

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ERICSSON INC.,

Petitioner

v.

KONINKLIJKE KPN N.V.¹,

Patent Owner

Case No. IPR2023-00902

U.S. Patent No. 9,438,572

PATENT OWNERS' PRELIMINARY RESPONSE

¹ The Petition names only Koninklijke KPN N.V. as Patent Owner, but the patent is co-owned by Koninklijke KPN N.V. and Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO, on both of whose behalf this Patent Owners' Preliminary Response is submitted.

Table of Contents

I.	INTRODUCTION	1
II.	THE '572 PATENT, THE REFERENCES RELIED UPON IN THE PETITION, AND THE PROPOSED GROUNDS FOR INSTITUTION	1
A.	The '572 Patent	1
B.	References Relied Upon in the Petition	3
1.	WO 2012/112124 A1 of Teo ("Teo") (Ex. 1005).....	3
2.	U.S. Patent App. Pub. No. 2013/0067552 of Hawkes <i>et</i> <i>al.</i> ("Hawkes") (Ex. 1006)	3
3.	Network Working Group, Request for Comments 4279, Eronen and Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)" ("RFC 4279") (Ex. 1007)	4
4.	U.S. Patent App. Pub. No. 2001/0019614 of Madoukh ("Madoukh") (Ex. 1011).....	4
5.	Document S3-070234 to 3GPP TSG SA WG3 Security Meeting #46b ("S3-070234") (Ex. 1013)	4
6.	U.S. Patent App. Pub. No. 2007/0171910 A1 of Kumar ("Kumar") (Ex. 1016).....	4
7.	U.S. Patent App. Pub. No. 2009/0016524 A1 of Park <i>et</i> <i>al.</i> ("Park") (Ex. 1017).....	5
8.	U.S. Patent App. Pub. No. 2009/0181643 A1 of Thakare ("Thakare") (Ex. 1018)	5
C.	Proposed grounds of institution	5
III.	THE CHALLENGED INDEPENDENT CLAIMS	6
IV.	CLAIM CONSTRUCTION	9

A.	Claim Construction Standard	9
B.	In Claim [1a], the initiation key must be associated with a “validity period” relative to which the validity of the initiation key is verified “based on a current time,” where the “validity period” cannot be a single point in time.....	9
C.	In Claim elements [1b] and [1d], the session key is generated “if the initiation key is deemed valid,” which is premised upon the initiation key having had its validity verified “based on a current time”	12
D.	Similar considerations apply to the “validity period,” and to the session key being generated “if the initiation key is deemed valid,” which is premised upon the initiation key having had its validity verified “based on a current time,” in independent Claims 15, 16, and 17.....	14
V.	THE PETITION DOES NOT ESTABLISH A REASONABLE LIKELIHOOD THAT ANY OF CLAIMS 1-17 OF THE ’572 PATENT IS UNPATENTABLE	14
A.	Ground 1 should be denied for failure to establish a reasonable likelihood that Teo in view of Madoukh renders Claims 1, 2, and 14 unpatentable.....	15
1.	Claim [1a]; the Petition fails to establish that Teo in view of Madoukh teach an initiation key that is associated with a “validity period” relative to which the validity of the initiation key is verified “based on a current time,” and where the “validity period” is not a single point in time	15
2.	Claim elements [1b] and [1d]; the Petition fails to establish that Teo in view of Madoukh teaches a session key that is generated “if the initiation key is deemed valid,” which is premised upon the initiation key having had its validity verified “based on a current time”	18
3.	Dependent Claims 2 and 14	20

4.	Lack of Reasonable Likelihood of Ground 1.....	21
B.	Ground 2 should be denied for failure to establish a reasonable likelihood that Teo in view of Madoukh and Hawkes renders Claims 3-5 and 15-17 unpatentable.....	21
C.	Ground 3 should be denied for failure to establish a reasonable likelihood that Teo in view of Madoukh and RFC 4279 renders Claims 6-9 unpatentable.....	22
D.	Ground 4 should be denied for failure to establish a reasonable likelihood that Teo in view of Madoukh, RFC 4279, and Kumar renders Claim 10 unpatentable.....	25
E.	Ground 5 should be denied for failure to establish a reasonable likelihood that Teo in view of Madoukh and S3-070234 renders Claims 11 and 12 unpatentable	26
F.	Ground 6 should be denied for failure to establish a reasonable likelihood that Teo in view of Madoukh and Thakare renders Claim 13 unpatentable.....	26
VI.	CONCLUSION.....	27

Table of Authorities

Cases

<i>Harmonic Inc. v. Avid Tech., Inc.</i> , 815 F.3d 1356 (Fed. Cir. 2016).....	14
<i>In re Robertson</i> , 169 F.3d 743 (Fed. Cir. 1999)	24
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	9

