

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 SUR-REPLY

TABLE OF CONTENTS

I.	Petitioner’s Reply fails to demonstrate the Petition meets limitations [1A] and [1B] and the corresponding requirements of all challenged claims	1
II.	The Petition separately fails as to “content encryption key identifiers”	17
III.	The Petition additionally fails as to the detecting and issuing requests limitations of [1D] and [1E]	21
IV.	Conclusion	26

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. Petitioner's Reply fails to demonstrate the Petition meets limitations [1A] and [1B] and the corresponding requirements of all challenged claims

The express language of the challenged claims requires (1) “initiating *a* media playback request and receiving a playback request response,” and (2) “parsing content information from the playback request response, the content information including content encryption keys.” Limitations [1A] and [1B] (emphasis added).

It is beyond dispute that all challenged claims thus require a *single* “playback request,” and a “playback request response” that includes *multiple* “content encryption *keys*.”

As Patent Owner's Response demonstrated, however, the Petition does not and cannot meet the above claim requirements. Petitioner's Reply only serves to confirm Patent Owner's showing.

First, Petitioner states that it satisfied limitations [1A] and [1B] by pointing to Peterka's paragraph 80. Reply at 4. That is wrong. Limitations [1A] and [1B] require that a *single* “playback request” generate a “response” that includes multiple “content encryption keys.” Peterka's paragraph 80, by contrast, merely states: “each rabbit is given keys to the current as well as the next segment.” Ex. 1005 ¶ 80. Peterka's paragraph 80 does *not* state that multiple content keys (one for the current segment and one for the next) are provided in response to a *single* “playback

request,” as Limitations [1A] and [1B] require. Thus, Peterka’s paragraph 80 cannot meet the challenged claims.

Indeed, Peterka’s paragraph 80 expressly teaches that each client request receives only *one* key in response, stating: “All consumer computers would negotiate *a* key for *each* segment in order to keep track of how many segments they watched.” Ex. 1005 ¶ 80 (emphasis added). The remainder of paragraph 80 further makes clear that Peterka does not provide the keys to the current segment and the next segment *at the same time*. (“[E]ach rabbit is given keys to the current segment as well as the next segment. This will give the caching server enough time to distribute the *next* segment keys *during* the current segment.”) Ex. 1005 ¶ 80 (emphasis added). Peterka needs “enough time” to provide the next segment content key because the client requests that key *separately* from the request it made for the current segment key, as demonstrated in the POR and again below. Peterka’s teaching that the client receives the key for a next segment during a current segment thus does *not* mean that the keys to the current and next segment were provided in response to a *single* request, as the challenged claims require.

Second, Petitioner’s own disclaimers as to the scope of its Petition theory establish the Petition’s failure, and defeat its reliance on Peterka’s paragraph 80. The

Petition’s theory expressly relies on Peterka’s “*client-initiated requests*” to meet the “media playback request” of limitation [1A]. Pet. 19-20 (“Peterka’s disclosed client-initiated requests to access media, e.g., program content, are each *initiating a media playback request* as recited.”) (emphasis Petition’s). The Petition also exclusively relies on Peterka’s pay-by-time model. Reply at 6. And the Petition further exclusively relies on Peterka’s “content keys” to meet the recited “content encryption keys” of the claims. Reply at 7; Pet. 23-24; Ex. 2011 at 37:14-20. Crucially, the Petition’s theory as to *all* limitations, including limitations [1A] and [1B], further restricts itself to Peterka’s “pull” key distribution model. Pet. 12 (“The Grounds herein rely on Peterka’s *pull model*.”) (emphasis Petition’s); Pet. 18 (“*Every element* of claims 1 and 16 is satisfied by or obvious over Peterka’s *pull* method.”) (emphasis added); Pet. 20 (relying on Peterka’s pull model in discussing Peterka’s paragraph 80).

