

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC,
Petitioner,

v.

DYNAPASS IP HOLDINGS LLC,
Patent Owner.

IPR2023-00425
Patent 6,993,658 B1

Before KEVIN F. TURNER, LYNNE H. BROWNE, and
JASON M. REPKO, *Administrative Patent Judges*.

BROWNE, *Administrative Patent Judge*.

DECISION
Final Written Decision
Determining Some Challenged Claims Unpatentable
35 U.S.C. § 314

I. INTRODUCTION

We have authority to hear this *inter partes* review under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons discussed below, we determine that Petitioner, Unified Patents, LLC has shown by a preponderance of the evidence that claim 5 of U.S. Patent No. 6,993,658 B1 (Ex. 1001, “the ’658 Patent”) is unpatentable and has not shown by a preponderance of the evidence that claims 1, 3, 4, and 6 are unpatentable. *See* 35 U.S.C. § 316(e) (2018); 37 C.F.R. § 42.1(d) (2019).

A. Procedural History

The Petition (Paper 1, “Pet.” or “Petition”) requested *inter partes* review of claims 1 and 3–6 of the ’658 Patent. Patent Owner, Dynapass IP Holdings, LLC, filed a Preliminary Response. Paper 8. Based upon the record at that time, we instituted *inter partes* review on all challenged claims on the grounds presented in the Petition. Paper 9.

After institution, Patent Owner filed a Response (Paper 13, “PO Resp.”), Petitioner filed a Reply (Paper 16, “Pet. Reply”), and Patent Owner filed a Sur-reply (Paper 19, “PO Sur-reply”).

On April 16, 2024, an oral hearing was held. The transcript of this hearing was entered in the record of this proceeding as Paper 31 (“Tr.”). During the oral hearing, Petitioner, for the first time, asserted that Patent Owner

filed amended infringement contentions in one of the corresponding District Court cases . . . which alleged that infringement of the claim passcode limitation is met by the password that the user uses for login or other information that is known to the user, such as the username or in termination that references or is an alias to the username.

Tr. 12.

On April 17, 2024, we ordered additional briefing on two questions: 1) is it too late for Petitioner to file a copy of the infringement contentions argued at oral argument; and 2) if the infringement contentions are allowed to be entered, what if any, weight should we give to a position taken by Patent Owner in a different, albeit related, proceeding (i.e., district court litigation). Paper 27 (“Order”). Petitioner filed a Supplemental Brief (Paper 28, “Pet. Supp.”), and Patent Owner filed a Response (Paper 30, “PO Resp. to Supp.”).

B. Real Parties in Interest

Petitioner identifies itself, Unified Patents, LLC, as the only real party-in-interest. Pet. 79. Patent Owner identifies itself, Dynapass IP Holdings LLC and DynaPass Inc., as the only real parties-in-interest. Paper 3, 1.

C. Related Matters

The parties identify the following as related district court matters: *Dynapass IP Holdings LLC v. Regions Financial Corporation*, 2:22-cv-00215 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. JPMorgan Chase & Co.*, 2:22-cv-00212 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. PlainsCapital Bank*, 2:22-cv-00213 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Woodforest National Bank*, 2:22-cv-00218 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Bank of America Corporation*, 2:22-cv-00210 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Wells Fargo & Company*, 2:22-cv-00217 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Truist Financial Corporation*, 2:22-cv-00216 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. PNC Financial Services*, 2:22-cv-00214

(EDTX 6-17-2022), *Dynapass IP Holdings LLC v. BOKF, National Association*, 2:22-cv-00211 (EDTX 6-17-2022), *Dynapass Inc. v. Mobile Authentication Corporation*, 8:18-cv-01173 (C.D. Cal. 7-3-2018). Pet. 80–81; Paper 3, 1–2.

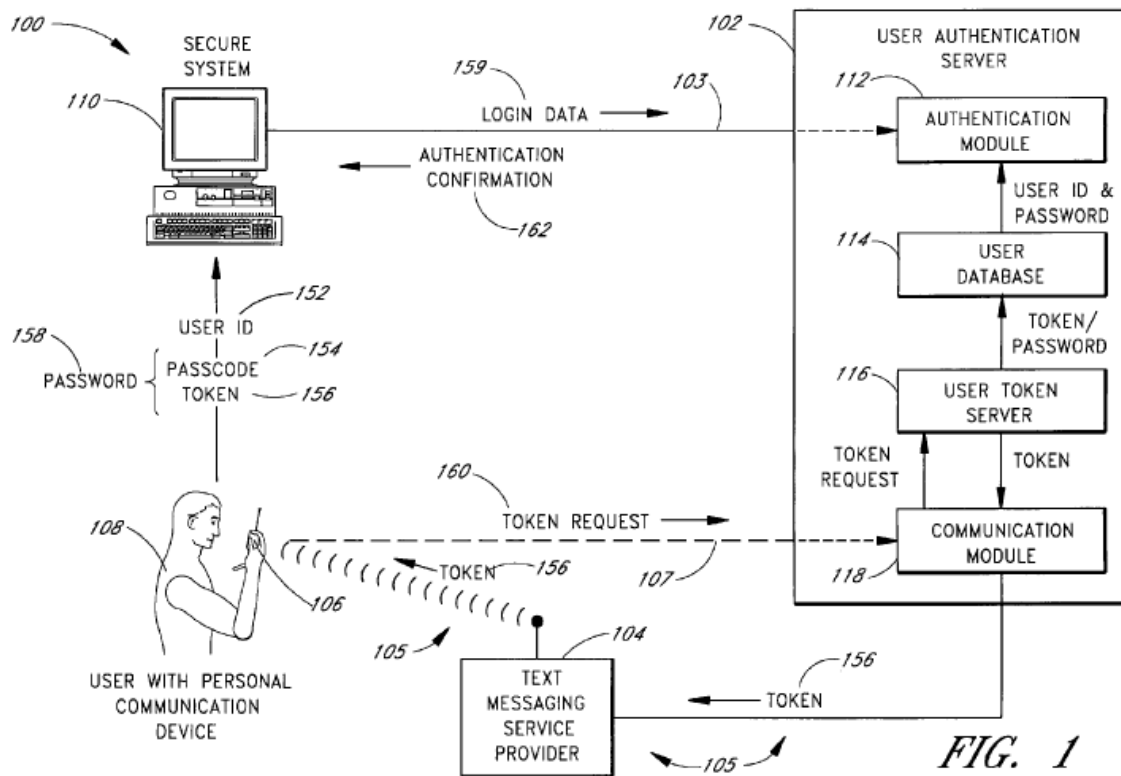
Patent Owner also identifies *Bank of America, N.A. v. Dynapass IP Holdings LLC*, IPR2023-00367 (filed January 3, 2022) as a related matter. Paper 3, 2.

D. The '658 Patent

The '658 Patent is titled “Use of Personal Communication Devices For User Authentication.” Ex. 1001, code (54). The invention “relates generally to the authentication of users of secure systems and, more particularly, the invention relates to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pagers.” *Id.* at 1:7–11.

One embodiment of the invention provides a password setting system that includes a user token server and a communication module wherein a user token server generates a random token in response to a request for a new password from a user. Ex. 1001, 1:63–2:2. “The server creates a new password by concatenating a secret passcode that is known to the user with the token” and “sets the password associated with the user’s user ID to be the new password.” *Id.* at 2:2–6. A “communication module transmits the token to a personal communication device, such as a mobile phone or a pager carried by the user.” *Id.* at 2:6–8. Then, the user concatenates the secret passcode with the received token in order to form a valid password, which the user submits to gain access to the secure system. *Id.* at 2:8–11.

Figure 1, reproduced below, “illustrates an overview, including system components, of a user authentication system 100 according to a preferred embodiment of the present invention.” Ex. 1001, 4:2–4.



As shown in Figure 1, user authentication system 100 includes authentication Server 102, text messaging Service provider 104, personal communication device 106 carried by user 108, and secure system 110 to which the authentication system 100 regulates access. *Id.* at 4:9–13. “[P]ersonal communication device 106 is preferably a pager or a mobile phone having SMS (short message Service) receive capability.” *Id.* at 4:13–15. Secure system 110 can be “any system, device, account, or area to which it is desired to limit access to authenticated users.” *Id.* at 4:18–20.

