotation boundary for that key. POR at 45-46; Ex. 1001 at 11:2-7; Ex. 2010 ¶ 109. Indeed, the '178 Patent never teaches that identifying or

IPR2025-00003 PO Sur-Reply, 21-22

PO's Sur-Reply Argument Attempts to Import FIG. 3 Into Claim



Trials@uspto.gov
571-272-7822

Paper 14
Entered: March 27, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC And
LENOVO (UNITED STATES) INC.,
Petitioner,

v.

ERICSSON AB,
Patent Owner.

IPR2025-00003
Patent 9,313,178 B2

Before GEORGIANNA W. BRADEN, NORMAN H. BEAMER, and SCOTT RAEVSKY, *Administrative Patent Judges*.

BEAMER, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

IPR2025-00003
Institution Decision
(Paper 14)

We are not persuaded at this stage by Patent Owner's interpretation of the detecting requirement. As discussed above, that interpretation hinges on the assumption that "detecting" in the claim limitation at issue only refers to detecting rotation boundaries that occur between normal rotation boundaries — *i.e.*, key rotations triggered by security issues or other specific events, rather than normal key rotations due to expiration of the current key.

This construction, however, improperly limits the scope of the claim to one aspect of the disclosed embodiment of the '178 patent that deals with the special case of key changes requested for security reasons outside of any fixed duration lifespan. Ex. 1001, 10:40–42. Considering, as we must, the disclosure of the '178 patent as a whole, the scope of the disclosure is directed broadly to key rotation in general, whether due to scheduled key expiration times or otherwise. *Id.* at code (57), Fig. 3, 1:63–65, 2:23–25, 3:26–28, 9:47–49; *see also Superguide Corp. v. DirecTV Enter., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004) ("Though understanding the claim language may be aided by explanations contained in the written description, it is important not to import into a claim limitations that are not part of the claim. For example, a particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment").

IPR2025-00003 Inst. Dec., 20-24

Patent Owner's Disputes (IPR2025-00003 Only)

IPR2025-00003 POR, Table of Contents

1. The Petition does not meet "the content information including content encryption keys. . ." as recited in all claims

2. The Petition does not meet "content encryption *key identifiers*" as recited in all claims

3. The Petition's expiration time theory does not meet "detecting content encryption key rotation boundaries"

4. The Petition's notification theory does not meet the "issuing requests" requirement of all challenged claims



IPR2025-00003 POR, Table of Contents

Patent Owner's "Issuing Requests" Argument

IPR2025-00003 Pet. Reply:

> PO's fourth argument focuses on the second of Peterka's two CEK rotation boundary detection methods—monitoring the content stream for a signal informing the client that a new key needs to be used for decryption. POR, 52-55. PO's argument

> PO's argument that "Peterka's 'pull' model…provides no mechanism for a client to reliably request and obtain the necessary 'new content key' ***before*** the client has received a signal to change keys" (POR, 53) contradicts PO's ITC argument that [1D]/[16E] and [1E]/[16F] did not need to occur in the recited order. Pet., 34 n.5. The ITC ***agreed with PO's*** pre-POR position, finding that neither the claims nor the specification supported requiring the steps to occur in order. EX-1032, 21-25; EX-1043. And, as Petitioner explained, even if that step order were required, Peterka's detection of content encryption boundaries by monitoring the expiration of keys satisfies that order. Pet., 34 n.5.

IPR2025-00003 Pet. Reply, 25-26

IPR2025-00003 Pet. Reply:

PO's argument that Peterka's "pull" model for key distribution is "incompatible with Peterka's signaled key change method" (POR, 55; *see* POPR, 23) was abandoned by PO during the ITC litigation. POPR Reply, 5; EX-1036, 56. Regardless, as the Petition explained, the two processes ***are*** compatible. PO conflates two separate, orthogonal concepts disclosed in Peterka—one which allows a client to ***acquire*** new keys before they are needed for decryption, and one which allows a client to ***apply*** keys to decrypt a stream of content at the correct time. Peterka teaches a client that does both. Pet., 11-12 (citing Wechselberger, ¶49); Pet., 33-34 (citing Wechselberger, ¶¶115-117). And Peterka expressly describes sending clients information for ***both*** detection operations in one key distribution message—i.e., key lifetime (for monitoring key expirations) and a key parity bit (for comparing against key change signals in the stream). Peterka, [0121] (cited at Pet., 34).

IPR2025-00003 Pet. Reply, 26

Patent Owner's Conflation of Processes

IPR2025-00003 Pet. Reply:

> Regardless, as the Petition explained, the two processes ***are*** compatible. PO conflates two separate, orthogonal concepts disclosed in Peterka—one which allows a client to ***acquire*** new keys before they are needed for decryption, and one which allows a client to ***apply*** keys to decrypt a stream of content at the correct time. Peterka teaches a client that does both. Pet., 11-12 (citing Wechselberger, ¶49); Pet.,

IPR2025-00003 Pet. Reply, 26

conflates two separate, orthogonal concepts disclosed in Peterka

IPR2025-00003 PO Sur-Reply:

> Petitioner's Reply does not and cannot dispute that Peterka's pull embodiment only relies on monitoring key expiration times in order to change content keys. Peterka's pull embodiment thus cannot meet limitation [1D]. POR at

IPR2025-00003 PO Sur-Reply, 23

Patent Owner's Revised Motions to Amend

US 9,313,178 B2

21. (Substitute for claim 1, if found unpatentable)

[21.1P] A method for handling secure distribution of content for over-the-top media delivery comprising:

[21.1] initiating a media playback request and receiving a playback request response;

[21.2] parsing content information from the playback request response, the content information including content encryption keys, content encryption key identifiers each assigned to an associated content encryption key, and content encryption key expiration times, said content encryption key identifiers each uniquely identifying each associated content encryption key from every other content encryption key for the entire duration of a media playback, said media playback corresponding to the media playback request response;

[21.3] retrieving content and manifest files from a content delivery server;

[21.3A] applying a first key for content decryption, said first key having a first expiration time defining a time-based content encryption key rotation boundary;

[21.4] detecting a notification, the notification including a notification-based content encryption key rotation boundary between periods of use of different content encryption keys in decrypting retrieved content, wherein the notification requires expiration of said first content encryption key earlier than said time-based content encryption key rotation boundary for said first key and after said notification-based content encryption key rotation boundary for said first key;

[21.5] issuing requests to a license server in response to detecting said notification-based content encryption key rotation boundary ahead of said time-based content encryption key rotation boundary for said first key to retrieve a second content encryption key to be used after ~~a~~ the notification-based content encryption key rotation boundary for said first key and before said time-based content encryption key rotation boundary for said first key is reached; and

[21.6] applying the second key for content decryption after the notification-based content encryption key rotation boundary for said first key and before said time-based content encryption key rotation boundary for said first key is reached.

US 11,122,313 B2

21. (Substitute for claim 1, if found unpatentable)

[21.P] A method for handling secure distribution of live video content for over-the-top media delivery comprising:

[21.1] sending a request for live media playback,

[21.2] receiving a live media playback request response, the live media playback request response comprising content encryption keys and content encryption key identifiers each assigned to an associated content encryption key;

[21.3] receiving encrypted live media content and manifest files from a content delivery server, wherein the encrypted live media content comprises one or more content encryption key rotation boundaries wherein each content encryption key rotation boundary is associated with a change to a different content encryption key to decrypt the received encrypted live media content and wherein said content encryption key identifiers each uniquely identify each associated content encryption key from every other content encryption key for the entire duration of the encrypted live media content;

[21.4] applying a first content encryption key to the encrypted live media content before a first time-based content encryption key rotation boundary, the first content encryption key having a first expiration time;

[21.5] prior to reaching the first time-based content encryption key rotation boundary, and in response to receiving a notification to expire said first content encryption key after a notification-based content encryption key boundary and before said first time-based content encryption key rotation boundary, requesting and obtaining a second content encryption key, the second content encryption key to be used after the notification-based content encryption key boundary and before the first time-based content encryption key rotation boundary is reached; and

[21.6] applying the second content encryption key for content decryption after the notification-based content encryption key boundary for the first key and before the first time-based content encryption key rotation boundary is reached.

Original Claims' "Before/After" Requirement

US 9,313,178 B2

issuing requests to a 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

applying the second key for content decryption after the key rotation boundary is reached.

the IMTA claims did. *See* PG, 4-5. Original claim 1 recited one "key rotation boundary" (hereafter, "***Boundary***") and required two actions relative to that claimed ***Boundary***: (1) "issuing requests to a license server ***ahead of*** a [***Boundary***] to retrieve a second [CEK]" and (2) "applying the second key for content decryption ***after*** the [***Boundary***] is reached." EX1001, claim 1.

IPR2025-00003 Pet. Opp. to RMTA, 2

US 11,122,313 B2

prior to reaching the first key rotation boundary, obtaining a second content encryption key, the second content encryption key to be used after the first content encryption key rotation boundary is reached; and

applying the second content encryption key for content decryption after the key rotation boundary is reached.

the IMTA claims did. *See* PG, 4-5. Original claim 1 recited a first "key rotation boundary" (hereafter, "***Boundary***") and required two actions relative to that claimed ***Boundary***: (1) "***prior to*** reaching the [***Boundary***], obtaining a second [CEK]" and (2) "applying the second [CEK] for content decryption ***after*** the [same ***Boundary***] is reached." EX1001, claim 1.

IPR2025-00004 Pet. Opp. to RMTA, 2

RMTA Claims Remove "Before"/"After" Requirement

US 9,313,178 B2

> As demonstrated, there is now no recited boundary (as existed in the original claims) for which the step of "issuing requests" must occur ***ahead of a Boundary*** ***and*** the step of "applying" the second CEK must occur ***after that same Boundary***. The RMTA claims are thus broader than the original claims in at least this respect. *Pannu v. Storz Instruments, Inc.*, 258 F.3d 1366, 1371 (Fed. Cir. 2001) ("[A] claim

IPR2025-00003 Pet. Opp. to RMTA, 4

Original '178 claims

issuing requests to a 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

applying the second key for content decryption after the key rotation boundary is reached.

