

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

ERICSSON AB,
Patent Owner.

Case IPR2022-00618
Patent No. 9,313,178

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	Introduction	1
II.	Background of the ’178 Patent and the challenged claims	3
III.	Person of ordinary skill in the art	6
IV.	The Petition fails to meet claims 6, 12-15, and 20	7
V.	The Petition fails to meet limitation 1.4 and 16.5, properly construed, and thus fails as to all challenged claims.	10
	A. “[D]etecting content encryption key rotation boundaries <i>between periods of use</i> ” should be construed to mean detecting key rotation boundaries <i>before</i> normal period-based expiration	11
	B. Patent Owner’s claim construction is not inconsistent with the concerns expressed in the Institution Decision	17
	C. The Petition’s theory cannot meet the challenged claims under the correct interpretation of limitations 1.4 and 16.5	21
VI.	Conclusion	22

EXHIBIT LIST

Exhibit No.	Description
2001	Declaration of Kayvan B. Noroozi in Support of Motion for Admission <i>Pro Hac Vice</i>
2002	U.S. Patent Publ. No. 2014/0237243 (publication of U.S. Application No. 14/266,368 filed April 30, 2014)
2003	U.S. Provisional Application Ser. No. 61/500,316, filed Jun. 23, 2011
2004	U.S. Patent No 2012/0331293(Publication of U.S. Patent Application Ser. No.: 13/530,997, filed on Jun. 22, 2012)

I. Introduction

As the Board's Institution Decision recognized, the Petition does not demonstrate unpatentability at least as to claims 6, 12-15, and 20.

Claim 6 recites prefetching a next key “after the *expected* expiration of the content encryption key *currently being applied*. . .” Ex. 1001 at 12:40-47 (emphasis added). The claim is thus directed to the situation where a current key is not expired by the packager 104 at the *expected* expiration time suggested by the workflow manager 102, and a new key is prefetched (*i.e.*, obtained prior to the retirement of the current key) after the *expected* expiration time of the current key. The Petition, by contrast, attempts to meet claim 6 by alleging that in the combination Peterka and Bocharov, “a client device would request a new content encryption key . . . *before* the *expected* expiration of the content encryption key currently being applied,” Pet. at 40 (emphasis added)—the exact opposite of what claim 6 requires. The Petition thus cannot prevail as to claim 6.

The Petition likewise fails as to claims 12-15 and 20. Whereas those claims require that the client issue a request for a new key, the Petition's theory relies on an embodiment in Peterka in which “new keys are not received in response to [a] request from the client for a new key,” as the Board has correctly found. Paper 11

at 26; *see also id.* at 22 n. 6. Accordingly, the Petition cannot establish unpatentability as to claims 12-15 and 20.

Moreover, as this Response demonstrates, the Petition's theory fails to meet independent claims 1 and 16, and thus all challenged claims, under the proper construction of “detecting content encryption key rotation boundaries *between periods of use*,” as recited in limitations 1.4 and 16.5. The '178 patent's specification consistently teaches that “period of use” and similar phrases refer to the normal period-based duration set for an encryption key. *See* Section V.A, *infra*. The claims' requirement of “detecting content encryption key rotation boundaries *between* periods of use” is thus limited to detecting rotation boundaries that arise *before* the normal period-based expiration time for a current key, such as due to a key change notification issued by the server. Accordingly, the claims cannot be met by a method or a system that is incapable of detecting pre-expiration time rotation boundaries.

At the same time, as demonstrated below, Patent Owner's claim construction is not inconsistent with the concerns raised by the Board in its Institution Decision. *See* Section V.B, *infra*. As an initial matter, Patent Owner's construction does not *exclude* from the scope of the claims the embodiment of changing encryption keys based on the expiration time of a current key. Rather, that embodiment is captured

by limitations 1.5 and 16.6 and is fully within the scope of the claims, provided that the “detecting” requirement of limitations 1.4 and 16.5 is met. Moreover, Patent Owner’s construction is also consistent with the Board’s grammatical analysis of limitations 1.4 and 16.5, as well as the specification’s teachings regarding steps 316 and 308 of Figure 3, which the Board had emphasized.

