

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

ERICSSON AB,
Patent Owner.

Case IPR2025-00004
Patent No. 11,122,313

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).....1

IV. The Substitute Claims Are Not Unpatentable Under §§ 101, 103, or 112.....16

V. Level of Ordinary Skill in the Art.....22

VI. Claim Construction 22

VII. Conclusion 22

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	Confidential Arbitration Agreement
Ex. 2003	Confidential Settlement Agreement
Ex. 2004	U.S. Patent Application Publ. No. US2020/0068241 (publication of U.S. Patent Application Ser. No 16/672,463, filed November 3, 2019)
Ex. 2005	U.S. provisional application Ser. No. 61/500,316, filed Jun. 23, 2011
Ex. 2006	U.S. Patent Application Publ. No. 2018/0192102 (publication of U.S. Application No. 15/910,911, filed Mar. 2, 2018 that issued as U.S. Pat. No. 10,477,257 on Nov. 12, 2019)
Ex. 2007	U.S. Patent Application Publ. No. 2016/019820 (publication of U.S. Application No. 15/067,129, filed Mar. 11, 2016 that issued as U.S. Pat. No. 9,912,975 on Mar. 6, 2018)
Ex. 2008	U.S. Patent Application Publ. No 2014/0237243 (publication of U.S. Application No. 14/266,368, filed Apr. 30, 2014 that issued as U.S. Pat. No. 9,313,178 on Apr. 12, 2016)
Ex. 2009	U.S. Patent Application Publ. No. 20120331293 (publication of U.S. patent application Ser. No. 13/530,997, filed Jun. 22, 2012 that issued as U.S. Pat. No. 8,751,807 on Jun. 10, 2014)
Ex. 2010	Declaration of John Villasenor, Ph.D. in Support of Patent Owner's Response for IPR2025-00004
Ex. 2011	Deposition Transcript of Mr. Anthony J. Wechselberger (Taken 5/29/25)
Ex. 2012	Declaration of John Villasenor, Ph.D. in Support of Patent Owner's Response for IPR2025-00003

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 1-7, 9, 11-17, and 19 of the ’313 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 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)

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 29 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.

Substitute claim #	Original claim #	Amendments
21	1	● for over-the-top media delivery; ● each content encryption 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 the media playback; ● applying a first content encryption key to the encrypted live media content before a first content encryption key rotation boundary, ● the first content encryption key having a first expiration time ● the first content encryption key rotation boundary was received as part of said received encrypted live media content ● requesting and obtaining a second content encryption key in response to receiving a notification to change said first content encryption key after a notification-based content encryption key boundary and before said first key rotation boundary; ● applying the second content encryption key for content decryption after a notification-based content encryption key boundary and before said first time-based key rotation boundary is reached.

REVISED CONTINGENT MOTION TO AMEND

Substitute claim #	Original claim #	Amendments
22	2	• Depends from amended claim 21; • the second content encryption key having an expiration time, the expiration time for the second content encryption key is equal to the remaining lifespan of the first expiration time at the time the first content encryption key was expired.
23	3	• Depends from amended claim 21; • the second content encryption key having an expiration time, the expiration time for the second content encryption key being equal to the first expiration time plus the remaining lifespan of the first expiration time at the time the first content encryption key was expired.
24	4	• Depends from amended claim 21.
25	5	• Depends from amended claim 21.
26	6	• Depends from amended claim 21.
27	7	• Depends from amended claim 21; • the retrieved content is divided into content segments, and the second content encryption key is applied to decrypt the same content segment for which the first content encryption key was used; • the notification to expire the first content encryption key is for security reasons.
28	9	• Depends from amended claim 21.
29	11	• For over-the-top media delivery; • each content encryption 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 the