Statutes

35 U.S.C. § 312(a)(3).....	14
35 U.S.C. § 313	1

Other Authorities

<i>Colas Solutions Inc. v. Blacklidge Emulsions Inc.</i> , IPR2016-01031, Paper 38 (P.T.A.B. November 2, 2017).....	24
--	----

Rules

37 C.F.R. § 42.107	1
37 C.F.R. § 42.24	29
37 C.F.R. § 42.24(b)(1).....	29
37 C.F.R. § 42.6(e).....	30

I. INTRODUCTION

Koninklijke KPN N.V. and Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO (“Patent Owners”), the co-owners of the patent, respectfully submit this Preliminary Response in accordance with 35 U.S.C. § 313 and 37 C.F.R. § 42.107, responding to the Petition for *inter partes* review (the “Petition”) filed by Ericsson Inc. (“Petitioner”) challenging Claims 1-17 (“the challenged claims”) of U.S. Patent No. 9,438,572 (the “’572 Patent”).

Petitioner has failed to meet its burden for at least the reasons that Petitioner fails to show that any of its references, or their combination, teach (i) an initiation key that is associated with a “validity period” relative to which the validity of the initiation key is verified “based on a current time,” where the “validity period” cannot be a single point in time, nor (ii) a session key being generated “if the initiation key is deemed valid,” which is premised upon the initiation key having had its validity verified “based on a current time.”

For the reasons set forth more fully below, institution should be denied.

II. THE ’572 PATENT, THE REFERENCES RELIED UPON IN THE PETITION, AND THE PROPOSED GROUNDS FOR INSTITUTION

A. The ’572 Patent

The ’572 Patent discloses a method for establishing a device-to-device (D2D) communication session between mobile devices, each of which are

individually connectable to a mobile network, and which are mutually connectable via a D2D communication channel. *See* Ex. 1001 at 1:12-14; 7:44-64. The method provides the advantage of giving more control to an operator of the mobile network over the D2D communications between mobile devices which are connectable to the mobile network. *See id.* at 2:23-25. Toward that end, the method involves preloading an initiation key on each of two mobile devices. *See id.* at 8:22-24. The initiation key is associated with a validity period, and the method involves, on each mobile device, verifying a validity of the initiation key based on the current time by determining whether the current time falls within the validity period. If the initiation key is deemed valid on each of the mobile devices, a session key is generated by using the initiation key in performing a key agreement procedure between the two mobile devices over the D2D communication channel, which results in the session key based on a match of the respective initiation keys used by each of the mobile devices. *See id.* at 8:25-47. The method then establishes a D2D communication session of the D2D communication channel based on the session key. *See id.* at 2:44-45.

Among other things, the method can provide an operator of the mobile network with control over D2D communications, for example by managing the frequency spectrum which is licensed by the operator, *e.g.*, to avoid interference;

or by granting only specific users access to the D2D communication, such as subscribers to a D2D service. *See id.* at 2:11-22.

B. References Relied Upon in the Petition

1. WO 2012/112124 A1 of Teo (“Teo”) (Ex. 1005)

Teo teaches a cellular mobile communication system that determines an encryption key for secure communication between communication terminals via a radio interface, which can include direction communication between the terminals without the data being communicated via a base station of the network. *See Ex. 1005 at 1:28-2:10.* The Petition cites Teo as teaching that its pre-shared Direct Communication Master Key or DMK has an associated lifetime, known as the “key_lifetime.”

2. U.S. Patent App. Pub. No. 2013/0067552 of Hawkes *et al.* (“Hawkes”) (Ex. 1006)

Hawkes teaches a technique of authentication in secure user plane location (SUPL) systems. A security credential that is specific to a mobile device is stored at the mobile device. The security credential is transmitted to a SUPL location platform to authenticate the mobile device as associated with a SUPL user based on a comparison of the device identifier to a stored device identifier. *See Ex. 1006 at [0009].*

3. Network Working Group, Request for Comments 4279, Eronen and Tschofenig, “Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)” (“RFC 4279”) (Ex. 1007)

RFC 4279 teaches protocols to support authentication of clients to servers using pre-shared keys (PSKs). *See* Ex. 1007 at 4-5.

4. U.S. Patent App. Pub. No. 2001/0019614 of Madoukh (“Madoukh”) (Ex. 1011)

Madoukh teaches a computer system that uses a hidden link dynamic key manager to provide increased security for encrypted data. *See* Ex. 1011 at [0005]. The system includes a key lifetime manager that monitors encryption key expiration dates and requests new encryption keys upon the expiration of old encryption keys. *See id.* at [0007].

5. Document S3-070234 to 3GPP TSG SA WG3 Security Meeting #46b (“S3-070234”) (Ex. 1013)

S3-070234 is cited in the Petition as describing “counters related to limiting key usage, e.g. to limit the number of key derivations from one parent key.” *See* Ex. 1013 at 1-2.

