

Filed: January 3, 2023

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.,
Petitioners,

v.

DYNAPASS IP HOLDINGS LLC,
Patent Owner.

IPR2023-00367
U.S. Patent 6,993,658

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT 6,993,658**

TABLE OF CONTENTS

I.	Relief Requested	1
II.	The '658 Patent.....	2
III.	Level of Ordinary Skill.....	3
IV.	Claim Construction.....	4
V.	Ground 1: Guthrie in Combination with Sormunen Renders Obvious the Challenged Claims.....	4
A.	Guthrie-Sormunen Combination	4
1.	Summary of the Guthrie-Sormunen Combination.....	4
2.	Guthrie and Sormunen Are Analogous Art and Combinable	7
3.	A POSITA Would Been Motivated to Implement Sormunen's Mobile Station and Method for Requesting and Obtaining Authentication Data at a Mobile Station in Guthrie to Improve Security	10
B.	Independent Claims	16
1.	Claim 1	16
2.	Claim 5.....	40
C.	Dependent Claims	52
1.	Claim 2: "The method of claim 1, wherein the new password is generated by concatenating the token and the passcode."	52
2.	Claim 3: "The method of claim 1, wherein the personal communication device is a mobile phone."	54
3.	Claim 6: "The system of claim 5, wherein the communication module is further configured to receive a	

	request from the user for the token, and wherein the control module is further configured to create the new password in response to the request.”	54
4.	Claim 7: “The system of claim 6, wherein the request is transmitted by the user through the personal communication device.”	55
VI.	Ground 2: Kato in Combination with Guthrie Renders Obvious the Challenged Claims.....	55
A.	Kato-Guthrie Combination.....	55
1.	Summary of the Kato-Guthrie Combination	55
2.	Kato Is Analogous Art and Combinable with Guthrie	56
3.	A POSITA Would Be Motivated to Add Guthrie’s Challenge-Response Process to Kato’s Three-Device Architecture and Would Have Had a Reasonable Expectation of Success	59
B.	Independent Claims	68
1.	Claim 1	68
2.	Claim 5	88
C.	Dependent Claims	92
1.	Claim 2	92
2.	Claim 3	93
3.	Claims 6 and 7.....	93
VII.	Institution Under 35 U.S.C. § 314(a) Is Appropriate in View of Petitioners’ <i>Sotera</i> Stipulation.....	93
VIII.	Institution Under 35 U.S.C. § 325(d) Is Appropriate in View of New References and Arguments	94
IX.	Mandatory Notices.....	95

A.	Real Parties-in-Interest	95
B.	Related Matters	96
C.	Lead and Back-Up Counsel	97
D.	Service Information	98
X.	Standing	98
XI.	Conclusion	98

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Abbott Diabetes Care Inc. v. DexCom, Inc.</i> , IPR2022-00922, Paper 13 (PTAB Nov. 3, 2022).....	40
<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH</i> , IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020).....	94
<i>Alcon Inc. v. AMO Dev., LLC</i> , IPR2021-00843, Paper 15 (PTAB Nov. 12, 2021).....	41
<i>Becton, Dickinson & Co. v. B. Braun Melsungen AG</i> , IPR2017-01586, Paper 8 (PTAB Dec. 15, 2017)	94
<i>Ex parte Davis</i> , Appeal No. 2008-3403, 2008 WL 4865519 (BPAI Nov. 10, 2008)	22
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (en banc)	4
<i>Sotera Wireless, Inc. v. Masimo Corp.</i> , IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020)	93
<i>Target Corp. v. Proxicom Wireless, LLC</i> , IPR2020-00931, Paper 10 (PTAB Nov. 10, 2020).....	41
<i>Williamson v. Citrix Online, LLC</i> , 792 F.3d 1339 (Fed. Cir. 2015) (en banc)	39
<i>Zeroclick, LLC v. Apple Inc.</i> , 891 F.3d 1003 (Fed. Cir. 2018)	40
<i>Zillow Grp., Inc. v. Int’l Bus. Machs. Corp.</i> , IPR2020-01656, Paper 8 (PTAB Mar. 15, 2021)	41
Statutes	
35 U.S.C. § 102(a)	1

35 U.S.C. § 102(b)	1
35 U.S.C. § 102(e)	1
35 U.S.C. § 103	1
35 U.S.C. § 112	40
35 U.S.C. § 314(a)	93
35 U.S.C. § 315(d)	93
35 U.S.C. § 325(d)	94

Regulations

37 C.F.R. § 42.104(b)(3).....	40, 41, 88
-------------------------------	------------

Other Authorities

<i>Memorandum re Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (June 21, 2022).....</i>	93
---	----

TABLE OF EXHIBITS

Exhibit	Description
Ex. 1001	U.S. Patent No. 6,993,658 B1 to Engberg et al. (“the ’658 Patent”)
Ex. 1002	Declaration of Dr. Peter Lawrence Reiher (“Reiher”)
Ex. 1003	Curriculum Vitae of Dr. Peter Lawrence Reiher
Ex. 1004	Prosecution History of the ’658 Patent
Ex. 1005	Japanese Patent Application Publication No. JP2000-10927 (Japanese language document) to Kato, filed June 25, 1998, published January 14, 2000 (“Kato”)
Ex. 1006	English Translation of Japanese Patent Application Publication No. JP2000-10927
Ex. 1007	U.S. Patent No. 6,161,185 to Guthrie et al., filed March 6, 1998, published December 12, 2000 (“Guthrie”)
Ex. 1008	U.S. Patent No. 5,060,263 to Bosen et al., filed March 9, 1988, published October 22, 1991 (“Bosen”)
Ex. 1009	U.S. Patent No. 6,609,206 B1 to Veneklas, filed February 5, 1999, published August 19, 2003 (“Veneklas”)
Ex. 1010	U.S. Patent No. 5,604,803 to Aziz, filed June 3, 1994, published February 18, 1997 (“Aziz”)
Ex. 1011	U.S. Patent No. 6,078,908 to Schmitz, filed April 22, 1998, published June 20, 2000 (“Schmitz”)
Ex. 1012	International Patent Application Publication No. WO 95/19593 to Kew et al., filed January 12, 1995, published July 20, 1995 (“Kew”)
Ex. 1013	U.S. Patent No. 5,153,919 to Reeds et al., filed September 13, 1991, published October 6, 1992 (“Reeds”)

Exhibit	Description
Ex. 1014	U.S. Patent No. 6,662,300 B1 to Peters, filed June 29, 1999, published December 9, 2003 (“Peters”)
Ex. 1015	U.S. Patent No. 5,668,876 to Falk et al., filed June 24, 1994, published September 16, 1997 (“Falk”)
Ex. 1016	U.S. Patent No. 5,491,752 to Kaufman et al., filed September 2, 1994, published February 13, 1996 (“Kaufman”)
Ex. 1017	U.S. Patent No. 5,736,932 to Bulfer et al., filed July 3, 1996, published April 7, 1998 (“Bulfer”)
Ex. 1018	International Patent Application Publication No. WO 97/31306 to Sormunen et al., filed February 6, 1997, published August 28, 1997 (“Sormunen”)
Ex. 1019	U.S. Patent Application Publication No. 2001/0007817 to Odagiri et al., filed December 8, 2000, published July 12, 2001 (“Odagiri”)
Ex. 1020	International Patent Application Publication No. WO 01/16899 A2, filed August 17, 2000, published March 8, 2001 (“Shields”)
Ex. 1021	U.S. Patent No. 6,430,407 B1 to Turtiainen, filed February 4, 1999, published August 6, 2002 (“Turtiainen”)
Ex. 1022	U.S. Patent No. 6,731,731 B1 to Ueshima, filed March 29, 2001, published May 4, 2004 (“Ueshima”)
Ex. 1023	U.S. Patent No. 6,259,909 B1 to Ratayczak et al., filed July 8, 1998, published July 10, 2001 (“Ratayczak”)
Ex. 1024	U.S. Patent Application Publication No. 2003/0046083 A1 to Devinney et al., filed November 21, 1997, published March 6, 2003 (“Devinney”)
Ex. 1025	U.S. Patent No. 6,535,855 B1 to Cahill et al., filed March 31, 1998, published March 18, 2003 (“Cahill”)

Exhibit	Description
Ex. 1026	U.S. Patent No. 7,260,221 B1 to Atsmon, filed May 15, 2001, published August 21, 2007 (“Atsmon”)
Ex. 1027	U.S. Patent No. 5,406,619 to Akhteruzzaman, filed March 31, 1994, published April 11, 1995 (“Akhteruzzaman”)
Ex. 1028	U.S. Patent No. 6,338,140 B1 to Owens et al., filed November 24, 1998, published January 8, 2002 (“Owens”)
Ex. 1029	U.S. Patent No. 5,887,065 to Audebert, filed October 2, 1997, published March 23, 1999 (“Audebert”)
Ex. 1030	U.S. Patent Application Publication No. 2002/0178370 A1 to Gurevich et al., filed December 29, 2000, published November 28, 2002 (“Gurevich”)
Ex. 1031	U.S. Patent No. 6,983,308 B1 to Oberhaus et al., filed December 22, 1998, published January 3, 2006 (“Oberhaus”)
Ex. 1032	U.S. Patent No. 6,035,406 to Moussa et al., filed April 2, 1997, published March 7, 2000 (“Moussa”)
Ex. 1033	Disclosure of Asserted Claims and Infringement Contentions, <i>Dynapass IP Holdings LLC v. JPMorgan Chase & Co. et al.</i> , Case No. 2:22-cv-00212 (Lead Case) (E.D. Tex. Sept. 8, 2022)

I. Relief Requested

Petitioners request *inter partes* review and cancellation of claims 1-3 and 5-7 (“the Challenged Claims”) of U.S. Patent No. 6,993,658 based on:

Exhibit	References	Type
Ex. 1005	Japanese Patent Application Publication No. JP2000-10927 (Japanese language document) to Kato, filed June 25, 1998, published January 14, 2000 (“Kato”) ¹	§ 102(a)
Ex. 1007	U.S. Patent No. 6,161,185 to Guthrie et al., filed March 6, 1998, published December 12, 2000 (“Guthrie”)	§ 102(e)
Ex. 1018	International Patent Application Publication No. WO 97/31306 to Sormunen et al., filed February 6, 1997, published August 28, 1997 (“Sormunen”)	§ 102(b)

The Challenged Claims are unpatentable under the following grounds:

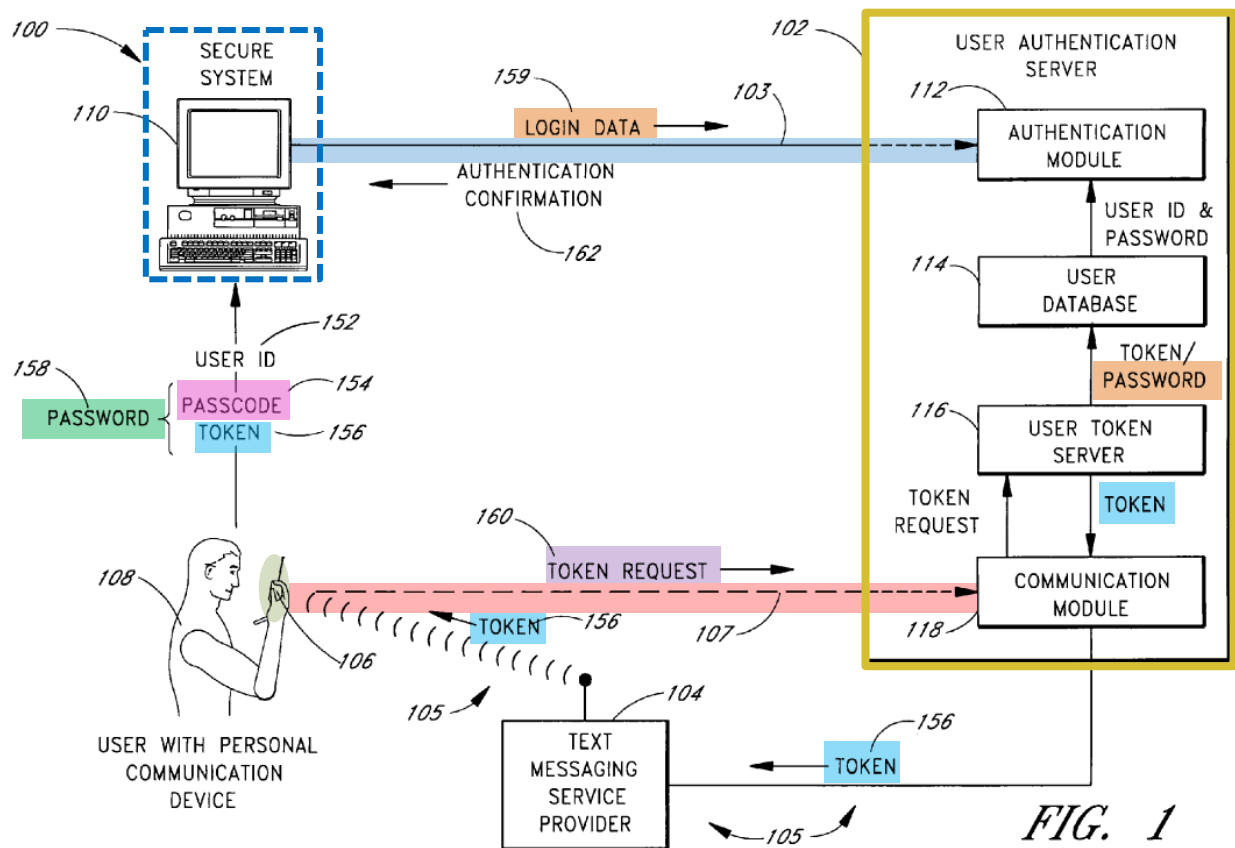
Ground	Claims	Reference(s)	Basis
1	1-3, 5-7	Guthrie, Sormunen	§ 103
2	1-3, 5-7	Kato, Guthrie	§ 103

¹ All reference cites are based on the translation (Ex. 1006).

II. The '658 Patent

The application for the '658 Patent was filed on March 6, 2000. Ex. 1001, 1. Dynapass asserted that the priority date of Challenged Claims is the March 6, 2000, filing date. Ex. 1033, 3.

The '658 Patent discloses authenticating a user to access a secure system based on a password. Ex. 1001, Abstract. A user authentication server authenticates the user by receiving a password from the user via a secure computer network and comparing the received password with a password associated with the user in a user database. *Id.*, Abstract, 3:8-14, 7:11-18, 7:40-67.



Id., FIG. 1.²

To obtain the password, the user sends a request for a token to a token server over a cell phone network via a personable communication device. *Id.*, 5:22-31, 6:1-12, 6:26-40, 7:46-63, 9:3-10. The user authentication server identifies the request with the user, generates a token, and transmits the token to the personal communication device. *Id.*, 1:63-2:15, 5:22-56, 6:4-12, 6:35-67, 7:31-39, 9:28-54, 10:59-62. The token server also generates a new password based on the token and a passcode and updates the user database. *Id.*, 6:59-64, 8:16-25, 8:53-63, 9:28-37. The token is not known to the user, but the passcode is. *Id.*, 4:36-39, 6:52-55, 9:21-25. Before the token expires, the user can submit the password to the user authentication server via the secure computer network to access the secure system. *Id.*, Abstract, 4:52-56, 7:57-67, 9:55-64.

III. Level of Ordinary Skill

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 least two years of prior experience with user

² All emphases and annotations added unless noted otherwise.

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. *Reiher*, 23.

IV. Claim Construction

The Board construes claims per *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). For this IPR, the plain meaning of each claim term can be applied. *Reiher*, 25-29. Petitioners reserve the right to contend that any of the Challenged Claims are indefinite.

V. Ground 1: Guthrie in Combination with Sormunen Renders Obvious the Challenged Claims

A. Guthrie-Sormunen Combination

1. Summary of the Guthrie-Sormunen Combination

Guthrie discloses authenticating a user to access network resources coupled to a server based on dynamic authentication data submitted via a client. To enhance security, Guthrie discloses using authentication data that includes three pieces of authentication information—a secret password known by the user (never transmitted across a network), a randomly generated challenge (transmitted to the user), and a response generated from the password and challenge (transmitted by the user). Guthrie, Abstract. Guthrie discloses sending a request for the challenge from the user via the client to the server, transmitting the challenge from the server to the client

over a computer network, calculating a response by a client Secure Authentication DataBase (“SADB”) calculator by performing a hashing algorithm on the password and challenge, and transmitting the response to the server for authentication. *Id.*, 7:60-8:6, 6:57-64, 7:27-38; Reiher, 55.

Like Guthrie, Sormunen discloses authenticating a user to access network resources based on a dynamic password submitted via an access terminal. Sormunen, p. 1, ll. 24-28, p. 7, ll. 9-18, FIG. 2. To increase security, Sormunen discloses a method of obtaining the dynamic password that includes a three-device architecture: sending a “password request” from the user via a mobile station (one device) to a password server (second device), transmitting the password to the mobile phone over a mobile communication network, and submitting the password to the password server via an access terminal (third device) for authentication. *Id.*, p. 5, l. 33–p. 7, l. 18; Reiher, 56.

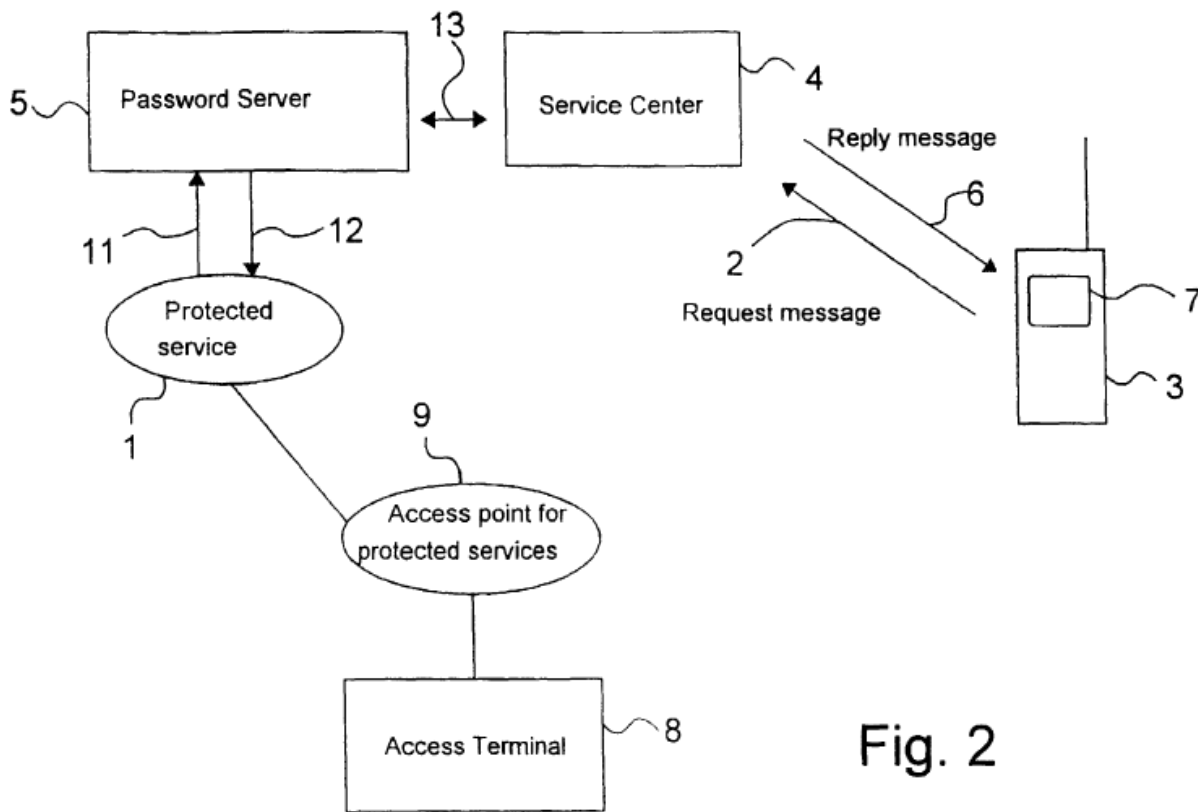


Fig. 2

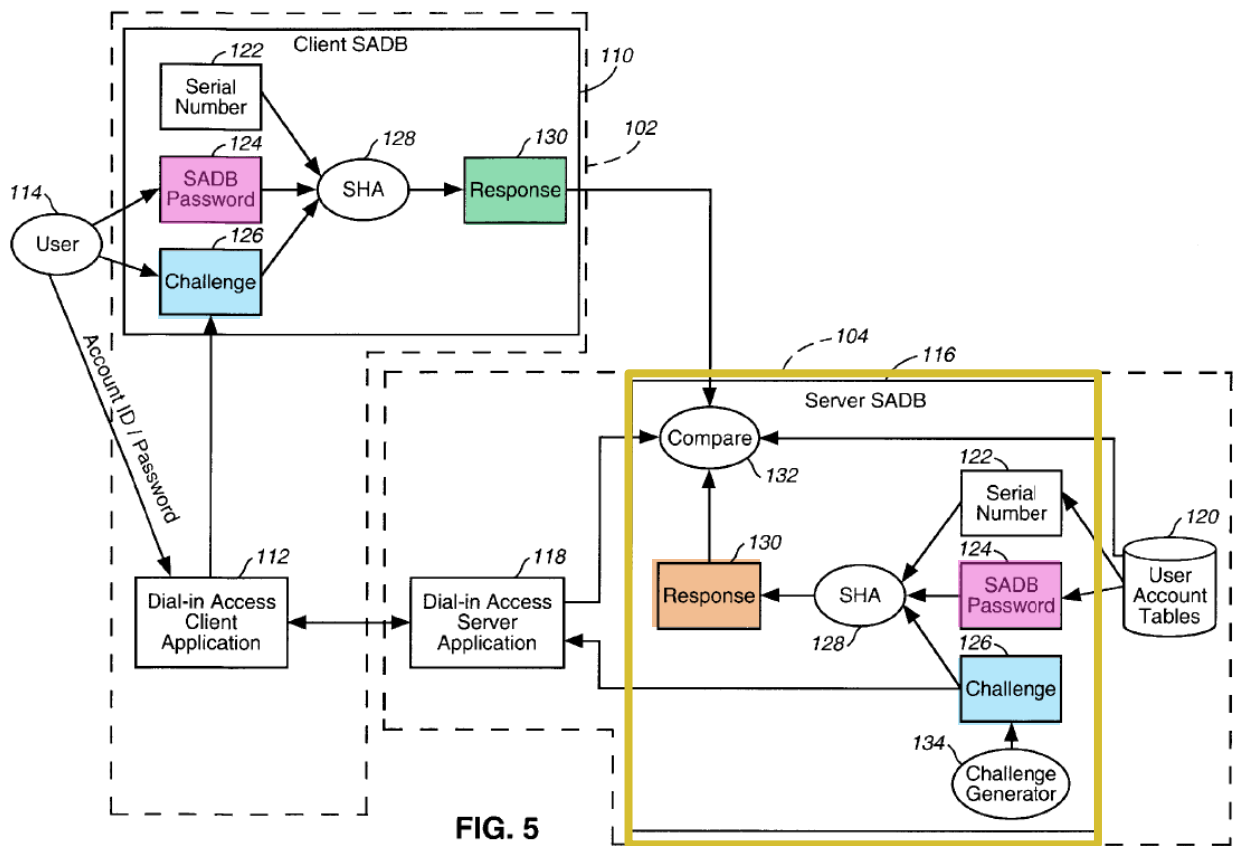
Sormunen, FIG. 2.