By contrast, construing the claims to encompass a method or system that *cannot* detect pre-expiration time rotation boundaries would fail to give meaning to the phrase “*between periods of use*,” and would be inconsistent with core claim construction principles. *SIPCO, LLC v. Emerson Elec. Co.*, 939 F.3d 1301, 1307 (Fed. Cir. 2019) (quoting *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1119 (Fed. Cir. 2004)).

Because the Petition’s only relevant theory—which relies on Peterka’s “pull” embodiment—exclusively requests new keys based on the expiration time of the current key, and lacks any ability to detect pre-expiration time key rotation boundaries, the Petition fails to demonstrate unpatentability under the proper construction of the challenged claims. *See* Section V.C, *infra*.

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 at 1, Abstract. The '178 Patent has 20 claims. The only independent claims are claim 1, which is directed to a method for handling secure distribution of content, and claim 16, which is directed to a computerized device operable as a client for handling secure distribution of content.

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 at 1:15-26. 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.*, 2:62-3:5.

Exemplary claim 1 correspondingly recites:

Element	Claim 1
[1.P]	A method for handling secure distribution of content comprising:
[1.1]	initiating a media playback request and receiving a playback request response;
[1.2]	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;
[1.3]	retrieving content and manifest files from a content delivery server;
[1.4]	detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content;
[1.5]	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
[1.6]	applying the second key for content decryption after the key rotation boundary is reached.

The Petition challenges claims 1-20 based on the Grounds below.

Ground	References	Basis	Challenged Claims
1A	Peterka, Bocharov	§ 103	1-4, 6-7, 12-13, 16-20
1B	Peterka, Bocharov, Peterka308, Chen	§ 103	7-9, 14-15, 19
1C	Peterka, Bocharov, Balraj	§ 103	5
1D	Peterka, Bocharov, Kelly	§ 103	10
1E	Peterka, Bocharov, Kelly, Eisen	§ 103	11

III. Person of ordinary skill in the art

For purposes of this 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. The Petition fails to meet claims 6, 12-15, and 20

Claim 6 recites the method of claim 4, further comprising “prefetching a next un-retrieved key within a period of time after the *expected* expiration of the content encryption key *currently being applied*, the period of time beginning at the *expected* expiration of the content encryption key *currently being used*, and ending at a duration calculated as a fixed percentage of a fixed periodic content encryption key expiration interval.” (emphasis added).

In its Institution Decision, the Board expressed concern that “prefetching *after* expiration does not make sense in the context of the ’178 patent.” Paper 11 at 26 (emphasis Board’s).

Claim 6, however, does not recite prefetching after *expiration*. Rather, it recites prefetching after “*expected* expiration of the content encryption key *currently* being applied,” and giving weight and meaning to the term “expected” and the phrase “currently being applied” is critical to a correct understanding of the claim and the associated teachings of the specification.

As the ’178 patent explains, content encryption keys are not necessarily expired at the exact time provided by the workflow manager 102 (WFM 102). Ex. 1001 at 8:9-13, 9:1-3. For instance, the ’178 patent teaches that “the fixed duration for key rotation may be viewed as a ‘target’ period, as the packager 104 may not

expire a key on the exact boundary,” and “[g]enerally, the packager 104 will not expire a key *earlier* than the end of a target period.” *Id.* at 8:9-13 (emphasis added). Thus, the ’178 patent teaches that content encryption keys may be expired at a time that is different than the intended or expected rotation time provided by the WFM 102, and in particular at a time *later* than the intended or expected rotation time. *Id.* To the same effect, the ’178 patent teaches that “[t]he key expiration time from the WFM 102 may be viewed as a ‘suggested’ expiration time, as the packager 104 may not be able to expire the key at the exact specified time.” *Id.* at 9:1-3. Moreover, the ’178 patent further teaches that “if the packager 104 is unable to obtain a new content encryption key from the WFM 102 prior to the expiration of the current content encryption key, the packager 104 will continue to use the current content encryption key until such time as it is able to obtain a new key from the WFM 102.” *Id.* at 6:33-37. Stated otherwise, a content encryption key can remain in use after its *expected* expiration until the packager 104 has obtained a new key from the WFM 102.

