

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 REPLY
IN SUPPORT OF ITS REVISED CONTINGENT MOTION TO AMEND

PO’S REPLY RE: REVISED CONTINGENT MOTION TO AMEND

Table of Contents

I.	The revised amended claims do not broaden claim scope	1
II.	The revised amended claims do not introduce new matter	5
III.	The Substitute Claims Are Not Unpatentable Under §§ 101, 103, or 112.....	7

EXHIBIT LIST

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

I. The revised amended claims do not broaden claim scope

Petitioner's opposition contends that the revised amended claims improperly expand the scope of the original claims to "cover implementations that the original claims did not." Opp. 1. Petitioner argues that while the original claims require requesting a second content encryption key *before* reaching the recited "boundary" and applying that second key *after* that same boundary, the revised amended claims do not contain the same requirement. Opp. 2-5.

Petitioner's assertion that the revised amended claims broaden the scope of the original claims is incorrect. The original claims recite, in relevant part:

[21.5]/[33/6] 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

[21.6/33.7] applying the second key for content decryption after the key rotation boundary is reached.

In the original claims, the "key rotation *boundary*" provides the point before which the second CEK must be requested, and "after" which it must be applied.

The revised amended claims contain the same before / after requirement, but the relevant "boundary" is now the "notification-based content encryption key boundary." It is this boundary that corresponds to the "key rotation boundary" of the original claims, as this is the boundary point around which key rotation will occur. The revised amended claims thus recite, in relevant part:

PO'S REPLY RE: REVISED CONTINGENT MOTION TO AMEND

[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;

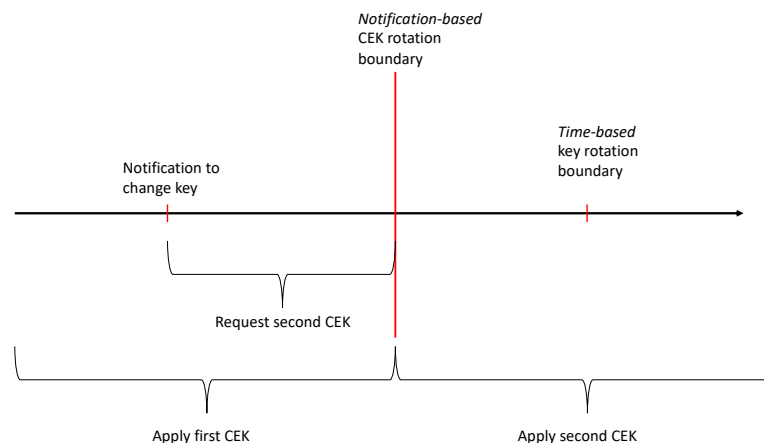
[21.5] *issuing requests* to a license server *in response to* detecting said notification-based content encryption key rotation boundary ahead of said time-based content encryption key rotation boundary for said first key **to retrieve** a second content encryption key to be used **after** the notification-based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

[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.

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 notification-based CEK *boundary* further defining the expiration point of the first key; (3) “*issuing requests* to a license server *in response to* detecting said notification-based content encryption key rotation boundary. . . *to retrieve*” a second CEK to be used *after* the notification-based CEK *boundary*; and (4)

PO’S REPLY RE: REVISED CONTINGENT MOTION TO AMEND

“applying the second key for content decryption *after* the notification-based content encryption key rotation *boundary* for said first key[.]” The illustration below depicts the before / after requirement of the revised amended claims.¹



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 revised amended claims do not broaden the original claim scope.

In arguing otherwise, Petitioner conflates the *notification* recited in the revised amended claims with the actual *boundary* that defines the point of key rotation. In limitation 21.4, a *notification* provides an upcoming notification-based

¹ In the provided illustration, the second CEK is applied before the first time-based key rotation boundary, and also maintained *after* the first time-based key rotation boundary. This represents one embodiment and is non-limiting.

PO'S REPLY RE: REVISED CONTINGENT MOTION TO AMEND
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 second CEK must then be applied *after* that same boundary. The revised amended claims thus maintain the before / after requirement of the original claims.

Petitioner's arguments based on the revised amended claims' "*time-based* key rotation boundary" are likewise inapposite. The "*time-based* key rotation boundary" is *not* an operative rotation boundary because it is preceded and trumped by the *notification-based* CEK rotation boundary, which causes early expiration. The *time-based* key rotation boundary thus does not correspond to the "key rotation boundary" of the original claims for purposes of Petitioner's claim scope dispute. It is the notification-based key boundary that corresponds to the "key rotation boundary" of the original claims in that respect.

