

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTEL CORPORATION,
Petitioner,

v.

VLSI TECHNOLOGY LLC,
Patent Owner.

IPR2019-01197
Patent 6,212,633 B1

Before THU A. DANG, LYNNE E. PETTIGREW, and
KIMBERLY McGRAW, *Administrative Patent Judges*.

DANG, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

A. Background

In response to a Petition (Paper 2, “Pet.”) filed by Intel Corporation (“Petitioner”), we instituted *inter partes* review of claims 1 and 13 (the “challenged claims”) of U.S. Patent No. 6,212,633 B1 (Ex. 1001, “the ’633 patent”). See Paper 15 (“Dec. Inst.”). During trial, VLSI Technology LLC (“Patent Owner”) filed a Response (Paper 26, “PO Resp.”), to which Petitioner filed a Reply (Paper 29, “Reply”). In turn, Patent Owner filed a Sur-Reply. Paper 33 (“Sur-Reply”). An oral hearing was held with the parties on November 2, 2020. A transcript of the hearing has been entered into the record (Paper 39, “Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This Decision is a Final Written Decision under 35 U.S.C. § 318(a) as to the patentability of the claims on which we instituted trial. Based on the record before us, Petitioner has shown by a preponderance of the evidence that claims 1 and 13 of the ’633 patent are unpatentable.

B. The ’633 Patent (Ex. 1001)

The ’633 patent, titled “Secure Data Communication over a Memory-Mapped Serial Communications Interface Utilizing a Distributed Firewall,” issued on April 3, 2001, from an application filed June 26, 1998. Ex. 1001, codes (54), (45), (22).

The ’633 patent relates to “data communication over a serial communications interface, as well as to secure data communication incorporating data encryption and/or access control.” *Id.* at 1:17–20. According to the ’633 patent, “[a] distributed firewall is utilized . . . to permit secure data transmission between selected nodes over the interface,” the distributed firewall incorporating “security managers in the selected

nodes that are respectively configured to control access to their associated nodes,” thereby “restricting access to such nodes to only authorized entities.” *Id.* at code (57). Furthermore, “encrypted transmissions may be supported to restrict unauthorized viewing of data transmitted between the selected nodes over the interface.” *Id.*

Figure 1, reproduced below, shows a “data processing system implementing a distributed firewall.” *Id.* at 4:52–54.

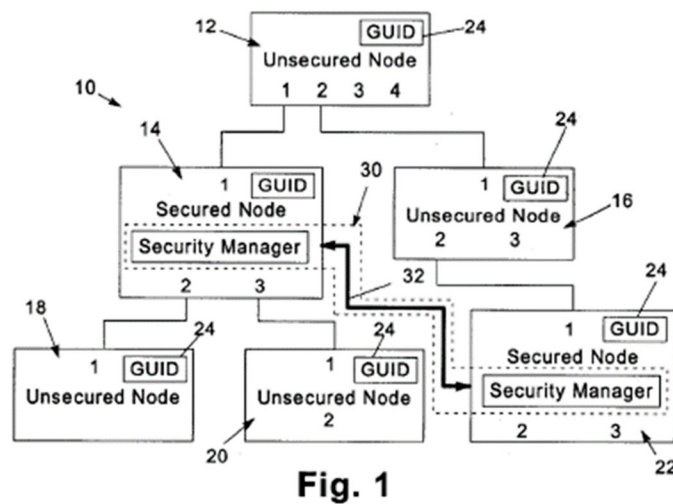


Figure 1 shows interface 10 including nodes 12–22 “interconnected with one another in a daisy-chained fashion,” each node having “one or more ports . . . selectively coupl[ing] to another port on another node in the interface.” *Id.* at 6:3–7. “Each node includes a globally unique identifier (GUID) 24 that uniquely identifies each node attached to the interface,” and the GUID of each node is “stored during production of the device within which the node is implemented.” *Id.* at 6:12–18. As shown in Figure 1, nodes 14 and 22 are “secured nodes, each of which utilizes an associated security manager 26, 28 [that] form a distributed firewall” 30 with “secured communications link” 32 therebetween. *Id.* at 6:19–24.

According to the '633 patent, a “distributed firewall” is a “collection of security managers that each control access to their associated secured nodes from the interface.” *Id.* at 6:26–28.

Figure 3, reproduced below, shows a “secured node.” *Id.* at 6:58–59.

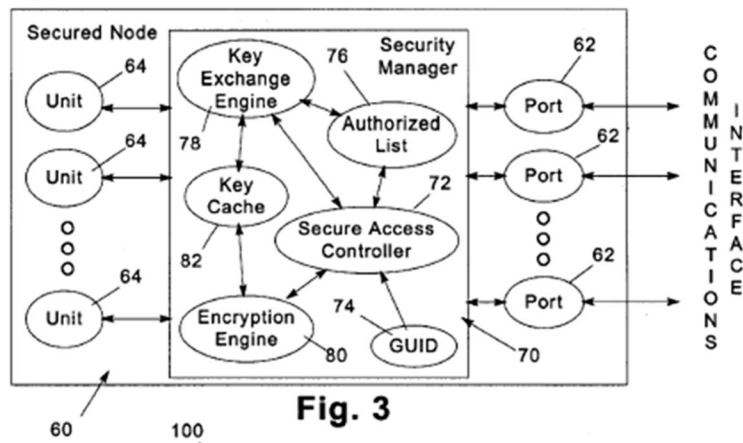


Figure 3 shows “secured node 60” including a “plurality of ports 62 that interface with a plurality of units 64,” each port 62 “represent[ing] a physical connection for the serial communication interface,” and each unit 64 “represent[ing] a particular device [to be] coupled to such a port.” *Id.* at 7:8–14. “To control access to one or more units 64 via the communications interface, security manager 70 is interposed between port 62 and unit 64.” *Id.* at 7:19–21. A security manager “includes secure access controller 72 that relies on a GUID 74 for the node, as well as authorized list 76 that stores information pertaining to other nodes that are authorized to communicate with the secured node.” *Id.* at 7:21–26. “[A]uthorization may be provided using . . . conventional digital signature and/or certification mechanisms,” for example, a “key exchange technique . . . using a key exchange engine 78.” *Id.* at 7:27–34. To ensure “controlled access to a secured node,” ensuring that “communications between secured nodes via a secured communication link may not be intercepted and monitored by unauthorized

nodes . . . , some form of encrypting of the communications between secured nodes is utilized.” *Id.* at 7:39–44.

C. Illustrative Claim

Of the challenged claims, claim 1 is the independent claim. Claim 13 depends from claim 1. Claim 1 is illustrative.

1. A data processing system, comprising:
 - (a) a plurality of nodes including at least first and second nodes;
 - (b) a memory-mapped serial communications interface coupled between the plurality of nodes and supporting peer-to-peer communication therebetween; and
 - (c) a distributed firewall including first and second security managers respectively disposed in the first and second nodes, the first and second security managers respectively configured to control access to the first and second nodes from the communications interface, and wherein the first security manager is configured to locally generate for the first node an authorization list of authorized nodes with which communication is authorized for the first node.

Ex. 1001, 22:39–53.

D. Prior Art and Asserted Grounds

We instituted *inter partes* review on all claims and all grounds in the Petition. Petitioner asserts that claims 1 and 13 are unpatentable on the following grounds (Pet. 40, 74):

Claim Challenged	35 U.S.C. §	References
1	103 ¹	Traw, ² Zou ³
13	103	Traw, Zou, Segal ⁴

Petitioner also relies on the Declaration of John D. Kubiadowicz, Ph.D. (the “Kubiadowicz Declaration”) in support of its unpatentability contentions. *See* Ex. 1002. Dr. Kubiadowicz was cross-examined by Patent Owner, and a transcript of his deposition was entered into the record. Ex. 2015. Patent Owner provides the Declaration of William Henry Mangione-Smith, Ph.D (the “Mangione-Smith Declaration”). Ex. 2012. Dr. Mangione-Smith was cross-examined by Petitioner, and a transcript of his deposition was entered into the record. Ex. 1020.

II. ANALYSIS

A. Level of Ordinary Skill in the Art

In determining whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham v. John Deere Co*, 383 U.S. 1, 17

¹ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), included revisions to 35 U.S.C. § 103 that became effective after the filing of the application that led to the ’633 patent. Therefore, we apply the pre-AIA version of 35 U.S.C. § 103.

² US 5,949,877, filed Jan. 30, 1997, issued Sept. 7, 1999 (Ex. 1003, “Traw”).

³ US 6,160,796, filed Jan. 6, 1998, issued Dec. 12, 2000 (Ex. 1004, “Zou”).

⁴ US 6,345,299 B2, filed Nov. 26, 1997, issued Feb. 5, 2002 (Ex. 1005, “Segal”).

(1966). Petitioner contends a person of ordinary skill in the art at the time of the alleged invention (“POSITA”) would have had “a Bachelor of Science or equivalent degree in Computer Science or Electrical Engineering and two years of graduate work, work experience, or the equivalent, in computer systems and architecture.” Pet. 40 (citing Ex. 1002 ¶ 30). Patent Owner does not articulate a level of skill for a POSITA. *See generally* PO Resp.

Based on our review of the ’633 patent, the types of problems and solutions described in the ’633 patent and cited prior art, we adopt and apply Petitioner’s definition of a person of ordinary skill in the art at the time of the claimed invention.

B. Claim Construction

For petitions filed on or after November 13, 2018, such as here, we apply 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. *See* Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340, 51,340, 51,358 (Oct. 11, 2018) (amending 37 C.F.R. § 42.100(b) effective November 13, 2018) (now codified at 37 C.F.R. § 42.100(b) (2019)); *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

We address the disputed claim terms discussed by the parties.

1. “distributed firewall” (claim 1)

Petitioner contends that the term “distributed firewall” should be construed to mean “a collection of security managers that each control the access to their associated nodes from the interface.” Pet. 39 (citing Ex. 1002

¶ 85). According to Petitioner, “[t]he proposed construction fully comports with the ’633 patent.” *Id.* (citing Ex. 1001, 3:52–56 (“The distributed firewall incorporates security managers in the selected nodes that are respectively configured to control access to their associated nodes, thereby restricting access to such nodes to only authorized entities”); Ex. 1002 ¶ 86).

Patent Owner responds that Petitioner’s construction is too broad, the term “distributed firewall” cannot be “encryption itself,” and “firewall” cannot be defined to include security managers that control access to the various nodes through encryption alone. PO Resp. 5, 11–12.