REVISED CONTINGENT MOTION TO AMEND

Substitute claim #	Original claim #	Amendments
		media playback; ● apply a first content encryption key to the encrypted live media content before a first content encryption key rotation boundary, ● the first content encryption key having a first expiration time, ● the first content encryption key rotation boundary was received as part of said received encrypted live media content; ● request and obtain a second content encryption key in response to receiving a notification to change said first content encryption key after a notification-based content encryption key boundary and before said first key rotation boundary; ● applying the second content encryption key for content decryption after a notification-based content encryption key boundary and before said first time-based key rotation boundary is reached.
30	12	● Depends from amended claim 29; ● the second content encryption key having an expiration time, the expiration time for the second content encryption key is equal to the remaining lifespan of the first expiration time at the time the first content expiration key was expired.
31	13	● Depends from amended claim 29; ● the second content encryption key having an expiration time, the expiration time for the second content encryption key being equal to the first expiration time plus the remaining lifespan of the first expiration time at the time the first content encryption key was expired.
32	14	● Depends from amended claim 29.

REVISED CONTINGENT MOTION TO AMEND

Substitute claim #	Original claim #	Amendments
33	15	• Depends from amended claim 29.
34	16	• Depends from amended claim 29.
35	17	• Depends from amended claim 29; • the retrieved content is divided into content segments, and the second content encryption key is applied to decrypt the same content segment for which the first content encryption key was used; • the notification to expire the first content encryption key is for security reasons.
36	19	• Depends from amended claim 29.

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 first time-based content encryption key rotation boundary; (3) requesting and obtaining a second content encryption key *in response to* (and thus after) 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, and (4) the second key for content decryption being applied after the notification-based encryption key rotation boundary for the first key and before the first time-based content key rotation boundary. Neither the Petition nor the Opposition demonstrate 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 Pursuant to 37 C.F.R. § 42.121(b)(1) and (b)(2), 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.² In particular, the ’313 patent issued from U.S. Patent Application No. 16/672,463, published as Patent Application Publ. No. US2020/0068241 (filed

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

² The support citations herein are not necessarily exhaustive or meant to limit the meaning of the corresponding limitations.

November 3, 2019) (Ex. 2004). The '313 patent claims priority to U.S. provisional application Ser. No. 61/500,316 (filed Jun. 23, 2011) (Ex. 2005), and U.S. patent application Ser. No. 15/910,911, published as Patent Application Publ. No. 2018/0192102 (filed Mar. 2, 2018) and issued as 10,477,257 (Nov. 12, 2019) (Ex. 2006), which is a continuation of U.S. patent application Ser. No. 15/067,129 (filed Mar. 11, 2016), published as Patent Application Publ. No. 2016/0198203 and issued as U.S. Pat. No. 9,912,975 (Mar. 6, 2018) (Ex. 2007), which is a continuation of U.S. patent application Ser. No. 14/266,368, published as Patent Application Publ. No. 2014/0237243 (filed Apr. 30, 2014) and issued as U.S. Pat. No. 9,313,178 (Apr. 12, 2016) (Ex. 2008), which is a continuation of U.S. patent application Ser. No. 13/530,997, published as Patent Application Publ. No. 2012/0331293 (filed Jun. 22, 2012) and issued as U.S. Pat. No. 8,751,807 (Jun. 10, 2014) (Ex. 2009).

Cla im #	Lim. ³	Ex. 2004	Ex. 2005 Provisional Appl.	Ex. 2006	Ex. 2007	Ex. 2008	Ex. 2009
21	[21P]	¶¶ 2, 3.	Abstract; pp. 1, 3	¶¶ 2, 3.	¶¶ 2, 3.	¶¶ 2, 3.	¶¶ 1, 2
	[21.1]	¶2-7; 33,	pp. 11-12;	¶2-7;	¶4-6; 33,	¶4-6;	¶30-33;

³ Limitation citations correspond to numbering shown in the claims appendix attached hereto.

