

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

BANK OF AMERICA, N.A.; TRUIST BANK; BOKF, N.A.;
WELLS FARGO BANK, N.A.; AND PNC BANK, N.A.,
Petitioner,

v.

DYNAPASS IP HOLDINGS LLC,
Patent Owner.

IPR2023-00367
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

Bank of America, Truist Bank, BOKF, Wells Fargo Bank, and PNC Bank (collectively “Petitioners”) filed a Petition (Paper 1 (“Pet.”)) requesting institution of an *inter partes* review of claims 1–3 and 5–7 of U.S. Patent No. 6,993,658 B1 (Ex. 1001, “the ’658 Patent”). Pet. 1, 95–96; Papers 2–6 (Powers of Attorney). Dynapass IP Holdings LLC (“Patent Owner”) timely filed a Preliminary Response. Paper 8 (“Prelim. Resp.”). Prelim. Resp. 1. With our authorization, Petitioner filed a Preliminary Reply (Paper 11, “Reply”) and Patent Owner filed a Preliminary Sur-reply (Paper 12, “Sur-reply”).

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 Petition fails to establish that there is a reasonable likelihood that Petitioner would prevail in challenging at least one of claims 1–3 and 5–7 of the ’658 Patent as unpatentable under the grounds presented in the Petition. Pursuant to § 314, we deny institution of an *inter partes* review as to the challenged claims of the ’658 Patent.

A. *Real Parties in Interest*

Petitioner identifies the real party-in-interest as Bank of America Corporation, Bank of America, N.A., BOKF, N.A., Okta, Inc., Truist Bank, Truist Financial Corp., Wells Fargo Bank, N.A., Wells Fargo & Company, PNC Bank, N.A., and The PNC Financial Services Group, Inc. Pet. 95–96.

Patent Owner identifies itself, Dynapass IP Holdings LLC and DynaPass Inc., as real parties-in-interest. Paper 7, 1.

B. Related Matters

The parties identify the following litigations as related district court matters: *Dynapass IP Holdings LLC v. Bank of America Corporation et al*, 2:22-cv-00210 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. BOKF, National Association et al*, 2:22-cv-00211 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. JPMorgan Chase & Co. et al*, 2:22-cv-00212 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. PlainsCapital Bank et al*, 2:22-cv-00213 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. PNC Financial Services et al*, 2:22-cv-00214 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Regions Financial Corporation et al*, 2:22-cv-00215 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Truist Financial Corporation et al*, 2:22-cv-00216 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Wells Fargo & Company et al*, 2:22-cv-00217 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Woodforest National Bank et al*, 2:22-cv-00218 (EDTX 6-17-2022). Pet. 96–97; Paper 7, 1–2.

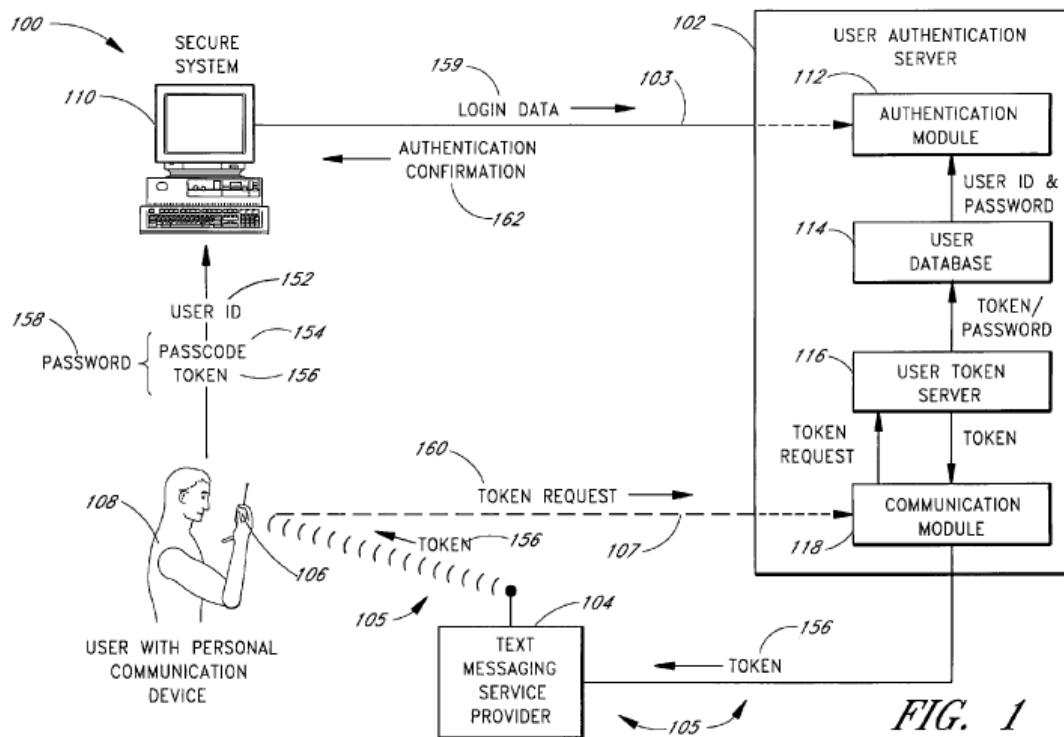
Patent Owner also identifies *Unified Patents, LLC v. Dynapass IP Holdings LLC*, IPR2023-00425 as a related matter. Paper 7, 2.

