

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, KRISTEN L. DROESCH, and
LYNNE H. BROWNE, *Administrative Patent Judges*.

BROWNE, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314, 37 C.F.R. § 42.4

I. INTRODUCTION

Unified Patents, LLC (“Petitioner”) filed a Petition (Paper 1 (“Pet.”)) requesting institution of an *inter partes* review of claims 1 and 3–6 of U.S. Patent No. 6,993,658 B1 (Ex. 1001, “the ’658 Patent”). Dynapass IP Holdings LLC (“Patent Owner”) timely filed a Preliminary Response. Paper 8 (“Prelim. Resp.”).

Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted unless the information presented in the Petition and any response thereto shows “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” Upon consideration of the Petition and the evidence of record, we conclude that the information presented in the Petition establishes that there is a reasonable likelihood that Petitioner would prevail in challenging at least one of claims 1 and 3–6 of the ’658 Patent as unpatentable under the grounds presented in the Petition. Pursuant to § 314, we hereby institute an *inter partes* review as to the challenged claims of the ’658 Patent.

A. *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.

B. *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.

C. 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

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.

D. 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.

E. 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

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).

II. ANALYSIS

A. 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 (“POSITA⁵”) “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. “For the purposes of [the Preliminary] Response only, Patent Owner does not dispute the level of skill of a person of ordinary skill in the art (‘POSITA’) identified in the Petition.” Prelim. Resp. 11.

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.

B. 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.

⁵ Person of ordinary skill in the art.

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. 9–13.⁶

“Patent Owner contends that claim construction is not necessary for the Board to determine that the Petition fails to demonstrate a reasonable likelihood that any challenged claim of the ’658 Patent is unpatentable.” Prelim. Resp. 11.

At this stage of this proceeding, we agree with the parties that claim construction is not necessary.

C. Patentability Challenges

1. Principles of Law: Obviousness

A claim is unpatentable 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 at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art;

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

(3) the level of skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations.⁷ See *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966).

2. *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. *Id.* at 6:5–10. “Analyzing means 12 then checks and/or compares this first received password with a master password list

⁷ The current record does not present or address any evidence of nonobviousness.

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. Ex. 1006 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 unauthorized 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.

3. *Ground 1: Alleged Obviousness of Independent Claim 5*

Petitioner asserts that claim 5 is unpatentable over the combined teachings of Veneklas 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 them claim 5. 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 the uncontested limitations ([5.0]–[5.2]), we have considered Petitioner’s evidence and arguments with respect to these limitations, including the relevant testimony of Dr. McNair and find it to be sufficient to show that Petitioner has demonstrated a reasonable likelihood of prevailing in showing 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;*

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. Pet. 26 (citing Ex. 1005, 4:8–15).

Specifically, Petitioner asserts that “*Veneklase* 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).

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

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 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.

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).

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.” Prelim. Resp. 17. 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.” *Id.* (citing 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)).

We disagree with Patent Owner's arguments. *Veneklase* 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 and/or resident within a communications channel and/or other communications medium.” Ex. 1005, 1:5–12. Patent Owner has not adequately demonstrated that the two-step authentication process is a key feature of Veneklase’s principle of operation such that the proposed modification would render Veneklase’s system inoperable. Rather, Patent Owner relies on unsupported attorney argument. *See* PO Resp. 17–18.

Incorporating Jonsson’s teachings related to using an algorithm to create a new password would not destroy the principle of operation of Veneklase’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 nonprecedential decision) supports the 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.

Patent Owner contends that “Petitioner provides zero evidence that the security of its proposed combination is superior to the existing multi-layer/level security in *Veneklase*.” Prelim. Resp. 19. Thus, according to Patent Owner, “there is no motivation to combine *Veneklase* and *Jonsson*.” *Id.* at 20.

We disagree with Patent Owner’s arguments. Petitioner does not propose modifying Veneklasé to include Jonsson’s teachings solely because the security of the proposed combination is superior to the security in Veneklasé. 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.* Moreover, the Petition explains how the proposed combination is more secure than Veneklasé’s system in that it prevents unauthorized persons from accessing the computer system by engaging in SIM swapping. *Id.* at 32.

Patent Owner contends that the portion of Veneklasé cited by Petitioner in support of its assertion that Veneklasé provides explicit motivation for using Jonsson’s algorithm in Veneklasé’s system “does not pertain to an algorithm.” Prelim. Resp. 20 (citing Pet. 32 (citing Ex. 1005, 9:20–10:11)).

We disagree with Patent Owner’s argument. Petitioner asserts that Veneklasé “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). 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.

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

Petitioner asserts that “*Veneklase* 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).⁹

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

Patent Owner agrees that “*Veneklase*’s system uses the received password (i.e., the first step in the two-step process) to lookup the user’s phone number and transmit the randomly generated code to the user.” Prelim. Resp. 22–23 (quoting Ex. 1005, 8:2–15; 6:10–37). Noting that “Petitioner’s proposed combination includes replacing *Veneklase*’s two-step authentication process (i.e., user transmission of *Veneklase*’s password, and subsequent user transmission of *Veneklase*’s random code) with the single step in *Jonsson* (i.e., user transmission of *Jonsson*’s response code),” Patent Owner contends that “[t]he Petition is silent on how, following the proposed modification to *Veneklase* which abolishes user transmission of *Veneklase*’s password, the user’s phone number will be identified, and thus how the randomly generated code will be transmitted to the user’s pager.” *Id.*

⁹ The Petition cites Ex. 1006. *Veneklase*, however, is Ex. 1005.

at 23–24. 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, *Veneklase*’s modified system is inoperative,” and thus, “there is no motivation for the proposed modification.” *Id.* at 24.