6. U.S. Patent App. Pub. No. 2007/0171910 A1 of Kumar (“Kumar”) (Ex. 1016)

Kumar teaches peer-to-peer communication in an ad hoc wireless network. A wireless device performs discovery of a target wireless device, performs authentication of the target wireless device, generates a session key, forms an ad

hoc wireless network with the target wireless device, and communicates peer-to-peer with the target wireless device via the ad hoc wireless network. See Ex. 1016 at Abstract.

7. U.S. Patent App. Pub. No. 2009/0016524 A1 of Park *et al.* (“Park”) (Ex. 1017)

Park teaches distributing keys within an ad hoc peer-to-peer network, where the key can have an expiration time. *See* Ex. 1017 at Abstract. Park is not relied upon as a combined reference in any of the combinations in the six grounds in the Petition.

8. U.S. Patent App. Pub. No. 2009/0181643 A1 of Thakare (“Thakare”) (Ex. 1018)

Thakare teaches testing authenticity of a packet in a packet-based communication between a mobile radio and a base station. Packets that fail the authenticity test are removed from the communication, retransmission of failed packets may be requested, and a new encryption key may be requested. *See* Ex. 1018 at [0008]-[0009].

C. Proposed grounds of institution

The proposed grounds are summarized in the table below:

Ground	'572 Patent Claims	Primary Reference	Secondary References	Type of Challenge
1	1, 2, 14	Teo ²	Madoukh	pre-AIA 35 U.S.C. § 103(a)
2	3-5, 15-17	Teo	Madoukh and Hawkes	pre-AIA 35 U.S.C. § 103(a)
3	6-9	Teo	Madoukh and RFC 4279	pre-AIA 35 U.S.C. § 103(a)
4	10	Teo	Madoukh, RFC 4279, and Kumar	pre-AIA 35 U.S.C. § 103(a)
5	11, 12	Teo	Madoukh and S3-070234	pre-AIA 35 U.S.C. § 103(a)
6	13	Teo	Madoukh and Thakare	pre-AIA 35 U.S.C. § 103(a)

III. THE CHALLENGED INDEPENDENT CLAIMS

The Petition should be denied institution because it fails to establish a reasonable likelihood that any of Claims 1-17 of the '572 Patent is unpatentable.

The challenged independent claims are as follows.

Independent Claim 1 reads:

1. Method for establishing a device-to-device (D2D) communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising:
preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period; and on each of the mobile devices:
verifying a validity of the initiation key based on a current time;

² Patent Owner does not concede the availability against the '572 Patent of any of the references relied upon in Grounds 1-6 as prior art under pre-AIA 35 U.S.C. § 103(a).

requesting a further initiation key via the mobile network if no initiation key is deemed valid;

if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel, the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices; and

establishing the D2D communication session over the D2D communication channel based on the session key.

Independent Claim 15 reads:

15. A non-transitory computer-readable medium configured to store instructions for, upon execution of the instructions on a mobile device, causing the mobile device to establish a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, by:

storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period;
verifying a validity of the initiation key based on a current time;
requesting a further initiation key via the mobile network if no initiation key is deemed valid;

if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; and

establishing the D2D communication session over the D2D communication channel based on the session key.

Independent Claim 16 reads:

16. Mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, the mobile device comprising:

- a storage area for storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period; and

- a computer subsystem for:

- verifying a validity of the initiation key based on a current time;

- requesting a further initiation key via the mobile network if no initiation key is deemed valid;

- if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; and

- a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.

Independent Claim 17 reads:

17. Mobile network arranged for preloading an initiation key on a mobile device when the mobile device is connected to the mobile network, the initiation key being associated with a validity period, the mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to the mobile network, the mobile device comprising:

- a computing subsystem for:

- verifying a validity of the initiation key based on a current time;

- requesting a further initiation key via the mobile network if no initiation key is deemed valid;

if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; and

a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.

IV. CLAIM CONSTRUCTION

A. Claim Construction Standard

In an *inter partes* review proceeding, claim terms are construed according to the same claim construction standard used in district courts as articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*). Without necessarily agreeing with the claim constructions identified in the Petition, Patent Owner here discusses the construction of claim terms that are relevant in the below discussion of claim elements, and which will be used in showing that institution should be denied.

B. In Claim [1a], the initiation key must be associated with a “validity period” relative to which the validity of the initiation key is verified “based on a current time,” where the “validity period” cannot be a single point in time

In element [1a], Claim 1 recites preloading an initiation key on each of the mobile devices, the “initiation key being associated with a *validity period*”

(emphasis added). *See* Ex. 1001 at 18:12-13. Subsequently, in element [1b], Claim 1 recites “verifying a **validity** of the initiation key ***based on a current time***” (emphasis added). *See id.* at 18:14-15.³ Taken together, based on the plain and ordinary meaning of these claim elements (as demonstrated by the words of the claim itself), the initiation key must be associated with a “validity period” relative to which the validity of the initiation key is verified “based on a current time.” The “validity period” cannot be a single point in time.

