

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS INC.,
Petitioner,

v.

SMART AUTHENTICATION IP, LLC,
Patent Owner.

Case IPR2017-02047
Patent 8,082,213 B2

Before KEVIN W. CHERRY, MICHELLE N. WORMMEESTER, and
JAMES A. WORTH, *Administrative Patent Judges*.

WORMMEESTER, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

Unified Patents Inc. (“Petitioner”) filed a Petition (Paper 3, “Pet.”) requesting *inter partes* review of claims 1–17 of U.S. Patent No. 8,082,213 B2 (Ex. 1001, “the ’213 patent”). We initially instituted an *inter partes* review as to claims 1–10 and 12–17 based on two of the three grounds presented in the Petition. Paper 9 (“Institution Decision” or “Inst. Dec.”); see 35 U.S.C. § 314(a). After institution of trial, in light of the Supreme Court’s decision in *SAS Institute Inc. v. Iancu*, 138 S. Ct. 1348 (2018), we modified our Institution Decision to include review of all the challenged claims and all the grounds presented in the Petition. Paper 14.

Smart Authentication IP, LLC (“Patent Owner”) filed a Patent Owner Response (Paper 18, “PO Resp.”), and Petitioner filed a Reply (Paper 20, “Pet. Reply”). With our authorization, Patent Owner subsequently filed a Sur-Reply (Paper 21, “PO Sur-Reply”).

On November 6, 2018, we conducted an oral hearing. A copy of the transcript (Paper 26, “Tr.”) is included in the record.

We have jurisdiction under 35 U.S.C. § 6(b). For the reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–10 and 12–17 of the ’213 patent are unpatentable. Petitioner has not made such a showing, however, with respect to claim 11 of the ’213 patent. This final written decision is issued pursuant to 35 U.S.C. § 318(a).

II. BACKGROUND

A. Related Proceedings

The parties identify several related district court cases. Pet. 1–2; Paper 4, 2.

B. The '213 Patent

The '213 patent relates to user authentication, where a user controls the level and complexity of an authentication process carried out by an authentication service provider (“ASP”) on behalf of both the user and an entity seeking to authenticate the user. Ex. 1001, 2:1–10.

To illustrate an example of user authentication according to the '213 patent, Figure 3 is reproduced below.

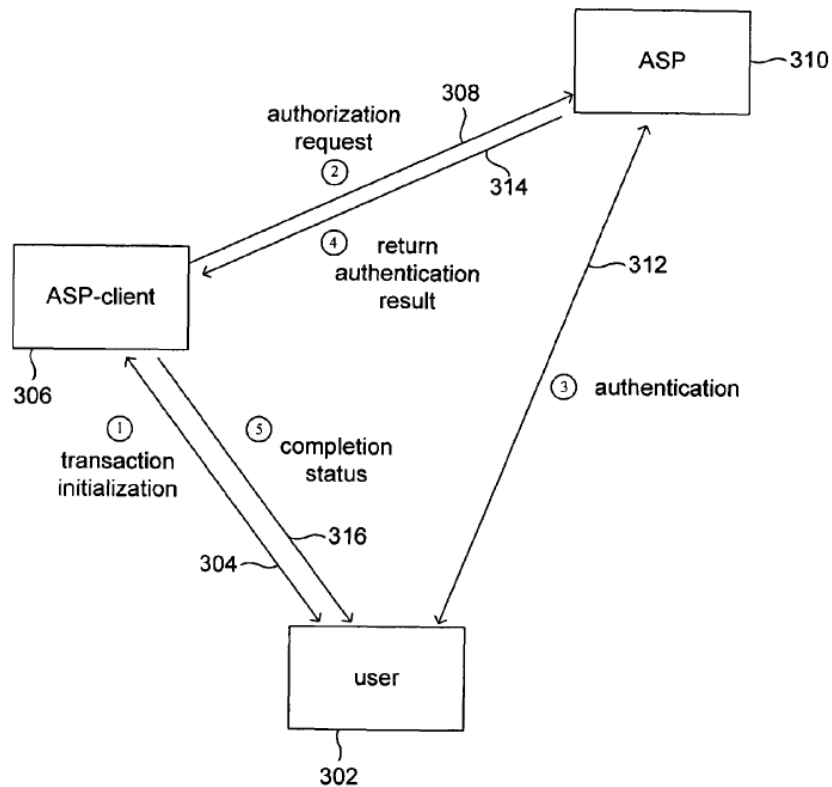


Figure 3

Figure 3 shows the interactions between a user, an ASP client, and an ASP. *Id.* at 3:47–48. First, the user starts an electronic transaction with the ASP client by requesting to log in to a commercial website or by requesting a product or service. *Id.* at 3:48–51. The ASP client obtains user information from the user. *Id.* at 3:51–55. The user information may include the user's name, the user's address or other contact information, the user's billing information, the user's employment information, or user-specified passwords. *Id.* at 4:18–27.

Next, the ASP client transmits an authentication request to the ASP to determine whether the user is authentic. *Id.* at 3:55–59. The authentication request includes the information obtained from the user. *Id.*

The ASP then carries out an authentication transaction with the user to authenticate the user according to predetermined authentication policies. *Id.* at 3:59–62. The user may specify each policy. *Id.* at 4:28–30. With respect to bank account transactions, for example, the user may specify that only transactions occurring between 1:00 pm and 4:00 pm on Monday through Friday are to be authorized, and that authorization must include variable-factor authentication using randomly generated passwords sent to the user's cell phone and furnished by the user to the bank during the transactions. *Id.* at 4:31–40.

Once the authentication transaction is complete, the ASP returns an authentication result to the ASP client, which uses the result to complete the electronic transaction with the user. *Id.* at 3:62–67.

C. Illustrative Claim

Petitioner challenges claims 1–17 of the '213 patent. Claims 1 and 12 are independent. Claim 1 is illustrative of the claims under challenge:

1. A user-authentication service implemented as routines that execute one or more computer systems interconnected by two or more communications media with both an authentication-service client, and a user, the user-authentication service comprising:

the one or more computer systems;

stored user-authentication policies specified by the user;

stored user information;

account interface routines that implement an account interface by which the user specifies, modifies, adds, and deletes user-authentication policies; and

authentication-interface routines that implement an authentication interface by which, following initiation of a transaction by the user with the authentication service client, the authentication-service client submits an authentication request, through the first communications medium or through a second communications medium, to authenticate the user, the authentication interface routines employing a variable-factor authentication, when specified to do so by stored user-authentication policies, to authenticate the user on behalf of the authentication-service client during which the user communicates with the user-authentication service through a third communications medium different from the first and second communications media and a user device different from that employed by the user to initiate the transaction with the authentication-service client.

D. The Instituted Grounds

Petitioner asserts in its Petition three grounds based on obviousness under 35 U.S.C. § 103. Pet. 4, 12–86. Although we initially instituted *inter*

partes review on fewer than all claims challenged in the Petition, we subsequently modified our Institution Decision to include review of all the challenged claims and all the grounds presented in the Petition. Inst. Dec. 2; Paper 14, 2. The instituted grounds are as follows.

Reference(s)	Basis	Claims Challenged
Harris ¹ and Owen ²	§ 103	1–17
Vandergeest ³ and Delany ⁴	§ 103	1–10
Vandergeest	§ 103	12–17

In support of the instituted grounds, Petitioner relies on the declarations of Stephen Gray (Exhibits 1003 and 1010).

III. ANALYSIS

A. Claim Construction

The claim construction standard applicable to this *inter partes* review proceeding is the broadest reasonable interpretation in light of the patent specification. See 37 C.F.R. § 42.100(b) (2017); *Cuozzo Speed Techs. LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016) (upholding the use of the broadest

¹ Harris, U.S. Patent No. 8,751,801 B2, issued June 10, 2014 (Ex. 1004).

² Owen, Int’l Publ’n No. WO 03/032126 A2, published Apr. 17, 2003 (Ex. 1006).

³ Vandergeest, U.S. Patent No. 7,765,580 B2, issued July 27, 2010 (Ex. 1005).

⁴ Delany, U.S. Publ’n No. 2002/0156879 A1, published Oct. 24, 2002 (Ex. 1007).

reasonable interpretation standard).⁵ Under this standard, claim terms generally are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

Petitioner provides proposed interpretations of the claim terms “user-authentication policies,” “specified by the user,” “variable-factor authentication,” and “returning an authentication result.” Pet. 10–12. Patent Owner does not respond. *See generally* PO Resp. In light of the parties’ arguments, we determine that no term requires express interpretation to resolve any controversy in this proceeding.

B. Obviousness over Harris and Owen: Claims 1–17

Petitioner argues that claims 1–17 of the ’213 patent would have been obvious over Harris and Owen. Pet. 12–50. Patent Owner responds that “Petitioner has failed to show that claims 1–11 are unpatentable as obvious in view of Harris and Owen for at least the reasons set forth in the Institution Decision.” PO Resp. 23 (citing Inst. Dec. 11–12). Patent Owner does not dispute Petitioner’s obviousness argument with respect to claims 12–17. *See id.* at 21–23. For the reasons explained below, we determine that Petitioner

⁵ The revised claim construction standard for interpreting claims in *inter partes* review proceedings as set forth in the final rule published October 11, 2018, does not apply to this proceeding because the new “rule is effective on November 13, 2018 and applies to all IPR, PGR and CBM petitions filed on or after the effective date.” Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340 (Oct. 11, 2018) (to be codified at 37 C.F.R. pt. 42).

has not demonstrated by a preponderance of the evidence that claims 1–17 would have been obvious over Harris and Owen.

