

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

META PLATFORMS, INC.; INSTAGRAM, INC.; WHATSAPP LLC; META
PLATFORMS TECHNOLOGIES, LLC; AND GIPHY, INC.

Petitioners

v.

VL COLLECTIVE IP LLC

Patent Owner

Case IPR2023-00923
U.S. Patent 7,266,682

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE '682 PATENT	2
	A. Overview of the '682 Patent.....	2
	B. Priority Date	5
III.	THE ASSERTED REFERENCES	5
	A. Handley (EX1005)	5
	B. Basturk (EX1006).....	6
	C. PacketCable (EX1007).....	9
IV.	LEVEL OF ORDINARY SKILL	11
V.	LEGAL STANDARDS	12
	A. Claim Construction	12
	B. Obviousness.....	12
	C. Prior Art.....	13
VI.	CLAIM CONSTRUCTION	14
VII.	PETITIONERS HAVE NOT DEMONSTRATED THAT ANY CHALLENGED CLAIM IS UNPATENTABLE	18
	A. The challenged claims are patentable over Handley in combination with Basturk (Ground I).	18
	1. The Petition does not show that Handley qualifies as prior art.....	18
	2. Petitioners fail to show that the POSITA would have been motivated to combine Handley and Basturk to arrive at the claimed invention.....	23
	3. Independent Claim 1	30

4.	Independent Claims 25-28	39
5.	All dependent claims are patentable over Handley in combination with Basturk.	40
B.	The challenged claims are patentable over PacketCable in combination with Handley (Ground II).....	40
1.	The Petition does not show that PacketCable qualifies as prior art.....	40
2.	Independent Claim 1	42
3.	Independent Claims 25-28	53
4.	Dependent Claims 22 and 24	54
5.	All dependent claims are patentable over PacketCable in combination with Handley.	54
C.	The challenged claims are patentable over PacketCable in combination with Basturk (Ground III).	55
1.	Petitioners fail to show that the POSITA would have been motivated to combine PacketCable with and Basturk to arrive at the claimed invention.	55
2.	Independent Claim 1	59
3.	Independent Claims 25-28	60
4.	Dependent Claims 22 and 24	60
5.	All dependent claims are patentable over PacketCable in combination with Basturk.	60
D.	The challenged claims are patentable over Handley in combination with Basturk and PacketCable (Ground IV).	61
1.	Dependent Claims 22 and 24	61
VIII.	CONCLUSION.....	61

TABLE OF AUTHORITIES

Cases

<i>Acceleration Bay, LLC v. Activision Blizzard, Inc.</i> , 908 F.3d 765 (Fed. Cir. 2018)	13
<i>ActiveVideo Networks, Inc. v. Verizon Communs., Inc.</i> , 694 F.3d 1312 (Fed. Cir. 2012)	27
<i>AstraZeneca AB v. Mylan Pharms. Inc.</i> , 19 F.4th 1325 (Fed. Cir. 2021)	13
<i>Blue Calypso, LLC v. Groupon, Inc.</i> , 815 F.3d 1331 (Fed. Cir. 2016)	41, 42
<i>David Netzer Consulting Eng'r LLC v. Shell Oil Co.</i> , 824 F.3d 989 (Fed. Cir. 2016)	12
<i>Ecolab, Inc. v. FMC Corp.</i> , 569 F.3d 1335 (Fed. Cir. 2009)	18
<i>Edwards Lifesciences LLC v. Cook Inc.</i> , 582 F.3d 1322 (Fed. Cir. 2009)	17
<i>Finjan Holdings, Inc. v. Sophos Limited</i> , IPR2015-01405, Paper 37 (PTAB Nov. 30, 2016)	21
<i>Grace Instrument Indus., LLC v. Chandler Instruments Co., LLC</i> , 57 F.4th 1001 (Fed. Cir. 2023)	12
<i>Icon Health & Fitness, Inc. v. Strava, Inc.</i> , 849 F.3d 1034 (Fed. Cir. 2017)	22
<i>In re Mouttet</i> , 686 F.3d 1322 (Fed. Cir. 2012)	13
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	13
<i>Jazz Pharms., Inc. v. Amneal Pharms., LLC</i> , 895 F.3d 1347 (Fed. Cir. 2018)	14, 22

ResQNet.com, Inc. v. Lansa, Inc.,
594 F.3d 860 (Fed. Cir. 2010) 21

Ruiz v. A.B. Chance Co.,
357 F.3d 1270 (Fed. Cir. 2004) 13

TQ Delta, LLC v. Cisco Sys.,
942 F.3d 1352 (Fed. Cir. 2019) 22

Weber, Inc. v. Provisur Techs., Inc.,
92 F.4th 1059 (Fed. Cir. 2024) 41

Regulations

37 C.F.R. § 42.100(b) 12

37 C.F.R. § 42.6(a)(3) 21

37 C.F.R. § 42.65(a).....22

PATENT OWNER'S EXHIBIT LIST

Exhibit	Description
2001	Declaration of Jaime F. Cardenas-Navia in Support of Motion for Admission Pro Hac Vice
2002	The Secure Real-time Transport Protocol (SRTP)
2003	Compare Results for EX1005
2004	Declaration of Stuart Stubblebine in Support of Patent Owner's Response
2005	Curriculum Vitae of Stuart G. Stubblebine, Ph.D.
2006	Transmission Control Protocol: RFC 793
2007	User Datagram Protocol: RFC 768
2008	Shai Halevi and Hugo Krawczyk, <i>MMH: Software Message Authentication in the Gbit/Second Rates</i>

I. INTRODUCTION

Petitioners have not shown that any challenged claim is unpatentable. Each of Petitioners' four asserted Grounds is fatally flawed.

Ground I fails outright because Petitioners have not shown that Handley qualifies as prior art. But that's not the only problem for Ground I. The combination of Handley and Basturk does not render any asserted claim obvious because Basturk teaches away from its combination with Handley, and the POSITA would have found Basturk's transport layer protocol incompatible with Handley's architecture.

Ground II also relies on Handley and thus it is fatally flawed. But Ground II also relies on PacketCable, which Petitioners have also failed to show was publicly accessible at the relevant time. The combination of PacketCable and Handley also does not disclose or render obvious every element of the '980 patent's independent claims. Both PacketCable and Handley are silent as to elements critical to the invention, and Petitioners fail to show that the difference would have been obvious.

Ground III suffers the infirmities of Grounds I-II. Ground III fails for the additional reason that, like Ground I, Basturk teaches away from combining it with PacketCable, and the POSITA would have found the combination incompatible.

Ground IV suffers the infirmities of Grounds I-III. It fails for the additional reason that Petitioners have not shown that Handley discloses the requirements of claims 22 and 24.

For the reasons explained herein, the Board should issue a final written decision finding all claims patentable.

II. THE '682 PATENT

A. Overview of the '682 Patent

The '682 patent addresses a problem in the transmission of real-time audio and visual data over the Internet. In the mid-1990s, the Real Time Transport Protocol, or RTP, was developed by the Internet Engineering Task Force (IETF), which was designed for end-to-end real-time transfer of streaming media. *See* EX1008 1, 72-73. But RTP had security vulnerabilities. EX1008, 72. Networks utilizing RTP were susceptible to security breaches at the transmitter, during transmission, and at the receiver. *See* EX1008, 72; EX1001, 2:44–3:10. Attackers could overload a network by sending mass data to receivers, which can harm system availability and performance. EX1001, 2:47–64. Although it was possible to for RTP traffic to be sent behind firewalls, EX1008, 72, firewalls did not solve such problems because it was a “simple matter for an attacker to send [its] meaningless (mass) data to addresses within the private network as well, that is to say, behind the firewall.” EX1001, 2:65–3:10.

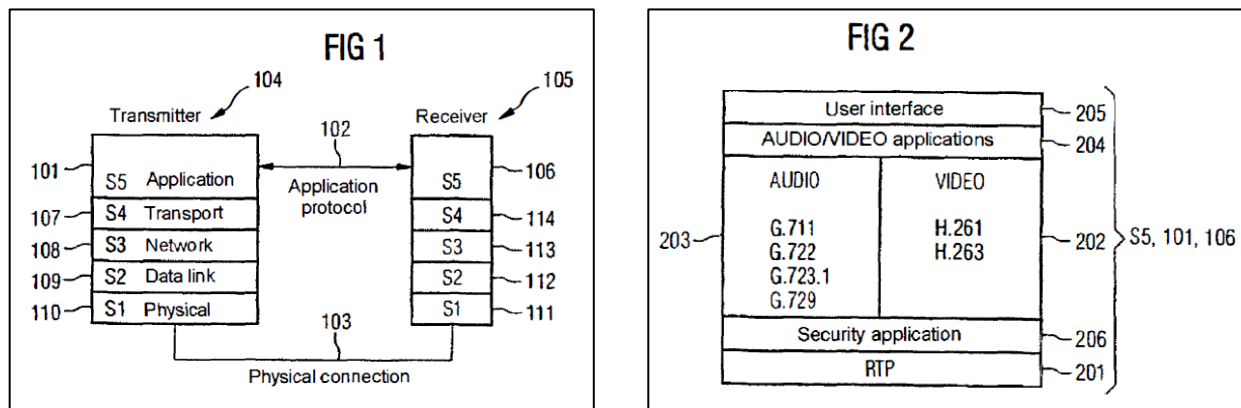
In one approach, the IPSEC protocol, “data packets of the Internet protocol (IP data packets) [could] be encapsulated and [could] be protected in terms of confidentiality and/or integrity.” EX1001, 3:16–41. It included a cookie-based

mechanism, linking fast one-way hash functions, random numbers, and IP addresses to one another. *Id.* But that solution was flawed because the “first ‘cookie’ transmitted from the transmitter to the receiver” was unprotected. EX1001, 3:30–34. The cookie method also could not protect against unwanted mass data at the application layer under real-time conditions. EX1001, 3:34–38. Structurally, it was not possible to link IPSEC to the security functions of an application layer. EX1001, 3:38–41.

The RTP specification expressly did not define authentication or message integrity services (or the necessary key management infrastructure) for RTP, expecting instead that authentication and integrity services would be provided by lower layer protocols in the future. EX1008, 50.

The ’682 patent’s inventors, however, recognized and solved RTP’s security problems with a solution of their own. The ’682 patent provides a solution to RTP’s security flaws by ensuring, at the receiver, that data being transmitted is not insecure or unwanted by inserting authentication data into the RTP data packets as an application protocol on an application layer at the transmitter before transmission. EX1001, 3:45-55, 7:6-23. The authentication data is included with the data packet and analyzed by the receiver to ensure that the transmitter and the receiver know each other. EX1001, Fig. 3, 3:49-55, 5:30-38. 7:6-23. If the receiver knows the transmitter, the data is processed; if not, the data is rejected. EX1001, 7:14-21.

The '682 patent teaches that authenticating RTP packets on the application layer (as an application protocol), as claimed in the '682 patent, is extremely advantageous from both a user and network perspective. EX1001, 3:49-4:30, 7:24-48. The “application layer” for purposes of the '682 patent refers to “the layers above the transport layer (layers above 4),” and the “application protocol” refers to “the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer.” EX1001, 2:6–11. Thus, with reference to Figures 1 and 2, the patent teaches an example where “directly above the layer 4 is the real time transport protocol (RTP)” in “the application layer (layer 5).” EX1001, 6:33–51, Figs. 1 and 2.



EX1001, Figs. 1 and 2

Authenticating RTP packets in the application layer permits reduced size of authentication data, because the authentication is of smaller data PDUs than at other layers, which improves speed and real-time availability of the entire communication system. EX1001, 3:60-4:10, 7:24-36. Another benefit is that it increases the

transmission system's performance and reduces the implementation complexity of the system. EX1001, 4:11-22. Once the receiver determines that the transmitter is known, the message is immediately accepted. EX1001, 4:3-7. If the receiver determines that the transmitter is not known, the message is immediately rejected, which means that no buffering or loading is performed, and no further action is needed. EX1001, 4:7-9.

