Trials@uspto.gov
Tel: 571-272-7822

Paper 11
Date: March 28, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

EXPERIAN INFORMATION SOLUTIONS, INC.,
Petitioner,

v.

DYNAPASS IP HOLDINGS LLC,
Patent Owner.

IPR2023-01406
Patent 6,993,658 B1

Before KEVIN F. TURNER, KRISTEN L. DROESCH, and LYNNE H. BROWNE, *Administrative Patent Judges.*

BROWNE, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Experian Information Solutions, Inc. ("Petitioner") filed a Petition (Paper 2 ("Pet.")), seeking *inter partes* review of claims 1–7 ("the challenged claims") of U.S. Patent No. 6,993,658 B1 (Ex. 1001 ("the '658 patent")). *See* Pet. 2. Dynapass IP Holdings LLC ("Patent Owner") filed a Preliminary Response. Paper 7 ("Prelim. Resp.").

Institution of an *inter partes* review is authorized by statute when "the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a); *see* 37 C.F.R. § 42.108 (2022). Upon consideration of the Petition and the evidence of record, we conclude that the information presented in the Petition does not establish that there is a reasonable likelihood that Petitioner would prevail in challenging at least one of claims 1–7 of the '658 Patent as unpatentable under the grounds presented in the Petition. Pursuant to § 314, we hereby deny institution of an *inter partes* review as to the challenged claims of the '658 Patent.

A. *Real Parties in Interest*

Petitioner identifies itself, Experian Information Solutions, Inc., as the only real party-in-interest. Pet. 53. Patent Owner identifies itself, Dynapass IP Holdings LLC and DynaPass Inc., as the only real parties-in-interest. Paper 4, 1.

B. *Related Matters*

Petitioner indicates that the '658 Patent is at issue in the following district court litigation: identify *Dynapass IP Holdings, LLC v. Amazon.com Inc.*, No. 2:23-cv-00063 (E.D. Tex.); *Dynapass IP Holdings, LLC v. The Charles Schwab Corporation*, No. 2:23-cv-00064 (E.D.); *Dynapass IP*

Holdings, LLC v. Experian Information Services, Inc., No. 2:23-cv-00066 (E.D. Tex.);; *Dynapass IP Holdings, LLC v. Simmons First National Corporation*, No. 2:23-cv-00068 (E.D. Tex. filed); *Dynapass IP Holdings, LLC v. Bank of America Corporation*, No. 2:22-cv-000210 (E.D. Tex.); *Dynapass IP Holdings, LLC v. BOKF, National Association*, No. 2:22-cv-000211 (E.D. Tex.); *Dynapass IP Holdings, LLC v. JPMorgan Chase & Co.*, No. 2:22-cv-000212 (E.D. Tex.);; *Dynapass IP Holdings, LLC v. PNC Financial Services Group, Inc.*, No. 2:22-cv-000214 (E.D. Tex.); *Dynapass IP Holdings, LLC v. Truist Financial Corporation*, No. 2:22-cv-000216 (E.D. Tex.); *Dynapass IP Holdings, LLC v. Wells Fargo & Company*, No. 2:22-cv-000217 (E.D. Tex.);; and *Jack Henry & Associates, Inc. v. Dynapass IP Holdings LLC*, No. 1:23-cv-00388 (D. Del.). Pet. 53–55. In addition, Patent Owner identifies district court litigation involving the '658 patent that was dismissed with prejudice. Paper 4, 1–4. As litigation that is dismissed with prejudice cannot affect or be affected by a decision in this proceeding, we do not list these matters.

Petitioner indicates that the '658 patent is involved in the following proceedings before the Board: *Unified Patents, LLC v. Dynapass IP Holdings, LLC*, IPR2023-00425 (PTAB) and *JPMorgan Chase & Co. v. Dynapass IP Holdings, LLC*, IPR2023-01331 (PTAB). Pet. 48–50. Patent Owner identifies an additional proceeding in which institution was denied. Paper 4, 2–4. As a proceeding in which institution was denied cannot affect or be affected by a decision in this proceeding, we do not list it.

C. *The '658 patent (Ex. 1001)*

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.

