

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

ERICSSON AB,
Patent Owner.

Case IPR2025-00003
Patent No. 9,313,178

PATENT OWNER'S REVISED CONTINGENT MOTION TO AMEND

Table of Contents

I.	Introduction.....	1
II.	Statement of Relief Requested.....	1
III.	The Substitute Claims Satisfy 37 C.F.R. § 42.121(a) and (b).....	1
IV.	The Substitute Claims Are Not Unpatentable Under §§ 101, 103, or 112.....	13
V.	Level of Ordinary Skill in the Art.....	19
VI.	Claim Construction	19
VII.	Conclusion	19

EXHIBIT LIST

Exhibit No.	Description
Ex. 2001	Declaration of Kayvan B. Noroozi in Support of Motion for Admission <i>Pro Hac Vice</i>
Ex. 2002	“Check.” Cambridge Dictionary, Cambridge University Press, (https://dictionary.cambridge.org/us/dictionary/english/check), accessed Jan. 16, 2025
Ex. 2003	“Detect.” Cambridge Dictionary, Cambridge University Press, (https://dictionary.cambridge.org/us/dictionary/english/detect#google_vignette), accessed Jan. 16, 2025
Ex. 2004	U.S. Pat. No. 10,136,452, titled “Enhanced PRACH for standalone contention based communications including unlicensed spectrum”
Ex. 2005	Confidential Settlement Agreement
Ex. 2006	Confidential Arbitration Agreement
Ex. 2007	U.S. Patent Application Publ. No. 2014/0237243 (publication of U.S. Application No. 14/266,368 filed April 30, 2014)
Ex. 2008	U.S. provisional application Ser. No. 61/500,316, filed Jun. 23, 2011
Ex. 2009	U.S. Patent Application Publ. No 2012/0331293(Publication of U.S. patent application Ser. No.: 13/530,997, filed on Jun. 22, 2012)
Ex. 2010	Declaration of John Villasenor, Ph.D. in Support of Patent Owner’s Response
Ex. 2011	Deposition Transcript of Mr. Anthony J. Wechselberger (Taken 5/29/25)

I. Introduction

Ericsson AB (“Ericsson” or “Patent Owner”) respectfully moves under 35 U.S.C. § 316(d) and 37 C.F.R. § 42.121 to conditionally amend challenged claims 1-10, 12-20 of the ’178 patent. In the event the Board finds the challenged claims unpatentable, Ericsson respectfully requests that the Board grant this revised motion to amend with respect to the corresponding proposed substitute claims.

As shown below, this motion and the substitute claims meet all requirements of 37 C.F.R § 42.121. Patent Owner is thus entitled to the contingent substitute claims unless Petitioner “prove[s] all propositions of unpatentability.” *Aqua Products v. Matal*, 872 F.3d 1290, 1310 (Fed. Cir. 2017). As this motion further demonstrates, Petitioner has not done so.

II. Statement of Relief Requested

To the extent the Board finds any of the original challenged claims unpatentable, Ericsson respectfully requests that the Board grant this revised motion to amend with respect to the corresponding proposed substitute claim(s).

III. The Substitute Claims Satisfy 37 C.F.R. § 42.121(a) and (b)

The revised substitute claims are not broadening: As demonstrated in the claims appendix, the proposed revised substitute claims retain all features of the corresponding original claims, and only add clarifying or narrowing limitations.

In particular, the revised substitute claims address the Board’s concerns

regarding limitations [21.6] and [33.7] as expressed in its Preliminary Guidance.

Paper 30 at 5. Those limitations now explicitly require that the second content encryption key be applied *after* the notification-based content encryption key rotation boundary and *before* the time-based rotation boundary.

The following table specifies how each proposed revised substitute claim clarifies and/or narrows each corresponding original claim.

Sub. claim #	Original claim #	Amendments
21	1	<ul style="list-style-type: none">● for over-the-top media delivery;● each content key identifier assigned to an associated content encryption key;● content key identifiers that each uniquely identify each associated content encryption key from every other content encryption key for the entire duration of a media playback, the media playback corresponding to the media playback response;● applying a first key for content decryption, the first key having a first content key expiration time defining a time-based content key rotation boundary;● 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.● the notification requiring expiration of the first content encryption key earlier than the time-based content key expiration boundary for the first key and after the notification-based content encryption key rotation boundary for said first key;● issuing requests to a license server <i>in response to</i> detecting the notification-based content encryption key rotation boundary to retrieve a second content encryption key to be used <i>after</i> the notification-based content encryption key rotation boundary for the first key and <i>before</i> the time-based content encryption key