REVISED CONTINGENT MOTION TO AMEND

Cla im #	Lim. ³	Ex. 2004	Ex. 2005 Provisional Appl.	Ex. 2006	Ex. 2007	Ex. 2008	Ex. 2009
		cls. 1, 11	Fig. 3; cl. 1	32-33, cls. 1, 4	cls. 1, 4	33, cls. 1, 16	Fig. 3
	[21.2]	¶¶6, 9, 29, 34, 35; cls. 1, 11	pp. 5, 11; cl. 1, 4	¶¶6, 9, 29, 33- 36; cls. 1, 4	¶¶6, 9, 29, 34, 35; cls. 1, 4	¶¶6, 9, 29, 34, 35; cls. 1, 16	¶¶4, 7, 26, 30-33, 36; cls. 1, 8, 23
	[21.3]	Abstract; ¶¶6, 10, 19-22, 37; cls. 1, 7, 8, 9	pp. 5-6, 7-8, 11-12; Figs. 2-3; cl.1, 16, 17	Abstract ; ¶¶6, 10, 17 34-36; cls. 1, 4	Abstract ; ¶¶6, 10, 32- 36;	Abstrac t; ¶¶5, 10, 24, 34-38; cls. 1, 14, 16	Abstract; ¶¶6-8, 19, 22, 30- 34; cls. 14, 15, 34; Fig. 3
	[21.4]	Abstract; ¶¶6, 9, 19-22, 33-37; cls. 1, 11; Fig. 3	Abstract; pp. 5, 6, 8, 10-13; cl. 13; Figs 2-3	Abstract ; ¶¶6-10 17-23, 26, 34- 36;; cls. 1, 4; Fig. 3	Abstract ; ¶¶6, 9, 26, 32- 36; cls. 1, 4; Fig. 3	Abstrac t; ¶¶6, 9, 29 35-37; cls. 1, 16; Fig. 3	Abstract; ¶¶6-8, 19, 22, 30- 34; cls. 14, 15, 34; Fig. 3
	[21.5]	Abstract; ¶¶6, 36, 37; Fig. 3; cls. 1, 16	Abstract; pp. 5, 6, 10- 13; cl. 13; Figs 2-3	Abstract ; ¶¶6, 34-36; Fig. 3; cls. 1, 4	Abstract ; ¶¶6, 32-36; Fig. 3; cls. 1, 4	Abstrac t; ¶¶6, 32-40; Fig. 3; cls. 1, 16	Abstract; ¶¶4, 30- 34; Fig. 3; cls. 1, 16
	[21.6]	¶¶6, 35- 37; Fig. 3; cls. 1, 16	Abstract; pp. 5, 6, 10- 13; cl. 13; Figs 2-3	¶¶6, 34- 36; Fig. 3; cls. 1, 4	¶¶6, 32- 36; Fig. 3; cls. 1, 4	¶¶6, 32- 40; Fig. 3; cls. 1, 16	Abstract; ¶¶21, 34- 40; Fig. 3
22		¶¶4, 6, 9, 20, 22-	Abstract; p. 8; Figs 2-3	¶¶4, 6, 9, 20,	¶¶4, 6, 20, 22,	¶¶4, 6, 20, 22,	¶¶21, 34- 40; Fig. 3

REVISED CONTINGENT MOTION TO AMEND

Claim #	Lim. ³	Ex. 2004	Ex. 2005 Provisional Appl.	Ex. 2006	Ex. 2007	Ex. 2008	Ex. 2009
		24, 30, 36-37; cls. 1, 2, 11		22- 24, 30, 35-37; cls. 1, 4	24, 30, 32-36; cls. 1, 4	24, 30, 34-40; cls. 1, 16	
23		¶¶4, 6, 20, 22, 24, 30, 36-37; cls. 1, 3, 11	Abstract; p. 4, 5, 8	¶¶4, 6, 9, 20, 22- 24, 30, 34-36; cls. 1, 4	¶¶4, 6, 20, 22, 24, 30-37; cl. 1	¶¶4, 6, 20, 22, 24, 30, 37, 38; cls. 1, 16	¶¶21, 34-40; Fig. 3
24		¶¶4, 9, 32, 33; cl. 4	Abstract; p. 4, 5, 8; Figs 2-3	¶¶4, 9, 31-33; cls. 1, 4	¶¶4, 9, 32-35; Fig. 3	Abstract; ¶¶3-4, 9, 32-40; cl. 1, 2, 16, 17	Abstract; ¶¶3, 4, 6, 7, 29, 32; Fig. 3; cls. 1, 5, 7
25		¶¶6, 9, 10, 19, 20; cl. 5, 16	pp. 2, 4-5, 7; cls. 21-23	¶¶6-10, 18-20	¶¶6-10, 18, 19.	¶¶6, 9, 10, 19, 20; cl. 8	¶¶17; cls. 18, 35
26		¶¶34, cls. 6, 16	pp. 4, 6-7, 11; cl. 6, 20, 26	¶¶6, 33-34	¶¶4, 6, 33.	Abstract ¶¶2, 3, 5, 33-34, cls. 1, 10, 16	¶¶31, cls. 5, 17, 21
27		¶¶7-10, 24-25, 29, 31, 36, 37; cls. 7, 17	Abstract; pp. 3-5, 7, 10-13; cl. 13-18; Figs 2-3	¶¶7-10, 24-25, 28-29, 31, 33-36	¶¶7, 8, 25, 28, 32-36	¶¶7-8, 10, 25, 28-30, 32-40; cls. 7,	¶¶5, 6, 26, 28, 29, 33, 34; cls. 18, 27