C. The '658 Patent

The '658 Patent is titled “Use of Personal Communication Devices For User Authentication.” Ex. 1001, code (54). The “invention relates 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 1:8–11.

One embodiment of the invention provides a password setting system that includes a user token server and a communication module. The 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. The 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.



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.

D. Illustrative Claims

Petitioner challenges claims 1–3 and 5–7. 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. Dependent claims 2 and 3 depend from claim 1 and claim 6 and 7 depend from claim 5. *Id.* at 12:16–19, 12:48–52.

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

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

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

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

[1.h] 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.preamble] A user authentication system comprising:

[5.a] a computer processor,

[5.b] 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.c] 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, [5.d] 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, [5.g] 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 1–3 and 5–7 would have been unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–3, 5–7	103	Guthrie, ¹ Sormunen ²
1–3, 5–7	103	Katou, ^{3,4} Guthrie

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 v. Jeffrey-Allan Indus., 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”) would have at least a bachelor’s degree in Electrical Engineering, Computer Science, Computer Engineering, or equivalent, and at

¹ US 6,161,185 to Guthrie et al., issued December 12, 2000 (“Guthrie”) (Ex. 1007).

² WO 97/31306, published August 28, 1997 (“Sormunen”) (Ex. 1008).

³ In accordance with the English translation, the inventor is Katou, not Kato.

⁴ JP 2000-10927 to Katou, published January 14, 2000 (“Katou”) (Ex. 1005). For purposes of this Decision we rely on the English translation of Katou (Ex. 1006).

least two years of prior experience with user authentication technologies for computer systems as of the earliest priority date of the '658 Patent—March 6, 2000. Additional education could substitute for professional experience and vice versa.

Pet. 3–4 (citing Ex. 1002 ¶ 23). “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. 10.

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 federal court claim construction standard that is used to construe a claim in a civil action under 35 U.S.C. § 282(b). This is the same 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. v. Am. Sci. & Eng’g*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

Petitioner contends that, “[f]or this IPR, the plain meaning of each claim term can be applied. Ex. 1002 ¶¶ 25–29.” 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. 10.

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

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*, 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).

2. Relevant Prior Art

a) Guthrie (Ex. 1007)

Guthrie is a U.S. patent that issued December 12, 2000. Ex. 1107, code (45). Petitioner asserts that Guthrie is prior art under pre-AIA 35 U.S.C. § 102(e). Pet. 1.