		rotation boundary for the first key; <ul style="list-style-type: none"> ● applying the second key for content decryption after the notification-based content encryption key rotation boundary for the first key and before the time-based content encryption key boundary for the first key.
22	2	<ul style="list-style-type: none"> ● Depends from claim 21; ● the second content encryption key having an expiration time equal to the remaining expiration time for the first key at the time the first key was expired.
23	3	<ul style="list-style-type: none"> ● Depends from claim 21; ● the second content encryption key having an expiration time equal to the original expiration time for the first key plus the remaining expiration time for the first key at the time the first key was expired.
24	4	<ul style="list-style-type: none"> ● Depends from amended claim 23.
25	5	<ul style="list-style-type: none"> ● Depends from amended claim 24.
26	6	<ul style="list-style-type: none"> ● Depends from amended claim 24.
27	7	<ul style="list-style-type: none"> ● Depends from amended claim 21.
28	8	<ul style="list-style-type: none"> ● Depends from amended claim 27.
29	10	<ul style="list-style-type: none"> ● Depends from amended claim 21.
30	12	<ul style="list-style-type: none"> ● Depends from amended claim 21; ● the retrieved content is divided into content segments, and the second key is applied to decrypt the same content segment for which the first content encryption key was used; ● the early expiration of the first content encryption key is for security reasons.
31	13	<ul style="list-style-type: none"> ● Depends from amended claim 30.
32	14	<ul style="list-style-type: none"> ● Depends from amended claim 30.

33	16	<ul style="list-style-type: none"> ● See claim 21, <i>supra</i>
34	17	<ul style="list-style-type: none"> ● Depends from amended claim 33; ● See claim 22, <i>supra</i>.
35	18	<ul style="list-style-type: none"> ● Depends from amended claim 33; ● See claim 23, <i>supra</i>.
36	19	<ul style="list-style-type: none"> ● Depends from amended claim 33
37	20	<ul style="list-style-type: none"> ● Depends from amended claim 33; ● See claim 30, <i>supra</i>.

The revised substitute claims are responsive: Petitioner, in its Opposition to the original Motion to Amend, has alleged that U.S. Pat. Pub. No. 2002/0172368 to Peterka, Ex. 1005 (“Peterka”) in combination with U.S. Patent No. 7,392,381 (Ex. 1042, “Traw”) teaches all limitations of the original proposed substitute claims. The Petition has also alleged that the prior art grounds presented therein meet all limitations of the original challenged claims. The revised proposed substitute claims are responsive to both the Petition and the opposition to the original motion to amend because each proposed revised substitute claim includes the following limitations, which taken as a whole, neither the Petition nor Petitioner’s opposition to the original motion to amend has demonstrated to be unpatentable: (1) content key identifiers assigned to each content encryption key and uniquely identifying each content encryption key from every other content encryption key for the entire duration of the media playback; (2) a first key having a time-based content encryption key rotation boundary; (3) detecting a notification,

the notification including a notification-based content encryption key rotation boundary and requiring expiration of the first content encryption key earlier than the time-based content encryption key rotation boundary for the first key and after the notification-based content encryption key rotation boundary for the first key; (4) the request for a second key being issued *in response to* (and thus after) detecting the notification-based content encryption key rotation boundary; and (5) the second key for content decryption being applied after the notification-based encryption key rotation boundary for the first key and before the time-based content key rotation boundary for the first key. Neither the Petition nor the Opposition to the Motion to Amend demonstrates unpatentability in view of those limitations.

At the same time, it is not necessary “that every word added to or removed from a claim in a motion to amend must be solely for the purpose of overcoming an instituted ground.” *Veeam Software Corp. v. Veritas Techs., LLC*, IPR2014-00090, Paper 48 at 28 (Jul. 17, 2017). Rather, the question is whether “the proposed claim as a whole is ‘responsive to a ground of unpatentability involved in the trial.’” *Id.* at 29. Beyond that threshold, Patent Owner may add other amendments that “serve[] the public interest by ensuring issuance of valid and clear patents,” including “additional limitations to address potential § 101 or § 112

issues.” *Id.* To the extent the Board finds that any other proposed amendments in a given substitute claim are not directly responsive to a ground of unpatentability here, those amendments are appropriate in view of the above.

The substitute claims are reasonable in number: Ericsson proposes only one substitute claim per original claim. 37 C.F.R. § 42.121(a)(3).