Under Peterka’s pay-by-time model, however, the first *client-initiated request* to access media occurs when a client *purchases* the right to view a pay-by-time content segment. POR at 22-23; Ex. 1005 ¶¶ 93, 129-131; Ex. 2010 ¶ 54. For instance, in Peterka’s Figure 7B, the first content key *requested* by the client is

Content Key 2. *Id.* No prior content key provided to clients ***without*** a client request can meet the Petition's theory.¹

Peterka teaches that under its pull model as applied to its pay-by-time distribution scheme, each client receives only ***one*** content key in response to each client request for media. Ex. 2010 ¶ 55; POR at 23-26. Indeed, Peterka expressly states: "Under a pull key distribution model, each client requests ***a*** new key and is individually responded to by the key distribution server." Ex. 1005 ¶ 110 (emphasis added). Peterka's Figure 8, which is directed to its pull distribution model, further teaches that a client requests "***a*** cryptographic key" and the server distributes "***the*** key to the client in response to the request," further establishing that each client-initiated request under Peterka's pull model only requests ***one*** content key and each response yields only ***one*** content key. Ex. 1005 Fig. 8; Ex. 2010 ¶ 56; POR at 24-25.

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

Thus, Peterka's paragraph 80 *cannot* be read to teach limitations [1A] and [1B] within the scope of the Petition's own limited theory. Since the Petition only relies on client-initiated requests for content keys made under the pay-by-time model using the "pull" distribution technique, Peterka's express teaching that each client-initiated pull request yields only *one* content key in response forecloses interpreting Peterka's paragraph 80 as meeting limitations [1A] and [1B].

Recognizing its problem, Petitioner's Reply now contends that the Petition's theory as to limitations [1A] and [1B] does not rely on Peterka's "pull" model and is not limited by Peterka's teachings as to its pull model. Reply at 5-6. But the Petition itself expressly stated, without qualification, that "[e]very *element* of claims 1 and 16 is satisfied by or obvious over Peterka's pull method." Pet. 18 (emphasis added). The phrase "every element" necessarily includes limitations [1A] and [1B]. Moreover, the Petition directly tied its reliance on Peterka's pull model to its reliance on Peterka's paragraph 80. Pet. 12. Petitioner's Reply arguments attempting to distance itself from Peterka's pull model for purposes of limitations [1A] and [1B] are thus foreclosed by the Petition's own statements. *Wasica Fin. GmbH v. Cont'l Auto. Sys.*, 853 F.3d 1272, 1286-87 (Fed. Cir. 2017) ("Shifting arguments in this fashion is foreclosed by statute, our precedent, and Board guidelines"). Moreover,

Petitioner's attempt to now distinguish between Peterka's client requests to access media content and Peterka's pull distribution model are unavailing. Under the Petition's theory, the client requests media content by making a pull request for the content key for a segment of pay-by-time media content that the client has decided to purchase. POR 23-26; Ex. 2010 ¶¶ 56-58. That pull request yields only one key in response, and thus limitations [1A] and [1B] cannot be met. *Id.*

Petitioner's attempt to distance itself from Peterka's teachings as to its pay-per-view and subscription models are likewise unfounded. Reply at 5. Patent Owner's discussion of those models demonstrated that Peterka has a unifying theme: one content key per client pull request. POR 10-14. Peterka's teachings in those respects thus necessarily illuminate the failures of the Petition's theory.

Petitioner likewise wrongly attempts to disregard Patent Owner's discussion of Peterka's free preview key, group key, and provisioning process. Reply at 6-7. Those aspects of Patent Owner's Response demonstrated that the Petition relied on portions of Figures 7A and 7B that did not correspond to any ***client-initiated request*** for media content, and thus could not satisfy limitations [1A] and [1B]. *See* Petition at 21-22, 24.

Retreating once again, Petitioner now contends that it never relied on Figure 7B as meeting the challenged claims, but instead only relied on that figure to support a contention of desirability and obviousness. Reply at 7-8. Petitioner attempts to distance itself from the Petition's direct reliance on Figure 7B because Patent Owner has demonstrated that the Petition simply mischaracterized and/or misinterpreted Peterka's teachings as to that figure—a significant blow to the credibility of the Petition and Petitioner's expert. In particular, the Petition stated that “Figure 7B shows two content keys CK0 and CK1 distributed in separate ECMs for each *request received* during a free preview period, and two content keys CK1 and CK2 distributed in separate ECMs for each *request received* during an initial key distribution period.” Pet. 21 (emphasis added). But Peterka itself teaches that CK0 and CK1 are each distributed *without any request* from the client, and this is fundamental to Peterka's design and principles of operation. POR at 15-22. Peterka provides CK0 and CK1 in Figure 7B to clients *without request* so that clients can access *free* program content and can decide whether to purchase (and thus request) the paid portions of the program content that begin with CK2. *Id.*