This construction follows from the plain meaning of the phrase “validity period,” which implies that the time period must be a time period for the “validity,” which is subsequently verified in element [1b] based on the current time. This plain meaning from the claim language is reinforced by the context throughout the specification of the ’572 Patent. For example, the specification describes that the “initiation key is associated with a validity period. The method 100 further comprises, on each of the mobile devices MD, verifying 140 a validity of the initiation key based on a current time... Hence, verifying the validity of the initiation key may comprise ***determining whether the current day falls within the***

³ Element [1a] recites “preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period”; *see* Ex. 1001 at 18:11-13; element [1b] recites “verifying a validity of the initiation key based on a current time”; *see id.* at 18:14-15.

validity period, and if so, whether the current day is either a first day or a last day of the validity period, and if so, whether the current time of the day falls within the validity period.” *See id.* at 8:25-41. A further example is given in the table at Col. 10 of the ’572 Patent, which shows a set of initiation keys each being “valid from” a certain time and “valid through” another time and describing that “the set of validity periods may be constituted at least in part by different but overlapping validity periods.” *See* Col. 10, lines 20-22. In addition, the dependent claims reinforce the requirement of a “validity period” in Claim 1, for example, in Claim 6 (the initiation keys “being associated with a respective set of validity periods”) and Claim 9 (“wherein the set of validity periods is constituted at least in part by different but overlapping validity periods”). These dependent claims, as well as the above passages from the specification, reinforce that the “validity period” must be a ***time period*** extending between a different starting time and ending time, and cannot be a single point in time.

Such passages, and the dependent claims, reinforce the plain language of claim elements [1a] and [1b], which have a clear requirement that the initiation key must be associated with a “validity period” relative to which the validity of the initiation key is verified “based on a current time,” and that the “validity period” cannot be a single point in time.

C. In Claim elements [1b] and [1d], the session key is generated “if the initiation key is deemed valid,” which is premised upon the initiation key having had its validity verified “based on a current time”

In element [1b], Claim 1 recites “verifying a validity of the initiation key based on a current time.” *See* Ex. 1001 at 18:14-15. In element [1d], Claim 1 continues with, “if the initiation key is deemed valid, generating a session key using the initiation key.” *See id.* at 18:18-19.⁴ Taken together, based on the plain and ordinary meaning of these claim elements (as demonstrated by the words of the claim itself), the session key is generated “*if* the initiation key is deemed valid” (emphasis added), which must be *premised upon* the initiation key having had its validity verified “based on a current time.”

This construction follows from the plain meaning of the phrase “if the initiation key is deemed valid,” which both implies conditionality of the generation of the session key on the initiation key having been deemed valid, and also refers back to the validity of the initiation key having been verified “based on a current

⁴ Element [1b] recites “verifying a validity of the initiation key based on a current time,” *see* Ex. 1001 at 18:14-15; element [1d] recites “if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel, the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile keys,” *see id.* at 18:18-24.

time” in element [1b]. This plain meaning from the claim language is reinforced by the context throughout the specification of the ’572 Patent. For example, the specification describes: “Hence, verifying the validity of the initiation key may comprise determining whether the current day falls within the validity period... The method 100 further comprises, on each of the mobile devices MD, *if the initiation key is deemed valid*, generating 160 a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices MD over the D2D communication channel DDC.” *See* Ex. 1001 at 8:36-47 (emphasis added). In addition, for example, the table in Col. 10 of the ’572 Patent shows examples of validity periods being “valid from” certain times and “valid through” certain times. *See* Col. 10, lines 1-23.

Such passages reinforce the plain language of claim elements [1b] and [1d], which have a clear requirement that the session key is generated “*if* the initiation key is deemed valid” (emphasis added), which must be *premised upon* the initiation key having had its validity verified “based on a current time.”

These claim constructions will be compared with the Petition and its cited references, below.

D. Similar considerations apply to the “validity period,” and to the session key being generated “if the initiation key is deemed valid,” which is premised upon the initiation key having had its validity verified “based on a current time,” in independent Claims 15, 16, and 17

As with Claim 1, elements [15a]/[15b]/[15d], [16a]/[16b]/[16d], and [17p]/[17a]/[17c], of independent Claims 15, 16, and 17, respectively, recite a “validity period,” and a session key being generated “if the initiation key is deemed valid” by having its validity verified “based on a current time,” in ways that are similar in relevant regards to elements [1a]/[1b]/[1d], above, and similar claim constructions (adapted for the “computer-readable medium,” “mobile device,” and “mobile network” context of those claims) apply to those corresponding elements for the same reasons.