A POSITA would have combined Guthrie and Sormunen to improve the security of Guthrie's system by implementing Sormunen's mobile station to request and receive Guthrie's challenge. Adding a mobile station to Guthrie's system would improve the secure identification of the user by requiring the user to possess a third device (from Sormunen) in addition to the user's secret password (from Guthrie). Ratayczak, 1:39-55, 2:4-34, 4:24-32 (teaching using a mobile telephone for transmitting authentication data allows for greater security); Reiher, 57.

2. Guthrie and Sormunen Are Analogous Art and Combinable

The '658 Patent discloses authenticating a user to gain access to a secure system based on a dynamic password. Ex. 1001, Abstract; § II; Reiher, 58.

Like the '658 Patent, Guthrie discloses a personal authentication system with a dynamic challenge-response process to enhance security. Guthrie, Abstract; Reiher, 59.



Guthrie, FIG. 5.

To access a server, a user initiates an authentication request for a challenge from the server. *Id.*, 7:49-63. A server SADB calculator identifies the user, generates a challenge (an eight-digit random value), and sends the challenge to the user via the client. *Id.*, 7:64-8:2, 10:39-46, 11:21-25. The server also generates an expected response based on the challenge and an SADB password associated with the user stored in a user account table, updates the expected response value stored in the table, and sets in the user account table a response valid timer that provides a limited duration in which in the user must generate a response. *Id.*, 10:46-58, FIG. 6. After receiving the challenge, the user's computer calculates the response based on the challenge and the user's SADB password and submits the response to the server. *Id.*, 6:65-7:6, 7:27-38. Before the timer expires, the server compares the expected response with the response from the client to authenticate the user. *Id.*, 7:7-9, 7:38-45, 11:60-12:42. If the timer has expired, the user cannot be authenticated without restarting the challenge-response process. *Id.*, 11:50-59, FIG. 8B; Reiher, 60.

Sormunen is in the same field of user authentication and addresses the same problem of regulating a user's access to a secure computer system as the '658 Patent and Guthrie. Like the '658 Patent, Sormunen discloses a personal authentication system with a dynamic process for obtaining authentication data using a personal communication device—a mobile station—to enhance security. Sormunen,

Abstract, p. 5, l. 33–p. 7, l. 7. Like the '658 Patent, to securely obtain the password, Sormunen sends a short message including a “password request” from a mobile station via a mobile communication network, like a cellular network. *Id.*, p. 4, l. 30–p. 6, l. 1, p. 7, l. 37–p. 8, l. 3. A password server receives the request, generates a password, and sends a reply message containing the password to the mobile station. *Id.*, p. 6, ll. 20-38. The user then submits, via an access terminal, the received password to access the protected service. *Id.*, p. 6, l. 35–p. 7, l. 24. Sormunen’s mobile station communicates with the password server over a mobile communication network (*id.*, p. 7, l. 37–p. 8, l. 3, p. 8, ll. 19-22), and the access terminal is connected with the protected service over a separate computer network (*id.*, p. 3, ll. 25-38, p. 8, ll. 5-7). *Reiher*, 61.

Guthrie and Sormunen are both analogous to the '658 Patent and are combinable. Both disclose user authentication systems and obtaining dynamic authentication data for authenticating a user to access a secured system. Both address the same problem—problems of conventional authentication systems based on a fixed password, which can be stolen or guessed, and the risk of transmitting a secret password over a computer network, which can more easily be read by unauthorized users than short message service (“SMS”) messages over a cellular network. Guthrie, 1:20-28, 1:49-63; Sormunen, p. 2, ll. 20-29, p. 3, ll. 4-5, p. 4, ll. 1-7, 18-24.

Because both address these problems in different ways, the combination creates a more secure system than either individually. *Reiher*, 62.

3. A POSITA Would Be Motivated to Implement Sormunen's Mobile Station and Method for Requesting and Obtaining Authentication Data at a Mobile Station in Guthrie to Improve Security

a. Motivation

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 by: (1) preventing transmission of authentication data over the computer network; (2) preventing transmission of the user's secret password over any network; and (3) additionally identifying the user based on the mobile device possessed by the user. *Id.*, 63.

First, 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. Guthrie's server generates a challenge and sends the challenge to the user via an Internet network. Guthrie, 10:39-46, 11:21-25, 4:65-5:4, 5:25-27. But Sormunen teaches that "unauthorized persons can easily read

information transferred via the Internet.” Sormunen, p. 3, ll. 4-5; Veneklase, 1:25-38 (Internet communication systems “have been especially prone to unauthorized ‘break-ins’, viral destruction, and/or unauthorized data modifications”); Kaufman, 3:9-25 (passwords sent to access a distributed system can be eavesdropped). Implementing 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.” Sormunen, p. 6, ll. 5-9; Reiher, 64.

Second, 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. In Sormunen, an unauthorized user could obtain Sormunen’s mobile station and dynamic password to access the secure system. Odagiri, [0004], [0038] (an unauthorized person may obtain a portable telephone, such as a Personal Handy-phone System (“PHS”)). The combined system, however, requires the user to use both the challenge (transmitted) and a secret password (not transmitted) to generate the response, ensuring that an unauthorized user in possession of the mobile station and challenge cannot access the secured system without the user’s secret password.

Bosen 2:26-31, 4:44-49 (improving security by making the generation of authentic passwords dependent not only on possession of a random challenge, but also on possession of confidential information); Falk, 4:32-45 (confirming the user's identity by requiring information from the user, the authentication center, and the cellular phone), 5:4-7 (the user must know the user's PIN, be in possession of the cellular telephone, and receive the appropriate challenge code); Reiher, 65.

Third, 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. The only user-specific data Guthrie requires for requesting the challenge is the user account ID. Guthrie, 7:60-63. A user account ID is typically not secret and can be known to an unauthorized user. *Id.*, 1:25-29; Kato, [0003]; Kaufman, 2:8-12. Using 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. Sormunen, p. 4, ll. 30-33 (SMS messages are sent based on a telephone number), p. 9, ll. 28-32 (using a telephone number of the mobile station to identify the user); Ueshima, Abstract, 16:13-20, 10:20-29, FIG. 3 (authenticating a user by identifying the user's number before generating and transmitting a password to the user); Kato, [0008] (disclosing

a mobile telephone terminal has a telephone number); Bulfer, 3:1-18 (identifying a user based on a wireless remote communication device having a unique number); Falk, 4:32-45, 5:4-7; Turtiainen, 8:1-53 (identifying a user based on user information associated with a mobile station). Such identification of the user ensures that an unauthorized user who obtains the user's account ID and account password still cannot obtain the challenge to access Guthrie's secured system so long as the unauthorized user does not obtain possession of the user's personal communication device. And even if an unauthorized user were to obtain possession of the user's personal communication device, they would additionally have to have the user's secret password—which cannot be intercepted via network communications—to access the system. 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. Reiher, 66.

b. Reasonable Expectation of Success

A POSITA would have had a reasonable expectation of success in implementing Sormunen's mobile station and method for requesting and obtaining authentication data at the mobile station in Guthrie's authentication system. Guthrie's server can receive and send short messages in the same way as Sormunen's password server. Guthrie discloses that its server can have a dial-in application

forming connections over Integrated Services Digital Network (“ISDN”) lines. Guthrie, 5:30-32, 13:48-53. Likewise, Sormunen’s password server can connect with the SMS center using ISDN connection. Sormunen, p. 8, ll. 15-18. Guthrie’s server, like Sormunen’s password server, is capable and ready to form the same ISDN connection with an SMS center to receive a challenge request and send a challenge in short messages over a mobile communication network. *Id.*; Reiher, 67.

A POSITA would have further had a reasonable expectation of success in implementing Guthrie’s challenge-response process using the mobile device of Sormunen (adding Sormunen’s mobile station to Guthrie) by either (1) having the mobile station receive the challenge, but implementing Guthrie’s SADB calculator on Guthrie’s client after the user manually enters the received challenge on the client; or (2) having the mobile station implement Guthrie’s SADB calculator and then having the user enter the resulting response on Guthrie’s client. Both implementations provide the security benefit recognized by Guthrie of requiring manual entry of authentication data. Guthrie, FIG. 9A, 7:29-34, 12:57-60; Reiher, 68.

In the first implementation, a POSITA would have had a reasonable expectation of success because Guthrie’s SADB calculator is already implemented in its client device and Guthrie expressly contemplates a user manually entering

information into the calculator. Guthrie, FIG. 9A, 7:29-34, 12:57-60; Reiher, 69.

In the second implementation, a POSITA would have had a reasonable expectation of success because Sormunen's mobile station is capable and ready for implementing Guthrie's client SADB calculator or secured hashing algorithm ("SHA"). Sormunen's mobile station is capable of performing SHA. Guthrie discloses that its SADB calculators can be implemented as software on various platforms, including a "palm top computer." Guthrie, Abstract, 3:59-63, 4:8-13, 5:18-22, 5:48-6:9, 12:43-53, 13:16-20. A POSITA would have understood that a "palm top computer" is a mobile computer like Sormunen's mobile station. Odagiri, [0038], [0046]-[0047]; Ueshima, 4:1-4, 9:14-22; Oberhaus, 1:21-23. And mobile stations were known to perform hash algorithms. Falk, 3:4-20, 4:19-45. Guthrie's SADB calculators are "not compute intensive," and "the central processing unit (CPU) and input/output (I/O) processing requirements for the calculators are minimal ... so that authentication can be calculated in substantially less than one second." Guthrie, 2:57-67. Sormunen teaches that its mobile station can be implemented with software applications to perform functions, such as forming and processing short messages (Sormunen, p. 7, ll. 25-34). A POSITA would have understood that Guthrie's SADB calculator would be readily implemented in Sormunen's mobile station as a software application. Reiher, 70.

B. Independent Claims

1. Claim 1

- a. **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:”**

Guthrie discloses 1[preamble]. *Id.*, 72-77.

The '658 Patent provides no definition for secure computer network, but the specification explain that a secure computer network is a “secure system” accessible over a network. Ex. 1001, Abstract, 4:20-26. The “preferred embodiment of the present invention is a password setting system for setting user passwords for a **secure system, such as a computer system.**” *Id.*, 1:63-66. The user simply enters a valid password to gain access to the secure system. *Id.*, 2:8-11, 2:49-3:3, 4:9-13, 4:20-26. The specification makes no mention of securing the network itself, but only restricting access to only users with a valid password. Reiher, 73.

Like the '658 Patent, Guthrie discloses “[a] *method of authenticating a user*”³ because it discloses “[a] personal authentication system [that] provides at least two levels of security” for regulating a user’s access to a server computer on a “computer network.” Guthrie, Abstract, 3:53-55, 3:66-4:3, 4:57-5:6, 16:33-37; Reiher, 74.

³ Claim language in italics throughout.

Guthrie discloses “*a first secure computer network*” because Guthrie discloses *securing* the server on the computer network by restricting access to users with an account and a valid response. Guthrie, 5:43-47, 11:60-64; Reiher, 75.

Guthrie discloses “*authenticating a user on a first secure computer network*” because Guthrie discloses authenticating a user to access a secured server using a challenge-response process based on data exchanged between a client and a server over a computer network. Guthrie, 4:50-5:15, 5:22-27, 16:33-37; Reiher, 76.

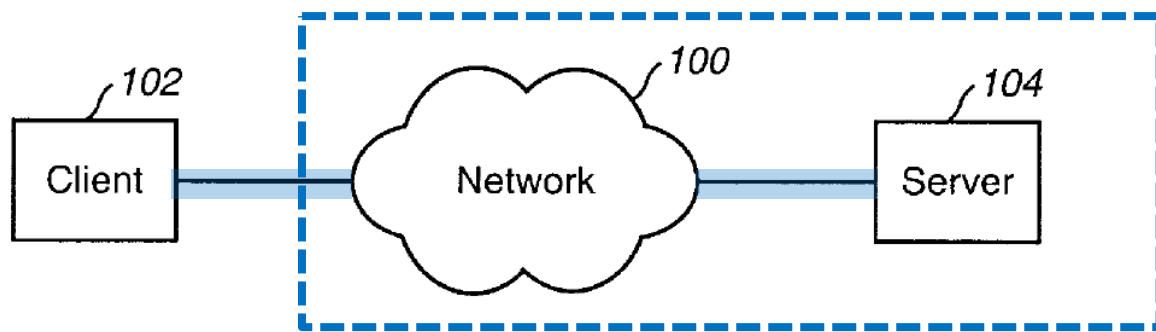


FIG. 1A

Guthrie, FIG. 1A.

Guthrie discloses “*the user having a user account on said first secure computer network*” because it discloses that the user “must initially establish an account with the server,” and the user account is stored in the user account database of the server. *Id.*, 5:35-47, 3:5-7, 6:6-9, 9:26-30. The user account database includes

tables of user accounts, including account IDs and account passwords with associated account IDs. *Id.*, 5:35-47, FIGS. 5-6; Reiher, 77.

- b. **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;”**

Guthrie in view of Sormunen renders obvious 1[a]. Reiher, 78-84.

Sormunen discloses “*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*” because Sormunen discloses a user using **a mobile station** (“*a personal communication device possessed by the user*”) to **request and receive passwords from a password server via an SMS center over a mobile communication network, such as a cellular network**. Sormunen, p. 4, l. 30–p. 5, l. 3, p. 8, ll. 19-22; Reiher, 79.

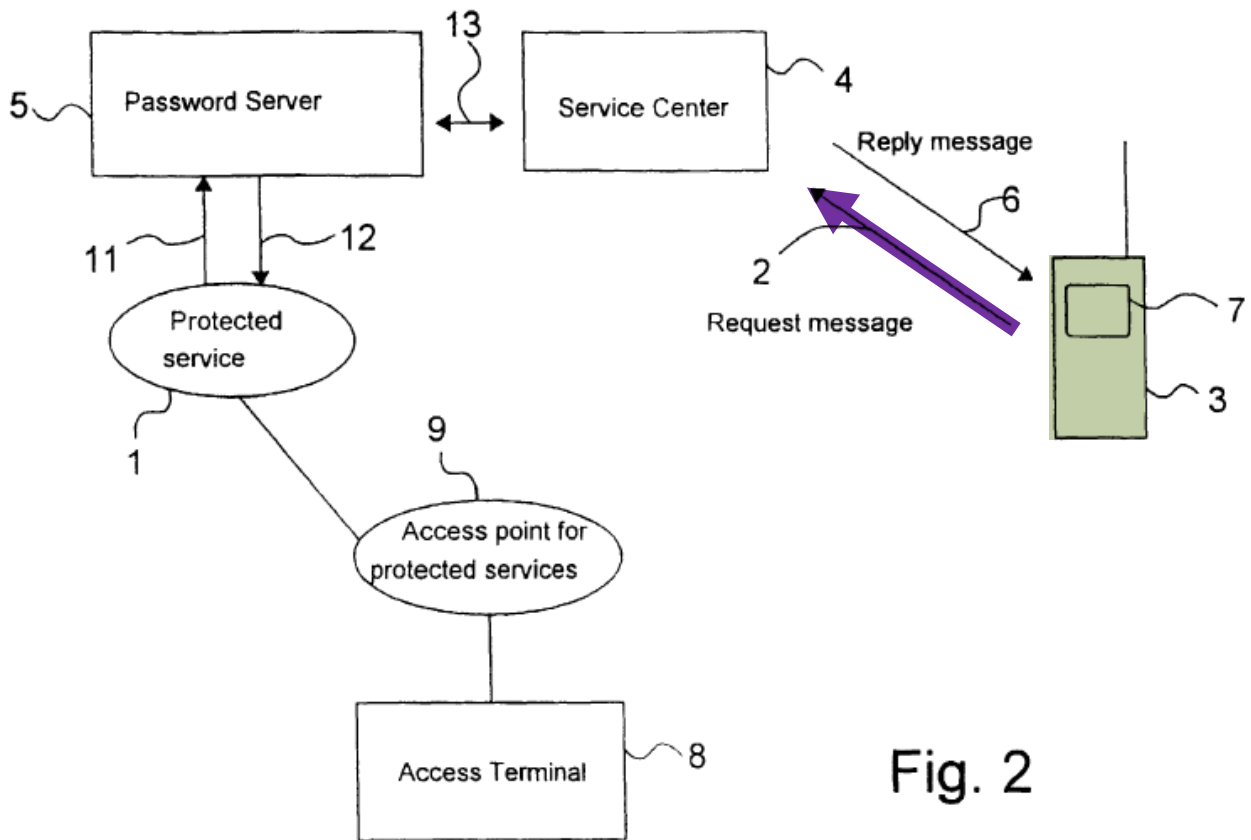
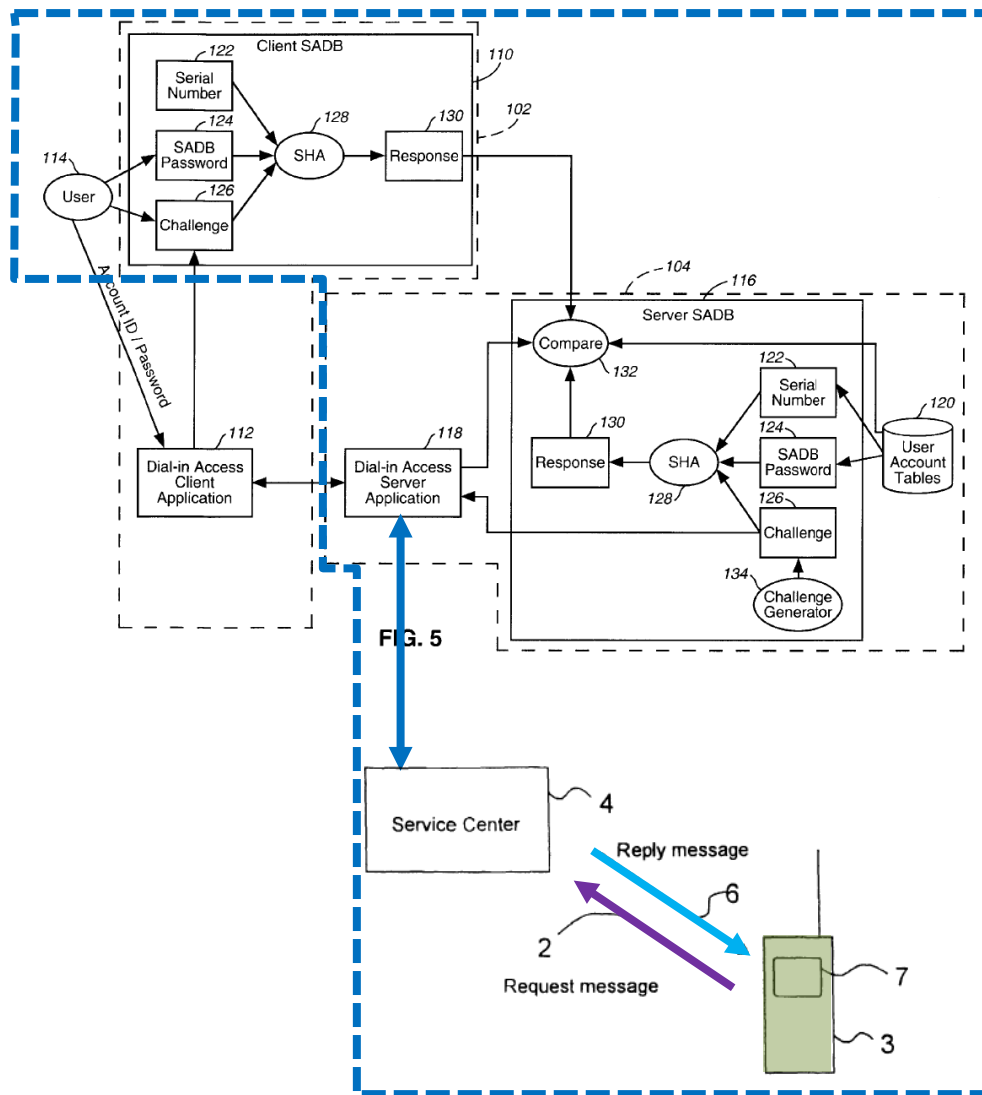


Fig. 2

Sormunen, FIG. 2.