Claim 6 captures the specification’s above teachings. The term “prefetching” in the context of the claim makes sense as it refers to obtaining a new key before ceasing to use a current key, with the additional nuance that the “prefetching” occurs *after* the time when the current key was *expected* to expire.

As the Board has already recognized, the Petition's combination of Peterka and Bocharov does not meet the requirements of claim 6. Paper 11 at 26. Indeed, the Petition asserts that under its combination, "a client device would request a new content encryption key . . . *before* the *expected* expiration of the content encryption key currently being applied. . . ." Pet. at 40 (emphasis added). The Petition's theory is thus exactly the opposite of what claim 6 recites: whereas claim 6 requires prefetching a new key *after* the expected expiration of the current key, the Petition proposes retrieving a new key "*before* the expected expiration" of the current key. Pet. at 40 (emphasis added). Accordingly, the Petition cannot establish that claim 6 is unpatentable.

The Petition likewise fails to establish unpatentability as to claims 12-15 and 20, as the Board has also recognized. Paper 11 at 26-27, 29. As the Board correctly found in its Institution Decision, the Petition's theory as to claims 12-15 and 20 "relies on the embodiment disclosed in Peterka wherein a parity bit or other means is used to notify the client that a new encryption key has been sent." Paper 11 at 26. But as the Board has further found, "this embodiment does not teach or suggest the subject matter of claim 1 [and claim 16] because the new keys are not received in response to [a] request from the client for a new key." *Id.* at 26; *see also id.* at 22 n. 6. Because claims 12-15 depend from claim 1 and claim 20 depends from claim

16, and because Peterka's parity bit embodiment cannot meet the underlying requirements of claims 1 and 16, the Petition's reliance on Peterka's parity bit embodiment also cannot establish unpatentability as to claims 12-15 and 20. *Id.* at 26-27, 29.

Accordingly, at least original claims 6, 12-15, and 20 should be upheld.

V. The Petition fails to meet limitation 1.4 and 16.5, properly construed, and thus fails as to all challenged claims.

The Board's Institution Decision correctly found that the Petition's theory based on Peterka's use of a predetermined bit to signal encryption key rotation boundaries "is not persuasive because the new keys being signaled are not received in response to request from the client for a new key," as required by claims 1 and 16. Paper 11 at 22 n. 6. The Board likewise correctly declined to consider any theory based on the "combination of the push and pull model" of Peterka, "which was not raised by Petitioner. . . ." *Id.*

Thus, the only theory at issue with respect to claims 1 and 16, and limitations 1.4 and 16.5 in particular, is Peterka's "pull model," in which "each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire. . . ." Paper 11 at 22.

As demonstrated below, however, the correct construction of limitations 1.4 and 16.5 requires detecting key rotation boundaries *before* normal period-based

expiration, which Peterka's pull model does not permit. Accordingly, the Petition's theory based on Peterka's pull model cannot demonstrate unpatentability as to any challenged claim.