V. THE PETITION DOES NOT ESTABLISH A REASONABLE LIKELIHOOD THAT ANY OF CLAIMS 1-17 OF THE ’572 PATENT IS UNPATENTABLE

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)).

Petitioner has failed to meet its burden.

A. Ground 1 should be denied for failure to establish a reasonable likelihood that Teo in view of Madoukh renders Claims 1, 2, and 14 unpatentable

1. Claim [1a]; the Petition fails to establish that Teo in view of Madoukh teach an initiation key that is associated with a “validity period” relative to which the validity of the initiation key is verified “based on a current time,” and where the “validity period” is not a single point in time

The Petition fails to establish that the cited combination of references teach element [1a], as construed above, because the Petition fails to show that Teo and Madoukh, or their combination, teach verifying the validity of an initiation key relative to a “validity period” based on “a current time,” where the “validity period” is not a single point in time.

To the contrary, the Petition cites Teo as teaching that, in a “Pre-shared key scenario,” its pre-shared Direct Communication Master Key or DMK (which the Petition identifies with the “initiation key”) has an associated lifetime, known as the “key_lifetime.” *See* Pet. at 12, 23. However, even if the DMK of Teo has a “key_lifetime,” the Petition makes no showing that this “key_lifetime” of Teo is a “validity period” that is used in *verifying the “validity” of the initiation key by being compared with a current time* as required by Claim 1. Contrary to the Petition’s assertion, *see* Pet. at 24, Teo does not teach any use of received

timestamps in relation to the “key_lifetime.” Timestamps such as T_{HR-BS} ’ and T_{HR-BS} ’ in Teo are disclosed to be used to determine whether a received message is fresh. *See, e.g.*, Ex. 1005 at 13-14 (“message freshness”). But contrary to what Petitioner seems to imply, such received timestamps are not taught as being used in relation to a “key_lifetime,” either in Teo or in Madoukh. In fact, Teo is silent on whether the “key_lifetime” of its DMK is used to determine validity or expiry of the DMK, let alone how such monitoring would occur. For the feature of verifying the validity of the initiation key, the Petition turns to a combination with Madoukh, which teaches requesting “new encryption keys upon the expiration of old encryption keys.” *See* Pet. at 24, citing Ex. 1011 at [0007]. However, even if combined (which is not conceded as obvious), the combination of Teo with Madoukh would merely involve only requesting new encryption keys “upon the expiration” of old encryption keys. And Madoukh makes clear that such a procedure of requesting new encryption keys upon the expiration of old ones merely involves comparing a current time with a single point in time: the “expiration” time of the old encryption key. *See* Ex. 1011 at [0007] (“a key lifetime manager operable to monitor encryption key expiration dates and request new encryption keys upon the expiration of old keys,” the “encryption keys change or rotate upon the occurrence of desired rotation events,” “when an encryption key

expires, the computer system will... use a new encryption key to encrypt the data”) (emphases added); *id.* at [0008] (“In an alternate embodiment, the key lifetime manager is operable to flag the expired keys and to change or deactivate the expired keys in the next client request or call.” (emphasis added). This is the consistent teaching of Madoukh on the lifetime. *See also* Ex. 1011 at [0048]: “The key lifetime manager (KLM) 88 monitors the lifetime of the SEK’s and system keys based on their expiration dates and timestamps.”; *see also id.* at [0094]. The key lifetime manager thus monitors the expiration dates and timestamps independently, to flag expired keys or request new encryption key upon the expiration of old keys, but this monitoring of expiration dates has no relation to the current time when an encryption key is actually used or intended to be used. Nor does Petitioner’s expert provide any reason why Madoukh’s procedure of requesting new encryption keys upon the expiration of old ones would be applied in the context of Teo to compare a current time with a range of times that begins, for example, at the starting time of Teo’s DMK key, rather than by comparing the current time only with a single time—the expiration time. *See* Ex. 1003 at ¶146. Accordingly, Teo in view of Madoukh does not involve verifying the validity of an initiation key relative to a “validity period” based on “a current time,” where the “validity period” is not a single point in time.

Petitioner's combination is therefore devoid of any showing of element [1a] as construed above.

