

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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

DYNAPASS IP HOLDINGS LLC,
Patent Owner.

Case No. IPR2023-00367
Patent No. 6,993,658

DECLARATION OF DR. PETER LAWRENCE REIHER

Table of Contents

I.	Introduction.....	1
II.	Qualifications.....	1
III.	Materials Considered	4
IV.	Relevant Legal Standards	8
	A. Level of Ordinary Skill in the Art.....	11
	B. Claim Construction	13
V.	The '685 Patent.....	16
	A. Overview of the '658 Patent.....	16
	B. Summary of the Prosecution History of the '658 Patent	18
VI.	Grounds of Unpatentability	21
VII.	State of the Art.....	21
	A. Two-factor Authentication (2FA) was Well Known.	21
	B. Cell Phones and Cell Networks were Well Known.....	23
	C. Use of Mobile Tokens was Well Known.....	27
	D. Contatenation of a Random Number and a Password was Well Known.	27
VIII.	Ground 1: Guthrie in Combination with Sormunen Renders Obvious Claims 1-3 and 5-7.....	30
	A. Guthrie-Sormunen Combination	30
	1. Summary of the Guthrie-Sormunen Combination.....	30
	2. Guthrie and Sormunen Are Analogous Art and Combinable...33	
	3. A person of ordinary skill in the art 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	36
B.	Independent Claims	43
1.	Claim 1	43
2.	Claim 5	67
C.	Dependent Claims	75
1.	Claim 2: “The method of claim 1, wherein the new password is generated by concatenating the token and the passcode.”	75
2.	Claim 3: “The method of claim 1, wherein the personal communication device is a mobile phone.”	77
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.”	77
4.	Claim 7: “The system of claim 6, wherein the request is transmitted by the user through the personal communication device.”	78
IX.	Ground 2: Kato in Combination with Guthrie Renders Obvious Claims 1-3 and 5-7	78
A.	Kato-Guthrie Combination.....	78
1.	Summary of the Kato-Guthrie Combination	78
2.	Kato and Guthrie are Analogous Art and Combinable.....	79
3.	A person of ordinary skill in the art Would Been Motivated to Add Guthrie’s Challenge-Response Process to Kato’s Three-Device Architecture and Would Have Had a Reasonable Expectation of Success in Doing So	82
B.	Independent Claims	92

1.	Claim 1	92
2.	Claim 5	113
C.	Dependent Claims	118
1.	Claim 2: “The method of claim 1, wherein the new password is generated by concatenating the token and the passcode.”	118
2.	Claim 3: “The method of claim 1, wherein the personal communication device is a mobile phone.”	118
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.” Claim 7: “The system of claim 6, wherein the request is transmitted by the user through the personal communication device.”	118
X.	Conclusion	119

I. INTRODUCTION

1. I, Dr. Peter Lawrence Reiher, submit this declaration to state my opinions on the matters described below.

2. I have been retained on behalf of Petitioners as an independent expert for the above-identified *inter partes* review proceeding involving U.S. Patent No. 6,993,658 (“the ’658 Patent”). Although I am being compensated for my time in connection with this IPR at my standard hourly consulting rate and reimbursed for reasonable out-of-pocket expenses, no part of my compensation depends on the outcome of this proceeding, and I have no other interest in this proceeding.

3. I have been asked to provide my technical review, analysis, insights, and opinions regarding the ’658 Patent and the above-noted references that form the basis for the invalidity grounds set forth in the Petition for *Inter Partes* Review of the ’658 Patent.

II. QUALIFICATIONS

4. I believe that I am well qualified to serve as a technical expert in this matter based upon my educational and work experience.

5. I received a BS in Electrical Engineering, specializing in computer science, from the University of Notre Dame in 1979. I received my MS in Computer Science from UCLA in 1983, and my Ph.D. in Computer Science from UCLA in 1987. After spending five years working on an operating systems project

at the Jet Propulsion Laboratory, I returned to UCLA, where I served as a research scientist and adjunct faculty member from 1992 until my retirement in 2021.

6. During this time at UCLA, I obtained research grants from several sources to study topics in computer and network security, operating systems and file systems, mobile computing, and related topics. The sources for these grants included DARPA, the National Science Foundation, the Department of Homeland Security, the Department of Education, the Intel Corporation, Microsoft, Hewlett Packard, Lockheed Martin, and GTE. The total amount of research funding I received exceeded \$10 million.

7. The topics I researched with these grants include distributed file systems, encrypted file systems, mobile computing, active networking security, distributed denial of service attacks and defenses against them, IP spoofing, vehicular network security, operating system security, and other related topics, specifically those related to computer security. Some of these research projects involved various authentication methods, such as the Truffles project, which used authentication methods in conjunction with a secure distributed file system. In the Panoply ubiquitous computing project, we experimented with multi-factor authentication in which one factor was physical location of the subject. I published over 140 articles on these research topics in conferences, including Infocom, ICNP, the Usenix Security Symposium, Usenix FAST, the Usenix Annual

Technical Conference, and ACSAC, and in journals, including IEEE Transactions on Computing, ACM Transactions on Storage, IEEE Transactions on Dependable and Secure Computing, ACM Mobile Computing and Communications Review, Computer Networks, IEEE Communications Surveys and Tutorials, and the Journal of Distributed and Parallel Databases. I am also a co-author of a book on distributed denial of service attacks, and have contributed chapters to several other books. I have also contributed a chapter on operating system authentication to an online textbook used in operating system classes.

8. During this time at UCLA, I served as the Ph.D. advisor for 18 students, counting only those who have received their degree to date. My students serve in various academic and industry positions, including at the University of Oregon, Florida State University, Harvey Mudd College, the Intel Corporation, Google, IBM, Oracle, ISI, and the Aerospace Corporation. Most of these students worked on security research for their Ph.D. topics, and many continue to perform security research and development in their current positions.

9. I have reviewed hundreds of papers for various computer science conferences, workshops, and journals, primarily papers on computer security issues. I have served as a co-editor of ACM Transactions on Internet Technology from 2007-2015. I have been a member of the program committee for dozens of conferences, and served as the program chair or general chair for half a dozen

conferences. I was vice chair of the IEEE ComSoc Communications and Information Security Technical Subcommittee from 2005-2007.

10. I have taught dozens of graduate and undergraduate classes at UCLA in the Computer Science Department, primarily classes on computer security and operating systems, with total enrollments in the thousands of students. My computer security class includes lectures and readings on different authentication technologies for secure computer systems.

11. I retired from the Department of Computer Science at the University of California, Los Angeles in 2021, but continue to teach classes in that department and advise Ph.D. students. I will be teaching an operating system course (for about 250 students) in the winter quarter of 2023, and a computer security class in the spring quarter of that year.

III. MATERIALS CONSIDERED

12. In forming my opinions, I have reviewed the following documents and any other documents cited in this declaration:

Exhibit	Description
Ex. 1001	U.S. Patent No. 6,993,658 B1 to Engberg. et al. (“the ’658 Patent”)
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”) ¹
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”)
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”)

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

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”)
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, 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”)
	<i>DIAL-IN SECURITY -- Passwords Aren't Enough</i> , Lenny Liebmann VARbusiness: 143. The Channel Company (July 1, 1995) (“Liebmann”)
	<i>Desperate Times Call For Desperate Measures</i> , David Willis, Network Computing: 72. Informa. (March 1, 1996) (“Willis”)
	<i>Smart token gestures of protection; Southern New England Telephone relies on smart-card token technology to secure their network</i> , Ziff Davis Media Inc., PC Week: N03 (January 22, 1996)
	<i>Bull Adds Support for Security Dynamics Authentication Tools Under ISM AccessMaster Enterprise Security Management Software</i> , Business Wire: 05061173 (May 6, 1997)
	<i>World's Largest Wholesale Distributor to Market ActivCard Strong Authentication Solutions</i> , PR Newswire (July 27, 1999)
	<i>InfoExpress and ActivCard Team to Provide Hardware Authentication for Virtual Private Networks Over the Internet</i> , Business Wire: 5200016 (May 20, 1996)
	<i>Securing the World Wide Web: smart tokens and their implementation</i> , Jones et al., Fourth International World Wide Web Conference (December 1995)
	<i>Authentication Techniques for Smart Cards</i> , R. A. Nelson, CardTech SecurTech '94 (February 1994)
	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)
	Alfred Menzies, Paul van Oorshot, and Scott Vanstone, <i>Handbook of Applied Cryptography</i> , CRC Press, 1997, page 390

	Bruce Schneier, <i>Applied Cryptography</i> , O'Reilly, 1996, page 194
	Robert Morris and Ken Thompson, <i>Password Security: A Case History</i> , Communications of the ACM, Vol. 22, No. 11, November 1979
	Peter Denning, <i>The Science of Computing: Passwords</i> , American Scientist, Vol. 80, No. 2, March-April 1992
	M. Luby and C. Rackoff, <i>A Study of Password Security</i> , J. Cryptology (1989) 1:151-158
	David Feldmeier and Philip Karn, <i>Unix Password Security: Ten Years Later</i> , Crypto'89, 1989
	Michael Jackson, <i>Linux Shadow Password HOWTO</i> , Linux Documentation Project, April 3, 1996

IV. RELEVANT LEGAL STANDARDS

13. In preparing this declaration and forming my opinions, I am relying on certain legal principles that counsel explained to me. My understanding of these concepts is summarized below.

14. I have been asked to provide my opinions regarding whether claims 1–3, 5-7 (“the Challenged Claims”) of the ’658 Patent are unpatentable, because they would have been obvious to a person having ordinary skill in the art at the time of the alleged invention, in light of the prior art. I have been advised and understand that prior art includes all analogous art, and that two separate tests define the scope of analogous prior art: (1) whether the art is from the same field of endeavor, regardless of the problem addressed and, (2) if the reference is not

within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved. It is my opinion that the Challenged Claims would have been obvious to a person having ordinary skill in the art at the time of the '658 Patent invention.

15. In forming my opinions expressed below, in addition to my knowledge and experience based upon my work in the fields of computer networks, computer and network security, mobile computing, and user authentication technologies for secure computer and network systems, I have considered the documents listed in the Table in Section III above.

16. I have been advised and understand that a dependent claim is a patent claim that refers back to another patent claim. I have been informed and understand that a dependent claim includes all of the limitations of the claim to which it refers.

17. I have been advised and understand that there are two ways in which prior art may render a patent claim unpatentable. First, the prior art can "anticipate" the claim. Second, the prior art can make the claim "obvious" to a person of ordinary skill in the art. I understand that for an invention claimed in a patent to be patentable, it must not be anticipated and must not be obvious based on what was known before the invention was made.

18. I have been advised and understand that a patent claim is unpatentable as anticipated under 35 U.S.C. § 102 if each element of that claim is present either explicitly or inherently in a single prior art reference. I have also been advised and understand that, to be an inherent disclosure, the prior art reference must necessarily disclose the limitation. The fact that the reference might practice or contain a claimed limitation is insufficient to establish that the reference inherently teaches the limitation.

19. I have been advised and understand that a claimed invention is unpatentable under 35 U.S.C. § 103 if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. I have also been advised and understand that the obviousness analysis takes into account factual inquiries, including the level of ordinary skill in the art, the scope and content of the prior art, and the differences between the prior art and the claimed subject matter.

20. I have further been advised and understand that the Supreme Court has recognized several rationales for combining references or modifying a reference to show obviousness of claimed subject matter. Some of these rationales include the following: (a) combining prior art elements according to known methods to yield predictable results; (b) simple substitution of one known element

for another to obtain predictable results; (c) use of a known technique to improve a similar device (method, or product) in the same way; (d) applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (e) choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; and (f) some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

21. When considering the issue of obviousness, I have been advised and understand that I should consider (1) the scope and content of the prior art; (2) the differences between the prior art and the claims at issue; (3) the level of ordinary skill in the art; and (4) evidence of secondary indicia of nonobviousness. I have been informed that secondary indicia of nonobviousness include (i) “long-felt need” for the claimed invention, (ii) commercial success attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) “copying” of the claimed invention by others.

A. Level of Ordinary Skill in the Art

22. In rendering the opinions set forth in this declaration, I have been asked to consider the '658 Patent's claims and the prior art through the eyes of a person of ordinary skill in the art. I understand that a person of ordinary skill in the

art is determined by considering (1) the type of problems encountered in the art, (2) prior art solutions to those problems, (3) the rapidity with which innovations are made, (4) the sophistication of the technology, and (5) the educational level and years of experience level of those working in the pertinent field.

23. I understand that I must evaluate the '658 Patent from the perspective of a person of ordinary skill in the art. That is, the '658 Patent must be evaluated through the eyes of a person with ordinary skill in the relevant art at the time of the invention of this patent as of its earliest priority date. It is my opinion that such a person of ordinary skill in the art as related to the '658 Patent 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 authentication technologies for computer systems at the time of the '658 Patent invention, that is as of the earliest priority date of the '658 Patent—March 6, 2000. If a person did not have a bachelor's degree, sufficiently greater relevant and practical experience with computer and network security and user authentication could provide an acceptable substitute. Likewise, further education beyond a bachelor's degree could compensate for a deficiency in practical experience.

24. Based on my educational background and experience, such as my experience with computer and network security and user authentication technologies (*see* paragraphs 5-11), I am qualified as at least a person of ordinary

skill in the art with respect to the '658 Patent. Thus, I am familiar with the knowledge of the person of ordinary skill in the art at the time of the '658 Patent invention. I am able to opine on how a person of ordinary skill in the art would have understood the disclosure and claims of the '658 Patent, the disclosures of the prior art, the motivation to combine the prior art, and what combinations would have been obvious and not have been obvious to one of ordinary skill in the art.

B. Claim Construction

25. I have been informed that in an *inter partes* review proceeding, claim terms should be construed under the same standard applied in federal district court cases. Under this standard, I have been informed that claim terms are generally given their ordinary and customary meaning as understood by one of ordinary skill in the art in light of the specification and the prosecution history pertaining to the patent. I understand, however, that claim terms are generally not limited by the embodiments described in the specification.

26. I understand that in addition to the claims, specification, and prosecution history, other evidence may be considered to ascertain the meaning of claim terms, including textbooks, encyclopedias, articles, and dictionaries. I have been informed that this additional evidence is often less significant and less reliable than the claims, specification, and prosecution history.

27. I have also been informed that claims should only be construed to the extent necessary to resolve any controversy.

28. I also have been informed of a special rule applied to claim limitations drafted in what is referred to as “means-plus-function” limitations. I understand that a “means-plus-function” limitation recites a structural component solely in terms of the function it performs. In other words, a patent claim may recite a structural element that is essentially a placeholder word (for example, the word “means”) presented in terms of the function it performs (e.g., a claim reciting a “means for [function]”). I understand that the special rule for construing means-plus-function limitations involves two steps: (1) identifying the claimed function, and (2) determining what structure, if any, disclosed in the specification corresponds to that claimed function.

29. Based on my review of these materials and my personal knowledge and experience, I have considered the plain and ordinary meaning of each term of the '658 Patent as it would have been understood by one skilled in the art at the time of the '658 Patent invention. I apply the plain and ordinary meaning of each claim term throughout this declaration.

30. I have been informed that the claim terms “*control module*” and “*authentication module*” may be considered as means-plus-function limitations. For the purpose of this declaration, I have been asked to consider the function and

the structure for the function as disclosed in the specification of the '658 Patent for each of these claim terms as they would have been understood by a person of ordinary skill in the art.

31. The claimed functions of the “*control module*” are “*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*” and “*to set a password associated with the user to be the new password,*” as recited in claim 5, and additionally “*to create the new password in response to the request,*” as further recited in claim 6. A person of ordinary skill in the art would have understood that the corresponding structure for performing these claimed functions in the specification of the '658 Patent is a software module executed on the computer processor of the token server. Ex. 1001, FIG. 4, 8:7-10.

32. The claimed functions of the “*authentication module*” are “*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*” and to “*activate[] access to the account in response to the password and deactivate[] 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.*” A person of ordinary skill in the art would have understood that the corresponding

structure for performing these claimed functions in the specification of the '658 Patent is a software module executed on the computer processor of the user authentication server. Ex. 1001, FIG. 1, 5:1-21.

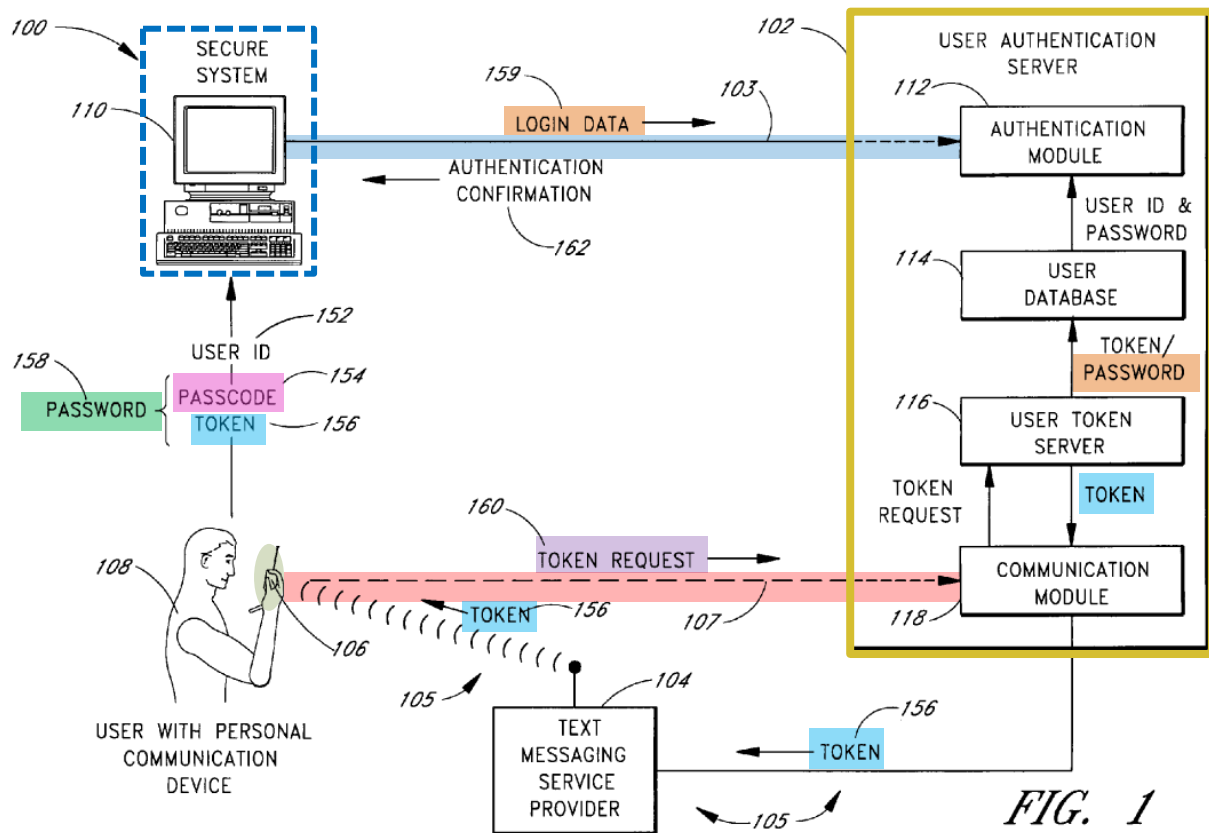
33. As discussed below, Guthrie discloses the same functions and structures of these claim terms as these constructions require and also reasonable equivalents.