1. *Harris*

Harris relates to user authentication based on multiple authentication factors. Ex. 1004, 2:35–38. To illustrate an example of user authentication according to Harris, Figure 7 is reproduced below.

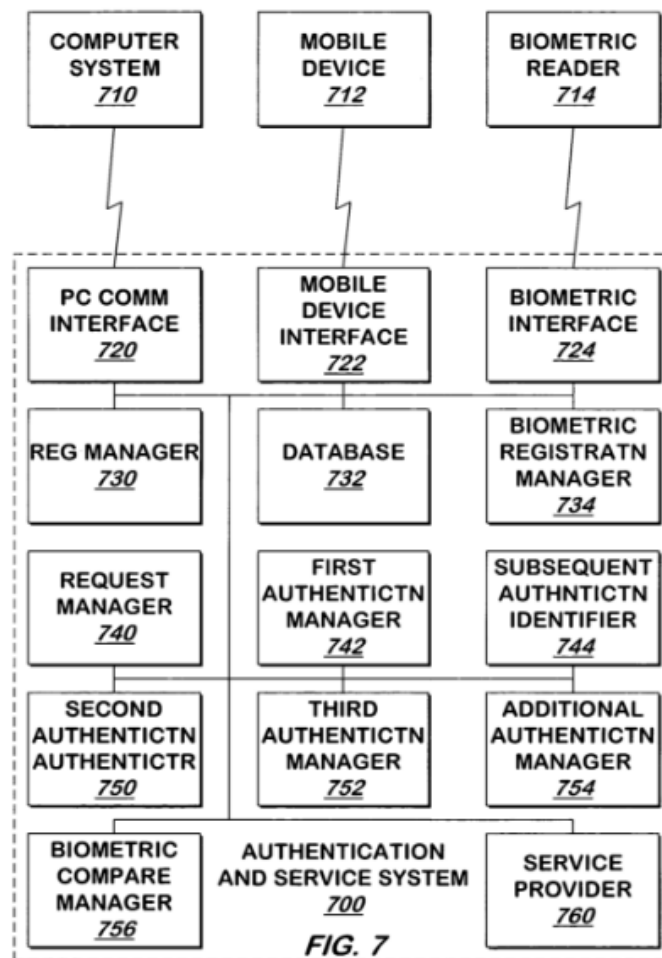


Figure 7 shows a system that uses two or more factors to authenticate a user to computer system 700 so that the computer system can process a request made by the user. *Id.* at 3:7–9, 18:9–16. When PC communication interface 720 receives a request from the user’s computer system 710, it

forwards the user's request to request manager 740. *Id.* at 19:19–22.

Request manager 740 signals first authentication manager 742, which then prompts the user for a user identifier and a password. *Id.* at 19:22–26. First authentication manager 742 compares the password received from the user to a password associated with the user that is stored in database 732. *Id.* at 19:26–28. If the passwords match, first authentication manager 742 provides the user identifier to request manager 740. *Id.* at 19:28–30.

Request manager 740 forwards the user identifier and the user's request to subsequent authentication identifier 744, which then tells request manager 740 the type and mode of any subsequent authentication factor that should be used to authenticate the user for the request. *Id.* at 19:31–35. If there is no such subsequent authentication factor, request manager 740 sends the user identifier and the request to service provider 760, which fulfills the request. *Id.* at 19:47–49. Otherwise, request manager 740 sends the type and mode of the second authentication factor and any third authentication factor to second authentication manager 750. *Id.* at 19:49–53.

Second authentication manager 750 performs the second authentication based on the type and mode of the second authentication factor. *Id.* at 18:54–56. For example, the second authentication may require retrieving a device identifier from the user's computer system, which is then compared with a device identifier registered for the user. *Id.* at 15:47–51. Alternatively, the second authentication may involve sending a secret to the user's mobile device, which the user then enters into a web page for comparison with a stored secret for that user. *Id.* at 15:61–16:17. If the second authentication is successful, second authentication manager 750

signals request manager 740 and sends the type and mode of any third authentication factor to third authentication manager 752. *Id.* at 19:56–67.

Third authentication manager 752 performs the third authentication. *Id.* at 20:16–19. If the third authentication is successful, third authentication manager 752 signals second authentication manager 750, which, in turn, signals request manager 740. *Id.* at 20:27–31. Request manager 740 then provides the user identifier and the user’s request to service provider 760, which fulfills the request. *Id.* at 20:31–33.

2. *Owen*

Owen also relates to multi-factor user authentication. Ex. 1006, 1:9–11. Owen describes a system with an authentication server that offers administrative utility for the management of server components. *Id.* at 24:3–4. For example, the authentication server allows for the creation, modification, enablement, and disablement of each component used. *Id.* at 24:4–6.

3. *Analysis*

The challenged claims can be divided into two sets of claims: claims 1–11 and claims 12–17. We address each set of claims in turn.

a. Claims 1–11

Independent claim 1, which is directed to a user-authentication service, recites an “authentication interface by which . . . the authentication-service client submits an authentication request . . . to authenticate the user.” For this limitation, Petitioner relies on Harris. In

particular, Petitioner provides an annotated version of Figure 7 of Harris, which is reproduced below. Pet. 25–26.

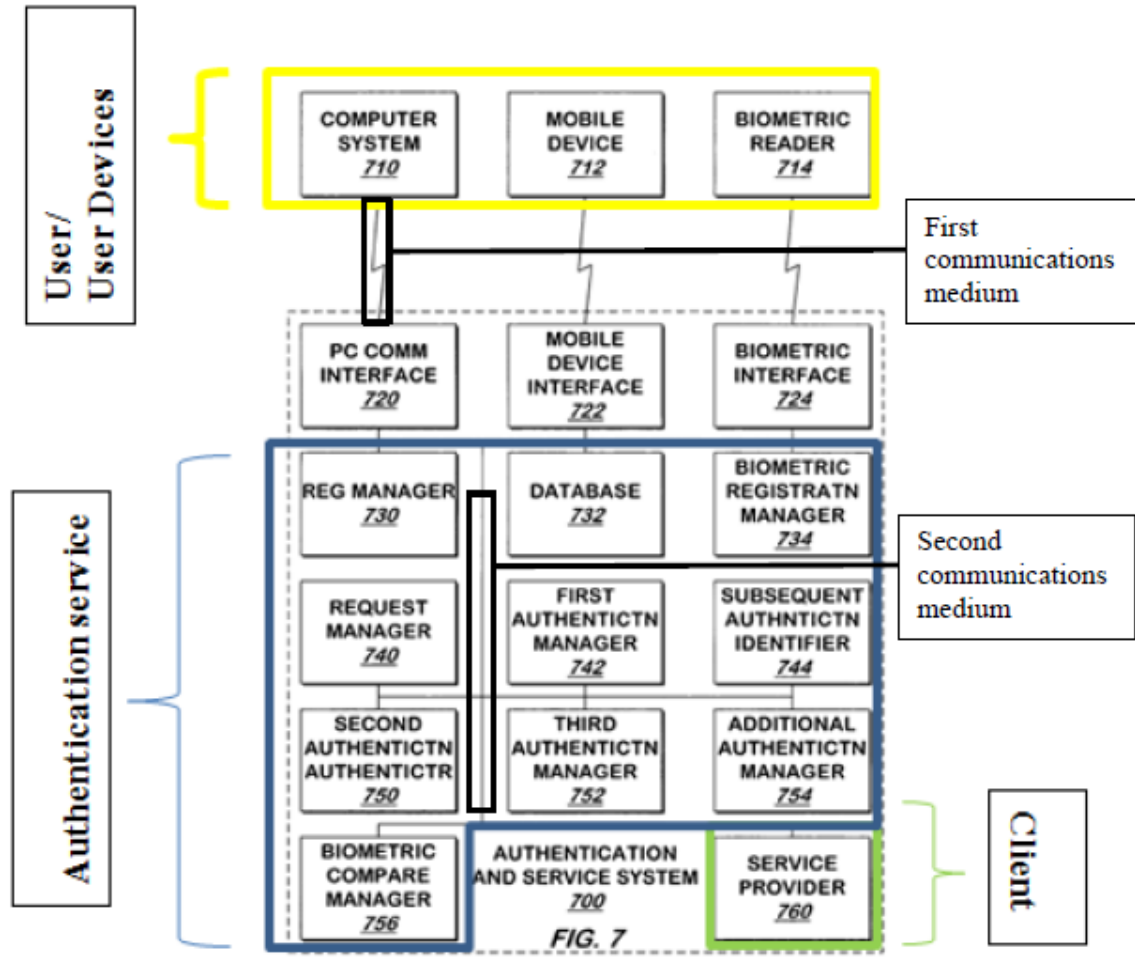


Figure 7 of Harris, as annotated by Petitioner

As discussed above, Figure 7 illustrates a system for authenticating a user to computer system 700 so that the computer system can process a request made by the user. Ex. 1004, 3:7–9, 18:9–16. Petitioner identifies Harris’s PC communication interface 720 as an “authentication interface” and Harris’s service provider 760 as an “authentication-service client.” Pet. 25–26. Petitioner further argues that Harris “describ[es] that a service provider (i.e., the claimed ‘client’) submits an authentication request through a second

communications medium to the authenticating service, via an authentication interface, to authenticate the user.” *Id.* at 25. As support, Petitioner asserts that Harris teaches that

“[w]hen the user makes a request [to the service provider], it may be made to a portion of the site that PC communication interface 720 identifies as a request, and so [the service provider, via] PC communication interface 720 forwards the request to request manager 740 [which is part of the authentication service] . . . [If authentication is successful, r]equest manager 740 then provides the request and user identifier to [the service provider], which provides the service.”

Id. at 26–27 (quoting Ex. 1004, 19:19–30) (alterations and omission added by Petitioner).

We are not persuaded by Petitioner’s argument. Petitioner interprets Harris’s PC communication interface 720 as providing an interface between service provider 760 and what Petitioner refers to as the “authentication modules.” *Id.* at 26; *see also* Pet. Reply 20 (“*Harris* discloses, or at least renders obvious, that interface 720 is used by service provider 760 to communicate with the other components of system 700.”). We understand such modules to comprise what Petitioner identifies as an “authentication service.” *See* Pet. 26 (annotated version of Figure 7 of Harris). However, Harris teaches that “[c]omputer system 710 communicates over a network such as the Internet with authentication and service system 700 via PC communication interface 720.” Ex. 1004, 18:22–24. That is, Harris’s PC communication interface 720 provides an interface between the user and system 700, which includes service provider 760 as well as the authentication modules. *See id.* at 18:28–32 (“When the user connects to a registration portion of a web site hosted by authentication and service

system 700 via PC communication interface 720, PC communication interface 720 provides the connection to registration manager 730.”); *id.* at 19:19–22 (“When the user makes a request, . . . PC communication interface 720 forwards the request to request manager 740.”). As we stated in our Institution Decision, Petitioner does not point us to any persuasive evidence showing that service provider 760 uses PC communication interface 720 to communicate with other components of system 700. Inst. Dec. 11. Indeed, Figure 7 of Harris shows that service provider 760 can communicate directly with other components of system 700 without going through PC communication interface 720. *See* Ex. 1004, Fig. 7; *see also id.* at 19:48–49 (“[R]equest manager 740 provides the request and user identifier to service provider 760.”).

In its Reply, Petitioner contends that “*Harris* teaches, or at least renders obvious, that the web site is provided by service provider 760.” Pet. Reply 21–22. As support, Petitioner points us to where Harris teaches that service provider 760 “fulfills the request” or “provides the service.” *Id.* (citing Ex. 1004, 19:47–49, 20:32–33). Petitioner additionally points us to where Harris teaches that, “[w]hen the user connects to a registration portion of a web site hosted by authentication and service system 700 via PC communication interface 720, PC communication interface 720 provides the connection to registration manager 730.” *Id.* at 21 (citing Ex. 1004, 18:28–32). According to Petitioner, “the web site submits the registration request of the user via interface 720 to the authentication modules.” *Id.* Petitioner asserts that Harris “states that this process applies for ‘requests’ generally.” *Id.* (citing Ex. 1004, 19:19–22).

We remain unpersuaded by Petitioner. Even if the web site in Harris is provided by service provider 760, Petitioner still has not directed us to any persuasive evidence showing that service provider 760 uses PC communication interface 720 to communicate with other components of system 700. For example, as Petitioner points out, Harris teaches that, “[w]hen the user connects to a registration portion of a web site . . . via PC communication interface 720, PC communication interface 720 provides the connection to registration manager 730.” Ex. 1004, 18:28–32 (*cited by* Pet. Reply 21). Similarly, Harris also teaches that, “[w]hen the user makes a request . . . to a portion of the site . . . [,] PC communication interface 720 identifies . . . and . . . forwards the request to request manager 740.” *Id.* at 19:19–22 (*cited by* Pet. Reply 21). These teachings do not describe service provider 760 using PC communication interface 720 to communicate with registration manager 730 or request manager 740.

Rather, the teachings in Harris indicate that PC communication interface 720 actively screens incoming communications from the user and forwards them to other components of system 700. In the latter scenario discussed above, once the user is authenticated, request manager 740 sends the user’s request to service provider 760 to be fulfilled. *Id.* at 19:47–49 (“If the type of any subsequent authentication factor is ‘none’, request manager 740 provides the request and user identifier to service provider 760, which fulfills the request.”), 20:25–33 (“[S]econd authentication manager 750 returns an indication that the user was authenticated to request manager 740. Request manager 740 then provides the request and user identifier to service provider 760, which provides the service.”); *see also id.* at 20:34–38 (“In one embodiment, subsequent authentication identifier 744 may also provide

to request manager 740 any additional authentication criteria and request manager 740 does not provide the request to service provider 760 until the additional authentication criteria are met.”). Accordingly, Harris’s PC communication interface 720 and what Petitioner identifies as the “authentication service” (see Pet. 26 (annotated version of Figure 7 of Harris)) function together much like a security guard who screens persons seeking access to a building. A person cannot enter the building to access any part of it until after the security guard has determined that the person carries the proper credentials for access.

Moreover, with respect to the recited “authentication request,” Petitioner relies on Harris’s teaching that PC communication interface 720 forwards “the request” to request manager 740. Pet. 26–27 (citing Ex 1004, 19:19–30). As we explained in our Institution Decision (Inst. Dec. 12), however, that request in Harris refers to the user’s request for service, not an authentication request to authenticate the user. See Ex. 1004, 15:23–29 (“After [registration] steps 402-408 . . . , the user can then authenticate himself or herself as part of a request for service.”), 19:19–30 (“When a user makes a request, . . . PC communication interface 720 forwards the request to request manager 740.”).

We also noted (Inst. Dec. 12) that the only component in Harris that seems to make an authentication request is request manager 740, not service provider 760. See Ex. 1001, claim 1 (reciting “the authentication-service client submits an authentication request”). For example, Harris teaches that the “[r]equest manager signals first authentication manager 742, which prompts the user for his or her user identifier and password,” and that “[f]irst authentication manager 742 compares the password to that associated with

the user in database 732.” Ex. 1004, 19:19–30. Thus, it is request manager 740 that submits an authentication request to first authentication manager 742 to authenticate the user.

In its Reply, Petitioner argues that “*Harris* discloses, or at least renders obvious, that the requests mentioned in columns 18–20 are authentication requests, not simply service requests.” Pet. Reply 23. For instance, Petitioner contends, “The initial description of Figure 7 makes it clear that the type of service requests being made are ones that require authentication.” Pet. Reply 23 (citing Ex. 1004, 18:9–16, 19:19–30). Petitioner also contends that “*Harris* teaches that the authentication managers within the authentication and service system 700 seek authentication of the user *before* the user is granted access to the requested service.” *Id.* at 24. In addition, Petitioner contends that, “while *Harris* discusses a user sending a request and then later being prompted for authentication credentials, *Harris* also teaches the option that the user can send a request along with authentication credentials.” *Id.* at 25–26 (internal citation omitted) (citing Ex. 1004, 15:30–32).

We disagree with Petitioner. That the service requests in *Harris* require authentication or that authentication is sought prior to fulfilling a request does not mean necessarily that the service requests are authentication requests. *Harris* teaches explicitly that “[t]he request for service may be a request for a web page, a request for access, such as physical access to a location, or a request for an action to be performed, such as the transfer of cash or securities from one account to another account.” Ex. 1004, 15:23–29. Contrary to what Petitioner argues, such requests are not by themselves authentication requests. See Pet. Reply 24 (“*Harris* discloses that a request

from a user to access the web site hosted by service provider 760 is an authentication request because the user must provide sufficient security credentials to access the web site.”). As discussed above, we find that an authentication request occurs in Harris when request manager 740 signals first authentication manager 742, which then prompts the user for the user’s identifier and password and compares the password to the password associated with the user in database 732. *See* Ex. 1004, 19:19–30. Our finding is consistent with the teachings in the ’213 patent. In particular, the ’213 patent teaches that “[t]he user 302 may initialize 304 an electronic transaction with the ASP client 306, such as by requesting to logon to a commercial website or requesting a product or service through an electronic medium,” and that “[t]he ASP client then transmits an authentication request 308 to the ASP 310 . . . to determine whether or not the user is authentic, so that the electronic transaction can proceed to completion.” Ex. 1001, 3:48–59. The service requests in Harris are like the electronic transaction in the ’213 patent, and the signal from request manager 740 to authentication manager 742 in Harris is like the authentication request in the ’213 patent.

Turning now to Petitioner’s reading of Harris’s teachings in the alternative (i.e., Petitioner’s reading that Harris teaches providing authentication credentials either after sending a request or along with the request), we note that Harris describes “a method of authenticating a user” that “involves several subprocesses,” including “Registration,” “Request for Service and Identification of the Factors,” “Authentication Using the Second Factor Identified,” and “Check for Other Authentication Steps, Provide Service when all are Completed.” Ex. 1004, 14:47–52, 15:22, 15:45, 16:63–

64. Figures 4A, 4B, 4C, and 4D provide flowcharts of Harris’s method, and Figure 7 shows a system for carrying out the method. *Id.* at 2:62–65 (“FIG. 4, consisting of FIGS. 4A, 4B, 4C, and 4D, is a flowchart illustrating a method of authenticating one or more users using two or more factors.”), 3:7–9 (“FIG. 7 is a system for authenticating a user using two or more factors.”). Accordingly, the descriptions of these figures should be read together, not in the alternative. For example, with respect to Figure 4B, Harris teaches that “the user may make the request for a service 410 and provides the user identifier and password of the user.” Ex. 1004, 15:30–32 (cited at Pet. Reply 26). With respect to Figure 7, Harris teaches that, “[w]hen the user makes a request, . . . PC communication interface 720 forwards the request to request manager 740,” and “[r]equest manager signals first authentication manager 742, which prompts the user for his or her user identifier and password.” Ex. 1004, 19:19–30 (*cited by* Pet. Reply 25). Read together, these teachings indicate that Harris’s step 410 of Figure 4B, in which the user makes a request for a service and provides the user’s identifier and password, is carried out by the system of Figure 7, where the user makes a request, PC communication interface 720 forwards the request to request manager 740, request manager 740 signals first authentication manager 742, and first authentication manager 742 prompts the user for the user’s identifier and password. That is, the description of the system of Figure 7 provides implementation details for the method steps of Figure 4B.

We note Patent Owner’s contention that, “[f]or the first time in its Reply, [Petitioner] now argues that Harris discloses *or at least renders obvious* claim 1’s recitation of ‘an authentication interface by which,

following initiation of a transaction by the user with the authentication-service client, the authentication-service client submits an authentication service request.” PO Sur-Reply 6. According to Patent Owner, “[t]he inclusion of this new argument is improper . . . and alone is grounds for the Board to refuse to consider the Reply in its entirety.” *Id.* Because we are unpersuaded by Petitioner’s arguments for the reasons given above, we need not address Patent Owner’s contention in this regard.

In view of the foregoing, we determine that Petitioner has not demonstrated by a preponderance of the evidence that independent claim 1 would have been obvious over Harris and Owen. As claims 2–11 depend from claim 1, we determine that Petitioner also has not demonstrated by a preponderance of the evidence that these dependent claims would have been obvious over Harris and Owen.

b. Claims 12–17

Independent claim 12 recites the step of “receiving user-identifying information from the authentication-service client.” For this limitation, Petitioner also relies on Harris. Specifically, Petitioner contends that Harris teaches that “the user may make the request for a service 410 and provides the user identifier and password of the user [to the client],” where “[t]he user identifier identifies the user.” Pet. 45 (citing Ex. 1004, 15:30–33, Fig. 4B). Petitioner also contends that “this information is sent from the client to the authentication system to perform the additional authentication procedures.” *Id.* Lastly, Petitioner contends that step 410 in Figure 4B of Harris “shows the authentication service ‘receiving user-identifying information from the authentication-service client.’” *Id.* (citing Ex. 1004, 15:30–44, Fig. 4B).

We disagree. The cited passage in Harris at column 15, lines 30–44, teaches that the user “provides the user identifier and password of the user” but does not indicate to which component the user information is being provided. In addition, Figure 4B is silent as to which component is providing the user information at step 410, indicating only that the information is received: “RCV REQ FOR SVC, USER ID, PASSWORD.”

Petitioner’s theory that Harris’s “client” (i.e., service provider 760) receives the user identifier from the user and provides it to the authentication system at step 410 seems inconsistent with other teachings in Harris. For example, Harris teaches that first authentication manager 742 prompts the user for a user identifier and a password, and, if the password matches a password that is stored in a database, provides the user identifier to request manager 740. Ex. 1004, 19:22–30. Next, request manager 740 forwards the user identifier to subsequent authentication identifier 744 to determine if further authentication is needed. *Id.* at 19:31–35. If further authentication is needed, subsequent authentication identifier 744 provides information about the authentication factors to be used to request manager 740, which forwards the information to the authentication managers to carry out further authentication steps. *Id.* at 19:49–53. Once the user is authenticated, request manager 740 forwards the user identifier along with the user’s request to service provider 760, which then fulfills the request. *Id.* at 19:47–49, 20:26–38. That is, the user identifier flows from the user to first authentication manager 742, then to request manager 740, and then to subsequent authentication identifier 744. The user identifier also flows from request manager 740 to service provider 760. Thus, Harris describes

providing the user identifier to service provider 760 but not *receiving* the user identifier from service provider 760.

We note that Petitioner does not address further in its Reply its assertion that claim 12 would have been obvious over Harris and Owen. See *generally* Pet. Reply. In view of the foregoing, we determine that Petitioner has not demonstrated by a preponderance of the evidence that independent claim 12 would have been obvious over Harris and Owen. As claims 13–17 depend from claim 12, we determine that Petitioner also has not demonstrated by a preponderance of the evidence that these dependent claims would have been obvious over Harris and Owen.

C. Obviousness over Vandergeest and Delany: Claims 1–10

Petitioner argues that claims 1–10 of the '213 patent would have been obvious over Vandergeest and Delany. Pet. 50–80. Patent Owner counters that the combination of Vandergeest and Delany does not teach the recited “variable-factor authentication.” PO Resp. 9. For the reasons explained below, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1–10 would have been obvious over Vandergeest and Delany.

1. Vandergeest

Vandergeest relates to user authentication using multi-factor techniques. Ex. 1005, 1:15–19. To illustrate an example of user authentication according to Vandergeest, Figure 3 is reproduced below.

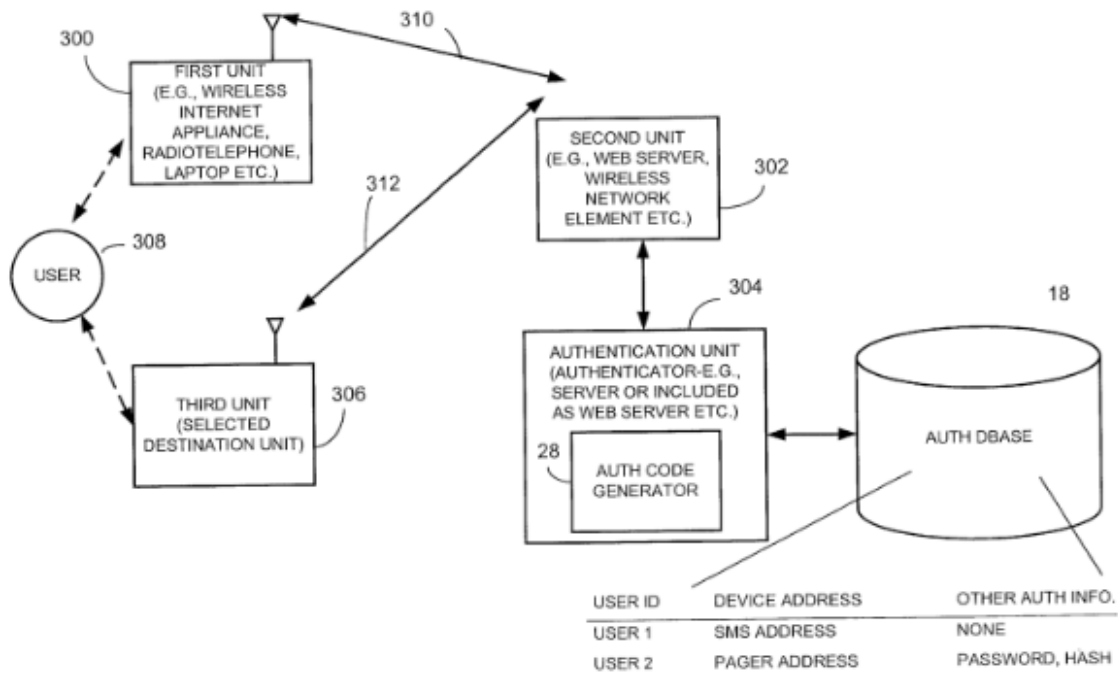


FIG. 3

Figure 3 shows a system with first unit 300, second unit 302, authenticator 304, authentication database 18, and third unit 306. *Id.* at 6:58–60. The first and second units are wireless devices that communicate with each other over a primary channel. *Id.* at 6:66–7:1. The third unit is also a wireless device, which belongs to the user, and it communicates with the second unit over a back channel. *Id.* at 7:1–5, 7:8–9.

The authentication database is populated with authentication information, such as a user ID and destination unit data, when the user registers with the authenticator. *Id.* at 4:35–40. The destination unit data identifies a destination unit, namely, the user’s third unit. *Id.* at 7:10–14.

Using the first unit, the user contacts the second unit for resources. *Id.* at 8:43–46. The second unit sends an authentication information request to the first unit, which prompts the user to enter a user ID. *Id.* at 8:46–49. Once the user enters the user ID, the first unit forwards the user ID to the

second unit, which, in turn, forwards the user ID to the authenticator to determine whether the user is listed in the database. *Id.* at 8:49–56. If the user is listed in the database, the authenticator determines which destination unit will receive an authentication code generated by authentication code generator 28. *Id.* at 8:63–65, 9:45–48.

The second unit sends the authentication code to the third device, which displays it to the user. *Id.* at 9:19–21. Next, the user enters the code into the first unit, which returns the code received from the user to the second unit. *Id.* at 9:22–26. The authenticator compares the returned code with the code that it generated. *Id.* at 9:26–30. If the codes match, the user is authenticated and uses the resources via the second unit. *Id.* at 9:30–32.

2. *Delany*

Delany relates to modifying group membership. Ex. 1007 ¶ 9. Delany describes an identity system that includes a user manager. *Id.* ¶ 107. The user manager handles functions concerning user identities and access privileges, including creation and deletion of user identity profiles, modification of user identity profile data, determination of access privileges, and credentials management of passwords and digital certificates. *Id.* ¶ 108. Individual users can add themselves to a group, modify their personal and professional information, and change information in their identity profiles that can determine their access rights. *Id.* ¶ 109.

3. Analysis

a. Independent Claim 1

With respect to independent claim 1, we address the parties’ arguments in turn.

As discussed above, claim 1 is directed to a user-authentication service. Petitioner relies primarily on Vandergeest. For example, claim 1 recites “one or more computer systems” that the preamble describes as being “interconnected by two or more communications media with both an authentication-service client, and a user.” Petitioner directs us to Figure 3 of Vandergeest, which is reproduced below. Pet. 55.

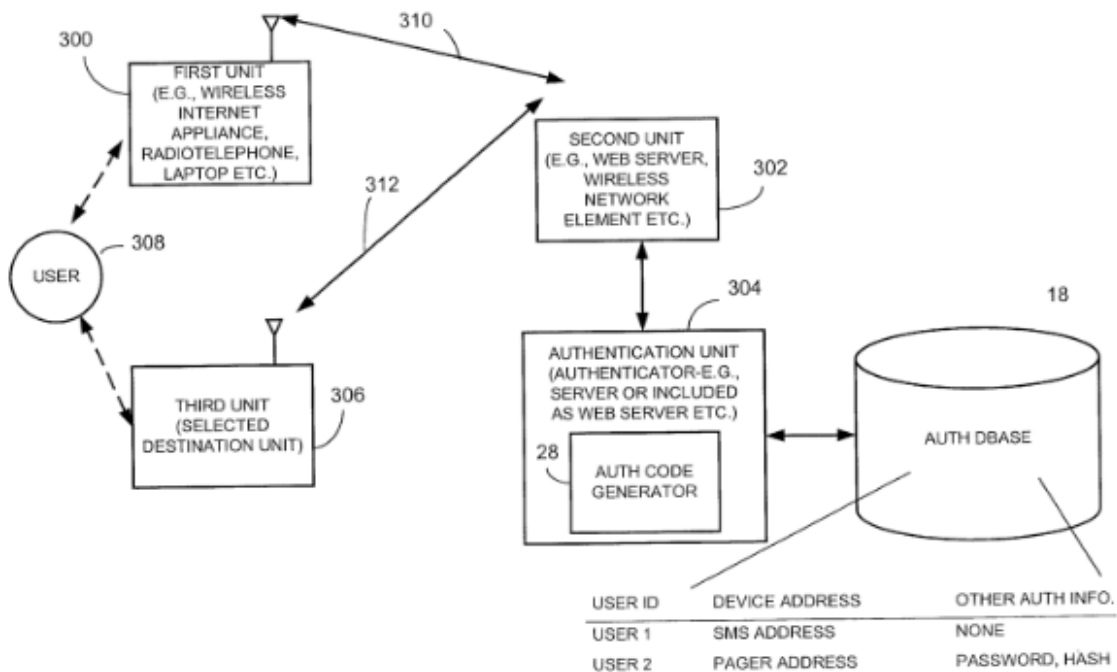


FIG. 3

Figure 3 shows a user authentication system with first unit 300, second unit 302, authenticator 304, authentication database 18, and third unit 306. Ex. 1005, 6:58–60. The system also includes user 308. *Id.* at Fig. 3.

Vandergeest teaches that the first, second, and third units are wireless devices. *Id.* at 6:66–7:5. Petitioner identifies Vandergeest’s second unit 302 as an “authentication-service client,” and points out that Vandergeest’s first and third units “represent different user-controlled devices.” Pet. 55 (citing Ex. 1005, 3:30–37). Petitioner further contends that “the units disclosed by *Vandergeest* are interconnected through a plurality of communication channels (i.e., communications media),” including primary wireless channel 310 and wireless back channel 312. *Id.* at 55–56. We are persuaded that Vandergeest teaches the recited “computer systems.”

Claim 1 further recites “stored user information.” For this limitation, Petitioner directs us to where Vandergeest teaches that “authentication database 18 stores, for a plurality of users, on a per-user basis, a user ID 24, associated password or hashed password 26 (if used) and destination unit data 22.” *Id.* at 59 (citing Ex. 1005, 4:31–40). We are persuaded that Vandergeest teaches the recited “stored user information.”

Claim 1 further recites an “account interface by which the user specifies, modifies, adds, and deletes user-authentication policies” that also are stored. For this limitation, Petitioner relies on both Vandergeest and Delany. Petitioner directs us to where Vandergeest describes a registration process during which the user provides information, such as destination unit data, that populates the authentication database. *Id.* at 59–60 (citing Ex. 1005, 4:38–61); *see also id.* at 57 (citing Ex. 1005, 4:34–35 (“[A]uthentication database 18 contains destination unit data 22 on a per user basis.”)). Petitioner contends that “[t]he destination unit data is a parameter of the authentication policy because it is used to carry [out] the authentication,” and that “[t]he user specifies a policy template, for example

the requirement of possession of a destination unit, during the registration process.” *Id.* at 57. According to Petitioner, “[t]he ‘destination unit data’ in combination with a policy template (e.g., send password to stored destination unit) is an authorization policy” that the user adds or specifies. *Id.* at 57, 60.

Although Petitioner contends that Vandergeest teaches adding and specifying user-authentication policies, Petitioner asserts that “Vandergeest does not specifically disclose the registration process includes routines by which the user can delete or modify existing policies.” *Id.* at 60 (emphases omitted). For this aspect of the limitation, Petitioner directs us to where Delany discusses “create, delete, and modify functions of user identity management.” *Id.* (citing Ex. 1007 ¶ 108). Delany teaches that individual users can add themselves to a user directory, modify their personal or professional information, such as addresses, and change information in their identity profiles that can determine their access rights. *Id.* at 61 (citing Ex. 1007 ¶ 109). According to Petitioner, an ordinarily skilled artisan “would have been motivated to combine the teachings of *Vandergeest* and *Delany* to incorporate the user-controlled account interface routines of *Delany* into the account management of *Vandergeest* to achieve predictable benefits.” *Id.* For example, Petitioner explains, “allowing users to delete policies would result in the predictable benefits of saving memory and ensuring there are no policies associated with old user devices that are no longer used/under the control of the user, thus increasing the security of the authentication procedure.” *Id.*

We are persuaded that the combination of Vandergeest and Delany teaches the recited “account interface.” We also determine that Petitioner’s

proffered reasoning for modifying Vandergeest's system to include the delete feature of Delany, namely, to keep policies current, is persuasive, as well as sufficient to support the legal conclusion of obviousness. *See In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (“[T]here must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.”). We find that Petitioner's same proffered reasoning (i.e., keeping policies current) supports modifying Vandergeest's system to include the modify feature of Delany as well.

Claim 1 further recites an “authentication interface by which . . . the authentication-service client submits an authentication request . . . to authenticate the user.” Claim 1 requires the authentication request to be made through a “first communications medium” or a “second communications medium” after the user initiates a transaction with the authentication-service client. For these limitations, Petitioner directs us to where Vandergeest teaches that “a user 308 may use the first unit 300 to contact the second unit 302 via primary wireless channel 310 wherein the second unit 302 has access-controlled resources requiring authentication.” Pet. 62 (citing Ex. 1005, 8:43–46). Vandergeest further teaches that second unit 302 prompts the user to enter authentication information via first unit 300, and then forwards the information (i.e., a user ID) to authenticator 304 through a “suitable communication link” so that authenticator 304 can determine whether the user is listed in the authentication database. Ex. 1005, 8:46–56. As discussed above, Petitioner identifies Vandergeest's second unit 302 as the “authentication-service client.” Pet. 62. Petitioner further identifies Vandergeest's primary channel 310 as a “first communications medium,” and Vandergeest's

“suitable communication link” between the second unit and the authenticator as a “second communications medium.” *Id.* According to Petitioner, “the authentication routines disclosed by *Vandergeest* include sending authentication information to the authentication unit through a second communications medium . . . to authenticate the user.” *Id.* at 63. We are persuaded that *Vandergeest* teaches the recited “authentication interface.”

Lastly, claim 1 recites a “variable-factor authentication . . . to authenticate the user . . . during which the user communicates with the user-authentication service through a third communications medium . . . and a user device.” Claim 1 requires the third communications medium to be different than the first and second communications media. Claim 1 also requires the user device to be different than the device that the user uses to initiate the transaction with the authentication-service client.

For these limitations, Petitioner directs us to where *Vandergeest* teaches that, if the user ID is listed in the database, authenticator 304 generates an authentication code for second unit 302 to send to the user’s third unit 306 over alternate or back channel 312. *Id.* at 64–65 (citing Ex. 1005, 8:63–67, 9:9–11, 13:61–64, Fig. 3); *see also* Ex. 1005, 9:16–20. Information about the user’s third unit 306, which is different than the user’s first unit 300, is stored in database 18. Ex. 1005, 4:35–38, 6:50–53 (*cited by* Pet. 65–66). The user obtains the code from third unit 306 and enters it into first unit 300, which returns the code to second unit 302 so that authenticator 304 can compare the returned code with the one it generated. *Id.* at 9:22–30. In sum, “an alternate channel is used during the session to provide authentication information in addition to user ID and/or password to provide multi-factor authentication.” *Id.* at 13:61–64. Petitioner identifies

Vandergeest’s authenticator 304 as part of a “user-authentication service.” See Pet. 64 (“the [authenticator] of *Vandergeest* corresponds to the ‘authentication service provider’ (ASP) of the ’213 Patent”).

We find that Vandergeest teaches the recited “variable-factor authentication.” As we stated in our Institution Decision (Inst. Dec. 22), this finding is consistent with the ’213 patent, which explains that variable-factor authentication may involve an authentication service provider communicating a password to a user through a cell phone during an electronic transaction over the Internet. Ex. 1001, 7:37–40; see also *id.* at 2:16–18 (“variable-factor authentication, in which the user, during the course of an authentication, provides both secret information as well as evidence of control of a tangible object”), 4:35–38 (“variable-factor authentication using randomly generated passwords sent via the user’s second cell phone and furnished by the user to ACME Bank during the transactions”).

In response, Patent Owner argues that the combination of Vandergeest and Delany does not teach or suggest the recited “variable-factor authentication,” which requires that “the user communicates with the user-authentication service through a third communications medium different from the first and second communications media.” PO Resp. 9 (citing Ex. 1001, claim 1). In particular, Patent Owner argues that Vandergeest (on which Petitioner relies for this limitation) does not teach the recited “third communications medium different from the first and second communications media” because Vandergeest “uses the alleged second communications medium—that is, the ‘suitable communication link’ between the second unit 302 and the authenticator 304—to both submit the

authentication request to the authenticator 304, and to receive the authentication code to send to the user's third unit as part of the authentication process." *Id.* at 16; *see also id.* at 20 ("[I]n Vandergeest the *different* communication medium is missing."). According to Patent Owner, "[s]uch multiple use of a communication medium is forbidden by claim 1" because "to be different the third communications medium cannot be the same communication medium that the authentication-service client uses to submit the authentication request." *Id.* at 17, 20. Referring to the '213 patent, Patent Owner contends that "one purpose of the *different* third communications medium . . . is to separate ASP-user communications from those passing through the authentication-service client" so that "authentication codes passed between the authentication service and the user are kept secret." *Id.* at 18 (citing Ex. 1002, 2:57–67, 3:20–25⁶). Patent Owner further contends that "[r]eading Vandergeest's 'suitable communication link' between the second unit 302 and the authenticator 304 as the third communications medium, as proposed by Petitioner, defeats this purpose." *Id.* at 18–19.

We disagree with Patent Owner. Claim 1 requires that the authentication-service client submit the authentication request through the first communications medium or the second communications medium. Claim 1 additionally requires that the user communicate with the user-authentication service through the third communications medium, which is different than the first and second communications media. As

⁶ Although Patent Owner cites portions of Exhibit 1002, we believe Patent Owner intended to cite instead the same portions of Exhibit 1001, which include the relevant language.

discussed above, Petitioner identifies Vandergeest’s second unit 302 as the recited “authentication-service client,” Vandergeest’s authenticator 304 as the recited “user-authentication service,” Vandergeest’s primary channel 310 as the recited “first communications medium,” Vandergeest’s “suitable communication link” between second unit 302 and authenticator 304 as the recited “second communications medium,” and Vandergeest’s back channel 312 as the recited “third communications medium.” To illustrate, Figure 3 of Vandergeest is reproduced below.

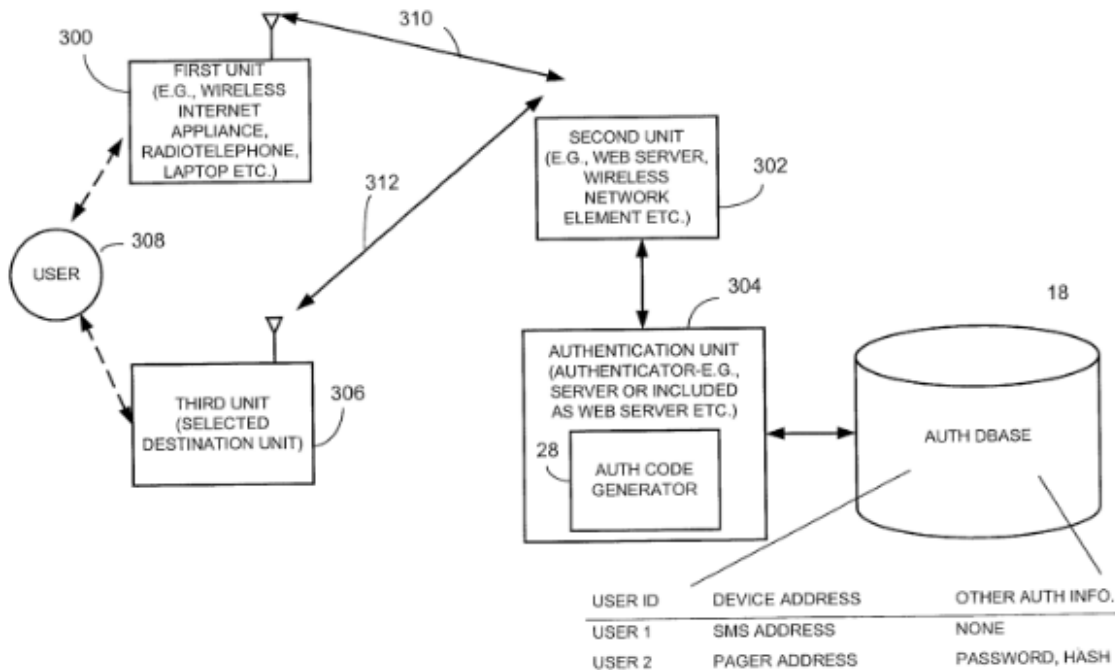


FIG. 3

Figure 3 is a diagram of a system for providing user authentication. Ex. 1005, 2:64–65. Vandergeest teaches that second unit 302 (i.e., the recited “authentication-service client”) submits an authentication request through a suitable communication link (i.e., the recited “second communications medium”), and that the user communicates with

authenticator 304 (i.e., the recited “user-authentication service”) through the suitable communication link as well as back channel 312 (i.e., the recited “third communications medium”). *Id.* at 8:52–63, Fig. 3.

The parties do not dispute that the user and authenticator 304 in Vandergeest communicate with each other using back channel 312. *See* Tr. 43:22–44:2 (Patent Owner stating, “The authentication code generator of the authentication unit produces the code. It passes that code back to the second unit over the same suitable communication link. And then the second unit transmits the code to the user’s third unit over the back channel 312.”). Nor do they dispute that Vandergeest’s suitable communication link and back channel 312 are different. *See* Tr. 45:10 (with respect to Vandergeest’s suitable communication link and back channel 312, Patent Owner stating that “[t]here are two media”). Rather, they dispute whether communications between the user and authenticator 304 using both the suitable communication link and back channel 312 fall within the scope of the claim, where the suitable communication link is also used by second unit 302 for submitting an authentication request. *See* Pet. Reply 7–11; Tr. 12:14–16 (Petitioner arguing that “the claim must have been written to have something like saying that you can only use the third communication medium which is different than the first and second medium”), 43:11–13 (Patent Owner arguing that “you cannot be different, you cannot be distinct, you cannot be another if, in fact, you are even in part the same”). We find that they do. The claim language does not limit communications between the user and the user-authentication service to communications through a single communications medium. *See* Ex. 1001, claim 1 (reciting “the user communicates with the user-authentication service through *a* third

communications medium”) (emphasis added). Thus, although the user communicates with authenticator 304 through the suitable communication link, it is the user’s communication with authenticator 304 through back channel 312 that satisfies the recited “third communications medium.”

As for Patent Owner’s argument regarding secrecy, we also disagree. Patent Owner contends that “[r]eading Vandergeest’s ‘*suitable communication link*’ between the second unit 302 and the authenticator 304 as the third communications medium, as proposed by Petitioner, defeats this purpose [of secrecy].” *Id.* at 18–19 (emphasis added). Petitioner, however, identifies Vandergeest’s *back channel 312* as the recited “third communications medium.” Patent Owner’s argument therefore does not adequately address Petitioner’s showing that Vandergeest’s back channel 312 teaches the recited “third communications medium.”

Nevertheless, we recognize Patent Owner’s point that the authentication code in Vandergeest is communicated through the suitable communication link between authenticator 304 (i.e., the recited “authentication service”) and second unit 302 (i.e., the recited “authentication-service client”). Even if the ’312 patent may have a purpose of keeping secret the authentication code, however, we find that such purpose stems from a concern about “electronic eavesdropping devices,” not a concern about the authentication-service client. *See* Ex. 1001, 1:54–55 (“[L]oss of user information to various electronic eavesdropping devices[] and other such events can quickly spell disaster for a user.”). Indeed, the ’312 patent teaches that “[t]he ASP interacts with the user in order to carry out authentications, *on behalf of ASP clients*.” *Id.* at 3:20–23 (emphasis added); *see also id.* at 7:50–56 (“In alternative embodiments, the ASP can

proactively push information to ASP clients so that authentication routines running on the ASP clients, using information provided beforehand by the ASP, may carry out all or a portion of the authentication process.”) (*cited by* Pet. Reply 12).

In view of the foregoing, we determine that Petitioner has demonstrated by a preponderance of the evidence that independent claim 1 would have been obvious over Vandergeest and Delany.

b. Dependent Claims 2–10

Claim 2 depends from claim 1 and recites that “the authentication service stores user-authentication policies and user information for multiple users, provides an account interface to the multiple users, and provides an authentication interface to multiple authentication-service clients.” For this limitation, Petitioner directs us to where Vandergeest teaches that “[t]he authentication database 18 stores, for a plurality of users, on a per-user basis, a user ID 24, associated password or hashed password 26 (if used) and destination unit data 22,” and that “[t]he authentication database 18 may be populated based on a registration process.” Pet. 66 (citing Ex. 1005, 4:38–39⁷); *see also* Ex. 1005, Fig. 3. Petitioner also directs us to where Vandergeest teaches that, “during a registration process, a user registers with the authentication unit [(i.e., “authentication service)].” Pet. 66 (citing Ex. 1005, 4:57–58). Lastly, Petitioner directs us to where Vandergeest

⁷ Petitioner cites Exhibit 1005, at column 4, lines 38 through 40. Pet. 66. We believe that Petitioner intended also to include lines 35 through 38 of column 4, which contain some of the language referred to in the Petition. *See id.*

teaches that the second unit (i.e., “authentication-service client”) may be “any other unit that has access to an authentication unit,” and contends that “it would have been obvious to a [person of ordinary skill in the art] to have multiple ‘second unit[s]’ that have access to the authentication service because having one authentication service for multiple clients would provide the predictable benefit of being more efficient (as opposed to a separate authentication service for each client).” *Id.* at 67. Patent Owner does not present separate arguments with respect to claim 2. *See* PO Resp. 21. Based on Petitioner’s argument and supporting evidence, as summarized above, we are persuaded that Vandergeest teaches the recited “authentication service.” *See* Ex. 1005, 4:35–39, 4:57–58, Fig. 3.

We further determine that Petitioner’s proffered reasoning for modifying Vandergeest’s system to include multiple second units, namely, to maximize system efficiency, is persuasive, as well as sufficient to support the legal conclusion of obviousness. *See Kahn*, 441 F.3d at 988. In addition, we determine that Petitioner’s proffered reasoning for combining Vandergeest and Delany with respect to independent claim 1, as discussed above, applies to dependent claim 2 as well.⁸

Claim 3, which also depends from claim 1, recites that “the user-authentication service undertakes the authentication procedure by” performing three steps. The first recited step is “using the electronically-encoded information about the user to retrieve all stored user-authentication policies for the user.” The second recited step is “conducting the authentication procedure in order to authenticate the user to the

⁸ We determine that this proffered reasoning also applies to the other dependent claims described below.

authentication-service client,” where “the retrieved stored user-authentication policies permit the authentication procedure to proceed.” The third recited step is “returning an authentication result to the authentication-service client.”

For the first recited step—that is, the “using” step—Petitioner directs us to where Vandergeest teaches “determining, based on a received user ID, which destination unit, other than the first unit 300, will receive an authentication code via the wireless back channel 312.” Pet. 68 (citing Ex. 1005, 8:57–60). As discussed above with respect to claim 1, Petitioner explains that “[t]he destination unit data is a parameter of the authentication policy because it is used to carry [out] the authentication,” and that “[t]he user specifies a policy template, for example the requirement of possession of a destination unit, during the registration process.” *Id.* at 57. Petitioner further explains that Figure 3 of Vandergeest shows that “each user has one stored policy in the authentication database (including user’s device address and other authentication information); thus by retrieving the policy, the system has retrieved *all* stored policies for that user.” *Id.* at 69–70 (citing Ex. 1005, Fig. 3).

For the second and third recited steps in claim 3—that is, the “conducting” and “returning” steps—Petitioner directs us to where Vandergeest teaches:

[O]ne destination unit, namely the third unit 306, has been designated by a destination unit identifier 22. This identifier provides sufficient information in order to allow the third unit 306 to be communicated to from the second unit 302. . . . [T]he generated authentication code as generated by the authentication code generator 28 . . . is sent via a wireless alternate channel 312 to a unit other than the first unit 300 [(i.e.,

the third unit)]. The authentication code is then provided to the user 308 via an audible or visual display associated with the third unit. The user through the user interface on the first unit, then inputs the authentication code into the first unit. The authentication code is then resent by the first unit to the second unit via the primary channel 310. The second unit 302 passes the resent authentication code to the authentication unit 304 where the authentication unit 304 compares the resent authentication code with the authentication code that was sent to the third unit 306. If they match, the user (i.e. first unit) is granted access.

Pet. 70–71 (citing Ex. 1005, 7:12–34, Fig. 4); *see also* Ex. 1005, Fig. 3.

Petitioner contends that, “because the user is granted access to the resources, authentication results must have been returned to the second [unit].” *Id.* at 71 (citing Ex. 1005, 9:30–31).

Patent Owner does not present separate arguments with respect to claim 3. *See* PO Resp. 21. Based on Petitioner’s argument and evidence, as summarized above, we are persuaded that Vandergeest teaches the “user-authentication service” recited in claim 3.

Claim 4 depends from claim 3 and recites that the authentication procedure for a single policy comprises “a uni-directional or bi-directional exchange of information with the user through the third communications medium.” For this limitation, Petitioner contends that Vandergeest’s “authentication unit sends secondary authorization information to the user over a ‘back channel’ (i.e., third communications medium) and then the user resends the information back to the second device over the original communications medium, thus comprising a uni-directional exchange of information over the back channel.” Pet. 73 (citing Ex. 1005, 4:10–55, Fig. 1). Patent Owner does not present separate arguments with respect to claim 4. *See* PO Resp. 21. Petitioner’s argument and evidence, as

summarized above, persuade us that Vandergeest teaches the recited “authentication procedure.”

Claim 5, which depends from claim 4, recites that “the information is a password that the user can subsequently input to the authentication-service client to prove to the authentication-service client that the user has been authenticated by the user-authentication service.” For this limitation, Petitioner directs us to where Vandergeest teaches:

The first unit returns the authentication code obtained as received by the third unit back to the second unit via the primary wireless channel as shown in block 412. The authenticator, as shown in block 414, authenticates the user using the returned authentication code that was sent via the primary channel with the authentication code sent via the back channel. If they correlate, the user is authenticated and proceeds to use the appropriate resources via the second unit 302.

Pet. 75–76 (citing Ex. 1005, 9:24–32). Petitioner further contends that Vandergeest’s “‘authentication code’ is merely a password because it represents a short alpha-numeric secret used to gain access to something.” Petitioner relies on the declaration testimony of Mr. Gray. *Id.* (citing Ex. 1003 ¶ 113). Patent Owner does not present separate arguments with respect to claim 5. See PO Resp. 21. We agree with Petitioner’s showing that Vandergeest teaches the recited “information.”

Claim 6, which depends from claim 5, recites that “the authentication result includes the password.” For this limitation, Petitioner directs us again to where Vandergeest teaches that the first unit sends the authentication code obtained from the third unit to the second unit, which forwards the code to the authenticator, which then compares the forwarded code with the code that the authenticator sent to the third unit. Pet. 76 (citing Ex. 1005, 7:28–

34, 9:24–32). Petitioner contends that, “[a]lthough *Vandergeest* does not explicitly say that the authentication result includes the password . . . , it would have been obvious to include the code within the authentication result because the code itself is what authenticates the user.” *Id.* at 76–77. Patent Owner does not present separate arguments with respect to claim 6. *See* PO Resp. 21. We determine that Petitioner’s argument and evidence establish that *Vandergeest* teaches the recited “authentication result,” and that Petitioner’s proffered reasoning for modifying *Vandergeest*’s system to include the authentication code as part of an authentication result, namely, to provide proof that the user is authenticated, is persuasive and sufficient to support the legal conclusion of obviousness. *See Kahn*, 441 F.3d at 988.

Claim 7 depends from claim 1 and recites that “the stored user information includes one or more of: . . . the user’s address; passwords specified by the user; the user’s contact information;” For this limitation, Petitioner directs us to where *Vandergeest* teaches that “the authentication database 18 stores, for a plurality of users, on a per-user basis, a user ID 24, associated password or hashed password 26 (if used) and destination unit data 22.” Pet. 77 (citing Ex. 1005, 4:34–40). Petitioner contends that *Vandergeest*’s associated password or hashed password 26 corresponds to the recited “passwords specified by the user.” *Id.* Petitioner also contends that *Vandergeest*’s destination unit data 22 corresponds to the recited “user’s address” and the recited “user’s contact information.” *Id.* Patent Owner does not present separate arguments with respect to claim 7. *See* PO Resp. 21. Based on Petitioner’s argument and supporting evidence, we are persuaded that *Vandergeest* teaches the recited “stored user information.”

Claim 8, which depends from claim 7, recites that “the user’s contact information includes one or more of: the user’s computer’s trusted communications addresses; trusted telephone numbers of the user’s landline and cell phones; contact information for the user’s trusted hand-held computing devices;” As discussed above with respect to claim 7, Petitioner contends that Vandergeest’s destination unit data 22 corresponds to the recited “user’s contact information.” Petitioner further directs us to where Vandergeest teaches that the destination unit data “provides sufficient information in order to allow the third unit 306 to be communicated to.” Pet. 78 (citing Ex. 1005, 7:12–16). In addition, Petitioner directs us to Figure 3 of Vandergeest, which shows that the address for the third unit can be an SMS address or a pager address. *Id.* (citing Ex. 1005, Fig. 3). According to Petitioner, these addresses correspond to the recited “contact information for the user’s trusted hand-held computing devices.” *Id.* We note that Vandergeest additionally teaches that “[t]he third unit 306 is . . . a wireless device, such as a pager, cell phone, PDA or other device that communicates with the second unit 302 over a wireless back channel 312, such as an SMS channel or other suitable channel.” Ex. 1005, 7:1–5. Patent Owner does not present separate arguments with respect to claim 8. See PO Resp. 21. We agree with Petitioner’s showing, summarized above, that Vandergeest teaches the recited “user’s contact information.”

Claim 9 depends from claim 1 and recites “a user-authentication policy specifies one or more of: constraints and parameters associated with user-authentication processes carried out by the user-authentication service on behalf of one or more, specified authentication-service clients.” For this limitation, Petitioner asserts that “*Vandergeest* discloses that the

user-authentication policy specifies which password or third device (i.e., different user device) must be in possession of the user and must be utilized as part of the user-authentication process for a specific authentication-service client.” Pet. 79 (citing Ex. 1005, 4:31–40, 8:63–67, Figs. 3–4). Petitioner contends that “[t]hese requirements, such as utilizing a specific password or specific third-device, are examples of constraints and parameters associated with user-authentication processes because they represent the substance of the authentication policies.” *Id.* Patent Owner does not present separate arguments with respect to claim 9. See PO Resp. 21. In light of Petitioner’s argument and evidence, we find that Vandergeest teaches the recited “user-authentication policy.”

Lastly, claim 10, which depends from claim 9, recites that the “constraints include one or more of: . . . communications-medium-related constraints; . . . and event constraints.” For this limitation, Petitioner contends that “*Vandergeest* discloses that a user can implement a ‘communications-medium related’ constraint based on the particular type of third unit that they register” by, for example, “register[ing] a cell phone that communicates via an ‘SMS channel’ or a pager that communicates via a ‘pager network.’” Pet. 80 (citing Ex. 1005, 7:1–5, 9:1–8). Petitioner additionally contends that “*Vandergeest* also discloses an ‘event constraint,’ such as requiring that the authentication code input happens within a certain period of time (i.e., the event must happen in a certain period of time).” *Id.* (citing Ex. 1005, 6:19–22). Patent Owner does not present separate arguments with respect to claim 10. See PO Resp. 21. We agree with Petitioner’s showing that Vandergeest teaches the recited “constraints.”

In view of the foregoing, we determine that Petitioner has demonstrated by a preponderance of the evidence that dependent claims 2–10 would have been obvious over Vandergeest and Delany.

D. Obviousness over Vandergeest: Claims 12–17

Petitioner argues that claims 12–17 of the '213 patent would have been obvious over Vandergeest. Pet. 81–86. Patent Owner does not respond to Petitioner's argument in this regard. *See generally* PO Resp. For the reasons explained below, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 12–17 would have been obvious over Vandergeest.

1. Independent Claim 12

Independent claim 12, which is directed to a method for authenticating, recites three steps. The first recited step is “receiving user-identifying information from the authentication-service client.” For this limitation, Petitioner identifies Vandergeest's second unit 302 as an “authentication-service client.” Pet. 81. Petitioner further directs us to where Vandergeest teaches that “[t]he second unit 302 contacts the authenticator 304 via a suitable communication link or bus, and passes the sent primary authentication information, namely the sent user ID, so that the authentication unit can determine if the user is listed in the authentication database 18.” *Id.* (citing Ex. 1005, 8:52–56). We find that Vandergeest's user ID corresponds to the recited “user-identifying information.” Accordingly, we are persuaded that Vandergeest teaches the recited “receiving” step.

The second step recited in claim 12 is “using the [received] user-identifying information . . . to authenticate the user of the authentication service by sending information to the user . . . through a communications medium different from the first communications medium.” According to the preamble of claim 12, the authentication-service client and the user communicate through a first communications medium. For these limitations, Petitioner identifies Vandergeest’s primary channel 310 as a “first communications medium.” See Pet. 81 (citing Ex. 1005, 8:43–46). Petitioner also identifies Vandergeest’s back channel 312 as a “communications medium different from the first communications medium.” *Id.* at 82. Petitioner explains that Vandergeest teaches using the user ID (i.e., the recited “user-identifying information”) to determine which destination unit should receive an authentication code. Pet. 82 (citing Ex. 1005, 8:56–60). Once determined, second unit 302 (i.e., the recited “authentication-service client”) sends the authentication code to the destination unit (i.e., third unit 306) through wireless back channel 312. Ex. 1005, 9:16–18, Fig. 3. The user then obtains the code from the destination unit and enters it into first unit 300, which returns the obtained code to second unit 302 through primary wireless channel 310 so that authenticator 304 can authenticate the user with the returned authentication code. *Id.* at 9:19–32, Figs. 3–4. We are persuaded by Petitioner’s showing that Vandergeest teaches the recited “using” step.

Lastly, the third step recited in claim 12 is “returning a[n] authentication result to the authentication-service client.” As discussed above, the user in Vandergeest obtains an authentication code from the destination unit and enters it into first unit 300, which returns the obtained

code to second unit 302 through primary wireless channel 310 so that authenticator 304 can authenticate the user with the returned authentication code. *Id.* at 9:19–32, Figs. 3–4. If the user is authenticated, the user may proceed to use the appropriate resources via second unit 302. *Id.* at 9:30–32. Petitioner contends that, “because the user is granted access to the resources, authentication results must have been returned to the second [unit].” Pet. 71 (cross-referenced by Pet. 84). In light of this argument and evidence, we are persuaded that Vandergeest teaches the recited “returning” step.

As we mentioned above, Patent Owner does not respond to Petitioner’s argument that independent claim 12 would have been obvious over Vandergeest. *See generally* PO Resp. Accordingly, in view of the foregoing, we determine that Petitioner has demonstrated by a preponderance of the evidence that claim 12 would have been obvious over Vandergeest.

2. *Dependent Claims 13–17*

Claim 13 depends from claim 12 and recites that, “as part of the authentication procedure, the authentication service transmits information to the user of the authentication service which the user of the authentication service then subsequently transmits to the authentication-service client.” For this limitation, Petitioner contends that Vandergeest teaches that “the authentication unit sends secondary authorization information to the user over a ‘back channel’ . . . and then the user resends the information back to the second device.” Pet. 85 (citing Ex. 1005, 4:10–55, Fig. 1). With respect to the embodiment shown in Figure 1, Vandergeest teaches sending an authentication code (which serves as secondary authentication information)

generated by authentication code generator 28 via an alternate channel to the user who then returns the code that was sent via the alternate channel to the second unit via a primary channel. Ex. 1005, 5:8–12, 5:33–49, Fig. 1; *see also id.* at 7:19–29 (in an alternative embodiment, similarly sending an authentication code to the user who then returns the code to the second unit), Fig. 3. We are persuaded by Petitioner’s argument and evidence that Vandergeest teaches the recited “authentication procedure.”

Claim 14 also depends from claim 12 and recites that “the user-authentication service undertakes the authentication procedure by” performing three steps. The first recited step is “using the electronically-encoded information about the user to retrieve all stored user-authentication policies for the user.” The second recited step is “conducting the authentication procedure in order to authenticate the user to the authentication-service client,” where “the retrieved stored user-authentication policies permit the authentication procedure to proceed.” The third recited step is “returning the authentication result to the authentication-service client.” Petitioner asserts that these limitations are similar to those recited in claim 3, and therefore relies on its argument that claim 3 would have been obvious over Vandergeest and Delany. Pet. 86. For the reasons discussed above, we are persuaded that Vandergeest teaches the recited “user authentication service.” *See supra* Section III.C.3.b.

Claim 15, which depends from claim 14, recites that the authentication procedure for a single policy comprises “a uni-directional or bi-directional exchange of information with the user through the third communications medium.” Petitioner asserts that this limitation is similar to the one recited in claim 4, and therefore relies on its argument that claim 4

would have been obvious over Vandergeest and Delany. Pet. 86. For the reasons discussed above, we are persuaded that Vandergeest teaches the recited “authentication procedure.” *See supra* Section III.C.3.b.

Claim 16, which depends from claim 15, recites that “the information is a password that the user can subsequently input to the authentication-service client to prove to the authentication-service client that the user has been authenticated by the user-authentication service.”

Petitioner asserts that this limitation is similar to the one recited in claim 5, and therefore relies on its argument that claim 5 would have been obvious over Vandergeest and Delany. Pet. 86. For the reasons discussed above, we are persuaded that Vandergeest teaches the recited “information.” *See supra* Section III.C.3.b.

Lastly, claim 17, which depends from claim 16, recites that “the authentication result includes the password.” Petitioner asserts that this limitation is similar to the one recited in claim 6, and therefore relies on its argument that claim 6 would have been obvious over Vandergeest and Delany. Pet. 86. For the reasons discussed above, we are persuaded that Vandergeest teaches the recited “authentication result.” *See supra* Section III.C.3.b.

As discussed above, Patent Owner does not respond to Petitioner’s arguments that dependent claims 13–17 would have been obvious over Vandergeest. *See generally* PO Resp. Accordingly, in view of the foregoing, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 13–17 would have been obvious over Vandergeest.

IV. CONCLUSION

For the foregoing reasons, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1–10 of the '213 patent are unpatentable under 35 U.S.C. § 103 as obvious over Vandergeest and Delany, and that claims 12–17 are unpatentable under 35 U.S.C. § 103 as obvious over Vandergeest.

Petitioner has not shown by a preponderance of the evidence that claim 11 is unpatentable.

V. ORDER

In consideration of the foregoing, it is hereby

ORDERED that claims 1–10 and 12–17 of the '213 patent are held *unpatentable*;

FURTHER ORDERED that claim 11 of the '213 patent has not been shown to be unpatentable; and

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

IPR2017-02047
Patent 8,082,213 B2

PETITIONER:

Roshan Mansinghani
Jonathan Stroud
UNIFIED PATENTS INC.
roshan@unifiedpatents.com
jonathan@unifiedpatents.com

PATENT OWNER:

Tarek N. Fahmi
Jason LaBerteaux
ASCENDA LAW GROUP, PC
tarek.fahmi@ascendalaw.com
jason.laberteaux@ascendalaw.com