B. Priority Date

Petitioners acknowledge that “[t]he earliest potential effective filing date of the ’682 Patent’s claims is January 18, 2000.” Paper (“Petition”) at 4. Petitioners and their expert, Dr. Bajaj, do not dispute that the challenged claims are entitled to the priority date of January 18, 2000. Petition, 4; EX1003, ¶44.

III. THE ASSERTED REFERENCES

A. Handley (EX1005)

Handley relates to an architecture for “so-called ‘real-time’ conferencing, including audio, video, shared whiteboards and other applications” over the Internet. EX1005 at 2. Handly describes an approach to multicast distribution to a group of receivers, in which senders send messages “to the *group*,” receivers express interest in receiving data “sent to *the group*,” and components called “routers” are the elements that “conspire to deliver data from senders to receivers.” EX1005, 2-3. In Handley, “[r]eceivers do not need to know who or where the senders are to receive

traffic from them. Senders never *need* to know who the receivers are.” EX1005, 3. See EX2004 ¶¶68-69.

Handley defines “real-time” traffic as “datagrams that are delay sensitive,” where “TCP traffic is normally not considered to be real-time traffic.” EX1005, 4-5. Handley suggests a routing model where “real-time” non-TCP traffic is segregated from and prioritized over non-real-time TCP traffic. See EX1005, 5. According to Handley, its approach of “classifying real-time traffic separately from non-real-time traffic and giving real-time traffic priority treatment ensures that real-time traffic sees minimum delays.” EX1005, 5. See EX2004 ¶70.

Handley states that “[a] *transport protocol* with the specific functions needed for this has been defined.” EX1005, 2. Handley states that “[t]he transport protocol for real-time flows is RTP,” citing RFC 1889. EX1005, 8. Handley states that “RTP is normally carried using UDP” and does not “provide any enhanced reliability over UDP.” EX1005, 8. See EX2004 ¶¶71-72.

Handley relies on standard RTP encryption functionality. EX1005, 12; See EX2004 ¶73.

B. Basturk (EX1006)

Basturk’s focus is on solving a problem specifically of *transport level* security—in explicit contrast to application level security—and suggests solving the transport level security problem with a secure *transport level* protocol. EX1006, 1.

Basturk expressly “distinguish[es] security features according to the layer of the communication structure to which they are most naturally associated,” stating that “the traditional features are mostly application level, while the new ones we deem necessary are transport level.” EX1006, 3. Basturk identifies “secure delivery” as the security concern of the paper, which Basturk suggests is “best addressed by the design of secure transport protocols.” EX1006, 1. Basturk states that “secure delivery” is “most naturally identified with the transport level.” EX1006, 3. See EX2004 ¶¶74-77.

Basturk’s solution is a transport level protocol, not an application level protocol. According to Basturk’s design, an application interacts with a “transport module” at the transport layer through an “interface,” where the task of “applying any cryptographic functions or taking other security steps is performed by the transport module.” EX1006, 4-5, 8. EX2004 ¶¶78-79.

Basturk teaches that its solution is a secure transport protocol with two phases: “initialization” and “steady state.” EX1006, 5, 9-10. During initialization, “an entity authentication and key exchange protocol is executed,” which “authenticates the parties and yields them a session key α .” EX1006, 5, 9. The session key α is generated and exchanged at the transport layer between “secure transport machines” (M_A and M_B)—the session key α is “known only to M_A and M_B ,” and the applications (A and B) “never see it.” EX1006, 10. In the steady state, “both data integrity and

secure delivery are provided by attaching to each packet a signature, computed under key α ,” “acknowledgments ... are also signed,” and “the data is encrypted, also under α .” EX1006, 5, 9-10. The transport modules (M_A and M_B) at the transport layer perform these steps. *Id.* Accordingly, “when [an application] wants to send a message m , it passes it to the secure transport machine, and the latter is responsible for relaying the message, applying any necessary cryptographic functions to it, taking care of retransmission, and in general providing all transport facilities.” EX1006 at 8. *See* EX2004 ¶80-83.

Basturk states that “[t]he provision of security is bound to somewhat degrade performance.” EX1006, 6. To purportedly minimize performance degradation caused by adding transport level security, Basturk suggests performing its transport level security computations in a manner that is called “on-the-fly.” EX1006, 7-8. Basturk states that “[t]he ability to achieve such on-the-fly processing depends on two major components,” where “[t]he first is the latency in retrieving the information needed to perform the necessary computations,” known as “context” (which includes “the shared session key”). EX1006, 12. According to Basturk, context retrieval creates latency because signature computation relies on the use of “secret information (key) shared by the two communicating parties,” which “must typically be retrieved upon receipt of a packet and this context retrieval step can introduce latency.” EX1006, 8. Basturk suggests reducing this context retrieval latency by

putting the context information early in each packet, namely in a security segment in the packet's header. EX1006, 12, 13, 15-16. See EX2004 ¶¶84-85.

The second component for on-the-fly processing “is the nature of the computations themselves,” meaning “MAC computations are kept simple and can start prior to context retrieval.” EX1006 at 13. According to Basturk, simplicity is achieved by using less computationally intensive standard functions. EX1006 at 13.). The ability for MAC_{α} computations to start prior to the completion of context retrieval is achieved by using a MAC algorithm that includes a portion that “depend[s] neither on α nor on the cryptographic primitive chosen in the initial option,” which permits computation to begin before the retrieval of context information (including the session key α) is complete. EX1006 at 13. See EX2004 ¶86.

C. PacketCable (EX1007)

According to PacketCable, its architecture is an “end-end broadband architecture that supports voice, video, and other multimedia services.” EX1007, 10. PacketCable says that its architecture “contains three networks: the ‘DOCSIS HFC Access Network,’ the ‘Managed IP Network’ and the PSTN.” EX1007, 12. Figure 1 (reproduced below) shows an “Embedded MTA Client” in the DOCSIS HFC Access Network displaying two distinct components: a “MTA” device and a “Cable Modem”. *Id.* PacketCable states that “[a]n MTA is a PacketCable client

device that contains a subscriber-side interface to the subscriber's CPE (e.g., telephone) and a network-side signaling interface to call control elements in the network." EX1007, 18; see EX2004 ¶¶90-92.

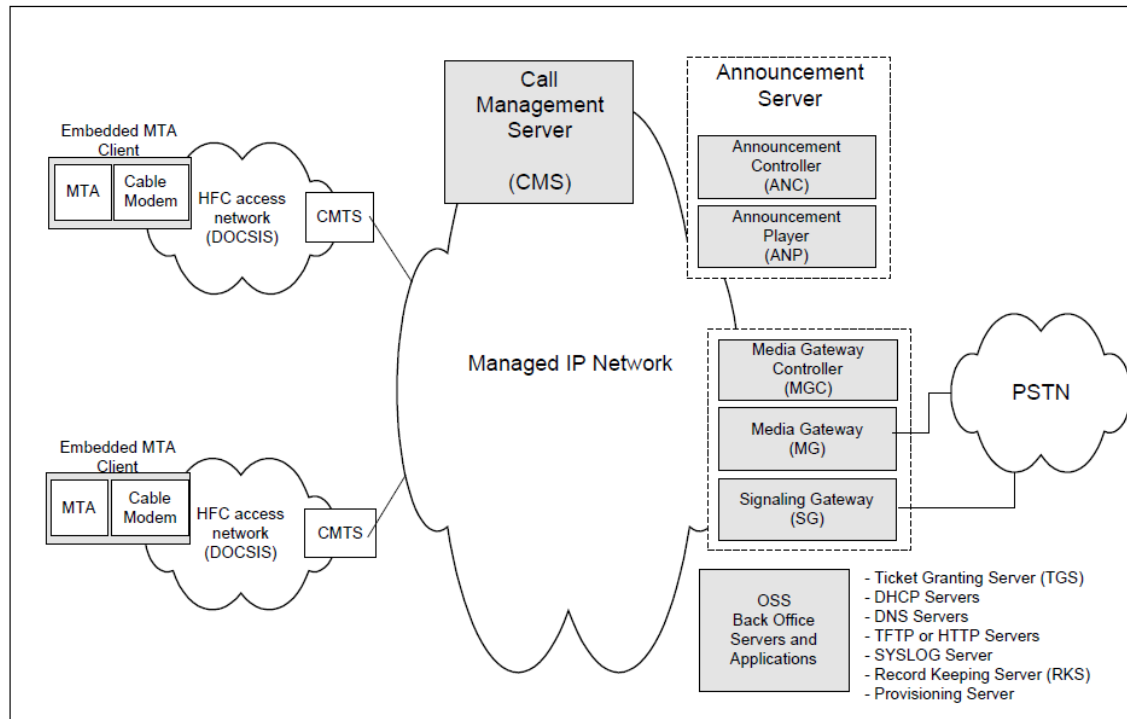


Figure 1. PacketCable Reference Architecture

EX1007, Figure 1

According to PacketCable, “unless otherwise noted, the term MTA refers to an embedded MTA,” or “E-MTA,” which “is a single hardware device that incorporates a DOCSIS 1.1 cable modem as well as a PacketCable MTA component.” EX2007, 18. PacketCable shows a conceptual functional architecture of an E-MTA. EX1007 at 20; see EX2004 ¶¶93-96.

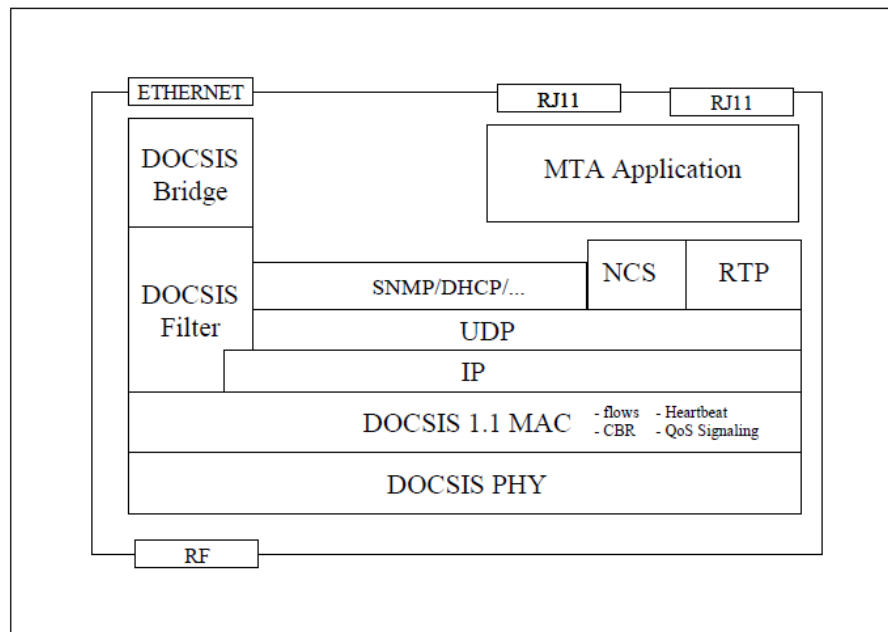


Figure 4. E-MTA Conceptual Functional Architecture

EX1007 at 20

In PacketCable, RTP “is used to transport all media streams,” and the MTAs are “responsible for ... Authentication, confidentiality and integrity of some messages between the MTA and other PacketCable network elements.” EX1007 at 15, 19, 31; see EX2004 ¶¶97-102.

IV. LEVEL OF ORDINARY SKILL

Petitioners set forth a level of ordinary skill. Petition, 9. Without agreeing to or acquiescing to Petitioners’ definition of the level of ordinary skill, this Response establishes that no challenged claim is unpatentable even under Petitioners’ definition.