As combined, a POSITA would have understood that Sormunen's mobile station is in communication with a cell phone network ("*second network*") that is different from Guthrie's secure computer system ("*first secure computer network*"). Reiher, 80.

A POSITA would have understood that the combination would transmit the **challenge request** and the **challenge** in short messages between Sormunen's mobile station and Guthrie's server, as shown below. *Id.*, 81.



Guthrie, FIG. 5; Sormunen, FIG. 2 (excerpted).

Guthrie discloses storing account information, shown below, in a user account database 120. Guthrie, 5:35-47, 7:64-8:6.

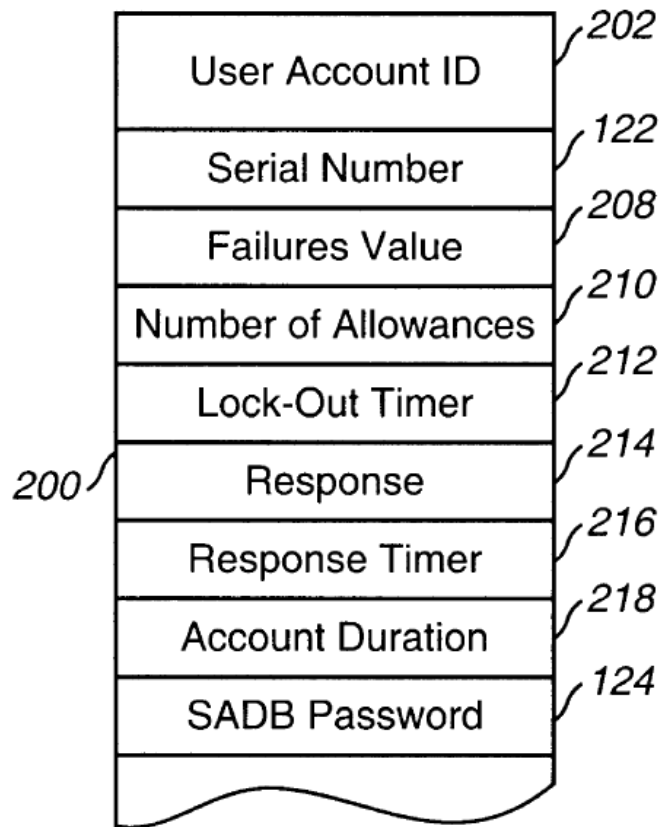


FIG. 6

Guthrie, FIG. 6. Guthrie's server's user database, as combined with Sormunen, would have been understood by a POSITA to further associate the user with the telephone number of the user's mobile station (*"associating the user with a personal communication device possessed by the user"*) for at least two reasons. First, Guthrie's server would need to first record the telephone number of Sormunen's mobile station to send a return challenge message to the user's mobile station. Second, a POSITA would have been motivated to store the user's telephone number

in the user's account for identifying the user in addition to the user's ID before generating the challenge to improve security. Kato, [0008]-[0009]; Bulfer, 3:1-18; Falk, 4:32-45, 5:4-7; § V.A; Reiher, 82-83.

A POSITA would have had a reasonable expectation of success in modifying Guthrie's account table to associate the user with its mobile station and modifying Guthrie's server to compare the telephone number associated with a received short message to that stored in the user's account. Such modifications would only require routine skill to achieve the expected result of storing the user's telephone number in Guthrie's account table and comparing two sets of telephone numbers, similar to Guthrie's storing and comparison of the user's password and account ID. Reiher, 84; *Ex parte Davis*, Appeal No. 2008-3403, 2008 WL 4865519, at *4-5 (BPAI Nov. 10, 2008) (finding using additional fields in a database obvious).

c. 1[b]: “receiving a request from the user for a token via the personal communication device, over the second network;”

Guthrie in view of Sormunen renders obvious 1[b]. Reiher, 85-88.

Guthrie discloses sending a request for a challenge (“*token*”) from a user via a client computer to the client server. Guthrie, 7:49-63. It would have been obvious to a POSITA to request a token, as disclosed by Guthrie, using Sormunen's mobile

station over a mobile communication network (“*via the personal communication device, over the second network*”). Reiher, 86.

Guthrie discloses at step 604 of Figure 7 that the user initiates a **request for a challenge** (“*token*”) from the client. Guthrie, 7:50-63. The challenge is “randomly generated” and “may be a string of eight alphanumeric characters or digits.” *Id.*, 6:57-64; Reiher, 87.

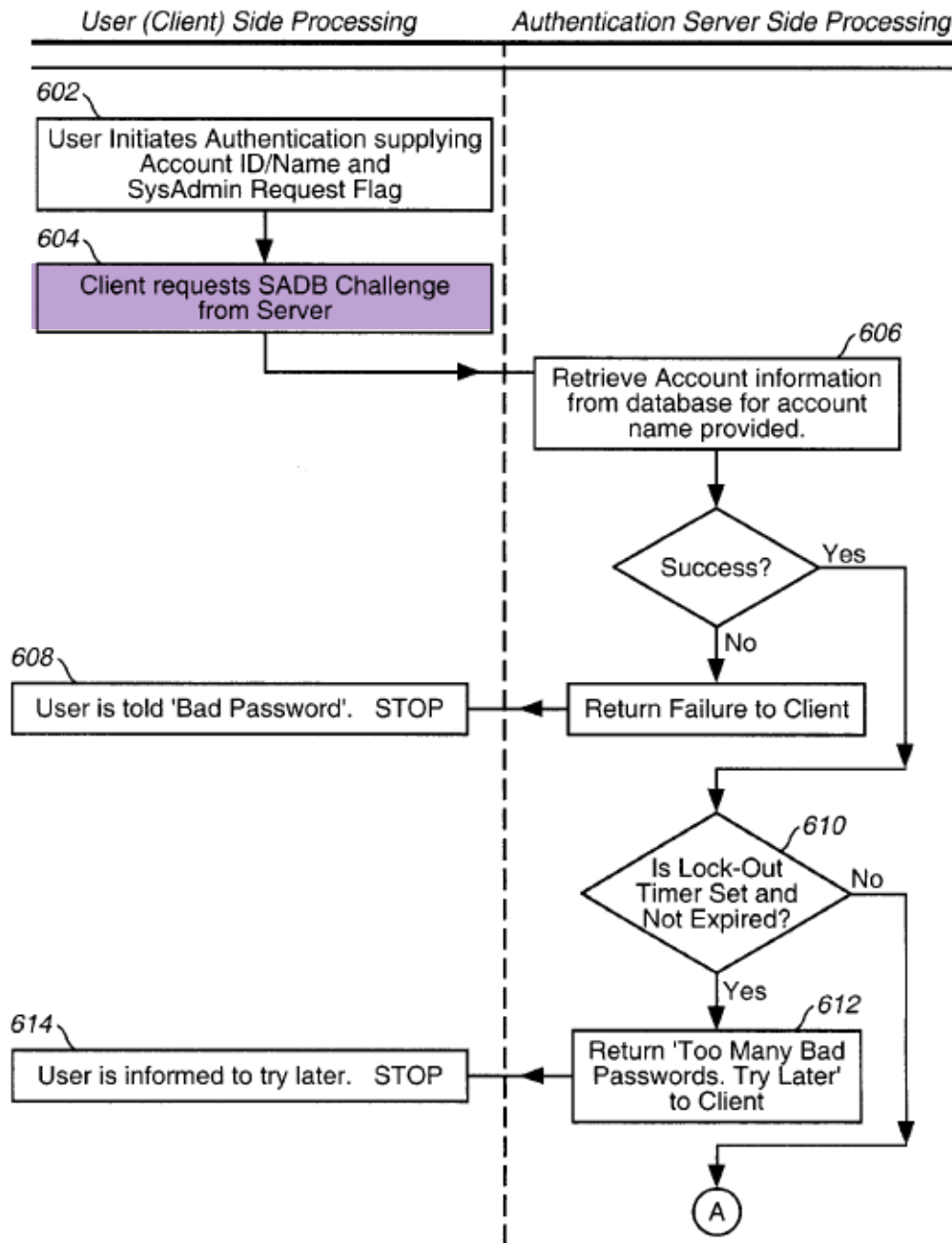


FIG. 7A

Guthrie, FIG. 7A.

A POSITA would have been motivated to implement Sormunen's mobile station and request for authentication data within Guthrie to add additional security by identifying the user before sending the challenge and would have had an expectation of success for this modification, as explained in Section V.A. Reiher, 88.

- d. **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;”**

Guthrie discloses 1[c]. *Id.*, ¶¶89-92.

Guthrie discloses generating an expected **response** value (“*new password*”) based on the **challenge** (“*token*,” unknown to the user) and an **SADB password** (“*passcode*,” known to the user). Guthrie's server receives the request for a challenge (“*token*”) and in response retrieves account information, shown below, from a user account database 120. Guthrie, 7:64-8:6. The user account table includes user account ID and an **SADB password** (“*passcode*”). Reiher, 90.

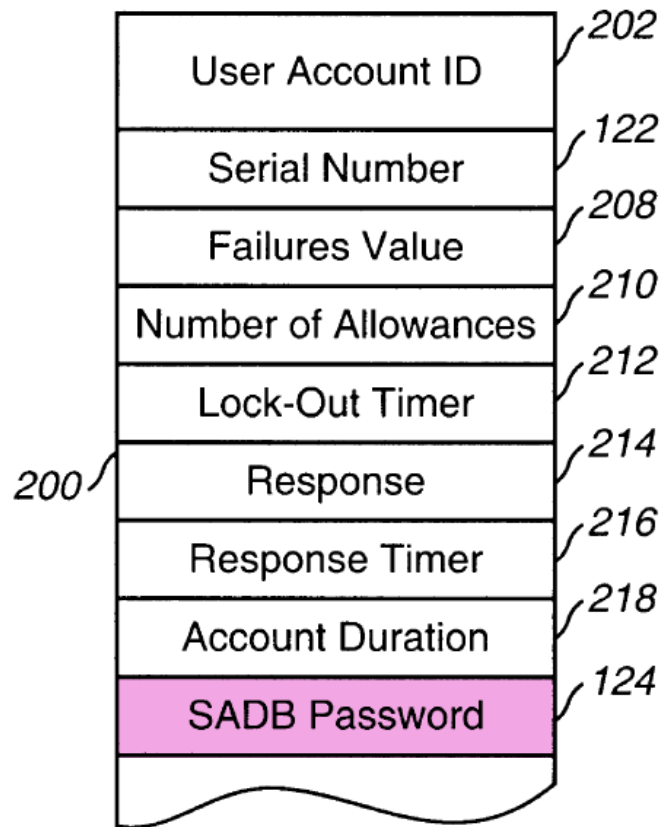


FIG. 6

Guthrie, FIG. 6.

After verifying the user's account information (step 656), Guthrie's server generates an eight digit or character challenge value ("token"). *Id.*, 10:39-46. In the next step (step 658), the server also generates an expected **response** value ("new password") based on the serial number, **SADB password** from the user's account table ("passcode"), and the **challenge** ("token"). *Id.*, 10:46-50; Reiher, 91.

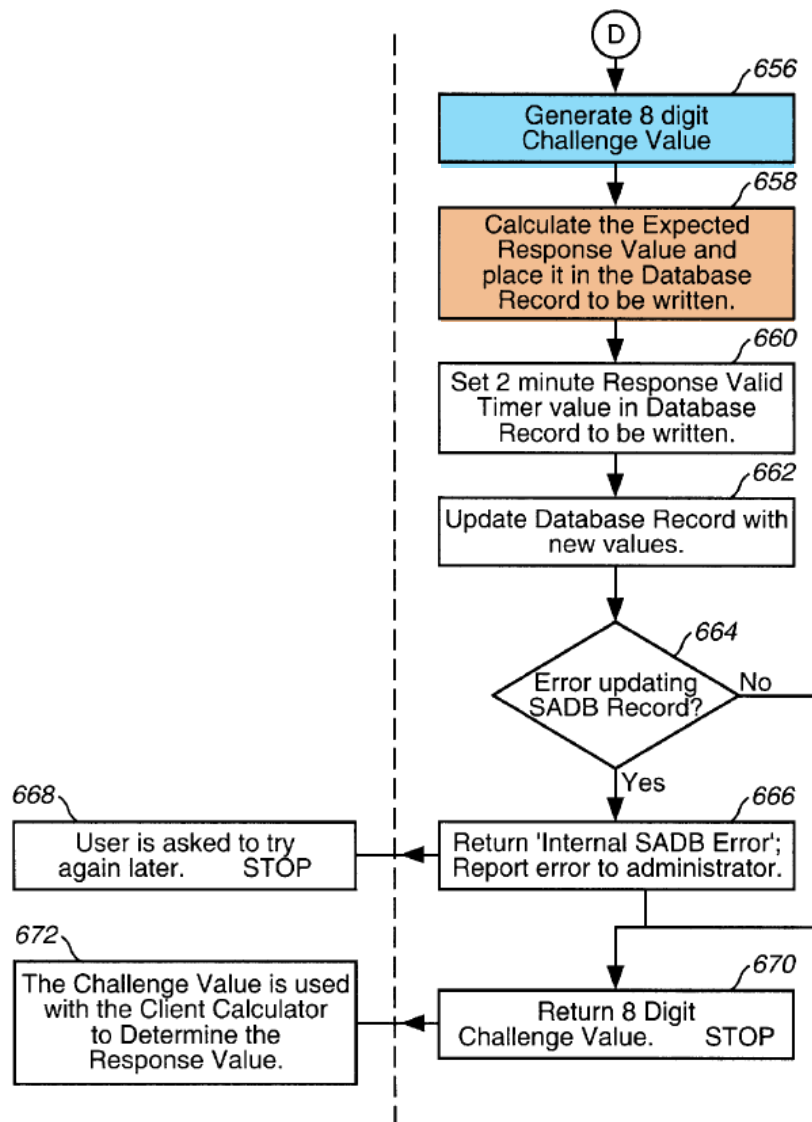
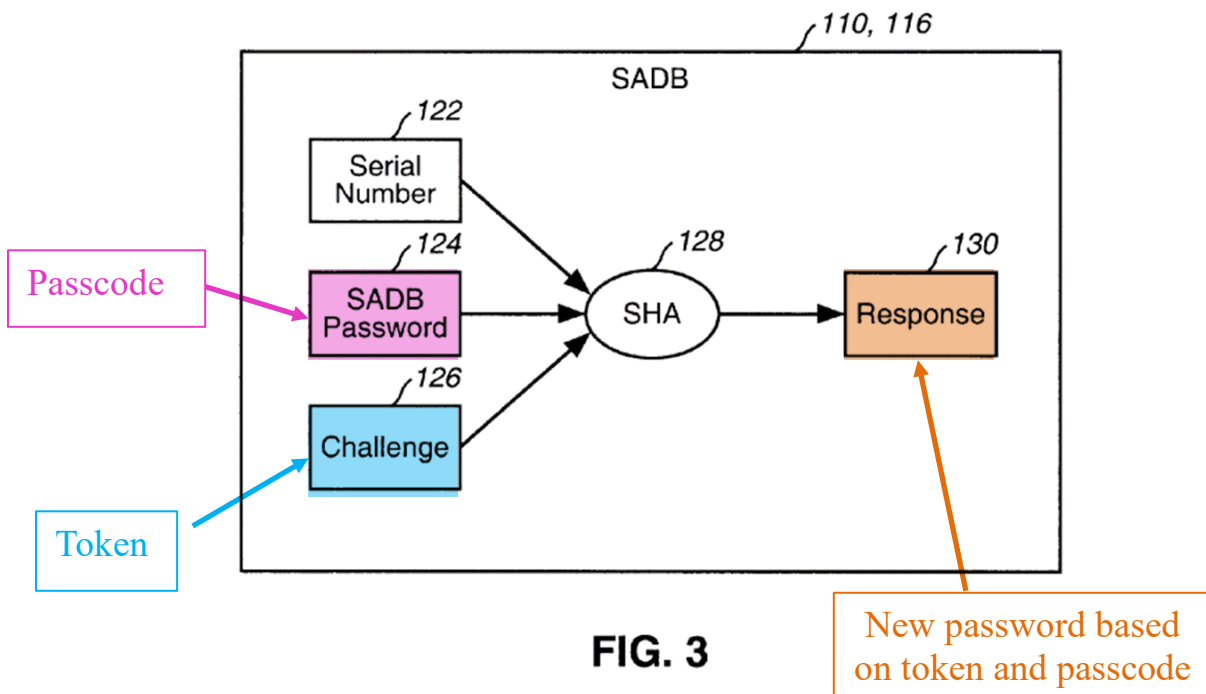


FIG. 7D

Guthrie, FIG. 7D.

Guthrie explains that its expected **response** value is generated based on the **challenge** (“*token*”) and the **SADB password** (“*passcode*”). Figure 3 of Guthrie is described as a “logical diagram of a process performed by the client and server

SADB calculators,” in which the **challenge**, the **SADB password**, and the serial number are “input together” into an SHA to compute a unique expected **response** value. *Id.*, 6:10-7:9. Guthrie’s challenge is unknown to the user because it is randomly generated at the server (*id.*, 6:57-64), and Guthrie’s SADB password is known to the user because it “may later be altered by the user” (“user’s often wish to personalize their passwords”) and is the “user’s ‘secret’” that is “provided by the user during authentication” (*id.*, 6:42-56). Reiher, 92.



Guthrie, FIG. 3.

- e. **1[d]: “setting a password associated with the user to be the new password;”**

Guthrie discloses 1[d]. Reiher, 93-96.

As explained in the previous Section, Guthrie’s expected response is the “*new password*.” Guthrie further discloses setting its expected response as the password associated with the user. Guthrie, 10:55-58; Reiher, 94.

In steps 658 and 662, Guthrie’s server updates and writes the expected **response** value (“*new password*”) into a response record in table 200 (“*setting a password associated with the user*”). Guthrie, 10:46-58; Reiher, 95.

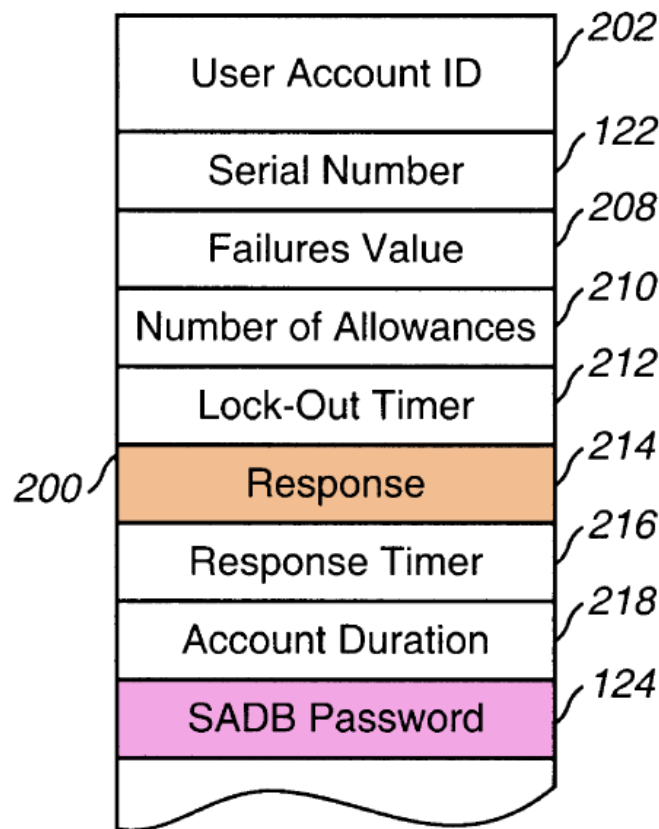
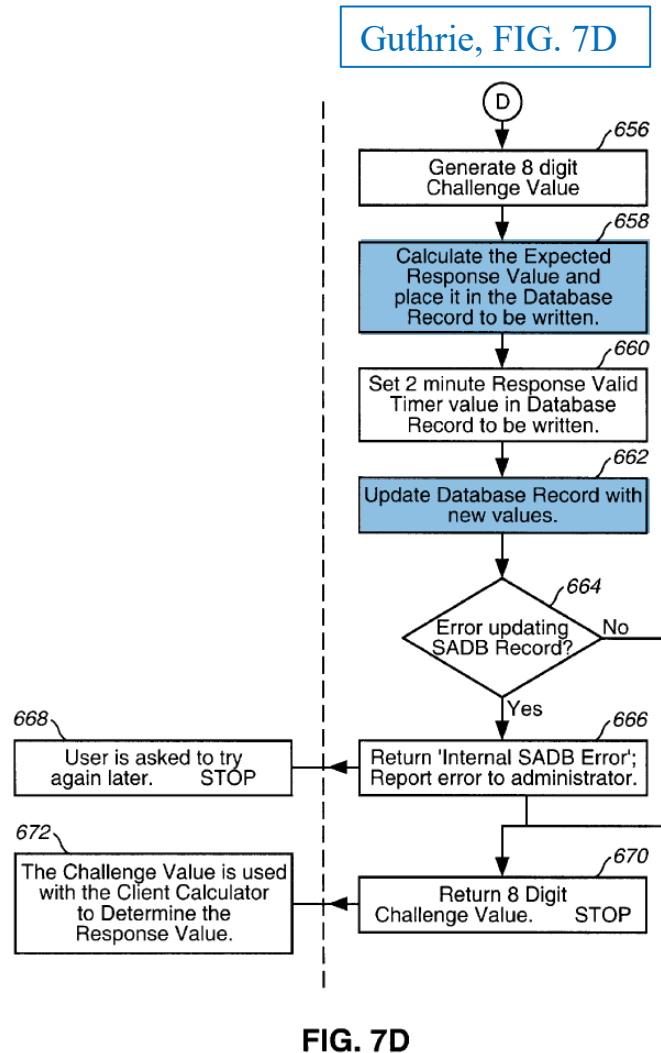
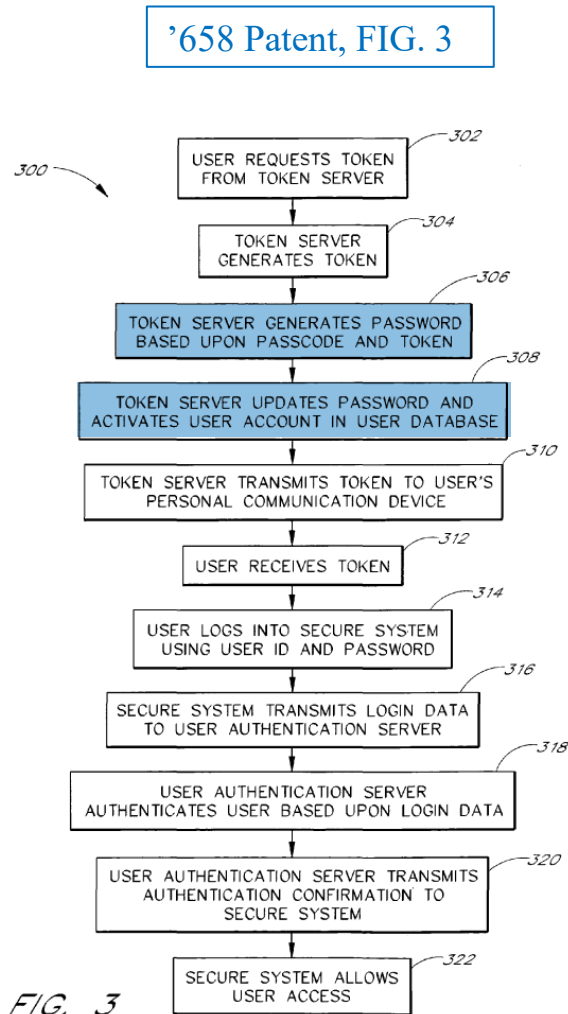


FIG. 6

Guthrie, FIG. 6.