Accordingly, contrary to Petitioner's assertion, the revised amended claims do not encompass any *additional* embodiments when they require that the second CEK be applied both after the *notification-based* CEK rotation boundary and before the *time-based* key rotation boundary. That additional language further limits the revised amended claims to require early expiration of the first CEK, *i.e.*, the first CEK must be rotated before its original *time-based* boundary. Petitioner's reliance on the fact that the revised claims require both obtaining and applying the

PO'S REPLY RE: REVISED CONTINGENT MOTION TO AMEND
second CEK before the *time-based* CEK boundary is thus misdirected for purposes
of Petitioner's claim scope broadening argument.

In sum, Petitioner's claim scope broadening allegations are without merit.

II. The revised amended claims do not introduce new matter

Petitioner additionally argues that limitations 21.6 and 33.7 introduce new matter that is not supported by the written description. Opp. 5-7. In particular, Petitioner contends that none of Patent Owner's citations provide written description support for applying a second CEK *before* "any rotation boundary." Opp. 6-7. Petitioner thus asserts that the written description does not support notification-based early key expiration, i.e., notification-based key rotation *before* the original *time-based* rotation boundary for that key. *Id.*

Petitioner is incorrect. As a threshold matter, satisfying written description does not require that the disclosure provide "*in haec verba*" support for the limitation at issue. *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1345-46 (Fed. Cir. 2016). Thus, Petitioner cannot establish a lack of written description by arguing that the specific wording of the limitations at issue is not present in the underlying disclosures. *Id.* Rather, so long as the disclosures reasonably allow persons of ordinary skill to recognize that the inventor invented what is claimed, the written description requirement is met. *Id.* at 1344.

PO'S REPLY RE: REVISED CONTINGENT MOTION TO AMEND

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 teachings as to explicit key change notification are *not* “independent of and, agnostic to, key rotation boundaries.” Opp. 7.

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.

PO'S REPLY RE: REVISED CONTINGENT MOTION TO AMEND

The provisional further provides that the workflow manager may initiate key rotation “as necessitated by security policies (e.g., the current content encryption key was compromised or the current encryption was found to be not sufficiently random).” Ex. 2008 at 10; *id.* at 8 (reiterating same). Since the provisional discloses the ability to rotate a key through explicit notification to address a key security compromise, it necessarily discloses setting a notification-based key rotation point *before* the original time-based key rotation point, since this is the logical time when a compromised key would be rotated for security reasons.

Finally, the provisional explicitly provides that a content encryption key may be expired *before* its fixed duration lifespan. Ex. 2008 at 9 (teaching that a key may be expired, for example, with “10 minutes left in its lifespan[.]”).

The '178 patent and all applications along the chain of priority include the above disclosures explicitly, and incorporate the teachings of the provisional by reference. Ex. 1001, 1:4-11; Ex. 2007, ¶¶ 6, 10, 35-36; Ex. 2009, ¶¶ 8, 33-34, Related US App. Data section. The amendments do not introduce new matter.

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

Petitioner does not dispute, and thus concedes, that the revised amended claims satisfy Section 101 and the indefiniteness provisions of Section 112. *See* Revised MTA at 16-17. Petitioner's obviousness contentions likewise fail.

PO'S REPLY RE: REVISED CONTINGENT MOTION TO AMEND

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 primarily relies on Peterka to meet those requirements, Opp. 13, but 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; Ex. 2010 ¶ 89; Pet. 25 (stating “the sequence number/timestamp is unique to each ECM/EMM[.]”). Peterka thus does not teach “content encryption key identifiers”; it only provides message identifiers, which do not suffice. Ex. 2010 ¶ 89.