REVISED CONTINGENT MOTION TO AMEND

Claim #	Lim. ³	Ex. 2004	Ex. 2005 Provisional Appl.	Ex. 2006	Ex. 2007	Ex. 2008	Ex. 2009
						17; Figs. 2, 3	
28		¶¶3, 7, 10, 18, 25, 36; cls. 9, 19	pp. 6, 9, cls. 15-17	¶¶3, 10, 18, 24, 35.	¶¶3, 10, 18, 24, 35.	¶¶3, 10, 18, 24, 34-35; cls. 14	¶¶8, 22, 33; cls. 15, 34
29	[29.P]	¶¶ 2, 3.	Abstract; pp. 1, 3	¶¶ 2, 3.	¶¶ 2, 3.	¶¶ 2, 3.	¶¶ 2, 3.
	[29.1]	¶16; cl. 11	pp. 1, 7	¶16; cl. 3	¶16; cl. 11	¶16; cl. 16	¶14; cls. 25, 37
	[29.2]	¶¶2-7; 33, cls. 1, 11	pp. 5, 11; cl. 1, 4	¶2-7; 32-33, cls. 1, 11	¶¶4-6; 32-33, cls. 1, 4	¶¶4-6; 33, cls. 1, 16	¶¶30-33; Fig. 3
	[29.3]	¶¶6, 9, 29, 34, 35; cls. 1, 11	pp. 5-6, 7-8, 11-12; Figs. 2-3; cl.1, 16, 17	¶¶6, 9, 29, 33-36; cls. 1, 4	¶¶6, 9, 32-36; cls. 1, 4	¶¶6, 9, 29, 34, 35; cls. 1, 16	¶¶4, 7, 26, 30-33, 36; Fig. 3; cls. 1, 8, 23
	[29.4]	Abstract; ¶¶6,10, 19-22, 37; cls. 7, 8, 9	Abstract; pp. 5, 6, 8, 10-13; cl. 13; Fig's 2-3]	Abstract ; ¶¶6, 10, 17 34-36; cls. 1, 4	Abstract ; ¶¶6, 10, 24, 32-36;	Abstract; ¶¶5, 10, 24, 34-38; cls. 1, 14, 16	Abstract; ¶¶6-8, 19, 22, 30-34; cls. 14, 15, 34; Fig. 3
	[29.5]	Abstract; ¶¶6, 9, 19-22,	Abstract; pp. 5, 6, 10-13; cl. 13;	Abstract ; ¶¶6-10 17-23,	Abstract ; ¶¶6, 9, 26, 32-	Abstract; ¶¶6, 9, 29	Abstract; ¶¶6-8, 19, 22, 30-