We agree with Petitioner’s proposed construction and thus adopt the construction. We are unpersuaded by Patent Owner’s contention that Petitioner’s proposed construction is too broad. PO Resp. 5.

Although we agree with Patent Owner that “distributed firewall” is “a known term of art,” and “firewall” may have “different nuances in different contexts,” the evidence of record does not support Patent Owner’s contention that the term “is far too well-defined to be confused with numerous other well-known data security techniques, like encryption.” *Id.* at 5–6. Further, the evidence of record does not support Patent Owner’s contention that “no POSITA would ever view email encryption as a ‘firewall’ that controls access to a user’s computer from the Internet,” wherein “[e]ncryption, rather, controls whether someone can read the email” but “encryption itself is not a firewall.” *Id.* (citing Ex. 2012 ¶¶ 58–60).

In the ’633 patent, claim 1 merely recites that a “distributed firewall” includes “first and second security managers respectively disposed in the first and second nodes,” wherein the first and second security managers are “respectively configured to control access to the first and second nodes from the communications interface.” Ex. 1001, 22:45–53. The plain language of

claim 1 does not support Patent Owner's contentions that "[a]lthough encryption can complement a firewall, encryption itself is not a firewall." PO Resp. 6; *compare* Ex. 1001, 22:45–53. Nothing in the Specification defines the term "firewall" to exclude controlling access with encryption, whether alone or with additional techniques.

By asserting that a "firewall" cannot encompass encryption itself, or that it cannot be defined to include security managers that control access through encryption alone, Patent Owner is advocating the narrowing of the claim beyond a construction in accordance with the ordinary and customary meaning as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. PO Resp. 6; *see* 37 C.F.R. § 42.100(b). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993). Our reviewing court "has repeatedly cautioned against limiting the claimed invention to preferred embodiments or specific examples in the specification." *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1346–47 (Fed. Cir. 2015). "[I]t is the claims, not the written description, which define the scope of the patent right." *Id.* at 1346. As such, we decline to narrow the claims as asserted by Patent Owner.

As Petitioner contends in its Reply, the '633 patent "expressly provides that '[a] distributed firewall is generally considered to be a collection of security managers that each control the access to their associated secured nodes from the interface.'" Pet. Reply 4–5 (citing Ex. 1001, code (57), 6:25–27, 3:52–56). We agree with Petitioner that "Petitioner's proposed construction requiring a collection of security managers that each control access to their associated nodes" is "in line with

the plain meaning and the '633 specification.” *Id.* (citing Ex. 1002 ¶¶ 85–87; Pet. 39).

As Petitioner points out, Patent Owner’s extrinsic evidence presented in its Response “post-date[s] the '633 patent’s filing date by more than a year, and thus [is] not even contemporaneous with the '633 patent.” Pet. Reply 5–6 (citing PO Resp. 5–6; *Phillips*, 415 F.3d at 1313 (“[T]he ordinary and customary meaning of a claim term is the meaning that the term would have to a [POSA] in question at the time of the invention, i.e., *as of the effective filing date of the patent application.*”)). Nevertheless, as Petitioner contends, under Patent Owner’s evidence, a “distributed firewall” is “a system that is spread out over a *plurality* of physical locations” and that “*prevents* computers in the...network from *communicating directly* with computers external to the network and vice versa.” *Id.* at 6. We agree with Petitioner that this definition “mirrors Petitioner’s construction that a distributed firewall is ‘a *collection* of security managers that each *control the access* to their associated nodes from the interface.’” *See id.* at 6–7 (citing Ex. 2012 ¶ 56–57 (quoting Ex. 2022 [Microsoft Dictionary])).

Furthermore, Patent Owner’s construction is not consistent with the understanding of an ordinarily skilled artisan. “The words of a claim are generally given their ordinary and customary meaning as understood by a person of ordinary skill in the art when read in the context of the specification and prosecution history.” *Thorner v. Sony Comput. Entm’t Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (emphasis added). As Petitioner points out, Patent Owner’s own expert “admitted on cross-examination that Petitioner’s construction is ‘not inconsistent’ with the plain meaning of ‘distributed firewall.’” Pet. Reply 7 (citing Ex. 1020, 63:6–18, 57:12–21). According to Petitioner, Patent Owner’s “extrinsic evidence supports the

argument that a ‘distributed firewall’ must act to control access to selected nodes on the system to ensure secure communications.” *Id.* at 8 (citing PO Resp. 6–7).

In its Sur-reply, Patent Owner adds that the “[t]he plain meaning of ‘distributed firewall’ requires a system that rejects data from a source that is not on the security manager’s authorization list” (PO Sur-reply 4), and that “the claim and specification make crystal clear that the controlling access *does* require use of the recited authorization list.” *Id.* at 5. However, by asserting that the distributed firewall requires the use of an authorization list (*id.*), Patent Owner is again advocating the narrowing of the claim beyond a construction in accordance with the ordinary and customary meaning as understood by one of ordinary skill in the art. As discussed above, we decline to narrow the claims beyond that in accordance with its ordinary and customary meaning. *See* 37 C.F.R. § 42.100(b); *Van Geuns*, 988 F.2d at 1184. As Petitioner contends, “the ’633 patent is clear that a distributed firewall is a collection of devices that each control access to their respective nodes,” but “does not necessarily require use of an authorization list to control that access,” as Patent Owner contends. Pet. Reply 8.

During oral argument, Patent Owner referred to the declaration testimony of Dr. Mangione-Smith that, in a distributed firewall model, each host device on the network is responsible for filtering traffic that it individually receives. Tr. 41:18–42:1 (citing Ex. 2012 ¶ 57). According to Patent Owner, a person of ordinary skill in the art would understand “a firewall prevents data from ever entering.” Tr. 43:19. However, such construction comports with Petitioner’s proposed construction. *See* Pet. 39; Ex. 1002 ¶ 85.

In view of the claim language, Specification, and evidence of record, we agree with Petitioner and interpret “distributed firewall” as “a collection of security managers that each control the access to their associated nodes from the interface.” Pet. 39.

2. *“first and second security managers respectively configured to control access to the first and second nodes from the communications interface” (claim 1)*

Before institution, Patent Owner argued that the term “control access” to a node in the phrase “first and second security managers respectively configured to control access to the first and second nodes from the communications interface” means “to restrict access to a secured portion of that node from the communications interface to only authorized nodes from the plurality of nodes.” Patent Owner’s Preliminary Response (“Prelim. Resp.”), Paper 9, 12; *see also id.* at 12–25. Petitioner argued that there is no need to construe the term “control access” and noted that Patent Owner “did not seek a construction for the term in at the District Court.” Pet. Reply to Patent Owner’s Preliminary Response, Paper 11, 5. Nevertheless, Petitioner contended that the plain and ordinary meaning of “control access” within the context of the claims “means to allow authorized nodes to have access, and not to allow unauthorized nodes to have access.” *Id.* at 6 (citing Ex. 1001, 7:27–31, 39–44).

In our Decision to Institute, based on the record at that time, we determined that the plain language of claim 1 does not state that “control access” is restricted to “only authorized nodes from the plurality of nodes,” as asserted by Patent Owner. Dec. Inst. 12 (citing Prelim. Resp. 24–25). Further, we determined that “the Specification does not state that the access

must be restricted to only authorized nodes of the plurality of nodes.” *Id.* at 12–13 (citing Ex. 1001).

Following institution, Patent Owner argues that claim 1’s limitation requiring the security managers to “control access to the ... nodes from the communications interface” requires “restricting access to the nodes to only authorized nodes.” PO Resp. 14–15; *see also id.* at 16 (stating that a “conclusion that claim 1 does not at least require restricting access to the first and second nodes to only authorized entities is untenable”). Patent Owner contends that this construction is compelled “both by lexicography and by independently sufficient disclaimer and disavowal of broader scope in the patent’s specification.” *Id.* at 15; *see also id.* at 22 (stating that a POSITA, “at a minimum, would have understood to ‘control access to the first and second nodes’ to mean to ‘restrict[] access to the first and second nodes to only authorized entities’”). Patent Owner contends that the ’633 patent “clearly evinces the inventors’ intent to define” controlling access to the node, “if not expressly, at least by implication, and also shows their intent to disclaim or disavow any scope of that term beyond restricting access to such nodes to only authorized nodes on the network.” *Id.* at 18. Patent Owner points to the “thereby clause” in the following paragraph of the ’633 patent as evidence that the patentee clearly and unmistakably evinces an intent to disavow or disclaim the full scope of the claim:

The ***invention*** addresses these and other problems associated with the prior art by utilizing in conjunction with a memory-mapped serial communications interface a distributed firewall to permit secure data transmission between selected nodes over the interface. The distributed firewall incorporates security managers in the selected nodes that are respectively configured to control access to their associated nodes, ***thereby restricting access to such nodes to only authorized nodes.***

Id. at 18 (quoting Ex. 1001, 3:48–56 (emphasis added by Patent Owner)).

Patent Owner further contends that, in the '633 patent's Specification, the phrases "control access" or "access control" appear multiple times, but "[n]one contradicts the teaching that controlling access refers to restricting access to a node to only authorized nodes." PO Resp. 19–20 (citing Ex. 1001, 1:17–20, 4:4–14, 7:19, 7:22–23, 10:2–5). Patent Owner contends that the Board's preliminary determination regarding the term "control access" in the Decision to Institute fails to address the Specification's use of the "thereby" clause "to link the phrases 'control access to their associated nodes' and 'restricting access to such nodes to only authorized entities.'" PO Resp. 21 (citing Ex. 1001, code (57), 3:52–56). In particular, according to Patent Owner, "the specification is '[r]eplete with references that indicate that the patentee was preeminently concerned with' restricting access to the nodes to only authorized entities." *Id.* (citing *Renishaw PLC v. Marposs Societa' Per Azioni*, 158 F.3d 1243, 1251 (Fed. Cir. 1998)). That is, "thereby" is a "signal" word, wherein "[s]ignal words also provide compelling evidence of an inventor's intent to accord a special meaning to a term." *Id.* at 17. According to Patent Owner, the "[s]ignal word 'thereby' also provides clear and unequivocal evidence of lexicography or at least a clear and unmistakable disavowal or disclaimer of scope," wherein "[w]ith the word 'thereby,' the specification signals that the act of controlling access to a node is intended to result necessarily in restricting access to that node to only authorized entities." *Id.* at 19 (citing *Nintendo of Am., Inc. v. iLife Techs.*, IPR2015-00112, Paper 39, 63 (PTAB Apr. 28, 2016) (defining "thereby" as "By that means; as a result of that")). Patent Owner also points to Petitioner's expert's cross-examination in which Dr. Kubiawicz agreed

that, “in the context of the ’633 patent, ‘thereby’ means ‘[a]nd as a result.’” *Id.* (citing Ex. 2015, 81:12–22).