V. LEGAL STANDARDS

A. Claim Construction

The Board construes claims “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b); *see Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). However, “if the specification reveals a special definition given to a claim term by the inventor, then the inventor’s lexicography governs, even if it differs from the term’s ordinary meaning.” *David Netzer Consulting Eng’r LLC v. Shell Oil Co.*, 824 F.3d 989, 994 (Fed. Cir. 2016) (citing *Phillips*, 415 F.3d at 1316); *Grace Instrument Indus., LLC v. Chandler Instruments Co., LLC*, 57 F.4th 1001, 1010 (Fed. Cir. 2023) (“Where the specification instructs as to the meaning of a claim term, ‘the inventor’s lexicography governs.’” (quoting *Phillips*, 415 F.3d at 1316)).

B. Obviousness

Proving obviousness requires showing that “the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious.” *Ruiz v. A.B. Chance Co.*, 357 F.3d 1270, 1275 (Fed. Cir. 2004) (quoting 35 U.S.C. § 103 (emphasis added)).

Petitioners bear the “burden to demonstrate both that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.” *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367 (Fed. Cir. 2016) (cleaned up).

“A reference that properly teaches away can preclude a determination that the reference renders a claim obvious.” *In re Mouttet*, 686 F.3d 1322, 1333 (Fed. Cir. 2012). “[A] prior art reference is said to teach away from the claimed invention if a skilled artisan upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken’ in the claim.” *AstraZeneca AB v. Mylan Pharms. Inc.*, 19 F.4th 1325, 1337 (Fed. Cir. 2021) (cleaned up).

C. Prior Art

“Whether a reference qualifies as a printed publication under § 102 is a legal conclusion based on underlying fact findings,” including as to “public accessibility.” *Acceleration Bay, LLC v. Activision Blizzard, Inc.*, 908 F.3d 765, 772 (Fed. Cir. 2018). “A reference is considered publicly accessible ‘upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.’” *Jazz Pharms., Inc. v. Amneal Pharms., LLC*,

895 F.3d 1347, 1355 (Fed. Cir. 2018).

VI. CLAIM CONSTRUCTION

In light of the intrinsic evidence, the POSITA would have interpreted the following claim term of the '682 patent as follows:

Term	Patent Owner' Construction
“application layer”	“the layers above the transport layer (layers above 4)”
“application protocol”	“the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer”

Independent claim 1 requires “providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level *as an application protocol on an application layer.*” EX1001, claims 1, 25-28. The POSITA would have understood the specification of the '682 patent to express a clear intent to define “application layer” and “application protocol” as stated above. EX2004, ¶61.

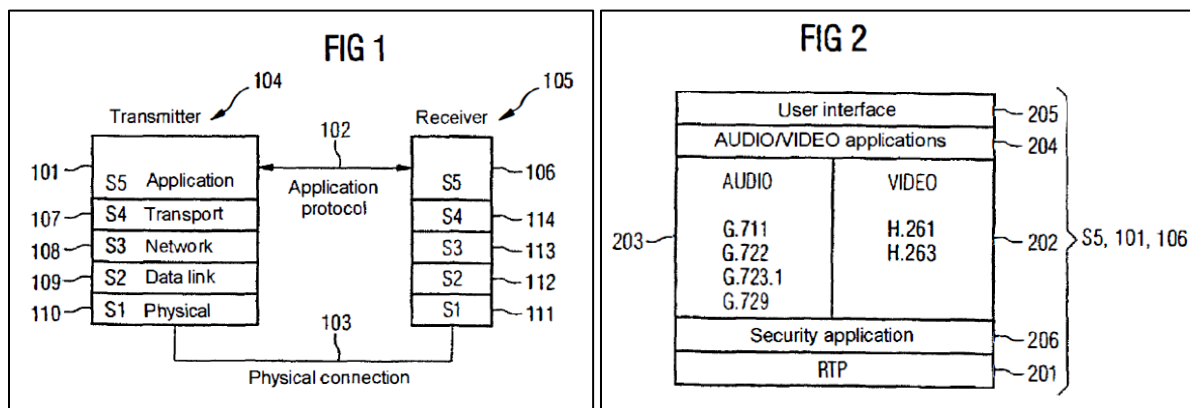
The context for the POSITA to interpret the '682 patent's “application layer” and “application protocol” terms includes the '682 patent's explanation of “[t]he OSI reference model (OSI model for short) from the International Standards

Organization (ISO),” which “has seven layers, each of which has a different functionality (in terms of abstraction).” EX1001 at 1:19–45 (describing layers 1 through 7); EX2004, ¶62. The ’682 patent explains that “[i]n the OSI model ... layer 4, a transport layer, uses a transport protocol ... layer 5 corresponds to a session layer using a session protocol, layer 6 corresponds to a presentation layer using a presentation protocol, and layer 7 corresponds to an application layer using an application protocol.” EX1001, 1:22-37. These explanations about the 7-layer OSI model are consistent with how a person of ordinary skill in the art would have understood the OSI model generally. EX2004, ¶62.

The ’682 patent further explains, however, that “[i]n practice, many applications do not always permit exact nomination of strict boundaries specifically between the upper protocol layers, particularly layers 5 to 7,” such that “layers above the transport layer 4 combine to form an ‘application layer’ for which ... an ‘application protocol’ is used.” EX1001 at 1:19–45. The specification further states that “[w]hen referring to application layer below, this denotes the layers above the transport layer (layers above 4)” and “[t]he application protocol *also denotes* the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer.” EX1001 2:6-11 (emphasis added). The POSITA would have understood these statements, which include the signals of “when referring to ... below,”

“denotes,” and “also denotes,” to express an intent by the author to set forth definitions for understanding those terms according to the definitions provided. EX2004, ¶63.

The POSITA would have understood those definitions to be consistent with the '682 patent's description of an exemplary protocol stack including an application layer and possible protocols in Figures 1 and 2, further confirming the patent's intent to provide definitions for understanding its technical disclosures. EX1001 at 5:65-6:2, Figure 1; EX2004, ¶64. The combined application layer with possible protocols of Figure 2 is consistent with the description of Figure 1. EX2004, ¶64.



EX1001, Figs. 1 and 2

Accordingly, the POSITA would therefore have understood the specification of the '682 patent to define “application layer” to mean “the layers above the transport layer (layers above 4)” and “application protocol” to mean “the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer.”

EX1001 2:6-11; EX2004, ¶65.

The POSITA would have understood that by setting forth these definitions in a preliminary section (“Background of the Invention”), the ’682 patent intends to define how these terms should be interpreted when referenced “below” in the other parts of the patent. See EX1001, 2:6-11; EX2004, ¶66. As the POSITA would have known, authors of technical documents commonly include definitional statements for terms that readers might be familiar with from usage in other contexts, but that should be understood in a particular way for purposes of that document. EX2004, ¶66. This is commonly done, for example, to provide clarity, reduce ambiguity, or to provide context for other technical matters to be understood. EX2004, ¶66. The patent thus indicates that its definitions of “application layer” and “application protocol” apply to the patent’s descriptions of the invention generally, and not just to a particular or preferred embodiment. See *Edwards Lifesciences LLC v. Cook Inc.*, 582 F.3d 1322, 1334 (Fed. Cir. 2009) (finding a patentee’s lexicography that “signal[ed] an intent to define the word to which it refers” was not limited to the preferred embodiment).

Furthermore, the POSITA would have understood the patent’s use of “denotes” to signal a definition of “application layer” and “application protocol.” EX1001 2:6–11; EX2004, ¶67. In *Ecolab, Inc. v. FMC Corp.*, 569 F.3d 1335, 1344–45 (Fed. Cir. 2009), the court found a patentee’s use of the word “denotes”

demonstrated that the patentee “clearly chose” to act as its own lexicographer to define the term “sanitize.” There, the court noted that “the patent explicitly states that the term ‘sanitize’ ‘denote[s] a bacterial population reduction to a level that is safe for human handling and consumption,” and held that by this statement in the specification, the patentee “clearly chose” “to act as his own lexicographer to define a patent term.” *Id.* (citing *Phillips*, 415 F.3d at 1316). Likewise, the inventors here used the word “denotes” to define “application layer” and “application protocol” in the context of their patent. EX1001 2:6–11. A person of ordinary skill in the art would have understood the use of “denotes” to indicate that “application layer” and “application protocol” is defined by what follows. EX2004, ¶67. The word “denotes” is a normal English word that is used in technical and academic writing in this way, and thus would have been understood by the POSITA. EX2004, ¶67.

The Board should therefore adopt Patent Owner’s construction.

VII. PETITIONERS HAVE NOT DEMONSTRATED THAT ANY CHALLENGED CLAIM IS UNPATENTABLE

A. The challenged claims are patentable over Handley in combination with Basturk (Ground I).

1. The Petition does not show that Handley qualifies as prior art.

Petitioners’ only theory as to how Handley (EX1005) allegedly qualifies as prior art is Petitioners’ unsupported assertion that Handley allegedly published on “February 11, 1999, in the Computer Networks journal.” Petition, 4. The entirety

of Petitioners' argument is this pair of sentences:

Handley (EX1005) – *Very Large Conferences on the Internet: The Internet Multimedia Conferencing Architecture and the MBONE*, published February 11, 1999, in the Computer Networks journal. Handley is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art.

Petition, 4. The Petition cites no other evidence for the purpose of supporting its assertions that Handley published on that date in that journal. See Petition, 4.

In its institution decision, the Board found that the Petition “cites to Dr. Houh’s Declaration testimony” in paragraphs 59-61 of his Declaration. Paper 16 at 14 (citing Pet. 4). The Petition “incorporated by reference” the entirety of Dr. Houh’s “overview” discussion of the asserted reference in Section VI of his report, which contains those paragraphs. Petition, 4. Dr. Houh’s only statement in those paragraphs regarding the alleged publication of Handley is nearly identical to the Petition’s:

Handley (EX1005) – *Very Large Conferences on the Internet: The Internet Multimedia Conferencing Architecture and the MBONE*, was published February 11, 1999, in the Computer Networks journal.

EX1003, ¶ 59.

The Handley document (EX1005), however, bears no indicia of either a publication date of “February 11, 1999” or that it was published in “the Computer Networks journal”—it has no publication markings at all. *See* EX1005.

In instituting this IPR, the Board found a reasonable likelihood that “Dr. Houh’s sworn testimony that Handley was published *on February 11, 1999 in the Computer Networks journal* is true.”¹ Paper 16 at 15 (emphasis added). The Board also found a reasonable likelihood that “a person of ordinary skill, exercising reasonable diligence, would have found Handley *in the Computer Networks Journal*.” *Id.* at 16 (emphasis added).

However, the Petition includes no *evidence* to support its assertion that Handley allegedly published in the Computer Networks journal on February 11, 1999. *See* Petition, 4. Following Petitioners’ assertion, there is no identification of any supporting evidence. *Id.* The Board’s observation that “[h]ere, the Petition states that Handley was published on February 11, 1999, in the Computer Networks Journal, and cites to Dr. Houh’s Declaration testimony,” Paper 16 at 14 (citing Pet. 4), is apparently referring to the Petition’s previous express incorporation by reference of an entire prior art “overview” section of Dr. Houh’s expert declaration:

¹ “Handley” is the document submitted with the Petition as Exhibit 1005. Paper 16 at 7 n.2.

Petitioners' challenge is based on the following prior art, for which a detailed overview is provided in the Declaration of Dr. Houh, which is incorporated by reference. EX1003, Section VI.

Petition, 4.

The Petition's express incorporation by reference of Section VI of Dr. Houh's declaration is a clear violation of 37 C.F.R. § 42.6(a)(3). 37 C.F.R. § 42.6(a)(3) ("Arguments must not be incorporated by reference from one document into another document."). *Finjan Holdings, Inc. v. Sophos Limited*, IPR2015-01405, Paper 37 at 37 n.11 (PTAB Nov. 30, 2016) ("Our rules prohibit arguments made in a supporting document from being incorporated by reference into a petition.")