A. “[D]etecting content encryption key rotation boundaries *between periods of use*” should be construed to mean detecting key rotation boundaries *before* normal period-based expiration

As a general rule of claim construction, “all claim terms are presumed to have meaning in a claim.” *SIPCO, LLC v. Emerson Elec. Co.*, 939 F.3d 1301, 1307 (Fed. Cir. 2019) (quoting *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1119 (Fed. Cir. 2004)). Thus, in *SIPCO*, the Federal Circuit reversed the Board's claim construction as unreasonably broad because it failed to give meaning to the term “low-power” in “low-power transceiver.” *SIPCO*, 939 F.3d at 1308. In particular, the Court found that a “*low-power* transceiver,” understood in view of the specification, was limited to a device with a limited transmission range. *Id.*

Here, the claim language at issue in limitations 1.4 and 16.5 does not simply recite “detecting content encryption key rotation boundaries.” Rather, the relevant claim language recites “detecting content encryption key rotation boundaries *between periods of use* of different content encryption keys.” Accordingly, a proper construction must give meaning and weight not simply to the requirement

of detecting content encryption key boundaries, but more specifically to detecting such rotation boundaries “*between periods of use.*”

As explained in the Preliminary Response, Paper 9 at 11, the '178 patent teaches two methods by which a current content encryption key can be expired: “*normal period-based expiration and an explicit key change notification.*” Ex. 1001 at 11:4-7 (emphasis added).

The '178 patent consistently uses the phrase “periods of use” to refer to the normal period-based duration of a content encryption key, *i.e.*, the fixed duration lifespan intended for that key as defined by the expiration period set by the WFM 102. For instance, the '178 patent teaches “generating a series of content encryption keys and providing them serially to a packaging server for encrypting a content item, wherein each content encryption key is provided upon *expiration* of a *period of use* of a serially preceding content encryption key.” 1:45-50 (emphasis added). In the above teaching, the specification expressly refers to the “expiration” of a “period of use” of a content encryption key, and thus plainly teaches that the phrase “period of use” is synonymous with the normal period-based duration intended for a key, as defined by the expiration period set by the WFM 102. Similarly, the '178 patent further teaches that “[t]he lifespan of the new content encryption key may be aligned to the *periodic use period boundaries* of the

previous content encryption keys.” *Id.* at 7:29-31 (emphasis added). The patent thus once again uses the term “periodic use period boundaries” to refer to the normal period-based expiration time of the content encryption key. The ’178 patent likewise teaches “a fixed ***period duration*** for key rotation,” *id.* at 8:7-10 (emphasis added), and “a periodic content encryption key expiration event.” *Id.* at 8:29-32.

Thus, the ’178 patent repeatedly and exclusively uses the term “periods of use” and similar phrases such as “periodic use period boundaries” and “fixed period duration” to refer to the normal period-based expiration of a content encryption key.

Given the patent’s consistent usage of “periods of use” and similar phrases to refer to the intended length of the normal period-based duration of an encryption key, it follows that the phrase “***between*** periods of use” as recited in claim 6 must mean an event that occurs ***during*** the current use period (or fixed-duration intended lifespan) of a current encryption key. Accordingly, giving meaning to the phrase “***between periods of use***” as recited in claim 6 requires interpreting limitations 1.4 and 16.5 to require “detecting content encryption key rotation boundaries” that arise ***during*** the normal period-based duration of a current key (*i.e.*, ***before*** the current key’s period-based rotation boundary would otherwise occur), such as due to an “explicit key change notification.” Ex. 1001 at 11:4-7.

That understanding of limitations 1.4 and 16.5 is well-supported by other teachings from the specification. The '178 Patent teaches that the workflow manager may issue a new *unsolicited* content encryption key, *id.* at 7:3-4, which in one embodiment “is pushed ahead of the current content encryption key with *explicit instructions* to apply the key as soon as possible, in which case the packager 104 *does not wait* until the current content encryption key has expired before applying the new content encryption key.” *Id.* at 7:11-16 (emphasis added).

The '178 Patent further explains that the WFM 102 may, for instance, “push[] the new content encryption key to the packager 104 when the current content encryption key is deemed to be no longer secure (e.g., if the content encryption key has been compromised).” *Id.* at 7:17-20.

Consistent with the above teachings, Fig. 3 of the Patent (shown below) depicts a flow chart describing a process for detecting the rotation of content encryption keys and retrieving updated content encryption keys.