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

Figure 5, reproduced below, shows Guthrie's system:

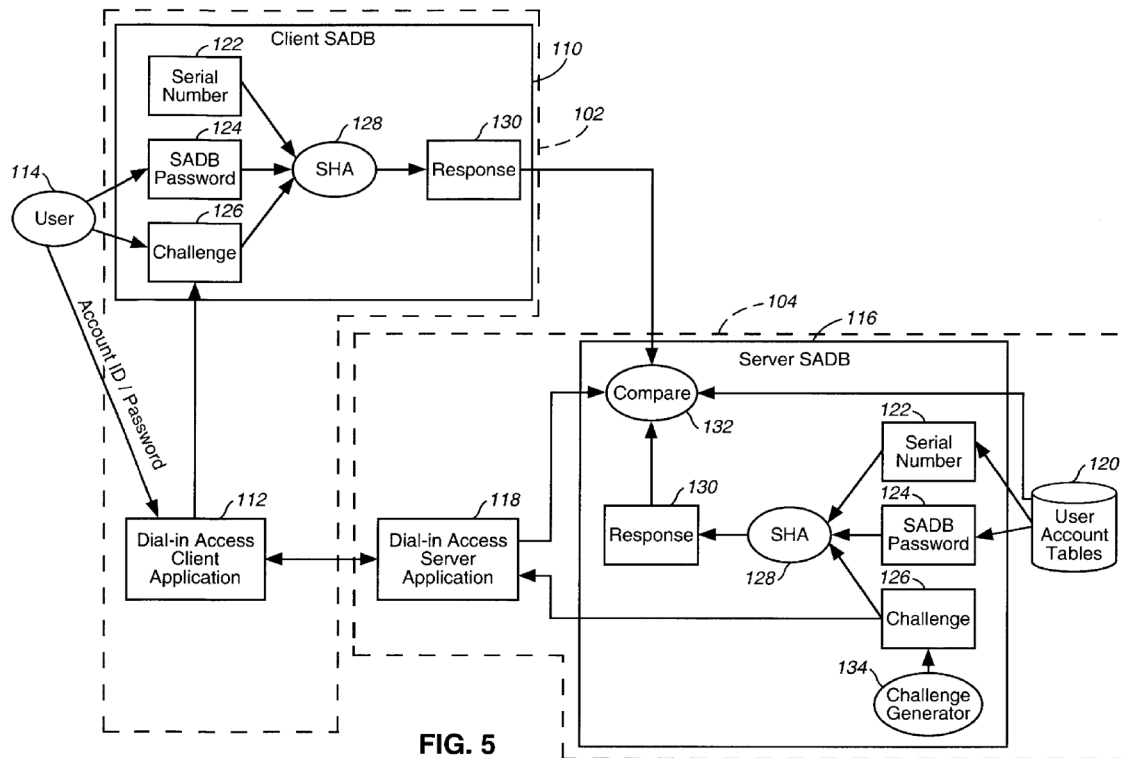


Figure 5 is a block diagram showing Guthrie's personal authentication process. Ex. 1005, 3:25–26. As shown in Figure 5, user 114 initially inputs the user's account and correct password to client 102. *Id.* at 7:16–17. Client 102, via client application 112, transmits the user account and account password to the server 104. *Id.* at 7:17–19. Server 104 validates the user account and password against user 114's account table stored in user account database 120. *Id.* at 7:20–22. If initial validation is successful, then server 104 employs challenge generator 134 in its SADB⁶ calculator 116 to generate challenge 126. *Id.* at 22–26.

⁶ Secure authentication database.

Client SADB calculator 110 prompts user 114 for its SADB password 124, which user 114 enters into the client 102. Ex. 1005, 7:27–29. User 114 enters the received challenge into client SADB calculator 110. *Id.* at 7:29–30. Client SADB calculator 110 generates, via SHA⁷ 128, response 130 using challenge 126, SADB password 124, and locally stored serial number 122. *Id.* at 7:34–37. Client 110 transmits response 130 to server 104. *Id.* at 7:37–38. Server SADB calculator 116 employs a compare routine 132 to compare receive response 130 with the response 130⁸ locally generated by the server 104. *Id.* at 7:38–41. Server 104 provides client 102 with a message indicating whether the authentication succeeded or failed, and enables appropriate access if successful. *Id.* at 7:42–44.

b) Sormunen (Ex. 1018)

Sormunen is a Patent Cooperation Treaty application published August 28, 1997. Ex. 1018, code (43). Petitioner asserts that Sormunen is prior art under pre-AIA 35 U.S.C. § 102(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. User information is transmitted in enciphered[] electronic form and the receiver can be recognized in order to prevent abuse.” *Id.* at 6:7–9.

⁷ Secure hashing algorithm.