The substitute claims are presented in claim listing: The accompanying claim appendix lists the proposed substitute claims and clearly shows the proposed amendments to each corresponding original claim. 37 C.F.R. § 42.121(b).

The substitute claims introduce no new matter: The below table demonstrates that each substitute claim is supported by each earlier-filed disclosure as to which the benefit of the filing date is sought.¹ In particular, the ’178 patent issued from Application No. 14/266,368, published as Patent Application Publ. No. 2014/0237243 (filed April 30, 2014) (Ex. 2007). The ’178 patent claims priority to U.S. provisional app. 61/500,316, filed Jun. 23, 2011 (Ex. 2008), and U.S. patent app. 13/530,997, filed Jun. 22, 2012, published as U.S. Patent Application Publ. No. 2012/0331293 (Ex. 2009) and issued as U.S. Pat. 8,751,807.

Claim #	Lim.	Provisional ’316	’243 Publication	’293 Publication
21	[21P]	Abstract; pp. 1, 3	Abstract; ¶¶1, 5; cls.	Abstract; ¶¶1-

¹ The support citations herein are not intended to be exhaustive or limiting.

Claim #	Lim.	Provisional '316	'243 Publication	'293 Publication
			1, 16	3, 5; cls. 1, 16
	[21.1]	pp. 3-8; 11-12; Fig. 3; cl. 1	¶5, 8; cls. 1-3, 16	¶5, 8; cls. 1, 25; Fig. 3
	[21.2]	pp. 5, 11; cl. 1, 4	¶¶3, 5, 8, 10, 20, 36; cls. 1, 16	¶¶3, 5, 7, 8, 10, 20, 36; cls. 1, 25
	[21.3]	pp. 5-6, 7-8, 11-12; Figs. 2-3; cl.1, 16, 17	¶¶5; 22; cls. 1, 16	Abstract; ¶¶3, 5, 15, 19, 32; Figs, 1, 3
	[21.3 A]	pp. 8, 12-13	¶¶36, 38, 39	¶¶33-34, 36
	[21.4]	Abstract; pp. 5, 6, 10-13; cl. 13; Figs 2-3	Abstract; ¶¶5, 9, 10, 23, 25, 26, 35, 36, 39; cls. 12, 20; Fig. 3	¶¶8, 34; cls. 14, 15; Fig. 3
	[21.5]	Abstract; pp. 5, 6, 10-13; cl. 13; Figs 2-3	¶¶3, 5, 8, 9, 21, 26, 32, 35, 36, 39; Fig. 3; cls. 1, 12-15, 16 and 20	¶¶3, 5, 7-8, 15, 19-20, 26, 30, 33, 34, 37; Fig. 3
	[21.6]	Abstract; pp. 5, 6, 10-13; cl. 13; Figs 2-3	¶¶5, 36, 39; Fig. 3; cl. 1, 16	¶¶3, 5, 7-8, 15, 19-20, 26, 30, 33, 34, 37; Fig. 3
22		Abstract; pp. 5, 6, 7, 10-13; cl. 13-18; Figs 2-3	¶¶3, 5, 8, 10, 20, 21, 24, 29, 35; cls. 1, 16	¶¶7-8, 33, 35-37; Fig. 3
23		Abstract; pp. 5, 6, 7, 10-13; cl. 13-18; Figs 2-3	¶¶5, 20, 23, 24, 29, 32; cls. 3	¶¶7-8, 33, 35-37; Fig. 3