RMTA '178 claims

[21.5] issuing requests to a license server in response to detecting said notification-based content encryption key rotation boundary ahead of said time-based content encryption key rotation boundary for said first key to retrieve a second content encryption key to be used after ~~a~~ the notification-based content encryption key rotation boundary for said first key and before said time-based content encryption key rotation boundary for said first key is reached; and

[21.6] applying the second key for content decryption after the notification-based content encryption key rotation boundary for said first key and before said time-based content encryption key rotation boundary for said first key is reached.

RMTA Claims Remove "Before"/"After" Requirement

US 9,313,178 B2

> As demonstrated, there is now no recited boundary (as existed in the original claims) for which the step of "issuing requests" must occur ***ahead of a Boundary*** ***and*** the step of "applying" the second CEK must occur ***after that same Boundary***. The RMTA claims are thus broader than the original claims in at least this respect. *Pannu v. Storz Instruments, Inc.*, 258 F.3d 1366, 1371 (Fed. Cir. 2001) ("[A] claim

IPR2025-00003 Pet. Opp. to RMTA, 4

Original '178 claims

issuing requests to a 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

applying the second key for content decryption after the key rotation boundary is reached.

RMTA '178 claims

[21.5] issuing requests to a license server in response to detecting said notification-based content encryption key rotation boundary ahead of said time-based content encryption key rotation boundary for said first key to retrieve a second content encryption key to be used after ~~a~~ the notification-based content encryption key rotation boundary for said first key and before said time-based content encryption key rotation boundary for said first key is reached; and

[21.6] applying the second key for content decryption after the notification-based content encryption key rotation boundary for said first key and before said time-based content encryption key rotation boundary for said first key is reached.

RMTA Claims Remove "Before"/"After" Requirement

US 11,122,313 B2

> As demonstrated, there is now no recited boundary (as existed in the original claims) for which the step of "obtaining a second CEK" must occur ***prior to the Boundary*** ***and*** the step of "applying" the second CEK must occur ***after that same Boundary***. The RMTA claims are thus broader than the original claims in at least this respect. *Pannu v. Storz Instruments, Inc.*, 258 F.3d 1366, 1371 (Fed. Cir. 2001)

IPR2025-00004 Pet. Opp. to RMTA, 4

Original '313 claims

prior to reaching the first key rotation boundary, obtaining a second content encryption key, the second content encryption key to be used after the first content encryption key rotation boundary is reached; and

applying the second content encryption key for content decryption after the key rotation boundary is reached.

RMTA '313 claims

[21.5] prior to reaching the first time-based content encryption key rotation boundary, and in response to receiving a notification to expire said first content encryption key after a notification-based content encryption key boundary and before said first time-based content encryption key rotation boundary, requesting and obtaining a second content encryption key, the second content encryption key to be used after the notification-based content encryption key boundary and before the first time-based content encryption key rotation boundary is reached; and

[21.6] applying the second content encryption key for content decryption after the notification-based content encryption key boundary for the first key and before the first time-based content encryption key rotation boundary is reached.

RMTA Claims Remove "Before"/"After" Requirement

US 11,122,313 B2

> As demonstrated, there is now no recited boundary (as existed in the original claims) for which the step of "obtaining a second CEK" must occur ***prior to the Boundary and*** the step of "applying" the second CEK must occur ***after that same Boundary***. The RMTA claims are thus broader than the original claims in at least this respect. *Pannu v. Storz Instruments, Inc.*, 258 F.3d 1366, 1371 (Fed. Cir. 2001)

IPR2025-00004 Pet. Opp. to RMTA, 4

Original '313 claims

prior to reaching the first key rotation boundary, obtaining a second content encryption key, the second content encryption key to be used after the first content encryption key rotation boundary is reached; and

applying the second content encryption key for content decryption after the key rotation boundary is reached.

RMTA '313 claims

[21.5] prior to reaching the first time-based content encryption key rotation boundary, and in response to receiving a notification to expire said first content encryption key after a notification-based content encryption key boundary and before said first time-based content encryption key rotation boundary, requesting and obtaining a second content encryption key, the second content encryption key to be used after the notification-based content encryption key boundary and before the first time-based content encryption key rotation boundary is reached; and

[21.6] applying the second content encryption key for content decryption after the notification-based content encryption key boundary for the first key and before the first time-based content encryption key rotation boundary is reached.

PO's RMTA Reply Re: Broadening

US 9,313,178 B2

[21.4] detecting a notification, the notification including a notification-based content encryption key rotation boundary between periods of use of different content encryption keys in decrypting retrieved content, wherein the notification requires expiration of said first content encryption key earlier than said time-based content encryption key rotation boundary for said first key and after said notification-based content encryption key rotation boundary for said first key;

[21.5] ***issuing requests*** to a license server ***in response to*** detecting said notification-based content encryption key rotation boundary ahead of said time-based content encryption key rotation boundary for said first key **to retrieve** a second content encryption key to be used **after** the notification-based content encryption key rotation **boundary** for said first key and before said time-based content encryption key rotation boundary for said first key is reached; and

IPR2025-00003 PO's RMTA Reply, 2

PO's RMTA Reply:

The revised amended claims thus require (1) "detecting a ***notification***" that specifies an upcoming notification-based content encryption key rotation boundary that is earlier than a previously provided time-based key rotation boundary; (2) the

IPR2025-00003 PO's RMTA Reply, 2

The revised amended claims thus require that the second CEK be requested "in response to" detection of an upcoming notification-based boundary, *i.e.*, ***before*** that boundary, and that the second CEK be applied ***after*** that same boundary. The

IPR2025-00003 PO's RMTA Reply, 3

rotation. In limitation 21.4, a ***notification*** provides an upcoming notification-based CEK boundary. Per 21.5, the second CEK must be requested "in response to" ***detecting*** that upcoming boundary, and thus ***before*** that boundary. Per 21.6, the

IPR2025-00003 PO's RMTA Reply, 3-4

PO's RMTA Reply Re: Broadening

US 11,122,313 B2

[21.5] prior to reaching the first time-based content encryption key rotation boundary, and ***in response to*** receiving a notification to expire said first content encryption key ***after*** a notification-based content encryption key ***boundary*** and before said before said first time-based content encryption key rotation boundary, ***requesting and obtaining a second content encryption key***, the second content encryption key to be used ***after*** the notification-based content encryption key ***boundary*** and before the first time-based content encryption key rotation boundary is reached; and

[21.6] ***applying*** the second content encryption key for content decryption ***after*** the notification-based content encryption key ***boundary*** for the first key and before the first time-based content encryption key rotation boundary is reached.

IPR2025-00004 PO's RMTA Reply, 2

PO's RMTA Reply:

The revised amended claims thus require that the second CEK be obtained "in response to" a notification of an upcoming notification-based boundary, *i.e.*, ***before*** that boundary, and that the second CEK be applied ***after*** that boundary. The

IPR2025-00004 PO's RMTA Reply, 3

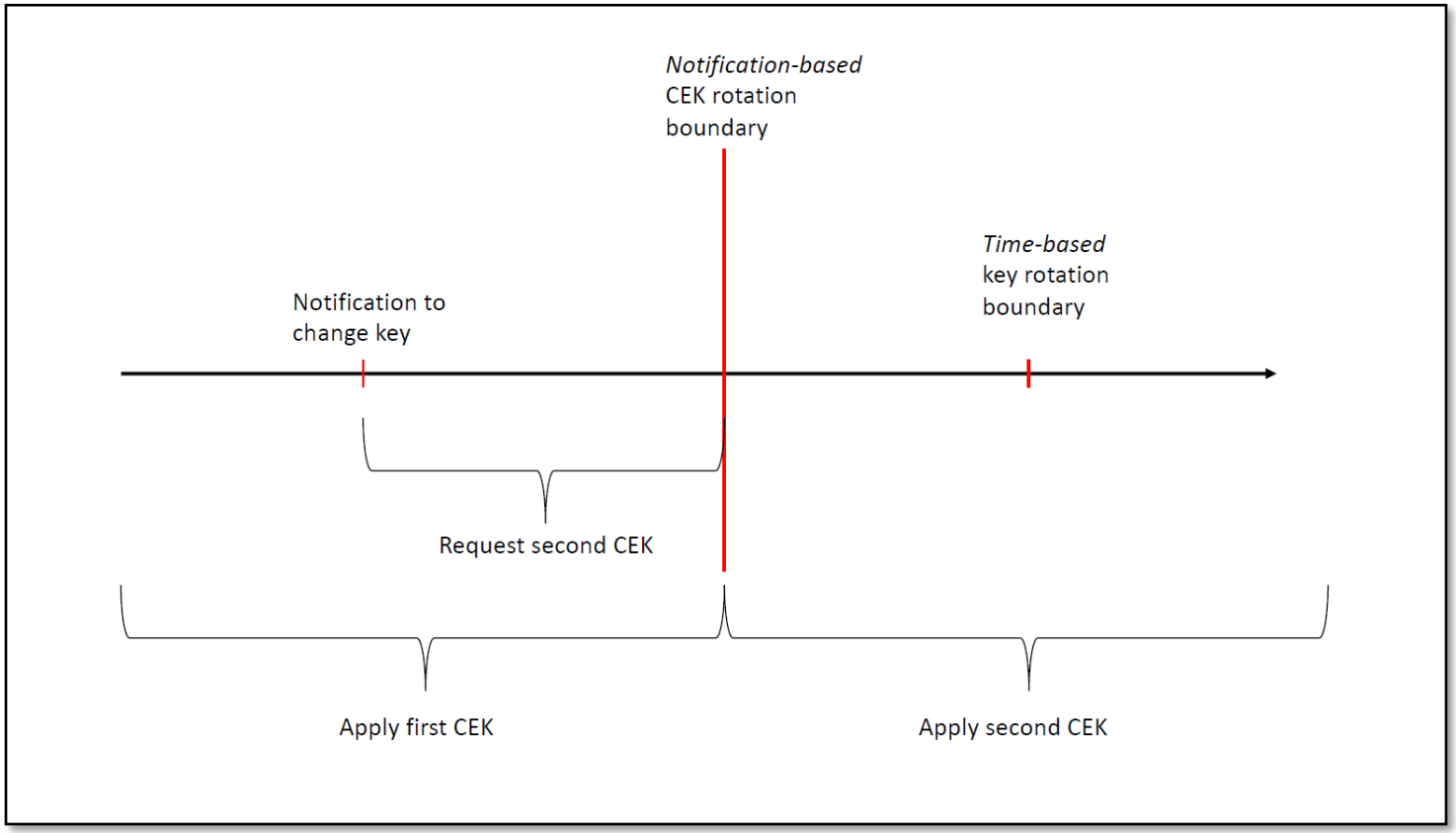
rotation. In limitation 21.5, a ***notification*** provides an upcoming notification-based CEK boundary. This limitation further requires that the second CEK must be requested and obtained "in response to" ***receiving a notification of*** that upcoming boundary, and thus ***before*** that boundary. Per 21.6, the second CEK must then be