REVISED CONTINGENT MOTION TO AMEND

Claim #	Lim. ³	Ex. 2004	Ex. 2005 Provisional Appl.	Ex. 2006	Ex. 2007	Ex. 2008	Ex. 2009
		33-37; cls. 1, 11; Fig. 3	Figs 2-3	26, 34-36;; cls. 1, 4; Fig. 3	36; cls. 1, 4; Fig. 3	35-37; cls. 1, 16; Fig. 3	34; cls. 14, 15, 34; Fig. 3
	[29.6]	Abstract; ¶¶6, 36, 37; Fig. 3; cls. 1, 16	Abstract; pp. 5, 6, 10-13; cl. 13; Figs 2-3	Abstract; ¶¶6, 34-36; Fig. 3; cls. 1, 4	Abstract; ¶¶6, 32-36; Fig. 3; cls. 1, 4	Abstract; ¶¶6, 32-40; Fig. 3; cls. 1, 16	Abstract; ¶¶4, 30; Fig. 3; cls. 1, 16
	[29.7]	¶¶6, 36, 37; Fig. 3; cls. 1, 16	pp. 5, 6, 10-13; cl. 1-4, 13; Figs 2-3]	¶¶6, 35-37; Fig. 3; cls. 1, 4	¶¶6, 32-36; Fig. 3; cls. 1, 4	¶¶6, 32-40; Fig. 3; cls. 1, 16	Abstract; ¶¶21, 34-40; Fig. 3
30		¶¶4, 6, 20, 22, 24, 30, 36-37; cls. 1, 2, 11	Abstract; p. 8; Figs 2-3	¶¶4, 6, 19, 21-23, 29, 35-36; cls. 1, 4	¶¶4, 6, 19-24, 30, 32-36; cls. 1, 4	¶¶4, 6, 20, 22, 24, 30, 34-40; cls. 1, 16	¶¶21, 34-40; Fig. 3
31		¶¶4, 6, 20, 22, 24, 30, 36-37; cls. 1, 3, 11	Abstract; p. 4, 5, 8,	¶¶4, 6, 19, 21-23, 29, 35-36; cls. 1, 4	¶¶4, 6, 19-24, 29-30, 32-36; cls. 1, 4	¶¶4, 6, 20, 22, 24, 30, 34-40; cls. 1, 16	¶¶21, 34-40; Fig. 3
32		¶¶4, 9, 32, 33; cl. 4	Abstract; p. 4, 5, 8; Figs 2-3	¶¶4, 9, 31-33; cls. 1, 4	¶¶4, 9, 32-35; Fig. 3	Abstract; ¶¶3-4, 9, 32-40; cl. 1, 2, 16, 17	Abstract; ¶¶3, 4, 6, 7, 29, 32; Fig. 3; cls. 1, 5, 7
33		¶¶6, 9,	pp. 4-5, 7;	¶¶6-10,	¶¶6-10,	¶¶6, 9,	¶¶17-19;

REVISED CONTINGENT MOTION TO AMEND

Claim #	Lim. ³	Ex. 2004	Ex. 2005 Provisional Appl.	Ex. 2006	Ex. 2007	Ex. 2008	Ex. 2009
		10, 19, 20; cl. 5, 16	cls. 21-23	18-20	18, 19.	10, 19, 20; cl. 8	cls. 18, 35
34		¶¶34, cls. 6, 16	pp. 4, 6-7, 11; cl. 6, 20, 26	¶¶6, 33-34	¶¶4, 6, 33.	Abstract ¶¶2-3, 5, 33, 34, cl. 1, 10, 16	¶¶31, cls. 5, 17, 21
35		¶¶¶7-10, 24, 25, 29, 31-37; cls. 7, 17	Abstract; pp. 3-5, 7, 10-13; cl. 13-18; Figs 2-3	¶¶¶7-10, 24-25, 28-29, 31, 33-36	¶¶¶7-9, 24-25, 28, 32-36	¶¶¶7-8, 10, 25, 28-30, 32-40; cl. 7, 17; Fig. 2, 3	¶¶¶5, 6, 26, 28, 29, 33, 34; cls. 18, 27
36		¶¶¶3, 7, 10, 18, 25, 36; cls. 9, 19	pp. 6, 9, cls. 15-17	¶¶¶3, 9-10, 17-18, 24, 35-36	¶¶¶3, 9-10, 17-18, 24, 35-36	¶¶¶3, 10, 18, 24, 34-35; cls. 14	¶¶¶8, 22, 33; cls. 15, 34

In particular, contrary to Petitioner’s Opposition, limitations [21.2] / [29.3], [21.5] / [29.6], and [21.6] / [29.7] as revised herein do not introduce new matter.