We disagree with Patent Owner’s contention that “control access to the first and second nodes” should be narrowly construed to mean “restrict access to the first and second nodes to only authorized entities.” PO Resp. 22. We agree with Petitioner that, by arguing that controlling access refers to restricting access to a node to “only authorized nodes” (PO Resp. 19–20), Patent Owner is advocating the narrowing of the claim beyond a construction in accordance with the ordinary and customary meaning as understood by one of ordinary skill in the art in the context of the entire patent, including the specification. *See* Pet. Reply 10–15; *see also Phillips*, 415 F.3d at 1313; 37 C.F.R. § 42.100(b). As discussed above, we decline to narrow the claims beyond that in accordance with its ordinary and customary meaning. *See* 37 C.F.R. § 42.100(b); *Van Geuns*, 988 F.2d at 1184.

Further, although Patent Owner contends that “control access” in the must be determined based on the Specification’s use of the “thereby” clause “to link the phrases ‘control access to their associated nodes’ and ‘restricting access to such nodes to only authorized entities’” because “thereby” is a “signal” word that “provides clear and unequivocal evidence of lexicography or at least a clear and unmistakable disavowal or disclaimer of scope” (PO Resp. 19–21), we are not persuaded. Such construction would require improperly importing a limitation into the claim that is not specifically recited in the claim. That is, “thereby” appears nowhere in the claim language. Instead, as Patent Owner points out, the term appears in a passage *in the Specification* describing an embodiment. *See* Ex. 1001, code (57), 3:52–56. “Though understanding the claim language may be aided by explanations contained in the written description, it is important not to

import into a claim limitations that are not part of the claim.” *Superguide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004); *see also Liebel-Flarsheim Co. v. Medrad Inc.*, 358 F.3d 898, 906 (Fed. Cir. 2004).

We agree with Petitioner that “there was no such lexicography or disclaimer” that would limit construction of the disputed phrase to mean “restrict access to the first and second nodes to only authorized entities.” Pet. Reply 2. A patentee may act as a lexicographer by giving a term a particular meaning in the specification with “reasonable clarity, deliberateness, and precision.” *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). Where an inventor chooses to be his own lexicographer and to give terms uncommon meanings, he must set out his uncommon definition in some manner within the patent disclosure so as to give one of ordinary skill in the art notice of the change. *Id.* We disagree with Patent Owner’s argument that a “thereby clause” provides clear and unequivocal evidence of lexicography or a clear and unmistakable disavowal or disclaimer of scope. PO Resp. 19.

Rather, we are persuaded by Petitioner’s arguments that Patent Owner’s position “is actually contrary to the intrinsic evidence, which teaches ‘selective secured nodes’ that control access to their nodes **and** also communicate with unsecured nodes.” Pet. Reply 2 (citing PO Resp. 15, 22; Prelim. Resp. 24). As Petitioner points out, on cross-examination, Patent Owner’s own expert “directly contradicted [Patent Owner’s] argument and his own Declaration, stating that a [POSITA] would not have understood the ‘thereby’ clause to be a lexicographic definition of the claim term ‘control access to [a node].’” *Id.* at 11 (citing Ex. 1020, 81:5–17 (“Q ... [W]ould a [POSITA] have understood ‘thereby restricting access’ is a lexicographic

definition of the claim limitation control access? A *I wouldn't say that either. ...*”).

We agree with Petitioner that the '633 patent “does not anywhere define, either directly or by disclaimer, ‘control access to [associated nodes]’ to prohibit **all** communications with unauthorized nodes,” wherein, for lexicography to apply, “a patentee must ‘clearly set forth a definition of the disputed claim term’ other than its plain and ordinary meaning.” Pet. Reply 13 (citing *Thorner*, 669 F.3d at 1365 (quoting *CCS Fitness v. Brunswick*, 288 F.3d 1359, 1366 (Fed. Cir. 2002))). Instead, “the '633 patent explains that ‘selective secured’ nodes can control access by setting up secure and restricted channels of communications with some nodes,” but “also having **unsecure channels** for communications with unauthorized nodes.” *Id.* at 14 (citing Ex. 1001, 9:66–10:2). As Petitioner points out, even Patent Owner admitted and the '633 patent makes clear that “selectively-secured nodes ‘can communicate under local control with **all unsecured nodes**, as well as with **any secured or other selectively-secured nodes as authorized.**’” *Id.* (citing PO Resp. 16 (quoting Ex. 1001, 9:66–10:2)).

Therefore, for the foregoing reasons, based on the complete record, we determine that the phrase “control access to the first and second nodes” should not be narrowly construed to mean “restrict access to the first and second nodes to only authorized entities,” as Patent Owner proposes. PO Resp. 22.

3. “*first security manager . . . configured to locally generate for the first node an authorization list of authorized nodes*”
(claim 1)

Petitioner contends that the term “locally generate for the first node” should be construed to mean “generate in the first node.” Pet. 37 (Ex. 1002

¶ 80). According to Petitioner, the '633 patent discloses, for example, “a self-directed node which ‘has an *internal* mechanism for authorizing another node in the interface for secure communications [and through which] *authorization lists are generated* dynamically . . . by polling for acceptable nodes on the interface.’” *Id.* at 37–38 (citing Ex. 1001, 10:9–15; Ex. 1002 ¶ 81). We agree with such construction because it is consistent with the Specification.

Although Patent Owner contends that, during prosecution, it “addressed the ‘unique and unexpected advantage’” of the locally generated list in that, “[b]y generating an authorization list locally, greater autonomy and flexibility is realized, as a node is *not necessarily reliant on another entity to generate its authorization information*” (PO Resp. 48–49 (citing Ex. 1008, 9)), we are not persuaded that the term should be narrowed to include such “advantage.” We are unpersuaded by Patent Owner’s contention that the term should be narrowed because the '633 patent’s “self-directed node” is “not entirely reliant on another entity to generate its authorization information,” but rather, “decides whether to authorize a device based on the pre-installed certificates locally stored on it[s] self-directed node itself.” *Id.* at 50 (citing 1001, 14:44–45; Ex. 2012 ¶¶ 104–105).

Here, claim 1 merely requires that the first security manager is configured “to locally generate for the first node an authorization list of authorized nodes.” Ex. 1001, 22:50–53. Contrary to Patent Owner’s contentions (Prelim. Resp. 48–50), the plain language of claim 1 does not require that the generation of the list not be “reliant on another.” *Id.* In fact, as Petitioner points out, such construction proposed by Patent Owner “is contrary to the teachings of the '633 patent,” wherein “[the '633 patent’s]

interactive node generates an authorization list by ‘*asking an external source* whether or not located devices on the interface should be authorized for communication with the node.’” Pet. Reply 22 (citing Ex. 1001, 10:43–47).

Therefore, for the foregoing reasons, based on the present record, we determine that the phrase “locally generate for the first node an authorization list of authorized nodes” does not require a node to be “not entirely reliant on another entity to generate its authorization information.” PO Resp. 48–50.

4. *Remaining Terms*

Petitioner asserts that a “memory-mapped . . . interface” should be “construed, consistent with its plain meaning and in light of the ’633 patent” to mean “an interface that allocates a unified memory space to one or more of the nodes coupled to the interface, with each node having a portion of the memory space that is accessible by other nodes by referring to specific memory addresses within that allocated portion.” Pet. 34 (citing Ex. 1002 ¶ 70). Petitioner also asserts that the term “serial communications interface” should be “construed to mean ‘an interface that transmits and receives data between nodes bit-by-bit.’” *Id.* at 36 (citing Ex. 1002 ¶ 76). Patent Owner does not dispute Petitioner’s proposed claim constructions for these terms. *See generally* PO Resp.; PO Sur-reply.

Only terms that are in controversy need to be construed, and only to the extent necessary to resolve the controversy. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). In the Decision on Institution, we determined that it is unnecessary to construe any of these claim terms expressly to resolve the

disputed issues before us. Dec. Inst. 13–14. We discern no reason or evidence that compels any deviation from our earlier determination in this Final Written Decision.

C. Principles of Law

A claim is unpatentable under § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, so-called secondary considerations.⁵ *Graham*, 383 U.S. at 17–18.

D. Asserted Unpatentability of Claim 1 over Traw and Zou and of Claim 13 over Traw, Zou, and Segal

Petitioner contends that claim 1 would have been obvious under 35 U.S.C. § 103(a) over Traw in view of Zou and claim 13 would have been obvious under 35 U.S.C. § 103(a) over Traw and Zou in view of Segal. Pet. 40, 74. Petitioner explains how the proffered combinations purportedly teach the subject matter of the challenged claims, and asserts that a person of ordinary skill in the art would have had reason to combine the teachings. *Id.* at 40–81.

We begin our discussion with a brief summary of Traw and Zou.

⁵ The parties do not present arguments or evidence of such secondary considerations, and thus, secondary considerations do not constitute part of our analysis.

1. *Traw*

Traw, titled “Content Protection for Transmission Systems,” issued on September 7, 1999. *See* Ex. 1003, codes (54), (45). Traw discloses a method for “protecting digital content from copying and/or other misuse as it is transferred between devices over insecure links,” which includes “authenticating that both a content source and . . . sink are compliant devices,” “establishing a secure control channel between the content source and the content sink,” “establishing a secure content channel, providing content keys,” and “transferring content.” *Id.* at code (57). Traw recognizes need for a “mechanism to distribute digitized versions of . . . material in a manner that largely eliminates unauthorized copying.” *Id.* at 1:32–37.

Figure 3 of Traw is reproduced below.