User authentication server 102 is configured to require that user 108 supply authentication information through secure system 110 in order to gain access to secure system 110. Ex. 1001, 4:32–35. Authentication information provided by the user includes user ID 152, passcode 154 and user token 156. *Id.* at 4:36–37. User ID 152 may be publicly known and used to identify the user and passcode 154 is secret and only known to the user 108, whereas token 156 is provided only to user 108 by user authentication server 102 through personal communication device 106. *Id.* at 4:39–44. To gain access to secure system 100, user 108 combines token 156 with passcode 154 to form password 158. *Id.* at 4:52–53. Thus, user 108 needs to have personal communication device 106 in order to gain access to secure system 110. *Id.* at 4:46–48. Further, token 156 has a limited lifespan, such as 1 minute or 1 day. *Id.* at 4:44–45.

E. Challenged Claims

Petitioner challenges claims 1 and 3–6. Pet. 1. Claims 1 and 5, reproduced below with Petitioner’s identifiers included, are the independent claims at issue in this proceeding. Ex. 1001, 11:43–12:13, 12:20–47. Claims 3 and 4 depend from claim 1 and claim 6 depends from claim 5. *Id.* at 12:16–19, 12:48–52.

1. [1.0] A method of authenticating a user on a first secure computer network, the user having a user account on said first secure computer network, the method comprising:

[1.1] associating the user with a personal communication device possessed by the user, said personal communication device in communication over a second network, wherein said second network is a cell phone network different from the first secure computer network;

- [1.2] receiving a request from the user for a token via the personal communication device, over the second network;
- [1.3] generating a new password for said first secure computer network based at least upon the token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user;
- [1.4] setting a password associated with the user to be the new password;
- [1.5] activating access the user account on the first secure computer network;
- [1.6] transmitting the token to the personal communication device;
- [1.7] receiving the password from the user via the first secure computer network, and
- [1.8] deactivating access to the user account on the first secure computer network within a predetermined amount of time after said activating, such that said user account is not accessible through any password, via said first secure computer network.

5. [5.0] A user authentication system comprising:

- [5.1] a computer processor,
- [5.2] a user database configured to associate a user with a personal communication device possessed by the user, said personal communication device configured to communicate over a cell phone network with the user authentication system;
- [5.3] a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user to be the new password;
- [5.4] a communication module configured to transmit the token to the personal communication device through the cell phone network, and

[5.5] an authentication module configured to receive the password from the user through a secure computer network, said secure computer network being different from the cell phone network, [5.6] wherein the user has an account on the secure computer network, wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via the secure computer network.

Ex. 1001, 11:43–12:13, 12:20–47.

F. Prior Art and Asserted Grounds

Petitioner asserts that claims 1 and 3–6 would have been unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
5	103	Veneklase, ¹ Jonsson ²
1, 3–6	103	Kew, ³ Sormunen ⁴

G. Evidence

Petitioner supports its challenged with the Declaration of Bruce McNair (Ex. 1003) and the Supplement Declaration of Bruce McNair (Ex. 1024). Patent Owner supports its Response with the Declaration of Rajeev Surati (Ex. 2003).

H. Consideration of Infringement Contentions

Petitioner contends that “(1) the Board may consider a party’s inconsistent positions from a different venue at the oral argument state of

¹ EP 0 844 551 A2, published May 27, 1998 (“Veneklase”) (Ex. 1005).

² WO 96/00485, published January 4, 1996 (“Jonsson”) (Ex. 1006).

³ WO 95/19593, published July 20, 1995 (“Kew”) (Ex. 1007).

⁴ WO 97/31306, published August 28, 1997 (“Sormunen”) (Ex. 1008).

this proceeding; and (2) [Patent Owner’s] contradictory statements should be given significant weight.” Pet. Supp. 1. Petitioner contends that “[t]he Board has broad discretion as to the conduct of the proceeding, including for issues not specifically addressed by the rules, and “may waive or suspend a requirement and place conditions on the waiver or suspension,” citing 37 C.F.R. §§ 42.5(a) and (b). *Id.*

Turning to the specifics of this Proceeding and the Board’s first question for which additional briefing was authorized, Petitioner contends that it was Patent Owner’s “noncompliance with mandatory discovery (Rule 42.51(b)(1)(iii)) and duty of candor” that led Petitioner to identify during oral argument what Petitioner asserts is Patent Owner’s inconsistent position. *Id.* Petitioner contends that while there is a general prohibition to the introduction of new evidence at an oral hearing, Patent Owner’s failure to serve amended infringement contentions (Ex. 1026) when it filed its Surreply was in violation of mandatory disclosure requirements and the duty of candor owed by parties to the Board. *Id.* Under these circumstances Petitioner contends the Board can and should waive this rule. *Id.* at 2 (citing *Dell Inc. v. Accelaron, LLC*, 884 F.3d 1364, 1369-70 (Fed. Cir. 2018)).

In answer to the Board’s second question, Petitioner contends that “Ex. 1026 should be afforded significant weight because it refutes [Patent Owner’s] arguments and discredits its expert’s verbatim assertions, while supporting Kew’s disclosure of the claimed ‘passcode’ of limitation [5.3].” Pet. Supp. 2.

Patent Owner responds that it complied with mandatory discovery and the duty of candor. PO Resp. to Supp. 1–3. Specifically, Patent Owner also responds that the “infringement contentions have been publicly available

since December 8, 2023, on the EDTX docket in the *JPMorgan Chase* consolidated case (exhibits to Dkt. 153), more than four months before oral argument” and “that proceeding was identified as a related matter in Patent Owner’s Mandatory Notices.” *Id.* at 1 (citing Paper 3). Patent Owner further responds that Rule 42.51(b)(1)(iii) applies only to “relevant information that is inconsistent with a position advanced by the party during the proceeding” and that the rule does not apply in the present instance because “the infringement contentions do not contain an inconsistent position.” *Id.* at 2.

Turning to the Board’s first question, Patent Owner contends that its position in the infringement contentions is not inconsistent with its position in this Proceeding because it has never argued that the claimed ‘passcode’ could not be a username. Instead, Patent Owner argued that “the claimed ‘passcode’ could not be *Kew*’s ‘user identification code.’” *Id.* at 3. Thus, Patent Owner contends that “it is too late for Petitioner to file a copy of the infringement contentions.” PO Resp. to Supp. 1.

In answer to the Board’s second question, Patent Owner contends that “the infringement contentions should be afforded no weight because they do not contain an inconsistent position.” PO Resp. to Supp. 3.

We agree with Patent Owner that it is too late for Petitioner to file a copy of the infringement contentions and argue that Patent Owner’s position in this Proceeding is inconsistent with its position in that proceeding. Petitioner had ample opportunity to raise its arguments about the infringement contentions well before the oral hearing. PO Resp. to Supp. 2. Patent Owner complied with our mandatory notice provision. Further, we agree with Patent Owner that its position in the infringement contentions is

not inconsistent with its position in this proceeding. Paper 3, 1. For these reasons, we decline to exercise our authority under 37 C.F.R. § 42.5(b) to consider the infringement contentions and the new arguments during an oral hearing.

II. ANALYSIS

A. *Principles of Law: Obviousness*

A claim is unpatentable as obvious under 35 U.S.C. § 103 if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations.⁵ See *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966).

The Supreme Court has made clear that we apply “an expansive and flexible approach” to the question of obviousness. *KSR*, 550 U.S. at 415. Whether a patent claiming the combination of prior art elements would have been obvious is determined by whether the improvement is more than the predictable use of prior art elements according to their established functions. *Id.* at 417. Reaching this conclusion, however, requires more than a mere showing that the prior art includes separate references covering each

⁵ The current record does not present or address any evidence of nonobviousness.

separate limitation in a claim under examination. *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011). Rather, obviousness requires the additional showing that a person of ordinary skill would have selected and combined those prior art elements in the normal course of research and development to yield the claimed invention. *Id.*

B. Level of Ordinary Skill in the Art

In determining the level of skill in the art, we consider the type of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level of active workers in the field. *Custom Accessories, Inc. v. Jeffrey-Allan Indus. Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986); *Orthopedic Equip. Co. v. U.S.*, 702 F.2d 1005, 1011 (Fed. Cir. 1983).