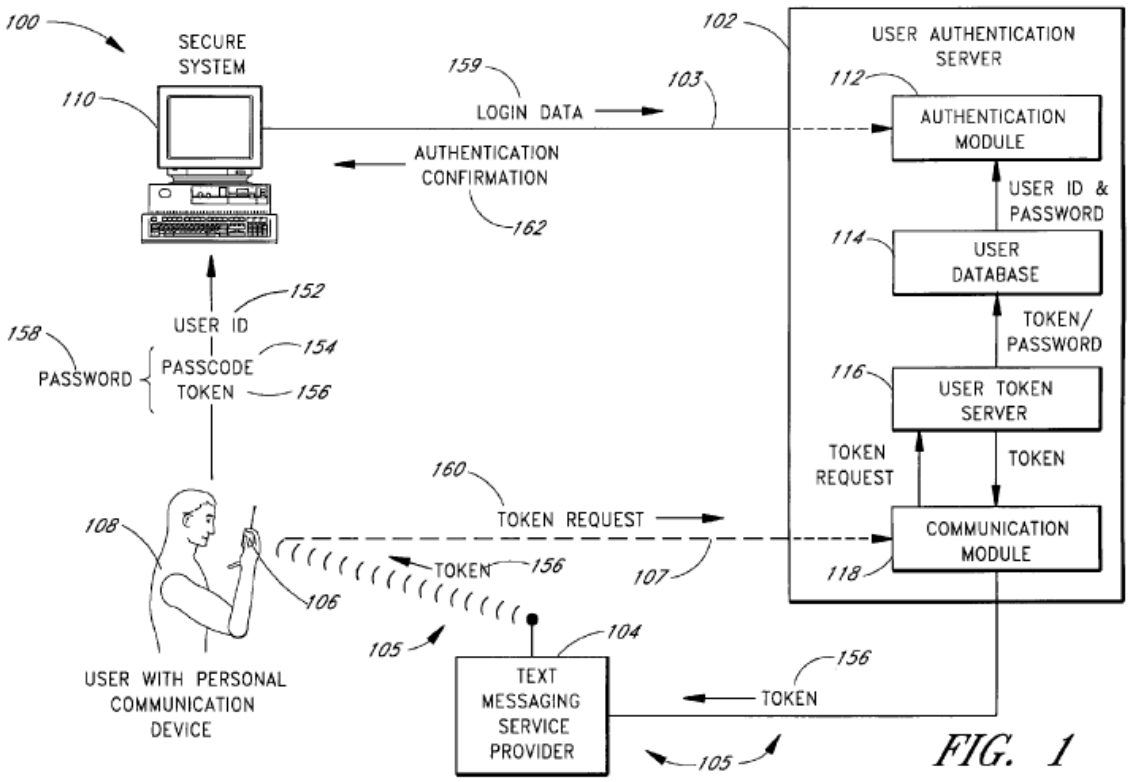

FIG. 1

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 108 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 1–7. 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 2, 3, and 4 depend from claim 1 and claims 6 and 7 depend or ultimately depend from claim 5. *Id.* at 12:16–19, 12:48–56.

> 1. [1.a] 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.b] 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.c] receiving a request from the user for a token via the personal communication device, over the second network;
>
> [1.d] 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.e] setting a password associated with the user to be the new password;

[1.f] activating access the user account on the first secure computer network;

[1.g] transmitting the token to the personal communication device;

[1.h] receiving the password from the user via the first secure computer network, and

[1.i] 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.a] A user authentication system comprising:

[5.b] a computer processor,

[5.c] 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.d] 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.e] a communication module configured to transmit the token to the personal communication device through the cell phone network, and

[5.f] 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, 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. *The Asserted Grounds of Unpatentability*

Petitioner asserts the following grounds of unpatentability (Pet. 15):

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–7	103	Sormunen,[1] Perlman[2]

F. *Evidence*

In support of its proposed grounds, Petitioner relies on the Declaration of Stephen Perkins, Ph.D. ("Dr. Perkins"). Ex. 1003. In our analysis below, we consider Dr. Perkin's testimony.