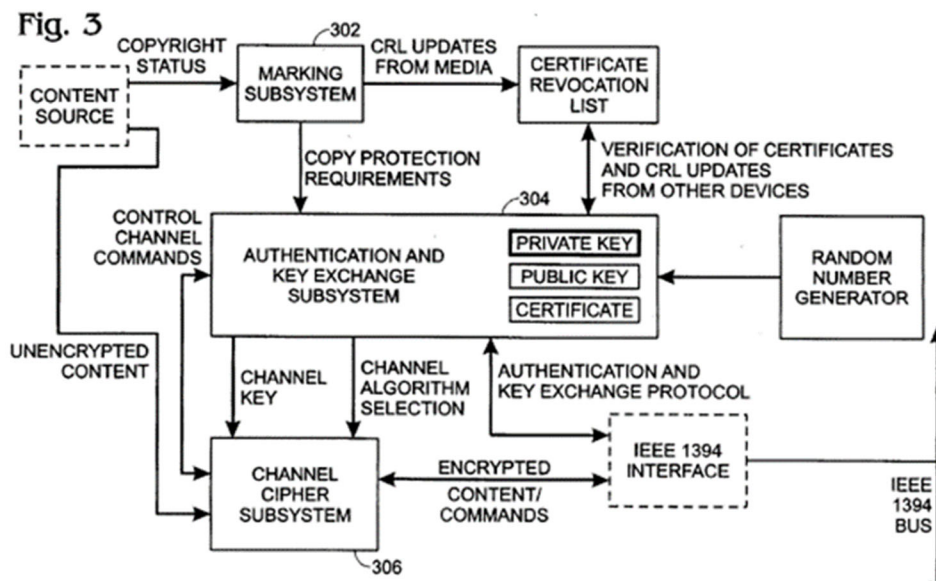


Figure 3 shows components of a source for protected content. *Id.* at 8:60–63. Figure 4 of Traw is reproduced below.

Fig. 4

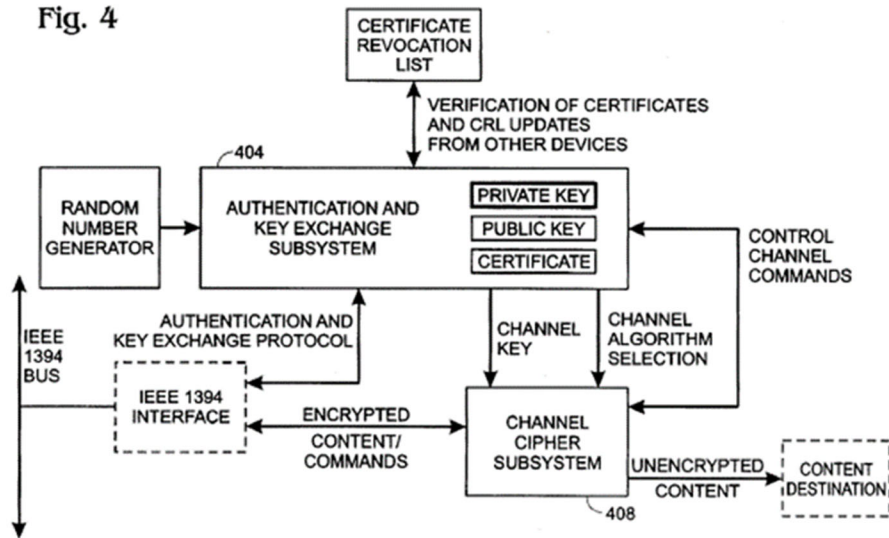


Figure 4 shows components for a receiver of protected content. *Id.* at 8:63–64. As shown in Figures 3 and 4, “subsystems in boxes with solid outlines are required for compliance,” wherein “[b]oxes with dashed outlines are subsystems which are common to compliant and non-compliant devices.” *Id.* at 8:64–67. “Authentication and Key Exchange 304, 404 is found in both Senders and Receivers of protected content,” and “is responsible for implementing protocols which are used to ensure that devices exchanging protected content are compliant.” *Id.* at 9:30–36. “The protocol is also used to select a channel encryption algorithm and exchange the control channel encryption key.” *Id.* at 9:36–38.

A compliant device that transmits protected content includes “Channel Encryption Subsystem 306” that encrypts control messages as well as protected content prior to transmission, wherein “keys used to encrypt the content and commands are passed to Channel Encryption Subsystem 306 from Authentication and Key Exchange Subsystem 304.” *Id.* at 9:58–65. A compliant device that receives protected content includes “Channel Decryption Subsystem 408” that “decrypts control messages and protected

content which are received from the serial bus,” wherein “[t]he keys used to decrypt the content and commands are passed to Channel Decryption Subsystem 408 from Authentication and Key Exchange Subsystem 404.” *Id.* at 10:7–13.

In various embodiments, “cryptographic technologies” are used “for protecting content being exchanged across communication links such as an IEEE 1394 bus,” wherein these communication links are used “to connect [consumer electronic] CE devices and [personal computers] PCs based multimedia applications.” *Id.* at 3:25–30. “Each compliant device contains a digital certificate which has been digitally signed . . . to certify that the device is compliant.” *Id.* at 3:35–37. The compliant device also contains “a list in non-volatile memory of devices whose compliance has been revoked,” wherein this “Certificate Revocation List (CRL)” can be “updated from other compliant devices” and can be “used to revoke the certificates of devices whose security has been compromised.” *Id.* at 3:38–43.

The operation of the content protection system includes: “creation of a License Authority, manufacture of compliant systems and media, system authentication and control channel key exchange, and protected content channel encryption.” *Id.* at 4:62–67. The License Authority is responsible for the creation of the CRL “composed of . . . a list (CRLD) of devices IDs whose compliance with the conditions of the license have been violated and detected by the License Authority.” *Id.* at 5:37–41. Compliant systems generate during manufacture a “public/private key pair (X^1 , X^{-1})” using key generation mechanism. *Id.* at 5:55–57.

“[W]hen a compliant device is added to a communication link such as an IEEE 1394 serial bus, a cryptographic protocol is used to authenticate . . . devices on the bus and establish control channels between them.” *Id.* at

6:60–65. For example, “compliant device (‘Device A’) which is a source of protected content (e.g., a DVD player) is attached to a serial bus which already has another compliant device (‘Device B’) which is a sink for protected content (e.g. a PC . . .) attached to it.” *Id.* at 6:65–7:3. “As soon as Device A has been initialized, it attempts to authenticate other devices attached to the serial bus to determine which are compliant.” *Id.* at 7:5–7. In this case, “Device A performs the protocol with Device B” by transmitting a signed message to Device B which contains “Device A’s certificate (A_{Cert})” and “Device A’s CRL version number (A_{CRLV}).” *Id.* at 7:7–13. When Device B receives the message, it checks the signature “to verify that the message has not been tampered with,” wherein “[i]f the signature is valid, . . . Device B checks to see if [Device A’s ID] A_{ID} (in A_{Cert}) has been revoked by searching its CRL (B_{CRLD}).” *Id.* at 7:14–29. “If A_{ID} is on the list, then Device B considers Device A non-compliant” and “refuses to continue.” *Id.* at 7:29–31. “If no errors have occurred up to this point, the two devices have authenticated each other.” *Id.* at 8:18–19. Accordingly, “non-compliant devices are unable to transmit or receive protected content.” *Id.* at 11:52–54.

2. Zou

Zou, titled “Method and System for Updating Device Identification and Status Information After a Local Bus Reset Within a Home Audio/Video Network,” issued on December 12, 2000. *See* Ex. 1004, codes (54), (45).

Zou “provides a mechanism whereby devices of the network are informed of the current status of the network after a local bus reset caused when a device is inserted into the network or when a device is removed from the network.” *Id.* at code (57). After a reset, “a new [Global Unique

Identification] GUID list is generated by a driver and passed to a high level program.” *Id.* “The high level program then compares the new GUID list with its own copy of an older version and generates a list of devices added to the network after the bus reset and a list of devices removed from the network after the bus reset.” *Id.* “This information is then forwarded to all devices on the network that previously specified certain call back information regarding current device status.” *Id.* at 3:18–28. Thus, Zou provides a mechanism for “maintaining a list of recently added or removed devices.” *Id.* at 3:48–52.

Figure 8 shows communication pathways between an application, a device control module (DCM), the communications media manager (CMM) and a link driver (*id.* at 4:20–22), and is reproduced below.

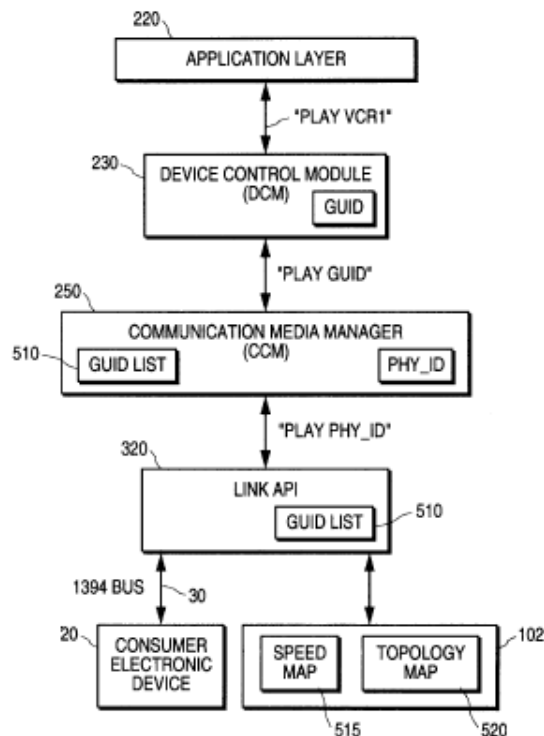


FIG.8

Figure 8 shows a home audio/visual initiative (HAVI) communication architecture which includes “application layer 220,” “device control module 230” for particular “device 20,” “CMM 250,” “link driver layer 320,” “electronic device 20” coupled to “IEEE 1394 communication bus 30,” “speed map 515” data structure, and “topology map 520” data structure. *Id.* at 22:10–15. In Zou, “application layer 220” references devices using multi-bit persistent GUIDs assigned to each device. *Id.* at 22:19–24. “CMM 250 contains a GUID list 510” that “is a listing of GUIDs in order of their associated physical identifications” and “is updated by the link driver 320 each time a bus reset event is detected.” *Id.* at 22:37–45.

Figure 12A shows a “general GUID update status list” (*id.* at 4:39–42), and is reproduced below.

632		634	
GUID VALUE		STATUS	
632a	GUID (Y)	REMAINED	634a
632b	GUID (U)	ADDED	634b
632c	GUID (X)	REMAINED	634c
632d	GUID (Z)	REMAINED	634d
632e	GUID (J)	REMAINED	634e
632f	GUID (N)	ADDED	634f
632g	GUID (I)	REMOVED	634g

FIG. 12A

Figure 12A shows a “GUID status stable” generated by a communications media manager (CMM) each time a local bus reset is generated. *Id.* at 24:15–17. The GUID status table includes “entries 632a–632g” regarding: “(1) which devices remain connected to the local bus 30 since the last GUID list 510 was compiled, e.g., after a local bus reset,” “(2) which devices have been just removed,” and “(3) which devices have

been just added since the last GUID list 510 was compiled.” *Id.* at 24:17–22.