Petitioner contends that a person of ordinary skill in the art (“POSITA”)⁶ “for the ’658 Patent would have had at least (1) an undergraduate degree in electrical and computer engineering or a closely related field; and (2) two or more years of experience in security. EX1001, generally; EX1003, ¶¶49-51.” Pet. 5. Patent Owner does not address the level of ordinary skill in the art. *See generally* PO Resp.

Based on the record presented, including our review of the ’658 Patent and the types of problems and solutions described in the patent and the cited prior art, we adopt Petitioner’s assessment of the level of ordinary skill in the art and apply it for purposes of this Decision.

⁶ Person of ordinary skill in the art.

C. Claim Construction

We apply the claim construction standard articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc), and its progeny. Only terms that are in controversy need to be construed, and then only to the extent necessary to resolve the controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (in the context of an *inter partes* review, applying *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

Petitioner states that “all terms should be given their plain meaning.” Pet. 6. Yet, Petitioner proposes claim construction for “cell phone network” and “[n]ot known to the user.” Pet. 9–13.⁷ As these terms are not in controversy, we do not construe them.

“Patent Owner contends that the Board instituted *inter partes* proceedings based, in part, on an incorrect interpretation of claim 5.” PO Resp. 9. Specifically, Patent Owner contends that “[t]he plain language of claim 5 requires activation of account access in response to generation of the claimed ‘new password.’” *Id.* (citing Ex. 2003 ¶¶ 65–67). Patent Owner contends further that “it follows, from the plain language of the claim, that creation of that password is a prerequisite to the ‘authentication module activat[ing] access to the account in response to the password.’” *Id.* at 10 (citing Ex. 1001, 12:27–47; Ex. 2003 ¶¶ 65–67). In addition, Patent Owner contends that its “interpretation of claim 5 is also consistent with the preliminary construction issued by the Eastern District of Texas” and that we

⁷ Petitioner also acknowledges that the Board may construe some limitations as means-plus-function limitations. Pet. 6.

are “required to apply the same claim-construction standard as in Federal district court.” *Id.* at 11.

Petitioner replies that Patent Owner’s “proposed construction improperly attempts to import limitations from the specification into the claims, and should be rejected.” Pet. Reply 1 (citing Phillips, 415 F.3d at 1323). Petitioner replies further that “[n]onetheless, this construction has no bearing on the patentability of the challenged claims at least because . . . the prior art cited in the Petition renders the challenged claims obvious, even under the district court’s construction.” *Id.* Thus, according to Petitioner, “a construction of this term is not necessary to resolve this proceeding.” *Id.* at 1–2 (citing *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017)).

Patent Owner responds by reiterating its argument that “[t]he Board should adopt the same claim construction as the court.” PO Sur-reply 1.

For there reasons discussed in Section II.D.3 below, we agree with Petitioner that for Ground 1, the prior art cited in the Petition renders challenged claim 5 obvious, even under the district court’s construction. Pet. Reply 1. For the reasons discussed in Section II.D.4 below, Petitioner’s challenge is deficient regardless of our construction of this term. Accordingly, construction of the term is not necessary to resolve this proceeding.

D. Patentability Challenges

1. Prior Art

a) Veneklase (Ex. 1005)

Veneklase is a European Patent application published May 27, 1998. Petitioner asserts that Veneklase is prior art under pre-AIA 35 U.S.C. § 102(a) and (b). Pet. 1.

Veneklase’s “invention relates to a security and/or access restriction system . . . adapted to grant only authorized users access to a computer system and/or certain data.” Ex. 1005, 1:5–9. Veneklase is directed to preventing exposure and hacking of user passwords (*id.* at 2:2–21), theft of user access cards (*id.* at 2:22–37), and interception and decryption of encryption of keys (*id.* at 2:37–57). The invention provides “a technique to substantially prevent the unauthorized interception and use of transmitted data . . . by splitting the data into a plurality of separate communication channels, each of which must be ‘broken’ for the entire data stream to be obtained.” *Id.* at 3:3–11.

In Veneklase’s system individual 18, desiring access to and within computer 80, utilizes a first communication channel 82 (e.g., a first telephone line, radio channel, and/or satellite channel) and communicates, by use of his or her voice or by use of a computer 19, a first password to analyzing means 12. Ex. 1005, 6:5–10. “Analyzing means 12 then checks and/or compares this first received password with a master password list which contains all of the authorized passwords associated with authorized entry and/or access to computer 80.” *Id.* at 6:10–14. If the received password matches an entry of the master password list, analyzing means 12 causes the random code generation means 14 to generate a pseudo-

random number or code and to transmit the number and/or code via a second communications channel 84, to the individual 85 associated with the received password 202 in the master password list. *Id.* at 6:27–37. “Once the pseudo-random number is received by the analyzing means 12, from channel 82, it is compared with the number generated by generation means 14.” *Id.* at 6:51–54. If the two codes are substantially the same, entry to computer 80 or to a certain part of computer 80 such as the hardware, software, or firmware portions of computer 80 is granted to individual 18. *Id.* at 6:54–58.

b) Jonsson (Ex. 1006)

Jonsson is a Patent Cooperation Treaty application published January 4, 1996. Petitioner asserts that Jonsson is prior art under pre-AIA 35 U.S.C. § 102(a) and (b). Pet. 1.

Jonsson provides an authentication procedure wherein the user carries a personal unit not limited to use with or physically connected to a terminal of any one specific electronic service. Ex. 1006, 2:30–34. Jonsson’s personal unit includes a receiver for receiving a transmitted challenge code and an algorithm unit which processes the challenge code, a user input such as a personal identification number (PIN) or electronically recognizable signature, and an internally stored security key for calculating a response code according to a pre-stored algorithm. *Id.* at 6:24–29.

c) Kew (Ex. 1007)

Kew is a Patent Cooperation Treaty application published July 20, 1995. Petitioner asserts that Kew is prior art under pre-AIA 35 U.S.C. § 102(a) and (b). Pet. 1.

Kew's invention relates to a method for "preventing unauthori[z]ed access to a host computer system." Ex. 1007, 1:3–5. Specifically, Kew describes a "method of preventing unauthorized access to a host computer system by a user at a remote terminal." *Id.* at 1:21–23. In Kew's method the host computer system accepts a user identification code input to the terminal by the user and generates a random code (Code A). *Id.* at 1:24–26. Using a transformation algorithm, Kew's computer system transforms Code A to transformed Code B. *Id.* at 1:27–30. The computer system also transmits Code A to user's receiver which transform's Code A to transformed Code C. *Id.* at 1:31–34. The user inputs Code C into the remote terminal and the computer system compares Code B with Code C, and if the Codes match permits access to the host computer system. *Id.* at 1:36–2:3.

d) Sormunen (Ex. 1008)

Sormunen is a Patent Cooperation Treaty application published August 28, 1998. Petitioner asserts that Sormunen is prior art under pre-AIA 35 U.S.C. § 102(a) and (b). Pet. 1.

Sormunen's "invention relates to a method and system for obtaining at least one item of user specific authentication data, such as a password and/or a user name." Ex. 1008, 1:3–5. Sormunen discloses the use of mobile communication systems including cellular systems, paging systems, and mobile phone systems. *Id.* at 4:36–5:1.

2. Ground 1: Alleged Obviousness of Independent Claim 5 Based on the Combined Teachings of Veneklase and Jonsson

Petitioner asserts that claim 5 is unpatentable over the combined teachings of Veneklase and Jonsson. Pet. 13. Petitioner addresses each limitation of claim 5 and provides the testimony of Dr. McNair in support of

its position with respect to each limitation. Pet. 17–46; Ex. 1003 ¶¶ 71–111. Patent Owner does not contest Petitioner’s assertions for limitations [5.0]–[5.2] of claim 5. For these uncontested limitations, we have considered Petitioner’s evidence and arguments, including the relevant testimony of Dr. McNair, and find it to be sufficient to show by a preponderance of the evidence that Veneklas, either alone or in combination with Jonsson, teaches or suggests these limitations. Accordingly, we focus our discussion on contested limitations [5.3]–[5.6] and Patent Owner’s arguments regarding these limitations.