IPR2025-00004 PO's RMTA Reply, 3-4

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

PO Illustrates Only One Scenario that Meets RMTA Claims

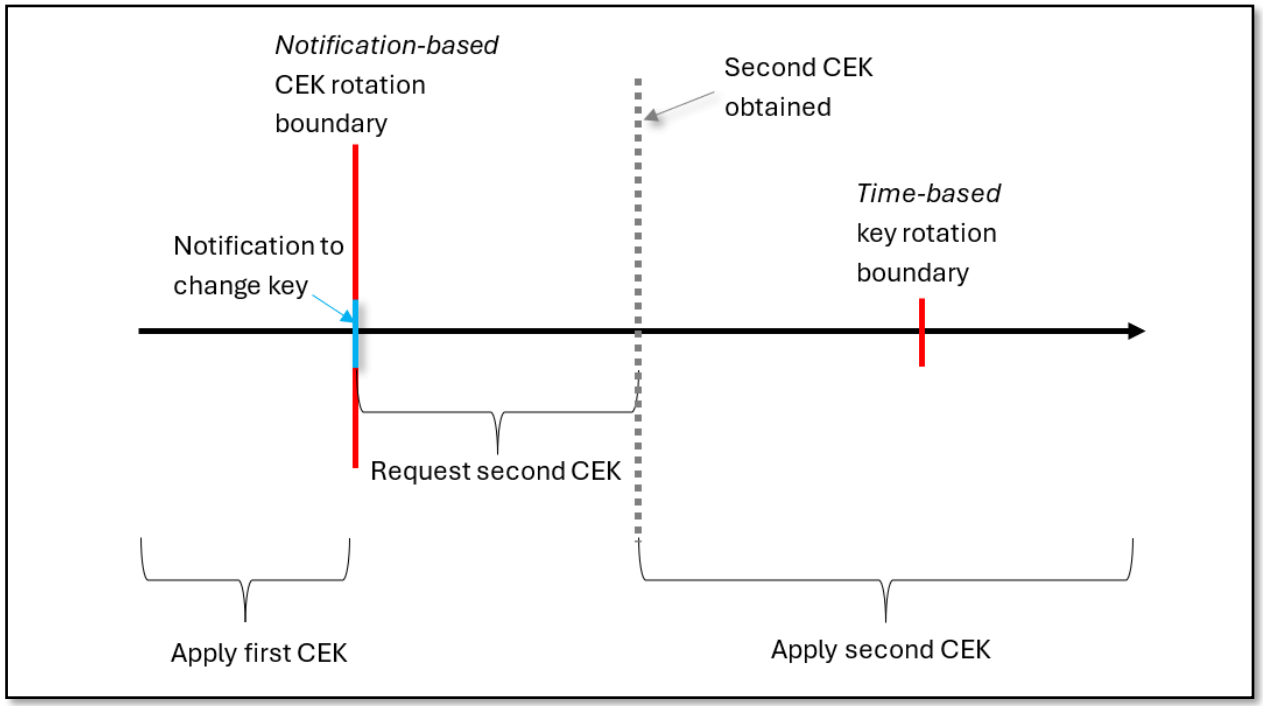
PO's RMTA Replies:



IPR2025-00003 PO's RMTA Reply, 3; IPR2025-00004 PO's RMTA Reply, 3

Additional Scenarios Met by RMTA Claims

Pet.'s RMTA Sur-Replies:

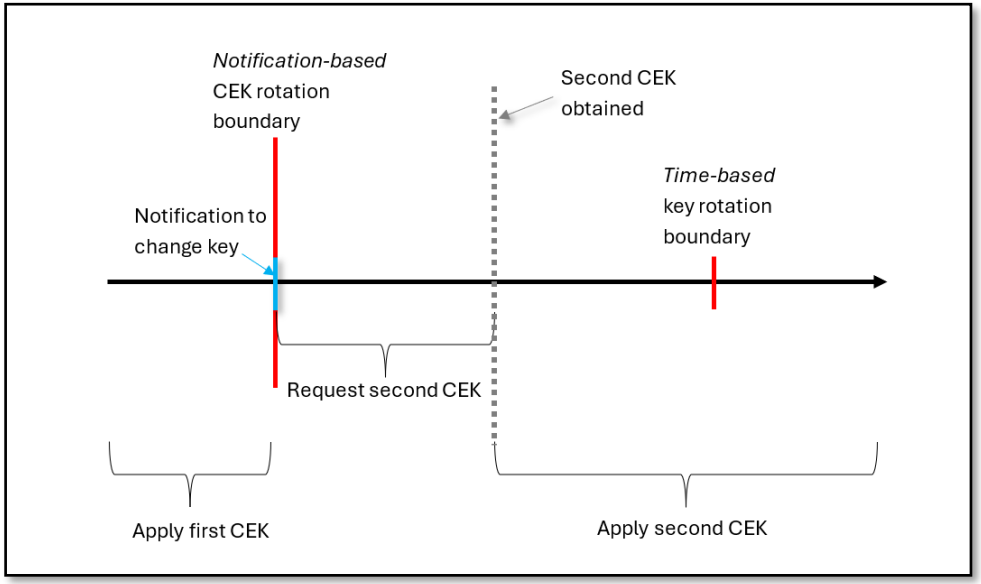


Nothing in the RMTA claims excludes a time gap between the client applying the first and second CEKs for decryption—a known issue (e.g., Suzuki, [0008]-[0010]; EX1001, 11:41-45) that would be expected, e.g., for unscheduled key changes that occur due to security compromise. The above scenario thus meets RMTA limitations

IPR2025-00003 Pet.'s RMTA Sur-Reply, 4; *see* IPR2025-00004 Pet.'s RMTA Sur-Reply, 4

Additional Scenarios Met by RMTA Claims

Pet.'s RMTA Sur-Replies:



occur due to security compromise. The above scenario thus meets RMTA limitations [21.5]-[21.6]: requests for the second CEK start ***at*** the notification-based CEK rotation boundary (***in response to detecting*** it), and the second CEK is applied for decryption ***after*** the notification-based CEK rotation boundary. Further, requests for the second CEK occur ***ahead of*** the time-based CEK rotation boundary, and the second CEK is applied for decryption ***before*** the time-based CEK rotation boundary.

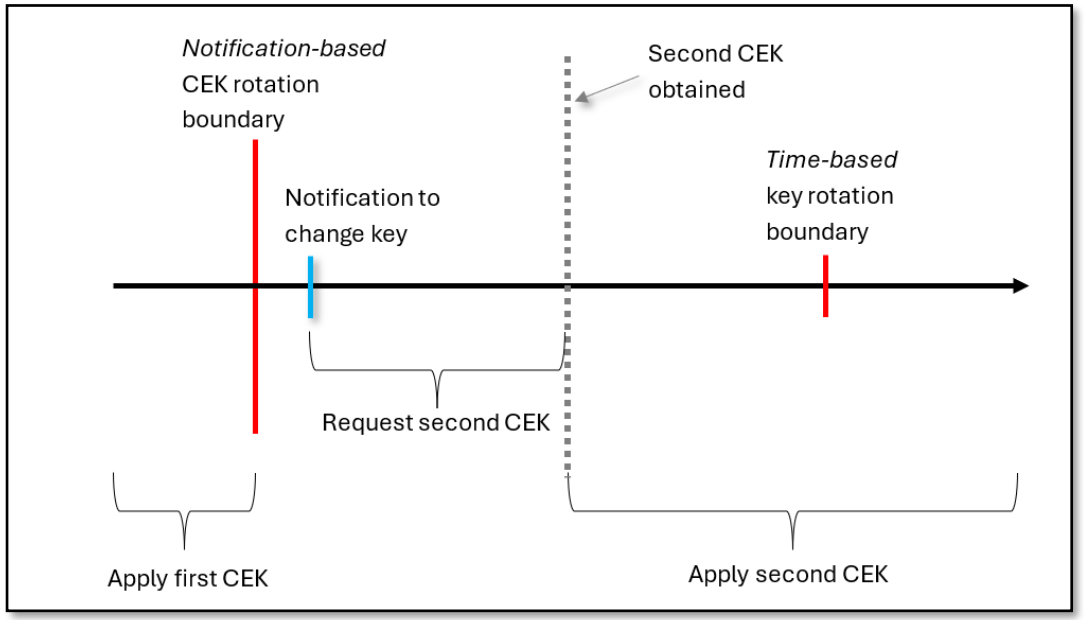
By contrast, the original claims' undisputed ***ahead of/after*** requirement is ***not*** met because there is no one boundary "before which the second CEK must be requested, ***and*** 'after' which it must be applied." Reply, 1.