V. THE '685 PATENT

A. Overview of the '658 Patent

34. I understand that the '658 Patent issued from U.S. Patent Application No. 09/519,829 on March 6, 2000. Ex. 1001, 1. I have also been informed that the filing date—March 6, 2000—is the earliest priority date of the '658 Patent.

35. The '658 Patent discloses a user authentication system and method of authenticating a user to gain access to 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.

Ex. 1001, FIG. 1.²

36. To obtain the password, the user sends a request for a token to a token server of the user authentication 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 in response to the request, 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

² All color or bold emphases and annotations in this petition have been added unless noted otherwise.

personal communication device can be a mobile phone or pager, the token request can be a phone call or SMS message, and the token can be transmitted in an SMS message or page data. *Id.*, 5:41-56, 9:47-54, 7:33-39, 10:14-20, 10:42-59, 11:9-20. The token server also generates a new password based on the token and a passcode of the user and updates the password associated with the user in a user database to the new password. *Id.*, 6:59-64, 8:16-25, 8:53-63, 9:28-37. The token can be a random sequence of numbers not known to the user, but the passcode is known to the user. *Id.*, 4:36-39, 6:52-55, 9:21-25. After receiving the token, before the token expires, the user can obtain the password based on the token and known passcode and submit the password to the user authentication server via the secure computer network to gain access to the secure system. *Id.*, Abstract, 4:52-56, 7:57-67, 9:55-64.

B. Summary of the Prosecution History of the '658 Patent

37. The application for the '658 Patent was filed on March 6, 2000. Ex. 1001, 1. The Examiner originally rejected the Challenged Claims as being anticipated over Australian Patent Application No. 63545/98 to Schmitz (an Australian counterpart application of Schmitz (Ex. 1011)), or obvious over Schmitz in view of "Handbook of Applied Cryptography," published in 1997 by Menezes et al. Ex. 1004, 128-130. Applicant traversed these rejections without amendments, arguing that Schmitz did not teach or suggest "*receiving a request*

transmitted by the personal communication device” because “Schmitz teaches receiving a request transmitted by a data input apparatus 1 while using the receiver 3 (i.e., a personal communication device) only for receiving the TAN [(password)].” *Id.*, 120 (emphasis in original). Applicant also argued that Menezes did not disclose or suggest “***generating a new password based at least upon a token and a passcode, . . . transmitting the token to the personal communication device; and receiving the password from the user***” because “the salt [(token)] taught by Menezes is only used internally in the system verifying the password and is not transmitted to the user each time a request is received.” *Id.*, 121-122 (emphasis in original).

38. The Examiner further rejected the Challenged Claims as being anticipated over U.S. Patent No. 5,323,146 to Glaschick (“Glaschick”) or U.S. Patent No. 6,226,364 to O’Neil (“O’Neil”), or obvious over O’Neil in view of Glaschick. *Id.*, 75-79, 101-103. Applicant originally traversed these rejections without amendments, arguing that “Glaschick is silent on using a *personal communication device* possessed by a user,” and O’Neil’s teaching of accessing cellular phone service through a cellular phone does not disclose “*access directly to the secure system* (i.e. not through the personal communication device).” *Id.*, 92-94. The Examiner rejected Applicant’s arguments, suggesting that “Applicant’s personal communication device . . . is simply a type of computer with programs,”

disclosed by Glaschick's computer with programs (*id.*, 77), and O'Neil's telephone system that requires authorization to access constituted a "secure system" (*id.*, 75).

In response, Applicant cancelled some claims and substantially amended the claims "to point out the separation of the network on which the user is being authenticated to access the user's account, and the personal communication device on the cell," and discussed those amendments with the Examiner in a telephone interview. *Id.*, 62, 71. The Examiner allowed the amended claims after making an Examiner's Amendment to address concerns with subject matter eligibility. *Id.*, 46.

39. In the Notice of Allowance issued on August 8, 2005, the Examiner stated that "no art could be found wherein 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.*, 44-48. The Examiner further distinguished the claims from references that teach "the user request is sent over the network account connection," that "do not suggest any password exchange," or that teach "use of a temporary account with a PIN, but the PIN is initially issued and not changeable." *Id.* As explained in Sections VIII and IX, the prior art used in this Petition discloses all these teachings missing from the prior art considered by the Examiner. For example, Kato and Sormunen both teach the user initiates a request for a password by a mobile phone over a cell phone network that is separate from the

secure computer network on which the user is being authenticated to access the user's account. *See below* Sections VIII.B.1.c, IX.B.1.c. And Guthrie discloses a personal authentication system with a dynamic challenge-response process to enhance security. Guthrie, Abstract.

VI. GROUND OF UNPATENTABILITY

40. Based on my review of the materials set forth above, including my application of the knowledge of a person of ordinary skill in the art, it is my opinion that claims 1-3 and 5-7 of the '658 Patent are rendered obvious to one of ordinary skill in the art.

41. In particular, it is my opinion that claims 1-3 and 5-7 of the '658 Patent would have been rendered obvious to one of ordinary skill in the art, based on the grounds shown below:

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

VII. STATE OF THE ART

A. Two-factor Authentication (2FA) was Well Known.

42. At the time of the '658 Patent invention, the concept of 2FA was well known. Moussa, 1:8-19 ("Security systems which attempt to authenticate a user are

based on one or more of three kinds of information: (1) secret information which is shared by the user and the system, such as a password, PIN, or pass phrase; (2) a physical object which is possessed by the user and recognized by the system, such as a physical key, token or active electronic device; and (3) biometric information which is unique to the user and which can be received and authenticated by the system, such as a fingerprint, handwritten signature, retinal scan, or voiceprint.

Security systems which use more than one of these factors are considered more secure than those which do not.”; see also e.g., Falk; Akhteruzzaman; Kew;

Peters; Ratayczak; Owens. In some instances, the user dials in and enters a personal identification number (PIN) or the like. The authentication unit at the communications server responds with a random number “challenge” that the user then enters into their token device. Next, the token device generates a response code (e.g., based on a preset encryption algorithm) that the user then enters. If the authentication device verifies that the response code is correct, then the session is established. Using a device possessed by the user for 2FA purposes was also well known because it allows authentication only when you can combine something you know with something you have.

43. The specification of the '658 Patent acknowledges one particular known 2FA system, RSA Security Inc.'s SecurID system, in the background:

The SecurID product, which is distributed by RSA Security Inc., solves many of the aforementioned problems by requiring a two-factor authentication process. The first factor is a user passcode or personal identification number. The second factor is a SecurID card that is possessed by the user. The SecurID card generates and displays unpredictable, one-time-only access codes that automatically change every 60 Seconds. The user supplies the displayed code upon logging into a system. The system has a corresponding code generator that allows verification of possession of the card.

Ex. 1001, 1:44-53.

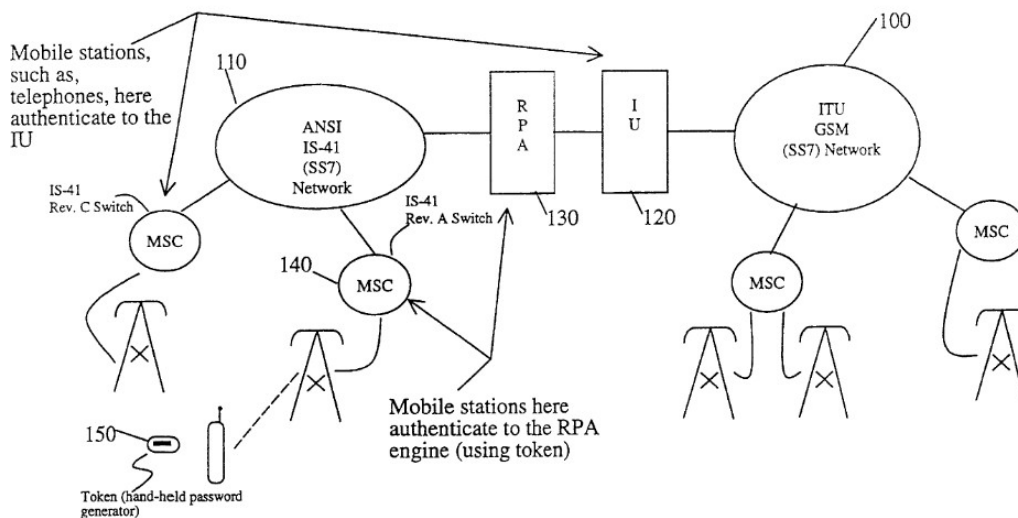
B. Cell Phones and Cell Networks were Well Known.

44. At the time of the '658 Patent invention, cell phones and cell phone networks were widely known and understood by those of skill in the art. It would have been readily understood by a person of ordinary skill in the art that a cell phone could operate as something you have for purposes of 2FA. Ueshima, 4:1-12 ("Herein, the portable mobile communication terminal means a portable telephone such as a so-called cellular phone or a PHS (personal handy phone system) terminal. In the present invention, the portable mobile communication terminal is used as a device which is analogous to the conventional password generator. Since the portable mobile communication terminal has already been wide spread, this invention is not only advantageous in view of the cost but also has a merit that the

user need not carry a password generator exclusively for the purpose of the authentication, as compared with the case where such special password generator is used.”); 16:61-67 (“According to the present invention, the user authentication is performed by the use of the telephone which is already wide spread at present. Therefore, the equivalent effect can be obtained at low cost as compared with the conventional technique which requires the hardware exclusively for use in authentication. It is especially convenient to use the cellular phone or the personal handyphone system.”).

45. Use of mobile phones for authentication was also well known. *See* Owens, 13:24–27 (“Referring to FIGS. 8 and 9, the following is a high level view of the process for subscriber validation using the RPA engine and the token for, by way of example, IS-41 subscribers operating, for example, mobile telephones”).

FIG. 8



Owens, FIG. 8; *see also* Devinney, [0076] (“The communication unit 416 in the client terminal may be a telephonic communication device, modem, internet access line, cellular telephone, digital PCS transmitter or any known local or remote voice/data interface, including as known busses and interfaces.”); Atsmon, Abstract (“A method of authentication using an electronic device (20), comprising: providing a computer (22, 24, 26, 28, 140) having a sound receiving (28) and generating sub-system including a microphone (26); providing a personal communicator (30, 144) which utilizes a communication network (148); initiating a connection by the computer (22, 24, 26, 28, 140), over the communications network (148), to the personal communicator (30, 144) and identifying the personal communicator (30, 144) responsive to an audio response of the personal communicator (30, 144) to the connection initiation. Preferably, the personal communicator (30, 144) is a cellular telephone”); 21:11-20 (“Alternatively or additionally, a cellular telephone may digitally sign a message that passes through it using the ID. A user may also be required to type a code, which is overheard by the computer and/or a remote code may be provided from a third computer, over the cellular network. Thus, a user is required to have the right cellular telephone, know a code and/or response and have a support of a third party.”).

46. Even “smartphones” were known at least as early as 1997. *See* Cahill, 4:21-30 (“This allows the invention to deliver information to the customer via any

communication means presently known, or that might be available in the future.

This includes telephone, telegraph, fax, beeper, one-way cable TV, one-way satellite, dial-out terminal, on-line terminal, Internet, Intranet or Extranet, SmartPhone, 2-way beeper, 2-way cable TV, 2-way satellite, Personal Digital Assistant (PDA), Personal Computer (PC), express mail delivery, commercial express delivery and various systems of the type mentioned above.”). A person of ordinary skill in the art would recognize a smartphone’s ability to send and receive tokens due to their capabilities of sending non-voice data. *See* Audebert, 16:17-24 (“Audebert”) (“The mechanisms described in the first embodiment can also be embedded in any other device possessed by the user, and offering the same characteristics, i.e., having their own source of energy 9A, a keypad 6, processor 9, the ability to produce clock pulses and a display 8 or a way to directly transmit the password to the second unit (communication channel). Such a device can be, e.g., a personal digital assistant (PDA), a phone, or a cellular phone.”).

47. Cell networks were also well-known and used for purposes of allowing cell phones to be used for authentication. *See* Atsmon, 20:6-12 (“It should be noted that different types of personal communicators use different types of communication networks. For example, analog beeper networks may include a human go-between, cellular beeper networks include local cells, telephone networks include telephone interchanges and integrated LAN telephony networks

use a same network for both voice and data communications.”); Owens, Abstract (“A method and/or system for validating subscribers includes an insecure communications network, such as, an IS-41 wireless telephone network connecting a plurality of telephone switches.”).

C. Use of Mobile Tokens was Well Known.

48. The use of tokens for 2FA was well known at the time of the ’658 Patent invention. *See* Owens; Gurevich; Cahill. For example, it was known to a person of ordinary skill in the art that tokens could be mobile. Gurevich, [0033] (“In another embodiment, the token is a general-purpose palm held computing device. In yet another embodiment, the token is a digital phone. In still another embodiment, the token is a smart card. Token may also be implemented entirely in software.”).

D. Contatenation of a Random Number and a Password was Well Known.

49. Concatenation of a random number and a password as an input to a hashing algorithm was a well known and widely used technique at the time of the ’658 Patent invention.

50. The ’658 Patent discloses that the token is random. Ex. 1001, Abstract, 2:1-2, 6:52-55. In several places, the patent indicates that the passcode is a secret. *Id.*, Abstract, 2:2-4, 4:36-41, 9:56-60. Combining a piece of secret information with a random number as an input to a cryptographic operation, such

as hashing or encryption, has been a common, well-known technique to ensure that the operation produced a unique output for many decades, long before the invention of the '658 Patent. It was used for many purposes in computer security. In one usage, a random number referred to as a *nonce* would be included with a secret message to be sent from one computer to another across a network, thus ensuring that the transmitted message was fresh and not a replay of a previously sent message. The purpose of the concatenation of the random token and passcode in the '658 Patent in one example is similar (Ex. 1001, Abstract, 2:64-66, 9:34-38), to ensure that a login attempt from a potentially malicious party is not a replay of a previous correct login attempt. In another classic use of this technique, a random number called an *initialization vector* was used to ensure that the encryption of even two small identical pieces of a text resulted in different encrypted values.

51. Another relevant classical use of combining a random value with a password before performing a computation is *password salting*. In password salting, a random number is concatenated with a secret password, with the result being passed through a hashing operation. Instead of storing the actual password, a computer can store the random number and the hashed value, allowing it to check validity of a password provided at login without the computer actually having a copy of the correct password. The basic operation of password salting is to generate a random number, concatenate it to a user-chosen password, perform a

computation (typically a form of hashing) on the concatenated result, and store the hashed result and the random number. To check attempts to provide a password for user authentication, the submitted password and the stored random number are hashed and compared to the stored hash, with only a perfect match indicating submission of the correct password. This is similar to the process described in the '658 Patent: generating a random number, concatenating it to a correct password, running the concatenation through a hashing algorithm, and checking user authentication against the hashed result with, again, only perfect matches indicating successful authentication.

52. Password salting is an old technique well known to anyone who has spent any time dealing with user authentication in computers. It dates back at least to a classic paper by Morris and Thompson, from 1979. Password salting is regarded as a good security practice for storage of passwords. It has been present in popular computer systems for decades, predating the '658 Patent, including Unix, Linux, and Macintosh operating systems. Any professional designing an authentication system involving passwords would be aware of password salting and its benefits, and would have known to apply a similar technique to obtain similar benefits. Thus, the generation of a new password by concatenation of a passcode and a random token would have been an obvious way to create a unique

piece of authentication for anyone with sufficient familiarity with computer authentication to work in the field.

53. Each of the concepts discussed above, as well as many others, were widely known by the time of the '658 Patent invention. Accordingly, the '658 Patent is nothing more than a recitation of knowledge that was well-known in the industry, and are at best, a recitation of well-known features and functionalities that took no more than an ordinary skill in the art to arrange in a known manner using conventional techniques.

VIII. GROUND 1: GUTHRIE IN COMBINATION WITH SORMUNEN RENDERS OBVIOUS CLAIMS 1-3 AND 5-7

54. In my opinion, Guthrie in combination with Sormunen renders obvious claims 1-3 and 5-7.

A. Guthrie-Sormunen Combination

1. Summary of the Guthrie-Sormunen Combination

55. 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 during the authentication process), a randomly generated challenge (transmitted to the user over the network), and a response generated based on the password and challenge (transmitted by the user for

authentication). 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. Guthrie, 7:60-8:6, 6:57-64, 7:27-38.

56. Like Guthrie, Sormunen discloses authenticating a user to access a protected service on a network 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. Sormunen, p. 5, l. 33–p. 7, l. 18.