II. ANALYSIS

A. *Level of Ordinary Skill in the Art*

Petitioner asserts that a person of ordinary skill in the art ("POSITA") "would have had a bachelor's degree in computer science, management of information systems, or electrical engineering, or similar field, with one-to-two years of experience in the design, support, or implementation of systems requiring user authentication." Pet. 14. Petitioner also asserts that "[a]dditional education may substitute for experience with user authentication" And "additional relevant experience with user authentication may substitute for education." *Id.* (citing Ex. 1003 ¶ 48). For the purposes of their Preliminary Response, Patent Owner "does not dispute the level of

[1] WO 97/31306, published August 28, 1997 ("Sormunen") (Ex. 1004).
[2] U.S. Patent No. 6,173,400 B1, filed July 31, 1998, issued Jan. 9, 2001 ("Perlman") (Ex. 1005).

skill of a" person of ordinary skill in the art identified in the Petition. Prelim. Resp. 11.

For purposes of this Decision, we adopt Petitioner's proposal as reasonable and consistent with the prior art. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (the prior art may reflect an appropriate level of skill in the art).

B. *Claim Construction*

We apply the same claim construction standard used in district court actions under 35 U.S.C. § 282(b), namely that articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). *See* 37 C.F.R. § 42.100(b). In applying that standard, claim terms generally are given their ordinary and customary meaning as would have been understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *Phillips*, 415 F.3d at 1312–13. "In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence." *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).

Petitioner asserts that "each claim term be given its plain and ordinary meaning as would be understood in the context of the specification and prosecution history, and that no specific construction of any claim term is required in this proceeding because the ground identified in this Petition demonstrates the unpatentability of the claims under any reasonable construction." Pet. 11. Although Petitioner argues that no specific claim construction is necessary, it addresses how a person of ordinary skill would understand "the terms 'passcode,' 'token,' and 'password,' as well as the

ordering of steps with respect to the creation of the password and the transmission of the token to the user's personal communication device." Pet. 11.

Petitioner contends that the '658 Patent provides that "a 'passcode' is a 'secret [string] known to the user." Pet. 12 (citing Ex. 1001, 2:13–14 ("secret information known to the user, such as the passcode")). Petitioner contends that the '658 Patent provides that "[a] token is a string 'that is provided to the user through an object possessed by the user.'" Pet. 12 (citing Ex. 1001, 2:14–15 ("information provided to the user through an object possessed by the user, such as the token")). Petitioner contends that the '658 Patent provides that the "password is a string generated based on the token and the passcode, such as by combining or concatenating them." Pet. 12 (citing Ex. 1001, 2:2–4 ("The server creates a new password by concatenating a secret passcode that is known to the user with the token.")).

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," and does not provide an alternate understanding of the plain and ordinary meaning of any claim terms. Prelim. Resp. 11.

At this stage of this proceeding, we determine that no claim terms require express construction in order to determine whether or not to institute *inter partes* review because doing so would have no effect on the analysis below. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'" (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

C. *Jurisdiction Over the '659 Patent*

Patent Owner contends that expiration of a patent removes the patent from the Patent Office's jurisdiction and returns it to the sole jurisdiction of the Article III courts. Prelim. Resp. 54. Patent Owner contends that "[w]ith the expiration of the '658 Patent in March 2020, the Board ceased to have jurisdiction over the '658 Patent, and this *inter partes* review proceeding should be terminated as a result." *Id.* at 54–55. We disagree.

Patent Owner grounds its contentions in the Supreme Court's pronouncement in *Oil States*, that "the decision to *grant* a patent is a matter involving public rights–specifically, the grant of a public franchise." Prelim. Resp. 53; *Oil States Energy Servs., LLC v. Greene's Energy Grp., LLC*, 138 S. Ct. 1365, 1373 (2018). According to Patent Owner, "[w]hen a patent expires . . . the public franchise ceases to exist and the franchisee (e.g., the patent owner) no longer has the right to exclude others" and "because the public franchise no longer exists, the Patent Office has nothing in its authority to cancel or amend." *Id.* at 54.