IPR2025-00003 Pet.'s RMTA Sur-Reply, 4; *see* IPR2025-00004 Pet.'s RMTA Sur-Reply, 4

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Additional Scenarios Met by RMTA Claims

Pet.'s RMTA Sur-Replies:



Above, requests for the second CEK start ***after*** the notification-based CEK rotation boundary (***in response to detecting*** it), and the second CEK is applied for decryption ***after*** the notification-based CEK rotation boundary. Further, requests for the second CEK occur ***ahead of*** the time-based CEK rotation boundary, and the second CEK is applied for decryption ***before*** the time-based CEK rotation boundary. This scenario thus meets RMTA limitations [21.5]-[21.6] but does not meet the original claims' undisputed ***ahead of/after*** requirement, because there is no boundary "before which the second CEK must be requested, ***and*** 'after' which it must be applied." Reply, 1.

IPR2025-00003 Pet.'s RMTA Sur-Reply, 5; *see* IPR2025-00004 Pet.'s RMTA Sur-Reply, 5

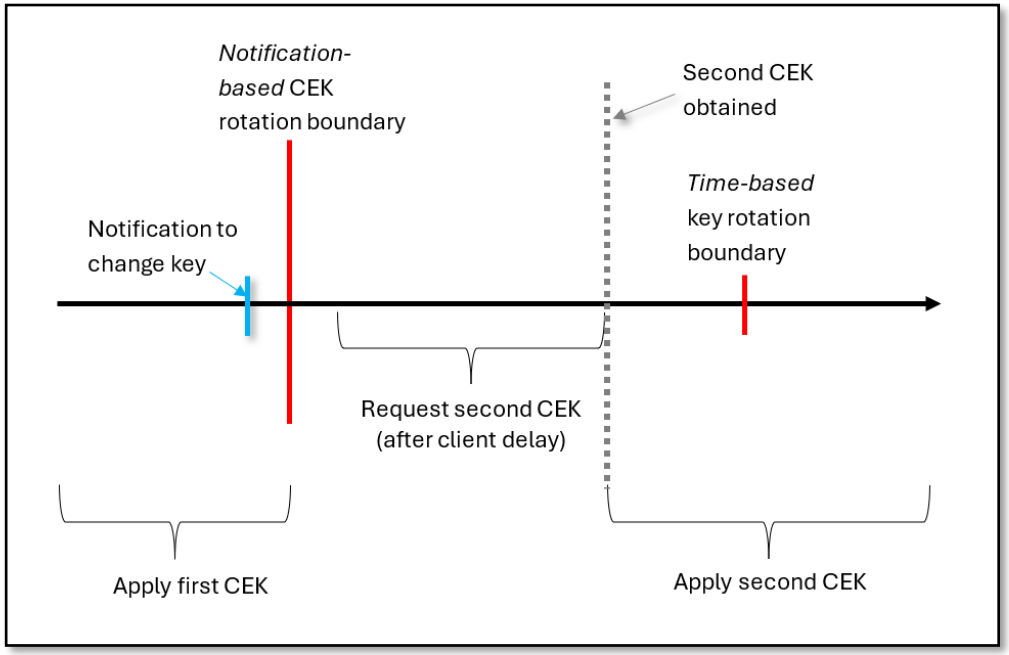
Additional Scenarios Met by RMTA Claims

IPR2025-00003 Pet.'s RMTA Sur-Reply, 3-6
IPR2025-00004 Pet.'s RMTA Sur-Reply, 3-6

Pet.'s RMTA Sur-Replies:

> Moreover, ***even if*** PO had amended its claims to ***require*** the "notification" in [21.4] to "includ[e]" an "upcoming" boundary—as PO falsely alleges it did already (Reply, 2, 3, 4)—the RMTA claims would ***still*** extend to scope that was excluded by the original claims. This can be seen in the below illustration—where the client requests a second CEK "in response to" the "notification to change key" but the requests are delayed (due to, e.g., processing latency) at the client.

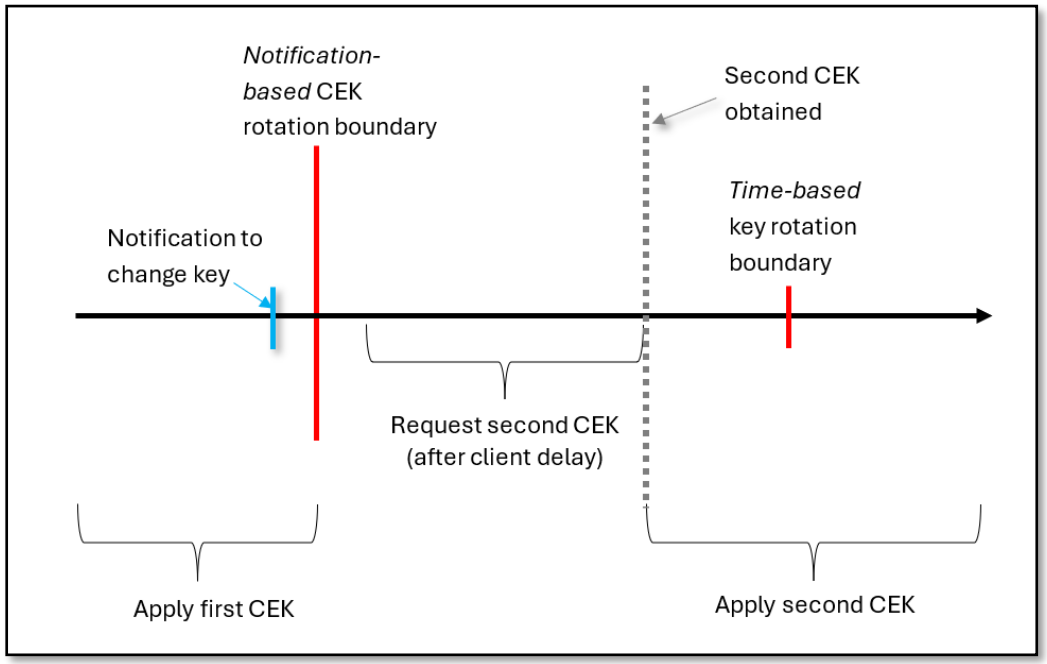
> Nothing in the RMTA claims excludes requesting a second CEK (***in response to detecting*** the notification-based boundary) ***after a delay***. Thus, the above scenario—



IPR2025-00003 Pet.'s RMTA Sur-Reply, 5-6; *see* IPR2025-00004 Pet.'s RMTA Sur-Reply, 5-6

Additional Scenarios Met by RMTA Claims

Pet.'s RMTA Sur-Replies:



detecting the notification-based boundary) *after a delay*. Thus, the above scenario—where both the requests for and application of the second CEK occur ***after*** the notification-based CEK rotation boundary and both the requests for and application of the second CEK occur ***before*** the time-based key rotation boundary—meets RMTA limitations [21.5]-[21.6]. It, however, does ***not*** meet the original claims' undisputed ***ahead of/after*** requirement, because there is no boundary "before which the second CEK must be requested, ***and*** 'after' which it must be applied." Reply, 1.

IPR2025-00003 Pet.'s RMTA Sur-Reply, 6; *see* IPR2025-00004 Pet.'s RMTA Sur-Reply, 6

RMTA Claims Introduce New Matter

IPR2025-00003 Pet. Opp. to RMTA, 5-7
IPR2025-00004 Pet. Opp. to RMTA, 5-7

RMTA '178 claims

[21.6] applying the second key for content decryption after the notification-based content encryption key rotation boundary for said first key and before said time-based content encryption key rotation boundary for said first key is reached.

[21.6] applying the second key for content decryption after the notification-based content encryption key rotation boundary for said first key and before said time-based content encryption key rotation boundary for said first key is reached.

RMTA '313 claims

[21.6] applying the second content encryption key for content decryption after the notification-based content encryption key boundary for the first key and before the first time-based content encryption key rotation boundary is reached.

[21.6] applying the second content encryption key for content decryption after the notification-based content encryption key boundary for the first key and before the first time-based content encryption key rotation boundary is reached.

None do. Every original claim required that a second key be applied for decryption ***after*** the rotation boundary that demarcated when the issuing requests step occurred, while no original claim required that a second key be applied for decryption ***before*** the demarcating rotation boundary. The Board recognized this. PG, 9. Likewise, the RMTA's cited paragraphs do not support the [21.6]/[33.7] amendments. Paragraph 5 mimics original claim 1, stating the device "applies the

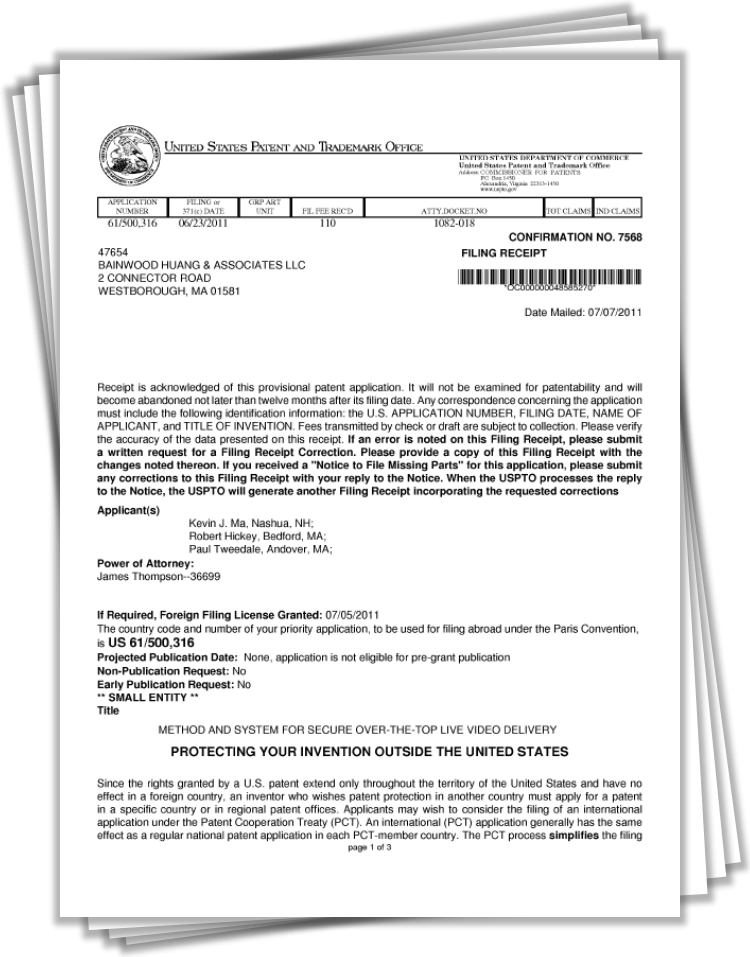
* * *

Nor would such a requirement make sense. In the "normal period-based expiration" case, the second key is applied for decryption ***after*** a rotation boundary. In the "explicit key change notification" case, replacement keys are applied independent of and, agnostic to, key rotation boundaries. Beyond PO's conclusory table, PO makes no attempt to demonstrate that a POSA would have understood the specification to support the new limitations. [21.6] and [33.7] violate § 316(d)(3).