- a) *Limitation [5.3]: a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user to be the new password;*

(1) Petitioner’s Assertions

Petitioner asserts that “*Veneklas* in combination with *Jonsson* teaches this limitation.” Pet. 26 (citing Ex. 1003 ¶¶ 83–90). Regarding Veneklas, Petitioner asserts that Veneklas discloses assigning a password to the user; receiving the password by use of a first communication channel; generating a code in response to the received password; transmitting the code to the user via a second communications channel; transmitting the code to the computer; and allowing access to the computer only after the code is transmitted to the computer. *Id.* (citing Ex. 1005, 4:8–15).

Specifically, Petitioner asserts that “*Veneklas* discloses a user/password check module (i.e., a control module) located on the host computer system 402 (i.e., the computer processor)” and that the “user/password check module assigns two passwords, one that is known to

the user and one that is not previously known to the user.” Pet. 26–27 (citing Ex. 1005, Fig. 6).⁸ Petitioner asserts further that “[w]hile *Veneklase* teaches an authentication system in which the user inputs both a token that is not known to the user beforehand (e.g., the random code) and a passcode that is known to the user (e.g., the received password), it does not disclose creating a new password based on those two items.” *Id.* at 28.

Turning to Jonsson, Petitioner asserts that Jonsson discloses an authentication system that “includes a service node that ‘generates a challenge code and requests that the challenge code be sent to the personal unit 20 via an authentication challenge network 28’” and that “[t]his challenge code generated by the system is a *token* because it is not known to the user before it is generated and sent to the user.” Pet. 28 (citing Ex. 1006, 4:24–5:6; Ex. 1003 ¶¶ 86–87). Petitioner asserts further that “*Jonsson* discloses the use of a ‘user input such as a personal identification number (PIN),’ which by its very nature of being a user defined input, is known to the user beforehand” and that “*Jonsson* discloses an algorithm that ‘calculates a response code [e.g., new password] based on the received challenge code [e.g., token], the user input (e.g., PIN) [e.g., passcode], and optionally [a] secret key.’” Pet. 29 (citing Ex. 1006, 3:3–10, 7:5–10, 8:12–14, 9:23–25).

Petitioner asserts that it would have been obvious to combine *Veneklase*’s token and passcode to “create a new password based on both of them.” *Id.* at 28. Petitioner then asserts that “*Veneklase*’s authentication system would incorporate *Jonsson*’s teachings related to using an algorithm

⁸ Here and for the remainder of this decision, we do not reproduce the colored font or bold emphasis used in the Petition.

to create a new password (e.g., response code) based on a known passcode (e.g., the received password/PIN) and an unknown token (e.g., the random code/challenge code).” *Id.* at 30 (citing Ex. 1003 ¶¶ 83–89). Thus, according to Petitioner,

Veneklase in combination with *Jonsson* teaches a control module (e.g., user/password check module) executed on the computer processor configured to create a new password (e.g., assigning a password to the user) based at least upon a token (e.g., random code) and a passcode (e.g., received password), wherein the token is not known to the user (e.g., generated by the system) and wherein the passcode is known to the user (e.g., received from the user), the control module further configured to set a password associated with the user to be the new password (e.g., set an expected response code).

Id. (citing Ex. 1003 ¶¶ 83–90).

In support of these assertions, Petitioner reasons that “[a] POSITA would have been motivated to make such a combination because having only the one password transmitted via the computer system is more efficient and secure.” Pet. 31 (citing Ex. 1003 ¶ 91). According to Petitioner, “*Veneklase*’s system allows for authentication through user input of a known and unknown code at separate times in a two-step process, while a POSITA would look to *Jonsson* because it would provide the added benefit of reducing the steps to a single step and thus reducing the amount of time required for the authentication process.” *Id.* Petitioner reasons further that “a POSITA would have been motivated to make such a combination because implementing *Veneklase*’s authentication system with the algorithm of *Jonsson*’s system provides an additional layer of security.” *Id.* at 31–32. According to Petitioner, a person of ordinary skill in the art “would have understood that the algorithm system has the added security benefit of

preventing unauthorized personnel from being able to access the system by engaging in SIM swapping.” *Id.* at 32.

In addition, Petitioner asserts that Veneklase “explicitly discloses embodiments in which data streams are encoded and decoded using algorithms for additional security.” Pet. 32 (citing Ex. 1005, 9:26–10:11; *KSR*, 550 U.S. at 418–419). Thus, according to Petitioner, “a POSITA would have been motivated to use an algorithm for creating a new password based on the known password and the previously-unknown randomly generated code, such as described in *Jonsson*, to provide additional security.” *Id.* (citing Ex. 1003 ¶ 92). And, Petitioner asserts that “[a] POSITA would further be motivated to combine *Veneklase* and *Jonsson* because the combination merely uses a known technique to improve similar devices in the same way.” *Id.* at 33 (citing *KSR* 550 U.S. at 401).

(2) Patent Owner’s Response

Patent Owner contends that “modifying *Veneklase*’s system by abolishing the two-step authentication process, as proposed by Petitioner, would violate *Veneklase*’s principle of operation.” PO Resp. 18. According to Patent Owner, “this two-step authentication process is a key feature of *Veneklase*’s principle of operation, and a POSITA would not seek to remove steps as Petitioner proposes” and that Veneklase provides unequivocal support for this position. *Id.* at 18–19 (citing Ex. 2003 ¶ 76; Ex. 1005, 7:16–28). Patent Owner contends that “the proposed modification of *Veneklase* is far too drastic to be considered obvious, and thus the combination of *Veneklase* and *Jonsson* fails to render claim 5 obvious.” *Id.* at 18 (citing MPEP § 2143.01(VI); *Plas-Pak Indus. v. Sulzer Mixpac AG*, 600 F. App’x. 755, 758 (Fed. Cir. 2015)).

Patent Owner contends further that “Petitioner provides zero evidence that the security of its proposed combination is superior to the existing multi-layer/level security in *Veneklase*.” PO Resp. 20–21 (citing Ex. 2003 ¶ 78). Specifically, with regard to Petitioner’s Sim swapping argument, Patent Owner contends that the proposed combination would provide better protection from hackers “because the hackers would still need *Veneklase*’s password.” *Id.* at 21 (citing Ex. 2003 ¶ 79). Thus, according to Patent Owner, “there is no motivation to combine *Veneklase* and *Jonsson*.” *Id.*

In addition, Patent Owner contends that the portion of *Veneklase* cited by Petitioner in support of its assertion that *Veneklase* provides explicit motivation for using *Jonsson*’s algorithm in *Veneklase*’s system “is not related to the authentication algorithm disclosed by *Jonsson*.” PO Resp. 22. Patent Owner also argues, with regard to this limitation, that the proposed combination “would be more prone to Denial of Service (DoS) attacks by hackers.” *Id.* at 21 (citing Ex. 2003 ¶ 79).⁹

Specifically, Patent Owner contends that Patent Owner contends that “if the proposed combination still relies on *Jonsson*’s teachings to identify the user’s device, then Petitioner is assuming that *Jonsson*’s ‘authentication request’ is not a password (i.e., not a secret)”, and “[i]f *Jonsson*’s ‘authentication request’ is not a password, then the proposed combination is open to Denial of Service attacks (DoS).” PO Resp. 28 (citing Ex. 2003 ¶ 90). Patent Owner contends that “[t]his is a flaw in *Jonsson*’s architecture and a flaw in the proposed combination” and that “*Veneklase*’s system with

⁹ Patent Owner provides its explanation of this argument in Section V.A.1.ii of its Response which pertains to limitation [5.4]. PO Resp. 28. We, however, address this argument in this section, where it is first raised.

its two passwords does not suffer from this flaw” such that “there is no motivation to combine *Veneklase* and *Jonsson* as proposed by Petitioner.” *Id.*

(3) Petitioner’s Reply

In reply to Patent Owner’s argument that the proposed modification would destroy Veneklase’s principle of operation, Petitioner asserts that Patent Owner “does not offer any evidence that the proposed modified system would have been inferior or that it would not work for Veneklase’s stated goal to ‘ensure that only authorized users gain access to a computer system.’” Pet. Reply 3 (citing Ex. 1005, 3:31–33). Petitioner asserts further that “superiority is not a requirement for a finding of obviousness.” *Id.* (citing *Bayer Pharma AG v. Watson Labs, Inc.*, 874 F.3d 1316, 1327 (Fed. Cir. 2017)).

