

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC and
LENOVO (UNITED STATES) INC.,
Petitioners,

v.

ERICSSON AB,
Patent Owner.

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

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	Introduction	1
II.	Background of the '178 Patent and the challenged claims	4
III.	Person of ordinary skill in the art	8
IV.	Claim construction	8
V.	The Petition's Ground 1 does not satisfy its burden as to limitations 1D/16E and 1E/16F	9
	A. The Petition's reliance on Peterka's "pull" embodiment cannot meet the claims' "detecting" requirement	9
	B. The Petition's alternative reliance on Peterka's bit signaling also cannot meet the claims as a whole	22
VI.	The Petition's Grounds 2-5 likewise fail to meet its burden as to limitations 1D/16E and 1E/16F	26
VII.	Conclusion	27

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”

I. Introduction

The '178 Patent, which is directed to “managing key rotation (use of a series of keys) and secure key distribution in over-the-top content delivery,” teaches two distinct key rotation scenarios. In the normal course of operation, there is a transition from one key to the next key (“rotation”) because of “normal period-based expiration” of the current key, Ex. 1001, 11:3-7, *i.e.*, because the “fixed duration lifespan” assigned to the current key has ended. *Id.* at 3:9-11. Crucially, in this scenario, “the license server **distributes** fixed duration lifespan information to the client.” *Id.* at 3:46-47 (emphasis added). The client is thus informed of when the current key will expire, and is made aware of the period-based key rotation boundary for that key **without** any need for the client to **detect** such a key rotation boundary. As a result, to adhere to a normal period-based key rotation boundary, the client simply “**checks** to see if the current content encryption key is going to expire in the near future[.]” *Id.* at 11:38-39 (emphasis added).

In the second key rotation scenario, however, the client may receive “an explicit key change notification . . . that applies to the current segment being decrypted.” *Id.* at 11:3-7. Such a notification informs the client that “a key change is signaled, *i.e.*, a key change was requested **outside** of any fixed duration lifespan.” *Id.* at 10:39-43 (emphasis added). In this non-period-based key rotation

scenario, the client receives the key change notification in a manifest file, a segment file name, or a header containing a flag that also “describes the expiration of the previous content encryption key and the content encryption key identifier of the new content encryption key to be applied.” *Id.* at 10:45-48, 10:54-57, 10:63-65. In this scenario, the client cannot identify the signaled key rotation boundary by performing a simple “check”—rather, the ’178 patent teaches that the client must “**detect**” the signaled key change and the signaled key rotation boundary. *Id.* at 11:38-41 (“the client 110 checks to see . . . if a content encryption key change request for a future segment **was detected**”) (emphasis added). “If a content encryption key change request is **detected**, the client notes the need to expire the current content encryption key and the content encryption key identifier of the new key to be used.” *Id.* at 10:65-11:1 (emphasis added).

Despite the ’178 Patent’s distinct use of the different terms “check” and “detect” to describe different steps in the context of the two different key rotation scenarios it teaches, the Petition rests its primary theory on **conflating** and equating the concepts of **checking** for an upcoming timer-based key rotation boundary with **detecting** a **non**-timer-based key rotation boundary. Pet. 31-33. On that basis, the Petition alleges that Peterka meets the “detecting” requirement of limitations 1D and 16E by “monitoring” or “checking” a timer for an upcoming key expiration.

Id. But as shown above and further demonstrated in detail below, that theory has no reasonable likelihood of success: “checking” is not “detecting,” either in the plain and ordinary meaning, or in the context of the ’178 Patent and its claims.

The Petition’s remaining alternative theories are further self-defeating and without basis. While the Petition attempts to rely on a different embodiment from Peterka in which a key change is signaled to the client, Peterka expressly teaches—and the Petition admits—that in that scenario the server *provides* the new key to the client without any request. That is fatal, however, because limitations 1E and 16F expressly require that the *client* request the new key, and the Board has already recognized that the “bit signaling” teachings of Peterka cannot meet the challenged claims for that very reason. IPR2022-00618, Paper 11 at 22 n.6. The Petition feebly alleges, in a single sentence, that it would have been obvious to modify Peterka to meet the challenged claims, but fails to provide *any reason why* an ordinary artisan would have allegedly been motivated to do so. And the Petition’s additional grounds, which are directed at other limitations and other claims, provide nothing further.