Accordingly, Peterka's Figure 7B cannot support the desirability or obviousness of an approach that Figure 7B *does not teach*, i.e., sending multiple

content keys in response to a single client request. *Cf.* Reply at 7-8. Patent Owner’s extensive demonstration that Figure 7B does not teach sending multiple content keys in response to one request thus necessarily refuted Petitioner’s “desirability/obviousness” contentions based on Figure 7B. Moreover, Patent Owner extensively refuted the Petition’s assertion that it would have been desirable or obvious to modify Peterka to send multiple content keys for multiple content segments in response to a single client request. POR at 33-36. Such a modification would have been contrary to the design purpose of Peterka’s pay-by-time model, particularly under a multicast key distribution scheme, causing clients to obtain access to content segments they *did not purchase*. *Id.*

As the above demonstrates, Petitioner’s contention that its “actual trial grounds . . . stand un rebutted” is thus entirely false. Reply at 8.

Equally without merit is Petitioner’s attempt to argue against the express language of limitations [1A] and [1B]. Petitioner contends that limitation [1A] does not require any request for a content key. Reply at 9-10. That is a red herring. Limitations [1A] and [1B] expressly recite “a media playback request,” “a playback request response,” and “content information including content encryption keys.” Accordingly, the Petition must demonstrate how the “playback request” of its theory

generates a “playback request response” that includes **multiple** “content encryption keys,” as limitations [1A] and [1B] require. Patent Owner has correctly held Petitioner to that requirement. Petitioner’s arguments that the “playback request” of the claims need not explicitly request any content encryption key is entirely beside the point. The salient fact is that the claims require that multiple content encryption keys be provided *in response* to a *single* media playback request. To meet that requirement, the **Petitioner’s theory** relies on a client-initiated request for content under the pay-by-time model using the pull distribution method, but this theory cannot meet what the claims expressly require, as shown above and in the Patent Owner Response. In short, nothing in Peterka teaches “a client that initiates a media playback request and receives multiple content keys in response,” as Petitioner contends. Reply at 10.

Petitioner’s allegations that Patent Owner presented “flawed” understandings of Peterka are likewise incorrect. Reply at 10-17.

Petitioner concedes (as it must) that in Figure 7B the free preview key and the group key are provided during provisioning and without client request. Reply at 11-12. But Petitioner attempts to argue that CK0 and CK1 are separate and are provided in response to client requests. *Id.* Petitioner’s contention is refuted by Figure 7B

itself, which shows CK0 packaged under the free preview key (FPK) and CK1 packaged under the group key (GK). CK0 and CK1 are thus necessarily provided in the same manner as the FPK and GK that encodes them respectively—without client request.