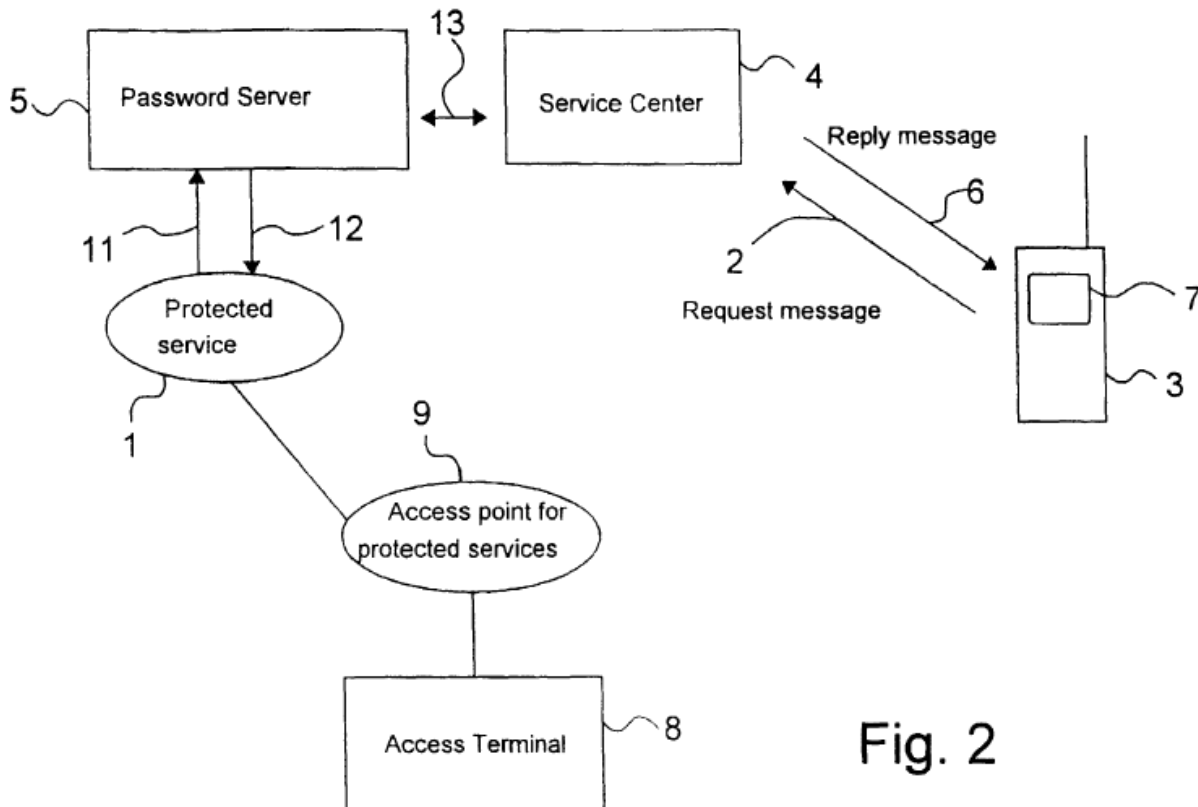


Fig. 2

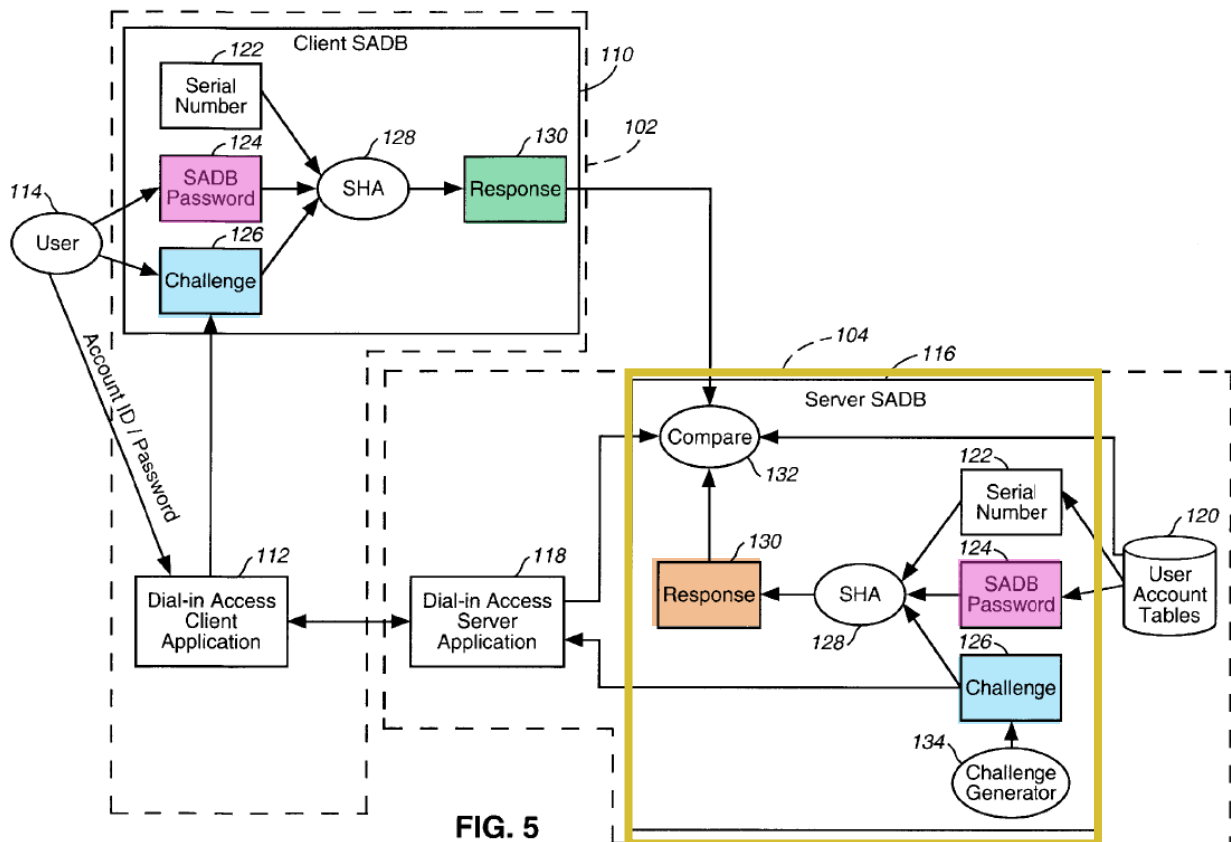
Sormunen, FIG. 2.

57. In my opinion, a person of ordinary skill in the art would have combined Guthrie and Sormunen to improve the security of Guthrie's system by implementing Sormunen's use of a mobile station as the device 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 in authenticating a user to access a remote system).

2. Guthrie and Sormunen Are Analogous Art and Combinable

58. The '658 Patent discloses a user authentication system and method of authenticating a user to gain access to a secure system based on a dynamic password. Ex. 1001, Abstract; *see above* Section V.A.

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



Guthrie, FIG. 5.

60. In Guthrie, 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 response valid timer expires, the server compares the expected response with the response from the client to authenticate the user; if there is a match, the user may access the server. *Id.*, 7:7-9, 7:38-45, 11:60-12:42. If the response valid timer has expired, the user cannot be authenticated without restarting the challenge-response process. *Id.*, 11:50-59, FIG. 8B.

61. Sormunen is in the same field of user authentication technologies and addresses the same problem of regulating a user's access to a secured 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 (e.g., password) 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, a user in Sormunen sends a short message including a “password request” from a mobile station via a mobile communication network, such as a cellular network. Sormunen, p. 4, l. 30–p. 6, l. 1, p. 7, l. 37–8, l. 3. A password server receives the request, generates a password in response to the request, and sends a reply message containing the password to the mobile station. Sormunen, p. 6, ll. 20-38. The user then submits, via an access terminal, the password received by the mobile station and its username to request access to a 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 that 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).

62. 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 would result in a more secure system than either individually.

3. A person of ordinary skill in the art 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

a. Motivation

63. In my opinion, a person of ordinary skill in the art 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 the security of Guthrie’s system 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 mobile device possessed by the user.

64. *First*, because Sormunen recognizes that cellular networks and SMS messaging are more secure than computer networks like the Internet, a person of ordinary skill in the art 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 during transmission. Guthrie discloses the server generates a challenge and sends the challenge to the

user via a network (Guthrie, 10:39-46, 11:21-25), and the network can be an Internet network (*id.*, 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; *see also* Veneklase, 1:25-38 (teaching Internet communication systems “have been especially prone to unauthorized ‘break-ins’, viral destruction, and/or unauthorized data modifications.”); Kaufman, 3:9-25 (teaching password sent from a workstation for accessing a distributed system can be eavesdropped and used by an imposter). 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.

65. *Second*, a person of ordinary skill in the art would have recognized that maintaining Guthrie’s never-transmitted secret password (i.e., SADB password), unlike Sormunen’s authentication data that is all transmitted over one network or another, would result in a combined system more secure than Sormunen alone. In Sormunen, an unauthorized user could obtain Sormunen’s mobile station and dynamic password to access the secure system. Odagiri, [0004], [0038] (teaching 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 to Sormunen's mobile station) and a secret password (not transmitted) to generate the response. This ensures that an unauthorized user who obtains possession of the mobile station and challenge cannot access the secured system so long as the unauthorized user does not know the user's secret password. *See* Bosen 2:26-31, 4:44-49 (teaching 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 that is easily customized for each user of the system); Falk, 4:32-45 (teaching triple checking the identity of the user by requiring information from three sources, including 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).

66. *Third*, using Sormunen's s mobile station to request and receive Guthrie's challenge would further improve security by additionally verifying the user based on a personal communication device possessed by the user. 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. *See* Guthrie, 1:25-29; Kato, [0003]; Kaufman, 2:8-12. Using Sormunen's mobile station to obtain Guthrie's challenge allows for a request for the challenge to be sent from a mobile station known to be associated with the user

(e.g., by a telephone number). This allows Guthrie's server to identify the user based on the telephone number associated with the mobile station in addition to the user account ID. Sormunen, p. 4, ll. 30-33 (teaching SMS messages are sent based on a telephone number), p. 9, ll. 28-32 (teaching giving a telephone number of the mobile station is used to identify the user); Ueshima, Abstract, 16:13-20, 10:20-29, FIG. 3 (teaching registering a user's telephone number in a register table and 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 (teaching identifying a user based on a wireless remote communication device having a unique number); Falk, 4:32-45 (teaching triple checking the identity of the user by requiring information from three sources, including 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); Turtiainen, 8:1-53 (teaching identifying a user based on user information associated with a mobile station used as a personal authentication device). 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 (i.e., SADB 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 provides.

b. Reasonable Expectation of Success

67. In my opinion, a person of ordinary skill in the art 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 sending short messages in the same way as Sormunen. 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 by using ISDN connection. Sormunen, p. 8, ll. 15-18. Thus, 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.*

68. A person of ordinary skill in the art 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 and hashing algorithm 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 and hashing algorithm and then having the user enter the resulting response on Guthrie's client. Both implementations would be obvious because both provide the security benefit of requiring manual entry of authentication data. Guthrie, FIG. 9A, 7:29-34 (the user can enter the challenge into the client SADB calculator manually), 12:57-60 ("[T]he user's authentication password must be entered interactively. As a result, human interaction in the authentication process is required.").

69. In the first potential implementation, a person of ordinary skill in the art 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.

70. In the second potential implementation, a person of ordinary skill in the art would have had a reasonable expectation of success because he or she

would have understood that Sormunen's mobile station is capable and ready for implementing Guthrie's client SADB calculator or secured hashing algorithm ("SHA"). *First*, 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 person of ordinary skill in the art would have understood that a "palm top computer" is a mobile computer similar to Sormunen's mobile station (Odagiri, [0038], [0046]-[0047]; Ueshima, 4:1-4, 9:14-22; Oberhaus, 1:21-23), and that mobile stations, such as mobile phones, were known to perform hash algorithms. Falk, 3:4-20, 4:19-45. Guthrie also teaches that its 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). Thus, a person of ordinary skill in the art would have understood that Guthrie's SADB calculator would be readily implemented in Sormunen's mobile station as a software application.

B. Independent Claims

1. Claim 1

71. In my opinion, Guthrie in view of Sormunen renders obvious 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:”**

72. In my opinion, Guthrie discloses 1[preamble].

73. The '658 Patent provides no definition of a secure computer network, but the relevant portions of the specification explain that a secure computer network is simply a “secure system” accessible over a network. Ex. 1001, Abstract, 4:20-26. The specification explains that 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, by encryption or other means, but is limited to securing the computer system by restricting access to only users that enter a valid password.

74. Like the '658 Patent, Guthrie discloses “[a] *method of authenticating a user*”³ because it discloses “[a] personal authentication system [that] provides at

³ Claim language in italics throughout.

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.

75. Guthrie discloses “*a first secure computer network*” because Guthrie discloses *securing* the server on the computer network by restricting access to only users who have established an account with the server and entered a valid response to a challenge generated by the server. *Id.*, 5:43-47, 11:60-64.

76. 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 and response process based on data exchanged between a client computer and a server computer, both coupled to a computer network. *Id.*, 4:50-5:15, 5:22-27, 16:33-37.

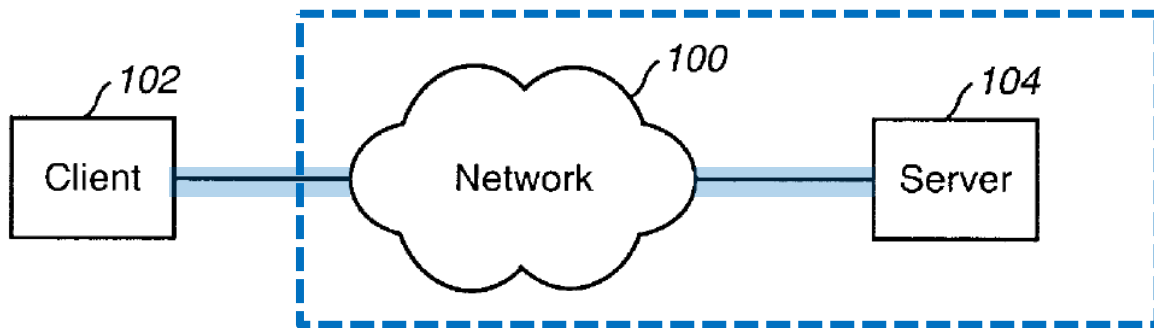


FIG. 1A

Id., FIG. 1A.

77. 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; *see also id.*, 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.

- 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;”**

78. In my opinion, Guthrie in view of Sormunen renders obvious 1[a].

79. 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.

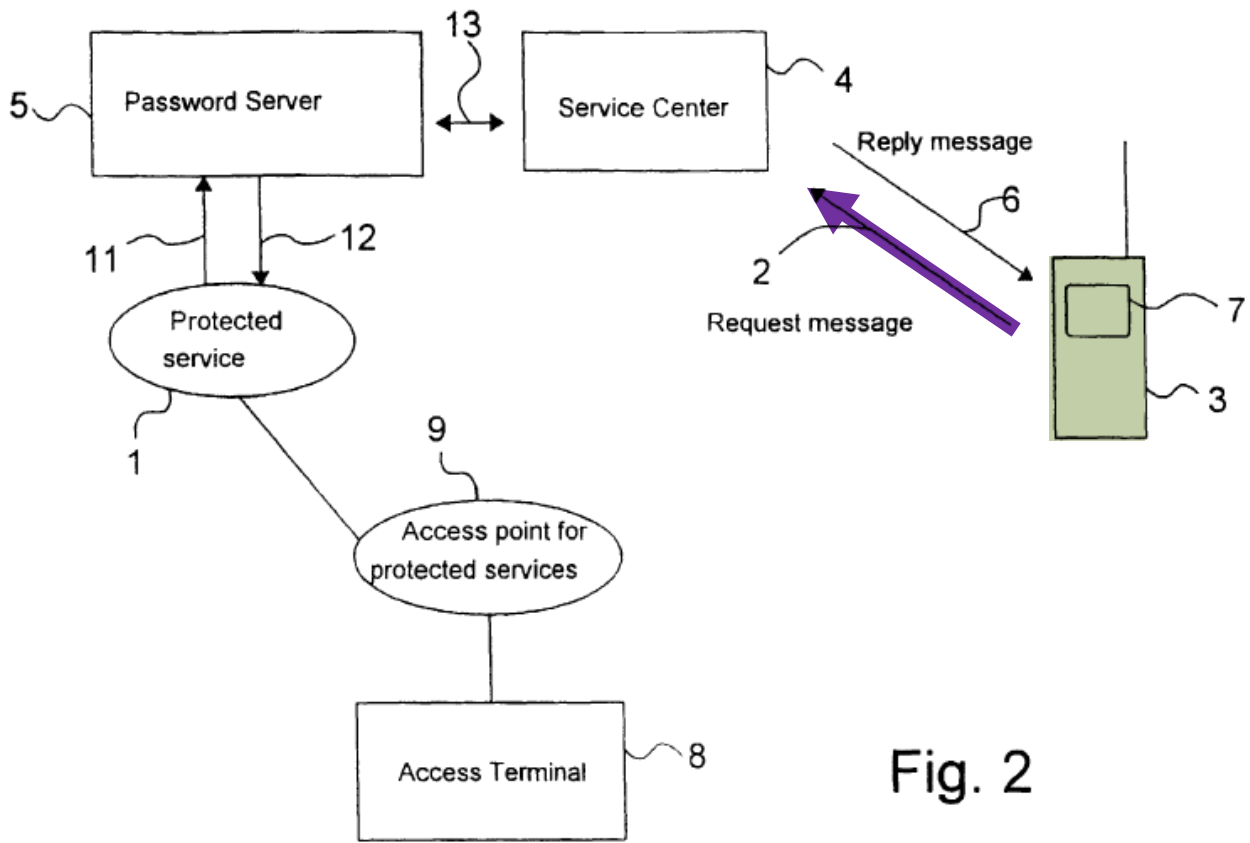
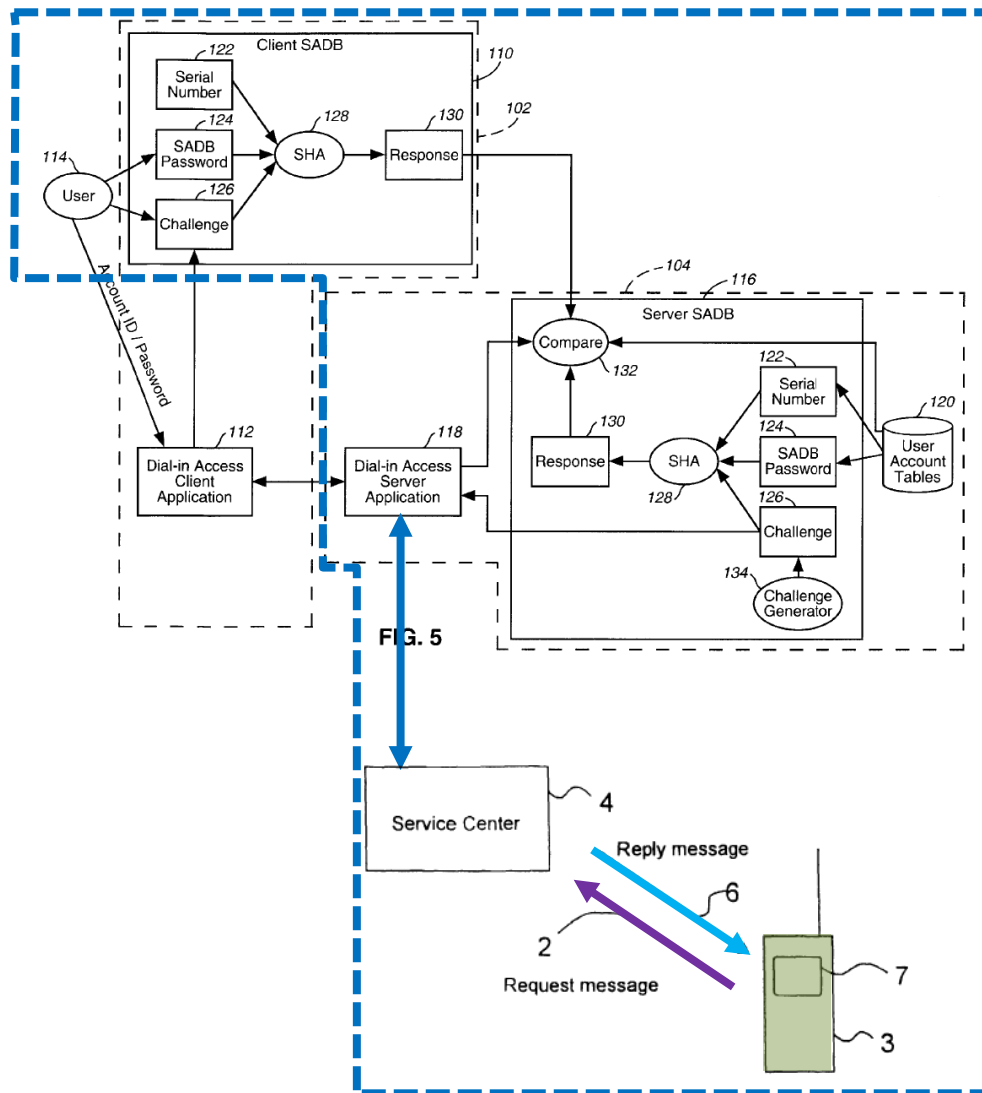


Fig. 2

Sormunen, FIG. 2.