Claim #	Lim.	Provisional '316	'243 Publication	'293 Publication
24		Abstract; pp. 5-7, 10-13; cl. 10; Figs 2-3	¶¶6, 8-10, 20, 21, 24, 25, 26, 29, 31, 36, 39; cl. 4, 18	¶¶34-37; Fig. 3
25		Abstract; pp. 5, 6, 7, 10-13; cl. 10; Figs 2-3	¶¶20, 21, 23, 31, 36, 39; cl. 4, 5, 7, 19	¶¶34-37; Fig. 3
26		Abstract; pp. 5, 6, 7, 10-13; cl. 10; Figs 2-3	¶¶8, 10, 20, 31, 36, 39; cls. 4, 5, 6, 18	¶¶34-37; Fig. 3
27		pp. 4-5, 7; cls. 21-23	¶¶9, 10, 20; cl. 7, 8, 19	¶¶6, 17; cl. 18, 35
28		pp. 4-5, 7; cls. 21-23	¶¶8-10, 20; 34, 31 cl. 7, 19	¶¶6, 17; cl. 18, 35
29		pp. 4, 6-7, 11; cl. 6, 20, 26	¶¶22, 33; cl. 10	¶¶19, 31; cl. 5, 17, 21
30		Abstract; pp. 3-5, 7-13; cl. 13-18; Figs 2-3	¶¶6, 7, 10, 24, 28, 29, 33, 35, 36; cl. 12, 20	¶¶5, 6, 28-32
31		pp. 6, 9; cl. 13	¶¶10, 24, 35; cl. 13	¶¶8, 22, 33; cl. 14
32		pp. 6, 9, cls. 15-17	¶¶10, 19, 24, 35; cl. 14	¶¶8, 22, 33; cl. 15
33	[33.P]	Abstract; pp. 1, 3	¶¶1, 5; 16, 17; cls. 16-20	Abstract; ¶¶1-3, 5; cls. 1, 16
	[33.1]	pp. 1, 7	¶¶16; cls. 16-20	¶¶14-15; cl. 25, 37; Fig. 1
	[33.2]	pp. 3-8; 11-12; Fig. 3; cl. 1	¶5, 8; cls. 1-3, 16	¶5, 8; cls. 1, 25; Fig. 3

Claim #	Lim.	Provisional '316	'243 Publication	'293 Publication
	[33.3]	pp. 5, 11; cl. 1, 4	¶¶3, 5, 8, 10, 20, 36; cls. 1, 16	¶¶3, 5, 7, 8, 10, 20, 36; cls. 1, 25
	[33.4]	pp. 5-6, 7-8, 11-12; Figs. 2-3; cl.1, 16, 17	¶¶5; 22; cls. 1, 16	Abstract; ¶¶3, 5, 15, 19, 32; Figs, 1, 3
	[33.4 A]	pp. 8, 12-13	¶¶36, 38, 39	¶¶33-34, 36
	[33.5]	Abstract; pp. 5, 6, 10-13; cl. 13; Figs 2-3	Abstract; ¶¶5, 9, 10, 23, 25, 26, 35, 36, 39; cls. 12, 20; Fig. 3	¶¶8, 34; cls. 14, 15; Fig. 3
	[33.6]	Abstract; pp. 5, 6, 10-13; cl. 13; Figs 2-3	¶¶3, 5, 8, 9, 21, 26, 32, 35, 36, 39; Fig. 3; cls. 1, 12-15, 16 and 20	¶¶3, 5, 7-8, 15, 19-20, 26, 30, 33, 34, 37; Fig. 3
	[33.7]	Abstract; pp. 5, 6, 10-13; cl. 13; Figs 2-3	¶¶5, 36, 39; Fig. 3; cl. 1, 16	¶¶3, 5, 7-8, 15, 19-20, 26, 30, 33, 34, 37; Fig. 3
34		Abstract; pp. 5, 6, 7, 10-13; cl. 13-18; Figs 2-3	¶¶3, 5, 8, 10, 20, 21, 24, 29, 35; cls. 1, 16	¶¶7-8, 33, 35-37; Fig. 3
35		Abstract; pp. 5, 6, 7, 10-13; cl. 13-18; Figs 2-3	¶¶5, 20, 23, 24, 29, 32; cls. 3	¶¶7-8, 33, 35-37; Fig. 3
36		pp. 4-5, 7; cls. 21-23	¶¶9, 10, 20; cl. 7, 8, 19	¶¶6, 17; cl. 18, 35
37		Abstract; pp. 3-5, 7-13; cl. 13-18; Figs 2-3	¶¶6, 7, 10, 24, 28, 29, 33, 35, 36; cl. 12, 20	¶¶5, 6, 28-32

Claim #	Lim.	Provisional '316	'243 Publication	'293 Publication

In particular, contrary to Petitioner’s Opposition, limitations [21.2] / [33.3], [21.5] / [33.6], and [21.6] / [33.7] as revised herein do not introduce new matter.

Limitations [21.2] and [33.3]: Petitioner argues that the '243 publication “does not describe the duration for which the uniqueness of any ‘identifier’ must be maintained” such that a POSA would have understood that the duration of the unique identifier “*could* . . . be shorter than the entire duration of media playback.” Pet. Opp. at 7–8 (emphasis added) (citing Ex. 1041 ¶¶ 311–13; Ex. 2007 ¶ 2).