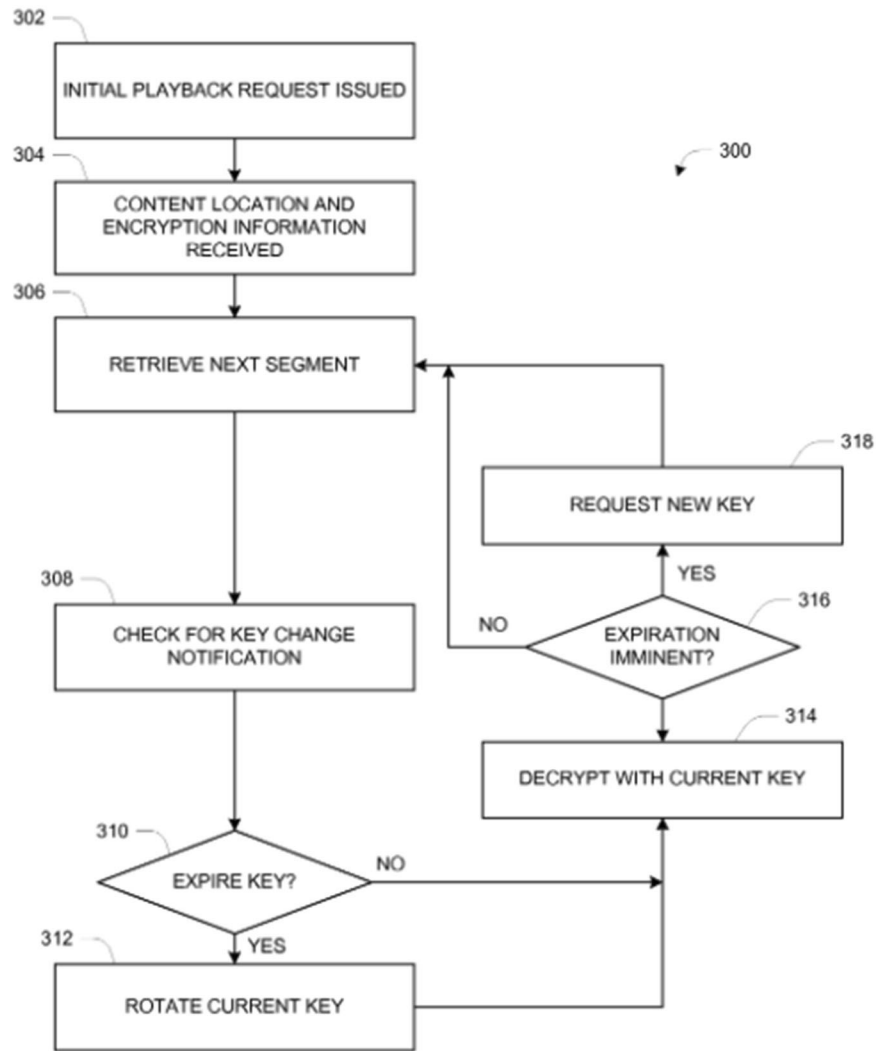


Fig. 3

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 10:39-43 (emphasis added). “If a content encryption 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. The client 110 then proceeds to step 310.” *Id.* at 10:65-11:2 (emphasis added).

“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.*** If the current content encryption key has not yet expired, processing proceeds to step 314. If the current content encryption key needs to be expired, processing proceeds to step 312 where the key is ‘rotated’, i.e., the current content encryption key is expired and a new one is put into use.” *Id.*, 11:3-12 (emphasis added).

Giving proper meaning to the phrase “between periods of use” as recited in claims 1 and 16 and in view of the specification’s relevant teachings thus requires interpreting limitations 1.4 and 16.5 to require detecting whether a key rotation boundary must occur ***before*** the time-based expiration of the current key (i.e., “***between periods of use*** of different content encryption keys”).