2. Claim elements [1b] and [1d]; the Petition fails to establish that Teo in view of Madoukh teaches a session key that is generated “if the initiation key is deemed valid,” which is premised upon the initiation key having had its validity verified “based on a current time”

The Petition turns to Madoukh for this feature but fails to show that Teo in view of Madoukh teaches that the session key is generated only *if* the initiation key has had its validity verified “based on the current time,” because the Petition reasons based on the fallacy *post hoc, ergo propter hoc*—an incorrect assumption of a causal relationship based on a sequential relationship. More specifically, the Petition reasons that “the pre-shared key approach discussed above would have occurred only *after* the mobile communication terminals determine that the DMK (i.e., ‘initiation key’) is valid, *e.g.*, based on comparing the current time with the DMK’s key_lifetime relative to the time stamp indicating the start of DMK’s validity period...” *See* Pet. at 32 (emphasis added). However, for the reasons discussed relative to element [1a], above, the Petition’s showing for the “key_lifetime” parameter is based on Madoukh requesting “new encryption keys upon the expiration of old encryption keys.” *See* Pet. at 24, citing Ex. 1011 at [0007]. And the mere teaching of requesting new encryption keys upon the

expiration of old ones does *not* imply that any “generating a session key” is premised upon an initiation key having had its validity verified “based on a current time,” as required by Claim 1. Rather, the Petition is merely reasoning that “the pre-shared key approach... would have occurred only after the mobile communication terminals determine” that the DMK is valid. *See* Pet. at 32. The Petition is, therefore, reasoning that just because a “pre-shared key approach” would occur after a DMK key is determined to be valid, it would follow that it would be premised upon the determination of validity. But that does not follow, and the Petition provides no showing that Teo in view of Madoukh teaches generating a session key “if the initiation key is deemed valid,” premised upon the initiation key having had its validity verified “based on a current time.” *See id.*

In particular, a POSITA would not “have found it obvious to implement *Madoukh*’s key life time manager to monitor whether *Teo*’s DMK has expired by checking whether the current time falls within the range of the DMK’s lifetime (*i.e.*, the time period starting at the time of the received timestamp (*e.g.*, T_{HR-BS}) through the expiration of the associated ‘key_lifetime’). *See* Pet. at 25. Firstly, the timestamps such as T_{HR-BS} in Teo are disclosed to be used to determine whether a received message is fresh. *See, e.g.*, Ex. 1005 at 13-14 (“message freshness”). But contrary to what Petitioner seems to imply, these received timestamps are not

disclosed to be used in relation to a “key_lifetime,” either in Teo or in Madoukh. Secondly, for the reasons discussed relative to element 1[a], above, Petitioner’s argument ignores how the (central) key lifetime manager (KLM) of Madoukh works. Even if Teo and Madoukh were to be combined, which is not conceded to be obvious, then a KLM as in Madoukh would be implemented on multiple communication terminals of Teo—but such KLMs would still function as a key lifetime manager as taught in Madoukh. Each of such KLMs would monitor the expiry of a key as a background process that is independent of a current time of using the key. That still does not result in “verifying a validity of the initiation key based on a current time” and “if the initiation key is deemed valid [based on the current time]... using the initiation key in performing a key agreement procedure...” as recited in elements [1b] and [1d].

The Petition therefore fails to show that Teo in view of Madoukh teaches elements [1b] and [1d], in addition to element [1a] as argued above, and consequently, fails to show that Teo in view of Madoukh teach independent Claim 1.

3. Dependent Claims 2 and 14

For at least the same reasons as given for Claim 1, from which Claims 2 and 14 depend, the Petition likewise fails to show that Teo and Madoukh or their

combination teach dependent Claims 2 and 14.

4. Lack of Reasonable Likelihood of Ground 1

The Petition therefore fails to demonstrate a reasonable likelihood that Claims 1, 2, and 14 of the '572 Patent are unpatentable in view of Teo in view of Madoukh.

B. Ground 2 should be denied for failure to establish a reasonable likelihood that Teo in view of Madoukh and Hawkes renders Claims 3-5 and 15-17 unpatentable

For the reasons discussed above relative to Ground 1, the Petition fails to show that Teo in view of Madoukh teaches elements [1a], [1b] and [1d] of Claim 1. In Ground 2, the Petition repeats its arguments from Ground 1, and relies upon Hawkes for allegedly teaching the following additional features of: “storing the initiation key in a secure storage area of each respective mobile device” (in dependent Claim 3); features of the “secure storage area” as a “trusted computing subsystem” (in dependent Claim 4) that is used to perform some of the elements of Claim 1 (in dependent Claim 5); a non-transitory memory storing instructions (Claim 15) and storing the initiation key (Claim [15a]); a mobile device, features of Claims 3 and 5, and “establishing” using “a mobile subsystem” (Claim 16); and similar features of Claims 5 and 16 (for Claim 17).

However, even if there were a motivation to combine Hawkes with Teo and

Madoukh (which is not conceded), and even if the above alleged additional features were to be taught by Hawkes (which is not conceded), Hawkes still would not remedy the above-discussed deficiencies of Teo in view of Madoukh relative to the features of Claim 1, and corresponding features of independent Claims 15, 16, and 17. It follows that Ground 2 should be denied for at least the same reasons as Ground 1.