IPR2025-00003 Pet. Opp. to RMTA, 6-7;
see IPR2025-00004 Pet. Opp. to RMTA, 6-7

Patent Owner's Citations Show the RMTA Claims Introduce New Matter

IPR2025-00003 PO's RMTA Reply, 6-7
IPR2025-00004 PO's RMTA Reply, 6-7



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

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

page 1 of 3

'316 Provisional
(IPR2025-00003 EX-2008; IPR2025-00004 EX-2005)

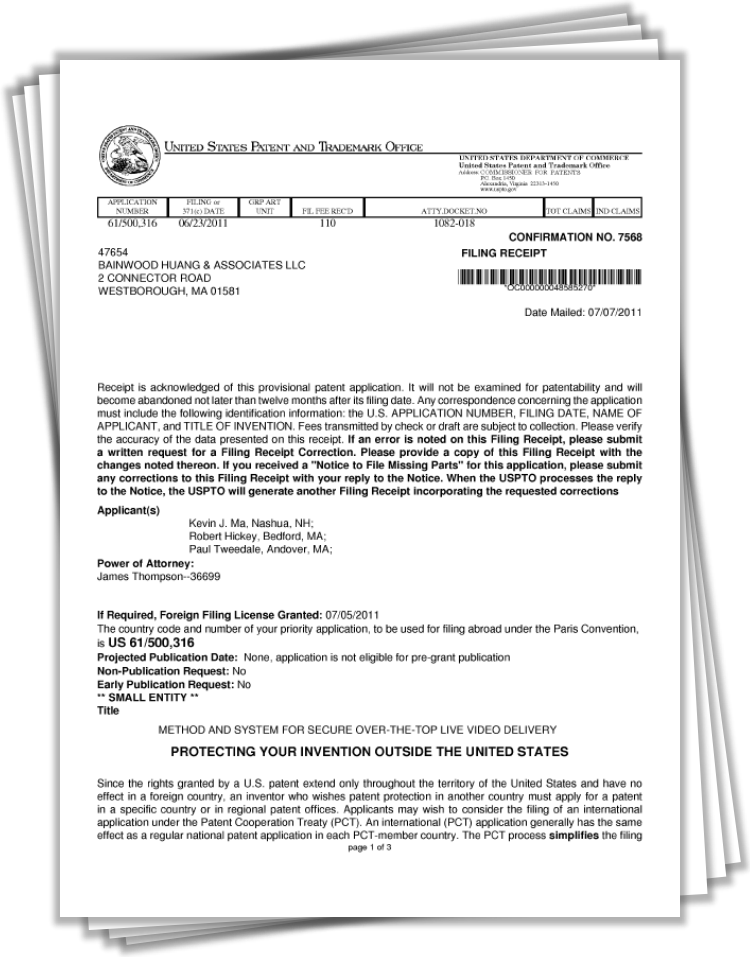
PO's RMTA Replies

> Moreover, the provisional teaches that the workflow manager "may initiate content encryption key rotation at any time, outside of the fixed duration lifespan of the existing key." Ex. 2008 at 5. The phrase "at ***any*** time" necessarily discloses a time ***before*** the original "fixed duration lifespan of the existing key," thus providing written description for limitations 21.6 and 33.7.

IPR2025-00003 PO's RMTA Reply, 6;
see IPR2025-00004 PO's RMTA Reply, 6-7

Patent Owner's Citations Show the RMTA Claims Introduce New Matter

IPR2025-00003 PO's RMTA Reply, 6-7
IPR2025-00004 PO's RMTA Reply, 6-7



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

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

page 1 of 3

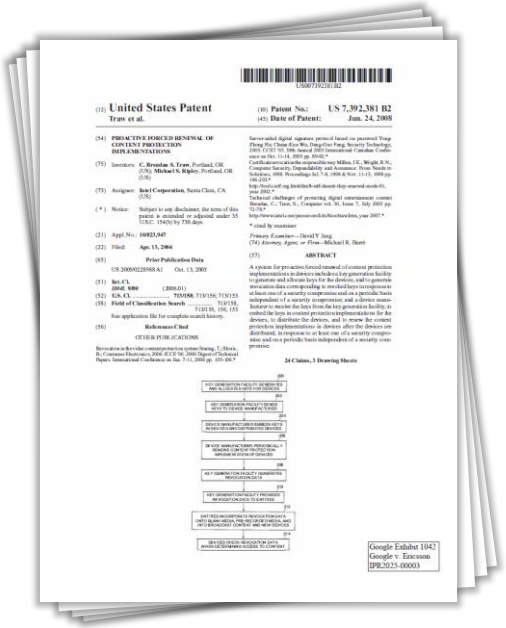
'316 Provisional
(IPR2025-00003 EX-2008; IPR2025-00004 EX-2005)

PO's RMTA Replies

Here, the provisional application (Ex. 2008) teaches that in the embodiment of Fig. 3 at step 304, the client 110 "retrieves and parses the content information, including . . . content key *expiration*." Ex. 2008 at 11 (emphasis added). Thus, in the embodiment of Figure 3, content encryption keys initially come with a content key expiration point, which is identified by the client at step 304. The provisional further teaches that *later on*, at step 308, "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." Ex. 2008 at 12 (emphasis added). The provisional thus necessarily discloses that a key change notification can *alter* the original point of key rotation that was initially defined for a given key. The provisional further teaches that the unscheduled key change notification "describes the expiration of the previous key." *Id.* Thus, contrary to Petitioner's assertion, the disclosure's

IPR2025-00003 PO's RMTA Reply, 6; *see*
IPR2025-00004 PO's RMTA Reply, 6

Traw (EX-1042)



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

(10) **Patent No.: US 7,392,381 B2**
(45) **Date of Patent: Jun. 24, 2008**

(54) **PROACTIVE FORCED RENEWAL OF CONTENT PROTECTION IMPLEMENTATIONS**

(75) Inventors: **C. Brendan S. Traw**, Portland, OR (US); **Michael S. Ripley**, Portland, OR (US)

(73) Assignee: **Intel Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 730 days.

(21) Appl. No.: **10/823,947**

(22) Filed: **Apr. 13, 2004**

(65) **Prior Publication Data**

US 2005/0229008 A1 Oct. 13, 2005

(51) **Int. Cl.**
H04L 9/00 (2006.01)

(52) **U.S. Cl.** 713/168; 713/156; 713/153

(58) **Field of Classification Search** 713/168, 713/155, 156, 153
See application file for complete search history.

(56) **References Cited**
OTHER PUBLICATIONS

Revocation in flat video content protection system Shuang, T.; Slavik, P.; Consumer Electronics, 2004. ICCE '04. 2004 Digest of Technical Papers. International Conference on Jan. 7-11, 2004 pp. 103-104.*

Server-aided digital signature protocol based on password Yong-Zhong Fu; Chuan-Kun Wu; Dong-Gen Feng; Security Technology, 2003. CCST 03. 36th Annual 2003 International Carnahan Conference on Oct. 11-14, 2003 pp. 59-63.*

Certification revocation the responsible way Miller, J.K.; Wright, R.N.; Computer Security, Dependability and Assurance: From Needs to Solutions, 1998. Proceedings Jul. 7-9, 1998 & Nov. 11-13, 1998 pp. 72-79.*

http://xrml.xrml.org. Institute's off-shoot chip renewal cards 01, year 2002.*

Technical challenges of protecting digital entertainment content Brundle, C.; Traw, S.; Computer vol. 36, Issue 7, July 2003 pp. 72-74.*

http://www.intel.com/pressroom/archive/backfiles_year 2007.*

* cited by examiner

Primary Examiner—David Y. Jung
(74) *Attorney, Agent, or Firm*—Michael R. Barré

(57) **ABSTRACT**

A system for proactive forced renewal of content protection implementations in devices includes a key generation facility to generate and allocate keys for the devices, and to generate revocation data corresponding to revoked keys in response to at least one of a security compromise and on a periodic basis independent of a security compromise; and a device manufacturer to receive the keys from the key generation facility, to embed the keys in content protection implementations for the devices, to distribute the devices, and to renew the content protection implementations in devices after the devices are distributed, in response to at least one of a security compromise and on a periodic basis independent of a security compromise.

24 Claims, 3 Drawing Sheets

Google Exhibit 1042
Google v. Ericsson
IPR2025-00003

Traw (EX-1042)

A system for proactive forced renewal of content protection implementations in devices includes a key generation facility to generate and allocate keys for the devices, and to generate revocation data corresponding to revoked keys in response to at least one of a security compromise and on a periodic basis independent of a security compromise; and a device manufacturer to receive the keys from the key generation facility, to embed the keys in content protection implementations for the devices, to distribute the devices, and to renew the content protection implementations in devices after the devices are distributed, in response to at least one of a security compromise and on a periodic basis independent of a security compromise.