The '658 Patent's steps 306 and 308 similarly have the token server update the user database with the generated new password. Ex. 1001, 6:59-67; Reiher, 96.



f. 1[e]: “activating access [to] the user account on the first secure computer network;”

Guthrie discloses 1[e]. Reiher, 97-100.

Guthrie discloses activating access to a user account after generating the expected response by setting a timer during which the expected response will grant

access, and when this process is combined with Sormunen's mobile station and method for requesting and obtaining authentication data at the mobile station, this limitation is obvious. *Id.*, 98.

In step 660, Guthrie discloses setting a response valid timer. Guthrie, 10:50-55. The response valid timer value is written into a response timer record of the user account table. *Id.*, 10:50-58. A POSITA would have understood that this activates the user account by allowing the user to use the response for gaining access to the server within the set period stored in the response timer record of the user's account table. Reiher, 99.

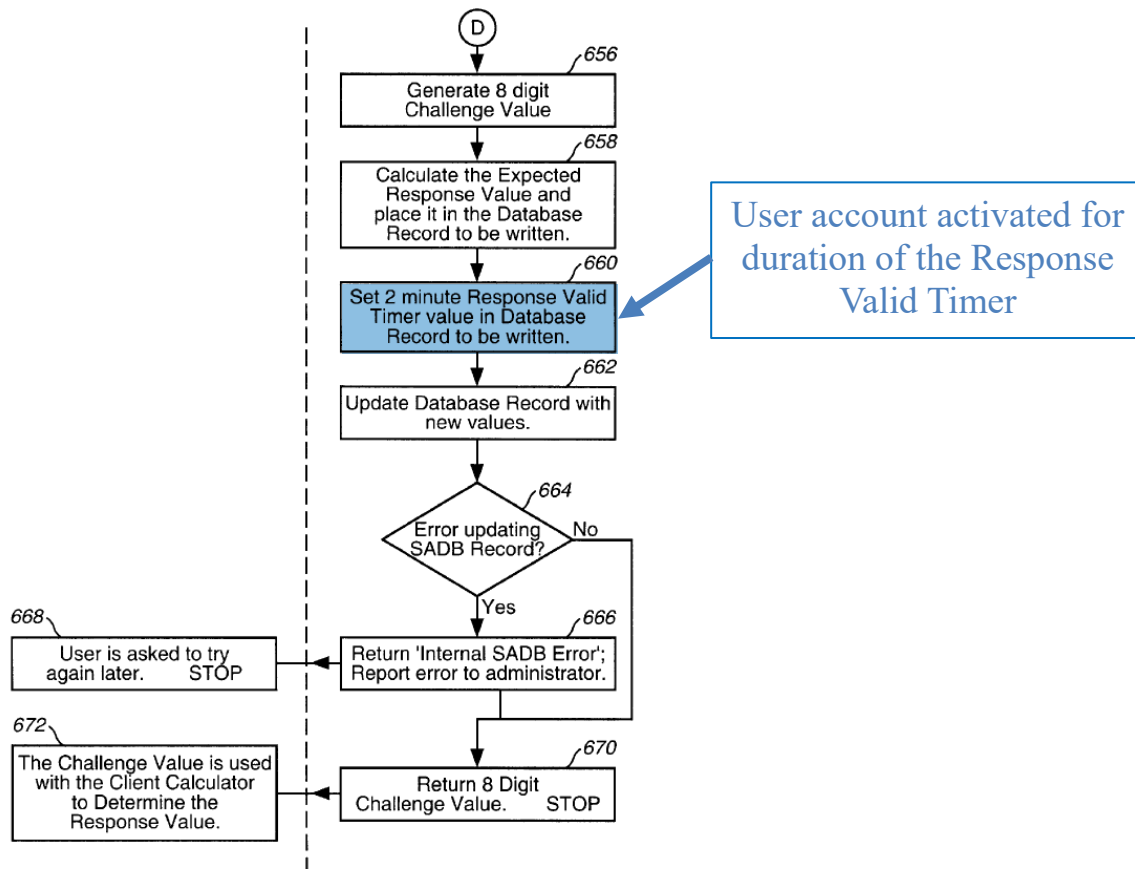


FIG. 7D

Guthrie, FIG. 7D.

Additionally, Guthrie discloses that “the server SADB calculator 116 employs a compare routine 132 to compare the receive response 130 with the response 130 locally generated by the server 104. The server 104 provides the client 102 with a message indicating whether the authentication succeeded or failed, and *enables appropriate access if successful.*” *Id.*, 7:38-45. Guthrie’s matching the received response to the expected response also activates access because Guthrie expressly states that appropriate access is enabled. Reiher, 100.

g. 1[f]: “transmitting the token to the personal communication device;”

Guthrie in view of Sormunen renders obvious 1[f]. *Id.*, 101-105.

Sormunen discloses transmitting a password to the user’s personal communication device. Because Guthrie combined with Sormunen uses Sormunen’s mobile station to obtain Guthrie’s challenge, the combination renders obvious transmitting Guthrie’s challenge (“*token*”) to Sormunen’s personal communication device. *Id.*, 102.

Sormunen’s password server generates a password in response to a password request in a short message and sends a reply message containing the password to the mobile station. Sormunen, p. 6, ll. 20-38; Reiher, 103.

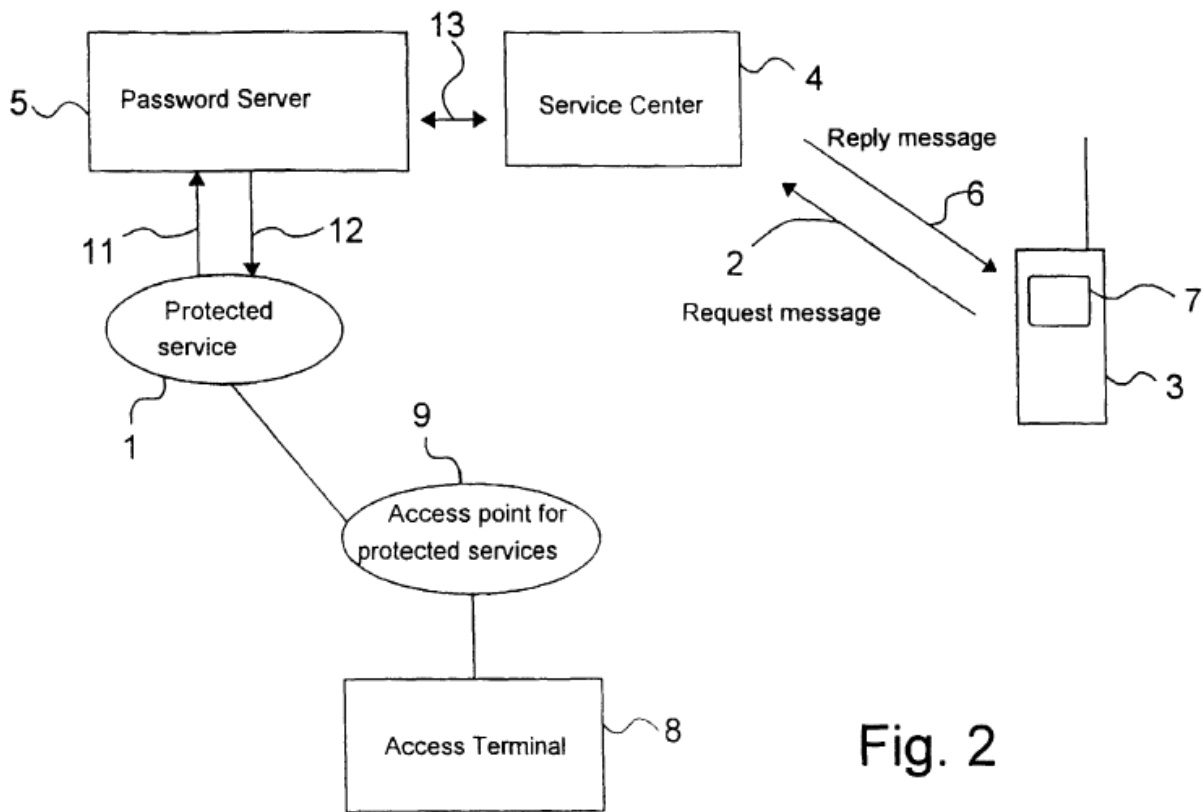
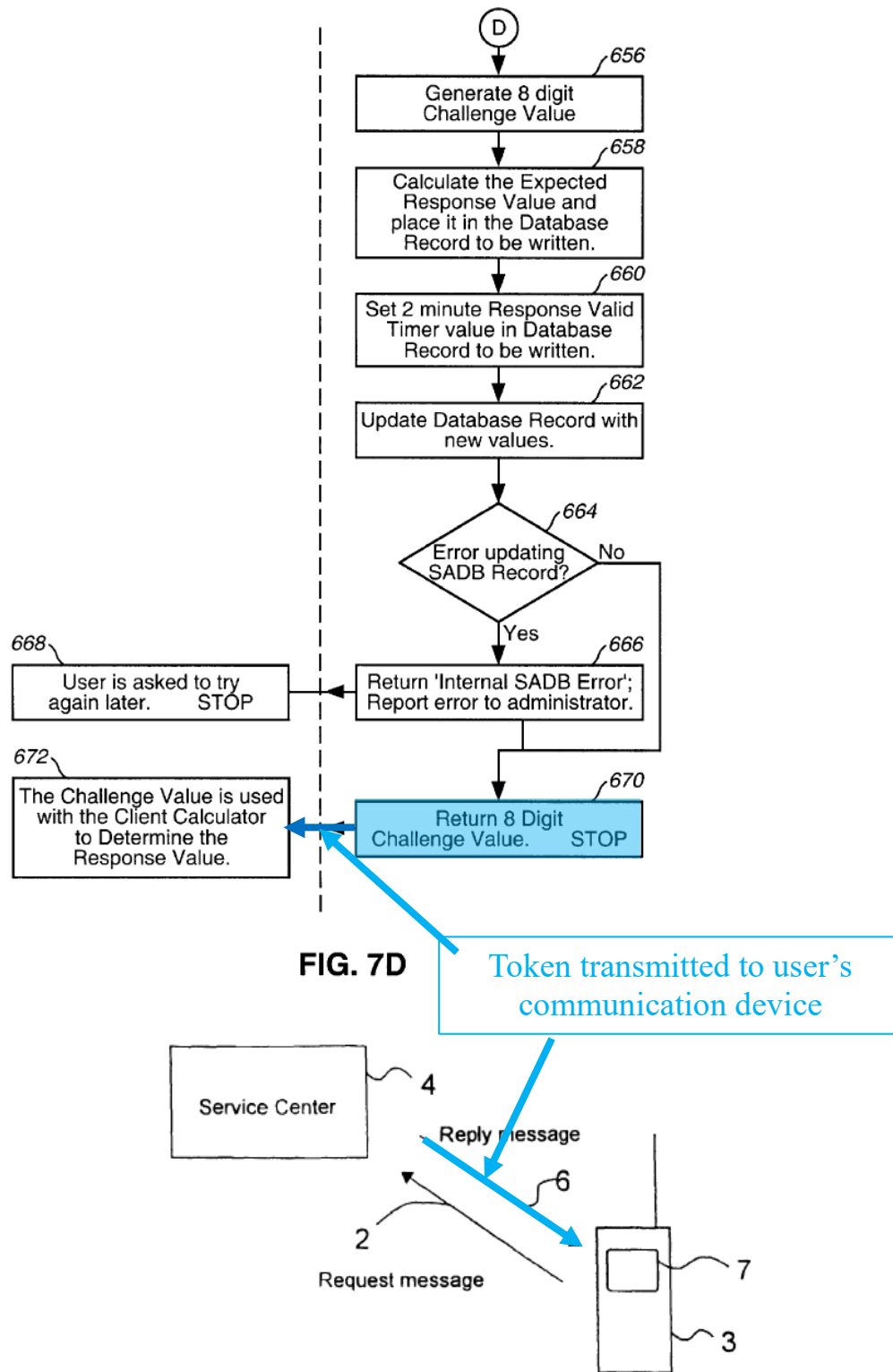


Fig. 2

Sormunen, FIG. 2.

In combination, rather than transmitting Guthrie's challenge to the client (Guthrie, 11:21-23, FIG. 7D), Guthrie's server would send the **challenge** ("token") to the mobile station ("*personal communication device*"), as taught by Sormunen—simply substituting Guthrie's challenge in place of Sormunen's password. Reiher, 104.



Guthrie, FIG. 7D; Sormunen, FIG. 2 (excerpted).

A POSITA would have implemented Sormunen's method of obtaining the password via a mobile station in Guthrie to prevent the challenge from being exposed during transmission to the user, as explained in Section V.A.3. Reiher, 105.

h. 1[g]: “receiving the password from the user via the first secure computer network; and”

Guthrie discloses 1[g]. *Id.*, 106-110.

In steps 802-806, Guthrie discloses that the user, after receiving the challenge, calculates the response based on the challenge and the user's SADB password and sends the **response** to the server, and the server receives the response (“*password*”) via the “*first secure computer network*” (Section V.B.1.a (1[preamble])). Guthrie, 6:65-7:6, 7:27-44, 11:27-35; Reiher, 107.

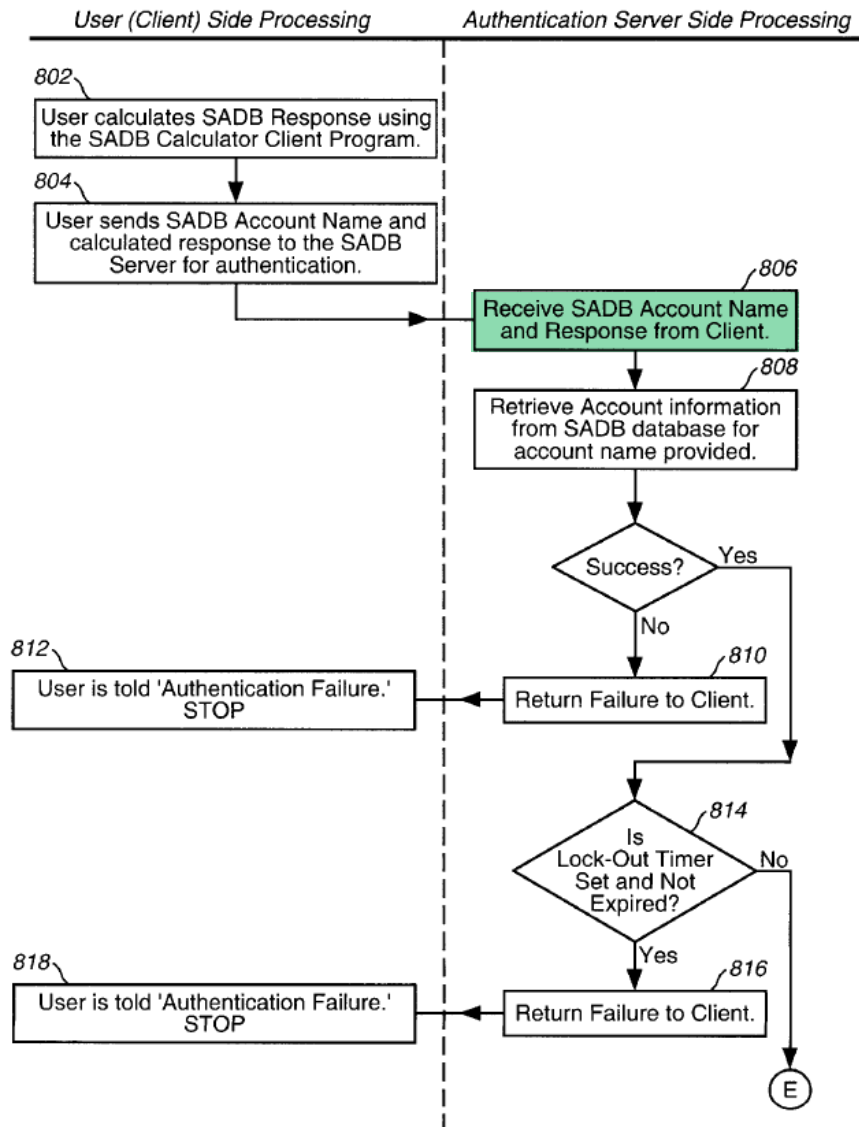
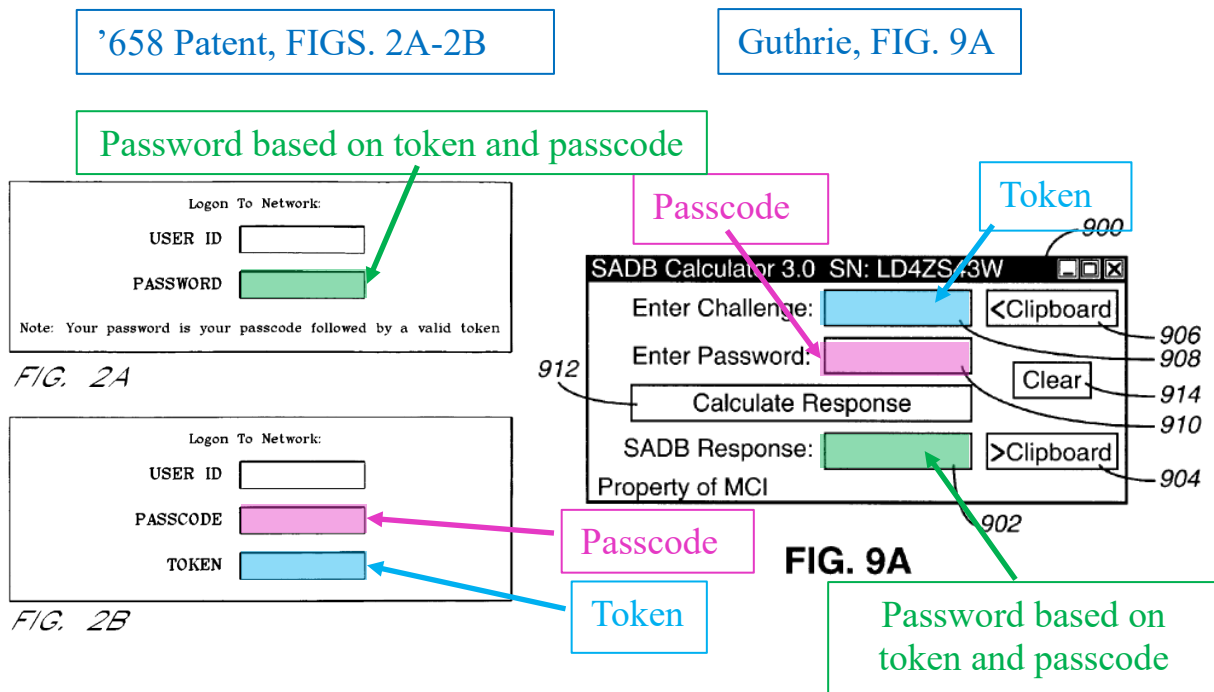


FIG. 8A

Guthrie, FIG. 8A.

In combination, Guthrie's client SADB calculator would either (1) remain at the client or (2) be implemented in Sormunen's mobile station to obtain the response, as explained in Section V.A.1. Reiher, 108.

In the first proposed combination, a POSITA would have understood that the user would obtain the response at the client using the challenge obtained from the mobile station and enter the response into the client for sending to the server, similar to the examples disclosed in the '658 Patent. Ex. 1001, 4:52-61, FIGS. 2A-2B; Reiher, 109.



In the second proposed combination, a POSITA would have understood that the user would receive at the mobile station the challenge in a reply message from the server, calculate the response at the mobile station based on the challenge and the user's known SADB password, and manually enter the response into an interface at Guthrie's client to transmit to Guthrie's server. Guthrie, 7:29-38, 12:57-60; Reiher, 110.

- i. **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.”**

Guthrie discloses 1[h]. Reiher, 111-113.