If Dr. Houh's incorporated testimony is to be treated as evidence in the Petition, the Petition and supporting evidence, taken together, is nevertheless insufficient to prove that Handley was published in the Computer Networks journal on February 11, 1999. As explained above, Handley itself includes no indicia of publication in the Computer Networks journal, thus it is insufficient. See *ResQNet.com, Inc. v. Lansa, Inc.*, 594 F.3d 860, 865-66 (Fed. Cir. 2010) (affirming finding of no public accessibility for document "not marked with any indicium of ... publication" and accompanied by "no evidence as to the source, publication, or public accessibility"). The Petition's assertion that Handley was published is not

evidence of public accessibility. *Icon Health & Fitness, Inc. v. Strava, Inc.*, 849 F.3d 1034, 1043 (Fed. Cir. 2017) (“Attorney argument is not evidence.”). Dr. Houh’s testimony is a conclusory assertion unaccompanied by underlying facts or data to support it, thus it “is entitled to little or no weight” under the Board’s rules, 37 C.F.R. § 42.65(a), and, in all events, cannot support a finding of public accessibility. *TQ Delta, LLC v. Cisco Sys.*, 942 F.3d 1352, 1358 (Fed. Cir. 2019) (“Conclusory expert testimony does not qualify as substantial evidence.”).

“A reference is considered publicly accessible ‘upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.’” *Jazz Pharms.*, 895 F.3d at 1355. Petitioners have failed to carry their burden in showing that Handley was publicly accessible. They do not present sufficient or persuasive evidence showing that Handley was published in Computer Networks Journal on February 11, 1999, which is the only basis for public accessibility set forth in the Petition.

Petitioners have filed a motion to submit supplemental information that is purportedly related to the Petition’s assertion that Handley was published in the Computer Networks journal on February 11, 1999. Paper 21. Patent Owner opposes Petitioners’ motion, and the Board has not ruled on Petitioners’ motion. Paper 25. Because Petitioners’ supplemental information is not admitted into the case now and

may never be, and because Patent Owner does not know if or how Petitioner will rely on it if admitted (*id.* at 6-8), Patent Owner does not address it here. Patent Owner reserves all rights to address Petitioners' proposed evidence in its Sur-Reply, to the extent Petitioners are permitted to (and do) rely on it in their Reply to this Patent Owner's Response. Patent Owner further notes that, as explained in its opposition to Petitioners' motion for supplemental information, Petitioners' supplemental information definitively shows that Handley was not published in Computer Networks Journal on February 11, 1999; a different document was instead, with a different set of authors, a different title, and many substantive differences as compared with Handley. *Id.* at 1-4, 6.

Finally, because Petitioners have not shown that Handley qualifies as prior art, Petitioners have failed to show that any challenged claim is unpatentable over the combination of Handley and Basturk.

2. **Petitioners fail to show that the POSITA would have been motivated to combine Handley and Basturk to arrive at the claimed invention.**
 - a. **The POSITA would not have been motivated to modify Handley with Basturk as suggested by Petitioners.**

Petitioners argue that “[a] POSITA would have been motivated to modify *Handley* with *Basturk* for many reasons,” citing paragraphs 63-70 of Dr. Houh's report. Petition, 10. As explained below, and as Dr. Stubblebine explains, each of

Petitioner's reasons are incorrect. EX2004, ¶104.

Petitioners acknowledge that Handley does not disclose “inserting, at the transmitter, authentication data at end of a whole RTP packet payload,” but assert that it would have been obvious to modify Handley with Basturk's “on-the-fly” computation methods because of its purportedly “known communication benefits,” such as “faster data transmission.” Petition, 10. Specifically, Petitioners claim that Basturk's “on-the-fly” processing would enable “MAC generation [to] be carried out *as data transmissions proceeds* rather than before *these operations* have completed,” because “[t]he goal is to avoid slowing down the regular flow of data.” Petition, 11. Petitioners' argument is incorrect for multiple reasons. EX2004, ¶105.

First, Petitioners' characterization of Basturk's “on-the-fly” processing is incorrect. EX2004, ¶106. Basturk's statement that “MAC generation should be carried out as data transmission proceeds rather than before *these operations* have completed” is not referring to computing a MAC while the *packet* is being transmitted, as Petitioners suggests. Petition, 11; EX2004, ¶106.

Instead, Basturk is referring to starting the process of computing the style of MAC during (or in parallel with) the process of *retrieving context data* for performing cryptographic operations. EX2004, ¶107. In other words, Basturk is referring to starting the process of MAC computation while the process of *retrieving context information* for computing a cryptographic portion of the MAC is being

performed. EX2004, ¶107; EX1006 at 8. Basturk does not, however, teach computing a MAC in parallel with “transmission of the packet” or that doing so would result in faster “data transmission,” as Petitioners’ expert, Dr. Houh, suggests. EX1003 ¶65. EX2004, ¶107.

As Dr. Stubblebine explains, data is passed up and down the layers of a protocol stack in Protocol Data Units (PDUs), which are passed only when PDU formation is completed. EX2004, ¶108. Data *transmission* does not occur until the data is passed down to the physical layer where it is transmitted (in conjunction with the link layer) as bits. EX2004, ¶108. The POSITA would have understood that if a packet requires information to be computed (*e.g.*, a signature), that information will always have to be computed before passing the PDU to the next layer. EX2004, ¶108. Accordingly, the POSITA would have understood that even with Basturk’s “on-the-fly” processing, packets would not be passed to the next layer until all computations for that packet are complete. EX2004, ¶108. The POSITA would therefore not have understood Basturk’s “on-the-fly” computation to be “done in parallel with the transmission of the packet” such that “the computed signature is placed at the end of the packet just as the transmission is completing,” as Dr. Houh incorrectly suggests. EX2004, ¶108; EX1003 ¶ 65.

Petitioners further assert that Basturk’s “secure transport protocol is compatible with *Handley’s* internet conferencing architecture,” and that the POSITA

would have found it obvious to use Basturk’s “on-the-fly” authentication method with Handley’s internet conferencing architecture. Petition, 11-13. Petitioners are incorrect. As explained above, Basturk’s secure transport protocol is a *transport level* protocol that specifically operates at the transport layer, not at the application layer. See § III.B, *supra*; EX2004, ¶110. And, as Petitioners point out, “Basturk teaches its security features ‘reflect[] the need to add security functionality in a way which is consistent with, and best matches, the existing communication structure’ and so that ‘[a]pplications using the regular transport protocol [will] not have to be modified at all.’” Petition, 11 (citing EX1006, 3, 5) (emphasis added). Basturk accomplishes that goal by expressly *not* implementing its security features at the application layer, and instead providing security specifically at the transport layer. See § III.B, *supra*; EX2004, ¶110. Accordingly, the POSITA would not have been motivated to modify Handley in a way that would arrive at the claimed invention, *i.e.*, at the application layer. *ActiveVideo Networks, Inc. v. Verizon Communs., Inc.*, 694 F.3d 1312, 1328 (Fed. Cir. 2012) (motivation to combine must explain “why a person of ordinary skill in the art would have combined elements from specific references *in the way the claimed invention does*”).

b. Basturk’s protocol for reliable transport is incompatible with Handley’s use of RTP.

As Dr. Stubblebine explains, it would not have been obvious to the POSITA

to modify Handley’s architecture, which uses RTP over the User Datagram Protocol (UDP), with Basturk’s transport protocol, which “is essentially an extension of the standard transport level *reliability* feature.” EX1006 at 4; EX2004, ¶111. The POSITA would have understood that “the standard transport level reliability feature” is a feature provided by protocols, such as the well-known Transmission Control Protocol (“TCP”). EX2004, ¶111; EX2006. Reliability is the ability to “recover from data that is damaged, lost, duplicated, or delivered out of order,” and is achieved through timeout and retransmission policies, reordering packets received out of order based on sequence numbers, and eliminating duplicates, among other things. EX2004, ¶111; EX2006 at 10; *id.* at 16 (“Transmission is made reliable via the use of sequence numbers and acknowledgments.”). The POSITA would have understood that the increase in reliability of TCP (and other reliable delivery protocols) comes at the cost of end-to-end delay caused by its reliability features. EX2004, ¶111.

The POSITA would also have understood that Basturk’s protocol, as “an extension of the standard transport level *reliability* feature,” would involve similar delays as other reliability protocols like TCP. EX2004, ¶112. Indeed, Basturk’s protocol achieves “secure delivery” by providing acknowledgements that include sequence numbers and are signed. EX2004, ¶112; EX1006 at 12 (“Secure delivery is guaranteed because the ACKs include sequence numbers and are signed.”). The

POSITA would therefore have understood that Basturk's protocol is a reliable delivery protocol like TCP and would therefore have similar end-to-end delay drawbacks. EX2004, ¶112.

Handley teaches away from using reliability protocols like Basturk's for transmitting RTP traffic. EX2004, ¶113. Handley teaches that "[r]eal-time internet traffic is defined as datagrams that are delay sensitive," such as where "where exceeding an end-to-end delay bound of a few hundred milliseconds renders the datagrams useless for the purpose they were intended." EX2004, ¶113; EX1005 at 4-5. Handley states that "For the purposes of this definition, TCP traffic is normally not considered to be real-time traffic." EX2004, ¶113; EX1005 at 5. The POSITA would have understood that Handley considers TCP traffic to be non-real-time because of the delay associated with its reliability features. EX2004, ¶113. The POSITA would have also understood that this is why Handley implements real-time RTP traffic over UDP, which is not a reliable delivery protocol, and distinguishes between real-time traffic (RTP over UDP) from non-real-time traffic (traffic over TCP) for prioritized processing. EX2004, ¶113; EX2007 at 1 ("[UDP] is transaction oriented, and delivery and duplicate protection are not guaranteed. Applications requiring ordered reliable delivery of streams of data should use the Transmission Control Protocol (TCP).").

The POSITA would have understood that because Basturk's protocol is a

reliable delivery protocol like TCP, it would be unsuitable for transporting Handley's real-time RTP traffic for the same reasons that Handley teaches TCP is unsuitable. EX2004, ¶114. Accordingly, the POSITA would have been discouraged and led away from modifying Handley's implementation of RTP over UDP with Basturk's reliable transport protocol.

Furthermore, the POSITA would have understood that because Basturk's protocol is a reliable delivery protocol like TCP, it would be unsuitable for use with Handley which relies on a multicast network for delivery of packets. EX2004, ¶115. Applications relying on multicast delivery networks can easily scale to many receivers because the senders do not need to do any additional work when a new receiver joins (or leaves) a multicast group. EX2004, ¶115. The same applies to broadcast delivery. EX2004, ¶115. The POSITA would also understand, however, that a multicast delivery is incompatible with a reliable delivery protocol such as TCP or any protocol based on TCP or that has similar functionality. EX2004, ¶115. This is because TCP is a connection-oriented protocol, which means it establishes a direct connection between two endpoints before data can be sent, where the sender and receiver know who each other are. EX2004, ¶115; EX2006 at 11. This connection setup is referred to as a three-way handshake. EX2004, ¶115; EX2006 at 33-34, 36 ("The 'three-way handshake' is the procedure used to establish a connection."). Using a reliability protocol like TCP or Basturk would be

incompatible with Handley’s architecture in which “[s]enders never *need* to know who the receivers are.” EX2004, ¶115; EX1005 at 3. That is because with a reliable delivery protocol, the senders must know who each of the receivers are. EX2004, ¶115; EX2006 at 11, 16.

The POSITA would have also understood that the use of a reliable delivery protocol would be incompatible with Handley because of the delays associated with the sender needing to process acknowledgement messages sent by receivers to determine if a retransmission of a message is required by a sender. EX2004, ¶116; EX2006 at 10 (“If the ACK is not received within a timeout interval, the data is retransmitted.”). Basturk’s protocol similarly uses acknowledgements, and thus would be incompatible with Handley due to delays caused by acknowledgment and retransmission. EX2004, ¶116; *see, e.g.*, EX1006 at 12 (“Secure delivery is guaranteed because the ACKs include sequence numbers and are signed.”).