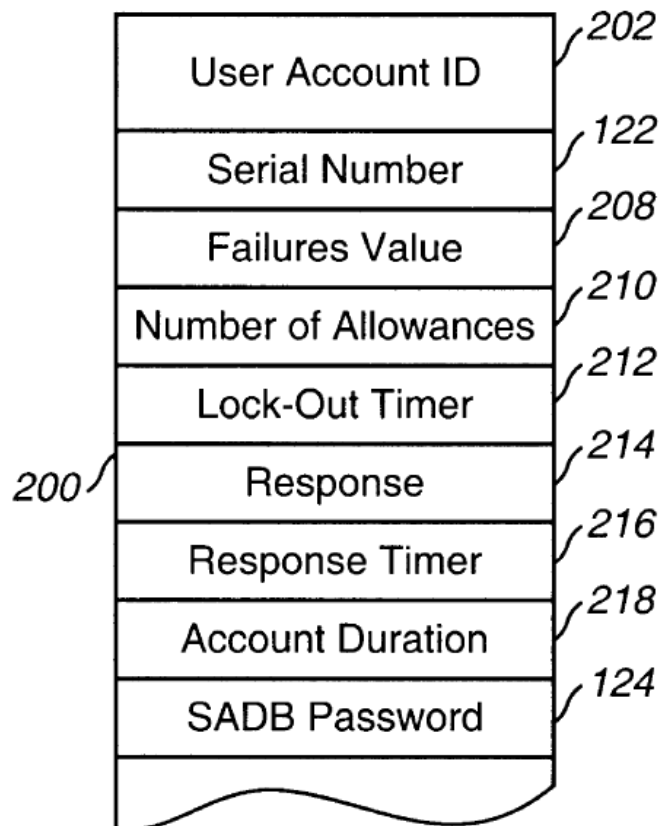
80. As combined, a person of ordinary skill in the art would have understood that Sormunen's mobile station is in communication with a cell phone network ("*second network*") that is different from Guthrie's secured computer system ("*first secure computer network*").

81. A person of ordinary skill in the art would have understood that the combination of Guthrie and Sormunen would transmit the **challenge request** and the responsive **challenge** in short messages between Sormunen's mobile station and Guthrie's server, as shown in the following combined figure.



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

82. Guthrie discloses storing account information, shown in account table 200 in Figure 6 below, in a user account database 120. Guthrie, 5:35-47, 7:64-8:6.

**FIG. 6**

Id., FIG. 6.

83. Guthrie's server's user database, as combined with Sormunen, would have been understood by a person of ordinary skill in the art 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 message with a challenge to the correct mobile station possessed by the user. *Second*, a person of ordinary skill in the art

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. *See* Kato, [0008]-[0009]; Bulfer, 3:1-18; Falk, 4:32-45, 5:4-7; *see above* Section VIII.A.

84. A person of ordinary skill in the art 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 adding one more field for storing the user's telephone number in Guthrie's account table 200 in Figure 6 and comparing two sets of telephone numbers, similar to Guthrie's storing and comparison of the user's password and account ID.

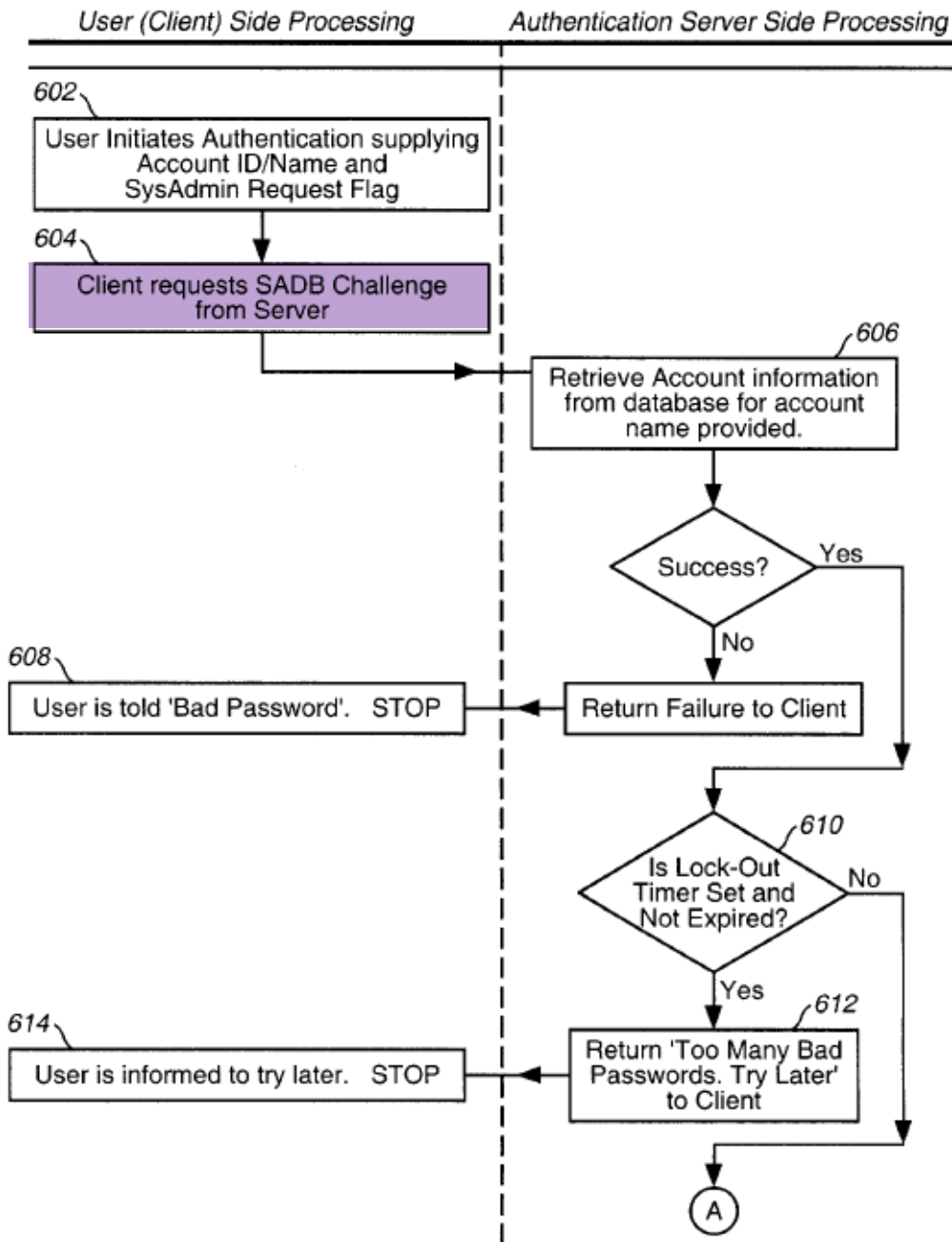
c. 1[b]: "receiving a request from the user for a token via the personal communication device, over the second network;"

85. In my opinion, Guthrie in view of Sormunen renders obvious 1[b].

86. 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 person of ordinary skill in the art 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"*).

87. 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. Guthrie's challenge is "an initial seed value" generated by the server. *Id.*, 4:18-19. The challenge is "randomly generated" and "may be a string of eight alphanumeric characters or digits." *Id.*, 6:57-64.

**FIG. 7A**

Guthrie, FIG. 7A.

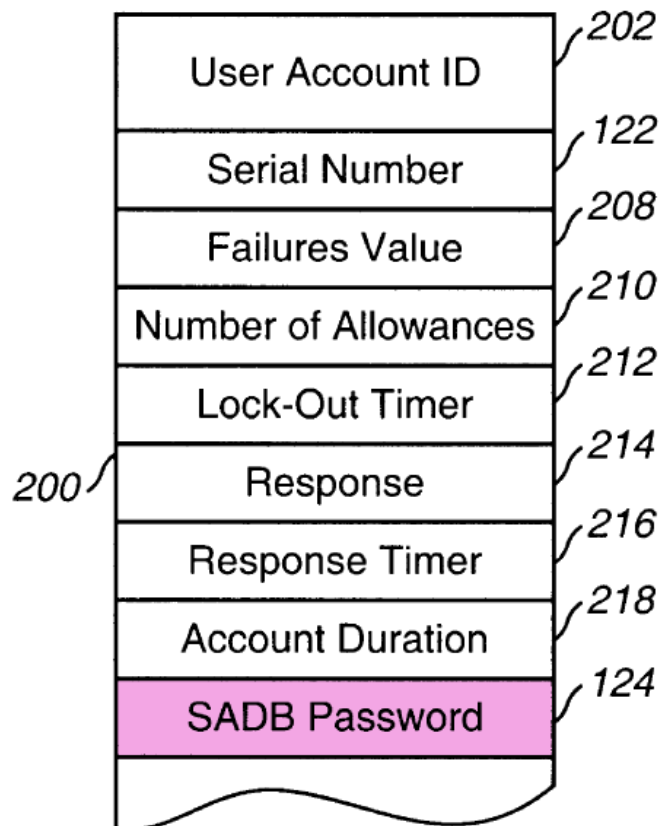
88. In my opinion, a person of ordinary skill in the art would have been motivated to implement Sormunen's mobile station and request for authentication

data from the mobile station in Guthrie to add additional security in identifying the user before sending the user the challenge and would have had expectation of success for this modification, as explained in Section VIII.A.

- 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;”**

89. In my opinion, Guthrie discloses 1[c].

90. 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 in account table 200 in Figure 6 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*”).

**FIG. 6**

Guthrie, FIG. 6.

91. After verifying the user's account information (step 656 in Figure 7D), Guthrie's server generates an eight digit or character challenge value ("token"). Guthrie, 10:39-46. In the next step (step 658 in Figure 7D), 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"). Guthrie, 10:46-50.

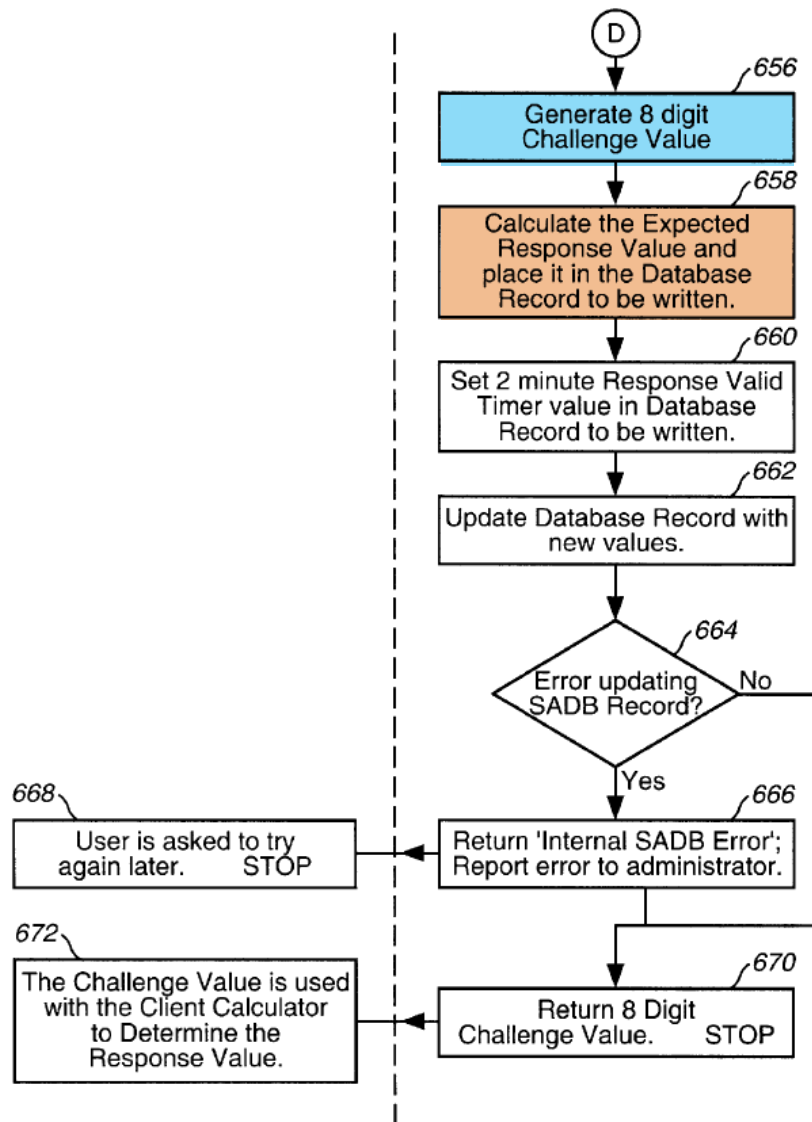
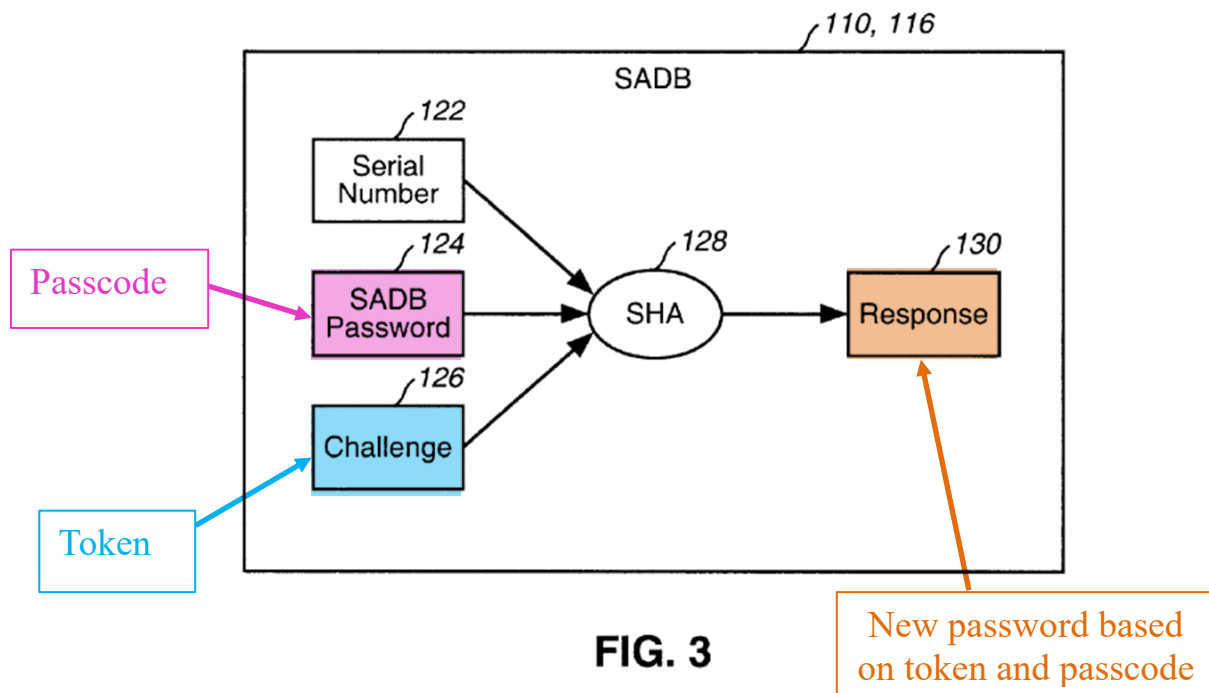


FIG. 7D

Guthrie, FIG. 7D.

92. 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).



Guthrie, FIG. 3.

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

93. In my opinion, Guthrie discloses 1[d].

94. 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.

95. In steps 658 and 662 of Figure 7D, Guthrie discloses that its server updates and writes the expected **response** value ("*new password*") into a response record in the user's table 200 ("*setting a password associated with the user*"). Guthrie, 10:56-58.

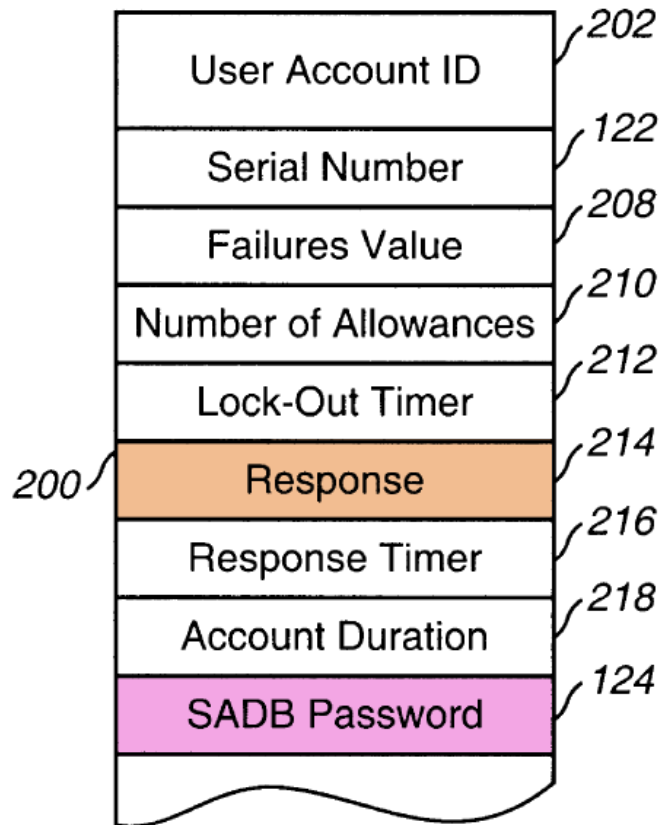
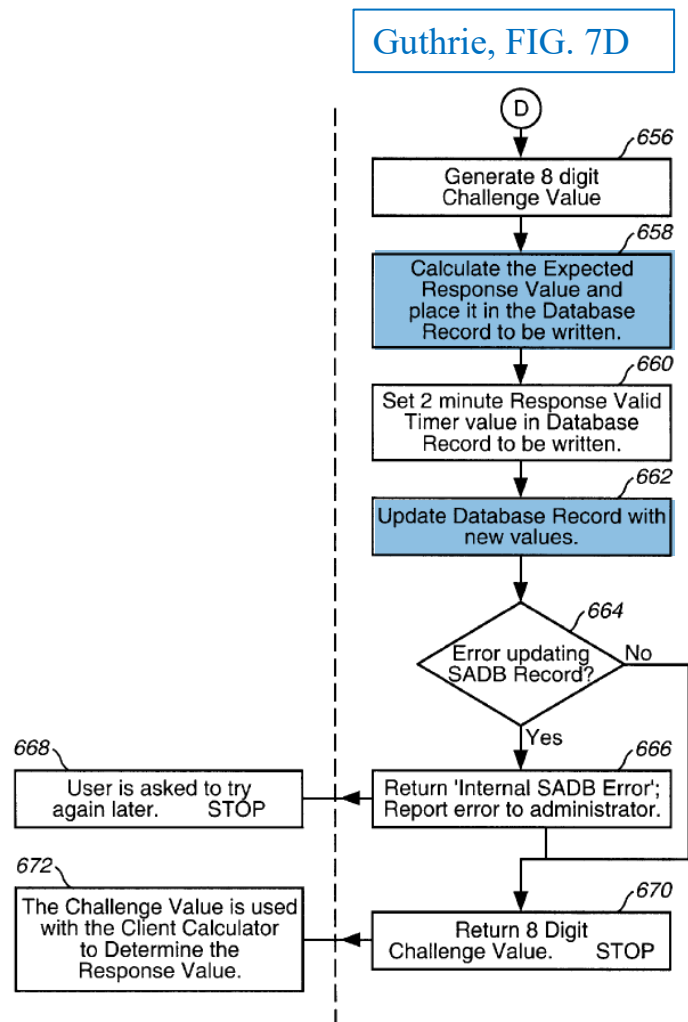
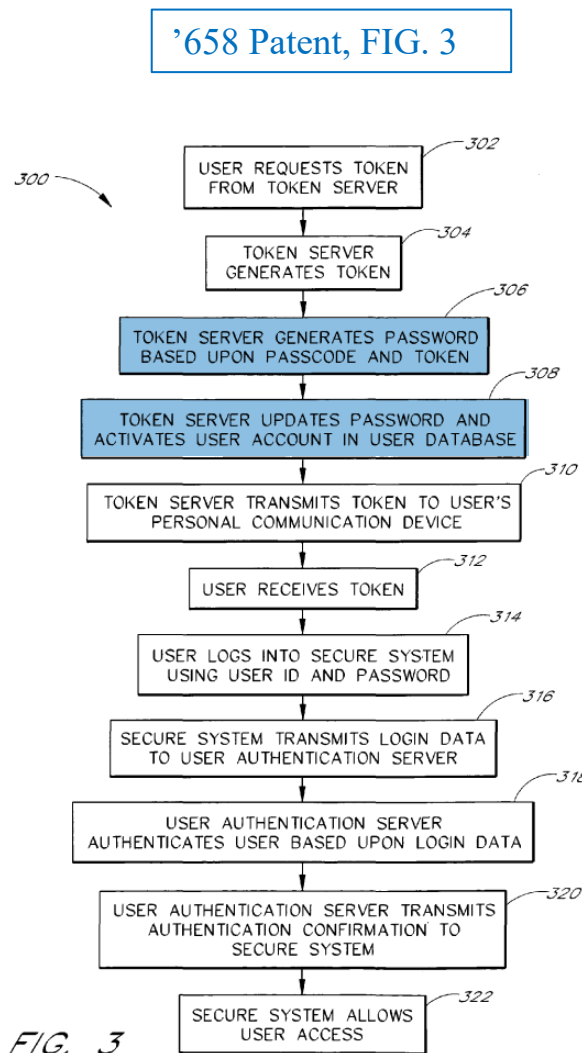


FIG. 6

Guthrie, FIG. 6.

96. This is similar to the '658 Patent's steps 306 and 308 where the token server updates the user database with the generated new password. Ex. 1001, 6:59-67.



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

97. In my opinion, Guthrie discloses 1[e].

98. 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.

99. In step 660 of Figure 7D, Guthrie discloses setting a response valid timer with the generation of a challenge and response. Guthrie, 10:50-55. The response valid timer value is written into a response timer record of the user account table. *Id.*, 10:55-58. A person of ordinary skill in the art 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.

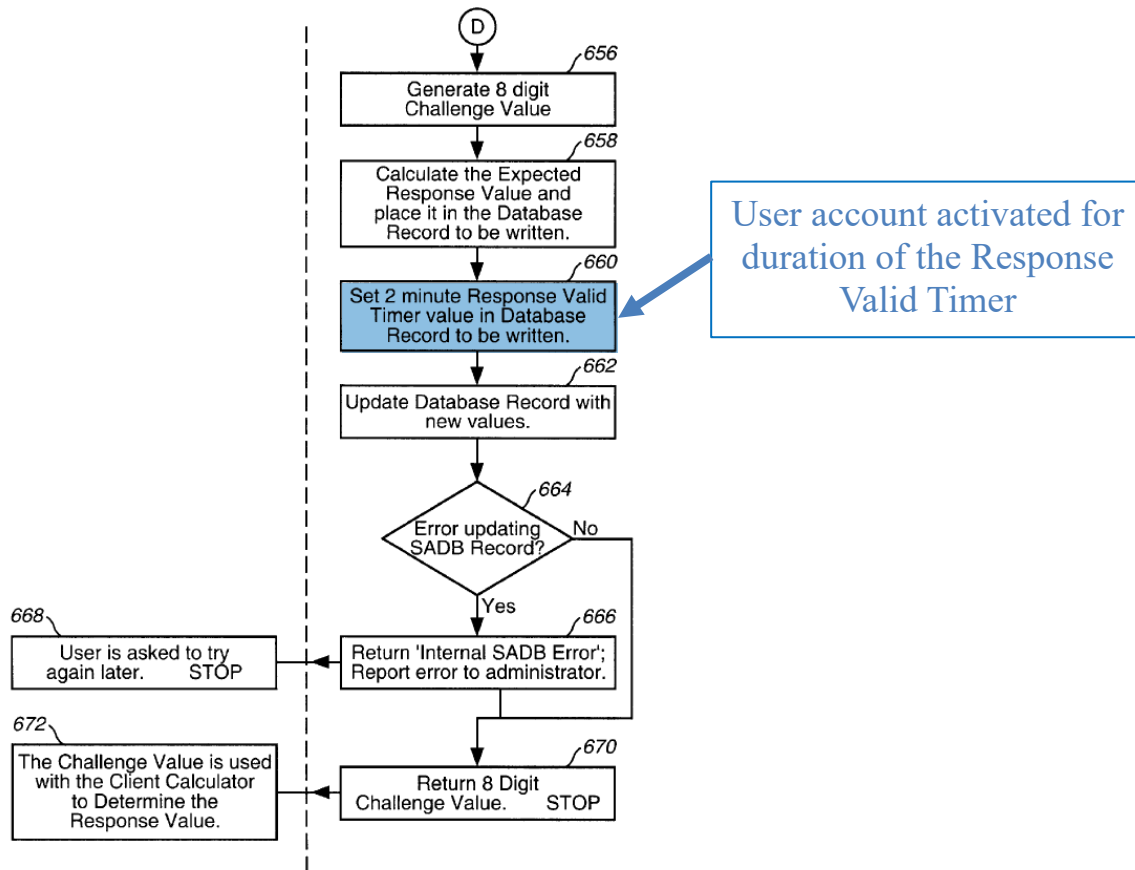


FIG. 7D

Guthrie, FIG. 7D.

100. 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. A person of ordinary skill in the art would have understood that Guthrie’s matching the

received response to the expected response is also activating access because Guthrie expressly states that appropriate access is enabled in this circumstance.

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

101. In my opinion, Guthrie in view of Sormunen renders obvious 1[f].

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

103. In Figure 2, Sormunen discloses that a 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.

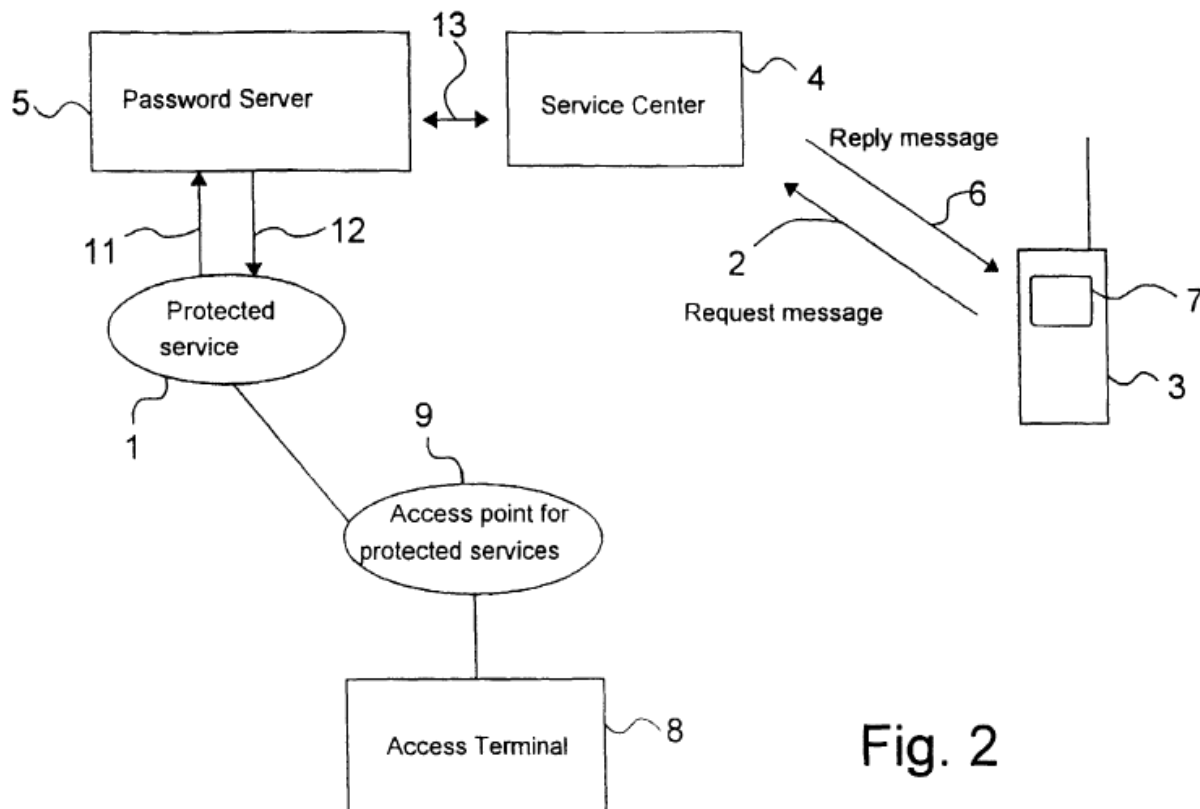
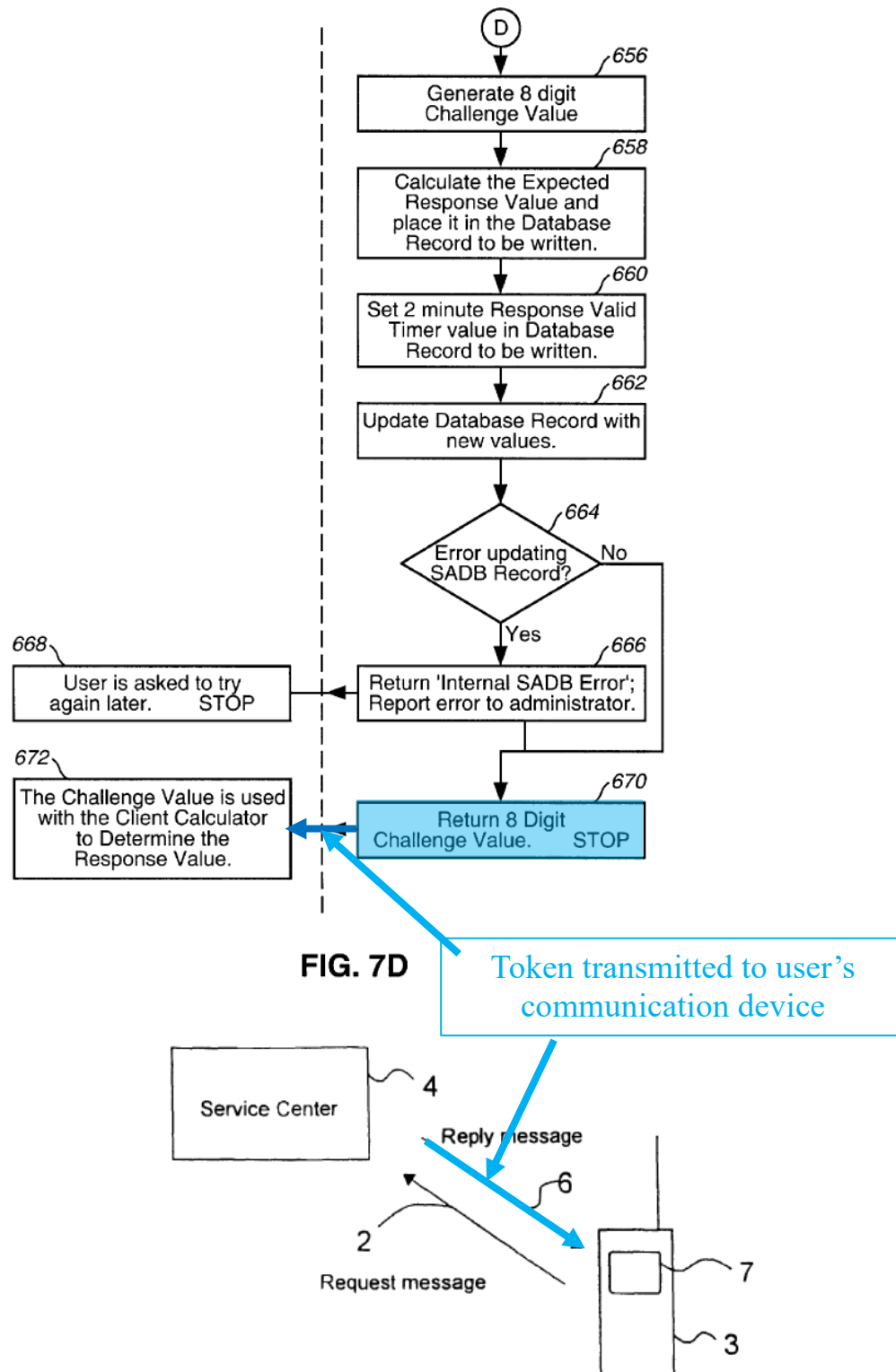


Fig. 2

Sormunen, FIG. 2.

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



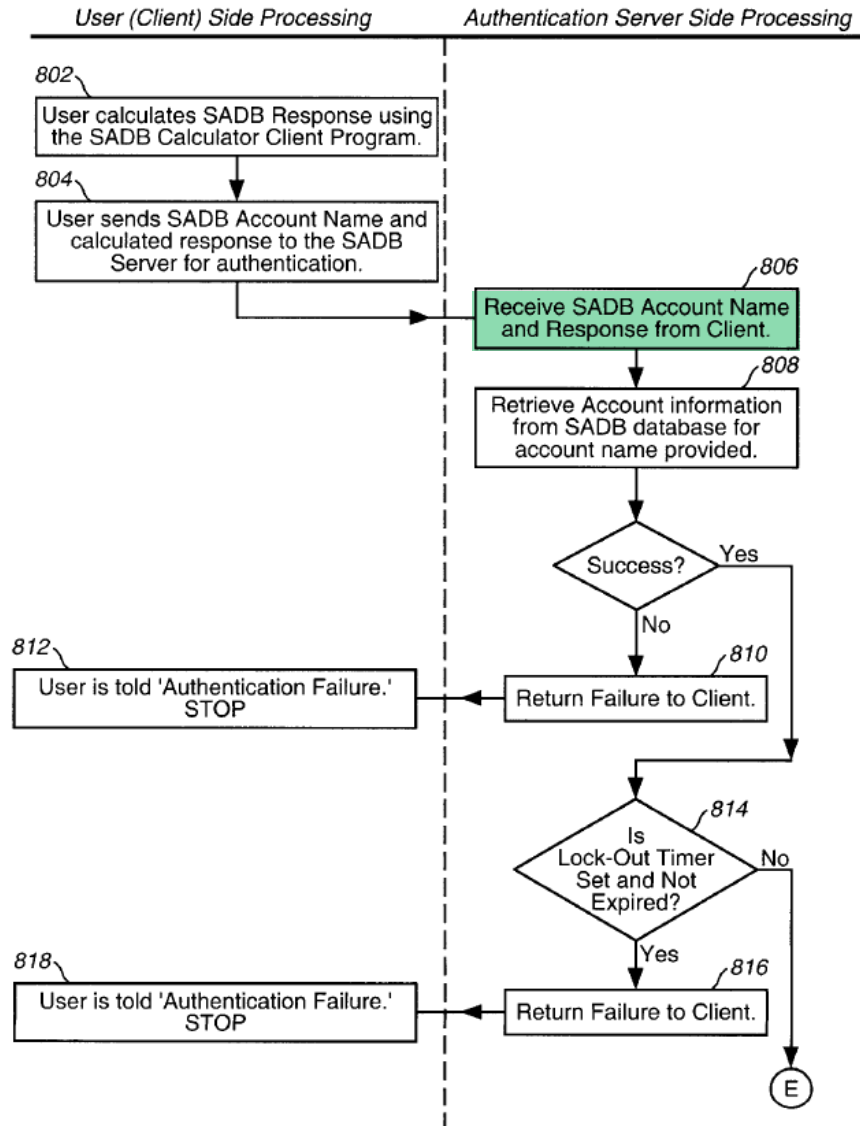
Guthrie, FIG. 7D; Sormunen, FIG. 2 (excerpted).

105. In my opinion, a person of ordinary skill in the art 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 VIII.A.3.

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

106. In my opinion, Guthrie discloses 1[g].

107. In steps 802-806 of FIG. 8A, 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*" (as described in 1[preamble])). Guthrie, 6:65-7:6, 7:27-44, 11:27-35; *see above* Section VIII.B.1.a.

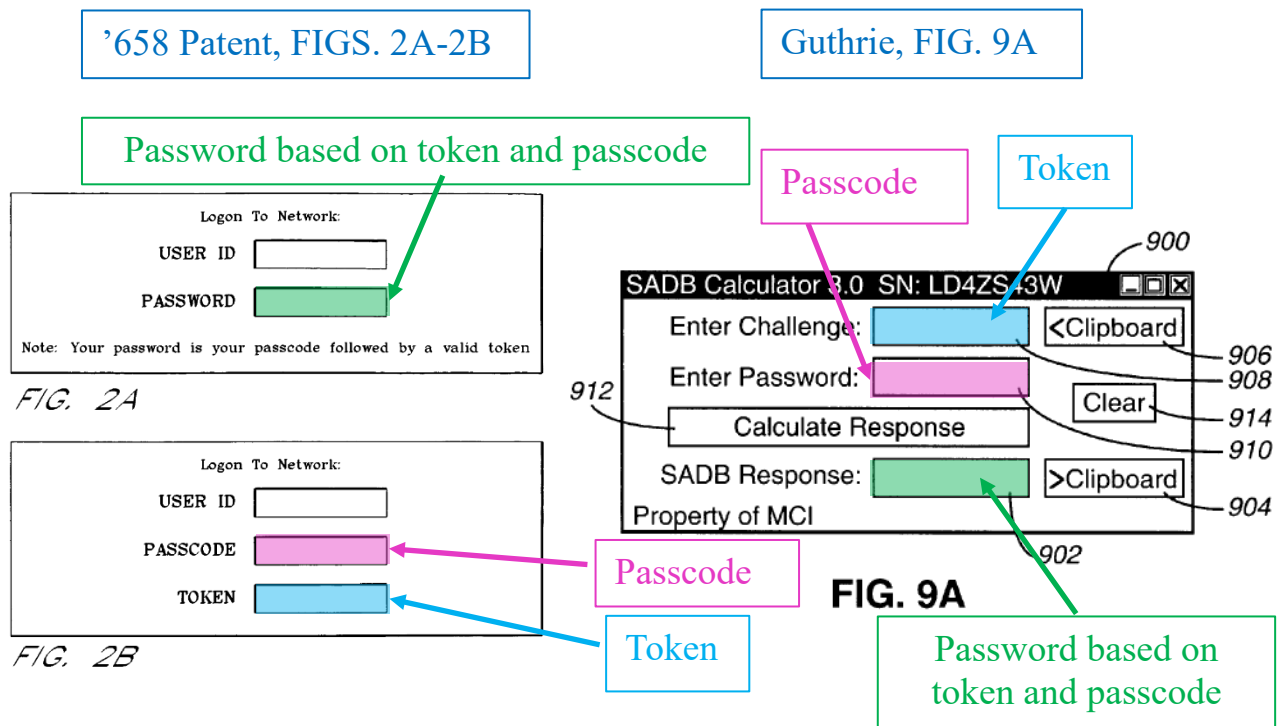
**FIG. 8A**

Guthrie, FIG. 8A.

108. In Guthrie combined with Sormunen, the 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 VIII.A.1.

109. As shown below, in the first proposed combination, a person of ordinary skill in the art 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.



110. In the second proposed combination, a person of ordinary skill in the art would have understood that the user would receive the challenge in a reply message from the server at the mobile station, 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 provided by Guthrie's client to transmit to Guthrie's server. Guthrie, 7:29-38, 12:57-60 ("[T]he user's authentication password must be entered interactively. As a result, human interaction in the authentication process is required.").

- 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.”**

111. In my opinion, Guthrie discloses 1[h].

112. Guthrie discloses deactivating access after two minutes of activating if the expected response is not received at the server. Guthrie, 10:50-55, 11:50-59.

113. In step 660 of Figure 7D, 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 person of ordinary skill in the art 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 current 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.

2. Claim 5

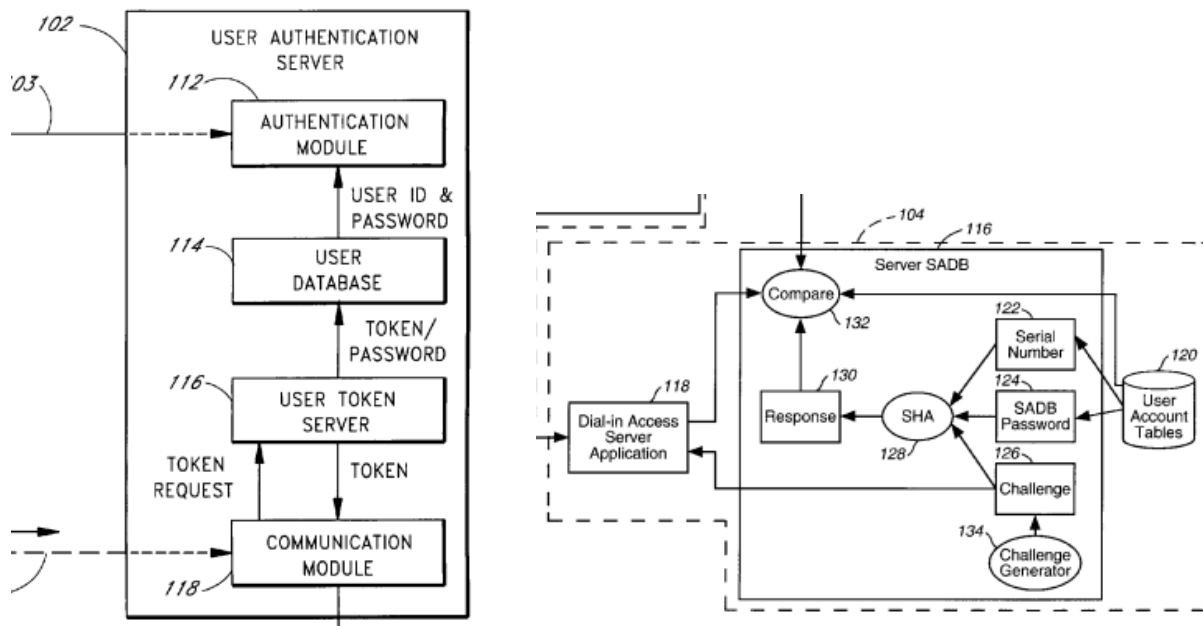
114. Independent claim 5 is substantially similar to claim 1 but styled as a system claim implementing routine hardware and software components. Claim 5 also is broader than claim 1 because it does not expressly require “*receiving a request from the user for a token via the personal communication device,*”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

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

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

116. In my opinion, 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.

117. 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).



Compare Ex. 1001, FIG. 1 (excerpted, left), with Guthrie, FIG. 5 (excerpted, right).

b. 5[a]: “a computer processor;”

118. In my opinion, Guthrie discloses 5[a] because it discloses that the response calculators are implemented in computer systems, such as a client computer and a server computer and require a center processing unit (“CPU”).

Guthrie, 2:57-67, 4:14-16, 4:50-57. A person of ordinary skill in the art would have understood a CPU of a computer system for implementing Guthrie's response calculator is "*a computer processor.*"

- c. **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;"**

119. In my opinion, Guthrie in view of Sormunen renders obvious 5[b]. 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.*" See above Section VIII.B.1.b.

120. 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 person of ordinary skill in the art 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 person of ordinary skill in the art would have had a reasonable expectation of success in this modification, as explained in 1[a]. *See above* Section VIII.B.1.b.

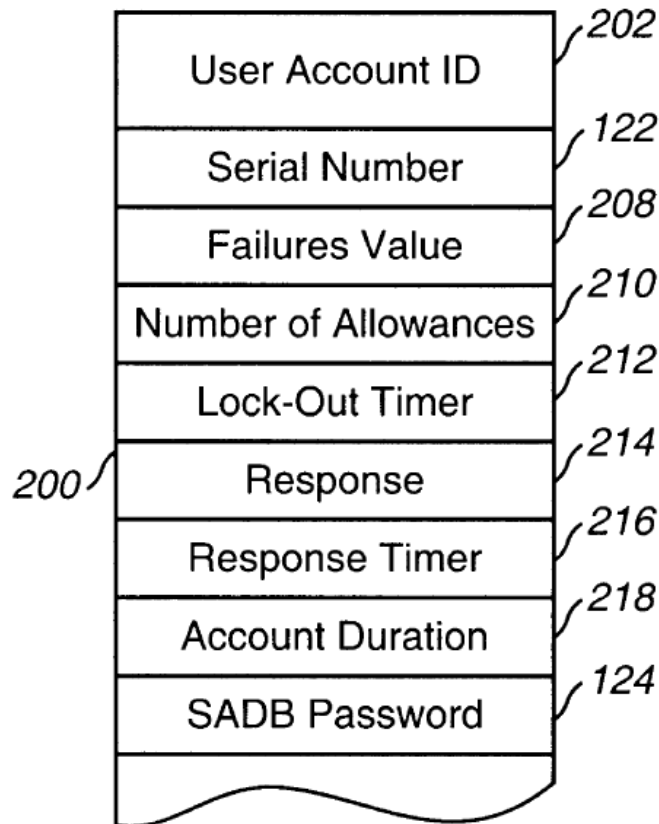


FIG. 6

Guthrie, FIG. 6.

121. Also, in my opinion, a person of ordinary skill in the art 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. *See above* Section VIII.A.3.

- d. 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,"**

122. In my opinion, Guthrie discloses 5[c] for the reasons 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]. *See above* Sections VIII.B.1.d, VIII.B.2.b.

123. 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).

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

124. In my opinion, Guthrie discloses 5[d] for the reasons 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]. *See above* Sections VIII.B.1.e, VIII.B.2.b.

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

125. In my opinion, 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*”). Guthrie, 5:22-35

(disclosing various “methods and/or apparatuses for establishing communications between the client 102 and server 104”); 13:48-53 (disclosing the dial-in application forming connections over ISDN lines); *see above* Section VIII.A.3.

126. 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 ...*”).

- g. 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,”**

127. In my opinion, Guthrie discloses 5[f] for the reasons explained for 1[g]. *See above* Section VIII.B.1.h. Guthrie also discloses “*the user has an account on the secure computer network,*” for reasons explained for 1[preamble] and 1[a]. *See above* Sections VIII.B.1.a-VIII.B.1.b.

128. 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.

- h. 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.”**

129. In my opinion, Guthrie discloses 5[g].

130. Guthrie discloses that its authentication module “*activates access to the account,*” for reasons explained for 1[e]. *See above* Section VIII.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, 10:50-58, 7:38-45; Section VIII.B.1.f. Guthrie also

disclose 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]. *See above* Sections VIII.B.2.g, VIII.B.1.i.

C. Dependent Claims

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

131. In my opinion, 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*”). *See above* Section VIII.B.1.d. A person of ordinary skill in the art would have understood that to perform a hashing algorithm, the input password and challenge would first be concatenated.

132. 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 also known for improving security of transmission of user authentication data. *Id.*, Abstract (inhibiting password attempts by using a hashing algorithm upon a password and token); Reeds,

Abstract (teaching 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 (teaching concatenating number sequences and hashing the concatenated string to form a hashed authentication sequence).

133. 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 person of ordinary skill in the art 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 known and understood 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”). And 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.

134. Thus, a person of ordinary skill in the art 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.

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

135. In my opinion, 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 person of ordinary skill in the art 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 VIII.A.

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."

136. In my opinion, Guthrie discloses claim 6 for the reasons 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]. *See above* Sections VIII.B.1.c-VIII.B.1.d, VIII.B.2.d, VIII.B.2.f.

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

137. In my opinion, Guthrie in view of Sormunen renders obvious claim 7 for the reasons explained in 1[b]. *See above* Section VIII.B.1.c. In my opinion, a person of ordinary skill in the art would have been motivated to implement Sormunen’s request from a mobile station in Guthrie to request the challenge to add additional security in identifying the user before sending the user the challenge and would have had an expectation of success for this modification, as explained in Section VIII.A.

IX. GROUND 2: KATO IN COMBINATION WITH GUTHRIE RENDERS OBVIOUS CLAIMS 1-3 AND 5-7

138. In my opinion, Kato in view of Guthrie renders obvious claims 1-3 and 5-7.

A. Kato-Guthrie Combination

1. Summary of the Kato-Guthrie Combination

139. Kato and Guthrie are in the same field of endeavor and address the same problem—restricting access to a secure computer system using an authentication method. But the two do so in different ways that independently improve the security of a computer system. Accordingly, a combination of these improvements would greatly improve the security of the computer system because the advantages compound. Kato discloses a three-device architecture in which a

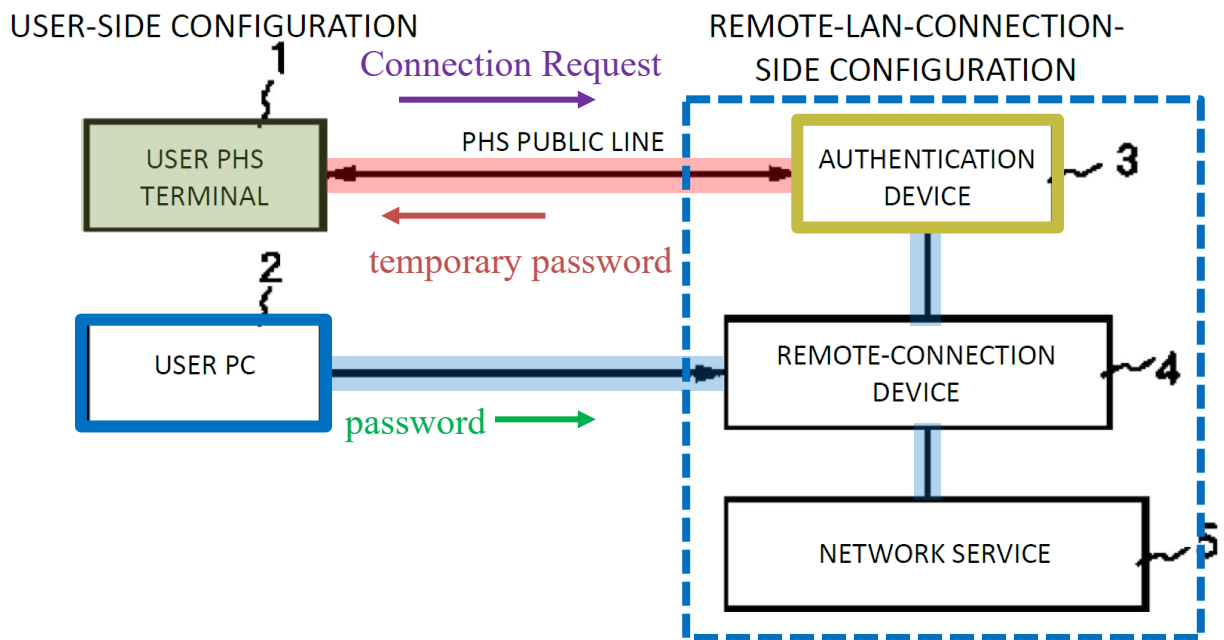
user has both a PC (a first device through which the user will access the secure computer network—a third device) and a PHS mobile device (a second device through which the user will receive a temporary password to enter on the PC).

140. 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 the security of Kato’s system because it adds the improved security of having multiple codes to the improved security of using multiple devices.

2. Kato and Guthrie are Analogous Art and Combinable

141. Like the '658 Patent, Kato discloses a user authentication system and method of authenticating a user to gain access to a networked computer system based on a temporary one-time password. Kato seeks to achieve the advantage of a one-time password without requiring users to obtain special hardware that can perform complex actions to obtain such a password. Kato, [0002], [0004], [0008]-[0009]. The user’s **portable telephone** contacts an **authentication device**. The authentication device provides the portable phone with a **temporary password** that will permit the user’s PC to access the desired network service. *Id.*

FIG. 1



Id., FIG. 1.

142. In detail, to obtain the temporary password, the user sends a connection request to the authentication device 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 and unrelated to the authentication-device password that the user provided to the authentication device.

Id. After receiving the temporary password, the user submits the temporary password to the remote-connection device via his PC. *Id.*, [0019]-[0020]. The remote-connection device asks the authentication device if the submitted temporary password is the correct one, permitting access to the desired network services if they match. *Id.*

143. But Kato authenticates the user to the network computer system with only a single temporary password generated at the authentication 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, in my opinion, a person of ordinary skill in the art would have looked to other references that use additional methodologies that prevent exposure of the entire password—like Guthrie.

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

145. Kato and Guthrie are in the same field of user authentication technologies and address the same problem of regulating a user's access to a secured computer system identified in 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 in

ways that have 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.

146. Like the '658 Patent, both references disclose solutions for these problems by implementing authentication based on two levels of security—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, 7:1-10. For these reasons, Kato and Guthrie are analogous art to the '658 Patent, and a person of ordinary skill in the art would have found it obvious to combine them.

3. A person of ordinary skill in the art Would Been Motivated to Add Guthrie's Challenge-Response Process to Kato's Three-Device Architecture and Would Have Had a Reasonable Expectation of Success in Doing So

a. Motivation

147. In my opinion, a person of ordinary skill in the art 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 the security of the system 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.

148. A person of ordinary skill in the art would have been motivated to incorporate Guthrie's challenge-response process into Kato's architecture to enhance security of Kato's authentication system 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 discloses generating 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). Guthrie, 4:39-41, 6:14-21, 6:57-64. Incorporating Guthrie's challenge-response process into Kato's architecture would generate a challenge and an expected response calculated from the user password and challenge, where the user password is not transmitted, as well as 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 entered by the user and transmitted to the authentication device would not be able to extract the user's secret password. Indeed, one-way hashing algorithms are well known and commonly used for securely transmitting secret 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 (inhibiting password attempts by using a hashing algorithm upon a password and token).

149. A person of ordinary skill in the art would realize the advantages of incorporating Guthrie's challenge-response process into Kato's architecture, in place of Kato's temporary password. 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. *See* 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. Incorporating Guthrie's teachings into Kato would require the user to use both the challenge (transmitted to the mobile telephone) and a secret password (not transmitted) to generate the response. This ensures that 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, which need not be available on the mobile device. Nor could an eavesdropper make use of the overheard temporary password, since such an eavesdropper would not have access to all information required to create the correct response to the challenge. *See* Bosen, 2:26-31, 4:44-49 (teaching improving security by making the generation of authentic passwords dependent not only possession of a random challenge, but also on possession of confidential information that is easily customized for each user of the system); Falk, 4:32-45 (teaching triple checking the identity of the user by requiring information from three sources, including 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).

b. Reasonable Expectation of Success

150. In my opinion, a person of ordinary skill in the art would have had a reasonable expectation of success in implementing Guthrie's challenge-response process into 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.

151. *First*, Guthrie discloses that its 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 teaches the 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." Guthrie, 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." Guthrie, 3:59-4:3.

152. A person of ordinary skill in the art 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 via a remote-connection device 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 person of ordinary skill in the art would have understood that Kato's PC and Guthrie's client computer are both computers performing similar functions and that computers include processor and memory devices. A person of ordinary skill in the art would have recognized that Guthrie's client SADB calculator would have been implemented on Kato's PC as software for execution by the processor of Kato's PC using ordinary skill and yielded predictable results of expected responses.

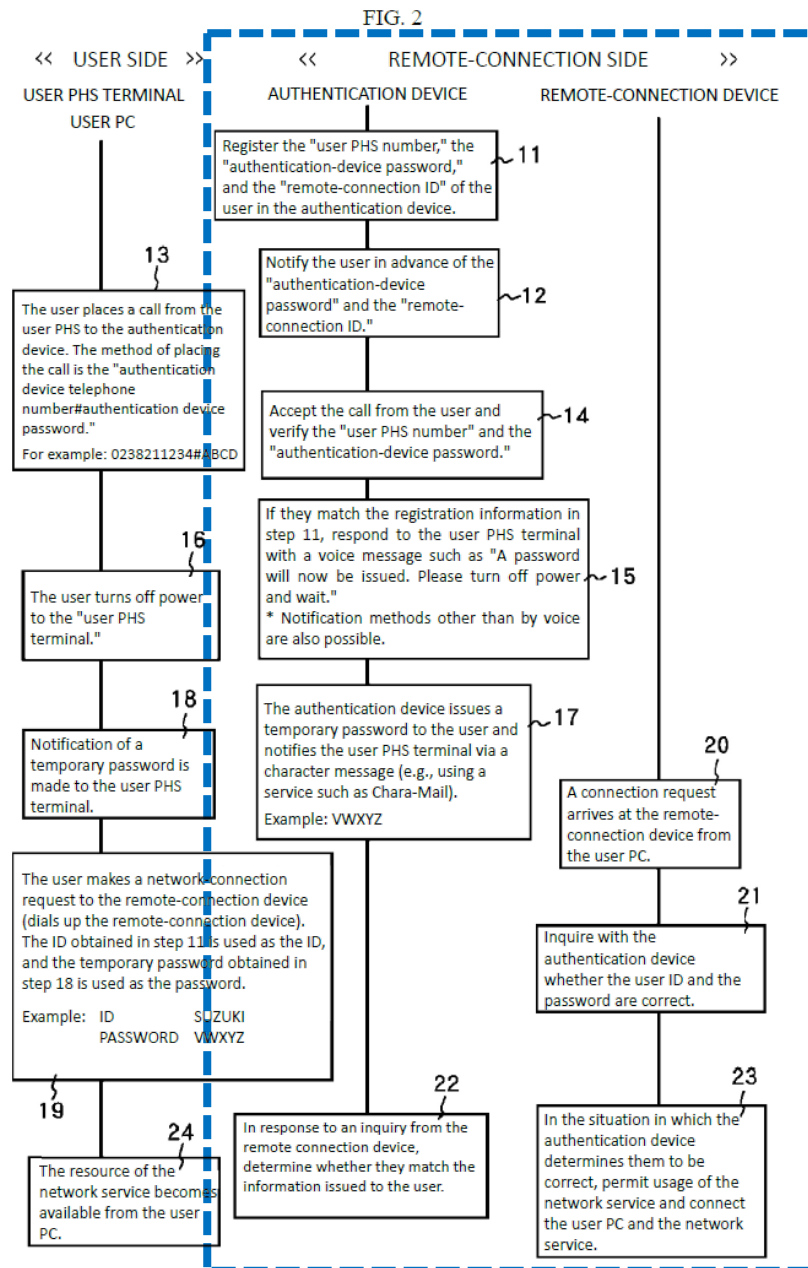
153. Alternatively, a person of ordinary skill in the art would have understood that Kato's PHS terminal would be modified using ordinary skill to implement Guthrie's client SADB calculator. A person of ordinary skill in the art would have understood that Kato's PHS terminal is a mobile device like a personal digital assistant ("PDA") and personal mobile computer (e.g., 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 a terminal for user authentication can be a PHS or a PDA with a telephone function); Oberhaus, 1:21-23 (“Examples of hand-held computing devices include pagers, mobile phones, personal digital assistants (PDAs), [and] palm-top computers”); *see also* Guthrie, 6:1-3. A person of ordinary skill in the art would have recognized that Guthrie’s client SADB calculator would be implemented on Kato’s PHS terminal as software for execution by the processor of the PHS terminal using ordinary skill to yield predictable results of the expected responses. Indeed, it was known that devices like Kato’s PHS terminal can perform encryption algorithms. Shields, p. 11 (teaching 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 (teaching using a cellular phone for calculating a response in a challenge-response process for user authentication); Turtiainen, 10:22-36 (teaching a mobile station calculates a response to a challenge according to a predefined algorithm based on the challenge and a secret).

154. Additionally, a person of ordinary skill in the art 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 person of ordinary skill in the art would have understood that these devices would include a processor, memory, and communication devices for performing functions like those of Guthrie's server calculator implemented on Guthrie's server. For example, 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 (e.g., 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.*, 7:74-8:6, 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). Thus, a person of ordinary

skill in the art 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.



Kato, FIG. 2.

155. Indeed, 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 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 person of ordinary skill in the art would have understood that Guthrie's server calculator, dial-in application, and database would be implemented on Kato's authentication device as software for execution by the processor of a computer using ordinary skill as taught by Guthrie and would yield predictable results.

156. Accordingly, a person of ordinary skill in the art 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. Indeed, a challenge-response process was well known and commonly implemented in various user authentication applications and systems. *See* Peters; Reeds; Bosen; Kaufman; *see also* Falk, 3:4-20; 4:19-45 (implementing a challenge-response process for user authentication using a cellular phone).

B. Independent Claims

1. Claim 1

157. In my opinion, Kato in view of Guthrie renders obvious 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:”**

158. In my opinion, Kato discloses 1[preamble].

159. As explained for Ground 1, the '658 Patent provides no definition of a secure computer network, but the relevant portions of the specification explain that a secure computer network is simply a “secure system” accessible over a network. Ex. 1001, Abstract, 4:20-26; *see above* Section VIII.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.*

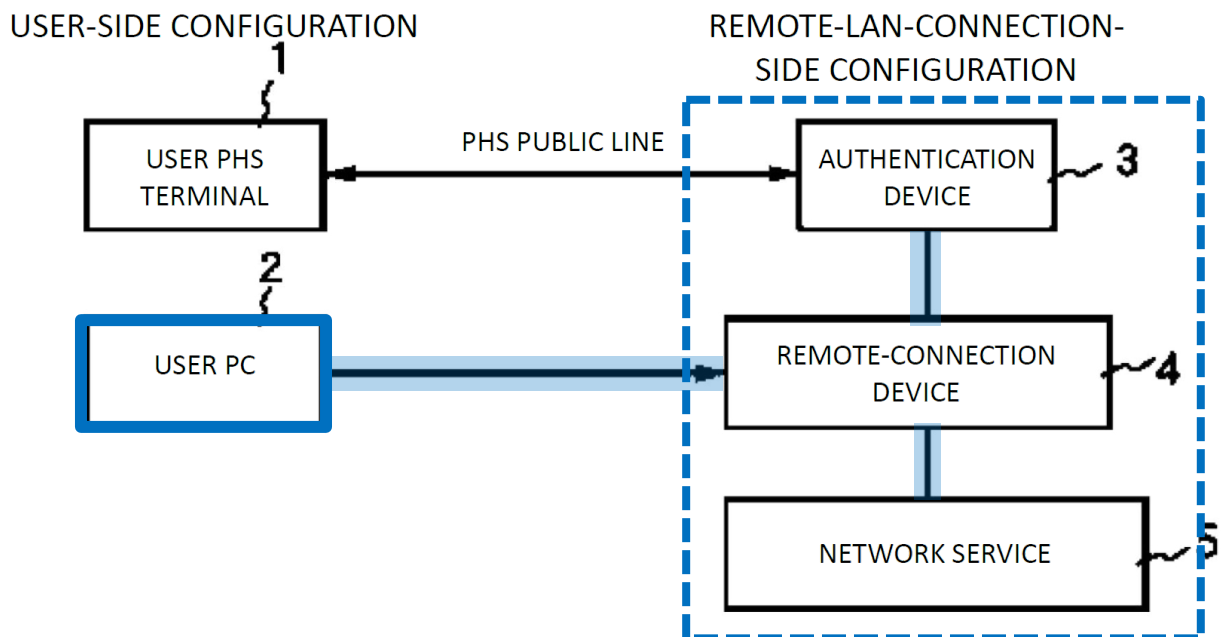
160. Kato discloses “[a] *method of authenticating a user*” because it discloses “an authentication system . . . , which, after verifying the validity of a user, permits usage of a resource of a network service from the user personal computer.” Kato, [0002], [0008].

161. 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

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](#). Kato, [0002], [0012].

FIG. 1



Id., FIG. 1.

162. 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].

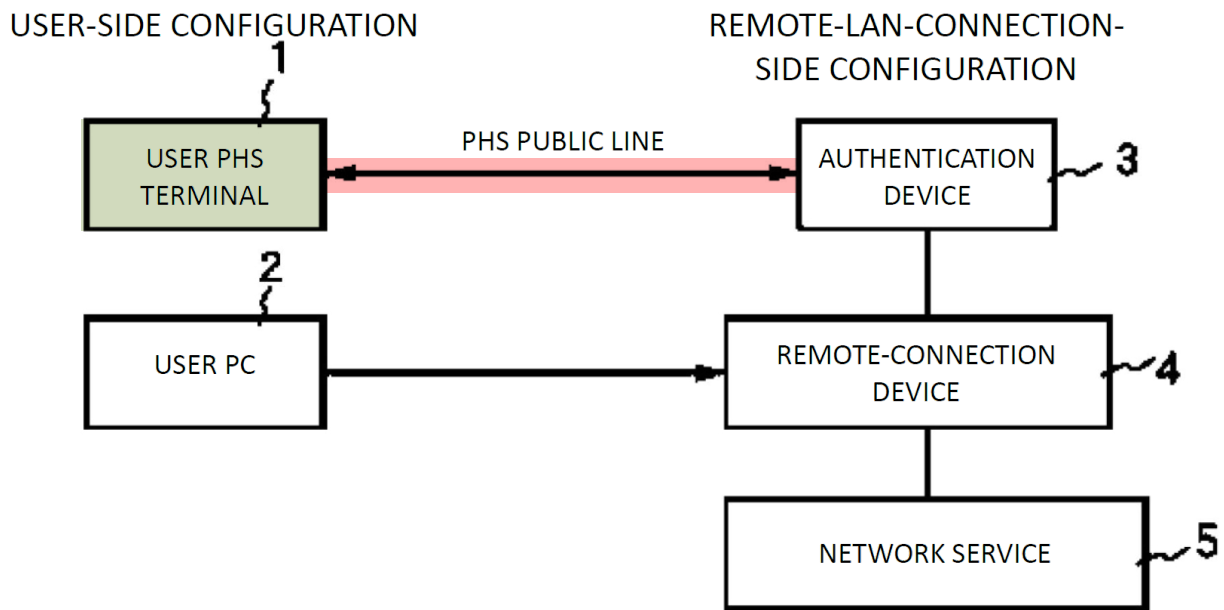
- b. 1[a]: “associating the user with a personal communication device possessed by the user, said personal communication device in communication over a second network, wherein said second network is a cell phone network different from the first secure computer network;”

163. In my opinion, Kato discloses 1[a].

164. 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].

165. 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 phone, in “**an international telephone utilization system**.” Kato, [0002], [0008], [0014]. A person of ordinary skill in the art would have understood that Kato’s mobile telephone is in communication with a cell phone network (“**second network**”) that is different from the secured computer system (“*first secure computer network*”).

FIG. 1



Id., FIG. 1.

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

166. In my opinion, Kato in view of Guthrie renders obvious 1[b].

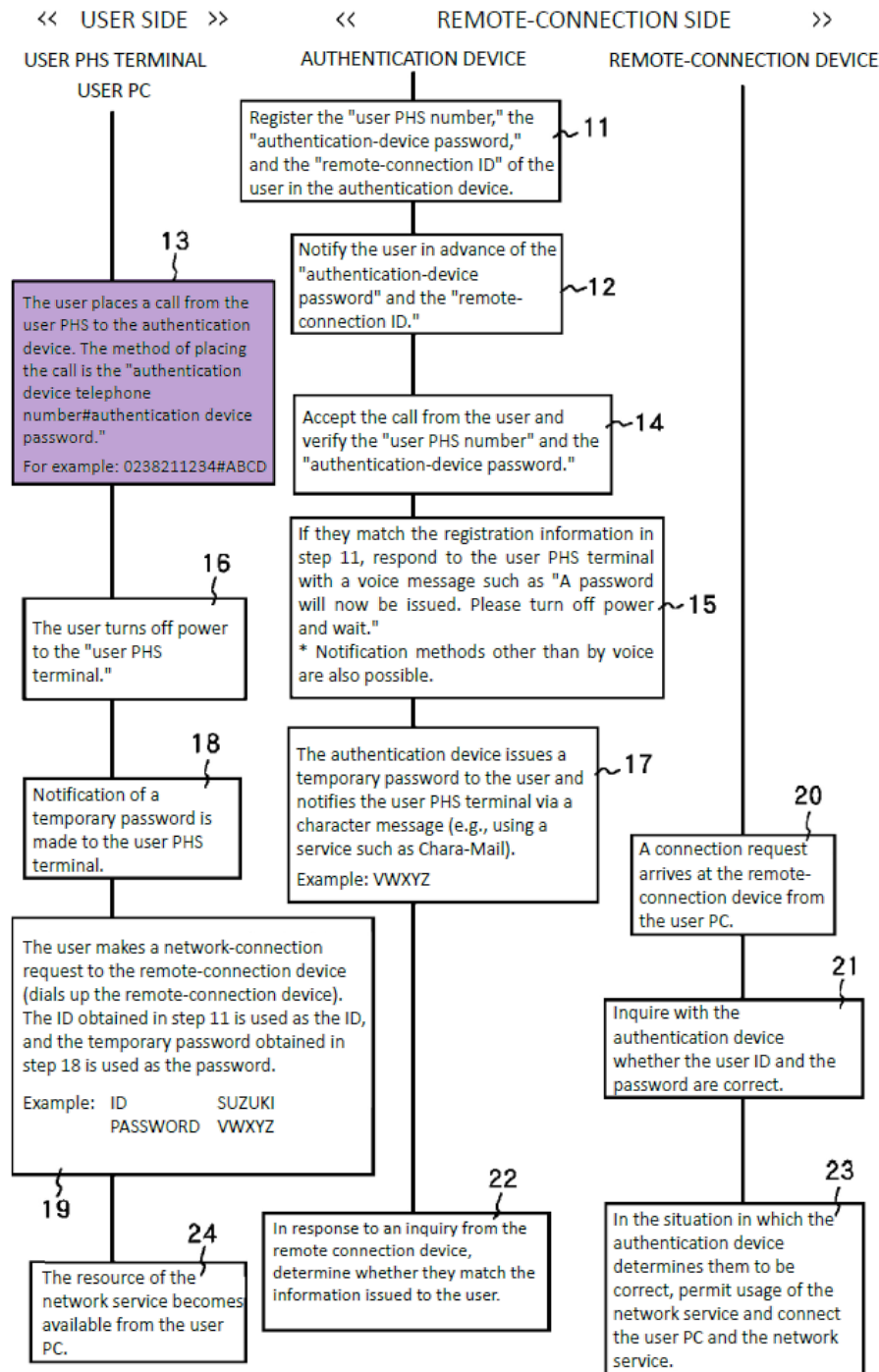
167. Kato discloses the architecture of sending a request from a user at a personal communication device over a second network. Guthrie discloses a request for a token. It would have been obvious to a person of ordinary skill in the art to request a token, as disclosed by Guthrie, within the architecture of Kato.

168. Kato’s Figure 2 discloses in 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].

FIG. 2



Id., FIG. 2.

169. 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 VIII.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 person of ordinary skill in the art to request a token (as disclosed by Guthrie) with Kato’s means for requesting a temporary password.

170. In my opinion, a person of ordinary skill in the art 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, so that Guthrie’s challenge-response process for generating Kato’s temporary password adds additional security and would have had an expectation of success for this modification, as explained in Section IX.A.

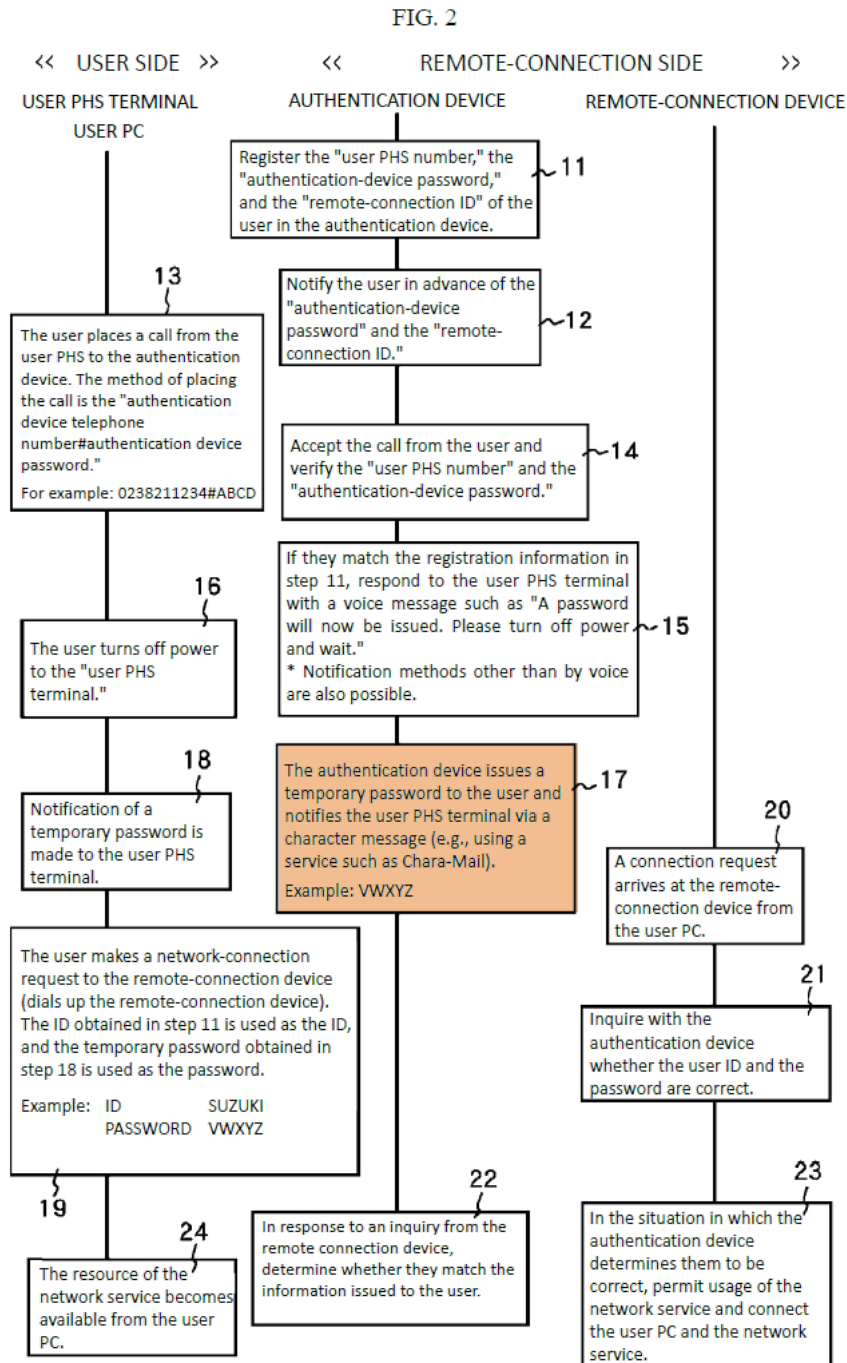
- d. **1[c]: “generating a new password for said first secure computer network based at least upon the token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user;”**

171. In my opinion, Kato in view of Guthrie renders obvious 1[c].

172. 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.*

173. Kato at step 17 in Figure 2 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. Kato, [0002], [0020], [0022].



Id., FIG. 2.

174. 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 Kato’s architecture is 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.

175. 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 VIII.B.1.d).

176. A person of ordinary skill in the art 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 person of ordinary skill in the art would have been motivated to make this modification of replacing Kato’s temporary password with Guthrie’s unique response because doing so would prevent eavesdroppers and portable device thieves from simply 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. *See above* Section IX.A.

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

177. In my opinion, Kato in view of Guthrie renders obvious 1[d].

178. Kato discloses setting a temporary password associated with the user as the password required to authenticate access to the secured 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.

179. As explained for 1[c] (Section IX.B.1.d), Kato’s authentication device issues a temporary password to the user 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. Kato, 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 VIII.B.1.e). Guthrie, 10:55-58.

180. A person of ordinary skill in the art would have been motivated to incorporate Guthrie’s challenge-response, including its “*new password*,” in place of Kato’s temporary password for the reasons explained in Section IX.A.

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

181. In my opinion, 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.

182. *First*, Kato discloses generating a one-time or temporary password, as explained for 1[c]. Kato, Abstract; *see above* Section IX.B.1.d. A person of ordinary skill in the art 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 person of ordinary skill in the art 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.