C. Ground 3 should be denied for failure to establish a reasonable likelihood that Teo in view of Madoukh and RFC 4279 renders Claims 6-9 unpatentable

For the reasons discussed above relative to Ground 1, the Petition fails to show that Teo in view of Madoukh teaches elements [1a], [1b] and [1d] of Claim 1. In Ground 3, the Petition repeats its arguments from Ground 1, and relies upon RFC 4279 for allegedly teaching the following additional features of: “preloading a set of initiation keys on each of the mobile devices” where the “set of initiation keys” is “associated with a respective set of validity periods” (in Claim [6a]); performing a key synchronization procedure (in Claim [6b]); preloading set of key identifiers and performing a key synchronization procedure based on the set of key identifiers (in Claim 7); disabling or removing the initiation key from the set of initiation keys after use (in Claim 8); and the validity periods being constituted at least in part by “different but overlapping validity periods” (Claim 9).

However, first, the Petition fails to show that RFC 4279 teaches the additional features of Claim [6a], which involve “preloading a set of initiation keys on each of the mobile devices” where the “set of initiation keys” is “associated with a respective set of validity periods.” The Petition alleges that, in Teo, because several emergency rescue personnel would need to directly communicate with each other, it would have been obvious that “there would be many terminals that would need to communicate with each other.” *See* Pet. at 53. However, that by no means would necessarily imply that a “set of initiation *keys*” (emphasis added), where “keys” is **plural**, would be preloaded “on *each* of the mobile devices” (emphasis added), and the Petition is devoid of any showing based on Teo that a set of plural keys would necessarily be loaded on *each* mobile device. *See id.* Nor would the statement that each “base station” would allegedly have its own “key_lifetime” value necessarily imply that each mobile device would have a set of plural keys loaded on it. Nor does the Petition provide any showing based on Teo that a set of plural keys would necessarily be loaded on each mobile device where the set of (plural) initiation keys is “associated with a respective set of validity *periods*” (plural, emphasis added) on *each* mobile device. *See id.* However, since Petitioner’s showing of these features is based on Teo alone, *see* Pet. at 53, its attempt at inherent anticipation fails. *See In re Robertson*, 169 F.3d 743, 745 (Fed.

Cir. 1999); *accord Colas Solutions Inc. v. Blacklidge Emulsions Inc.*, IPR2016-01031, Paper 38 at 24-25 (P.T.A.B. November 2, 2017) (PTAB rejected argument of inherent obviousness where missing feature was not necessarily present). The Petition’s showing for element [6a] is therefore defective.

In addition, RFC 4279 does not teach the additional features of Claim 9, in which the validity periods of Claim [6a] are constituted at least in part by “different but overlapping validity periods,” since the Petition’s argument for that feature relies on its argument for Claim 6. *See* Pet. at 58-59. Also, for Claim 9, the Petition refers to the Park reference (Ex. 1017) as “an example of such an occurrence” of overlapping time periods—but Park is not relied upon as a reference in Ground 3. *See* Pet. at 59. The Petition’s citation of Park in Ground 3 should, therefore, be given no weight because it is not part of the combination in Ground 3.

Furthermore, even if there were a motivation to combine RFC 4279 with Teo and Madoukh (which is not conceded), and even if the above alleged additional features for Claims 6-9 were to be taught by RFC 4279 (which is not conceded), RFC 4279 still would not remedy the above-discussed deficiencies of Teo in view of Madoukh relative to the features of Claim 1. Since Claims 6-9 depend directly or indirectly on Claim 1, it follows that Ground 3 should be denied

for at least the same reasons as Ground 1.

D. Ground 4 should be denied for failure to establish a reasonable likelihood that Teo in view of Madoukh, RFC 4279, and Kumar renders Claim 10 unpatentable

For the reasons discussed above relative to Ground 1, the Petition fails to show that Teo in view of Madoukh teaches elements [1a], [1b] and [1d] of Claim 1. In addition, for the reasons discussed above relative to Ground 3, the Petition fails to show that Teo in view of Madoukh and RFC 4279 teaches Claim 6. In Ground 4, the Petition repeats arguments from Grounds 1 and 3, and relies upon Kumar for allegedly teaching the additional features relating to a “virtual network identity” in dependent Claim 10.

However, even if there were a motivation to combine Kumar with Teo, Madoukh, and RFC 4279 (which is not conceded), and even if the above alleged additional features of a “virtual network identity” of Claim 10 were to be taught by Kumar (which is not conceded), Kumar still would not remedy the above-discussed deficiencies of Teo in view of Madoukh relative to the features of Claim 1, and of Teo, Madoukh, and RFC 4279 relative to Claim 6. It follows that Ground 4 should be denied for at least the same reasons as Grounds 1 and 3.