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 Veneklase’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,*

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 “*Veneklase* 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 [Veneklase’s] communication network is [a] *secure computer network* because the use of the authentication procedures described in *Veneklase* make secure the host computer system.” *Id.* at 40 (citing Ex. 1005, 9:3–14; Ex. 1003 ¶¶ 101–104).

Patent Owner contends that Petitioner’s assertions “conveniently glosses over the fact that the proposed combination requires modifying *Veneklase*’s ‘pager 420’ to execute an algorithm that ‘calculates a response code based on the received challenge code [and] the user input (e.g., PIN),’ as performed by Jonsson’s ‘personal unit 20.’” Prelim. Resp. 26 (citing Ex. 1006, 8:12–14). Patent Owner further contends that “Petitioner presents zero evidence that *Veneklase*’s ‘pager 420’ is capable of executing such an algorithm.” *Id.*

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 [(i.e. pagers)], allowing the present invention to be implemented through software.” Ex. 1006, 7:27–31. Thus, Jonsson’s disclosure provides evidence that pagers, such as *Veneklase*’s pager 420, are capable of executing Jonsson’s algorithm.

In addition, Patent Owner contends that “Petitioner’s proposed combination also fails to disclose ‘an authentication module configured to receive the password from the user through a secure computer network.’” Pet. 27. As best understood, Patent Owner appears to be arguing that in Jonsson’s system the password is not “received from the user” because it is not displayed to the user.

The claim language at issue, however, does not require that the password be known to the user. Rather, it requires that it be received from the user (in other words from the user's device). Thus, Patent Owner's argument is unconvincing.

- 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.*

Petitioner asserts that Veneklasé 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. 1005,¹⁰ 6:45–7:10, 8:18–27). Petitioner asserts further that “*Veneklasé* 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).¹¹

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)

¹⁰ The Petition cites Ex. 1006; however, Veneklasé is Ex. 1005.

¹¹ See note 5.

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 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 “*Veneklas*’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.

Patent Owner contends that “neither asserted reference discloses activating an account. And the Petition fails to argue, let alone show, that either reference discloses activating account access in response to generation of the new ‘password,’ which is ‘based at least upon a token and a passcode.’” Prelim. Resp. 30–31 (citing Pet. 41–46). Patent Owner contends further that “[i]nstead, Petitioner incorrectly relies on steps in the prior art that occur well after the claimed ‘password’ is created.” *Id.* at 31.

We disagree with Patent Owner’s arguments. Claim 5 requires that the account be activated in response to the password. Ex. 1001, 12:41–43. It does not require that the account be activated in response to creation of the password. *Id.* On the record before us, Petitioner has adequately demonstrated that *Veneklas* discloses activation of the account in response to the password. *See* Pet. 41–42.

In addition, Patent Owner argues “that ‘the predetermined period would be the time between receipt of the token (e.g., randomly generated challenge code) and the sending back of the newly created password (e.g., response code),’” and so, Petitioner’s assertion “is flawed on its face because

the claimed ‘predetermined amount of time’ is the timeframe between activation and deactivation of the account.” Prelim. Resp. 31 (citing Ex. 1001, 12:41–45).

We disagree with Patent Owner’s argument. Claim 5 requires an authentication module that “deactivates the account within a predetermined amount of time after activating the account.” Ex. 1001, 12:43–54). It does not require that the predetermined amount of time correspond to the entire time period between activation and deactivation of the account. On the record before us, Petitioner has adequately demonstrated that Veneklasė discloses deactivation of the account within a predetermined amount of time. *See* Pet. 42–43.

e) Conclusion Regarding Ground 1

We have considered Petitioner’s evidence and arguments with respect to all limitations of claim 5, including the relevant testimony of Dr. McNair and find it to be sufficient to show that Petitioner has demonstrated a reasonable likelihood of prevailing in showing that Veneklasė and Jonsson, either alone or in combination, disclose each limitation of claim 5.

4. Ground 2: Alleged Obviousness of Claims 1 and 3–6

Having determined that Petitioner has demonstrated a reasonable likelihood of prevailing as to claim 5 on the basis of Ground 1, we do not address the patentability challenge on the basis of Ground 2.

III. CONCLUSION

For the foregoing reasons, we are persuaded that the Petition demonstrates a reasonable likelihood of prevailing in showing the unpatentability of at least one of the challenged claims of the ’658 Patent. Because Petitioner has satisfied the threshold for institution as to at least one

claim, we institute *inter partes* review on all claims and all grounds raised in the Petition. *See SAS Institute Inc. v. Iancu*, 138 S. Ct. 1348, 1359–60 (2018) (holding that a decision to institute under 35 U.S.C. § 314 may not institute on fewer than all claims challenged in the petition).

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1 and 3–6 of the '658 Patent is instituted with respect to all grounds set forth in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the '658 Patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

IPR2023-00425
Patent 6,993,658 B1

FOR PETITIONER:

Jordan M. Rossen
Ashraf Fawzy
UNIFIED PATENTS, LLC
jordan@unifiedpatents.com
afawzy@unifiedpatents.com

For PATENT OWNER:

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