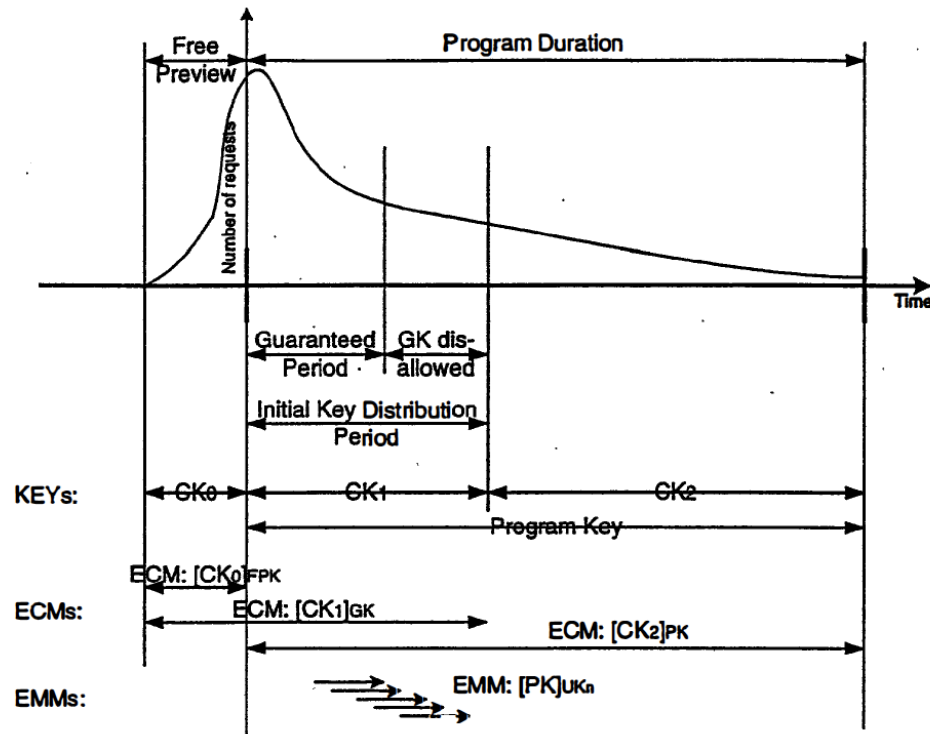


Fig. 7B

Peterka makes that reality explicit, stating: “In block 408, a content key is provided. The content key is encrypted with a free preview key as shown in block 412. The encrypted content key is then provided to the plurality of clients as shown

by block 416.” Ex. 1005 ¶ 85. Peterka additionally *defines* the free preview key as the key “used to distribute the CK [content key] . . . for the content during the initial free preview period.” *Id.* ¶ 103. Peterka adds: “This may be a fixed key known to all clients or distributed during provisioning.” *Id.* Peterka thus explicitly forecloses Petitioner’s argument that CK0 in Figure 7B is provided in response to a client request. Reply 12.

Similarly, Peterka teaches that the “group key” is “used to distribute the CK [content key]” for the initial viewing period that comes after the free preview in Figure 7B. Ex. 1005 ¶ 102. Peterka further explicitly states: “Clients will get the GK [group key] ahead of program events sold on . . . PBT [pay-by-time] basis, for instance during provisioning.” *Id.* Peterka additionally states: “Fig. 7B shows an entitlement control message in which a content key is encoded with a group key (ECM:[CK1]GK).” *Id.* ¶ 122. Petitioner’s argument that Figure 7B does not show CK1 being provided to clients without any client request is thus once again false. Reply at 12.

Petitioner’s reliance on the “number of requests” graph in Figure 7B is particularly specious. Petitioner contends that the “number of requests” plot at the top of Figure 7B *corresponds* to the ECMs sent at the bottom of Figure 7B such

that “the ECMs / content keys [] would be sent *in response*” to the requests plotted above. Reply at 13 (emphasis added). That is not true, and Figure 7B itself refutes that contention. In Figure 7B, at the far left of the figure, the number of requests is plotted as zero, and thus no requests have been made at all at that time. Yet directly below, the ECM carrying CK0 has been sent, and the ECM carrying CK1 has also been sent.