In *Oil States*, the Supreme Court explained that "[*i*]*nter partes* review is 'a second look at an earlier administrative grant of a patent.'" *Oil States*, 138 S. Ct. at 1374 (quoting *Cuozzo Speed Techs., LLC v. Lee*, 579 U.S. 261, 279 (2016)). The Board has relied on this statement to conclude that the Patent Office has jurisdiction over expired patents in *inter partes* review proceedings. *Google LLC and YouTube, LLC v. Robocast, Inc.*, IPR2023-00593, Paper 14 at 8–12 (PTAB Sept. 18, 2023); *Apple, Inc. v. Gesture Tech. Partners*, LLC, IPR2021-00922, Paper 10 at 17–18 (PTAB Nov. 29, 2021); *Apple, Inc. v. Gesture Tech. Partners*, LLC, IPR2021-00921, Paper 24 at 36–38 (PTAB Dec. 5, 2022).

The Federal Circuit has also affirmed the Board's determination with

respect to expired claims in *inter partes* review. *See*, *e.g.*, *Wasica Fin. GmbH v. Cont'l Auto. Sys., Inc.*, 853 F.3d 1272, 1279 (Fed. Cir. 2017) (noting that '[t]he Board construes claims of an expired patent in accordance with Phillips . . . [and] [u]nder that standard, words of a claim are generally given their ordinary and customary meaning')."). This is consistent with our contemporaneous interpretation of our regulations as demonstrating that expired patents are properly considered to be within our jurisdiction. 37 C.F.R. § 42.100(b); *see also*, *e.g.*, 83 Fed. Reg. 51,341 (Oct. 11, 2018) (Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board) ("The claim construction standard adopted in this final rule also is consistent with the same standard that the Office has applied in interpreting claims of expired patents and soon-to-be expired patents.).

Furthermore, the statutes governing *inter partes* review do not limit them to unexpired patents. *See* 35 U.S.C. §§ 311(b), 311(c), 315; *see also Sony Corp. v. Iancu*, 924 F.3d 1235, 1239–41 (Fed. Cir. 2019) (affirming that a case or controversy before the PTAB existed when a patent was expired; articulating the importance of the Board's review of expired patents since expired patents can be asserted for past infringement).

Even if none of these factors alone is dispositive, they are collectively consistent with the Board's jurisdiction extending to cover expired patents. More particularly, Patent Owner does not adequately explain why the Board's authority to take "a second look at an earlier administrative grant of a patent" ends when the patent term expires even though the rights granted by the patent are not yet exhausted. *Oil States*, 138 S. Ct. at 1374. We accordingly disagree that the Board lacks jurisdiction over expired patents.

D. *Patentability Challenge*

1. Legal Standards

Petitioner bears the burden to demonstrate unpatentability, and that burden never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

A claim is unpatentable for obviousness 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." 35 U.S.C. § 103; *see also KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when in evidence, objective evidence of nonobviousness.[3] *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

2. Prior Art

a. Sormunen (Ex. 1004)

Sormunen is a Patent Cooperation Treaty application published August 28, 1997. Petitioner asserts that Sormunen is prior art under pre-AIA 35 U.S.C. § 102(a) and (b). Pet. 15.

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 disclose that its method and

[3] The parties have not directed our attention to any objective evidence of obviousness or non-obviousness.

system "can be applied also for obtaining a personal identity number (PIN) of bank and credit cards and corresponding charge cards." *Id.* at 9:26–28. Sormunen discloses the use of mobile communication systems including cellular systems, paging systems, and mobile phone systems. *Id.* at 4:36–5:1. For illustrative purposes, Sormunen's Figure 2 is reproduced below:

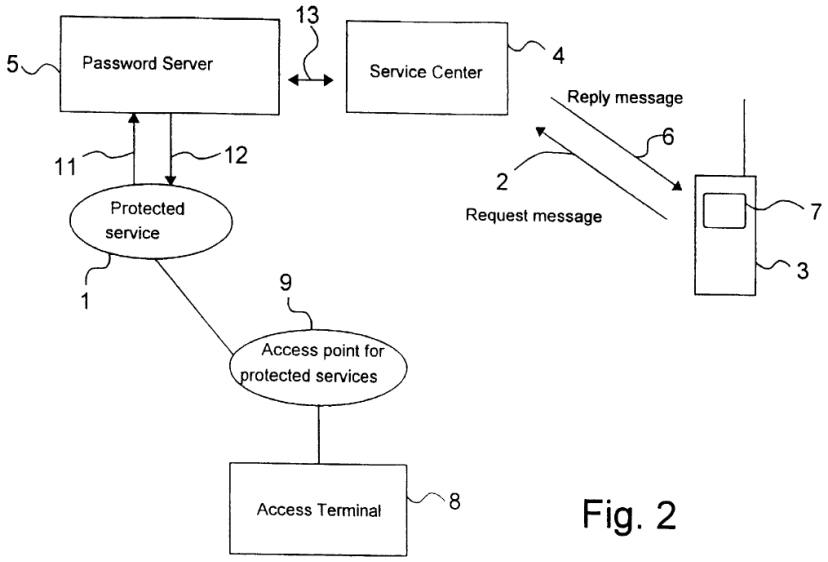

Fig. 2

Figure 2 shows a preferred embodiment of a two-way method for transmitting a username and password in response to user specific authentication data. *Id.* at 5:26–27, 5:33–34.

One way the user can obtain a password for use of protected service 1 is by sending short message 2 with the sender's authentication data from paging terminal 3. Ex. 1001, 5:35–38; 6:3–4. Password server 5 transmits the password and/or the user name to short message service center 4, which forms reply message 6, which is sent to the paging terminal 3 in enciphered form. *Id.* at 6:35–38. As further shown in Figure 2, reply message 6 can be shown to the user by display means 7 on paging terminal 3 to allow use of protected service 1. *Id.* at 6:35–7:7.

The second way the user can obtain a password is by inputting a username and a password into data processor 8 for subsequent verification in service 9. Ex. 1001, 7:9–7:11. "[V]erification service 9 transmits the given data to the [protected] service 1, which sends a check request 11 of the user name and the password to the password server 5." *Id.* at 7:9–11. Password server 5 examines the data and communicates in reply message 12 to protected service 1 whether the inputted username and password are correct. *Id.* at 7:14–16. Data processor 8 can have a data transmission connection to mobile station 3. *Id.* at 7:25–26. As further shown in Figure 2, reply message 6 may be processed in the application software of mobile station 3 "and transmitted to the data processor 8, whereby the user is given his or her user-specific authentication data for using the information service." *Id.* at 7:32–34.

b. Perlman (Ex. 1005)

Perlman is a U.S. patent for "Methods and Systems for Establishing a Shared Secret Using an Authentication Token." Ex. 1005, code (54). Petitioner asserts that Perlman is prior art under pre-AIA 35 U.S.C. § 102(a) and (e). Pet. 20. Perlman discloses "a method for establishing a shared secret among a plurality of devices, compris[ing] the steps of providing an authentication token; and utilizing the authentication token to establish a shared secret among the plurality of devices." Ex. 1005, 3:14–19.

For illustrative purposes, Perlman's Figure 4a is reproduced below:

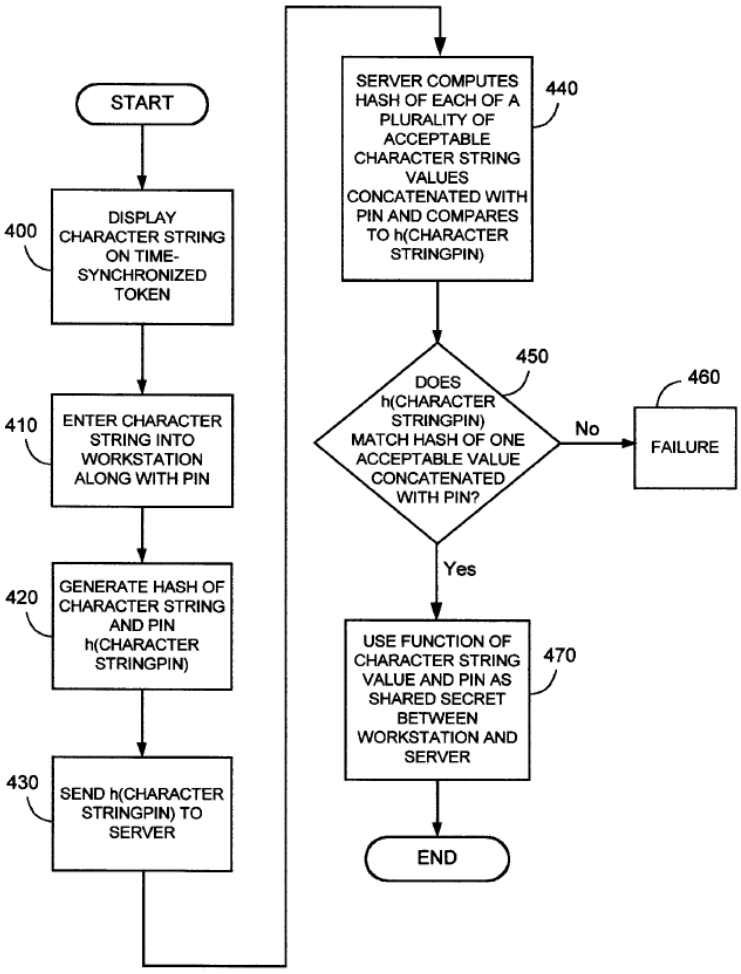

FIG. 4a

Figure 4a shows the generation of a character string on a time-synchronized token 170 (step 400), which is then communicated to workstation 120 along with a PIN (step 410). *Id.* at 8:55–60. After receiving the character string, the workstation executes a commercially available hash program to generate a hash of the character string and the PIN (step 420), which is sent to server 130 (step 430). *Id.* at 8:63–66, Fig. 4a.

As further shown in Figure 4a, server 130 then computes a plurality of acceptable character strings using the PIN, which is already known to the

server, and compares these acceptable character strings with the hash of the character string and the PIN received from workstation 120 (step 440 and 450). *Id.* at 8:66–9:5. "If a match is found, the server and workstation use a function of the character string and the PIN (e.g., a hash of the character string concatenated with a PIN concatenated with a constant) as a shared secret (step 470)." *Id.* at 9:6–10.

3. Alleged Obviousness of Claims 1–7

Petitioner asserts that claims 1–7 are unpatentable over the combined teachings of Sormunen and Perlman. Pet. 15–47. Patent Owner disagrees. Prelim. Resp. 12–40. In particular, Patent Owner disputes Petitioner's assertions regarding limitations [1.c], [1.d], [1.f], [1.h], and [1.i] of independent claim 1 and limitations [5.d] and [5.f] of independent claim 5. *Id.* at 17–40. Our determination with respect to limitations [1.c], [1.d], and [5.d] is dispositive. Accordingly, we focus our analysis on these limitations.

Central to Petitioner's challenge is its identification of Somunen's PIN as corresponding to the claimed "token." Pet. 32–37 (addressing limitations [1.c]–[1.d]), 46 (addressing limitation [5.d]). For the reasons discussed below, we do not agree with Petitioner that Somunen's bank or credit card PIN is a token, per our understanding of that limitation in the context of the '658 Patent.

4. Limitation [1.c]: receiving a request from the user for a token via the personal communication device, over the second network

Petitioner asserts that Sormunen's step of receiving request message 2 corresponds to the claimed "receiving a request from the user," Sormunen's paging or mobile terminal corresponds to the claimed "personal communication device," and Sormunen's cell phone network corresponds to

the claimed "second network." Pet. 33 (citing Ex. 1003, ¶ 166; Ex. 1004, Fig. 2). Petitioner asserts further that because Sormunen's short message 2 can include a password request, one of ordinary skill in the art would have understood "that this password would have the same role or function as the claimed 'passcode." *Id.* (citing Ex. 1003 ¶ 167). In addition, Petitioner asserts that Sormunen discloses requesting and receiving a PIN over a cell phone network. Pet. 33–34 (citing Ex. 1003 ¶ 168; Ex. 1004, 9:26–37).

Petitioner asserts further that a person of skill "would appreciate that a password and a PIN could be used together for greater security" and that such a person "would have found it obvious for the new password to be [a] combination of the known password (passcode) and the PIN (token) generated in response to the request." Pet. 34 (citing Ex. 1003 ¶ 168).