Accordingly, the Board should decline to institute the Petition.

II. Background of the '178 Patent and the challenged claims

United States Patent 9,313,178 (“the '178 Patent”), titled “Method and System for Secure Over-The-Top Live Video Delivery,” is directed to a method “for managing key rotation (use of series of keys) and secure key distribution in over-the-top content delivery.” Ex. 1001, 1 (Abstract).

The '178 Patent teaches that “[a]s content delivery models move away from streaming distribution over private networks to Web-based delivery of files over the public Internet, referred to as over-the-top (OTT) delivery, traditional content protection paradigms must be modified to support new delivery protocols, e.g., HTTP Live Streaming. For live streaming content with long or indefinite durations, use of a single encryption key for the entire duration increases the probability that the key may be compromised.” Ex. 1001, 1:18-26. The '178 Patent teaches that “[t]here are many protocols and methods for generating segmented content . . . each segment is independently playable, and therefore needs to be independently encrypted and decryptable. Segments are typically of a fixed duration and, in the case of video content, begin with a key-frame and contain no inter-segment references. Segmentation is performed on each of the different encoding generated by the transcoder, by parsing the resultant encoding and determining segment boundaries.” Ex. 1001, 2:46-58. “Segments are encrypted on segment boundaries

using the current content encryption key and current initialization vector (IV). . . .

The generation of new strongly random values for use as content encryption keys and the rotation of content encryption keys provides protection from content encryption keys being compromised in long lived streams.” *Id.* at 2:62-3:5.

The '178 patent teaches that “[t]he transitioning between use of different keys is [] referred to herein as key ‘rotation.’” *Id.* at 1:63:65. “In step 310, the client 110 checks the expiration of current content key to see if a new key should be applied. There are two cases—normal period-based expiration, and an explicit key change notification received in step 308 that applies to the current segment being decrypted.” *Id.* at 11:3-7. In the case of normal period-based expiration, “the workflow manager generates content encryption keys with a fixed duration lifespan on a fixed periodic basis.” *Id.* at 3:9-11. “[T]he license server distributes fixed duration lifespan information to client.” *Id.* at 3:46-47. By contrast, in the case of an explicit key change notification that is not period-based, the '178 patent teaches that “a key change is signaled, i.e., a key change [is] requested outside of any fixed duration lifespan,” for instance, “for security reasons[.]” *Id.* at 10:39-43. In particular, “the workflow manager may initiate content encryption key rotation at any time, outside of the fixed duration lifespan of the existing key.” *Id.* at 3:53-55. “The packager is responsible for providing in-band notification to the client for

the key change.” *Id.* at 4:13-15. The key change notification may be provided, for instance, in a manifest file (such as an m3u8 file, a Smooth Streaming file, or a DASH MPD file), or in the segment file name of the content, or in a header prepended to the content (such as a Microsoft PlayReady header, an MPEG/3GP DASH header, or a proprietary segment format header). *Id.* at 4:15-27. The notification from the packager to the client—whether as a flag in a header, a manifest file, or a file name—“describes the expiration of the previous content encryption key and the content encryption key identifier of the new content encryption key to be applied.” *Id.* at 10:45-48, 10:54-57, 10:63-65. “If a content encryption key change request is *detected*, the client notes the need to expire the current content encryption key and the content encryption key identifier of the new key to be used.” *Id.* at 10:65-11:1 (emphasis added).

Exemplary claim 1 correspondingly recites:

Element	Claim 1
[1.Pre]	A method for handling secure distribution of content comprising:
[1A]	initiating a media playback request and receiving a playback request response;
[1B]	parsing content information from the playback request response, the content information including content encryption keys, content

	encryption key identifiers, and content encryption key expiration times;
[1C]	retrieving content and manifest files from a content delivery server;
[1D]	detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content;
[1E]	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
[1F]	applying the second key for content decryption after the key rotation boundary is reached.

The Petition challenges claims 1-6, 10, 12, 14, 16-18, 20. The Petition's Grounds are summarized below.