Guthrie discloses deactivating access after two minutes if the expected response is not received at the server. *Id.*, 112.

In step 660, Guthrie’s server sets a two-minute response valid timer (“*a predetermined amount of time after said activating*”) in the user account table to provide a limited duration within which the user must generate the appropriate response. Guthrie, 10:50-55. If the response valid timer expires, the server does not allow the user to gain access to the user account, even if the response is a valid response. *Id.*, 11:50-59. A POSITA would have understood that the response valid timer causes the server to “*deactivat[e] access to the user account on the first secure computer network*” when the timer expires by deactivating the user’s ability to access the user account on the server even if the password is received (“*said user account is not accessible through any password, via said first secure computer network*”). Guthrie’s response valid timer is similar to the ’658 Patent’s steps 518 and 520 where the user account is deactivated if the token’s expiry time has expired,

and the user will not be able to log in using the password (token + secret passcode).

Ex. 1001, 9:55-64, FIG. 5; Reiher, 113.

2. Claim 5

Independent claim 5 is substantially similar to claim 1 but styled as a system claim implementing routine hardware and software components. Claim 5 also is broader than claim 1 because it does not expressly require “*receiving a request from the user for a token via the personal communication device,*” but only “*transmit[ting] the token to the personal communication device through the cell phone network*”—both of which are disclosed by the combination. Reiher, 114.

Guthrie in view of Sormunen renders claim 5 obvious for the same reasons explained for claim 1, aside from its hardware and software components, like a processor executing various software modules, which are separately addressed below. *Id.*, 115.

a. Means-Plus-Function

Petitioners asserted in its invalidity contentions before the district court that the following terms are subject to 35 U.S.C. § 112, sixth paragraph: (1) “*control module,*” and (2) “*authentication module.*” Preliminarily, these limitations do not use the term “means” and thus are presumed not to be subject to interpretation as means-plus-function. *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1348 (Fed. Cir. 2015) (en banc). In the absence of evidence that a term would be understood by

a POSITA as means-plus-function, the Board “must presume that the term is not interpreted as a means-plus-function limitation.” *Abbott Diabetes Care Inc. v. DexCom, Inc.*, IPR2022-00922, Paper 13 at 12 (PTAB Nov. 3, 2022) (citing *Zeroclick, LLC v. Apple Inc.*, 891 F.3d 1003, 1008 (Fed. Cir. 2018)). As the Board has recognized, “forcing Petitioner to take [an approach of advocating for means-plus-function construction] would appear to completely undermine the party presentation principle by imposing a duty on Petitioner to make an argument against its interest in our proceedings that is not required by our Rules.” *Abbott Diabetes*, IPR2022-00922, Paper 13 at 15.

Nonetheless, for a term that may be construed as means-plus-function, 37 C.F.R. § 42.104(b)(3) requires a petitioner to “identify the specific portions of the specification that describe the structure, material, or acts corresponding to each claimed function.”

(1) “*Control module*”: Petitioners contend that the corresponding structure in the specification is a software module executed on the computer processor of the token server to perform the function recited in the claim. Ex. 1001, FIG. 4, 8:7-10.

(2) “*Authentication module*”: Petitioners contend that the corresponding structure in the specification is a software module executed on the computer

processor of the user authentication server to perform the function recited in the claim. *Id.*, FIG. 1, 5:1-21.

To the extent the Board finds any term should be construed as means-plus-function, whether Petitioners identify structure compliant with 37 C.F.R. § 42.104(b)(3) is a separate inquiry from whether the identified structure is sufficiently definite, and Petitioners' alternative indefinite assertion does not preclude review. *Zillow Grp., Inc. v. Int'l Bus. Machs. Corp.*, IPR2020-01656, Paper 8 at 11 (PTAB Mar. 15, 2021) ("Patent Owner cites no authority nor are we aware of any authority for the proposition that we may not assess the patentability of claims in an *inter partes* review because the Petitioner also challenges those claims as indefinite in District Court."); *Target Corp. v. Proxicom Wireless, LLC*, IPR2020-00931, Paper 10 at 9 (PTAB Nov. 10, 2020) (noting that "[a]lternative pleading before a court is common practice"); *Alcon Inc. v. AMO Dev., LLC*, IPR2021-00843, Paper 15 at 16 (PTAB Nov. 12, 2021) (instituting review despite petitioner's allegation before the district court that the claim is indefinite when the Board was "able to construe the disputed claim term with sufficient precision to address the obviousness arguments").

Here, Petitioners' alternative indefiniteness position does not subvert its identification of the corresponding structure for either of these terms in the

specification, compliant with 37 C.F.R. § 42.104(b)(3), because the specification's disclosure is of commensurate detail with that in the prior art and provides sufficient precision for the Board to address the obviousness argument.

b. 5[preamble]: “A user authentication system comprising:”

Guthrie discloses 5[preamble] because it discloses “[a] personal authentication system [that] provides at least two levels of security” for regulating a user's access to a server computer on a “computer network.” Guthrie, Abstract, 3:53-55, 3:66-4:3, 4:57-5:6, 16:33-37. Guthrie also discloses that “[t]he system operates across many different software and hardware platforms.” *Id.*, Abstract, 4:8-10; Reiher, 116.

Guthrie's server 104 is nearly identical to the '658 Patent's user authentication server 102, including the same components: user database (Guthrie's user account tables 120), control module (Guthrie's high-level portion of server 104 including server SADB 116, SHA 128, and response 130), communication module (Guthrie's dial-in access server application 118), and authentication module (Guthrie's server SADB 116 including compare routine 132). Reiher, 117.

- d. 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;”**

Petitioners asserted before the district court that “*user database*” and “*personal communication device*” should be construed as means-plus-function. Petitioners expressly waive that prior assertion and contend that these terms should be construed according to their plain and ordinary meaning because they connote sufficient structure in view of the specification of the ’658 Patent.

Guthrie in view of Sormunen renders obvious 5[b]. *Id.*, 119-120.

For reasons explained in 1[a], Sormunen discloses “*a personal communication device possessed by the user*” and that “*said personal communication device [is] configured to communicate over a cell phone network.*”

§ V.B.1.b; Reiher, 119.

Guthrie in view of Sormunen renders obvious “*a user database configured to associate a user with a personal communication device.*” Guthrie discloses a user account database 120 (“*user database*”) storing account information, shown in account table 200 in Figure 6 below. Guthrie, 5:35-47, 7:64-8:6. The user account table includes a user account ID and an SADB password, among other information. As explained in 1[a], because in Guthrie combined with Sormunen, the server

communicates with a mobile station in short messages, a POSITA would have modified Guthrie's user account database to associate the user with the telephone number of the mobile station ("*to associate the user with a personal communication device possessed by the user*") such that the server can send a message to the correct mobile station possessed by the user and identify the user with improved security based on the mobile station's telephone number. A POSITA would have had a reasonable expectation of success in this modification, as explained in 1[a].
§ V.B.1.b; Reiher, 120.

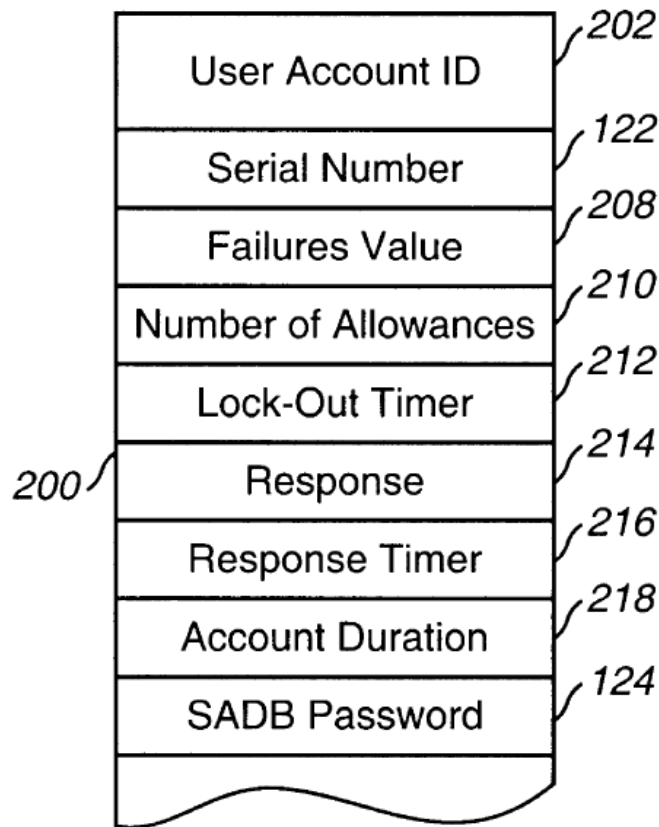


FIG. 6

Guthrie, FIG. 6.

Also, a POSITA would have found it obvious to configure Sormunen's mobile station to communicate in Guthrie's server (*"said personal communication device configured to communicate over a cell phone network with the user authentication system"*) because Guthrie's server is equipped for receiving and sending short messages from Sormunen's mobile station in the same way as taught by Sormunen to further improve authentication security. § V.A.3; Reiher, 121.

- e. **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,”**

Guthrie discloses 5[c] as explained in 1[c] and because Guthrie’s high-level portion of server 104 including server SADB 116, SHA 128, and response 130 (“*control module*”) is implemented on the computer processor of the server computer, as explained in 5[a]. §§ V.B.1.d, V.B.2.c; Reiher, 122.

The ’658 Patent explains that the control module is “the top level component of the user token server 116. The control module 402 preferably handles any tasks or functions not handled by the other modules of the token server 116, in addition to controlling the other modules [and] ... preferably maintains a supplemental user database 404” Ex. 1001, 8:16-24. Similarly, Guthrie’s server 104 manages all high-level functions of the system including subcomponents server SADB 116 (that handles operations like generating the expected response, using SHA 128 and response 130) (Guthrie, 5:30-42, 6:10-27, 7:64-8:6), as well as managing and accessing user account database 120 (*id.*, 5:43-47, 6:65-67, 7:19-22, 7:64-8:6). Reiher, 123, 31.

f. 5[d]: “the control module further configured to set a password associated with the user to be the new password;”

Guthrie discloses 5[d] as explained in 1[d] and because Guthrie’s high-level portion of server 104 (including server SADB 116, SHA 128, and response 130) (“*control module*”) is implemented on the computer processor of the server computer, as explained in 5[a]. §§ V.B.1.e, V.B.2.c; Reiher, 124.

g. 5[e]: “a communication module configured to transmit the token to the personal communication device through the cell phone network; and”

Petitioners asserted before the district court that “*communication module*” should be construed as means-plus-function. Petitioners expressly waive that prior assertion and contend that this term should be construed according to its plain and ordinary meaning because it connotes sufficient structure in view of the specification of the ’658 Patent.

Guthrie in combination with Sormunen renders obvious 5[e] because Guthrie discloses its server can have a dial-in application (“*communication module*”) that in combination with Sormunen would have been configured to send a challenge in a short message to Sormunen’s mobile station over a mobile communication network (“*transmit the token to the personal communication device through the cell phone network*”). § V.A.3; Guthrie, 5:22-35 (disclosing various “methods and/or apparatuses for establishing communications between the client 102 and server

104”). The ’658 specification similarly discloses that the communication module is “phone dialer 622.” Ex. 1001, 10:31-22; *see also id.*, 8:12-15 (“The various functional components may, however, be seamlessly integrated into one or more executable *programs, data structures, and/or physical components*”), 7:33-38 (“In the preferred embodiment, the communication module 118 is a *mobile phone, ...*”), 10:15-16 (“The communication module 118 is a *mobile phone 602* with SMS send capability.”), 10:22-26 (“In this case, the communication module 118 is an *ISDN card or an X.25 connection card 612 ...*”); Reiher, 125-126.

- h. 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,”**

Guthrie discloses 5[f] as explained for 1[g]. § V.B.1.h. Guthrie also discloses “*the user has an account on the secure computer network,*” as explained for 1[preamble] and 1[a]. §§ V.B.1.a-V.B.1.b; Reiher 127.

The ’658 Patent explains that the authentication module is “code or software ... that authenticates users upon login” and “may be any code, device, or module capable of authenticating a user.” Ex. 1001, 5:1-10. The “authentication module 112 preferably responds to an authentication request transmitted over the computer network 103 by supplying an authentication confirmation.” *Id.*, 5:10-15. Similarly,

Guthrie discloses that its server SADB 116 including compare routine 132 (“*authentication module*”) is an application or software routine implemented on the computer processor of the server computer. Guthrie, 4:14-16, 4:57-60. Guthrie’s compare routine 132 “compare[s] the receive[d] response 130 with the response 130 locally generated by the server” and provides “a message indicating whether the authentication succeeded or failed, and enables appropriate access if successful.” *Id.*, 7:38-45; Reiher, 128, 32.

- i. **5[g]: “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.”**

Guthrie discloses 5[g]. Guthrie discloses that its authentication module “*activates access to the account,*” for reasons explained for 1[e]. § V.B.1.f. Guthrie also discloses that the activation is “*in response to the password*” because Guthrie sets the response valid timer once it generates the response (“*password*”) and “*enables appropriate access*” when a user-submitted response matches the expected response. Guthrie, 7:38-45, 10:50-58; § V.B.1.f. Guthrie discloses that its authentication module, as explained for 5[f], “*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,” for reasons explained for 1[h]. §§ V.B.2.h, V.B.1.i; Reiher, 129-130.

C. Dependent Claims

1. **Claim 2: “The method of claim 1, wherein the new password is generated by concatenating the token and the passcode.”**

Guthrie discloses claim 2 because, as explained for 1[c], Guthrie uses a hashing algorithm to generate the new password based on Guthrie’s SADB password (“*passcode*”) and challenge (“*token*”). § V.B.1.d. A POSITA would have understood that to perform a hashing algorithm, the input password and challenge would first be concatenated. Reiher, 131.

Hashing algorithms were known in the art and understood to “include any one-way routine for transmitting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence.” Kaufman, 9:47-52. Hashing algorithms were known to improve security of transmission of user authentication data. *Id.*, Abstract (inhibiting password attempts by using a hashing algorithm upon a password and token); Reeds, Abstract (concatenating a secret password and a random number and passing the concatenated information to a hash function for generating an output for cell phone authentication), 9:1-9 (concatenating

number sequences and hashing the concatenated string to form a hashed authentication sequence); Reiher, 132.

Guthrie explains that its SHA that generates the new password is not unique, stating, “As is known, a[n] SHA is a one-way hashing algorithm which generally cannot be reverse computed.” Guthrie, 6:17-19. In Guthrie, “[b]y employing the serial number 122, SADB password 124 [(“*passcode*”)] and challenge 126 [(“*token*”)], the SHA 128 generates a unique response 130.” *Id.*, 6:21-23. A POSITA would have understood that when Guthrie states that it “employs” certain inputs including the passcode and token, it is concatenating them to form a single input, as was commonly done in the art. Kaufman, 9:43-47 (“[H]ashing algorithm’ is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a ‘hashing equation’ upon one or more of the input data”). This is consistent with the disclosure of the ’658 Patent, which explains that “the password is a hashed concatenation of the passcode and the token.” Ex. 1001, 2:64-65; Reiher, 133.

A POSITA would have understood that Guthrie at least suggests concatenating its passcode and token for input into its SHA, or it would have been obvious to try concatenation as a well-known method for performing generic hashing algorithms like Guthrie’s SHA. Reiher, 134, 49-53.

2. Claim 3: “The method of claim 1, wherein the personal communication device is a mobile phone.”

Sormunen discloses claim 3 because its mobile station can be “a cellular system mobile station, such as a GSM mobile station,” capable of sending and receiving short messages over a “cellular network.” Sormunen, p. 5, ll. 1-3, p. 6, ll. 4-12, p. 12, ll. 32-34. A POSITA would have found it obvious to implement Sormunen’s request from a mobile station (“*mobile phone*”) in Guthrie’s authentication system to further improve security, as explained in Section V.A. Reiher, 135.

3. Claim 6: “The system of claim 5, wherein the communication module is further configured to receive a request from the user for the token, and wherein the control module is further configured to create the new password in response to the request.”

Guthrie discloses claim 6 as explained in 1[b] and 1[c] and because Guthrie discloses a dial-in access server application 118 (“*communication module*”) and a high-level portion of server 104 (including server SADB 116, SHA 128, and response 130) (“*control module*”), as explained in 5[c] and 5[e]. §§ V.B.1.c-V.B.1.d, V.B.2.e, V.B.2.g; Reiher, 136.

4. Claim 7: “The system of claim 6, wherein the request is transmitted by the user through the personal communication device.”

Guthrie in view of Sormunen renders obvious claim 7 as explained in 1[b].

§ V.B.1.c. A POSITA would have been motivated to implement Sormunen’s request from a mobile station in Guthrie to request the challenge to add additional security by identifying the user before sending the challenge and would have expected success for this modification, as explained in Section V.A. Reiher, 137.

VI. Ground 2: Kato in Combination with Guthrie Renders Obvious the Challenged Claims

A. Kato-Guthrie Combination

1. Summary of the Kato-Guthrie Combination

Kato and Guthrie are in the same field of endeavor and address the same problem—restricting access to a secured computer system using an authentication method—but in different ways that independently improve security. The combination improves the security of Kato’s system. Kato discloses a three-device architecture in which a user has both a PC (a first device to access the secure computer network—a third device) and a PHS mobile device (a second device to receive a temporary password to enter on the PC). Reiher, 139.

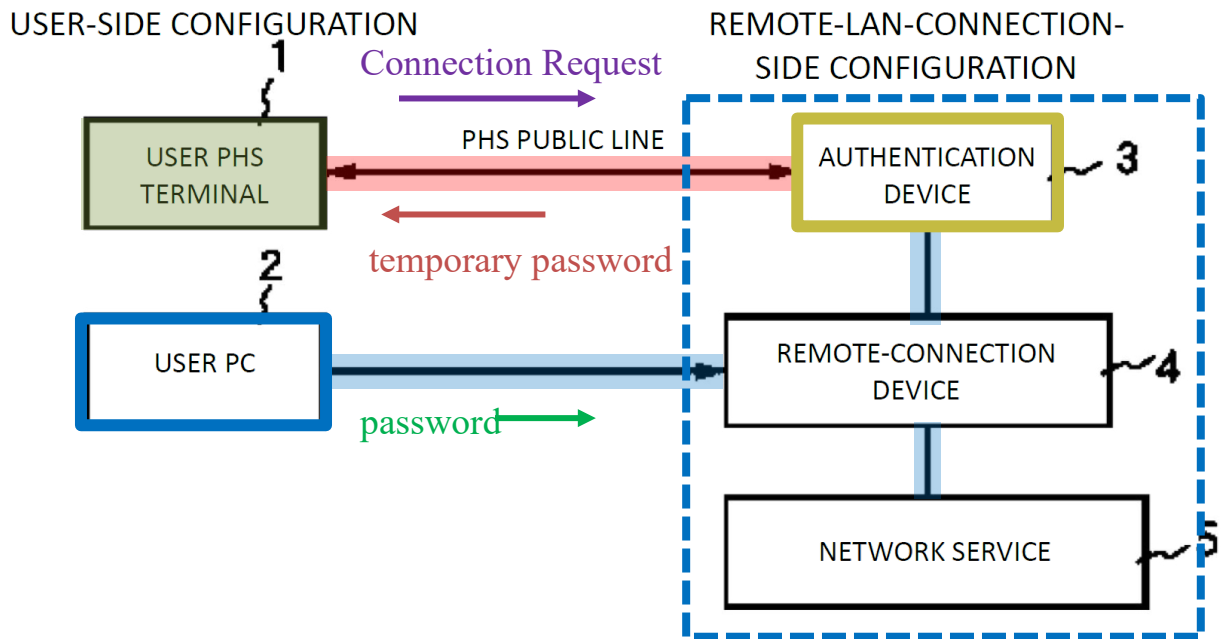
Guthrie discloses a system of only two devices (client and server) but using three different pieces of authentication information (a challenge-response

process)—a password set by the user, a randomly generated challenge, and an expected response generated by performing a hashing algorithm on the password and challenge. Implementing Guthrie’s challenge-response method within the three-device architecture of Kato would improve Kato’s security by having multiple codes in addition to multiple devices. *Id.*, 140.

2. Kato Is Analogous Art and Combinable with Guthrie

Like the ’658 Patent, Kato discloses authenticating a user to gain access to a networked computer system based on a temporary password. Kato, [0002], [0004], [0008]-[0009]. An authentication device authenticates the user by receiving a password from the user via a secure computer network and comparing the submitted password with a temporary password issued to the user. *Id.*; Reiher, 141.

FIG. 1



Kato, FIG. 1.

To obtain the temporary password, the user sends a connection request by making a phone call to the authentication device from a PHS terminal, such as a mobile telephone. *Id.*, [0008], [0012]-[0014], [0016]. The authentication device identifies the user by comparing the user's PHS number and authentication-device password associated with the phone call request based on such information having been preregistered. *Id.*, [0008], [0016]-[0017]. When these pieces of information match, the authentication device transmits the temporary password to the user PHS terminal via a character message. This temporary password is distinct from the authentication-device password. *Id.* After receiving the temporary password, the

user submits the temporary password to the remote-connection device via the secure computer network to gain access to network. *Id.*, [0019]-[0020]; Reiher, 142.

But Kato authenticates the user to the network computer system with only a single temporary password generated at the server and transmitted to the user—during which it could be exposed or compromised—a method cautioned against in Guthrie. Guthrie, 4:16-28. Thus, a POSITA would have looked to other references that use additional methodologies that prevent exposure of the entire password. Reiher, 143.

Like the '658 Patent and Kato, Guthrie discloses a personal authentication system with a dynamic challenge-response process to enhance security, as explained in Section V.A.2. *Id.*, 144.