The designations used in Peterka’s Figure 7B—CK0, CK1, and CK2—likewise do not meet limitation [21.2]. *Cf.* Opp. 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 ¶ 94. Peterka’s figure labels are not a motivation to modify Peterka’s teachings. *Id.*

Moreover, Petitioner contends that Peterka’s message identifiers *already* serve to uniquely identify keys and to avoid key confusion, Pet. 25, Ex. 2010 ¶ 94, thus belying and defeating its contrary contention that a POSA would have been motivated to directly assign identifiers to Peterka’s content encryption

PO'S REPLY RE: REVISED CONTINGENT MOTION TO AMEND

keys themselves. *Cf.* Opp. 13-14. A POSA would not have been motivated to solve a problem that the Petition itself concedes Peterka does not have. Ex. 2010 ¶ 95. Petitioner incorrectly contends that a POSA “would have recognized the need to differentiate between keys, especially for scenarios where a *single* comprised key held by multiple clients needed to be targeted for revocation.” Opp. 14 (emphasis original). But Petitioner’s theory relies on content keys that are *multicast*ed in ECM messages with only *one* content key sent per message. Pet. 21, 25. The Petition itself contends that because only one key is sent in each message, and each message has a *message* identifier, the content key in each message can be uniquely identified, thus obviating any need for a specific *key identifier* that is directly assigned to the content key itself. Pet. 25-26; Ex. 2010 ¶¶ 93-95. Since each content key is *multicast*ed in a message sent to multiple clients, all clients holding that key could identify the key using the same single message identifier in the event of a revocation. Thus, Petitioner’s rationale fails to motivate its modification.

As for limitation [21.5], Petitioner still does not identify any *teaching* in Peterka or Traw of a client requesting a new key *in response to* a key change notification. Try as it might, Petitioner cannot rewrite Peterka’s express teaching that the client always *already has* the new key to which it has been notified to change. Ex. 2010 ¶¶ 120-129; Ex. 1005 ¶ 116 (Peterka stating that “when a new

PO'S REPLY RE: REVISED CONTINGENT MOTION TO AMEND

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.*") (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 ("[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."). Traw never teaches having a client request a new key in response to a notification to rotate the keys. Petitioner's reliance on Traw at 2:43-64 does not show otherwise. Opp. 19. In the cited passage, Traw teaches that the "[c]ontent protection implementations" taught therein must be renewed (replaced)

PO'S REPLY RE: REVISED CONTINGENT MOTION TO AMEND

“on a periodic basis, independent of whether revocation has occurred.” Ex. 1042 at 2:56-60. Traw further states: “In one embodiment, the renewal is achieved by an on-line download of at least a portion of a *new content protection implementation*[.]” (emphasis added). Traw’s teaching is thus in reference to its content protection implementation, and is “independent of whether revocation has occurred.” *Id.* That teaching in no way discloses a client requesting and obtaining a new *key* in response to a notification of an upcoming early key rotation boundary, as [21.5] requires. Petitioner’s obviousness theory thus fails for all revised claims.

Petitioner’s Ground 6 combinations based on the Petition’s Grounds 2-5 fail for the same reasons above. The Petition concedes that Peterka-Suzuki only requests new keys when the remaining lifetime/validity time of a current key reaches a “setting value” and not in response to a notification. Pet. 51-57. Moreover, Ground 6 provides no viable motivation to meet limitation 21.2 because the Petition itself demonstrates that Peterka has no need for directly assigned, unique key identifiers. Pet. 25-26; Ex. 2010 ¶¶ 94-95.

With respect to **Claim 23**, Petitioner relies on an obvious-to-try theory, but 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. Rather,

PO'S REPLY RE: REVISED CONTINGENT MOTION TO AMEND

Petitioner broadly contends that setting the expiration time of the second key to *any* time after the expiration of the first key was simply *one* obvious option. By that logic, existence could be reduced to “hot dog” or “not hot dog,” and everything that is “not hot dog”—from space shuttles to semiconductors to 5G communication standards—would be one finite and obvious option. Petitioner simply has no prior art disclosing claim 23, and cannot provide an evidence-backed obviousness showing with particularity, as it must. 35 U.S.C. § 312(a)(3).

Petitioner also cannot demonstrate obviousness for **Claim 30**. Claim 30 requires assigning a second key to the same *segment* as the first key. 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 (“Peterka describes applying a different content encryption key to each segment.”). Peterka thus cannot meet claim 30. And Traw merely teaches applying a second key for decryption of the overall media playback—“*content* originally slated to be decrypted by the first key.” Opp. at 23. That does not equate to using the second key to decrypt the same content *segment* as the first key.

Accordingly, the revised amended claims are patentable.

Respectfully submitted,
/s/ Kayvan Noroozi

PO'S REPLY RE: REVISED CONTINGENT MOTION TO AMEND
CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing **PATENT OWNER'S
REPLY IN SUPPORT OF ITS REVISED CONTINGENT MOTION TO
AMEND** was served electronically via e-mail on December 29, 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: December 29, 2025