Turning to Patent Owner’s argument that the proposed combination would not prevent SIM swapping, Petitioner asserts that “the proffered combination would require access to the user’s device, which augments the security of the system by preventing SIM swapping, and negates any concerns over a hacker knowing a password.” Pet. Reply 4 (citing Pet. 32). According to Petitioner, “the hacker would need to know the password **and** have the user’s actual device in order to gain access to the system.” *Id.* As such, Petitioner asserts that “the proposed modification alters the method of operation, but does not destroy the intended purpose of providing security.” *Id.*

In reply to Patent Owner’s “Denial of Service” argument, Petitioner asserts that a “Denial of Service” attack is

characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. DoS attacks are aimed at devices and networks with exposure to the Internet. Their goal is to cripple a device or network so that external users no longer have access to network resources. **Without hacking password files or stealing sensitive data**, a denial-of-service hacker simply fires up a program that will generate enough traffic to a particular site that it denies service to the site's legitimate users.

Pet. Reply 4–5 (quoting Ex. 1019, 1:14–23). According to Petitioner, a DoS¹⁰ attack is not dependent on knowing a password and the combined system “would not be ‘more prone’ to DoS attack.” *Id.* at 5 (citing Ex. 1024 ¶¶ 7–9). Thus, Petitioner asserts that a person of ordinary skill in the art “would not be discouraged from combining Veneklasé’s system with the teachings of Jonsson based on any possibility of increased DoS attacks.” *Id.*

(4) Patent Owner’s Sur-reply

In response to Petitioner’s Reply, Patent Owner reiterates its position that the proposed combination would change Veneklasé’s principle of operation. PO Sur-reply 2–3. Patent Owner also reiterates its arguments regarding SIM swapping, “Denial of Service,” and lack of motivation to combine Veneklasé and Jonsson. *Id.* at 3–6.

(5) Discussion

We disagree with Patent Owner’s argument that the proposed modification would violate Veneklasé’s principle of operation. PO Resp. 18. Veneklasé is directed to “a security and/or access restriction system . . . which is adapted to grant only authorized users access to a computer system and/or to certain data which may be resident within the computer system

¹⁰ Denial of Service.

and/or resident within a communications channel and/or other communications medium.” Ex. 1005, 1:5–12. The portion of Veneklas cited by Patent Owner to support its position states that

Applicant’s foregoing computer security embodiment, utilizes two distinct communications channels and a random number generator in order to ensure that an authorized user of a computer system is notified that someone or something is seeking access to the computer system with his or her password. Moreover, Applicant’s foregoing invention is very cost effective as it employs substantially “off the shelf” and readily available components. Further, the use of a “secret” password, a “secret” substantially random number, and a “secret” second channel allows for multiple levels of security before access to the computer system is achieved and provides enhanced security over the prior art.

Ex. 1005, 7:16–28. We do not agree with Patent Owner that these statements unequivocally support its position that Veneklas’s two-step authentication process is a principle of operation of its system. Rather, the quoted statements indicate that Veneklas’s use of two distinct communication channels and a random number generator are key features of Veneklas’s system that provide multiple levels of security and enhance security of that system. As modified Veneklas’s system still uses two distinct communication channels and a random number generator. Thus, to the extent that Veneklas’s enhanced security measures (i.e. two distinct communication channels and a random number generator) are a principle of operation of Veneklas’s system, the proposed modification does not destroy this principle of operation or render Veneklas’s system inoperable.

Moreover, incorporating Jonsson’s teachings related to using an algorithm to create a new password would not destroy the principle of operation of Veneklas’s security system because it only changes how

Veneklase accomplishes its goal of preventing unauthorized access to a computer system, rather than defeating its goal of preventing such access. *See In re Mouttet*, 686 F. 3d 1322, 1332 (Fed. Cir. 2012). Further, we do not agree that *Plas-Pak* (a routine decision¹¹) supports Patent Owner’s contention that the proposed combination impermissibly changes Veneklase’s principle of operation as Patent Owner has not identified differences between the two authentication processes that would be “unlikely to motivate a person of ordinary skill to pursue” the proposed combination. *Plas-Plak*, 600 F. App’x at 757-59.

We also disagree with Patent Owner’s argument that there is no motivation to combine Veneklase and Johnson. PO Resp. 20–21. Petitioner does not propose modifying Veneklase to include Jonsson’s teachings solely because the security of the proposed combination is superior to the security in Veneklase. Rather, Petitioner asserts that “[a] POSITA would have been motivated to make such a combination because having only the one password transmitted via the computer system is more *efficient* and secure.” Pet. 31 (citing Ex. 1003 ¶ 91). The Petition explains how the combination is more efficient in that it requires only a single step which reduces the amount of time required for the authentication process. *Id.*

We also agree with Petitioner’s reasoning that a person of ordinary skill in the art would have been “motivated to combine *Veneklase* and

¹¹ “A routine decision is binding in the case in which it is made, even if it is not designated as precedential or informative, but it is not otherwise binding authority.” Patent Trial and Appeal Board, Standard Operating Procedure 2 (Rev. 11) 2 (July 24, 2023), *available at* https://www.uspto.gov/sites/default/files/documents/20230724_ptab_sop2_rev11_.pdf.

Jonsson because the combination merely uses a known technique to improve similar devices in the same way.” Pet. 33 (citing *KSR*, 550 U.S. at 401).

Jonsson discloses a known algorithm and *Veneklase* discloses a system that is similar to *Jonsson*’s. In the absence of any evidence that applying *Jonsson*’s algorithm to *Veneklase*’s system is beyond the skill of a person of ordinary skill in the art, we agree that “the improvement is [no] more than the predictable use of prior art elements according to their established functions.” *KSR*, 550 U.S. at 401.

In addition, we disagree with Patent Owner’s argument that *Veneklase* doesn’t provide explicit motivation for the proposed combination because “the section of *Veneklase* cited by Petitioner does not pertain to an algorithm.” PO Resp. 22. The cited portion of Exhibit 1005 discloses, in relevant part, that

System 70, as further shown, includes a data stream dividing means 74 which in one embodiment comprises a commercially available one input and two channel output time division or statistical multiplexor which samples the bits of received data and places, in a certain predetermined manner (e.g. alternately) some of the received data bits onto the first communications channel 76 and some of the received data bits onto the second communications channel 78. In this manner, one attempting to wrongfully intercept and/or access the data stream 72 would need access to both communications channels 76, 78 and would need to know the dividing *algorithm* that dividing means 74 utilizes to divide the received data for placement onto channels 76, 78.

Ex. 1005, 9:33–48.

The cited portion further states, in relevant part, that

security system 70 further includes a decoding means 88 which may comprise a commercially available microprocessor operating under stored algorithmic program control and which contains “mirror image” of the *algorithm* used to divide the data

stream transmitted to it by means 74. In this manner, the data from each of the channels 76,78 is reconstituted onto single channel 89, in substantially the exact same manner that it was received by means 74.

Id. at 9:50–58. Thus, the cited portion of Veneklas does pertain to an algorithm. Moreover, assuming that Patent Owner is correct that “the ‘algorithm’ disclosed by *Veneklas* is not related to the authentication algorithm disclosed by *Jonsson*,” this is inapposite. The question before us is not whether Jonsson’s algorithm is related to an algorithm that already exists in Veneklas, the question is whether it would have been obvious to modify Veneklas to use Jonsson’s algorithm.

Further we agree with Petitioner that “a DoS attack is not dependent on knowing a password” and the combined system “would not be ‘more prone’ to DoS attack.” We credit Dr. McNair’s testimony regarding this issue. Pet. Reply 5 (citing Ex. 1024 ¶¶ 7–9).

b) Limitation [5.4]: a communication module configured to transmit the token to the personal communication device through the cell phone network;

(1) Petitioner’s Assertions

Petitioner asserts that “*Veneklas* discloses that ‘host computer 402 checks the received identification code and cross references the received password code against a pager phone number list resident within the user table 414 which is stored within computer 402.’” Pet. 35 (quoting Ex. 1005, 8:1–5). Petitioner asserts further that “the generated random number code and pager number are passed ‘to the commercially available and conventional automatic dialer 418,’ which ‘telephones the conventional and commercially available pager 420 by means of conventional and commercially available communication channel 422 (e.g., voice line) and

transmits the code to the user's pager.” *Id.* (citing Ex. 1005, 7:52–8:17, Fig. 6).¹²

Thus, according to Petitioner, “*Veneklase* teaches a communication module (e.g., automatic phone/pager dialer 418) configured to transmit the token to the personal communication device through the cell phone network (e.g., transmit the random code through communication channel 422).” Pet. 37 (citing Ex. 1003 ¶¶ 97–100). Petitioner asserts that “[a] POSITA would have understood that the ‘conventional and commercially available communication channel 422’ described in *Veneklase* is the same type of cell phone network disclosed in the ’658 patent, which repeatedly makes clear that it covers both networks that communicate with cell phones and those that communicate with pagers.” *Id.* at 36.