Kato and Guthrie are in the same field of user authentication and address the same problem of regulating a user's access to a secure system as the '658 Patent. Ex. 1001, Abstract, 1:28-59, 2:49-67; Kato, [0002], [0009]; Guthrie, Abstract, 1:7-9, 3:53-55. Kato and Guthrie both disclose user authentication systems using similar methods and devices with independent advantages. Both references address problems of conventional authentication systems based on either a fixed password, which can be stolen or guessed, or one-time password authentication using a one-time password generation card, which is expensive and can be lost. Kato, [0003]-

[0004]; Guthrie, 1:20-28, 1:49-63; Ex. 1001, Abstract, 1:28-59; Reiher, 145.

Both references disclose solutions to these problems by implementing two-level authentication—a first level based on a password known to the user and a second level based on a temporary password generated unknown to the user. And like the '658 Patent, both references disclose a computer terminal for receiving a password from the user and a server or device that generates the temporary password and compares the password from the user to the temporary password to authenticate the user. Kato, [0019]-[0020]; Guthrie, 4:14-28, 6:65-7:9. For these reasons, Kato and Guthrie are analogous art to the '658 Patent, and a POSITA would have found it obvious to combine them. Reiher, 146.

3. A POSITA Would Be Motivated to Add Guthrie's Challenge-Response Process to Kato's Three-Device Architecture and Would Have Had a Reasonable Expectation of Success

a. Motivation

A POSITA would have found it obvious to add Guthrie's challenge-response process to Kato's three-device architecture, in place of Kato's singular temporary password, to further improve security by: (1) preserving Kato's architecture, which adds security by transmitting a token to a different, known device of the user than the device that will access the secured system (Ueshima, 4:1-12, 16:61-67 (it is advantageous and especially convenient to use a portable telephone, such as a

cellular phone or a PHS that has already been widespread, for user authentication)), while (2) benefitting from Guthrie's challenge-response process that uses three separate codes such that exposing one or two of the codes during transmission would still prevent unauthorized access—an improvement over Kato's single temporary password. Reiher, 147.

A POSITA would have been motivated to incorporate Guthrie's challenge-response process into Kato to enhance Kato's security by preventing the user's secret password from being exposed during transmission. Guthrie teaches that its system “can be practiced ... with other specific steps in a routine, different security algorithms, different hardware, etc.,” and “may be combined with a system's conventional authentication procedures to provide at least two levels of security, in addition to other security features.” Guthrie, 3:59-4:3. Guthrie generates its expected response using “a secured, one-way hashing algorithm which is difficult, if not impossible to reverse compute,” by combining a serial number, a user password (known to the user), and a challenge (randomly generated, unknown to the user). *Id.*, 4:39-41, 6:14-21, 6:57-64. Incorporating Guthrie's challenge-response process into Kato would generate a challenge and an expected response calculated from the user password and challenge, using a hashing algorithm to add an additional level of security. *Id.* An unauthorized user eavesdropping on the transmission of either the

challenge (transmitted to the user's communication device) or the response (transmitted to the authentication device) would not be able to extract the user's secret password. One-way hashing algorithms were well known and commonly used for securely transmitting authentication data. Peters, Abstract, 2:19-35, FIG. 1 (generating a password by hashing a user's password and a unique string); Reeds, Abstract, 5:17-22, 9:1-9 (authenticating a user based on an output of a hash function that hashes a concatenation of a secret password and random number and other information); Kaufman, Abstract, 4:39-62 (using a hashing algorithm upon a password and token). Reiher, 148.

A POSITA would have been motivated to incorporate Guthrie's challenge-response process into Kato, in place of Kato's temporary password, to further enhance Kato's security by only transmitting the challenge and not the user's secret password, preventing exposure of the password, and by requiring the user's secret password in addition to the challenge to obtain the response. Kato merely requires the user to submit the user ID and the temporary password to the authentication device. Kato, [0019]-[0020]. A user ID is typically not secret and can be known to an unauthorized user. Guthrie, 1:25-28; Kato, [0003]; Kaufman, 2:8-12. An unauthorized user could obtain Kato's mobile telephone and the temporary password. Odagiri, [0004], [0038] (teaching an unauthorized person may obtain a

portable telephone, such as a PHS). Or an eavesdropper could observe the temporary password and use it to falsely authenticate himself. The combination requires the user to use both the challenge (transmitted to the mobile telephone) and a secret password (not transmitted) to generate the response. This ensures an unauthorized user who obtains possession of the mobile device and challenge cannot use it to access Kato's secured system so long as the unauthorized user does not know the user's secret password. Nor could an eavesdropper use the overheard temporary password, because they would not have access to all information required to create the correct response to the challenge. Bosen, 2:26-31, 4:44-49 (improving security by making the generation of authentic passwords dependent on possession of a random challenge and confidential information); Falk, 4:32-45, 5:4-7; Reiher, 149.

b. Reasonable Expectation of Success

A POSITA would have had a reasonable expectation of success in implementing Guthrie's challenge-response process in Kato's architecture because (1) Guthrie's response calculators can be implemented on various platforms, and (2) Kato's system is well-equipped to incorporate the challenge-response process. Reiher, 150-156.

First, Guthrie's response calculators can be implemented as software on various software and hardware platforms, including a "palm top computer" (akin to

Kato's PHS terminal). Guthrie, Abstract, 3:59-65, 4:8-13, 5:18-22, 5:48-6:9, 12:43-53, 13:16-20. Guthrie's response calculators are "not compute intensive" and "the central processing unit (CPU) and input/output (I/O) processing requirements for the calculators are minimal ... so that authentication can be calculated in substantially less than one second." *Id.*, 2:57-67. Guthrie teaches that its system "can be practiced ... with other specific steps in a routine, different security algorithms, different hardware, etc.," and "may be combined with a system's conventional authentication procedures to provide at least two levels of security, in addition to other security features." *Id.*, 3:59-4:3; Reiher, 151.

A POSITA would have understood that Kato's user PC would be modified using ordinary skill to implement Guthrie's client SADB calculator. Kato discloses a user PC that obtains authentication data, such as user ID and temporary password, for transmitting to an authentication device to gain access. Kato, [0020]. Like Kato's PC, Guthrie's client is a computer that receives the authentication data for transmitting to the server to gain access. Guthrie, 4:14-28, 7:49-8:6, 11:26-8:42, FIGS. 8A-8C, 9A. Guthrie further discloses how to enter the authentication data at the client via a user interface. Guthrie, 12:61-13:10, FIG. 9A. A POSITA would have understood that Kato's PC and Guthrie's client computer are both computers with processor and memory devices performing similar functions. A POSITA would have

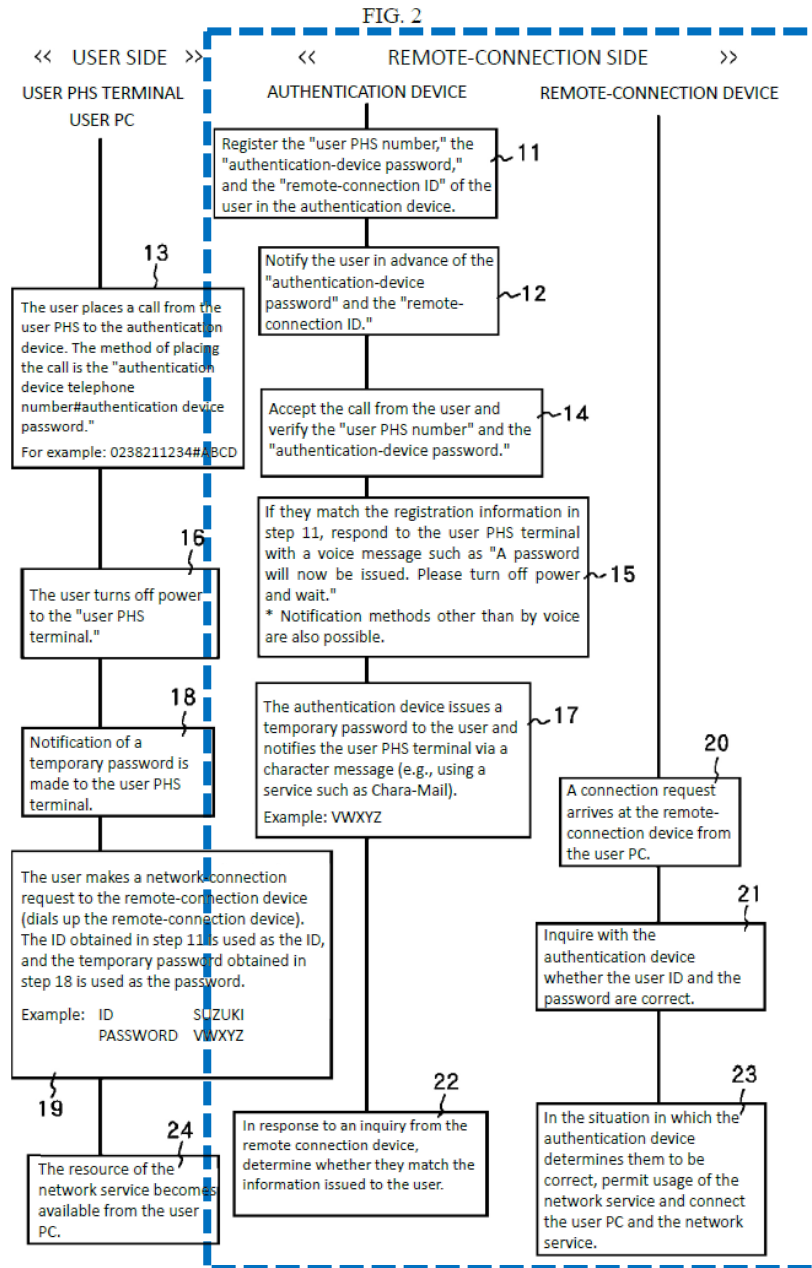
recognized that Guthrie's client SADB calculator would have been implemented on Kato's PC as software executed by the processor using ordinary skill and yielded predictable results of expected responses. Reiher, 152.

Alternatively, a POSITA would have understood that Kato's PHS would be modified using ordinary skill to implement Guthrie's client SADB calculator. A POSITA would have understood that Kato's PHS terminal is a mobile device like a personal digital assistant ("PDA") and personal mobile computer (a "palm top computer") that include processor and memory devices for executing software operations. Odagiri, [0038], [0046]-[0047] (teaching the hardware of a PHS or mobile personal computer includes a CPU and memory); Ueshima, 4:1-4, 9:14-22 (teaching using a PHS or a PDA with a telephone function as a mobile terminal for user authentication); Oberhaus, 1:21-23 ("Examples of hand-held computing devices include pagers, mobile phones, personal digital assistants (PDAs), [and] palm-top computers"); Guthrie, 6:1-3. A POSITA would have recognized that Guthrie's client SADB calculator would be implemented on Kato's PHS terminal as software executed by the processor using ordinary skill to yield predictable results of the expected responses. It was known that devices like Kato's PHS terminal can perform encryption algorithms. Shields, p. 11 (using a PDA for generating an encrypted response by applying a hashing algorithm to a sequence of values); Falk,

3:4-20, 4:19-45 (using a cellular phone for calculating a response in a challenge-response process); Turtiainen, 10:22-36 (a mobile station calculates a response to a challenge according to a predefined algorithm using the challenge and a secret password); Reiher, 153.

A POSITA would have understood that modifying Kato's authentication and remote-connection devices to implement Guthrie's challenge-response process, including the server SADB calculator, dial-in application, and database, would have required only ordinary skill. A POSITA would have understood that these devices would include a processor, memory, and communication devices for performing functions like those of Guthrie's server calculator. Kato's authentication and remote-connection device collectively perform various functions for user authentication based on stored user information—preregistering the user's authentication information (telephone number, password, ID) (Kato, [0008]); identifying the user based on the user's authentication-device password and remote-connection ID, managing a user password request, and issuing a temporary password to the user's PHS terminal in response to the request (*id.*, [0013]); and comparing the user's submitted password to the temporary password issued to the user, and permitting access to the network service (*id.*, [0020]). Likewise, Guthrie's server includes storing the user's authentication information (e.g., account ID, password, challenge,

and response in a user account database 120 (Guthrie, 5:35-47, FIGS. 5-6)), identifying the user based on the user account ID (*id.*, 7:64-8:6, FIG. 7A), receiving a request challenge from the client (*id.*, 7:60-63, FIG. 7A), generating a challenge and calculating an expected response to the request (*id.*, 10:39-50, FIG. 7D), comparing the response received from the user to the expected response (*id.*, 11:60-64, FIG. 8B), and permitting access to the server (*id.*, 12:37-42, FIG. 8C). A POSITA would have recognized that Kato's authentication device and remote-connection device would be modified to perform the similar functions of Guthrie's server calculator. Reiher, 154.



Kato, FIG. 2.

It was well known that authentication devices, like Kato's authentication device, that would communicate with both a mobile phone and a personal computer to control access to network service, can be a computer or a server, similar to

Guthrie’s server computer. Ratayczak, 3:63-67 (it is “well known” that “access device A ... may also be constituted by a computer or a server”); Kaufman, 8:23-45 (an authentication server can be a computer programmed to function as a conventional authentication server and include a token generating routine). A POSITA would have understood that Guthrie’s server calculator, dial-in application, and database would be implemented on Kato’s authentication device as software executed by the processor using ordinary skill, as taught by Guthrie, to yield predictable results. Reiher, 155.

A POSITA would have recognized that the implementation details of a challenge-response process taught by Guthrie would apply to Kato’s three-device architecture as software implemented on similar devices using conventional components and known techniques because challenge-response process were well known and commonly implemented in various user authentication applications and systems. Peters; Reeds; Bosen; Kaufman; Falk, 3:4-20, 4:19-45; Reiher, 156.

B. Independent Claims

1. Claim 1

a. 1[preamble]

Kato discloses 1[preamble]. Reiher, 158-162.

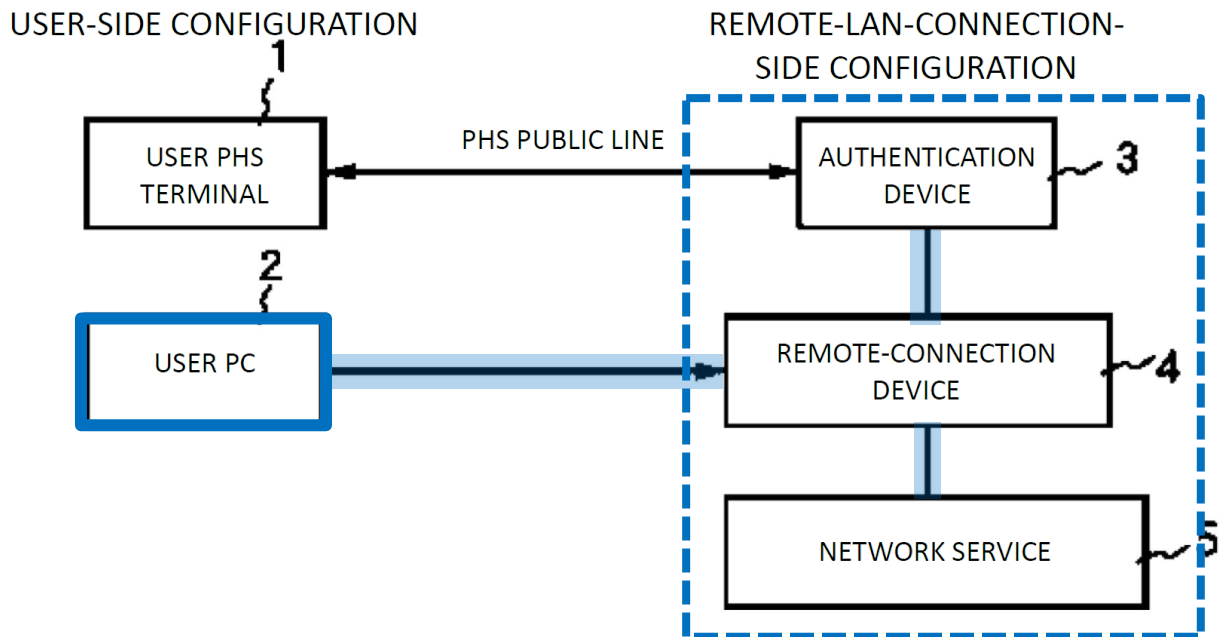
As explained for Ground 1, the ’658 Patent provides no definition of a secure computer network, but the specification explains that a secure computer network is

simply a “secure system” accessible over a network. Ex. 1001, Abstract, 4:20-26; § V.B.1.a. Kato similarly discloses a secure computer system accessible over a network. Kato, [0002], [0008]. Kato discloses a “*first secure computer network*” because Kato requires authentication to access parts of the networked computer system. *Id.*; Reiher, 159.

Kato discloses “[*a*] method of authenticating a user” because it discloses “an authentication system ... , which, after verifying the validity of a user, permits usage of a resource of a network service from the user personal computer.” Kato, [0002], [0008]; Reiher, 160.

Kato discloses “*authenticating a user on a first secure computer network*” because Kato discloses that the authentication system includes a remote-connection device and an authentication device that regulate a user’s access to a network resource by confirming authentication data, such as the password and the remote-connection ID, received from a personal computer. Kato, [0008]-[0009]. Kato discloses that the *remote-connection device, the authentication device, and the network are connected by LAN connection*. *Id.*, [0002], [0012]; Reiher, 161.

FIG. 1



Kato, FIG. 1.

Kato discloses “the user having a user account on said first secure computer network” because it discloses the authentication device preregisters “a telephone number, a password, and a remote-connection ID of the simplified, mobile-telephone terminal.” Kato, [0002], [0008]; Reiher, 162.

b. 1[a]

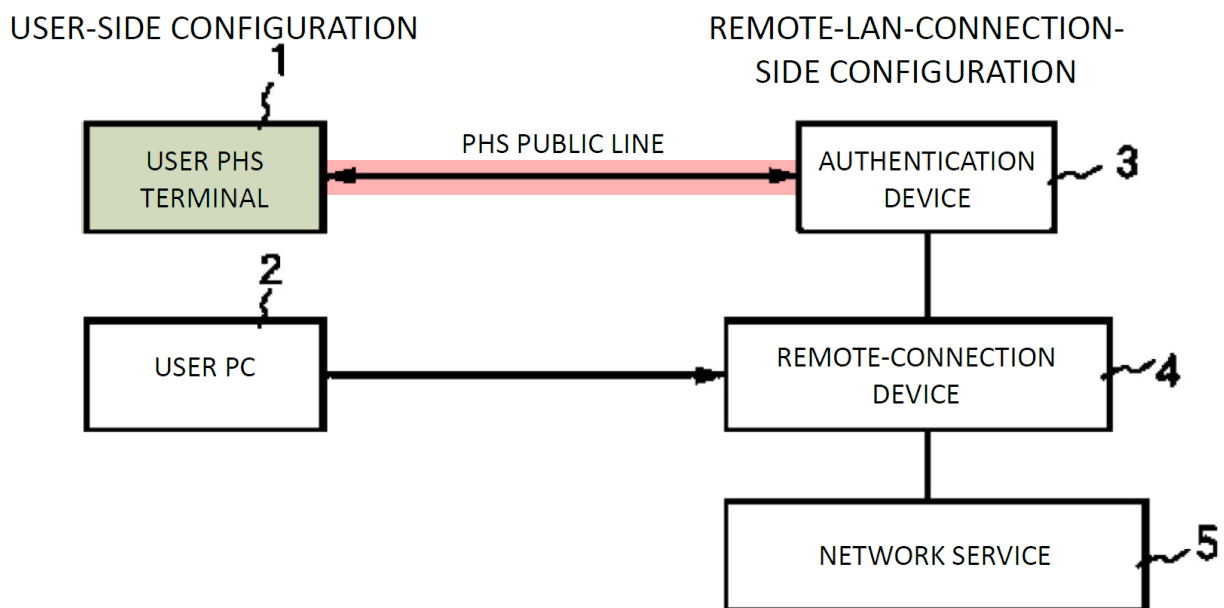
Kato discloses 1[a]. Reiher, 163-165.

Kato discloses “associating the user with a *personal communication device possessed by the user*” because it discloses “preregister[ing] a telephone number, a

password, and a remote-connection ID of the simplified, **mobile-telephone terminal**.” Kato, [0008]-[0009]; Reiher, 164.

Kato discloses “*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*” because Kato discloses using a PHS terminal, such as a mobile telephone, in “**an international telephone utilization system**.” Kato, [0002], [0008], [0014]. A POSITA would have understood that Kato’s mobile telephone is in communication with a cellular network (“**second network**”) different from the secure computer system (“*first secure computer network*”); Reiher, 165.