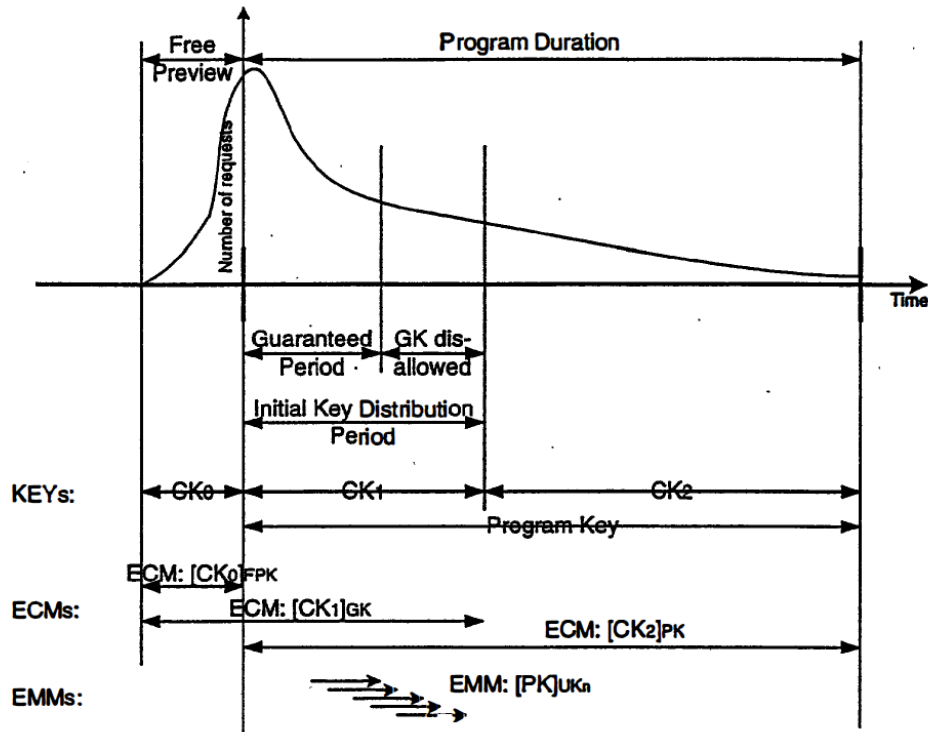


Fig. 7B

Since both CK0 and CK1 are sent at times when *no* requests have been made, Figure 7B makes clear that CK0 and CK1 are not sent “in response” to the requests plotted above. Rather, as Peterka explains, the “requests” shown at the top of Figure 7B correspond to requests for *paid* content, which begins with CK2. Thus, the only key provided in response to the requests shown at the top of Figure 7B is CK2. POR at 21-23.

Petitioner next alleges there is a teaching in Peterka whereby multiple content keys are provided in response to a client-initiated request for media access without the use of the pull distribution model. Reply at 16. There is no such teaching. Peterka's paragraph 80 simply states that the key for the next segment is provided during the current segment to avoid service interruptions, *not* that both the current content key and next content key are provided in response to *one* request, as the challenged claims require. Moreover, the Petition's theory expressly relies on the pull distribution model for “every element” of the challenged claims. Pet. 18. Under the pull model, each content key must be requested one at a time. POR 23-26. This is consistent with Peterka's paragraph 80, which expressly states that “[a]ll consumer computers would negotiate *a* key for *each* segment in order to keep track of how many segments they have watched.” Thus, Patent Owner did not

“conflate” the concepts of a client-initiated request for media content and the manner in which Peterka distributes the content key for such content. Reply at 16.

Petitioner further contends that its obviousness theory would not conflict with the purpose of Peterka’s pay by time model. Reply at 16-17. Petitioner states that Peterka does not restrict content keys for paid content segments to only those clients that have agreed to purchase those segments. *Id.* Petitioner’s assertions are once again refuted by Peterka itself. In Figure 16B, Peterka teaches that the “second key” (i.e., the key corresponding to the first *paid* content segment) is provided “to each of the clients that ***purchased*** the program content during the guaranteed period.” Ex. 1005 Fig. 16. Peterka further teaches that a client is provided a key for decrypting paid program content after the client has indicated its agreement to ***purchase*** that content. *Id.* ¶ 85. Indeed, Peterka states: “In block 520 the remaining portion of the program is distributed to the client computers that requested the remaining program content in block 512 so as to ***prevent*** the remaining client computers from being able to receive or view the encrypted remaining portion of the program without the proper decryption tools.” *Id.* ¶ 89 (emphasis added). Similarly, Peterka states: “Key 2 would be actual content encryption key delivered ***only*** to those clients that purchased the content.” *Id.* ¶ 93

(emphasis added). Petitioner thus wrongly implies that Peterka's paragraph 80 teaches providing clients with a content key for a next segment that they have ***not agreed to purchase***. Peterka makes clear that only clients that have *agreed to purchase* the next segment will receive the content key for that next segment. Peterka so explains in detail with respect to the illustration of Figure 7B and the "guaranteed period" in particular. POR 28-29; Ex. 1005 ¶¶ 130-133; Ex. 2010 ¶ 62. Only those clients who agree to *purchase* the paid program content during the "guaranteed period" will be provided the content key for the upcoming paid program segment sufficiently ahead of time to avoid service interruptions. Ex. 1005 ¶ 133 ("Block 1740 shows the number of clients that will ***purchase*** the program content during the guaranteed time period is estimated. In block 1750 an initial key distribution period is provided having a duration long enough to provide cryptographic keys to the ***purchasing*** clients so as to prevent reception of the program content from being interrupted at the ***purchasing*** clients.") (emphasis added).