(2) Patent Owner’s Response

After noting that “following Petitioner’s proposed modification to *Veneklase*, the user in *Veneklase* no longer transmits the password to the system,” Patent Owner contends that “*Veneklase* needs the received password to lookup the phone number of the user in a password list and transmit the randomly generated code to the user’s pager.” PO Resp. 25. Given this alleged need in *Veneklase*, Patent Owner contends that the Petition is silent on how “the user’s phone number will be identified, and thus how the randomly generated code will be transmitted to the user’s pager.” *Id.* According to Patent Owner, “[w]ith *Veneklase*’s modified system being unable to search the password list for a phone number, and thus unable to transmit the randomly generated code to the user’s pager,

¹² The Petition cites Ex. 1006. *Veneklase*, however, is Ex. 1005.

Veneklas’s modified system is inoperative.” *Id.* at 25–26 (citing Ex. 2003 ¶ 86).

Patent Owner contends further that “Jonsson’s teachings still require looking up the user’s phone number” and that

if the proposed combination still relies on *Jonsson*’s teachings to identify the user’s device, then the overall authentication process in the proposed combination still has two steps: (1) the user transmits *Jonsson*’s “authentication request” to the system to trigger generation of a “challenge code” . . . then (2) the user transmits the “response code.” (Ex. 1006, 9:26-30, 11:4-13, Fig. 3) to the system.

PO Resp. 26–27 (citing Ex. 1006, 9:1–4, 9:26–30, 10:18–20, 11:4–13, Fig. 3). Thus, according to Patent Owner, “Petitioner’s rationale for combining *Veneklas* and *Jonsson* is not actually realized, and a POSITA would not be motivated to execute the proposed combination.” *Id.* at 27 (citing Ex. 2003 ¶ 89).

(3) Petitioner’s Reply

Replying to Patent Owner’s argument that the proposed combination would render *Veneklas* inoperable, Petitioner asserts that “the Petition relies on the combination of *Veneklas* and *Jonsson* to identify the device in response to the request for authorization as described in *Jonsson*” and that “the Petition is clear that it is *Jonsson*’s use of only a *single transmitted password* that allows for enhanced security over the twice transmitted password of *Veneklas*.” Pet. Reply 5–6 (citing Pet. 30–32).

(4) Patent Owner’s Sur-Reply

Patent Owner responds to Petitioner’s argument that the proposed combination relies on *Jonsson*’s transmission of a single password, by reiterating its argument that the proposed combination does not actually

reduce the number of steps required such that a person of ordinary skill in the art would not be “motivated to execute the proposed combination. PO Sur-reply 7 (citing PO Resp. 27).

(5) *Discussion*

We disagree with Patent Owner’s characterization of the proposed modification as it pertains to limitation [5.4]. It is our understanding that in the proposed combination, the user’s device would be identified in accordance with Jonsson’s teachings not Veneklasē’s. *See* Pet. 30–32. In other words, the user’s device would be identified in response to the user’s request for authentication as described in Jonsson. *See e.g.*, Ex. 1006, 9:2–8; 10:13–27, Fig. 3). Accordingly, the ability to look up the user’s phone number is not a requirement of the combination and Patent Owner’s argument is inapposite.

- c) *Limitation [5.5]: an authentication module configured to receive the password from the user through a secure computer network, said secure computer network being different from the cell phone network,*

(1) *Petitioner’s Assertions*

Petitioner asserts that “[i]n the combination with *Jonsson* discussed with respect to element [5.3], a POSITA would have understood that the new password . . . being sent back to computer 402 and compared against the expected value is the one created by the algorithm based on both the known passcode . . . and the randomly generated token.” Pet. 38 (citing Ex. 1003 ¶¶ 83–89). Petitioner asserts further that “*Veneklasē* discloses that [the] communication in which the user submits its credentials to the host computer and the initial sending of the random code to the personal device ‘[utilizes] two distinct communication channels.’” *Id.* at 39 (citing Ex. 1005,

3:50–4:3, 7:11–28). Petitioner also asserts that a “POSITA would have understood that [Veneklasé’s] communication network is [a] secure computer network because the use of the authentication procedures described in *Veneklasé* make secure the host computer system.” *Id.* at 40 (citing Ex. 1005, 9:3–14; Ex. 1003 ¶¶ 101–104).

(2) *Patent Owner’s Response*

Patent Owner contends that “Petitioner presents zero evidence that *Veneklasé*’s ‘pager 420’ is capable of executing” Jonsson’s algorithm. PO Resp. 30. Patent Owner contends further that “*Jonsson* expressly states that its algorithm requires a highly specialized ‘personal unit,’ not just an off-the-shelf pager” and that “‘the personal unit is a separate unit, thereby minimizing or avoiding the need to customize a [personal] communication device,’ which teaches away from the Petitioner’s proposed combination.” *Id.* (citing Ex. 1006, 6:24–7:26, Fig. 2; Ex. 2003 ¶ 95). According to Patent Owner, the fact that . . . Jonsson indicates that a personal communication device would require customization, “indicates that *Veneklasé*’s ‘pager 420’ is not capable of executing” Jonsson’s algorithm. *Id.* (citing Ex. 2003 ¶ 96).

(3) *Petitioner’s Reply*

Petitioner replies that Patent Owner’s argument “is directly contradicted by Jonsson’s disclosure, as noted by the Board, ‘the capacity for performing the necessary calculations exists in conventional cellular telephones and personal communication units [(i.e., pagers)], allowing the present invention to be implemented through software’” and that Jonsson’s statements about a preferred embodiment requiring a separate unit does not obviate Jonsson’s teachings. Pet. Reply 6–7 (citing Paper 9, 22; Ex. 1006, 7:21–31).

(4) *Patent Owner's Sur-reply*

Patent Owner responds that Petitioner misrepresents its argument in that it is arguing that Veneklase's pager could not perform Jonsson's algorithm, not that it was arguing that the pager could not perform any algorithm. PO Sur-reply 8. According to Patent Owner, "neither Petitioner nor its expert muster any evidence that an off-the-shelf pager, in 1996, could execute *Jonsson's* specialized security algorithms." *Id.*

(5) *Discussion*

We disagree with Patent Owner's arguments. Jonsson explicitly teaches that "the capacity for performing the necessary calculations exists in conventional cellular telephones and *personal communication units*, allowing the present invention to be implemented through software." Ex. 1006, 7:27–31 (emphasis added). Jonsson further explains that "personal unit 20 can be essentially a conventional pager." *Id.* at 6:29–31. Thus, Jonsson's disclosure provides evidence that pagers, such as Veneklase's pager 420, are capable of executing Jonsson's algorithm.

Moreover, Patent Owner's arguments appear to be based on whether or not Jonsson's algorithm can be physically performed with Veneklase's pager. This, however, is not the relevant inquiry. The relevant inquiry is whether the claimed subject matter would have been obvious to those of ordinary skill in the art in light of the *combined teachings* of Veneklase and Jonsson. *See In re Keller*, 642 F.2d 413, 425 (CCPA 1981). Further, "[i]t is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of the elements." *In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012).

- d) *Limitation [5.6]: wherein the user has an account on the secure computer network, wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via the secure computer network.*

(1) Petitioner's Assertions

Petitioner asserts that Veneklas discloses that the user 404 sends a “password or pseudo-random code back to computer 402 where it is compared within the software subroutine module denoted as “code compare” 416 in Figure 6’ and ‘[i]f the comparison yields a match, the user 404 is allowed access to computer 402 and/or to a portion of computer 402.’” Pet. 41 (citing Ex. 1005,¹³ 6:45–7:10, 8:18–27). Petitioner asserts further that “Veneklas discloses an embodiment which ‘includes a timer or “timing means” 40 which may comprise one or more software subroutines which are adapted to operate and/or execute within and/or upon computer 80,’ such as a watchdog timer.” *Id.* at 42 (citing Ex. 1005, 8:28–39).¹⁴

Petitioner asserts that in the combination with Jonsson “a POSITA would have understood that the new password (e.g., response code) being sent back to computer 402 and compared against the expected value is the one created by the algorithm based on both the known passcode (e.g., PIN) and the randomly generated token (e.g., challenge code).” Pet. 43 (citing Ex. 1003 ¶¶ 83–89). Thus, according to Petitioner, “the predetermined period would be the time between the receipt of the token (e.g., randomly

¹³ The Petition cites Ex. 1006; however, Veneklas is Ex. 1005.