Turning to Perlman, Petitioner asserts that it "teaches using a character string generated by an authentication token to augment an existing character string" such that a person of skill "would have appreciated that Perlman teaches augmenting a known character string using a requested character string unknown to the user, at least at that point (*token*)." Pet. 34 (citing Ex. 1003 ¶ 169; Ex. 1005, 4:38–64, 8:49–9:9,11:8–20).

Patent Owner contends that Sormunen does not disclose a request for its PIN. Prelim. Resp. 18. Patent Owner contends further that, to the extent that Sormunen discloses a request for its PIN, the PIN is not received over a cell phone network. *Id.* at 18–19.

Patent Owner's arguments are not convincing. Sormunen discloses that "the present invention can be applied also for obtaining a . . . PIN." Ex. 1004, 9:26–27. Moreover, Sormunen explicitly states that the PIN "is transmitted to the paging device or the mobile station of the user." *Id.* at 9:36–37. We agree with Petitioner that such transmission would be over a

cell phone network. Pet. 33–34. We do not, however, agree that Petitioner has adequately demonstrated that Sormunen discloses receiving a request from the user for a token as required by limitation [1.c].

Petitioner's reasoning as set forth in the Petition is incomplete. Petitioner shows that Sormunen discloses receiving a request from the user for a password and that a person of skill in the art would understand Sormunen's password to be a passcode as claimed. Pet. 32–33. Petitioner further shows that Sormunen discloses that its method can be applied to obtain a PIN for a bank or credit card. *Id.* at 19. Petitioner, however, does not adequately explain why one skilled in the art would understand Sormunen's PIN to be a token. *Id.*

Sormunen describes a method for a user to obtain an item of user authentication data such as a password. Ex. 1004, 1:1–5. After describing its method for obtaining a password, Sormunen discloses that its method can be used to obtain other user authentication data such as a PIN for a bank or credit card. *Id.* at 9:26–28. As such, both Sormunen's password and its PIN correspond to the claimed passcode. In other words, Sormunen's PIN is simply a numerical password.

Lacking an adequate explanation of why a person of skill in the art would understand Sormunen's PIN to be a token, Petitioner's reasoning that a person of skill in the art would understand Sormunen to disclose receiving a request for a token lacks rational underpinning. Pet. 34. Further, given that Sormunen's PIN, like its password, corresponds to the claimed passcode, Petitioner's reasoning that a person of skill in the "would have found it obvious for the new password to be a combination of the known password (passcode) and the PIN (token) generated in response to the request" also lacks rational underpinning. *Id.*

Petitioner does not rely on Perlman to cure these deficiencies in Petitioner's reasoning. Pet. 34. In fact, it is unclear what role Petitioner's statements about Perlman's disclosure and a person of skill's understanding of that disclosure play in the proposed combination.

5. Limitation [1.d]: 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

Petitioner asserts that "Sormunen discloses that upon account setup, the new user may have a password assigned or selected" and that a person of skill in the art "would have understood that this initial password teaches the claimed 'passcode.'" Pet. 35 (citing Ex. 1004, 3:25–32; Ex. 1003 ¶ 173). Petitioner asserts further that a person of skill in the art "would understand that security can be improved by augmenting the string known to the user with a PIN to create a more secure password," and thus, "would know from Sormunen to combine the disclosed initial password with the new PIN to create a new password." *Id.*

Petitioner asserts further that a person of ordinary skill in the art "would have understood that concatenation was a predetermined function for modifying a first character string with another character string to produce a second character string" and "would have appreciated that Perlman teaches concatenating a known secret character string with a generated character string provided through a token." *Id.* at 36 (citing Ex. 1003 ¶¶ 174–175). According to Petitioner, one of ordinary skill in the art "would have appreciated that the resulting character string could be used more securely as a password than the original known secret character string" and "would have been motivated to combine the teachings of Perlman with Sormunen" by augmenting "[t]he original password set for the user (including one proposed

by the user) . . . by concatenating it with a generated PIN." Pet. 36 (citing Ex. 1003 ¶ 175).