3. Independent Claim 1

a. Element [1.1]

i. Basturk teaches away from modifying Handley’s application layer with Basturk’s transport protocol.

Basturk expressly states that its design of a secure transport protocol “reflects the need to add security functionality in a way which is *consistent with, and best matches, the existing communication structure*” and so that “[a]pplications using

the regular transport protocol should not have to be modified at all.” EX1006 at 3, 5. Basturk further indicates that implementing its security features at the application layer would be “poor design,” “belies the layered communication structure,” would “adversely affect performance,” would “mak[e] implementation significantly harder,” duplicate functionality” and “degrade performance.” EX1006 at 4 n.3, 12. The POSITA would have understood Basturk to discourage and lead away from modifying an existing application layer communication structure to include the features of Basturk’s protocol. EX2004, ¶¶117-118.

ii. Petitioners do not show that Handley or Basturk discloses this claim element.

Petitioners argue that “a POSITA would have understood that *Handley* discloses the implementation of *authentication* at the RTP packet level” based on Handley’s use of “RTP encryption,” Petition, 17, which Dr. Houh explains is “the encryption [that] is specified by RTP.” EX1003 ¶ 78. However, the POSITA would have understood that while the RTP specification includes provisions for packet *encryption*, RTP explicitly states that “[a]uthentication and message integrity are not defined” in the RTP specification. EX2004, ¶119; EX1008 at 50. Accordingly, the POSITA would not have understood Handley’s mentioning of RTP’s encryption schemes to disclose providing authentication at the RTP packet level. EX2004, ¶119.

Petitioners concede that “Basturk does not explicitly disclose RTP.” Petition, 11. Petitioners identify nothing in Basturk that discloses “providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer.” See Petition, 15-19; EX2004, ¶120.

iii. The POSITA would not have found it obvious to combine the teachings of Handley and Basturk as Petitioners suggests.

For the reasons explained in Sections VII.A.2 and VII.A.3.a.i-ii above, Petitioners have not shown that “a POSITA would have found it obvious to implement Basturk’s secure transport protocol and its authentication techniques to Handley’s internet conferencing architecture.” Petition, 18 (citing Section X.A.1); EX2004, ¶121.

Petitioners have also failed to show that Element [1.1] would have been obvious the POSITA in view of Handley in combination with Basturk. EX2004, ¶122.

Petitioners point to Basturk’s statements that “[a]pplication level security features,” including encrypting and signing data before passing it to the transport layer, “are easily (and usually) provided by application level security.” Petition, 18. Basturk, however, does not disclose or suggest “providing transmitter-to-receiver authentication *at a [RTP] packet level*” or that doing so is “easily” or “usually” done. EX2004, ¶123. Indeed, Petitioners concede that “Basturk does not explicitly

disclose RTP.” Petition, 11. Furthermore, the RTP specification itself—the document that defines the features of RTP—makes clear RTP does not provide authentication or integrity, EX1008 at 50 (“[a]uthentication and message integrity are *not defined*”), and it expresses the clear expectation that “authentication and integrity services will be provided by *lower layer protocols*,” *i.e.*, at a layer lower than RTP, and thus not at the application layer. EX2004, ¶123; EX1008 at 50 (emphasis added). Thus, the POSITA would not have found it obvious to provide authentication at an RTP packet level as an application protocol on an application layer in view of the combination of Handley and Basturk. EX2004, ¶123.

Petitioners also point to Basturk’s transport level integrity feature whereby “data is signed by [transport machine] M_A under the session key α ” and “[o]n receiving a signed packet, M_B uses α to verify the signature.” Petition, 18. Petitioners then states that “key elements” of this technique “takes place as an application protocol on an application layer” because “cryptographic functions such as key exchange and selection of a key to use for communication, occur at the application layer, since such keys are passed from the application layer to the transport layer.” Petitioners are incorrect. EX2004, ¶124.

As Dr. Stubblebine explains, once Basturk’s application A passes a long-lived key a to the transport level, *i.e.*, to the secure transport machine M_A , “*the machine* initiates and executes an authentication and key exchange protocol with M_B ,” which

“results in the distribution of a new (fresh) session key α while making sure that this key is authentic (ie. known only to M_A and M_B).” EX2004, ¶125; *see* § III.B, *supra*; EX1006 at 9 (emphasis added). Then, “the task of applying any cryptographic functions or taking other security steps” is left to the transport machine at the transport layer. EX2004, ¶125; *see* § III.B, *supra*; EX1006 at 4, 8. Basturk is clear that “only the transport machines M_A and M_B know about the session key,” and that it is never seen at the application layer. EX2004, ¶125; *see* § III.B, *supra*; EX1006 at 10 (“A and B never see it.”). Accordingly, the POSITA would have understood that Basturk’s protocol, which Basturk makes clear is a transport level protocol below the application layer, does not provide authentication as an application protocol on an application layer. EX2004, ¶125.

b. Element [1.2]

Petitioners argue that “a POSITA would have understood and found obvious” that in the proposed combination of Handley and Basturk, authentication data (a MAC) (1) “would be placed at the end of the whole RTP packet payload to enable ‘on-the-fly’ signature computation and verification,” and (2) “[would] allow[] the transmitter to transmit data while simultaneously computing the authentication data.” Petition, 20. Both of Petitioners arguments are incorrect. EX2004, ¶126.

i. Basturk’s “on-the-fly” signature computation is not enabled by the use of a trailer.

As explained above, Basturk’s “on-the-fly” technique is enabled by (1)

putting context information early in each packet, (*i.e.*, in a security segment in the packet's header) to reduce context retrieval latency, and (2) using a MAC algorithm that permits computation to begin before the retrieval of context information (including the session key α) is complete. *See* § III.B, *supra*; EX2004, ¶127.

In view of Basturk's clear teachings of how on-the-fly processing is enabled, the POSITA art would have understood Basturk to teach that "on-the-fly" processing is enabled first by locating context information for signature verification early in the packet—not by locating the signature at the end of the packet in a trailer. EX2004, ¶87. A person of ordinary skill in the art would have understood that this placement of context information is how the reduction in context retrieval time would be achieved. EX2004, ¶87. Conversely, a person of ordinary skill in the art would have also understood that Basturk's placement of the packet *signature* (*i.e.*, the MAC) in a trailer is not what enables the retrieval of the *context information* to be performed "as quickly as possible." EX1006 at 12; EX2004, ¶119.

Furthermore, a person of ordinary skill in the art would have understood Basturk to teach that "on-the-fly computation" is further enabled by choosing a style of MAC algorithm that permits part of the computation to be performed on a received message before context is retrieved—not by placing the MAC in a trailer. EX2004, ¶88. A person of ordinary skill in the art would have understood that the signature computation style depends on the algorithm selected, not where the

signature value is located in the packet. EX2004, ¶88. In other words, placing the signature value in a trailer would not result in a style of signature computation that can be started before context is retrieved. EX2004, ¶88.

A person of ordinary skill in the art would therefore have understood that neither of the two “components” for enabling Basturk’s “on-the-fly” computation requires or is enabled by locating the signature value (MAC_{α}) in a trailer. EX2004, ¶89. The POSITA would therefore not have been motivated to use a trailer to achieve “on-the-fly” processing. EX2004, ¶89.

ii. Basturk’s on-the-fly processing does not enable simultaneous data transmission and authentication data computation

Petitioners’ argument that placing the MAC in a trailer would “allow[] the transmitter to transmit data while simultaneously computing the authentication data” is incorrect for similar reasons explained above regarding Petitioners incorrect motivation to combine Handley and Basturk. See § VII.A.2.a; EX2004, ¶126.

As Dr. Stubblebine explains, data is passed between the layers of a protocol stack in PDUs only their formation is completed, including signature generation. EX2004, ¶108. Data *transmission* does not occur until the PDUs are passed down to the physical layer where the data transmitted (in conjunction with the link layer) as bits. EX2004, ¶108. Accordingly, the POSITA would have understood that even with Basturk’s “on-the-fly” processing, packets would not be passed to the next layer

until all computations for that packet, including the MAC, are complete. EX2004, ¶108. This means that the transmitter would not transmit the data while simultaneously computing the MAC, as Petitioners incorrectly suggest. EX2004, ¶108.

Although not discussed in the Petition, Dr. Houh further opines that “the Ethernet standard ... employs the same design choice reasoning to include a ‘Frame Check Sequence’ (‘FCS’) at the end of the Ethernet frame *so it can be computed during transmission and appended to the end of the frame.*” EX1003 ¶ 85 (emphasis added). As Dr. Stubblebine explains, in the context of Ethernet, transmission refers to generating and transmitting electromagnetic waves on a physical medium at ISO layer 1 (in conjunction with the link layer ISO layer 2) where the PDU is a single bit. EX2004, ¶128; see EX1014 at 32, 142-143.

Dr. Stubblebine further explains that the POSITA would have found it obvious to implement Ethernet’s bit-by-bit transmission principles at higher level protocols, including RTP. EX2004, ¶129-133. This is because the PDU needs to go through the process of encapsulation down the protocol stack until it reaches the physical layer, which is where bit-by-bit transmission on the physical layer occurs. EX2004, ¶129. This transmission at the physical layer does not happen before the processing at higher layers is complete. EX2004, ¶129. Accordingly, the use of on-the-fly processing and/or a trail in a higher layer PDU would not allow “signature

computation [to be] done in parallel with the transmission of the packet,” as Dr. Houh incorrectly suggests. EX2004, ¶129; EX1003, ¶85. Thus, the POSITA would not have been motivated to add a trailer to an RTP packet or use on-the-fly processing based on the physical layer transmission process that Dr. Houh describes. EX1003, ¶85; EX2004, ¶109.

Dr. Stubblebine further explains that the POSITA would have understood that RTP looks for information in the *header* to check for validity issues, including “to verify that incoming packets have been correctly decrypted.” EX2004, ¶134; EX1008 at 59. This further demonstrates that the POSITA would not have been motivated to add a trailer to an RTP packet based on the location of error checking data in a lower level protocol. To the contrary, RTP provides a method for extending the RTP *header* to support additional information, which can advantageously be “*less expensive to process because it is not conditional nor in a variable location.*” EX2004, ¶134; EX1008 at 14-15. Accordingly, the POSITA would not have been motivated to use on-the-fly or a trailer at the end of an RTP packet based on the use of trailers in other lower level protocols.

c. Element [1.3]

Petitioners concede that “Handley does not expressly disclose ‘inserting, at the transmitter, authentication data at end of a whole RTP packet payload,’ Petition, 10, thus they have not shown that Handley discloses ascertaining “whether the

receiver knows the transmitter based on the RTP packet level authentication data,” as the claim requires. *See* § VII.A.3.a-b, *supra*; EX2004, ¶135.

Furthermore, Petitioners concede that Basturk does not disclose RTP, Petition, 11, thus they have not shown that Basturk discloses ascertaining “whether the receiver knows the transmitter based on the RTP packet level authentication data,” as the claim requires. *See* § VII.A.3.a-b, *supra*; EX2004, ¶136.

Petitioners alleges that Element [1.3] would have been obvious over the combination of Basturk and Handley, based on their arguments for Elements [1.1] and [1.2]. *See* Petition, 20. But “*the* RTP packet level authentication data” of Element [1.3] refers to the authentication data “at end of a whole RTP packet payload” that was inserted “as an application protocol on an application layer” per the requirements of Elements [1.1] and [1.2]. For the reasons explained above, Petitioners have not shown that it would have been obvious to the POSITA to combine Handley and Basturk to arrive at the requirements of Elements [1.1] and [1.2]. *See* § VII.A.3.a-b, *supra*; EX2004, ¶137. Accordingly, Petitioners have not shown that Element [1.3] was disclosed or rendered obvious for the same reasons. EX2004, ¶137.