Thus, providing clients who have ***not*** agreed to purchase an upcoming paid program segment with the content key for that segment, as the Petition's obviousness theory would do, directly contradicts Peterka's teachings and design,

and would not have been obvious or desirable. Nor would such an approach be consistent with Peterka's aims of avoiding service interruptions, as Petitioner contends. Reply at 17. Peterka plainly desires to **block** service to clients that have not agreed to purchase pay-by-time content. That is a central purpose of Peterka's encryption key design and its pay-by-time model. Ex. 1005 ¶ 89 ("In block 520 the remaining portion of the program is distributed to the client computers that requested the remaining program content in block 512 so as to **prevent** the remaining client computers from being able to receive or view the encrypted remaining portion of the program without the proper decryption tools.") (emphasis added); *id.* ¶ 93 ("Key 2 would be actual content encryption key delivered **only** to those clients that purchased the content.") (emphasis added).

For the same reasons, it is irrelevant whether Suzuki taught sending multiple keys in a single message, as Petitioner contends. Reply at 17-20. The question is not whether an ordinary artisan *could* have sent multiple content keys in response to a single request, but rather whether the ordinary artisan would have been *motivated* to modify Peterka to do so. Patent Owner has demonstrated that the ordinary artisan would **not** have found that modification desirable because doing so would give multiple clients access to paid content that they did not agree to

purchase, contrary to the entire purpose and design of Peterka’s pay-by-time model. POR 36-37; Ex. 2010 ¶ 78.

Accordingly, the Petition fails to meet limitations [1A] and [1B] and the corresponding requirements of all challenged claims.

II. The Petition separately fails as to “content encryption key identifiers”

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

The Federal Circuit has repeatedly held that the patentee’s use of the phrase “referred to herein” constitutes lexicography, particularly where (as here) the phrase is not used to simply describe an embodiment but rather describes the relevant claim element in its entirety. *Kyocera Senco Indus. Tools Inc. v. Int’l Trade Comm’n*, 22 F.4th 1369, 1378 (Fed. Cir. 2022) (holding that the specification’s statement that “[t]his bottom position is also sometimes referred to

herein as the ‘driven position’” was definitional as to “driven position” because “[n]othing about this statement suggests the ‘bottom position’ is merely an example of a driven position. It is *the* driven position.”) (emphasis original); *ParkerVision, Inc. v. Vidal*, 88 F.4th 969, 976 (Fed. Cir. 2023) (“The patentee’s use of the phrases ‘as used herein’ and ‘refer to’ conveys an intent for sentence 5 to be definitional.”) (citing *Kyocera*, 22 F.4th at 1378).

Thus, the specification’s teaching here that “[e]ach content encryption key in the history is *assigned a unique* identifier which is *referred to herein* as the content encryption key identifier,” Ex. 1001 at 3:28-32 (emphasis added), necessarily defines and limits the term “content encryption key identifier” as recited in the claims.

For that reason, Petitioner’s argument that the claims themselves do not expressly recite a unique identifier assigned to the corresponding content encryption key is beside the point. Reply at 20. And Petitioner’s argument that Patent Owner has not shown lexicography is likewise false. Reply at 20-21. Notably, Petitioner’s contention that the specification teaching at issue is directed to one embodiment of a server-side workflow manager is false. Reply at 21. The sentence at issue unequivocally defines the term “content encryption key

identifier” for all purposes, and in no way limits the meaning of that term based on any particular embodiment. Ex. 1001 at 3:28-32.

Petitioner’s contention that Peterka’s ECM sequence numbers or time stamps “closely track” the ’178 patent’s specification teachings regarding “content encryption key identifiers” are unavailing for the same reason. The specification requires that a “content encryption key identifier” be *uniquely assigned* to the corresponding content encryption key itself, whereas Peterka’s ECM sequence numbers and time stamps are assigned to a message (ECM) that itself carries *multiple* keys, and are thus not uniquely assigned to the content key within that message. POR at 39-40. Petitioner’s further argument that Peterka’s *message* identifiers are “unique enough” thus fails for the same reason—those identifiers are assigned to each message, which carries multiple keys, not to the specific content key within a message, as the challenged claims require. Reply at 21-22.

Petitioner’s pivot to its obviousness modification theories likewise fails. Petitioner’s Reply fails to address Patent Owner’s point that the Petition itself contends that Peterka’s *message* identifiers already adequately serve the purpose of differentiating between keys, thus defeating any motivation for modifying Peterka simply to meet the requirements of the challenged claims. POR at 40-41.