¹⁴ See note 5.

generated challenge code) and the sending back of the newly created password (e.g., response code).” *Id.*

Turning to the deactivating part of limitation [5.6], Petitioner asserts that “*Veneklase*’s teaching is within the scope of the recited deactivating limitation because it is nearly identical to how this limitation is described in the ’658 Patent.” Pet. 43.

(2) Patent Owner’s Response

Patent Owner contends that “the Petition incorrectly identifies a process that occurs after compare module 416 receives the alleged ‘password’ from the user, unlike claim 5, which requires that the ‘authentication module’ activates access to the account in response to creation of the new ‘password,’ not in response to receiving the ‘password’ from the user.” PO Resp. 35–36 (citing Ex. 2003 ¶ 99). Patent Owner contends further that “Petitioner’s argument is flawed on its face because the claimed ‘predetermined amount of time’ is the timeframe between activation and deactivation of the account.” *Id.* at 36 (citing Ex. 1001, 12:20–47).

In addition, Patent Owner contends that “even if Petitioner were correct, that configuration would be contrary to the claim language, which requires that the ‘authentication module’ activate and deactivate access to the account.” *Id.* (citing Ex. 1001, 12:37–47). Patent Owner contends further that “[b]ecause the Petition alleges that the ‘predetermined period of time’ begins with ‘receipt of the token (e.g., randomly generated challenge code)’ by ‘pager 420’ it would be the ‘personal communication device,’ not the ‘authentication module’ . . . that activates access to the account.” *Id.* at 37 (citing Pet. 43; Ex. 2003 ¶ 101). Finally, Patent Owner argues that “the period of time identified in the Petition is not predetermined; rather, it is

driven by the user's activity, which is contrary to the plain language of this claim element.” *Id.* (citing Ex. 2003 ¶ 102).

(3) Petitioner's Reply

In reply to Patent Owner's argument that “Veneklasé does not activate access in response to the ‘creation of the new ‘password,’” Petitioner asserts that “the claim does not include the language ‘creation of’ or any variation thereof. Thus, [Patent Owner's] attempts to import unclaimed limitations from the specification should be rejected.” Pet. Reply 7 (citing PO Resp. 35; *Phillips*, 415 F.3d at 1323). Petitioner replies further that “the combination of Veneklasé and Jonsson discloses this limitation even under the court's [and Patent Owner's] interpretation.” *Id.*

Specifically, Petitioner asserts that “Jonsson discloses creating ‘an expected response code,’ (e.g., password), at which point access to the account is activated, and access is granted when the ‘expected response code’ matches the received response code.” Pet Reply 8 (citing Ex. 1006, 10:2–5). According to Petitioner, a person of ordinary skill in the art “would have understood that the ‘expected’ response code indicates that the account access is activated because it is awaiting (i.e., expecting) a response” and “[a]s such, Jonsson teaches activating access to the account in response to the creation of the password under the district court's interpretation.” *Id.* (citing Ex. 1024 ¶ 17).

Petitioner asserts further that “Jonsson discloses that “the challenge code and the response is unique for each transaction” and “[a]s such, a POSITA would have understood that account access is not activated prior to the sending of the challenge code to the user and the creation of the expected response code (e.g., new password) at least because prior response codes

would not have worked.” Pet. Reply 8 (citing Ex. 1006, 3:16–18; Ex. 1024 ¶ 18).

In reply to Patent Owner’s argument that “the claimed predetermined amount of time is the timeframe between activation and deactivation of the account,” Petitioner asserts that a person of ordinary skill in the art “would have understood that this claim limitation simply means any predetermined period *after* activation.” Pet Reply 9 (citing PO Resp. 36; Ex. 1024 ¶ 19). Petitioner asserts further that

In the combined system of Veneklas and Jonsson, the predetermined period would include the time from receiving the challenge code (at or after account activation, as discussed above) and the sending of the response code, which would be governed by Veneklas’s teaching that the password must be “received within a predetermined period of time.”

Id. (citing Ex. 1005, 8:40–49; Ex. 1024 ¶ 19).

In reply to Patent Owner’s argument that in the proposed combination it would be the personal communication device not the authentication module that activates access to the account, Petitioner asserts that Patent Owner’s argument “is again based on a misunderstanding of the claim limitation that the predetermined amount of time must include the entire time from activation of the account to deactivation of the account.” Pet. Reply 9–10 (citing Ex. 1024 ¶ 20). According to Petitioner, “this is simply not what the claim recites. Rather, the claim recites ‘deactivates the account *within* a predetermined amount of time *after* activating the account’” such that “the predetermined amount of time begins at some point after activation.” *Id.* at 10. Based on this understanding of the claim limitation, Petitioner asserts that “this limitation is met by Veneklas’s teaching that the password must be ‘received within a predetermined period of time’ . . .

applied to Jonsson’s sending of the response code after receiving the challenge code” such that “the ‘authentication module’ (i.e., ‘code compare module 416’ in the ‘host computer’) is responsible for account deactivation.” *Id.* (citing Ex. 1005, 8:40–49; Ex. 1024 ¶20).

In reply to Patent Owner’s argument that in the proposed combination the predetermined period of time varies, Petitioner asserts that “this line of attack completely ignores Veneklasé’s teaching that the password must be ‘received within a predetermined period of time.’” Pet. Reply 10 (citing Ex. 1024 ¶ 21).

(4) Patent Owner’s Sur-Reply

Patent Owner responds that Petitioner has changed its mapping with respect to the “activates access to the account” limitation and “should be held to its original mapping.” PO Resp. 10. Turning to the “predetermined amount of time” limitation, Patent Owner reiterates its position that “the claimed ‘predetermined amount of time’ should be construed as the entire window between activation and deactivation of the account” and that the claimed “predetermined period of time” does not read on Veneklasé’s “predetermined amount of time.” *Id.* at 11–12.

Patent Owner also reiterates its position that in the proposed combination the authentication module does not deactivate the account and that in the proposed combination the “predetermined period of time” varies in that the length of that time is user dependent. PO Resp. 11–13.

(5) Discussion

We agree with Petitioner that Patent Owner’s argument are premised on a misunderstanding of this claim limitation. Patent Owner’s arguments read the specification (e.g. the flowchart shown in Fig. 5) into the limitation.

Moreover, we do not agree with Patent Owner that Petitioner has changed its mapping. Rather, Petitioner has provided further explanation of the basis of its challenge in response to Patent Owner's arguments.

Specifically, with regard to the requirement that the "authentication module activates access to the account *in response* to the password" we agree with Petitioner that the proposed combination would have rendered this limitation obvious to one of skill in the art even if the word "creation" is read into the limitation. Ex. 1001, 12:41–43. We also agree with Petitioner that the predetermined amount of time need not include the entire time from activation of the account to deactivation of the account and credit Dr. McNair's testimony that "this limitation is met by Veneklasé's teaching that the password must be 'received within a predetermined period of time' (EX1005, 8:40-49) applied to Jonsson's sending of the response code after receiving the challenge code EX1005, 8:40-49." Ex. 1024 ¶ 20.

In addition, we agree with Petitioner that Veneklasé teaches that the password must be received within a predetermined period of time, such that the proposed combination meets the deactivation requirement of this limitation. Pet. Reply 10 (citing Ex. 1024 ¶ 21).

e) Conclusion for Ground 1

For the reasons discussed above we find that each limitation of claim 5 is taught or suggested by Veneklasé and Jonsson and that a person of ordinary skill would have successfully combined the teachings of these references with a reasonable expectation of success. Based on our review of the entire record of this proceeding, we determine that Petitioner has shown, by a preponderance of the evidence, that claim 5 is unpatentable over the combined teachings of Veneklasé and Jonsson.