Figures 12B–C respectively show “an ‘added’ GUID update status list” and “a ‘removed’ GUID update status list” (*id.* at 4:43–51), and are reproduced below.

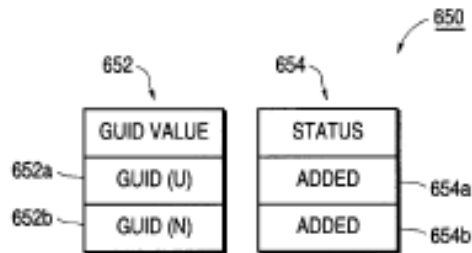


FIG.12B

Figure 12B above shows “subset status table 650” generated by the CMM which contains “entries 652a–652b indicating only which devices have been added to the local bus 30 since the last GUID list 510 was compiled.” *Id.* at 24:36–39.

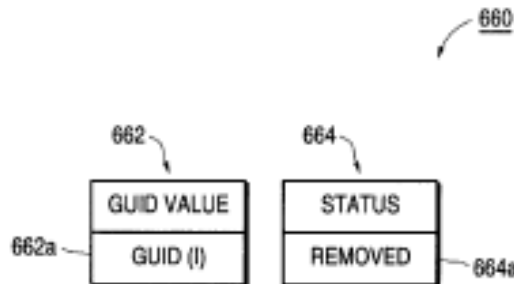


FIG.12C

Figure 12C above shows “subset status table 600” generated by the CMM which contains “entries (662a) indicating only which devices have been removed from the local bus 30 since the last GUID list 510 was compiled.” *Id.* at 24:39–43.

3. *Analysis of Claim 1*

(a) *“A data processing system” (Preamble)*

Petitioner contends that the combination of Traw and Zou teaches or suggests the features recited in the preamble of claim 1. Pet. 40–43. In particular, Petitioner contends “Traw teaches a content protection system that allows devices to ‘securely . . . transfer[] protected content . . . over otherwise insecure communication links.’ The devices transferring the protected content include ‘computers [and] other digital consumer electronic (CE) devices’ that can produce and play the protected multimedia content.” Pet. 40 (citation omitted) (quoting Ex. 1003, 3:21–24, 1:12–22). According to Petitioner, “[b]ecause Traw discloses a content protection system with interconnected devices that are capable of transferring and processing protected media content, Traw teaches a ‘data processing system.’” *Id.* at 41 (citing Ex. 1002 ¶¶ 119–120).

Further, Petitioner contends that “Zou discloses a ‘home audio/video network’ . . . within which ‘several consumer electronics products . . . can be coupled to communicate together via a standard bus (e.g., IEEE 1394 serial communication bus).” *Id.* at 42 (citing Ex. 1004, 2:60–65, code (57); Ex. 1002 ¶ 121). According to Petitioner, “Zou further discloses that ‘any device (having appropriate capabilities) . . . can send or receive communication packets from any other device in the . . . network,’ and that “the devices can process the communication packets to determine the current status of device on the . . . network.” *Id.* at 42–43 (citing Ex. 1004, Fig. 1B, 6:31–33, 6:21–24, 4:52–5:8, Figs. 13–15E). Thus, Petitioner contends “[b]ecause Zou discloses interconnected devices that can transfer and process data, Zou teaches a ‘data processing system.’” *Id.* at 43 (citing Ex. 1002 ¶¶ 122–124).

Patent Owner does not dispute Petitioner's contentions. *See generally* PO Resp.; PO Sur-reply. We agree with Petitioner's analysis and find that Traw and Zou teach a "data processing system" recited in claim 1 for the reasons explained by Petitioner.⁶

(b) "a plurality of nodes including at least first and second nodes"

Petitioner contends that "Traw teaches 'a plurality of nodes including at least first and second nodes' by disclosing '**devices** [with multiple components communicating] over insecure links,' 'such as an IEEE 1394 bus.'" Pet. 43 (quoting Ex. 1003, 1:42–44, 3:25–28). In particular, Petitioner contends that "Traw repeatedly refers to devices (including 'Device A' and 'Device B') coupled to the IEEE 1394 serial bus, such as a DVD player or PC computer, and each of those devices includes a node." *Id.* at 42–43 (citing Ex. 1003, 6:61–7:3, Figs. 3–4).

Further, according to Petitioner, "as shown in Figure 1, Zou discloses 'several consumer electronics products . . . [that] can be coupled to communicate together via a standard bus (e.g., IEEE 1394 serial communication bus),' including, for example, 'personal computers (PCs), [and] digital video disk players (DVDs) etc.'" *Id.* at 46 (citing Ex. 1004, 2:61–65, 6:9–24; 6:26–29; Ex. 1002 ¶ 128). Moreover, Petitioner contends that "each of Zou's devices includes additional components that are also interfaced to the IEEE 1394 bus." *Id.*

Patent Owner does not dispute Petitioner's contentions. *See generally* PO Resp. We agree with Petitioner's analysis and find that Traw and Zou

⁶ Because we determine Petitioner has sufficiently shown the cited art teaches the subject matter recited in the preamble, we need not determine whether the preamble is limiting.

teach “a plurality of nodes including at least first and second nodes” recited in claim 1 for the reasons explained by Petitioner.

(c) *“a memory-mapped serial communications interface coupled between the plurality of nodes and supporting peer-to-peer communication therebetween”*

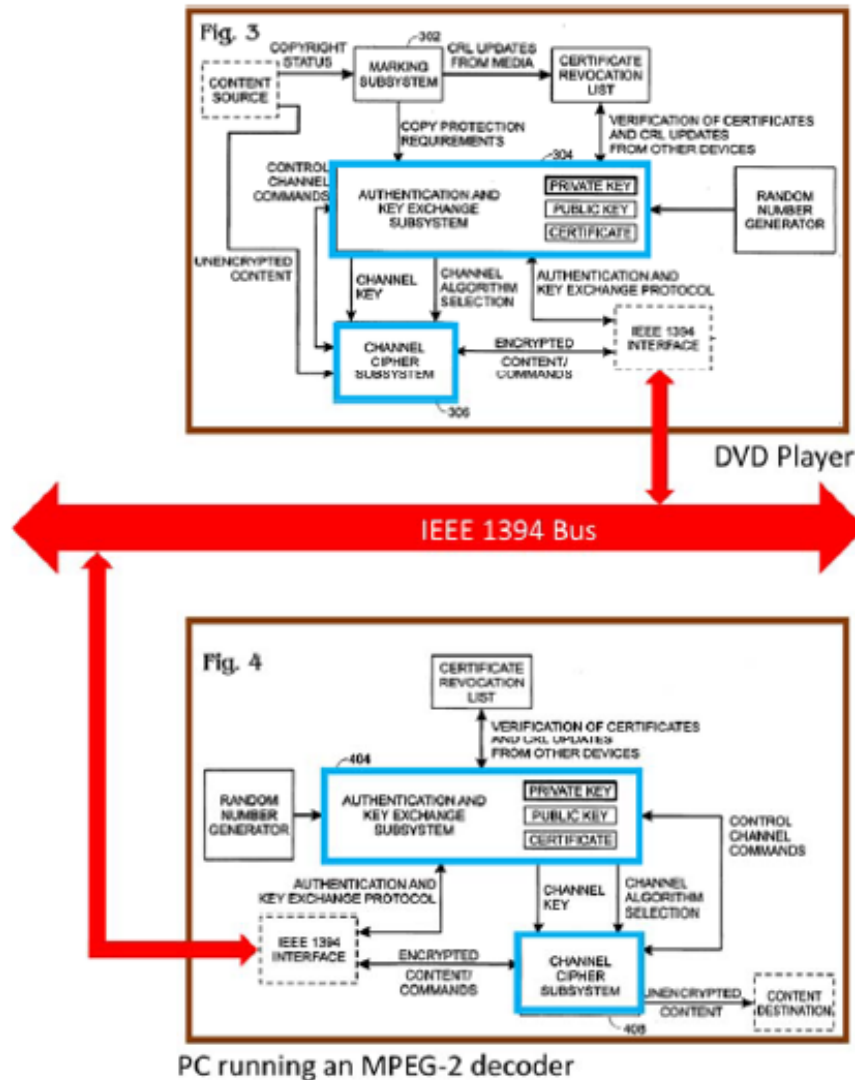
Petitioner contends that “Traw and Zou each disclose use of an IEEE 1394 interface, which the ’633 patent admits is ‘one example of a “memory-mapped serial communications interface.”’” Pet. 48 (citing Ex. 1001, 2:29–37, 6:52–54, 12:3–7, 19:2–4; Ex. 1003, 3:25–28, 6:61–65; Ex. 1004, code (57), 6:16–21; Ex. 1002 ¶¶ 131–132, 134). Further, Petitioner contends “both Traw and Zou also disclose that the IEEE 1394 interface is ‘coupled between the plurality of nodes.’” *Id.* at 48–49 (citing Ex. 1003, 1:42–44, 1:66–2:2, 3:25–28, 6:61–7:4, Figs. 3–4; Ex. 1002 ¶¶ 133, 135; Ex. 1004, code (57), 6:16–21, Figs. 1B, 2). Petitioner then contends that “Traw and Zou both expressly disclose using the IEEE 1394 serial bus for peer-to-peer communication.” Pet. 52 (citing Ex. 1003, 3:64; Ex. 1004, 6:29–30; Ex. 1002 ¶¶ 136–138).

Patent Owner does not dispute Petitioner’s contentions. *See generally* PO Resp. We agree with Petitioner’s analysis and find that Traw and Zou teach “a memory-mapped serial communications interface coupled between the plurality of nodes and supporting peer-to-peer communication therebetween” recited in claim 1 for the reasons explained by Petitioner.

(d) *“a distributed firewall including first and second security managers respectively disposed in the first and second nodes, the first and second security managers respectively configured to control access to the first and second nodes from the communications interface”*

Petitioner asserts that Traw discloses “both a key exchange engine and an encryption engine disposed in respective nodes,” and thus, “discloses the

claimed security managers.” Pet. 53 (citing Ex. 1002 ¶ 139). According to Petitioner, “Figures 3 and 4 in Traw (reproduced below, as annotated) illustrate a block diagram of components of source and sink compliant devices that allow transmission and receipt of secure content, respectively.” *Id.*



Pet. 53–54 (citing Ex. 1003, 1:66–2:2, 6:65–7:4, Figs. 3–4). Annotated Figures 3–4 from the Petition show Traw’s source and sink devices indicated by brown boxes, each including an authentication and key exchange

subsystem and a channel cipher subsystem indicated by blue boxes, interconnected via an IEEE 1394 bus indicated by red arrows.

Petitioner contends that, in Traw, “[t]he source and sink devices, which include the claimed ‘first and second nodes,’ communicate with each other via the IEEE 1394 interface,” wherein, “[w]ithin each of the nodes are two components that collectively function as the ’633 patent’s ‘security manager:’ (1) Authentication and Key Exchange (AKE) subsystem 304, 404 . . . ; and (2) Channel Cipher (CC) Subsystem 306, 408.” Pet. 54–55 (citing Ex. 1003, 6:57–8:28, 8:30–57; Ex. 1002 ¶ 140). In particular, Petitioner contends that “Traw’s AKE subsystem is responsible for authenticating compliant devices and exchanging keys for secure communication, which is just like the key exchange engine in a security manager of the ’633 patent.” *Id.* at 55 (citing Ex. 1002 ¶ 141, *comparing* Ex. 1003, 9:33–38, 9:62–65, 10:10–12, 3:34–37, *with* 1001, 7:27–34). Moreover, Petitioner contends that “Traw’s CC subsystem is responsible for encrypting protected content, which is just like the ‘encryption engine’ within the ‘security manager’ of the ’633 patent.” *Id.* at 56 (citing Ex. 1002 ¶ 142; *comparing* Ex. 1003, 9:59–62, 10:8–10, *with* Ex. 1001, 7:52–54, claim 6). According to Petitioner, in Traw, “together, the AKE subsystem 304, 404 and the CC subsystem 306, 408 disposed in two nodes (*e.g.*, within the source device and the sink device) demonstrate the claimed first and second security managers,” wherein “Traw discloses both authorization (using the AKE subsystem) and encryption (using the CC subsystem) techniques that are used to control access to the first and second nodes.” *Id.* at 57 (citing Ex. 1002 ¶¶ 143–146; Ex. 1003, 1:44–48).

Petitioner contends that, “like the ’633 patent, Traw teaches using digital signature and certification techniques to authenticate compliant

devices (*i.e.*, devices authorized for secure content transfer),” wherein Traw uses “the same Diffie-Hellman key exchange protocol used in the ’633 patent to perform key exchanges,” and an “encryption technique used in the CC subsystem of Traw is the same ‘DES’ encryption algorithm taught in the ’633 patent.” Pet 58–61 (citing Ex. 1002 ¶¶ 147–156, *comparing* Ex. 1003, 2:66–67, 3:34–37, 3:45–47, 6:57–8:29, 8:32–41, 9:30–39, 9:59–65, 10:7–9, 10:11–13, *with* Ex. 1001, 7:27–49, 11:45–54).

Accordingly, Petitioner asserts that, since the proper construction for “distributed firewall” is “a collection of security managers that each control the access to their associated nodes,” and Traw discloses AKE and CC subsystems as “security managers that each control access to their associated [secured] nodes from the interface,” Traw discloses the claimed “distributed firewall.” Pet. 61 (citing Ex. 1002 ¶ 156).

Patent Owner responds that, in the ’633 patent, “the inventive distributed firewall controls access to the receiving node *irrespective of whether the incoming data is encrypted*” (PO Resp. 8 (citing Ex. 2012 ¶ 74)), whereas “Traw’s system does not work this way,” and thus, Traw “has no distributed firewall.” *Id.* at 9 (Ex. 2012 ¶¶ 68–69, 75–78). In particular, Patent Owner contends that, different from Traw, the ’633 patent “describes an innovative distributed firewall for protecting secured nodes, some of which may be ‘secured-only’ nodes and some of which may be ‘selectively-secured nodes.’” *Id.* at 6 (citing Ex. 1001, Figs. 12, 17). According to Patent Owner, when a packet arrives at any secured node in the ’633 patent, the security manager will first query whether the source node is on the receiving node’s authorization list, wherein “if the source node is not on the authorization list, no secure communications are permitted therewith.” *Id.* at 7–8 (citing Ex. 1001, 15:65–16:53, 21:60–62). That is,

according to Patent Owner, “[r]egardless of whether the data is encrypted (secured), if the source node is not on the authorization list, no access is allowed.” *Id.* at 8.

We are not persuaded by Patent Owner’s contentions because these contentions are based upon a claim construction that we do not adopt. As stated above in Section II.B.1, we will not narrow the term “distributed firewall” to exclude security managers that control access to the various nodes through encryption. Thus, although Patent Owner contends that Traw differs from the ’633 patent because, in the ’633 patent, “encryption does not control access to the node” (PO Resp. 8 (citing Ex. 2012 ¶ 74)), and the patent “never suggests . . . encryption *alone suffices* to control access to a given node” as in Traw (*id.* at 11–12 (emphasis added)), nothing in the claims, even in view of the Specification, precludes applying encryption for access control, whether alone or in combination with other techniques. *See* Ex. 1001, 22:39–53 (“claim 1”).

We note that Patent Owner acknowledges that there are embodiments in the ’633 patent that are used in conjunction with encryption, even if Patent Owner contends that “such encryption is optional.” PO Resp. 6. Patent Owner similarly acknowledges that, in Traw’s system, some data is encrypted, even if Patent Owner contends “nothing, including the encrypted data, is ever corrupted, disregarded, or otherwise rejected.” *Id.* at 9. Here, Patent Owner points out that the specification of the ’633 patent discloses, “in selected embodiments of the invention, *encryption transmissions* may be supported *to restrict unauthorized viewing* of data transmitted between the selected nodes over the interface.” *Id.* at 11–12 (citing Ex. 1001, 3:56–59, 1:17–20; Ex. 2012 ¶¶ 60–62) (emphasis added).

Given our construction for the term “security managers respectively configured to control access” in Section II.B.2 above, we also are unpersuaded by Patent Owner’s contention that “there is no mechanism in Traw to control access to the sink.” PO Resp. 11 (citing Ex. 2012 ¶ 81). That is, we are unpersuaded by Patent Owner’s contention that “Traw/Zou does not teach any first security manager configured to control access to a first node” because “Traw/Zou does not restrict access to the alleged first node to only authorized entities.” PO Resp. 15. As discussed in Section II.B.2 above, we will not narrowly construe the claim to “restrict access to the first and second nodes to only authorized entities,” as Patent Owner proposes. Nevertheless, as discussed above in Section II.B.2, as Petitioner points out, even Patent Owner “admitted” and the ’633 patent “makes clear” that, like Traw’s system, “selectively-secured nodes ‘can communicate under local control with *all unsecured nodes*, as well as with *any secured or other selectively-secured nodes as authorized.*’” Pet. Reply 14 (citing PO Resp. 16 (quoting Ex. 1001, 9:66–10:2)).

Patent Owner also contends that “[t]he POSITA would have recognized Traw’s system is nothing less than Petitioner Intel’s own Digital Transport Copy Protection (‘DTCP’) protocol.” PO Resp. 30–31 (citing Ex. 2012 ¶¶ 41–43). According to Patent Owner, “a witness testified on behalf of Petitioner before Congress that DTCP *only* affected protected content and did not affect communication of unprotected content.” *Id.* at 33 (citing Ex. 2020, 42). Similarly, Patent Owner contends that the commercial embodiment of the “License Authority” described in Traw “represented to the Federal Communication Commission (FCC) that ‘DTCP is *not intended to protect information that should otherwise be transmitted between devices in the clear,*’” and thus, “content delivered to the consumer in-the-

clear ***would not be protected by DTCP.***” *Id.* at 35 (citing Ex. 2021, 5, n.8; Ex. 2017, 3). Accordingly, Patent Owner contends that “Petitioner’s testimony to Congress, and the Licensing Authority’s statements to the FCC, confirm the POSITA would have understood Traw to teach that it does not restrict non-compliant sources from communicating with a sink or transmitting unprotected content,” because “the AKE and CC subsystems of Fig. 4 play[] no role in that process.” *Id.* at 41. During oral argument, Patent Owner added that a “firewall” cannot encompass DTCP technology, since it does not prevent data from entering. Tr. 44:1–45:8.

We are unpersuaded by Patent Owner’s contentions that a “firewall” cannot encompass DTCP technology because they are also based upon a construction that would require improperly importing a limitation into the claim that is not specifically recited in the claim. As stated above in Section II.B.1, we construe “distributed firewall” as “a collection of security managers that each control the access to their associated nodes from the interface.” That is, the plain language of claim 1 does not preclude the “firewall” in a DTCP system as long as the system comprises security managers controlling access to the associated nodes.

We are persuaded by Petitioner’s contention that Traw discloses “authorization (using the AKE subsystem) and encryption (using the CC subsystem) techniques that are used to control access to the first and second nodes.” Pet. 57–58 (citing Ex. 1002 ¶¶ 144–146; Ex. 1003, 1:44–48). In particular, in an exemplary embodiment, Traw discloses establishing control channels between devices on an IEEE 1394 serial bus (Ex. 1003, 6:60–65), with the devices authenticating one another (Ex. 1003, 8:18–19), wherein one device determines if the other is “non-compliant.” *Id.* at 7:29–31. *See also id.* at 6:65–7:29. In such case, “non-compliant devices are unable to

transmit or receive protected content.” *Id.* at 11:52–54. In this embodiment, according to Petitioner, “Traw describes two types of devices, compliant device capable of securely transferring protected content and non-compliant devices that are unable to transfer or receive protected content,” wherein “non-compliant devices are unable to transmit or receive protected content.” Tr. 10:10–16.

Accordingly, we are persuaded by Petitioner’s contention that claim 1’s “distributed firewall including first and second security managers” encompasses Traw’s AKE and CC subsystems respectively disposed in the source and sink devices, respectively configured to control access to the source and sink devices from an interface. Pet. 61. That is, in Traw, each device communicating via the IEEE-1394 bus includes therein AKE and CC subsystems for determining whether a source device is non-compliant, wherein, as Petitioner contends, “Traw controls access to the associated compliant device by establishing secure channels only with other compliant devices (through authentication and key exchange) and exchanging protected content only via the secure channels.” Pet. Reply 16; *see also* Ex. 1003, 6:60–7:31.