EX-1042, Abstract

An embodiment of the present invention is a system wherein revocation of cryptographic keys is used in combination with periodic renewal of compliant content protection implementations in a way that dramatically improves the security of the overall content protection system. In the present invention, devices for accessing protected content must be periodically renewed. In conjunction with the renewal mechanism, revocation is also used to prevent access to content if the devices' keys have been compromised.

EX-1042, 1:65-2:6

Embodiments of the present invention are applicable to security applications in general, but are described herein in terms of their use in a system for protecting content (such as audiovisual entertainment content) against unauthorized access, copying or distribution. The security systems include means for revoking implementations, including but not limited to content protection systems. In the case of a content protection system, embodiments of the present invention may be used by content providers and implementers of consumer electronics devices, especially where those devices may include software for assisting in implementing content protection and wherein the software may be updated via a communication mechanism (such as via the Internet, for example). Such systems employ a cryptographic protocol

EX-1042, 2:15-2:28

Pet. Opps. to RMTAs

> Traw describes two types of key revocation in which current content keys are replaced: (1) periodic/planned key revocation (Traw, 5:33-35, 6:10-12); and (2) non-periodic/unplanned key revocation based on compromised keys, security attacks, or emergency situations (*id.*, 3:65-66, 4:37-39, 5:5-7, 5:37-39, FIG. 2). Messages are transmitted "to users and/or devices announcing" the key revocation. *Id.*, 5:63-65.

IPR2025-00003 Pet. Opp. to RMTA, 9; IPR2025-00004 Pet. Opp. to RMTA, 9

Traw (EX-1042):

> according to an embodiment of the present invention. In this system, revocation of keys may be performed proactively on a periodic basis, rather than only reactively in response to an attack, as in prior systems. A key generation facility 102

EX-1042, 3:65-66

Reasons to Combine Peterka and Traw

Pet. Opps. to RMTAs

> ***First***, Peterka and Traw are in the same field of art.

> ***Second***, Peterka and Traw share common objectives to prevent unauthorized access to content. *Compare* Peterka, [0135]-[0146] (describing "rules and conditions for providing content in a multicasting environment" to authorized clients), *with* Traw, 2:15-19 (describing protecting content from "unauthorized access"). Peterka recognizes the risk of security attacks and provides security mechanisms to protect against them—e.g., periodically rotating keys "at regular intervals," "a time stamp" in key-distribution ECMs "to protect against replay attacks." Peterka, [0105], [0110], [0121]; EX1041, ¶¶265-266. Traw likewise recognizes the benefits of periodic key renewals. *E.g.*, Traw, 3:63-66 ("[R]evocation of keys may be performed proactively on a periodic basis, rather than only reactively in response to an attack.").

IPR2025-00003 Pet. Opp. to RMTA, 9-10; *see* IPR2025-00004 Pet. Opp. to RMTA, 10

Reasons to Combine Peterka and Traw

Pet. Opps. to RMTAs

> ***Third***, POSAs understood well that notwithstanding Peterka's described security mechanisms including key rotation, the security of systems like Peterka's could be improved to address breaches. *See* EX1040 (Villasenor Dep.), 135:20-136:5, 139:7-140:24; *see also id.*, 136:6-25. For example, Traw recognizes the benefits of "non-scheduled revocation" in systems like Peterka's including for keys that "have been compromised" (*id.*, 6:39-49) and to protect against "a more general set of threats" or attacks (*id.*, 6:49-57). Peterka leaves to POSAs' discretion how to rectify a security attack. *See* Peterka, [0110]; EX1041, ¶¶266-267. POSAs understood from Traw that compromised keys should be revoked, including in systems like Peterka with key rotation. Traw, 6:39-56; EX1041, ¶267. POSAs also understood that Traw's security-driven key revocation teachings complement and support Peterka's goal of limiting media access to authorized users—a goal Traw itself shares. EX1041, ¶267.

IPR2025-00003 Pet. Opp. to RMTA, 10-11;
see IPR2025-00004 Pet. Opp. to RMTA, 10-11

PO's Expert Affirmed Reasons to Combine

Villasenor:

Q. Okay. There wasn't any reason back in June 2011 to use both normal period-based key rotation and explicit key change notifications, was there?

A. Well, I would disagree.

In other words, are you saying there's no reason why a system would have needed to do that?

Q. Yeah.

A. Well, no. I don't agree with that assertion.

Villasenor Dep. (EX-1040), 135:20-136:5

So you can sort of have the best of both worlds. You can have the kind of predictability -- with that kind of system, you can have the predictability and kind of mechanized operation of a time-based key rotation while also benefiting from the protections that you get if you have the ability to rotate to cause a boundary to occur earlier than the otherwise scheduled time.

And, again, I gave an example of a half hour. Maybe it's a day or maybe it's a week.

And, you know, obviously the longer it gets, the more benefit -- the more risk there would be that a key would get compromised.

But even if the key rotation is 30 seconds, maybe if it gets compromised, you want to rotate it after 2 seconds and not wait those extra 28 seconds. So it applies across all the time scales.

Villasenor Dep. (EX-1040), 140:7-24

Pet. Opps. to RMTAs:

POSAs thus would have been motivated to improve Peterka's system (*see* EX1040, 135:20-136:5, 139:7-140:24; *see also id.*, 136:6-25) in view of Traw by: (1) providing a notification to clients that a certain key is compromised and requires early expiration (Traw, 5:63-65, 4:62-65) using Peterka's content packet "signaling methods" for key changes (Pet., 11; Peterka, [0116]-[0120]); (2) having the client obtain a replacement key using Peterka's "pull" method (Pet., 11-12; Peterka, [0105]-[0106]) when notified that the current key has been revoked before the originally-scheduled expiration of the compromised key (Traw, 6:18-21); and (3) having the client apply the replacement key for decryption when the replacement key is received, before the originally-scheduled expiration of the compromised key in order to minimize service interruptions (Peterka, [0105]). EX1041, ¶268.

This modified system—"Peterka-Traw"—would have maintained Peterka's overall system while beneficially improving security by including a mechanism to handle successful security attacks—namely, revoking and requiring replacement of a compromised key before it is set to expire (as taught by Traw). EX1041, ¶268.

IPR2025-00003 Pet. Opp. to RMTA, 11-12; *see* IPR2025-00004 Pet. Opp. to RMTA, 11-12

Peterka-Traw Renders Obvious RMTA Claims

Pet. Opps. to RMTAs:

> RMTA claim 21 amends original claim 1. RMTA, Claims App'x, i-ii. Unchanged claim limitations are obvious for the reasons set forth in Ground 1 (Pet, 19-37) and amended limitations are obvious over Peterka-Traw. EX1047, ¶343.

IPR2025-00003 Pet. Opp. to RMTA, 12; *see* IPR2025-00004 Pet. Opp. to RMTA, 12

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Peterka-Traw: Limitation [21.2]

IPR2025-00003 Pet. Opp. to RMTA, 12-15
IPR2025-00004 Pet. Opp. to RMTA, 13-14

Pet. Opps. to RMTAs:

Peterka-Traw includes Peterka's sequence number or timestamp delivered to a client along with a CEK in an ECM/EMM, each of which POSAs understood constitutes a unique CEK identifier that identifies the specific key in the ECM/EMM. Pet., 25-26; Peterka, [0121]; EX1003, ¶¶91-92; EX1041, ¶¶274-277. This understanding of CEK identifier is consistent with the '178 Patent, which likewise describes key identifiers "selected based on" other data such as "a segment number of the prepared content." EX1001, 3:34-35, 4:8-10, 6:1-4, 6:17-19.

IPR2025-00003 Pet. Opp. to RMTA, 13; *see* IPR2025-00004 Pet. Opp. to RMTA, 13

Peterka (EX-1005):

a format for such messages. Under this format, a sequence number or a time stamp to protect against replay attacks is provided. Furthermore, in another field of the EMM and

EX-1005, [0121]

Specifications:

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

'178 Patent, 3:32-36; '313 Patent, 3:40-45

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 seg-

'178 Patent, 4:4-10; '313 Patent, 4:12-19

identifier. In one embodiment, the content encryption key identifiers are based off a next sequential integer value, offset from the previous content encryption key identifier. In another 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 seg-

'178 Patent, 5:63-6:4; '313 Patent, 6:6-14

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Peterka-Traw: Limitation [21.2]

Pet. Opps. to RMTAs:

the content key parsed from an ECM/EMM. *Id.*; Pet. 26; EX1003, ¶94. Traw teaches assigned "key IDs" for targeted revocations. Traw, 3:32-46. Moreover, assigning identifiers (e.g., key numbers) to CEKs to distinguish keys was a well-known key management technique. Suzuki, [0013], [0016], [0030]-[0031], [0043]-[0048], [0080]-[0084], FIG. 5; Pestoni, 12:16-35; EX1003, ¶¶93-96. In systems where multiple keys are utilized (e.g., Peterka-Traw), POSAs would have recognized the need to differentiate between keys, especially for scenarios where a ***single*** compromised key held by multiple clients needed to be targeted for revocation. EX-1047, ¶350 (citing Traw, 3:35, 4:45). Assigning CEK identifiers for such purposes would have constituted implementing known methods (assigned CEK identifiers) to known systems (Peterka-Traw's key rotation system) to achieve predictable results (a key management scheme that distinguishes between keys). *KSR Int'l v. Teleflex*, 550 U.S. 398, 416 (2007); EX1047, ¶350. POSAs would have reasonably expected success using ***assigned*** key identifiers because this was a well-known option for key identifiers. EX1047, ¶351. Thus, Peterka-Traw meets PO's "assigned" requirement