Ground	References	Basis	Challenged Claims
1	Peterka	§ 103	1-6, 10, 12, 16-18, 20
2	Peterka, Suzuki	§ 103	1-6, 10, 12, 16-18, 20
3	Peterka, Bocharov	§ 103	1-6, 10, 12, 14, 16-18, 20

PATENT OWNER'S PRELIMINARY RESPONSE

4	Peterka, Suzuki, Bocharov	§ 103	1-6, 10, 12, 14, 16-18, 20
5	Peterka, Bocharov, Peterka308, Chen	§ 103	7-8, 19

III. Person of ordinary skill in the art

For purposes of this Preliminary Response, Patent Owner does not dispute the Petition's proposed level of skill for a person of skill in the art ("POSA"), because the level of skill in the art is not necessary for addressing any disputes between the parties.

IV. Claim construction

The Board does not construe claim terms that are not in dispute. *Shenzhen Liown Electronics Co. v. Disney Enterprises, Inc.*, IPR2015-01656, Paper 7 at 10 (Feb. 8, 2016) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). The Petition does not raise a dispute as to any claim construction issues. Pet. 9. Patent Owner does not believe the Board need resolve any claim construction issues at this stage. Nonetheless, to the extent the Board believes Patent Owner's arguments herein raise claim construction issues, Patent Owner provides the evidentiary bases and arguments in support of its positions below.

V. The Petition's Ground 1 does not satisfy its burden as to limitations 1D/16E and 1E/16F

A. The Petition's reliance on Peterka's "pull" embodiment cannot meet the claims' "detecting" requirement

The Petition's primary theory relies on Peterka's pull embodiment, in which Peterka's clients "monitor" the expiration time for a current segment. Pet. 32. The Petition contends that **monitoring** key expiration times, i.e., monitoring a timer, constitutes "**detecting** content encryption key rotation boundaries" as recited by limitation 1D. Pet. 32-33 (emphasis added).

That theory does not meet the plain language of limitation 1D, is inconsistent with the teachings of the specification, and wrongly conflates the plain and ordinary meaning of "monitoring" and "checking"—on the one hand—with "detecting" on the other.

"Claim terms are generally given their plain and ordinary meanings to one of skill in the art when read in the context of the specification and prosecution history." *DDR Holdings, LLC v. Priceline.com LLC*, 2024 U.S. App. LEXIS 31009, at *6 (Fed. Cir. Dec. 9, 2024) (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc)).

Here, the claim language at issue recites "**detecting** content encryption key rotation boundaries"—it does **not** recite either "monitoring" or "checking for" key

rotation boundaries. The claim language on its face is thus not met by merely “monitoring” or “checking” for key rotation boundaries, such as by monitoring or checking a timer.

The Petition nonetheless attempts to equate “checking” with “detecting,” asserting that the specification “describes *detecting* such boundaries by: (1) *checking* the expiration time of the current key (normal period-based expiration) or (2) *checking* for an explicit key change notification/signal.” Pet. 31-32 (emphases added). That is false. To the contrary, the specification never equates “checking” the expiration time or “checking” for a notification with “*detecting*” a key rotation boundary. Rather, as explained below, the specification consistently distinguishes between merely checking and the further distinct step of “detecting.”

In describing step 308 of Figure 3, the patent teaches that “the client 110 *checks* to see if a key change is signaled, i.e., a key change was requested outside of any fixed duration lifespan.” Ex. 1001, 10:39-42 (emphasis added). The patent then further teaches that *only* “[i]f a content encryption key change request is *detected*, the client notes the need to expire the current content encryption key and the content encryption key identifier of the new key to be used.” Ex. 1001, 10:65-11:1 (emphasis added). The patent thus teaches that “*checking*” for a key change notification signal is a separate and preceding step to “*detecting*” such a

notification, and thus a key rotation boundary. Stated otherwise, the patent teaches that the client must first **check** for a key change signal, and then (when available) **detect** such a signal. Expiration of a current key and rotation to a new key occurs only if the client has **detected** a key change signal, **not** simply because the client has **checked** for a key change signal. Ex. 1001, 10:65-11:1.

It is the separate step of “**detecting**” the key change notification—not the mere act of “checking”—that is recited by the claims, and that is necessary to meet the claims. *See* limitation 1D & 16E.