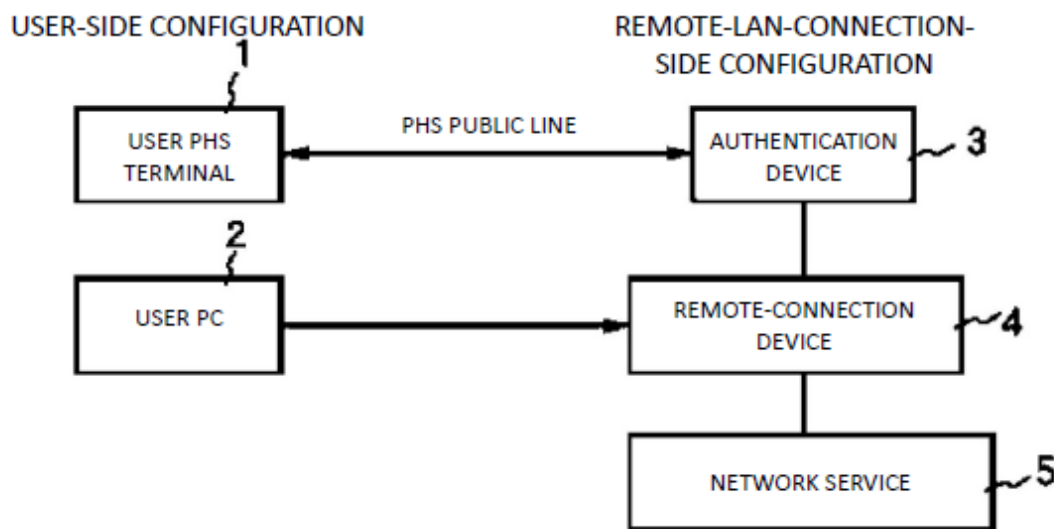
⁸ We note the use of reference numeral 103 in reference to the received response and the locally generated response. Despite the use of the same reference numeral, we understand the received response and the locally generated response to be different elements of the disclosed invention.

c) Katou (Ex. 1006)

Katou is a Patent Cooperation Treaty application published January 14, 2000. Ex. 1006, code (43). Petitioner asserts that Katou is prior art under pre-AIA 35 U.S.C. § 102(a). Pet. 1.

Katou relates to “an authentication system and an authentication device that permits the provision of a local area network (LAN) service only to proper users. Ex. 1006 ¶ 2. Fig. 1, reproduced below, “is a block diagram of one embodiment of [the] authentication system.” *Id.* ¶ 12.

FIG. 1



As shown in Figure 1, authentication device 3 is a device that verifies the validity of a user and performs: management of a user-password request/notification function; issuance of a temporary password in response to a connection request from the user; and notification of the temporary password to user PHS terminal 1 and remote-connection device 4. Ex. 1006 ¶ 13. “Based on the ‘temporary password’ issued by the authentication device 3, the remote-connection device 4 accepts the connection request

from the user PC 2, which is a computer system for user connection, and remotely connects a proper user or an inquiring user to the authentication device 3.” *Id.* ¶ 14. User Personal Handy-phone System (PHS) terminal 1 is a commercially available simplified mobile telephone having a user-password request/notification function. *Id.* If a user makes a request to authentication device 3 for a temporary password and the user is properly authenticated, then authentication device 3 gives notification of the temporary password. *Id.*

3. *Ground 1: Alleged Obviousness of Claims 1–3 and 5–7 Based on the Combined Teachings of Guthrie and Sormunen*

For this Ground, Patent Owner contests Petitioner’s reasoning in support of the proposed combination. Prelim. Resp. 15–20. As our determination with respect to Petitioner’s reasoning is dispositive for this Ground, we focus our discussion on that reasoning and Patent Owner’s arguments pertaining to it.