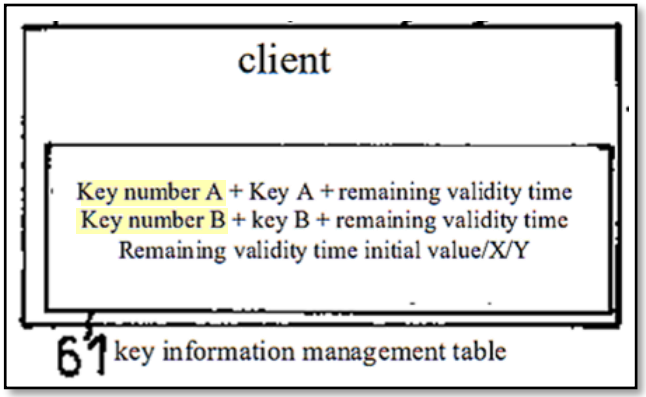
IPR2025-00003 Pet. Opp. to RMTA, 13-14; *see* IPR2025-00004 Pet. Opp. to RMTA, 14

Traw (EX-1042):

cies. For example, in a content protection system based on public key cryptography, revocation may entail distributing a list of key IDs to be revoked, where each revocation list entry may specify either a single key ID or a range (e.g., starting and ending values) of key IDs. For such a system, a particular

EX-1042, 3:32-36

Suzuki (EX-1006):



EX-1006, FIG. 5 (excerpted)

Pestoni (EX-1012):

In various embodiments, playback device **100** may be configured to decrypt each segment **440***a-c* with the respective decryption key of key box **420**. In some embodiments, key box **420** may specify a key identifier for each key within the key box. Likewise, each encrypted segment **440***a-c* may

EX-1012, 12:16-20

Peterka-Traw: ’178 Limitation [21.4]

Pet. Opp. to RMTA:

Regardless, Peterka-Traw satisfies this limitation. EX1047, ¶¶364-366. Traw teaches revoking a key that has been compromised due to a security breach ***before*** that key would ordinarily be rotated (Traw, 3:17-19, 5:29-31, 5:35-39, 6:12-21, 6:39-57) and notifying client devices of such revocations (*id.*, 4:62-65, 5:63-65). EX1047, ¶364. In Peterka-Traw, keys would ordinarily be rotated based on the time-based CEK rotation boundary as described above in [21.3A]. Peterka, [0105], [0110], [0121]; EX1047, ¶365. Further, in Peterka-Traw, notifications of these unscheduled key revocations are transmitted to (and detected by) the client using Peterka's key change signaling methods. EX1047, ¶366; Peterka, [0116]-[0120]. POSAs would understand the notification as a signal to stop using the CEK; it is thus a notification-based CEK rotation boundary. EX1047, ¶366. Peterka-Traw's client thus detects a notification-based CEK rotation boundary where the notification requires expiration of the first CEK earlier than the time-based CEK rotation boundary for the first key and after the notification-based CEK rotation boundary for the first key.

IPR2025-00003 Pet. Opp. to RMTA, 17

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Peterka-Traw: Limitation [21.5]

Pet. Opps. to RMTAs:

EX1047, ¶370. POSAs would have been motivated to implement Peterka-Traw such that when the client detects an unscheduled key revocation (Traw, 3:17-19, 4:63-65, 5:35-65, 6:12-21, 6:39-57) using Peterka's key change signaling methods (Peterka, [0116]-[0120]), the client requests a new key immediately, so that it can be used before the current (compromised) key is set to expire. EX1047, ¶¶371-373. This would minimize the impact of service interruptions. EX1047, ¶373; Peterka, [0105].

IPR2025-00003 Pet. Opp. to RMTA, 18; *see* IPR2025-00004 Pet. Opp. to RMTA, 18

Peterka-Traw: Limitation [21.5]

Pet. Opps. to RMTAs:

PO's attorney argues that neither Peterka nor Traw teach a client requesting a key in response to receiving notice that a key must be changed. RMTA, 16-17. This assertion makes no sense in the context of Peterka, which teaches that under the pull key distribution model relied upon by Petitioner, "the responsibility of determining when a new key is required" is "passed to the client" and "each client requests a new key and is individually responded to by the key distribution server." Peterka, [0106], [0110]. Based on Peterka's teachings, POSAs understood that "in response to" ***any***

IPR2025-00003 Pet. Opp. to RMTA, 18; *see* IPR2025-00004 Pet. Opp. to RMTA, 18

Peterka Teaches Clients Requesting Keys When Needed

Peterka (EX-1005):

[0106] The pull key distribution model allows each client to actively request keys from the server. In **FIG. 8, a** flow chart **800** is illustrated for implementing a pull key distribution system. In block **810** a server receives a request for a cryptographic key from a client. The server logs the request for the key in block **814**. For example, such a log entry could be made in a log such as a database maintained by the server. In block **818,** the key and its expiration time are distributed to the client in response to the request by the client. Thus the server need not monitor the status of the client's keys; rather, the responsibility of determining when a new key is required can be passed to the client. In block

EX-1005, [0106]

[0110] Under a pull key distribution model, each client requests a new key and is individually responded to by the key distribution server. The server can maintain a list of

EX-1005, [0110]

Wechselberger:

to by the key distribution server" (Peterka, [0110]). Based on Peterka's teachings, POSITAs understood that "in response to" ***any*** scenario where Peterka's client determines a new key is required to decrypt content, the client request a new key. This includes scenarios such as the one I described for my modification in view of Traw—where Peterka's client determines that it does not have a required key due to notice of a key revocation.

IPR2025-00003 EX-1047, ¶374; IPR2025-00004 EX-1047, ¶327

Traw Teaches Client Requesting Key in Response to Receiving Notice that a Key Must be Changed

IPR2025-00003 Pet. Opp. to RMTA, 18-19
IPR2025-00004 Pet. Opp. to RMTA, 18-19

Pet. Opps. to RMTAs:

PO's attorney argument also misreads Traw, asserting that Traw only "teaches that a notification instructs the client to change to a key that the client has already been provided." RMTA, 16. This is wrong. Traw discloses "requir[ing]" content

IPR2025-00003 Pet. Opp. to RMTA, 18; *see* IPR2025-00004 Pet. Opp. to RMTA, 18

Traw (EX-1042):

process to gain access to the content. In the event that such authentication secret values are compromised and distributed, means are provided for revoking the compromised information. To limit potential negative effects of such revocation on consumers, revocable information may be assigned on a fine granularity (e.g., uniquely to each product), or, if revocable information is common to a large number of products, such products may be required to be renewable (i.e. replaceable) in the event of revocation.

* * *

tion has occurred. In one embodiment, the renewal is achieved by an on-line download of at least a portion of a new content protection implementation, although other mechanisms may also be used (e.g., distribution of CDROMs or DVDs with the updated software). A would-be attacker wish-

EX-1042, 2:43-64

1. A method for periodically renewing content protection implementations in devices, the method comprising:

* * *

wherein the new content protection implementation comprises (a) new software to replace at least part of the existing software for presenting protected content and (b) a new key to supersede the existing key for facilitating presentation of protected content; and

EX-1042, claim 1

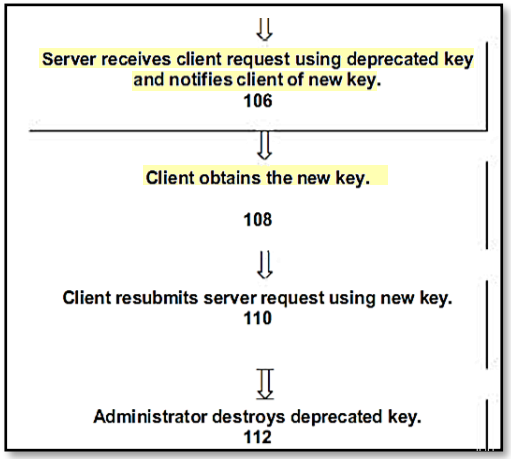
Requesting New Key in Response to Key Revocation

Pet. Opps. to RMTAs:

> Traw, 2:43-64. Traw's disclosure of having keys be renewable via a "download" "in the event" of revocation is unsurprising: the basic, unremarkable concept of a client requesting a new key in response to notice that a key has been revoked was well-known in client-server contexts (*e.g.*, EX1048, [0017]-[0018], FIG. 1; EX1049, [0147]-[0155]), and far from inventive in the Peterka-Traw context, given the desirability of minimizing service interruptions. EX1047, ¶¶375-377; Peterka, [0105].

IPR2025-00003 Pet. Opp. to RMTA, 19; *see* IPR2025-00004 Pet. Opp. to RMTA, 19

Gassoway (EX-1048):



EX-1048, FIG. 1 (excerpted)

Pelton (EX-1049):

> [0147] Various embodiments of the central key management system **10** are typically configurable to provide any or all of the following functions:

> [0150] Allowing key deletion, revocation, suspension and/or reissue of specific subject keys by a specific administrator role **54** for the entire key management domain;

> [0153] Presenting configuration options for key request, key maintenance, regular status, notification, and alerts for each subject (the system preferably allows profiling

EX-1049, [0147]-[0155]

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Peterka-Traw: Limitation [21.6]

Pet. Opps. to RMTAs:

As with the IMTA, [21.6] (*supra* p. 3, §I.A) was revised to ***eliminate*** the "ahead of"/"after" step sequence relative to "the key rotation boundary" recited in original claim 1. Regardless, Peterka-Traw satisfies this limitation. EX1047, ¶378. POSAs would have been motivated to implement Peterka-Traw to minimize "service interruptions" (Peterka, [0105]), such that when the client receives the second (replacement) key due to Traw's unscheduled key revocation (Traw, 3:17-19, 4:63-65, 5:35-39, 5:63-65, 6:12-21, 6:39-57), the client promptly applies the second key for decryption, before the current key is set to expire (i.e., before "said time-based [CEK] rotation boundary for said first key"), allowing the client to resume consuming content. EX1047, ¶379; Peterka, [0106], [0116]; EX1003, ¶124.