Patent Owner argues that "the Petition conveniently glosses over the fact that *Sormunen's* 'PIN' is for a bank/credit card" and "is reused multiple times (i.e., multiple visits to ATMs, multiple visits to merchants) over months, if not years." Prelim. Resp. 22 (quoting Ex. 1004, 9:26–28). According to Patent Owner, "[t]hat is in stark contrast to *Perlman's* "character string," which, as discussed above, can only be used for a single authentication attempt.'" Prelim. Resp. 22 (citing Ex. 1004, 9:35–10:2).

Patent Owner further argues that the combined teachings of Sormunen and Perlman would not have resulted in greater security because "it is only necessary for a hacker to intercept the concatenation of Sormunen's 'PIN' and 'password' to gain access." Prelim. Resp. 22–23.

We agree with Patent Owner that Petitioner's reasoning in support of the proposed combination lacks rational underpinning because combining Sormunen's password and PIN (both of which are known to the user) would not result in greater security. Moreover, for the reasons discussed above, we do not agree with Petitioner that Sormunen's PIN is a token. Sormunen's PIN is nothing more than a numerical passcode provided to a user when a charge card is ordered or when a new PIN is required because a prior PIN has been compromised. Ex. 1004, 9:28, 9:34–10:2. Given that both Sormunen's password and its PIN are passcodes known to the user, Petitioner's reasoning that a person of skill in the art would know from Sormunen to combine its password and PIN lacks rational underpinning. Further, Petitioner's reasoning that a person of skill in the art "would understand that a PIN would commonly be generated by known techniques

to produce a randomized string" is not supported by Sormunen, because Sormunen does not disclose a PIN produced by a randomized string.

Petitioner's reliance on Perlman does not cure these deficiencies in Petitioner's reasoning. Pet. 35–37. Although, we agree with Petitioner that Perlman discloses a token, the Petition does not rely on Perlman's teachings of a token to replace Sormunen's PIN.[4] *Id.*

> 6. *Limitation [5.d]: 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;*

For contested limitation [5.d], Petitioner relies on its assertions set forth above regarding limitations [1.d] and [1.e]. Pet. 46 (citing Ex. 1003 ¶ 199). Thus, Petitioner's assertions regarding limitation [5.d] suffer from the same deficiencies as its assertions regarding limitation [1.d] discussed in the previous section.

7. *Determination re Claim 1–7*

For the reasons discussed above, Petitioner has not shown a reasonable likelihood of prevailing for independent claims 1 and 5. Claims 2–4 depend from claim 1. Thus, Petitioner's assertions with respect to claims 2–4 suffer from the same deficiencies as its assertions for claim 1. Claims 6 and 7 depend from claim 5, and therefore, suffer from the same deficiencies as its assertions for claim 5. For these reasons, Petitioner has

[4] We note that a factor largely contributing to the inadequacy of Petitioner's assertions is the fact that the word "PIN" is used in Sormunen to refer to a passcode, whereas the same word is used in Perlman to refer to a token, and Petitioner conflates these terms in its challenge.

not shown a reasonable likelihood of prevailing for claims 1–7.

E. *Discretionary Denial Under 35 U.S.C. §§ 314(a) and 325(d)*

Patent Owner contends that we should exercise our discretion to deny institution under 35 U.S.C. §§ 314(a) and 325(d). Prelim. Resp. 43–53. As we deny institution on the merits, we do not reach Patent Owner's request that request that we exercise our discretion to deny the Petition under 35 U.S.C. §§ 314(a) or 325(d).

III. CONCLUSION

Based on the current record, we determine Petitioner has not shown a reasonable likelihood of prevailing with respect to at least one claim of the '658 patent. Accordingly, we deny institution of *inter partes* review

IV. ORDER

In consideration of the forgoing, it is hereby

ORDERED that the Petition is denied, and no trial is instituted.

For PETITIONER:

James B. Hatten
R. Scott Feldmann
BAKER & HOSTETLER LLP
jhatten@bakerlaw.com
sfeldmann@bakerlaw.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
IPRDYNAPASSWSL@wsltrial.com