E. Ground 5 should be denied for failure to establish a reasonable likelihood that Teo in view of Madoukh and S3-070234 renders Claims 11 and 12 unpatentable

For the reasons discussed above relative to Ground 1, the Petition fails to show that Teo in view of Madoukh teaches elements [1a], [1b] and [1d] of Claim 1. In Ground 5, the Petition repeats its arguments from Ground 1, and relies upon S3-070234 for allegedly teaching the additional features relating to a “usage count” in dependent Claims 11 and 12.

However, even if there were a motivation to combine S3-070234 with Teo and Madoukh (which is not conceded), and even if the above alleged additional features of a “usage count” of Claims 11 and 12 were to be taught by S3-070234 (which is not conceded), S3-070234 still would not remedy the above-discussed deficiencies of Teo in view of Madoukh relative to the features of Claim 1. It follows that Ground 5 should be denied for at least the same reasons as Ground 1.

F. Ground 6 should be denied for failure to establish a reasonable likelihood that Teo in view of Madoukh and Thakare renders Claim 13 unpatentable

For the reasons discussed above relative to Ground 1, the Petition fails to show that Teo in view of Madoukh teaches elements [1a], [1b] and [1d] of Claim 1. In Ground 6, the Petition repeats its arguments from Ground 1, and relies upon Thakare for allegedly teaching the additional features relating to “requesting a

further initiation key via the mobile network if the key agreement procedure fails”
in dependent Claim 13.

However, even if there were a motivation to combine Thakare with Teo and Madoukh (which is not conceded), and even if the above alleged additional features relating to “requesting a further initiation key via the mobile network if the key agreement procedure fails” of Claim 13 were to be taught by Thakare (which is not conceded), Thakare still would not remedy the above-discussed deficiencies of Teo in view of Madoukh relative to the features of Claim 1. It follows that Ground 6 should be denied for at least the same reasons as Ground 1.

VI. CONCLUSION

The Board should not institute *inter partes* review on any of the grounds set forth in the Petition.

Respectfully submitted this 1st day of September, 2023.

/Lawrence P. Cogswell III, Ph.D. 71,441/
Lawrence P. Cogswell III, Ph.D.
Lead Counsel
Reg. No. 71,441
Hamilton, Brook, Smith & Reynolds, P.C.
155 Seaport Blvd.
Boston, Massachusetts 02210
Phone: (617) 607-5900
Fax: (978) 341-0136

Timothy J. Meagher
First Back-up Counsel
Reg. No. 39,302
Hamilton, Brook, Smith & Reynolds, P.C.
155 Seaport Blvd.
Boston, Massachusetts 02210
Phone: (617) 607-5900
Fax: (978) 341-0136

Keith J. Wood
Second Back-up Counsel
Reg. No. 45,235
Hamilton, Brook, Smith & Reynolds, P.C.
155 Seaport Blvd.
Boston, Massachusetts 02210
Phone: (617) 607-5900
Fax: (978) 341-0136

***Attorneys for Patent Co-Owners
Koninklijke KPN N.V. and Nederlandse
Organisatie voor Toegepast-
Natuurwetenschappelijk Onderzoek TNO***

CERTIFICATE OF COMPLIANCE

I hereby certify that this Patent Owner Preliminary Response complies with the type- volume limitations of 37 C.F.R. § 42.24(b)(1), because it contains 6,469 words, as calculated by the Microsoft Word program excluding the parts of the brief exempted by 37 C.F.R. § 42.24.

/Lawrence P. Cogswell III, Ph.D. 71,441/
Lawrence P. Cogswell III, Ph.D.
Reg. No. 71,441
Hamilton, Brook, Smith & Reynolds, P.C.
155 Seaport Blvd.
Boston, Massachusetts 02210
Phone: (617) 607-5900
Fax: (978) 341-0136

***Lead Counsel for Patent Co-Owners
Koninklijke KPN N.V. and Nederlandse
Organisatie voor Toegepast-
Natuurwetenschappelijk Onderzoek TNO***

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), I hereby certify that on September 1, 2023, the foregoing ***Patent Owner Preliminary Response*** is being served electronically by agreement of the parties at the following email service addresses:

chad.walters@bakerbotts.com
doug.kubehl@bakerbotts.com
jeff.becker@bakerbotts.com
andrew.grado@bakerbotts.com

/Lawrence P. Cogswell III, Ph.D. 71,441/
Lawrence P. Cogswell III, Ph.D.
Reg. No. 71,441
Hamilton, Brook, Smith & Reynolds, P.C.
155 Seaport Blvd.
Boston, Massachusetts 02210
Phone: (617) 607-5900
Fax: (978) 341-0136

***Lead Counsel for Patent Co-Owners
Koninklijke KPN N.V. and Nederlandse
Organisatie voor Toegepast-
Natuurwetenschappelijk Onderzoek TNO***