FIG. 1



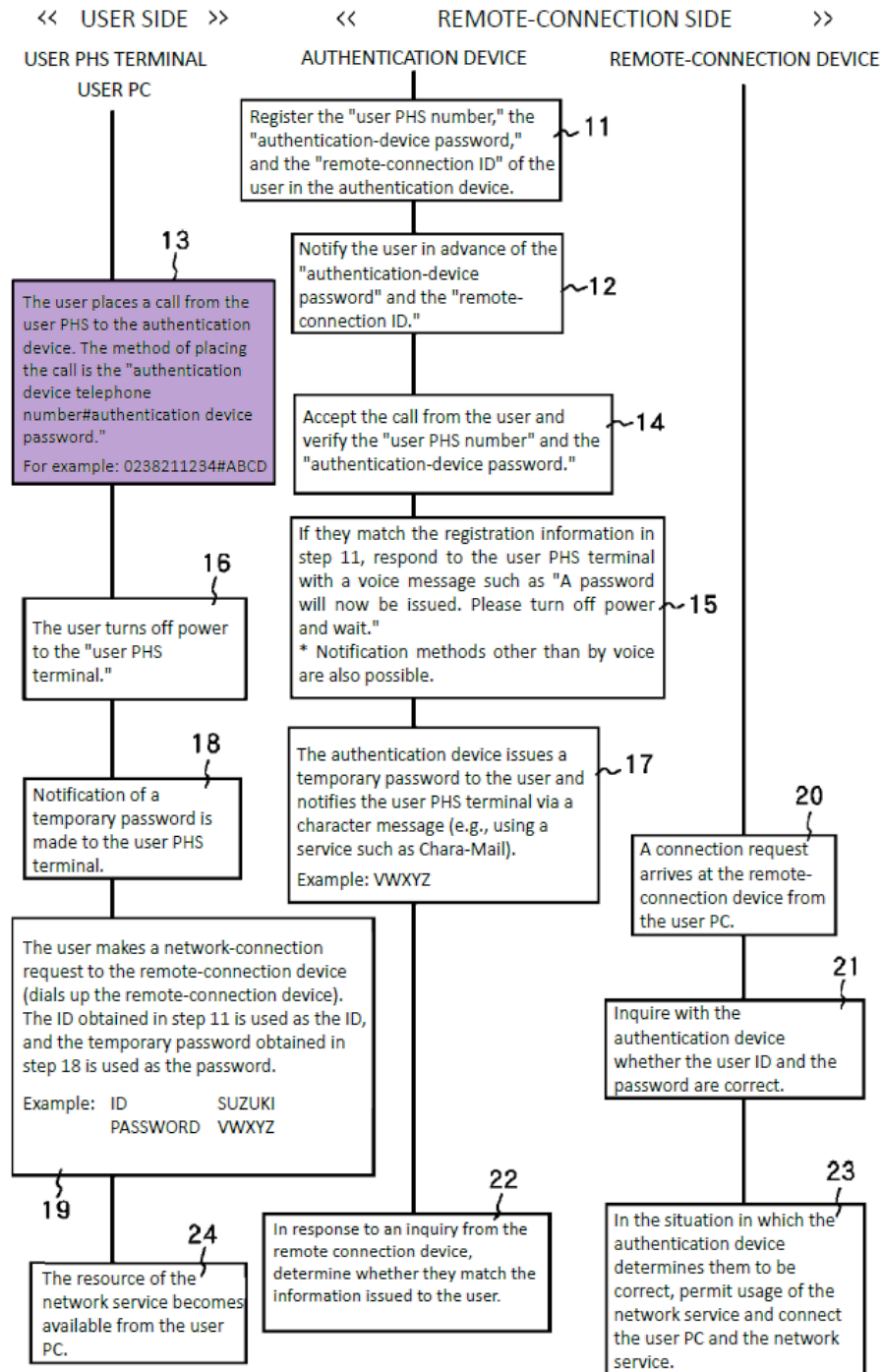
Kato, FIG. 1.

c. 1[b]

Kato in view of Guthrie renders obvious 1[b]. Reiher, 166-170. Kato discloses sending a request from a user at a personal communication device over a second network. Guthrie discloses a request for a token. It would have been obvious to a POSITA to request a token, as disclosed by Guthrie, within the architecture of Kato. *Id.*, 167.

Kato discloses at step 13 that the authentication device receives a request from the user for a temporary password via a call (“*over the second network*”) from the PHS terminal (“*personal communication device*”). Kato, [0016]-[0017]; Reiher, 168.

FIG. 2



Kato, FIG. 2.

Kato does not expressly disclose that its request for a temporary password is “a request from the user for *a token*.” As explained in Ground 1 (Section V.B.1.c), Guthrie discloses requesting a token similar to Kato’s request for a temporary password, and it would have been obvious to a POSITA to request a token (as disclosed by Guthrie) with Kato’s means for requesting a temporary password. Reiher, 169.

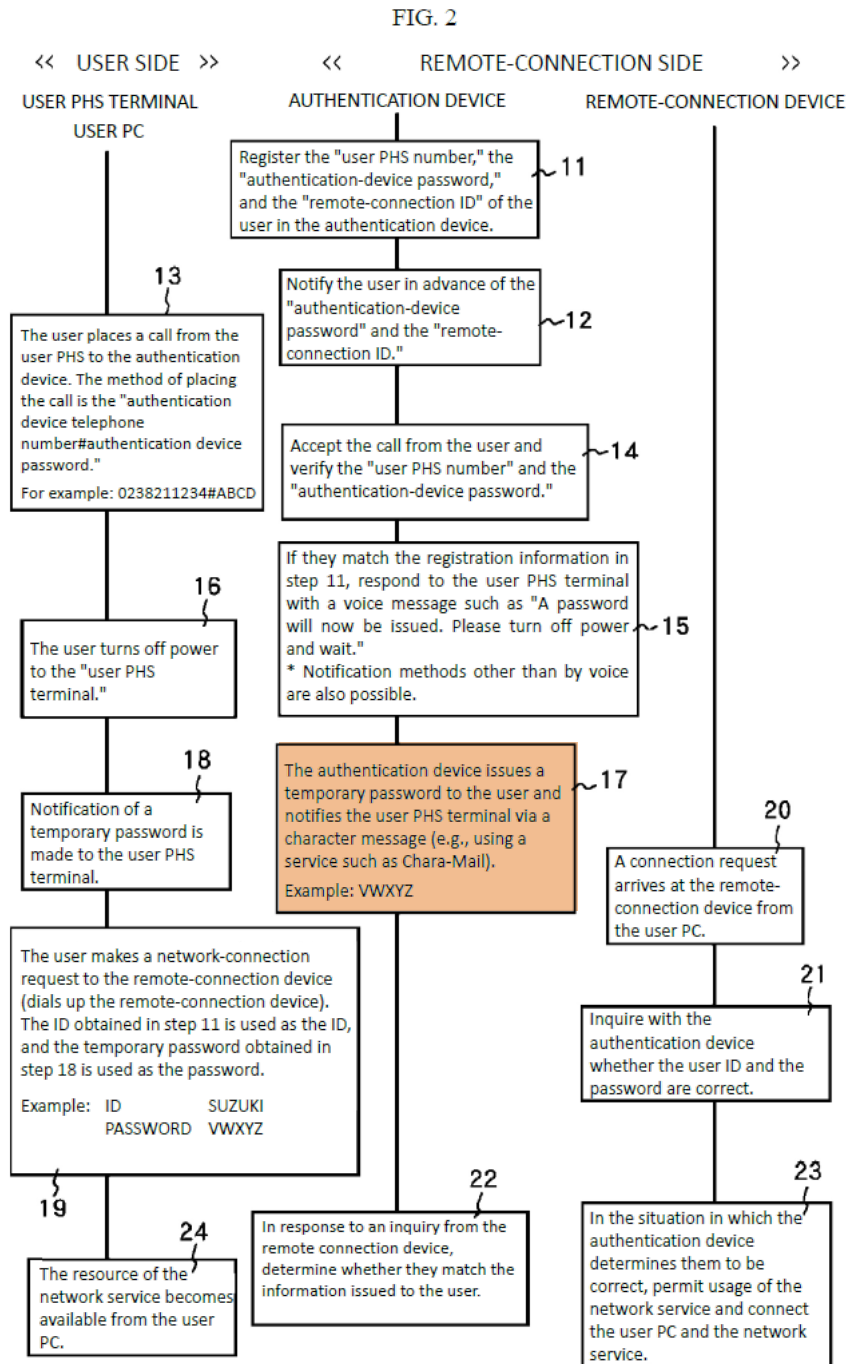
A POSITA would have been motivated to incorporate Guthrie’s challenge into Kato in place of Kato’s request for a temporary password sent from the PHS terminal and would have had an expectation of success for this modification, as explained in Section VI.A. *Id.*, 170.

d. 1[c]

Kato in view of Guthrie renders obvious 1[c]. *Id.*, 171-176. Kato discloses generating a temporary password for accessing the first secure computer network but does not disclose that the temporary password is based upon the token and a passcode. Guthrie discloses generating an expected response based on the challenge (“*token*”) and password (“*passcode*”). As combined by replacing Kato’s temporary password with Guthrie’s expected response, this limitation is obvious. *Id.*, 172.

Kato at step 17 discloses that its authentication device generates a temporary password for the user to access the secure computer network. Kato, [0018]. Kato

discloses that at step 22, its authentication device receives and confirms the user-submitted password to grant the user access to the network. *Id.*, [0002], [0020]-[0022]; Reiher, 173.



Kato, FIG. 2.

While Kato discloses generating a temporary password (“*a new password*”), Kato’s temporary password is not expressly “*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.*” When combined with Guthrie’s process for generating an expected response value based on a challenge and password, however, generating a new password based upon an unknown token and known passcode is obvious. Reiher, 174.

Guthrie discloses generating an expected response value (“*new password*”) based on the challenge (“*token*,” unknown to the user) and an SADB password (“*passcode*,” known to the user), as explained for Ground 1 (Section V.B.1.d). Reiher, 175.

A POSITA would have understood that Guthrie’s expected response generation, based on the known passcode and unknown token, would be incorporated into Kato, replacing generation of Kato’s temporary password. A POSITA would have been motivated to replace Kato’s temporary password with Guthrie’s unique response to prevent eavesdroppers and portable device thieves from using the temporary password to falsely authenticate themselves and would have had an expectation of success for this modification because it is an addition of

a known solution to a known problem within a reference ripe for improvement.

§ VI.A; Reiher, 176.

e. 1[d]

Kato in view of Guthrie renders obvious 1[d]. Reiher, 177-180. Kato discloses setting a temporary password associated with the user as the password required to authenticate access to the secure computer system. Guthrie discloses the “*new password*,” as explained in the previous Section. It would have been obvious to set Guthrie’s new password as the password associated with the user in place of Kato’s temporary password. *Id.*, 178.

As explained for 1[c] (Section VI.B.1.d), Kato’s authentication device issues a temporary password and compares a user-submitted password to the temporary password. Kato, [0018]-[0020]. Kato also discloses the temporary password is a one-time password generated in response to the user’s request. *Id.*, Abstract, [0013]. Kato’s temporary password, however, is not the claimed “*new password*,” but it would have been obvious to replace Kato’s temporary password with Guthrie’s expected **response** (“*new password*”), as also explained for 1[c]. Guthrie further discloses setting its expected response as the password associated with the user, as explained for Ground 1 (Section V.B.1.e). Guthrie, 10:55-58; Reiher, 179.

A POSITA would have been motivated to incorporate Guthrie's challenge-response, including its "*new password*," in place of Kato's temporary password as explained in Section VI.A. Reiher, 180.

f. 1[e]

Kato in view of Guthrie renders obvious 1[e] for two reasons: (1) Kato at least suggests that access to the user account is activated when the temporary password is issued, and when Kato's temporary password is replaced with Guthrie's expected response, this limitation is obvious; and (2) Guthrie expressly discloses activating access to a user account after generating the expected response by setting a timer during which the expected response will grant access, and when this process is combined with Kato's architecture, this limitation is obvious. *Id.*, 181-184.

First, Kato discloses generating a one-time or temporary password, as explained for 1[c]. § VI.B.1.d. Kato, Abstract. A POSITA would have understood that once Kato generates the temporary password, the authentication system allows the user to use the temporary password to gain access to the network, at least suggesting activating the user's ability to access the user account with the temporary password. When Kato's temporary password is replaced with Guthrie's expected response, as explained for 1[c], a POSITA would have understood the combination

to teach activating the user's account by allowing the user to use the response to access the account if the expected response is received. Reiher, 182.

Second, Guthrie discloses this limitation as explained for Ground 1 in Section V.B.1.f. *Id.*, 183.

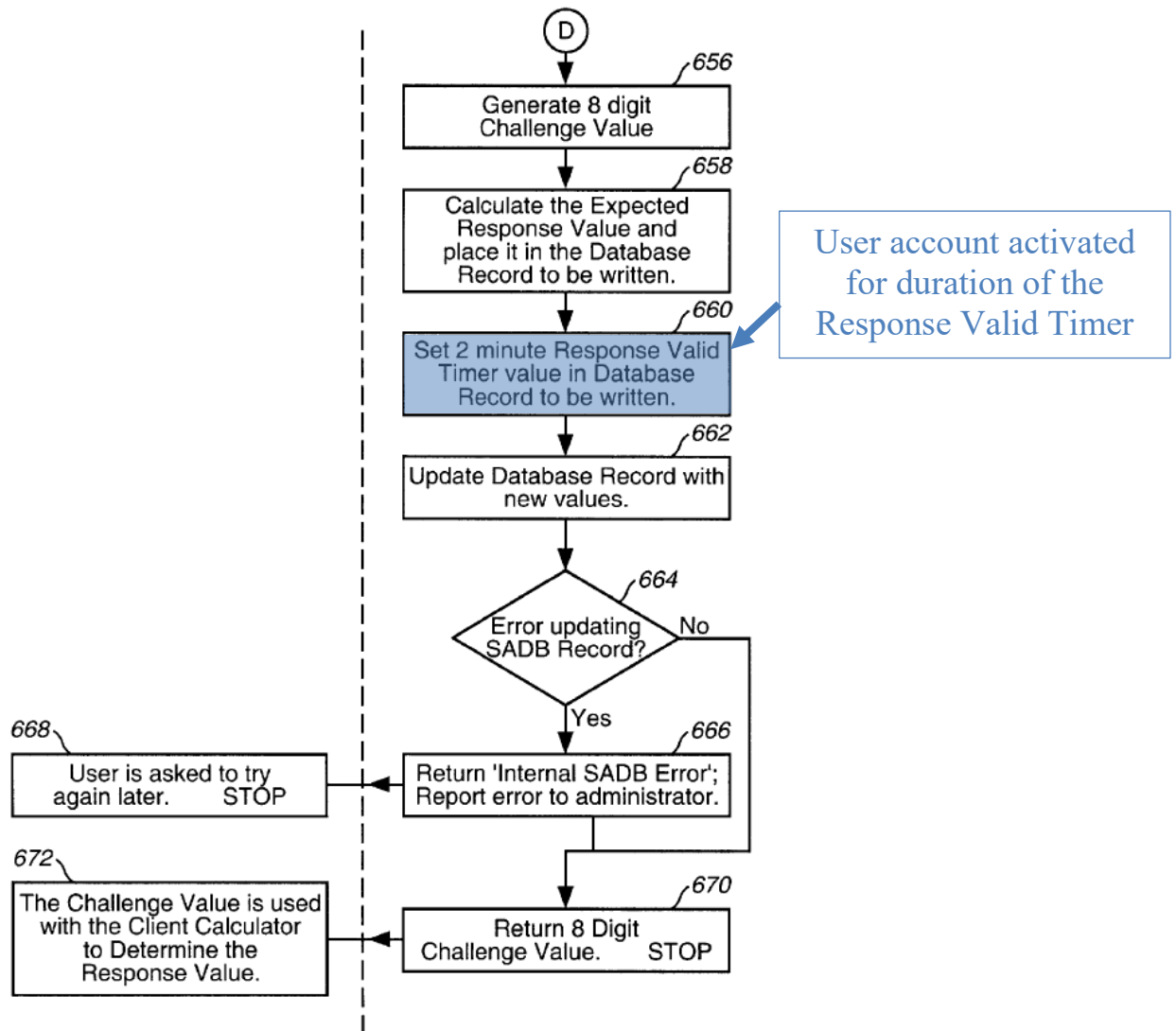


FIG. 7D

Guthrie, FIG. 7D.

A POSITA would have been motivated to incorporate Guthrie's activation using a timer into Kato's architecture to further enhance security of Kato's authentication system by providing a limited period of activation, preventing unauthorized access. Although Kato's temporary password is set each time there is a request for a one-time password, Kato does not disclose whether the temporary password has any time limitation. Kato, [0004], [0014]. Guthrie restricts access based on a response valid timer. Guthrie, 10:50-55, 11:50-64, FIGS. 7D, 8B. A POSITA would have readily understood the benefit of incorporating Guthrie's user account access according to its response valid timer. If the response valid timer has not expired, the user can access the secured system. *Id.* Incorporating Guthrie's valid timer into Kato would further increase security by allowing access only when the user has immediate access to the PHS terminal. Setting a time limitation for activating access to a user account was well known and conventional to increase security in authentication. Veneklase, 7:8-41; Aziz, 6:61-7:15; Schmitz, 8:53-59; Kew, 8:25-9:3. And a POSITA would have had a reasonable expectation of success in incorporating Guthrie's timer into Kato's architecture because it was a software modification to limit the period of accessibility when the new password is operable to grant access to the user account, requiring only routine skill to achieve expected results. Reiher, 184

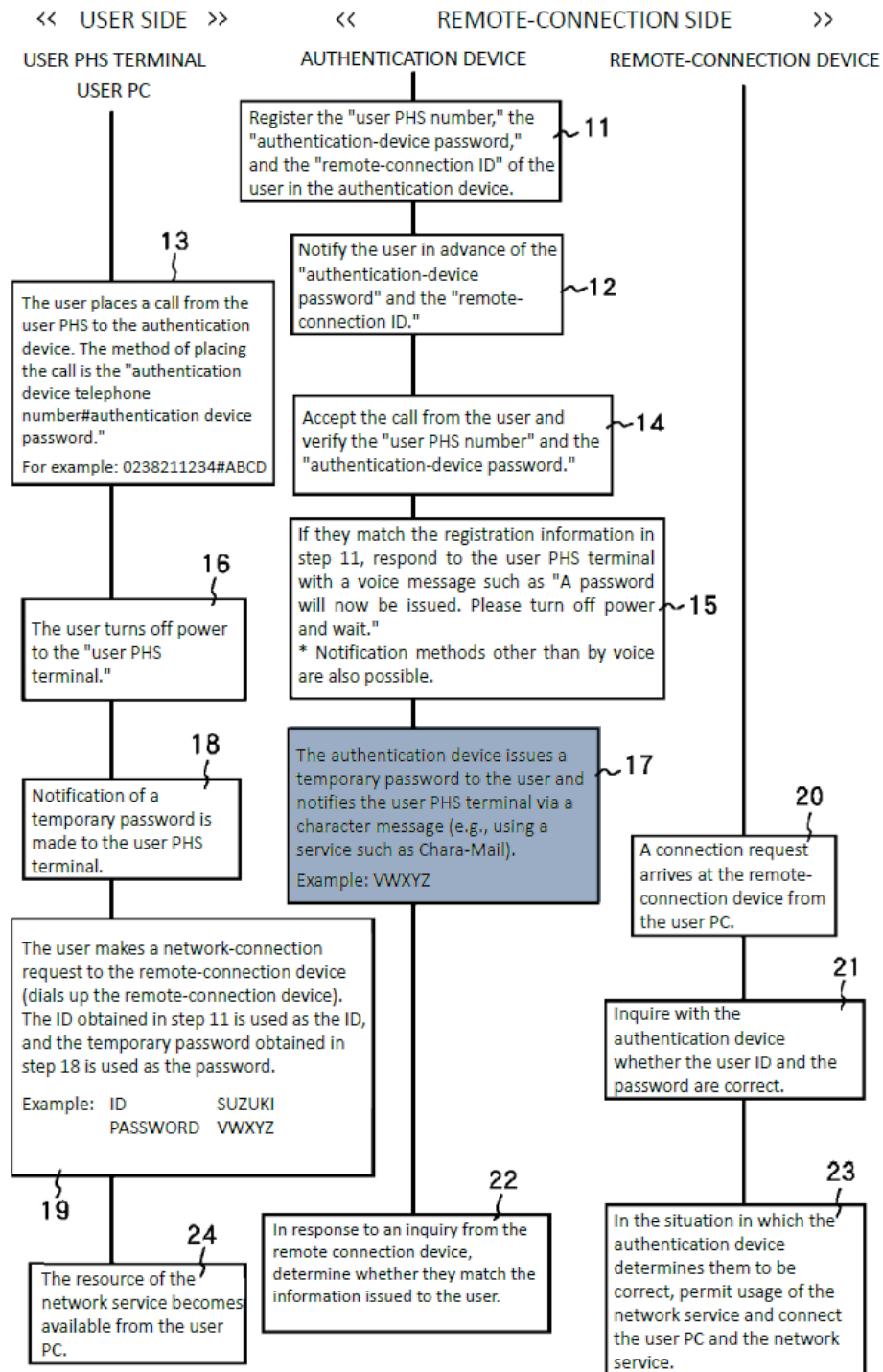
g. 1[f]

Kato in view of Guthrie renders obvious 1[f]. *Id.*, 185-189.

Kato discloses transmitting a temporary password to the user's personal communication device. As Kato combined with Guthrie replaces Kato's transmitted temporary password with Guthrie's challenge, the combination renders obvious transmitting the challenge ("*token*") to the user's personal communication device. *Id.*, 186.

In step 17, Kato discloses that its authentication device issues the temporary password to the user PHS terminal and notifies the user PHS terminal via a character message. Kato, [0018]; Reiher, 187.

FIG. 2



Kato, FIG. 2.

In combination with Guthrie, rather than transmitting Kato's temporary password to the user's communication device, Kato's authentication device would instead transmit a challenge as disclosed by Guthrie and explained for Ground 1. § V.B.1.g; Reiher, 188.

A POSITA would have incorporated Guthrie's challenge-response process into Kato such that Kato's authentication device transmits Guthrie's challenge ("*token*") to the user PHS terminal ("*personal communication device*") as explained in Section VI.A. Reiher, 189.