The patent further evidences the distinction between “checking” and “detecting” through its careful use of those two separate terms in describing step 316 of Figure 3. The patent teaches: “In step 316, the client **checks** to see if the current content encryption key is going to **expire** in the near future **or** if a content encryption key change request for a future segment was **detected** in step 308.” Ex. 1001, 11:38-41 (emphasis added). Thus, in the case of a normal period-based expiration, the client only “**checks** to see if the current content encryption key is going to expire[.]” *Id.* By contrast, in the context of a non-period-based “key change request,” the client “**checks** to see . . . if a content encryption key change request for a future segment **was detected** in step 308.” *Id.* Stated otherwise, identifying a period-based key rotation boundary only requires “checking” for an

upcoming expiration, whereas identifying a non-period-based key rotation boundary requires ***detecting*** such a boundary. Ex. 1001, 11:38-41.

Other passages of the '178 patent likewise consistently distinguish between monitoring or checking the time remaining on a segment timer, on the one hand, and the distinct act of ***detecting*** a key change notification. For instance, the '178 patent further teaches: "If the current content encryption key is not close to expiring ***and*** a content encryption key change request was ***not detected*** in step 308, processing proceeds back to step 306" Ex. 1001, 11:45-48 (emphasis added). And to the same effect, "[i]f 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." Ex. 1001, 11:48-53 (emphasis added). In both instances, the '178 patent again distinguishes between time-based key rotation boundaries (those based on the key "expiring") and key change ***requests*** that must be "***detected***." The patent thus once again distinguishes between, and does not equate, the separate acts of (1) monitoring or checking a timer for an upcoming key expiration and (2) "***detecting***" a ***non***-timer-based key change request.

Critically, in no instance does the '178 Patent use the term “detect” to describe a key change boundary associated with the expiration of a timer. And in no instance does the '178 Patent teach that merely *checking* for a non-timer-based key change notification is equivalent to actually *detecting* such a key rotation boundary.

The '178 Patent's consistent distinction between “checking” for a timer expiration and “detecting” a non-timer-based key change request is further supported by the patent's teachings as to how the client is provided with information regarding each of those two distinct key rotation boundaries.

In the case of normal period-based expiration, “the license server *distributes* fixed duration lifespan information to the client.” *Id.* at 3:46-47 (emphasis added). The client thus has no need to *detect* normal period-based key rotation boundaries, and instead simply “*checks* to see if the current content encryption key is going to expire in the near future[.]” *Id.* at 11:38-39 (emphasis added).

By contrast, in the case of non-period-based key change request, “the packager 104 notifies the client 110 of the key change by prepending a header to the encrypted content which contains a flag that describes the expiration of the previous content encryption key and the content encryption key identifier of the new content encryption key to be applied.” Ex. 1001, 10:43-48. The header may

be, for instance, a “Microsoft PlayReady header,” an “MPEG/3GP DASH header,” or a “proprietary segment format header.” Alternatively, the key change notification can be provided “by updating a manifest file that describes the encrypted content with a flag that describes the expiration of the previous content encryption key and the content encryption key identifier of the new content encryption key to be applied.” Ex. 1001, 10:50-58. That manifest file may be, for instance, “an m3u8 file,” a “Smooth Streaming manifest file,” or a “DASH MPD file.” In another embodiment, “the packager 104 notifies the client 110 of the key change in the file name of the encrypted content by appending a flag that describes the expiration of the previous content encryption key and the content encryption key identified of the new content encryption key to be applied.” Ex. 1001, 10:58-65.

In this scenario, the client cannot identify the signaled key rotation boundary by performing a simple “check”—rather, the ’178 patent teaches that the client must “*detect*” the signaled key change and the signaled key rotation boundary by discovering them through an analysis of headers, manifest files, and/or file names that may contain at least partly hidden flags signaling a key change. *Id.* at 11:38-41 (“the client 110 checks to see . . . if a content encryption key change request for a future segment *was detected*”) (emphasis added). “If a content encryption key

change request is ***detected***, the client notes the need to expire the current content encryption key and the content encryption key identifier of the new key to be used.” *Id.* at 10:65-11:1 (emphasis added).