The Board’s Preliminary Guidance correctly rejected that allegation. The '243 publication describes several examples in which content encryption key identifiers are unique for the entire duration of the media playback because the unique content encryption key identifiers are assigned sequentially, including (1) “based on the wall clock time offset from the beginning of the live stream” (Ex. 2007 ¶¶ 8, 10) or “from the time the initial content encryption key identifier was generated,” *id.* ¶ 20; (2) “based on a segment number of the prepared content,” *id.* ¶¶ 8, 10; (3) “based on a relative offset to the initial content encryption key identifier,” which is set to zero, *id.* ¶ 20; and (4) “based off a next sequential

integer value, offset from the previous content encryption key identifier.” *Id.* In these examples, each time offset and each segment number is unique from the next and increases over the course of the live stream or over the course of assigning identifiers. Thus, no new matter is introduced.

Moreover, Petitioner’s contention that the unique identifier *could* be assigned for a period shorter than the entire media playback is irrelevant. Pet. Opp. at 7-8. That argument merely states that the specification supports *additional* embodiments in which the unique identifier has a *shorter* duration than what the amended claims recite. It is not evidence that the written description fails to support limitation [21.2] and its equivalents.

Limitation [21.5] and [33.6]: Petitioner contends the written disclosure does not support “issuing requests for a second key to be used before any key rotation boundary.” Opp. at 7. The Board’s Preliminary Guidance correctly disagreed, Paper 30 at 8, explaining that the ’243 publication describes circumstances in which “a key change is signaled . . . outside of any fixed duration lifespan” for security reasons. Ex. 2007 ¶ 35. The relevant disclosures further teach that a new key may be requested in response to a notification *rather than* an upcoming expiration time, and this necessarily discloses that the request for a new key in response to a notification may occur *before* the original time-based rotation

boundary for the current key. Ex. 2008, at 13 (“If the current content encryption key is within a fixed threshold of expiring *or* a content encryption key change request was detected in step 308, processing proceeds to step 318 where the client 110 requests a new content encryption key from the license server 106.”) (emphasis added). Moreover, the disclosures teach that a key change notification may be issued due to security concerns with the current key, Ex. 2008 at 8-9, and a POSA would readily understand that disclosure to teach requesting a second key in response to a notification before the expiration time for the first key.

Limitation [21.6] and [33.7]: For the same reasons explained with respect to limitations [21.5] and [33.6], Petitioner likewise incorrectly alleges that “there is no description of applying a second key for decryption before any rotation boundary,” Pet. Opp. 6, as recited by limitation [21.6] and [33.7]. In particular, the disclosures teach that “[o]nce the request for a new content encryption key has been sent in step 318, processing proceeds back to step 306 where the client 110 begins retrieving the next segment.” Ex. 2008 at 13. A POSA would understand that in the system and method of the disclosed invention, the client cannot retrieve the next segment without having received and applied the second key. *See also* Ex. 2007 ¶ 36; Prelim. Guidance at 8.

Moreover, revised limitation [21.6] and [33.7] expressly require that the

second key for content decryption is applied *after* the notification-based content encryption key rotation boundary for the first key, thus resolving the concerns raised in the Preliminary Guidance regarding new matter. *See, e.g.*, Ex 2008 at 13 (teaching that client 110 requests a new key after “a content encryption key change request was detected in step 308”).

IV. The Substitute Claims Are Not Unpatentable Under §§ 101, 103, or 112

Section 101: Petitioner’s contention that the proposed substitute claims fail under Section 101 is self-defeating and plainly contrary to governing law.

Petitioner states that the proposed substitute claims are directed to the “abstract idea of using CEKs [content encryption keys] to encrypt and decrypt information (media content segments)[.]” Paper 28 at 25. But using content encryption keys for encryption and decryption of digital media content is not an “abstract idea.” It is the epitome of a technological solution to a technological problem. Moreover, the claims do not generically recite the function of using content encryption keys.

Rather, they provide detailed recitations as to *how* content encryption keys should be used and rotated “for handling secure distribution of content for over-the-top media delivery” in a manner that improves computing technology by, among other things, enhancing security. Ex. 2008 at 3 (“New methods are required for the management of key rotation and key distribution to ensure security for OTT

content delivery.’’). The claims are thus patent eligible. *Ancora Techs. v. HTC Am., Inc.*, 908 F.3d 1343 (Fed. Cir. 2018); *Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999 (Fed. Cir. 2018). Petitioner has not demonstrated otherwise.