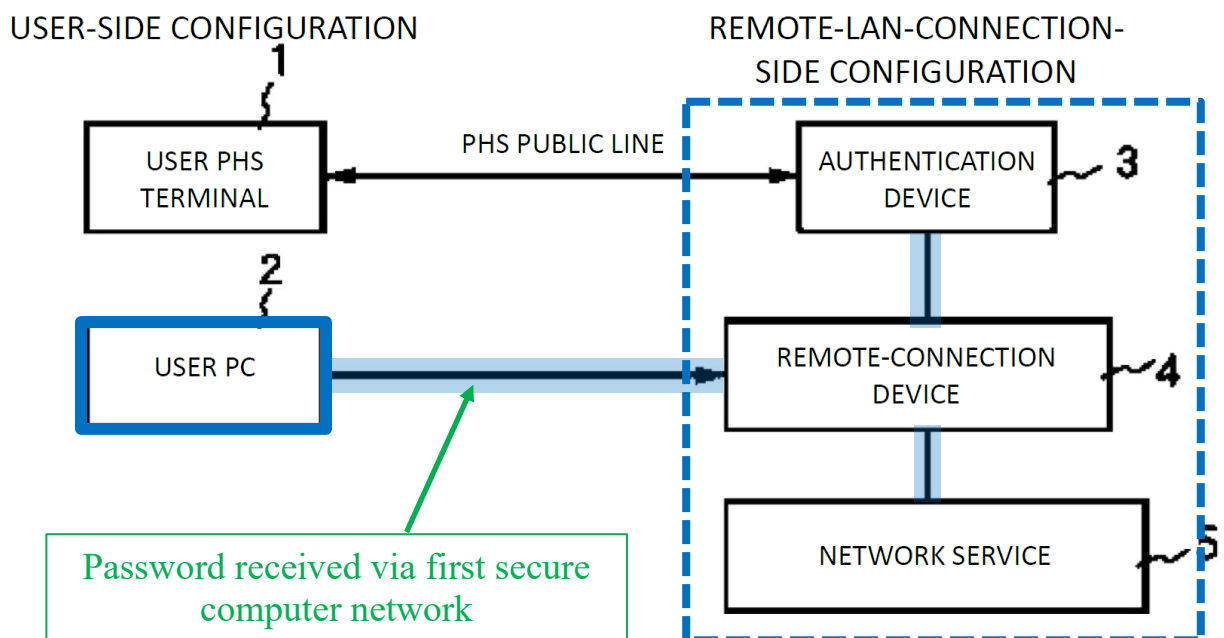
h. 1[g]

Kato in view of Guthrie renders obvious 1[g]. *Id.*, 190-197.

Kato discloses the architecture of having three separate devices—a user PC for accessing a secure computer system, a user communication device for receiving a temporary password, and a secure computer network, as explained for 1[preamble] and 1[a]. §§ VI.B.1.a-VI.B.1.b. Kato does not disclose generating the password, but Kato in combination with Guthrie renders the password obvious, as explained for 1[c]-1[d]. §§ VI.B.1.d-VI.B.1.e. As combined, a POSITA would have understood that Guthrie's password would be entered by the user to be received via Kato's first secure computer network. Reiher, 191.

Kato discloses that the “user PC 2, which is the computer system for user connection, connects to the remote-connection device 4” “[b]ased on a ‘temporary password’ ... notifi[ed] to the user PHS terminal 1” from the authentication device. Kato, [0015]. User PC 2 uses the temporary password received on the PHS terminal 1 to request access to the first secure computer network by sending a connection request including a user-submitted password. *Id.*, [0018]-[0020]. The authentication device determines whether the information, including the user-submitted password, provided in the authentication request matches the information issued to the user, and, if it matches, grants the user access to the secure computer network. *Id.*, [0020]-[0021]; Reiher, 192.

FIG. 1

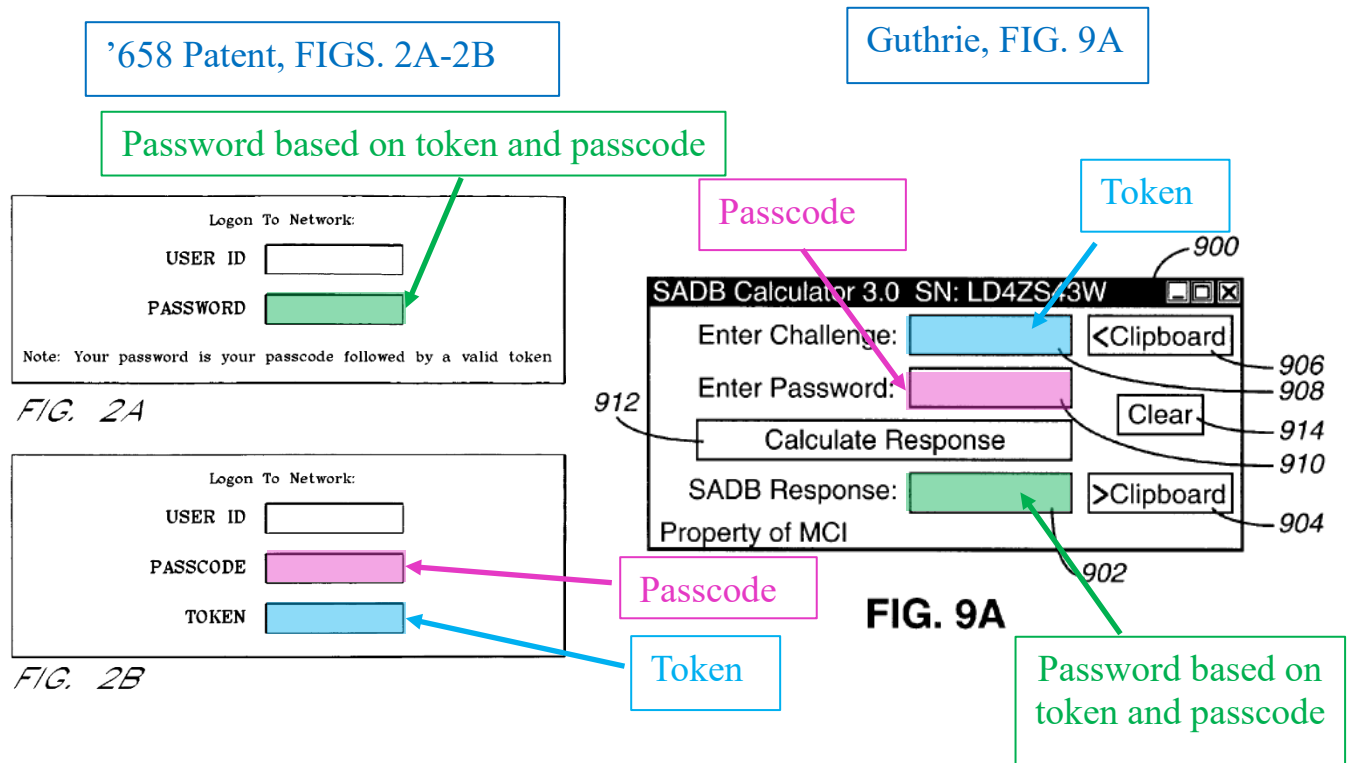


Kato, FIG. 1.

As explained for 1[c]-1[d], however, Kato does not disclose the claimed password, but Guthrie does, as explained in Ground 1. § V.B.1.h. As combined, the challenge-response process of Guthrie would be used within the architecture of Kato depicted above, replacing Kato's temporary password with Guthrie's response ("*the password*"). Reiher, 193.

A POSITA would have been motivated to implement Guthrie's challenge-response process within Kato's two-client-device architecture (comprising PHS terminal and PC 2) in one of two ways, either of which renders this limitation obvious. *First*, Guthrie's challenge-response could be implemented within Kato such that a user receives Guthrie's challenge (similar to receiving Kato's temporary password) on Kato's PHS terminal and manually enters the challenge into Kato's PC 2 (in place of Kato's temporary password entry) to generate the **response** for the user to manually enter the generated response for transmission to Kato's server (as contemplated by Guthrie). Guthrie, 12:61-13:10, FIG. 9A, 12:57-60 ("[T]he user's authentication password must be entered interactively. As a result, human interaction in the authentication process is required."). *Second*, Guthrie's challenge-response could be implemented within Kato such that the PHS terminal receives Guthrie's challenge, performs the response generation algorithm, and provides the **response** to

the user (similar to providing Kato's temporary password to a user) for manual entry into Kato's PC 2 and transmission to Kato's server (in place of Kato's temporary password entry). A POSITA would have understood that Kato's PHS terminal is capable and ready for the modification of performing Guthrie's SHA. This is because (1) mobile phones were known to perform hash algorithms (Falk, 3:4-20, 4:19-45 (using a cellular phone or a pager to calculate a response of a challenge using a hash algorithm)); and (2) Guthrie expressly discloses that its SHA can be performed on a "palm top computer," which a POSITA would have understood to be similar to a mobile device such as Kato's PHS terminal. Guthrie, 6:1-38; Odagiri, [0038], [0046]-[0047]; Ueshima, 4:1-4, 9:14-22; Oberhaus, 1:21-23. Both methods would have been obvious to a POSITA looking to add additional security to Kato's system and would have required only routine skill to implement. Guthrie, 12:61-13:10, FIG. 9A; Falk, 3:4-20, 4:19-45; Turtiainen, 10:22-36. Both methods are similar to the examples disclosed in the '658 Patent. Ex. 1001, 4:52-61, FIGS. 2A-2B; Reiher, 194-196.



A POSITA would have been motivated to incorporate Guthrie's challenge-response process, including the server's receipt of the response ("*password*"), into Kato's architecture and would have had an expectation of success for this modification as explained in Section VI.A. Reiher, 197.

i. 1[h]

Kato in view of Guthrie renders obvious 1[h]. *Id.*, 198-200. As explained for Ground 1, Guthrie discloses deactivating access after two minutes of activating if the expected response is not received at the server. § V.B.1.i; Guthrie, 10:50-55; Reiher, 198.

A POSITA would have been motivated to incorporate Guthrie's deactivation

using a timer into Kato's architecture to further enhance security of Kato's authentication system by providing a limited period of activation, preventing unauthorized access for reasons discussed in Section VI.A. Although Kato's temporary password is set each time there is a request for a one-time password, Kato does not disclose whether the temporary password has any time limitation. Kato, [0004], [0014]. But Guthrie restricts access based on a response valid timer, as explained for Ground 1. § V.B.1.i. Incorporating Guthrie's response valid timer into Kato would further increase security by ensuring the user has immediate access to the PHS terminal to access the secure system. Reiher, 199-200.

2. Claim 5

Kato in combination with Guthrie renders claim 5 obvious for the same reasons explained for claim 1, aside from its hardware components and software modules, which are separately addressed below. Reiher, 201-211. To the extent any terms in claim 5 or its dependent claims are determined to be means-plus-function, Petitioner has met its burden under 37 C.F.R. § 42.104(b)(3), as explained for Ground 1 in Section V.B.2.a.

a. 5[preamble]

Kato discloses 5[preamble] because it discloses “an authentication system and an authentication device that permit[] the provision of a local area network (LAN) service only to proper users.” Kato, [0001]; Reiher, 202.

b. 5[a]

Kato at least suggests 5[a] because it discloses an authentication device that performs computing functions a POSITA would have understood require a computer processor. For example, Kato's authentication device 3 performs the processing steps of:

preregister[ing] a telephone number, a password, and a remote-connection ID of the simplified, mobile-telephone terminal; notif[ying] the user of the password and the remote-connection ID; receiv[ing] the telephone number and the password from the user simplified, mobile-telephone terminal; compar[ing] such with the preregistered telephone number and password; and, when they match, issu[ing] a temporary password to the user simplified, mobile-telephone terminal

Kato, [0008]. A POSITA would have understood these steps including receiving, storing, comparing, and generating data to be routine functions of a computer processor. Ratayczak, 3:63-67; Kaufman, 8:23-45; Reiher, 203.

c. 5[b]

Kato alone or in combination with Guthrie renders obvious 5[b]. Kato discloses “*associat[ing] 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,*” as explained for 1[a].

§ VI.B.1.b. A POSITA would have understood that to associate a user with a personal communication device by “preregister[ing] a telephone number, a password, and a remote-connection ID of the simplified, mobile-telephone terminal” (Kato, [0008]-[0009]), the information would have been stored in a database. Reiher, 204.

To the extent Kato does not expressly disclose a “*user database*,” the combination similarly teaches a “*user database*” associating the user with the personal communication device because Guthrie discloses storing account information in a user account database 120, as explained for Ground 1. § V.B.2.d; Guthrie, 5:35-47, 7:64-8:6; Reiher, 205.

A POSITA would have found it obvious to use a user database like that expressly taught by Guthrie to store the user registration information of Kato to organize the user’s data for later use in the authentication process. A POSITA would have had a reasonable expectation of success in adding a user database like that taught by Guthrie in Kato’s authentication system because using databases to store and access information was commonly known at the time and required only routine skill to implement. Reiher, 206.

d. 5[c]

Kato in combination with Guthrie renders obvious 5[c] as explained for 1[c] and because Guthrie discloses a “*control module*,” as explained for Ground 1. §§ VI.B.1.d, V.B.2.e; Reiher, 207.

e. 5[d]

Kato in combination with Guthrie renders obvious 5[d] as explained for 1[d] and because Guthrie discloses a “*control module*,” as explained for Ground 1. §§ VI.B.1.e, V.B.2.f; Reiher, 208.

f. 5[e]

Kato in combination with Guthrie renders obvious 5[e] as explained for 1[f] and because Guthrie discloses activating access “*in response to the password*” and a “*communication module*,” as explained for Ground 1. §§ VI.B.1.g, V.B.2.g; Reiher, 209. A POSITA would have been motivated to incorporate Guthrie’s communication module into Kato’s authentication system because Kato discloses transmitting messages to its PHS terminal and a POSITA would have understood using Guthrie’s communication module for such communications would require only ordinary skill to apply a known technique to a known device to achieve the expected result of transmitting the messages. *Id.*

g. 5[f]

Kato in combination with Guthrie renders obvious 5[f]. Kato in view of Guthrie teaches “*receiv[ing] the password from the user through a secure computer network,*” as explained for 1[g]. Kato discloses that “*the user has an account on the secure computer network,*” as explained in 1[preamble]. Kato discloses the “*secure computer network being different from the cell phone network,*” as explained for 1[a]. Guthrie discloses an “*authentication module,*” as explained for Ground 1. §§ VI.B.1.a-VI.B.1.b, VI.B.1.h, V.B.2.h; Reiher, 210.

h. 5[g]

Kato in combination with Guthrie renders obvious 5[g]. Kato in view of Guthrie teaches that Guthrie’s authentication module “*activates access to the account in response to the password,*” for reasons explained in 1[e] 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,*” for reasons explained in 1[h]. §§ VI.B.1.f, VI.B.1.i; Reiher, 211.

C. Dependent Claims

1. Claim 2

Kato in view of Guthrie renders obvious claim 2. Reiher, 212, 49-53; *see* § V.C.1.

2. Claim 3

Kato discloses claim 3 because its personal communication device is a “Personal Handy-phone System (PHS) terminal[,]” which Kato describes as a “commercially available simplified, mobile-telephone terminal” capable of making mobile telephone calls and receiving text data. Kato, [0002], [0025], FIGS. 1-2; Reiher, 213.

3. Claims 6 and 7

Claims 6 and 7 are substantially similar to 1[b] and 1[c], which require receiving a request for a token from the user’s mobile communication device (1[b]) and generating a new password in response (1[c]). Therefore, Kato in view of Guthrie renders obvious claims 6 and 7 for the same reasons it renders obvious 1[b] and 1[c] and because Guthrie discloses the “*communication module*” and “*control module*,” as explained in 5[c] and 5[e]. §§ VI.B.1.c-VI.B.1.d, VI.B.2.d, VI.B.2.f; Reiher, 214.

VII. Institution Under 35 U.S.C. § 314(a) Is Appropriate in View of Petitioners’ *Sotera* Stipulation

Under the Interim Procedure, “the PTAB will not discretionarily deny institution in view of parallel district court litigation where a petitioner presents a stipulation not to pursue in a parallel proceeding the same grounds or any grounds that could have reasonably been raised before the PTAB.” *Memorandum re Interim*

Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation at 3 (June 21, 2022). Petitioners stipulate that if the Board institutes IPR, they will not pursue in the related district court proceeding “any ground [that Petitioner] raised or that could have been reasonably raised” during this proceeding. *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 at 18-19 (PTAB Dec. 1, 2020) (citation omitted) (precedential as to § II.A); 35 U.S.C. § 315(d). Discretionary denial under *Fintiv* is not applicable to this Petition.

VIII. Non-Institution Under 35 U.S.C. § 325(d) Is Inappropriate

Section 325(d) denial would be improper because this Petition presents new prior art and arguments not previously presented to the Office. *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 at 7-9 (PTAB Feb. 13, 2020) (precedential) (“*Advanced Bionics*”); and *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 at 17-18 (PTAB Dec. 15, 2017) (precedential as to § III.C.5, first paragraph) (“*Becton, Dickinson*”).

Under the *Advanced Bionics* step 1 and *Becton, Dickinson* factors (a), (b), and (d), none of Guthrie, Sormunen, or Kato was before the Examiner in prosecution. Ex. 1004.

Even under a broad reading of these cases, denial would be improper because the art relied on in this Petition is not substantially the same as, or cumulative of,

any art considered during prosecution. The Examiner relied on Schmitz, Glaschick, and O’Neil, and noted that they do not disclose “the transaction for determining the password in the setting up of a new calling-card-derived temporary network account is performed entirely over a connection other than that used by eventual network account” (*id.*, 47-48), which is taught by each of Kato and Sormunen. §§ V-VI; Reiher, 37-39. Kato and Sormunen are not cumulative of any of the references cited by the Examiner because each discloses the features that the Examiner considered not disclosed in those references.

IX. Mandatory Notices

A. Real Parties-in-Interest

The real parties-in-interest for this Petition are:

- 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.,⁴ and
- The PNC Financial Services Group, Inc.⁵

B. Related Matters

To Petitioners' knowledge, the '658 Patent is involved in the following:

Name	Number	Court	Filed
<i>Dynapass IP Holdings LLC v. Bank of America Corp.</i>	2:22-cv-00210	EDTX	June 17, 2022
<i>Dynapass IP Holdings LLC v. BOKF National Assn.</i>	2:22-cv-00211	EDTX	June 17, 2022
<i>Dynapass IP Holdings LLC v. JPMorgan Chase & Co.</i>	2:22-cv-00212	EDTX	June 17, 2022
<i>Dynapass IP Holdings LLC v. PlainsCapital Bank</i>	2:22-cv-00213	EDTX	June 17, 2022
<i>Dynapass IP Holdings LLC v. PNC Financial Services Group, Inc.</i>	2:22-cv-00214	EDTX	June 17, 2022

⁴ PNC Bank, N.A. is the successor by merger to BBVA USA, which merged into PNC Bank, N.A. in 2021.

⁵ The PNC Financial Services Group, Inc. is the successor by merger to BBVA USA Bancshares, Inc., which merged into The PNC Financial Services Group, Inc. in 2021.

Name	Number	Court	Filed
<i>Dynapass IP Holdings LLC v. Regions Financial Corp.</i>	2:22-cv-00215	EDTX	June 17, 2022
<i>Dynapass IP Holdings LLC v. Truist Financial Corp.</i>	2:22-cv-00216	EDTX	June 17, 2022
<i>Dynapass IP Holdings LLC v. Wells Fargo & Co.</i>	2:22-cv-00217	EDTX	June 17, 2022
<i>Dynapass IP Holdings LLC v. Woodforest National Bank</i>	2:22-cv-00218	EDTX	June 17, 2022

C. Lead and Back-Up Counsel

Lead Counsel	Back-Up Counsel
Lionel M. Lavenue (Reg. No. 46,859) lionel.lavenue@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Tel: 571-203-2700 Fax: 202-408-4400	Kara A. Specht (Reg. No. 69,560) kara.specht@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 271 17th Street, NW, Suite 1400 Atlanta, GA 30363-6209 Tel: 404-653-6400 Fax: 404-653-6444 Cory C. Bell (Reg. No. 75,096) cory.bell@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 2 Seaport Lane, 6th Floor Boston, MA 02210-2001 Tel: 617-646-1641 Fax: 202-408-4400 Xirui Zhang (Reg. No. 78,809) xirui.zhang@finnegan.com Finnegan, Henderson, Farabow,

Lead Counsel	Back-Up Counsel
	Garrett & Dunner, LLP 2 Seaport Lane, 6th Floor Boston, MA 02210-2001 Tel: 617-646-1626 Fax: 202-408-4400

D. Service Information

Please address correspondence to counsel at the addresses above and Dynapass-IPR@finnegan.com. Petitioners consent to service by e-mail.

X. Standing

The '658 Patent is eligible for *inter partes* review and Petitioners are not barred or estopped from requesting review.

XI. Conclusion

Petitioners have established a reasonable likelihood of success and request the Board institute review and cancel the Challenged Claims.

Dated: January 3, 2023

Respectfully submitted,

/Lionel M. Lavenue/

Lionel M. Lavenue, Lead Counsel
Reg. No. 46,859

CERTIFICATION UNDER 37 C.F.R. § 42.24(d)

Pursuant to 37 C.F.R. § 42.24(a)(1)(i), the undersigned hereby certifies that the foregoing **Petition for *Inter Partes* Review** contains 13,928 words, excluding the parts of this Petition that are exempted under 37 C.F.R. § 42.24(a), as measured by the word-processing system used to prepare this paper.

/Lionel M. Lavenue/

Lionel M. Lavenue, Lead Counsel
Reg. No. 46,859

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(a), the undersigned certifies that on January 3, 2023, a copy of the foregoing **Petition for *Inter Partes* Review, Petitioners' Power of Attorneys and Designation of Lead and Back-up Counsel, and Exhibits 1001-1033** were served by Priority Mail Express on the correspondence address of record indicated in the Patent Office's Patent Center system for U.S. Patent No. 6,993,658.

Miguel Medina
DynaPass Inc
P.O. Box 11510
Costa Mesa, CA 92627

A courtesy copy has been served on litigation counsel at:

John Wittenzellner
Williams, Simons, and Landis, PLLC
1735 Market St.
Suite A #453
Philadelphia, PA 19103

Date: January 3, 2023

By: /Daniel E. Doku/
Daniel E. Doku
Litigation Legal Assistant
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP