

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DUO SECURITY INC., CENTRIFY CORPORATION, and
TRUSTWAVE HOLDINGS, INC.,
Petitioner,

v.

STRIKEFORCE TECHNOLOGIES, INC.,
Patent Owner.

Case IPR2017-01064
Patent 8,484,698 B2

Before KERRY BEGLEY, KIMBERLY MCGRAW, and
JOHN A. HUDALLA, *Administrative Patent Judges*.

BEGLEY, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Duo Security Inc., Centrifly Corporation, and Trustwave Holdings, Inc. (collectively, “Petitioner”) filed a Petition requesting *inter partes* review of claims 1–17, 19–24, 53, and 54 of U.S. Patent No. 8,484,698 B2 (Ex. 1001, “’698 patent”). Paper 2 (“Pet.”). StrikeForce Technologies, Inc. (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

Pursuant to 35 U.S.C. § 314(a), an *inter partes* review may not be instituted unless “the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” Having considered the Petition and the Preliminary Response, we determine that the information presented does not show that there is a reasonable likelihood that Petitioner would prevail in establishing the unpatentability of any of the challenged claims of the ’698 patent. Thus, for the reasons given below, we deny institution of an *inter partes* review.

I. BACKGROUND

A. RELATED MATTERS

The parties represent that the ’698 patent is the subject of numerous ongoing and completed actions before various district courts. Paper 3, 2–3; Pet. 6. In actions before the U.S. District Court for the District of New Jersey, Patent Owner alleges that Petitioner infringes the ’698 patent (Case Nos. 2:16-cv-03571, 2:16-cv-03573, and 2:16-cv-03574). Paper 3, 2; Pet. 6.

In addition, before the Office, the ’698 patent also is the subject of IPR2017-01041, filed by Petitioner. Pet. 6–7; Paper 3, 2.

B. THE ’698 PATENT

The ’698 patent is directed to security systems that provide user authentication. Ex. 1001, 1:20–25. According to the ’698 patent, prior art authentication systems typically are in-band systems in which data and authentication information are exchanged on a single channel. *Id.* at 2:31–3:14, 5:63–6:12, Fig. 1. To increase security, the ’698 patent instead implements an out-of-band system with “an authentication channel that is separated from the [access] channel carrying the information . . . for actual information transfer.” *Id.* at 3:14–20, 4:52–57, 6:9–23; *see id.* at 1:20–25.

In particular, the '698 patent discloses a multichannel, out-of-band security system for granting or denying access to a host computer in response to a user's access request. *Id.* at [57], 4:34–36. In the first authentication factor, the user seeking access to the host computer presents user identification and password data over an access channel. *Id.* at [57], 4:36–39. This information is intercepted and transmitted to a security computer, which verifies the information. *Id.* at [57], 4:35–36. Next, in the second authentication factor, the security computer communicates with the user through a peripheral device, such as a telephone, within a separate authentication channel. *Id.* at [57], 4:39–42. The security computer authenticates the user via a password entered on the telephone keypad and may further authenticate the user using a biometric system, which controls access based on “characteristics of the human body,” such as fingerprints or voice. *Id.* at [57], 2:13–17, 4:39–46, 6:47–59. Upon obtaining a match, the security computer instructs the host computer to grant access. *Id.* at [57].

One embodiment of the disclosed security system is illustrated in Figure 1A, reproduced below. *Id.* at 5:17–20, 6:30–33, Cert. of Corr.

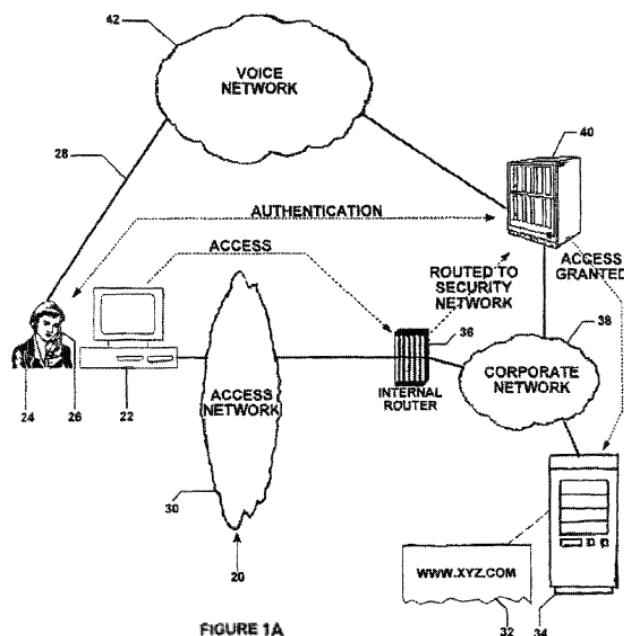


Figure 1A depicts first embodiment 20 applied to a wide area network, such as the Internet, where the user seeking access and its equipment are remote from the host computer. *Id.* at 5:17–20, 6:14–18, 6:30–33; *see id.* at 5:43–45, 6:34–59, 9:10–12:26, Figs. 9A–E. In access network 30, user 24 using remote computer 22 requests access to web page 32 located at host computer 34. *Id.* at 6:33–40, 9:24–27. In the first authentication factor, host computer 34 requests a login procedure in which the user is prompted to enter a user identification and password. *Id.* at 9:27–33. After the user enters this information, router 36, internal to corporate network 38, diverts the information to out-of-band security network 40 containing security computer 52, where authentication occurs. *Id.* at 6:40–42, 6:60–66, 9:33–35. Security computer 52 verifies the password using stored password information. *Id.* at 9:36–54; *see id.* at 7:11–25. Upon verification, security computer 52 sends a verification message to host computer 34, which transmits the message to remote computer 22. *Id.* at 9:55–10:19, Fig. 9B.

In the second authentication factor, security computer 52 initiates an out-of-band telephone call to user 24. *Id.* at 6:35–37, 10:20–30. When the user answers telephone 26, security computer 52 retrieves and plays for the user a prompt to enter a dual tone multi frequency (“DTMF”) password on the telephone keypad. *Id.* at 10:30–48, 15:50–55, 17:19–20. Security computer 52 verifies the DTMF password entered by the user. *Id.* at 10:48–65. Security computer 52 then retrieves and plays for the user a prompt for a speech password. *Id.* at 11:10–37. Using voice recognition technology, security computer 52 verifies that the speech password received from user 24 has the same pattern as a previously stored sample of the user’s speech pattern. *Id.* at 11:26–30, 11:37–42; *see id.* at 6:47–59. After verifying that the stored and received speech patterns match, security

computer 52 informs the user that access is granted and sends an authentication message to host computer 34. *Id.* at 11:57–12:24. Host computer 34 then grants access to the authenticated user. *Id.* at 12:24–26.

C. ILLUSTRATIVE CLAIM

Of the challenged claims, claims 1, 53, and 54 of the '698 patent are independent. Claim 1, reproduced below, is illustrative:

1. A software method for employing a multichannel security system to control access to a computer, comprising the steps of:
 - receiving at an interception device in a first channel a login identification demand to access a host computer also in the first channel;
 - verifying the login identification;
 - receiving at a security computer in a second channel the demand for access and the login identification;
 - outputting from the security computer a prompt requesting transmission of data;
 - receiving the transmitted data at the security computer;
 - comparing the transmitted data to predetermined data; and
 - depending on the comparison of the transmitted and the predetermined data, outputting an instruction from the security computer to the host computer to grant access to the host computer or deny access thereto.

Ex. 1001, 14:30–46.

D. EVIDENCE OF RECORD

The Petition relies upon the following asserted prior art references: U.S. Patent No. 5,699,513 (issued Dec. 16, 1997) (Ex. 1003, “Feigen”); U.S. Patent No. 5,668,876 (issued Sept. 16, 1997) (Ex. 1005, “Falk”); and European Patent Application Publication No. 0444351 A2 (published Sept. 4, 1991) (Ex. 1102, “Flanagan”).

In addition, Petitioner supports its contentions with the Declaration of Patrick McDaniel, Ph.D. (Ex. 1101).

E. ASSERTED GROUND OF UNPATENTABILITY

Petitioner asserts that claims 1–17, 19–24, 53, and 54 of the ’698 patent are unpatentable under 35 U.S.C. § 103¹ as obvious over Feigen, Flanagan, and Falk. Pet. 10.

II. ANALYSIS

A. CLAIM CONSTRUCTION

The Board interprets claim terms of an unexpired patent using the “broadest reasonable construction in light of the specification of the patent.” 37 C.F.R. § 42.100(b); *see Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016) (upholding the use of the broadest reasonable interpretation standard). We presume a claim term carries its “ordinary and customary meaning,” which is the meaning “the term would have to a person of ordinary skill in the art” at the time of the invention. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007) (citation omitted).

1. “*biometric analyzer*” (claims 10 and 11)

Petitioner argues that “biometric analyzer,” as recited in claims 10 and 11 of the ’698 patent, is a means-plus-function limitation governed by 35 U.S.C. § 112(6). Pet. 19. Specifically, Petitioner sets forth its proposed construction as follows:

biometric analyzer (claim 10, and all Challenged Claims depending therefrom) — This term is governed by 35 U.S.C. §112(6). Function: *analyzing a monitored parameter of the accessor*. Structure: *monitoring the particular parameter of the*

¹ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112–29, 125 Stat. 284, 287–88, 296–97 (2011), revised 35 U.S.C. § 103 as well as 35 U.S.C. § 112. Because the application that issued as the ’698 patent was filed before the effective date of the relevant sections of the AIA, we refer to the pre-AIA version of §§ 103 and 112 throughout this Decision.

individual person; including (sic) the parameter to a mathematical representation or algorithm therefore (sic); retrieving a previously stored sample (biometric data), (sic) thereof from a database and comparing the stored sample with the input of the accessor. See Ex. 1001 at 6:55-59.

Pet. 19 (instances of “(sic)” included by Petitioner); see Ex. 1101 ¶ 45.

Petitioner asserts this proposed construction is supported by its overview of the ’698 patent specification and prosecution history. Pet. 16; see *id.* at 10–15. Further, Petitioner represents that Petitioner “seeks to have” the U.S. District Court for the District of New Jersey adopt this construction in an ongoing related case. *Id.* at 6, 20. Petitioner also contends this proposal is “consistent with” constructions adopted by the U.S. District Court for the District of Delaware in a previous case involving the ’698 patent in which Petitioner was not a party. *Id.* at 20; see Ex. 1012, 39–42, 54; Ex. 1013, 1–3, 6. In its unpatentability analysis of claims 10 and 11, Petitioner argues that the asserted prior art, specifically Flanagan, describes the structure required in its proposed construction of “biometric analyzer.” Pet. 54–56. Patent Owner disputes Petitioner’s showing in this regard. Prelim. Resp. 56–60.

Claim 10 depends indirectly from independent claim 1 and additionally recites “receiving in a biometric analyzer the biometric signal.” Ex. 1001, 15:6–7. Claim 11, which further depends from claim 10, specifies that “the biometric analyzer comprises one of a voice recognition program, a fingerprint verification program, or both.” *Id.* at 15:8–10.

The U.S. Court of Appeals for the Federal Circuit has held that a claim term’s “[f]ailure to use the word ‘means’ . . . creates a rebuttable presumption” that 35 U.S.C. § 112(6) does not apply and, thus, that the term is not a means-plus-function limitation. *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1348 (Fed. Cir. 2015) (en banc). A patent challenger, such

as Petitioner, can overcome this presumption by showing that the claim term: (1) “fails to recite sufficiently definite structure,” or (2) “recites function without reciting sufficient structure for performing that function.” *Id.* at 1348–49 (quotations and citations omitted). The governing standard is “whether the words of the claim are understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure.” *Id.* Moreover, if § 112(6) applies and the term is a means-plus-function limitation, construction of the term requires: (1) “identif[ication of] the claimed function,” and (2) a determination of “what structure, if any, disclosed in the specification corresponds to,” i.e., is “clearly link[ed]” to or “associate[d]” with, the claimed function. *Id.* at 1351–52.

Our rules make clear that it is Petitioner’s burden to explain, in detail, how the challenged claim is to be construed with supporting factual and legal analysis. Specifically, 37 C.F.R. § 42.104(b)(3) requires the Petition to “set forth . . . [h]ow the challenged claim is to be construed” and for a means-plus-function limitation, to “identify the specific portions of the specification that describe the structure, material, or acts corresponding to each claimed function.” In addition, 37 C.F.R. § 42.22(a)(2) requires the Petition to include “[a] full statement of the reasons for the relief requested, including a detailed explanation of the significance of the evidence including material facts, and the governing law, rules, and precedent.”

Here, the Petition falls far short of these requirements of our rules by merely stating a bare conclusion that “biometric analyzer” is a mean-plus-function limitation pursuant to 35 U.S.C. § 112(6) and listing the alleged structure and function with one unexplained citation to the ’698 patent specification. Pet. 19. Claims 10 and 11 do not include the word “means,” yet Petitioner provides no analysis directed to rebutting the resulting

presumption, under governing Federal Circuit precedent, that § 112(6) is inapplicable. *See Williamson*, 792 F.3d at 1348–49. Nor does Petitioner provide any evidence, such as expert testimony, regarding whether an ordinarily skilled artisan would have understood “biometric analyzer” to have “sufficiently definite meaning as the name for structure.” *See id.*

Moreover, even if we were to conclude that “biometric analyzer” should be construed as a means-plus-function limitation, Petitioner’s analysis is insufficient. Petitioner offers no explanation regarding why the claimed function would be “analyzing a monitored parameter of the accessor,” as Petitioner proposes. Pet. 19 (emphasis omitted). Given that claim 10 recites only “receiving in a biometric analyzer the biometric signal,” it is unclear, on this record, how or why Petitioner’s proposed function comports with any claimed function. Ex. 1001, 15:6–7. In addition, as to the alleged corresponding structure, Petitioner’s general reference to the Petition’s entire synopsis of the specification and bald citation, without any analysis or explanation, to five lines of the specification, which do not refer to a “biometric analyzer,” are insufficient to address why or how this passage discloses structure that corresponds to any function recited in claims 10 and 11. *See id.* at 6:55–59; Pet. 16, 19 (citing Ex. 1001, 6:55–59); *see also* Pet. 10–15.

Furthermore, Petitioner’s references to asserted and adopted claim constructions in related district court cases are unpersuasive and inadequate to ameliorate the conclusory analysis in the Petition. First, Petitioner refers to the District of Delaware’s claim construction in a previous case involving the ’698 patent. The District of Delaware, however, did not construe the claim term “biometric analyzer” as recited in the ’698 patent. *See* Pet. 20; Ex. 1012, 39. Rather, the court construed the term as recited in *different*

claims of *different* patents related to the '698 patent, specifically claim 28 of U.S. Patent No. 7,870,599 B2 ("599 patent") and claim 7 of U.S. Patent No. 8,713,701 B2 ("701 patent"). *See* Ex. 1012, 1–2, 39, 54. Significantly, in contrast to claims 10 and 11 of the '698 patent at issue here, claim 28 of the '599 patent and claim 7 of the '701 patent expressly recite that the claimed "biometric analyzer" is "for analyzing a monitored parameter of [said]/[the] accessor"—which Petitioner inexplicably proposes as the function of the "biometric analyzer" in this case. *Id.* at 39; Ex. 1001, 15:6–10; Pet. 19. Second, Petitioner's representation that it has requested that the District of New Jersey adopt its proposed construction is of no persuasive value, particularly given that Petitioner does not represent that the court has adopted this construction, and did not include in the record the relevant claim construction briefing before the district court or any claim construction order by the court. *See* Pet. 20.

Therefore, Petitioner has not complied with the requirements of 37 C.F.R. §§ 42.22(a)(2) and 42.104(b)(3) with respect to the construction of "biometric analyzer," as recited in claims 10 and 11 of the '698 patent. Accordingly, we deny institution of *inter partes* review of claims 10 and 11 based on this deficiency in the Petition—in addition to the substantive defects in Petitioner's showing for these claims discussed below.

2. Other Claim Terms

Petitioner proffers numerous other claim terms for construction. Pet. 16–20. Patent Owner argues that no construction of these terms is necessary and contests Petitioner's proposed construction for some terms. *See* Prelim. Resp. 13–24. Based on our review of the record and the dispositive issues in our determination of whether to institute *inter partes* review, we determine that none of these terms requires an express

construction to resolve the issues presented by the patentability challenges.

See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc., 200 F.3d 795, 803 (Fed. Cir. 1999) (holding that only claim terms that “are in controversy” need to be construed and “only to the extent necessary to resolve the controversy”).

B. ALLEGED OBVIOUSNESS OVER FEIGEN, FLANAGAN, AND FALK

Petitioner argues claims 1–17, 19–24, 53, and 54 of the '698 patent would have been obvious over Feigen, Flanagan, and Falk. Pet. 34–64. Patent Owner disputes these assertions. Prelim. Resp. 24–62.

1. Overview of Feigen

Feigen provides an “improved method and apparatus for providing security for a communication network” through “user authentication.” Ex. 1003, 7:55–58; *see id.* at 1:5–13, 1:56–2:12, 7:57–67. In particular, Feigen provides security for inside network 14 via security host 26, which ensures that only users who are authentic and “authorized to do so may access application services residing on inside network 14.” *Id.* at [57], 2:57–3:3. Figure 1 of Feigen is reproduced below.

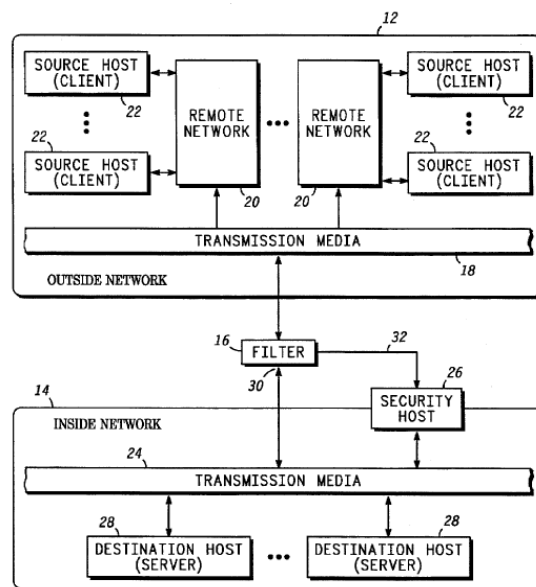


FIG. 1

Figure 1 depicts computer network environment 10 with inside network 14 and outside network 12, which preferably is the Internet. *Id.* at 2:20–23, 2:36–47. Outside network 12 features transmission media 18, coupled to remote networks 20, which contain source hosts 22 running client applications. *Id.* at 2:48–54. Inside network 14, in turn, features transmission media 24, which is coupled to filter 16, security host 26, and destination hosts 28. *Id.* at 2:61–64. Within inside network 14, a security service runs on security host 26 and application services run on destination hosts 28. *Id.* at 2:63–3:1, 3:16–18. Filter 16, located between outside network 12 and inside network 14, is “desirably . . . a conventional filtering device, such as a router, bridge, gateway, or the like.” *Id.* at 2:39–41, 3:3–9.

When a client application running on source host 22 in outside network 12 requests a connection, via a first connection request message, with an application service running on destination host 28 in inside network 14, filter 16 recognizes that the connection request has a source address in outside network 12 and a destination address in inside network 14. *Id.* at 3:46–50, 3:66–4:6, Fig. 2 (entry 52); *see id.* at 3:66–7:54, Figs. 3–5. Accordingly, “filter 16 routes this first connection request to security host 26,” which “intercept[s]” the request and “prevents it from being transmitted within inside network 14.” *Id.* at 4:6–9, 5:5–8; *see id.* at [57], 3:60–65, Fig. 3. Source host 22 then sends a second connection request message, requesting connection to the security service on security host 26. *Id.* at 4:12–14; *see id.* at 5:27–32. The security service begins a communication session with source host 22. *Id.* at 4:19–22, 6:44–50.

During this session, the security service confirms the first connection request by authenticating and authorizing the user operating source host 22. *Id.* at [57], 4:23–25. Specifically, the security service performs a one-factor

authentication in which the service prompts the user to enter user identification data and determines whether the received data “indicate[] that the user is an authentic user.” *See id.* at 6:50–59. In the preferred embodiment, this authentication uses a one-time password, but the “strength” of the authentication process “may vary in accordance with the needs of network 14.” *Id.* at 6:59–67. If the security service confirms the user’s authenticity, it proceeds to determine whether the user is authorized to access the requested application service on destination host 28 by, for example, considering user privileges. *Id.* at 7:33–41. If the security service fails to confirm the user’s authenticity or authorization, it sends a “failed access message” to the client and continues to prevent the request “from being released onto inside network 14,” thereby preventing connection with destination host 28. *Id.* at 7:1–7, 7:41–45.

Upon confirming that the user is authentic and authorized to access the requested application service on destination host 28, the security service on security host 26 “releases . . . to inside network 14” the “first connection request [that] it ha[d] intercepted.” *Id.* at [57], 4:25–27, 5:53–57, 7:45–49, Figs. 3, 5. The targeted application service at destination host 28 “then acknowledge[s] the connection request” and “a communication session . . . commence[s].” *Id.* at 4:27–30, 7:49–51; *see id.* at [57], 5:57–59.

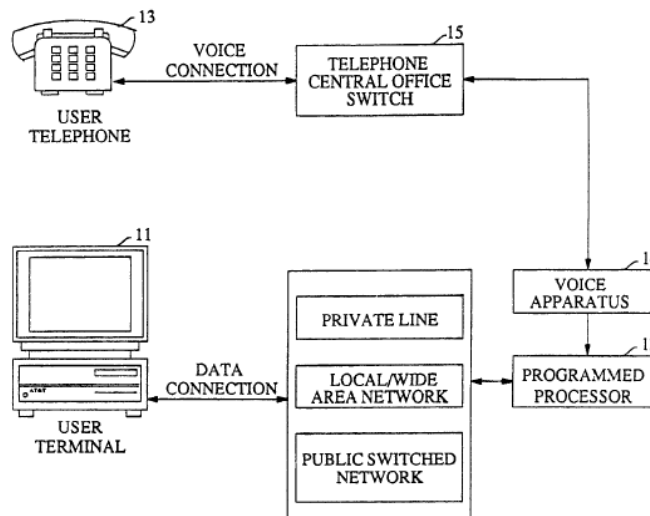
2. Overview of *Flanagan*

Flanagan is directed to a “voice password-controlled security system.” Ex. 1102, [57], 2:15–17. According to *Flanagan*, security in “computer systems typically” has employed “preassigned passwords,” but passwords and, thus, the security of password-controlled systems are “often breached” as a result of “human failings” (e.g., selecting obvious passwords or failing to change standard passwords). *Id.* at 1:23–48. “To help overcome these

problems,” password-controlled systems have been augmented by requiring a user to possess a unique device “adapted to execute a secret encryption algorithm.” *Id.* at 1:48–2:6. Flanagan explains that the “basic problem with these security systems, however, is that they allow access by a user without ascertaining his or her true identity – i.e., without establishing some personal uniqueness, such as through fingerprints, DNA,” or voice. *Id.* at 2:7–12. Therefore, Flanagan provides a two-factor authentication system that “substantially enhance[s]” security by not only confirming the user’s login and password information but also verifying the user’s voice, using a “high[ly] reliabl[e] . . . voice recognition system,” via a call to a telephone “associated with the user.” *Id.* at [57], 2:15–3:1, 7:13–16.

Flanagan depicts an illustrative embodiment of its security system in Figure 1, reproduced below. *Id.* at 3:10–13, 3:25–27.

FIG. 1



In the embodiment illustrated in Figure 1, a user at user terminal 11 “wishes to access certain restricted programs in programmed processor 12” and initiates a data connection with processor 12. *Id.* at 3:25–40, 4:36–43. In the first authentication factor, processor 12 prompts the user to enter login

and password information, and checks whether the information matches that of a user entitled to access. *Id.* at 2:35–40, 3:44–49, Fig. 3. Processor 12 then proceeds to the second authentication factor in which it “establish[es] a voice connection to user telephone 13,” through telephone central office switch 15, using a “pre-assigned telephone number associated with the user.” *Id.* at 3:49–4:4; *see id.* at [57], 2:17–20, 2:43–50, 5:28–36, Fig. 3. Processor 12 generates and prompts the user to repeat a random four-digit number. *Id.* at 4:12–20, 6:15–36. Next, using a voice recognition technique, processor 12 compares the received speech with pre-stored reference speech of the four-digit number for the user and assigns a “confidence recognition factor indicating the closeness of the match” of the speech patterns. *Id.* at 2:52–57, 4:20–29, 6:38–49. “If the confidence recognition factor is greater than [a] threshold value,” processor 12 affords the user “access to its resources” and specifically, its restricted programs. *Id.* at [57], 2:25–27, 4:29–31, 4:41–43, 6:49–56; *see id.* at 2:57–3:1, Fig. 3.

3. Overview of Falk

Falk provides an authentication system that requires a user attempting to access an electronic service to carry a separate personal unit. Ex. 1005, [57], 1:5–9, 1:65–2:5. In particular, in Falk’s two-factor authentication system, the user must know the appropriate user personal identification number (“PIN”) and possess the correct personal unit 20, which calculates a response code based on the PIN, a received challenge code, and an internal secret key. *See id.* at [57], 4:32–37, 5:4–7, 5:30–34, 5:45–47, 7:5–7, Fig. 3.

Falk’s authentication process begins when a user at terminal 22 (e.g., a telephone or computer) initiates a request for access to service node 26 by transmitting the request over service access network 24 to service node 26. *Id.* at 3:8–13, 5:20–24, 6:3–6. “[S]ervice node 26, in response to the access

request, requests authentication via an authentication challenge network 28.”

Id. at 6:12–15; *see id.* at 6:63–67. Service node 26 generates, or causes authentication center 30 to generate, a challenge code, which is sent to personal unit 20 (e.g., a pager). *Id.* at 5:25–29; *see id.* at [57], 3:4–9, 4:8–31, 6:15–18. Personal unit 20 then prompts the user to input a PIN and generates a response code using a stored algorithm, based on the PIN, the challenge code, and a secret key. *Id.* at 5:29–34, 5:45–47; *see id.* at [57], 6:19–22, 7:5–7. Next, personal unit 20 may display the response code, the user may manually input the response code into terminal 22, and the code may be transmitted to authentication center 30. *See id.* at 5:48–54, 6:31–45.

Authentication center 30 compares the received response code to an expected response code. *Id.* at 5:54–62, 6:41–42, 7:14–15. Authentication center 30 then may send a message to “inform . . . service node 26 of the results,” i.e., whether the user is “authenticated/not authenticated.” *Id.* at 5:55–57, 6:46–48, 7:14–17. If the response code is acceptable and the user is authenticated, service node 26 permits the user access to its services. *Id.* at 5:57–59, 6:55–58, Fig. 3. If, however, the response code is not acceptable and the user is not authenticated, service node 26 denies the user access to its services. *Id.* at 6:48–50, Fig. 3.

4. *Alleged Motivation to Combine Feigen, Flanagan, and Falk* (Claims 1–17, 19–24, 53, and 54)

a. *Legal Standards*

A patent claim is unpatentable as obvious under 35 U.S.C. § 103(a) if “the differences between” the recited 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.” 35 U.S.C. § 103(a). An invention “composed

of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). Rather, to establish obviousness, it is petitioner’s “burden to demonstrate both that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016) (quotations omitted); see *KSR*, 550 U.S. at 418. Moreover, a petitioner cannot satisfy this burden by “employ[ing] mere conclusory statements” and “must instead articulate specific reasoning, based on evidence of record,” to support an obviousness determination. *Magnum Oil*, 829 F.3d at 1380. Stated differently, there must be “articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *KSR*, 550 U.S. at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

The “factual inquiry” into the reasons for “combin[ing] references must be thorough and searching, and the need for specificity pervades” *In re Nuvasive, Inc.*, 842 F.3d 1376, 1381–82 (Fed. Cir. 2016) (quotations omitted). A determination of obviousness cannot be reached where the record lacks “explanation as to *how* or *why* the references would be combined to produce the claimed invention.” *TriVascular, Inc. v. Samuels*, 812 F.3d 1056, 1066 (Fed. Cir. 2016); see *Nuvasive*, 842 F.3d at 1382–86 (holding that an obviousness determination cannot be reached where there is no “articulat[ion of] a *reason why* a [person having ordinary skill in the art] would combine” and “modify” the prior art teachings). This required explanation as to how and why the references would be combined avoids an impermissible “hindsight reconstruction,” using “the patent in suit as a guide

through the maze of prior art references, combining the right references in the right way so as to achieve the result of the claims in suit.” *TriVascular*, 812 F.3d at 1066; *In re NTP, Inc.*, 654 F.3d 1279, 1299 (Fed. Cir. 2011).

b. Discussion

Petitioner argues that one of ordinary skill in the art “would have been motivated to combine the teachings of Feigen, Flanagan, and Falk.”²

Pet. 40–45. As support, Petitioner asserts that Feigen discloses “single factor authentication” but “specifically suggests that the reader seek out stronger authentication techniques to use within its invention” by stating that the “strength” of the “authentication process . . . may vary in accordance with the needs of network 14.” *Id.* at 40 (emphasis omitted) (quoting Ex. 1003, 6:59–62); *see* Ex. 1101 ¶¶ 96–97, 99. According to Petitioner and Dr. McDaniel, one of ordinary skill would have understood that higher security can be achieved through known “[m]ultifactor authentication systems,” which often combine two or more categories of authentication

² We note that, as Patent Owner argues, Petitioner’s arguments, along with Dr. McDaniel’s supporting testimony, regarding the proposed combinations and modifications of Feigen, Flanagan, and Falk are often vague and non-specific. *See, e.g.*, Prelim. Resp. 44–51. To the extent Petitioner intended to proffer proposed combinations or modifications distinct from those we discuss below, Petitioner has not met its burden to state any such combinations or modifications clearly and with specificity (and, thus, to notify adequately Patent Owner and the Board of any such combinations and modifications). *See Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (“[T]he Petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” (citing 35 U.S.C. § 322(a)(3))); *Liberty Mut. Ins. Co. v. Progressive Cas. Ins. Co.*, Case CBM2012-00003, slip op. at 14–15 (PTAB Oct. 25, 2012) (Paper 8) (representative decision) (“[I]t is the responsibility of the Petitioner to clearly articulate [the proposed combination].”); 35 U.S.C. § 312(a)(3); 37 C.F.R. §§ 42.22(a)(2), 42.104(b)(4)–(5).

approaches, including “(i) something the user knows,” such as a password or PIN, “(ii) something the user has,” such as a key card, and “(iii) something the user is,” i.e., a physical characteristic, such as fingerprints or voice.

Pet. 21–23, 40–41; Ex. 1101 ¶¶ 50–54, 97–98. Therefore, Petitioner and Dr. McDaniel represent that an artisan—interested in heightening security as suggested by Feigen—“would have logically consulted” references related to “two-factor authentication,” such as Flanagan, which implements “something the user knows,” “has,” and “is” approaches, and Falk, which implements “something the user knows” and “has” approaches. Pet. 40–41, 44; Ex. 1101 ¶¶ 89, 100, 107.

Specifically, Petitioner argues that one of ordinary skill “would have been motivated to address the need for enhanced security identified in Feigen by applying the teachings of Flanagan,” given Flanagan’s statements that “the security of password-controlled systems is often breached” and that its voice password-controlled security system provides a higher level of security by “ascertaining [the] true identity” of the user. Pet. 42–43 (quoting Ex. 1102, 2:7–20); Ex. 1101 ¶¶ 101–102, 105. In particular, Petitioner proposes to implement Flanagan’s second authentication factor, establishing a voice connection to telephone 13 associated with the user and using voice recognition to verify received voice information, in Feigen’s system and specifically, to “augment[]” Feigen’s security host 26 “to include” and “to perform” this functionality as “additional [authentication] steps.”³

³ Pet. 41–43 (proposing to “implement[] Flanagan’s ‘something the user has’ and ‘something the user is’ approaches as additional steps to Feigen’s ‘something the user knows’ password authentication”); Ex. 1101 ¶¶ 101–105 (same); Pet. 46–47 (“When Flanagan is combined with Feigen, security host (26) in Feigen is augmented to include Flanagan’s second form of

According to Petitioner and Dr. McDaniel, this combination of Feigen and Flanagan would have required only “known techniques of implementing Flanagan’s ‘something the user has’ and ‘something the user is’ approaches as additional steps to Feigen’s ‘something the user knows’ password authentication.” Pet. 42; Ex. 1101 ¶¶ 102–105.

To this combination of Feigen and Flanagan, Petitioner proposes to “further combine[]” Falk’s teaching regarding its authentication center 30 “send[ing] a message to the service node 26,” to which the user is seeking access, to “inform the service node 26 of the results” of authentication such that service node 26 grants or denies access to the user. Ex. 1005, 5:54–57, 6:40–58, 7:14–18, Fig. 3; Pet. 35, 39, 45, 51 (citing Ex. 1005, 5:48–57, 6:44–58, 7:14–17, Fig. 3); see Pet. 61, 64; Ex. 1101 ¶¶ 92–93, 108, 132, 176, 198. Petitioner argues that these disclosures of Falk teach “sending an instruction to the host computer to grant or deny access,” as the challenged claims of the ’698 patent require. Pet. 35. Specifically, Petitioner relies on these disclosures of Falk⁴ as allegedly teaching the limitation of independent

authentication – voice recognition via telephone (13) over a channel extending through telephone central switch (15).”); Ex. 1101 ¶¶ 119, 163, 183 (same); Pet. 48–49 (“When combined with Flanagan, . . . [Feigen’s] security host (26) . . . performs a second factor authentication . . . through a voice verification process over telephone network (15).”); Ex. 1101 ¶ 126, 170, 190 (same); see Pet. 34–35, 37–39 (composite figure of Feigen and Flanagan and chart showing the alleged correspondence between ground 1 and the ’698 patent), 45–51, 60–64; Ex. 1101 ¶¶ 131, 175, 197.

⁴ Even if Petitioner were to rely on Feigen or Flanagan as allegedly teaching or suggesting these limitations, the passages of these references cited in the Petition are insufficient to teach or suggest the limitations. First, as to Feigen, the “failed access message” that security host 26 “return[s]” when the user is not authentic or authorized is “sen[t] . . . to the client”—not to destination host 28, the alleged “host computer,” which is the required

claims 1 and 53 that recites “outputting an instruction from the security computer to the host computer to grant access to the host computer or deny access thereto,” as well as the nearly identical limitation of independent claim 54.⁵ Accordingly, to reach the methods and apparatus recited in

recipient of the instruction per the claim language. Ex. 1003, 7:1–7, 7:36–45, Fig. 3 (task 104); *e.g.*, Pet. 50. Moreover, security host 26’s “release[]” of the connection request message, sent by source host 22, “to inside network 14” when the user is authentic and authorized does not teach or suggest the required instruction to grant or deny access to the host computer. Ex. 1003, [57], 4:3–6, 4:24–31, 7:45–51, Figs. 3, 5 (task 116); *see id.* at 10:4–27. Specifically, source host 22’s connection request message, itself, is a request, not an instruction to grant or deny access. Further, in merely releasing that message to inside network 14, without more, security host 26 does not output an instruction to grant or deny access to destination host 28—even if destination host 28, after receiving the message, ultimately communicates with the user. Rather, security host 26—by either allowing the request to inside network 14, or sending a failed access message to the client and preventing the request from reaching network 14—effectively grants or denies access to destination host 28. Accordingly, the cited portions of Feigen alone do not teach or suggest sufficiently the relevant limitations, and Petitioner does not explain why or how they do so. Second, in Flanagan, processor 12, to which the user seeks access, “compares” received voice information to pre-stored voice information for the user and only if they match, “affords” the user “access to its resources,” specifically its restricted programs. Ex. 1102, [57], 2:23–27, 2:52–3:1, 3:25–31, 4:20–34, 4:39–43, 6:49–56, Figs. 3–4. Thus, Flanagan does not teach or suggest outputting any instruction to grant or deny access to the host computer.

⁵ Pet. 35 (explaining that Falk is “further combined to teach sending an instruction to the host computer to grant or deny access”); *id.* at 50–51, 61, 64 ((Petition’s analysis of relevant claim limitations) (referring to Feigen and Flanagan without asserting that they teach or suggest any instruction to grant or deny access and expressly relying on Falk’s “authenticated or not authenticated message” as teaching an “instruction . . . to grant or deny access”)); *id.* at 35, 39 (relying on Falk alone for alleged teaching of “security computer (40) instruct[ing] host computer (34) to grant access or deny access”); *see* Ex. 1101 ¶¶ 92–93, 132, 176, 198; *see also* Ex. 1103, 27,

independent claims 1, 53, and 54 and the challenged claims that depend from claim 1, Petitioner proposes combining “this functionality from Falk” with the combined system of Feigen and Flanagan such that Feigen’s “security host (26) . . . issue[s] an instruction to destination host (28) to grant or deny access based on the comparison of [Flanagan’s] voice information received from telephone (13).” Pet. 45, 51; Ex. 1101 ¶¶ 108, 132, 176; see Pet. 61, 64; Ex. 1101 ¶ 198.

In support of this proposed combination, Petitioner argues, and Dr. McDaniel opines, that a skilled artisan would have been “motivated to combine Feigen and Flanagan with Falk at least because Falk is focused on the same security processes that provide authentication and authorization of users.” Pet. 43; Ex. 1101 ¶ 106; see Ex. 1101 ¶ 108. Petitioner and Dr. McDaniel further allege that “[l]ike Flanagan, Falk teaches two-factor authentication using ‘something the user knows’ and ‘something the user has.’” Pet. 44; Ex. 1101 ¶ 107. Moreover, Petitioner and Dr. McDaniel represent that “Feigen, Flanagan, and Falk each describe a system where the security system grants or denies the user’s access.” Pet. 44; Ex. 1101 ¶ 108. Thus, according to Petitioner and Dr. McDaniel, the combination of Feigen, Flanagan, and Falk “would have been obvious to a skilled artisan seeking to implement the heightened level of authentication . . . suggested by Feigen.” Pet. 44–45; Ex. 1101 ¶ 108; see Pet. 40–41; Ex. 1101 ¶ 89.

From these assertions, Petitioner and Dr. McDaniel conclude: “Accordingly, it would have been obvious to employ the instruction

30–32, 98, 101–02, 131, 134–36 (asserting that only Falk, not Feigen or Flanagan, “describes outputting an instruction from the security computer to the host computer to grant . . . or deny access” and, thus, that “*Feigen, Flanagan, and Falk* combined describe” the relevant claim limitations).

mechanisms used in these references to grant or deny access to a user,” including “implementing [Feigen’s] security host (26) to issue an instruction to destination host (28) to grant or deny access” “in the same way that authentication center (30) in Falk transmits to service node (26) the result of a comparison of a response code from personal unit (20) with an expected response.” Pet. 45; see Ex. 1101 ¶ 108. Dr. McDaniel further opines that this proposed implementation “would use known techniques with predictable results, as described in the references, and yield an instruction to grant or deny access, as called for in the [’]698 Patent.” Ex. 1101 ¶ 108.

In response, Patent Owner argues that even if an ordinarily skilled artisan would have been motivated to combine Feigen and Flanagan as Petitioner proposes,⁶ Petitioner does not demonstrate why such an artisan would have “*further modif[ied]* the combination of Feigen and Flanagan with Falk” and, therefore, fails to “justify its proposed three-reference combination.” Prelim. Resp. 26–27, 30. Patent Owner argues that “[t]o the extent Petitioner purports to base its motivation to combine . . . on the assertion that all three references are in the same field, this is insufficient” to provide a reason, with rational underpinning, to combine specific teachings of the references. *Id.* at 31 n.10. Patent Owner also contends Petitioner’s assertions that Flanagan and Falk have the same teachings raise “questions as to why a [person of ordinary skill in the art] would have been motivated to combine *both* Flanagan and Falk into Feigen,” yet “Ppetitioner never

⁶ Patent Owner advances numerous alleged deficiencies in Petitioner’s proffered motivation to combine Feigen, Flanagan, and Falk. Prelim. Resp. 25–37, 44–50. As discussed below, we agree with Patent Owner that Petitioner’s alleged reasons to combine Falk with Feigen and Flanagan are deficient. Thus, we need not address Patent Owner’s other assertions.

addresses what benefit Falk allegedly brings to the proposed combination that would not have been present with Flanagan alone.” *Id.* at 30 n.9.

Moreover, Patent Owner asserts that Petitioner “does not propose incorporating Falk’s second-factor authentication ‘challenge code’ into the combined Feigen/Flanagan system to yield a system with yet another authentication factor.” *Id.* at 31–32. Rather, according to Patent Owner, “Petitioner relies on Falk only for its alleged disclosure of transmitting an instruction to a host computer to grant or deny access.” *Id.* at 32. Thus, Patent Owner argues that “Petitioner’s proposed Feigen/Flanagan/Falk combination does not align with its purported motivation to incorporate Falk” and Petitioner is merely “cherry-pick[ing] from disparate disclosures in a failed attempt to try to cobble together the claimed invention of the ’698 patent” in a “classic case of improper hindsight analysis.” *Id.* at 31–32.

We agree with Patent Owner that Petitioner’s arguments and evidence are insufficient to explain and demonstrate *why* an ordinarily skilled artisan would have combined Feigen and Flanagan with Falk and more particularly, Falk’s teaching regarding sending a message to service node 26 with the result of an authentication determination. We find Petitioner’s proffered reasons to combine Falk to be excessively generic and to lack the specificity that our governing precedent requires of a motivation to combine. *See, e.g., Nuvasive*, 842 F.3d at 1381–82 (“[T]he factual inquiry whether to combine references must be thorough and searching, and the need for specificity pervades” (quotations omitted)); *Magnum Oil*, 829 F.3d at 1380 (“To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements” and “must instead articulate specific reasoning, based on evidence of record”). In particular, Petitioner’s vague assertions do not substantiate a reason that would have prompted one of

ordinary skill in the art to combine the specific relevant *element* or *teaching* of Falk—i.e., authentication center 30 sending a message to service node 26 with the result of the user authentication—with Feigen and Flanagan to achieve the invention recited in the challenged claims of the ’698 patent. *See KSR*, 550 U.S. at 418 (“[I]t can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the *elements* in the way the claimed new invention does.” (emphasis added)); *Magnum Oil*, 829 F.3d at 1381 (“[I]t was [petitioner’s] burden to demonstrate . . . that a skilled artisan would have been motivated to combine the *teachings* of the prior art references to achieve the claimed invention” (second alteration in original) (emphasis added) (quotations omitted)); *ActiveVideo Networks, Inc. v. Verizon Commc’ns, Inc.*, 694 F.3d 1312, 1328 (Fed. Cir. 2012) (determining that obviousness showing was deficient for “fail[ure] to explain why a person of ordinary skill in the art would have combined *elements* from specific references *in the way the claimed invention does*” (first emphasis added)).

In particular, Petitioner’s assertions that Feigen, Flanagan, and Falk are “focused on the same security processes that provide authentication and authorization of users” and describe “security system[s] [that] grant[] or den[y] the user’s access,” as well as that Flanagan and Falk both “teach[] two-factor authentication using ‘something the user knows’ and ‘ . . . has,’” are insufficient to support an obviousness showing. Pet. 43–44; *see id.* at 40–41; Ex. 1101 ¶¶ 94, 100, 106–108. These arguments assert no more than that the three references are in the same field and their disclosed systems share broad and general similarities, such as providing for user authentication that results in a grant or denial of user access. We agree with Patent Owner that these assertions, without more, are inadequate to provide

sufficiently specific reasoning, with rational underpinning, to combine Falk—and particularly, Falk’s message from authentication center 30 to service node 26 upon completion of user authentication—with Feigen and Flanagan. *See* Prelim. Resp. 30–31 nn.9–10; *TRW Auto. US LLC v. Magna Elecs., Inc.*, Case No. IPR2014-00257, slip op. at 4 (PTAB Aug. 28, 2014) (Paper 18) (“That each reference may be in the field of ‘vehicular vision’ is insufficient, in and of itself, to provide a reason with rational[] underpinning as to why one of ordinary skill in the art would have sought to combine specific teachings of such references.”). For example, Petitioner never identifies or explains adequately any benefit or improvement gained by adding Falk, and specifically, Falk’s relevant message, to the proposed combination of Feigen and Flanagan. *See Nuvasive*, 842 F.3d at 1384–86 (holding obviousness determination to be unsupported where petitioner asserted only that a skilled artisan would have been motivated to combine the prior art “to obtain additional information,” yet the record lacked any articulation as to “why the additional information would benefit [a skilled artisan]” and “why [such an artisan] would have been motivated” “to obtain this additional information”).

Likewise deficient are Petitioner’s arguments that a skilled artisan would have been motivated to combine *both* Flanagan and Falk with Feigen to address Feigen’s suggestion to “heighten the strength” of the one-factor authentication in Feigen, because Falk, “[l]ike Flanagan,” “teaches two-factor authentication using ‘something the user knows’ and ‘ . . . has.’” Pet. 40–41, 44–45; *see* Ex. 1101 ¶¶ 89, 100, 107–108. First, Petitioner does not explain persuasively why an artisan would have further modified the combined teachings of Feigen and Flanagan to send a message to security host 26 with the authentication result as taught by Falk. As Petitioner

argues, Flanagan teaches two-factor authentication using “something the user knows” (login and password) and “something the user has” (user telephone 13 with a pre-assigned number)—as well as “something the user is” (the user’s voice). See Ex. 1102, [57], 2:7–3:1, 3:44–58, 4:12–34, 4:39–50, 5:28–36, 6:15–56, Figs. 3–4; Pet. 41–42. Flanagan touts its second authentication factor as “substantially enhanc[ing]” security over systems that only require a user to enter a password (i.e., “something the user knows”) and to “possess[]” a certain device (i.e., “something the user has”) by verifying a “personal uniqueness” of the user, specifically voice (i.e., “something the user is”), using a “high[ly] reliab[le] . . . voice recognition” technique. Ex. 1102, [57], 1:23–2:31, 7:13–16; see Pet. 42–43; Ex. 1101 ¶¶ 55 (opining that at the relevant time, the “use of biometric authentication as part of multifactor systems” was considered “highly desirable”), 101–102.

As explained above, Petitioner proposes to implement Flanagan’s second authentication factor, which includes calling user telephone 13 (“something the user has”) and verifying received voice information (“something the user is”), in Feigen. *E.g.*, Pet. 42–43 (asserting that the combination of Feigen and Flanagan would “implement[] *Flanagan’s* ‘*something the user has*’ and ‘*something the user is*’ approaches as additional steps to Feigen’s ‘something the user knows’ password authentication” (emphasis added)); *id.* at 46–47 (“When Flanagan is combined with Feigen, security host (26) in Feigen is augmented to include *Flanagan’s second form of authentication* – voice recognition via telephone (13)” (emphasis added)); *id.* at 34–39, 48–49; Ex. 1101 ¶¶ 90–93, 102–105, 119, 126, 163, 183. Indeed, Petitioner relies on the same proffered reasoning—i.e., achieving the heightened level of security and authentication that Feigen suggests—to support combining Flanagan’s

second authentication factor with Feigen. *See* Pet. 40–43 (arguing that “one of ordinary skill in the art would have been motivated to combine Feigen and Flanagan to achieve Feigen’s suggestion of stronger security by security host (26)” and similarly, “to address the need for enhanced security identified in Feigen by applying the teachings of Flanagan”); Ex. 1101 ¶¶ 89, 96–105. Even assuming that this proffered reasoning is sufficient support for the proposed combination of Feigen with Flanagan’s second authentication factor, it does not provide sufficient explanation as to why an ordinarily skilled artisan—having implemented this combination of Feigen with Flanagan’s second authentication factor and, thus, increased Feigen’s authentication and security level—also would look to add Falk, and specifically, Falk’s teaching of sending a message to security host 26 with the authentication result, to this combination of Feigen and Flanagan.

Second, as Patent Owner points out, although Petitioner proposes to combine Flanagan’s second authentication factor with Feigen, Petitioner does not articulate clearly or adequately a proposed combination of Falk’s second authentication factor—which includes sending a challenge code to personal unit 20, which in turn then generates a response code that is sent to authentication center 30 and compared to the expected response code—with Feigen and Flanagan.⁷ *See* Ex. 1005, 5:24–33, 5:45–62, Fig. 3; Prelim.

⁷ Given that Petitioner does not articulate such a combination, Petitioner also fails to explain *how* such a combination of Feigen with *both* Flanagan’s and Falk’s second authentication factors, which use devices such as a telephone (Flanagan) and a pager (Falk), would operate, as required to support a motivation to combine. *See Personal Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 994 (Fed. Cir. 2017) (holding an obviousness determination improper where the record lacked a “clear, evidence-supported account” of “how the combination” would work).

Resp. 31–32; Pet. 35–45; Pet. 51, 61, 64 (arguing that “[u]sing” Falk’s “functionality” regarding sending an “authenticated or not authenticated message,” Feigen’s security host 26 “can issue an instruction to destination host (28) to grant or deny access *based on the comparison of [Flanagan]’s voice information received from telephone (13)*” (emphasis added)); Ex. 1101 ¶¶ 132, 176 (same). Rather, Petitioner specifically proposes to combine only Falk’s alleged teaching of an instruction to service node 26 to grant or deny access.⁸ Accordingly, we agree with Patent Owner that the proffered reasoning of Petitioner regarding increasing the authentication and security level in Feigen does not relate or link sufficiently to the specific teaching of Falk that Petitioner proposes to combine with Feigen and Flanagan. See Prelim. Resp. 31–32; *ActiveVideo*, 694 F.3d at 1328 (determining that expert testimony was insufficient to support an obviousness showing where it “b[ore] no relation to any specific combination of prior art elements”).

In addition to the deficiencies in Petitioner’s proffered reasons to combine discussed above, Petitioner’s argument and evidence lack adequate

⁸ Pet. 45 (proposing to “implement[]” in Feigen’s security host 26, Falk’s teaching of authentication center (30) “transmit[ing] to service node (26) the result of a comparison” of a received and expected response code); Ex. 1101 ¶ 108 (same); Pet. 35–39 ((chart “show[ing] the correspondence between” ground 1 and the ’698 patent) (relying on Falk only for alleged teaching of “security computer (40) instruct[ing] host computer (34) to grant access or deny access”)); Ex. 1101 ¶ 93 (same); see also Pet. 51, 61, 64 ((analysis of independent claims 1, 53, and 54) (arguing that “[u]sing” Falk’s “functionality” of sending an “authenticated or not authenticated message” to service node 26, Feigen’s security host 26 “can issue an instruction to destination host (28) to grant or deny access based on the comparison of [Flanagan]’s voice information received from telephone (13) via telephone central switch (15)”)); Ex. 1101 ¶¶ 132, 176 (same).

support for the motivation to combine Falk with Feigen and Flanagan for an additional, independent reason. In particular, Petitioner fails to address meaningful relevant differences between the operation and functionality of Feigen's destination host 28 and Falk's service node 26 with respect to connection or access requests and why, despite these differences, an ordinarily skilled artisan would have been motivated to combine Feigen's system, modified by Flanagan, with Falk's message to service node 26 regarding the authentication result, as Petitioner proposes.

Specifically, in Falk, service node 26 "receives" the user's access request and "in response," it "requests authentication." Ex. 1005, 6:4–16, 6:63–67; *see id.* at 5:20–25. After authentication, authentication center 30 "sends a message" to "inform the service node 26 of the results"—i.e., "authenticated/not authenticated"—and service node 26 grants access if the authentication was successful and denies access if the authentication was unsuccessful. *Id.* at 6:45–58, 7:14–18; *see id.* at 5:52–58. Accordingly, these disclosures of Falk make clear that while authentication center 30 is performing the authentication, service node 26—having received the user's access request and requested authentication of the user in response to that request—is awaiting the result of the pending authentication. Thus, authentication center 30, upon completing the requested authentication, informs service node 26 of the result of the authentication that it requested.

Feigen, in contrast, operates differently. In Feigen, source host 22 in outside network 12 sends a connection request message for an application service on destination host 28 in inside network 14—but filter 16 "routes" the request to security host 26, which "intercept[s]" the request. Ex. 1003, 4:3–10, 5:5–10. Security host 26 "prevents [the connection request] from being transmitted within inside network 14," and thus from "reach[ing] its

intended destination” of destination host 28, unless and until it determines that the user is authentic and authorized. *Id.* at 4:3–31, 5:5–10; *see id.* at [57], 7:1–7, 7:33–51, Figs. 3, 5. If security host 26 determines that the user is not authentic or authorized, it sends a “failed access message to the client” and “continue[s] to prevent” the request “from being released onto inside network 14,” thereby preventing connection with destination host 28. *Id.* at 7:1–7, 7:40–45, Fig. 5 (tasks 102–104, 114). If, however, security host 26 determines that the user is authentic and authorized, it “release[s]” the request and the request is received by destination host 28. *Id.* at [57], 4:22–31, 7:45–51, Fig. 3, Fig. 5 (task 116). Accordingly, as a result of security host 26’s interception of the connection request, destination host 28 has not received, and is not even aware of, the connection request while security host 26 is performing authentication. Nor does destination host 28 request the authentication. Rather, destination host 28 receives the connection request only if security host 26 determines that the user is authorized and authentic, and is never made aware of the request if the user is not authorized or authentic. Therefore, security host 26 essentially acts as a gatekeeper, handling whether access to inside network 14, and destination host 28 therein, is granted or denied by either allowing the request onto inside network 14, or sending the client a failed access message and preventing the request from being transmitted onto the network.

Petitioner does not address these distinctions in the operation of Feigen’s and Falk’s systems or articulate why—despite these differences—one of ordinary skill would have been motivated to combine Feigen’s system with Falk’s teaching of sending service node 26 the result of the authentication (i.e., authenticated/not authenticated), based on which service node 26 grants or denies access to the user. In particular, Petitioner fails to

explain adequately why an artisan would have been motivated to modify Feigen to issue such a message to destination host 28, which—in contrast to Falk’s service node 26—does not request, and is unaware of, the authentication and does not receive the connection request unless and until security host 26 determines that the user is authorized. *See generally* Pet. 36–37, 45–47, 60–62 (relying, in unpatentability analysis, on Feigen’s teachings regarding filter 16 and security host 26 intercepting a connection request and preventing it from being transmitted to inside network 14).

Accordingly, we determine that Petitioner’s argument and evidence is insufficient to explain and support a reason, with rational underpinning, to combine Feigen and Flanagan with Falk, and particularly, Falk’s teaching of sending a message with the authentication result to service node 26, to achieve the methods and apparatus in independent claims 1, 53, and 54 as well as the challenged claims that depend from claim 1. Thus, Petitioner has not shown a reasonable likelihood that it would prevail in establishing that Feigen, Flanagan, and Falk render obvious claims 1–17, 19–24, 53, and 54.

III. CONCLUSION

In conclusion, for the reasons given, we determine that the Petition does not establish a reasonable likelihood that Petitioner would prevail in showing that the challenged claims of the ’698 patent, claims 1–17, 19–24, 53, and 54, are unpatentable. Thus, we do not institute *inter partes* review of any of the challenged claims on any of the asserted grounds.

IV. ORDER

Accordingly, it is:

ORDERED that pursuant to 35 U.S.C. § 314(a), the Petition is *denied*, and no trial is instituted as to any claim of U.S. Patent No. 8,484,698 B2.

IPR2017-01064
Patent 8,484,698 B2
For PETITIONER:

Duo Security Inc.

John D. Garretson (Lead Counsel)
Amy M. Foust
SHOOK, HARDY & BACON L.L.P.
jgarretson@shb.com
afoust@shb.com

Centrify Corporation

Darren M. Franklin
SHEPPARD, MULLIN, RICHTER, & HAMPTON LLP
dfranklin@sheppardmullin.com

Trustwave Holdings, Inc.

Brian A. Jones
MCDERMOTT WILL & EMERY
bajones@mwe.com

For PATENT OWNER:

Steven Pepe (Lead Counsel)
James L. Davis, Jr.
Matthew J. Rizzolo
ROPES & GRAY LLP
steven.pepe@ropesgray.com
james.l.davis@ropesgray.com
matthew.rizzolo@ropesgray.com