Section 112: Petitioner’s allegations regarding indefiniteness have also been obviated by the revised proposed substitute claims. Revised limitations [21.5] and [33.7] provide an antecedent basis for “the expiration time-based key rotation boundary.” Revised limitations [21.2] and [33.3] clarify that the content key identifier is unique for the “entire duration” of the media playback. And claims 22-26 and 33-37 now provide an antecedent basis for “the content expiration time” for the second content encryption key. Additionally, the revised claims add further clarity and precision to obviate any other allegations of indefiniteness.

Section 103: Finally, Petitioner has not met its burden of demonstrating obviousness.

With respect to Limitation [21.2], Petitioner’s arguments are the same as for the original claims, but further fail to meet the revised substitute claims in light of the explicit additional requirements recited therein. Limitation [21.2] requires content encryption key identifiers to uniquely identify each content encryption key from every other content encryption key for the entire duration of a media playback. And each unique content encryption key identifier must be “assigned” to

the corresponding content encryption key itself. Petitioner’s reliance on Peterka’s assignment of “a sequence number or a timestamp” to ECM/EMM messages fails to meet Limitation [21.2]. Peterka’s sequence numbers or timestamps are only assigned to its ECM/EMM messages, and not the content key included in those messages. Ex. 1005 ¶121 (teaching that the disclosed sequence number or time stamp is provided under “a format for such messages”); Ex. 2010 ¶ 89; Pet. 25 (stating “the sequence number/timestamp is unique to each ECM/EMM[.]”). Peterka’s sequence numbers or time stamps are thus not “content encryption key identifiers” as recited in Limitation [21.2]; they are only message identifiers, which cannot meet the challenged claims. Ex. 2010 ¶ 89.

The designations used in Peterka’s Figure 7B—CK0, CK1, and CK2—likewise do not meet limitation [21.2]. *Cf.* Paper 28 at 15. Peterka uses CK0, CK1, and CK2 as descriptive labels for its patent figures and teachings; it does not disclose or suggest sending any such labels to clients as key identifiers. Ex. 2010 ¶ 94.

Moreover, since Petitioner contends that Peterka’s message identifiers already serve to uniquely identify keys and to avoid key confusion, there would be no motivation to add key identifiers Peterka does not need to solve a problem it does not have. Ex. 2010 ¶ 95.

With respect to limitation [21.5], Petitioner *says* that a POSA would have been motivated to do exactly what the amended claims require, but identifies no teaching in either Traw or Peterka that discloses or even suggests limitation [21.5]. Limitation [21.5] requires requesting a second key “*in response to* detecting said notification-based content encryption key rotation boundary.” Petitioner does not identify any teaching in Peterka of a client requesting a new key *in response to* a key change notification. To the contrary, Peterka expressly teaches that the client always *already has* the new key to which it has been notified to change. Ex. 2010 ¶¶ 120-129. In its signaling embodiment, Peterka teaches that “when a new 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.*” Ex. 1005 ¶ 116 (emphasis added). Peterka further reiterates that the new content key “has recently been distributed to the client.” *Id.* ¶117. Peterka thus does not teach a client first receiving a key change notification and then, in response to that notification, issuing a request for a second key, as limitation [21.5] requires.

Traw likewise fails to meet the “*in response to*” requirement of limitation [21.5]. Like Peterka, Traw expressly teaches that a notification instructs the client to change to a key that the client has already been provided. Ex. 1041 at Abstract (“a device manufacturer embeds the keys in content protection implementations for

the devices, and to renew the content protection implementations in devices after the devices are distributed, in response to at least a security compromise”); 5:7-65 (“the key generation facility generates and allocates keys for devices . . .and may also include an expiration date, such that the key may be scheduled to be revoked on a certain date . . . [T]he device manufacturer embeds the keys in manufactured devices . . . [and] cause[s] the periodic renewal of the devices’ content protection implementations, which may include new keys in the new content protection implementation installed in the devices. The key generation facility generates revocation data . . . covering keys that are to be revoked such that devices having revoked keys cannot access protected content using the revoked keys.”). Traw never teaches having the client request the keys in response to a notification to rotate the keys. Traw thus simply further confirms that the revised proposed substitute claims are not obvious.

Petitioner’s combinations based on the Petition’s Grounds 2-5 fail for the same reasons above. The Petition confirms that the Peterka-Suzuki combination only sends requests for additional keys whenever the remaining lifetime/validity time of a current key reaches a particular “setting value” and not in response to a notification. Pet. 54-55.