3. *Ground 2: Alleged Obviousness of Claims 1 and 3–6 Based on the Combined Teachings of Kew and Sormunen*

Petitioner asserts that claims 1 and 3–6 are unpatentable over the combined teachings of Kew and Sormunen. Pet. 46. Petitioner addresses each limitation of claims 1 and 3–6 and provides the testimony of Dr. McNair in support of its position with respect to these claims. Pet. 46–79; Ex. 1003 ¶¶ 112–167. Our determination for limitation [5.3] below is dispositive for claim 5 and its dependent claim 6, with respect to this ground. Further, as Petitioner relies on its assertions for claim 5 in its challenge to claim 1, it is also dispositive for claim 1, and its dependent claims 3 and 4. Pet. 72. Accordingly, we focus our discussion on limitation [5.3] and Patent Owner’s arguments regarding this limitation.

- a) *Limitation [5.3]: a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user to be the new password;*

(1) Petitioner’s Assertions

Petitioner asserts that

Kew discloses that after the user enters his user identification code, “the security server 5 then generates a random code (Code A) and subjects this number to an encryption using the same one-way algorithm as is stored in the user’s receiver 6 together with the corresponding identity code” to create a “transformed code (Code B).

Pet. 60–61 (citing Ex. 1007, 8:5–10). Petitioner asserts further that Kew “discloses that ‘the security server 5 also transmits the random code to a paging system 7 along with an identifier or identifying tag which can be

recognized by the receiver unit 6.” *Id.* at 61 (citing Ex. 1007, 8:12–15).

Petitioner asserts that

Kew discloses that after the receiver unit 6 receives the random number, it “uses the received random number and the identity code stored in its own EPROM to produce a transformed code (Code C) via its own characteristic algorithm,” which is the same as the one used by the security server 5 to produce transformed code (Code B).

Id. (citing Ex. 1007, 8:33–36). Petitioner asserts further that *Kew* “discloses that ‘terminal 2, at the behest of the security server 5 prompts the user to input the transformed Code C displayed by the receiver unit 6’ and then ‘security server 5 compares the input Code C with the transformed Code B.’” *Id.* citing (Ex. 1007, 9:5–11).

Based on these disclosures, Petitioner reasons that a person of ordinary skill in the art “would have understood that *Kew*’s security server is setting transformed Code B that it created by encryption to be the new password.” *Id.* (citing Ex. 1003 ¶¶ 136–139). Thus, according to Petitioner, *Kew* teaches a control module executed on the computer processor configured to create a new password (Code B) based at least upon a token (Code A) and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, wherein the control module is configured to set a password associated with the user to be the new password. Pet. 62–63 (citing Ex. 1003 ¶¶ 136–140).

(2) Patent Owner’s Response

Patent Owner contends that “the Petition does not teach or suggest this limitation because it fails to even consistently identify the alleged ‘passcode’ for . . . *Kew*.” PO Resp. 42. Specifically, Patent Owner contends that “[i]n one instance, Petitioner identifies *Kew*’s ‘identity code’ as the

claimed ‘passcode,’ and in another instance, Petitioner identifies the ‘actual name or PIN’ as the claimed ‘passcode.’” *Id.* (citing Pet. 62–63).

Patent Owner contends that “neither is the claimed ‘passcode.’” *Id.* (citing Ex. 2003 ¶108). Patent Owner contends that “*Kew*’s ‘identity code’ is not the claimed ‘passcode’ because this claim element requires that ‘the passcode is known to the user.’” *Id.* Patent Owner contends further that “*Kew*’s ‘actual name or PIN’ are not the claimed ‘passcode’ because neither is part of the claimed ‘password,’ along with the claimed ‘token,’ as is required by this claim element. *Id.* at 45–46 (citing Ex. 1001, 12:28–30).

(3) Petitioner’s Reply

Petitioner replies that “[t]he Petition identified the User ID/IdentityCode as the ‘passcode’ limitation. Pet. Reply 11. According to Petitioner, a person of ordinary skill in the art “would have understood that the ‘identity code’ ‘corresponds’ to a user-known identification code, which is entered by the user during the authentication process.” *Id.* (citing Ex. 1007, 3:1–6, 8:2–9). Petitioner replies further that a person of ordinary skill in the art “would have readily understood that both the user ID and the ‘corresponding identity code’ are used to generate a password in the event that they are not identical.” *Id.* at 12 (citing Ex. 1024 ¶ 24).

(4) Patent Owner’s Sur-reply

Patent Owner responds that *Kew*’s “identity code” is not the claimed “passcode” because “[t]he claim language is unequivocal: ‘the passcode is known to the user.’” PO Sur-reply 14 (citing Ex. 1001, 12:29–32). According to Patent Owner, “Petitioner is unable to identify any disclosure in *Kew* that the “identity code” is known to the user” and “[f]acing that

reality, Petitioner fabricates unrealistic scenarios to argue that *Kew*'s 'identity code' is known to the user." *Id.* (citing Pet. Reply 11–16).

Patent Owner responds further that *Kew*'s "user identification code" is not the claimed "passcode" because *Kew*'s user identification code is never combined with *Kew*'s Code A (identified in the Petition as corresponding to *Kew*'s token). PO Sur-reply 16. Patent Owner also responds that *Kew*'s "user identification code" and "identity code" are not the same. *Id.* at 17.

(5) *Discussion*

We agree with Patent Owner that Petitioner has not adequately demonstrated that *Kew*'s user identification code or identity code correspond to the claimed "passcode." *Kew*'s user identification code does not correspond to the claimed passcode, because it is not used in conjunction with a token to generate a new password as required by this limitation. Ex. 1007, 7–9. *Kew*'s identity code does not correspond to the claimed passcode because there is no indication in *Kew* that the user knows the identity code. *Id.* We further agree with Patent Owner that *Kew*'s "user identification code" and "identity code" are not the same as these terms are clearly used to denote different codes in *Kew*'s specification. *Id.*

Sormunen is not relied on to cure this deficiency in *Kew*. Pet. 60–63.

b) *Conclusion for Ground 2*

For the reasons discussed above, Petitioner has not demonstrated that *Kew* and Sormunen would have rendered claim 5 and its dependent claim 6 obvious to one of ordinary skill in the art. As the Petition relies on the challenge to claim 5 to meet the corresponding limitations of claim 1, Petitioner has also not demonstrated that claim 1 and its dependent claims 3

and 4 would have been obvious to a person of ordinary skill in the art. Based on our review of the entire record of this proceeding, we determine that Petitioner has not shown, by a preponderance of the evidence, that claims 1 and 3–6 are unpatentable over the combined teachings of Kew and Sormunen.

III. CONCLUSION

For the foregoing reasons, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claim 5 is unpatentable on the basis set forth in the following table. We also determine that Petitioner has not demonstrated, by a preponderance of the evidence, that claims 1, 3, 4, and 6 are unpatentable on the basis set forth in this table.¹⁵

¹⁵ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this Final Decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. §§ 42.8(a)(3), (b)(2).

Claim(s)	35 U.S.C. §	References	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
5	103(a)	Veneklase, Jonsson	5	
1, 3–6	103(a)	Kew, Sormunen		1, 3–6
Overall Outcome			5	1, 3, 4, 6

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, Petitioner has demonstrated by a preponderance of the evidence that claim 5 of U.S. Patent No. 6,993,658 B1 is unpatentable;

FURTHER ORDERED that, Petitioner has not demonstrated by a preponderance of the evidence that claims 1, 3, 4, and 6 of U.S. Patent No. 6,993,658 B1 are unpatentable; and

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

IPR2023-00425
Patent 6,993,658 B1

FOR PETITIONER:

Timothy Murphy
Jordan Rossen
UNIFIED PATENTS
tj@unifiedpatents.com
jordan@unifiedpatents.com

How-Ying Liou
Vishal Khatri
Matthew Johnson
Evan Tassis
JONES DAY
aliou@jonesday.com
vkhatr@jonesday.com
mwjohnson@jonesday.com
etassis@jonesday.com

For PATENT OWNER:

John Wittenzellner
Todd E. Landis
Michael J. Fagan, Jr.
Mark McCarthy
WILLIAMS SIMONS & LANDIS PLLC
johnw@wsltrial.com
tlandis@akingump.com
mfagan@wsltrial.com
mmccarthy@wsltrial.com