4. Independent Claims 25-28

Petitioners arguments for independent claims 25-28 rely on their arguments for Elements [1.1]-[1.3]. *See* Petition, 36-41. Accordingly, Petitioners have failed

to show that claims 25-28 would have been obvious over the combination of Handley and Basturk for the reasons explained above with respect to Elements [1.1]-[1.3]. See §§VII.A.1-3, *supra*.

5. All dependent claims are patentable over Handley in combination with Basturk.

Claims 2-24 depend on claim 1. Claim 1 is patentable over Handley in combination with Basturk for the reasons explained above. See §§VII.A.1-3, *supra*. Accordingly, by their dependency on claim 1, claims 2-24 are patentable over Handley in combination with Basturk.

B. The challenged claims are patentable over PacketCable in combination with Handley (Ground II).

1. The Petition does not show that PacketCable qualifies as prior art.

Petitioners claim that PacketCable “published” on December 1, 1999 (a date that appears on the face of PacketCable). Petition, 5; EX1007. However, the Petition fails to support the assertion that PacketCable “published” on that date—PacketCable itself does not describe that date as a publication date, and Petitioners fail to show that it is. Dr. Houh’s declaration provides no more than the Petition regarding PacketCable’s alleged publication. EX1003, ¶61.

Petitioners’ Reply to Patent Owner’s Response argues that there’s “no suggestion that [PacketCable] was not intended for public distribution,” and alleges that PacketCable’s “purpose is to be adopted, thus inferring public accessibility.”

Paper 14 at 3. But that is not the standard for public accessibility.

“The standard for public accessibility is whether interested members of the relevant public could locate the reference by reasonable diligence.” *Weber, Inc. v. Provisur Techs., Inc.*, 92 F.4th 1059, 1067 (Fed. Cir. 2024). Petitioners point to the present-day CableLabs website as purported evidence of how a “[r]easonably diligent POSITA” would “confirm with CableLabs” about PacketCable’s accessibility. Paper 14 at 3. But this fails to meet Petitioners’ burden for multiple reasons.

First, the present-day CableLabs website does not show accessibility at the relevant time, *i.e.*, before the ’682 patent’s undisputed priority date. *See Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1349 (Fed. Cir. 2016) (considering whether evidence of website publication “was disseminated to the interested public *before the critical date*” (emphasis added)). Petitioners offer no evidence of accessibility by any other means besides the present day CableLabs website, which is insufficient. *See id.*

Second, Petitioners’ evidence of public accessibility at the relevant time is insufficient as a matter of law. The Federal Circuit has found more evidence of accessibility insufficient to meet a petitioner’s burden. For example, in *Blue Calypso*, the reference at issue was a report co-authored by the petitioner’s expert. *Blue Calypso*, 815 F.3d at 1348. The court considered the testimony of the

petitioner's expert of when the report was "publicly available," but found it insufficient because "there was no evidence that the ordinarily skilled artisan would know" how to locate the report. *Id.* at 1349-50.

Importantly, the court in *Blue Calypso* also declined to credit an "inference" that the reference would have been locatable. *Id.* There, the court declined to infer that the reference would have been locatable by means of a "search engine" because "[t]he record is devoid of any evidence that a query of a search engine before the critical date, using any combination of search words, would have led to" the reference. *Id.* This case is similar. Petitioners' assertion that PacketCable's purpose as a standard is to be adopted, "even to the extent that is true," "does not allow [the Board] to automatically infer" that an interested party exercising reasonable diligence at the relevant time would have located PacketCable because Petitioners offered "no evidence that the ordinarily skilled artisan would know" how to find it. *See id.* at 1349-50. Also, PacketCable is a "technical report," not a proposed standard. EX1007, 1. The inference that Petitioner advances thus does not even apply to PacketCable.

2. Independent Claim 1

a. Element [1.1]

Petitioners argue that "a POSITA would have understood (1) that manipulating RTP packets, *e.g.*, implementing RC4 or adding a MAC, results in

authentication at the packet level and (2) RTP packets are created at the application layer because RTP is an application protocol. As such, PacketCable discloses this element.” Petition, 45. Petitioners have not shown that PacketCable discloses or would have rendered obvious this claim element. EX2004, ¶140.

Petitioners have not shown that PacketCable’s alleged “implementing RC4 or adding a MAC” is provided “as an application protocol on an application layer,” as this element requires. EX2004, ¶141. The Petition incorporates Section IV of Dr. Houh’s Declaration, *see* Petition, 9, and Dr. Houh argues that the RTP specification’s description of the use of “application level framing” means that “some protocol functions are implemented in the application.” EX1003 ¶52. But Petitioners identify no RTP protocol functions “implemented in the application” in PacketCable, *e.g.*, in an “MTA Application.” *See* Petition, 44-45. Nor do they show that PacketCable’s implementation of RTP uses the application level framing concept as described in the RTP specification, which is that RTP may “provide the information required by a particular application” and may be “integrated into the application processing rather than being implemented as a separate layer.” *See* EX1008 at 4.

As Dr. Stubblebine explains, PacketCable indicates to the POSITA that MTA *devices* generally are responsible for providing secure transport services, including “Authentication, confidentiality and integrity of some messages between the MTA

and other PacketCable network elements,” namely those sent over the “pkt-s6” interface, which is a network interface for sending “[e]nd-to-end media packets between two MTAs” generally. EX2004, ¶142; see § III.C, *supra*. However, Dr. Stubblebine explains that PacketCable does not disclose the involvement of an application, *e.g.*, the “MTA Application.” *Id.* PacketCable indicates to the POSITA that PacketCable uses the MTA device to provide secure transport services whereby “RTP packets are encrypted directly with RC4, without any additional security layers” and “[a]n MMH-based MAC (Message Authentication Code) optionally provides message integrity.” EX1007 at 45; EX2004, ¶142. PacketCable, however, does not disclose how this optional additional security feature would be included. EX2004, ¶142. PacketCable relies on RTP (RFC 1889) “to transport all media streams,” EX1007 at 31, 57, but authentication and integrity are expressly “not defined” in the RTP protocol specification RFC 1889. EX1008 at 50; EX2004, ¶142. Accordingly, Petitioners have not shown that the POSITA would have understood PacketCable’s “implementing RC4 or adding a MAC” to be provided as an application protocol on an application layer. EX2004, ¶142.

Petitioners further argue that this element “would have been obvious in view of PacketCable in combination with Handley,” incorporating by references their arguments for Element [1.1] under Ground I for Handley combined with Basturk. Petition, 45. Petitioners arguments are incorrect for the reasons explained above

regarding Element [1.1] under Ground I. *See* § VII.A.3.a, *supra*; EX2004, ¶143.

b. Element [1.2]

i. Petitioners do not show that PacketCable discloses providing RTP packet-level authentication “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload.”

Petitioners argue that “PacketCable discloses this element or at least rendered it obvious.” Petition, 45. However, Petitioners do not actually show where PacketCable allegedly discloses it. *See* Petition, 45-48; EX2004, ¶144. Nor do Petitioners show that this claim element is inherently disclosed, as Petitioners suggests at least three different places where data could be placed in a packet (*i.e.*, “in the middle of the packet payload,” “the beginning,” and “the end of the payload”). Petition, 46; EX2004, ¶144.

The POSITA would have understood that PacketCable does not disclose this element, either expressly or inherently. EX2004, ¶145. PacketCable says that the PacketCable architecture “specif[ies], for each defined protocol interface, the underlying security mechanisms (such as IPSec) that provide the protocol interface with the security services it requires, e.g., authentication, integrity, confidentiality.” EX1006 at 42; EX2004, ¶145. PacketCable states that for MTA-MTA or MTA-MG communications, “RTP packets are encrypted directly with RC4, without any additional security layers,” and that “[a]n MMH-based MAC (Message

Authentication Code) optionally provides message integrity.” EX1006, 45; EX2004, ¶145.

According to PacketCable, “[e]ncryption is applied to the packet’s payload but not to its header,” and “[t]he MAC computation” for the optional MAC “spans the packet’s unencrypted header and encrypted payload.” *Id.* 47. Based on this, the POSITA would have understood that PacketCable does not disclose “inserting, at the transmitter, authentication data at end of a whole RTP packet payload,” as required by this claim element. EX2004, ¶146. While PacketCable mentions that “[e]ach RTP packet may include an optional message authentication code (MAC)” and that “MAC computation spans the packet’s unencrypted header and encrypted payload,” the POSITA would not have understood this to disclose (explicitly or inherently) inserting the optional MAC “at end of a whole RTP packet payload.” EX1007 at 47; EX2004, ¶146. PacketCable is completely silent as to where in an RTP packet the optional MAC would be inserted. EX2004, ¶146. Indeed, Petitioners does not show that PacketCable discloses placing the MAC at any of the theoretical locations they suggest. Petition, 46-48. EX2004, ¶146.

PacketCable’s non-disclosure of Element [1.2] is consistent with the POSITA’s understanding of the RTP protocol specification, which explicitly does not define an authentication service, and instead states that “[a]uthentication and message integrity are not defined in the current specification of RTP” and teaches

that “[i]t is expected that authentication and integrity services will be provided by *lower layer protocols* in the future.” EX1008 at 50 (emphasis added); EX2004, ¶148. That is, the RTP specification does not disclose inserting a MAC “at end of a whole RTP packet payload,” and, in fact, contemplates authentication and integrity services would be provided by *lower layer protocols* instead. EX2004, ¶148. A person of ordinary skill in the art would therefore have understood that PacketCable does not disclose (explicitly or inherently) “inserting, at the transmitter, authentication data at end of a whole RTP packet payload.” EX2004, ¶148.

ii. Petitioners do not demonstrate that this element would have been obvious to the POSITA in view of PacketCable and Handley.

Petitioners make an assortment of arguments as to why this element would have been obvious, but none satisfies their burden. EX2004, ¶149

Petitioners identify no negative impacts to “performance” that would result from placing, for example, a MAC in “in the middle” of a packet payload or even in the middle of a packet header. EX2004, ¶150. Regardless, in the context of RTP, the POSITA would have understood that RTP provides a header extension mechanisms to allow additional data to be placed in the header. EX2004, ¶150. The POSITA would have understood that the RTP header is comprised of fixed-length or length-determinable portions (including the extended portion), making it computationally easier (and thus more efficient) to find the data there as opposed to

the payload area, which is of a variable (and undefined) length and would require more computational resources to find the data there. EX2004, ¶150.

Petitioners do not identify any “packet fragmentation issues” that would favor putting data at the end of an RTP packet payload. EX2004, ¶151. PacketCable states that “[e]ach RTP packet may include an optional message authentication code (MAC).” EX1007 at 47; EX2004, ¶151. Given that “each” packet could include a MAC, Petitioners have not identified a reason why putting it in the middle of the payload or in the header would cause a fragmentation issue that would be avoided by putting it at the end. EX2004, ¶151.

Petitioners also identify no implementation complications that would favor putting PacketCable’s MAC at the end of an RTP packet instead of the middle of the payload area or in the header. EX2004, ¶152. Dr. Houh mentions that “data in the packet would be interrupted” and that “extra data fields would be needed to identify the exact location” of the MAC, but he offers no reason why a need for additional data fields to locate data would favor placing PacketCable’s MAC at the end of an RTP packet payload (which has a variable and undefined length). EX1003, ¶178. The POSITA would have understood that data can be found more quickly in an area with defined and/or fixed-length (or easily-determinable-length) fields, such as a header. EX2004, ¶152. And, as Dr. Stubblebine explains, RTP provides mechanisms for placing additional data in the header (*e.g.*, in a header extension),

which is advantageously “less expensive to process because it is not conditional nor in a variable location.” EX2004, ¶152; *see* EX1008 at 14-15. Moreover, the POSITA would have known and considered that RTP looks for information in the header to check for validity issues, including “to verify that incoming packets have been correctly decrypted.” EX2004, ¶152; EX1008 at 59.

Petitioners’ KSR-based “finite solutions” rationale based on putting data at the beginning or end of a payload is inapt because RTP does not define a trailer and instead defines a mechanism for placing additional information in the header. EX2004, ¶154.

Furthermore, as RTP can rely on the underlying UDP protocol for providing checksum services, EX1008 at 3; EX2004, ¶155, thus the POSITA would not have been motivated to include a trailer at the end of an RTP packet based on the use of checksums in lower layer protocols. EX2004, ¶155. RTP also looks for information in the *header* to check for validity issues, including “to verify that incoming packets have been correctly decrypted,” EX1008 at 59, which further demonstrates that the POSITA would not have been motivated to add a trailer to an RTP packet based on the location of error checking data in a lower level protocol. EX2004, ¶155.

Petitioners’ general suggestion that the POSITA would have understood that “the authentication data would go at the end of the whole RTP packet payload because it would reduce the latency of delivering the packet *since* placing the

authentication data at the beginning of the payload requires storing the packet, computing the authentication data, transmitting the packet to the network” Petition, 46-47. Petitioners’ concern about “storing the packet” is misplaced. As Dr. Stubblebine explains, for example, all PDU components need to be stored at least in temporary memory as the PDU is being prepared for passing down the protocol stack to the next layer. EX2004, ¶156. The POSITA would not have been motivated to add a trailer to end of the whole RTP packet payload based to avoid storing the packet. EX2004, ¶156. Nor would “computing the authentication data” motivate the use of a trailer. EX2004, ¶156. The same authentication process would be used to compute the authentication data if the authentication data were placed in the header or the beginning of the packet payload. EX2004, ¶156. Thus, the POSITA would not have been motivated to add a trailer to end of the whole RTP packet based on computing the authentication data. EX2004, ¶156.

The POSITA also would not have been motivated to add a trailer to end of the whole RTP to “reduce the latency of delivering the packet” at the sender side as part of “transmitting the packet to the network” to “allow the transmitter to transmit data while simultaneously computing the checksum and prevent any unnecessary transmission delay by having to first compute the checksum and then transmit the payload.” Petition, 47. EX2004, ¶157. First, the POSITA would have understood that RTP provides a mechanism placing additional information in the header, as

discussed above. EX2004, ¶158. Further, the PDU needs to go through the process of encapsulation down the protocol stack until it reaches the physical layer, which is where bit-by-bit transmission on the physical layer occurs. EX2004, ¶158. This transmission at the physical layer, however, does not depend on the location of authentication data within the RTP packet. EX2004, ¶158. Higher level protocol layers are simply encapsulated within the data link layer frame. EX2004, ¶158. Ethernet does not, for example, investigate these payloads to do anything different based on where a higher layer placed certain data. EX2004, ¶158. For similar reasons, the location of authentication data in a higher layer PDU would have no impact on whether one would or would not need to “first compute the checksum and then transmit the payload.” EX2004, ¶158. As Dr. Stubblebine explains, bit-by-bit transmission occurs at the physical layer (not at the RTP packet level), and the location of authentication data within the higher layer PDUs (such as an RTP packet) would not make that transmission faster. EX2004, ¶159. The POSITA would not have been motivated to add a trailer to an RTP packet based on the physical layer transmission process that Petitioners describe. EX2004, ¶158.

As Dr. Stubblebine explains, to the extent Petitioners are suggesting that “placing authentication at the end of the whole RTP packet payload” somehow results in bit-by-bit processing benefits occurring across all layers going down to the physical layer where transmission occurs bit-by-bit; they have not shown this.

EX2004, ¶160. This is contrary to how network protocol stacks operate. EX2004, ¶161. PDUs are created at higher layers and passed to lower layers for encapsulation. EX2004, ¶160.

Dr. Stubblebine further explains that to the extent Petitioners are suggesting that somehow bit-by-bit processing occurs at one or more layers above the physical layer; they hasn't shown how this decreases latency in transmission at the physical layer (where transmission occurs). EX2004, ¶161. For example, it makes no sense to pass data bit by bit from the transport layer (e.g. UDP or TCP) to the networking layer (e.g. IP), or to create IP, UDP, or TCP payloads of individual bits. EX2004, ¶161. This is not how protocol stacks are implemented. At each layer, encapsulation requires the receipt of the entire PDU before passing it down to the lower layer. EX2004, ¶161. Protocol stacks operating bit by bit would cause tremendous computational complexity issues and would lead to increased latency and storage issues. EX2004, ¶161. This is because doing so would require the task of managing system state information to try to keep track of individual bits associated with partial data being communicated at each layer instead of processing entire PDUs. EX2004, ¶161.

Accordingly, Petitioners have not shown that the POSITA would have found it obvious to put PacketCable's MAC in a trailer at the end of an RTP packet payload. EX2004, ¶¶162-163.

Petitioners further incorporate their arguments regarding Element [1.2] under Ground I, which, for the reasons explained above, do not show that the POSITA would have found Element [1.2] obvious. *See* § VII.A.b, *supra*; EX2004, ¶164.

c. Element [1.3]

Petitioners alleges that Element [1.3] would have been obvious over the combination of PacketCable and Handley, based on their arguments for Elements [1.1] and [1.2] under Ground II. *See* Petition, 48. But “*the* RTP packet level authentication data” of Element [1.3] refers to the authentication data that was inserted “at end of a whole RTP packet payload” per the requirements of Element [1.2]. For the reasons explained above, Petitioners have not shown that it would have been obvious to the POSITA to combine PacketCable and Handley to arrive at the requirements of Element and [1.2]. *See* §§ VII.B.2.a-b, *supra*. Thus, Petitioners have not shown that Element [1.3] was disclosed or rendered obvious for the same reasons. Petitioners’ additional arguments regarding Element [1.3] do not remedy those deficiencies. EX2004, ¶165.

3. Independent Claims 25-28

Petitioners arguments for independent claims 25-28 rely on their arguments for Elements [1.1]-[1.3]. *See* Petition, 59-64. Accordingly, Petitioners have failed to show that claims 25-28 would have been obvious over the combination of PacketCable and Handley for the reasons explained above with respect to Elements

[1.1]-[1.3]. See §§VII.B.1-2, *supra*; EX2004, ¶166.

4. Dependent Claims 22 and 24

a. Claim 22

Petitioners allege that PacketCable’s “media gateway” acts as a “switch,” and that “[i]nclusion of a gateway would have been obvious to a POSITA.” Petition, 59. However, Petitioners fail to show that PacketCable’s media gateway satisfies the requirements of the “receiver” or “transmitter” of claim 1. Petitioners do not explain whether or how the act of switching data “between a particular IP flow and a particular PSTN port” involves “inserting... authentication data at end of a whole RTP packet payload” (let alone “as an application protocol on an application layer”) or “ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data.” The POSITA would have understood that IP is at a lower layer than the application layer. EX2004, ¶167; *see, e.g.*, EX1007 at 20.

b. Claim 24

For the same reasons explained for claim 22 under Ground II, Petitioners have not shown that the combination of PacketCable and Handley discloses or renders obvious claim 24. EX2004, ¶168.

5. All dependent claims are patentable over PacketCable in combination with Handley.

Claims 2-24 depend on claim 1. Claim 1 is patentable over PacketCable in

combination with Handley for the reasons explained above. *See* § VII.B.2, *supra*. Accordingly, by their dependency on claim 1, claims 2-24 are patentable over PacketCable in combination with Handley.

C. The challenged claims are patentable over PacketCable in combination with Basturk (Ground III).

1. Petitioners fail to show that the POSITA would have been motivated to combine PacketCable with and Basturk to arrive at the claimed invention.

a. Basturk teaches away from modifying PacketCable with Basturk's transport protocol.

For the reasons explained above in Section VII.A.3.a.i, *supra*, Basturk teaches away from modifying the application layer with its transport level protocol. Basturk teaches away from modifying PacketCable at the application layer for the same reasons it teaches away from modifying Handley at the application layer. *See* § X.A.1.a, *supra*; EX2004, ¶169.

b. Basturk's protocol for reliable transport is incompatible with PacketCable's use of RTP over UDP.

The POSITA would have understood that end-to-end delay caused by reliability features is undesirable for the transmission of real-time data such as that carried by RTP. EX2004, ¶170. Indeed, Handley discusses how reliable protocols like TCP are generally not suitable for transporting real-time data using RTP, thus it seems to provide a solution for better transport of RTP over UDP. EX2004, ¶170.

PacketCable, like Handley, carries RTP over UDP and thus would be similarly sensitive to performance degradation caused by delays of having a reliable protocol. EX1007 at 20; EX2004, ¶170. Accordingly, the POSITA would have understood that because Basturk's protocol is a reliability protocol, it would be unsuitable for transporting PacketCable's real-time RTP traffic for the same reasons that Handley teaches TCP is unsuitable. EX2004, ¶170. Accordingly, the POSITA would have been discouraged and led away from modifying PacketCable's implementation of RTP over UDP with Basturk's reliable transport protocol. EX2004, ¶170.

c. The POSITA would not have been motivated to modify PacketCable with Basturk as suggested by Petitioners.

Petitioners asserts that “[a] POSITA would have been motivated to use Basturk's ‘on-the-fly’ signature computation with PacketCable's architecture framework” due to the purported known benefits, including reduced latency and faster transmission, and would have had a reasonable expectation of success in doing so. Petition, 64-66. Petitioners are incorrect. EX2004, ¶171.

One of Basturk's requirements for enabling “on-the-fly” computation is that “[s]ignature computation starts before the retrieval of connection context” for messages received by a receiver, which is enabled by using a style of MAC computation that can be started without knowing the key or other cryptographic information retrieved from context. EX1006 at 8, 13; EX2004, ¶172. This “on-the-

fly” processing cannot be achieved using PacketCable’s security framework. EX2004, ¶172.

According to PacketCable’s security framework, “[t]he MAC computation spans the packet’s unencrypted header and encrypted payload.” EX1007 at 47. Thus, the MAC computation—whether the MMH algorithm of PacketCable or Basturk’s algorithm, cannot even begin to be processed on the transmitter until encryption of the encrypted payload happens. EX2004, ¶173. To perform the encryption, context retrieval must necessarily take place prior to the start of any MAC computation over the encrypted payload. EX2004, ¶173. This is so even with Basturk’s MAC algorithm (which requires no key to compute the hash portion of the MAC computation) because even the portion that requires no key is computed over the entire encrypted data. EX2004, ¶173. A context retrieval is necessary to retrieve the key used to encrypt the payload data. EX2004, ¶173. Thus, the basic security structure of the PacketCable design means “on-the-fly” cannot be achieved on the packet transmission side, and thus no purported benefits of “on-the-fly” can be realized. EX2004, ¶173.

The POSITA would have understood that “on-the-fly” is also not achievable for packet reception in PacketCable. EX2004, ¶174. The POSITA would have understood that PacketCable’s “only” specified MAC algorithm is incompatible with Basturk’s “on-the-fly” processing. EX1007 at 47; EX2004, ¶174. Although

PacketCable says that its MAC algorithm can be negotiated, “the only one that is currently specified is MMH.” EX1007 at 47; EX2004, ¶174. In other words, the only MAC algorithm specified for PacketCable is a MAC based on the MMH algorithm of which a fast version was known at the time. EX2008 (Halevi); EX2004, ¶174.

The POSITA would have understood that a MAC based on MMH is incompatible with Basturk. EX2004, ¶175. Basturk requires the ability to start processing the message before the cryptographic key needs to be used because the claimed benefit is to reduce latency by performing some computation while waiting for context retrieval. EX2004, ¶175. Basturk uses this time to retrieve the key. However, as Dr. Stubblebine explains, a MAC based on the MMH is unable to start processing the message before retrieving the cryptographic key. EX2004, ¶176; EX2008 at 9.

As such, a context retrieval would be required before processing any portion of the message using the secure MAC based on MMH. EX2004, ¶177. Consequently, the delay associated with context retrieval would be unavoidable in PacketCable, meaning that “on-the-fly” cannot be achieved. EX2004, ¶177.

2. Independent Claim 1

a. Petitioners’ arguments for Grounds I and II fail to show that the POSITA would have found claim 1 obvious over PacketCable and Basturk.

For each of Elements [1.1], [1.2], and [1.3], Petitioners incorporate by reference their arguments regarding those claim elements from Grounds I-II. Petitioners have failed to show that Elements [1.1], [1.2], and [1.3] would have been obvious over the combination of PacketCable and Basturk for the same reasons explained with respect to those Elements under Grounds I-II, *supra*, which are incorporated here by reference. See §§ VII.A.3 and VII.B.2, *supra*; EX2004, ¶178.

b. Element [1.3]

Petitioners alleges that Element [1.3] would have been obvious over the combination of PacketCable and Basturk, based on their arguments for Elements [1.2] and [1.3] under Grounds I and II. Petition, 66. But “*the* RTP packet level authentication data” of Element [1.3] refers to the authentication data that was inserted “at end of a whole RTP packet payload” per the requirements of Element [1.2]. For the reasons explained above, Petitioners have not shown that it would have been obvious to the POSITA to combine PacketCable and Basturk to arrive at the requirements of Element and [1.2]. See § VII.A.3 and VII.B.2, *supra*. Petitioners have not shown that Element [1.3] was disclosed or rendered obvious for the same reasons; EX2004, ¶179.

3. Independent Claims 25-28

Petitioners arguments for independent claims 25-28 rely on their arguments for Elements [1.1]-[1.3]. *See* Petition, 69-72. Accordingly, Petitioners have failed to show that claims 25-28 would have been obvious over the combination of PacketCable and Basturk for the reasons explained above with respect to Elements [1.1]-[1.3]. *See* §§VII.A.3 and VII.B.2, *supra*.

4. Dependent Claims 22 and 24

a. Claim 22

For the reasons that explained for claim 22 of Ground II, Petitioners have not shown that the combination of PacketCable and Basturk discloses or renders obvious claim 24. *See* § VII.B.4.a; EX2004, ¶180.

b. Claim 24

For the reasons that explained for claim 22 of Ground II, Petitioners have not shown that the combination of PacketCable and Basturk discloses or renders obvious claim 24. *See* § VII.B.4.b; EX2004, ¶181.

5. All dependent claims are patentable over PacketCable in combination with Basturk.

Claims 2-24 depend on claim 1. Claim 1 is patentable over PacketCable in combination with Basturk for the reasons explained above. Accordingly, by their dependency on claim 1, claims 2-24 are patentable over PacketCable in combination with Basturk; EX2004, ¶182.

D. The challenged claims are patentable over Handley in combination with Basturk and PacketCable (Ground IV).

1. Dependent Claims 22 and 24

a. Claim 22

For the same reasons that explained for claim 22 of Grounds II and III, Petitioners have not shown that the combination of PacketCable, Handley, and Basturk discloses or renders obvious claim 22; EX2004, ¶184.

b. Claim 24

For the same reasons that explained for claim 22 of Grounds II and III, Petitioners have not shown that the combination of PacketCable, Handley, and Basturk discloses or renders obvious claim 24; EX2004, ¶185.

VIII. CONCLUSION

For the reasons stated above, every challenged claim should be found patentable.

Dated: March 13, 2024

By: /Christine E. Lehman/
Christine E. Lehman
PTO Reg. No. 38,535
Counsel for Patent Owner

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that this Patent Owner's Response complies with the type-volume limits of 37 C.F.R. § 42.24 and consists of 13,099 words, excluding the table of contents, a table of authorities, certificate of service, this certificate of compliance, or table of exhibits, and claim listing. The undersigned has relied on the word count feature of the word-processing system used to prepare this paper (Microsoft Word).

Dated: March 13, 2024

Respectfully submitted,

/Christine E. Lehman/

Christine E. Lehman

PTO Reg. No. 38,535

Counsel for Patent Owner

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a copy of the foregoing **PATENT OWNER'S RESPONSE** was served on March 13, 2024, via electronic mail to Meta_VideoLabs@kirkland.com, as agreed to by counsel for Petitioners, upon the following counsel:

W. Todd Baker
todd.baker@kirkland.com
KIRKLAND & ELLIS LLP
1301 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Ellisen Shelton Turner
ellisen.turner@kirkland.com
KIRKLAND & ELLIS LLP
2049 Century Park East
Los Angeles, CA 90067

Jonathan D. Brit
jonathan.brit@kirkland.com
KIRKLAND & ELLIS LLP
601 Lexington Avenue
New York, NY 10022

Dated: March 13, 2024

/Christine E. Lehman/
Christine E. Lehman

APPENDIX A

No.	Claim Language
Preamble [1]	A method for transmitting data from a transmitter to a receiver, comprising:
Element [1.1]	providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer
Element [1.2]	by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;
Element [1.3]	ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and
Element [1.4]	accepting, by the receiver, the whole RTP packet payload, if the receiver knows the transmitter, and otherwise rejecting the whole RTP packet payload.
Claim 2	The method as claimed in claim 1, wherein the authentication data are determined based on at least part of a protocol data unit available on the application layer, and the application protocol being linked to a secret by the transmitter.
Claim 3	The method as claimed in claim 2, wherein the secret between the transmitter and the receiver is one of a key for symmetric encryption and a key pair for asymmetric encryption.
Claim 4	The method as claimed in claim 2, wherein the part of the protocol data unit available on the application layer includes at least one of a sequence number and a timestamp.
Claim 5	The method as claimed in claim 2, wherein the secret is an encryption operation performed using one of a one-way hash function and a message authentication code with a key known only to the receiver and the transmitter to be authenticated.
Claim 6	The method as claimed in claim 2, wherein said ascertaining includes cryptographic verification using parameters and including at least one of a decryption operation and a cryptographic checksum check.
Claim 7	The method as claimed in claim 2, wherein said ascertaining includes cryptographic verification using parameters and including at least one of a decryption operation and a cryptographic checksum check.
Claim 8	The method as claimed in claim 2, wherein the linking to the secret is carried out by at least one of cryptographic linking to at

	least one further parameter, particularly by virtue of an encryption operation and a cryptographic checksum and key information.
Claim 9	The method as claimed in claim 8, wherein the secret between the transmitter and the receiver is one of a key for symmetric encryption and a key pair for asymmetric encryption.
Claim 10	The method as claimed in claim 8, wherein the part of the protocol data unit available on the application layer includes at least one of a sequence number and a timestamp.
Claim 11	The method as claimed in claim 8, wherein the encryption operation is performed using one of a one-way hash function and a message authentication code with a key known only to the receiver and the transmitter to be authenticated.
Claim 12	The method as claimed in claim 8, wherein said ascertaining includes verification at the receiver to determine whether the receiver knows the transmitter.
Claim 13	The method as claimed in claim 12, wherein the secret between the transmitter and the receiver is one of a key for symmetric encryption and a key pair for asymmetric encryption.
Claim 14	The method as claimed in claim 12, wherein the part of the protocol data unit available on the application layer includes at least one of a sequence number and a timestamp.
Claim 15	The method as claimed in claim 12, wherein the encryption operation is performed using one of a one-way hash function and a message authentication code with a key known only to the receiver and the transmitter to be authenticated.
Claim 16	The method as claimed in claim 12, wherein the verification is cryptographic verification using parameters and including at least one of a decryption operation and a cryptographic checksum check.
Claim 17	The method as claimed in claim 16, wherein the secret between the transmitter and the receiver is one of a key for symmetric encryption and a key pair for asymmetric encryption.
Claim 18	The method as claimed in claim 17, wherein the part of the protocol data unit available on the application layer includes at least one of a sequence number and a timestamp.
Claim 19	The method as claimed in claim 18, wherein the encryption operation is performed using one of a one-way hash function and a message authentication code with a key known only to the receiver and the transmitter to be authenticated.

Claim 20	The method as claimed in claim 19, wherein the authentication is carried out between the transmitter and the receiver before the data are transmitted from the transmitter to the receiver.
Claim 21	The method as claimed in claim 20, wherein the receiver and transmitter are used in Internet telephony.
Claim 22	The method as claimed in claim 21, wherein the receiver and transmitter are each disposed in at least one of a switching node and a switching installation.
Claim 23	The method as claimed in claim 20, wherein the receiver and transmitter provide packet-switched telephone services.
Claim 24	The method as claimed in claim 23, wherein the receiver and transmitter are each disposed in at least one of a switching node and a switching installation.
Preamble [25]	A system for transmitting data, comprising:
Element [25.1]	a transmitter providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level by inserting authentication data at end of a whole RTP packet payload; and
Element [25.2]	a receiver to determine whether the transmitter is known based on the RTP packet level authentication data, to accept the whole RTP packet payload if the transmitter is known and to reject the whole RTP Packet payload if the transmitter is not known,
Element [25.3]	wherein the whole RTP packet payload comprises a whole RTP packet payload header comprising at least one of a sequence number and a time stamp, and
Element [25.4]	wherein the inserting the authentication data at end of the whole RTP packet payload comprises
Element [25.5]	generating a message authentication code (MAC) according to a common secret between the transmitter and the receiver and using the whole RTP packet payload header sequence number and timestamp,
Element [25.6]	and appending the MAC to the end of the whole RTP packet payload,
Element [25.7]	and if a MAC obtained by a receiver is same as a MAC contained in transmitted whole RTP packet Payload received by the receiver, the receiver accepts the transmitted whole RTP packet.
Preamble [26]	A transmitter for sending data to a receiver, comprising:
Element [26.1]	a processor providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level by inserting authentication data at end of a whole RTP packet payload; and

Element [26.2]	a transmitter to send the whole RTP packet payload including the inserted authentication data to the receiver,
Element [26.3]	wherein the whole RTP packet payload comprises an RTP header comprising at least one of a sequence number and a time stamp, and
Element [26.4]	wherein the processor inserts the authentication data at the end of the whole RTP packet payload by generating a message authentication code (MAC) according to a common secret between the transmitter and the receiver and using the whole RTP packet payload header sequence number and timestamp, and appending the MAC to the end of the whole RTP packet payload.
Preamble [27]	A receiver for receiving data from a transmitter, comprising:
Element [27.1]	a processing unit communicably connecting with the transmitter,
Element [27.2]	determining whether the transmitter is known based on the transmitter providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level by inserting authentication data at end of a whole RTP packet payload, and
Element [27.3]	accepting the whole RTP packet payload if the transmitter is known, and rejecting the whole RTP packet payload if the transmitter is not known, based upon the RTP packet level authentication data,
Element [27.4]	wherein the whole RTP packet payload comprises a whole RTP packet payload header comprising at least one of a sequence number and a time stamp, and
Element [27.5]	wherein the processing unit obtains the authentication data added by the transmitter to the end of the whole RTP packet payload by generating a message authentication code (MAC) according to a common secret between the transmitter and the receiver and using the whole RTP packet payload header sequence number and timestamp.
Preamble [28]	A method of transmitting data from a transmitter to a receiver, comprising:
Element [28.1]	providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level by inserting authentication data at end of a whole RTP packet payload;
Element [28.2]	ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and

Element [28.3]	accepting the whole RTP packet Payload at the receiver, if the receiver knows the transmitter, and otherwise rejecting the whole RTP Packet payload,
Element [28.4]	wherein the whole RTP packet payload comprises a whole RTP Packet payload header comprising at least one of a sequence number and a time stamp,
Element [28.5]	and wherein the inserting the authentication data at the end of the whole RTP packet payload
Element [28.6]	comprises generating a message authentication code (MAC) according to a common secret between the transmitter and the receiver and using the whole RTP packet payload header sequence number and timestamp,
Element [28.7]	and appending the MAC to the end of the whole RTP packet payload,
Element [28.8]	and if a MAC obtained by a receiver is same as a MAC contained in a transmitted whole RTP packet payload received by the receiver, the receiver accepts the transmitted whole RTP packet payload.