Moreover, with respect to Ground 5, the Petition's motivation rested on the premise that a client holding keys "for multiple future segments" would benefit from the uniquely assigned key identifiers of the challenged claims, but Patent Owner demonstrated that Peterka does not teach or render obvious a client holding keys for "multiple future segments," thus eliminating the condition precedent underlying the Petition's Ground 5 motivation. POR at 42-43. Petitioner's Reply once again fails to address (and thus concedes) that point.

Finally, Petitioner's assertion that an ordinary artisan would have been motivated to use key identifiers such as CK0, CK1, and CK2 as shown in Peterka's Figure 7B is plainly mistaken. Petitioner does not address Patent Owner's showing that the terms CK0, CK1, and CK2 in Peterka are never disclosed as *key identifiers*, but are rather merely *descriptive labels* provided in Peterka's written description for purposes of explanation and illustration. POR at 40-41. Since the Petition itself contends that Peterka's *message* identifiers adequately serve the purpose of differentiating between keys, the POSA would have no reason to modify Peterka to use the descriptive labels of Peterka's written description as actual key identifiers. The only reason for such a modification would be to meet

the requirements of the challenged claims, which is the essence of impermissible hindsight bias.

III. The Petition additionally fails as to the detecting and issuing requests limitations of [1D] and [1E]

Petitioner's Reply cannot demonstrate that the Petition's theory meets the actual "process *for detecting the rotation of content encryption keys*" set forth in Figure 3 of the '178 Patent. Ex. 1001 at 9:47-49; Fig. 3; Ex. 2010 ¶ 106. Instead, Petitioner argues that Patent Owner's explanation of what the detecting limitation requires "bears no relation to the claims, finds no support in the intrinsic record, and departs wildly from PO's previous allegations[.]" Reply at 24. Petitioner's attempt at misdirection is unavailing. The Patent Owner Response demonstrated in extensive detail, with support from Patent Owner's expert, that the specification defines the "process for detecting the rotation of content encryption keys" through Figure 3 and its associated teachings. POR at 43-49. Patent Owner showed that this "*process*" is what the "detecting" language of limitation [1D] requires, i.e., checking a key's expiration time *and* checking for an explicit key change notification for that key and then identifying the applicable key rotation boundary in light of both items of information. *Id.* Patent Owner specifically demonstrated that in the flow diagram of Figure 3, which defines the "detecting" limitation of the

claims, the client must *always* “check for key change notification” as stated in step 308. POR at 46; Fig. 3; Ex. 2010 ¶ 107. That step is not optional. *Id.*; Ex. 1001 at 10:39-42. The specification further teaches that at step 310, the client must check *both* the expiration time of the current key and any key change notification in order to detect the correct key rotation boundary for that key. POR at 45-46; Ex. 1001 at 11:2-7; Ex. 2010 ¶ 109. Indeed, the '178 Patent never teaches that identifying or even monitoring the expiration time of a key *alone* (without checking for any key change notification signals) can constitute “detecting” a key rotation boundary as recited in the claims. Ex. 2010 ¶ 111. Thus, contrary to Petitioner’s assertions, Patent Owner’s arguments are extensively supported by the intrinsic record and the claim language, and it is Petitioner that seeks to ignore the relevant evidence. Moreover, Petitioner’s assertion that Patent Owner’s Response presents a more robust understanding of the “detecting” limitation than the one set forth in its Preliminary Response is simply irrelevant. Patent Owner is not bound by its Preliminary Response arguments, and Patent Owner can (and should) adjust its positions in view of the Board’s Institution Decision where appropriate. Here, Patent Owner took note of the Board’s comments regarding the specification’s teachings as to the “detecting” limitation, and the explanation set forth in the POR

responds to and resolves the Board’s prior concerns. Those realities make Patent Owner’s position *more* credible, not less.

Petitioner’s Reply does not and cannot dispute that Peterka’s pull embodiment only relies on monitoring key expiration times in order to change content keys. Peterka’s pull embodiment thus cannot meet limitation [1D]. POR at 50-51.