Thus, while the patent’s description of step 308 in the flow diagram of Figure 3 states “***check*** for key change notification,” the specification makes clear that the initial step of *checking* for the notification is not equivalent to the further step of “*detecting*” such a notification. Ex. 1001, 10:39-42 (teaching that at “step 308 [] the client 110 ***checks*** to see if a key change is signaled, i.e., a key change was requested outside of any fixed duration lifespan.”); *id.* at 10:65-11:1 (further teaching that only “[i]f a content encryption key change request is ***detected***, the client notes the need to expire the current content encryption key. . . .”) (emphases added). It is the further act of “***detecting***,” and not simply the preliminary and distinct act of “checking,” that is recited by claims 1, 16, and their dependents, and that is necessary to meeting those claims. Indeed, the ’178 Patent later reiterates the same distinction by teaching that “[i]n step 316, the client ***checks*** to see . . . if a content encryption key change request for a future segment was ***detected*** in step 308.” *Id.* at 11:38-41 (emphasis added). Thus, while the patent teaches that the client “checks” for a key change notification, and “checks” if a key change request was “***detected***,” the patent teaches that it is the act of ***detecting*** that identifies the

non-period-based key rotation boundary, not the act of checking if such a detection occurred or if such a notification was received. *Id.* at 10:39-42, 10:65-11:1, 11:38-41, 11:45-53.

The patent's distinct use of the terms "check" and "detect" is further supported by the distinct plain and ordinary meanings of those two terms as provided by dictionary definitions. The Cambridge Dictionary defines "check" as "to make certain that something or someone is correct, safe, or suitable by examining it, him, or her quickly," or "to find out about something." Ex. 2002 (also available at: <https://dictionary.cambridge.org/us/dictionary/english/check>). By contrast, the Cambridge Dictionary defines "detect" as "to notice something that is *partly hidden or not clear*, or to *discover* something, especially using a special method," or "to discover something, usually using special equipment." Ex. 2003 (also available at: https://dictionary.cambridge.org/us/dictionary/english/detect#google_vignette) (emphasis added); *Masimo Corp. v. Sotera Wireless, Inc.*, 2023 U.S. App. LEXIS 25626, at *6-7 (Fed. Cir. Sept. 28, 2023) (confirming that the Board may rely on dictionary definitions so long as they do not contradict the intrinsic evidence).

Thus, a key rotation boundary defined by the expiration of a timer is simply "checked," i.e., identified through quick examination of the timer. *See* Ex. 1001,

11:38-41 (“In step 316, the client 110 **checks** to see if the current content encryption key is going to expire in the near future”) (emphasis added). That makes perfect sense because a timer only a quick examination, and requires no discovery of information that is even partly hidden or not clear. Indeed, the ’178 Patent teaches that “the license server **distributes** fixed duration lifespan information to the client.” *Id.* at 3:46-47 (emphasis added). By contrast, a key rotation boundary defined by, for instance, a notification from the server to the client, must be detected precisely because such a boundary is not clear and is at least partly hidden in a flag in a manifest file, a header, or a segment file name. Ex. 1001, 10:65-11:1 (“If a content encryption key change request is **detected**, the client notes the need to expire the current content encryption key”) (emphasis added); *id.* at 10:43-65.

Accordingly, the Petition’s theory based on Peterka’s pull embodiment—which only teaches clients “checking” or “monitoring” a timer for normal period-based expiration, Pet. at 31-33—cannot meet the “**detecting**” requirement of limitations 1D and 16E.

In addition to the above analysis and evidence, that conclusion is further supported by at least two past decisions that have likewise refused to equate “detect” with other distinct terms used in the patents at issue. In *Apple Inc. v. Omni*

MedSci, Inc., 2024 U.S. App. LEXIS 15066 (Fed. Cir. June 21, 2024), the Federal Circuit refused to construe “identify an object” and “detect an object” as having interchangeable meanings. *Id.* at *8-*13. In particular, the Federal Circuit “reject[ed] Apple’s argument that the specification *consistently* and interchangeably refers to ‘identify’ and ‘detect’ in a manner sufficient to overcome the usual presumption that those different terms have different meanings.” *Id.* at *12 (emphasis original). And in *CenTrak, Inc. v. Sonitor Techs. Inc.*, 2015 U.S. Dist LEXIS 173756 (D. Del. Jan. 4, 2016), the District of Delaware refused to equate “detect” with “receive.” *Id.* at *7-*14. As with the Federal Circuit, the District of Delaware emphasized that the patent’s use of different words carries a presumption that the terms have different meanings, and found that the intrinsic evidence and dictionary definitions only further confirmed that presumption. *Id.* at *14 (“The claim language, specification, and prosecution history of the ‘909 patent, as discussed above, accurately reflect the distinct meanings of these two different words. Likewise, Defendant fails to point to any convincing evidence in the specification or prosecution history to suggest the patentee meant these two distinct words to mean the same thing, or for either term to depart from its plain and ordinary meaning.”).

And giving distinct meaning to the separate terms “check” and “detect” is also supported by various usage examples showing that “checking” and “detecting” are distinct acts, even where they are related. *See, e.g., Vivint, Inc. v. Alarm.com Inc.*, 754 F. App'x 999, 1006 (Fed. Cir. 2018) (describing art teaching the use of “error *checking* to *detect* a compromised communication path”) (emphasis added); Ex. 2004 (U.S. Pat. 10,136,452) at 25:11-15 (“the UE will perform a CCA *check* and *detect* a successful CCA”) (emphasis added).

Here, the patentee's distinct use of the terms “check” and “detect” to describe different steps and actions within the context of the '178 patent, as well as the distinct plain and ordinary meanings of those two terms, likewise should not be overridden or ignored.

Because the plain and ordinary meaning of “detect” is not met by simply checking or monitoring a timer for a key rotation boundary, and because the '178 patent repeatedly distinguishes “detecting” a key change request from the separate act of monitoring and checking the timer for an upcoming key expiration time, the Petition cannot meet the “detecting” limitation of claims 1, 16, and their dependents by relying on Peterka's teaching of monitoring or checking a timer for key rotation boundaries. *See* Ex. 1001, 11:45-48 (“If the current content encryption key is not close to expiring **and** a content encryption key change request was **not**

detected in step 308, processing proceeds back to step 306”); *id.* at 11:48-53

(“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).

Nor does Patent Owner’s explanation above “improperly limit[] the scope of the claim to one aspect of the disclosed embodiment of the ’178 patent,” as the Board was previously concerned. *See* IPR2022-00618, Paper 11 (Inst. Dec.) at 20.

As an initial matter, Claim 16 and its dependents are system claims. Claim 16 simply recites a device that is designed to “detect content encryption key rotation boundaries” in the manner described above. Claim 16 and its dependents do not require actual detection to be met. Rather, those claims simply cannot be met by a design like Peterka’s pull embodiment, in which no “detection” of key rotation boundaries can occur, and where instead key rotation boundaries are exclusively defined by timer expiration periods that the client need only check and monitor. As for the method of claim 1 and its dependents, Patent Owner’s explanation above does not limit those method claims to only being met by key rotation boundaries defined by *notifications*. Rather, those method claims can be met by any type of key rotation boundary that requires *detection* (which, as

explained above, cannot encompass merely timer-based key rotation boundaries).

That is because the claim is not limited to detecting *notifications*, but rather is directed to detecting content encryption key rotation boundaries, which may be defined by means other than notifications. At the same time, timer-based key rotation boundaries cannot meet the “detecting” limitation of the claims because they neither require nor entail any detection, and are instead simply identified through mere checking and monitoring, as the specification itself teaches. *See, e.g.*, Ex. 1001, 11:38-41 (“In step 316, the client ***checks*** to see if the current content encryption key is going to ***expire*** in the near future ***or*** if a content encryption key change ***request*** for a future segment was ***detected*** in step 308.”) (emphasis added). Accordingly, Patent Owner’s explanation does not unduly limit the claims. It merely comports with the patentee’s express claim language, and is consistent with the patentee’s repeatedly distinct use of “detecting” to describe an act that goes beyond mere “checking.”

In sum, the “detecting” limitation does not refer to *all* key rotation boundaries because not all key rotation boundaries require or entail the step of “detecting” as recited in the claims. *Cf.* IPR2022-00618, Paper 11 (Inst. Dec.) at 21. The Petition thus cannot meet the challenged claims by simply relying on Peterka’s timer-based key rotation boundaries, which merely require the client to

“monitor” or “check” for such boundaries, and which Peterka’s client need not and does not “detect.”