With respect to **Claim 23**, Petitioner never contends, much less proves, that

it was one of a set of finite and obvious options to set the expiration time of a second key as equal to the original time of the first key plus the remaining life of the first key at expiration, as claim 23 requires. Petitioner thus fails to meet the requirements of its obvious to try theory for that claim.

Petitioner also cannot demonstrate obviousness for **claim 30**. Claim 30 requires assigning a second key to the same *segment* as the first key, among other things. Petitioner's expert has testified that in Peterka, each key is for one segment, and there is only one segment per key. Ex. 1003 ¶ 77 ("In particular, Peterka describes subdividing a media stream into 'segments' and applying a different content encryption key to each segment."). Peterka thus cannot meet claim 30. And Traw never teaches applying more than one key to a *segment*. Rather, Traw allegedly teaches applying a second key for decryption of the overall media playback. This is a different and broader concept. Using a second key to decrypt the same overall media playback content does not equate to using the second key to decrypt the same content *segment* as the first key. Nothing in Traw teaches the innovative requirement of claim 30 wherein a second key is applied to decrypt the same content *segment* as the first key, and Peterka expressly teaches the opposite, i.e., that each segment should only be decrypted using one key.

For these reasons the combination of Peterka-Traw does not teach nor

suggest the method and system of the '178 patent.

V. Level of Ordinary Skill in the Art

Patent Owner agrees with Petitioner's expert regarding the level of ordinary skill in the art. Ex. 1003, ¶41.

VI. Claim Construction

At this stage, Patent Owner does not propose any specific claim constructions as it is not Patent Owner's burden to demonstrate patentability of the proposed substitute claim over the prior art. While Patent Owner believes the new proposed limitations, plainly understood, establish patentability of the proposed claim, Patent Owner reserves the right to propose claim constructions as needed to respond to any allegations of unpatentability presented by Petitioner.

VII. Conclusion

Patent Owner respectfully requests, to the extent any original claim is deemed unpatentable, the Board grant the corresponding proposed substitute claim.

Respectfully submitted,

/Kayvan B. Noroozi/

Kayvan B. Noroozi, Admitted *Pro Hac Vice*

Peter C. Knops, Reg. No. 37,659

NOROOZI PC

11601 Wilshire Blvd., Suite 2170

Los Angeles, CA 90025

Attorneys for the Patent Owner

Date: October 15, 2025

CLAIMS APPENDIX

Underlining and strikethrough text show the modifications to the original claim being made in the corresponding substitute claim.

1-8 (Canceled)

10 (Canceled)

12-14 (Canceled)

16-20. (canceled)

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.

22. (Substitute for claim 2, if found unpatentable)

The method of claim 21~~4~~, wherein the content encryption keys and content encryption key identifiers returned in the playback request response include the content encryption key and associated identifier currently being applied, as well as a future content encryption key and associated identifier yet to be applied, and further wherein said second content encryption key having an expiration time, the expiration time for said second content encryption key being equal to the remaining lifespan of said first expiration time at the time said first content encryption key was expired.

23. (Substitute for claim 3, if found unpatentable)

The method of claim 21~~4~~, wherein the content encryption key expiration returned in the playback request response is expressed as an expected minimum interval between periodic key rotation, and further wherein said second content encryption key having an expiration time, the expiration time for said second content encryption key being equal to the first expiration time plus the remaining lifespan of said first expiration time at the time said first content encryption key was expired.

24. (Substitute for claim 4, if found unpatentable)

The method of claim 233, further comprising: timing the prefetching of a next un-retrieved content encryption key based on an expected expiration of the content encryption key currently being used.

25. (Substitute for claim 5, if found unpatentable)

The method of claim 244, further comprising: prefetching a next un-retrieved key a fixed duration before the expected expiration of the content encryption key currently being used.

26. (Substitute for claim 6, if found unpatentable)

The method of claim 244, further comprising: prefetching a next un-retrieved key within a period of time after the expected expiration of the content encryption key currently being applied, the period of time beginning at the expected expiration of the content encryption key currently being used, and ending at a duration calculated as a fixed percentage of a fixed periodic content encryption key expiration interval.

27. (Substitute for claim 7, if found unpatentable)

The method of claim 214, wherein subsequent content encryption key identifiers are predictable based on a predetermined known progression.

28. (Substitute for claim 8, if found unpatentable)

The method of claim 277, further comprising: the identifier being calculated as monotonically increasing sequential integer values based on the number of segments or video frames generated during a fixed periodic content encryption key expiration interval.