183. *Second*, in step 660 of Figure 7D, Guthrie discloses setting a response valid timer with the generation of a challenge and response. Guthrie, 10:50-55. A person of ordinary skill in the art would have understood that this activates the user

account by allowing the user to use the response for gaining access to the server if the response is received within the period set by the response valid timer.

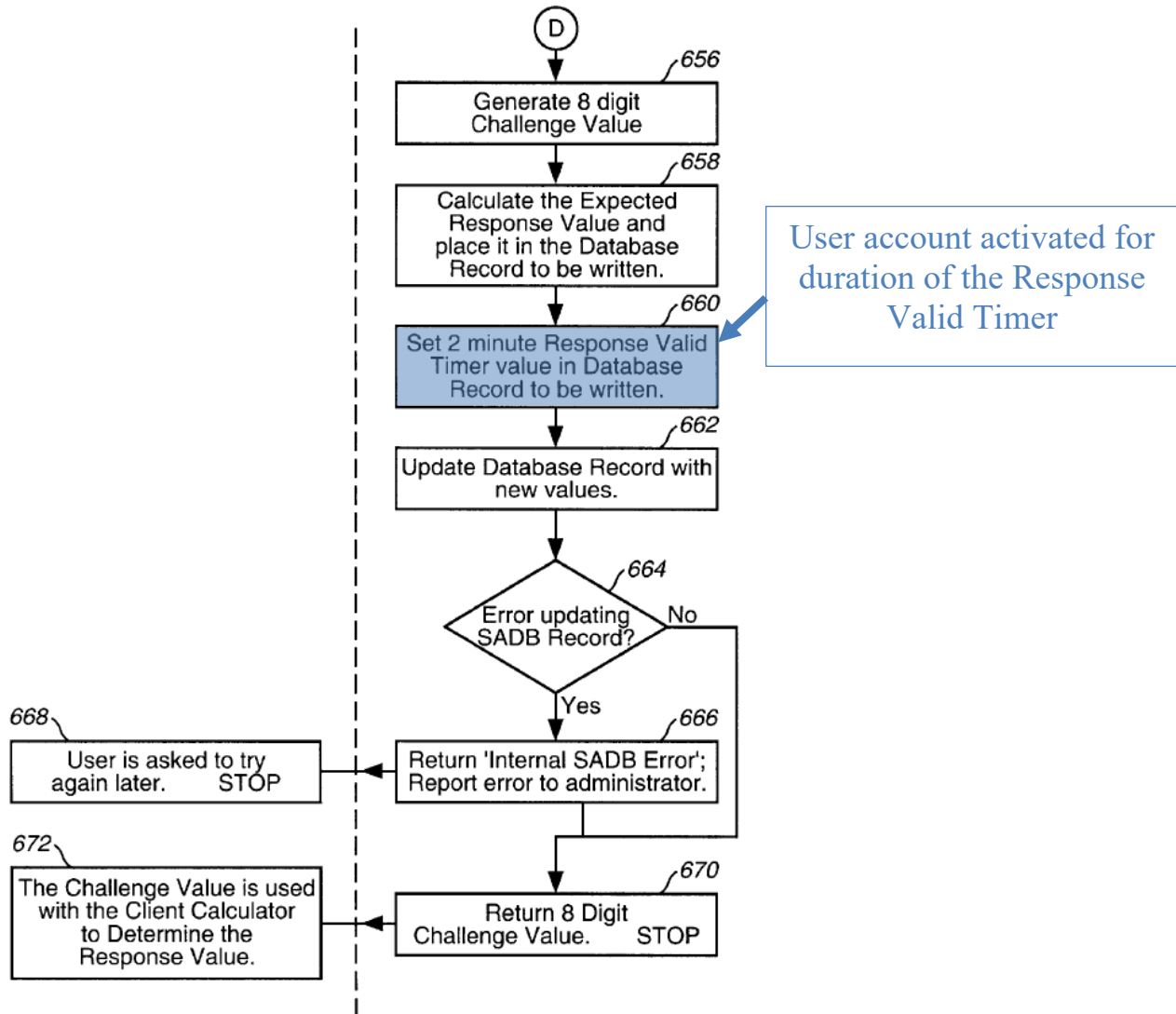


FIG. 7D

Guthrie, FIG. 7D.

184. In my opinion, a person of ordinary skill in the art 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 person of ordinary skill in the art 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. Indeed, setting a time limitation for activating access to a user account was well known and conventional to increase security in authentication. *See* Veneklasen, 7:8-41; Aziz, 6:61-7:15; Schmitz, 8:53-59; Kew, 8:25-9:3. And a person of ordinary skill in the art 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.

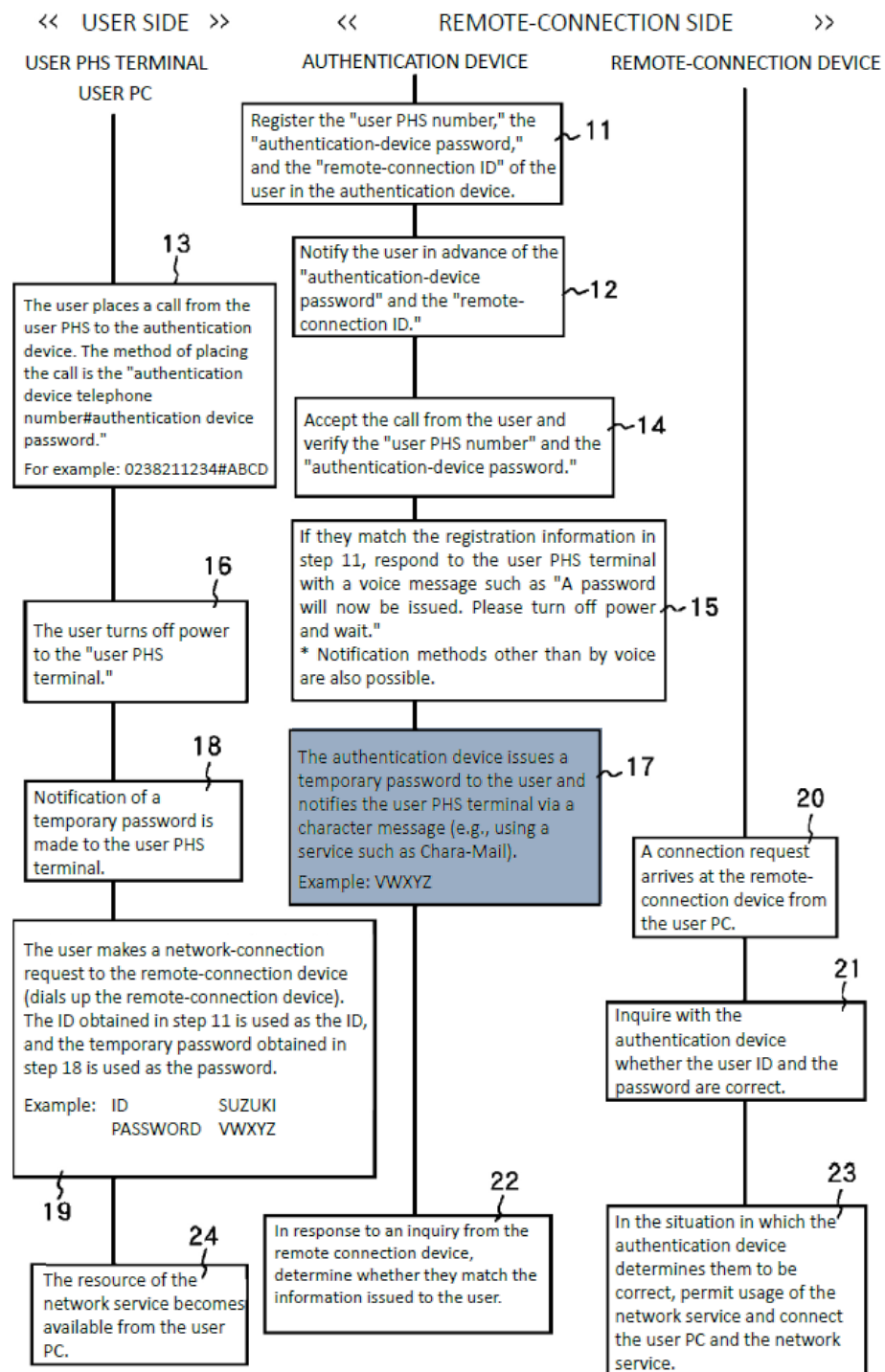
g. 1[f]: “transmitting the token to the personal communication device;”

185. In my opinion, Kato in view of Guthrie renders obvious 1[f].

186. 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.

187. In step 17 of Figure 2, 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].

FIG. 2



Id., FIG. 2.

188. 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, as explained for Ground 1 (Section VIII.B.1.g).

189. A person of ordinary skill in the art would have incorporated Guthrie's challenge-response process into Kato such that Kato's authentication device transmits the Guthrie's challenge ("*token*") to the user PHS terminal ("*personal communication device*") for the reasons explained in Section IX.A.

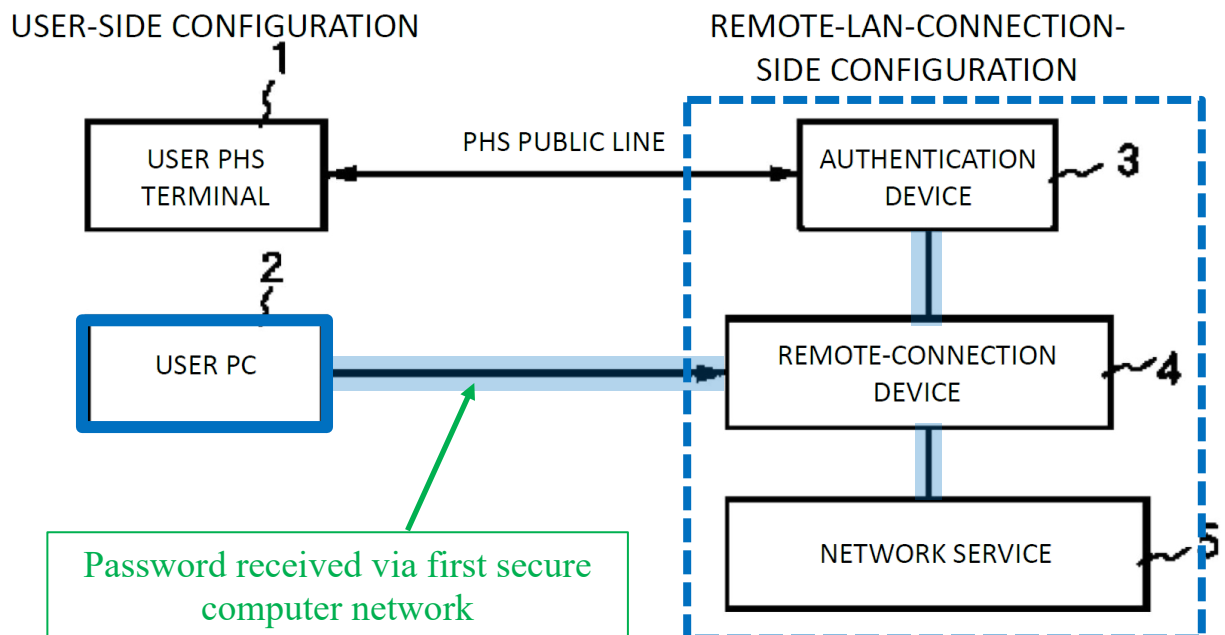
h. 1[g]: "receiving the password from the user via the first secure computer network; and"

190. In my opinion, Kato in view of Guthrie renders obvious 1[g].

191. Kato discloses the architecture of having three separate devices—a user PC for accessing a secured computer system, a user communication device for receiving a temporary password, and a secure computer network, as explained for 1[preamble] and 1[a]. *See above* Sections IX.B.1.a-IX.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]. *See above* Sections IX.B.1.d-IX.B.1.e. As combined, a person of ordinary skill in the art would have understood that Guthrie's password would be entered by the user to be received via Kato's first secure computer network.

192. 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 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].

FIG. 1



Id., FIG. 1.

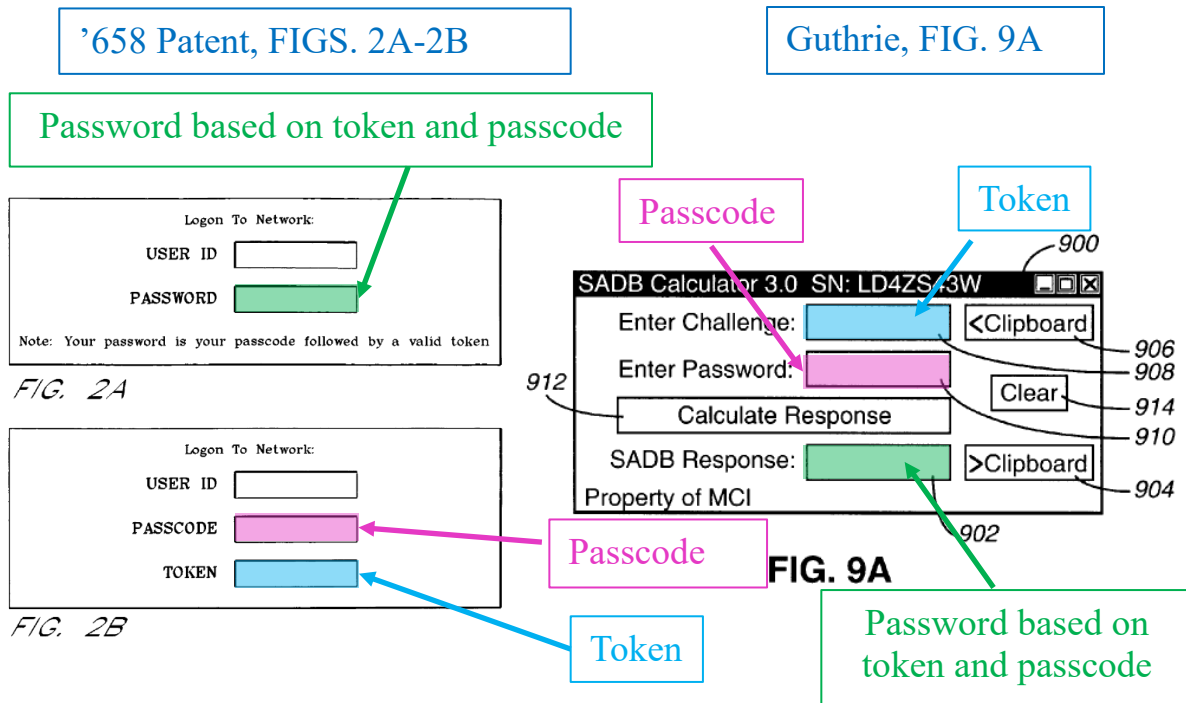
193. As explained for 1[c]-1[d], however, Kato does not disclose the claimed password, but Guthrie does, as explained in Ground 1 (Section VIII.B.1.h). As combined, the challenge-response process of Guthrie would be used within the architecture of Kato depicted above, replacing Kato's temporary password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

194. In my opinion, a person of ordinary skill in the art 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.

195. *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; *see also id.*, 12:57-60 ("[T]he user's authentication password must be entered interactively. As a result, human interaction in the authentication process is required.").

196. *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 person of ordinary skill in the art 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 person of ordinary skill in the art would have understood to be 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 person of ordinary skill in the art 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. Indeed, both methods are similar to the examples disclosed in the '658 Patent. Ex. 1001, 4:52-61, FIGS. 2A-2B.



197. In my opinion, a person of ordinary skill in the art 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 for the reasons explained in Section IX.A.

- 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."**

198. In my opinion, Kato in view of Guthrie renders obvious 1[h]. Guthrie discloses deactivating access after two minutes of activating if the expected

response is not received at the server. Guthrie, 10:50-55, 11:50-59; *see above* Section VIII.B.1.i.

199. In my opinion, a person of ordinary skill in the art 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 IX.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 (Section VIII.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.

200. Indeed, setting a time limitation for accessing a secure system was well known and conventional to increase security in authentication. *See Veneklasen*, 7:8-41; *Aziz*, 6:61-7:15; *Schmitz*, 8:53-59; *Kew*, 8:25-9:3. And a person of ordinary skill in the art 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.

2. Claim 5

201. In my opinion, Kato in combination with Guthrie renders claim 5 obvious for the same reasons as explained for claim 1, aside from its hardware components and software modules, which are separately addressed below.

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

202. In my opinion, 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].

b. **5[a]: “a computer processor;”**

203. In my opinion, Kato at least suggests 5[a] because it discloses an authentication device that performs computing functions a person of ordinary skill in the art 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[y]ing 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 ... remote-connection ID

Kato, [0008]. A person of ordinary skill in the art 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.

- c. **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;”**

204. In my opinion, Kato alone or in combination with Guthrie renders obvious 5[b]. Kato discloses “*associate[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]. *See above* Section IX.B.1.b. A person of ordinary skill in the art would have understood that to associate a user with a personal communications 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.

205. 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, shown in account table 200 in Figure 6 below, in a user account

database 120, as explained for Ground 1 (Section VIII.B.2.c). Guthrie, 5:35-47, 7:64-8:6.

206. In my opinion, a person of ordinary skill in the art 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 person of ordinary skill in the art 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. *Id.*

- d. **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,”**

207. In my opinion, Kato in combination with Guthrie renders obvious 5[c] for the reasons explained for 1[c] and because Guthrie's discloses a “*control module*,” as explained for Ground 1. *See above* Sections IX.B.1.d, VIII.B.2.d.

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

208. In my opinion, Kato in combination with Guthrie renders obvious 5[d] for the reasons explained for 1[d] and because Guthrie discloses a “*control module,*” as explained for Ground 1. *See above* Sections IX.B.1.e, VIII.B.2.e.

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

209. In my opinion, Kato in combination with Guthrie renders obvious 5[e] for the reasons explained for 1[f] and because Guthrie discloses activating access “*in response to the password*” and a “*communication module,*” as explained for Ground 1. *See above* Sections IX.B.1.g, VIII.B.2.f. A person of ordinary skill in the art 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 person of ordinary skill in the art 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]: “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,”**

210. In my opinion, 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. *See above* Sections IX.B.1.a-IX.B.1.b, IX.B.1.h, VIII.B.2.g.

- h. 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.”**

211. In my opinion, Kato in combination with Guthrie renders obvious 5[g]. Kato in view of Guthrie teaches that Guthrie’s authentication module “*activates access [to] the user 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]. *See above* Sections IX.B.1.f, IX.B.1.i.

C. Dependent Claims

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

212. In my opinion, Kato in view of Guthrie renders obvious claim 2, for reasons explained for Ground 1. *See above* Section VIII.C.1.

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

213. In my opinion, 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” capable of making mobile telephone calls and receiving text data. Kato, [0002], [0025], FIGS. 1-2.

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.”

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

214. 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]. *See above* Sections IX.B.1.c-IX.B.1.d, IX.B.2.d, IX.B.2.f.

X. CONCLUSION

215. For the reasons set forth above, in my opinion, a person of ordinary skill in the art as described in paragraph 23 would have considered the Challenged Claims of the '658 Patent to be obvious over the prior art discussed above.

216. In signing this declaration, I understand that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in this case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

217. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: January 3, 2023

By: 

Peter Lawrence Reiher, Ph.D.