Petitioner asserts that a “POSITA would have found it obvious to implement Sormunen’s mobile station and method for requesting and obtaining authentication data at the mobile station in Guthrie’s authentication system to further improve security.” Pet. 10. Petitioner articulates three reasons in support of its assertion. Patent Owner disagrees with Petitioner’s reasoning. Prelim. Resp. 15–20. We discuss each of Petitioner’s articulated reasons in turn.

a) *First Reason*

Petitioner asserts that “because Sormunen recognizes that cellular networks and SMS messaging are more secure than computer networks like the Internet, a POSITA would have been motivated to implement

Sormunen’s mobile station in Guthrie to request and receive Guthrie’s challenge to prevent the challenge from being exposed over the computer network.” Pet. 10. Petitioner asserts further that “Sormunen teaches that ‘unauthorized persons can easily read information transferred via the Internet.’” *Id.* at 10–11 (citing Ex. 1018, 3:4–5).⁹ Based on these assertions, Petitioner reasons that “[i]mplementing Sormunen’s method of obtaining authentication data in short messages over a mobile communication network in Guthrie would have reduced the risk of exposing the challenge to an unauthorized user and improved security because ‘it is almost impossible for outsiders to decipher the content of the short messages.’” *Id.* at 11 (citing Ex. 1018, 6:5–9; Ex. 1002 ¶ 64).

Patent Owner contends that Petitioner’s first articulated reason for the proposed combination fails because “*Sormunen* does not recognize that cellular networks and SMS messaging are more secure than computer networks.” Prelim. Resp. 16. According to Patent Owner, “*Sormunen* states that unenciphered data (i.e., nonencrypted data) can be read when transmitted over the Internet” and “that SMS messages sent ‘in enciphered form’ (i.e., encrypted) are ‘almost impossible for outsiders to decipher.’” *Id.* (citing Ex. 1018, 3:4–5, 6:5–9). Patent Owner further notes that “*Sormunen* states that its system can be implemented over an Internet connection.” *Id.* at 16–17 (citing Ex. 1018, 6:12–17; 6:38–7:4) (internal quotations omitted).

We agree with Patent Owner that Petitioner’s first articulated reason in support of the proposed combination lacks rational underpinning because

⁹ Here and throughout the remainder of this Decision, citations to references that are not the basis for the challenge being discussed are omitted.

Sormunen does not support the premise that cellular networks and SMS messaging are more secure than computer networks.

b) Second Reason

Petitioner asserts that “a POSITA would have recognized that maintaining Guthrie’s never-transmitted secret password, unlike Sormunen’s authentication data that is all transmitted over one network or another, would result in a more secure combined system.” Pet. 11. According to Petitioner, the combined system would ensure “that an unauthorized user in possession of the mobile station and challenge cannot access the secured system without the user’s secret password.” *Id.* at 11–12 (citing Ex. 1002 ¶ 65).

Patent Owner contends that “*Guthrie* already does not transmit the user’s password,” “[s]o combining *Sormunen* with *Guthrie* does not address any alleged deficiency in *Guthrie*.” Prelim. Resp. 18 (citing Ex. 1007, 4:23–27, 6:10–27, Fig. 3).

Although we are unaware of any requirement that a secondary reference, such as Sormunen, need address an alleged deficiency in a base reference, such as Guthrie, in order to demonstrate obviousness, we agree with Patent Owner that Petitioner’s second articulated reason in support of the proposed combination lacks rational underpinning, in that Petitioner’s reasoning appears to support the idea that Sormunen’s teachings should not be applied to Guthrie. Further, it appears that Petitioner’s second reason is not so much an articulation of reasons to combine the references as it is further explanation of the proposed combination.

c) Third Reason

Petitioner asserts that “using Sormunen’s mobile station to request and receive Guthrie’s challenge further improves security by additionally

verifying the user by their personal communication device.” Pet. 12. Petitioner asserts further that “[t]he only user-specific data Guthrie requires for requesting the challenge is the user account ID” and that a “user account ID is typically not secret and can be known to an unauthorized user.” *Id.* (citing Ex. 1007, 1:25–29, 7:60–63).

In addition, Petitioner asserts that “[u]sing Sormunen’s mobile station to obtain Guthrie’s challenge allows the challenge request to be sent from a user-associated mobile station (by a telephone number). This allows Guthrie’s server to identify the user based on the mobile station in addition to the user account ID.” *Id.* at 12–13 (citing Ex. 1018, 4:30–33, 9:28–32). Petitioner asserts further that “requiring all three components of the combination—a mobile station, a secret password, and a challenge—results in a more secure system than either Guthrie or Sormunen individually.” *Id.* at 13 (citing Ex. 1002 ¶ 66).

