

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS LLC,
Petitioner,

v.

MONARCH NETWORKING SOLUTIONS LLC,
Patent Owner.

IPR2020-01708
Patent 7,756,507 B2

Before THU A. DANG, ROBERT J. WEINSCHENK, and NORMAN H.
BEAMER, *Administrative Patent Judges*.

DANG, *Administrative Patent Judge*.

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

INTRODUCTION

A. Background

In response to a Petition (Paper 1, “Pet.”) filed by Unified Patents LLC (“Petitioner”), we instituted *inter partes* review of claims 1–5 (the “challenged claims”) of U.S. Patent No. 7,756,507 (Ex. 1001, “the ’507 patent”). See Paper 26 (“Dec. Inst.”). During trial, Monarch Networking Solutions LLC (“Patent Owner”) filed a Response (Papers 33–34, “PO Resp.”), to which Petitioner filed a Reply (Papers 40–41, “Pet. Reply”). In turn, Patent Owner filed a Sur-Reply. Papers 43–44 (“PO Sur-Reply”). An oral hearing was held with the parties on March 1, 2022. A transcript of the hearing has been entered into the record (Papers 57, 60, “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 1–5 of the ’507 patent are unpatentable.

B. The ’507 Patent

The ’507 patent, titled “Method and Device for Authenticated Access of a Station to Local Data Network in Particular Radio Data Networks,” issued on July 13, 2010, from Application No. 10/493,489, having a foreign application priority date of October 24, 2001. Ex. 1001, codes (54), (45), (21), (30).

The ’507 patent relates to methods, devices and systems for the authenticated access to a data network by means of a station compatible with the data network. See Ex. 1001, code (57). For determining the authenticity

of a subscriber, characteristic information is transmitted by the data network to a device external to the data network having authentication of subscribers, and the subscriber then transfers the characteristic information received manually to the station after it has been shown. *Id.* at 4:9–30. An illustration of the sequence of an authentication method of the '507 patent's system is depicted in Figure 2, reproduced below:

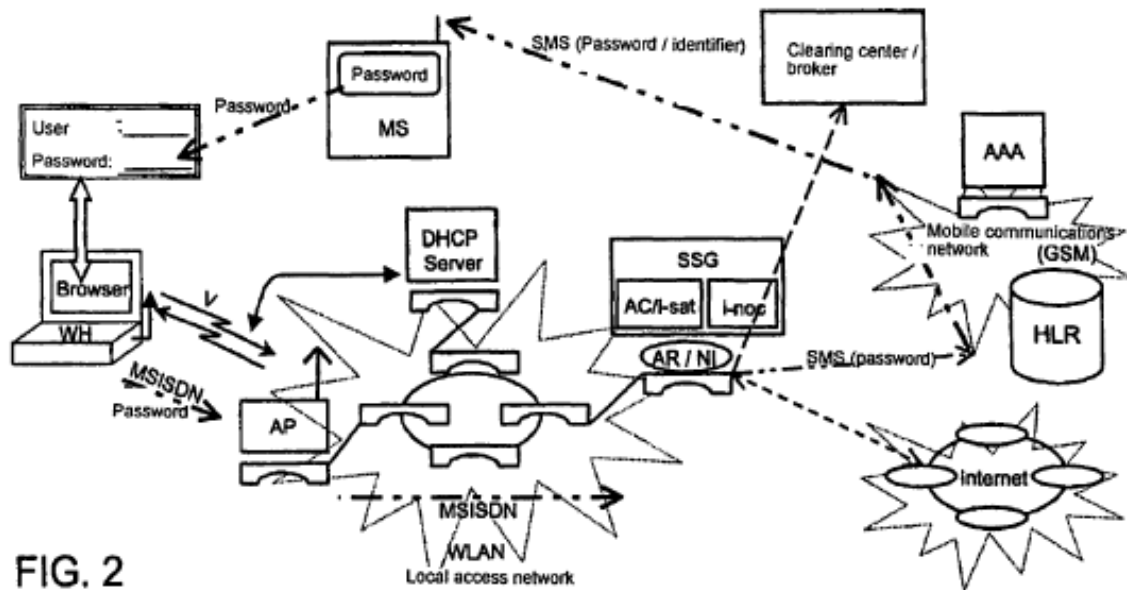


FIG. 2

Figure 2 of the '507 patent shows a schematic illustrating the sequence of operations in the accessing of a network by a station, and the corresponding authentication of the station. *Id.* at 9:1–4.

As shown in Figure 2, the subscriber or operator of station WH inputs an access number or telephone number (mobile directory number), and the identification number or telephone number is sent via access point AP to service selection gateway SSG. *Id.* at 9:42–47. Service selection gateway SSG then generates a password that is transmitted as an identifier via a telecommunications network to mobile station MS. *Id.* at 9:48–66. Next, the subscriber reads off the identifier from mobile station MS, inputs the

read information into station WH, and the identifier is then sent by station WH via access point AP to service selection gateway SSG. *Id.* at 10:1–5. Service selection gateway SSG checks as to whether the identifier matches the password originally generated, wherein, if the identifier checks out, station WH is cleared and permitted access to special services and/or the Internet. *Id.* at 10:6–16.

C. The Challenged Claims

Of the challenged claims, claim 1 is the sole independent claim. Claims 2–5 depend from claim 1. Claim 1 is illustrative, and is reproduced below:

1. A method for authenticated access by a station compatible with a data network, where access of the station is to an access point for such a data network, comprising:

transmitting identification information to the access point;

providing and transmitting a password via an interface to an authenticated device of a system or network external to the access point, having an authenticating function, whereby the identification information is directly assigned to the device authenticated in the external system or network and access to data of the authenticated device is available at a location of the station or of the access point;

transferring the password sent to the authenticated device from the authenticated device to the station;

based on the password received at the station, the station transmitting an attempted copy of the password to the access point;

comparing the attempted copy of the password received from the station by the access point with the password sent to the authenticated device; and

if the comparison is positive, enabling access of the station to at least some services and functions at the access-point end or at the network end.

Ex. 1001, 12:51–13:6.

D. Asserted Grounds of Unpatentability

We instituted *inter partes* review on all claims and all grounds in the Petition. Petitioner asserts that claims 1–5 of the '507 patent are unpatentable on the following grounds (Pet. 1):

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–5	103	Vandergeest ¹
1–5	103	Engberg, ² Stewart ³

Petitioner relies on the declaration of Michael I. Shamos, Ph.D. (Ex. 1003) in support of its unpatentability contentions. Patent Owner provides the Declaration of Eric B. Cole, Ph.D. Ex. 2031. Dr. Cole was cross-examined by Petitioner, and a transcript of his deposition was entered into the record. Ex. 1058.

¹ U.S. Patent Publication No. 2002/0169988 A1, published November 14, 2002, filed May 14, 2001 (Ex. 1007, “Vandergeest”).

² PCT Publication No. WO 01/67219, published September 13, 2001, filed March 6, 2001 (Ex. 1004, “Engberg”).

³ PCT Publication No. WO 01/37517 A2, published May 25, 2001, filed November 3, 2000 (Ex. 1005, “Stewart”).

ANALYSIS

A. *Real Parties in Interest*

Petitioner identifies only itself as a real party in interest (“RPI”), and “certifies that no other party exercised control or could exercise control over [its] participation in this proceeding, the filing of this petition, or the conduct of any ensuing trial.” Pet. 82.

Patent Owner, however, contends that Cisco is an RPI. *See* PO Resp. 2; PO Sur-reply 14–20. Patent Owner contends that the evidence showing that Cisco is an RPI is as follows:

1. Petitioner’s business model is functionally identical to RPX’s. PO Resp. 56; PO Sur-reply 15–16 (citing *RPX Corporation v. Applications in Internet Time, LLC*, IPR2015-01750, Paper 128 (P.T.A.B. October 2, 2020)).
2. The shared interests of Petitioner and Cisco support Cisco’s position as an RPI. PO Resp. 56–59; PO Sur-reply 16–17.
3. Cisco’s relationship with Petitioner also highlights the RPI status of Cisco. PO Resp. 59–60; PO Sur-reply 17–18.
4. Cisco was interested in and stood to benefit from the IPR. PO Resp. 61; PO Sur-reply 18.
5. Cisco desired the review of the patent as illustrated by its actions in litigation against Patent Owner. PO Resp. 61; PO Sur-reply 19–10.

Petitioner responds that “[t]here is no time bar or estoppel that would impact this trial” that Patent Owner “has already settled its dispute with Cisco.” Pet. Reply 16–17. Thus, according to Petitioner, “[a]s in prior instances, there is no basis to revisit Petitioner’s RPI designation.” *Id.* at 17

(citing *Unified Patents, LLC v. B# On Demand, LLC*, IPR2020-00995, Paper 40, 49-50 (Nov. 10, 2021)).

35 U.S.C. § 312(a)(2) requires that the “petition identif[y] all real parties in interest.” 35 U.S.C. § 312 (2018). This provision serves important notice functions to patent owners, to identify whether a petitioner is barred from bringing an IPR due to an RPI that is time-barred or otherwise estopped, and to the Board, to identify conflicts of interests that are not readily apparent from the identity of the petitioner. *See NOF Corp. v. Nektar Therapeutics*, IPR2019-01397, Paper 30 at 6 (PTAB Feb. 10, 2020) (citing Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,759 (Aug. 14, 2012); Patent Trial and Appeal Board Consolidated Trial Practice Guide (Nov. 2019), available at <https://www.uspto.gov/sites/default/files/documents/tpgnov.pdf>, 12–13 (“Consolidated Trial Practice Guide”)).

Here, Patent Owner does not set forth any allegations regarding a potential time bar under 35 U.S.C. § 315(b) or potential estoppel under 35 U.S.C. § 315(e) with respect to Petitioner’s alleged failure to name Cisco as an RPI. During the oral hearing, Patent Owner contended that because Cisco is a real party in interest, Petitioner should “be required to update its mandatory disclosures to reflect that.” Tr. 8. However, Patent Owner acknowledged that, even if Petitioner is required to update its mandatory disclosures, the Board would still need to reach the merits and render a final written decision on the patentability of the challenged claims. *Id.*

Petitioner responded during the oral hearing that the Board need not address whether a party is an unnamed RPI because “Cisco is not time barred at the time that the petition was filed,” “Cisco has never been stopped from filing an IPR and no estoppel pertaining to Cisco could have barred this

IPR.” Tr. 5. Petitioner further contends that Patent Owner has “no evidence” to support its RPI allegations and “the evidence is that Cisco did not request and this IPR was not filed on—at the behest of Cisco.” *Id.* at 5–6; *see also id.* at 6 (arguing that facts in *RPX Corp.* differ from those in this proceeding).

For the following reasons, we decline to address whether Petitioner should be required to update its mandatory disclosures to name Cisco as an RPI.

As Patent Owner acknowledged during the oral hearing, the District Court litigation between Cisco and Patent Owner has been settled and dismissed. Tr. 10:20–24. That is, Patent Owner acknowledged that there is no issue of estoppel under § 315(e). *Id.* at 11:1–5.

As Petitioner pointed out, there are facts in *RPX Corp.* not present in this case. Tr. 6. In *RPX Corp.*, an unnamed RPI, Salesforce, was served with a complaint for infringement more than one year prior to the filing of the Petition. *See RPX Corp.*, Paper 128, 7 (limiting “analysis to whether the § 315(b) time-barred entity Salesforce should have been identified as an RPI or privy”). The Board recognized that failing to name a time-barred RPI “creates the danger of ‘two bites at the apple’ that the statutes were meant to prevent via § 315(e) estoppel provisions and the § 315(b) time bar.” *Id.* at 34.

In this case, Patent Owner does not contend that Cisco or any member of Petitioner was time barred as of the date the Petition was filed. As Petitioner pointed out, Cisco was not time barred when the Petition was filed. Tr. 5. Consequently, even if we were to determine that Cisco is an RPI

of Petitioner, the § 315(b) time bar is not implicated because Cisco was not time barred at the time the Petition was filed.

Because we determine that neither the time bar nor estoppel provisions of 35 U.S.C. § 315 are implicated in this case, “we need not address whether [Cisco] is an unnamed RPI.” *SharkNinja Operating LLC v. iRobot Corp.*, IPR2020-00734, Paper 11, 18 (Oct. 6, 2020) (precedential).

B. 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 (1966). Relying on the declaration of Dr. Shamos, Petitioner contends a person of ordinary skill in the art at the time of the alleged invention (“POSITA”) would have had “a bachelor’s degree in electrical engineering, computer science or the equivalent, and in addition, one year of work experience involving password authentication, electronic payments and wireless communication,” wherein “[h]igher levels of education may substitute for less experience, and more experience may substitute for the specified level of education.” Pet. 10 (citing Ex. 1003 ¶¶ 53–54). In turn, relying on the declaration of Dr. Cole, Patent Owner contends a POSITA would have had “a bachelor’s degree in computer science, electrical engineering, computer engineering, or a related field (or its equivalent), and at least three years of experience working in networking, specifically in the area of network security.” See PO Resp. 8–9 (citing Ex. 2031 ¶ 49). In particular, according to Patent Owner, “[d]evice authentication (such as that taught by the ’507 Patent) is a tool used to provide authenticated and secure

access to data networks,” wherein “authentication becomes much more complex when it involves multiple networks.” *Id.* at 9 (citing Ex. 2031 ¶¶ 50–52).

We consider the level of ordinary skill in the art to be reflected by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1354–55 (Fed. Cir. 2001) (holding that absent evidence to the contrary, “the prior art itself [may] reflect[] an appropriate level” of ordinary skill in the art). Here, the prior art of record reflects the following: Vandergeest is directed to providing user authentication by communicating primary authentication information to an authentication unit via a primary channel, such as over the Internet (Ex. 1007, code (57)); Engberg is directed to a user authentication server that receives a request for a token (Ex. 1004, code (57)); and Stewart is directed to providing access and/or roaming features on a network system. Ex. 1005, code (57).

In general, we agree with the areas of agreement in the parties’ proposals. In particular, we agree a POSITA would have had a bachelor’s degree in electrical engineering, computer science or the equivalent. Pet. 10; PO Resp. 8–9. Although we agree with Patent Owner that “[d]evice authentication (such as that taught by the ’507 Patent) is a tool used to provide authenticated and secure access to data networks,” Patent Owner has not explained sufficiently why “experience working in networking, specifically in the area of network security” is necessary. PO Resp. 8–9. So we adopt Petitioner’s proposed general experience of work involving “password authentication,” and “wireless communication,” wherein [h]igher levels of education may substitute for less experience, and more experience may substitute for the specified level of education” (Pet. 10), which

comports with the level of ordinary skill in the art reflected in the prior art of record. Accordingly, we determine that a person of ordinary skill would have a bachelor's degree in electrical engineering, computer science or the equivalent, and in addition, at least one year of work experience involving password authentication and wireless communication, wherein higher levels of education may substitute for less experience, and more experience may substitute for the specified level of education.

C. Claim Construction

We construe each 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). Under this standard, claim terms are generally given their plain and ordinary meaning as would have been understood by a POSITA at the time of the invention and in the context of the entire patent disclosure. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc).

Petitioner contends that it is “unaware of a court having construed any Challenged Claim,” and that, “[n]o specific construction of any term is required because the relied-upon prior art meets each of the claimed terms under any proper construction.” Pet. 10 (citing *Nidec Motor Corp.*, 868 F.3d at 1017). Patent Owner contends that it “does not propose or identify any claim constructions.” PO Resp. 22.

We determine that it is unnecessary to construe any claim term expressly to resolve the disputed issues before us. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms that . . . are in controversy, and only to the extent

necessary to resolve the controversy.’’)) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

D. Obviousness over Vandergeest

Petitioner contends that claims 1–5 of the ’507 patent would have been obvious over Vandergeest. Pet. 19–43. In response, Patent Owner contends Petitioner fails to prove any of the challenged claims would have been obvious over Vandergeest. PO Resp. 25–44.

1. Principles of Law

Petitioner bears the burden of establishing the unpatentability of any claim by a preponderance of the evidence. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). This burden of persuasion never shifts to the patent owner. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

A patent claim is unpatentable under 35 U.S.C. § 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 ordinary skill in the art; and (4) objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

2. Vandergeest

Vandergeest, titled “Method and Apparatus for Providing User Authentication Using a Back Channel,” is directed to a method and

apparatus for providing user authentication by communicating primary authentication information to an authentication unit via a primary channel, such as over the Internet. Ex. 1007, codes (54), (57). In Vandergeest, an authentication code generated by the authentication unit is sent to a destination unit, the destination unit retransmits the authentication code to the user unit in a way that is transparent to a user of the user unit, and the user unit then sends the received re-transmitted authentication code back to the authentication unit. *Id.* at code (57). An illustration of Vandergeest's system for providing user authentication is depicted in Figure 3, reproduced below:

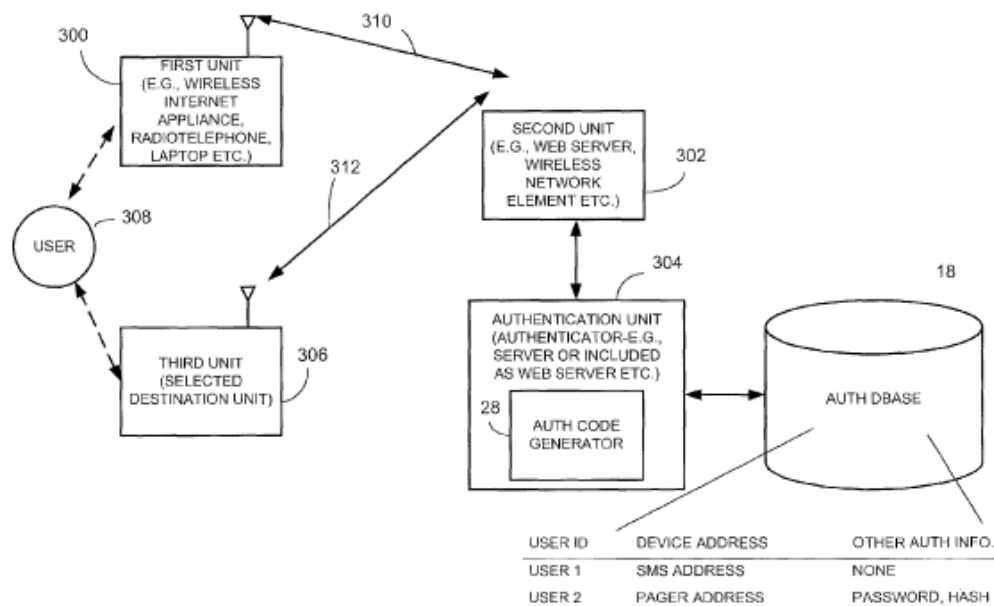


FIG. 3

Figure 3 of Vandergeest shows an embodiment wherein a destination unit, other than the user unit requesting user authentication, is used to receive the generated authentication code. *Id.* ¶ 27.

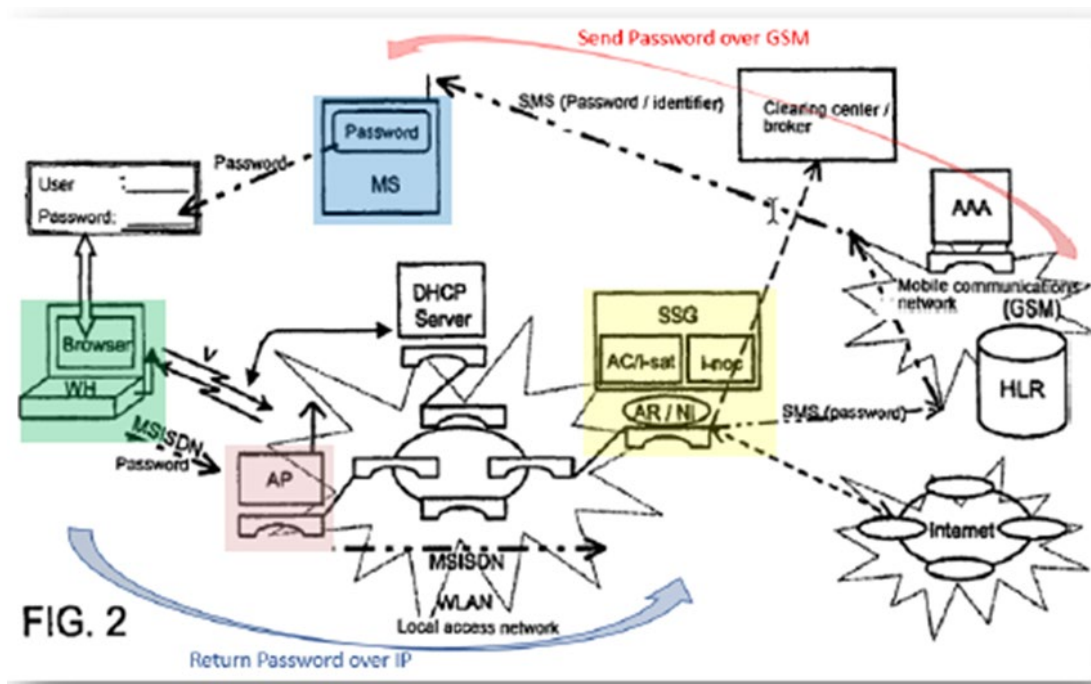
As shown in Figure 3, the system includes first (user) unit 300, second (server) unit 302, authentication unit 304, authentication database 18, and

third (user) unit 306, wherein first unit 300 and second unit 302 are wireless devices that communicate over primary wireless channel 310, and third unit 306 is also a wireless device that communicates with second unit 302 over wireless back channel 312. *Id.* ¶ 28. First unit 300 includes a primary channel controller used to communicate over the Internet to second unit 302, and third unit 306 is preferably the personal property of user 308, not a public device. *Id.* ¶ 29. User 308, in a prior registration step, provides a destination unit identifier for third (destination) unit 306 to allow third unit 306 to be communicated to from second unit 302, the information being stored in authentication database 18 and available to second unit 302 through authentication unit 304. *Id.*

In operation, the generated authentication code generated by authentication code generator 28 in authentication unit 304 is sent via wireless alternate channel 312 to a unit other than first unit 300, i.e., third unit 306. *Id.* The authentication code is then provided to user 308 via an audible or visual display associated with third unit 306, and user 308 then input the authentication code into first unit 300 through a user interface. *Id.* The authentication code is then resent by first unit 300 to second unit 302 via primary channel 310, and second unit 302 passes the resent authentication code to authentication unit 304, where authentication unit 304 then compares the resent authentication code with the authentication code that was sent to third unit 306. *Id.* If the compared codes match, user 308 (i.e., first unit 300) is granted access. *Id.*

3. Analysis

Petitioner contends that claims 1–5 of the ’507 patent would have been obvious over Vandergeest (Pet. 19–43). According to Petitioner, the ’507 patent is directed to “providing authenticated access to a data network by sending a password to a separate device (e.g. a cellphone) over a separate network (e.g. a cellular network)” (*id.* at 2 (citing Ex. 1001, 1:41–43, 3:46–4:43, 4:55–57, 6:39–50)), and the password is then “used to gain access to the ‘data network, data or the like,’” wherein “[t]he data network may be a LAN that is wired or wireless.” *Id.* (citing Ex. 1001, 3:54–60; Ex. 1003 ¶ 27). In particular, Petitioner provides an annotated version of Figure 2 of the invention, shown below, to illustrate its contentions.



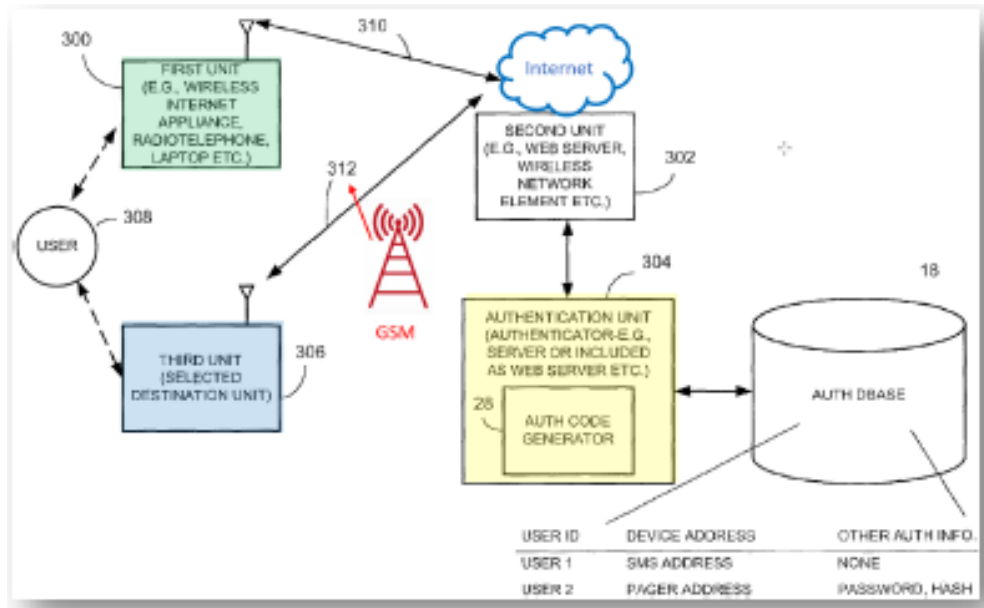
Id. at 4. Annotated Figure 2 of the '507 patent from the Petition illustrates “one embodiment of authenticating a laptop (green) by providing a password to a cellphone (blue).” *Id.* at 3 (citing Ex. 1003 ¶ 29).

According to Petitioner, a user accesses the data network by inputting at laptop WH (green) identification information (initial login), and laptop WH (green) sends the identification to service selection gateway SSG (yellow) via local access network WLAN and access point AP (pink). Pet. 3 (citing Ex. 1001, 3:64–67, 9:38–51, Fig. 2; Ex. 1003 ¶¶ 30–31). Service selection gateway SSG (yellow) receives the identification information, generates a password to authenticate the user, and transmits the password to cellphone MS (blue) via an SMS message and a GSM cellular network. *Id.* at 4 (citing Ex. 1001, 9:50–61; Ex. 1003 ¶ 32). The user reads the password from cellphone MS (blue) and inputs it into laptop WH (green), and laptop WH (green) sends the copy of the password back to service selection gateway SSG (yellow) via local access network WLAN and access point AP (pink). *Id.* at 5 (citing Ex. 1001, 9:62–10:5; Ex. 1003 ¶ 33). Service selection gateway SSG (yellow) then checks whether the password received from laptop WH (green) matches the password sent to cellphone MS (blue), wherein, if they match, laptop WH (green) is cleared to access the data network, data and the like. *Id.* (citing Ex. 1001, 10:6–16; Ex. 1003 ¶ 34).

Petitioner contends that Vandergeest, like the '507 patent, “teaches authenticated access of a computer to a data network using a password sent to a cellphone over a cellular network.” Pet. 19. That is, Vandergeest “is analogous art to the '507 Patent, as it is in the same field of endeavor, seeks to solve the same problem, and presents the same solution.” *Id.* (citing Ex. 1003 ¶ 102).

According to Petitioner, as shown in its annotated Figure 3 of Vandergeest, reproduced below, Vandergeest discloses “providing user authentication to allow a user to gain access to an application(s) or system’

via a primary channel (data network) by sending an authentication code via a secondary channel (cellular network).” Pet. 20 (citing Ex. 1007 ¶¶ 2, 15).



Id. at 20. Annotated Figure 3 of Vandergeest from the Petition shows an authentication system comprising first unit 300 (e.g., a laptop) (green), second unit 302 (e.g., a web server or wireless network element), authentication unit 304 (yellow), third unit 306 (e.g., a cellphone) (blue), primary channel 310 (leading to and/or including a LAN and/or the Internet), and back (or alternate) channel 312 (e.g., GSM network). *Id.* (citing Ex. 1007 ¶¶ 27–28, 35, Fig. 3; Ex. 1003 ¶ 105).

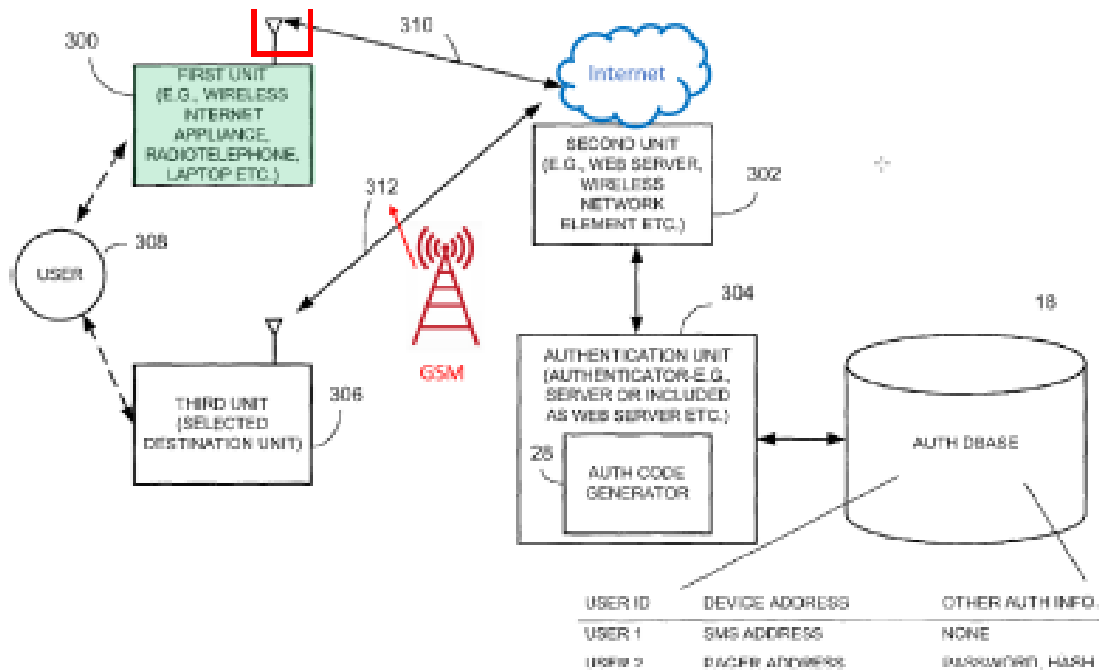
According to Petitioner, like the '507 patent, in Vandergeest, “a laptop gains authenticated access to a data network by (1) receiving a one-time password at a cellphone and (2) transferring the password to the laptop, which returns it to the data network for authentication.” Pet. 19–20 (citing Ex. 1003 ¶ 104).

a. Claim 1

- i. *“A method for authenticated access by a station compatible with a data network, where access of the station is to an access point for such a data network”*

Petitioner contends that, “[t]o the extent the preamble is limiting, it is taught or rendered obvious by Vandergeest in light of the knowledge of a [POSITA].” Pet. 23–29. According to Petitioner, Vandergeest teaches a method for authenticating a user’s access “by a laptop (*station*) compatible via TCP/IP communications over a LAN and/or the Internet (*compatible with a data network*),” where “access to the laptop (*station*) is to a wireless access point (*access point*) for such a data network.” *Id.* at 23 (citing Ex. 1003 ¶ 112).

Petitioner contends that, in Vandergeest, “laptop 300 (*station*) includes a ‘suitable interface to allow the exchange of information with another device on the Internet’ . . . , a wireless antenna . . . and TCP/IP stack for communication over the Internet using primary wireless channel 310.” Pet. 25 (quoting Ex. 1007 ¶ 19). Petitioner provides an annotated version of Figure 3 of Vandergeest, shown below, to illustrate its contentions.



Id. at 25. Annotated Figure 3 of Vandergeest in the Petition shows “a system for providing authenticated access to wireless laptop 300 (green) in communication with web server 302 through a primary wireless channel 310 that includes a wireless LAN and access point providing data access to the Internet.” *Id.* at 26. Petitioner contends that “Vandergeest discloses that the wireless laptop can communicate through a ‘local area network,’” wherein “using WLANs and wireless access points was within the general knowledge of a [POSITA].” *Id.* at 27 (citing Ex. 1007 ¶ 43; 1003 ¶ 117).

Petitioner contends that “applicant admitted that an array of IEEE 802.11b access points were known and available.” Pet. 13 (citing Ex. 1001, 3:28–37). Relying on its declarant, Dr. Shamos, Petitioner further contends that “[t]he access point itself, in fact is not particularly pertinent to the purported invention claimed by the ’507 Patent, beyond being the computer equipment through which a computer communicates with a data network,” wherein “[a]ll networks, both wired and wireless, are accessed from a connection point, i.e. an access point.” *Id.* at 13–14 (citing Ex. 1003 ¶¶ 67–

68). During the oral hearing, Petitioner explained that its position, as supported by “expert testimony and evidence,” is that a POSITA “looking at laptop in this timeframe, communicating wirelessly over the Internet, that discloses to them the most popular form, . . . this wireless LAN 802.11 access point.” Tr. 22–23.

Patent Owner replies that “Petitioner never clearly identifies the purported ‘access point’ or ‘data network’ within Vandergeest.” PO Resp. 25 (citing Pet. 23–29; Ex. 2031 ¶ 66). According to Patent Owner, Petitioner “fails to point out what in Vandergeest represents the access point” (*id.* at 26), wherein “Petitioner asserts (without supporting evidence) that any wireless communication link includes the claimed access point.” *Id.* at 27. As to Petitioner’s contention that “Vandergeest describes that second unit 302 may include a ‘**wireless network element**’” wherein a “[POSITA] understood that the wireless network element includes a wireless access point” (*id.* at 27–28 (citing Pet. 26)), Patent Owner contends that “Petitioner provides no evidence that a POSITA would understand a wireless network element to be an access point.” *Id.* at 28 (citing Ex. 2031 ¶¶ 67–70). According to Patent Owner, “Vandergeest simply describes unit 302 as a ‘wireless device[] that communicate[s] over a primary wireless channel.’” *Id.* (citing Ex. 1007 ¶ 28).

Patent Owner contends that Petitioner fails to meet “its burden of demonstrating that the use of an access point to a data network in the claimed manner was obvious” because “access points are *not* always necessary for Wireless LANs.” PO Resp. 29 (citing Pet. 29; Ex. 1024 (textbook on wireless LAN); Ex. 1013 (Kalavade provisional application)). Furthermore, Patent Owner contends that Petitioner has not shown that the

use of access points for a data network “was within the general knowledge of a POSITA *at the time of invention*,” because, although Petitioner references Kalavade for such general knowledge, “Kalavade was published well after the claimed priority date on the face of the ’507 patent.” *Id.* at 29–30 (citing Pet. 27; *comparing* Ex. 1001, code (30) *with* Ex. 1025, code (43)).

As to Petitioner’s reliance on Dr. Shamos’s declaration, Patent Owner contends that Dr. Shamos largely relies on 1) Exhibit 1013, which is a “provisional application”; 2) Exhibit 1006, “which does not discuss or utilize the term ‘access point,’ and which Dr. Shamos makes no attempt to analyze; 3) 47 C.F.R. § 15.247, “which [also] does not discuss or utilize the term ‘access point;’” and 4) Exhibit 1035, which Dr. Shamos “quotes a single paragraph with no explanation as to how the access points described relate to the access point for a data network required by the ’507 invention.” PO Resp. 31 (citing Ex. 1003 ¶¶ 63–66, 70–71).

As to Petitioner’s contention that “access points are ‘deemed’ to include even ‘network cards in computers and the like” (Pet. 28, n. 2 (citing Ex. 1001, 3:58–63), Patent Owner contends that a “network card” does not necessarily include an “access point.” PO Resp. 32 (citing Ex. 2031 ¶¶ 74–75). That is, according to Patent Owner, “Petitioner’s inherency argument fails to show that the ‘access point’ is ‘necessarily present’ in the prior art.” *Id.* at 33.

We are persuaded by Petitioner’s contention that “access of the station is to an access point for such a data network” is taught or rendered obvious by Vandergeest in light of the knowledge of a POSITA. Pet. 23–29. Vandergeest’s Figure 3 is reproduced below:

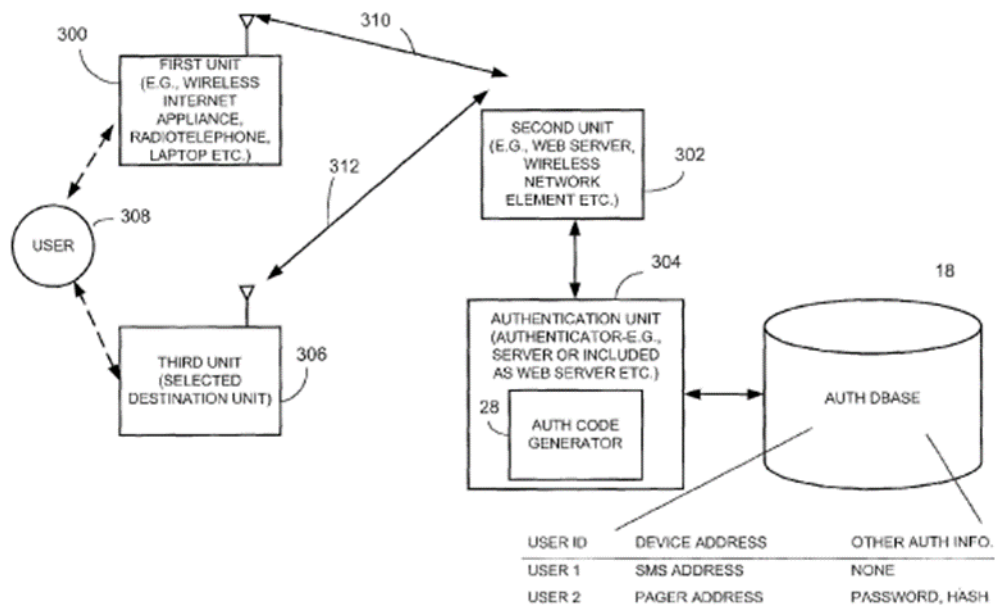


FIG. 3

As shown in Figure 3 of Vandergeest, wireless laptop 300 communicates with web server 302 through primary wireless channel 310. We are persuaded by Petitioner’s evidentiary showing that, as understood by a POSITA, it was well-known to connect a laptop to a wireless network using an access point. Pet. 13–15; Pet. Reply 3–7; Ex. 1003 ¶¶ 63–73; Exs. 1018–1025; 1034–1035. Petitioner’s Exhibit 1023, for example, discusses that “WLANs consist of Access Points (APs) and Stations,” wherein “the APs are the connection between the wireless and fixed-line world.” Ex. 1023, 2, Figure 1 (WLAN Overview). Similarly, Petitioner’s Exhibit 1035, for example, discusses that “the access point (AP) is the particular device for connecting mobile stations (STA) and wired stations.” Ex. 1035, Abstract. Thus, the evidence of record shows that “it was well-known to connect a laptop to a WLAN using an access point,” and a POSITA would have recognized that Vandergeest’s wireless laptop 300 connects to primary

wireless channel 310 using an access point. Pet. 13–15; Pet. Reply 3–7; Ex. 1003 ¶¶ 63–73; Exs. 1018–1025; Ex. 1034; Ex. 1035.

Moreover, even if Vandergeest does not teach the claimed access point to a POSITA, it would have been obvious based on Vandergeest. Specifically, the evidence of record shows that it would have been obvious to implement Vandergeest’s primary wireless channel using an IEEE 802.11 WLAN. Pet. 14–15, 29; Ex. 1003 ¶¶ 70–71, 121–122. Specifically, a POSITA would have recognized that an IEEE 802.11 WLAN provides well-known benefits, including mobility, cost savings, reliability, and reduced installation costs. Pet. 14–15, 29; Ex. 1003 ¶ 70. Further, the evidence of record shows that a POSITA would have known that Vandergeest’s laptop accesses the IEEE 802.11 WLAN via an access point. Pet. 14–15; Ex. 1003 ¶ 71; Ex. 1035, 2646.

Patent Owner argues that Petitioner’s rationale for implementing Vandergeest’s primary wireless channel using an IEEE 802.11 WLAN “is a strawman argument” because claim 1 “does not recite a WLAN, it recites an access point for a data network.” PO Resp. 29. Patent Owner’s argument is unavailing because “any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining elements in the manner claimed,” not just “the problem the patentee was trying to solve.” *KSR*, 550 U.S. at 420.

Patent Owner also points to the failures of Petitioner’s “inherency argument” (PO Resp. 28, n. 2), and that “access points are not *always necessary* for Wireless LANs” (*id.* at 29 (emphasis added)). But, as discussed above, we find Petitioner has demonstrated persuasively that using “access points” is taught or rendered obvious by Vandergeest in light of the

knowledge of a POSITA. Pet. 23–29. Thus, we need not address Petitioner’s alternative “inherency” argument.

Patent Owner contends that Petitioner erred in relying on Kalavade for showing that use of access points for a data network “was within the general knowledge of a POSITA at the time of invention.” PO Resp. 29–30. Because we do not rely on Kalavade in our determination that the use of access points was within the general knowledge of a POSITA, we need not address Patent Owner’s argument.

Based on the complete record presented, Petitioner has demonstrated persuasively that Vandergeest teaches or renders obvious “an access point,” and in particular, “a method for authenticated access by a station compatible with a data network, where access of the station is to an access point for such a data network,” as recited in claim 1, regardless of whether the preamble is limiting.

- ii. *“providing and transmitting a password via an interface to an authenticated device of a system or network external to the access point, having an authenticating function”*

Petitioner contends that Vandergeest teaches generating and sending (*providing and transmitting*) an authentication code/token (*password*) via an interface to a GSM phone (*authenticated device*) of a GSM network (*of a system or network external to the access point*). Pet. 31–32.

In particular, Petitioner contends that, in Vandergeest, authentication code generator 28 of authentication unit 304 “generates an authentication code (*password*) and sends it to GSM phone 306 (*an authenticated device*) on wireless back channel 312 (i.e., the GSM network) (*a system or network external to the access point*),” wherein “[w]ireless back channel 312 is an

interface to GSM phone 306 as claimed, providing communication from authentication unit 304 to GSM phone 306 via the GSM network.” Pet. 32–33 (citing Ex. 1007 ¶¶ 27, 30, 35, 36, Figs. 3–4; Ex. 1003 ¶¶ 129–130) (emphasis omitted). Citing Dr. Shamos’ declaration for support, Petitioner contends that, in Vandergeest, “the GSM network and phone both have an authentication function.” *Id.* at 32 (citing Ex. 1003 ¶ 128) (emphasis omitted). According to Petitioner, “Vandergeest’s disclosure of GSM—like the GSM embodiments of the ’507 Patent—is a teaching of an *authenticated device of a system or network external to the access point, having an authentication function,*” wherein “Vandergeest’s GSM network (*a system or network external to the access point*) has an *authentication function,*” and “the GSM network authenticates the GSM phones in the network in the ordinary course, making them *authenticated devices.*” *Id.* at 32–33 (citing Ex. 1007 ¶ 35 (“[I]f the user 308 has a GSM radiotelephone . . . accessible via short messaging service, no other authentication data may be necessary.”)).

Patent Owner replies that “Petitioner fails to show that Vandergeest’s third unit 306 satisfies the requirement of an authenticated device in an external network that has an authentication function.” PO Resp. 34 (citing Ex. 2031 ¶¶ 76–82). Patent Owner contends that “the Challenged Claims remove the need for prior registration of a subscriber station,” whereas, conversely, “Vandergeest requires authenticating **both** of the user devices (the first unit and the third unit) on the second unit (the web server), without any reliance on authenticating functions of an external network.” *Id.* (citing Ex. 2031 ¶¶ 45–48, 78–79). That is, in Vandergeest, “[t]o enable use of third unit 306 to authenticate a user, Vandergeest requires a registration

process for both the first *and* the third unit,” wherein “the registration process of Vandergeest fails to rely on any third party or external network for authentication.” *Id.* at 35–36 (citing Ex. 1007 ¶ 29; Ex. 2031 ¶¶ 79–80).

According to Patent Owner, “the claimed method requires that the device be authenticated in the external system or network,” wherein “[a]t best, Vandergeest teaches that the third unit is an authenticated device known to the second unit, not of an external network.” PO Resp. 37–38. Thus, “Vandergeest explicitly teaches using the authentication functions at the second unit, not the wireless back channel.” *Id.* That is, Patent Owner contends that “a POSITA would understand that authentication for Vandergeest is occurring solely at the authentication unit, and not in the wireless channel 312.” PO Sur-reply 6 (quoting Ex. 2031 ¶¶ 78–79).

Patent Owner also contends that “a POSITA would not understand the GSM network of Vandergeest to be an ‘external system or network’” as Petitioner maps. PO Resp. 42 (citing Pet. 31–32 (Vandergeest annotated Fig. 3)). According to Patent Owner, “[b]y requiring coupling of the second unit (the access point for the data network identified by Petitioner) into the authentication process,” a POSITA “would not view the two networks of Vandergeest as an ‘external system or network.’” *Id.* at 43 (citing Ex. 2031 ¶¶ 86–90). That is, a POSITA would have understood this to mean that “the data network . . . is directly involved with authenticating the device in the GSM network,” and thus, “the authentication is not occurring ‘external to the data, network but rather as an extension of the authentication process occurring in the data network.’” *Id.*

We are persuaded by Petitioner’s contention that, in light of the knowledge of a POSITA, Vandergeest teaches “transmitting a password to

an authenticated device of a system or network external to the access point, having an authenticating function.” Pet. 31–32; *see* Ex. 1001, 12:55–57.

Here, Vandergeest teaches a GSM device such as a GSM radiotelephone as third unit 306 accessible via short message service. Ex. 1007 ¶ 35. Vandergeest teaches that the GSM phone communicates with the second unit over a GSM network that is separate from primary wireless channel 310. *Id.* ¶¶ 27, 35–36, Fig. 3. As Petitioner points out, Vandergeest’s disclosure of GSM is like the GSM embodiments of the ’507 patent, wherein “Vandergeest’s GSM network (*a system or network external to the access point*) has an authentication function,” and “the GSM network authenticates the GSM phones in the network in the ordinary course, making them authenticated devices.” Pet. 32–33; Ex. 1007 ¶ 35 (emphases omitted). Specifically, the evidence of record shows that a POSITA would have known that Vandergeest’s GSM network includes an authentication function that authenticates the GSM phone on the network as a prerequisite to SMS messaging. Pet. 12, 33–34; Ex. 1003 ¶ 59; Ex. 1015, 21, 71.

Patent Owner contends that “a POSITA would understand that authentication for Vandergeest is occurring solely at the authentication unit.” PO Sur-reply 6 (quoting Ex. 2031 ¶¶ 78–79). We disagree. The evidence of record shows that “[j]ust like the ’507 Patent, GSM phones were known to be authenticated in the GSM network, using authentication function of GSM standards.” Pet. Reply 9; Pet. 11–13; Exs. 1009–1010, 1014–1015. Petitioner’s Exhibits 1009–1010, for example, describe that GSM phones are to be authenticated in the GSM network using GSM authentication algorithms. Ex. 1009, 21–26; Ex. 1010, 10.

Patent Owner argues that “[t]o enable use of third unit 306 to authenticate a user, Vandergeest requires a registration process for both the first unit **and** the third unit” in which “the user 308 provides the destination unit identifier for each unit” to the second unit. PO Resp. 35. Patent Owner contends that, as a result, “the registration process of Vandergeest fails to rely on any third party or external network for authentication.” *Id.* at 36. Patent Owner’s argument is unavailing. Patent Owner does not dispute that a GSM network authenticates a GSM phone as a prerequisite to SMS messaging. *See* PO Resp. 33–39; PO Sur-reply 5–6. Thus, the evidence of record indicates that, independent of any registration process, Vandergeest’s GSM network authenticates the GSM phone. Ex. 1003 ¶ 59; Ex. 1015, 21, 71. We agree with Petitioner that “an extra step of registration does not take Vandergeest’s authenticated GSM phones outside of the claims.” Pet. Reply 10.

Patent Owner also argues that “Vandergeest couples the data network to the GSM network in such a way that a POSITA would not understand the GSM network of Vandergeest to be an ‘external system or network.’” PO Resp. 42. Specifically, Patent Owner contends that if the user has a pager, “the pager network may require entry of a password in addition to a user ID as part of the primary authentication information,” which indicates that “the data network . . . is directly involved in authenticating the device.” *Id.* at 43. Patent Owner’s argument is unavailing. Petitioner relies on an embodiment in which Vandergeest’s third unit is a GSM phone, not a pager. Pet. 32–33. Patent Owner does not identify any evidence indicating that Vandergeest’s primary wireless channel is involved in authenticating a GSM phone on the GSM network. *See* PO Resp. 42–44. In fact, Vandergeest teaches that,

unlike a pager, “if the user 308 has a GSM radiotelephone as the third unit 306, accessible via short messaging service, no other authentication data may be necessary.” Ex. 1007 ¶ 35.

Moreover, even if any coupling does exist between Vandergeest’s primarily wireless channel and GSM network, the ’507 patent “describes ‘loosely coupling’ between the WLAN and the GSM network.” Pet. Reply 12–13 (citing Ex. 1001, 8:17–21). We agree that “Vandergeest’s disclosure of GSM—like the GSM embodiments of the ’507 Patent—is a teaching of an authenticated device of a system or network external to the access point” (Pet. 32–33), wherein, any “coupling” between the WLAN and the GSM network is similar to embodiments in the ’507 patent. Pet. Reply 12–13; *see* also Ex. 1001, 8:17–21.

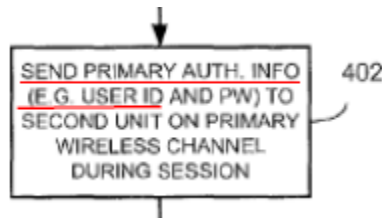
On this record presented, in light of the knowledge of a POSITA, we are persuaded by Petitioner’s contention that Vandergeest’s GSM phone is an authenticated device in the external GSM network that has an authentication function. Pet. 32–33; Pet. Reply 9.

Based on the complete record presented, Petitioner has demonstrated persuasively that Vandergeest teaches “providing and transmitting a password via an interface to an authenticated device of a system or network external to the access point, having an authenticating function,” as recited in claim 1.

- iii. “transmitting identification information to the access point” whereby “the identification information is directly assigned to the device authenticated in the external system or network”

Petitioner contends that “Vandergeest discloses or renders obvious. . . sending a user ID and telephone number (*identification information*[]) to the access point.” Pet. 30 (citing Ex. 1001, 3:64–67; Ex. 1003 ¶ 123).

Petitioner provides an annotated version of Figure 4 of Vandergeest, shown below, to illustrate its contentions.



Id. at 30 (citing Ex. 1007 ¶ 29, Fig. 4; Ex. 1003 ¶ 124). Annotated Figure 4 of Vandergeest in the Petition shows step 402 of the authentication method, wherein “laptop 300 sends primary authentication information, such as a user ID (*identification information*) out to the primary channel 310.” *Id.*

Petitioner also contends that “a user ‘provides the destination unit identifier for each destination unit’, e.g., an identifier (e.g., number) of GSM phone 306, that ‘provides sufficient information in order to allow’ communication with GSM phone 306.” Pet. 30 (citing Ex. 1007 ¶ 29, Fig. 3). According to Petitioner, “[t]his destination unit identifier includes a telephone number.” *Id.* at 31 (citing Ex. 1007 ¶ 36, Fig. 3; Ex. 1003 ¶¶ 125–126). Petitioner contends that a POSITA would have understood that “transfers of the user ID and telephone number from laptop 300 over the primary channel 310 transmits the information to the access point.” *Id.* (citing Ex. 1003 ¶ 127).

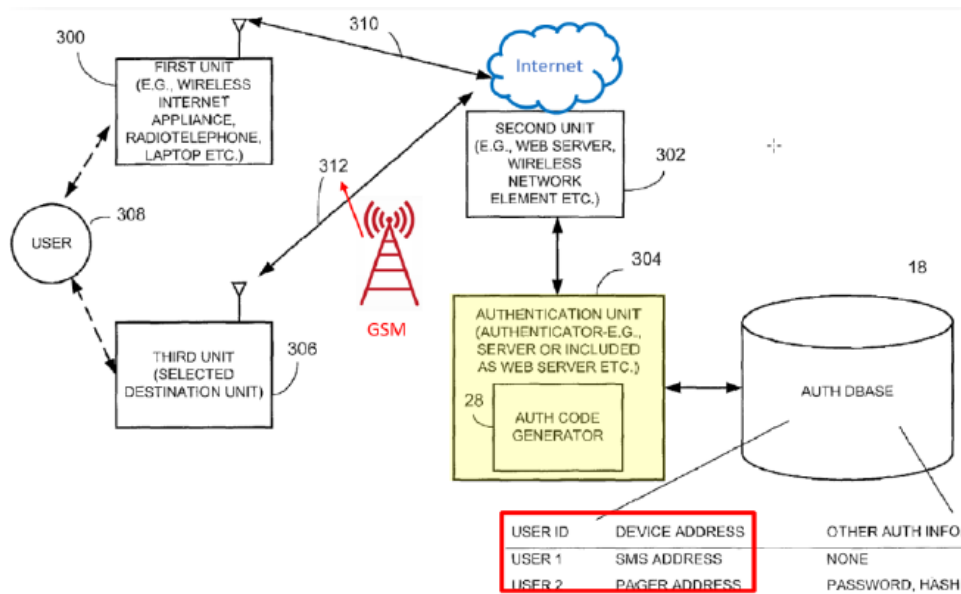
According to Petitioner, Vandergeest discloses that “the user ID and phone number (*identification information*) are directly assigned to the GSM phone (*authenticated device*) in the GSM network (*in the external system or network*).” Pet. 35–36. As Petitioner points out during the oral hearing, Petitioner is “using both user ID and telephone number” to map to the claimed “identification information.” Tr. 32.

Patent Owner contends that “Petitioner first suggests that the claimed identification information would correspond to Vandergeest’s user ID.” PO Resp. 40 (citing Ex. Pet. 30 (citing Ex. 1007 ¶ 34, Fig. 4; Ex. 1003 ¶ 35)). Patent Owner then contends that “Petitioner subsequently changes what it points to for the identification information to be the phone number assigned to the phone instead of the user ID.” *Id.* at 40–41 (citing Pet. 31–32). Patent Owner contends that Patent Owner should not be required to guess that Petitioner’s invalidity ground. *Id.* at 41 (citing Ex. 2031 ¶¶ 83–85).

Nevertheless, during the oral hearing, Patent Owner contends that Vandergeest’s user ID “does not qualify as identification information, because it is not assigned to an externally authenticated device,” wherein the claim language “requires that the identification information is directly assigned to the device authenticated in an external system.” Tr. 51. According to Patent Owner, Vandergeest’s user ID “can be associated with a multitude of destination devices.” *Id.* at 52. As to the phone number, Patent Owner contends that “the phone number is not transmitted through any access point as part of Vandergeest authenticated access solution,” wherein “the claims require . . . that the identification information be transmitted to the access point.” *Id.* at 53.

Here, Petitioner contends that “Vandergeest discloses or renders obvious. . . sending a user ID and telephone number (identification information[]) to the access point.” Pet. 30 (citing Ex. 1001, 3:64–67; Ex. 1003 ¶ 123). That is, although Patent Owner contends that it has to “guess” as to Petitioner’s invalidity grounds (PO Resp. 41), Petitioner relies on Vandergeest for disclosing identification information directly assigned to the GSM phone (authenticated device) in the GSM network (in the external system or network), such as the user ID and phone number. Pet. 35–36. As Petitioner points out during the oral hearing, Petitioner is “using both user ID and telephone number” to map to the claimed “identification information.” Tr. 32. Even Patent Owner acknowledges that Petitioner is relying on Vandergeest’s user ID as well as Vandergeest’s telephone number for the claimed “identification information.” PO Resp. 40–41 (arguing that relying on both the user ID and telephone number requires Patent Owner to “guess”).

Vandergeest illustrates in Figure 4 a method of authenticating laptop 300, wherein in step 402, the user at laptop 300 enters primary authentication information, such as a user ID, to send out to primary wireless channel 310. Ex. 1007 ¶¶ 31, 34, Fig. 4. Vandergeest teaches that authentication database 18 “stores, for a plurality of users, on a per-user bases, a user ID 24, associated password or hashed password 26 (if used) and destination unit data 22.” *Id.* ¶ 29, Fig. 3. Petitioner’s annotated version of Figure 3 of Vandergeest, shown below, illustrates this point.



Pet. 31–32; Pet. Reply 42. Annotated Figure 3 of Vandergeest as set forth in the Petition illustrates a system for authenticated access. As shown in Vandergeest’s annotated Figure 3, the user ID (“USER 1”) is directly assigned to the GSM device (red box) in the authentication database.

During oral argument, Patent Owner argued that Vandergeest’s user ID does not qualify as identification information because the claim language “requires that the identification information is directly assigned to the device authenticated in an external system.” Tr. 51. In particular, Patent Owner argued that because “[t]he user ID can be associated with a multitude of destination devices,” “the user ID is not directly assigned to an external authenticated device.” Tr. 51:24–52:14. Patent Owner’s argument is not timely because it was presented for the first time at the oral hearing. See PO Resp. 39–41; PO Sur-reply 6–8; Tr. 51:24–52:14, 68:4–69:21; Consolidated Trial Practice Guide 85–86 (Nov. 2019) (“TPG”), available at <https://www.uspto.gov/TrialPracticeGuideConsolidated>; see also Paper 8, 7 (“During an oral hearing, a party . . . may only present arguments relied upon in the papers previously submitted.”); *Dell Inc. v. Acceleron, LLC*, 884

F.3d 1364, 1369 (Fed. Cir. 2018) (holding that the Board was not obligated to consider an “untimely argument . . . raised for the first time during oral argument”). Moreover, Patent Owner’s argument is unavailing. For example, Vandergeest’s Figure 3 teaches an embodiment in which the user ID (“USER 1”) is assigned to only one device. Ex. 1007, Fig. 3.

Based on the complete record presented, Petitioner has demonstrated persuasively that Vandergeest teaches “transmitting identification information to the access point” whereby “the identification information is directly assigned to the device authenticated in the external system or network,” as recited in claim 1.⁴

iv. Remaining limitations

Patent Owner does not address separately Petitioner’s explanations and supporting evidence regarding the remaining limitations of independent claim 1. *See generally* PO. Petitioner provides detailed explanations as to how Vandergeest teaches or suggests the remaining claim limitations of claim 1, citing Dr. Shamos’s declaration for support. *See* Pet. 36–40 (citing Ex. 1001, 10:1–3, 4:14–18; Ex. 1002, 32 (prosecution history); Ex. 1007 ¶¶ 3, 21, 28, 29, 34, 36, 38–39, 43, 49, Figs. 3–4; Ex. 1003 ¶¶ 136–147).

⁴ Because we are persuaded by Petitioner’s reliance on Vandergeest’s user ID for teaching “transmitting identification information to the access point” whereby “the identification information is directly assigned to the device authenticated in the external system or network,” we need not address Petitioner’s alternative reliance on Vandergeest’s telephone number. Nonetheless, we note that Vandergeest teaches that, in a registration step, the user provides the destination unit identifier (e.g., the phone number) for each destination unit to the second unit over the primary wireless channel. Pet. 30; Ex. 1007 ¶ 29.

Having reviewed Petitioner's arguments and supporting evidence in the present record, we find that Petitioner has demonstrated persuasively that these limitations of independent claim 1 would have been obvious over Vandergeest.

b. Dependent claims 2–5

Petitioner contends that Vandergeest teaches “wherein the password is randomly generated or is randomly selected from a list with a large number of redefined passwords or another entity at the access-point end or at the network end,” as recited in claim 2. Pet. 41 (citing Ex. 1007 ¶ 28; Ex. 1003 ¶¶ 149–150). Petitioner also contends that Vandergeest teaches “wherein the transmission of the password is carried out by a short message service,” as recited in claim 3. *Id.* at 41–42 (citing Ex. 1001, 4:38–49; Ex. 1007 ¶¶ 28, 30, 35; Ex. 1003 ¶ 151). Further, Petitioner contends that Vandergeest teaches “wherein the transmission of the password is carried out by an indirect use of authentication functions in the system or network external to the access point or data network with the authenticated device,” as recited in claim 4. *Id.* at 42–43 (citing Ex. 1001, 4:38–49; Ex. 1003 ¶¶ 152–153). Petitioner then contends that Vandergeest teaches “wherein a mobile station or a subscriber identification card of a cellular mobile radio communication system is used as the authenticated device of the system or network external to the access point or data network,” as recited in claim 5. *Id.* at 43 (citing 1007 ¶¶ 21, 24, 30; Ex. 1003 ¶¶ 154–155).

Patent Owner does not address separately Petitioner's explanations and supporting evidence regarding dependent claims 2–5. *See generally* PO Resp. Having reviewed Petitioner's arguments and supporting evidence in

the present record, we find that Petitioner has demonstrated persuasively that the limitations of claims 2–5 would have been obvious over Vandergeest.

c. Vandergeest Conclusion

For the reasons discussed above, we determine Petitioner has proven, by a preponderance of the evidence, claims 1–5 would have been obvious over Vandergeest.

F. Obviousness over Engberg and Stewart

Petitioner contends that claims 1–5 of the '507 patent would have been obvious over Engberg and Stewart. Pet. 43–75. In response, Patent Owner contends that Petitioner fails to prove that the challenged claims would have been obvious over the combination of Engberg and Stewart. PO Resp. 44–54.

1. Engberg

Engberg, titled “Use of Personal Communication Devices for User Authentication,” discloses a user authentication server that receives a request for a token, wherein the request is transmitted from a personal device, such as a mobile phone or a pager, carried by a user, and the server generates a random token in response to the request and creates a new password with the token. Ex. 1004, codes (54), (57). The server then sets the user’s password to the new password and transmits the token of the personal device to the user using its communication module, and the user concatenates a secret passcode with the received token to form a valid password, and then submits

such secret passcode to a secure system to gain access to the secure system.
Id. at code (57).

An illustration of one embodiment of Engberg's authentication system is depicted in Figure 1, reproduced below:

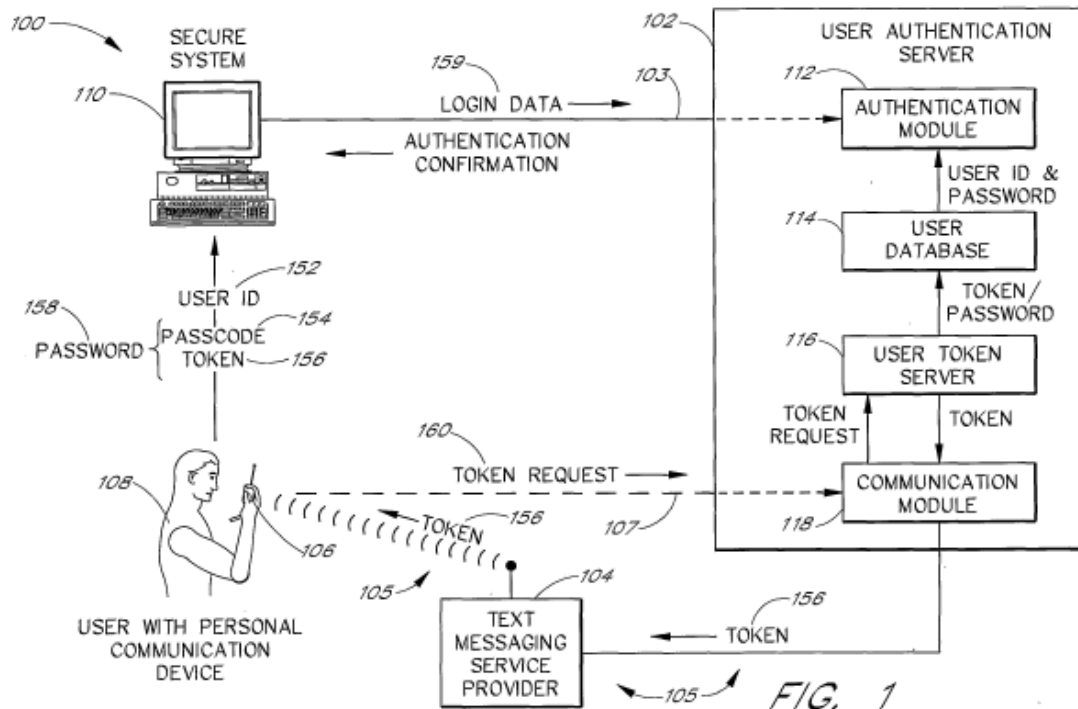


Figure 1 shows user authentication system 100 that includes user authentication server 102, text messaging service provider 104, personal communication device 106 carried by user 108, and secure system 110 to which authentication system 100 regulates access. *Id.* at 5:2–4. As shown in Figure 1, secure system 110 is connected to user authentication server 102 by computer network 103. *Id.* at 5:11–12. User authentication server 102 is configured to require user 108 to supply authentication information through secure system 110, including user ID 152, passcode 154, and user token 156, wherein token 156 is provided to user 108 by user authentication server 102

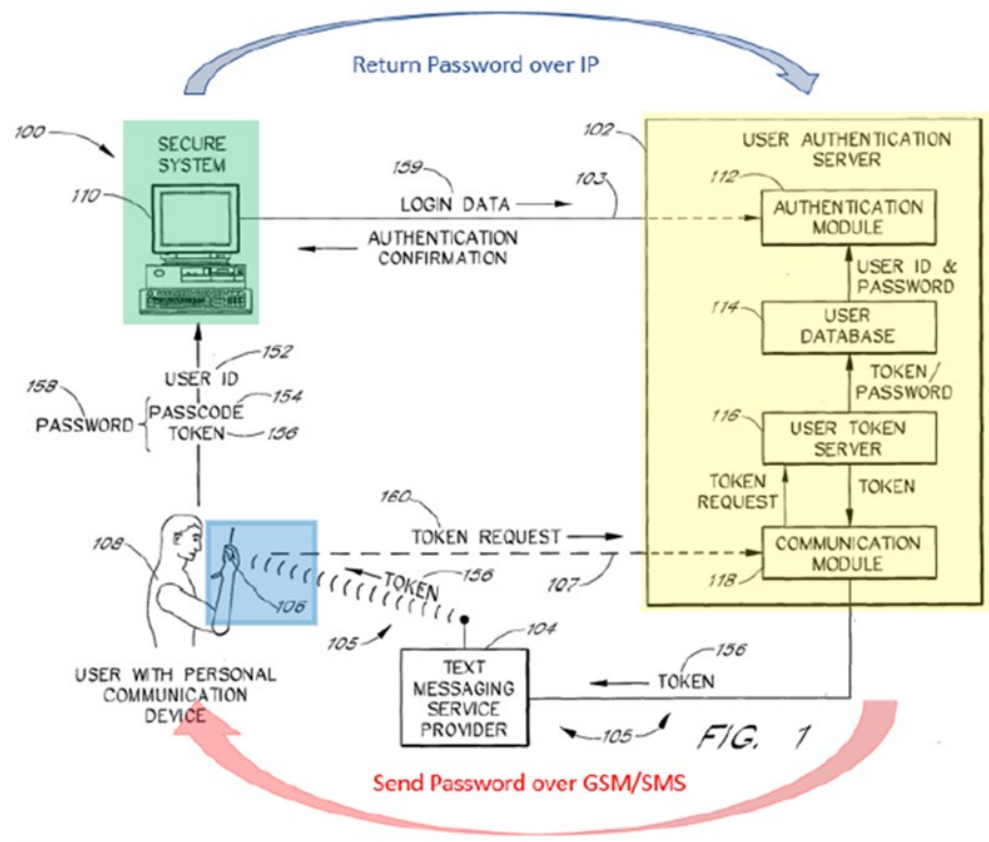
through user 108's personal communication device 106 on an as needed basis. *Id.* at 5:16–22.

2. Stewart

Stewart, titled “Distributed Network Communication System Which Enables Multiple Network Providers to Use a Common Distributed Network Infrastructure,” discloses providing access and/or roaming features on a network system, wherein the network system includes a plurality of wireless and/or wired access points coupled to a network. Ex. 1005, codes (54), (57). Stewart recognizes that “it would be desirable to provide a system and method which enables a common wireless network infrastructure to be used by two or more network service providers,” and thus, “allows a plurality of service providers to utilize a common set of access points to provide service to a potentially overlapping set of customers.” *Id.* at 1:29–32.

3. Analysis

Petitioner contends that, Engberg, like the '507 patent, “teaches providing authenticated access to a computer connected to a data network through the use of a password sent via a separate network to a cellphone.” Pet. 43. That is, Engberg “is analogous art to the '507 Patent, in the same field of endeavor, seeking to solve the same problem, and presenting the same solution.” *Id.* at 43–44 (citing Ex. 1003 ¶ 156). Petitioner provides an annotated version of Figure 1 of Engberg, shown below, to illustrate its contentions.



Id. at 45. Annotated Figure 1 of Engberg from the Petition shows “authentication of users” in which “user tokens” are sent to “personal communication devices such as mobile telephone[.]” *Id.* at 44 (citing Ex. 1004, 1:5–7, 2:13, 7:1) (emphasis omitted, alteration in original).

According to Petitioner, as shown in annotated Figure 1 of Engberg from the Petition, token 156 (password) is transmitted to cellphone 106 (blue) from user authentication server 102 (yellow) via text messaging service provider 104, and user 108 then inputs token 156 into workstation (green) that transmits a copy of token 156 back to authentication server 102 (yellow) over computer network 103. *Id.* at 44–45 (citing Ex. 1004, 8:1–5, 5:32–33, 8:1). Authentication server 102 (yellow) then compares the sent and received tokens/passwords, and if they match, user 108 is granted access

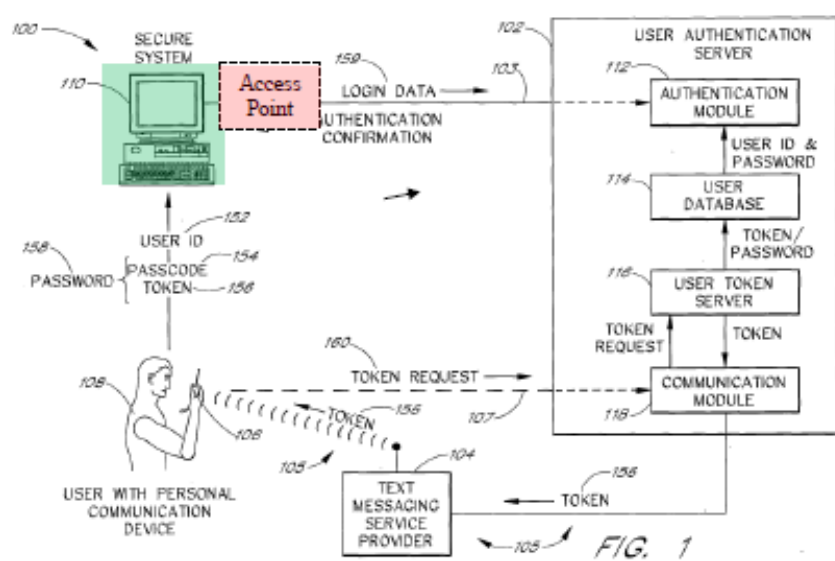
to secure system 110 via workstation (green). *Id.* at 45 (citing Ex. 1004, 3:17–18, 8:9–14, 13:27–30; Ex. 1003 ¶ 159).

a. Claim 1

- i. “A method for authenticated access by a station compatible with a data network, where access of the station is to an access point for such a data network”

Petitioner contends that, “[t]o the extent the preamble is limiting, Engberg in view of Stewart teaches, or renders it obvious.” Pet. 52–61. According to Petitioner, Engberg discloses that “user authentication server 102 requires ‘user 108 supply authentication information through the secure system 110 in order to gain access to the secure system 110.’” *Id.* at 52–53 (citing Ex. 1004, 5:16–17, 6:1–2, Fig. 1) (emphasis omitted). Petitioner contends that a POSA would have understood that “Engberg teaches that secure system 110 includes a computer network (*data network*), such as a LAN, having limited access,” and that “Engberg’s workstation is *compatible with a data network*.” *Id.* at 54.

Further, Petitioner contends that a POSITA would have understood that “the networked workstations of Engberg communicate with a network, such as computer network 103, through an *access point* in the context of the ’507 Patent.” Pet. 55. In particular, Petitioner points out that “the ’507 Patent describes access points broadly,” and thus contends that a POSITA would have understood “from Engberg’s disclosure of network interface cards and computer network 103, that Engberg includes an *access point* for network communications.” *Id.* (citing Ex. 1004, 10:37–38). Petitioner provides an annotated version of Figure 1 of Engberg, shown below, to illustrate its contentions.



Id. at 56. Annotated Figure 1 of Engberg in the Petition shows authentication system 100 in which workstation(s) (green) communicate with computer network 103 through an access point (pink, shown as added dashed block). *Id.* (citing Ex. 1004, 10:37–38, Fig. 1; Ex. 1003 ¶ 178). According to Petitioner, “Engberg taught and suggested to a POS[IT]A authenticated access of a workstation (*station*) to a computer network (*data network*) via computer network access equipment (*access point*).” *Id.* (citing Ex. 1003 ¶ 179) (emphasis omitted).

Moreover, Petitioner contends that “[w]hile Engberg does not provide express disclosure of the access point,” a POSITA would have been motivated “to combine Engberg’s authenticated access teachings with teachings of a ‘secure system’ in the form of a controlled-access LAN, . . . where access points are used to control internet access for guests,” as exemplified by Stewart. Pet. 56–57 (citing Ex. 1005, Ex. 1003 ¶ 180). According to Petitioner, Stewart discloses that a “user operating a portable computing device (PCD) 110 may communicate with one of the access points 120 to gain access to network services, such as Internet access.” *Id.* at

57–58 (citing Ex. 1005, 5:12–14) (emphasis omitted). That is, “Stewart expressly teaches access points.” *Id.* (emphasis omitted).

Accordingly, Petitioner contends that a POSITA would have readily combined the teachings of Engberg and Stewart, wherein, “[i]n the combined system, the authenticated access provided by Engberg would be to an *access point* such as an AP 120 of Stewart, providing authenticated access to the network 130 of Stewart (*a data network*).” Pet. 58–59 (citing Ex. 1003 ¶ 184).

Patent Owner replies that “Petitioner’s primary reference (Engberg) does not discuss access points for data network—in fact, the term ‘access point’ is not used within Engberg.” PO Resp. 44. Patent Owner contends that, although Petitioner contends that Engberg’s workstations communicate with network 103 through an access point, “Petitioner’s argument is again based on the incorrect assumption that any network interface card, without more, is an access point for a data network.” *Id.* According to Patent Owner, “a POSITA would understand that a network card can be used in applications other than providing access points for a data network, such as providing a direct connection between two computers.” *Id.* at 44–45 (citing Ex. 2031 ¶ 92).

Patent Owner then contends that “Petitioner does not cite to any specific teaching in Engberg or Stewart that suggests a POSITA would have been motivated to incorporate the *access points* taught by Stewart into the invention of Engberg.” PO Resp. 45. Instead, according to Patent Owner, Petitioner argues that “a POSITA would have been motivated to utilize a *WLAN* as taught by Stewart,” but “[t]he claims do not specifically recite a *WLAN*.” *Id.* That is, Petitioner does not answer “why or how a POSITA

would have used an access point such that it—for example—receives ‘identification information’ or an ‘attempted copy of the password,’ as set forth in the ’507 patent. *Id.* at 46–47.

Patent Owner further contends that “the focus of Engberg and Stewart are considerably different,” wherein “Engberg is focused on securing access to a particular resource by a user authentication server that’s accessed through a network connection” while “Stewart, on the other hand, [is] focused on . . . enabling a network infrastructure to support multiple network providers.” Tr. 56–57. Thus, according to Patent Owner, “adding wireless infrastructure to the authentication system of Engberg would be at increased cost, wireless spectrum interference, and bandwidth or throughput limitation.” Tr. 56.

We are persuaded by Petitioner’s contention that “access of the station is to an access point for such a data network” is taught or rendered obvious by Engberg in view of Stewart. Pet. 52–61. Engberg teaches a secure system connected to a user authentication server via a computer network. Pet. 48, 54–55; Ex. 1004, 5:11–12; 10:37–38, Figs. 1, 7B. Stewart teaches an IEEE 802.11 WLAN with access points. Pet. 57–58; Ex. 1005, 4:34–36, 4:24–27. The evidence of record shows that it would have been obvious to implement Engberg’s computer network using Stewart’s IEEE 802.11 WLAN such that Engberg’s secure system accesses the IEEE 802.11 WLAN via an access point. Pet. 48–52, 56–57; Ex. 1003 ¶¶ 164–172, 180. Specifically, a person of ordinary skill in the art would have known that an IEEE 802.11 WLAN provides well-known benefits, including mobility, cost savings, reliability, and reduced installation costs. Pet. 14–15, 49; Ex. 1003 ¶¶ 70, 167.

Although Patent Owner contends that Petitioner's reliance on Engberg's network interface card as an "access point" is in error (PO Resp. 44–45), Petitioner also relies on the secondary reference to Stewart for such explicit teachings of "access points," where "access points are used to control internet access for guests." Pet. 56–57. Here, Patent Owner acknowledges that Stewart explicitly teaches "access points." PO Resp. 46–47 (arguing that there is no motivation "to incorporate the access points taught by Stewart into the invention of Engberg" (emphasis omitted)). Although Patent Owner contends that Petitioner does not answer "why or how a POSITA would have used an access point," as set forth in the '507 patent (*id.*), Petitioner explains:

In the combined system, the authenticated access provided by Engberg would be to an access point such as an AP 120 of Stewart, providing authenticated access to the network 130 of Stewart (a data network), for the access to resources on network 130 and/or Internet access based on the authenticated user's prior subscriber status.

Pet. 59 (emphasis omitted).

We also find unavailing Patent Owner's contention that Petitioner fails to cite to any specific teaching in Engberg or Stewart "that suggests a POSITA would have been motivated to incorporate the access points taught by Stewart into the invention of Engberg." PO Resp. 45 (emphasis omitted). The Supreme Court has clearly stated the "combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR*, 550 U.S. at 416. In this case, the evidence of record shows that combining the teachings of Engberg and Stewart "would involve no more than the use of prior art elements according to known methods to yield predictable results." Pet. 48; Ex. 1003 ¶ 164;

KSR, 550 U.S. at 410. That is, “[d]oing so would involve no more than deploying Stewart and Engberg together according to their intended purposes to achieve predictable results of a more secure WLAN, where subscriber cell phones were used as part of authentication.” Pet. 51; Ex. 1004, 1:18–38; Ex. 1003 ¶ 169.

We consider whether incorporating Stewart’s access point into the system in Engberg, as set forth in Petitioner’s annotated version of Figure 1 of Engberg (Pet. 56 (“access point” shown as added dashed pink block)), was “uniquely challenging or difficult for one of ordinary skill in the art” or “represented an unobvious step over the prior art.” *See Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007) (citing *KSR*, 550 U.S. at 418). We find that the proposed combination “was well within the skill of a [POSITA],” without “involving any unpredictable, counterintuitive or technologically challenging steps.” Pet. 51; Ex. 1003 ¶¶ 169–170. Further, according to Petitioner, as supported by Dr. Shamons’s declaration, a POSITA “would have readily recognized that Stewart’s network 130 had benefits of wireless roaming, wide commercial settings, and cost-sharing among Internet access providers, which would be a beneficial implementation of Engberg’s ‘secure system.’” Pet. 49–50 (citing Ex. 1003 ¶ 167).

On this record, Petitioner’s rationale that a POSITA would have been motivated to incorporate Stewart’s “access point” as the access point proposed in Petitioner’s annotated version of Figure 1 of Engberg (Pet. 56) is sufficiently supported.

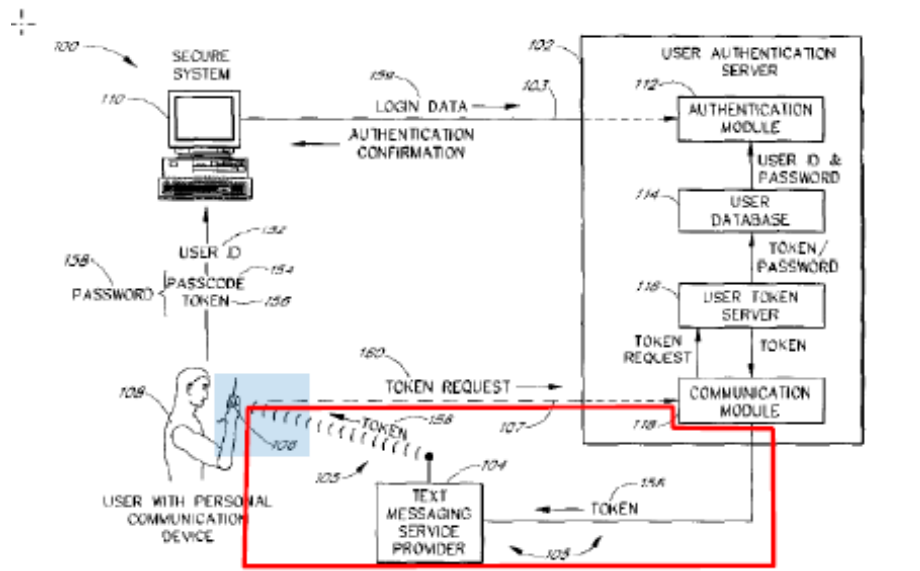
Although Patent Owner contends that “the focus of Engberg and Stewart are considerably different,” wherein “adding wireless infrastructure

to the authentication system of Engberg would be at increased cost, wireless spectrum interference, and bandwidth or throughput limitation” (Tr. 56–57), as Petitioner points out, the “law does not require that a particular combination must be preferred, or the most desirable, combination described in the prior art in order to provide motivation.” Pet. Reply 8; *see In re Fulton*, 391 F.3d 1195, 1200 (Fed. Cir. 2004); *Winner Int’l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 n.8 (Fed. Cir. 2000) (“The fact that the motivating benefit comes at the expense of another benefit, however, should not nullify its use as a basis to modify the disclosure of one reference with the teachings of another.”).

Based on the complete record presented, Petitioner has demonstrated persuasively that the combination of Engberg and Stewart teaches “an access point,” and in particular, “a method for authenticated access by a station compatible with a data network, where access of the station is to an access point for such a data network,” as recited in claim 1, regardless of whether or not the preamble is limiting.

- ii. *“providing and transmitting a password via an interface to an authenticated device of a system or network external to the access point, having an authenticating function”*

Petitioner contends that Engberg discloses “providing and transmitting a password via an interface to an authenticated device of a system or network external to the access point, having an authenticating function” as recited in claim 1. Pet. 62. Petitioner provides an annotated version of Figure 1 of Engberg, shown below, to illustrate its contentions.



Id. at 62 (citing Ex. 1004, Fig. 1; Ex. 1003 ¶ 189). Annotated Figure 1 of Engberg shows “token 156 (password) being transmitted and provided via communication link 105 (*interface*) (red) to personal communication device 106 (blue) (*an authenticated device*) of mobile service provider 104 (*of a system or network external to the access point, having an authenticating function*).” *Id.* at 61. As shown in annotated Figure 1 of Engberg, “a user ID and telephone number (*identification information*) is directly assigned to device 106 and a user views token 156 on the device 106 and enters it into the workstation (*access to data of the authenticated device is available at a location of the station or of the access point*).” *Id.*

Petitioner contends that “Engberg’s cellular/SMS network is a system or network external to the access point,” because “the cellular/SMS network is separate from, and does not communicate with, the access point of Engberg/Stewart.” Pet. 64–65 (citing Ex. 1004, Fig. 1; Ex. 1003 ¶ 192) (emphasis omitted). According to Petitioner, a POSITA would have understood that, “in Engberg, mobile phone service provider 104 authenticates personal communication device 106 to ensure that token 156 is

‘provided only to the user 108’ via the ‘secure text messaging’ of, e.g., SMS.” *Id.* at 65 (citing Ex. 1004, 5:8, 5:20–19 [sic], 6:12–13). Petitioner contends that, as previously discussed, “the authentication function was part and parcel of cellular networks and GSM/SMS systems, which Engberg disclosed,” and thus, “the cellular phone of Engberg is an authenticated device because it is authenticated by the cellular network.” *Id.* (citing Ex. 1003 ¶ 193).

Patent Owner replies that Engberg does not teach that personal communication device 106 “is authenticated in an external system having an authentication function,” but rather, “user authentication server authenticates 102 the second device (personal communication device 106).” PO Resp. 47–48 (citing Ex. 2031 ¶¶ 95–98). According to Patent Owner, in Engberg, “user authentication server 102 authenticates personal communication device 106 without the use of the authentication functions of an external network and allows sending tokens to personal communication devices that are not authenticated devices of an external network.” *Id.* at 48 (citing Ex. 2031 ¶¶ 95–98). That is, according to Patent Owner, “Engberg describes using SMS to transmit token 156 to personal communication device 106” (*id.* at 49 (citing Ex. 1004, 5:19–20, 6:12–13)), but does not teach that “the personal communication device 106 is an authenticated device of a system or network external to the access point, having an authentication function.” *Id.* (citing Ex. 2031 ¶¶ 95–98).

We are persuaded by Petitioner’s contention that, in light of the knowledge of a POSITA, the combination of Engberg in view of Stewart teaches “transmitting a password to an authenticated device of a system or network external to the access point, having an authenticating function.”

Engberg teaches a personal communication device (e.g. a GSM phone) that communicates with the user authentication server over a GSM network that is separate from the computer network. Pet. 62–64; Ex. 1004, 6:10–15 (“Ericsson T-28”), 10:10–17, Figs. 1, 6A, 6B. The evidence of record shows that a person of ordinary skill in the art would have known that Engberg’s GSM network includes an authentication function that authenticates the GSM phone on the network as a prerequisite to SMS messaging. Pet. 12, 33–34, 65; Ex. 1003 ¶ 59; Ex. 1015, 21, 71. Further, Engberg teaches that “SMS is a secure text messaging capability that is incorporated into most digital mobile phone,” wherein text messaging service provider 104 authenticates personal communication device 106 to ensure that token 156 is “provided only to the user 108” via the “secure text messaging” of, e.g., SMS. Ex. 1004, 5:8–9, 5:20–22, 6:12–15. As Petitioner explains, “the authentication function was part and parcel of cellular networks and GSM/SMS systems, which Engberg disclosed,” wherein “the cellular phone of Engberg is an authenticated device because it is authenticated by the cellular network.” Pet. 65; Ex. 1003 ¶ 193. As Petitioner points out above with respect to Vandergeest, “[j]ust like the ’507 Patent, GSM phones were known to be authenticated in the GSM network, using authentication function of GSM standards.” Pet. 11–13; *see also* Exs. 1009, 1010, 1014 1015.

Patent Owner argues that Engberg’s user authentication server authenticates the personal communication device, not the external network. PO Resp. 47–49. As discussed above, Patent Owner contends that Engberg’s personal communication device either 1) requests a token from the authentication server; or 2) pre-registers to receive a token from the

authentication server. *Id.* at 48. According to Patent Owner, “sending the token in this manner . . . avoids authenticating the personal communication device in an external network.” *Id.* Patent Owner’s argument is unavailing. Patent Owner does not dispute that a GSM network authenticates a GSM phone as a prerequisite to SMS messaging. *See* PO Resp. 47–50; PO Sur-reply 12–13. Thus, the evidence of record indicates that, independent of any token communication, Engberg’s GSM network authenticates the GSM phone. Ex. 1003 ¶ 59; Ex. 1015, 21, 71.

Based on the complete record presented, Petitioner has demonstrated persuasively that the combination of Engberg and Stewart teaches “providing and transmitting a password via an interface to an authenticated device of a system or network external to the access point, having an authenticating function,” as recited in claim 1.

iii. *“transmitting identification information to the access point” whereby “the identification information is directly assigned to the device authenticated in the external system or network”*

Petitioner contends that “Engberg teaches transmitting a ‘user ID’ (*identification information*) over a computer network to an authentication server,” wherein a POSITA “understood that transmission over a computer network, wired or wireless, involve an access point such as Stewart’s access point 120.” Pet. 59 (citing Ex. 1003 ¶ 185). For example, Petitioner contends that, in Engberg, “a user requests authenticated access by transmitting the user’s identifier, e.g., a ‘user ID’ through the workstation and network 103.” *Id.* at 59–60 (citing Ex. 1004, 9:13–14, Figs. 2C, 7B; Ex. 1003 ¶ 186).

According to Petitioner, “Engberg teaches a ‘user ID’ (*identification information*) that is associated with (*directly assigned to*) a phone number of a personal communication device (*the device authenticated in the external system or network*) in a database,” so that an SMS message can be sent to the phone. Pet. 65–66 (citing Ex. 1004, 9:30–31).

Petitioner further contends that,

[t]o the extent that *directly assigned to the device authenticated* requires the phone number itself, then it would have been obvious for a [POSITA] to modify Engberg’s method described above to transmit the phone number as the identification information.

Pet. 66.

Patent Owner contends that “Petitioner first suggests that the identification information would be a user ID.” PO Resp. 51 (citing Pet. 59 (citing Ex. 1004, Fig. 2C; Ex. 1003 ¶ 185)). Patent Owner then contends that “Petitioner subsequently changes what it points to for the identification information to be a telephone number instead of the user ID.” *Id.* at 51–52 (citing Pet. 61). Patent Owner contends that Patent Owner should not be required to guess that Petitioner’s invalidity ground. *Id.* at 52 (citing Ex. 2031 ¶¶ 101–103). Nevertheless, during the oral hearing, Patent Owner contends that “Engberg does not teach transmitting a phone number to an access point.” Tr. 60–61.

Here, Petitioner contends that “Engberg teaches a ‘user ID’ (*identification information*) that is associated with (*directly assigned to*) a phone number of a personal communication device” and that “it would have been obvious for a [POSITA] to modify Engberg’s method described above to transmit the phone number as the identification information.” Pet. 65–66

(citing Ex. 1004, 9:30–31). That is, although Patent Owner contends that it has to “guess” as to Petitioner’s invalidity grounds (PO Resp. 52), Petitioner relies on Engberg for teaching the claimed “identification information” directly assigned an authenticated device in the GSM network, such as the user ID and phone number. Pet. 65–66. As Petitioner points out during the oral hearing, Petitioner is “using both user ID and telephone number” to map to the claimed “identification information.” Tr. 39–40. Even Patent Owner acknowledges that Petitioner is relying on Engberg’s user ID as well as Engberg’s telephone number for the claimed “identification information.” PO Resp. 51–52 (arguing that relying on both the user ID and telephone number requires Patent Owner to “guess”).

Engberg teaches transmitting a user ID to the user authentication server via the computer network. Pet. 59–60; Ex. 1004, 9:13–14, Fig. 2C. Engberg also teaches that the user ID is directly assigned to a GSM phone authenticated in the GSM network. Pet. 60, 66; Ex. 1004, 3:29–30, 8:26–27, 9:30–31. For example, Engberg teaches that its “system includes a first user database configured to associate a user ID with a phone number of a personal communication device.” Ex. 1004, 3:29–30. We are persuaded by Petitioner’s reliance on Engberg for teaching a “user ID (identification information) that is directly assigned to a personal communication device (the device authenticated in the external system or network) in a database, so that an SMS message can be sent to the phone.” Pet. 65–66 (citing Ex. 1004, 9:30–31).

As discussed above, Patent Owner argued during the oral hearing that because “[t]he user ID can be associated with a multitude of destination devices,” “the user ID is not directly assigned to an external authenticated

device.” Tr. 51:24–52:14. Patent Owner’s argument is not timely because it was presented for the first time at the oral hearing. *See* PO Resp. 50–52; PO Sur-reply 13–14; Tr. 51:24–52:14, 68:4–69:21; TPG, 85–86. Moreover, Patent Owner’s argument is unavailing. For example, Engberg teaches that its “system includes a first user database configured to associate *a user ID with a phone number of a personal communication device*,” which indicates that a user ID is assigned to just one personal communication device. Ex. 1004, 3:29–30 (emphasis added).

Based on the complete record presented, Petitioner has demonstrated persuasively that the combination of Engberg and Stewart teaches “transmitting identification information to the access point” whereby “the identification information is directly assigned to the device authenticated in the external system or network,” as recited in claim 1.⁵

vi. Remaining limitations

Patent Owner does not address separately Petitioner’s explanations and supporting evidence regarding the remaining limitations of independent claim 1. *See generally* PO Resp. Petitioner provides detailed explanations as to how Engberg and Stewart teach or suggest the remaining claim limitations of claim 1, citing Dr. Shamos’s declaration for support. *See* Pet. 69–73 (citing Ex. 1004, 5:27–33, 6:1–2, 7:14–23, 7:36–37, 8:1–5, 8:9–12, 8:14; Ex. 1005, 3:3–21, 7:20–26, 9:22–26, 11:15–31, Fig. 1; Ex. 1003 ¶¶

⁵ Petitioner also relies on Engberg’s phone number as teaching identification information. Pet. 66–68. Because we are persuaded by Petitioner’s reliance on Engberg’s user ID for teaching “transmitting identification information to the access point” whereby “the identification information is directly assigned to the device authenticated in the external system or network,” we need not address Petitioner’s alternative reliance on Engberg’s telephone number.

205–212). Based on the complete record presented, Petitioner has demonstrated persuasively that these limitations of independent claim 1 would have been obvious over Engberg and Stewart.

b. Dependent claims 2–5

Patent Owner does not address separately Petitioner’s explanations and supporting evidence regarding dependent claims 2–5. *See generally* PO Resp. Petitioner contends that Engberg teaches or renders obvious “wherein the password is randomly generated or is randomly selected from a list with a large number of redefined passwords or another entity at the access-point end or at the network end,” as recited in claim 2. Pet. 73 (citing Ex. 1004, 2:5–6, 5:34–35, 7:14–15, 9:18–20; Ex. 1003 ¶ 213). Petitioner also contends that Engberg teaches “wherein the transmission of the password is carried out by a short message service,” as recited in claim 3. *Id.* at 74 (citing Ex. 1004, 5:7–9, 6:17–18, 6:27–41; Ex. 1003 ¶ 214).

Further, Petitioner contends that Engberg teaches or renders obvious “wherein the transmission of the password is carried out by an indirect use of authentication functions in the system or network external to the access point or data network with the authenticated device,” as recited in claim 4. Pet. 74 (citing Ex. 1001, 4:38–49; Ex. 1003 ¶ 215). Petitioner then contends that Engberg teaches or renders obvious “wherein a mobile station or a subscriber identification card of a cellular mobile radio communication system is used as the authenticated device of the system or network external to the access point or data network,” as recited in claim 5. Pet. 43 (citing Ex. 1004, 1:5–7; 5:5–7, 6:20–21, 7:36–39, 10:10–17; *compare with* Ex. 1001, 9:64–65; Ex. 1003 ¶¶ 216–217).

Based on the complete record presented, Petitioner has demonstrated persuasively that the limitations of claims 2–5 would have been obvious over Engberg and Stewart.

c. Engberg/Stewart Conclusion

For the reasons discussed above, we determine Petitioner has proven, by a preponderance of the evidence, that claims 1–5 would have been obvious over Engberg and Stewart.

III. CONCLUSION

For the foregoing reasons, we are persuaded on the record at hand that Petitioner has demonstrated by a preponderance of the evidence that challenged claims 1–5 of the '507 patent are unpatentable.

IV. ORDER

For the reasons given, it is

ORDERED that, based on a preponderance of the evidence, claims 1–5 of U.S. Patent No. 7,756,507 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.

In summary:

Claims	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
1–5	103	Vandergeest	1–5	
1–5	103	Engberg, Stewart	1–5	
Overall Outcome			1–5	

IPR2020-01708
Patent 7,756,507 B2

PETITIONER:

John M. Baird
Patrick D. McPherson
Paul Belnap
DUANE MORRIS LLP
jmbaird@duanemorris.com
pdmcperson@duanemorris.com
phbelnap@duanemorris.com

Roshan S. Mansinghani
Michelle Callaghan
UNIFIED PATENTS LLC
roshan@unifiedpatents.com
michelle@unifiedpatents.com

PATENT OWNER:

Michael F. Heim
Robert A. Bullwinkel
HEIM, PAYNE & CHORUSH, LLP
mheim@hpcllp.com
abullwinkel@hpcllp.com