By contrast, interpreting the claims to encompass methods or systems that are incapable of detecting pre-expiration time key rotation boundaries would fail to give meaning to the phrase “***between periods of use***,” and would thus be inconsistent with fundamental precepts of claim construction. *SIPCO, LLC v.*

Emerson Elec. Co., 939 F.3d 1301, 1307 (Fed. Cir. 2019) (quoting *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1119 (Fed. Cir. 2004)).

B. Patent Owner's claim construction is not inconsistent with the concerns expressed in the Institution Decision

Patent Owner recognizes that the Board's Institution Decision expressed several concerns with respect to adopting Patent Owner's proposed construction of limitations 1.4 and 16.5. Respectfully, however, Patent Owner's construction is not inconsistent with the Board's concerns, as demonstrated below.

First, Patent Owner's construction does *not* "limit[] the scope of the claim to one aspect of the disclosed embodiment of the '178 patent that deals with the special case of key changes requested for security reasons outside of any fixed duration lifespan." Paper 11 at 20-21. As Patent Owner explained in its Preliminary Response, limitations **1.5** and **16.6** encompass issuing requests for a new encryption key due to *either* (1) normal period-based expiration (i.e., the end of the current key's fixed duration lifespan) *or* (2) a key change instruction detected by the client in between the current key's period of use (i.e., before the current key's normal period-based expiration). Paper 9 at 15-16. In that respect, limitations 1.5 and 16.6 thus capture steps 316 and 318 of Fig. 3, which teach that "[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.*” *Id.* at 11:48-53 (emphasis added).

Thus, Patent Owner’s construction only limits the scope of *limitations* 1.4 and 16.5, but it does not exclude the embodiment of requesting a new key based on the normal period-based expiration of the current key from the scope of claims 1 and 16 *as a whole*.

Stated otherwise, under Patent Owner’s construction claims 1 and 16 cannot be met where a client *cannot* detect whether a key rotation boundary has been set prior to the normal period-based expiration of a current key (i.e., “between periods of use” as recited in limitation 1.4 and 16.5), but claims 1 and 16 can be met where a client performs that detection step, concludes that no such pre-period-based rotation is necessary, and simply requests a new key prior to period-based expiration of the current key for use after the current key’s period-based expiration (as covered within the scope of limitations 1.5 and 16.6).

Second, Patent Owner agrees with the Board that “it is the ‘*boundaries*’ that are ‘*between periods of use*’ of different content encryption keys,”” Paper 11 at 21 (emphasis Board’s). That observation is entirely consistent with Patent Owner’s construction, wherein limitations 1.4 and 16.5 require that the client

detect whether there is a key rotation boundary “between periods of use” of current keys, *i.e.*, before the normal period-based expiration of a current key.

By contrast, interpreting limitation 1.4 to encompass merely recognizing that the fixed duration set for a current key is close to expiration would not constitute detecting a boundary that is “*between periods of use* of different content encryption keys,” and would give no meaning to the crucial phrase “*between periods of use*,” in violation of the Federal Circuit’s repeated precedents. *SIPCO, LLC v. Emerson Elec. Co.*, 939 F.3d 1301, 1307 (Fed. Cir. 2019) (quoting *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1119 (Fed. Cir. 2004)).

Third, the “detecting” limitation does not correspond to step 316 of Figure 3. *Cf.* Paper 11 at 21-22. Rather, step 316 corresponds to the next limitation of the claims (the “issuing requests” limitation, or limitations 1.5 and 16.6). The specification teaches that: “In step 316, the client 110 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 at 11:38-41 (emphasis added). The phrase “was detected” is only used in reference to a “key change request” requiring rotation of a current key prior to its normal period-based expiration. Thus, that is the only type of key rotation

boundary for which “detection” is taught to occur. Moreover, the use of the past tense—“*was detected*”—teaches that the “detecting” step has *already occurred* at step 308, *prior* to step 316. By contrast, at step 316 the client performs a further step—*checking* whether the current key is either set to expire soon *or* if a change request was received for key rotation prior to the key’s natural expiration. The “checking” aspect of step 316 is not expressly recited in any claim limitation, but is ultimately captured by limitations 1.5 and 16.6, which require issuing a request for a new key ahead of the rotation boundary of the current key. To that end, the specification teaches that as part of step 316, “[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.” *Id.* at 11:48-53 (emphasis added).