29. (Substitute for claim 10, if found unpatentable)

The method of claim ~~21~~¹, wherein license server communications are secured and authenticated using a selected one of Secure Sockets Layer and a token-based technique using a token encrypted with a symmetric key.

30. (Substitute for claim 12, if found unpatentable)

The method of claim ~~21~~¹, wherein said retrieved content is divided into content segments, and said second content encryption key is applied to decrypt the same content segment for which the first content encryption key was used and further wherein actual content encryption key rotation boundaries are detected based on real-time in-band notifications and said notification-based expiration of the first content encryption key is for security reasons.

31. (Substitute for claim 13, if found unpatentable)

The method of claim ~~30~~¹², wherein content encryption key rotation boundaries are detected based on notifications in an unencrypted header portion of the encrypted content files.

32. (Substitute for claim 14, if found unpatentable)

The method of claim ~~30~~¹², wherein content encryption key rotation boundaries are detected based on notifications present in the content manifest file, the content manifest file being selected from an m3u8 file, an IIS Smooth Streaming manifest file, a DASH MPD file and a proprietary manifest file.

33. (Substitute for claim 16, if found unpatentable)

[33.P] A computerized device operable as a client for handling secure distribution of content for over-the-top media delivery, comprising:

[33.1] memory operative to store computer program instructions;

one or more processors;

input/output interface circuitry; and

interconnect circuitry coupling the memory, processors and input/output interface circuitry together,

wherein the processors are operative to execute the computer program instructions from the memory to cause the computerized device to:

[33.2] initiate a media playback request and receive a playback request response;

[33.3] parse 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;

[33.4] retrieve content and manifest files from a content delivery server;

[33.4A] apply a first key for content decryption, the first key having a first content key expiration time period defining a time-based content key expiration boundary;

[33.5] detect a notification, the notification including a notification-based content encryption key rotation boundaries 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 the time-based content key expiration boundary for said first key and after said notification-based content encryption key rotation boundary for said first key;

[33.6] issue requests to a license server in response to detecting said notification-based content encryption key rotation boundary ahead of a said time-based content 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

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

34. (Substitute for claim 17, if found unpatentable)

The computerized device of claim 3346, wherein the content encryption keys and content encryption key identifiers returned in the playback request response include the first content encryption key and associated identifier currently being applied, as well as a future content encryption key and associated identifier yet to be applied and further wherein the second content encryption key having an expiration time, the expiration time for said second content encryption key being equal to the remaining lifespan of said first expiration time at the time said first content encryption key was expired.

35. (Substitute for claim 18, if found unpatentable)

The computerized device of claim 3417, wherein the computer program instructions further cause the computerized device to time the prefetching of a next un-retrieved content encryption key based on an expected expiration of the content encryption key currently being used and further wherein said second content encryption key having an expiration time, the expiration time for said second content encryption key being equal to the first expiration time plus the remaining lifespan of said first expiration time at the time said first content encryption key was expired.

36. (Substitute for claim 19, if found unpatentable)

The computerized device of claim 3346, wherein subsequent content encryption key identifiers are predictable based on a predetermined known progression.

37. (Substitute for claim 20, if found unpatentable)

The computerized device of claim 3346, wherein said retrieved content is divided into content segments, and said second key is applied to decrypt the same content segment for which the first content encryption key was used and wherein actual content encryption key rotation boundaries are detected based on real-time in-band notifications and said early expiration of the first content encryption key currently being used is for security reasons.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing **REVISED PATENT OWNER'S CONTINGENT MOTION TO AMEND** was served electronically via e-mail on October 15, 2025, on the following counsel of record for Petitioner:

Scott McKeown, Reg. No. 42866

SMcKeown-PTAB@wolfgreenfield.com

Anant K. Saraswat, Reg. No. 76,050

ASaraswat-PTAB@wolfgreenfield.com

Turhan F. Sarwar, pending admission pro hac vice

TSarwar-PTAB@wolfgreenfield.com

Elizabeth A. DiMarco, pending admission pro hac vice

Elizabeth.DiMarco@wolfgreenfield.com

Wolf, Greenfield & Sacks, P.C.

600 Atlantic Avenue Boston, MA 02210-2206

Telephone: 617-646-8000

Facsimile: 617-646-8646

/Kayvan Noroozi/

Kayvan Noroozi

NOROOZI PC

11601 Wilshire Blvd., Suite 2170

Los Angeles, CA 90025

Tel.: 310-975-7074

Counsel for Patent Owner

Date: October 15, 2025