B. The Petition’s alternative reliance on Peterka’s bit signaling also cannot meet the claims as a whole

The Petition alternatively relies on Peterka’s teaching of signaling a “predetermined bit” to notify the client of a key change, citing Peterka’s paragraphs 116 and 117. Pet. at 33-34. The Petition’s alternative theory also fails.

Peterka’s paragraphs 116 and 117 are part of Peterka’s “push” embodiment, in which a new key is sent to the client *without any request*. To that end, Peterka’s paragraph 116 teaches: “when a new content key is implemented, the implementation will be signaled to the clients so that the clients can begin utilizing *the new content key with which they have been provided*.” Ex. 1004 ¶ 116 (emphasis added). And Paragraph 117 further discloses that at the time the client receives the “predetermined bit” upon which the Petition’s alternative theory relies, “a new key [] has recently *been distributed* to the client.” Ex. 1004 ¶ 117 (emphasis added). In the embodiments of paragraphs 116-121, the client thus *already has* the new key, and does not issue any request for a new key.

That evidence is fatal to the Petition’s alternative “bit signaling” theory because limitations 1E and 16F expressly require that the *client request* a new key from the server ahead of an upcoming key rotation boundary. Accordingly, the

Petition's alternative theory based on Peterka's bit signaling cannot meet the challenged claims as a whole.

Indeed, the Board previously recognized that reality, stating that "Petitioner's alternative reliance on the disclosure in Peterka of using a predetermined bit to signal encryption key rotation boundaries, outside the context of the 'pull model' embodiment, is not persuasive because the new keys being signaled are not received in response to request from the client for a new key." IPR2022-00618, Paper 11 (Inst. Dec.) at 22 n. 6.

Seeking to sidestep the problem, the Petition contends that Peterka's teachings regarding its bit signaling are not "exclusive" to its push model. Pet. at 33. That assertion is false, and is directly refuted by Peterka. As noted, the Petition relies on Peterka's paragraphs 116 and 117 for the teaching of the bit signaling. Pet. at 33. In paragraph 116, Peterka expressly teaches: "when a new content key is implemented, the implementation *will be signaled* to the clients so that clients can begin utilizing *the new content key with which they have been provided.*" Ex. 1005 ¶ 116 (emphasis added). Thus, Peterka's paragraph 116 unequivocally ties the use of the bit signaling to the provision of a new key from the server to the client without any request from the client. Peterka's paragraph 117 is to the same effect, stating: "a predetermined bit can be used to indicate if an old or current

content key should be used as opposed to a new content key *which has recently been distributed to the client.*” Ex. 1005 ¶ 117 (emphasis added). As Peterka’s paragraph 117 states, the predetermined bit can only instruct the client to use one of three keys, all of which the client *already has received* without any request—an old key, a current key, or a new “which has recently been distributed to the client.” *Id.* Peterka’s bit signaling teaching is thus intimately tied to, and inseparable from, its “push” embodiment, and cannot be relied upon to meet the challenged claims as a whole. In any case, the Petition identifies no embodiment from Peterka in which (1) a bit signal is provided from the server to the client requesting a non-timer-based key change; *and* (2) the client *requests* a new key from the server, rather than automatically receiving one from the server, as limitations 1D/16E and 1E/16F require.

Attempting to sidestep the problem once again, the Petition contends that “signaling when to use a key in the client’s possession does not require Peterka’s server to push updated keys.” Pet. 33-34 (emphasis removed). But that argument attempts to flip Petitioner’s burden and the law of unpatentability on its head: Peterka’s only teaching is that Peterka’s server *does* push updated keys to the client along with its signal as to which key should be used, and the Petition thus cannot demonstrate unpatentability based on Peterka’s signaling teachings. Moreover, the

Petition's own statement acknowledges that Peterka's signaling instructs the client "to use a key *in the client's possession*." Pet. 33-34 (emphasis added). Since the key is in the client's possession already, Peterka's client plainly does not "issu[e] *requests* to a license server ahead of a key rotation boundary to *retrieve* a second content encryption key. . . .," as limitations 1E and 16F require.