Given our construction for the term “security managers respectively configured to control access” in Section II.B.2 above, we are persuaded by Petitioner’s contention that Traw discloses “control access” by “the compliant device determin[ing] whether or not to establish a secure channel.” Pet. Reply 17. Although Patent Owner contends that Traw does not control access because “‘protected content’ is designated as ‘protected’ *before* it enters Traw’s system” rather than “designated as ‘protected’ by Traw itself” (PO Resp. 24 (citing Ex. 1003, 3:41, 6:48, 9:15)), as Petitioner points out, Patent Owner’s own expert acknowledges, that similarly in the

'633 patent, “the secure data exchange mode is executed *after* the authorization mode and the key exchange mode.” Pet. Reply 19 (citing Ex. 1020, 146:5–8). According to Petitioner, “Traw’s authentication mode—during which other compliant devices are identified for secure communication—corresponds to the '633 patent’s authorization mode.” *Id.* at 20 (citing Ex. 1002 ¶¶ 97, 147–148, 155). That is, “[j]ust like the '633 patent, Traw is directed to providing secure communications between the two nodes that are connected to an otherwise unsecure communication interface.” Tr. 9:25–10:1.

Based on the complete record presented, we agree with Petitioner’s analysis and find that the combination of Traw in view of Zou teaches “a distributed firewall including first and second security managers respectively disposed in the first and second nodes, the first and second security managers respectively configured to control access to the first and second nodes from the communications interface.”

(e) “the first security manager is configured to locally generate for the first node an authorization list of authorized nodes with which communication is authorized for the first node”

Petitioner contends that “Traw teaches generating within a node all the information populated in the authorization list: (1) the identification of other authenticated devices (corresponding to ‘GUID 144’) and (2) the public keys that uniquely identify authenticated devices (corresponding to ‘public key 146’).” Pet. 62–63 (citing Ex. 1002 ¶¶ 158–159). Petitioner then contends “Zou adds the very simple teaching that such information taught to be locally generated by Traw, can be maintained in a list format.” *Id.* at 63. In particular, according to Petitioner, “Traw teaches that its authentication process involves (1) receiving from another device its

certificate, and (2) validating the received certificate to confirm that it is indeed compliant,” wherein the certificate includes “among other things, ***‘the unique device ID (X_{ID})’ of the device*** that owns the certificate.” *Id.* at 63 (citing Ex. 1003, 3:34–36, 6:26–27). Further, according to Petitioner, “[i]n addition to the ‘unique device ID (X_{ID})’, the certificate also includes the device’s ‘public key X¹.’” *Id.* at 64 (citing Ex. 1003, 6:26–31, 7:14–18).

Although “Traw does not explicitly state that the locally generated information is maintained using a list format,” Petitioner contends that “utilizing a list to keep track of desired information was well-known in the art, such as found in both Traw itself (for other data items) and Zou.” *Id.* at 68 (citing 1002 ¶ 171). In particular, Petitioner contends that “Traw teaches utilizing a list called a Certificate Revocation List (or CRL) for revoking certificates assigned to devices that are no longer compliant.” *Id.* (citing Ex 1003, 3:39–44). Thus, according to Petitioner, “Traw teaches using a list to maintain device IDs.” *Id.* (citing Ex. 1002 ¶ 172). Petitioner further contends that “Zou also teaches the simple concept of utilizing a list to maintain the identities of specific devices on an IEEE 1394 interface,” such as, for example, a “GUID list” of “globally unique identifiers” of “those IEEE 1394 devices.” *Id.* at 68–69 (citing Ex. 1004, 3:32–35, Fig. 11A; Ex. 1002 ¶ 173).

According to Petitioner, such a combination “would have been a routine modification using known techniques to achieve a predictable outcome.” *Id.* at 70 (citing Ex. 1002 ¶ 174). Petitioner contends that “[t]he system disclosed in Zou would have been a natural candidate for combination with Traw because just like Traw, Zou ‘relates to equipment for home audio/video electronics’ in which ‘several consumer electronics products . . . can be coupled to communicate together via a standard bus

(e.g., IEEE 1394 serial communication bus).” *Id.* at 72 (citing Ex. 1004, 1:11–12, 2:61–65; Ex. 1002 ¶ 177). Further, Petitioner contends “Traw teaches that ‘new devices/applications’ may be added to its system,” and Zou provides “support for ‘hot plugging’ and ‘unplugging,’ including management of device identification and topology,” wherein “a skilled artisan implementing Traw would have been motivated to combine Traw with a reference [such as Zou] that discloses how the ‘new devices/applications’ could be handled.” *Id.* at 73 (citing Ex. 1003, 4:6–11; Ex. 1004, 12:1–4, 15:45–16:12; Ex. 1002 ¶ 178).

In response, Patent Owner contends that “Traw’s sink has no need for any authorization list” because “all devices can and will communicate with all other devices in Traw,” and thus, “ordinary artisans would have understood that any list generated with Traw/Zou is not an authorization list *of authorized nodes with which communication is authorized for the first node.*” PO. Resp. 46–47 (citing Ex. 2012 ¶¶ 96–99). Patent Owner contends that, “[d]uring authentication in Traw, one device (the device being initialized) receives a certificate from another device,” but “the initializing device does not check that received certificate against a locally stored certificate or any other locally stored information.” *Id.* at 51 (citing Ex. 1003, 7:5–27; Ex. 2012 ¶¶ 106–107). That is, “any ‘list’ in Traw/Zou is not locally generated.” *Id.* According to Patent Owner, instead, “the Traw/Zou system necessarily requires an initializing node to rely on other entities, namely, other nodes and the License Authority, to generate the lists.” *Id.* at 51–52 (citing Ex. 1003, 7:27–31, 5:37–38; Ex. 2012 ¶¶ 108–109).

Patent Owner’s contentions do not undermine Petitioner’s showing. As a preliminary matter, we note that by arguing that a “list” is not “locally generated” when the system “necessarily requires an initializing node to rely

on other entities . . . to generate the lists” (PO Resp. 51–52), Patent Owner is proposing a construction that would require improperly importing a limitation into the claim that is not specifically recited in the claim. As discussed above in Section II.B.3, we will not adopt Patent Owner’s proposed construction of “locally generate for the first node an authorization list of authorized nodes” as requiring “not entirely reliant on another entity to generate its authorization information.”

We are persuaded by Petitioner’s contention that “to verify the other device’s certificate, Traw/Zou’s device uses the public key of the license authority that is *locally stored in the Traw/Zou’s device*.” Pet. Reply 24 (citing Ex. 1001, 5:34–36). That is, Petitioner contends that “Traw teaches using a list to maintain device IDs” (Pet. 68 (citing Ex. 1002 ¶ 172)), and that “Zou also teaches the simple concept of utilizing a list to maintain the identities of specific devices on an IEEE 1394 interface.” *Id.* at 68–69 (citing Ex. 1004, 3:32–35, Fig. 11A; Ex. 1002 ¶ 173).

Although Patent Owner contends that “all devices can and will communicate with all other devices in Traw” (PO. Resp. 46–47 (citing Ex. 2012 ¶¶ 96–98)), we agree with Petitioner that “Traw’s compliant device operates just like the ’633 selective secured nodes that are indisputably covered by the claims of the ’633 patent,” wherein “like the selective secured nodes of the ’633 patent, Traw’s compliant devices communicate with other authorized nodes over a secure channel, but also are able to communicate with other noncompliant devices over unsecured channels.” Pet. Reply 25. As Petitioner contends, “it does not matter that compliant devices in Traw can also communicate with noncompliant devices” (*id.*), because “Traw discloses generating in a node the information that is populated in the ’633 authorization list: the identities of the authorized

nodes.” Pet 64 (citing Ex. 1002 ¶ 162). Thus, we find that an ordinary artisan would have understood that a list generated by the Traw-Zou combination is “an authorization list of authorized nodes with which communication is authorized for the first node” as claimed.

Here, as Petitioner points out and as shown in Figures 3 and 4 of Traw, Traw creates a “CRL” for each node (i.e., source or sink) “composed of . . . a list (CRLD) of devices IDS whose compliance with the conditions of the license have been violated.” See Ex. 1003, 5:37–41, Figs. 3–4. That is, Traw teaches generating, for a node, a list of nodes with which communication is *not* authorized for the node. *Id.* Thus, in Traw, to determine the nodes that are in compliance, and thus *are authorized* for communication with the node, the CRL list is used to determine the nodes that are *not* on the list. *Id.* Petitioner then contends that, Zou, on the other hand, teaches “the simple concept of utilizing a list to maintain the identities of specific devices on an IEEE 1394 interface.” Pet. 68–69 (citing Ex. 1004, 3:32–35, Fig. 11A; Ex. 1002 ¶ 173).

We agree with Petitioner’s analysis and find that Traw in combination with Zou teaches that “the first security manager is configured to locally generate for the first node an authorization list of authorized nodes with which communication is authorized for the first node,” for the reasons explained by Petitioner.

(f) Conclusion regarding claim 1

For the foregoing reasons, we agree with Petitioner’s analysis and find that the combination of Traw and Zou renders obvious claim 1.

4. Analysis of Claim 13

Petitioner contends the limitations of dependent claim 13 would have been obvious over the combination of Traw and Zou in view of Segal, and

provides explanations and supporting evidence to support its contentions. *See generally* Pet. 74–81. In particular, Petitioner contends that “Segal discloses a ‘distributed firewall’ 40 comprising a plurality of firewall units” (Pet. 75), wherein “each firewall unit maintains a ‘shared list’ akin to the authorization list of the ’633 patent,” and “each firewall unit uses the shared list to limit communications to those between authorized nodes.” *Id.* at 76–77 (citing Ex. 1005, 2:60–3:15). Accordingly, Petitioner contends that “one of ordinary skill in the art would have been motivated to combine Traw’s AKE subsystems with . . . Segal’s teaching of shared lists.” *Id.* at 78 (citing Ex. 1002 ¶ 189).

Petitioner contends that “one of ordinary skill in the art looking to implement AKE subsystems in the combination of Traw and Zou would have consulted, and integrated teachings from, literature relating to a distributed firewall, such as Segal,” particularly “to reduce the computational burden associated with authentication processes,” which is “exactly what Segal’s teaching is directed to.” Pet. 79 (citing Ex. 1002 ¶ 190). In particular, according to Petitioner, “Segal teaches that by sharing the authorization lists, the nodes coupled to the interface need not individually update their own authorization lists through the computationally expensive authentication process.” *Id.* Accordingly, Petitioner contends that one of ordinary skill in the art “would have understood the benefit of integrating Segal’s list sharing technique with Traw’s authentication processes to reduce the number of times the authentication processes are performed,” wherein “this benefit would have been particularly attractive if the skilled artisan were to implement Traw’s AKE subsystems in resource-constrained devices, such as ‘disk drives’ used in Traw.” *Id.* at 79–80 (citing Ex. 1003, 3:30–33; Ex. 1002 ¶ 190). That is, according to Petitioner,

combining Traw’s AKE subsystems with Segal’s teaching of list sharing would have entailed “merely adding to Traw’s AKE subsystems Segal’s list sharing routine, which is independent of other routines executed by Traw’s AKE subsystems,” yielding “predictable results.” *Id.* at 80 (citing Ex. 1002 ¶ 190).