Patent Owner contends that “Petitioners fail to identify any evidence that requesting a challenge via a mobile station is more secure than requesting it via user account ID.” Prelim. Resp. 19 (citing Pet. 12). Patent Owner further contends that “the declaration of Dr. Reiher should be afforded no weight for this argument because the declaration does nothing more [than] restate Petitioners’ argument without any additional supporting evidence or reasoning.” *Id.* at 19–20 (comparing Pet. 12–13 to Ex. 1002 ¶ 66; citing *Xerox Corp., et al. v. Bytemark, Inc.*, IPR2022-00624, Paper 9, pp. 15–16 (PTAB Aug. 24, 2022) (Precedential)).

We agree with Patent Owner that Petitioner does not provide adequate support for its assertion that challenge requests via mobile station are more secure than challenge requests that rely on a user account ID. Petitioner

identifies no such teaching in Guthrie or Sormunen. Further, we agree with Patent Owner that Dr. Reiher's testimony amounts to no more than a restatement of Petitioner's argument in the Petition without the support of additional evidence. We, therefore, give this testimony little weight. *Xerox*, IPR2022-00624, Paper 9 at 15–16.

d) Conclusion re Ground 1

For the reasons discussed above, we determine that Petitioner's articulated reasoning in support of the proposed combination that forms the basis of this challenge lacks rational underpinning. Accordingly, Petitioner fails to demonstrate a reasonable likelihood of prevailing for any claim on this ground.

4. Ground 2: Alleged Obviousness of Claims 1–3 and 5–7 Based on the Combined Teachings of Katou and Guthrie

For this Ground, Patent Owner contests Petitioner's reasoning in support of the proposed combination. Prelim. Resp. 27–33. As our determination with respect to Petitioner's reasoning is dispositive for this Ground, we focus our discussion on that reasoning and Patent Owner's arguments pertaining to it.

Petitioner asserts that a "POSITA would have found it obvious to add Guthrie's challenge-response process to [Katou's] three-device architecture, in place of [Katou's] singular temporary password, to further improve security." Pet. 59.

Petitioner asserts that a "POSITA would have been motivated to incorporate Guthrie's challenge-response process into [Katou] to enhance [Katou's] security by preventing the user's secret password from being exposed during transmission." Pet. 60.

Patent Owner contends that “[*Katou*] does not contemplate that data such as the temporary password might be intercepted while being transmitted to the mobile device—in fact, [*Katou*] boasts that its authentication system provides ‘extremely strong security’ and that it would be ‘extremely difficult for a third party to improperly use the network service.’” Prelim. Resp. 32 (citing Ex. 1005 ¶ 22). Thus, according to Patent Owner, “a POSITA would not be motivated to incorporate *Guthrie* or any other reference into [*Katou*] to improve the [*Katou*] system’s security.”

Although we do not agree with Patent Owner that *Katou*’s statements about the strength of its security preclude improvement of that security, we agree with Patent Owner that Petitioner’s reasoning is flawed because *Katou* does not contemplate transmitting the user’s secret password. Rather, *Katou* describes a system that issues a temporary password upon request for user authentication. *See, e.g.*, Ex. 1005, Abs. Moreover, Petitioner has not adequately explained how *Guthrie*’s hashing algorithm and challenge-response process would be implemented in *Katou*’s system.

Petitioner’s further reasoning that a “POSITA would have been motivated to incorporate *Guthrie*’s challenge-response process into [*Katou*], in place of *Kato*’s temporary password, to further enhance [*Katou*’s] security by only transmitting the challenge . . . , preventing exposure of the password, and by requiring the user’s secret password in addition to the challenge to obtain the response” suffers from the same deficiencies.

For these reasons, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing for any claim on this ground.

III. CONCLUSION

For the foregoing reasons, the Petition fails to demonstrate a reasonable likelihood of prevailing in showing the unpatentability of at least one of the challenged claims of the '658 Patent.

IV. ORDER

In consideration of the foregoing, it is hereby:

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

IPR2023-00367
Patent 6,993,658 B1

FOR PETITIONER:

Lionel M. Lavenue
Kara A. Specht
Cory Bell
Xirui Zhang
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
lionel.lavenue@finnegan.com
kara.specht@finnegan.com
cory.bell@finnegan.com
xirui.zhang@finnegan.com

For PATENT OWNER:

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