Finally, the Petition's contention that "using Peterka's key change signaling with Peterka's pull model would have been obvious" cannot meet its prima facie burden. Pet. 34. That allegation appears in a single sentence. *Id.* It is entirely devoid of any discussion. Indeed, the Petition does not even allege (much less provide evidence of) a *motivation* for its naked obviousness allegation. *In re Nuvasive*, 842 F.3d 1376, 1382-83 (Fed. Cir. 2016) (requiring "*a reason why* a PHOSITA would combine the prior art references") (emphasis original). The Petition's *ipse dixit* obviousness contention thus cannot demonstrate a reasonable likelihood of success. *KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) ("Rejections on obviousness grounds cannot be sustained by mere conclusory statements."). Moreover, the Petition itself acknowledges that Peterka's signaling instructs the client "to use a key *in the client's possession*." Pet. 33-34 (emphasis added). There would thus be no reason to modify Peterka's client to "pull" a key that is already "*in the client's possession*." Pet. 33-34 (emphasis added).

VI. The Petition's Grounds 2-5 likewise fail to meet its burden as to limitations 1D/16E and 1E/16F

The Petition's Grounds 2, 4, and 5 are irrelevant to limitations 1D/16E and 1E/16F and thus cannot support institution in view of the above.

The Petition's Ground 3 likewise continues to rely on the same theories with respect to limitations 1D/16E and 1E/16F. Pet. 61-62. Since those limitations cannot be met for the reasons above, the Petition's additional arguments regarding the additional limitations of dependent claims 12 and 20 are likewise irrelevant.

Nonetheless, the Petition's additional reliance on Bocharov does not warrant institution as to those dependent claims. In Bocharov, there is no teaching of content encryption keys at all, and the Petition never contends or demonstrates otherwise. Bocharov thus does not teach "detecting" content encryption key rotation boundaries. Moreover, Peterka's bit signal is already accompanied by a new key from the server to the client, without any client request, and thus combining Peterka's signaling with Bocharov's manifest file cannot meet limitations 1E/16F and the challenged claims as a whole.

Finally, the Petition's obviousness allegation as to the combination of Peterka and Bocharov likewise cannot meet its prima facie burden. Pet. 64. The Petition alleges, in a single sentence, that "it would have been obvious to implement Peterka-Bocharov's manifest to provide information needed for clients

to detect the need for and acquire the keys necessary to switch to a different encoding.” Pet. 64. But once again, that assertion is devoid of any discussion, and does not so much as allege (much less provide evidence of) a *motivation*. *Nuvasive*, 842 F.3d at 1382-83 (requiring “a reason why a PHOSITA would combine the prior art references”); *KSR*, 550 U.S. at 418 (“Rejections on obviousness grounds cannot be sustained by mere conclusory statements.”). And the Petition’s fleeting obviousness modification ignores and fails to reconcile with the fact that Peterka’s bit signal instructs the client “to use a key *in the client’s possession*.” Pet. 33-34 (emphasis added). There is thus no need or reason for Peterka’s client to “acquire” any keys in response to a bit signal notification, as the Petition’s modification theory proposes, because Peterka’s client already *has* the necessary key. The Petition cannot be instituted as to any claim based on fleeting, entirely unsupported, and self-defeating obviousness assertions that do not meet the Petition’s basic legal requirements.

VII. Conclusion

For the reasons above, the Board should decline to institute the Petition.

Respectfully submitted,

/s/ Kayvan B. Noroozi

Peter C. Knops, Reg. No. 37,659
Kayvan B. Noroozi, *Pro Hac Vice*

PATENT OWNER'S PRELIMINARY RESPONSE

NOROOZI PC
11601 Wilshire Blvd., Suite 2170
Los Angeles, CA 90025
Attorneys for the Patent Owner

Date: January 16, 2025

CERTIFICATION OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned **PATENT OWNER'S PRELIMINARY RESPONSE** specified in 37 C.F.R. § 42.24 has 5,992 words, in compliance with the 14,000 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

Counsel for Patent Owner

Date: January 16, 2025

CERTIFICATION OF SERVICE

The undersigned hereby certifies that the foregoing **PATENT OWNER'S PRELIMINARY RESPONSE** was served electronically via e-mail on January 16, 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: January 16, 2025