Thus, Patent Owner’s construction is not inconsistent with the Board’s concerns about reading the teachings of step 316 out of the claims. Rather, Patent Owner’s construction continues to encompass step 316’s method of proceeding to step 318, and requesting a new key, *regardless* of whether the current key is close to expiration or a key change request “*was detected*” at step 308, as encompassed by limitations 1.5 and 16.6.

C. The Petition's theory cannot meet the challenged claims under the correct interpretation of limitations 1.4 and 16.5¹

It is undisputed that under Peterka's "pull" embodiment, which is the only embodiment relevant to this proceeding in view of the Board's Institution Decision, the client device does not "detect" any key rotation boundaries prior to the normal period-based expiration of the current key.

As the Petition itself admits, Peterka's "pull" embodiment, as disclosed in Peterka's paragraphs 105, 106, 114, and its Fig. 8, simply teaches that the client keeps track of "*known key expiry times* that allow the client to request new keys *ahead of the expiration* or key rotation boundary." Pet. at 35 (emphasis added). Peterka's paragraph 105 further teaches that in its "*pull model*," "each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire so as to avoid service interruptions." Ex. 1004 ¶ 105. The other passages the Petition cites—Peterka's paragraph 106, 114, and Fig. 8—all teach the same.

Peterka's "pull" model does not include the possibility of any key change notification received by the client ahead of the natural key expiry time of a current key, nor any other non-time-based key rotation boundary, and there is thus no such

¹ The Petition solely relies on Peterka as teaching or suggesting limitations 1.4 and 1.5. Pet. at 34-36.

non-time-based key rotation boundary for the client to “detect,” as required in limitations 1.4 and 16.5. To the contrary, Peterka teaches that in its “pull model,” the *client* makes all key change determinations, entirely based on the expiration time of the current key. Ex. 1004 ¶ 105 (“Under the pull model, each client keeps track of the keys and their expiration times and actively requests new keys before current keys expire so as to avoid service interruptions. *Alternatively*, the push model migrates responsibility to the server which keeps track of active clients and distributes new keys to them before the current keys expire.”); *id.* ¶ 106 (explaining that under the pull model, “the server need not monitor the status of the client’s keys; rather, *the responsibility of determining when a new key is required can be passed to the client.*”) (emphasis added).

Accordingly, the Petition cannot establish unpatentability as to any challenged claim under the proper construction of limitations 1.4 and 16.5.

VI. Conclusion

For the reasons above, the Board should find all challenged claims not unpatentable, and at least should find claims 6, 12-15, and 20 not unpatentable.

Respectfully submitted,

/s/ Kayvan B. Noroozi

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

Kayvan B. Noroozi, *Pro Hac Vice*
NOROOZI PC
11601 Wilshire Blvd., Suite 2170
Los Angeles, CA 90025
Attorneys for the Patent Owner

Date: November 28, 2022

CERTIFICATION OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned **PATENT OWNER'S RESPONSE** specified in 37 C.F.R. § 42.24 has 4,662 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: November 28, 2022

CERTIFICATION OF SERVICE

The undersigned hereby certifies that the foregoing **PATENT OWNER'S RESPONSE** was served electronically via e-mail on November 28, 2022, on the following counsel of record for Petitioner:

LEAD COUNSEL	BACK-UP COUNSEL
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 3200 RBC Plaza 60 South Sixth Street Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR50095-0082IP1@fr.com	Thomas A. Rozylowicz, Reg. No. 50,620 Nicholas W. Stephens, Reg. No. 74,320 3200 RBC Plaza 60 South Sixth Street Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 PTABInbound@fr.com

/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 28, 2022