As for the Petition’s key change signal notification theory, Patent Owner’s Response demonstrated that this theory fails for a separate reason—the “issuing requests” requirement of limitation [1E]. Patent Owner explained that in Peterka, clients do not “issue requests” for a new key where the rotation boundary is defined by a key change notification, as the combination of limitations [1D] and [1E] require. Rather, Peterka teaches that when a key change signal is issued, clients “can begin utilizing the new content key with which they *have been provided.*” Ex. 1005 ¶ 116 (emphasis added); POR at 52-53. Since clients have already been provided the key, there is no reason or basis for clients to issue a request for that key, as limitation [1E] requires. Moreover, Peterka’s clients operating under the pull model could not have issued a request for the new key *before* receiving a key change signal since they could not know a key change

signal was forthcoming. In sum, the two approaches are simply at odds and incompatible. Under the pull model, “the server need not monitor the status of the client’s keys[.]” Ex. 1005 ¶ 116. But under the key change signal method, the server *must* monitor the status of the client’s keys, since it is the server that decides when a key should be used and it is the server that informs the client of that change. POR at 53-54; Ex. 2010 ¶ 125.

Petitioner cannot grapple with those facts, so it instead argues that limitations [1D] and [1E] do not need to occur in the recited order. Reply at 25. But Petitioner misses the point. The argument was never that Peterka must teach receiving a key change notification first and then issuing a request for a new key second. Rather, it was simply that Peterka must teach doing *both* within the same embodiment. Peterka fails to do so because when Peterka provides a key change notification, it *also* provides the new key without the client issuing any request for that key, and when Peterka’s client requests a new key through its pull model, it *only* does so because of an upcoming expiration time, and never because of a key change signal. POR at 52-55. For the same reasons, it would not have been obvious to use Peterka’s key change signal with its pull model: Peterka’s clients cannot know whether to ask for a new key *before* they receive a signal to change keys, so

Peterka's clients cannot reliably pull the next key they will need when key change occurs due to a signaled notification. POR at 55; Ex. 2010 ¶¶ 123, 127-128.

Indeed, what key Peterka's client last pulled is the key that will have to be replaced due to the key change signal. Thus, Peterka's clients operating under the pull model cannot have pulled the key they will need in response to a key change notification.

Fleeing once again, Petitioner argues that Patent Owner "abandoned" the arguments it presents here during the ITC litigation. That contention is desperate and wishful. Patent Owner is not *limited* in this proceeding to the arguments it presented at the ITC, and Petitioner cannot identify any law that supports such a finding.

Finally, Petitioner's assertion that Peterka describes sending clients both the key lifetime and a key parity bit "***for comparing against key change signals in the stream***" fails to address Patent Owner's arguments or cure Peterka's deficiencies. Reply at 26 (emphasis added). As Petitioner itself states, the client only receives a parity bit for comparing against future potential key change signals. But this does not allow the client to determine *when* to issue a request for a new key in relation to a potential key change notification signal. The parity bit only allows the client to

identify a key change signal if and when one is sent to it. Under the pull model, however, it is the client that must request each next key, whereas under the key change signal approach, it is the *server* that tells the client to move to a new key with which the client has already “***been provided***.” Ex. 1005 ¶ 116 (emphasis added). As noted, these concepts are directly at odds. Even with the parity bit, clients operating under Peterka’s pull model cannot implement Peterka’s key change signal teaching of “utilizing the new content key with which they ***have been provided***” in response to a key change notification. Ex. 1005 ¶ 116 (emphasis added). Because Peterka’s clients operating under the pull model cannot know *when* to request a new key in relation to a key change signal that has not arrived, and because Peterka’s clients operating under the key change signal model *must* already *have* the new key when the key change signal is sent to them, the pull model and the key change signal model are simply incompatible and it would not have been obvious to combine them.

IV. Conclusion

For the reasons above, the Board should find all challenged claims not unpatentable.

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: November 12, 2025

CERTIFICATION OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned **PATENT OWNER'S SUR-REPLY** specified in 37 C.F.R. § 42.24 have 5,380 words, in compliance with the 5,600 word limit set forth in 37 C.F.R. § 42.24(b)(1). This word count was prepared using Microsoft Word 365.

/Kayvan Noroozi/
Kayvan Noroozi
11601 Wilshire Blvd., Suite 2170
Los Angeles, CA 90025
Tel.: 310-975-7074

Counsel for Patent Owner

Date: November 12, 2025

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing **PATENT OWNER'S SUR-REPLY** was served electronically via e-mail on November 12, 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: November 12, 2025