According to Petitioner, “Segal’s teaching—sharing of authorization lists—is the type of operation that Traw’s AKE subsystems would have carried out” because “Traw’s AKE subsystems form a distributed firewall, just like the firewall units form a distributed firewall.” *Id.* (*comparing* Ex. 1003, 8:23–28, *with* Ex. 1005, 2:51–58).

However, Patent Owner contends, “a sink’s AKE subsystem [such as that in Traw] would not have been able to use Segal’s received list” because “Traw’s system cannot function without a control key,” “Traw discloses no mechanism for sending a control key over the IEEE-1394 bus,” and “[a] device cannot use another device’s public key and device ID to generate a control key.” PO. Resp. 53–54 (citing Ex. 2012 ¶¶ 114–116).

Further, according to Patent Owner, Petitioner’s proposed combination “adds computational burden by adding the step of sending and receiving a list serving no function in the receiving device,” wherein Petitioner fails to “articulate a viable rationale for combining” the teachings. PO Resp. 54–55 (citing Ex. 2012 ¶ 134). According to Patent Owner, “[i]t is never obvious to add the teachings of a secondary reference (here, Segal)” when “the alleged advantage provided by the secondary reference (‘sharing of authorization lists’) is not needed by the primary reference.” *Id.* at 63–64 (citing *Ex parte Meinass*, Application No. 11/493,963, Appeal No. 2011-003085 at 4–5 (PTAB May 1, 2013) (reversing obviousness rejection where secondary reference’s teaching served no purpose in the primary reference)).

According to Patent Owner, instead, “Traw teaches away from the alleged rationale for combining these references” of “reduc[ing] the number of times the authentication processes are performed,” because Traw “uses authentication to ensure the local system’s CRLs are as current as they can possibly be.” *Id.* at 64 (citing Pet. 79).

We are not persuaded by Patent Owner’s contentions that Traw’s AKE subsystem “would not have been able to use Segal’s received list” (PO Resp. 53), which do not appear to address the combination of references as proposed by Petitioner. Here, we agree with Petitioner’s reliance on Segal merely for the teaching that “by sharing the authorization lists, the nodes coupled to the interface need not individually update their own authorization lists through the computationally expensive authentication process.” Pet. 79. As Petitioner points out in its Reply, “[t]he Petition explained how a POSA would have understood that Zou’s authorization list could be *used* by a receiving node in Traw to streamline and initiate the process of setting up authorizations with other authorized nodes” (Pet. Reply 26 (citing Pet. 79)), and thus, one of ordinary skill in the art would merely look to Segal’s teaching for the sharing of the authorization list in the Traw/Zou combination.

Although, according to Patent Owner, Petitioner has not explained “how the receiving device of Traw/Zou would have *used* the list after it were received” based on the teachings of Segal (PO Resp. 53), Petitioner was not required to make such a showing. As Petitioner points out, “claim 13 merely requires that ‘the second security manager is configured to *generate* an authorization list,’ not that it is configured to *use* the authorization list.” Pet. Reply 26; *see also* Ex. 1001, 23:36–42 (“claim 13”). In fact, in his deposition, Dr. Mangione-Smith acknowledges that, although the phrase

“envisions using the authorization list,” it “appears to only be constrained to constructing – generating the list.” Ex. 1020, 156:9–12.

Nevertheless, as Petitioner points out, “[t]he Petition explained how a POSA would have understood that Zou’s authorization list could be used by a receiving node in Traw to streamline and initiate the process of setting up authorizations with other authorized nodes.” Pet. Reply 26 (citing Pet. 79). Once one of ordinary skill has turned to Segal for the teaching of sharing of an authorization list, he or she need not bodily incorporate the precise system of Segal into the system in the proposed combination of Traw and Zou. *See In re Keller*, 642 F.2d 413, 425 (CCPA 1981); *see also In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012). “A person of ordinary skill is also a person of ordinary creativity, not an automaton.” *KSR*, 550 U.S. at 421.

We are also unpersuaded by Patent Owner’s contention that “Traw teaches away from the alleged rationale for combining these references” of ““reduc[ing] the number of times the authentication processes are performed,”” because Traw “uses authentication to ensure the local system’s CRLs are as current as they can possibly be.” PO Resp. 64 (citing Pet. 79). As Petitioner points out, Patent Owner’s contention is predicated “on the erroneous assumption that a ‘directed node’ in Traw/Zou/Segal would have had to perform authentication processes with every other node on the interface.” Pet. Reply 3. However, according to Petitioner, a “directed node” in the Traw/Zou/Segal combination “would have had to perform only the Diffie-Hellman key exchanges,” “*only* with those nodes on the received authorized list,” and “not the separate authentication processes.” *Id.* In particular, Petitioner contends that, to agree on the control channel encryption key for the authorization list, “a directed node might have

performed *Diffie-Hellman key exchanges* but it would not have needed to perform the authentication process,” thereby “reduc[ing] the number of times the authentication processes are performed,” and “reduc[ing] the computational burden associated with authentication processes.” Pet. Reply 27–28.

Petitioner explains that, in the proposed combination, “a directed node would need to perform Diffie-Hellman key exchanges only with the nodes on the authorization list, and the number of nodes on that list could be substantially smaller than all the nodes coupled to the interface.” Pet. Reply 28 (citing Ex. 1020, 176:1–6). Petitioner’s contention is acknowledged by Dr. Mangione-Smith during deposition. *See* Ex. 1020, 182:11–185:3 (A: “It is a fair process that node A can accept a list of nodes that B thinks it should trust and then haul it through all the regularly disclosed Traw steps and determine whether or not it actually trusts the nodes on that list,” Q: “And the number of nodes on that list can be substantially smaller than all the nodes that are coupled to the interface, correct?” A: “. . . I believe so.”) As Petitioner explained during oral argument, “[t]here are multiple steps in the authentication process,” and once “you send over an authorization list to Traw, to the device in Traw, it could forego some of the authorization lists or authentication steps that would be necessary and discussed in Traw,” wherein “the computational burden as discussed in Traw is alleviated.” Tr. 22:19–24.

Accordingly, we find unpersuasive Patent Owner’s contention that Petitioner’s proposed combination “adds computational burden by adding the step of sending and receiving a list serving no function in the receiving device.” PO Resp. 54–55 (citing Ex. 2012 ¶ 134). Instead, we are persuaded by Petitioner’s contention that one of ordinary skill in the art

“would have understood the benefit of integrating Segal’s list sharing technique with Traw’s authentication processes to reduce the number of times the authentication processes are performed.” Pet. 79–80 (citing Ex. 1003, 3:30–33; Ex. 1002 ¶ 190). That is, we find Petitioner has provided “articulated reasoning with some rational underpinning” to support its contention of obviousness. *See In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006).

We are also unpersuaded by Patent Owner’s contention that “Traw teaches away from the alleged rationale for combining these references” of “reduc[ing] the number of times the authentication processes are performed.” PO Rep. 64. In particular, we find that Traw does not constitute a ‘teaching away’ because it “does not criticize, discredit, or otherwise discourage” the sharing of an authorization list for reducing the steps in the authentication processes. *See In re Fulton*, 391 F.3d 1195, 1200–01 (Fed Cir. 2004). Obviousness requires only a showing “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 from doing so.” *See Bristol-Myers Squibb Co. v. Teva Pharms. USA, Inc.*, 752 F.3d 967, 973 (Fed. Cir. 2014).

Here, the question is whether combining the references was “uniquely challenging or difficult for one of ordinary skill in the art” or “represented an unobvious step over the prior art.” *Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007) (citing *KSR*, 550 U.S. at 421). We are persuaded by Petitioner’s contention that combining Traw’s AKE subsystems with Segal’s teaching of list sharing would have entailed “merely adding to Traw’s AKE subsystems Segal’s list sharing routine,

which is independent of other routines executed by Traw’s AKE subsystems,” yielding “predictable results.” Pet. 80 (citing Ex. 1002 ¶ 190).

On this record, Petitioner has provided sufficient support that “a skilled artisan would have had reason to combine the teaching of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success from doing so.” *PAR Pharm., Inc. v. TWI Pharm., Inc.*, 773 F.3d 1186, 1193 (Fed. Cir. 2014).

Based on the foregoing discussion, we agree with Petitioner’s analysis and find that the combination of Traw, Zou and Segal renders obvious claim 13.

III. CONCLUSION

For the reasons discussed above, we determine Petitioner has proven, by a preponderance of the evidence, that challenged claims 1 and 13 of the ’633 patent are unpatentable. The chart below summarizes are conclusions regarding the challenged claims.

Claims	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1	103	Traw, Zou	1	
13	103	Traw, Zou, Segal	13	
Overall Outcome			1, 13	

IV. ORDER

It is

ORDERED that, based on a preponderance of the evidence, claims 1 and 13 of U.S. Patent No. 6,212,633 B1 have been shown to be unpatentable; and

FURTHER ORDERED that, because this is a final written decision, parties to this proceeding seeking judicial review of our decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2019-01197
Patent 6,212,633 B1

FOR PETITIONER:

John V. Hobgood
Donald R. Steinberg
S. Calvin Walden
WILMER, CUTLER, PICKERING,
HALE AND DORR, LLP
John.Hobgood@wilmerhale.com
Don.Steinberg@wilmerhale.com
Calvin.Walden@wilmerhale.com

FOR PATENT OWNER:

Bridget Smith
Kenneth J. Weatherwax
Flavio Rose
Edward Hsieh
Parham Hendifar
Patrick Maloney
Jason C. Linger
LOWENSTEIN AND WEATHERWAX LLP
smith@lowensteinweatherwax.com
weatherwax@lowensteinweatherwax.com
rose@lowensteinweatherwax.com
hsieh@lowensteinweatherwax.com
hendifar@lowensteinweatherwax.com
maloney@lowensteinweatherwax.com
linger@lowensteinweatherwax.com