IPR2025-00003 Pet. Opp. to RMTA, 19; *see* IPR2025-00004 Pet. Opp. to RMTA, 19

Substitute Claim 22

Pet. Opps. to RMTAs:

> Substitute claim 22 mirrors original claim 2. RMTA, Claims App'x, ii. Unchanged claim limitations are obvious for the reasons set forth in Ground 1. Pet., 37; EX1047, ¶380. Claim 22 newly requires the second CEK expiration time to be "equal to the remaining lifespan of said first expiration time at the time said first [CEK] was expired." Peterka-Traw satisfies this limitation. EX1047, ¶381.
>
> POSAs understood there were three options for setting the expiration time of a replacement key: (1) ***before*** the original key expiration; (2) ***at the same time*** as the original key expiration; or (3) ***after*** the original key expiration. EX1047, ¶382. All three options would have been obvious to try. *Id.*; *KSR*, 550 U.S. at 421.

IPR2025-00003 Pet. Opp. to RMTA, 20; *see* IPR2025-00004 Pet. Opp. to RMTA, 20

Pet.'s RMTA Sur-Replies:

> The Board has recognized that (1) ***before***, (2) ***during/at the same time***, or (3) ***after*** an event are finite and obvious options—and not too "broad" under *KSR*. *Ex Parte Schinelli*, No. APPEAL 2025-000921, 2025 WL 3514783, at *5 (P.T.A.B. Nov. 19, 2025); *Ex Parte Ahmavaara*, No. APPEAL 2019-001889, 2020 WL 8184997, at *12 (P.T.A.B. Dec. 24, 2020). Moreover, PO does not dispute that

IPR2025-00003 Pet.'s RMTA Sur-Reply, 11-12;
see IPR2025-00004 Pet.'s RMTA Sur-Reply, 11-12

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Substitute Claim 22

Pet. Opps. to RMTAs:

POSAs had multiple reasons to try setting the second CEK's expiration time to be equal to the time remaining lifespan for the prior CEK. ***First***, the remaining lifespan of the first (compromised) CEK was already known to both the client and the server, and setting the CEK expiration time for the second CEK as equal to the remaining lifespan for the first CEK would minimize the need to adjust any existing time variables associated with the upcoming key rotation. EX1047, ¶384. ***Second***, adjusting the second CEK's expiration time such that it was not the same time as the first CEK would have required changing already-staged key rotation boundaries tied to future media segments, including interstitial segments like ads, previews, etc. that were common in multicast content distribution. *Id.*, ¶385 (citing Peterka, [0122], FIG. 7B; Peterka308, [0024], [0029], [0032]; Chen, [0034]-[0044], FIGs. 2A-2C). Using the remaining lifespan of the original (first) key would avoid the need to adjust these already-staged rotation boundaries. *See* EX1047, ¶384.

IPR2025-00003 Pet. Opp. to RMTA, 20-21; *see* IPR2025-00004 Pet. Opp. to RMTA, 20-21

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Substitute Claim 23

Pet. Opps. to RMTAs:

Substitute claim 23 mirrors original claim 3 and requires the second CEK expiration time to be "equal to the first expiration time plus the remaining lifespan of said first expiration time at the time said first [CEK] was expired." RMTA, Claims App'x, ii. Unchanged limitations are obvious as set forth in Ground 1. Pet., 38-41.

Claim 23's amendment falls within option #3 described above for substitute claim 22: expiration for the second (replacement) CEK ***after*** the expiration of the first (compromised) key. EX1047, ¶388. As noted above, setting the second CEK's expiration time for ***after*** the first (compromised) CEK's expiration was one of three obvious-to-try options. *Id.*, ¶389; *KSR*, 550 U.S. at 421. POSAs would have understood that setting the second CEK to both be applied ***before*** the first (compromised) key expires[2] and then expire ***after*** the first CEK would have expired[3] would mean that the CEK originally staged to be applied to the next media segment was no longer usable for the upcoming segment. EX1047, ¶390.

IPR2025-00003 Pet. Opp. to RMTA, 21-22; *see* IPR2025-00004 Pet. Opp. to RMTA, 21-22

Substitute Claim 23

Pet. Opps. to RMTAs:

To address this, POSAs would have been motivated to set the second CEK's expiration time to be equal to the remaining lifespan for the pre-existing expiration set for the first CEK plus the fixed expiration time (period duration) originally assigned for the first CEK. *Id.* This would provide Peterka-Traw's servers an additional key rotation period to better handle potential latency issues that would predictably arise from numerous clients attempting to replace the compromised key ***and*** the now-defunct key that was originally staged. *Id.*; Peterka, [0080] (noting the issue of "a large load on the caching server on the segment boundaries"). This implementation also would avoid disrupting the encryption/decryption of future media segments by desirably allowing POSAs to avoid adjusting already-staged key rotation boundaries. Peterka, [0122], FIG. 7B; EX1047, ¶390 (citing Peterka308, [0024], [0029], [0032]; Chen, [0034]-[0044], FIGs. 2A-2C).

IPR2025-00003 Pet. Opp. to RMTA, 22; *see* IPR2025-00004 Pet. Opp. to RMTA, 22

Pet. Opps. to RMTAs:

Peterka discloses content divided into segments encrypted (and decrypted) with a different key. Pet., 10, 36-37; Peterka, [0080]-[0082], [0091]-[0101], [0106], [0116], [0121]-[0125], FIGs. 7A-7B. Peterka’s modified system in Peterka-Traw includes a mechanism for responding to security attacks: revoking and requiring replacement of a compromised key before its set expiration. The second CEK is used to decrypt content originally slated to be decrypted by the first (compromised) CEK, and the early expiration of the first (compromised) CEK is for security reasons. Traw, 1:65-2:2, 2:15-19, 3:65-66, 4:37-39, 5:5-39, FIG. 2; EX1047, ¶¶395-396.

IPR2025-00003 Pet. Opp. to RMTA, 23; *see* IPR2025-00004 Pet. Opp. to RMTA, 23

Additional Traw Combinations

IPR2025-00003 Pet. Opp. to RMTA, 24-25
IPR2025-00004 Pet. Opp. to RMTA, 24-25

Pet. Opps. to RMTAs:

POSAs would also have combined Traw with the original grounds set forth in the Petition (Grounds 2-5), for the same reasons discussed *supra* §II.A.3. EX1047, ¶398. Grounds 6B-6E meet substitute claims 21-26, 29-30, 33-35, and 37 for the same reasons discussed *supra* §§II.A.4-II.A.9, ***and also*** meet substitute claims 27-28, 32, and 36 for the reasons discussed in Grounds 2-5:

Ground and Reference(s)		Substitute Claims
6B	Peterka, Suzuki, Traw	21-26, 29-30, 33-35, 37
6C	Peterka, Bocharov, Traw	21-26, 29-30, **32**-35, 37
6D	Peterka, Suzuki, Bocharov, Traw	21-26, 29-30, **32**-35, 37
6E	Peterka, Bocharov, Peterka308, Chen, Traw	**27-28**, **36**

IPR2025-00003 Pet. Opp. to RMTA, 24; *see* IPR2025-00004 Pet. Opp. to RMTA, 24

Limitation [21.2] in view of Suzuki

Pet. Opps. to RMTAs:

> If PO argues that Peterka-Traw does not disclose PO's new [21.2] requirement that the CEK identifiers are "each assigned to an associated [CEK]," at least Grounds 6B and 6D, which rely upon Suzuki's "key number" teachings to modify the base combination, meet this clause. Grounds 6B and 6D implement Peterka's system to

> [0080], FIG. 2; EX1003, ¶¶150-161), 60-63 (citing EX1003, ¶¶186-192). POSAs recognized the importance of using identifiers for keys (like Suzuki's key numbers) in multiple-key systems to help differentiate amongst keys, and further recognized that unique identifiers (like Suzuki's key numbers) helped ensure the system does not confuse keys. *See* Pet., 48; EX1003, ¶153. This would have been especially important in Peterka-Traw for single-key revocation scenarios. EX1047, ¶¶353-354.

IPR2025-00003 Pet. Opp. to RMTA, 24-25; *see* IPR2025-00004 Pet. Opp. to RMTA, 24-25

Limitation [21.2] in view of Suzuki

Pet. Opps. to RMTAs:

> Suzuki's key numbers (for identifying keys) (Suzuki, [0030]) in Ground 6B and 6D meet [21.2]'s "assigned" requirement. POSAs understood that each key number in those implementations was "assigned" to a key because the "key number" is information that is specifically associated with the key to facilitate "identifying the key." EX1047, ¶354; Suzuki, [0013].

IPR2025-00003 Pet. Opp. to RMTA, 25; *see* IPR2025-00004 Pet. Opp. to RMTA, 25

Suzuki (EX-1006):

> key number (information for identifying the key)

EX-1006, [0013]

Limitation [21.2] in view of Suzuki

Pet. Opps. to RMTAs:

> Moreover, implementing Suzuki's "key number for identifying the key" (Suzuki, [0030]) to be sufficiently "unique" to distinguish amongst keys "for the entire duration of a media playback," as claimed would have been obvious. *See supra* p. 15. POSAs would have been motivated to ensure (and reasonably expected success that) a client could uniquely identify keys even in scenarios where the client ultimately acquired all the keys needed for the entire duration of media playback because the "need to identify" and "know which key to use when" is "fundamental" to "anybody who has worked with crypto-based content information distribution systems" (EX2011, 39:7-40:13), because Peterka ***itself*** illustrates such a scenario (Peterka, [0092], FIGs. 7A-7B), and because it was common to use key IDs sufficiently unique to allow clients to keep track of keys required to playback a piece of content (*e.g.*, Pestoni, 12:4-35, FIG. 4). EX1047, ¶355.

IPR2025-00003 Pet. Opp. to RMTA, 25; *see* IPR2025-00004 Pet. Opp. to RMTA, 25