Limitations [21.2] and [29.3]: Petitioner argues that the ’313 Application “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 ¶¶ 273–275; Ex. 2004 ¶ 2).

The Provisional Application 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. 2005 at 5); (2) “based on a segment number of the prepared content,” *id.*; (3) using monotonically increasing integer values. *Id.* at 2. 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 [29.6]: 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 29 at 8, explaining that the '241 publication describes circumstances in which “a key change is signaled . . . outside of any fixed duration lifespan” for security reasons. Ex. 2004 ¶ 36. 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. 2005 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. 2005 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. *See also* Ex. 2007 ¶ 36; Prelim. Guidance at 8.

Limitation [21.6] and [29.7]: For the same reasons explained with respect to limitations [21.5] and [33.6], Petitioner’s allegation 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 [29.7], is incorrect. 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. 2005 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.

Moreover, revised limitation [21.6] and [29.7] 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 2005 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 27 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. 2005 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 [21.2] and [29.3] clarify that the content key identifier is unique for the “entire duration” of the media playback. Revised Claims 22 and 30 now clearly recite an antecedent basis. Claims 23 and 31 have been revised to remove “previously set” and “originally assigned.” 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 ¶ 88; Pet. 24 (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 ¶ 88.

The designations used in Peterka’s Figure 7B—CK0, CK1, and CK2—likewise do not meet limitation [21.2]. *Cf.* Paper 27 at 15-16. 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 ¶

93.

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 ¶ 94.

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. 2012 ¶¶ 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. 47, 49-51.

With respect to **Claim 23**, Petitioner never contends 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 27**. Claim 27 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 ¶ 76 (“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 27. 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 27 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 '313 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, ¶40.

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,

/s/ Kayvan 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.

1-7 (Canceled)

9 (Canceled)

11-17 (Canceled)

19. (Canceled)

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.

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

The method of claim 21~~1~~, wherein the content encryption keys and content encryption key identifiers comprise the first content encryption key and associated identifier as well as the second content encryption key and associated identifier 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~~1~~, wherein the content encryption key rotation boundaries are expressed as an expected minimum interval between boundaries, 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 21~~4~~, further comprising obtaining a third content encryption key a fixed duration before the expected expiration of the second content encryption key.

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

The method of claim 21~~4~~, wherein subsequent content encryption key identifiers are predictable based on a predetermined known progression.

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

The method of claim 21~~4~~, 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.

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

The method of claim 21~~4~~, wherein said live media 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 wherein the content encryption key rotation boundaries comprise real-time in-band notifications and further wherein said notification to expire said first content encryption key is for security reasons.

28. (Substitute for claim 9, if found unpatentable)

The method of claim 21~~4~~, wherein the content encryption key rotation boundaries comprise 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.

29. (Substitute for claim 11, if found unpatentable)

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

[29.1] 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:

[29.2] send a request for live media playback;

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

[29.4] receive 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;

[29.5] apply 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;

[29.6] 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 the first time-based content encryption key rotation boundary, request and obtain 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 content encryption key rotation boundary is reached; and

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

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

The computerized device of claim 2944, wherein the content encryption keys and content encryption key identifiers comprise the first content encryption key and associated identifier as well as the second content encryption key and associated identifier 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.

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

The computerized device of claim 2944, wherein the content encryption key rotation boundaries are expressed as an expected minimum interval between boundaries, 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.

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

The computerized device of claim 2944, wherein the processors are further operative to execute the computer program instructions from the memory to cause the computerized device to obtain a third content encryption key a fixed duration before the expected expiration of the second content encryption key.

33. (Substitute for claim 15, if found unpatentable)

The computerized device of claim 2944, wherein subsequent content encryption key identifiers are predictable based on a predetermined known progression.

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

The computerized device of claim 2944, 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.

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

The computerized device of claim 2944, wherein said live media 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 wherein the content encryption key rotation boundaries comprise real-time in-band notifications and further wherein said notification to change to said first content encryption key is for security reasons.

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

The computerized device of claim 2944, wherein the content encryption key rotation boundaries comprise 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.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing **PATENT OWNER'S
REVISED 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